Guide d'administration
TWP Version 4.1

Tables des matières

1. Vue d'ensemble 5

1.1. Introduction 5
1.2. Architecture 5
1.2.1. Introduction 5
1.2.2. Configuration Standard 6
1.3. Fonctionnalités 7
1.3.1. Serveur 7
1.3.2. Toolkit 7
1.3.3. Internet 7

2. Installation 9

2.1. Configuration requise 9
2.1.1. Configuration minimale 9
2.1.2. Estimation du volume de stockage requis 9
2.1.3. Environnement 10
2.2. Première installation 11
2.2.1. Applications non supportées 11
2.2.2. Installation 12
2.3. Procédure de mise à jour 15
2.3.1. Mise à jour depuis une version 4.1 15
2.3.2. Mise à jour depuis une version 3.2 15
2.3.3. Réinstallation complète 17

3. Configuration minimale du serveur 19

3.1. Société et domaine 19
3.2. Principales étapes pour valider une installation standard 19
3.3. Première configuration d'un domaine pour une installation standard 24
3.3.1. Récupérer le fichier de licence 25
3.3.2. Installer le fichier de licence 27
3.3.3. Créer un lien PBX 29
3.3.4. Créer le premier utilisateur 31
3.3.5. Créer votre premier groupe d'utilisateurs 33
3.3.6. Ajouter le premier utilisateur à un groupe 34
3.3.7. Donner l'autorisation à l'application Caller 35
3.3.8. Démarrage des Services 37
3.3.9. Installer et tester le Caller 38

4. Lien pour A5000 41

4.1 Généralités 41
4.2. Lien VTI-XML 42
4.3. Lien CSTA 45

5. Gestion des plans de numérotation 47

5.1. Règles standards 49
5.2. Traitement d'un numéro 49

5.3. Règles avancées 50

6. Méthodes d'authentification 53

6.1. Configuration 53
6.2. Authentification Windows 53
6.2.1. Pré requis : avec Contrôleur de domaine 54
6.2.2. Pré requis : sans Contrôleur de domaine 54
6.3. Authentification LDAP 55
6.4. Authentification TWP 56
6.5. Pas d'authentification 57

7. Gestion des utilisateurs 59

7.1. Créer un utilisateur manuellement 59
7.2. Importer des utilisateurs 59
7.2.1. Importer des utilisateurs depuis LDAP 60
7.2.2. Importer des utilisateurs depuis Active Directory 61
7.2.3. La fenêtre d'import utilisateur 63
7.2.4. Autorisations de visualisation des contacts 63
7.3. Gestion des Groupes 64
7.4. Gestion des autorisations 65
7.4.1. Autorisation Applications 66
7.4.2. Autorisation Annuaire 66
7.4.3. Autorisation calendriers 67
7.4.4. Autorisation groupe intercom 68
7.4.5. Autorisation puits d'appels 68
7.4.6. Autorisation Journaux d'appels 69

8. Annuaires et collaboration 71

8.1. Généralités 71
8.2. Synchronisation annuaire – Fusion de contact – Champs spécifiques 75
8.2.1. Synchronisation annuaire 75
8.2.2. Fusion des contacts 76
8.2.3. Champs Spécifiques : Contact VIP 76
8.2.4. Champs Spécifiques : liste rouge 77
8.3. Création d'un connecteur LDAP 79
8.4. Création d'un annuaire ODBC 81
8.4.1. Connecteur 81
8.4.2. Champs 82
8.4.3. Exemples de connecteurs ODBC 84
8.5. Configuration connecteur Lotus 85
8.5.1. Configuration connecteur public Lotus 85
8.5.2. Configuration connecteur privé Lotus 85
8.5.3. Connecteur Calendrier 88
8.5.4. Configuration du serveur Lotus 88
8.6. Annuaires / Calendrier MS Exchange 2003/2007 95
8.6.1. Création d'un connecteur annuaire public 96
8.6.2. Connecteur Calendrier 99
8.7. Annuaires / Calendrier MS Exchange 2010 / Office 365 100
8.7.1. Création du connecteur public / privé 100
8.7.2. Astuce Exchange 2010 : connecteur public avec sélection de dossier(s) 103
8.7.3. Astuce Office 365 : annuaire privé en public 104
8.7.4. Connecteur Calendrier 104
8.7.5. Comptes de connexion des connecteurs privés 105
8.7.6. Configuration serveur Exchange : Accès aux boîtes utilisateur (contacts privés et calendriers) 105

8.8. Add-In Client Outlook 110
8.8.1. Prérequis.....110
8.8.2. Installation 111
8.8.3. Configuration 111
8.8.4. Utilisation 112
8.8.5. Maintenance 113
8.9. Intégration Google Apps 114
8.9.1. Configuration du compte Google Apps 114
8.9.2. Activer les APIs 117
8.9.3. Autoriser les APIs.....118
8.9.4. Configuration des connecteurs dans TWP.....121
8.9.5. Création d'un connecteur annuaire privé.....122
8.9.6. Création d'un connecteur Calendrier.....122

9. Configuration des applications 125

9.1. Configuration du Caller 125
9.1.1. Contacts privés 126
9.1.2. Présence téléphonique - Intercom 126
9.1.3. Présence Calendrier - collaboration 129
9.1.4. Numéro de Messagerie vocale 129
9.1.5. Alerte emails – Configuration SMTP 130
9.1.6. Journaux d'appels d'autres utilisateurs.....130
9.1.7. Fonctionnalités Patron-Secrétaire 131
9.1.8. Toutes les fonctionnalités à activer ou désactiver.....133
9.1.9. Fonctionnalité SMS 136
9.2. Configuration de l'Alerter.....137
9.2.1. Personnalisation et paramètres 137
9.2.2. Configuration de puits d'appels 140
9.3. Configuration d'un Soft phone 143
9.4. Configuration de l'application de Statistiques 145
9.4.1. TWP Stats.....146
9.4.2. TWP Stats Admin 146
9.5. Configuration des automates d'appel pour les applications Rules, Mail, VideoShare.....147
9.5.1. Connexion SIP 148
9.5.2. Configuration des automates d'appel 149
9.6. Configuration de l'application Rules 149
9.6.1. Configuration des automates d'appel 150
9.6.2. Configuration des paramètres Rules 150
9.7. Configuration de l'application VideoShare.....151
9.7.1. Configuration des automates d'appel 151
9.7.2. Configuration des paramètres liés à la conférence Audio – Vidéo et partage d'applications 151

10. Maintenance 153

10.1. Gérer les profils des administrateurs 153
10.2. Paramètres du système et mode Expert.....155
10.2.1. Suppression automatique de données : journaux d'appels 155
10.2.2. Suppression automatique de données : Statistiques 156
10.3. Services 157
10.4. Etat des connexions.....158
10.5. Etat des postes.....159
10.6. Traces 160
10.7. Sauvegarde de la configuration.....161
10.8. Troubleshooting 162
10.8.1 Problème standard 162

11. Annexes 165

11.1. Installation sur Windows 2008 – 2012 x64 165
11.1.1. Paramétrage IIS 165
11.1.2. Paramétrage serveur : Sécurité renforcée d'Internet Explorer et Firewall.....168

1. Vue d'ensemble

1.1. Introduction

TWP Server est une passerelle de téléphonie d'entreprise.

Parfaitement intégrée à votre infrastructure informatique et téléphonie, elle optimise considérablement la productivité et augmente les services disponibles aux utilisateurs. Elle permet d'exploiter toutes les fonctions du PBX, au travers des services Web. Elle vous permet de centraliser la gestion des fonctions de téléphonie.

1.2. Architecture

1.2.1. Introduction

L'architecture TWP est composée des éléments suivants:

- Un serveur qui agit comme une passerelle entre le monde de la téléphonie et le Système d'Information.
- Un PBX ou un réseau avec un accès TCP / IP.
- Poste Client (un ordinateur et un poste téléphonique associé pour chaque utilisateur)

Tous types de postes téléphoniques peuvent être utilisés: numérique, analogique, DECT, IP,

téléphone logiciel… Aucune modification de la configuration du poste de travail n'est requise.

Voici une liste de composants externes, qui peuvent s'intégrer à l'architecture TWP:

- Base de données clients
- Applications métier
- Applications Web
- Annuaire Exchange ou Lotus Notes
- Annuaire PBX
- Applications mobile
- Microsoft (Active Directory, contrôleur de domaine, etc.)
- Annuaire LDAP

1.2.2. Configuration Standard

Le serveur TWP permet de relier la téléphonie (PBX, postes téléphoniques) au réseau informatique d'entreprise (serveurs de données, ordinateurs des utilisateurs…).

1.3. Fonctionnalités

1.3.1. Serveur

L'application TWP Server est utilisée pour:

- Contrôler la téléphonie au travers de Services Web
- Gérer les connexions aux annuaires de l'entreprise (SQL, Exchange, LDAP, ODBC, Lotus)
- Gérer les journaux d'appels entrants et sortants de chaque utilisateur
- Gérer un annuaire inversé
- Gérer la sécurité des droits d'accès aux annuaires
- Définir les droits et services de chaque groupe d'utilisateurs
- Administrer à distance (WEB)
- Gérer le journal d'incidents

1.3.2. Toolkit

TWP est un kit de développement (API) basé sur les Services Web. Ce kit vous permet de développer et intégrer des fonctions de téléphonie de manière transparente dans vos propres applications. Une documentation spécifique et des outils Toolkit sont disponibles sur ce CD- ROM.

1.3.3. Internet

TWP Internet vous permet de fournir la fonction de rappel automatique (fonction double appel transfert).

Voici quelques exemples d'applications:

- "Call Back" bouton de rappel automatique
- E-mail avec bouton de rappel automatique
- gestion de la téléphonie pour le travail à distance

TWP Internet nécessite le développement d'applications Web, ce qui signifie que vous devez disposer d'au moins une licence TWP Toolkit.

2. Installation

2.1. Configuration requise

La configuration requise dépend du nombre d'utilisateurs déclaré ayant accès aux services TWP. Pour toutes configurations, un serveur avec Windows Server 2008 R2 ou Windows Server 2012 est nécessaire.

2.1.1. Configuration minimale

- Avant d'installer TWP, vérifier que la configuration serveur respecte les conditions suivantes :
  - Systèmes d'exploitation :
    - Windows 2008 Server (versions Standard, Enterprise, Web Edition)
    - Windows 2012 Server (versions Standard, Enterprise, Web Edition)
  - Une version 64 bits est indispensable si le module de conférence doit être utilisé

- Internet Information Services (IIS). IIS doit être installé avant TWP server (voir la section ci-dessous pour Windows 2008 Server)

- *Windows 2008 et 2012 Server nécessitent une configuration IIS. La procédure est décrite dans l'annexe, au chapitre 11.1.1.*

2.1.2. Estimation du volume de stockage requis

L'installation standard nécessite un espace disque minimum d'environ 1 Go. Cependant, l'espace disque requis peut augmenter de manière significative selon le nombre d'utilisateurs, le volume des annuaires, le type d'application installée et l'activité du site.

Une zone de stockage de 40 Go sera suffisante dans la plupart des cas, voici les règles visant à déterminer si une zone de stockage accrue est requise:

- Une base de contacts (y compris tous les annuaires, privé et public) avec un total supérieur à 100 000 / 150 000 entrées, selon le nombre de champs qui sont remplis.
- Les applications audio augmentent le volume des données stockées, à un taux minimum de 1 à 2 Ko par seconde d'enregistrement vocal.

2.1.3. Environnement

Droits Windows : les droits administrateur sont nécessaires pour installer et faire fonctionner TWP Server.

Domaine / Groupe de travail : Il existe deux possibilités pour intégrer TWP Server dans l'environnement réseau de l'entreprise:

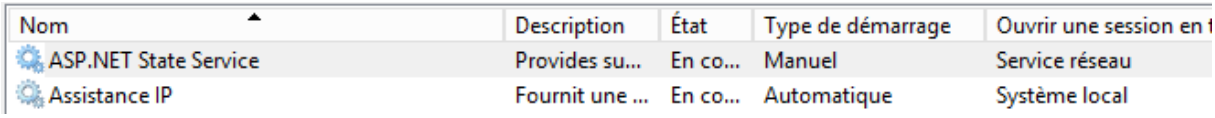
- Domaine : dans ce cas, les droits des utilisateurs sont gérés par le contrôleur de domaine. TWP Server doit être enregistré dans le domaine.
  Groupe de travail: Dans ce cas, les utilisateurs sont directement gérés sur le serveur TWP.

DHCP : L'utilisation d'une adresse IP fixe est obligatoire pour TWP Server.

2.2. Première installation

***Attention**: Vérifier qu'IIS est installé et configuré avant de commencer l'installation. Dans le cas d'une mise à jour ou d'une réinstallation TWP, suivre les indications dans la partie « 2.3 Procédure de mise à jour WP ».*

***Attention**: Vérifier également que le service ASP.NET State Service est bien démarré avant de commencer l'installation.*
Il est possible qu'à partir de Windows Server 2012 SP1 ou de mises à jour Windows Update, ce service soit désactivé. Réactiver-le en faisant un clic droit sur le service, Propriétés, choisir Type de démarrage « Manuel », puis faire OK. Il démarrera de toute façon en fonction d'autres services.



Avant de lancer la procédure d'installation, se connecter sur le serveur en tant qu'administrateur. Vérifier également que le nom de la machine est définitif.

2.2.1. Applications non supportées

TWP Server est installé avec plusieurs services susceptibles d'entrer en conflit avec des applications déjà existantes. Par conséquent, il est déconseillé d'installer les applications suivantes sur TWP Server:

- Contrôleur de domaine
- Microsoft Exchange Server
- N'importe quel serveur web utilisant le port 80 (Apache server, etc.).

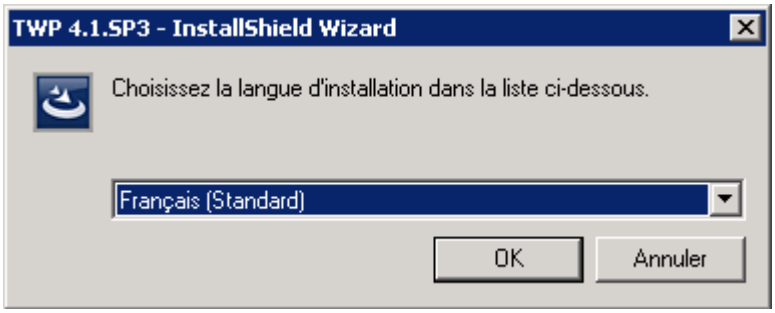
Désinstaller ces applications avant de continuer l'installation.

2.2.2. Installation

Insérer le CD-Rom Server.
Après quelques secondes l'écran ci-dessous s'affichera. S'il ne s'affiche pas, ouvrir le fichier *autorun.htm*.

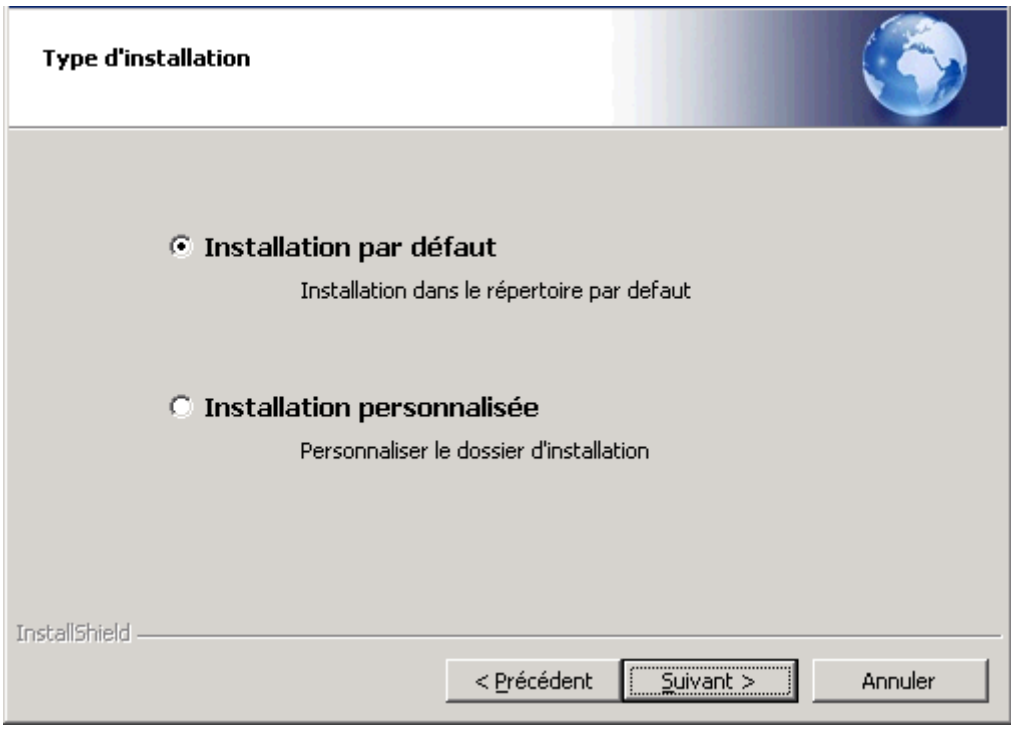
Le menu d'installation apparaît:

Choisir l'option Installer. Choisir la langue.

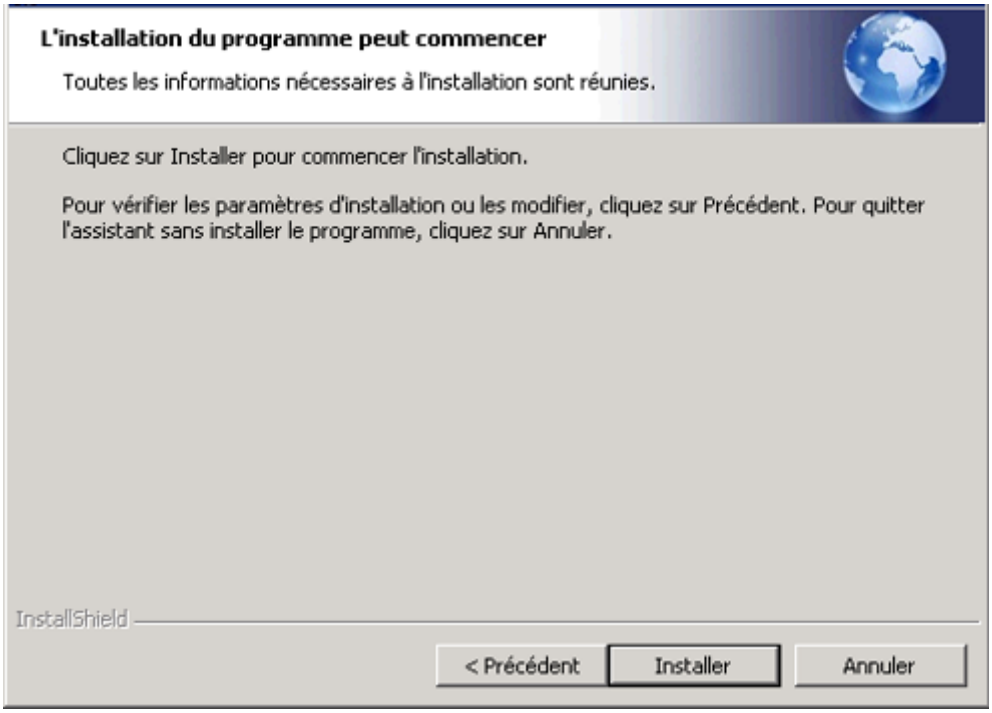


Choisir l'option OK pour lancer l'installation.

Choisir l'option Suivant.



Choisir l'option Installation par défaut pour une installation dans C:\Program Files…
Choisir l'option Installation personnalisée pour choisir le répertoire.



Choisir l'option Installer pour continuer l'installation puis l'option Terminer pour terminer l'installation.

Deux icones sont créés sur le bureau :

- TWP Admin, pour accéder à l'application administration.
- TWP Caller, pour lancer l'application.

2.3. Procédure de mise à jour

2.3.1. Mise à jour depuis une version 4.1

Le CD-Rom d'installation d'une version 4.1 permet également de faire la mise à jour d'une version 4.1 précédente déjà installée, il suffit de suivre la même procédure que l'installation standard (cf. chapitre 2.2.2).

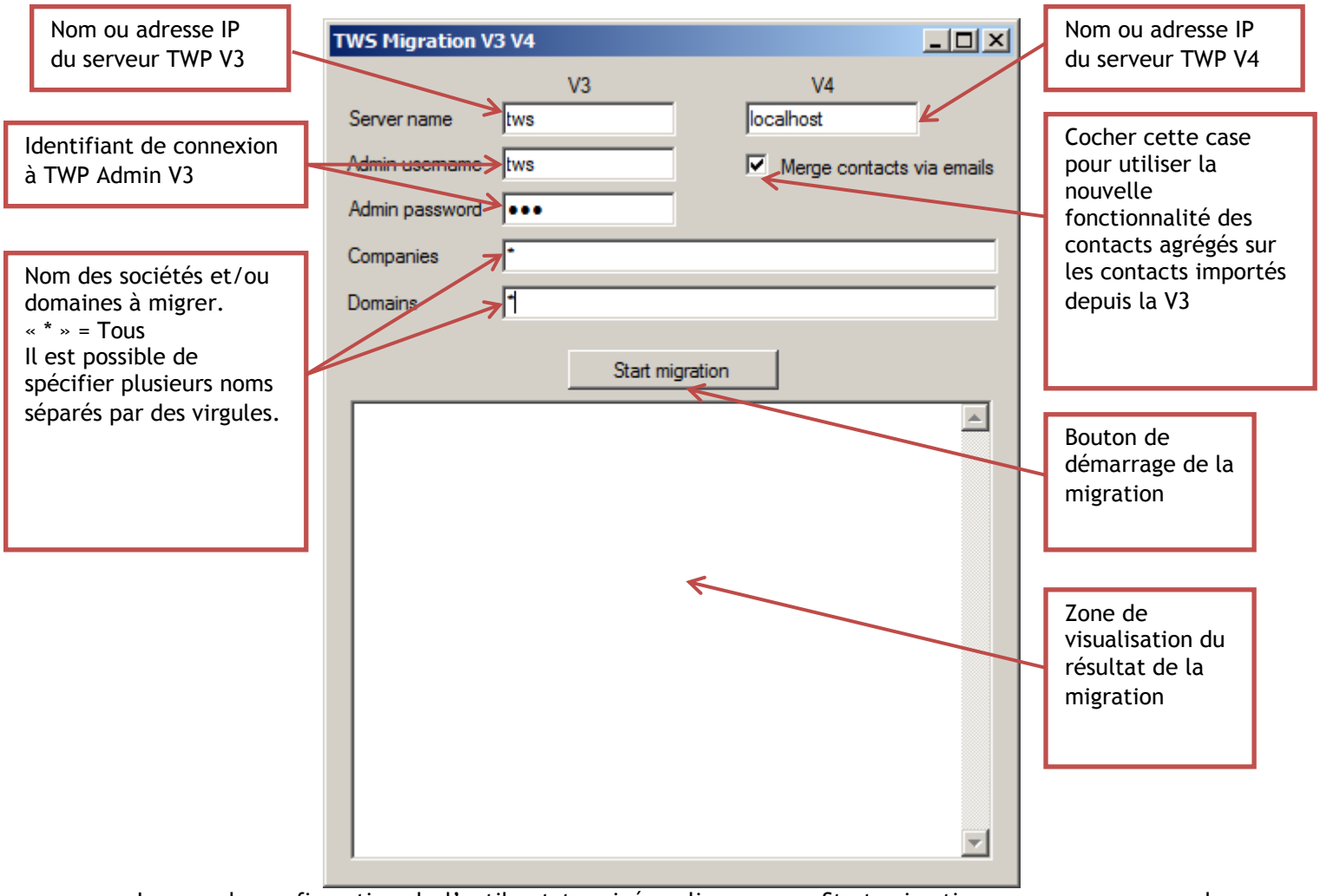
2.3.2. Mise à jour depuis une version 3.2

En cas de mise jour depuis une version 3.2:

- Laisser la version 3.2 installée
- Faire une installation de la version 4.1 (cf. chapitre 2).
- Charger le nouveau fichier de licences dans l'administration v4 (cf. chapitre 3.3.1 et 3.3.2)
- Exécuter l'outil de mise à niveau 3.2 vers 4.1 (cf. paragraphe suivant)
- Arrêter tous les services de la version 3.2 et désactiver les

Le logiciel de migration se trouve dans le répertoire d'installation de TWP 4.1 :
« \TWS4\TWS_Tools\TWS_Migration_V3_V4 ».

Lancer l'exécutable nommé : « TWS_Migration_V3_V4.exe ».



Lorsque la configuration de l'outil est terminée, cliquer sur « Start migration » pour commencer la migration.

/!\ ATTENTION. Toutes les données présentes sur le serveur V4 seront effacées. Le serveur V3 n'est pas modifié par cette procédure.

Les données migrées de la V3 sont :

- Les utilisateurs de l'administration TWP
- Les sociétés
- Les domaines
- Les liens PBX
- Les groupes d'automates
- Les puits d'appels
- Les serveurs de collaboration
- Les groupes intercom
- Les annuaires et leurs contacts
- Les utilisateurs TWP et leur poste
- Les groupes
- Les autorisations
- Les listes de contacts
- Les règles de renvois

Voici un exemple de résultat de migration correct :

```
------------ START --------------
```

```
Initialization...done
Dropping existing V4 databases...done
Authenticating on V3... done
Authenticating on V4... done
Creating admin users... 1 done
Creating applications... 20 done
Creating companies... 1 done
Creating domains... 1 done
Creating pbx links... 2 done
Creating directories... 7 done
Creating groups... 1 done
Creating users... 1 done
Creating bots groups... 1 done
Creating phone queues... 1 done
Creating scripts... 2 done
Creating collaboration servers... 0 done
Creating intercom groups... 0 done
Creating mail servers... 0 done
Creating SMS providers... 0 done
Creating Telenor links... 0 done
Creating callback groups... 0 done
Creating directory servers A5000... 1 done
Creating directory servers Intelligate... 0 done
Creating RCC connections... 0 done
Creating email configurations... 3 done
Creating authorizations... 14 done
Creating contacts... 3046 done
Indexing contacts... done
Set 'None' Authentication... Done
Importing user data...
1 users concerned
2 contacts lists done
6 personal contacts done
0 personal contacts not found
0 personal contacts failed
1 rules found
1 rules + 0 VM rules created
-------------- END ---------------
```

N.B. : Quel que soit le résultat de la migration depuis une version 3.2, il sera utile de :

- Redémarrer le service TWS4$TWS_VTIXMLServices pour la supervision des groupes intercoms
- Configurer comme il se doit les postes des utilisateurs en soft phone dans l'administration (voir chapitre *9.3*)

2.3.3. Réinstallation complète

Avant de commencer l'installation, pour des raisons de sécurité, il est recommandé d'effectuer une copie de sauvegarde de la configuration actuelle (voir chapitre 10.7.)

Désinstallation

1. Depuis le panneau de configuration lancer la désinstallation du Serveur
2. Effacer tous les fichiers dans C:\program files\tws4

Puis réinstaller comme décrit dans le *chapitre 2.2.2*.

3. Configuration minimale du serveur

3.1. Société et domaine

Le serveur TWP peut être partagé entre les entreprises, qui sont totalement indépendantes les unes des autres.

Nota: il n'est pas possible de partager les ressources entre les entreprises.

Chaque domaine est rattaché à une entreprise. Un domaine est un groupe d'utilisateurs qui sont dans la même entreprise avec un environnement technique identique.

Il est nécessaire de créer plusieurs domaines si:

- Les utilisateurs ne sont pas raccordés au même PBX.
- Les utilisateurs ne sont pas connectés au même serveur de messagerie ou calendrier.

Même en ayant plusieurs domaines, certaines informations peuvent être partagées entre eux :

- Annuaires.
- Présence Téléphonique.
- Présence
- Présence Calendrier

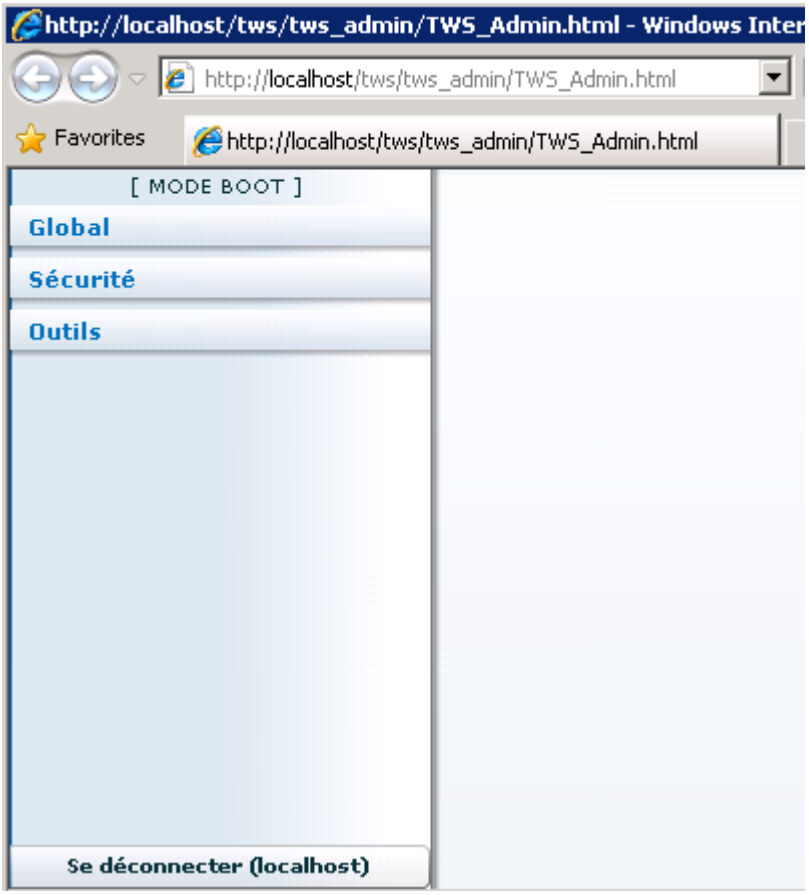
3.2. Principales étapes pour valider une installation standard

Sur le bureau du serveur, cliquer sur le raccourci TWP_Admin. La fenêtre d'identification apparaît comme ci-dessous.

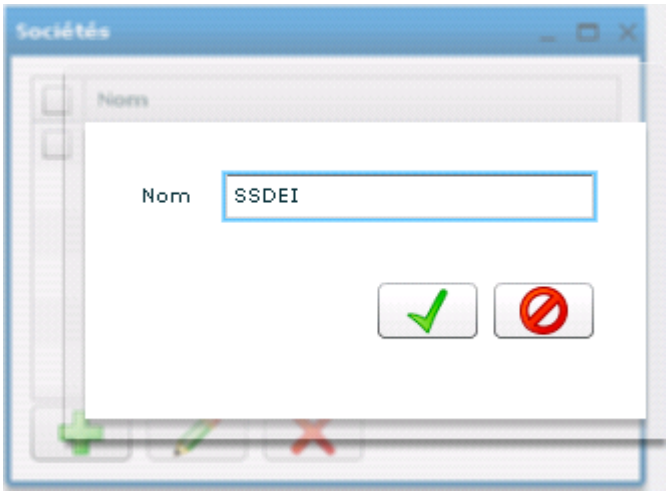
Pour accéder aux pages d'Administration TWP, accéder à l'URL suivante:
http://servername/tws/tws_admin/TWS_Admin.html

Le nom d'utilisateur par défaut est "tws" et le mot de passe par défaut est "tws".

Une fois l'utilisateur et le mot de passe saisis, cliquer sur Go.
Vous entrez dans le « Mode d'initialisation ».

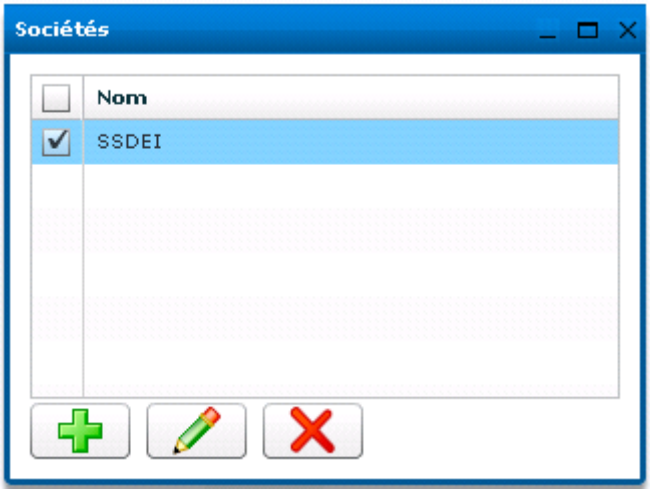


Pour créer une société, sélectionner les menus *Global* / *Sociétés*, puis cliquer sur "+".

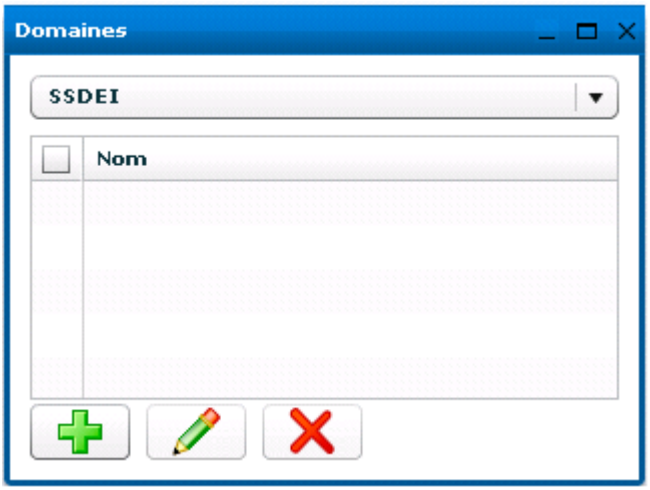


Entrer le nom de la société et cliquer sur le bouton "Enregistrer".

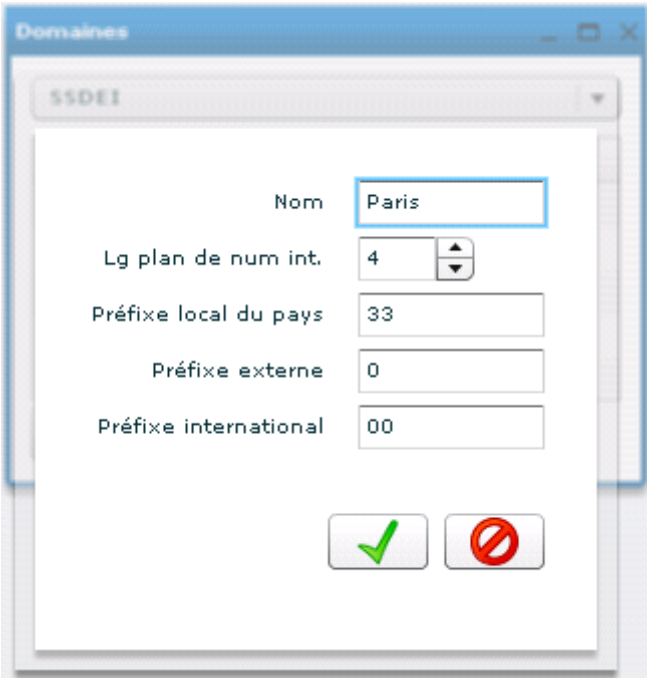
N.B. : Noter bien que ce nom de société sera dans les applications dans la fiche contact des utilisateurs qui seront configurés plus tard.



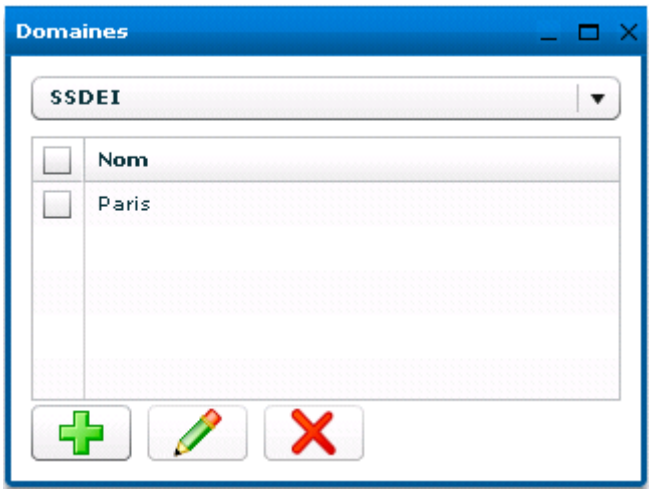
Puis créer un domaine sur cette société, sélectionner les menus *Global* / *Domaines*.
N.B. : Si vous créer plusieurs domaines et sociétés, noter bien que des informations peuvent être partagées entre différents domaines mais aucune entre sociétés.



Sélectionner dans la liste déroulante la société dans laquelle le domaine doit être créé, et cliquer sur le bouton "+".



Entrer le nom de domaine et définir votre plan de numérotation en mentionnant par exemple la longueur du plan de numérotation interne. Cliquer sur le bouton "Enregistrer".

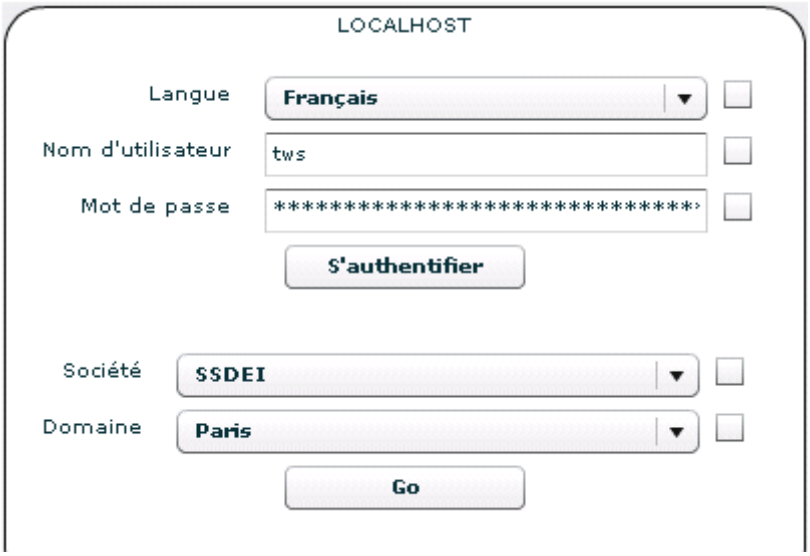


Ici, nous avons créé le domaine « Paris » dans la société « SSDEI ».

Cliquer sur le bouton *Déconnecter* en bas à gauche de l'écran.

3.3. Première configuration d'un domaine pour une installation standard

Sélectionner la société et le domaine à configurer.



Cliquer sur "Go" pour continuer la configuration.

3.3.1. Récupérer le fichier de licence

Afin de pouvoir utiliser la solution et activer les licences de manière définitive, il est nécessaire de se munir de :

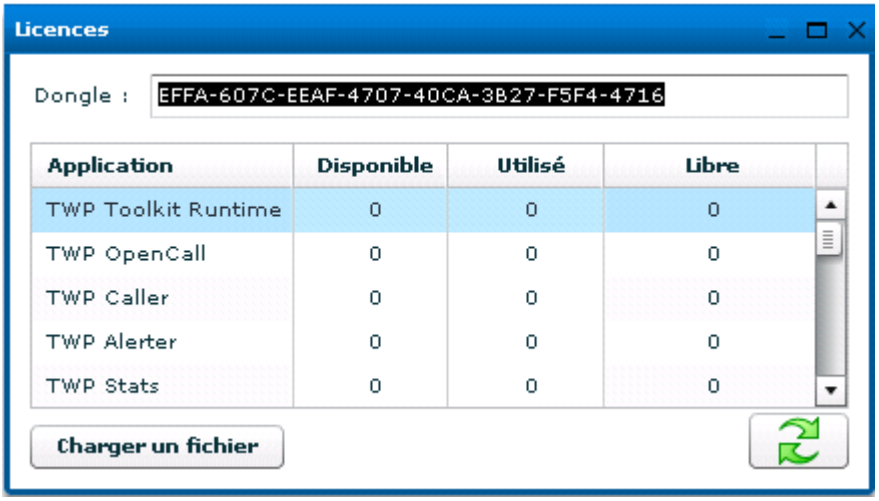
- Numéro de série (Voucher)
- Numéro de Dongle virtuel
- Lien URL d'activation des licences

Récupérer le numéro de Dongle

Sélectionner les menus *Sécurité* / *licences* puis copier le numéro de Dongle qui apparaît comme suit :

Attention : pour les machines virtuelles : Avant de réaliser la manipulation

- Fixer l'adresse MAC de la machine avant de récupérer le numéro de Dongle.
- Environnement VMWare : ne pas renommer l'environnement vSphere Center
- Environnement VMWare : ne pas modifier l'adresse IP de l'environnement vSphere Center



Si aucun numéro de Dongle ne figure sur le formulaire de licences, vérifier si le service Windows TWS4$TWS_WebServices est bien lancé: si ce n'est pas le cas, démarrer ce service et essayer à nouveau. Sinon, contacter votre support.

Récupérer le certificat de licences

Rendez-vous à l'adresse suivante et entrer votre voucher reçu par email, à l'endroit indiqué.

http://register.algoria.fr/Licences/aastra.aspx

http://register.algoria.fr/Licences/

Si le numéro de série (Voucher) n'est pas encore associé à un numéro de Dongle virtuel (DongleID), saisir le numéro de Dongle virtuel, puis cliquer sur « Valider ».

Lorsque le voucher est associé au numéro de Dongle, il est possible de récupérer la licence soit :

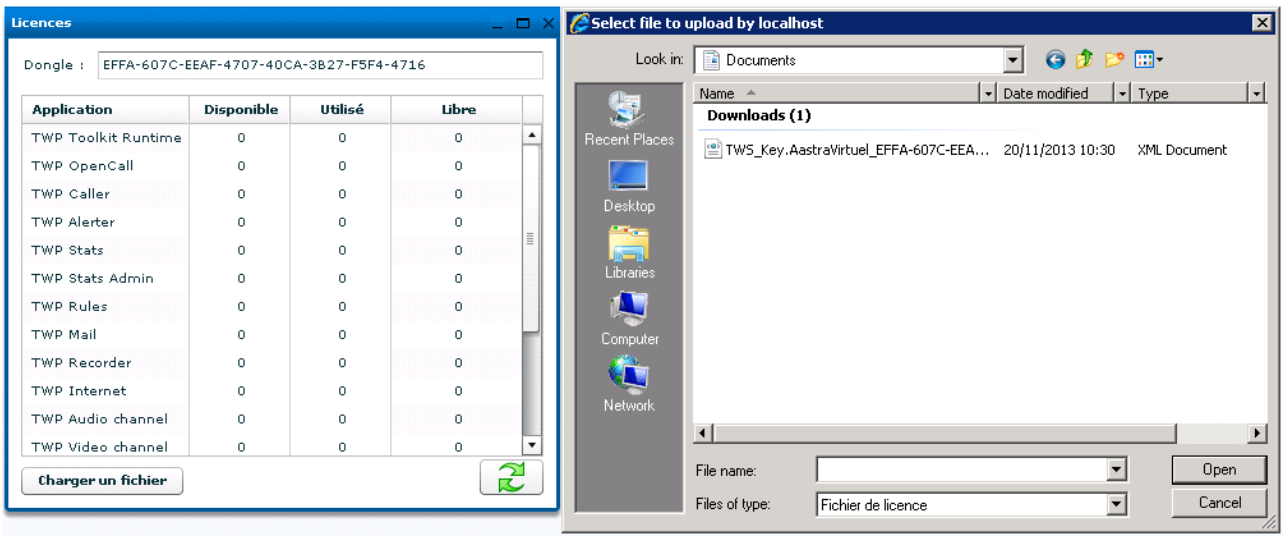
- en téléchargement direct en cliquant sur le bouton « Récupérer la licence »,
- par email en cochant d'abord la case « Par mail », en indiquant une adresse mail et enfin en cliquant sur le bouton « Récupérer la licence ».

Il est possible d'accéder aux détails de votre commande en cliquant sur le bouton « Détails ».

S'il est impossible d'avoir le fichier de licence, contacter le support.

3.3.2. Installer le fichier de licence

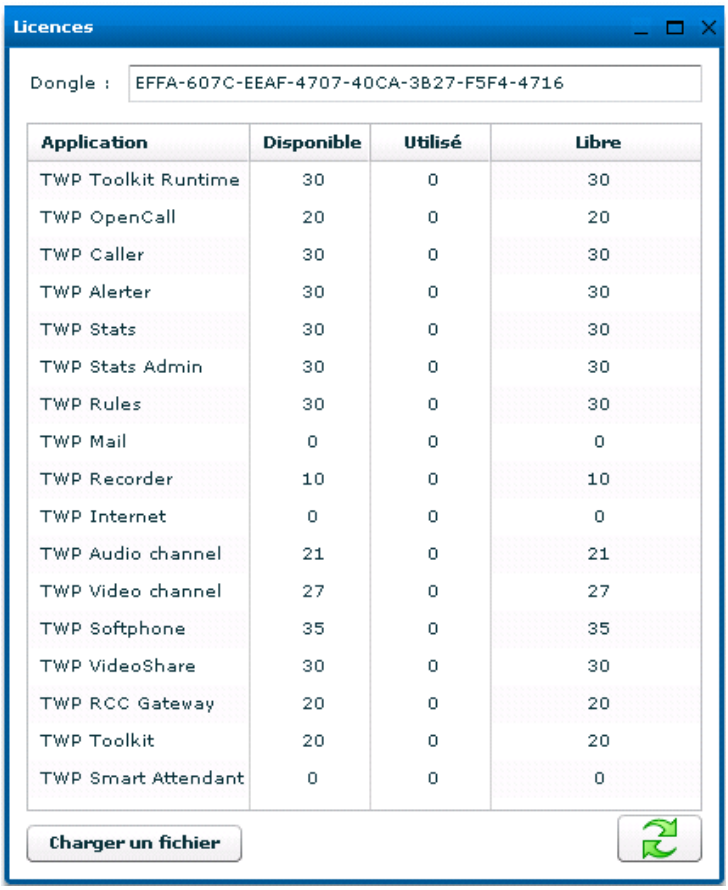
Dans l'administration, sélectionner le menu *Sécurité* / *licences*.



Cliquer sur "Charger un fichier" et sélectionner votre fichier de clé. Les licences commandées par le client doivent apparaitre validées sur cet écran.

Si aucun numéro de Dongle ou aucun certificat ne figurent sur le formulaire de licences, vérifier si le

service Windows TWS4$TWS_WebServices est bien lancé: si ce n'est pas le cas, démarrer ce service et essayer à nouveau. Sinon, contacter votre support.

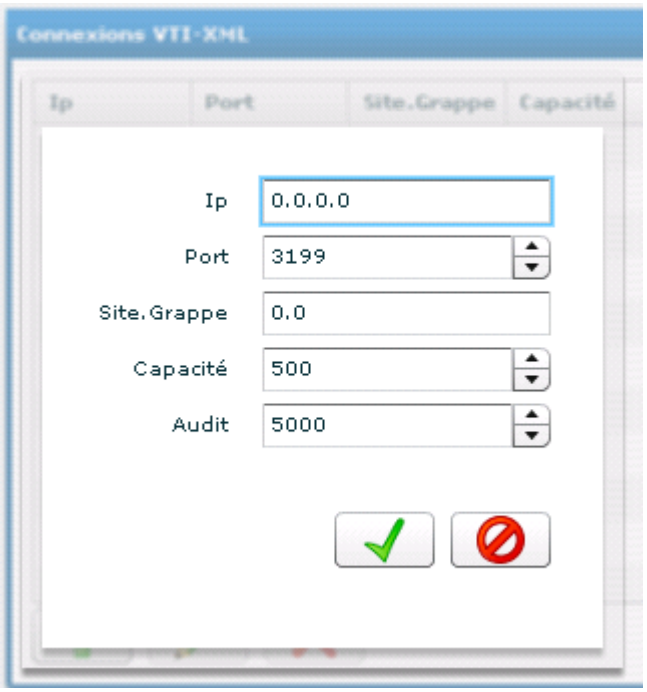


3.3.3. Créer un lien PBX

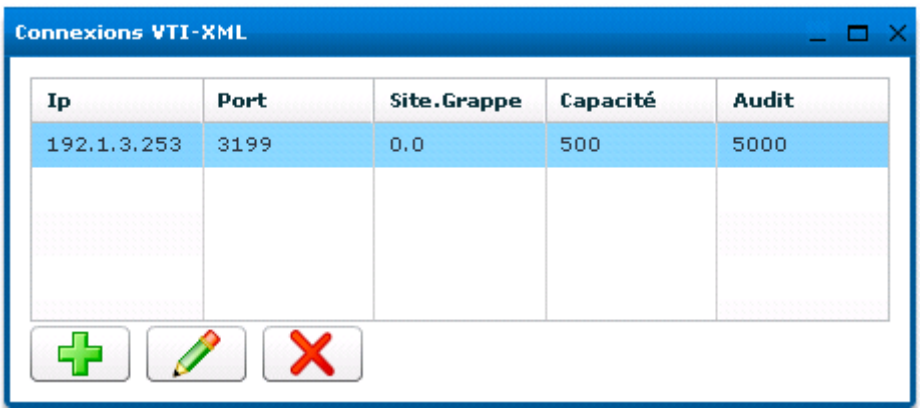
Configurer un lien VTIXML

Sélectionner le menu *Connexions / Connexions VTI-XML*. Cliquer sur le bouton "+" et configurer votre lien

Remplir l'adresse IP de votre IPBX, le port par défaut pour VTIXML est 3199 (ne changer jamais cette valeur).
Il est possible de configurer plusieurs liens VTIXML dans le cadre d'une architecture multi-site/multi-nœud, dans ce cas il est important de mentionner les informations de *Site.Grappe*. Définir alors le nombre de connexions maximum supportées sur chaque lien.



Cliquer sur le bouton "Enregistrer".

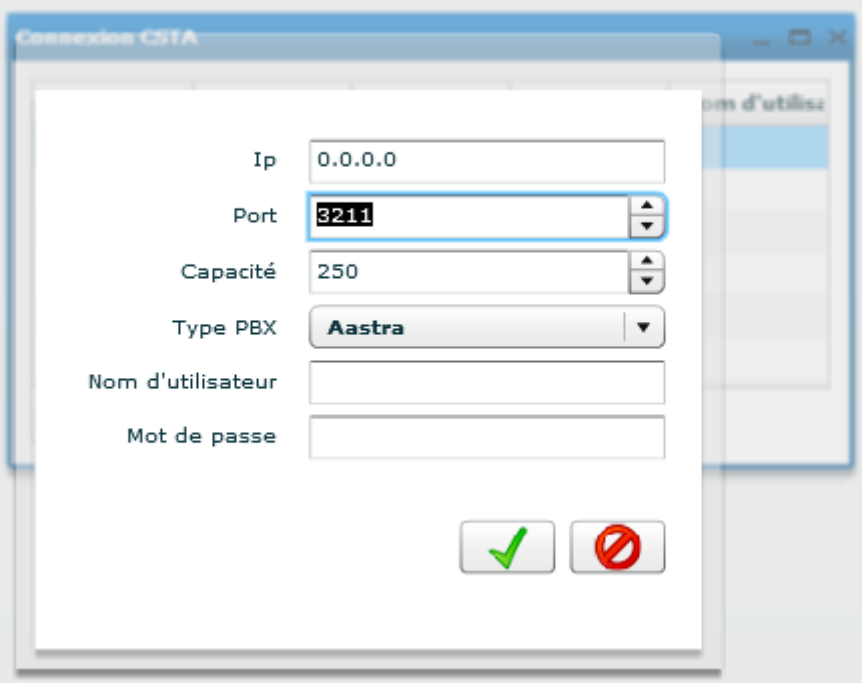


Information: *Redémarrer le service VTI-XML si des changements sont faits.*

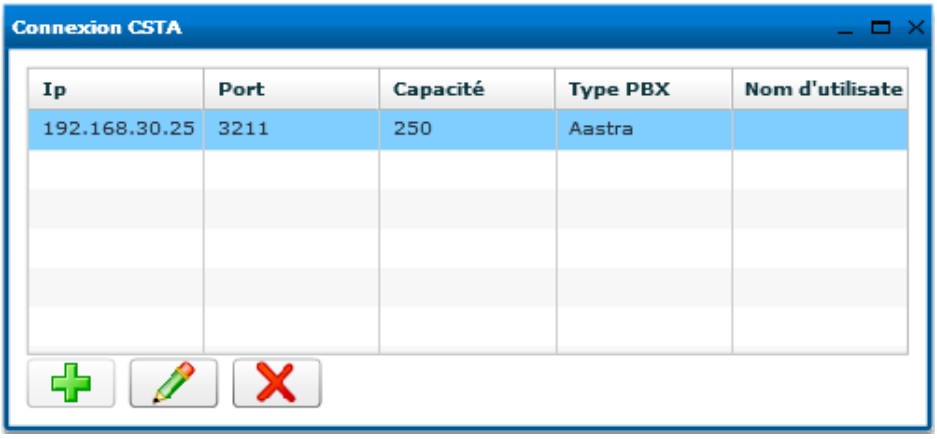
Configurer un lien CSTA

Sélectionner le menu *Connexions* / *Connexion CSTA*. Cliquer sur le bouton "+" et configurer votre lien.

Remplir l'adresse IP de votre IPBX, le port par défaut pour CSTA dépend du type de PBX choisi, définir les nom d'utilisateur et mot de passe dans le cas où il y en a besoin et selon le type de PBX choisi.



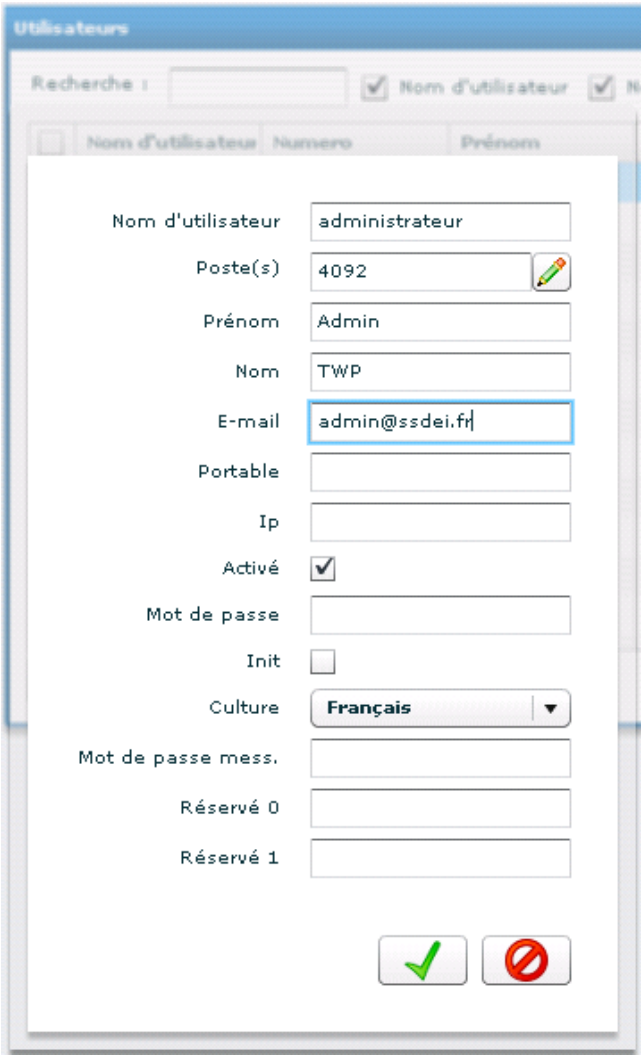
Cliquer sur le bouton "Enregistrer".



***Information**: Redémarrer le service CSTA si des changements sont faits.*

3.3.4. Créer le premier utilisateur

Sélectionner le menu Utilisateurs / Utilisateurs puis cliquer " + "

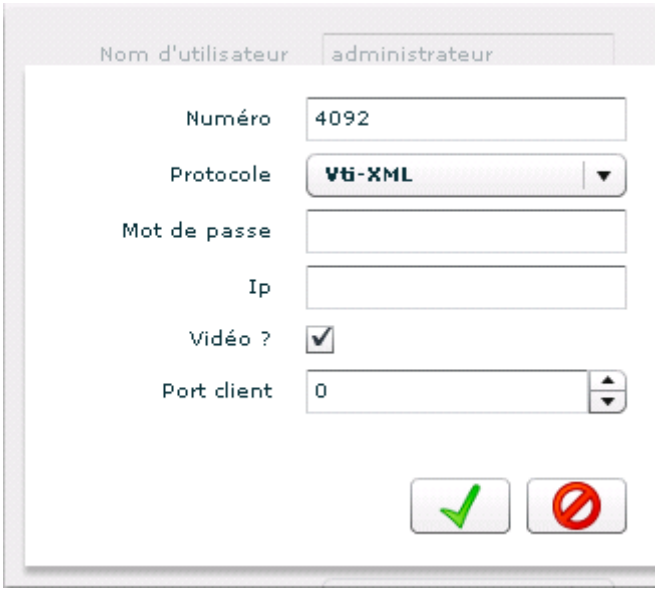


- *Nom d'utilisateur* : Si l'authentification Windows est utilisée, le nom d'utilisateur doit être le login Windows configuré sur le domaine. Sinon, il s'agit du login TWP que l'utilisateur devra saisir pour s'authentifier.
- *Prénom - Nom - Portable*: Informations affichées dans la fiche contact de l'utilisateur et disponibles par recherche
- *E-mail* : l'adresse de messagerie de l'utilisateur est utilisée par plusieurs applications TWP, pour la gestion du statut Présence Calendrier, la messagerie vocale unifiée, et les contacts privés en particulier. Vérifier que les adresses de messagerie sont correctes.
- *Ip* : ne rien renseigner. L'adresse IP qui y est marquée peut être utilisée pour un procédé d'authentification.
- *Activé* : Permet d'activer ou de désactiver un utilisateur
- *Mot de passe* : Si le procédé d'authentification choisi pour l'utilisateur est TWP alors le mot de passe de celui-ci peut être modifié à ce niveau.
- *Culture* : permet de définir la langue choisie par défaut dans les applications de l'utilisateur.

- Le mot de passe de la messagerie vocale est celui de la messagerie vocale PBX.

Définition du poste associé à cet utilisateur :

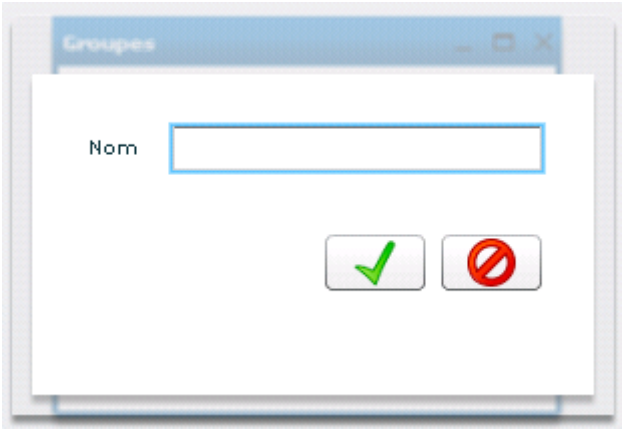
- *Numéro* : Numéro de poste.
- *Protocole* : en fonction du type de supervision qui doit être faite sur votre IPBX: VTIXML- CSTA....
- *Mot de passe* de poste : Non utilisé en CSTA mais important pour la supervision VTIXML
- *IP* : Facultatif, utilisé pour le Recorder
- *Vidéo* : Activation ou non de la vidéo point à point pour l'utilisateur du poste



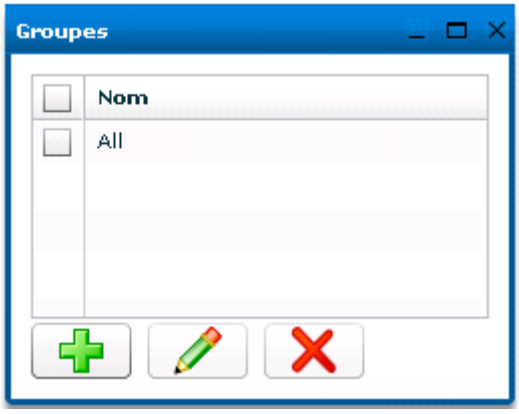
Enregistrer la fiche de poste ainsi que celle de l'utilisateur pour que toute modification soit prise en compte.

3.3.5. Créer votre premier groupe d'utilisateurs

Sélectionner le menu *Utilisateurs* / *Groupes* et cliquer sur “+”

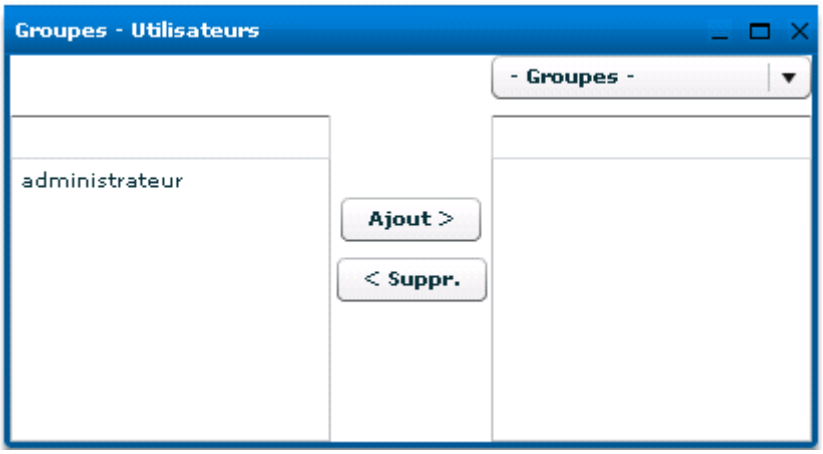


Entrer le nom pour ce groupe: "All" par exemple, et enregistrer.

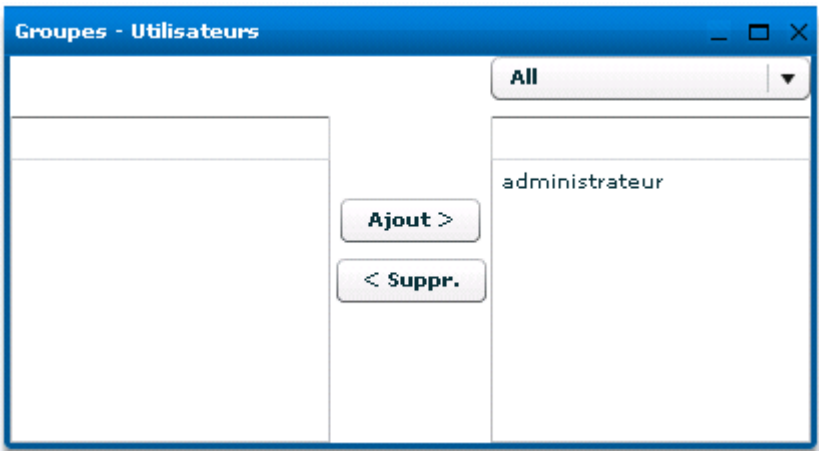


3.3.6. Ajouter le premier utilisateur à un groupe

Sélectionner le menu *Utilisateurs* / *Groupes - Utilisateurs*.



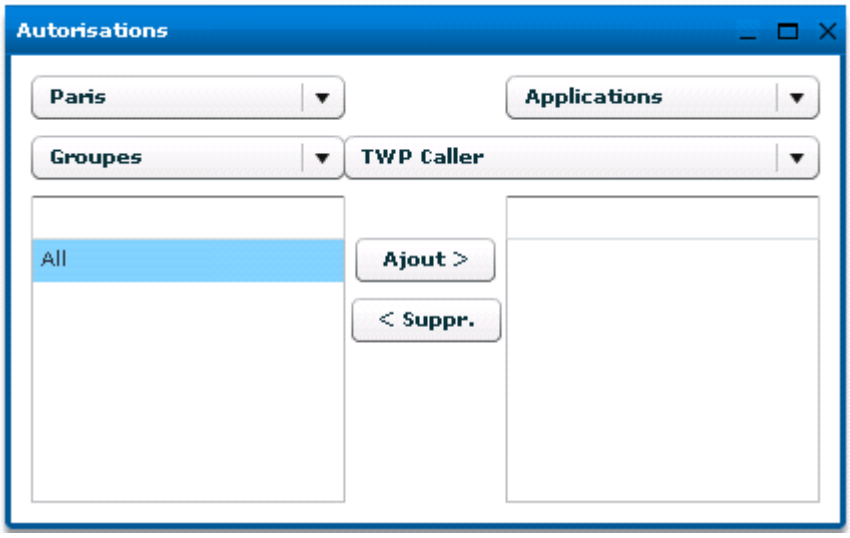
Sélectionner le groupe "All" de la liste déroulante. Ajouter l'utilisateur à ce groupe : sélectionner le nom de l'utilisateur et cliquer sur *Ajouter*.



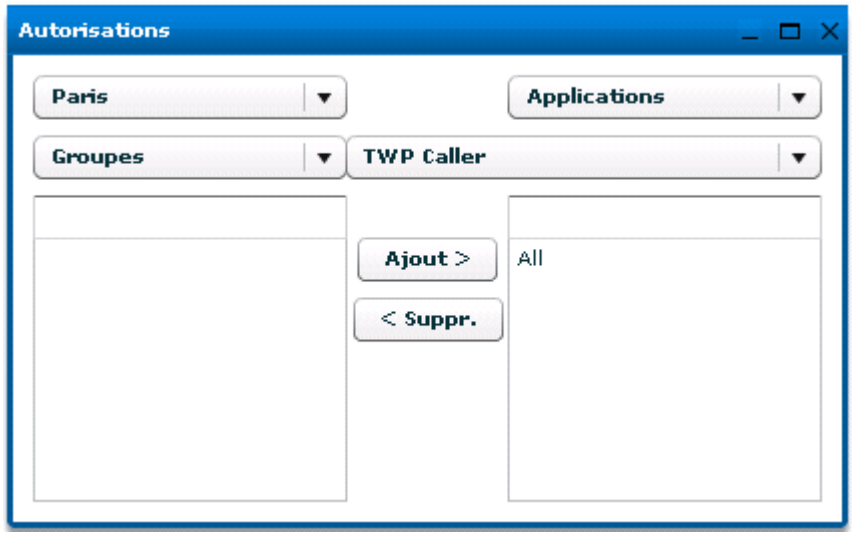
3.3.7. Donner l'autorisation à l'application Caller

Sélectionner le menu *Utilisateurs* / *Autorisations*.

Sélectionner "*Applications*" dans la liste déroulante en haut à droite, puis sélectionner TWP Caller dans la liste déroulante en dessous à droite.

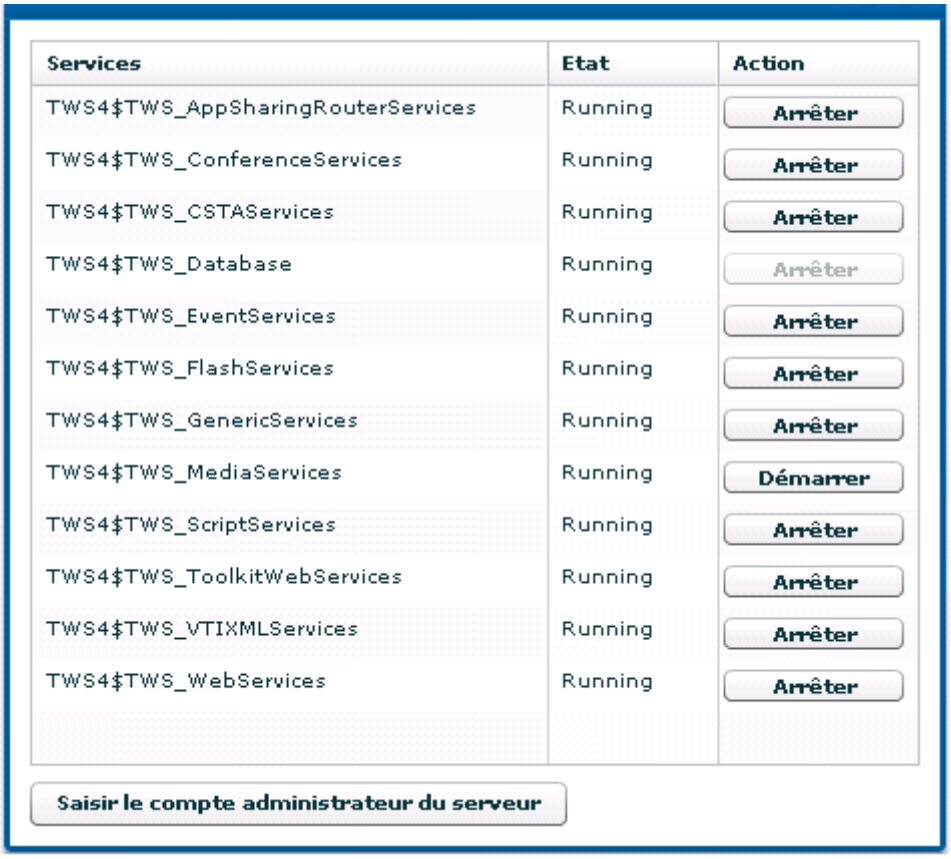


Sélectionner le groupe "All" et cliquer "*Ajouter*", afin que tout utilisateur de ce groupe soit autorisé à exécuter l'application TWP Caller.


Autorisations
Paris
Applications
Groupes
TWP Caller
Ajout >
< Suppr.
All

3.3.8. Démarrage des Services

Sélectionner menu *Outils* / TWP *Services*.



Cliquer sur "*Saisir le compte administrateur du serveur*": Entrer les informations de l'administrateur local de la machine afin de démarrer et arrêter les services Windows depuis cet écran.

Cliquer "*Enregistrer*".

- Démarrer TWS4$TWS_Database
- Démarrer TWS4$TWS_GenericServices, les autres services seront lancés automatiquement

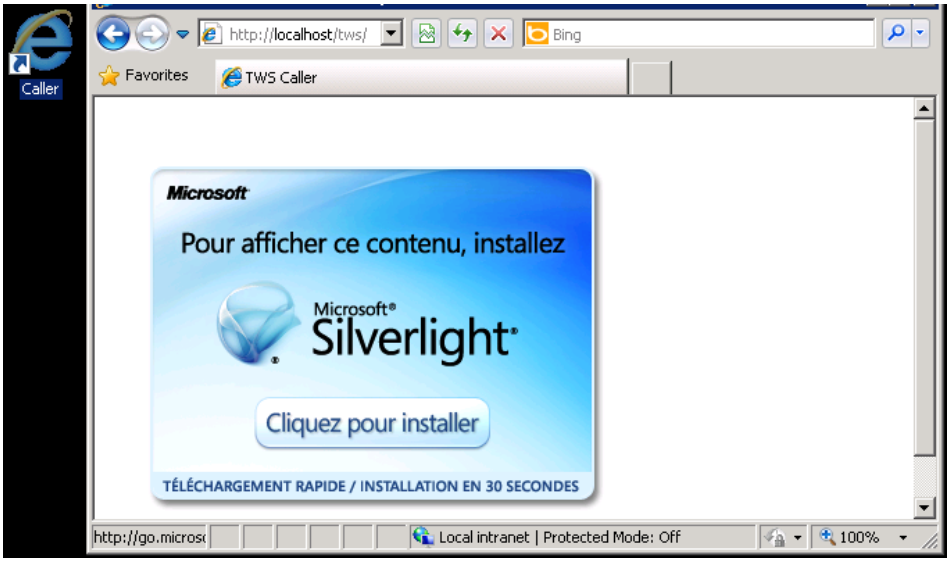
3.3.9. Installer et tester le Caller

Il existe 2 façons d'installer l'application dans les sessions des utilisateurs :

- TWP _Launcher.msi : cet outil d'installation permet déployer automatiquement ou manuellement dans les sessions Windows des utilisateurs TWP Caller.
  Par contre, il n'y a pas d'installation automatique de Microsoft Silverlight. Il doit être au préalable installé.
  La documentation TWP _Launcher.pdf est réservée à la description de cet outil d'installation.

- Installation via l'URL http://nomduserveur/tws/ sur différents navigateurs compatibles avec Silverlight (voir le tableau de compatibilité : https://www.microsoft.com/getsilverlight/get-started/install/default.aspx).
  Windows 10 : L'installation se fait via Internet Explorer installé par défaut.
  Mac OS : L'installation peut se faire via Safari moyennant une configuration (voir la documentation d'utilisation TWS) ou Mozilla Firefox.

Cliquer sur le raccourci "TWP Caller" sur le bureau du serveur. Une page web s'ouvre.



Celle-ci vous permet d'installer Silverlight si nécessaire, et dans ce cas rafraichir la page pour ensuite de démarrer TWP Caller.

L'application doit se lancer et le nom d'utilisateur et son numéro de poste associé doivent être visibles dans la barre de titre.

Vous êtes maintenant prêts à tester votre premier appel avec TWP Caller. (Voir guide d'utilisateur TWP Caller)

4. Lien pour A5000

4.1 Généralités

Afin de contrôler les fonctions de téléphonie de l'abonné, le serveur établit des liens de supervision CTI avec un IPBX ou un réseau de d'IPBX A5000. Selon les abonnés et l'usage prévu, deux types de protocole peuvent être utilisés: CSTA (standard ECMA) et VTI-XML (protocole propriétaire AASTRA).

TWP peut établir un lien CSTA et plusieurs liens VTI-XML simultanément avec un réseau de PBX par domaine. Chaque lien multiplexe la supervision de plusieurs abonnés. Chaque lien est limité dans le nombre maximum de supervisions permanentes selon son type et les caractéristiques de la connexion avec le PBX.

***Attention**: Consultez l'ICM AASTRA pour connaître les contraintes techniques liées aux capacités de liaison, selon la version de logiciel de /'A5000 ainsi que les conseils d'interface.*

Afin d'être en mesure de servir un grand nombre d'utilisateurs, TWP implémente un mécanisme de lien VTI-XML multiples, permettant de cumuler chaque capacité.

***Attention**: un lien est suffisant quand le nombre total d'abonnés VTI-XML ne dépasse pas la capacité d'un lien et que l'architecture est mono-site ou multi-sites / mono-nœud.*

Plusieurs liens doivent être créés quand le nombre total d'abonnés VTI-XML dépasse la capacité d'un lien ou l'architecture est multi-site / multi-nœud.

L'algorithme d'allocation des supervisions d'abonnés aux liens VTI-XML fonctionne selon plusieurs modes:

- Le mode explicite : pour chaque lien utilisé sur une grappe, l'administrateur désigne les sites pour lesquels les abonnés doivent être supervisés par ce lien.
    - Si plusieurs liens explicites sont possibles pour un site/grappe donné, TWP distribue les supervisions en remplissant les liens les moins chargés en premier
    - Si tous les liens explicites sont saturés, les supervisions débordent sur d'autres liens en remplissant les liens les moins chargés en premier
- Le mode implicite: quand le site/grappe n'est pas explicitement associé à un lien, TWP distribue les supervisions en remplissant les liens les moins chargés en premier.

Ces deux modes peuvent être combinés : une partie des sites/grappes est explicitement associée avec un lien et le reste est associé dynamiquement.

Chaque lien est défini principalement par:

- L'adresse IP du site de connexion
- Le site/grappe associé explicitement avec le lien
- La capacité maximale de la liaison

Il est obligatoire de définir le lien CSTA pour la gestion des renvois d'appels.
Le serveur CSTA configuré sur le PABX doit être dédié au lien avec le serveur TWP.

4.2. Lien VTI-XML

La configuration des différents liens doit respecter les principes d'ingénierie suivants:

- La capacité d'un lien ne doit pas dépasser la capacité maximale du site de connexion (cf. LCI AASTRA)
- La liste des sites/grappes sur le lien doit contenir au minimum le site/grappe du site de connexion
- Au moins un lien doit être créé dans chaque centre d'un multi-centre.
- Il est recommandé que vous créiez un lien vers chaque site/grappe avec une carte IP qui supporte VTI-XML
- La répartition des sites/grappes doit favoriser le plus court "chemin d'accès réseau" de routage
- Dans le cas d'une supervision "du site de transit", la répartition des sites/grappes doit favoriser les sites qui ont la meilleure connexion.

Avant de configurer les différents liens, il est recommandé de remplir un tableau qui permet d'associer le lien et le site/grappe de l'abonné.

		Lien 0	Lien 1	Lien 2
Centre		1	2	3
Site		1.1	2.1	3.1
Capacité		500	250	200
Adresse IP		IP address 1	IP address 2	IP address 3
Site	**Centre**			
1.*	1	500		
2.*	2		250	
3.*	3			100
4.*	3			100

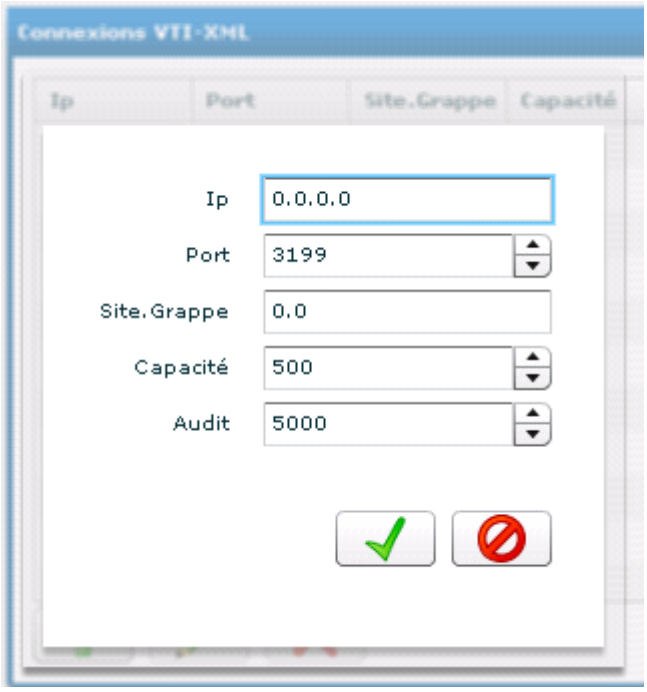
Ici nous voyons que:

- Chaque centre a un lien
- Sites 1, 2 et 3 sont supervisés avec " le plus court chemin d'accès réseau "
- Lien 2, qui est connecté à site 3, permet le routage de la supervision de sites 3 et 4.

Les parties "état des connexions" et "état des postes" sont utilisés pour vérifier la répartition des liens avec les supervisions (voir 10.4. Etat des connexions et voir 10.5. Etat des postes).

Création du lien VTIXML

Le lien VTIXML est utilisé pour surveiller tout type de poste, sauf i2052.
Sélectionnez menu *Connexion / Connexions* VTI-XML, puis cliquez sur le bouton " + "

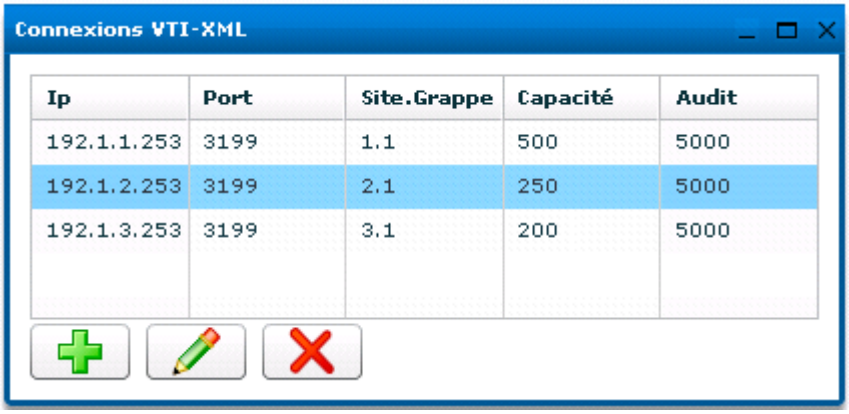


Par défaut, vous devez remplir :

- L'adresse IP de l'IPBX,
- Le site/grappe si vous voulez créer plus d'un lien
- La capacité (voir LCI).

Cliquez sur le bouton enregistrer pour sauvegarder les informations.
***Information**: Vous devez redémarrer le service VTI-XML si vous avez fait des changements*

Dans le cas d'une architecture multi-site et la création de plusieurs liens VTI, voici un exemple :



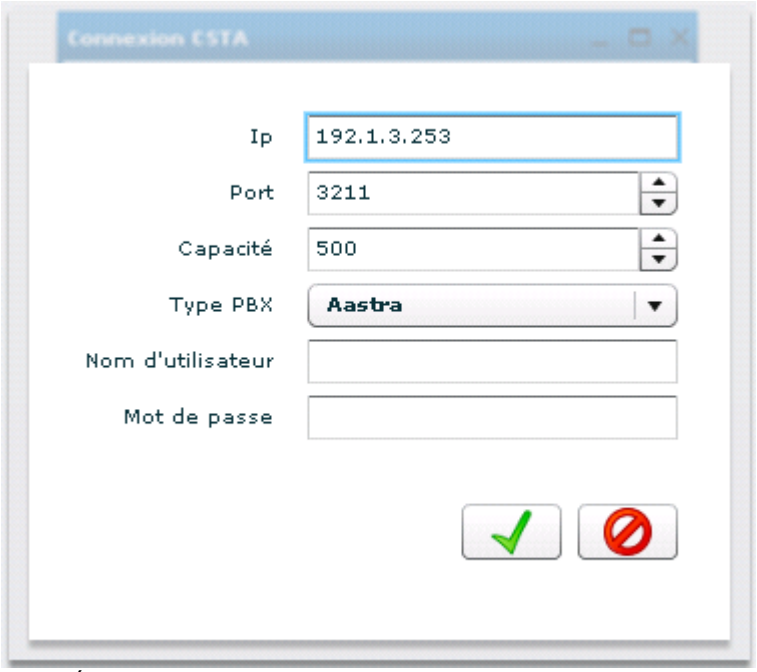
Après redémarrage du service, vous pouvez vérifier l'état des connexions créées ainsi que la supervision des postes supervisés (voir 10.4. Etat des connexions et voir 10.5. Etat des postes).

4.3. Lien CSTA

Un lien CSTA est utilisé pour gérer des renvois simples (voir guide d'utilisation Caller), ou le poste I2052 avec un TWP Caller.

N.B.: Seulement un lien CSTA est supporté par domaine.

Sélectionnez menu *Connexions* / *Connexion CSTA* puis cliquez sur "+".



Par défaut, vous devez préciser:

- L'adresse IP de l'IPBX,
- Le port CSTA (3211 par défaut dans le mode non délimité): ce port doit être unique dans un multi site et dédié à une seule application (voir spécifications Aastra pour un lien CSTA)
- Le type de PBX : "Aastra"
- La capacité (cf. LCI)
- Le nom d'utilisateur et mot de passe ne sont pas utilisés dans ce cas

Cliquez sur "sauvegarder".

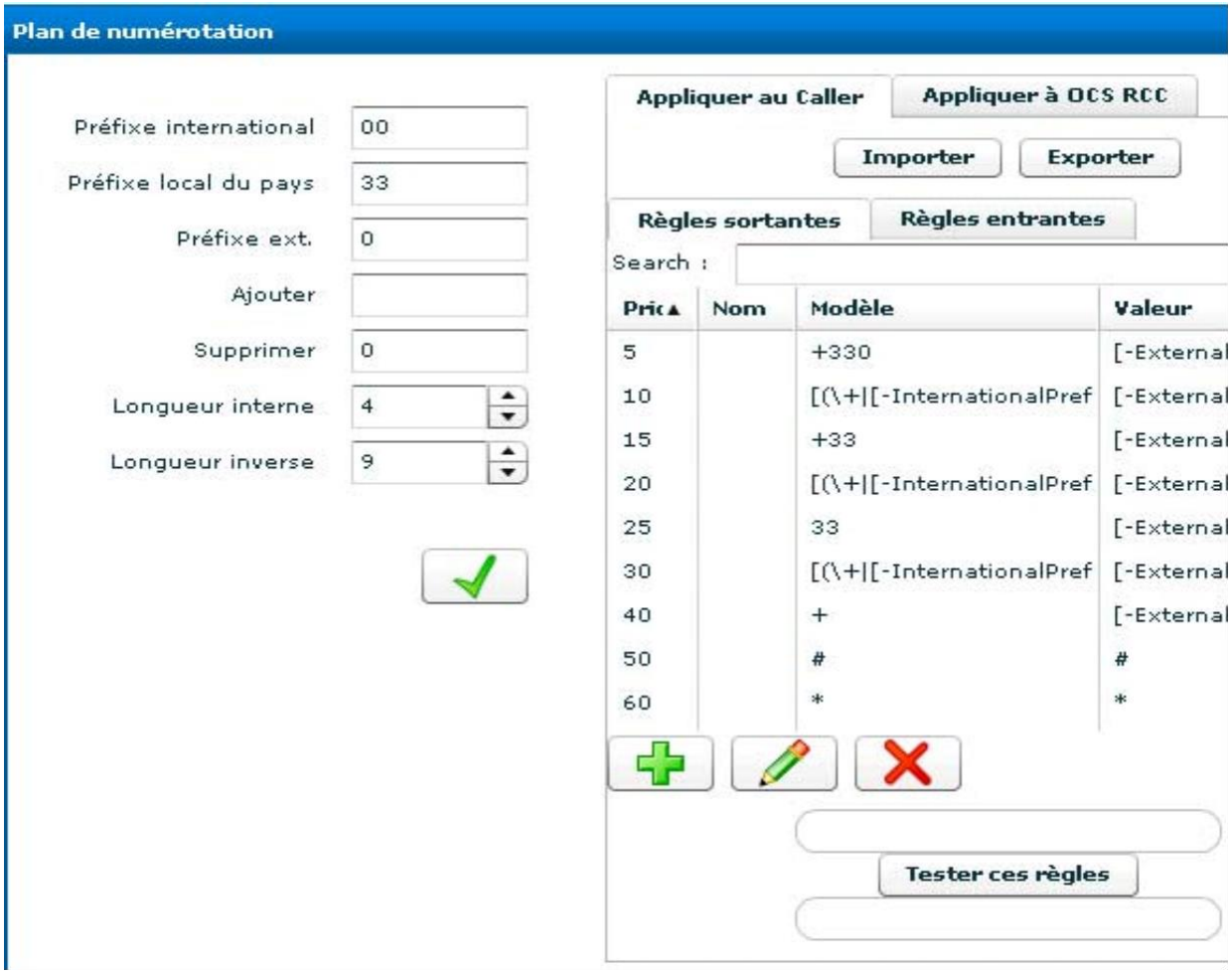
Information: *Vous devez redémarrer le service CSTA si vous faites des changements.*

5. Gestion des plans de numérotation

La gestion du plan de numérotation vous permet de définir des règles de transformation des numéros :

- Composés ou trouvés dans les fiches afin de les rendre composables (par exemple suppression du «+» pour les numéros au format international)
- Reçus pour permettre la recherche dans l'annuaire inverse

Sélectionnez *Téléphonie/Plan de numérotation*.

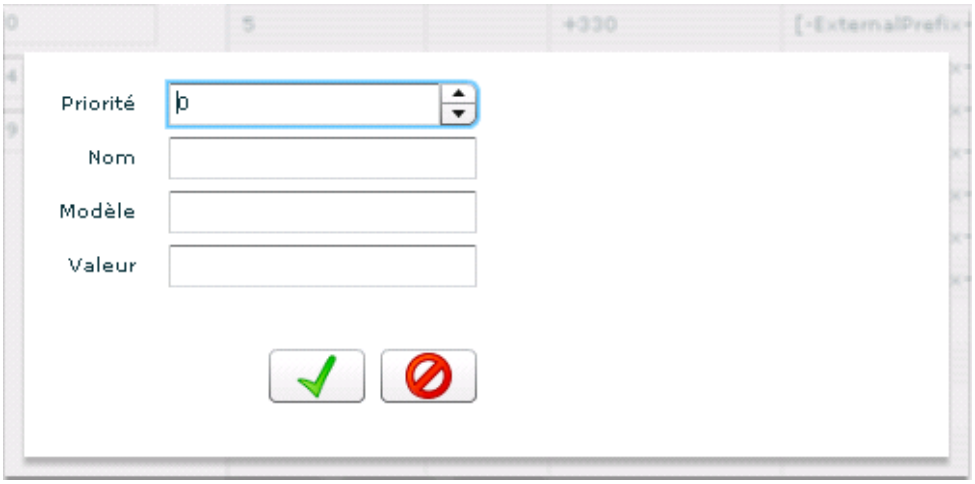


Sur la gauche, définissez les règles globales.

- *Préfixe International*: préfixe utilisé pour les appels internationaux.
- *Préfixe local du pays*: préfixe international pour le pays d'installation, par exemple 33 pour la France.
- *Préfixe Externe*: préfixe utilisé pour faire des appels externes. (Préfixe d'accès au réseau public)
- *Ajouter*: chaîne de caractères à ajouter au début du numéro appelant sur des appels entrants.
- *Supprimer*: chaîne de caractères à enlever au début du numéro appelant sur des appels entrants.
- *Longueur interne*: la longueur maximale d'un numéro d'appel interne.
- *Longueur interne inversé*: la longueur utilisée pour résoudre des appels entrants.

A droite, vous définissez les règles spécifiques de votre plan de numérotation (par défaut quelques règles standards sont créées).

Pour ajouter une règle à votre installation, cliquer sur "+". Cette fenêtre s'ouvre pour vous permettre de décrire la nouvelle règle.



- *Priorité*: priorité des règles, lors du traitement d'un numéro, une seule règle est appliquée, c'est celle ayant la priorité la plus basse et pour laquelle le numéro à remplacer est identique au numéro à transformer. Autrement dit quand une règle est trouvée et appliquée, le processus de transformation est terminé.
- *Modèle*: chaîne de caractères à remplacer
- *Valeur*: chaîne de caractères qui remplace le modèle

Par exemple:

Pour le modèle au caractère "+", il sera remplacé par "00'.
Pour un modèle avec la chaîne "361", il sera remplacé par "361".

Les règles sont choisies dans un ordre de priorité, en partant du haut vers le bas. Dès qu'une règle est prise en compte, les règles suivantes seront ignorées.
Les modèles sont recherchés uniquement en début de chaîne.

5.1. Règles standards

Les règles standards incluses sont les suivantes :

- Tout caractère non-numérique est supprimé, sauf pour les +, #, * lorsqu'ils sont en premier
- "+33(0)": devient 00 (donc +33 (0) 123456789 devient 00123456789)
- "+330" : devient 00
- "#" : devient " # " (pas de transformation).
- "*" : devient " * "(pas de transformation).

Cas particuliers: Tout numéro qui commence par le préfixe international + le préfixe national (0033 ou +33) sera remplacé par le préfixe réseau + préfixe national ("33155171889" devient "00155171889").

5.2. Traitement d'un numéro

Voici l'algorithme de la transformation du plan de numérotation: La première opération consiste à détecter si une règle est applicable:

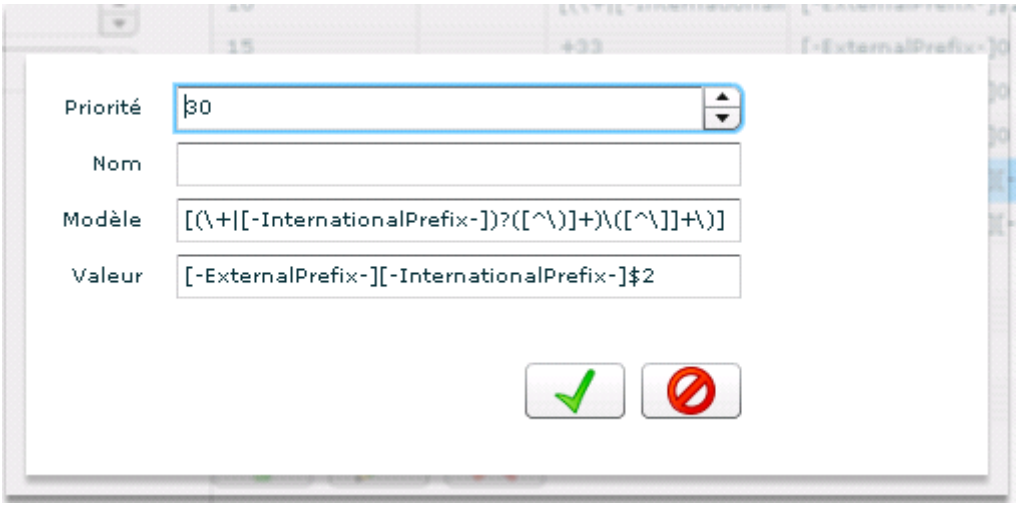
Deux cas

- *Pas de règle trouvée*. Dans ce cas, si un numéro est plus long qu'un numéro local, le préfixe externe est ajouté; sinon, le numéro est renvoyé comme tel.
- *Une règle est applicable*, deux cas sont possibles:
    - *Le numéro commence avec un "+"*. La transformation est appliquée puis le préfixe réseau est ajouté si nécessaire. Par exemple: +3912334477 -> 0 00 3912334477
    - *Le numéro ne commence pas avec un "+"*. Seule la transformation du plan de numérotation est appliquée. Par exemple: si nous avons la règle: modèle = 03611 valeur = 03611, quand on numérote 03611, il devient 03611, et le préfixe du réseau externe ne sera pas ajouté.

5.3. Règles avancées

Il est possible de définir des règles basées sur des expressions régulières.

Dans l'impression d'écran ci-dessus, la règle (qui a une priorité de 30) est une expression régulière:



Cette règle transforme par exemple +42(0)141906666 en 00042141906666. Elle ajoute le préfixe international et le préfixe externe et supprime le préfixe national si nécessaire.

Détails du modèle:

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)]
```

Les Crochets du modèle informe qu'il s'agit d'une expression régulière.

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)]-> 42(0)141906666
```

Le '+', un caractère spécial utilisé dans les expressions régulières, est précédé par un '\' pour montrer que l'expression recherchera un "+" dans la chaîne. Le caractère '?' Indique que l'expression va rechercher un ou zéro '+'. La règle traite donc des nombres tels que +42 (0) et 42 (0), etc…

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)] -> 42(0)141906666
```

[-InternationalPrefix-] représente les chiffres du préfixe international mentionné dans la colonne de gauche. L'expression recherchera cette valeur pour la recopier dans le résultat.

```
[(\+|[-InternationalPrefix-])?([^\)]+)\([^\]]+\)] -> 42141906666
```

Les caractères '(' et ')', les caractères spéciaux utilisés dans les expressions régulières, sont précédés par un '\' indiquant que l'expression sera à la recherche de '(' et ')'.

Détails de la valeur : [-ExternalPrefix-][-InternationalPrefix-]$2

'$2' sera remplacé par la valeur saisie (voir « détails du modèle » ci-dessus). Dans notre exemple, notre règle remplace +42(0) par 0042 et le reste est recopié.

Pour plus d'informations sur les expressions régulières:
http://msdn.microsoft.com/fr-fr/library/hs600312(VS.80).aspx

Test du plan de numérotation:

Vous pouvez vérifier vos règles de translation de numérotation de la manière suivante :

Saisir un numéro dans la case située au-dessus du bouton «*tester le plan de num*», cliquer, le numéro transformé est affiché dans la case inférieure. C'est le numéro qui sera envoyé à l'IPBX.

6. Méthodes d'authentification

6.1. Configuration

Qu'ils soient créés manuellement ou importés d'une base de données, les utilisateurs doivent être authentifiés lorsqu'ils utilisent les applications. Il existe plusieurs méthodes d'authentification avec TWP qu'il est possible de configurer dans l'administration :

- Authentification *Windows* : valeur de paramètre applicatif « *WindowsSecurity* »
- Authentification *LDAP* : valeur de paramètre applicatif « *LDAP* »
- Authentification TWP : valeur de paramètre applicatif « *TWS* »
- Authentification *None* ou pas d'authentification : valeur de paramètre applicatif « *None* »

Pour modifier ou appliquer une méthode d'authentification à un utilisateur, un groupe d'utilisateurs ou à tout un domaine, aller dans l'administration, menu *Applications / Paramètres applicatifs* puis choisir TWP *Server*. Chercher « *AuthMethods* ».

Il est possible de renseigner les différentes valeurs en les séparant par « | ». Dans l'exemple ci-dessus, tous les utilisateurs pourront à la fois exécuter l'application Caller en étant automatiquement authentifié depuis leur session Windows ou en précisant le nom d'utilisateur à lancer.

6.2. Authentification Windows

C'est le système d'authentification historique de la solution TWP. L'authentification est réalisée via les comptes de session Windows des utilisateurs.

6.2.1. Pré requis : avec Contrôleur de domaine

Lors du lancement de l'application Caller ou de l'utilisation de services web authentifiés, il n'y a pas de pop-up d'authentification qui s'affiche pour ce mode.

- Sur le contrôleur de domaine tous les utilisateurs de la société doivent posséder un compte
- Le serveur TWP doit être dans le même domaine Windows que les utilisateurs.
- L'utilisateur doit se connecter sur son poste avec un login/mot de passe qui est son identifiant sur le domaine.
- Dans l'administration les noms des utilisateurs TWP doivent être identiques aux noms d'utilisateurs du domaine.

6.2.2. Pré requis : sans Contrôleur de domaine

Pour ne pas avoir de pop-up d'authentification :

- Les utilisateurs et le serveur doivent être dans le même WorkGroup (groupe de travail Windows).
- Il faut déclarer les mêmes noms d'utilisateurs sur le serveur dans le gestionnaire des utilisateurs Windows que sur les machines clientes (utilisateurs Windows), et dans l'administration.
- Les utilisateurs doivent se connecter sur leur machine avec leur compte local (qui sera le même que celui défini sur le serveur et dans l'administration) et non en administrateur.
- **Attention** : Si l'utilisateur change son mot de passe en local (sur sa machine cliente) il faut le changer aussi dans le gestionnaire des utilisateurs Windows sur le serveur TWP.

Avec pop-up d'authentification :

- On déclare les utilisateurs sur le serveur (utilisateurs Windows).
- L'utilisateur devra entrer son login/mot de passe à chaque lancement de l'application Caller ou de l'utilisation de services web authentifiés.
- L'utilisateur peut se connecter comme bon lui semble sur sa machine locale (dans ce genre d'architecture en général en administrateur de sa machine).

6.3. Authentification LDAP

L'authentification est réalisée via les comptes LDAP des utilisateurs.

Pré requis :

- Les utilisateurs doivent tous être déclarés sur un (ou plusieurs) serveur LDAP.
- Le serveur LDAP doit être accessible depuis le serveur TWP :
  Pour configurer les informations de connexion au serveur LDAP, aller dans l'administration, menu *Applications / Paramètres applicatifs*, choisir TWP *Server*. Il faut remplir les champs suivant.
  Noter que les valeurs peuvent être renseignées pour un utilisateur ou un groupe ou un domaine
  - *AuthLdapServer* : adresse IP du serveur LDAP
  - *AuthLdapPort* : port de connexion.
  - *AuthLdapDn* : Où pointer dans l'arborescence du LDAP. La valeur par défaut est « ? ». « ? » est remplacé par le nom de l'utilisateur. Il est possible de renseigner d'autres valeurs comme « `OU=PARIS, DC=SSDEI, DC=local, CN=?` »

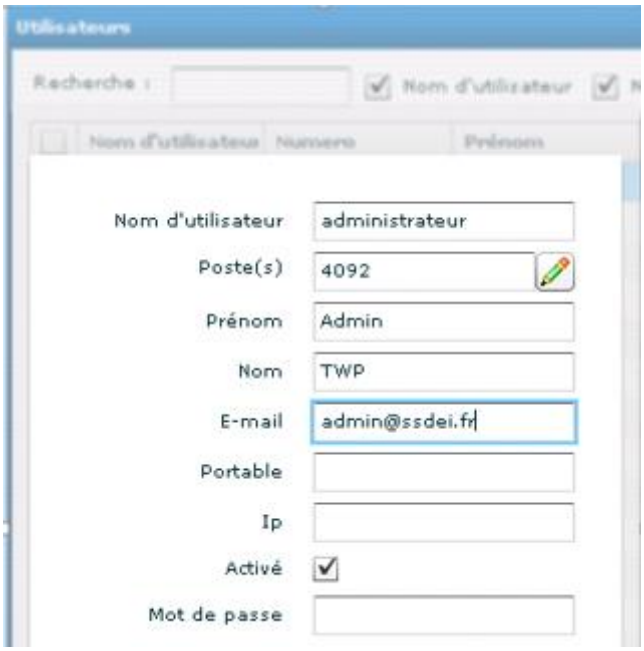
- Le nom de l'utilisateur doit être présent avec ou sans « *AuthLdapDn* » dans le serveur LDAP.
- Le mot de passe de l'utilisateur est le même que celui du serveur LDAP.
- A la première connexion avec l'application Caller, un pop-up d'authentification (TWP) apparait, l'utilisateur entre son login/mot de passe. Si l'utilisateur coche la case « sauvegarder » le pop-up ne réapparait pas. S'il veut changer de nom d'utilisateur, il peut décocher la fonctionnalité de connexion automatique dans les préférences, menu *Général*.

6.4. Authentification TWP

L'authentification est réalisée directement sur le serveur via les nom d'utilisateur et mot de passe renseignés dans l'administration.

Pré requis :

- Ni besoin de domaine, ni besoin de WorkGroup. Peu importe comment l'utilisateur se connecte à sa session.
- Les utilisateurs peuvent être déclarés manuellement ou par divers imports annuaire dans l'administration.
- Chaque utilisateur doit avoir un mot de passe et celui-ci doit être renseigné manuellement par l'administrateur
  Pour renseigner le mot de passe de connexion de l'utilisateur, aller dans l'administration, menu *Utilisateurs* / *Utilisateurs*. Editer un utilisateur puis modifier la valeur de « *mot de passe* ».



- A la connexion l'utilisateur doit renseigner le même mot de passe que l'administrateur lui a attribué.
- A la première connexion avec l'application Caller, un pop-up d'authentification (TWP) apparait, l'utilisateur entre son login/mot de passe. Si l'utilisateur coche la case « sauvegarder » le pop-up ne réapparait pas. S'il veut changer de nom d'utilisateur, il peut décocher la fonctionnalité de connexion automatique dans les préférences, menu *Général*.

6.5. Pas d'authentification

L'authentification est réalisée directement sur le serveur via le nom de l'utilisateur.

Pré requis :

- Ni besoin de domaine, ni besoin de WorkGroup. Peu importe comment l'utilisateur se connecte à sa session.
- Les utilisateurs peuvent être déclarés manuellement ou par divers imports annuaire dans l'administration.
- L'utilisateur devra renseigner son login au lancement.
- A la première connexion avec l'application Caller, un pop-up d'authentification (TWP) apparait, l'utilisateur entre son login. Si l'utilisateur coche la case « sauvegarder » le pop-up ne réapparait pas. S'il veut changer de nom d'utilisateur, il peut décocher la fonctionnalité de connexion automatique dans les préférences, menu *Général*.

7. Gestion des utilisateurs

Les utilisateurs peuvent être créés manuellement ou importés d'une base de données.

7.1. Créer un utilisateur manuellement

Voir la section 3.3.4

7.2. Importer des utilisateurs

Dans TWP, vous pouvez synchroniser vos utilisateurs avec une base de données externe. Cela vous aidera à créer un grand nombre d'utilisateurs très rapidement.

Pour importer des utilisateurs, sélectionnez menu Utilisateurs / Import(s) Utilisateurs puis cliquez sur le bouton '+'.

Il y a 3 types d'imports:

- LDAP
- Active Directory
- A5000 INT

Nota: Le processus d'import se fait uniquement dans un sens, depuis la base de données externe vers la base d'utilisateurs.

Il y a également des types de synchronisation différents:

- Insertion, mise à jour et suppression: Créer des nouveaux utilisateurs, mise à jour des utilisateurs existants, effacer des utilisateurs
- Insertion, mise à jour et désactivation: Créer des nouveaux utilisateurs, mise à jour des utilisateurs existants, désactiver les utilisateurs supprimés.
- Insertion, mise à jour: Créer des nouveaux utilisateurs, mise à jour des utilisateurs existants
- Mise à jour seulement: Mise à jour des utilisateurs existants

7.2.1. Importer des utilisateurs depuis LDAP

Dans la liste déroulante 'Type d'Import' sélectionnez "*LDAP*".

Tous les champs standards sont pré-remplis. Les Informations requises sont les suivantes :

Informations requises:

Informations:

- Description: description d'importation des utilisateurs
- Hôte: Adresse IP du serveur LDAP
- Port: 389, le port par défaut pour la connexion LDAP
- Identifiant / mot de passe: Login pour la connexion LDAP

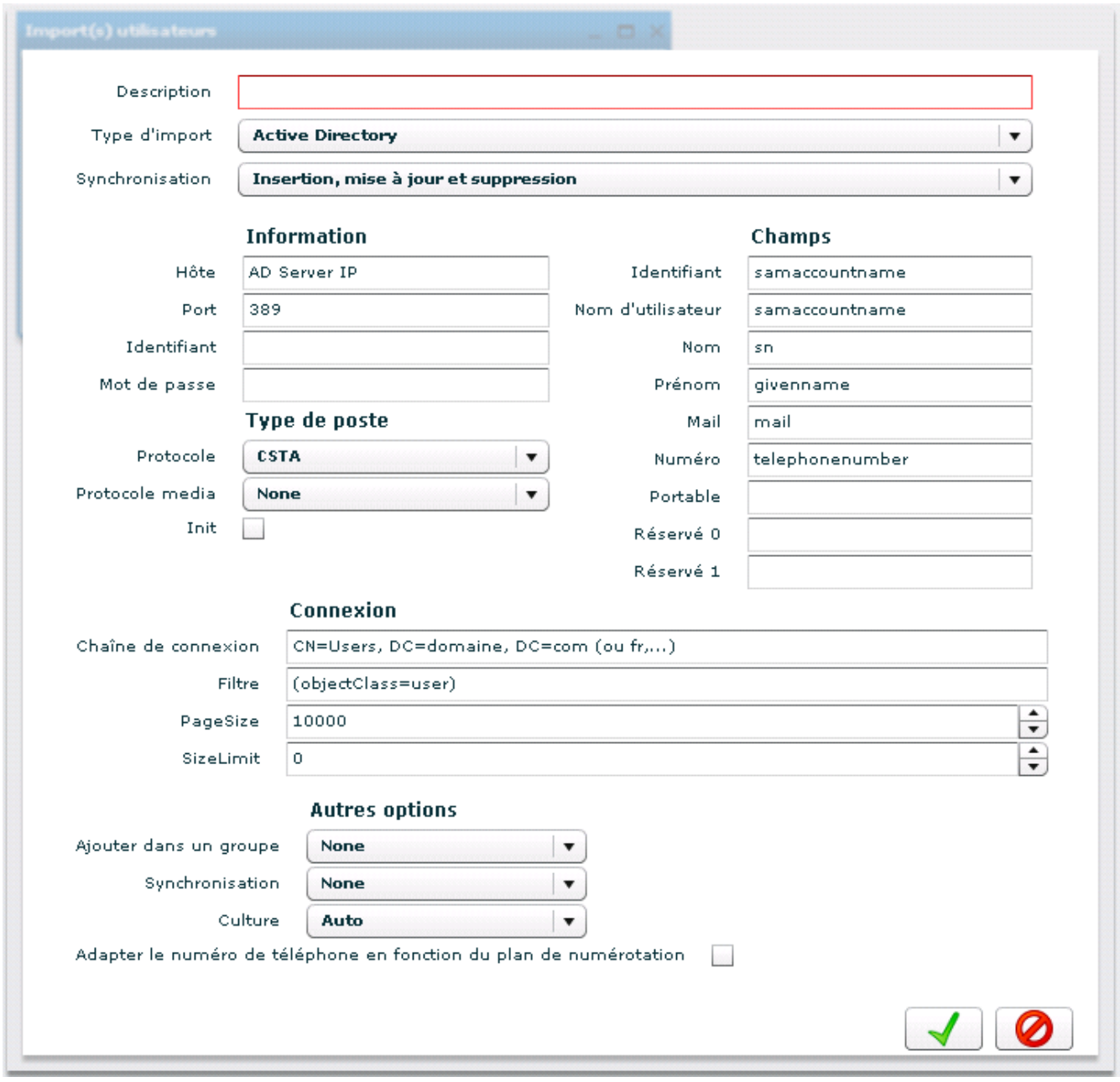
- Protocole media : la valeur par défaut « None » ne doit pas être modifiée

Champs: Etablir le lien entre les champs LDAP et les champs TWP : selon le schéma LDAP.

Connexions:
- Chaîne de connexion: Base DN de votre connexion
- Filtre: Filtre LDAP pour la requête de recherche

7.2.2. Importer des utilisateurs depuis Active Directory

Dans la liste déroulante 'Type d'Import' sélectionnez "*Active Directory*".



Tous les champs standards sont pré-remplis. Vous devez définir:

Informations requises:

Informations:

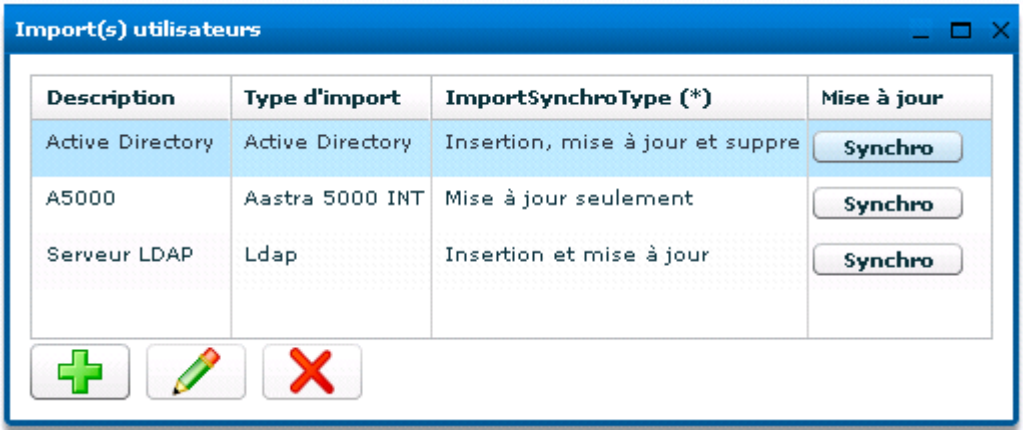
- Description: description d'importation des utilisateurs
- Hôte: Adresse IP du serveur DC
- Port: 389, le port par défaut pour la connexion DC
- Identifiant / mot de passe: Login pour la connexion AD

Champs: Les champs standards AD sont pré-remplis, vous pouvez ajouter les schémas des champs privés.

Connexions:

- Chaîne de connexion: Base DN de votre connexion
- Filtre : Filtre LDAP pour la requête de recherche

7.2.3. La fenêtre d'import utilisateur



 Création d'un nouvel import

 Modification d'un import

 Suppression d'un import

Pour activer une synchronisation, cliquez sur un des boutons « *Synchro* ».

Dès que la synchro est finie, un compte rendu est publié et le résultat est visible dans le menu *Utilisateurs*.

Si vous glissez la souris sous les résultats, les détails de la synchronisation s'affichent:

- Créer: nombre de nouveaux utilisateurs ajoutés.
- A jour: nombre d'utilisateurs mises à jour.
- Ignoré: nombre d'échecs d'ajout. Des utilisateurs sont ignorés s'ils ne possèdent aucun numéro de téléphone.

Attention: l'import utilisateur est lié au Service TWS4$TWS_WebServices, celui-ci doit toujours être démarré. Si le service est arrêté, il est impossible de faire une synchronisation.

7.2.4. Autorisations de visualisation des contacts

Pour avoir accès aux fiches contacts des utilisateurs importés, il faut absolument donner des droits sur l'annuaire lié à cet import (voir chapitre 7.4.2. Autorisation Annuaire).

7.3. Gestion des Groupes

Gestion générale

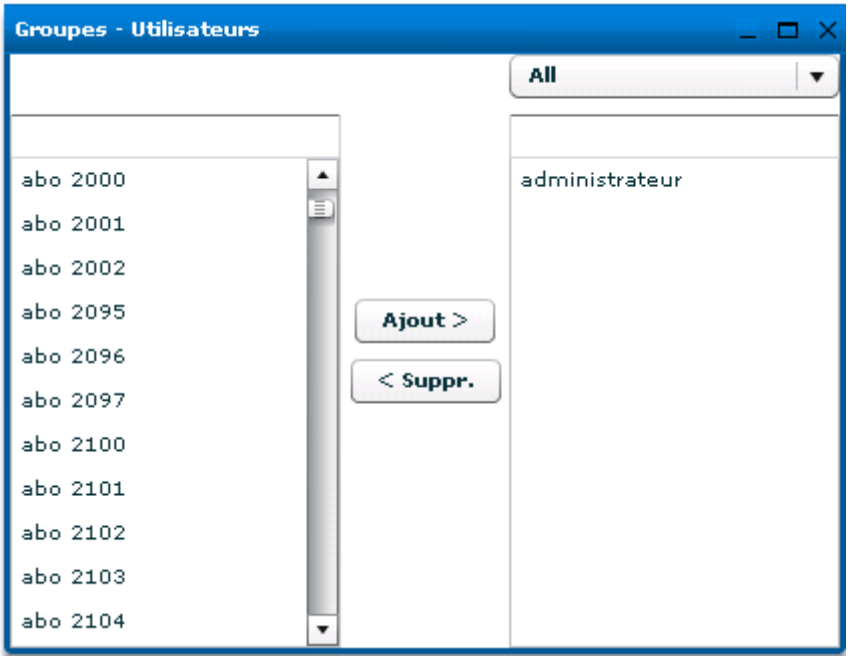
Choisissez le menu *Utilisateurs / Groupes*.

« Groupes » contient des groupes d'utilisateurs qui partagent des caractéristiques communes. Ces groupes seront ensuite utilisés pour définir l'accès aux applications, services, logs, etc…

Pour créer un groupe, *voir chapitre 3.3.5*.

Gestion des utilisateurs

Choisissez le menu *Utilisateurs / Groupes d'Utilisateurs*. Ce menu est utilisé pour définir les utilisateurs inclus dans les groupes définis dans le dernier menu



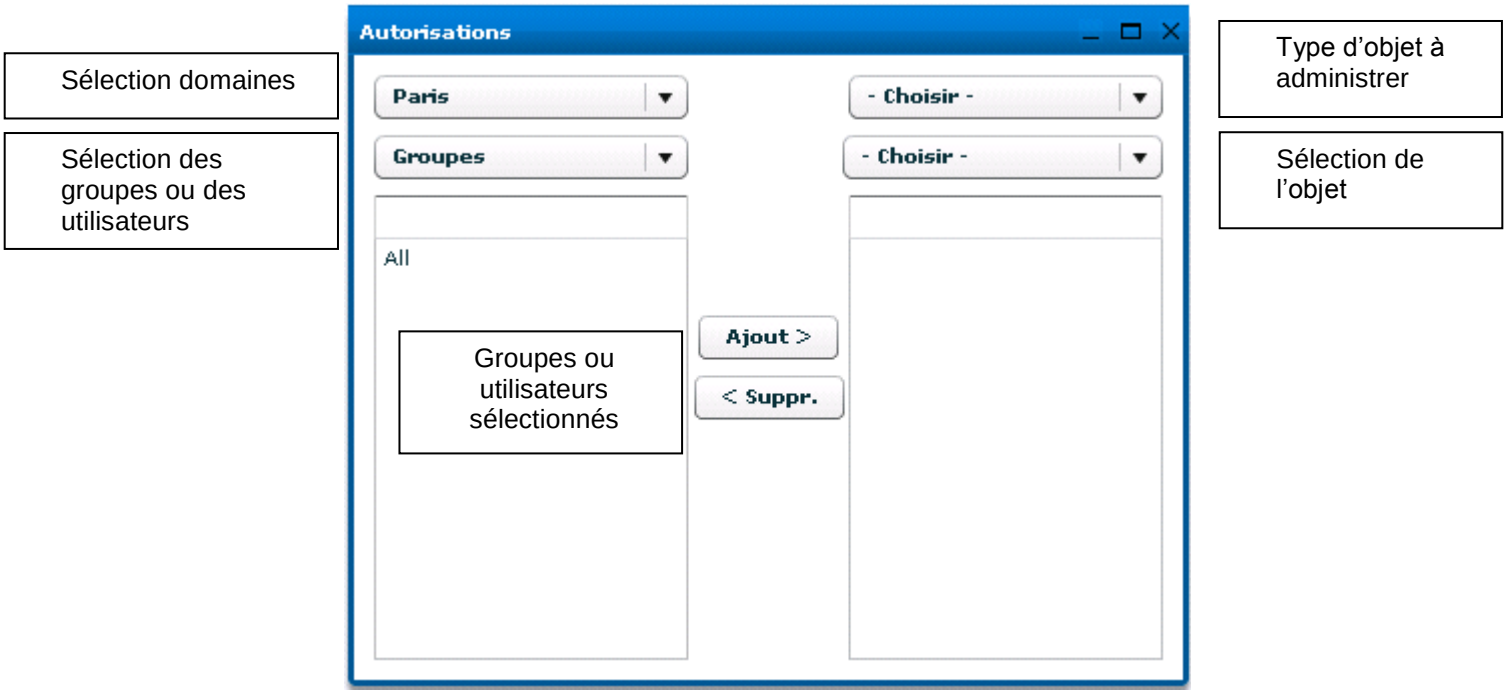
Depuis la liste de choix en haut à droite, vous pouvez sélectionner le groupe à gérer. Dans la liste à gauche, vous pouvez voir tous les utilisateurs qui ne sont pas encore dans le groupe sélectionné. La barre en haut à gauche vous permet de filtrer une recherche des utilisateurs.

Pour ajouter un utilisateur dans un groupe:

- Sélectionnez le groupe dans la liste de choix en haut à droite
- Sélectionnez un (ou plusieurs avec 'ctrl') utilisateurs et cliquez "*Ajout >*"

7.4. Gestion des autorisations

Menu *Utilisateurs* / *Autorisations* est la fenêtre centrale utilisée pour gérer tous les droits d'objets ou d'utilisateurs ou de Groupes sur le serveur.



Pour donner les droits à un utilisateur ou groupe d'utilisateurs à un objet (applications, annuaires, …), il faut procéder comme il suit :

1. Dans la liste en haut à droite, sélectionner le type d'objet à administrer
2. Juste en dessous, sélectionner l'objet en question
3. Dans la liste en haut à gauche, sélectionner le domaine auquel appartient l'utilisateur ou le groupe d'utilisateurs. Le domaine de la session est sélectionné par défaut.
4. Dans la liste du dessous sélectionner *groupes* ou *utilisateurs*. Il apparaîtra alors tous les utilisateurs ou groupes d'utilisateurs du domaine.
5. Il suffit ensuite de sélectionner l'utilisateur ou le groupe à gauche et de cliquer sur le bouton *Ajouter* pour lui donner les droits à l'objet.

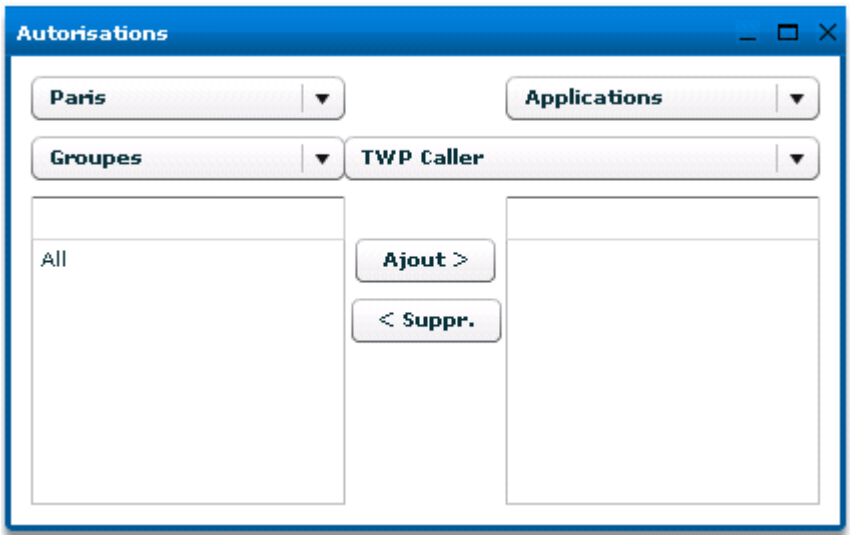
***Attention** : Seules les autorisations sur les Statistiques et les Enregistrements se font différemment*. C'est-à-dire, le point 2. permettra plutôt de sélectionner l'utilisateur qui aura les droits sur les Statistiques/Enregistrements des autres utilisateurs au lieu de l'objet Statistiques/Enregistrements de celui-ci. Cela permettra aussi au point 5. de donner à un seul utilisateur les droits de visualisations sur les Statistiques/Enregistrements de tout un groupe d'utilisateurs.

7.4.1. Autorisation Applications

L'exemple ci-dessous montre l'autorisation pour l'application Caller.

Tous les utilisateurs dans les groupes 'All' peuvent exécuter l'application Caller.

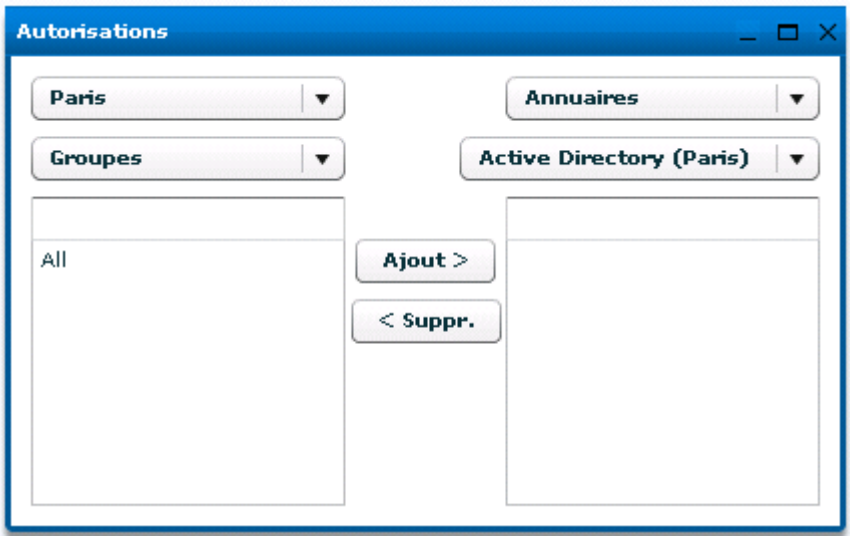
Toute autorisation à une application consomme automatiquement un nombre de licences correspondant.



7.4.2. Autorisation Annuaire

L'exemple ci-dessous montre l'autorisation pour l'annuaire Active Directory (qui est l'annuaire créé précédemment de l'import utilisateur) sur le domaine Paris.

Le groupe All sur le domaine Paris a le droit de voir l'annuaire Active Directory sur le domaine Paris.

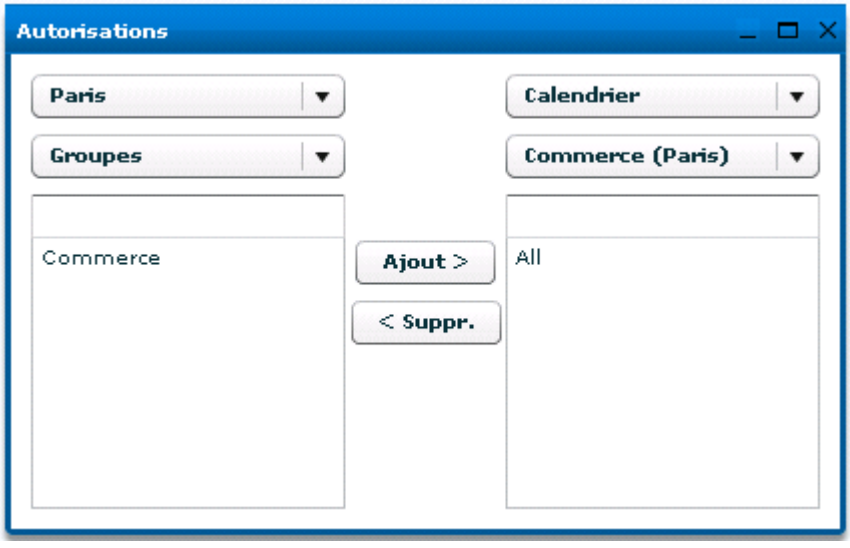


N.B. : Les annuaires peuvent être partagés entre domaines.

Ci-dessous un exemple d'autorisation multi-domaines. Tous les utilisateurs dans le groupe All sur le domaine Paris ont le droit de voir l'annuaire Public sur le domaine Nice.

7.4.3. Autorisation calendriers

Pour autoriser un utilisateur à voir les évènements de calendrier d'un autre utilisateur, allez dans le menu *Utilisateurs* / *Autorisations*. Dans l'exemple ci-dessous, le groupe All est autorisé à voir le calendrier du groupe Commerce du même domaine Paris.



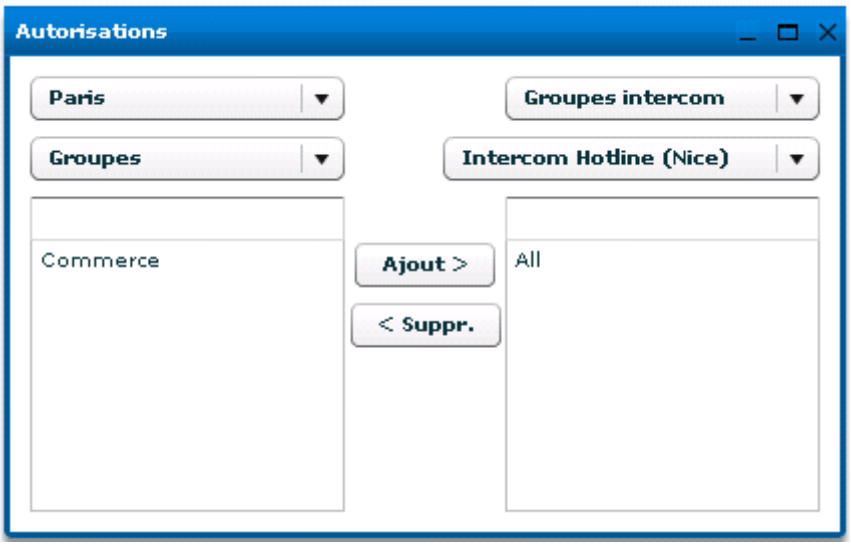
Sélectionner *Calendrier* dans le type d'objet, puis sélectionner les groupes d'utilisateurs qui veulent partager leur calendrier, enfin sélectionner le groupe ou l'utilisateur qui doit voir ces calendriers et cliquer sur *'Ajouter'*.

N.B. : Noter que les calendriers peuvent également être partagés entre domaines.

7.4.4. Autorisation groupe intercom

L'exemple ci-dessous montre l'autorisation pour le groupe intercom « Intercom Hotline » sur le domaine « Nice ».

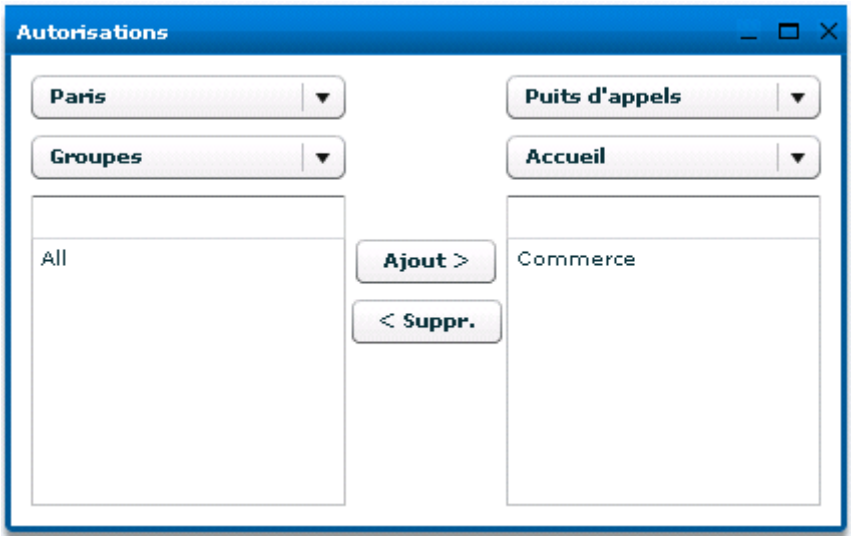
Tous les utilisateurs dans le groupe All sur le domaine Paris ont le droit de voir la présence téléphonique des postes d'utilisateurs gérés par le groupe intercom « Intercom Hotline » du domaine « Nice ».



N.B. : Les groupes intercom peuvent être partagés entre domaines.

7.4.5. Autorisation puits d'appels

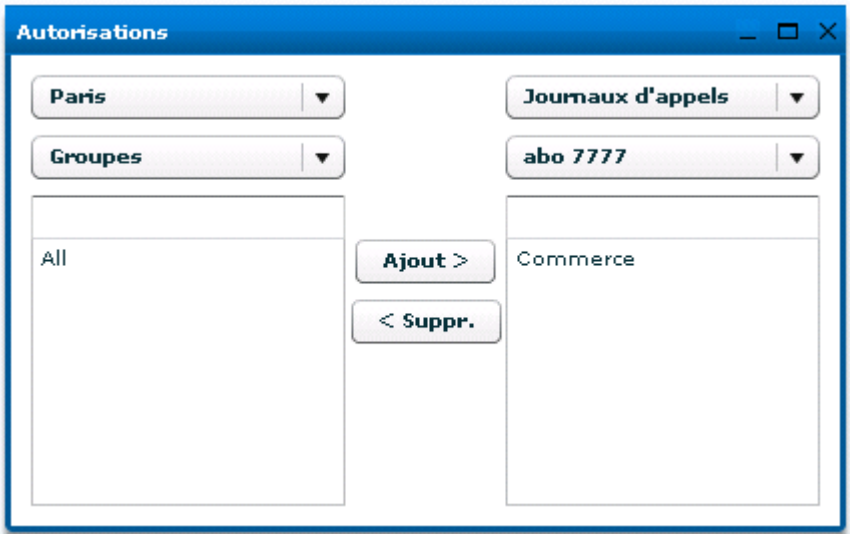
Tous les utilisateurs du groupe Commerce du domaine Paris ont le droit de voir le puits d'appels « Accueil ».



N.B. : Les puits d'appels ne peuvent pas être partagés entre domaines.

7.4.6. Autorisation Journaux d'appels

Tous les utilisateurs du groupe Commerce du domaine Paris ont le droit de voir les journaux d'appels de l'utilisateur « abo 7777 ».



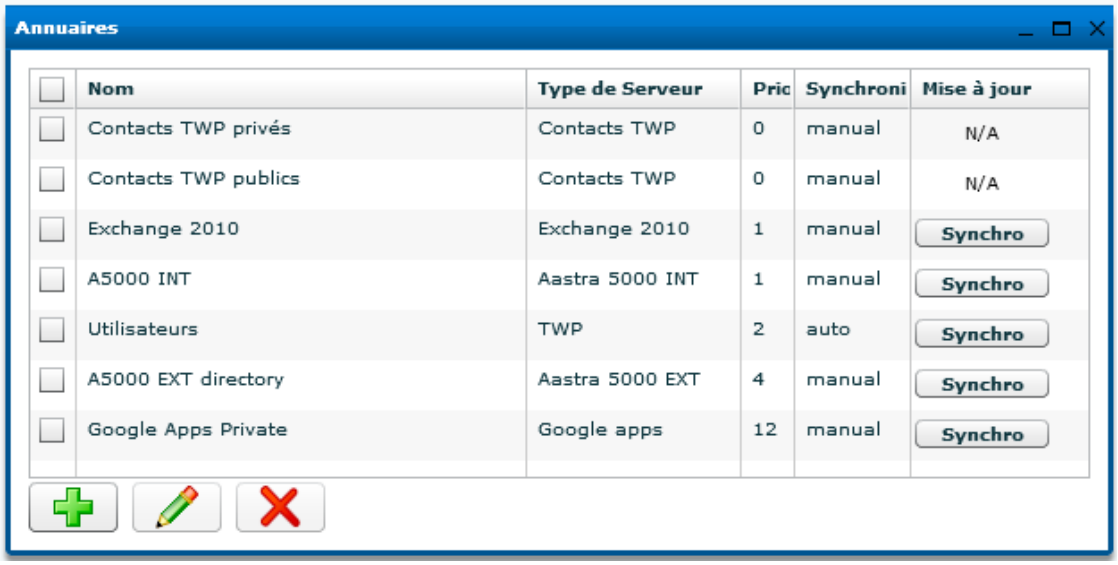
N.B. : Les journaux d'appels ne peuvent pas être partagés entre domaines.

8. Annuaires et collaboration

8.1. Généralités

Dans Administration, sélectionnez *Informatique* puis *Annuaires*.

Une table s'ouvre incluant les différentes connexions aux annuaires déjà configurées.



Pour créer un annuaire, cliquez sur « + ».

La création d'un annuaire est faite en 3 étapes :

- Onglet connecteur : Création d'un connecteur annuaire
- Onglet champs : Renseignements des champs à faire correspondre
- Onglet synchronisation : Configuration de la Synchronisation

Onglet connecteur:

Vous avez besoin de remplir certaines informations dans cette fenêtre d'annuaire en fonction du connecteur annuaire que vous créez.

Nom: Description de l'annuaire

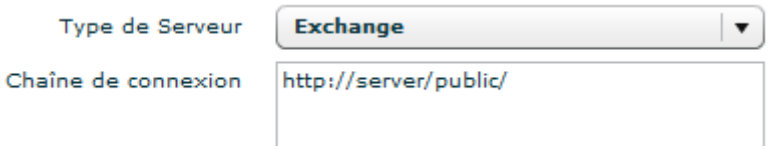
Type d'annuaire: Permet d'activer ou désactiver un annuaire

- *Exemple* : Désactiver l'annuaire, ce qui ne pourra pas être synchronisé.
- TWP : L'annuaire est public.
- *Privé* : L'annuaire est privé.

Priorité: Cette valeur permet de définir l'ordre de priorité des Annuaires dont TWP est connecté simultanément. TWP affichera les informations sur appel entrant/sortant depuis l'annuaire avec le nombre de priorité le plus bas.

Exemple: un contact existe dans les annuaires Exchange, SQL et LDAP, tous déclarés sur TWP Server. Si des informations du contact sont affichées avec TWP Alerter, les informations provenant de l'annuaire avec la priorité la plus basse seront affichées (identité, société, lien vers fiche clients…).

Type de serveur:



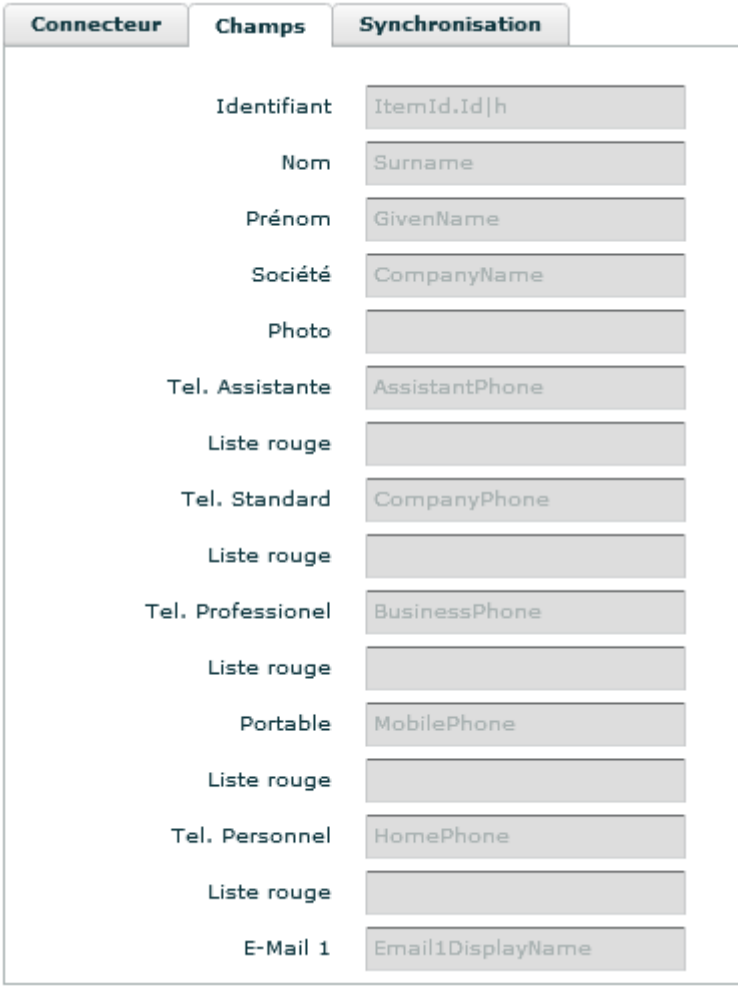
Le connecteur annuaire peut être configuré pour:

- *Exchange* : MS Exchange server 2003 / 2007 /2010
- *LOTUS* : Lotus domino server version 7.5 / 8
- *LDAP* : tout serveur LDAP
- *ODBC* : Base de données ODBC
- *OLE DB* : Base de données OLE DB
- *SQL* : Serveur base de données SQL
- TWP : Annuaire utilisateurs TWP

Les champs restants sont utilisés pour créer un connecteur annuaire selon le type de connecteur annuaire.

Onglet Champs:

Les champs ci-dessous correspondent aux noms des champs d'annuaire.
Ces champs sont utilisés pour établir une correspondance entre les champs de l'annuaire interne TWP et ceux d'un annuaire externe.



Ajout d'options

Il est possible d'ajout différentes options dans les champs des annuaires. Pour cela, il faut ajouter un « pipe » « | » après le nom du champ à synchroniser et une lettre qui correspond à l'option à exécuter.

Exemple : « `Surname|u` »

Options :

- ***a*** : transforme la valeur du champ en valeur d'adresse postale et permet à l'utilisateur de cliquer sur le lien résultant pour une recherche directe sur un site de cartographie.
  Note : L'URL du site de cartographie est configurable dans l'administration menu *Applications* / *Paramètres applicatifs* / TWP *Caller*, chercher « *MapServiceURL* ».
- ***h*** : hashe la valeur du champ
- ***i*** : rend invisible la valeur du champ dans la fiche du contact dans le Caller. Ce champ reste néanmoins accessible dans l'Alerter.

- ***l*** : passe toutes les lettres de la valeur du champ en minuscule
- ***m*** : passe la première lettre de la valeur du champ en majuscule suivi du reste en minuscule
- ***u*** : passe toutes les lettres de la valeur du champ en majuscule
- ***p*** : permet d'ajouter des éléments à la valeur du champ
    - Format : `p::[value]{0}::[Regexp]`
    - Exemple : `PhoneNumber|p::9{0}::^[0-9]{4}$`
        - « `PhoneNumber` » : nom du champ à synchroniser
        - « `::` » : séparateur
        - « `p` » : nom de l'option
        - « `9{0}` » : Le chiffre 9 sera ajouté au début de chaque valeur du champ PhoneNumber.
          ({0} représente la valeur synchronisé et peut être placé n'importe où dans l'expression)
        - « `^[0-9]{4}$` » est l'expression régulière qui valide le fait que la valeur de champ correspond (ici) à un numéro de 4 chiffres. (optionnel)

Pour ajouter plusieurs options, il faut les séparer à l'aide d'une virgule « , ».

Exemple : « `Surname|h,u,p::9{0}::^[0-9]{4}$` »

Onglet Synchronisation Annuaires:

Voir le chapitre suivant 8.2.

8.2. Synchronisation annuaire – Fusion de contact – Champs spécifiques

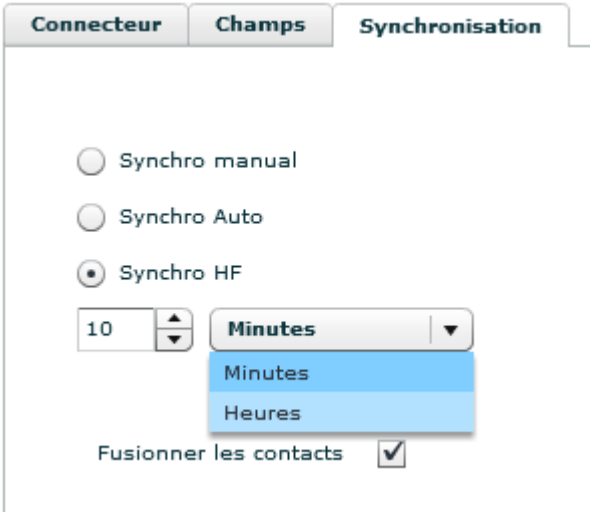
8.2.1. Synchronisation annuaire

Il y a trois types de synchronisation annuaire :

- *Manuel* : pour synchroniser un annuaire, cliquez sur le bouton *Synchro* dans la fenêtre qui liste les annuaires.
- *Automatique* : pour activer une synchronisation tous les jours à une heure prédéfinie.

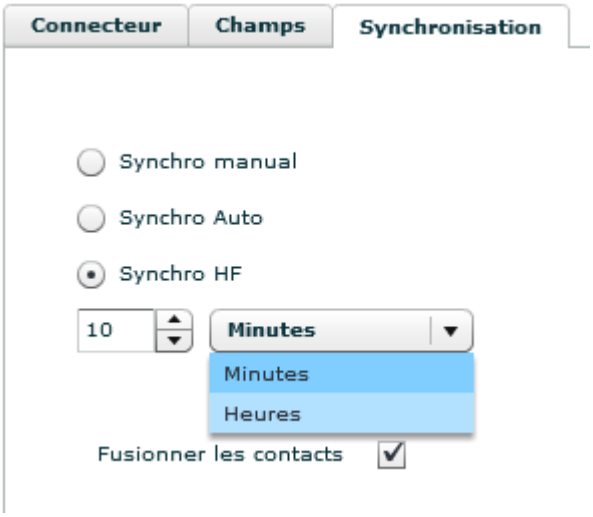
  Pour configurer l'heure de la synchronisation, sélectionnez les menus *Applications* / *Paramètres applicatifs* > *Paramètres Système*, recherchez l'option *timeSynchronizationDirectories* (Expert Mode) et changer la valeur par défaut.

  Attention : le format correct est : HH:MM
- *HF* : Fréquence Haute vous permet d'activer une synchronisation régulière. Vous pouvez choisir une fréquence en minutes ou heures.



8.2.2. Fusion des contacts

Dans l'onglet Synchronisation, il est possible pour un annuaire de cocher la case autorisant le système à fusionner les informations de ses contacts avec celles provenant des contacts d'autres annuaires qui ont également la case cochée.



*La fusion des informations entre contacts se fait en fonction de l'adresse **Email**.*

En effet, si deux ou plusieurs contacts (provenant de l'ensemble des annuaires) ont la même adresse email, leurs différentes informations seront fusionnées et présentées au sein d'une seule fiche annuaire.

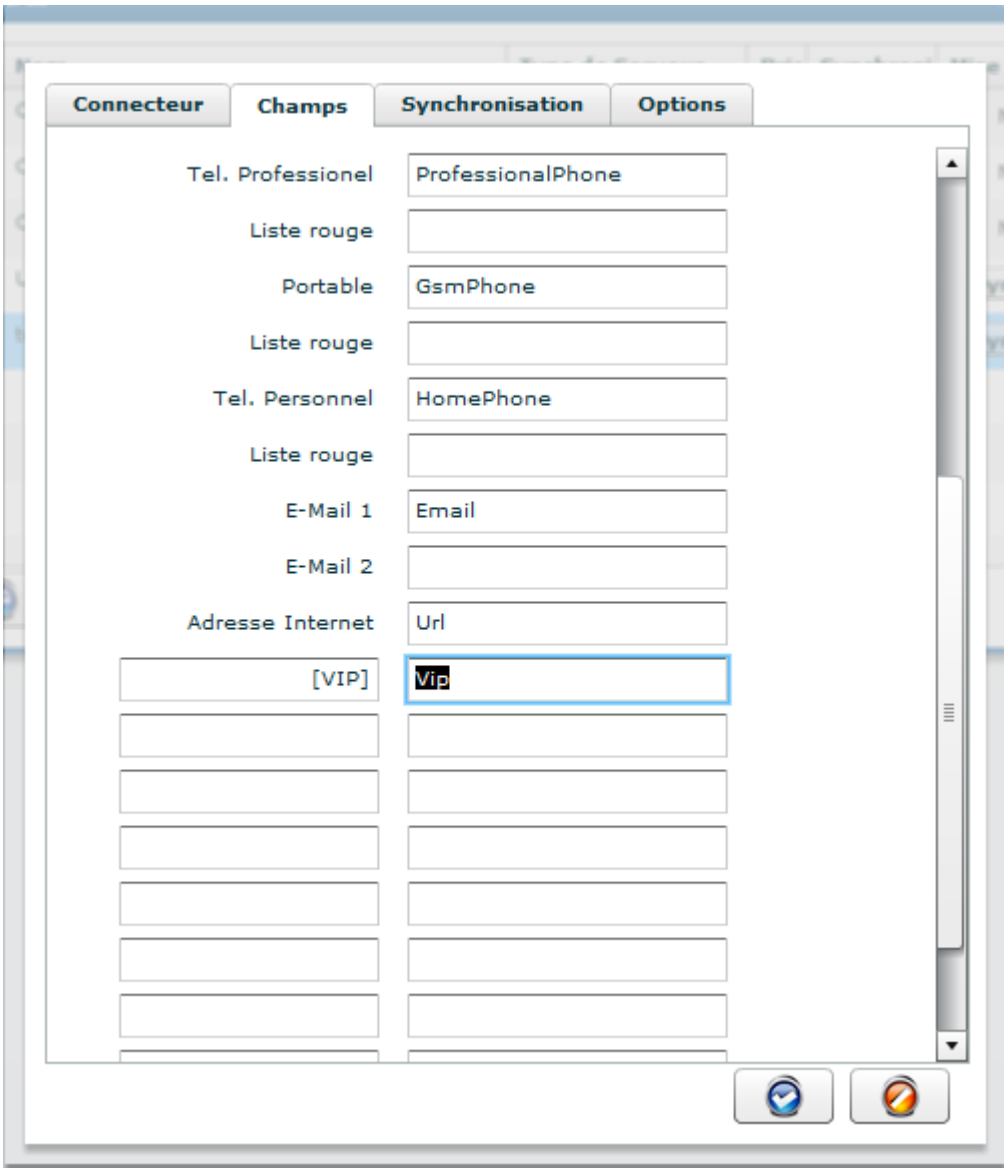
Par exemple, si les utilisateurs configurés dans l'administration possèdent des adresses email, la fusion des informations de ceux-ci se fera automatiquement avec un autre annuaire si la case « Fusionner les contacts » est cochée pour les annuaires en question.

L'avantage de cette fonctionnalité est de permettre à ces utilisateurs de voir dans la même fiche contact d'un de leur collègue des informations venant d'autres annuaires non disponibles depuis la liste des utilisateurs TWP.

8.2.3. Champs Spécifiques : Contact VIP

Afin d'activer la reconnaissance de contact VIP dans les applications Caller, Alerter et Smart Attendant, il faut configurer l'annuaire source comme expliqué ci-dessous :

Dans un des champs privées de l'annuaire vous devez mettre le libellé [VIP] et faire correspondre avec le nom du champ de votre annuaire externe (voir imprime écran ci-dessous) :



Ici, le champ de votre annuaire externe se nomme « Vip ». Ainsi si ce champ Vip de votre annuaire est renseigné, le contact sera vu comme un contact Vip et le contenu du champ sera affiché lors d'un appel entrant (dans une file d'attente partagée ou dans un appel direct).

8.2.4. Champs Spécifiques : liste rouge

Le système de la liste rouge permet de ne pas afficher le numéro de contact dans les applications, mais uniquement son nom.
La fonctionnalité est utile si l'utilisateur ne voit pas le numéro également de son poste physique : donc pour les postes Softphone ou d'autres postes liés à la liste rouge du PBX (dans ce dernier cas, l'annuaire du PBX doit être configuré dans l'administration).

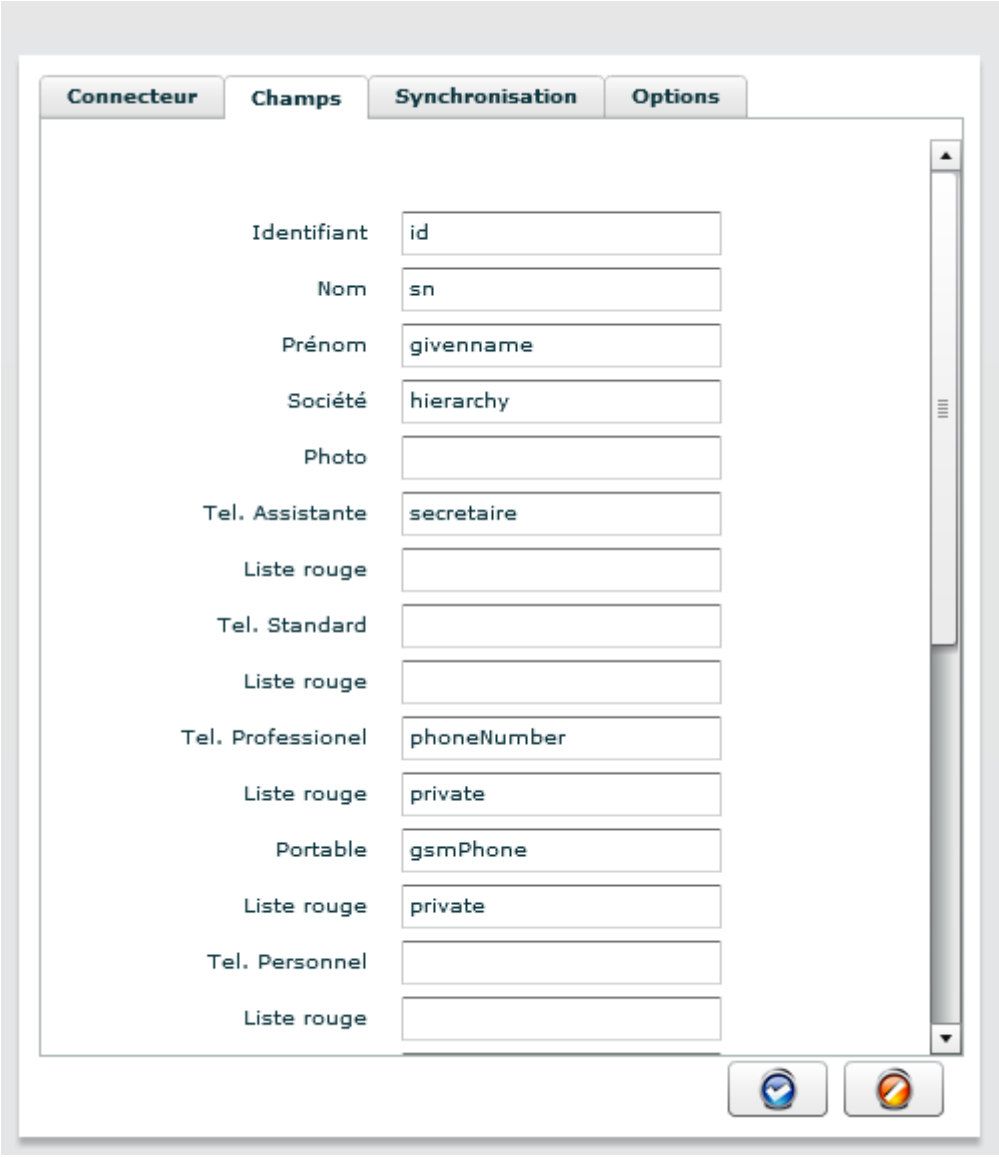
Pour configurer cette fonctionnalité, il faut remplir dans le champ spécifique « liste rouge » lié au type de numéro à cacher (ou pas), le nom du champ de la base externe contenant l'une des valeurs ci-dessous :

- Pour cacher le numéro du contact, la valeur doit être une des suivantes : « *1* » or « *true* » or « *yes* » or « *y* » or « *lr* » or « *rf* »
- Pour afficher le numéro du contact, la valeur doit être différente de celles-ci-dessus.

Exemple : Voici une base de données contenant des informations de contacts.

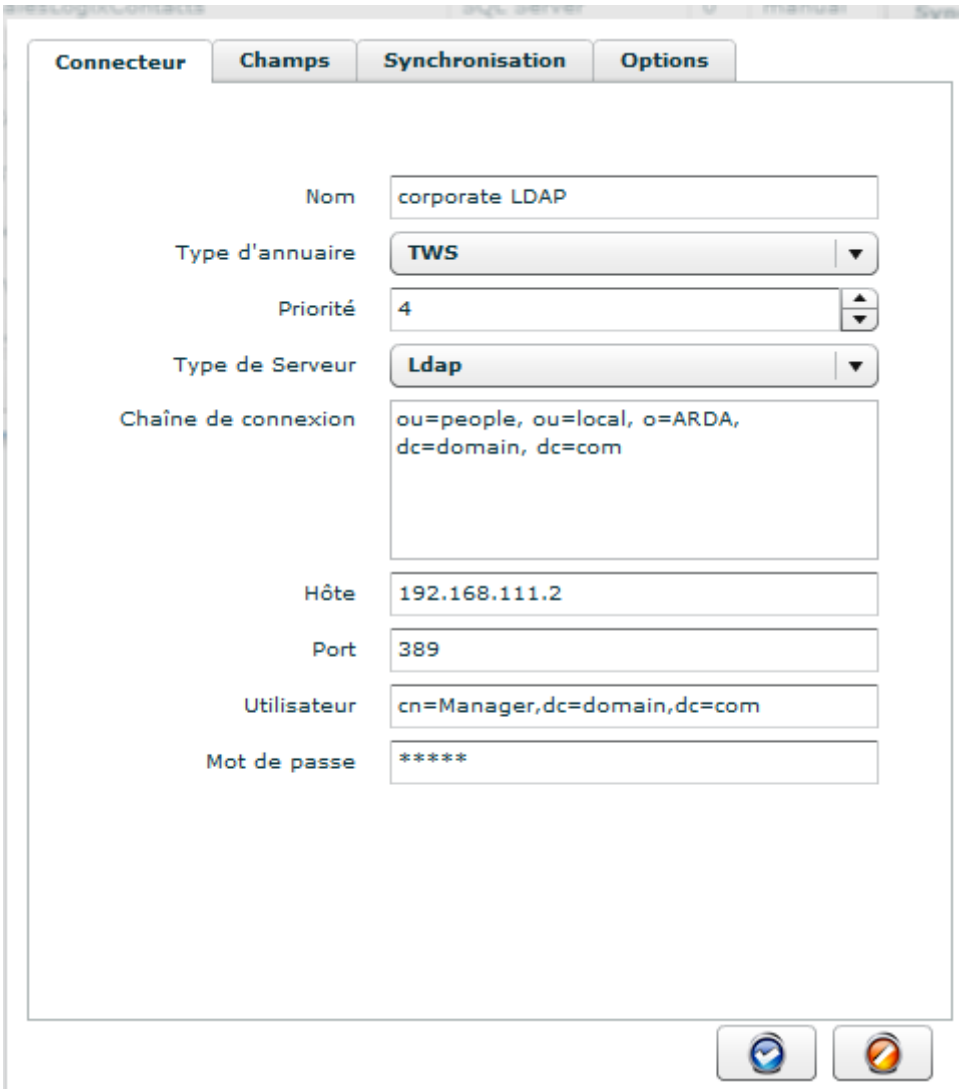
id	sn	givenname	hierarchy	secretaire	phoneNumber	gsmPhone	private
1	Francis	Dupont	Compta		6660		0
2	Noa	Hollande	Direction	4694	4594	0601020304	1
…							

Voici comment configurer l'annuaire pour que les numéros du contact « Noa Hollande » (sauf le numéro de l'assistant) ne soient pas affichés :



8.3. Création d'un connecteur LDAP

La connexion à un serveur d'annuaire LDAP se définit de la manière suivante.



Onglet connecteur:

Les champs suivants sont requis:

- **Chaîne de Connexion**: Base DN du connecteur
  Exemple : `ou=people, ou=local, o=ARDA, dc=domain, dc=com`
- **Hôte**: Adresse IP ou nom du serveur LDAP.
- **Port:** Port du serveur LDAP. (389 par défaut)
- **Nom**: Nom d'utilisateur ayant accès en lecture aux fiches à rapatrier
- **Mot de passe**: Mot de passe.

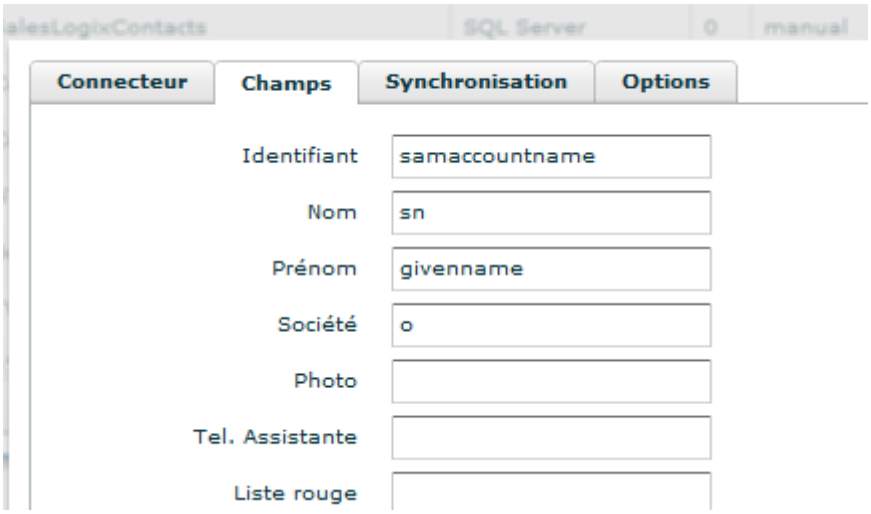
Remarque : Afin de valider les informations de connexion et le schéma LDAP, nous conseillons d'utiliser un outil tel que LDAP Admin (http://www.ldapadmin.org/).

Onglet champs:

Dans la partie champs, vous devez ajouter le nom des champs LDAP.

Attention: Vous avez besoin de remplir les noms en minuscule. Nous recommandons l'utilisation de LDAP Admin pour récupérer les noms des champs.

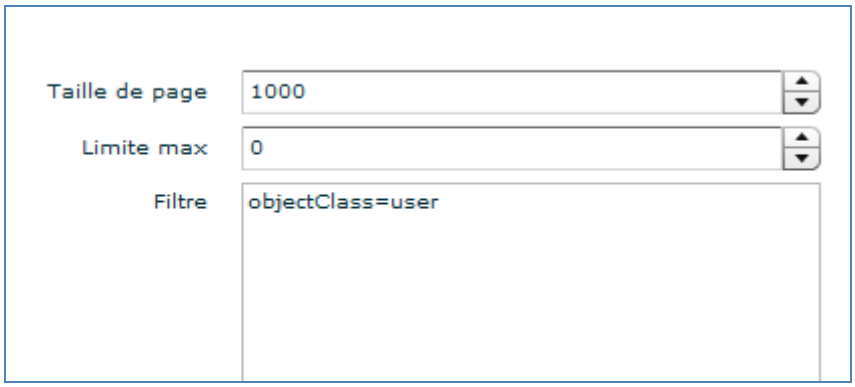
Ci-dessous est un exemple de récupération des champs dans un schéma de type people:



Onglet options:

Dans cet onglet vous pouvez ajouter des paramètres avancés pour une connexion LDAP.

- Taille de page: nombre de ligne chargé pour une requête
- Limite taille: nombre maximum de ligne chargé par le serveur LDAP
- Filtre: Filtre LDAP appliqué à la requête de recherche.

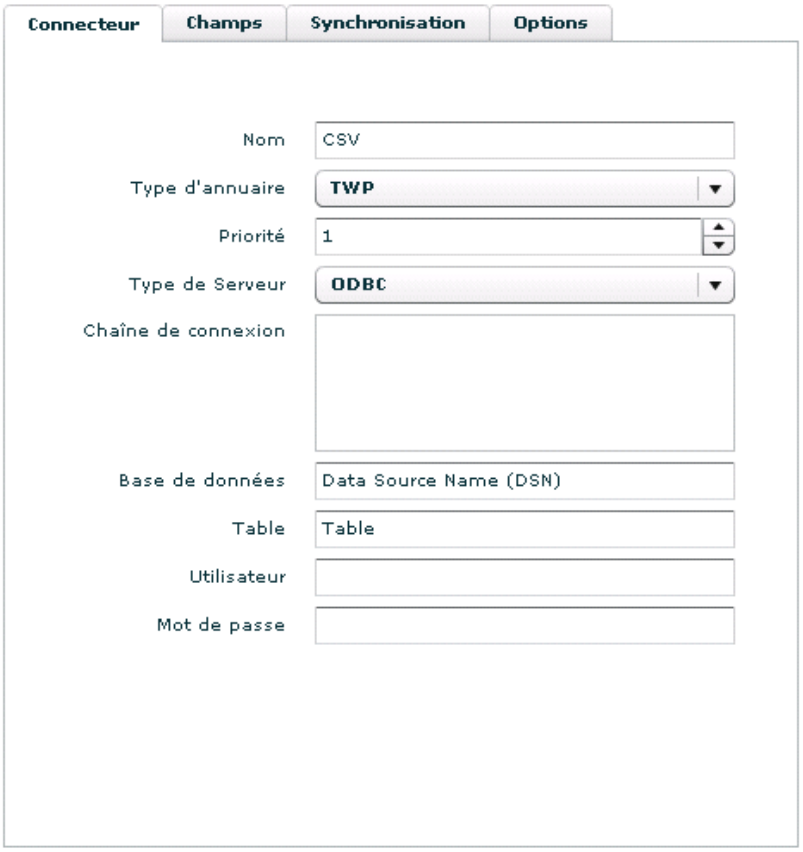


Sauvegarder les données et faire une synchronisation manuelle pour tester le bon fonctionnement du connecteur.

Remarque : Penser à donner des droits annuaires correspondant pour les utilisateurs devant accéder à cet annuaire.

8.4. Création d'un annuaire ODBC

Dans le menu *Informatique* / *Annuaire*, pour créer un nouveau connecteur annuaire ODBC, cliquez sur le bouton « + » et sélectionnez ODBC comme type de serveur:



8.4.1. Connecteur

Il existe 2 façons de créer une connexion ODBC. Notez que quelle que soit la manière vous devez installer les drivers correspondants à la base de données sur laquelle vous voulez vous connecter.

Connexion ODBC Système :

Dans ce cas il faut créer un connecteur ODBC système à l'aide du panneau de configuration Windows.

Les sources ODBC supportées par le serveur doivent être définies en 32 bits, sur un serveur 64 bits il faut utiliser le programme adbcad32.exe présent dans le répertoire C:\Windows\SysWOW64.

Lorsque la source ODBC système est définie vous pouvez ensuite :

- Soit définir dans le champ *Chaîne de connexion*: DSN=nom_de_votre_source_ODBC_Windows.
- Soit définir dans le champ *Base de données*, le nom de votre source ODBC Windows.

Table: remplissez le nom de la table dans laquelle TWP a besoin de récupérer des informations.

Connexion ODBC TWP :

Il est également possible de définir directement une chaine de connexion, dans ce cas il n'est pas utile de définir une source ODBC système à l'aide du panneau de configuration.

Ci-dessous quelques exemples de chaines de connexion :

MySQL:

```
Driver={mySQL};Server=myServerAddress;Port=3306;Option=131072;Stmt=;Database=myDataBase;User=myUsername;Password=myPassword;
```

AS/400:

```
Driver={Client Access ODBC Driver (32-bit)};System=my_system_name;Uid=myUsername;Pwd=myPassword;
```

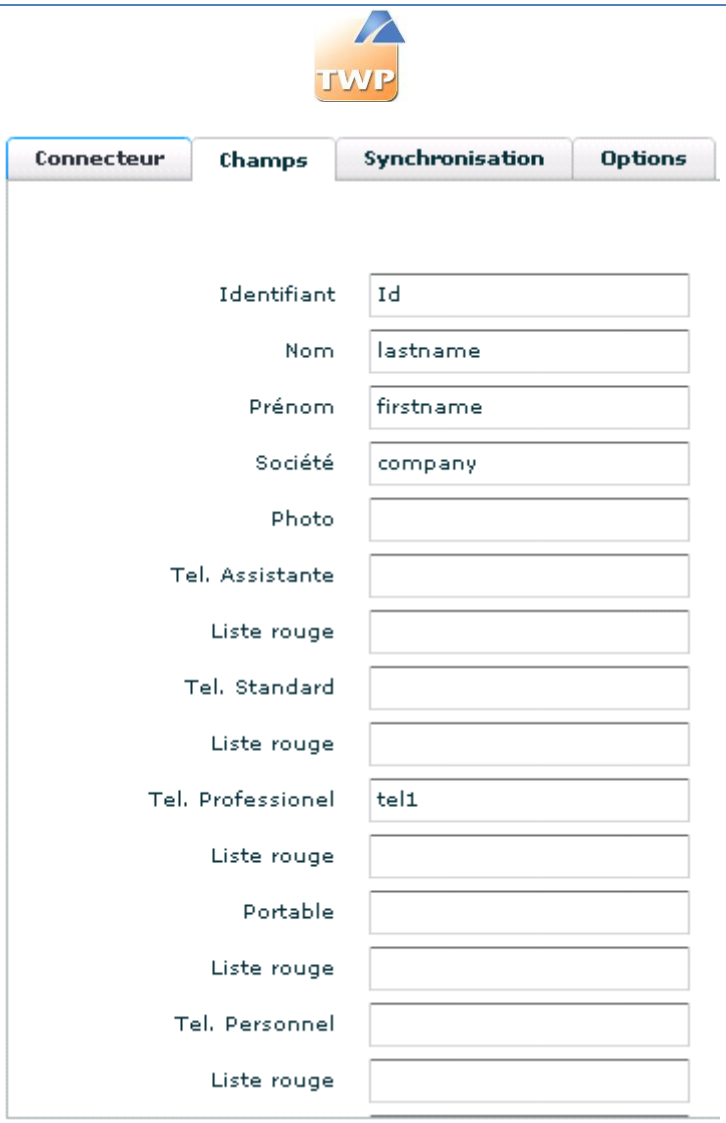
Excel: `Driver= {Microsoft Excel Driver (*.xls)};Dbq=C:\Annuaires\Annuaire.xls;`

Table: remplissez le nom de la table dans laquelle TWP a besoin de récupérer des informations.

8.4.2. Champs

***Attention** : Pour une connexion ODBC liée au fichier Excel, CSV, éviter tout nom de colonnes (de champs) contenant des caractères spéciaux, des ponctuations ou autres espaces pour ne pas avoir des erreurs lors de la tentative de synchronisation des annuaires en question.*

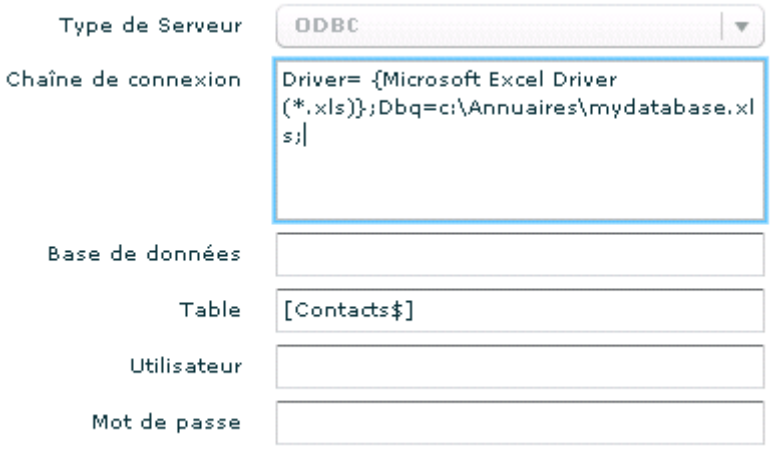
Ci-dessous un exemple de configuration de la correspondance entre les champs de l'annuaire TWP et les champs d'une feuille Excel ou d'un fichier CSV (la première ligne du fichier représente les champs).



N.B. : Parmi les champs à faire correspondre, le champ Identifiant est important dans la mise à jour des fiches de contact distinctes qui seront présentes dans les applications. Cela permettra également que ces applications puissent lier d'autres informations à la même fiche contact quelle que soit la mise à jour par nouvelle synchronisation de l'annuaire.

8.4.3. Exemples de connecteurs ODBC

Exemple d'un annuaire Excel:



Chaîne de connexion: `Driver= {Microsoft Excel Driver (*.xls)};Dbq=c:\Annuaires\Annuaire.xls;`

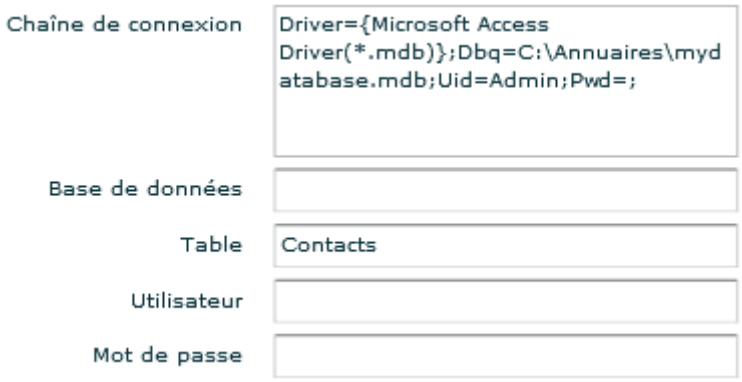
Table: [Contacts$] Nom de la feuille du fichier Excel « Contacts » contenant les données (N'oubliez pas d'ajouter $ à la fin entre les crochets).

Exemple d'un annuaire CSV:

Chaîne de Connexion: `Driver={Microsoft Text Driver (*.txt; *.csv)};Dbq=c:\Annuaires;`
Table: mydatabase.csv (nom du fichier CSV)

Attention: Nom du fichier ne doit pas contenir des caractères spéciaux.

Exemple d'un annuaire Access



Chaîne de Connexion:

```
Driver={Microsoft Access
Driver(*.mdb)};Dbq=C:\Annuaires\mydatabase.mdb;Uid=Admin;Pwd=;
```

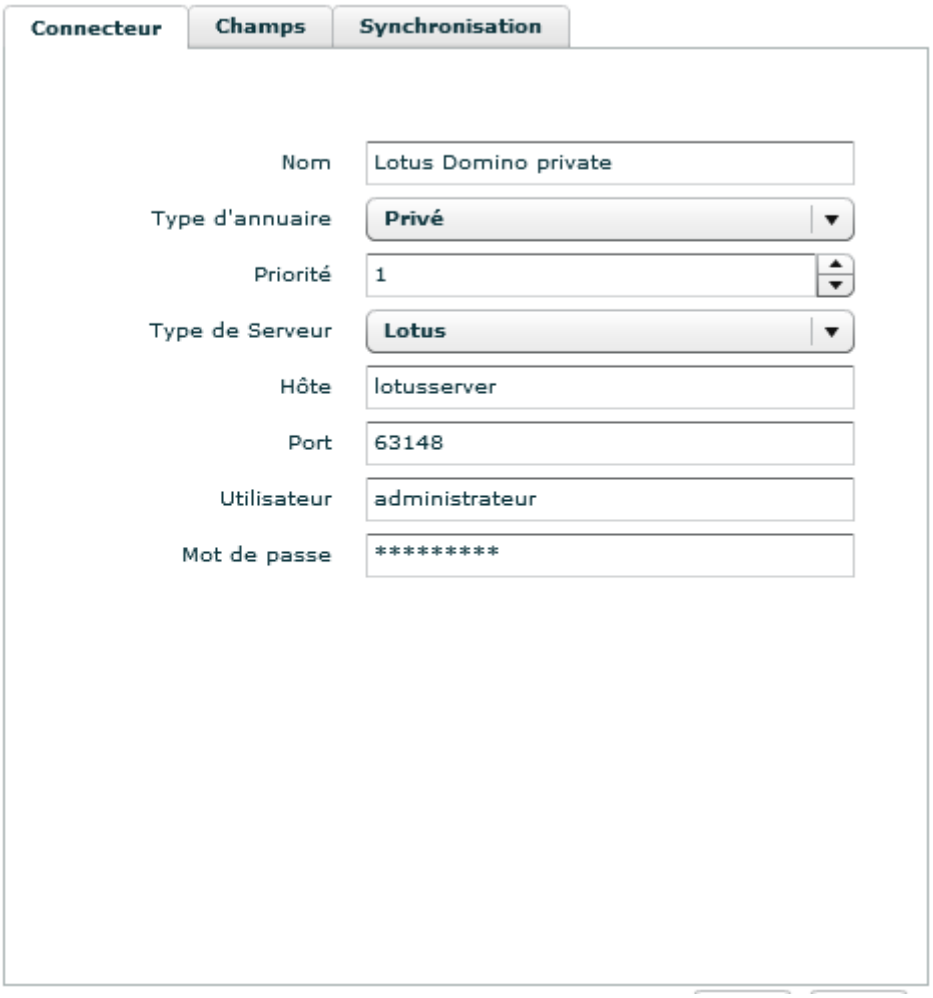
Table: Contacts

8.5. Configuration connecteur Lotus

8.5.1. Configuration connecteur public Lotus

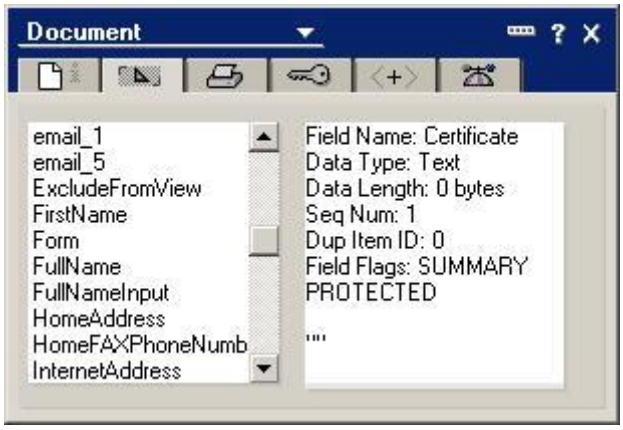
La configuration d'un annuaire public Lotus est similaire à un annuaire LDAP. Voir chapitre « 8.3 Connecteur LDAP »

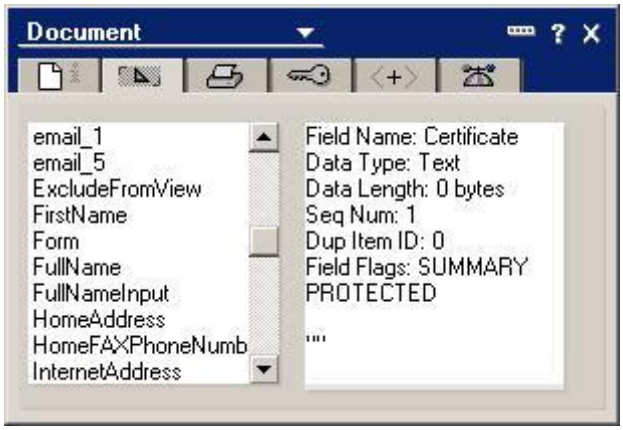
8.5.2. Configuration connecteur privé Lotus



- **Hôte:** Nom ou adresse IP du serveur Lotus
- **Port:** Port serveur Lotus (port par défaut: 389)
- **Utilisateur:** Nom de l'administrateur Lotus
- **Mot de passe:** Mot de passe de l'administrateur Lotus

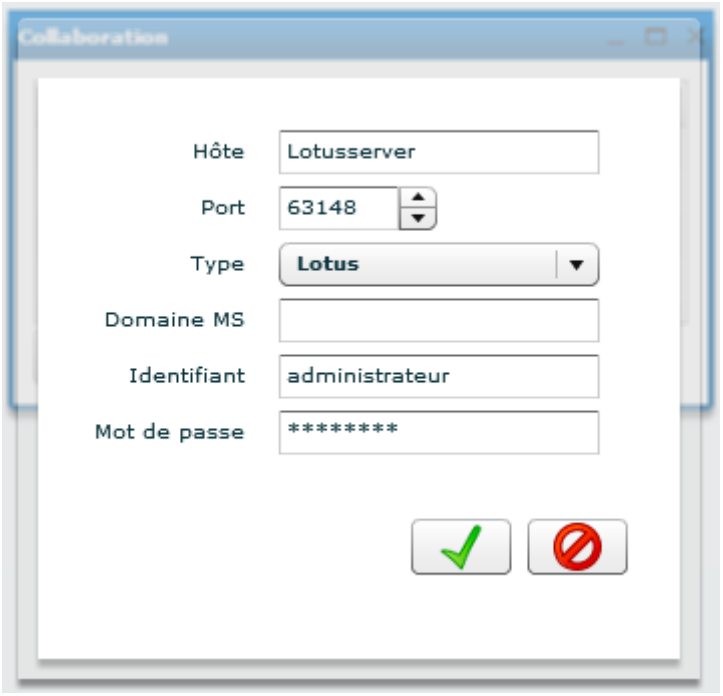
Pour connaître les différents champs à remplir dans la section Champs: Dans Lotus Notes, sélectionnez un contact, faites un clic droit et sélectionnez *Propriétés*, dans la deuxième section, vous trouverez la liste des champs à utiliser.


Document
email_1
email_5
ExcludeFromView
FirstName
Form
FullName
FullNameInput
HomeAddress
HomeFAXPhoneNumb
InternetAddress
Field Name: Certificate
Data Type: Text
Data Length: 0 bytes
Seq Num: 1
Dup Item ID: 0
Field Flags: SUMMARY
PROTECTED
""


Document
email_1
email_5
ExcludeFromView
FirstName
Form
FullName
FullNameInput
HomeAddress
HomeFAXPhoneNumb
InternetAddress
Field Name: Certificate
Data Type: Text
Data Length: 0 bytes
Seq Num: 1
Dup Item ID: 0
Field Flags: SUMMARY
PROTECTED
""

8.5.3. Connecteur Calendrier

Ouvrez "*Informatique*" puis "*Collaboration*", puis cliquez "+".



Définissez l'adresse IP ou le nom de votre serveur Lotus Domino.

Définissez l'identifiant et le mot de passe à utiliser pour se connecter au serveur Domino, cet utilisateur doit avoir le droit de lecture des calendriers des utilisateurs TWP.

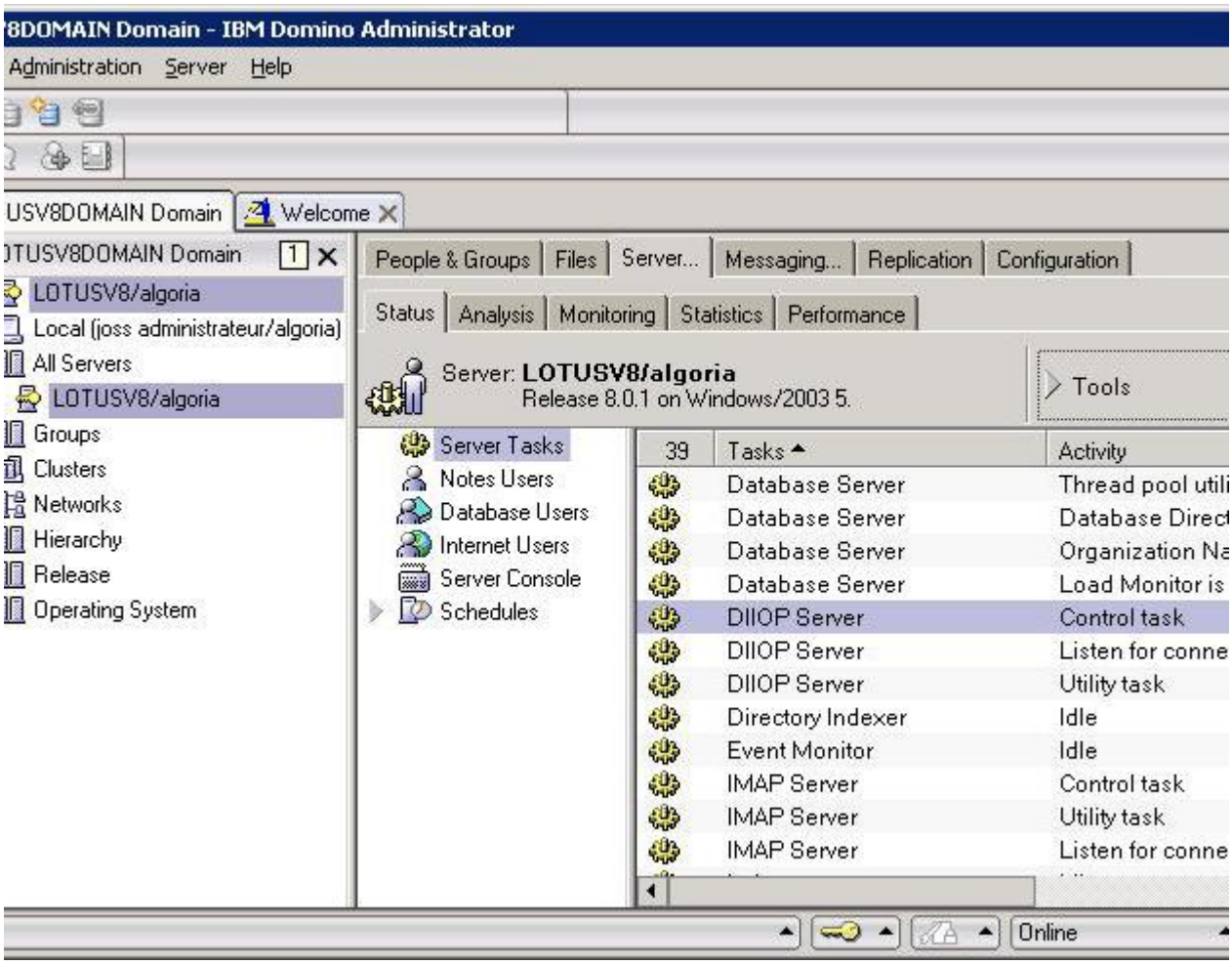
Afin d'être en mesure de voir la présence calendrier d'un utilisateur, assurez-vous que l'adresse mail de l'utilisateur renseignée dans le champ E-mail est une adresse valide.

8.5.4. Configuration du serveur Lotus

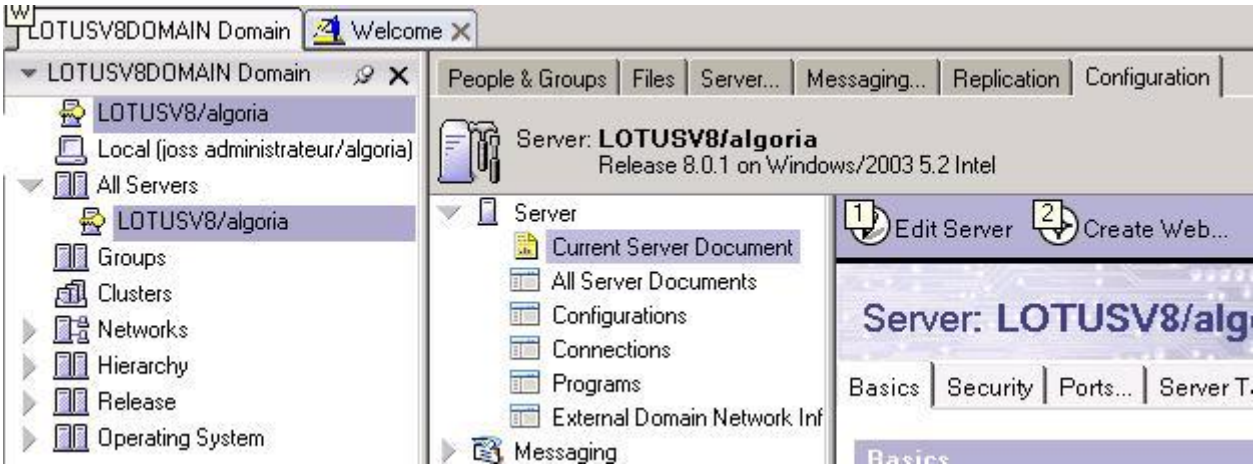
La version Domino Server 8.0.1 ou une version plus récente sont supportées :

Configuration DIIOP: DIIOP est utilisé par le connecteur d'annuaire.

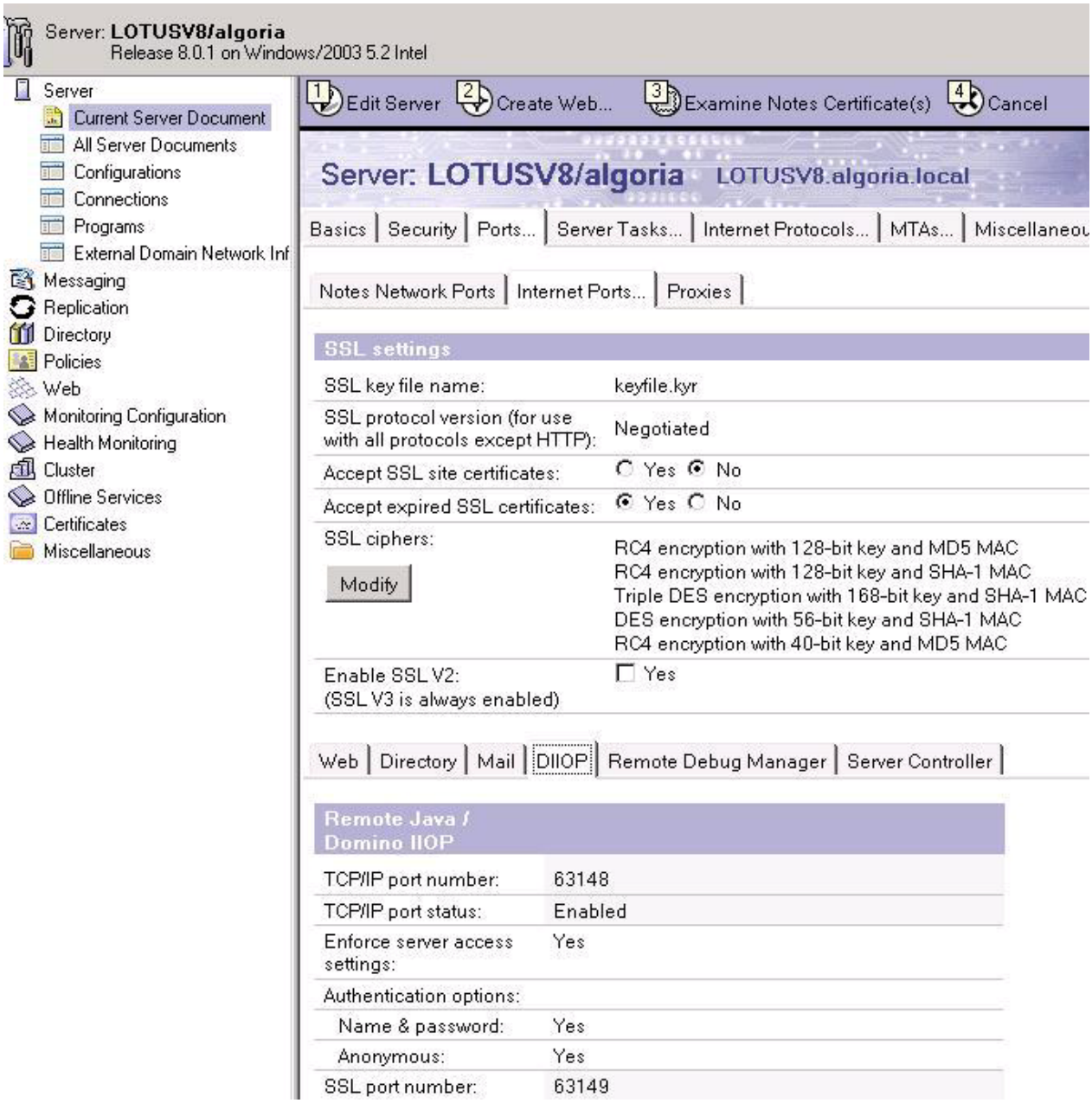
Pour vérifier si le service est activé, allez dans la section *Administration Server/Status* et cherchez le service *DIIOP*:



Sélectionnez la section *Configuration* et *Serveur actuel*.



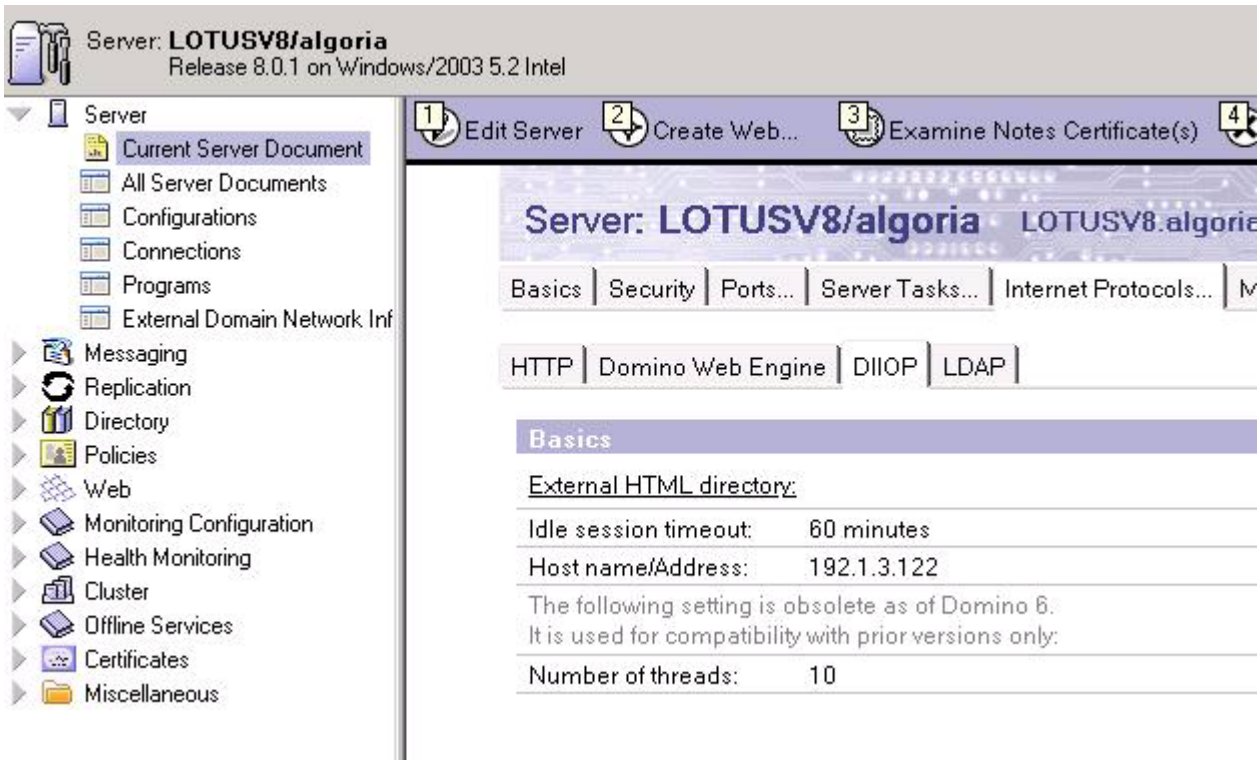
Vous devez à présent vérifier si les ports DIOP ports sont configurés:


Server: LOTUSV8/algoria
Release 8.0.1 on Windows/2003 5.2 Intel
Server
Current Server Document
All Server Documents
Configurations
Connections
Programs
External Domain Network Inf
Messaging
Replication
Directory
Policies
Web
Monitoring Configuration
Health Monitoring
Cluster
Offline Services
Certificates
Miscellaneous
1 Edit Server
2 Create Web...
3 Examine Notes Certificate(s)
4 Cancel
Server: LOTUSV8/algoria LOTUSV8.algoria.local
Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneou
Notes Network Ports | Internet Ports... | Proxies
SSL settings
SSL key file name: keyfile.kyr
SSL protocol version (for use with all protocols except HTTP): Negotiated
Accept SSL site certificates: Yes No
Accept expired SSL certificates: Yes No
SSL ciphers:
Modify
RC4 encryption with 128-bit key and MD5 MAC
RC4 encryption with 128-bit key and SHA-1 MAC
Triple DES encryption with 168-bit key and SHA-1 MAC
DES encryption with 56-bit key and SHA-1 MAC
RC4 encryption with 40-bit key and MD5 MAC
Enable SSL V2:
(SSL V3 is always enabled) Yes
Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller
Remote Java / Domino IIOP
TCP/IP port number: 63148
TCP/IP port status: Enabled
Enforce server access settings: Yes
Authentication options:
Name & password: Yes
Anonymous: Yes
SSL port number: 63149

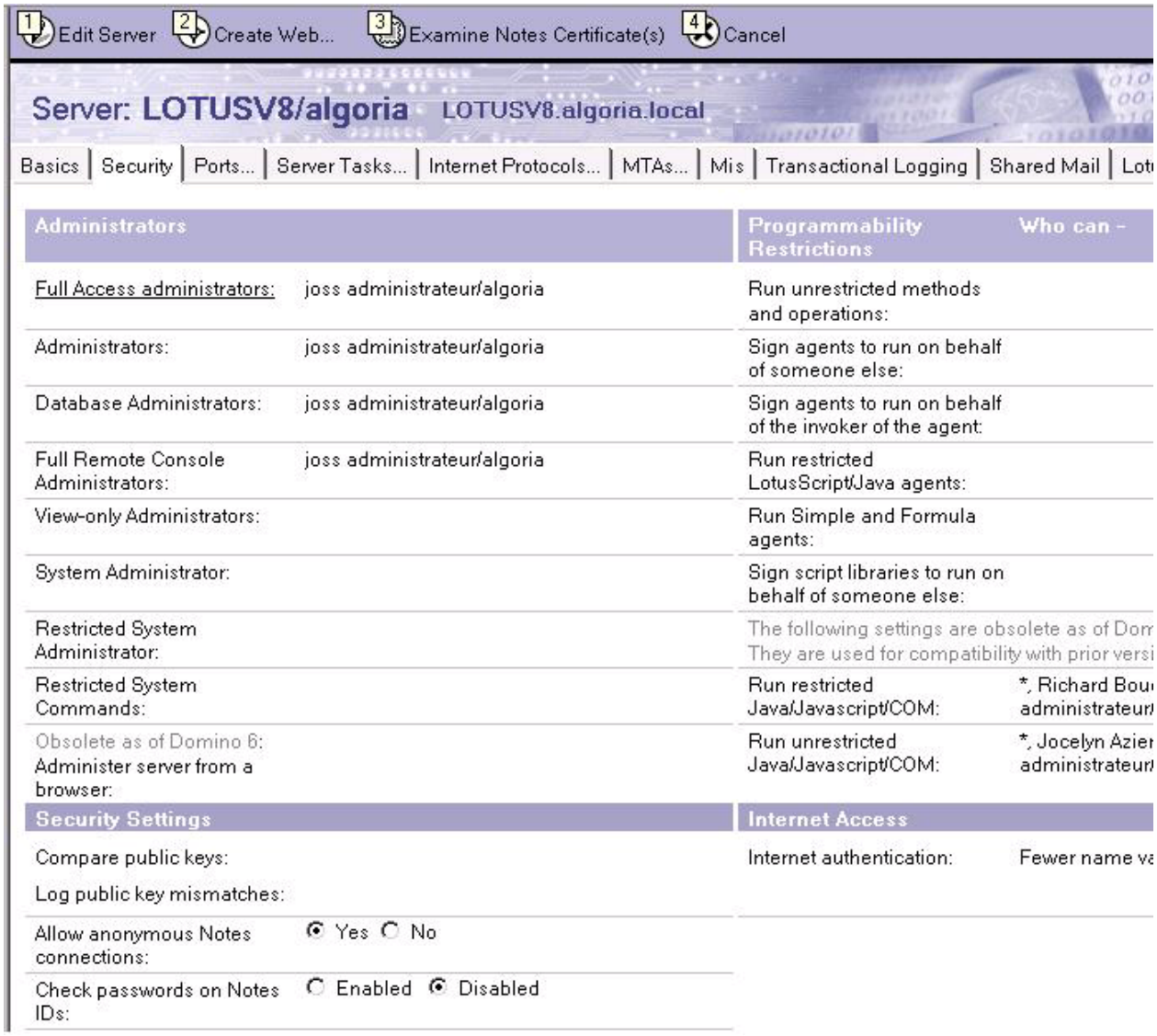
Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller

Remote Java / Domino IIOP	
TCP/IP port number:	63148
TCP/IP port status:	Enabled
Enforce server access settings:	Yes
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	63149
SSL port status:	Enabled
Authentication options:	
Client certificate:	N/A
Name & password:	Yes
Anonymous:	Yes

Vérifiez que le champ de l'adresse IP de votre serveur Lotus est renseigné :
Si ce champ est modifié, veuillez redémarrer le service Windows Lotus.

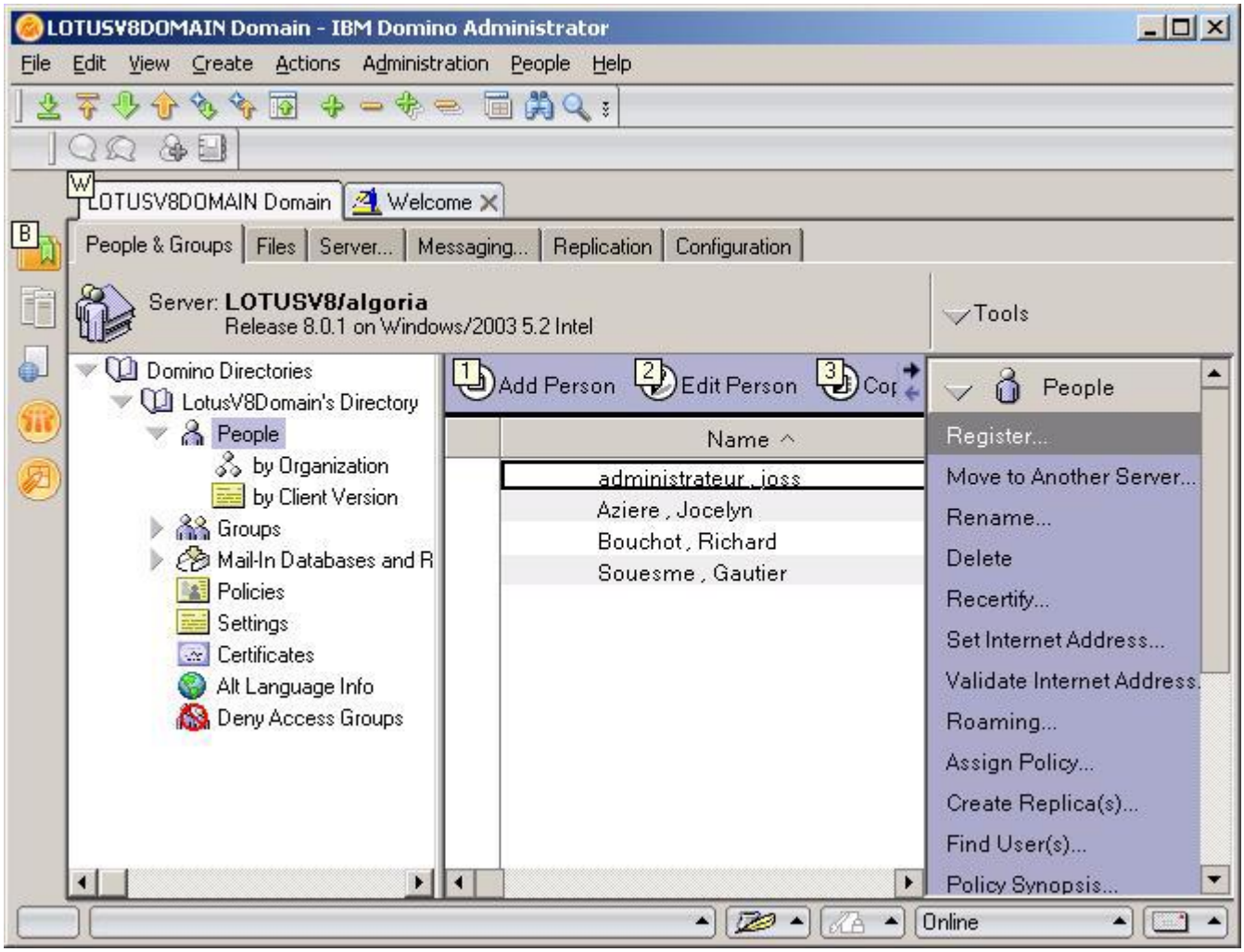


Dans l'onglet *Sécurité*, vous devez ajouter les options Java aux utilisateurs:



Création et configuration de l'utilisateur Lotus:

Pour créer un nouvel utilisateur, cliquez sur "*Register*":

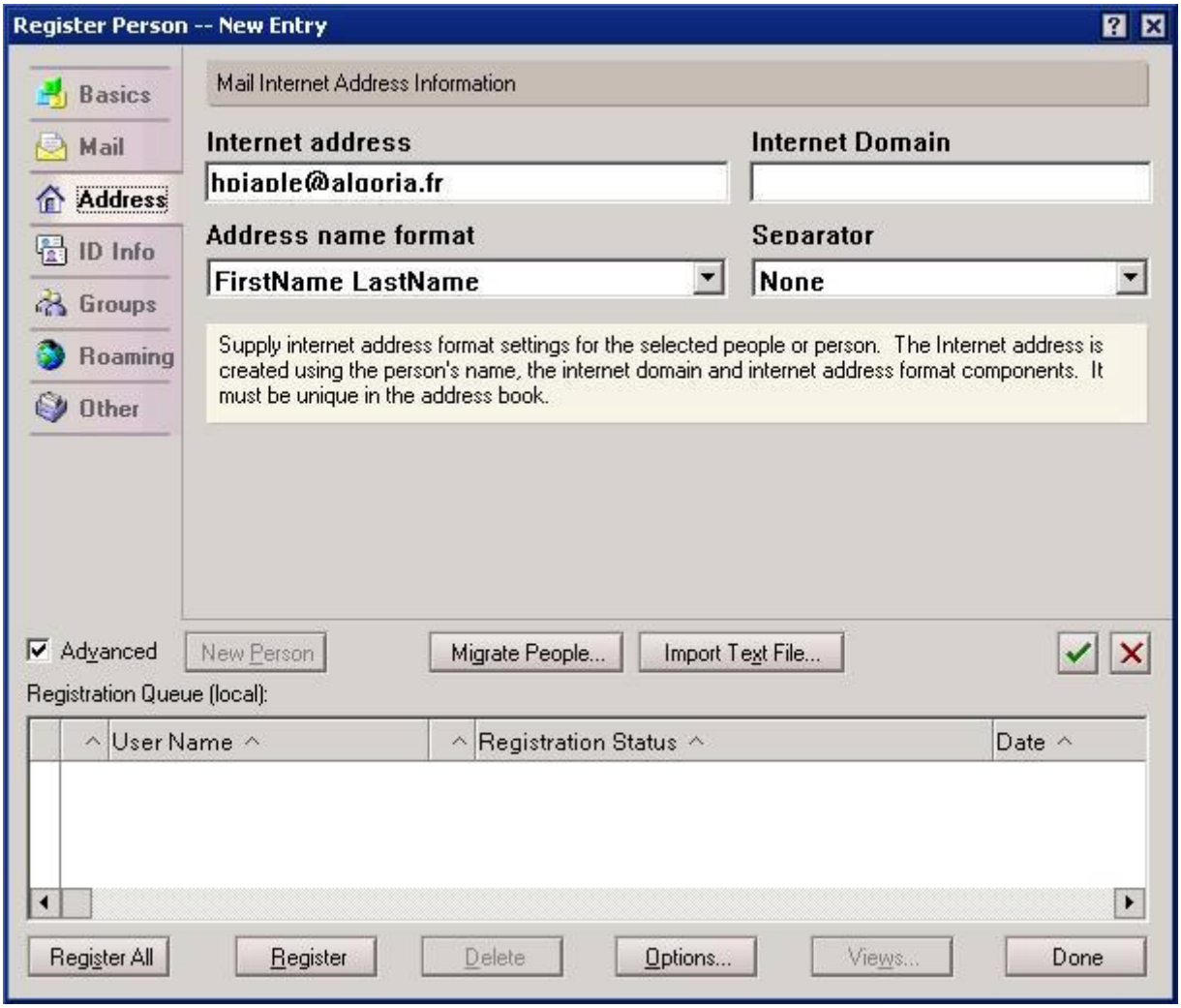

LOTUSV8DOMAIN Domain - IBM Domino Administrator
File Edit View Create Actions Administration People Help
LOTUSV8DOMAIN Domain
Welcome
People & Groups
Files
Server...
Messaging...
Replication
Configuration
Server: LOTUSV8/algoria
Release 8.0.1 on Windows/2003 5.2 Intel
Tools
Domino Directories
LotusV8Domain's Directory
People
by Organization
by Client Version
Groups
Mail-In Databases and R
Policies
Settings
Certificates
Alt Language Info
Deny Access Groups
1 Add Person
2 Edit Person
3 Cop
Name
administrateur , joss
Aziere , Jocelyn
Bouchot , Richard
Souesme , Gautier
People
Register...
Move to Another Server...
Rename...
Delete
Recertify...
Set Internet Address...
Validate Internet Address...
Roaming...
Assign Policy...
Create Replica(s)...
Find User(s)...
Policy Synopsis...
Online

Remplissez les champs requis.

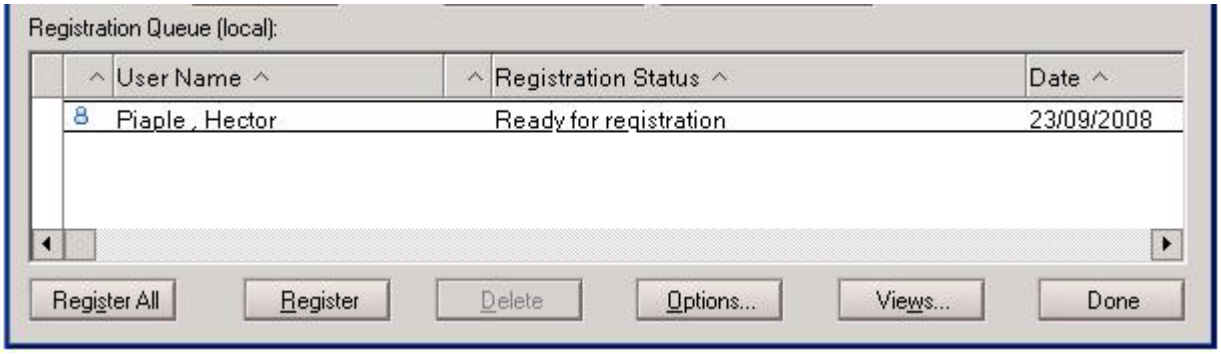
Attention: *Le nom court (Short name) doit être le même que celui de l'utilisateur TWP.*

Sélectionnez la section Adresse. Dans Adresse Internet, renseignez l'email de l'utilisateur. Renseigner l'ensemble des champs requis.

Attention: *cette adresse email doit être la même que celle renseignée dans TWP.*



Une fois que tous vos contacts ont été créés, cliquez sur "Enregistrer tout".

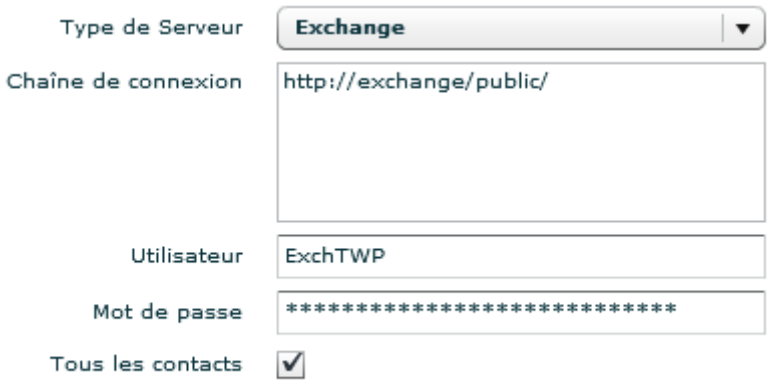


8.6. Annuaires / Calendrier MS Exchange 2003/2007

8.6.1. Création d'un connecteur annuaire public

La connexion à un serveur d'annuaire Exchange se définit de la manière suivante.

Onglet Connecteur:



Type d'annuaire:

- *Contacts publics* : sélectionner TWP pour une connexion aux annuaires publics.
- *Contacts privés utilisateur* : Sélectionner **Privé** pour une connexion aux contacts privés de l'utilisateur exchange.

Attention : Assurez-vous que l'adresse mail de l'utilisateur est renseignée dans le champ E-mail et est son adresse mail Exchange.

Type de serveur: Exchange.

Chaîne de Connexion: C'est l'URL qui ouvre l'annuaire Exchange, TWP supporte des URLs HTTP et HTTPS. Exchange 2007 utilise le protocole HTTPS par défaut.
L'URL est généralement: http://exchangeservername/public.

Identifiant /mot de passe: Le login utilisé par TWP pour se connecter au serveur exchange.

- *Contacts publics* : Ce compte doit avoir le droit en lecture et écriture sur l'annuaire Exchange.
- *Contacts privés utilisateur* : Ce compte doit avoir le droit en lecture sur les contacts privés de la boîte de l'utilisateur.

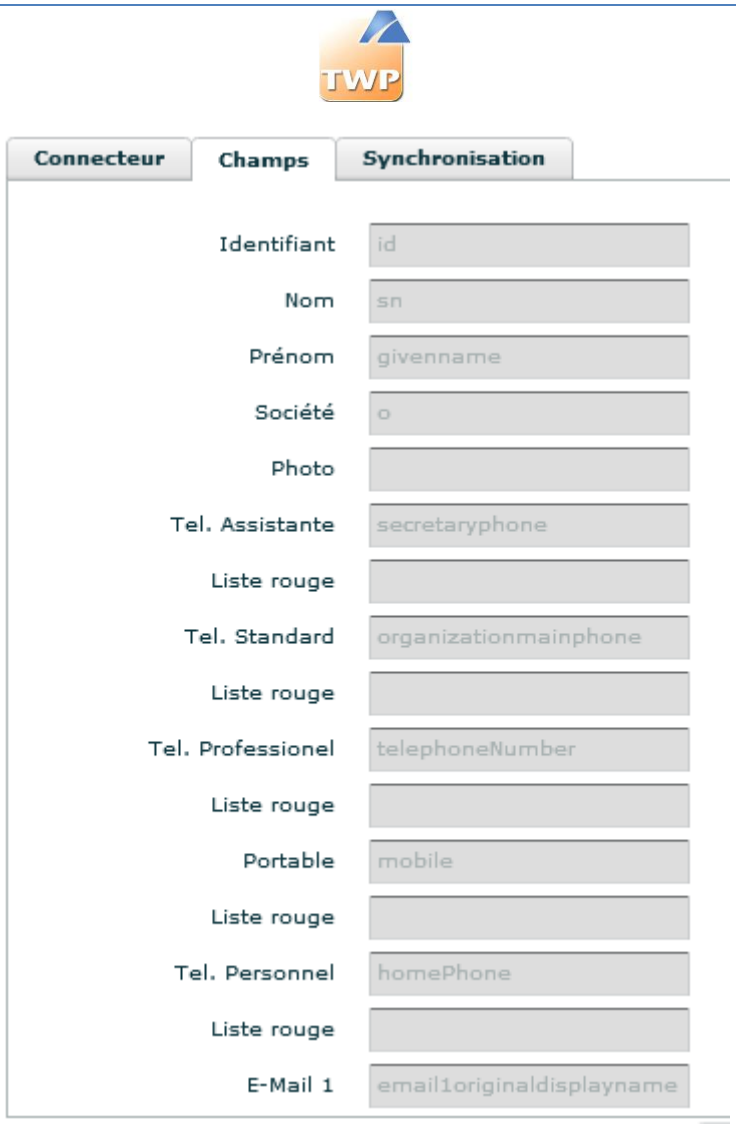
Tous les contacts: Le champ "Tous les contacts" permet de chercher tous les contacts dans les sous-dossiers/annuaires.

Si vous voulez limiter la synchronisation des contacts à un annuaire, ajoutez le nom de l'annuaire à la fin de l'URL de connexion, par exemple: "http://192.168.0.1/public/commerce" et décochez la case "Tous les contacts".

Attention : Assurez-vous également que les autorisations sont correctement définies, voir chapitre 7.4.2.

Onglet Champs:

Pour les annuaires Exchange, les champs sont pré-remplis.



Cependant, vous pouvez ajouter des champs dans les cellules des champs privés. 10 champs privés peuvent être utilisés, de *Réservé 0 (Private0)* à *9 (Private9)*. Ces champs peuvent être configurés manuellement.

Voir ci-dessous des exemples de champs Exchange qui pourraient être utilisés:

- givenName = prénom
- sn = nom
- o = société
- secretaryphone = numéro de téléphone assistant
- mobile = numéro portable
- homePhone = numéro maison
- organizationmainphone = numéro standard
- account = compte
- authorig
- bday = date de naissance

- businesshomepage = page web de la société (url)
- callbackphone
- customerid = identifiant client
- departement = department
- email1 = E-mail 1
- email2

- email3
- employeenumber = numéro poste téléphonique de l'employé
- facsimiletelephonenumber = numéro fax
- ftpsite = site ftp
- homeCity = ville de l'employé
- homeCountry = pays de l'employé
- homefax = numéro fax maison
- homephone2 = numéro maison 2
- telephonenumber2 = numéro é
- office2telephonenumber = poste de l'employé 2
- othermobile = 2ème numéro de portable
- otherTelephone = autre numéro téléphone
- pager = pager

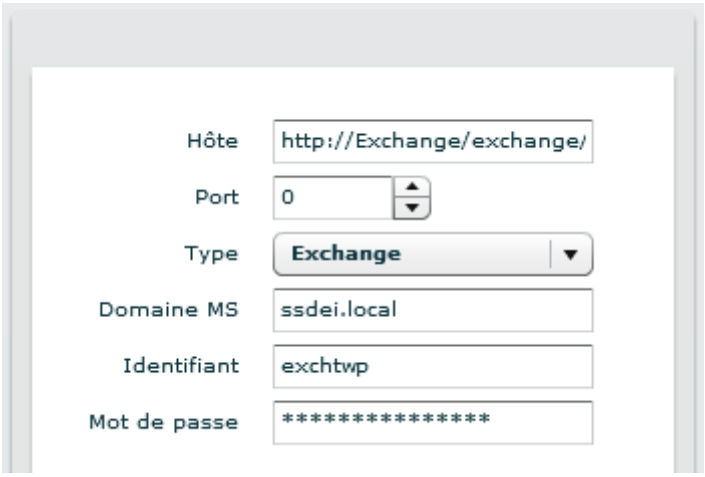
Tous les champs sont accessibles à cette adresse :
http://msdn.microsoft.com/en-us/library/office/aa563261(v=exchg.80).aspx

Information: Positionner toujours le préfixe urn:schemas:contacts: au cas où le champ simple ne fonctionnerait pas
E.g. urn:schemas:contacts:mobile

8.6.2. Connecteur Calendrier

TWP permet aux utilisateurs de voir le statut calendrier des autres utilisateurs TWP dans leur liste de contacts ainsi que dans la recherche annuaire (voir guide d'utilisation TWP Caller).

Dans le menu administration, ouvrez "Informatique" puis "Collaboration", puis cliquez “+”.



Il est possible de définir plus d'un lien.

Définissez l'URL de votre serveur Exchange en fonction de la configuration de votre serveur : http://server_exchange/exchange/ ou https://server_exchange/exchange/.

Définissez l'identifiant et mot de passe à utiliser pour se connecter au serveur Exchange : cet utilisateur doit avoir le droit de lecture des calendriers des utilisateurs TWP.

Attention : Afin d'être en mesure de voir la présence calendrier d'un utilisateur TWP, assurez-vous que l'adresse email renseignée dans le champ Email de l’utilisateur est bien son adresse email Exchange.

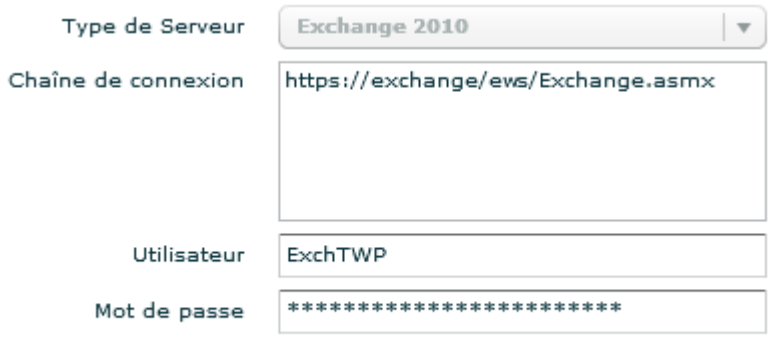
Attention : Assurez-vous également que les autorisations sont correctement définies, voir chapitre 7.4.3.

8.7. Annuaires / Calendrier MS Exchange 2010 / Office 365

8.7.1. Création du connecteur public / privé

La connexion à un serveur d'annuaire Exchange ou Office 365 se définit de la manière suivante.

Onglet Connecteur:



Type d'annuaire:

- *Contacts publics* : sélectionner TWP pour une connexion aux annuaires publics. ***(uniquement Exchange 2010)***
- *Contacts privés utilisateur* : Sélectionner **Privé** pour une connexion aux contacts privés de l'utilisateur exchange.

Attention : Assurez-vous que l'adresse mail de l'utilisateur est renseignée dans le champ E-mail et est son adresse mail Exchange.

Type de serveur: Exchange 2010. ***(Même pour une connexion vers Office 365)***

Chaîne de Connexion: C'est l'URL qui donne droit aux services web Exchange permettant d'accéder aux contacts.
L'URL pour Exchange 2010 se présente comme ceci : https://exchangeservername/ews/exchange.asmx.
Pour Office 365, l'URL est : https://outlook.office365.com/ews/Exchange.asmx.

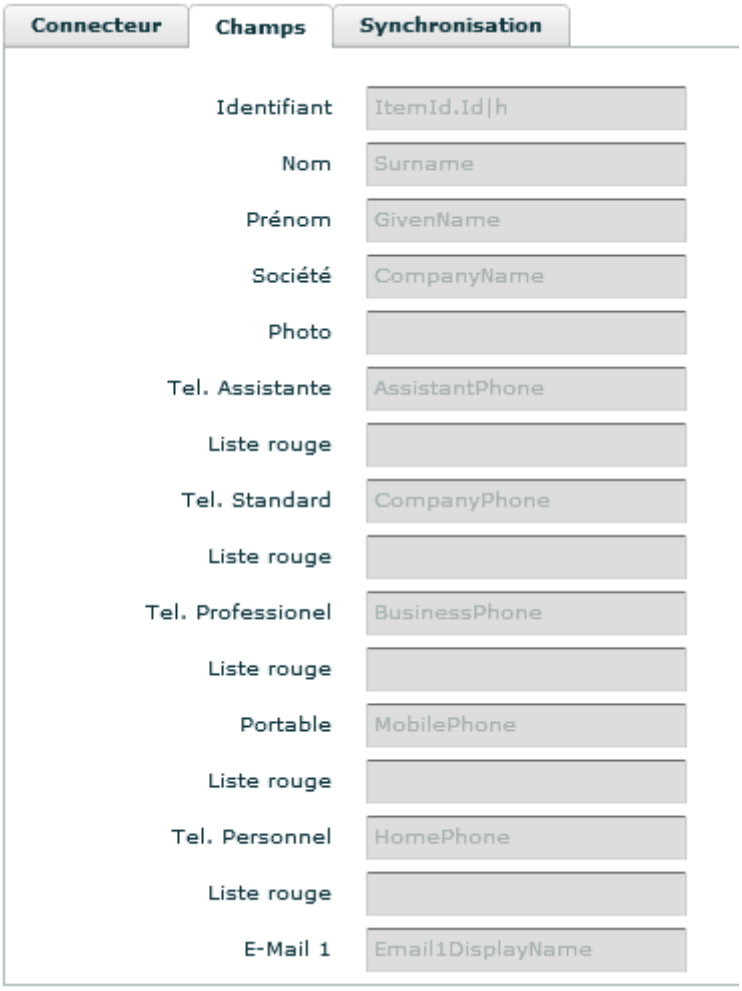
Identifiant /mot de passe: Le login utilisé par TWP pour se connecter au serveur exchange.

- *Contacts publics* ***(uniquement Exchange 2010)*** : Ce compte doit avoir le droit en lecture sur les dossiers publics.
- *Contacts privés utilisateur* : Il est possible d'autoriser la connexion de différentes manières. Voir chapitre 8.7.5.

Attention : Assurez-vous également que les autorisations sont correctement définies, voir chapitre 7.4.2.

Onglet Champs:

Pour les annuaires Exchange, les champs sont pré-remplis.



Cependant, vous pouvez ajouter des champs dans les cellules des champs privés. 10 champs privés peuvent être utilisés, de *Réservé 0 (Private0)* à *9 (Private9)*. Ces champs peuvent être configurés manuellement.

Voir ci-dessous des exemples de champs Exchange qui pourraient être utilisés:

- AssistantName
- AssistantPhone
- Birthday
- BusinessAddress
- BusinessAddressCity
- BusinessAddressCountry
- BusinessAddressPostalCode
- BusinessAddressState
- BusinessAddressStreet
- BusinessFax
- BusinessHomePage
- BusinessPhone
- BusinessPhone2
- CallbackPhone

- CarPhone
- Categories
- Children
- Comment
- Companies
- CompanyName
- CompanyPhone
- CompleteName
- ConversationId
- CreatedTime
- Culture
- Department
- DisplayName
- EffectiveRights
- Email1Address
- Email1DisplayAs
- Email1DisplayName
- Email1Type
- Email2Address
- Email2DisplayAs
- Email2DisplayName
- Email2Type
- Email3Address
- Email3DisplayAs
- Email3DisplayName
- Email3Type
- EntryId
- Gender
- Generation
- GivenName
- HasAttachments
- HasPicture
- HomeAddress
- HomeAddressCity
- HomeAddressCountry
- HomeAddressPostalCode
- HomeAddressState
- HomeAddressStreet
- HomeFax
- HomePhone
- HomePhone2
- Id
- Importance
- Initials
- InstantMessengerAddress1
- InstantMessengerAddress2
- InstantMessengerAddress3
- IsAssociated
- IsHidden
- ItemClass
- ItemId
- JobTitle
- LastModifiedTime
- LastModifierName
- Manager
- MiddleName
- Mileage

- MimeContent
- MobilePhone
- Nickname
- OfficeLocation
- OtherAddress
- OtherAddressCity
- OtherAddressCountry
- OtherAddressPostalCode
- OtherAddressState
- OtherAddressStreet
- OtherFax
- OtherPhone
- Pager
- ParentId
- PrimaryPhone
- Profession
- RadioPhone
- SearchKey
- SelectedMailingAddress
- Sensitivity
- Size
- SpouseName
- Subject
- Surname
- Title
- WeddingAnniversary

Tous les champs sont accessibles à cette adresse :
http://msdn.microsoft.com/en-us/library/office/aa581315(v=exchg.140).aspx

8.7.2. Astuce Exchange 2010 : connecteur public avec sélection de dossier(s)

Dans la chaîne de connexion d'un connecteur Exchange 2010, il est possible de renseigner pour la synchronisation uniquement certains dossiers.

Format d'une chaîne de connexion avec sélection de dossiers :
https://exchange_server/ews/Exchange.asmx|public|dossier1,dossier2/sous-dossier1/sous-dossier2,...

Attention : Il faut bien suivre l'arborescence des dossiers et respecter la casse. Plusieurs dossiers peuvent être renseignés en les séparant par des virgules « , ». Les sous-dossiers sont séparés des dossiers parents par des « / ».

Exemple : https://exchange_server/ews/Exchange.asmx|public|General/Algo Distributeurs/Export,General/Algo Fournisseurs

8.7.3. Astuce Office 365 : annuaire privé en public

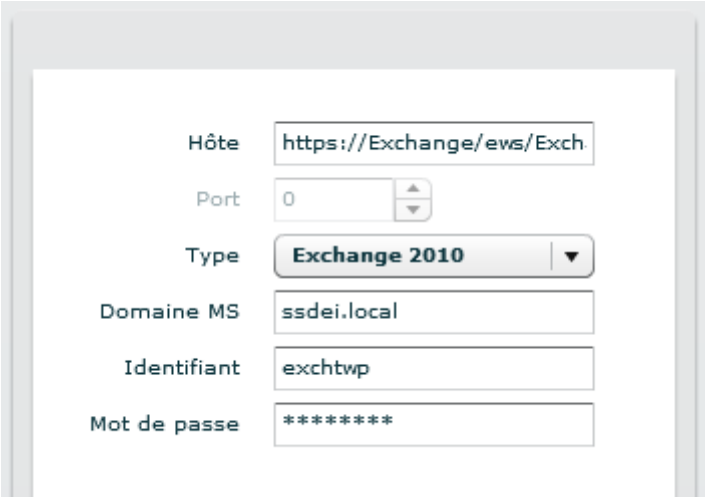
Pour permettre aux utilisateurs de visualiser les mêmes contacts provenant d'un seul connecteur à Office 365, il est possible de configurer celui-ci en public.
Ce connecteur synchronisera de toute façon les contacts privés d'un seul utilisateur mais les rendra public. Les informations à renseigner sont ci-après :

Type d'annuaire : TWS
Type de serveur : Exchange 2010
Chaîne de connexion : https://outlook.office365.com/ews/Exchange.asmx|user
Utilisateur : email du compte à synchroniser

8.7.4. Connecteur Calendrier

TWP permet aux utilisateurs de voir le statut calendrier des autres utilisateurs TWP dans leur liste de contacts ainsi que dans la recherche annuaire (voir guide d'utilisation TWP Caller).

Dans le menu administration, ouvrez "Informatique" puis "Collaboration", puis cliquez "+".



Il est possible de définir plus d'un lien.

Définissez l'URL de votre serveur Exchange : https://server_exchange/ews/Exchange.asmx
Définissez l'URL de votre serveur Office 365 : https://outlook.office365.com/ews/Exchange.asmx

Définissez l'identifiant et mot de passe à utiliser pour se connecter au serveur Exchange ou à Office 365 : cet utilisateur doit avoir le droit de lecture des calendriers des utilisateurs TWP. Voir également le chapitre 8.7.5 pour les comptes de connexion des connecteurs.

Attention : Afin d'être en mesure de voir la présence calendrier d'un utilisateur TWP, assurez-vous que l'adresse email renseignée dans le champ Email de l'utilisateur est bien son adresse email Exchange.

Attention : Assurez-vous également que les autorisations sont correctement définies, voir chapitre

7.4.3.

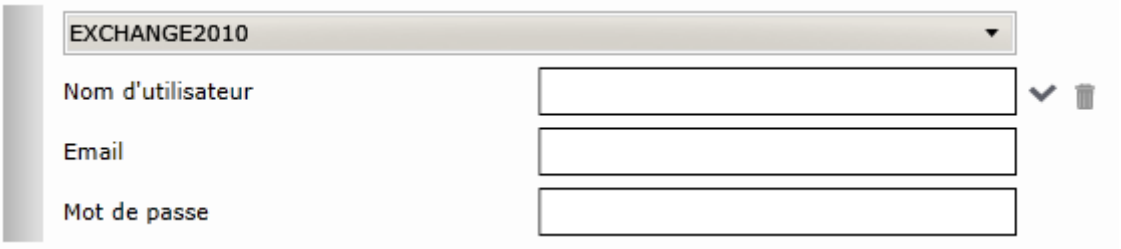
8.7.5. Comptes de connexion des connecteurs privés

Pour autoriser les connecteurs à récupérer les contacts privés et les rendez-vous Calendrier des utilisateurs Exchange 2010 ou Office 365, il est possible de définir des comptes de connexion de différentes manières :

- *Compte Exchange/Office 365 ayant accès aux boîtes des utilisateurs (chapitre 8.7.6)* : ce compte doit avoir le droit en lecture sur les contacts privés et le calendrier de la boîte de l'utilisateur.

- *Compte Exchange/Office 365 sans droit particulier* : chaque utilisateur pourra dans son client de messagerie Outlook ajouter l'autorisation en relecteur pour le compte en question.

- *Compte Exchange/Office 365 de collaboration* : à renseigner directement depuis l'application Caller (Menu *Préférence*, *Contact*, *Collaboration*).



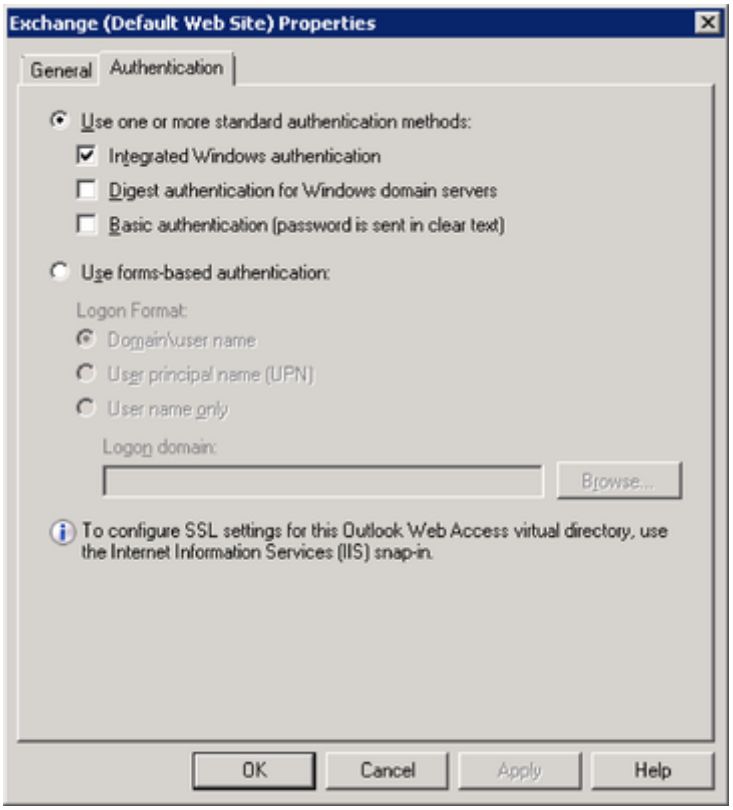
  - *Nom d'utilisateur* : Nom de l'utilisateur qui est autorisé à lire le contenu de la boite mail (peut être le même que l'Email)
  - *Email* : email du compte à synchroniser
  - *Mot de passe* : Mot de passe du compte à synchroniser

8.7.6. Configuration serveur Exchange : Accès aux boîtes utilisateur (contacts privés et calendriers)

Configuration du type d'authentification

Le serveur utilise l'authentification NTLM avec les modes "Integrated Windows Authentication " ou "Basic authentication".
Après un changement de type d'authentification il faut redémarrer le serveur exchange.
Dans Exchange Management Console, Microsoft Exchange -> Server Configuration -> Mailbox -> Tab WebDAV, double cliquer sur :

- Exchange (Default Web Site) et cocher “Integrated Window authentication" ou "Basic authentication" dans l’onglet “Authentication”.



- Exchweb (Default Web Site) et cocher “Integrated Window authentication" ou "Basic authentication" dans l’onglet “Authentication”.

- Public (Default Web Site) et cocher “Integrated Window authentication" ou "Basic authentication" dans l’onglet “Authentication”.

Configuration des droits d'accès

2 solutions possibles

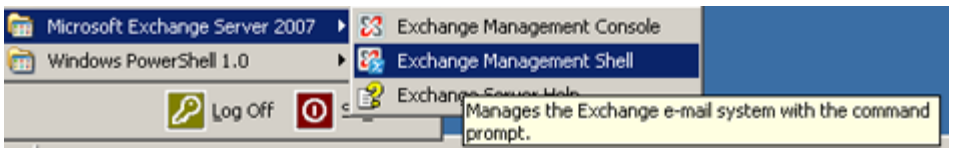
1. Donner les droits d’accès sur toutes les boîtes Exchange 2007 server
2. Donner les droits d’accès depuis MS Outlook

Solution 1: Donner les droits « Receive-As » sur toutes les boîtes Exchange 2007 server

Premièrement vous devez déclarer un utilisateur avec une boîte Exchange dédiée.

Ensuite utiliser le Management Shell pour donner les droits en lecture sur l'ensemble des boîtes pour cet utilisateur spécifique:

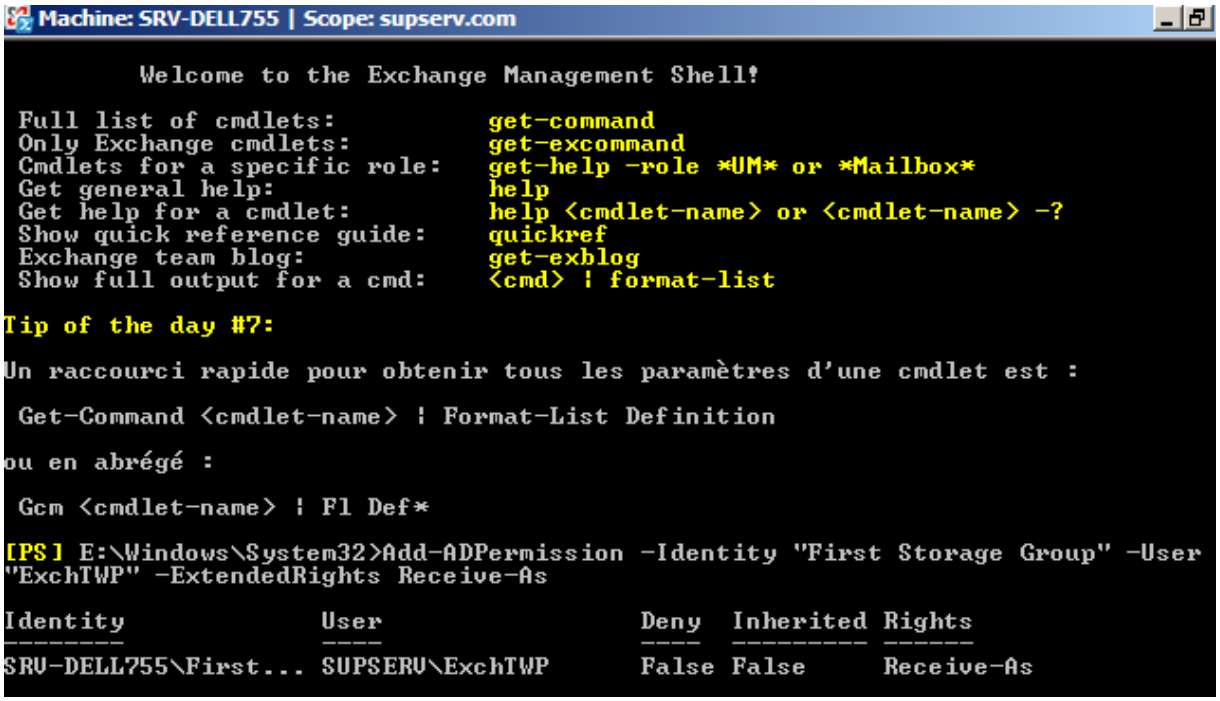
Cliquer sur "Start" → "All programs" → "Microsoft Exchange Server 2007" → "Exchange Management Shell".



Pour donner les droits "Receive-As" sur l'ensemble des boîtes :

```
Add-ADPermission -Identity "Mailbox Store" -User "Trusted User" -ExtendedRights
Receive-As
```

Remplacer "Mailbox Store" par le nom de la database exchange ("First Storage Group" dans l'exemple ci-dessous) and "Trusted User" par le nom de l'utilisateur dédié ("ExchTWP" dans notre exemple).



Afin de vérifier les droits accordés passer la commande suivante:

```
Get-ADPermission -Identity "Mailbox Store" -User "Trusted User"
```

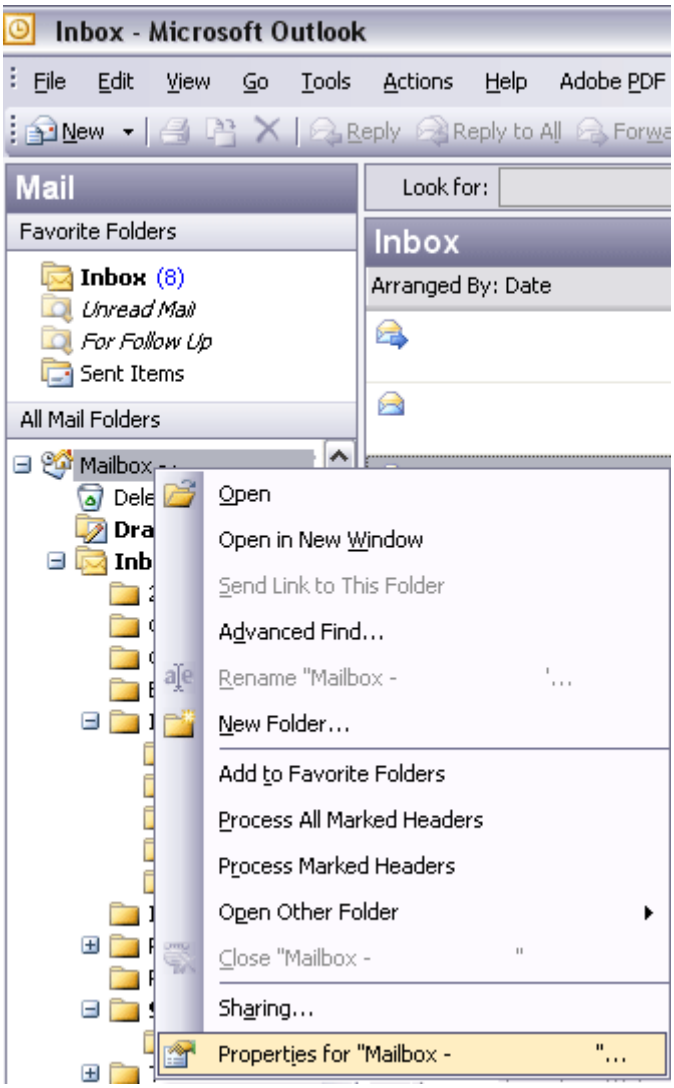
Pour supprimer les droits "Receive-As" passer la commande suivantes:

```
Remove-ADPermission -Identity "Mailbox Store" -User "Trusted User" -ExtendedRights
Receive-As
```

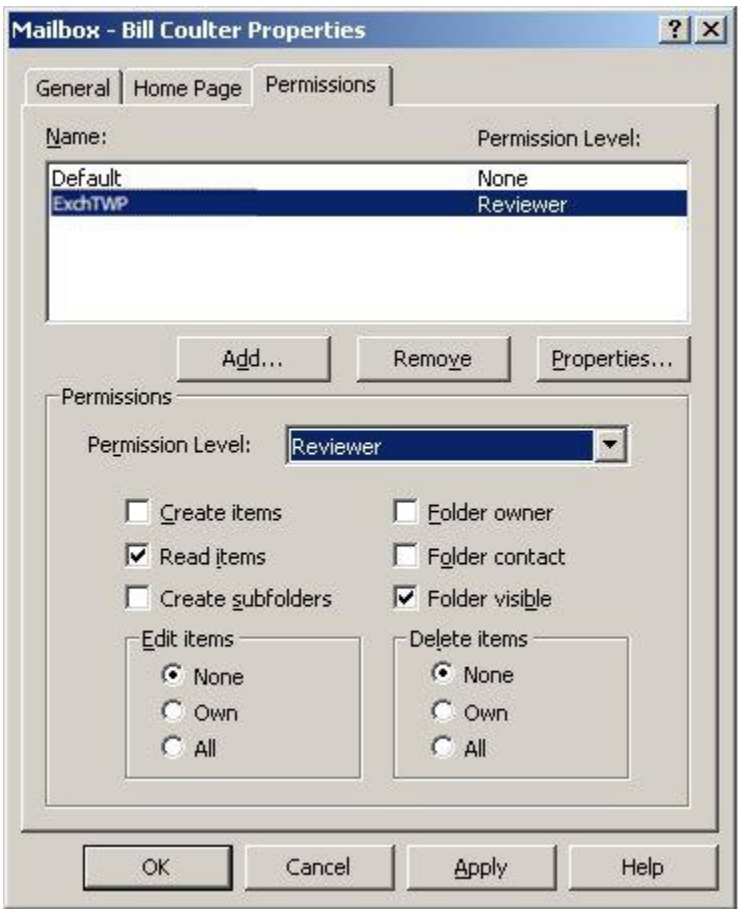
Note: il faut quelques minutes pour que les droits soient pris en compte, ou bien il faut relancer le service "Microsoft Exchange Information Store").

Solution 2: donner les droits depuis MS Outlook

Depuis Outlook, sélectionner "Boite de réception", faire un clic droit puis *propriétés*.



Donner les droits de relecteur à l'utilisateur dédié ("ExchTWP" dans notre exemple).



Pour partager également son Calendrier, faire la même configuration sur le dossier calendrier.

8.8. Add-In Client Outlook

L'add-in client Outlook permet aux utilisateurs directement via leur Caller de récupérer les contacts privés de leur Outlook connecté à Exchange ou non.

8.8.1. Prérequis

Systèmes compatibles

- Windows Server 2012 / Windows Server 2012 R2
- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003
- Windows 8
- Windows 7
- Windows Vista
- Windows XP

Applications nécessaires

- Microsoft .Net Framework 4.0 Full package
- Avoir lancé une fois l'application Caller
- Versions Microsoft Outlook compatible :
    - Microsoft Outlook 2013
    - Microsoft Outlook 2010
    - Microsoft Outlook 2007 (Partiellement)

      Attention : Avec Microsoft Outlook 2007 aucun affichage du bouton de synchronisation n'est présent dans Microsoft Outlook. Seule la synchronisation automatique des contacts au démarrage de Microsoft Outlook est disponible.
- Les versions TWP Server compatibles sont les versions *supérieures ou égales à la 4.1.1341*.

Protocoles et Ports

L'AddInOutlook a besoin de pouvoir accéder au serveur TWP via la liste des ports suivants :

- Lien avec les web services : port HTTP *8000*.

8.8.2. Installation

Installer l'application

Dans le DVD, chercher AddInOutlook. Exécuter le fichier *setup.exe*. Suivez les fenêtres d'installations, et cliquez sur le bouton « next » pour passer d'une étape à l'autre. L'installation dure environ 1 à 2 minutes.

Ce qui est installé avec ce package :

- TWS_AddInOutlook

8.8.3. Configuration

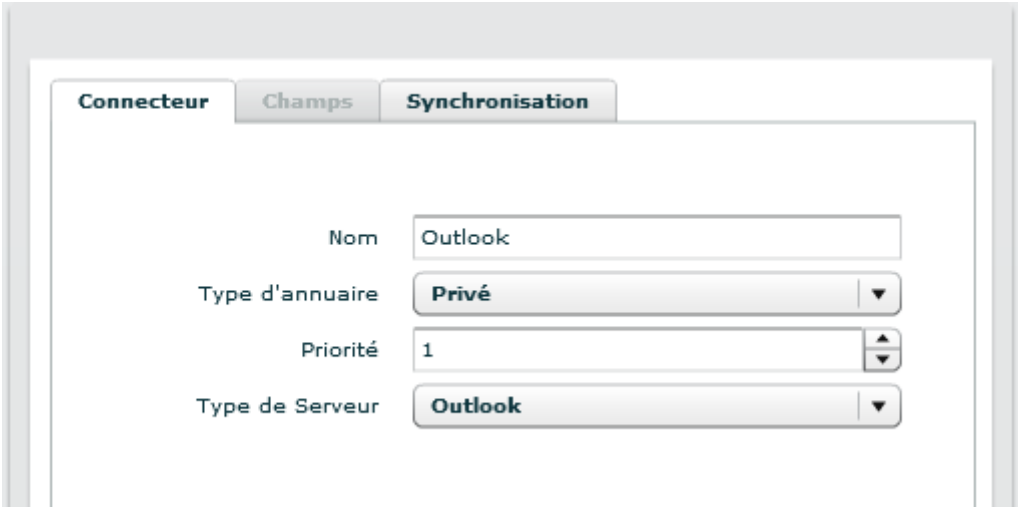
Serveur TWP

1. *Création de l'annuaire Outlook*

Le serveur TWP doit être dans une version supérieure à la version 4.1.1341.

Vous devez créer un annuaire Outlook dans l'administration du serveur en cliquant sur le bouton « + », dans le menu *Informatique* / *Annuaires* :

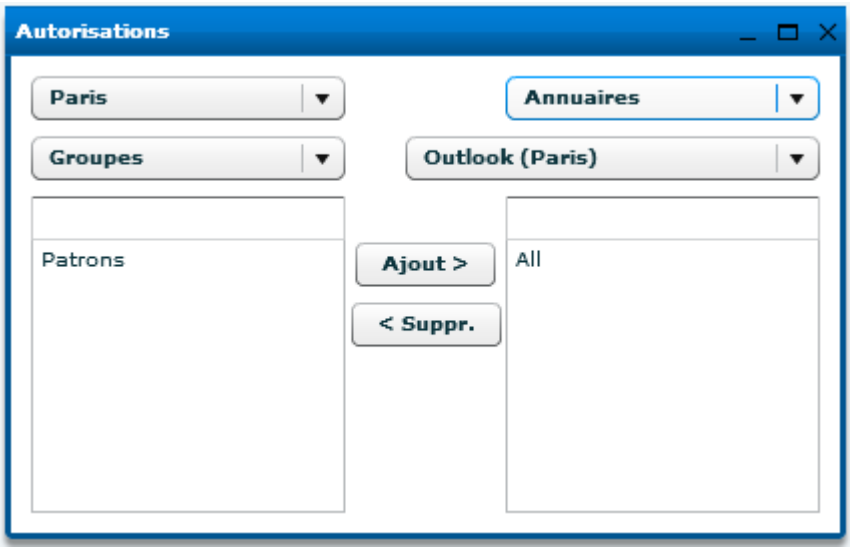
- Mettez le nom que vous désirez.
- Choisissez la valeur « *Privé* » en tant que type d'annuaire.
- Choisissez la priorité que vous souhaitez (plus la priorité est faible plus l'annuaire sera prioritaire pour la résolution de nom…).
- Et sélectionnez le type de serveur « *Outlook* », puis sauvegarder votre annuaire.



2. *Autoriser l'accès à l'annuaire Outlook*

Afin que l'AddInOutlook puisse copier les contacts privés Outlook dans la base de données du serveur,

vous devez autoriser les utilisateurs ayant installé l'AddInOutlook à utiliser l'annuaire Outlook (voir ci-dessous).



Ici l'ensemble des utilisateurs présents dans le groupe utilisateur « All », ont le droit d'utiliser l'annuaire Outlook du domaine Paris.

Attention : Vous devez autoriser les utilisateurs et les groupes utilisateurs à l'annuaire Outlook de leurs domaines. Dans l'exemple ci-dessus le groupe « All » fait partie du domaine « Paris ».

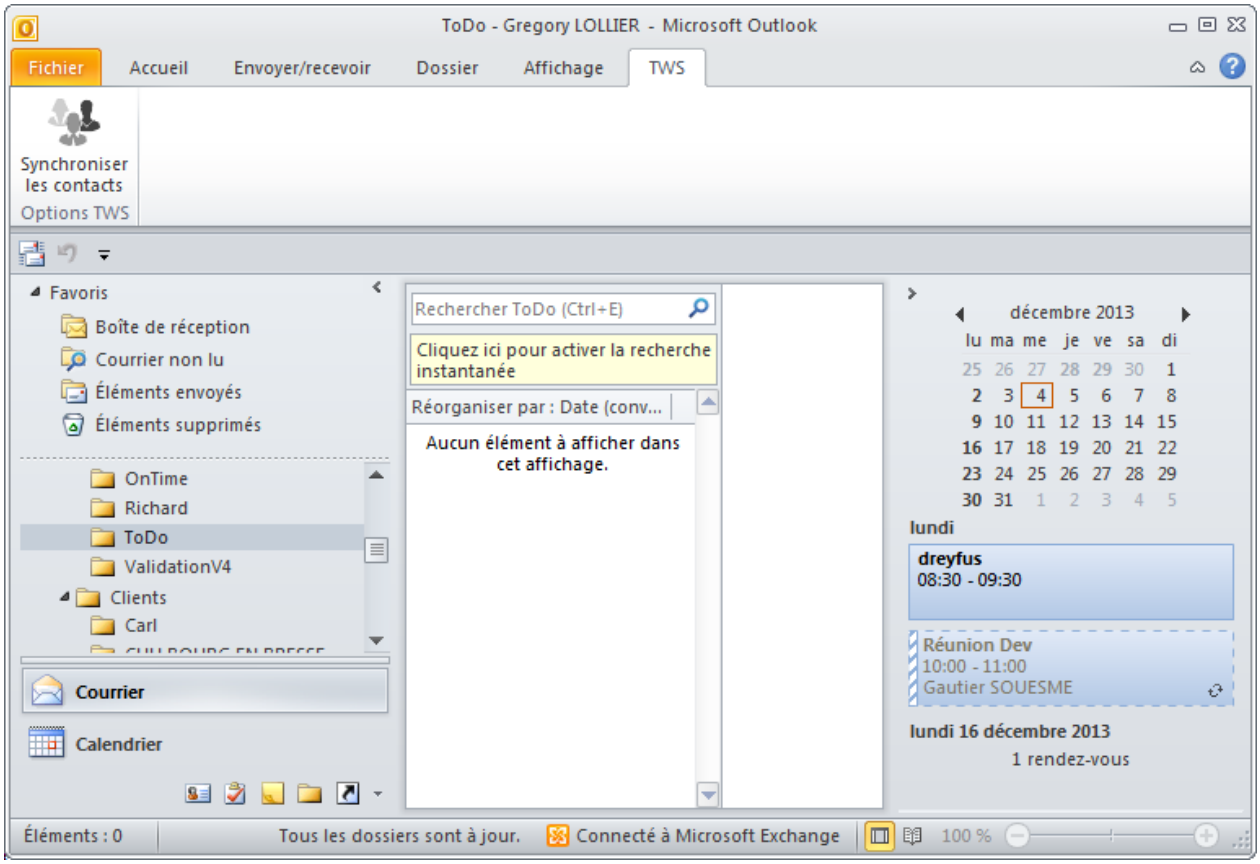
3. *Identification*

L'identification de l'utilisateur, vers lequel seront synchronisés les contacts Microsoft Outlook, se fait grâce à l'application Caller. Vous devez au moins avoir démarré une fois votre application Caller après l'installation de l'AddInOutlook.

8.8.4. Utilisation

Les utilisateurs ayant installé L'AddInOutlook, verront apparaitre (après un redémarrage de Microsoft Outlook) un nouvel onglet se nommant « TWS ». Dans cet onglet les utilisateurs trouveront un bouton de synchronisation de leurs contacts privés Microsoft Outlook. A chaque clique sur ce bouton une synchronisation de vos contacts s'exécute vers le serveur TWS.

De plus la synchronisation des contacts se fait de manière automatique à chaque redémarrage de Microsoft Outlook.



8.8.5. Maintenance

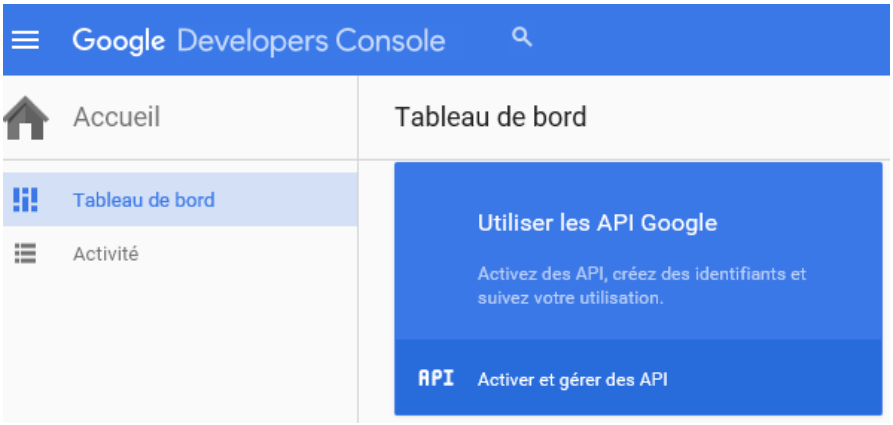
L'application AddInOutlook, logue dans le fichier Log_AddInOutlook.txt dans les fichiers temporaires de l'ordinateur sur lequel s'exécute Microsoft Outlook.

8.9. Intégration Google Apps

8.9.1. Configuration du compte Google Apps

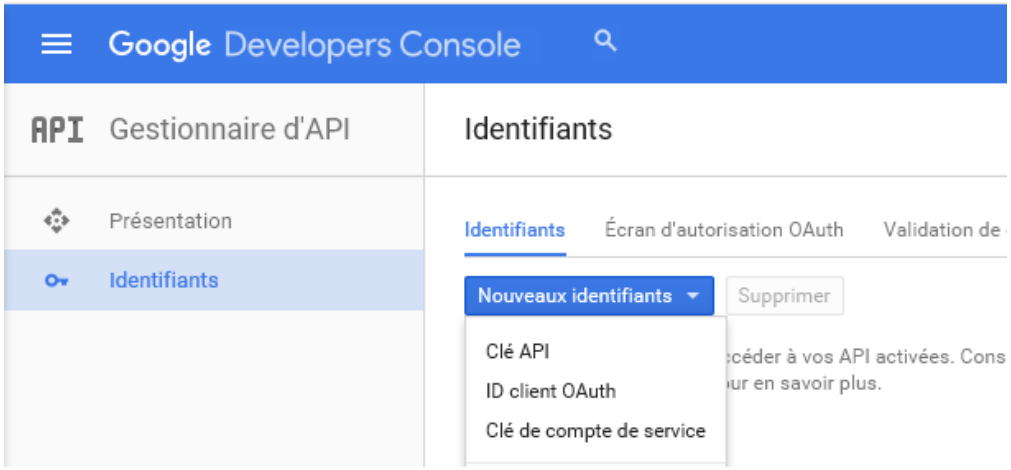
Création d'un nouveau projet Google Apps

Aller à la page web : https://console.developers.google.com/project et créer un nouveau projet. Ouvrir ce projet puis aller dans « *Utiliser les API Google* » puis « *Identifiants* ».

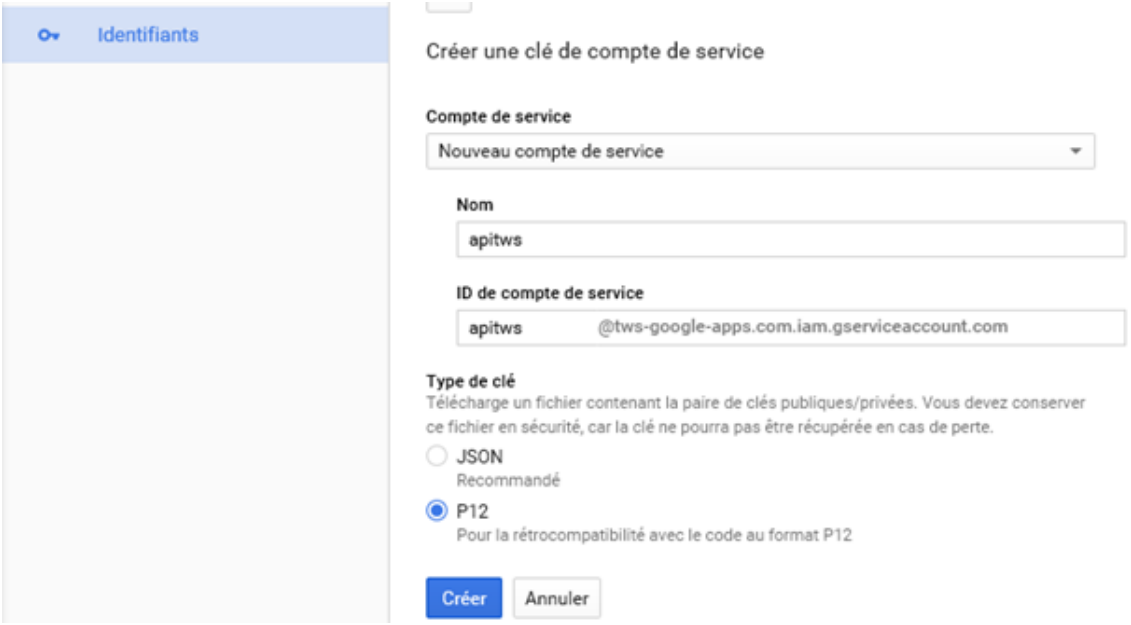


Création d'une clé de compte de service

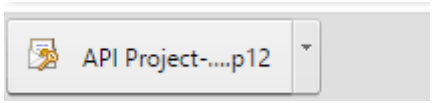
Dans « *Identifiants* » *et onglet* « *Identifiants* », créez un nouvel identifiant. Choisissez « *Clé de compte de service* ».



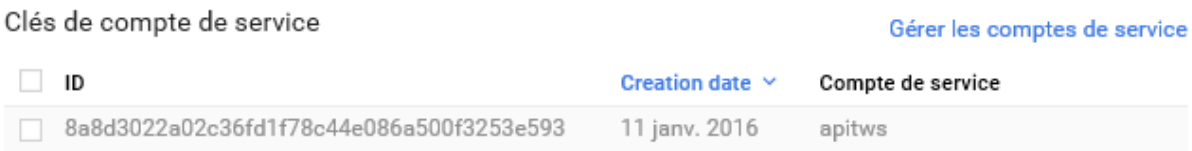
Choisissez ensuite « *Nouveau compte de service* » puis donnez un nom à ce compte. Ici c'est « *apitws* ». Sélectionner ensuite « *P12* » et faîtes « *Créer* ».



Le navigateur vous proposera de télécharger un fichier de *type P12*. Sauvegardez ce fichier dans votre ordinateur.

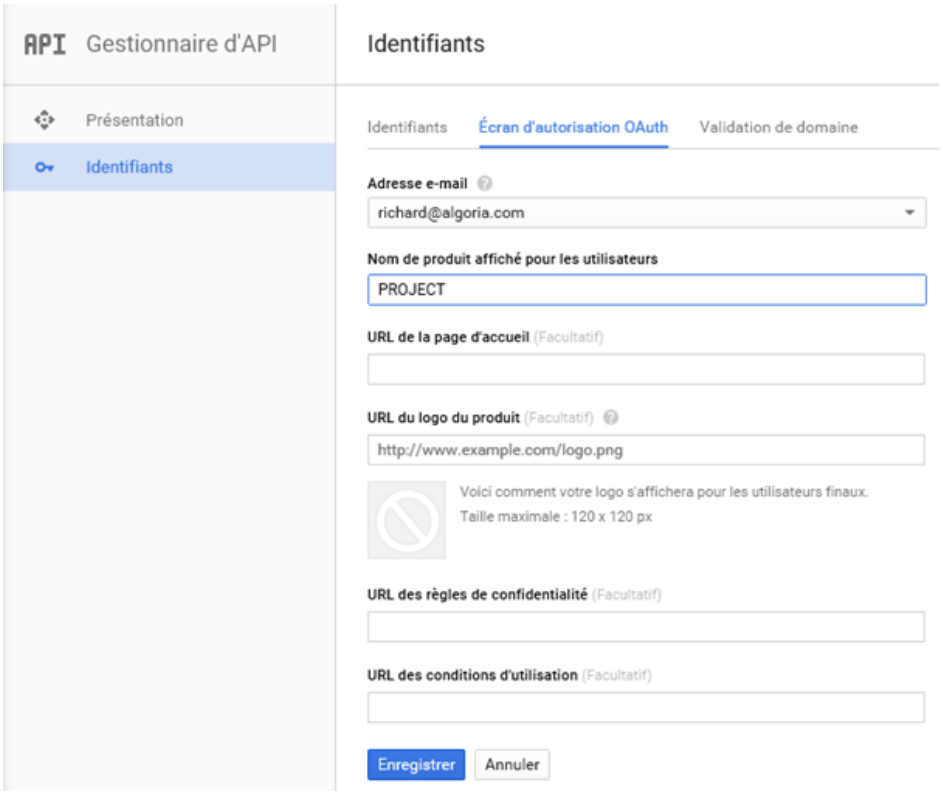


La clé de compte de service est créée.

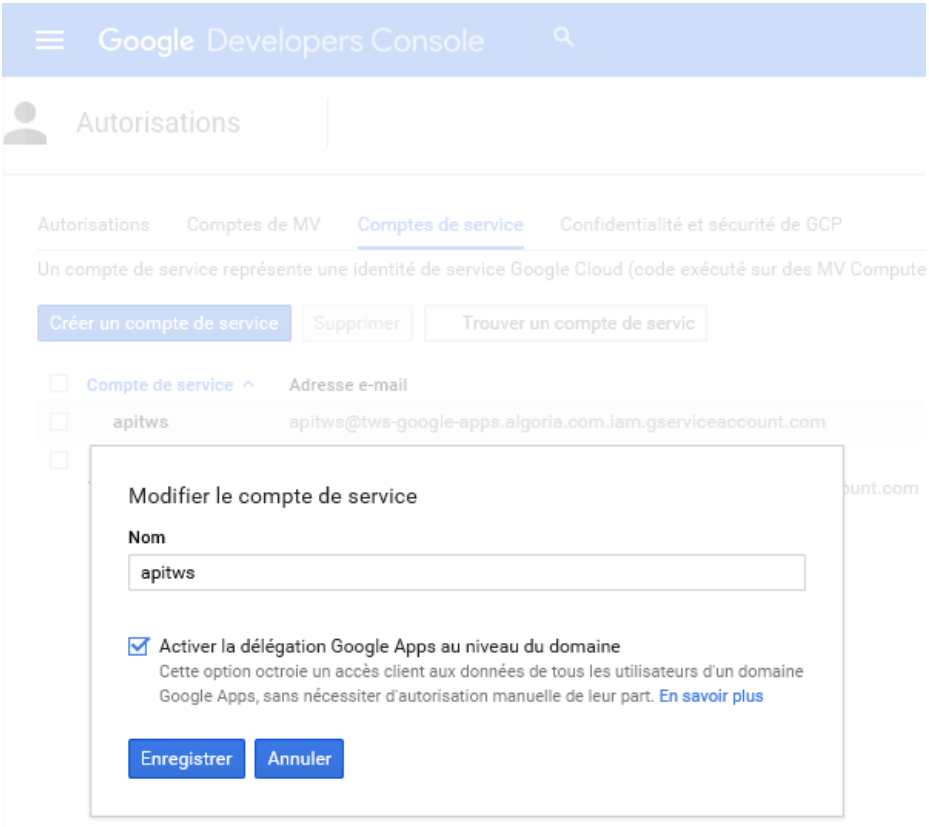


Création d'un ID client lié à la clé de compte de service

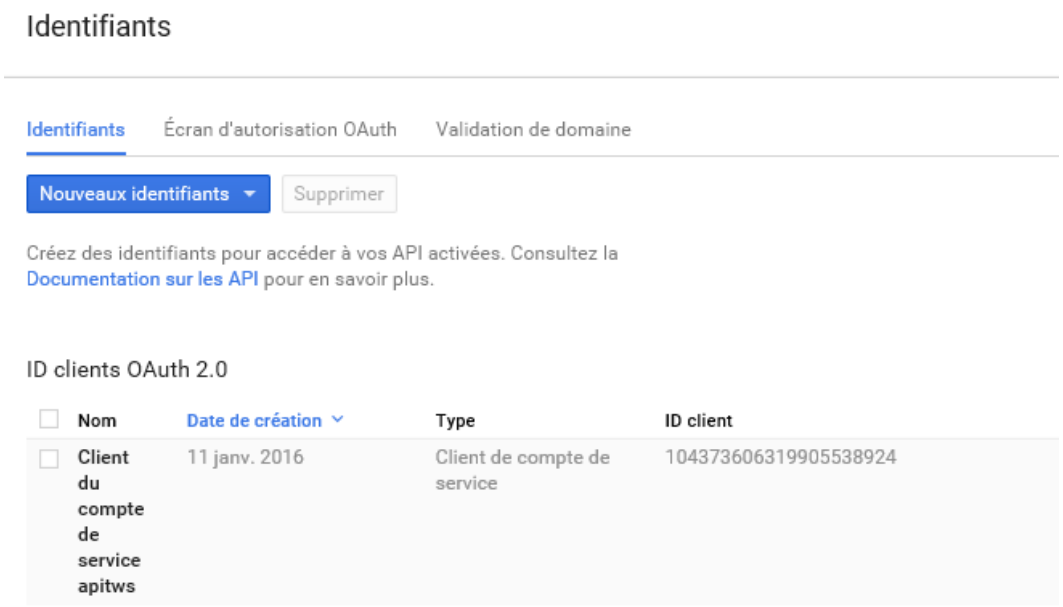
Avant de créer l'ID client, il est nécessaire de renseigner un nom de produit. Dans le menu « *Identifiants* » et l'onglet « *Ecran d'autorisation Oauth* », donnez un nom de produit comme ci-dessous :



Ensuite dans le menu « Identifiants » et l'onglet « Identifiants », cliquer sur « *Gérer les comptes de service* » dans le paragraphe « *Clés de compte de service* ». Sélectionner le compte créé et à droite un bouton vous permettra d'éditer le compte.
Cochez la case « *Activer la délégation Google Apps au niveau du domaine* » et enregistrez.

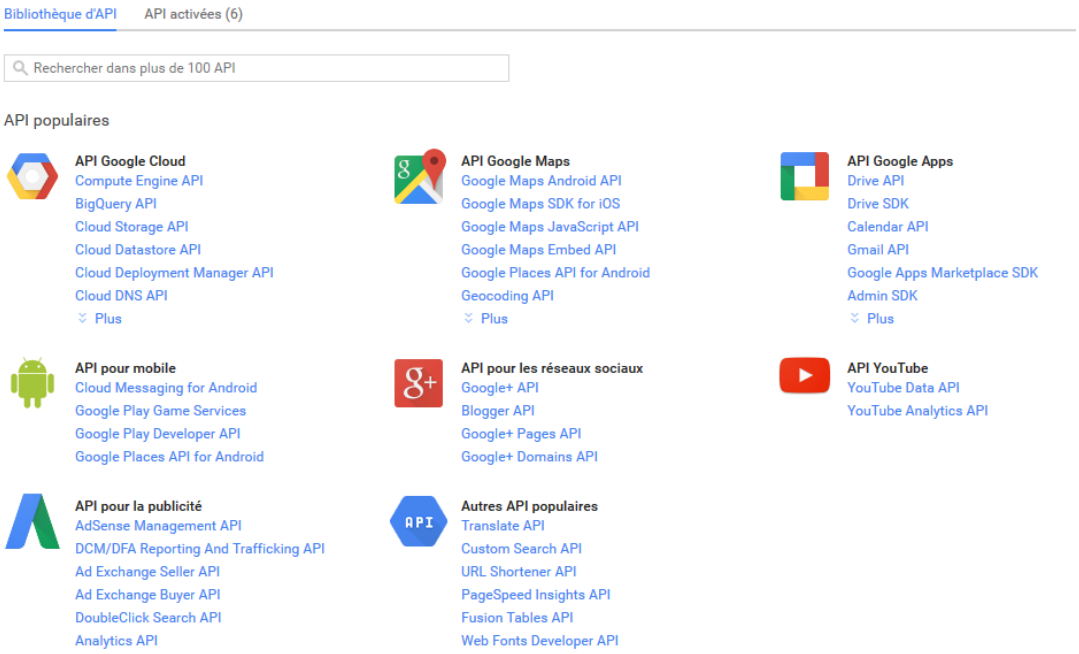


Ainsi, un nouvel identifiant client a été créé. Celui-ci sera utilisé pour accéder aux différentes données et API. Retenez cet « *ID Client* ».

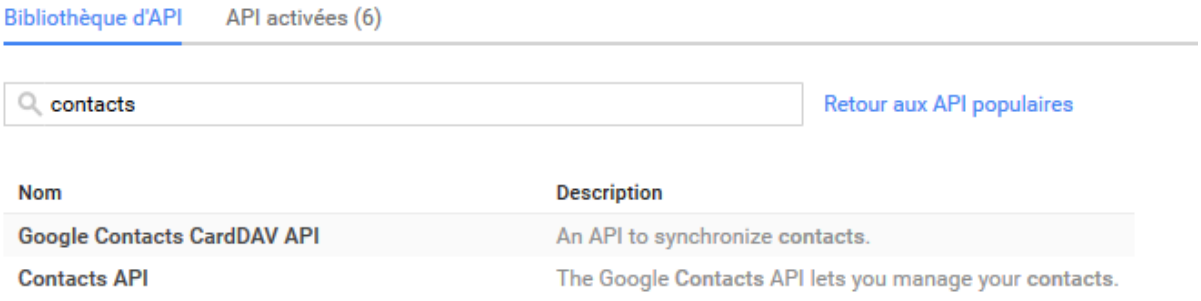


8.9.2. Activer les APIs

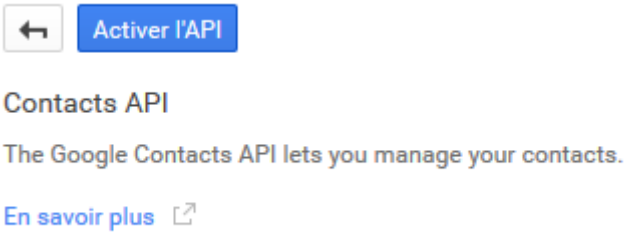
Ouvrez le menu « *Présentation* », onglet « *Bibliothèque d'API* » puis dans la section « *API Google Apps* » vous trouverez les 2 APIs à activer.



Dans la zone de recherche, vous pouvez taper « *Contacts* ».



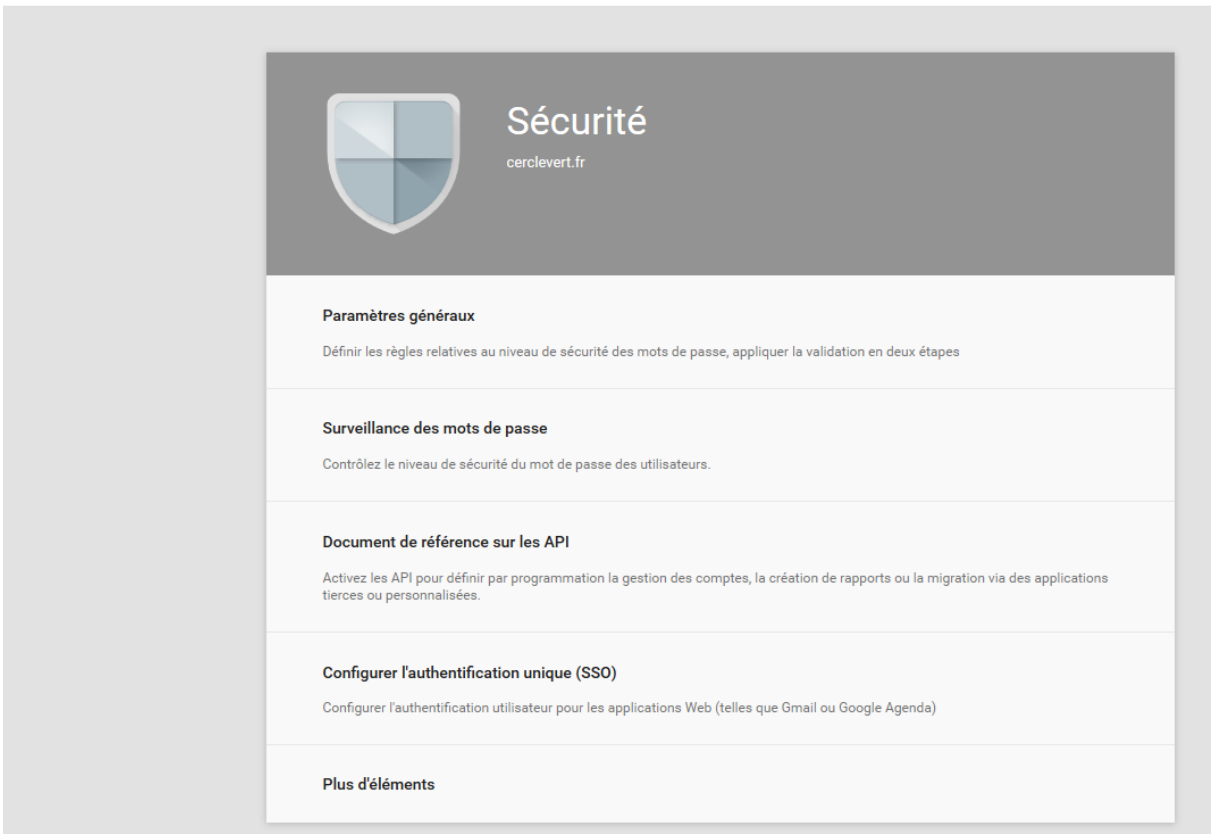
Sélectionnez « Contacts API » et Activez l'API



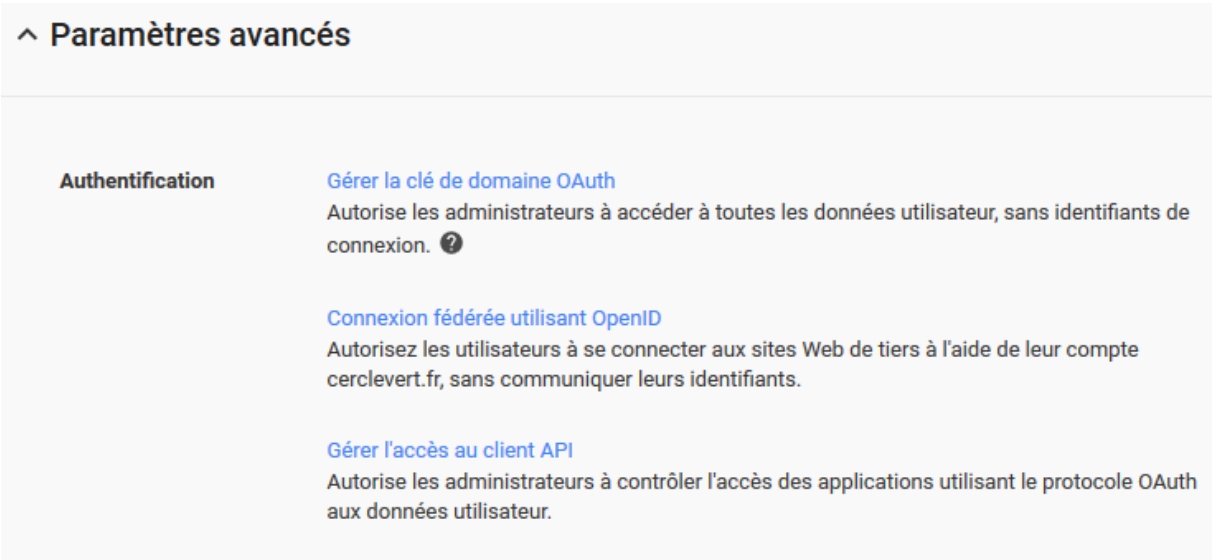
Faites de même en recherchant l'API pour les Calendriers (« *Calendar* »).
Une fois terminé, sélectionnez le menu « API activées » pour vérifier que vos APIs sont bien actives.

8.9.3. Autoriser les APIs

Allez à la page web : https://www.google.fr/intx/fr/work/apps/business/. Connectez-vous à votre domaine Google Apps et sélectionnez la console d'administration.
Ouvrez le menu « Sécurité » et cliquez sur « Plus d'éléments ».



Ouvrez les « Paramètres avancés » et cliquez sur « Gérer l'accès au client API ».

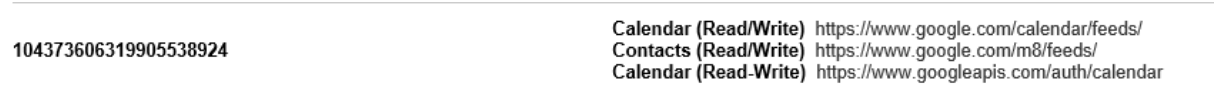


Maintenant, vous devez enregistrer les applications Web afin d'accéder aux données des services.

Renseignez votre « *ID CLIENT* » précédemment créé dans « *Nom du client* » (voir chap. *Création d'un ID client lié à la clé de compte de service*). Puis dans le champ « *Un ou plusieurs champs d'application d'API* » renseignez les URL suivantes séparées par des virgules, comme ci-dessous :

https://www.google.com/calendar/feeds/,https://www.google.com/m8/feeds/,https://www.googleapis.com/auth/calendar

Puis appuyez sur « *Autoriser* ».



Votre compte Google Apps est correctement configuré.

8.9.4. Configuration des connecteurs dans TWP

Prérequis

Pour que TWP puisse communiquer avec Google Apps, nous avons besoin de :
- l'adresse email configurée précédemment dans le compte de service de Google
- le fichier *P12*
- Nom de domaine que vous utilisez dans Google Apps

Configuration

Renommer le fichier *P12* de cette façon : « *api-google-[NomUtilisateur].p12* »
Le [NomUtilisateur] correspond au nom de l'utilisateur présent dans l'adresse email du compte Google Apps développeur.

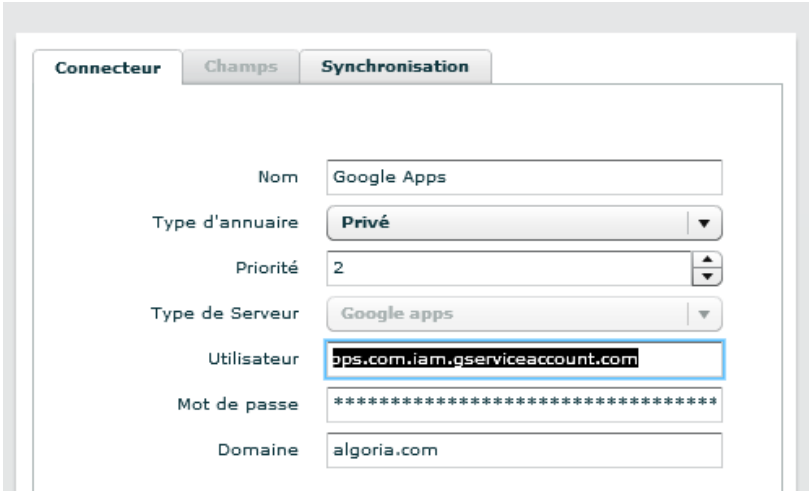
Ex :
Email : apitws@tws-google-apps.com.iam.gserviceaccount.com
Nom de l'utilisateur : apitws
*Fichier : **api-google-apitws.p12***

Copier ensuite ce fichier dans le répertoire [InstallTWP]\TWS4\TWS_Web\TWS_Config.

Pour que TWP puisse synchroniser l'annuaire et les calendriers Google Apps, l'adresse mail de l'utilisateur TWP soit correspondre à l'adresse mail de l'utilisateur Google Apps.

8.9.5. Création d'un connecteur annuaire privé.

Dans l'administration de TWP, créer un nouvel annuaire Google Apps de type privé et nommer le comme vous le désiré.

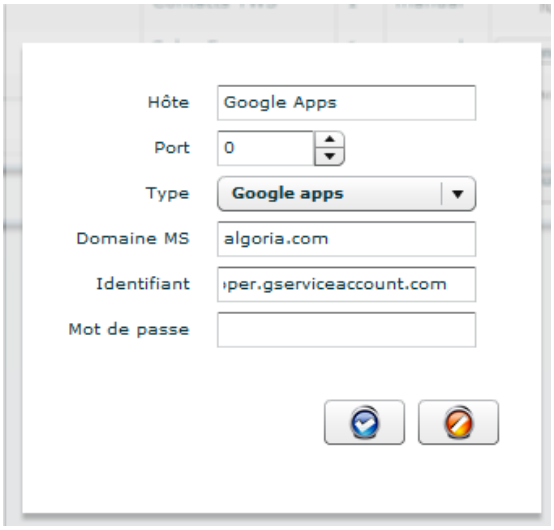


Dans le champ *Utilisateur*, inscrire l'adresse email complète.
Dans le champ *Domaine*, inscrire le nom de votre domaine.

Le champ Mot de passe n'est pas utilisé.
Sauvegardez et vous pouvez lancer une synchronisation.

8.9.6. Création d'un connecteur Calendrier

Dans l'administration de TWP, créer un nouveau connecteur de collaboration Google Apps.



Choisissez le type Google Apps.
Dans le champ *Identifiant*, inscrire l'adresse email complète.
Dans le champ *Domaine*, inscrire le nom de votre domaine.

Le champ Mot de passe n'est pas utilisé.
Le champ Hôte n'est pas utilisé. Vous pouvez utiliser ce champ pour nommer le connecteur.

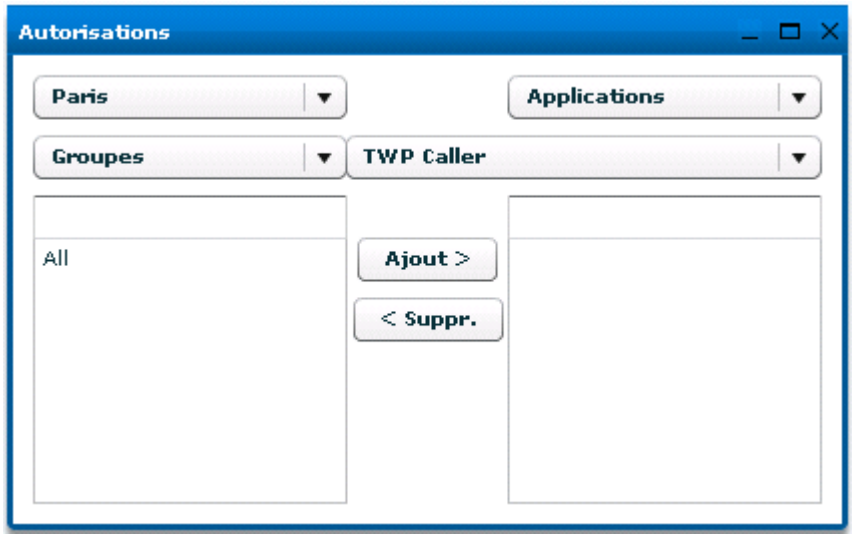
9. Configuration des applications

9.1. Configuration du Caller

L'application Caller est la brique de base des applications TWP. Elle contient de nombreuses fonctionnalités apportant une valeur ajoutée à l'utilisation habituelle de la téléphonie en entreprise. Parmi les fonctionnalités suivantes un certain nombre nécessite un minimum de configuration :

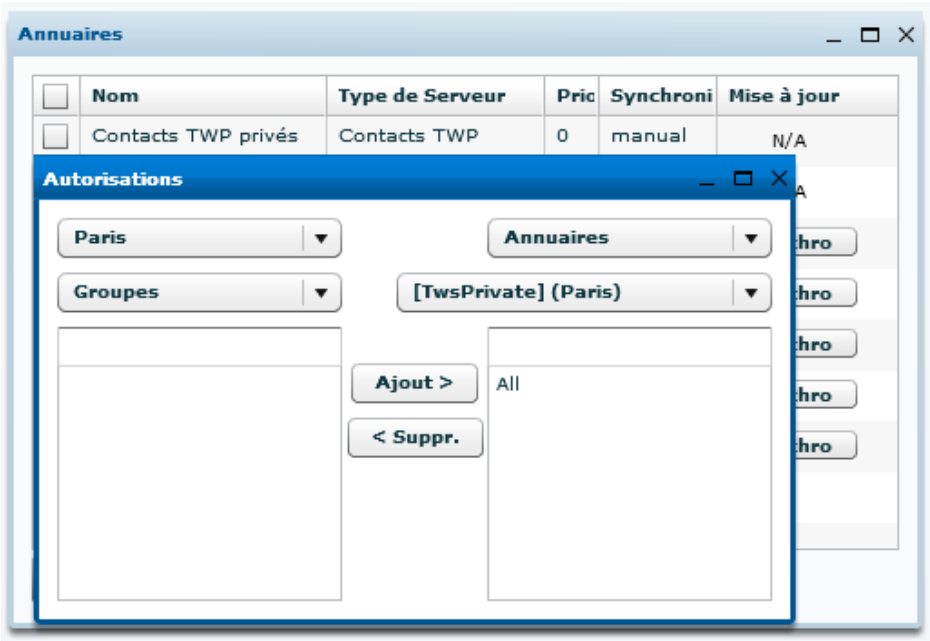
- recherche multi-annuaires,
- liste de contacts,
- présence téléphonique des contacts,
- présence calendrier des contacts,
- présence TWP des contacts,
- chat texte, vidéo et partage d'applications point à point (avec un seul contact)
- partage d'informations : notes, notifications, journaux d'appel
- les règles de renvoi d'appel
- nouveaux messages vocaux (PBX A5000)
- alerte e-mail lors d'un appel en absence

Tout utilisateur dispose de ces fonctionnalités en ayant droit à l'application Caller qui consomme une licence Caller.
Pour donner les droits à l'application Caller, dans l'administration menu *Utilisateurs* / *Autorisations* choisir en haut à droite Applications puis TWP Caller en dessous. Sélectionner donc le groupe d'utilisateurs ou l'utilisateur à gauche et cliquer sur le bouton *Ajouter*.



9.1.1. Contacts privés

Avec l'application Caller, les utilisateurs ont la possibilité de créer leurs propres contacts privés et uniquement visible dans leur Caller.
Pour cela, il suffit de vérifier que l'utilisateur en question possède bien les droits sur l'Annuaire *[TwsPrivate]*.



9.1.2. Présence téléphonique - Intercom

Pour disposer de la présence téléphonique de ses contacts (numéros de téléphone internes) – équivalent des touches de supervision sur un téléphone physique – il faut absolument configurer les groupes Intercom propres à TWP.

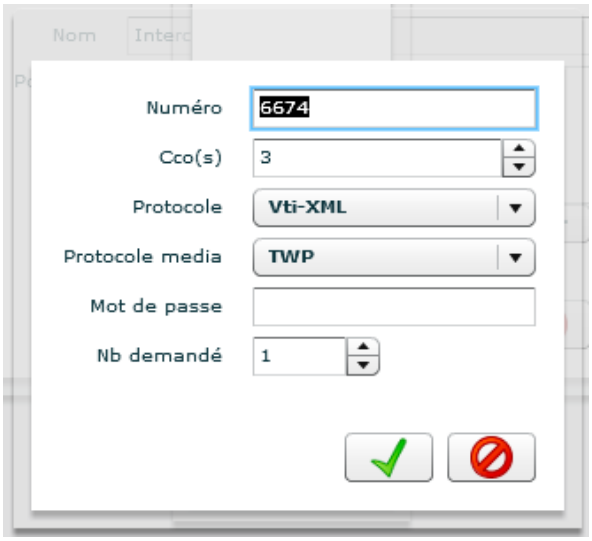
1. **Créer un groupe Intercom TWP :**

   Il y a plusieurs manières de créer un groupe Intercom :

- *A partir d'un numéro de poste physique existant* : vous possédez déjà un ou plusieurs postes qui contiennent les touches de supervision de postes dont l'état devra être visible, alors ces numéros peuvent être renseignés pour créer un groupe intercom.

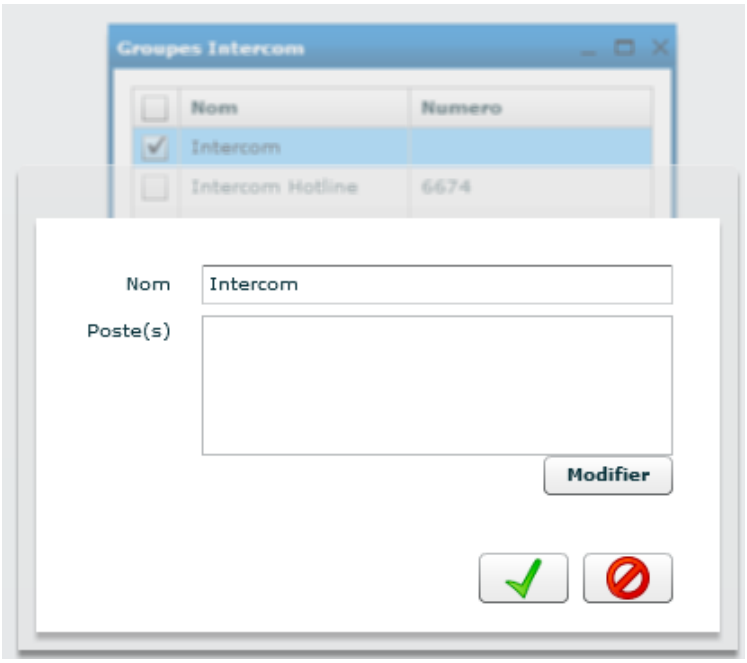
Numéro : Premier numéro de(s) poste(s) à renseigner.
Protocole : choisir le protocole de supervision du poste.
Protocole media : Dans le cas d'un poste physique existant, sélectionner *None*.
Mot de passe : Mot de passe de poste si existant, utile pour la demande de supervision.
Nb demandé : Nombre de poste à renseigner. Si le numéro est 6674 et que vous renseigné 2 alors seront créés les 6674 et 6675.

- *A partir d'un numéro de poste virtuel* : créer dans votre PBX un poste virtuel lié à aucun poste physique (par exemple poste VTIXML/IP sur A5000). Sur ce poste, créer des touches de supervision des postes dont l'état devra être visible. Renseigner ce numéro dans la configuration d'un groupe intercom.



Numéro : Premier numéro de(s) poste(s) à renseigner.
Protocole : choisir le protocole de supervision du poste.
Protocole media : Dans le cas d'un poste virtuel, sélectionner *TWP*.
Mot de passe : Mot de passe de poste si existant, utile pour la demande de supervision.
Nb demandé : Nombre de poste à renseigner. Si le numéro est 6674 et que vous renseigné 2 alors seront créés les 6674 et 6675.

- *A partir d'aucun numéro* : vous pouvez créer un groupe Intercom sans numéro. Dans ce cas, il faut absolument que les postes des utilisateurs possèdent eux-mêmes des touches de supervision des autres postes dont l'état devra être visible.



2. **Donner les autorisations pour les utilisateurs au groupe Intercom créé :** Seuls les utilisateurs qui auront droit au même groupe Intercom pourront se voir entre eux ou voir l'état des postes supervisés par les postes du groupe Intercom. (voir chapitre 7.4.4)

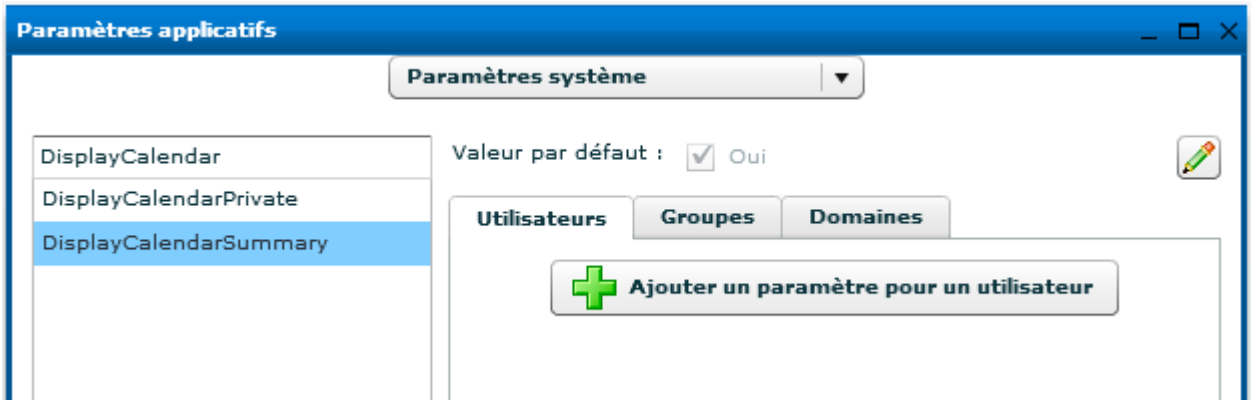
Attention : Sur PBX AASTRA, bien vérifier que les postes qui sont censés se superviser sont bien dans le *même groupe intercom PBX cette fois-ci*.

9.1.3. Présence Calendrier - collaboration

Voir chapitres 8.5.3, 8.6.2, 8.7.4 selon le type de serveur de messagerie dont vous disposez.

Après avoir configuré les connecteurs vers les serveurs de messagerie ainsi que les autorisations nécessaires, tous les utilisateurs autorisés ont la possibilité de voir des évènements calendrier : le statut ainsi que le détail en survolant l'image du contact.

Il est possible cependant de brider la fonctionnalité pour un utilisateur, un groupe ou un domaine. Aller dans le menu *Applications / Paramètres applicatifs* puis *Paramètres système* et rechercher « *DisplayCalendar* » et là il y aura 2 paramètres :



- *DisplayCalendarSummary* : Oui ou Non le détail de l'évènement Calendrier d'un contact est visible par des utilisateurs (état occupé, sur la fiche contact - autre état, en passant la souris sur la photo du contact)
- *DisplayCalendarPrivate* : Oui ou Non l'information (état et détail) d'un évènement Calendrier PRIVE est visible par d'autres utilisateurs. Un évènement Calendrier normal sera visible par les mêmes utilisateurs.

9.1.4. Numéro de Messagerie vocale

Avec l'application Caller, un utilisateur peut directement faire appel à sa messagerie vocale en cliquant sur le bouton prévu à cet effet dans la barre verticale.

Pour modifier cette valeur, aller dans le menu *Applications / Paramètres applicatifs*, choisir TWP *Caller* puis chercher « *vmNumber* ». Renseigner ensuite le numéro de messagerie vocale dans la valeur par défaut. Il est possible aussi de donner un numéro différent par utilisateur ou groupe ou domaine.

9.1.5. Alerte emails – Configuration SMTP

Avec l'application Caller, un utilisateur peut recevoir par email une alerte lui informant d'un appel en absence. Pour avoir cette fonctionnalité, il faut configurer les paramètres SMTP.

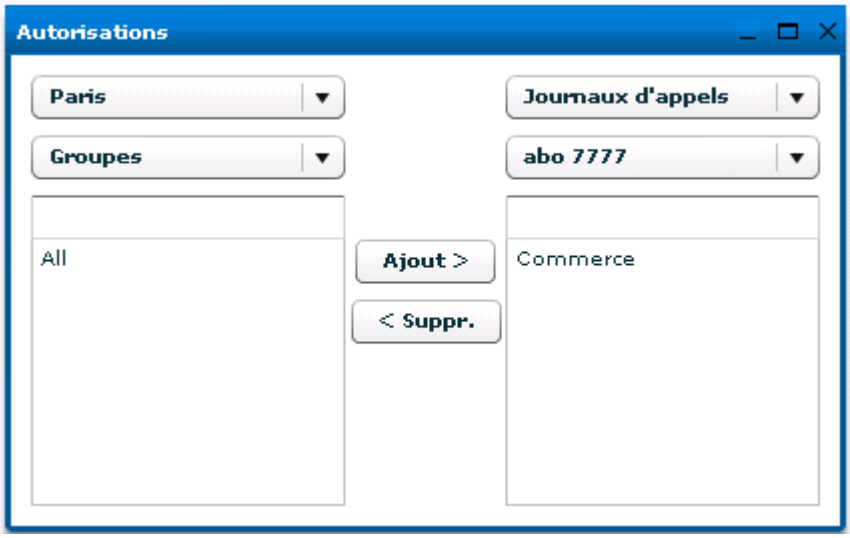
Dans le menu *Applications / Paramètres applicatifs*, choisir TWP *Server* puis chercher « smtp ». Renseigner ensuite l'adresse du serveur SMTP dans la valeur par défaut. Il est possible aussi de donner une adresse différente par utilisateur ou groupe ou domaine.

Avancé
Si vous devez renseigner le port ainsi qu'un compte pour la connexion SMTP alors cochez la case *(Mode Expert)* et vous pourrez modifier les paramètres « *SmtpAuthUserName* » pour le nom d'utilisateur, « *SmtpAuthPassword* » pour le mot de passe de ce compte et « *SmtpServerPort* » pour le port de connexion.

9.1.6. Journaux d'appels d'autres utilisateurs

Avec l'application Caller, un utilisateur peut avoir accès aux journaux d'appel d'un contact via son journal d'évènements. Pour qu'il puisse visualiser ces journaux d'appel il faut au préalable donner des autorisations. (Voir le chapitre 7.4.6)

Tous les utilisateurs du groupe Commerce du domaine Paris ont le droit de voir les journaux d'appels de l'utilisateur « abo 7777 ».



Les données des journaux d'appels des utilisateurs sont conservées uniquement pendant un certain nombre de jours (voir chapitre 10.2.1.).

9.1.7. Fonctionnalités Patron-Secrétaire

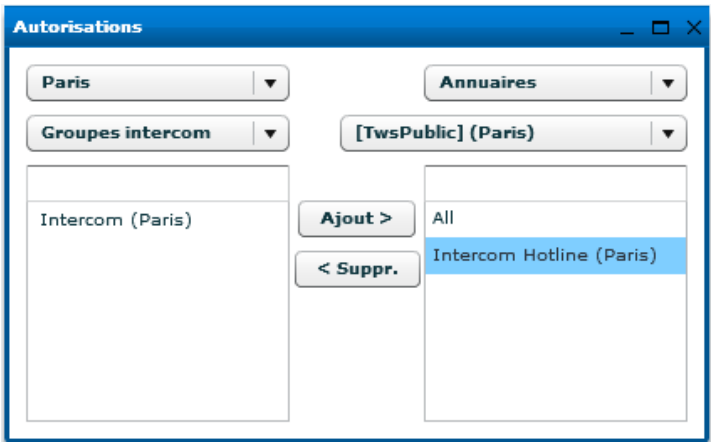
Avec l'application Caller, des informations particulières d'un ou plusieurs utilisateurs (les patrons) peuvent être vu par d'autres utilisateurs (les secrétaires) :

- Le détail (prénom et nom du correspondant si présent dans les annuaires ou numéro) de l'appel qui arrive sur l'un des postes des patrons pour pouvoir entre autre intercepter l'appel si besoin.
- La règle de renvoi active qu'un des patrons a mis en place

Autoriser un utilisateur à voir le détail d'un appel d'un autre utilisateur (dans sa fiche contact) :

N.B. : Pour les PBX A5000 dont les postes sont supervisés en VTIXML, les informations d'appels sont affichées uniquement lors de la sonnerie. Pour les autres PBX supervisés en CSTA, les informations sont affichées dès que l'appel a été décroché.

1. Configurer un groupe intercom (voir chapitre 9.1.2.) et autoriser les utilisateurs (patrons et secrétaires) à ce même groupe.
2. Donner les autorisations annuaires à ce groupe intercom. C'est grâce à ces autorisations que le nom du contact apparaîtra si le numéro est trouvé des annuaires en question.



3. Créer un nouveau groupe dans le menu *Utilisateurs* / *Groupes*.
4. Depuis le menu *Utilisateurs* / *Groupes-Utilisateurs*, Y ajouter les utilisateurs (les patrons) dont les informations d'appels seront visibles.
5. Dans le menu *Applications* / *Paramètres applicatifs*, sélectionner TWP *Caller* et configurer le paramètre « *AuthorizeSupervisionInformation* » comme ci-dessous :

Dans l'onglet *Utilisateurs* ou *Groupes*, choisir l'utilisateur ou le groupe d'utilisateurs qui devra voir l'information après avoir cliqué sur le bouton *Ajouter…* Puis renseigner comme valeur le nom du groupe d'utilisateurs créé précédemment et enfin valider.

Ici, par exemple l'utilisateur « ban » verra les informations d'appel entrant du groupe d'utilisateurs « Patrons ».

6. Dans le cas où un ou plusieurs utilisateurs du groupe « Patrons » appartiennent à plusieurs groupe Intercom, il est préférable de fixer le groupe Intercom qui sera choisi pour la résolution du numéro en nom.

   Pour cela, dans le menu *Applications* / *Paramètres applicatifs*, sélectionner TWP *Caller*, ne pas oublier d'activer le « mode Expert » (chap. 10.2) et configurer le paramètre « *SupervisionInformationIGroup* » comme ci-dessous, sur le domaine ou en valeur par défaut uniquement :

Ici, seul les autorisations annuaires du groupe Intercom de nom « Intercom Hotline » seront pris en compte pour la résolution du numéro en nom dans l'affichage des informations d'appels pour les utilisateurs du domaine « Paris ».

Attention : Redémarrer le service TWS4$TWS_EventServices après toutes modifications de ces paramètres.

Autoriser un utilisateur à voir la première règle de renvoi active d'un autre utilisateur (en passant la souris sur sa photo) :

1. Créer un nouveau groupe dans le menu *Utilisateurs* / *Groupes*
2. Y ajouter les utilisateurs (les patrons) dont la première règle de renvoi active sera visible depuis le menu Utilisateurs / *Groupes-Utilisateurs*
3. Dans le menu *Applications* / *Paramètres applicatifs*, sélectionner TWP *Caller* et configurer le paramètre « *AuthorizeShareRulesGroup* » comme ci-dessous :

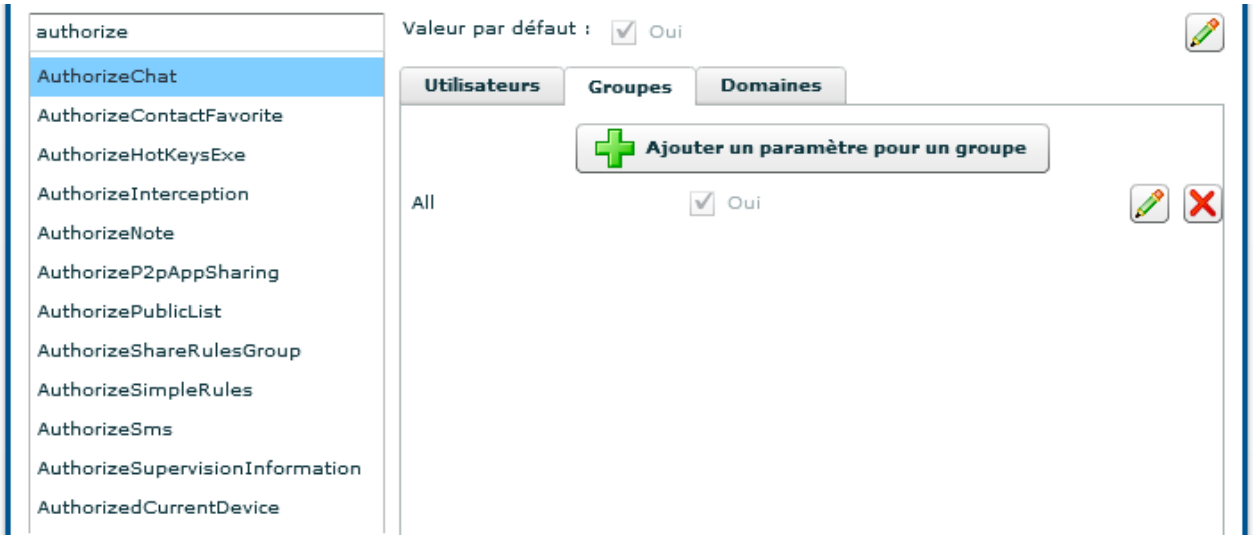
Dans l'onglet *Utilisateurs* ou *Groupes*, choisir l'utilisateur ou le groupe d'utilisateurs qui devra voir l'information après avoir cliqué sur le bouton *Ajouter…* Puis renseigner comme valeur le nom du groupe d'utilisateurs créé précédemment et enfin valider.

Ici, par exemple l'utilisateur « ban » verra la première règle de renvoi active des utilisateurs du groupe « Patrons ».

9.1.8. Toutes les fonctionnalités à activer ou désactiver

Avec l'application Caller, il est possible de rendre visible ou invisible certaines fonctionnalités à un nombre d'utilisateurs ou même à tous les utilisateurs.

Dans le menu *Applications* / *Paramètres applicatifs*, sélectionner TWP *Caller* et rechercher « Authorize » et tous les paramètres qui permettent d'activer ou de désactiver des fonctionnalités Caller apparaîtront.



- *AuthorizeChat* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de faire du chat (texte) entre eux. Le bouton de chat apparaîtra ou non dans la fiche contact.

- *AuthorizeContactFavorite* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de créer leurs contacts privés. Le bouton de création apparaîtra ou non dans le gestionnaire de contacts.

- *AuthorizeHotKeys* : Oui ou Non l'utilisateur a le droit d'utiliser les raccourcis clavier « *Ctrl+F1 / +F2 / … / +F11*» pour générer un appel vers le numéro d'un contact choisi. L'utilisateur choisi le raccourci correspondant directement depuis la fiche du contact.

- *AuthorizeHotKeysExe* : Oui ou Non l'utilisateur a le droit d'utiliser le raccourci clavier « *Ctrl+F12* » pour générer un appel de numéro surligné. L'utilisateur peut modifier ce paramètre depuis les préférences de son Caller.

  N.B. : Ce paramètre n'interdit pas aux utilisateurs d'appliquer d'autres raccourcis clavier (« Ctrl+F1 », « Ctrl+F2 », …) à des contacts via la fiche du contact.

- *AuthorizeInterception* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit d'intercepter des appels arrivant sur les postes de contacts.

- *AuhtorizeNote* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de poster une note public ou non. Le champ texte dans le journal d'évènements pour publier une note apparaîtra ou non.

- *AuthorizeP2pAppSharing* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de déclencher un partage d'application depuis leur PC. Le bouton dans la fenêtre de conversation apparaîtra ou non.

- *AuthorizePublicList* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de mettre une liste privée en liste publique pour qu'elle soit accessible

par d'autres utilisateurs. Le bouton public apparaîtra ou non dans la fenêtre de gestion des listes dans le gestionnaire de contacts.

- *AuthorizeShareRulesGroup* : voir chapitre 9.1.7

- *AuthorizeSimpleRules* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de modifier, créer ou supprimer les règles de renvoi (simples ou avancées). Tous les boutons de gestion des règles de renvois sont disponibles ou non.

- *AuthorizeSms* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit d'envoyer un sms sur un numéro de mobile de contact. Le bouton envoyer un sms apparaîtra ou non dans la fiche contact.

- *AuthorizeSupervisionInformation* : voir chapitre 9.1.7

- *AuhtorizedCurrentDevice* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de créer un nouveau poste courant. Le bouton de création apparaîtra ou non dans les profils.

Paramètres à modifier à partir de la 4.1.SP2b en Mode Expert

- *AuthorizedAdvancedSearch* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de faire une recherche avancé depuis le Caller. La recherche avancée s'active depuis le Caller en cliquant sur la loupe, l'icône de la recherche.

- *AuthorizedCalendarPresences* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de visualiser les évènements Calendrier des contacts faisant partie des listes du Caller.

- *AuthorizedCreateProfil* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de créer un nouveau profil depuis le menu correspondant dans les préférences du Caller.

- *AuthorizedCustomMessagePresences* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont de créer et d'utiliser des messages pour des présences personnalisées.

- *AuthorizedEmailNotification* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de configurer les notifications par mail lors d'appels manqués ou de messages vocaux laissés.

- *AuthorizedExternalChat* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de chatter avec des correspondants externes si un compte de collaboration externe est configuré.

- *AuthorizedMultiChat* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de chatter lors d'une session de conférence.

- *AuthorizedSaveChat*: Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de configurer le mécanisme de sauvegarde des messages instantanés. Si c'est Non, les messages ne seront jamais sauvegardés.

- *AuthorizedPhoneSupervisionPresences* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de visualiser les évènements téléphoniques des contacts faisant partie des listes du Caller.

- *DisplaySimpleRules* : Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de visualiser les règles de renvois créées ou activées depuis le poste téléphonique depuis le menu Profils des Préférences.

- *AuthorizedForwardOriginAll, AuthorizedForwardOriginExternal, AuthorizedForwardOriginInternal, AuthorizedForwardPresenceAsbsent, AuthorizedForwardPresenceBusy, AuthorizedForwardPresenceCalendar, AuthorizedForwardPresenceOffline, AuthorizedForwardPresenceOnline, AuthorizedForwardTypeBusy, AuthorizedForwardTypeImmediate, AuthorizedForwardTypeNoAnswer* :

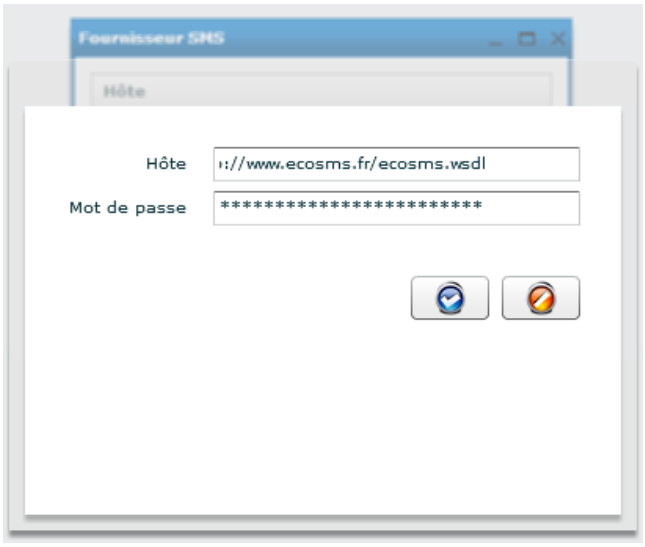
  Oui ou Non l'utilisateur, le groupe d'utilisateurs ou les utilisateurs d'un domaine ont le droit de créer des règles de renvois avec des paramètres spécifiques : l'origine de l'appel, le type de présence ou le type de renvoi à réaliser.

9.1.9. Fonctionnalité SMS

Depuis l'application Caller, il est possible d'envoyer un sms vers le téléphone mobile d'un contact.
La solution TWP fonctionne avec un unique fournisseur de SMS qui se nomme J2S Telecom.

Contacter J2S Telecom
J2S TELECOM - Espace Performance - bâtiment C1/C2 – 35760 Saint Grégoire
+33 (0) 2.99.23.60.81 - contact@j2stelecom.com

Configurer un fournisseur SMS
Dans le menu *Téléphonie / Fournisseur SMS*, ajouter un nouveau fournisseur en cliquant sur le bouton « + » puis remplir les informations comme ci-dessous :



- *Hôte* : Renseigner l'URL de service web de J2S. En général c'est : http://www.ecosms.fr/ecosms.wsdl
- *Mot de passe* : c'est une clé donnée par J2S.

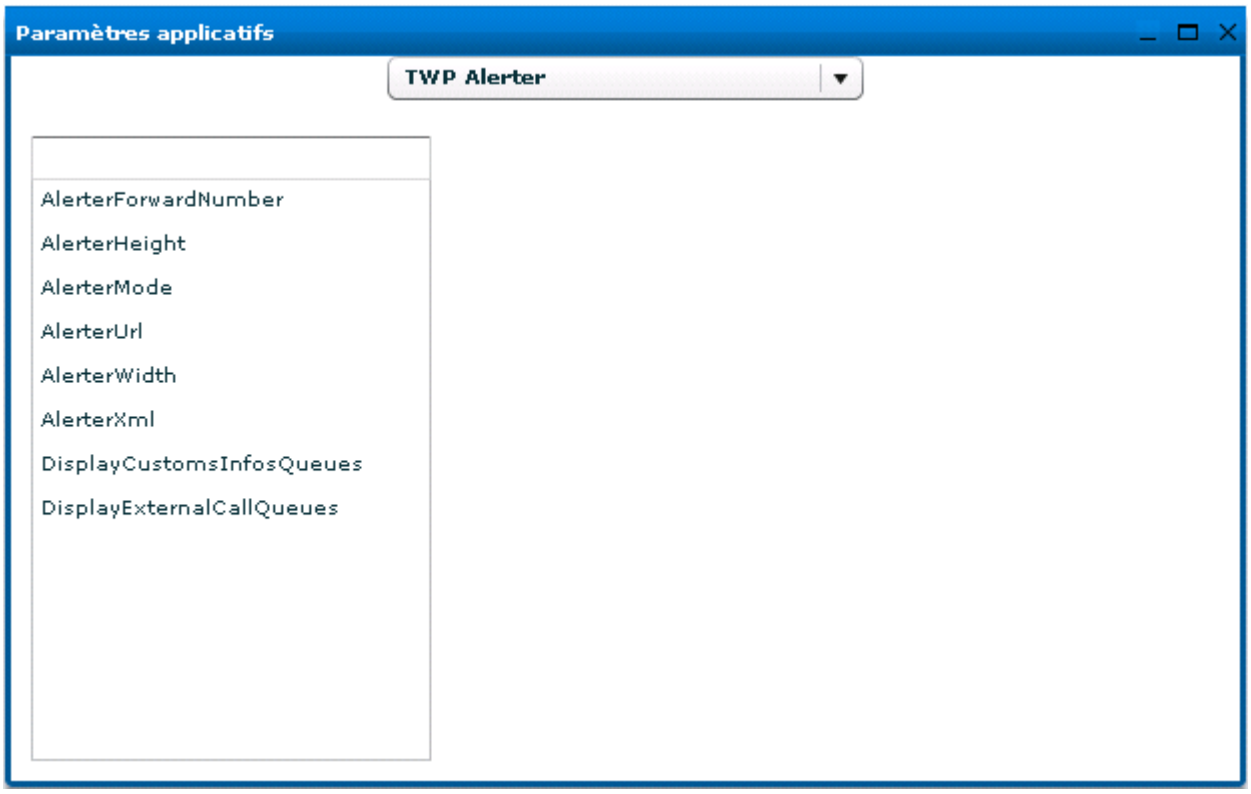
9.2. Configuration de l'Alerter

L'application Alerter est un outil de remontée de fiche avancée et personnalisable. Elle inclut également la fonctionnalité de files d'attente partagées (puits d'appel).
Pour disposer de ces fonctionnalités l'utilisateur doit avoir droit à l'application Alerter, ce qui consommera une licence Alerter.

9.2.1. Personnalisation et paramètres

Sélectionnez le menu *Application* / *Paramètres applicatifs*.

Sélectionnez l'application TWP *Alerter*.



Chaque paramètre a une valeur par défaut défini pendant l'installation. Elle peut être changée. Il est possible de définir la valeur d'un paramètre par utilisateur, groupe ou domaine. Dans ce cas, cette valeur remplacera la valeur par défaut.

Paramètre *'AlerterWidth'*: Ce paramètre défini la largeur de la fenêtre Alerter en pixels.

Paramètre *'AlerterHeight'*: Ce paramètre défini la hauteur de la fenêtre Alerter en pixels.

Paramètre *'AlerterMode'*: Ce paramètre configure le mode de l'Alerter affiché pour les utilisateurs. Deux valeurs possibles:

- « XML »
  - Affiche les boutons d'action téléphonique (Répondre, dévier)
  - Affiche les informations de l'appelant (personnalisable)

- « URL »
  - Affiche les boutons d'action téléphonique (Répondre, dévier)
  - Affiche une page HTML choisi par l'administrateur.

Paramètre *'AlerterXml'*: Ce paramètre est utilisé quand le paramètre *'AlerterMode'* est configuré à « *XML* ». Il contient le nom du fichier XML utilisé pour personnaliser l'affichage des informations des contacts.
Ce fichier se situe dans "\TWS4\TWS_Web\TWS_Config\TWS_Alerter\".

Ce fichier XML est un fichier possédant la balise principale suivante :

<alerter></alerter>

Cette balise « alerter » peut contenir un attribut :

- **vip="true"** ou **vip="false"** : si la valeur est égale à true cela active le mode VIP. Si des contacts sont vus comme VIP le fond du pop-up d'Alerter s'affichera de la couleur choisi dans les préférences du Caller (menu Thème).

Le contenu de la balise <alerter> peut contenir trois types des balises :

<**text**>Texte à afficher</**text**> : Pour afficher du texte.

<**image**>http://urldelimage.com/image.jpg</**image**> : Pour afficher une image.

<**button**>Texte du bouton</**button**> : Pour permettre une action utilisateur.

Chacune de ces balises accepte les attributs suivants :

x="10" y="5" : Pour le placement en pixels de l'élément au sein de la fenêtre Alerter (l'origine est le coin supérieur gauche)

directory="exchange" : Pour conditionner l'affichage de l'élément par l'annuaire dans lequel est présent l'appelant. Il est possible de spécifier plusieurs annuaires en les séparant par des virgules. Si « none » est spécifié, l'élément ne sera affiché que si l'appelant n'est présent dans aucun annuaire.

La balise <button> accepte les attributs suivants :

exe="c:\Windows\notepad.exe [-PhoneNumber-]" : Lance un exécutable lors du clic par l'utilisateur. Ici, ouvre un bloc note avec le numéro de téléphone de l'appelant en tant que nom de fichier.

url="http://www.google.fr/search?q=[-DisplayName-]" : Ouvre une url dans le navigateur par défaut lors du clic de l'utilisateur. Ici, ouvre une recherche Google avec le nom complet de l'appelant.

Dans le fichier XML, chaque champ est délimité par '[-' et '-]' et est remplacé par l'information de l'appelant ou de l'appelé.

Les champs disponibles sont:

- [-Lastname-] : remplacé par le nom de l'appelant
- [-Firstname-] : remplacé par le prénom de l'appelant
- [-DisplayName-] : remplacé par le nom complet de l'appelant
- [-CompanyName-]: remplacé par le nom de la société de l'appelant
- [-Picture-] : remplacé par l'url de la photo de l'appelant

- [-AssistantPhone-] : remplacé par le numéro assistant de l'appelant
- [-StandardPhone-] : remplacé par le numéro standard de l'appelant
- [-WorkPhone-] : remplacé par le numéro bureau de l'appelant
- [-MobilePhone-] : remplacé par le numéro mobile de l'appelant
- [-HomePhone-] : remplacé par le numéro personnel de l'appelant
- [-Email1-] : remplacé par l'email 1 de l'appelant
- [-Email2-] : remplacé par l'email 2 de l'appelant
- [-Url-] : remplacé par le site web de l'appelant
- [-PhoneNumber-] : remplacé par le numéro en cours de l'appelant
- [-ServerName-] : remplacé par le nom du serveur TWP
- [-PersonGuid-] : remplacé par l'identifiant interne de l'appelant
- [-Contact2DisplayName-] : remplacé par le nom complet du redirecteur de l'appel
- [-Contact2PhoneNumber-] : remplacé par le numéro du redirecteur de l'appel
- [-[VIP]-] : remplacé par le contenu VIP d'un contact (cf. Champs spécifiques des annuaires)

Pour les champs privés supplémentaires, par défaut l'information du contact remplacera les éléments suivants :

- [-Custom0-] à [-Custom9-] : remplacés par les champs privés de 0 à 9 de l'appelant configurés au niveau de l'annuaire.

L'utilisation des noms de champs [-Custom0-] à [-Custom9-] est déconseillée dans l'Alerter. La configuration des champs d'un annuaire permet de les nommer comme souhaité. Il est préférable de mentionner dans le fichier XML le nom donné au champ entouré par '[-' et '-]'.

Exemple : Ici l'information à renseigner dans l'Alerter est : [-Id-].

Les champs de l'appelé disponibles sont:

- [-MyFirstname-] : remplacé par le prénom de l'appelé
- [-MyLastname-] : remplacé par le nom de l'appelé
- [-MyUsername-] : remplacé par le nom d'utilisateur de l'appelé
- [-MyCompany-]: remplacé par le nom de la société de l'appelé
- [-MyDevice-] : remplacé par le numéro de poste de l'appelé
- [-MyGsmPhone-] : remplacé par le numéro mobile de l'appelé
- [-MyEmail-] : remplacé par l'email de l'appelé
- [-MyExternalKey-] : remplacé par l'identifiant de l'appelé
- [-MyCustom0-] : remplacé par le champ privé 0 de l'appelé
- [-MyCustom1-] : remplacé par le champ privé 1 de l'appelé

Paramètre *'AlerterUrl'*: Ce paramètre est utilisé quand le paramètre *'AlerterMode'* est configuré à « URL ». Il contient l'adresse web à afficher dans l'Alerter. Vous pouvez configurer l'URL en ajoutant les paramètres vus ci-dessous.

Par exemple: `http://www.google.fr/search?q=[-DisplayName-]`

9.2.2. Configuration de puits d'appels

Pour configurer correctement une file d'attente, suivez la procédure ci-dessous :

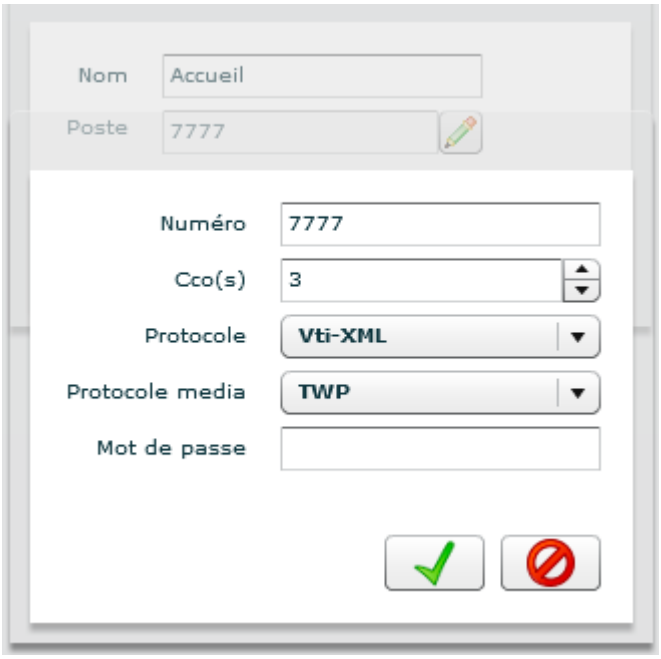
3. **Créer un puits d'appel :**

Il y a plusieurs manières de créer un puits d'appel.
Dans le menu Téléphonie / Puits d'appels, cliquer sur le bouton « + » pour ajouter un nouveau puits. Donner un nom puis le numéro et cliquer sur le bouton d'édition. Renseigner les informations comme il suit :

- *A partir d'un numéro de poste physique existant* : vous possédez déjà un poste physique qui peut être supervisé par TWP, alors son numéro peut être renseigné pour créer un puits d'appels.

Numéro : numéro de poste à renseigner.
Cco(s) : Nombre de lignes disponibles. **Valeur non utilisée** car le poste possède déjà physiquement un nombre de ligne.
Protocole : choisir le protocole de supervision du poste.
Protocole media : Dans le cas d'un poste physique existant, sélectionner ***None***.
Mot de passe : Mot de passe de poste si existant, utile pour la demande de supervision.

- *A partir d'un numéro de poste virtuel* : créer dans votre PBX un poste virtuel lié à aucun poste physique (par exemple poste VTIXML/IP sur A5000). Renseigner son numéro dans la configuration du puits d'appel.

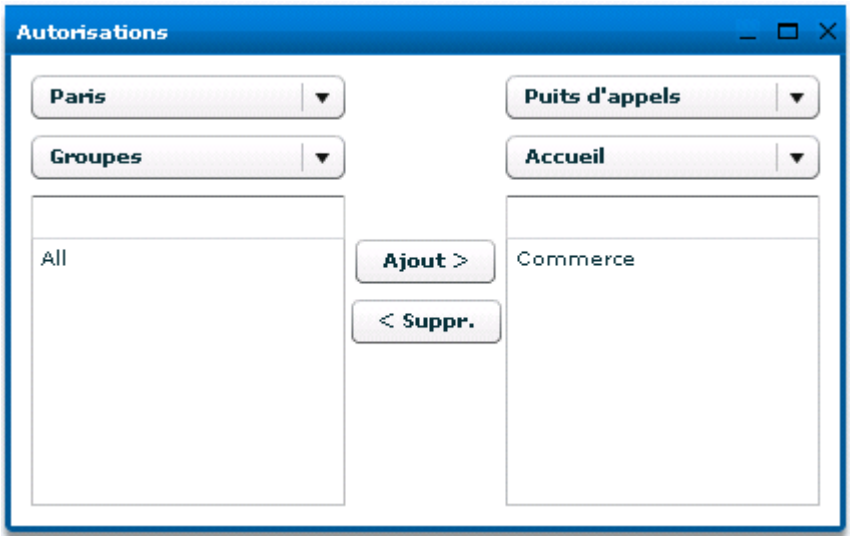


Numéro : numéro de poste à renseigner.
Cco(s) : Nombre de lignes disponibles. Veuillez à en mettre suffisamment pour avoir un nombre d'appels simultanés conséquent.
Protocole : choisir le protocole de supervision du poste.
Protocole media : Dans le cas d'un poste virtuel, sélectionner *TWP*.
Mot de passe : Mot de passe de poste si existant, utile pour la demande de supervision.

4. **Donner les autorisations de visualisation aux utilisateurs :**

Dans le menu *Utilisateurs* / *Autorisations*, sélectionner en haut à droite *Puits d'appels* puis en dessous le puits d'appel à autoriser. Donner ensuite les droits aux utilisateurs ou groupes. (Voir chapitre 7.4.5)

Dans l'exemple, tous les utilisateurs du groupe Commerce du domaine Paris ont le droit de voir le puits d'appels « Accueil ».

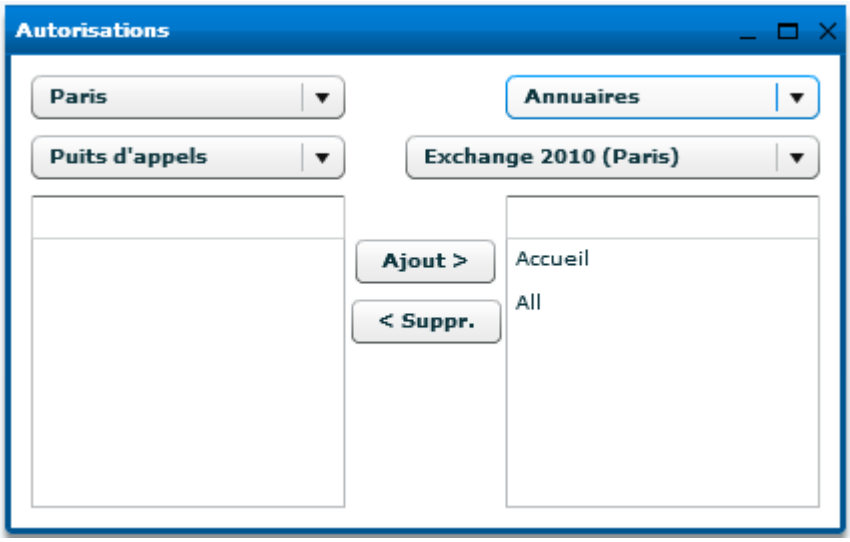


5. **Droits aux annuaires :**

   Pour pouvoir afficher les noms, prénoms et sociétés des correspondants qui appellent, le puits d'appel peut être autorisé à avoir accès aux annuaires TWP.
   Ainsi les correspondants faisant partie de l'annuaire en question seront automatiquement reconnus.

   Dans le menu *Utilisateurs / Autorisations*, sélectionner en haut à droite *Annuaires* puis en dessous l'annuaire à autoriser. Dans la liste de gauche en bas, sélectionner *Puits d'appel* et donner ensuite les droits à un puits d'appels.

   Dans l'exemple le groupe « All » et le puits d'appel « Accueil » ont droit à un annuaire Exchange.



Information : Noter que, comme la fenêtre Alerter, la fenêtre puits d'appel peut également afficher les informations des champs privés des annuaires mais ceci est à activer directement dans les préférences du Caller de chaque utilisateur menu *Alerte*.

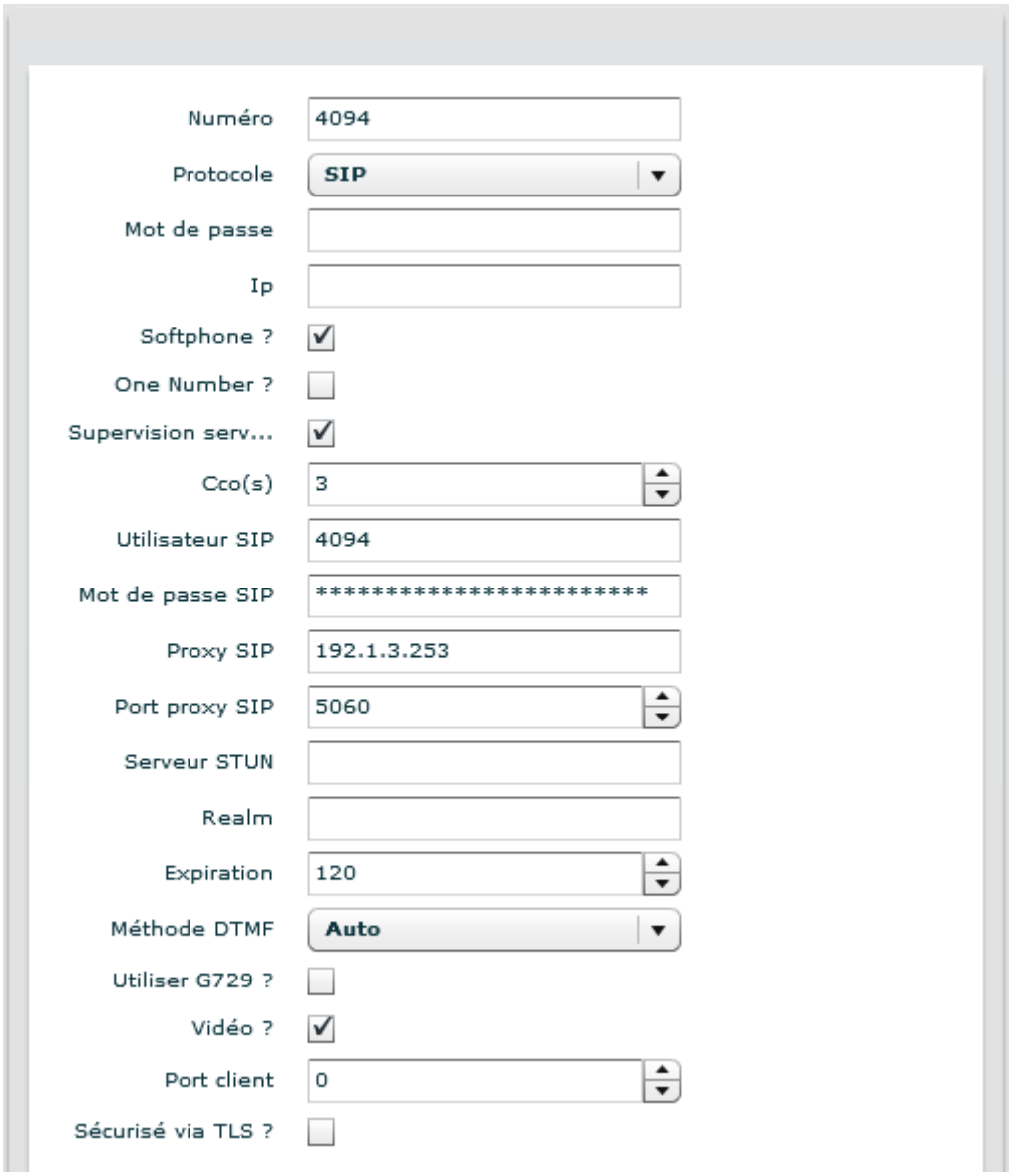
9.3. Configuration d'un Soft phone

Pour définir le poste d'un utilisateur en Soft phone vous devez passer par le menu de gestion des utilisateurs pour créer ou modifier l'utilisateur comme expliqué dans le chapitre 3.3.4.

1. *Configuration*

Pour créer un poste soft phone, allez dans le menu Utilisateurs / Utilisateurs et créez ou éditez un utilisateur.

Définissez le numéro de poste: 4094 par exemple, et cliquez sur le stylo la fenêtre de propriété suivante apparait après avoir choisi « SIP » come protocole.



Définissez les propriétés comme montré dans cet impression-écran :

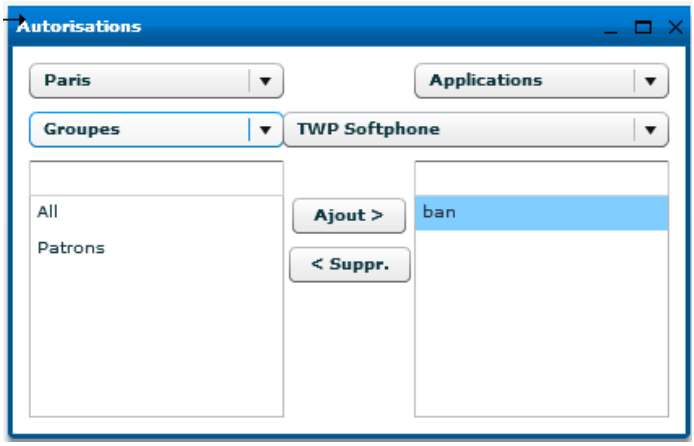
- **Numéro:** le numéro d'extension du Soft phone
- **Protocole:** SIP
- **Mot de passe:** Mot de passe de l'abonné PBX
- **IP:** seulement utilisé pour le recorder IP
- **One Number :** coché le soft phone est en poste associé
- **Cco(s):** le nombre de CCos affecté au Soft phone
- **Utilisateur Sip:** Identifiant SIP
- **Mot de passe SIP:** le mot de passe (MD5) du poste SIP s'il en a un.
- **Proxy SIP:** Adresse IP du proxy SIP (en général, adresse IP du PBX)
- **Port Proxy:** port du proxy SIP.
- **Serveur STUN:** réservé
- **Realm:** réservé.
- **Méthode DTMF**: RTP pour être en mode RFC2833 ou SIPINFO
- **G729**: coché pour autoriser le G729.
- **Vidéo:** coché pour autoriser les appels vidéo.
- **TLS:** coché pour utiliser une connexion cryptée.

Remarque : l'IPBX doit avoir été configuré en conséquence.

2. *Autorisations*

La fonctionnalité Soft Phone est soumise à licence. Il faut donner des autorisations à l'utilisateur possédant un poste configuré en Soft Phone.

Pour donner ces autorisations, allez dans le menu *Utilisateurs* / *Autorisations* et appliquer les droits comme ci-dessous. Dans cet exemple, l'utilisateur « ban » lance son Caller en mode Soft phone.



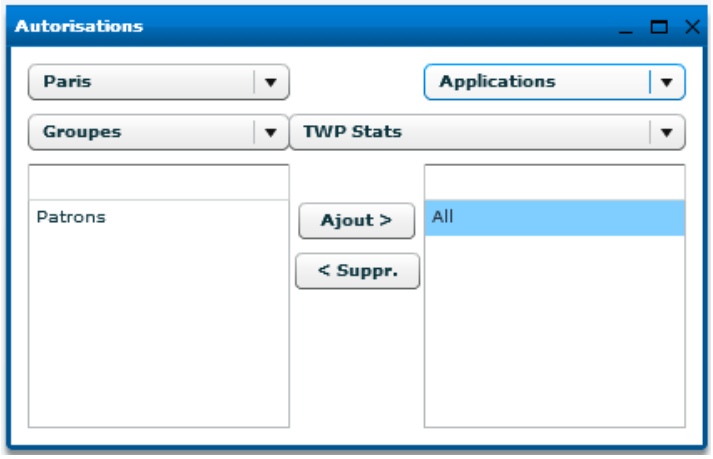
9.4. Configuration de l'application de Statistiques

Grâce à l'application de statistiques, un utilisateur peut visualiser par différents graphiques et sur différentes données ses informations d'appels ou celles d'autres utilisateurs.

Les données statistiques des utilisateurs sont conservées uniquement pendant un certain nombre de jours (voir chapitre 10.2.2.).

9.4.1. TWP Stats

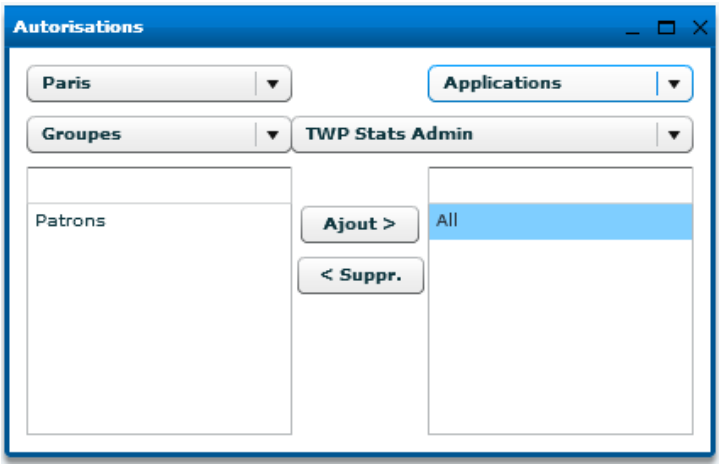
Pour disposer de cette application et permettre à un utilisateur de visualiser ses propres statistiques, il suffit de donner les autorisations à l'application TWP *Stats*, dans l'administration menu *Utilisateurs* / *Autorisations*. Cela consomme 1 licence Stats par utilisateur.



9.4.2. TWP Stats Admin

1. *Autorisations Application*

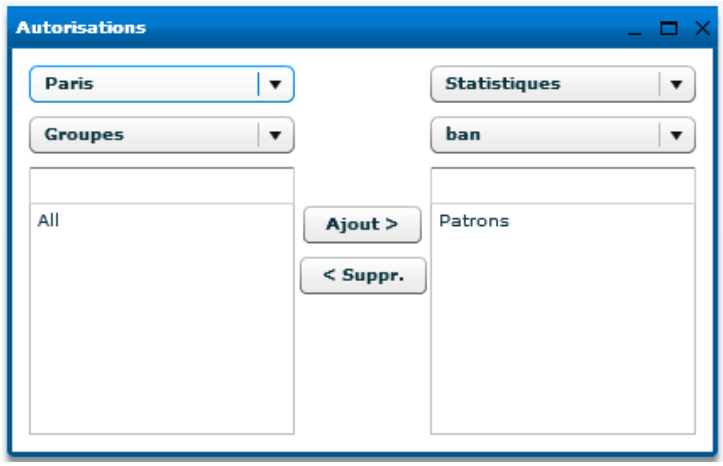
Pour disposer de cette application et permettre à un utilisateur de visualiser les statistiques d'autres utilisateur, il faut donner les autorisations à l'application TWP *Stats Admin*, dans l'administration menu *Utilisateurs* / *Autorisations*. Cela consomme 1 licence Stats Admin par utilisateur.



2. *Autorisations Statistiques Utilisateurs*

Pour que l'utilisateur ait accès aux statistiques d'autres utilisateurs, il faut également donner des autorisations sur les statistiques des utilisateurs en question.
Dans l'administration menu *Utilisateurs* / *Autorisations*, choisir *Statistiques* dans la liste en haut à droite. Contrairement aux autorisations sur les autres objets, celles sur les statistiques se fait à l'inverse (voir chapitre 7.4).

En effet l'exemple ci-dessous montre que l'utilisateur « ban » a accès aux statistiques des utilisateurs du groupe « Patrons ».

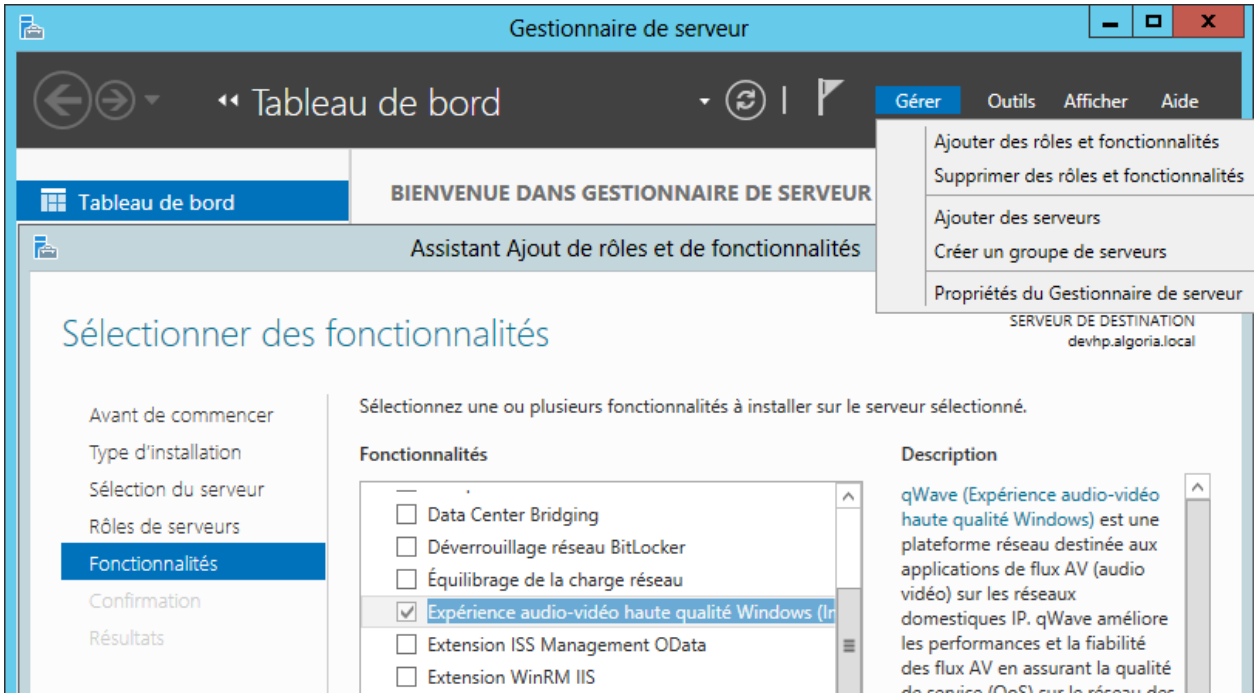


9.5. Configuration des automates d'appel pour les applications Rules, Mail, VideoShare

Les automates d'appel permettent à l'utilisateur de configurer une annonce vocale dans une règle pour qu'elle soit lue avant le renvoi d'appel pour l'application Rules.
Les automates d'appel permettent de mettre en conférence un utilisateur, maître de conférence, et les participants.

Prérequis :

- Installer la fonctionnalité *Expérience Audio-Vidéo haute qualité Windows* du système Windows depuis la fenêtre du *Gestionnaire de serveur* / *Gérer* / *Ajouter des rôles et fonctionnalités*.
  Exemple sur un serveur Windows 2012 ci-dessous.
  Attention : Sans cette fonctionnalité, le service TWS4$TWS_ConferenceServices ne démarre pas.

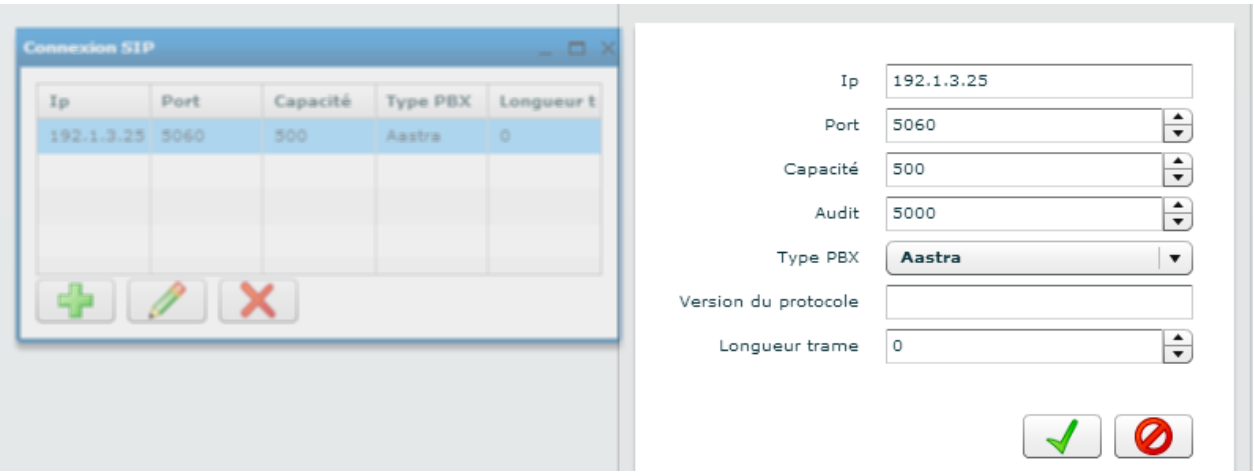


- Le central téléphonique (PBX) doit permettre la supervision de poste virtuel SIP via une connexion SIP.

9.5.1. Connexion SIP

Avant de configurer les automates à utiliser dans les différentes applications, il faut créer la connexion SIP nécessaire à leur enregistrement sur le PBX.

Dans l'administration, Menu *Connexions* puis *Connexion SIP*, cliquer sur le bouton + pour ajouter une nouvelle connexion SIP.



Dans la nouvelle fenêtre qui s'ouvre rentrer les informations les plus essentielles comme il suit :

- **Ip** : adresse IP du PBX qui supporte l'enregistrement SIP
- **Port** : Port du PBX pour l'enregistrement SIP
- **Type PBX** : Choisir le type de PBX

Laisser les valeurs des autres informations par défaut. Valider ensuite. Une nouvelle connexion SIP est créée.

N.B. : Une seule connexion SIP sera nécessaire et sera utilisée. Pour configurer une 2e connexion SIP, il faut absolument le faire dans un nouveau domaine.

9.5.2. Configuration des automates d'appel

Pour configurer ces automates, aller dans l'administration, menu *Applications* puis choisir l'application concernée : TWP *Rules*, TWP *VideoShare*. Si dans les menus n'apparaît pas l'application liée aux automates à créer alors cliquer sur le menu *Applications* puis éditer l'application concernée. Cliquer ensuite sur le bouton *Modifier*, puis dans la nouvelle fenêtre sur le bouton +.

Dans la nouvelle fenêtre qui s'ouvre rentrer les informations comme il suit :

- **Numéro** : premier numéro de la suite de numéros d'automates à créer
- **Protocole** : *SIP* uniquement
- **Protocole media** : *None* uniquement
- **Mot de passe** : Mot de passe d'enregistrement SIP de tous les postes automates à créer. *0000* par défaut.
- **Nb demandé** : Nombre de numéro d'automates à créer à la suite du *Numéro* donnée plus haut.

Valider puis fermer dans les fenêtres.
Les automates sont créés. **Il est nécessaire de redémarrer le service TWS4$TWS_MediaServices pour qu'ils soient enregistrer au niveau du PBX.**

9.6. Configuration de l'application Rules

Sans l'application Rules, un utilisateur peut déjà renvoyer des appels en configurant des règles simples qui fixeront à leur activation les renvois dans le PBX. Grâce à l'application Rules, celui-ci pourra effectuer des renvois à partir de règles avancées extrêmement configurables qui se basent sur un certain nombre de fonctionnalités à configurer.

9.6.1. Configuration des automates d'appel

Voir le chapitre *9.5 Configuration des automates d'appel pour les applications Rules, Mail, VideoShare*.

9.6.2. Configuration des paramètres Rules

Un certain nombre de paramètres permettent de régler des fonctionnalités des règles avancées. Pour accéder à ces paramètres, aller dans l'administration, Menu *Applications* puis *Paramètres applicatifs*. Sélectionner TWP *Rules*.

- **CIRCULARLEVEL** : *Nombre* de renvoi à interdire avant retour au premier poste qui fait le renvoi. Si le système rencontre ce conflit, aucun renvoi n'est exécuté.
  0 = aucune vérification
  1 = A ne peut pas renvoyer vers A
  2 = B ne peut pas renvoyer vers B et ne peut pas renvoyer vers A qui renvoie vers B …

- **EMERGENCYNUMBER** : *numéro* d'urgence à joindre si les numéros vers lesquels les utilisateurs vont renvoyer leurs appels ne répondent pas (dans le cas de *TRANSFERVERIFICATION* = *Oui* (True))

- **EMERGENCYNUMBERCALLTIMES** : *Nombre* de fois que le numéro d'urgence sera joint dans le cas où personne ne répond

- **IsUserAuthorizedToCreateWithAdminRules** : *Oui* ou *Non* l'utilisateur pourra créer ses propres règles lorsque l'administrateur lui en affectera d'autres

- **TRANSFERVERIFICATION** : *oui* ou *non* le système pourra vérifier que les appels renvoyés par les utilisateurs seront bien décrochés par leur correspondant. Si une règle contient un faux numéro comme numéro de renvoi, le système détectera et renverra vers le numéro d'urgence si configuré.

- **WAITTIMENOREPLY** : Temps en *secondes* d'attente pour une règle avancée (RULES) avant renvoi sur non réponse

- **WAITTIMENOREPLYPBX** : Temps en *secondes* d'attente pour une règle PBX/simple avant renvoi sur non réponse. Cette valeur doit être copiée de celle du PBX.

9.7. Configuration de l'application VideoShare

9.7.1. Configuration des automates d'appel

Voir le chapitre *9.5 Configuration des automates d'appel pour les applications Rules, Mail, VideoShare*.

9.7.2. Configuration des paramètres liés à la conférence Audio – Vidéo et partage d'applications

Un certain nombre de paramètres permettent de gérer certaines configurations liées à la conférence Audio – Vidéo et partage d'applications. Pour accéder à ces paramètres, aller dans l'administration, Menu *Applications* puis *Paramètres applicatifs*.

Sélectionner TWP *MediaServer*.

- **AppSharingRouterIP** : Adresse IP de la machine qui fait fonctionner le service TWS4$TWS_AppSharingRouterServices. **Il est important de modifier cette valeur et mettre l'adresse IP du serveur TWP**.

- **AppSharingRouterPort** : Port de la machine qui fait fonctionner le service TWS4$TWS_AppSharingRouterServices sur lequel sera adressée toute demande concernant le partage d'application. Par défaut, la valeur est 8202.

(Expert Mode)

- **MediaServerSIP_IP** : Adresse IP de la machine qui fait fonctionner le service TWS4$TWS_ConferenceServices. Il est important de modifier cette valeur si le service fonctionne sur un serveur déporté.

- **MediaServerSIP_Port** : Port de la machine qui fait fonctionner le service TWS4$TWS_ConferenceServices sur lequel sera adressée toute demande concernant les conférences Audio - Video. Par défaut, la valeur est 8201.

10. Maintenance

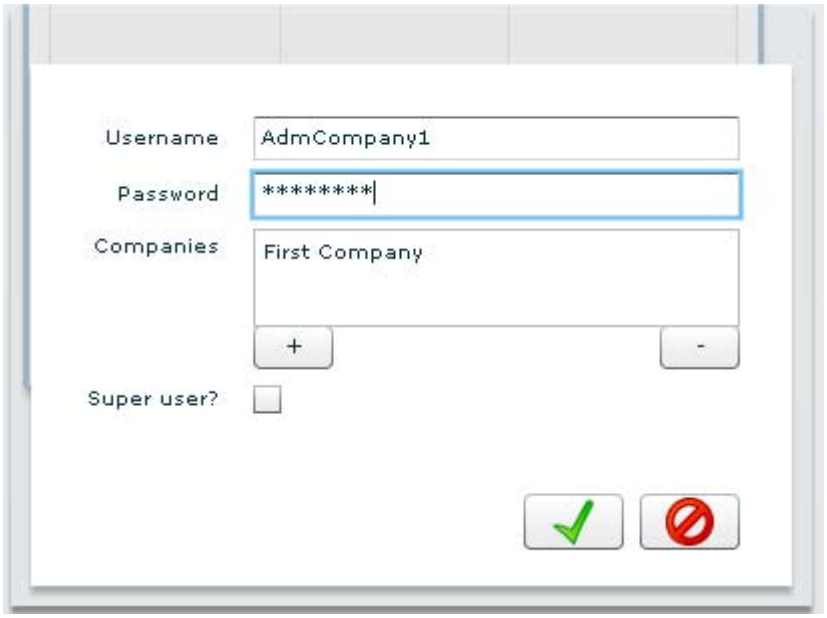
10.1. Gérer les profils des administrateurs

Les administrateurs ont généralement pour tâche de gérer les droits spécifiques d'un utilisateur.

Si vous souhaitez limiter l'accès de l'interface d'administration à une seule entreprise, il vous faut créer un nouveau compte administrateur.

Sélectionnez le menu Global / Utilisateurs de TWP admin.

Cliquez sur "+".



Entrez le nom de l'administrateur ainsi que son mot de passe, puis ajoutez la liste des entreprises autorisées pour cet administrateur en cliquant sur le bouton "+".

L'option Super Utilisateur autorise l'utilisateur concerné à accéder à toutes les entreprises.

10.2. Paramètres du système et mode Expert

Paramètres du système

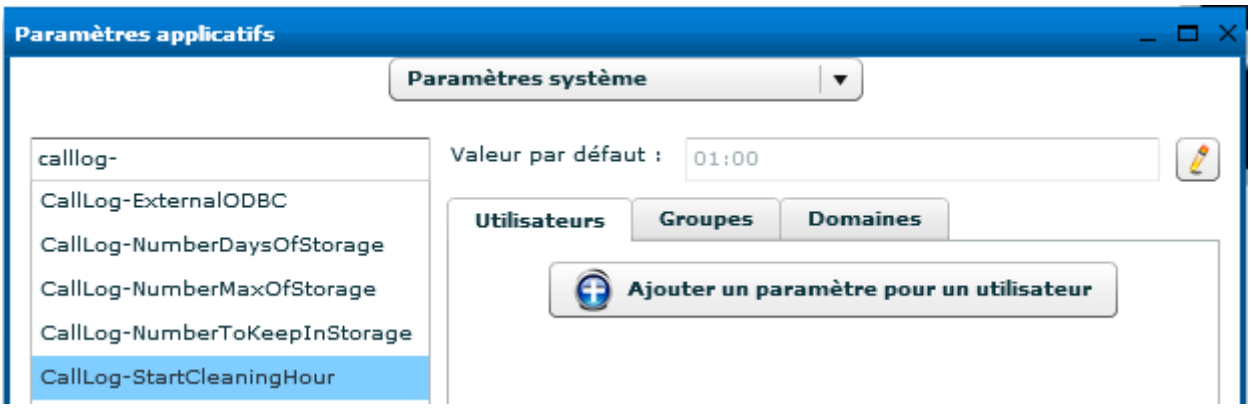
Tous les paramètres standards du système pour le TWP server sont contenus dans le menu *Applications /Paramètres applicatifs* puis *Système*. Ne modifiez aucun de ces paramètres sauf si décrits dans ce document ou que le support vous le demande.

Mode Expert

Quel que soit le type de paramètre, système ou applicatif, il existe des paramètres visibles uniquement en mode Expert. Vous pouvez activer ce mode dans l'administration en passant la souris à droite du bouton « *se déconnecter* ». La case à cocher s'affichera et à ce moment cliquer dessus et de nouveaux paramètres apparaîtront.

10.2.1. Suppression automatique de données : journaux d'appels

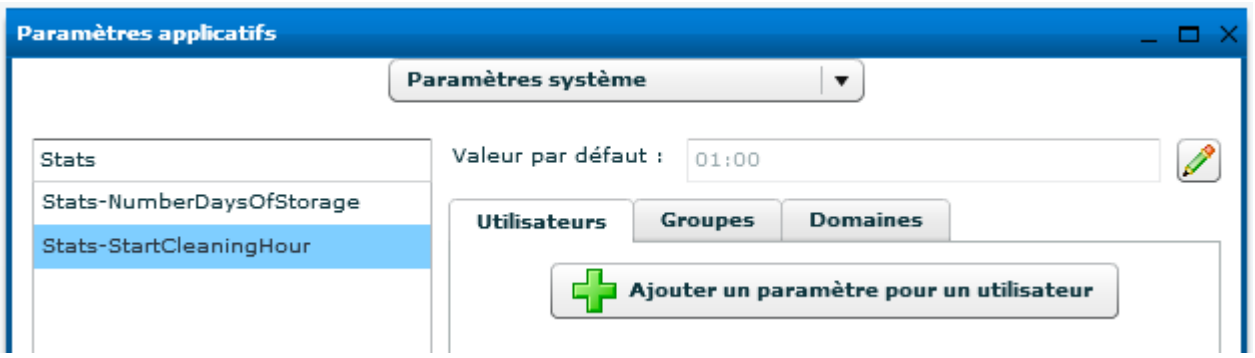
Dans le menu *Applications /Paramètres applicatifs* puis *Système*, chercher « *CallLog-* » et 3 paramètres s'afficheront :



- *CallLog-StartCleaningHour* : sous le format HH:MM (heure et minute), modifier uniquement la valeur par défaut pour renseigner le moment de la journée où le nettoyage des journaux d'appels se fera.
- *CallLog-NumberMaxOfStorage* : Nombre de lignes par type de journal d'appels (Entrant, Sortant, Manqué) à conserver au bout d'une journée. Valeur par défaut 30.
- *CallLog-NumberDaysOfStorage* : Indépendamment du paramètre précédent, celui-ci désigne le nombre de jours pendant lesquels des appels dans un journal seront conservés. Valeur par défaut 30.
- *CallLog-NumberToKeepInStorage* : Indépendamment des paramètres précédents, celui-ci désigne le nombre minimum d'appels à conserver dans le journal d'un utilisateur. Valeur par défaut 30.

10.2.2. Suppression automatique de données : Statistiques

Dans le menu *Applications* /*Paramètres applicatifs* puis *Système*, chercher « *Stats-* » et 2 paramètres s'afficheront :

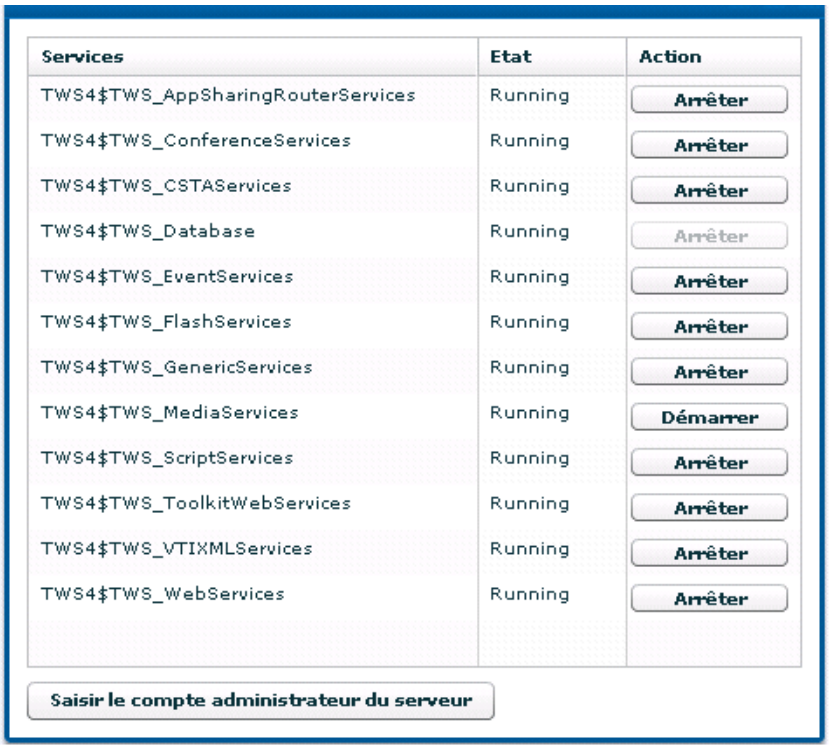


- *Stats-StartCleaningHour* : sous le format HH:MM (heure et minute), modifier uniquement la valeur par défaut pour renseigner le moment de la journée où le nettoyage des données statistique se fera.
- *Stats-NumberDaysOfStorage* : Ce paramètre désigne le nombre de jours pendant lesquels des données statistique seront conservés.

10.3. Services

Ouvrez le menu déroulant Maintenance et cliquez sur le menu TWP Service.

Ce menu vous permet de contrôler le statut des services TWP server.



Cliquez sur "*Saisir le compte administrateur du serveur*": vous devez entrer les informations de l'administrateur local de la machine afin de démarrer et arrêter les services Windows depuis cet écran.

Cliquez "*Enregistrer*".

- Démarrer TWS4$TWS_Database
- Démarrer TWS4$TWS_GenericServices, les autres services seront lancés automatiquement

10.4. Etat des connexions

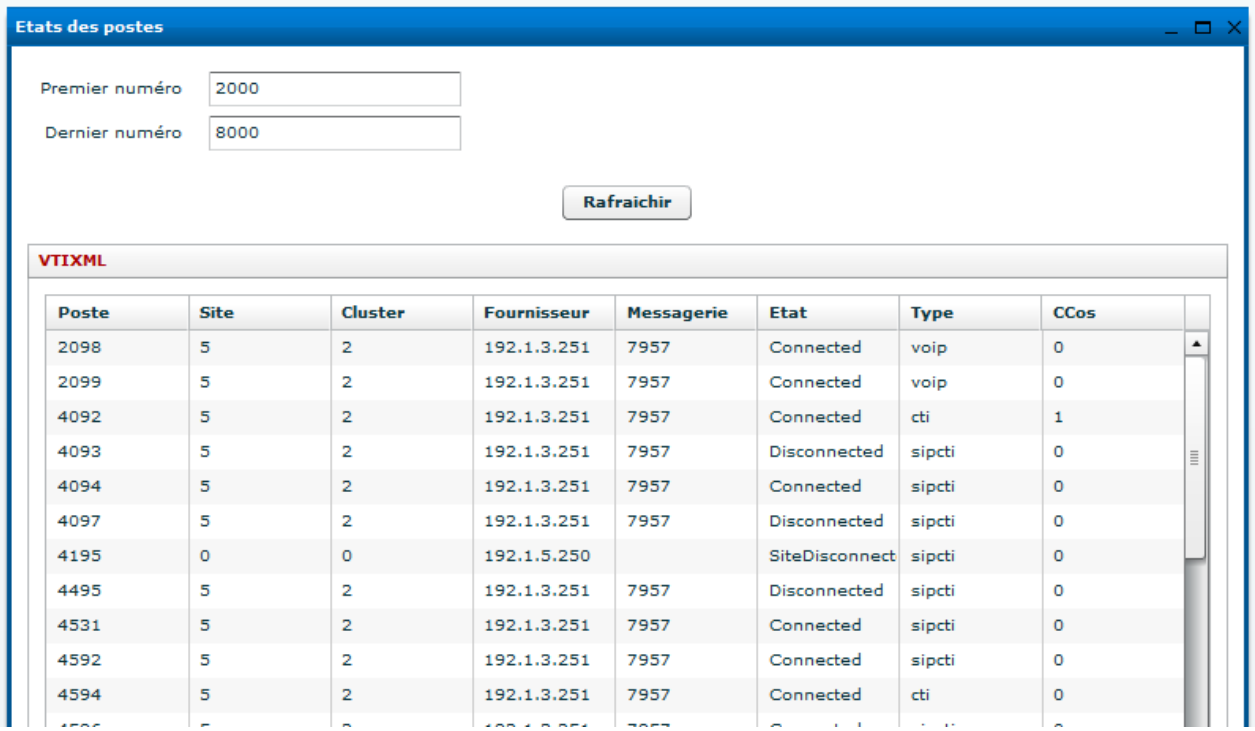
Ouvrez le menu déroulant *Outils* et cliquez sur le menu *Etat des Connexions*. Ce menu vous permet de vérifier l'état des connexions PBX.

L'exemple ci-dessous montre le statut des connexions VTIXML:

- *Hôte*: adresse IP de l'IPBX
- *Connecté*: vrai (true) si le lien est connecté
- *Courant*: nombre de postes supervisés par ce lien
- *Site*: Site.Grappe défini pour ce lien (seulement pour le connecteur VTIXML)
- *Domaine*: Nom du domaine affecté au lien
- *Port*: port TCP utilisé par le connecteur
- *Total*: nombre maximal de postes supervisés par ce lien

10.5. Etat des postes

Ouvrez le menu *Outils*, *Etat des Postes*. Entrez le premier et le dernier numéro de postes que vous voulez superviser et cliquez sur Rafraichir:



Poste	Site	Cluster	Fournisseur	Messagerie	Etat	Type	CCos
2098	5	2	192.1.3.251	7957	Connected	voip	0
2099	5	2	192.1.3.251	7957	Connected	voip	0
4092	5	2	192.1.3.251	7957	Connected	cti	1
4093	5	2	192.1.3.251	7957	Disconnected	sipcti	0
4094	5	2	192.1.3.251	7957	Connected	sipcti	0
4097	5	2	192.1.3.251	7957	Disconnected	sipcti	0
4195	0	0	192.1.5.250		SiteDisconnect	sipcti	0
4495	5	2	192.1.3.251	7957	Disconnected	sipcti	0
4531	5	2	192.1.3.251	7957	Connected	sipcti	0
4592	5	2	192.1.3.251	7957	Connected	sipcti	0
4594	5	2	192.1.3.251	7957	Connected	cti	0

- *Postes*: numéro de l'abonné
- *Site*: Site ou est enregistré l'abonné (VTIXML seulement)
- *Cluster*: Cluster ou est enregistré l'abonné (VTIXML seulement)
- *Fournisseur*: Identifiant de la connexion fournisseur
- *Messagerie*: numéro de boîte vocale affecté à l'abonnement
- *Etat*: Connected / Disconnected
- *Type*: CTI / VOIP / SIPCTI, type de supervision du poste.
- *CCos*: nombre de CCos (seulement pour le Soft phone).

10.6. Traces

Ouvrez le menu *Outils/Traces*.

Vous pouvez tracer TWP services à distance en utilisant le logiciel Syslog ou en déclenchant les PDU. Cette option est seulement utilisée sous la supervision du support technique.

Trace Pdu:

Ne démarrez pas l'option "start Pdu trace" sans y avoir été invité par le support technique. Sélectionnez le protocole que vous souhaitez tracer.

Start: démarrez la trace Pdu pour le numéro du poste défini dans le champ. Entrez le caractère '*' pour tracer tous les échanges.

Stop: arrêtez la trace Pdu

Le répertoire contenant la trace est dans:

- CSTA: C:\ \Program Files\TWS4\TWS_Services\TWS_CSTAServices\Trace
- VTI-XML: C:\ \Program Files\TWS4\TWS_Services\TWS_VTIXMLServices\Trace

Syslog:

Entrez l'adresse IP spécifiée par le support technique. Il s'agit de l'IP de la machine qui utilise le logiciel Syslog:

Start: démarrez le syslog

Stop: arrêtez le syslog
Les traces seront envoyées au serveur syslog à l'adresse définie.

10.7. Sauvegarde de la configuration

Faire une sauvegarde de la base de données

- Aller dans le répertoire « \TWS4\TWS_Web\TWS_Data\DatabaseBackup »
- Exécuter « backup.bat »
- La sauvegarde se trouve dans le dossier « data » et porte le nom du jour

Faire une sauvegarde complète de la configuration

- Sauvegarder les dossiers :
    - \TWS4\TWS_Web\TWS_Config
    - \TWS4\TWS_Web\TWS_Data

Faire une restauration de la base de données

- Aller dans le répertoire « \TWS4\TWS_Web\TWS_Data\DatabaseBackup »
- Exécuter « restore.bat »
- Une liste des sauvegardes disponibles s'affiche. Saisir le nom de la sauvegarde à restaurer
- La base de données TWP est restaurée

Créer une tache planifiée pour la sauvegarde de la base de données

- Aller dans « \TWS4\TWS_Web\TWS_Data\DatabaseBackup »
- Exécuter « backup_create_windows_task.bat »
- La tâche est créée, elle exécute le script « backup.bat » quotidiennement à 2h du matin
- Le gestionnaire des tâches planifiées s'ouvre, il est possible de modifier la tâche « TWS_DATABASE_BACKUP » pour en affiner sa configuration. [facultatif]

Copier automatiquement les sauvegardes sur un autre ordinateur

- Editer le fichier « backup.bat » avec bloc-notes.
- Compléter la ligne « set COPYPATH= » avec un chemin où copier la sauvegarde

(Exemple : set COPYPATH=\\10.0.0.1\share\Backup\TWP)

- Enregistrer les modifications

10.8. Troubleshooting

10.8.1 Problème standard

Ci-dessous, vous trouverez quelques exemples de disfonctionnement, avec les sources possibles de problèmes et leurs solutions.

Type de problème	Message d'erreur ou symptômes	Test	Détails ou actions
L'application ne démarre pas	Certains utilisateurs ne peuvent pas se connecter	Les paramètres de l'utilisateur sont mal définis (vérifiez dans l'administration du TWP)	Les champs suivants sont obligatoires: - Nom d'utilisateur - Autorisation (serveur et applications) - N° du poste - Type de poste
	Licences	Les licences (applications ou serveur) ne sont pas prises en compte	Consultez le chapitre 7.4.1 pour accéder ou vérifier les licences via l'administration TWP.
	PABX	La connexion au PBX ne fonctionne pas	Vérifiez la concordance entre l'adresse IP entrée dans l'administration TWP et l'adresse PBX.
	Services	Les services TWP n'ont pas démarré	Vérifiez leur état (Démarré/Arrêté) via l'administration. Démarrez-les si besoin
	Certains utilisateurs ne peuvent pas se connecter	Le nom de l'utilisateur n'a pas été sauvegardé sur ce serveur ou sur le serveur du domaine	Si les domaines sont différents entre l'utilisateur et TWP server, ajoutez l'utilisateur (même nom d'utilisateur login, même mot de passe) dans le compte du serveur local
	CSTA	En mode CSTA: vérifier le nombre de licences CSTA dans le PBX	Selon les PBX, le nombre de licences doit correspondre au nombre de licences utilisées dans le mode CSTA
	CSTA	En mode CSTA: vérifier la configuration du port CSTA (ex : 3211 pour A5000 cf. doc)	Le port CSTA n'est pas toujours configuré par défaut dans le PBX.
	"Accès refusé"	L'utilisateur n'a pas les droits d'accès au serveur http	Vérifiez les droits de l'utilisateur sur TWP server
Echec de l'importation des annuaires	Le temps d'attente est long (en mode manuel)	Normal s'il y a beaucoup de documents	L'importation de documents peut prendre du temps s'ils sont nombreux. N'interrompez pas le processus

	Echec de l'import des annuaires Exchange(1)	L'identifiant/mot de passe sont erronés	Dans les champs Identifiant/Mot de passe, vous devez entrer un nom d'utilisateur avec les droits *Serveur du domaine* Ex*change pour le bon serveur Exchange*.
	Echec de l'import des annuaires Exchange (2)	L'adresse de connexion est erronée	Testez l'URL de connexion dans Internet Explorer (ceci devrait vous ouvrir une page vers Outlook Web Access)
	Echec de l'import LDAP	Le nom d'utilisateur/mot de passe ont mal été renseignés /ou les clés LDAP sont erronées	Attention aux majuscules/minuscules pour les groupes ou noms de domaines

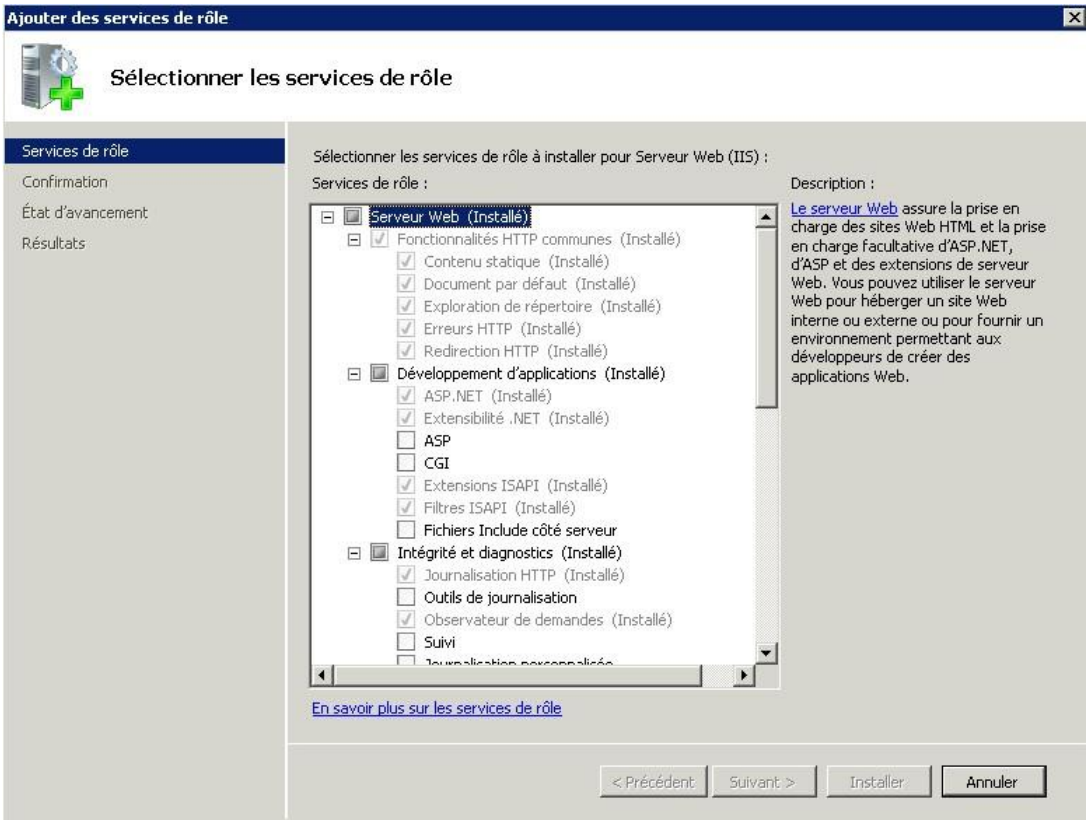
11. Annexes

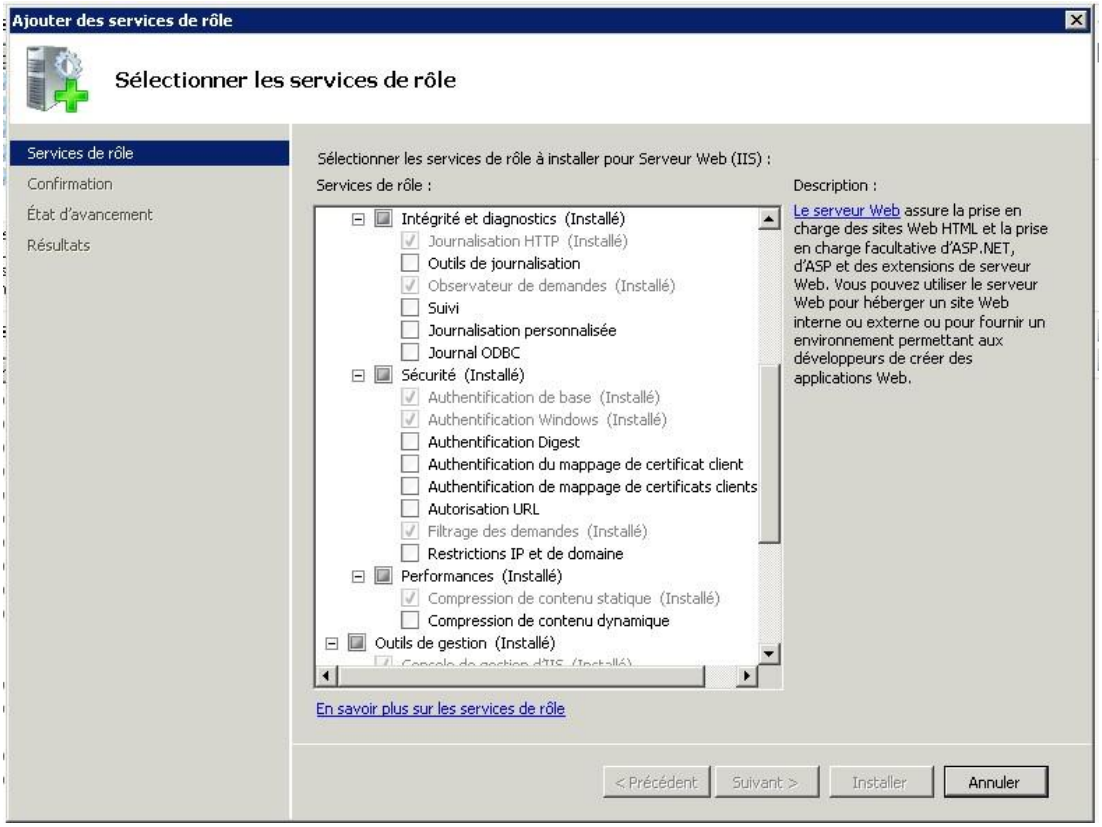
11.1. Installation sur Windows 2008 – 2012 x64

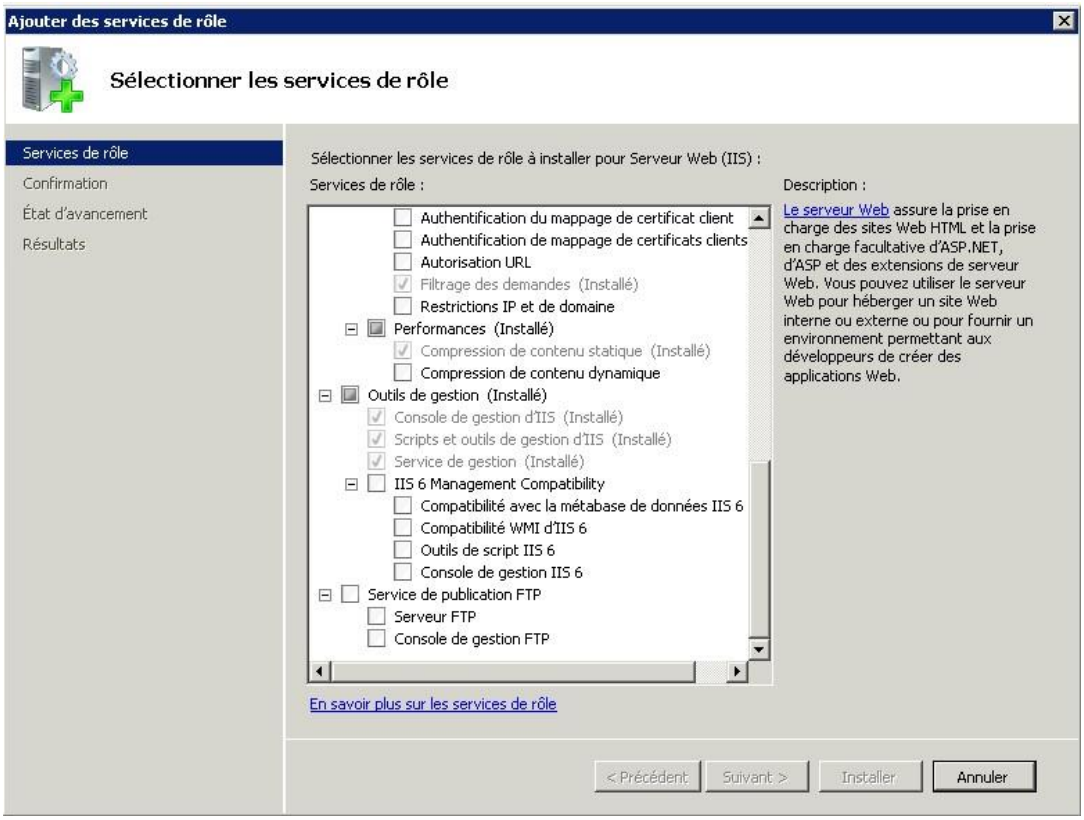
11.1.1. Paramétrage IIS

Au niveau du Gestionnaire de serveur, sélectionner le menu permettant d'ajouter de nouveaux rôles (*clic droit sur le menu Rôles > Ajouter un rôle* pour w2008 - *Gérer > Ajouter des rôles et fonctionnalités* pour w2012).
Ci-dessous la liste des services à installer :

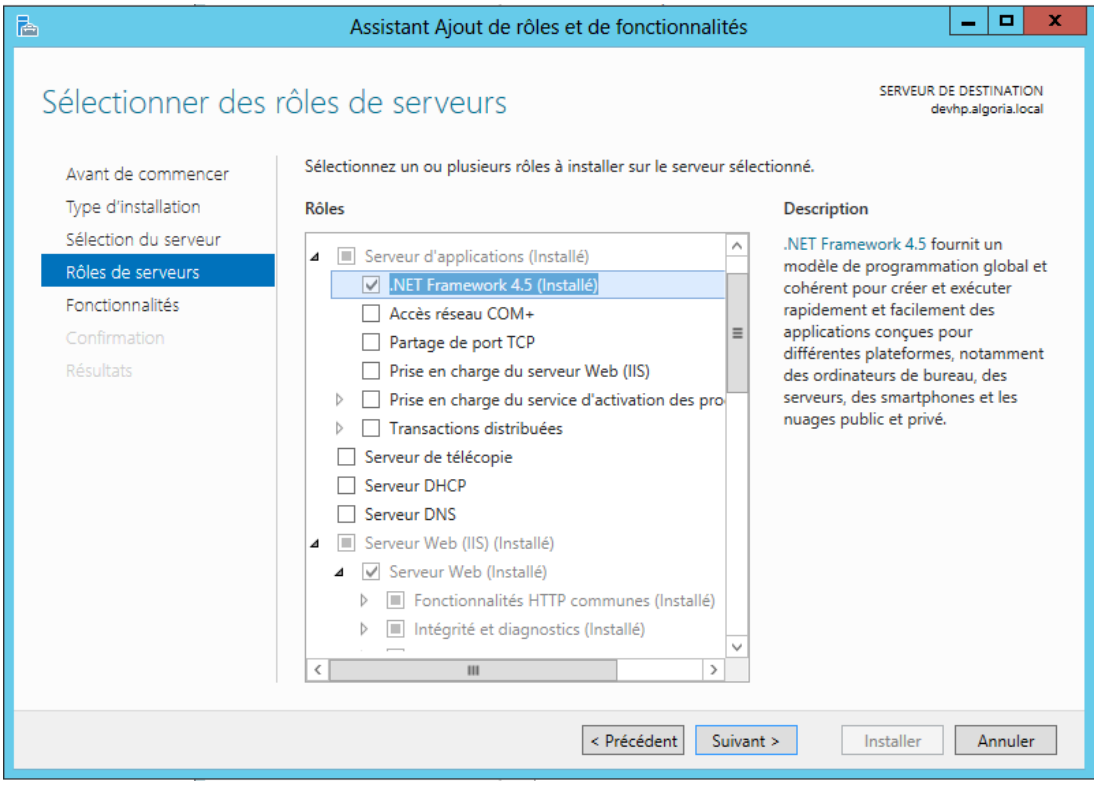
- ***Sous W2008 & W2012:***

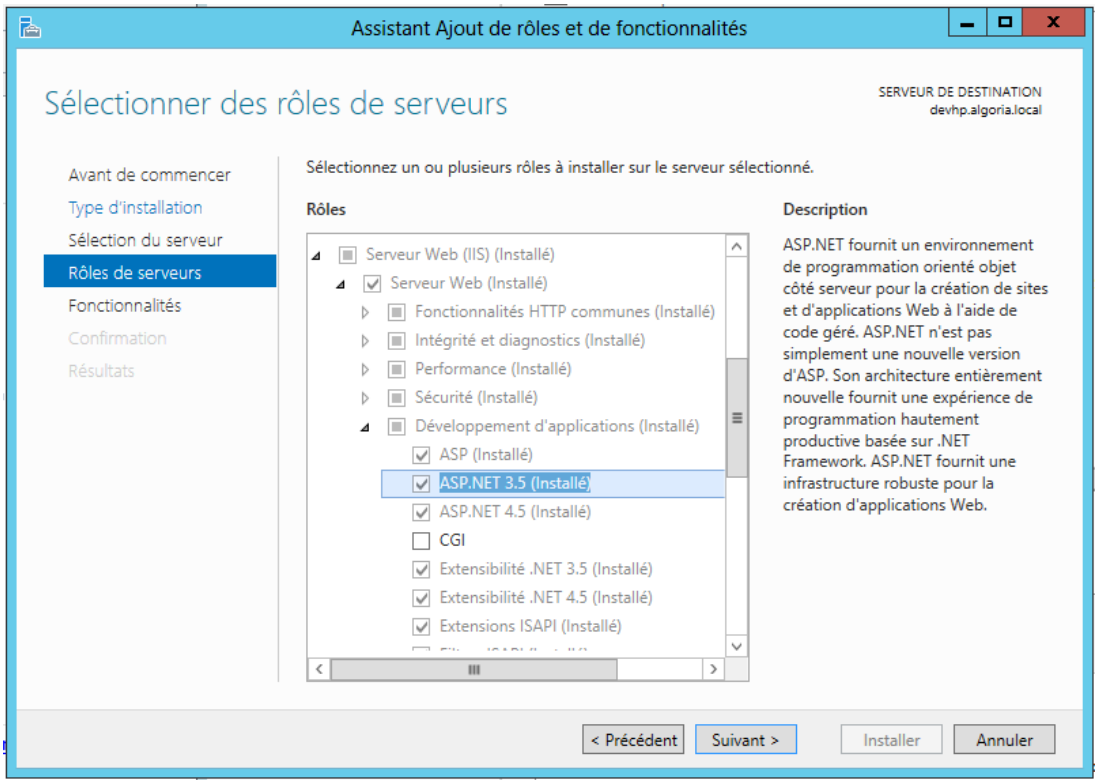



Ajouter des services de rôle
Sélectionner les services de rôle
Services de rôle
Confirmation
État d'avancement
Résultats
Sélectionner les services de rôle à installer pour Serveur Web (IIS) :
Services de rôle :
Intégrité et diagnostics (Installé)
Journalisation HTTP (Installé)
Outils de journalisation
Observateur de demandes (Installé)
Suivi
Journalisation personnalisée
Journal ODBC
Sécurité (Installé)
Authentification de base (Installé)
Authentification Windows (Installé)
Authentification Digest
Authentification du mappage de certificat client
Authentification de mappage de certificats clients
Autorisation URL
Filtrage des demandes (Installé)
Restrictions IP et de domaine
Performances (Installé)
Compression de contenu statique (Installé)
Compression de contenu dynamique
Outils de gestion (Installé)
Description :
Le serveur Web assure la prise en charge des sites Web HTML et la prise en charge facultative d'ASP.NET, d'ASP et des extensions de serveur Web. Vous pouvez utiliser le serveur Web pour héberger un site Web interne ou externe ou pour fournir un environnement permettant aux développeurs de créer des applications Web.
En savoir plus sur les services de rôle
< Précédent
Suivant >
Installer
Annuler


Ajouter des services de rôle
Sélectionner les services de rôle
Services de rôle
Confirmation
État d'avancement
Résultats
Sélectionner les services de rôle à installer pour Serveur Web (IIS) :
Services de rôle :
Authentification du mappage de certificat client
Authentification de mappage de certificats clients
Autorisation URL
Filtrage des demandes (Installé)
Restrictions IP et de domaine
Performances (Installé)
Compression de contenu statique (Installé)
Compression de contenu dynamique
Outils de gestion (Installé)
Console de gestion d'IIS (Installé)
Scripts et outils de gestion d'IIS (Installé)
Service de gestion (Installé)
IIS 6 Management Compatibility
Compatibilité avec la métabase de données IIS 6
Compatibilité WMI d'IIS 6
Outils de script IIS 6
Console de gestion IIS 6
Service de publication FTP
Serveur FTP
Console de gestion FTP
Description :
Le serveur Web assure la prise en charge des sites Web HTML et la prise en charge facultative d'ASP.NET, d'ASP et des extensions de serveur Web. Vous pouvez utiliser le serveur Web pour héberger un site Web interne ou externe ou pour fournir un environnement permettant aux développeurs de créer des applications Web.
En savoir plus sur les services de rôle
< Précédent
Suivant >
Installer
Annuler

- ***W2012*** **:** En plus les fonctionnalités « *.Net Framework 4.5* », « *ASP.NET 3.5* » et « *ASP.NET 4.5* » doivent être cochées



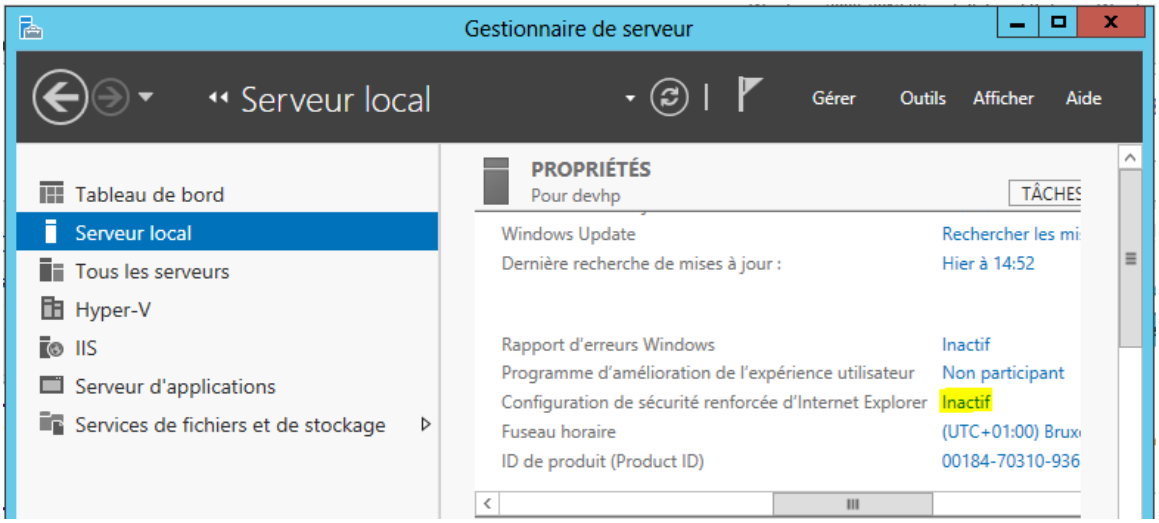


Après avoir sélectionné les différents rôles, cliquez sur « Suivant », installer et puis fermer la fenêtre lorsque ce sera terminé.
IIS est installé. Un redémarrage sera nécessaire.

11.1.2. Paramétrage serveur : Sécurité renforcée d'Internet Explorer et Firewall

Pour terminer cette installation :

- Désactiver la « sécurité renforcée d'Internet Explorer » via le Gestionnaire du serveur. Par exemple sur un serveur W2012 :



- Désactiver si possible le Firewall ou gérer les connexions au serveur conformément aux pré-requis.