Remote Worker via MBG

04/2023
AMT/PTD/PBX/0161/3/3/FR
MANUEL DE MISE EN ŒUVRE

Avertissement

Bien que les informations contenues dans ce document soient considérées comme pertinentes, Mitel Networks Corporation (MITEL ®) ne peut en garantir l'exactitude.

Les informations sont susceptibles d'être modifiées sans préavis et ne doivent pas être interprétées de quelque façon que ce soit comme un engagement de Mitel, de ses entreprises affiliées ou de ses filiales.

Mitel, ses entreprises affiliées et ses filiales ne sauraient être tenus responsables des erreurs ou omissions que pourrait comporter ce document. Celui-ci peut être revu ou réédité à tout moment afin d'y apporter des modifications.

Aucune partie de ce document ne peut être reproduite ou transmise sous une forme quelconque ou par n'importe quel moyen - électronique ou mécanique – quel qu'en soit le but, sans l'accord écrit de Mitel Networks Corporation.

SOMMAIRE

1 INTRODUCTION

1.1 DEFINITION

Cluster : Système téléphonique de la famille MITEL MiVoice 5000 composé de systèmes physiques (Mitel 5000 Gateways, Mitel 500, MiVoice 5000 Server ou C2IC) ou virtualisés (MiVoice 5000 Server) reliés à un MiVoice 5000 Server central, appelé Cluster Server.

Cluster Server : Système MiVoice 5000 Server physique ou virtualisé dédié au pilotage global du Cluster. Ce système peut être dupliqué.

1.2 DOCUMENTS DE REFERENCE

Les documents associés sont disponibles sur le site Mitel.com.

1.3 GLOSSAIRE

MBG : MiVoice Border Gateway

RCS : Redirection & Configuration Server

AMC : Applications Management Center Serveur de licence

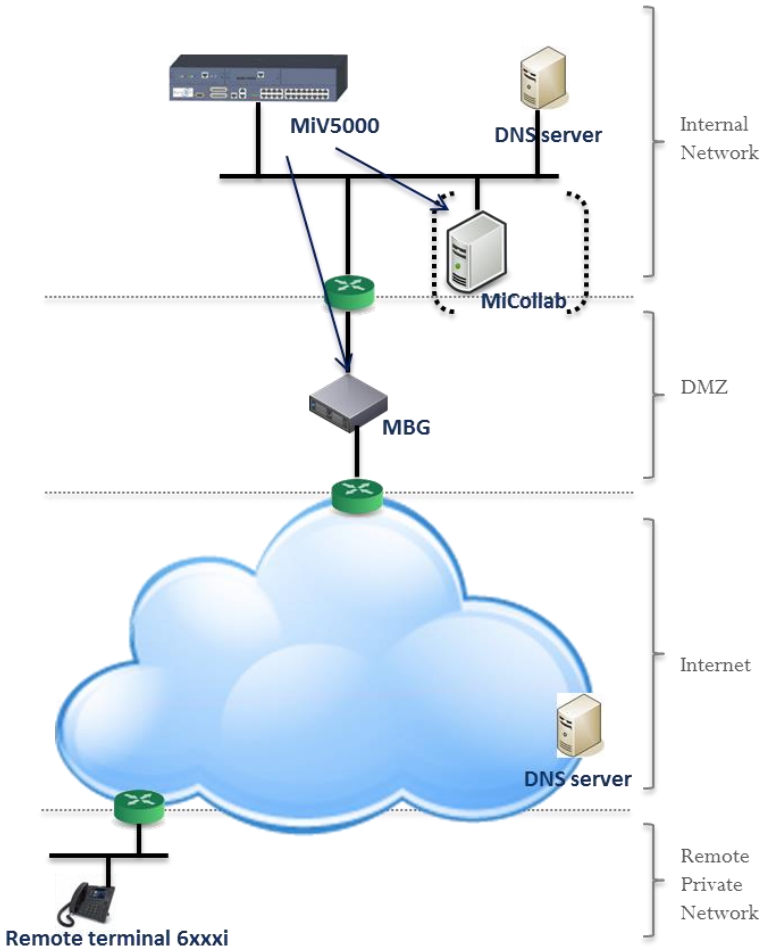
ICP : IP Communication Platform (iPBX)

1.4 RESTRICTIONS

La fonctionnalité Remote Worker décrite dans ce document s'applique uniquement aux terminaux MiVoice 6800 SIP et 6900 IP phones.

2 ARCHITECTURE GENERALE

Exemple d'architecture :



Le but est pour un poste 6800 SIP ou 6900 IP phone installé à distance d'avoir quasiment les mêmes fonctionnalités qu'un poste du même type, installé dans le réseau local de l'entreprise.

La connexion du poste distant relié à Internet est routée ensuite via un MBG au réseau local.

Le MBG permettant d'associer l'adresse publique à l'adresse locale de l'iPBX, le poste récupérant ses fichiers de configuration se comporte comme un poste local au site.

Le MBG peut être selon l'architecture :

- Un équipement externe autonome localisé dans la DMZ,
- Intégré (embarqué) dans le serveur MiCollab,
- En Cluster avec MiCollab dans le réseau local,

Son provisionning est assuré selon l'architecture :

- Soit manuellement (MBG Stand alone)
- Soit par le serveur MiCollab.

Lorsque le MiV5000 provisionne un serveur MiCollab situé dans la DMZ, le firewall doit autoriser notamment l'accès au MiV5000.

La résolution des noms de domaine du MBG est assurée par un serveur DNS public.

Une sécurisation est réalisée à partir d'une clé générée dans l'iPBX et est intégrée au chemin d'accès de l'URL permettant aux postes de télécharger leurs configurations.

En configuration multisite, le MBG ne peut se connecter qu'à un seul iPBX MiVoice5000, tous les postes Remote worker devront être déclarés sur cet iPBX.

3 PRINCIPE DE DEPLOIEMENT

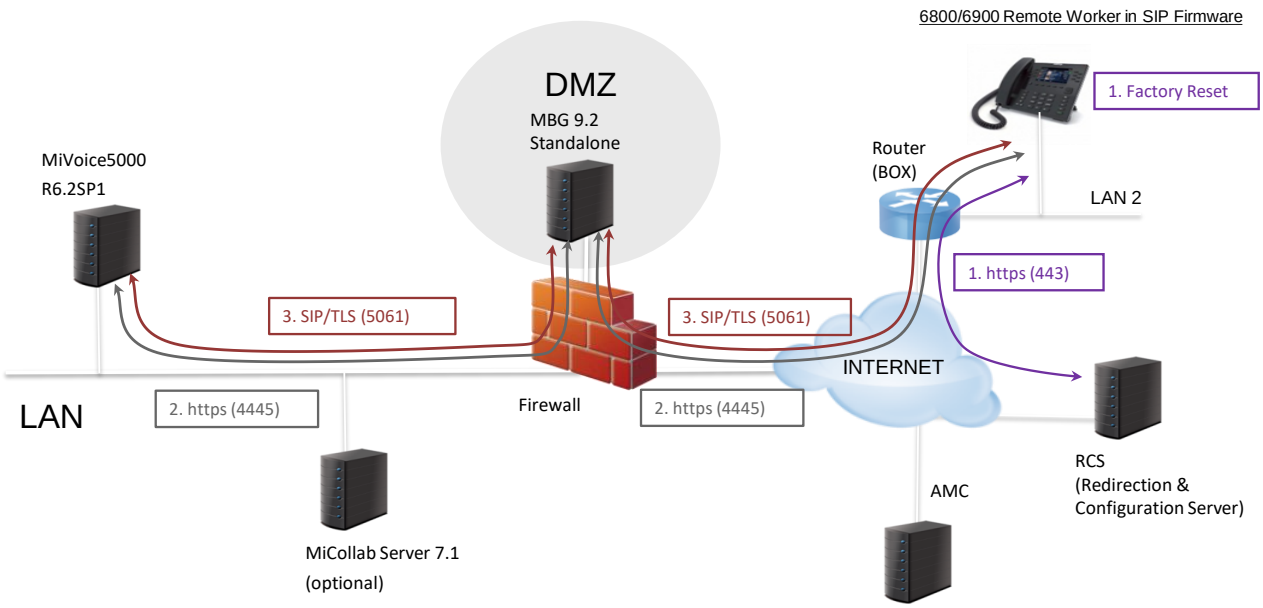
Opérations préalables :

L'URL publique à atteindre est renseignée soit par configuration manuelle au niveau des postes Remote worker soit en utilisant un serveur RCS.

Le poste se connecte, suite à un Factory reset, à l'URL cryptée permettant le déploiement.

Le poste télécharge les fichiers de configuration issus de l'iPBX via le MBG. Fichiers de type aastra.cfg, mac.cfg, software.

Le poste redémarre et envoie son REGISTER.



4 SYNTHESE DES DIFFERENTES ETAPES POUR LE DEPLOIEMENT DES REMOTE WORKERS

La procédure peut être décomposée en trois types d'action :

- Configuration générique à réaliser par l'installateur,
- Préparation au déploiement à réaliser par l'installateur et l'administrateur réseau par poste,
- Déploiement des postes à réaliser par les Remote Workers ou l'administrateur réseau.

L'ordre chronologique suivant est à respecter :

Configuration générique (Chapitre 5)

Configuration du FireWall

Génération de la clé hash sur MiVoice 5000

Déclaration ou non d'un serveur RCS (utilisé pour la configuration des postes distants pour l'accès à l'iPBX de rattachement MiVoice 5000)

Configuration au niveau MBG

- Licence
- Configuration du Profil réseau
- Configuration au point d'accès IP de MiVoice 5000
- Paramétrages SIP commun à tous les postes Remote Worker

Paramétrages complémentaires MBG

Configuration de la connexion/authentification avec un MBG sur MiVoice 5000

Côté Interface MBG :
Côté Web admin MiVoice 5000 :
Configuration du MBG en white list

Configuration de TMA sur MiVoice 5000

- Configuration de l'application
- Définition et configuration des Serveur de téléchargement pour les postes Remote Workers

Préparation au déploiement (Chapitre 6)

Déclaration des equipements SIP (postes 6800 SIP et 6900 IP phones)

Cas d'un MBG Standalone

Cas d'un MBG embarqué ou en mode Cluster avec MiCollab

Configuration spécifique d'un Softphone client MiCollab

Préparation du fichier csv Remote Worker à partir du fichier Provisionning générique

Gestion des postes Remote Worker par TMA

- Prérequis – Préparation du fichier "csv" à partir du fichier provisionning
- Déploiement à partir du serveur de téléchargement :
  - Prérequis
  - Déploiement par TMA embarqué
  - Déploiement par TMA géré à partir MiVoice 5000 manager

Visualisation/Inventaire des postes remote Worker

Déploiement des postes (Chapitre 7)

Configuration du poste distant pour l'accès au serveur de configuration MiVoice 5000

- Utilisation d'un serveur RCS
- sans serveur RCS

Mise en service de poste Remote Worker

Toutes ces étapes sont décrites dans l'ordre et en détail dans les paragraphes suivants.

5 CONFIGURATION GENERIQUE

5.1 CONFIGURATION DU FIREWALL

Pour permettre le trafic entre le LAN/DMZ vers Internet, la configuration suivante doit être la suivante au niveau des ports :

Port Range	Direction	Description
TCP 4445 (HTTPS)	Internet -> DMZ (MBG)	https connection between 68xxi and MBG (download configuration files, XML features)
TCP 4445 (HTTPS)	DMZ (MBG) -> LAN	https connection between MBG and MiV5000 (download configuration files, XML features)
TCP 5061 (SIP/TLS)	Internet -> DMZ (MBG)	SIP connection between 68xxi and MBG
TCP 5061 (SIP/TLS)	DMZ (MBG) -> LAN	SIP connection between MBG and MiV5000
UDP 20000 to 31000	Internet -> DMZ (MBG) DMZ (MBG) -> LAN	Range of SRTP ports configured in MBG settings

Configuration des ports de l'accès distant (Box)

Les ports doivent être ouverts au niveau du routeur (Box) distants.

En général, aucune configuration n'est à faire car les flux sortants sont naturellement autorisés par les Box.

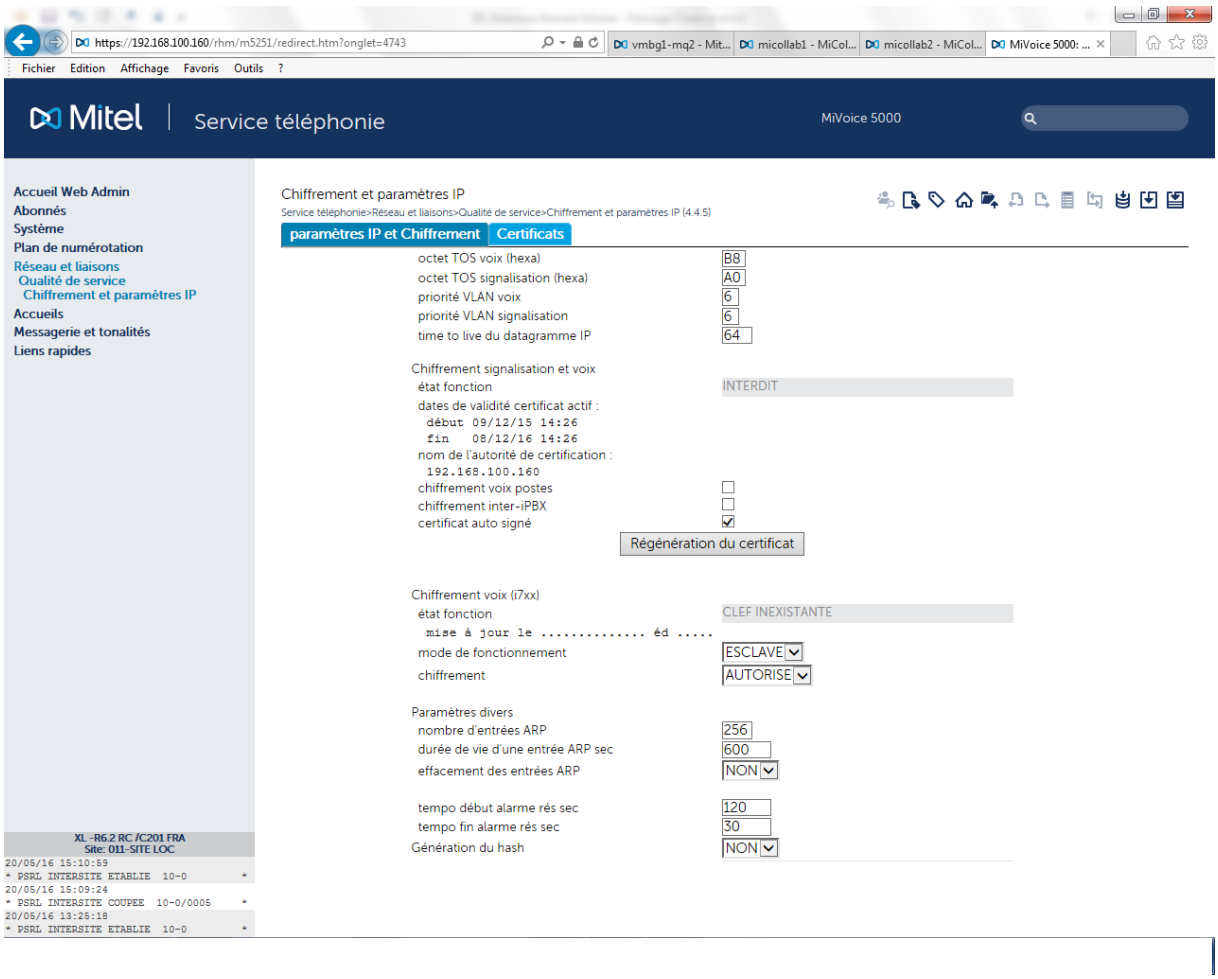
Port Range	Direction	Description
TCP 4445 (HTTPS)	Lan (BOX) -> Internet	https connection between 68xxi and MBG (download configuration files, XML features)
TCP 5061 (SIP/TLS)	Lan (BOX) -> Internet	SIP connection between 68xxi and MBG
UDP 40000 to 51000	Lan (BOX) -> Internet	Range of SRTP ports configured in 68xxi settings

5.2 GENERATION DE LA CLE HASH

La clé hash doit être générée par le MiVoice 5000. Elle est ensuite intégrée dans le chemin de la configuration URL.

Cette clé est unique et est contrôlée par le PBX pour permettre au terminal de télécharger les fichiers.

Menu **RESEAU ET LIAISONS>Qualité de service>Chiffrement et paramètres IP**



- Dans le champ **Génération du hash**, sélectionner **OUI**

IMPORTANT : Un message d'avertissement « régénérer le hash va impacter tous les postes Remote worker déployés » est visualisé si l'exploitant demande une régénération du hash.

- Entrer ensuite le mot de passe du compte Webadmin en cours,
- Cliquer sur **Confirmation**,

Le champ **Chemin pour le téléchargement des fichiers** : est renseigné en lecture seule.

Le but étant que l'administrateur puisse le copier/coller ensuite dans l'URL d'accès aux fichiers de configuration poste.

5.3 CONFIGURATION DU POSTE DISTANT POUR L'ACCES A L'IPBX DE RATTACHEMENT MIVOICE 5000

Comme le poste est déporté, il n'est pas possible de fournir automatiquement l'URL du MBG à atteindre.

Deux méthodes sont possibles :

- L'utilisation d'un serveur RCS,
- La configuration de l'URL directement sur le poste à partir de l'interface Web du poste.

Les postes 6900, livrés en sortie usine avec un firmware Minet, doivent être migrés en firmware SIP. Le téléchargement du firmware SIP peut être fait soit au préalable par l'installateur, soit directement via le serveur RCS (pour tous les postes de l'installation, ou unitairement par fichier Mac).

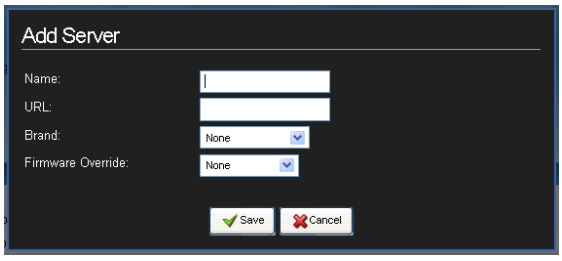
5.3.1 UTILISATION D'UN SERVEUR RCS

Le serveur RCS permet un déploiement simplifié des postes 6800 SIP et 6900 IP phones mais nécessite l'ouverture d'un compte pour y accéder.

5.3.1.1 Ouverture d'un compte d'accès au RCS

Note : Se référer au document relatif à l'ouverture d'un compte RCS.

Ecran de login au serveur RCS.



5.3.1.2 Configuration de l'accès au serveur de configuration MiVoice 5000 avec serveur RCS

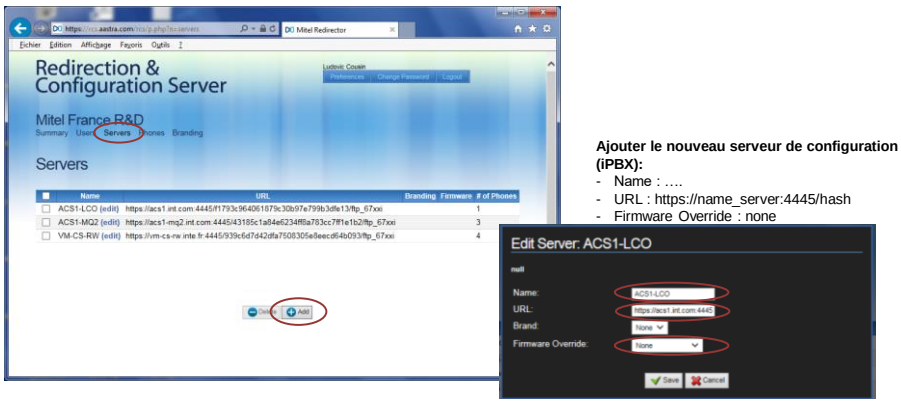
Le service de redirection et configuration (RCS) est un service qui facilite le déploiement des postes 6800 SIP et 6900 IP phones (Se référer à la documentation RCS pour plus de précisions).

URL d'accès au serveur RCS : **https://rcs.aastra.com/rcs/login.php**

A partir de l'écran d'accueil du RCS

- Dans le menu **Servers**, indiquer les informations pour atteindre le MBG :
  - **Name** : Le nom ou l'adresse de l'adresse publique du MBG,
  - **URL (Chemin HTTPS)** : Le chemin d'accès intégrant :
    - L'hôte représenté soit par le FQDN soit par l'adresse IP publique du MBG et le port associé (4445).
    - la clé hash de l'URL permettant aux postes de télécharger leur fichier de configuration. Voir valeur paragraphe 5.2,

    Exemple : https://name_server:4445/hash
- Cliquer sur **Save**.



Ajouter le nouveau serveur de configuration (iPBX):
- Name : ….
- URL : https://name_server:4445/hash
- Firmware Override : none

Firmware override :

- Si l'installation a beaucoup de postes 6900, il est intéressant de migrer automatiquement les postes 6900 de la version Minet en SIP. Cette mise à jour vaudra aussi tant pour les postes 6800 et 6900.

- Prendre un firmware SIP, avec une version minimale 5.0.0.

Il y aura autant d'URL différentes qu'il y a de MiVoice 5000 Server sur lesquelles les Remote workers sont déclarés.

IMPORTANT : Un MBG ne peut être associé qu'à un seul iPBX MiVoice 5000 pour la fonctionnalité Remote Worker.

5.3.2 CONFIGURATION DE L'URL DIRECTEMENT SUR LE POSTE

Se référer au paragraphe 7.1.2.

5.4 CONFIGURATION DU MBG

Accès à l'interface MBG

https://mbg_address/server-manager

La configuration au niveau du MBG comporte plusieurs phases :

- Déclaration des licences MBG
- Configuration du profil réseau

  Menu **MiVoice Border Gateway,** onglet **System configuration>Network profiles**
- Redémarrage MBG

  Menu **MiVoice Border Gateway**, onglet **System Status**
- Configuration du point d'accès IP au MIVOICE 5000

  Menu **MiVoice Border Gateway,** onglet **Service Configuration>ICPs**
- Paramétrages SIP communs à tous les postes Remote Worker du MBG

  Menu **MiVoice Border Gateway,** onglet **System configuration>Settings**
- Paramétrages complémentaires spécifiques Remote Worker

  Menu **Configurations** Onglet **Overrides**.
- Configuration de la connexion/authentification entre le MBG et l'iPBX.

La plupart des configurations sont identiques quelle que soit l'architecture MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster.

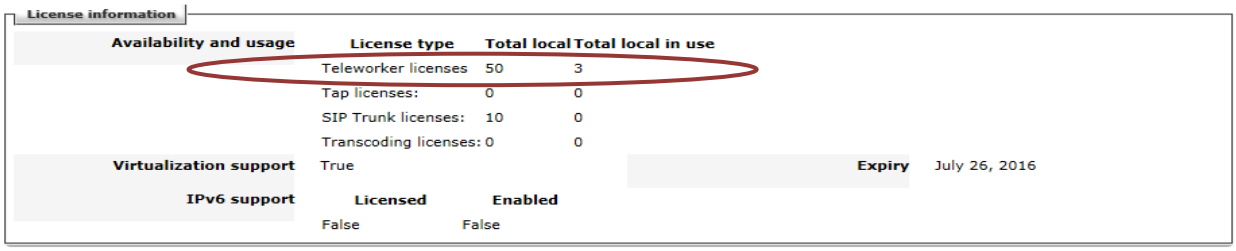
D'autres ne le sont pas et dans ces cas, l'architecture sera reprécisée en début de paragraphe.

Ce chapitre ne décrit la configuration à effectuer côté MBG que pour la fonctionnalité RemoteWorker. Se référer à la documentation du MBG pour plus de précisions sur son utilisation et son administration.

5.4.1 LICENCES

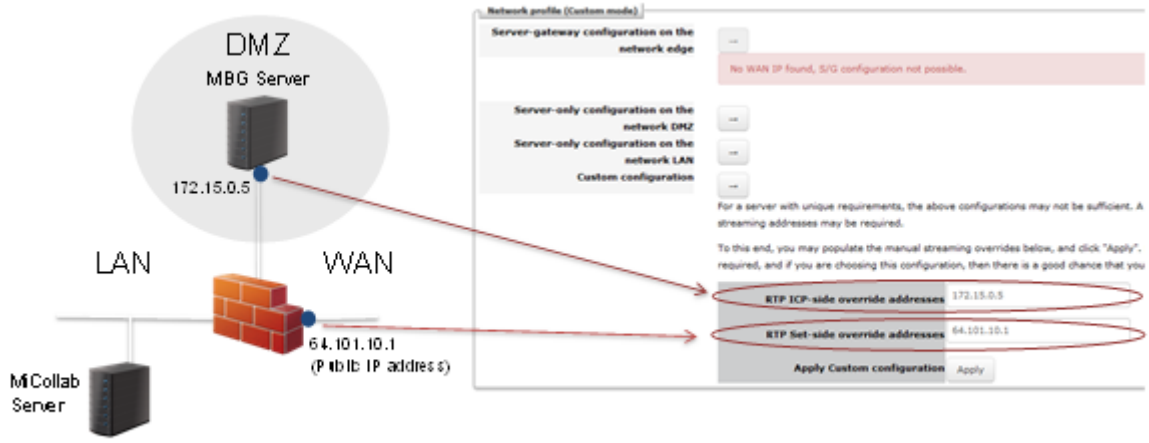
Les licences **Teleworkers** sont nécessaires pour le MBG.

Menu Menu **MiVoice Border Gateway,** onglet **System>Dashboard**



5.4.2 CONFIGURATION DU PROFIL RÉSEAU

Menu **MiVoice Border Gateway**, onglet **Network>Profiles**



- Entrer les valeurs **RTP ICP-side override addresses** :

  TBC : Adresse du serveur MBG
- Entrer les valeurs **RTP Set-side override addresses** :

  TBC : Adresse Publique
- Cliquer sur **Apply** pour la prise en compte des paramètres.

ICP => **I**P **C**ommunication **P**latform = MiVoice5000

Redémarrer ensuite le service MBG. Se référer au paragraphe suivant.

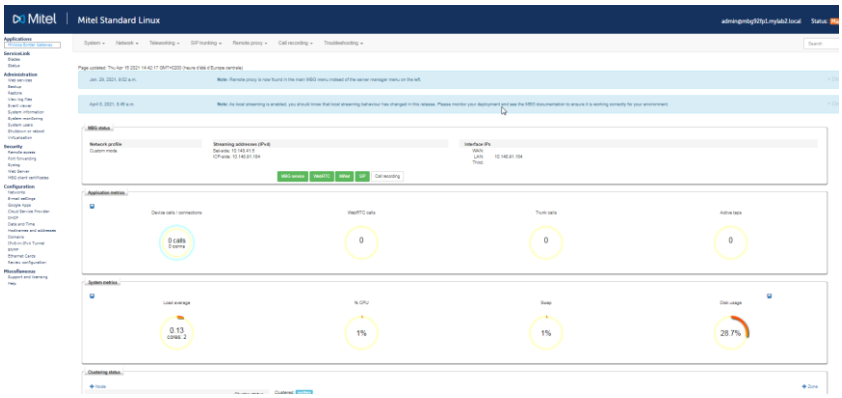
5.4.3 REDÉMARRAGE DU MBG

✓ **Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster**

A partir du menu **MiVoice Border Gateway**, onglet **System>Dashboard** :

Dans la zone **MBG Status** :

- Cliquer sur **MBG service**
- Cliquer sur **Stop**
- Cliquer sur **Start** ensuite pour le redémarrage.



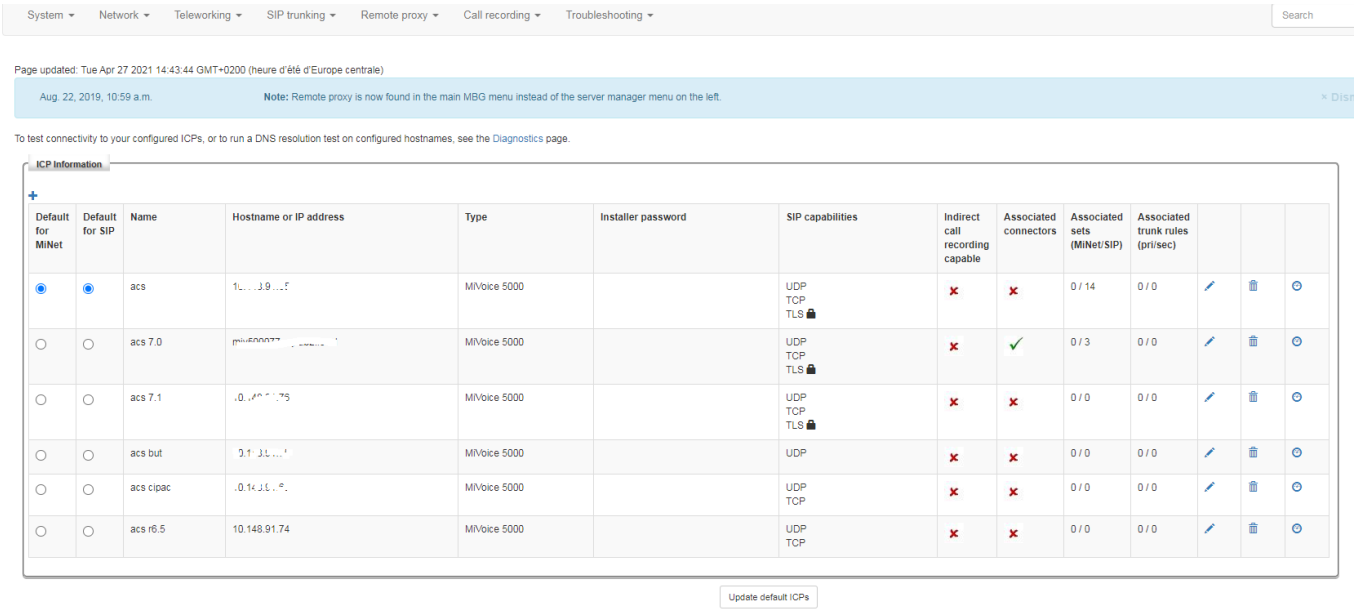
5.4.4 CONFIGURATION AU POINT D'ACCÈS IP DE MIVOICE 5000

✓ **Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster**

Menu **MiVoice Border Gateway,** onglet **Network>ICPs**

Dans la liste proposée, Sélectionner l'iPBX considéré,

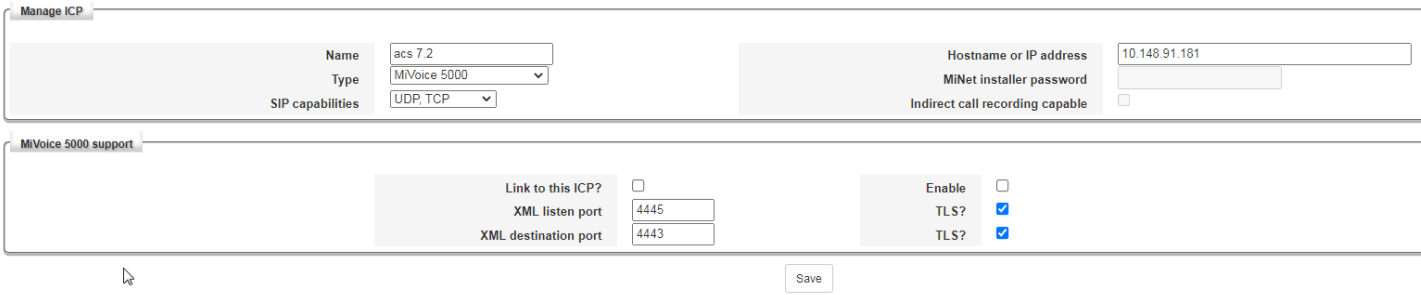
- Cliquer sur l'icône Crayon (Modification)



Renseigner les champs suivants :

Zone **Manage ICP**

Name : Nom de l'iPBX



Zone **Manage ICP**

Hostname or IP address : Adresse IP du MiVoice 5000

Type : MiVoice 5000

SIP capabilities : UDP, TCP, TLS > Connexion SIP entre MBG and MiVoice 5000 en TLS (5061)

Zone **MiVoice 5000 support**

XML listen port : Port public sur lequel le MBG est en écoute (default value 4445).

XML destination port : MiV5000 port (4445 non configurable dans MiVoice 5000).

5.4.5 PARAMÉTRAGES SIP COMMUN À TOUS LES POSTES REMOTE WORKER

✓ **Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster**

Menu **MiVoice Border Gateway,** onglet **System>Settings**

Configurer les champs suivants relatifs aux options de sécurité RTP :

SIP Support :

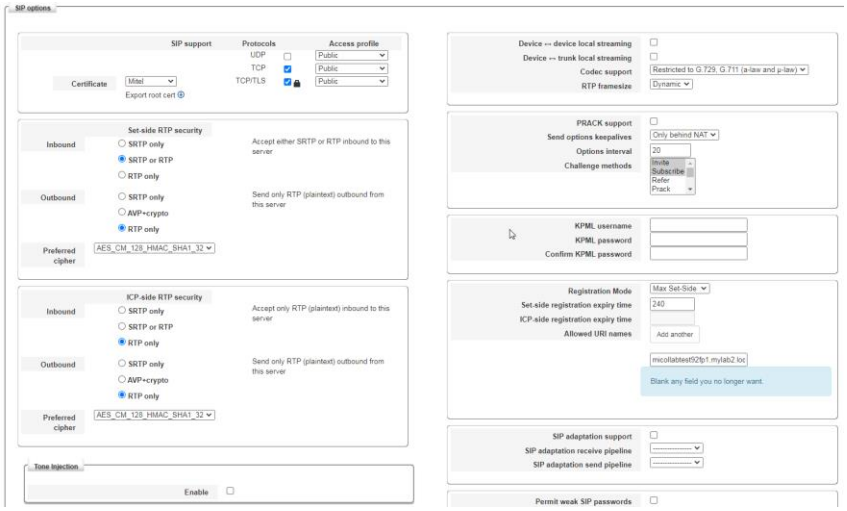
- UDP : Disable
- TCP : Public
- TCP/TLS : Public

- Set-side RTP security inbound : SRTP only
- Set-side RTP security outbound : SRTP only
- ICP-side RTP security Inbound : SRTP or RTP
- ICP-side RTP security Outbound : AVP+crypto

La clé de chiffrement préconisée est :

- AES_CM_128_HMAC_SHA1_80 (default is _32)

Il existe également une option pour le certificat TLS qui doit être Mitel.



5.4.6 CONFIGURATION DE LA CONNEXION/AUTHENTIFICATION ENTRE LE MBG ET L'IPBX

✓ **Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster**

5.4.6.1 Principe

La connexion entre le MBG et le MiVoice 5000 doit être créée pour :

- Obtenir les devices SIP **Set-side username, Set-side password** et **lcp-side username** configurés dans le MBG. Ces paramètres seront utilisés pour le déploiement par TMA.
- Synchroniser le MiVoice 5000 quand un mot de passe **Set-side** a été changé dans la MBG.

Le principe d'authentification avec le MBG se déroule en plusieurs étapes :

- Démarrer le service Web
- Ajouter un nouveau client dans le MBG
- Déclarer un nouvel équipement SIP dans MiVoice 5000

5.4.6.2 Procédure détaillée

Avertissement :

Cette procédure se déroule séquentiellement en utilisant alternativement les menus du MBG et de Webadmin MiVoice 5000.

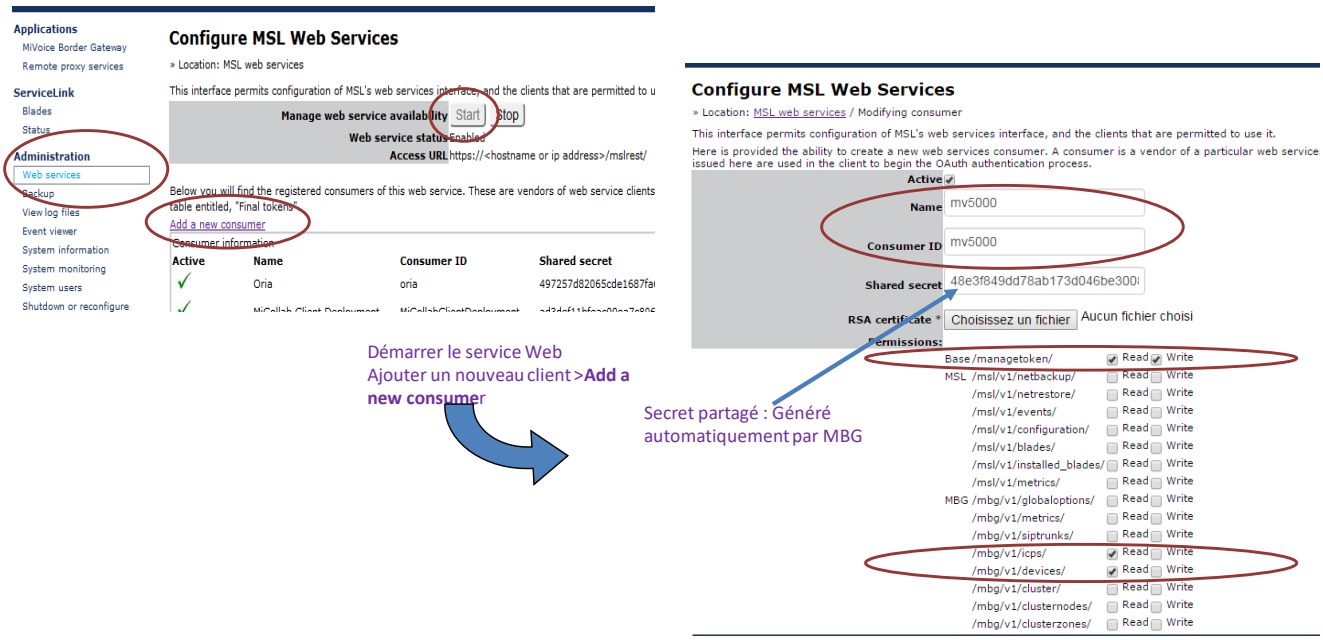
L'ordre des séquences est à respecter impérativement.

Côté Interface MBG :

L'utilisateur doit créer via le menu **Administration>Web services, onglet Add a new consumer** un compte utilisateur que le MiVoice 5000 utilisera pour s'authentifier.

Un compte comporte deux données indispensables à l'étape d'authentification :

- l'Identité du compte (chaîne de 40 caractères maximum) > Champs **Name** et **Consumer ID**
- Son code secret (chaîne de 40 caractères maximum) généré et affiché automatiquement par le MBG. > Champ **Shared secret**.



Côté Web admin MiVoice 5000 :

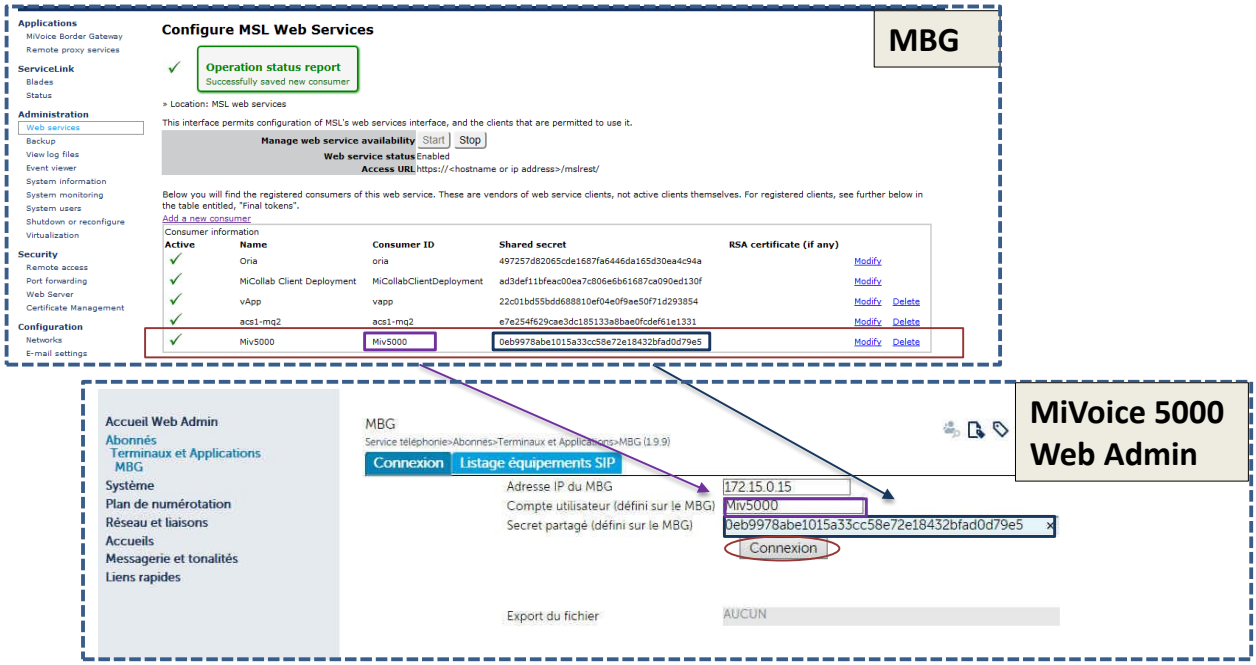
Menu **Abonnés>Terminaux et Applications>MBG**

Saisir les paramètres suivants :

- L'adresse IP du MBG,
- L'ID du compte utilisateur (défini sur le MBG),
- Le code secret partagé associé au compte (défini sur le MBG),
- Appuyer sur Entrée

Le bouton **Connexion** apparait ensuite.

- Cliquer sur ce bouton **Connexion**.



Le MBG et l'iPBX doivent être synchronisés (même heure).

IMPORTANT : Dans le cas d'un iPBX de type MiVoice 5000 Server, l'OS doit être impérativement au minimum en version 6.7 ou la dernière version des patches OS doit avoir été installée.

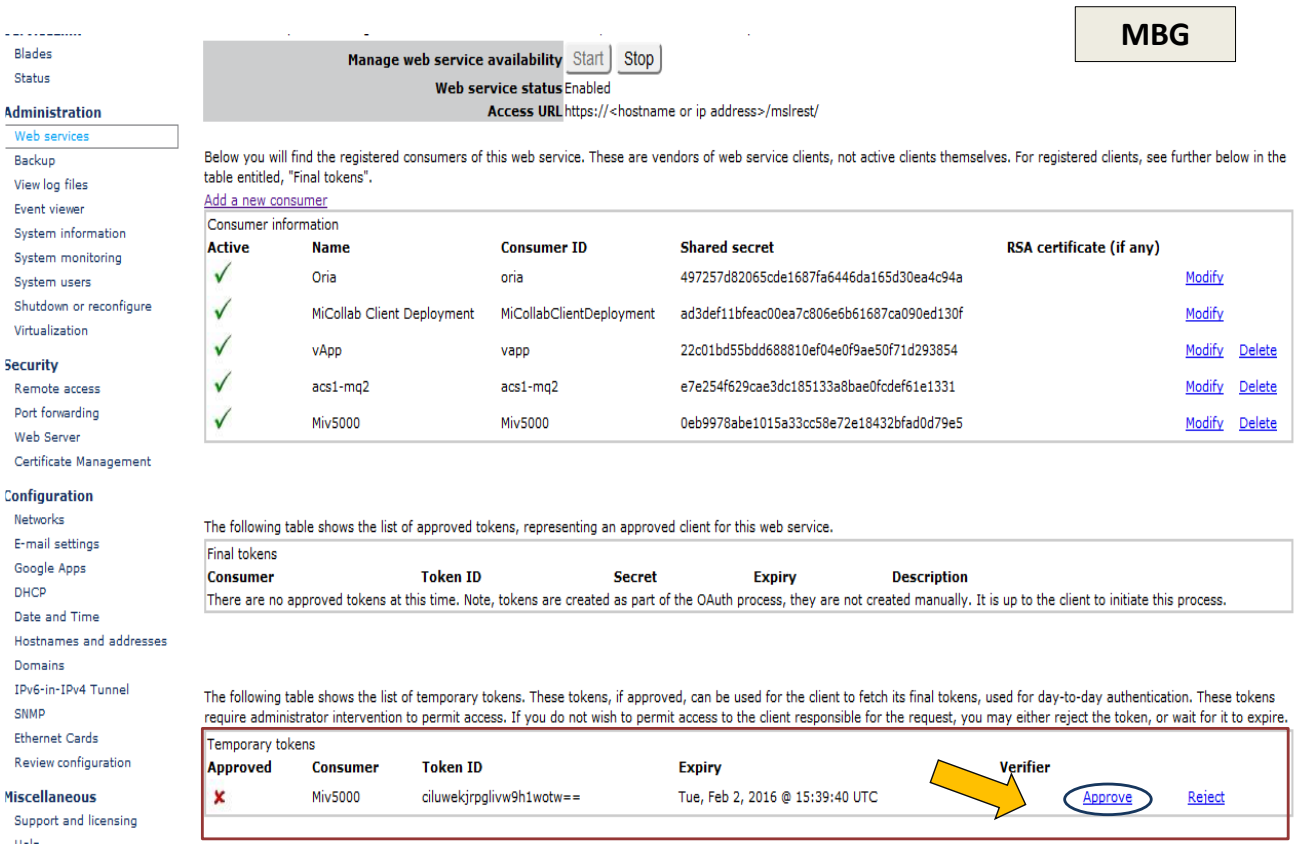
Côté Web admin MiVoice 5000 :

Appuyer sur le bouton **Connexion**. Le menu **Service téléphonie>Abonnés>Terminaux et Applications>MBG** présente alors le champ **Code de vérification**.

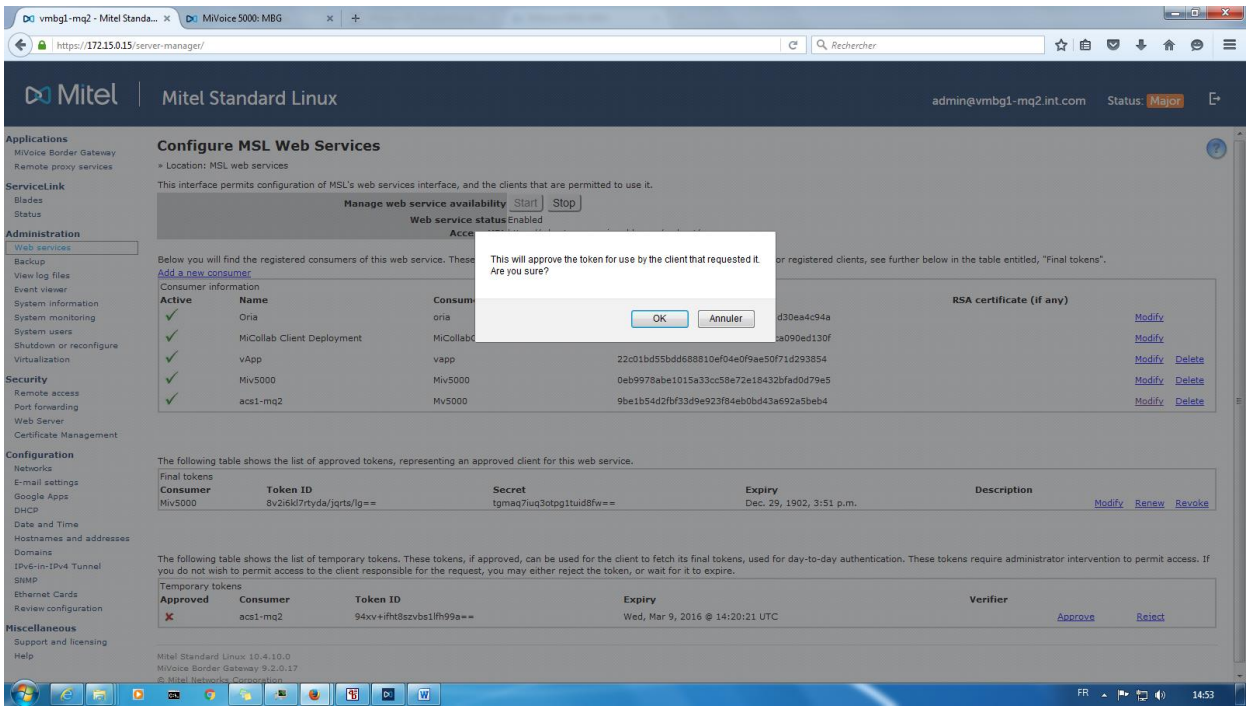
Côté Interface MBG :

Un jeton (token) temporaire d'authentification a été créé par le MiVoice 5000 sur le MBG (avec une durée de validité d'une heure). Il apparaît dans le menu **Administration>Web services> « Temporary token »**.

- L'administrateur doit alors approuver ce jeton temporaire via le lien **Approve** .



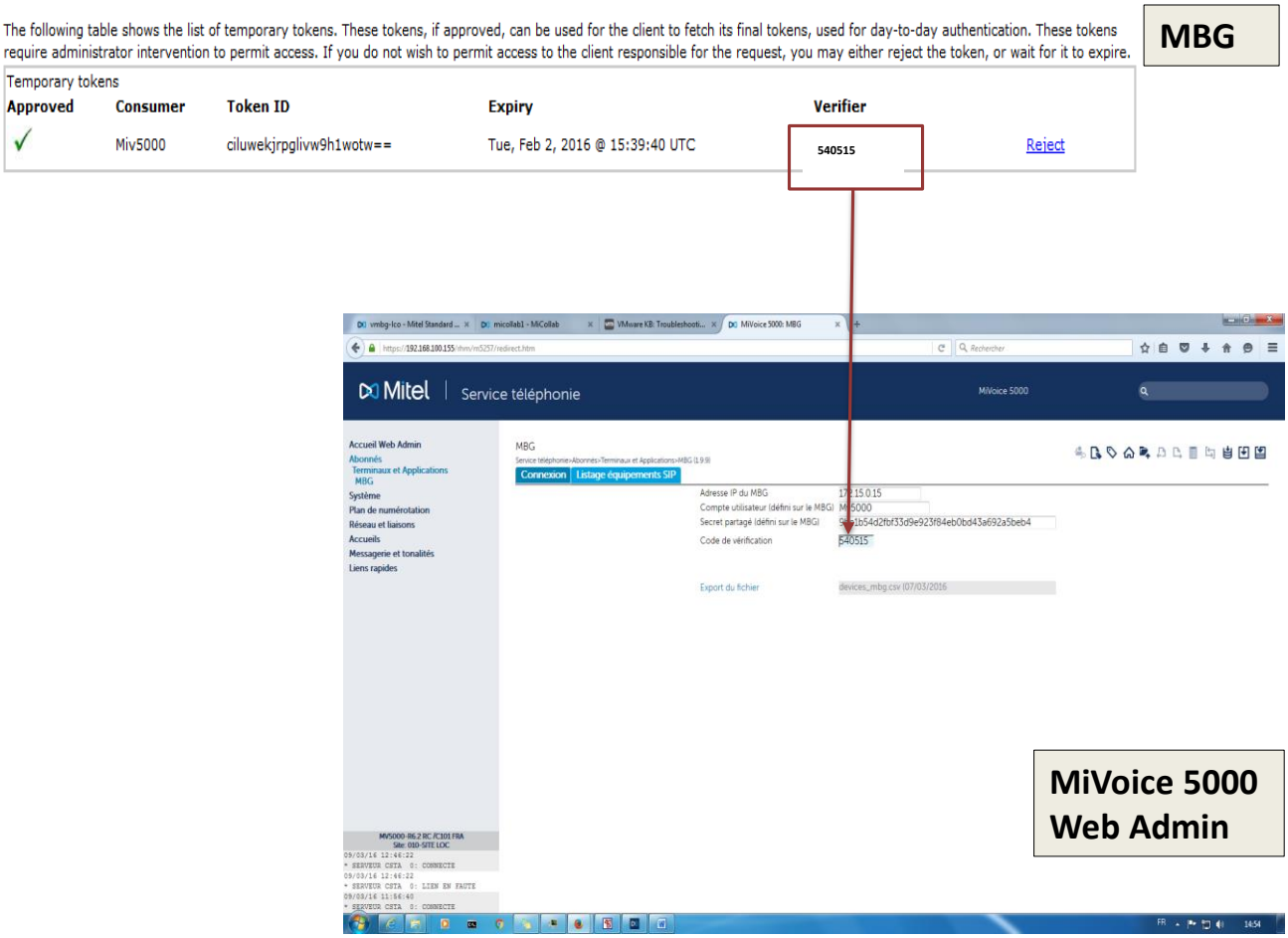
- Cliquer sur **OK**.



Lorsque le jeton temporaire est approuvé, un code **verifier** est généré. Ce code est à entrer dans Webadmin de MiVoice 5000 comme **Code de vérification**.

Côté Interface MBG :

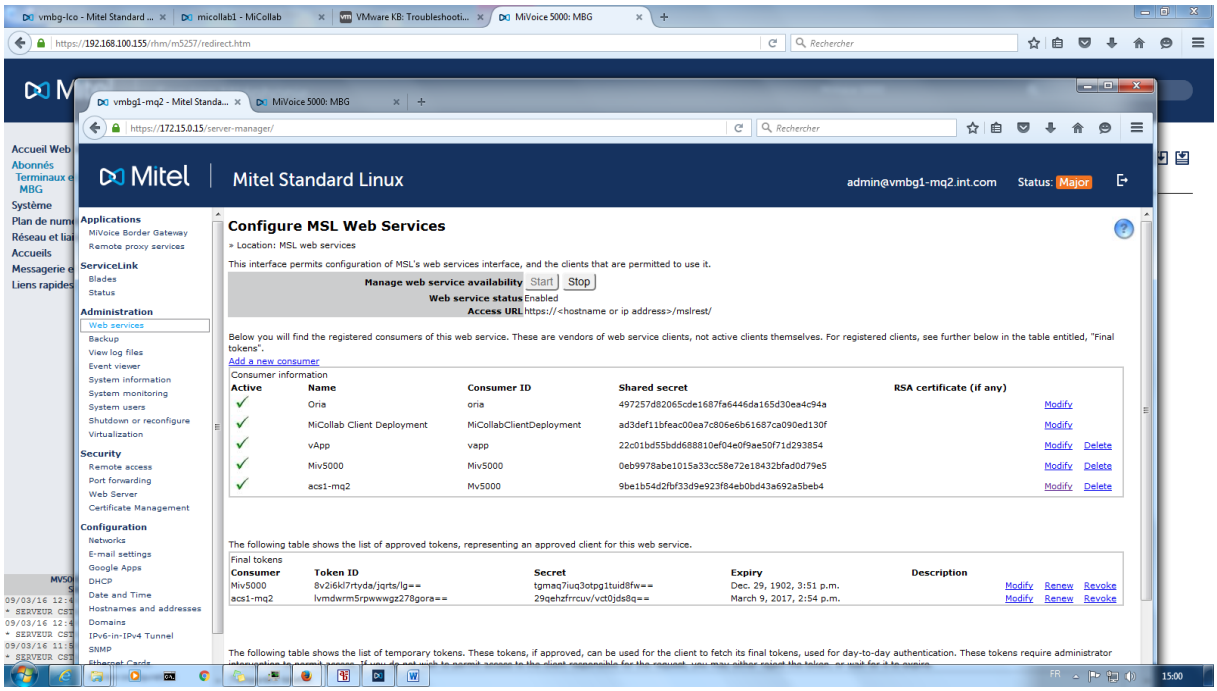
L'exploitant doit copier le code **Verifier** associé à ce jeton temporaire et le coller dans le champ **Code de vérification** dans le menu **Service téléphonie>Abonnés>Terminaux et Applications>MBG**.

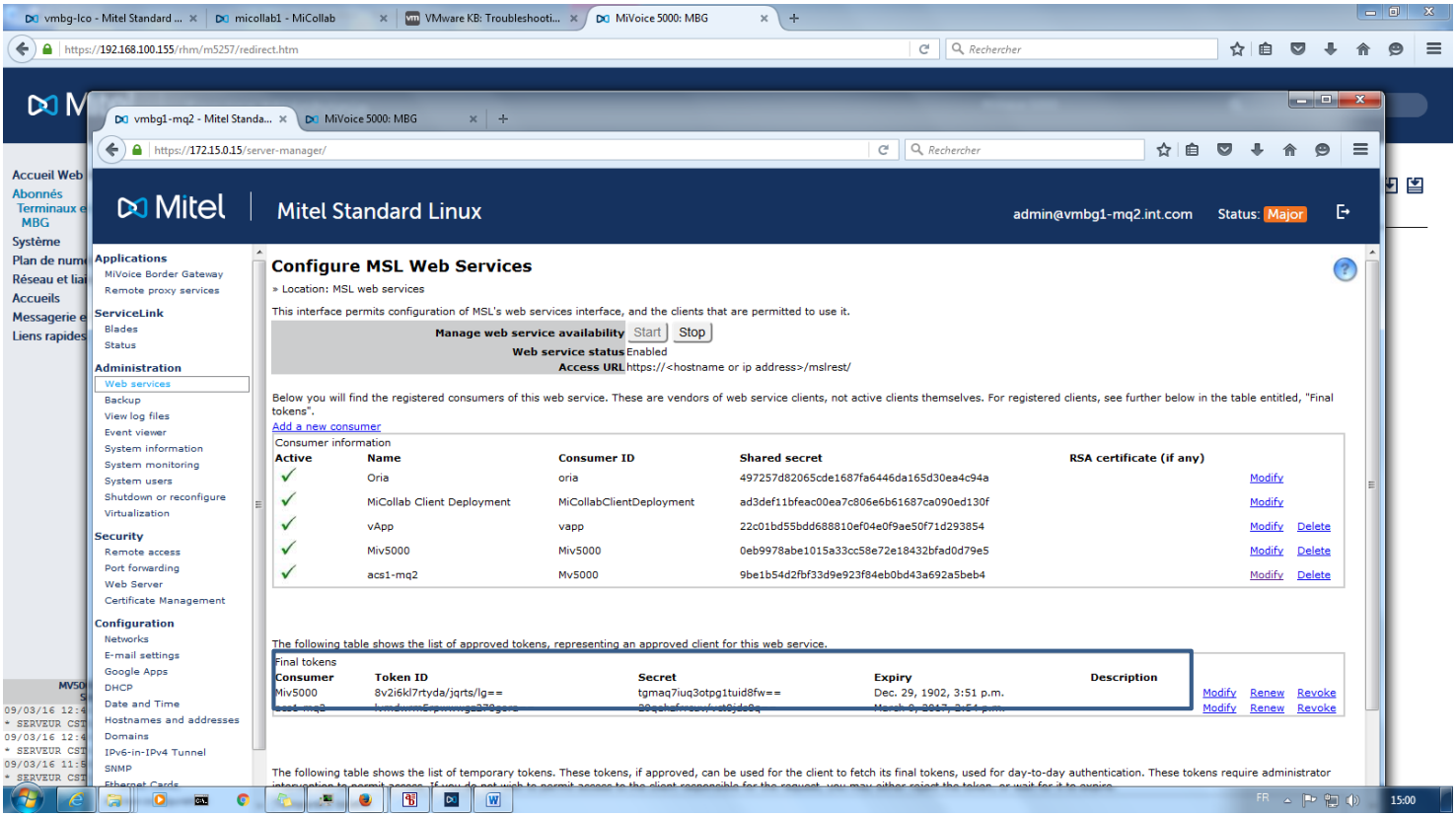


Côté Web admin MiVoice 5000 :

Quand le champ **Code de vérification** est saisi côté MiVoice 5000, le MiVoice 5000 confirme au MBG le token d'authentification.

Le MBG alloue alors au MiVoice 5000 un token final d'authentification (une paire Token ID et le secret associé avec une durée de validité d'un an).




vmbg-lco - Mitel Standard ...
micollab1 - MiCollab
VMware KB: Troubleshooti...
MiVoice 5000: MBG
https://192.168.100.155/rhm/m5257/redirect.htm
vmbg1-mq2 - Mitel Standa...
MiVoice 5000: MBG
https://172.15.0.15/server-manager/
Mitel
Mitel Standard Linux
admin@vmbg1-mq2.int.com
Status: Major
Applications
MiVoice Border Gateway
Remote proxy services
ServiceLink
Blades
Status
Administration
Web services
Backup
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reconfigure
Virtualization
Security
Remote access
Port forwarding
Web Server
Certificate Management
Configuration
Networks
E-mail settings
Google Apps
DHCP
Date and Time
Hostnames and addresses
Domains
IPv6-in-IPv4 Tunnel
SNMP
Configure MSL Web Services
» Location: MSL web services
This interface permits configuration of MSL's web services interface, and the clients that are permitted to use it.
Manage web service availability
Start
Stop
Web service status Enabled
Access URL https://<hostname or ip address>/mslrest/
Below you will find the registered consumers of this web service. These are vendors of web service clients, not active clients themselves. For registered clients, see further below in the table entitled, "Final tokens".
Add a new consumer
Consumer information
Active
Name
Consumer ID
Shared secret
RSA certificate (if any)
Oria
oria
497257d82065cde1687fa6446da165d30ea4c94a
Modify
MiCollab Client Deployment
MiCollabClientDeployment
ad3def11bfeac00ea7c806e6b61687ca090ed130f
Modify
vApp
vapp
22c01bd55bdd688810ef04e0f9ae50f71d293854
Modify
Delete
Miv5000
Miv5000
0eb9978abe1015a33cc58e72e18432bfad0d79e5
Modify
Delete
acs1-mq2
Mv5000
9be1b54d2fbf33d9e923f84eb0bd43a692a5beb4
Modify
Delete
The following table shows the list of approved tokens, representing an approved client for this web service.
Final tokens
Consumer
Token ID
Secret
Expiry
Description
Miv5000
8v2i6kl7rtyda/jqrts/lg==
tgmaq7iuq3otpg1tuid8fw==
Dec. 29, 1902, 3:51 p.m.
Modify
Renew
Revoke
Modify
Renew
Revoke
The following table shows the list of temporary tokens. These tokens, if approved, can be used for the client to fetch its final tokens, used for day-to-day authentication. These tokens require administrator
15:00

Côté Web admin MiVoice 5000 :

Une fois le token final d'authentification obtenu du MBG,

le menu **Service téléphonie>Abonnés>Terminaux et Applications>MBG** présente l'ID du token final et la date de fin de validité de celui-ci.

Lorsque la connexion est établie :

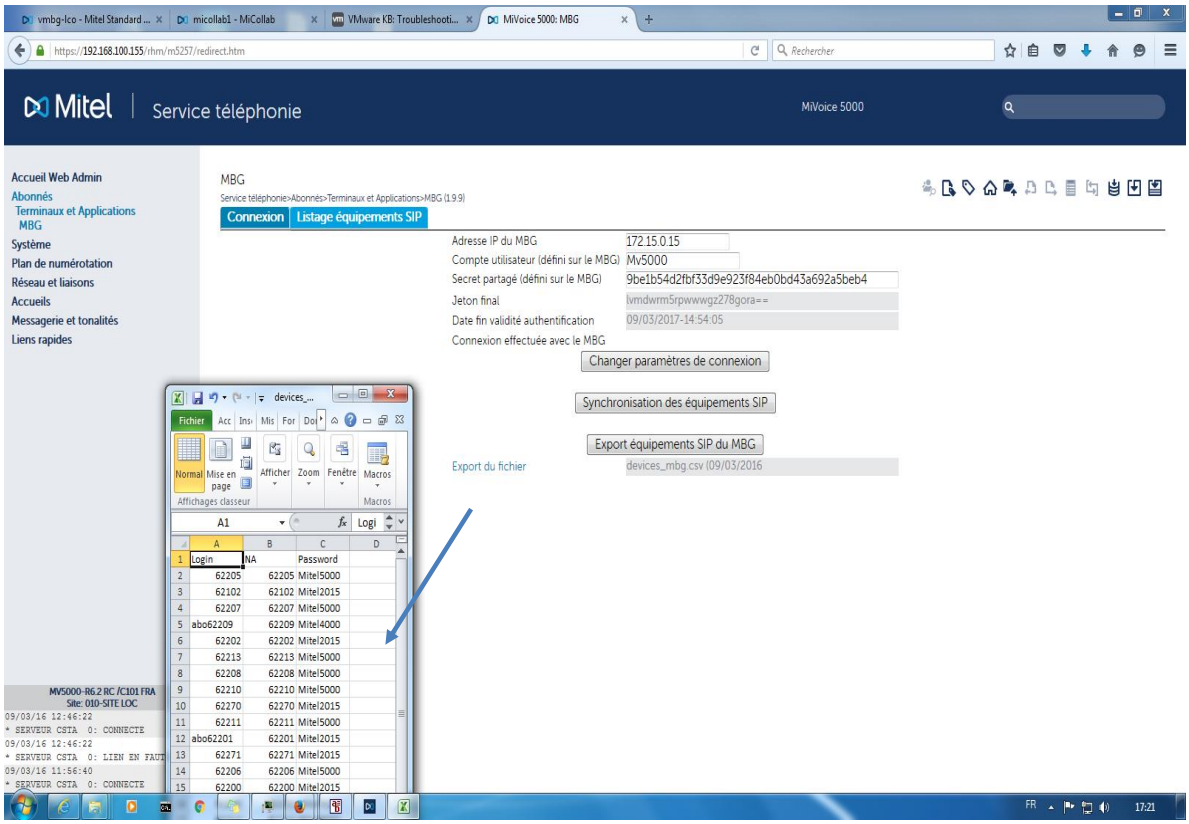
Les actions des différents boutons permettent ensuite les actions suivantes :

- **Changer paramètres de connexion :** Bouton permettant de supprimer tous les paramètres pour permettre de recommencer l'authentification en cas de changement de compte utilisateur, ou un changement de MBG.
- **Synchronisation des équipements SIP :** Bouton permettant l'import des équipements SIP rattachés à l'iPBX local et déclarés dans le MBG.
- **Export équipements SIP du MBG :** bouton provoquant la création du fichier **devices_mbg.csv**.
- **Export du fichier** : Export du fichier **devices_mbg.csv** sur le PC local ; Utile pour les fichiers MAC.

Le fichier **devices_mbg.csv** comporte plusieurs colonnes issues des valeurs définies au niveau du MBG (se référer au paragraphe 6.1) :

- **Login** : **Set-side username** (Valeur du Login du Remote Worker)
- **NA** : **Icp-side username** (Numéro d'abonnement du Remote Worker)
- **Password** : **Set-side password** (Mot de passe MD5 entre le poste et le MBG)

Se référer ensuite au chapitre 6.4 pour l'exploitation de ce fichier.



5.5 CONFIGURATION DU MBG EN WHITE LIST

✓ **Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster**

Comme le MBG concentre le flux de tous les usagers à distance, l'adresse IP du MBG doit être mise dans la White list l'iPBX pour éviter Black listage automatique indésirable du MBG par l'iPBX.

Côté Webadmin de l'iPBX

A partir du menu **Service téléphonie>Réseau et liaisons>Qualité de service>Sécurité SIP**

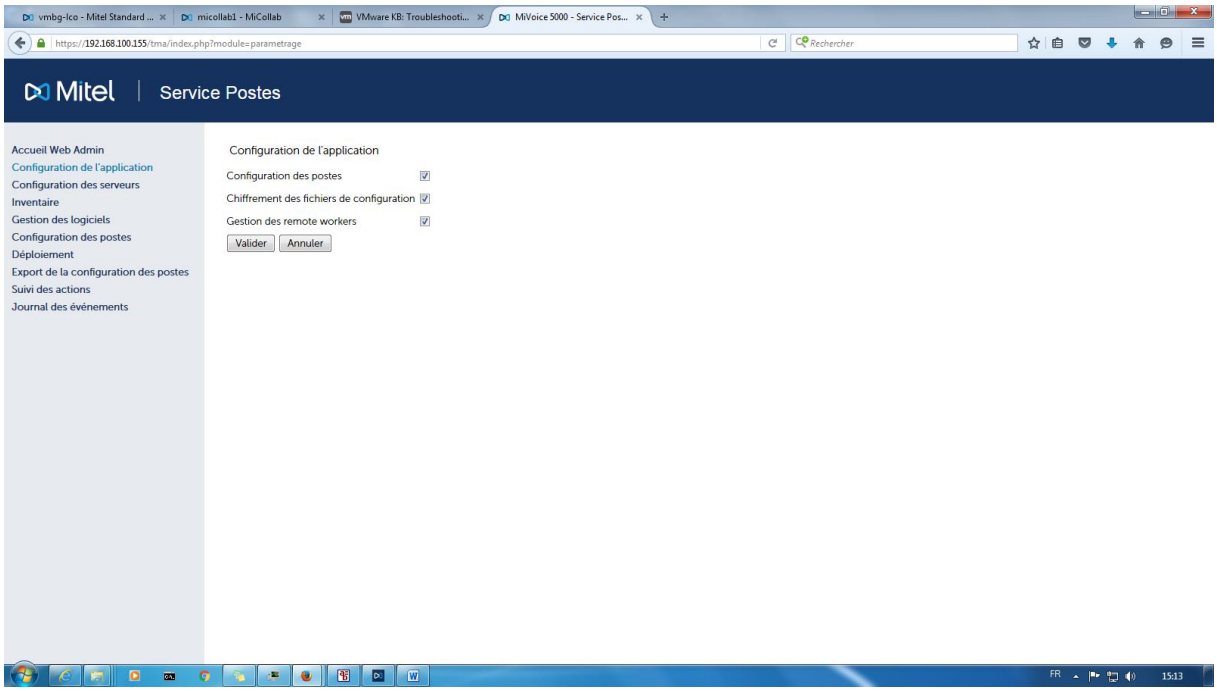
Définir l'adresse du MBG dans la Whitelist.

Se référer au document MiVoice 5000 - Manuel d'exploitation.

5.6 CONFIGURATION DE L'APPLICATION TMA (SERVICE POSTES)

Menu **Configuration de l'application**

- Cocher les cases comme indiqué :



Le chiffrement des fichiers n'est pas impératif mais est fortement recommandé.

Dans le cas de TMA embarqué, le serveur FTP embarqué (= « local ») est défini automatiquement dès que la case **Gestion des remote workers** est activée.

5.7 DEFINITION DES SERVEURS DE TELECHARGEMENT POUR LES REMOTE WORKERS

Le but est de définir les serveurs de téléchargement dédiés aux postes Remote Worker.

Dans le cas de TMA embarqué :

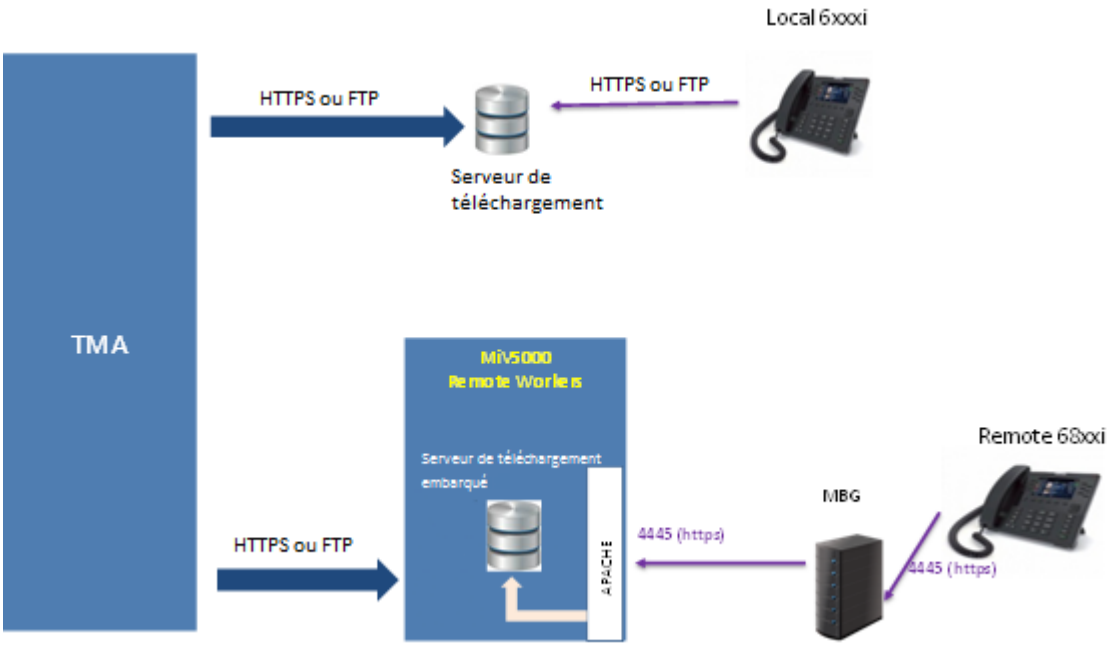
Le serveur local FTP est automatiquement ajouté pour les postes Remote Worker (voir paragraphe précédent).

IMPORTANT : L'iPBX intégrant ce serveur FTP embarqué doit être le même que celui sur lequel sont déclarés les abonnements de type Remote Worker.

Dans le cas de TMA/TMA-EP centralisé dans le MiVoice 5000 Manager :

Définir le ou les serveurs dédiés aux postes Remote Worker.

Note : Si le même serveur doit être utilisé pour les postes locaux et Remote Worker, il doit être déclaré deux fois (une fois pour les postes Remote Worker et une fois pour les postes locaux).



5.7.1 Configuration du serveur de téléchargement pour les Remote Workers

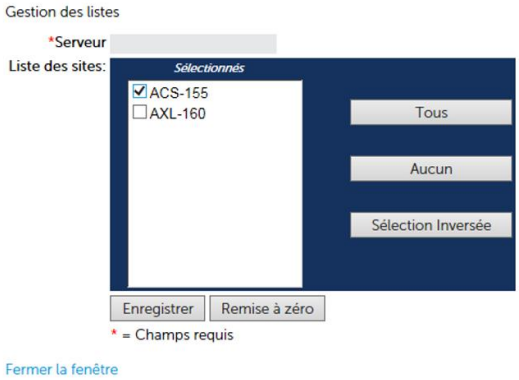
Les informations nécessaires sont les suivantes :

- Nom
- Adresse IP (doit correspondre au PBX sur lequel sont définis les remote workers)
- Port : valeur figée à 21
- Liste du site sur lequel sont déclarés les Remote Workers rattachés au serveur de téléchargement considéré,
- Infos login/mot de passe écriture pour les postes 6xxxi, renseigner par défaut avec les valeurs du serveur FTP embarqué (compte FTP mngt_ftp_67xxi)

Une fois ces informations validées, le serveur apparaitra dans le tableau "Liste des serveurs Remote Workers"

A partir du menu **Configuration des serveurs**

- Cliquer sur **Ajouter un nouveau serveur** dans la zone dédiée aux Remote Worker
- Renseigner tous champs nécessaires comme indiqué précédemment,
- Définir la liste des sites iPBX rattachés à ce serveur pour les Remote Workers (bouton **Modifier la liste des sites** dans l'écran précédent),



- Sélectionner uniquement le site de rattachement des Remote Workers
- Enregistrer et Valider.

Une fois ces informations validées, le serveur de téléchargement apparait dans le tableau **Liste des serveurs**.

- L'action **Modifier le serveur** permet de modifier les paramètres du serveur
- L'action **Supprimer le serveur** permet de supprimer le serveur.

6 PREPARATION AU DEPLOIEMENT

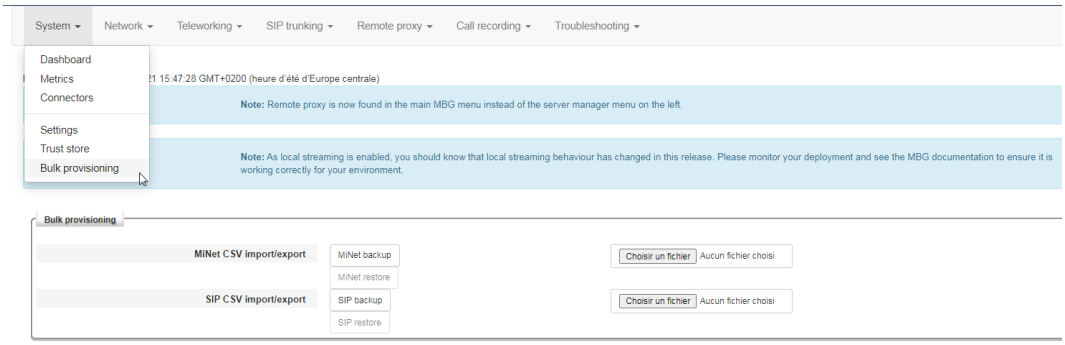
6.1 DECLARATION DES EQUIPEMENTS SIP (POSTES 6800 SIP ET 6900 IP PHONES)

✓ **Non commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster (voir les différents paragraphes suivants).**

6.1.1 CAS D'UN MBG STANDALONE

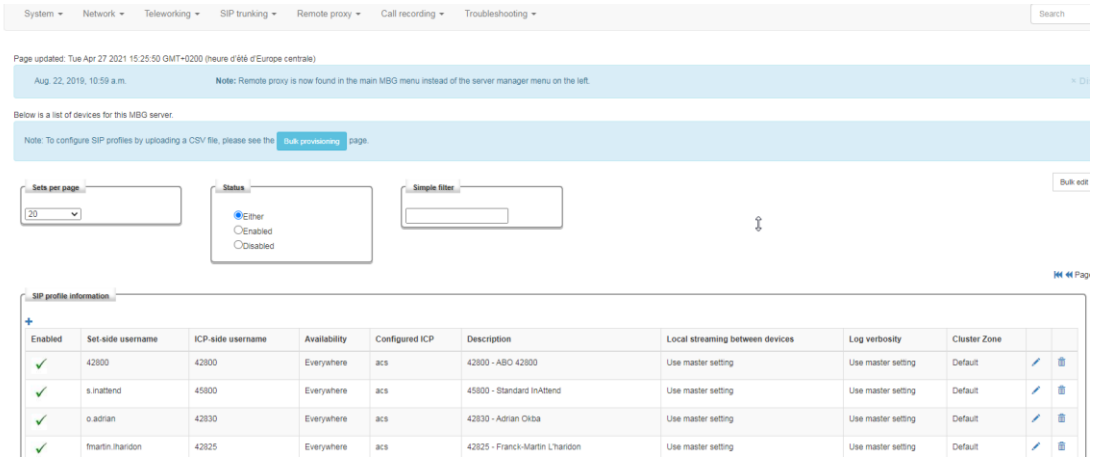
Cette configuration est à effectuer pour chaque poste 68xxi en mode Remote Worker.

Les équipements peuvent également être créés par téléchargement d'un fichier CSV > Menu **System>Bulk provisioning**.



Configuration des postes Remote Worker

Menu **MiVoice Border Gateway**, onglet **Teleworking>SIP**



Dans la zone **SIP profil information**, cliquer sur + en haut à gauche de la zone **SIP profile information**.

Dans la fenêtre suivante, configurer les paramètres comme indiqué ci-après :

Configured ICP:

- **ICP** => **I**P **C**onnection **P**oint = MiVoice5000

  Set-side username:

- Valeur du Login du Remote Worker

  Set-side password:

- Mot de passe MD5 entre le poste et le MBG

  Icp-side username:

- Numéro d'abonnement du Remote Worker

Icp-side password:

- Mot de passe MD5 de l'abonnement MiVoice 5000

Description:

- Nom considéré pour l'équipement utile par exemple pour un listage.

Après avoir renseigné tous les champs, cliquer sur **Save**.

Reprendre la procédure pour les équipements SIP suivants.

6.1.2 CAS D'UN MBG EMBARQUÉ OU EN MODE CLUSTER AVEC MICOLLAB

Les postes 6800 SIP et 6900 IP phone Remote Worker ne fonctionnent qu'en mode SSO.

Lorsque le MBG est en Cluster avec MiCollab, les équipements SIP sont provisionnés par MiCollab server. L'identification suivante est réalisée pour tous les abonnés Remote Worker :

Menu **MiVoice Border Gateway**, onglet **Teleworking>SIP**

Dans la zone **SIP profil information**, cliquer sur +

Configurer les champs suivants comme indiqué :

Set-side username: Login

Set-side password: Généré aléatoirement par le serveur MiCollab.

6.2 CONFIGURATION SPECIFIQUE D'UN SOFTPHONE CLIENT MICOLLAB

✓ **Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster**

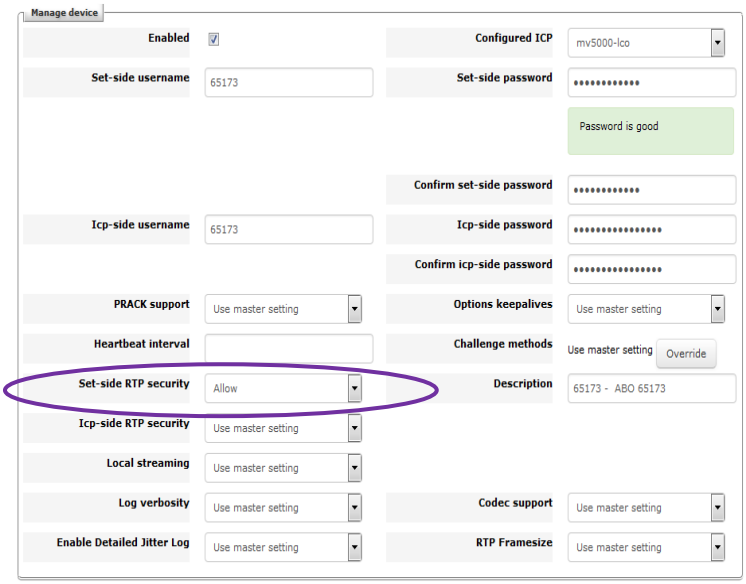
Ce cas ne concerne que des utilisateurs ayant un poste Remote Worker 6800 SIP ou 6900 IP phone et un poste Softphone Micollab en accès distant.

Pour l'abonnement considéré, le poste distant doit être logué avant le poste Softphone Micollab.

Le chiffrement n'étant pas disponible actuellement sur les Softphones Client MiCollab, il est nécessaire d'effectuer la configuration suivante :

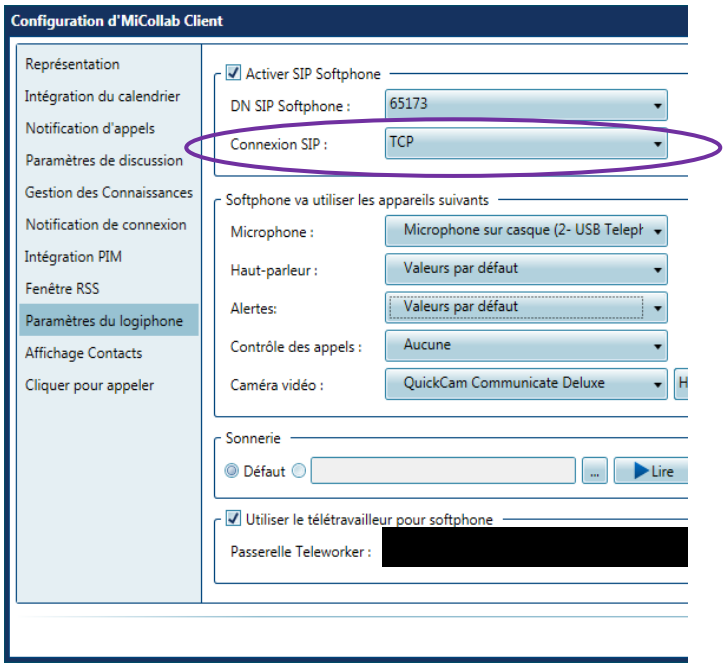
Au niveau du MBG :

Permise mais non imposée



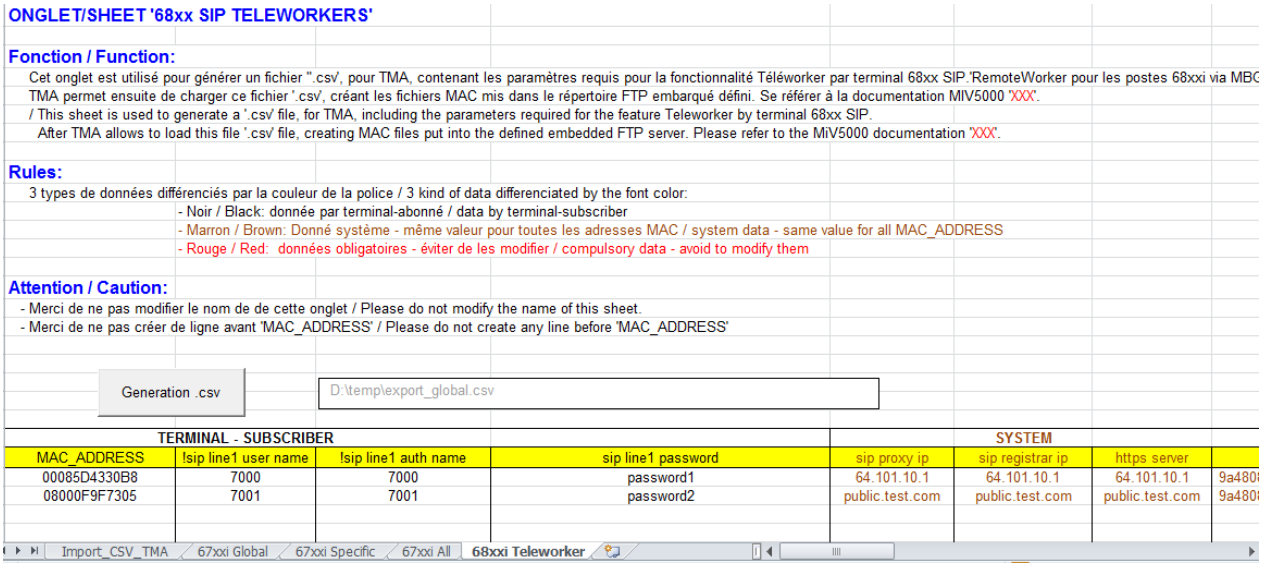
Au niveau du Softphone Client MiCollab :

Non chiffrée impérativement



6.3 PREPARATION DU FICHIER CSV REMOTE WORKER A PARTIR DU FICHIER PROVISIONNING GENERIQUE

Le fichier **TMA_provisionning_6xxxi@version.xls** est disponible sur l'extranet Mitel.



ONGLET/SHEET '68xx SIP TELEWORKERS'

Fonction / Function:

Cet onglet est utilisé pour générer un fichier ".csv', pour TMA, contenant les paramètres requis pour la fonctionnalité Téléworker par terminal 68xx SIP 'RemoteWorker pour les postes 68xxi via MBC
TMA permet ensuite de charger ce fichier '.csv', créant les fichiers MAC mis dans le répertoire FTP embarqué défini. Se référer à la documentation MIV5000 'XXX'.
/ This sheet is used to generate a '.csv' file, for TMA, including the parameters required for the feature Teleworker by terminal 68xx SIP.
After TMA allows to load this file '.csv' file, creating MAC files put into the defined embedded FTP server. Please refer to the MiV5000 documentation 'XXX'.

Rules:

3 types de données différenciés par la couleur de la police / 3 kind of data differenciated by the font color:
- Noir / Black: donnée par terminal-abonné / data by terminal-subscriber
- Marron / Brown: Donné système - même valeur pour toutes les adresses MAC / system data - same value for all MAC_ADDRESS
- Rouge / Red: données obligatoires - éviter de les modifier / compulsory data - avoid to modify them

Attention / Caution:

- Merci de ne pas modifier le nom de de cette onglet / Please do not modify the name of this sheet.
- Merci de ne pas créer de ligne avant 'MAC_ADDRESS' / Please do not create any line before 'MAC_ADDRESS'

Generation .csv | D:\temp\export_global.csv

TERMINAL - SUBSCRIBER				SYSTEM			
MAC_ADDRESS	!sip line1 user name	!sip line1 auth name	sip line1 password	sip proxy ip	sip registrar ip	https server	
00085D4330B8	7000	7000	password1	64.101.10.1	64.101.10.1	64.101.10.1	9a480
08000F9F7305	7001	7001	password2	public.test.com	public.test.com	public.test.com	9a480

Import_CSV_TMA | 67xxi Global | 67xxi Specific | 67xxi All | **68xxi Teleworker**

- Renseigner l'onglet **68xxi Teleworker** en respectant les règles ci-dessous (règles rappelées également dans ce même fichier).
- Générer ensuite le fichier au format CSV (bouton **Generation .CSV**)

Les autres onglets concernent les données Globales et Spécifiques relatives à tous les postes 6xxxi SIP Phones. Se référer au document Manuel d'installation des Postes 6xxxi - AMT/PTD/TR/0043.

Règles pour les Remote Workers (rappelées dans le fichier) :

3 types de données sont à différencier par la couleur de la police :

Noir : Données à renseigner pour chaque poste Remote Worker

Marron : Données système à renseigner commune à toutes les adresses MAC

Rouge : Données obligatoires à éviter de modifier.

Exemple :

Fonction / Function:

Cet onglet est utilisé pour générer un fichier ".csv', pour TMA, contenant les paramètres requis pour la fonctionnalité Téléworker par terminal 68xx SIP.'RemoteWorker pour les postes 68xxi via MBG'
TMA permet ensuite de charger ce fichier '.csv', créant les fichiers MAC mis dans le répertoire FTP embarqué défini. Se référer à la documentation MIV5000 'XXX'.
/ This sheet is used to generate a '.csv' file, for TMA, including the parameters required for the feature Teleworker by terminal 68xx SIP.
After TMA allows to load this file '.csv' file, creating MAC files put into the defined embedded FTP server. Please refer to the MiV5000 documentation 'XXX'.

Rules:

3 types de données différenciés par la couleur de la police / 3 kind of data differenciated by the font color:
- Noir / Black: donnée par terminal-abonné / data by terminal-subscriber
- Marron / Brown: Donné système - même valeur pour toutes les adresses MAC / system data - same value for all MAC_ADDRESS
- Rouge / Red: données obligatoires - éviter de les modifier / compulsory data - avoid to modify them

Attention / Caution:

- Merci de ne pas modifier le nom de de cette onglet / Please do not modify the name of this sheet.
- Merci de ne pas créer de ligne avant 'MAC_ADDRESS' / Please do not create any line before 'MAC_ADDRESS'

Generation .csv

D:\temp\export_global.csv

TERMINAL - SUBSCRIBER				SYSTEM			
MAC_ADDRESS	!sip line1 user name	!sip line1 auth name	sip line1 password	sip proxy ip	sip registrar ip	https server	https path
00085D4330B8	7000	7000	password1	64.101.10.1	64.101.10.1	64.101.10.1	9a48085c1b816fd1b512e8b186686a6
08000F9F7305	7001	7001	password2	public.test.com	public.test.com	public.test.com	9a48085c1b816fd1b512e8b186686a6

Cliquer sur le Bouton
Generation .csv

```
23  ;TERMINAL - SUBSCRIBER;;;;SYSTEM;;;;;COMPULSORY;;;;;;;;;;;;;;;;;;;;;
24  MAC_ADDRESS;!sip line1 user name;!sip line1 auth name;sip line1 passwo
25  00085D4330B8;7000;7000;password1;64.101.10.1;64.101.10.1;64.101.10.1;9
26  08000F9F7305;7001;7001;password2;public.test.com;public.test.com;publi
```

Liste complète :

Données à renseigner pour chaque Remote Worker

- **MAC_ADDRESS :** Adresse MAC des postes 6800 SIP ou 6900 IP phone Remote Worker
- **!sip line1 user name :** Login de l'abonné (issu du MBG fichier devices_mbg.csv)
- **!sip line1 auth name :** Login abonné (issu du MBG fichier devices_mbg.csv)
  - En mode SSO : Login abonné
  - Sans mode SSO : Numéro de l'abonné
- **sip line1 password :** Mot de passe Set-side (issu du MBG fichier devices_mbg.csv)

Données systèmes à renseigner identique à toutes adresses MAC

- sip proxy ip : Adresse publique ou nom du MBG
- sip registrar ip : Adresse publique ou nom du MBG
- **https server : Adresse publique ou nom du MBG**
- **https path : Valeur du hash du MiVoice 5000**
- keyboard script : URL d'accès à l'iPBX pour les postes Remote Worker

6.4 GESTION DES POSTES REMOTE WORKER PAR TMA

6.4.1 PRÉREQUIS

Le fichier CSV est disponible (créé à partir du fichier Provisionning). Se référer au paragraphe 6.3.

6.4.2 DÉPLOIEMENT À PARTIR DU SERVEUR DU TÉLÉCHARGEMENT

6.4.2.1 Principe

L'action consiste à partir du menu **Déploiement** de l'application TMA, d'envoyer sur le serveur de téléchargement dédié aux postes Remote worker les éléments suivants :

- Le certificat CA_Mitel.pem est à déposer (Champ **Autre fichier, template, certificat …)**
- Fichier(s) de données spécifiques mac.cfg généré à partir de l'import d'un fichier csv (Champ **Fichier (csv) remote workers**)

Note : Le menu "Fichier (csv) spécifique" est grisé car inutile pour la gestion des remote workers, ce menu est utile uniquement pour envoyer des fichiers spécifiques sur un serveur de téléchargement pour les postes no Remote Worker.

6.4.2.2 Déploiement par TMA embarqué

Le serveur FTP embarqué doit être actif.

L'action consiste uniquement à générer le fichier remote Worker et à envoyer le certificat:

Pour les autres fichiers, le serveur FTP embarqué contient déjà la bonne version logicielle "postes" et le fichier de données globales associés

A partir du Menu **Déploiement** :

- Sélectionner le serveur "local" dans la liste des serveurs FTP "Remote Workers",
- A partir du champ **Fichier (csv) remote workers**, importer le le fichier "csv" relatif aux Remote Worker issu du fichier provisionning défini au paragraphe 6.3
- A partir du champ **Autre fichier, template, certificat …)**, importer le fichier certificat,
- Cliquer sur **Valider**.

L'action est lancée immédiatement.

Le déroulement de l'action est consultable à partir du menu **Suivi des actions** et **Journal des évènements.**

Lorsque l'action est terminé, le message **Déploiement réalisé** est visualisé.

6.4.2.3 Déploiement par TMA géré à partir MiVoice 5000 manager

A partir du Menu **Déploiement**

- Choisir un serveur dans la liste des serveurs Remote workers,
- Eventuellement choisir une version logicielle dans la liste "Version logicielle",
- Eventuellement importer un fichier de données globales,
- A partir du champ **Fichier (csv) remote workers**, importer le le fichier "csv" relatif aux Remote Workers issu du fichier provisionning défini au paragraphe 6.3.
- A partir du champ **Autre fichier, template, certificat …)**, importer le fichier certificat.
- Cliquer sur **Valider**.

L'action est lancée immédiatement.

Le déroulement de l'action est consultable à partir du menu **Suivi des actions** et **Journal des évènements**.

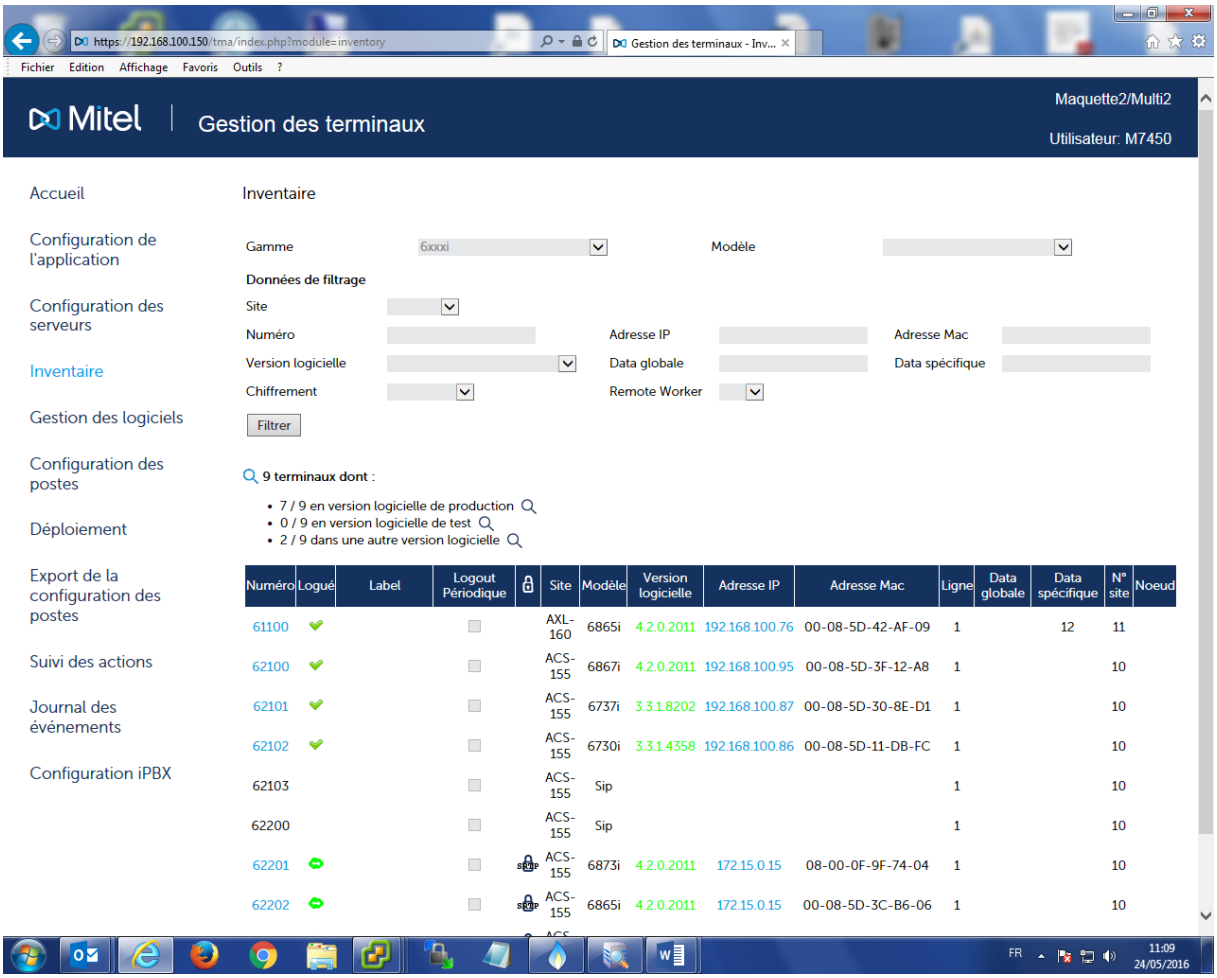
Lorsque l'action est terminée, le message **Déploiement réalisé** est visualisé.

6.5 VISUALISATION/INVENTAIRE DES POSTES REMOTE WORKER

Une fois l'action de déploiement déroulée avec succès, la liste des postes Remote Workers est visualisable à partir du menu principal de l'application TMA, sélectionner le menu **Inventaire**.

Dans le menu **Inventaire**, bouton **Gestion des remote workers**, présentation des listes des postes "remote workers" par site.

Dans le cas TMA Embarqué : Une seule liste "local"



L'icône est relatif aux postes Remote Workers et indique que le poste est déployé et connecté.

Actions possibles : Visualisation ou Suppression

Visualisation : Fenêtre "Gestion des remote workers "

Liste des adresses MAC des postes "remote worker" qui ont été déployés

Un ou plusieurs postes peuvent être supprimés impliquant une suppression du fichier spécifique en local et sur le serveur FTP

Suppression : Suppression de tous les fichiers spécifiques associés aux terminaux décrits dans la liste en local et sur le serveur de téléchargement.

Une fonction **Filtrage** est également disponible.

7 DEPLOIEMENT DES POSTES REMOTE WORKER

✓ **Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster**

L'administrateur récupère l'adresse MAC du poste 6800 SIP ou 6900 IP phone destiné à l'utilisateur distant.

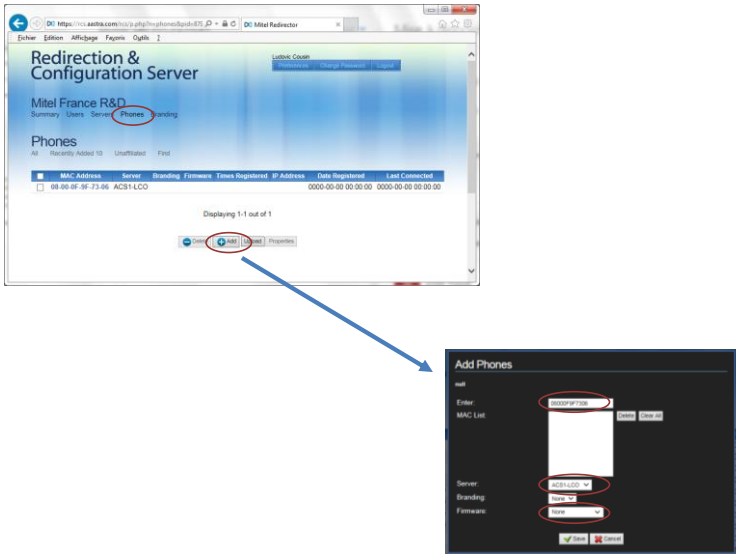
7.1 CONFIGURATION DE L'IPBX DE RATTACHEMENT POUR CHAQUE POSTE REMOTE WORKER

7.1.1 AVEC RCS

URL d'accès au serveur RCS : **https://rcs.aastra.com/rcs/login.php**

A partir de l'écran d'accueil du RCS

- Dans le menu **Phones**, renseigner les différents champs comme suit :
- Les adresses MAC de chaque poste attaché à l'IPBX défini ci-dessous,
- Entrer le nom du serveur de configuration (iPBX),
- Branding : **None**
- Firmware Override :
  - Le poste 6900 peut être migrer du firmware Minet vers le firmware SIP par cet opération
  - Prendre un firmware SIP, avec une version minimale 5.0.0.
- Cliquer sur **Save**.



Le poste distant, suite à un reset usine (en mode SIP) se connectera au serveur RCS et récupérera automatiquement l'adresse du MBG associé à l'iPBX considéré.

7.1.2 SANS SERVEUR RCS

La configuration est à réaliser par l'administrateur ou par l'utilisateur (selon les instructions données par l'administrateur) pour chaque poste en Remote Worker.

Effectuer au préalable un reset factory du poste via le menu **Reinit**.>**Retour à la configuration usine**.

Se connecter à l'interface Web du poste : **https:\\@IP du 6800 SIP ou 6900 IP Phone (en mode SIP)**

Dans le menu **Serveur configuration** :

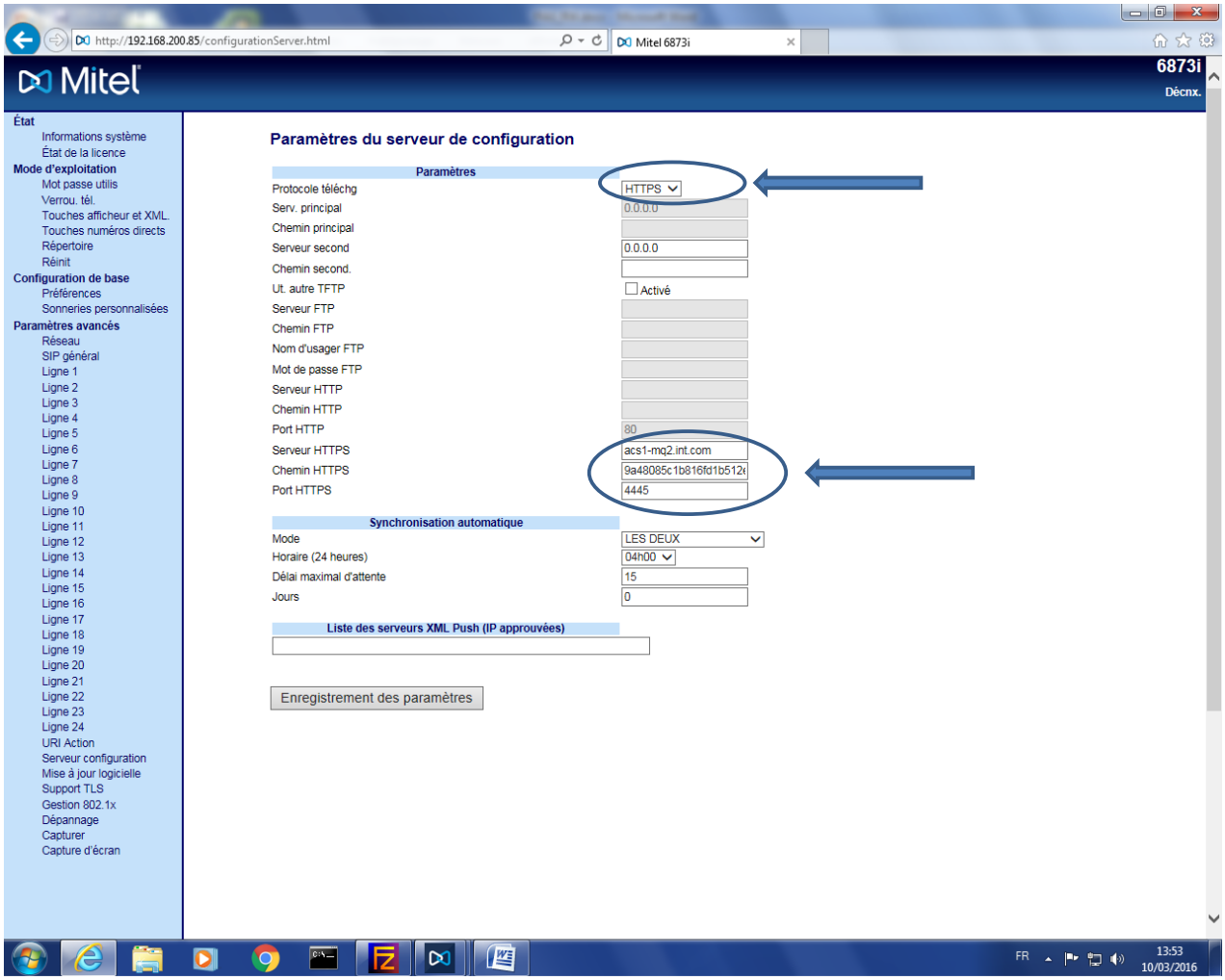
Renseigner les valeurs suivantes :

- **Protocol télécharg** : HTTPS,
- **Serveur HTTPS** : Le nom ou l'adresse de l'adresse publique du MBG,
- **Chemin HTTPS** : Le chemin d'accès intégrant la clé hash de l'URL permettant aux postes de télécharger leur fichier de configuration. Voir valeur paragraphe 5.2,

  Exemple : **https://name_server:4445/3f52a279885152701d8f2f39d9bcfc36/ftp_67xxi**

- **Port HTTPS** : Port correspondant pour la liaison **4445**.

Enregistrer alors les paramètres, puis effectuer un simple démarrage du poste. Il peut être nécessaire de désactiver les options DHCP.



Le poste distant, suite à un redémarrage, standard se connectera ensuite à son iPBX de rattachement via le MBG et récupérera ses fichiers de configuration.

8 CONFIGURATION DES NUMEROS D'URGENCE POUR LES REMOTE WORKERS FIXES

IMPORTANT :

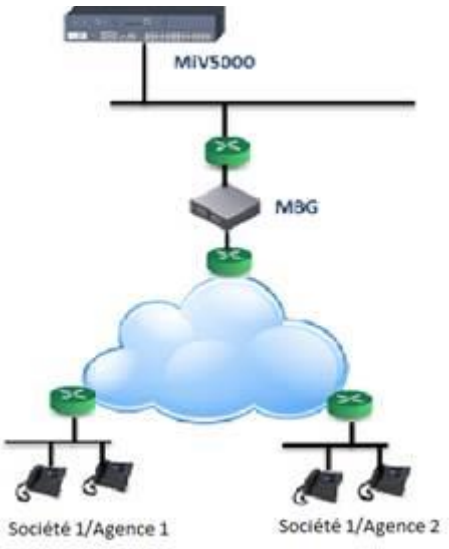
Pour ce paragraphe, se référer parallèlement au document Mitel Gateways et MiVoice 5000 Server – Manuel d'Exploitation pour la configuration du Plan de numérotation, des numéros abrégés et des numéros spéciaux pour les appels d'urgence. Ce document est disponible sur le site Mitel.

8.1 PRINCIPE

Pour un travailleur distant l'appel vers un numéro d'urgence doit être effectué vers le service concerné relatif à sa localisation.

Exemple : Si le 18 est composé par le travailleur distant, l'appel est effectué vers le numéro public des pompiers de la région considérée.

Dans le cas où les télétravailleurs sont situés sur différents sites et raccordés via un MBG, la localisation à base adresse IP n'est pas adaptée car dans ce cas tous les abonnés sont vus avec la même adresse IP.



Pour résoudre ce contrainte les numéros abrégés sont utilisés. Les numéros abrégés peuvent être définis selon la hiérarchie administrative.

Pour chaque hiérarchie les numéros abrégés peuvent être définis avec des numéros publics différents.

Pour appliquer ce mécanisme aux numéros spéciaux, la configuration du numéro spécial doit être modifiée dans le menu des numéros spéciaux.

En exemple, si un utilisateur compose le 119, soit le 00130964718 soit le 00130964719 sera appelé, selon sa hiérarchie (localisation) administrative de l'abonné.

De cette manière, un groupe de personnes appartenant à la même hiérarchie administrative peut appeler le même numéro de service d'urgence en composant simplement le même numéro spécial.

Les étapes principales pour permettre les appels d'urgence vers des numéros publics différents et relativement à la localisation sont les suivantes :

- Le principe est de regrouper les abonnés d'un ou plusieurs sites ayant la même localisation géographique dans la même hiérarchie administrative.
- Créer des hiérarchies administratives différentes par région géographique des agences.
- Affecter une hiérarchie administrative identique pour chaque abonnement d'une même agence (Société1/Agence 1 dans l'exemple)
  Cette hiérarchie administrative doit correspondre à la localisation de l'agence des abonnés.

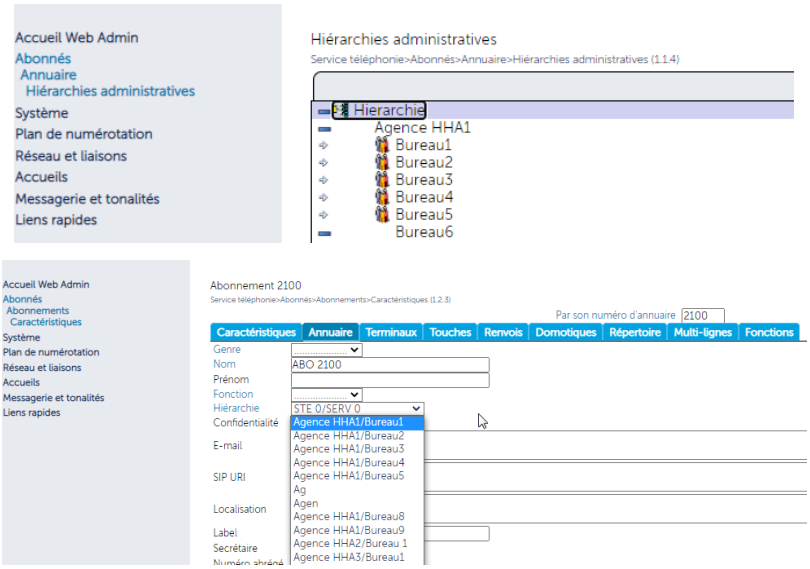
- Définir des numéros abrégés en fonction de la hiérarchie administrative
- Configurer les numéros spéciaux (numéros d'urgence) relatifs au numéro abrégé et les affecter respectivement selon la hiérarchie administrative. Ex :
    - Configurer les numéros spéciaux avec le préfixe de numéro abrégé (Ex: * 3529) combiné avec le numéro précédemment déclaré du service d'urgence à composer (00130964018).
- Déclarer dans l'annuaire des fiches externes le numéro d'appel public des services d'urgence requis de chaque région géographique et leur affecter le même numéro abrégé avec la hiérarchie administrative correspondante à la région concernée.

De cette manière, un groupe de personnes appartenant à la même hiérarchie administrative peut appeler le même numéro de service d'urgence en composant simplement le même numéro spécial.

8.2 CONFIGURATION

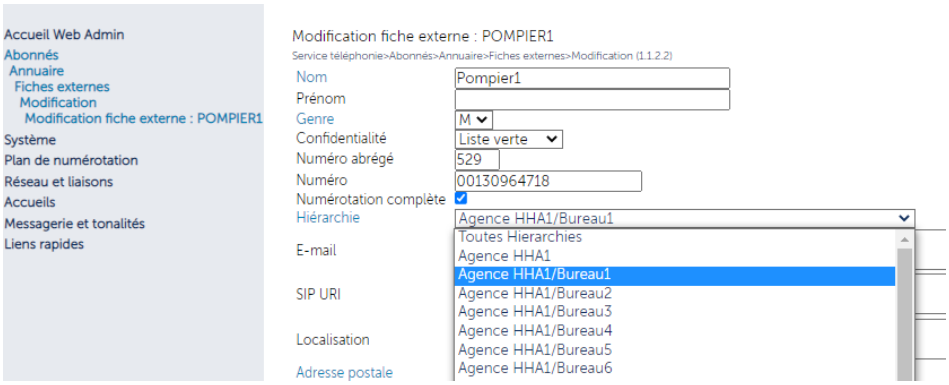
- Regrouper les abonnés d'une ou plusieurs agences ayant la même localisation géographique dans la même hiérarchie administrative.

Menu **Abonnés>Annuaire>Hiérarchies administratives**.

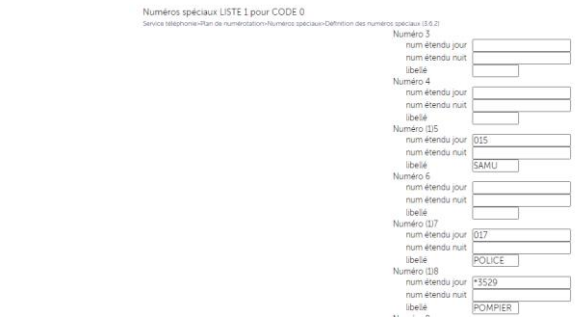


- Déclarer dans l'annuaire des fiches externes le numéro d'appel public des services d'urgence requis de chaque région géographique et leur affecter le même numéro abrégé avec une hiérarchie administrative différente.

Menu **Abonnés>Annuaire>Fiches externes**



- Configurer les numéros spéciaux avec le préfixe de numéro abrégé (Ex: * 3529) combiné avec le numéro précédemment déclaré du service d'urgence à composer (00130964718).
- Pour appliquer ce mécanisme aux numéros spéciaux, modifier la configuration du numéro spécial (11) 19 dans le menu des numéros spéciaux ci-dessus, comme illustré ci-dessous.
- Modification du numéro spécial avec le numéro abrégé considéré (*3529)



Visu des numéros spéciaux pour CODE 0

Service téléphonie>Plan de numérotation>Numéros spéciaux>Visualisation des numéros spéciaux (3.6.3)

Liste	Numéro	Numéro de jour	Numéro de nuit	Libellé
0	(11)2	0112		URGENCE
0	(11)5	0115		SAMU SOC
0	(11)9	0119		MALTRAIT
1	(1)5	015		SAMU
1	(1)7	017		POLICE
1	(1)8	*3529		POMPIER

Dans l’annuaire, le même numéro abrégé est associé à deux numéros publics correspondants à deux localisations.

Visualisation des numéros abrègés

Service téléphonie>Abonnés>Annuaire>Visualisations>Numérotation abrégée générale (1.1.5.3)

N° abrégé	Numéro	Nom	Autorisé pour
(*3) 001	01[illegible]	EXT601	Toutes Hierarchies
(*3) 002	013[illegible]	Nouvel_essai	Toutes Hierarchies
(*3) 111		S.Paja	Toutes Hierarchies
(*3) 114	208	ABO 208	Toutes Hierarchies
(*3) 123		Ihl	Toutes Hierarchies
(*3) 168	5225	ABO 5225	Toutes Hierarchies
(*3) 209	119	Y.Houmaire	Toutes Hierarchies
(*3) 224	01[illegible]	Abregeos	Toutes Hierarchies
(*3) 333	01[illegible]	E.ABO 6000	Toutes Hierarchies
(*3) 428	4017	Marco	Agence HHA1/Bureau1
(*3) 428	001[illegible]	Camille	Agence HHA1/Bureau2
(*3) 443	5600	Test_samu	Toutes Hierarchies
(*3) 529	00130964718	Pompier1	Agence HHA1/Bureau1
(*3) 529	00130964719	Pompier2	Agence HHA1/Bureau2
(*3) 530	0[illegible]	S.Henri	Toutes Hierarchies
(*3) 600		ABO 600	Toutes Hierarchies
(*3) 650	01[illegible]	Abo650	Toutes Hierarchies
(*3) 666	[illegible]	ABO 8123455000	Toutes Hierarchies

Cette configuration peut être répétée autant de fois que les numéros d'urgence sont différents selon la localisation : Pompiers, hôpital, police, etc).

9 CONFIGURATION DU MODE OTT POUR LES ACCES AUX APPLICATIONS WEB CLIENT ET USER PORTAL

9.1 PRINCIPE

Cette configuration permet aux travailleurs distants d'accéder via Internet en mode OTT et sans VPN aux applications :

- MiVoice 5000 User Portal via MiVoice 5000 Manager,
- MiVoice 5000 Manager Web Client,
- MiVoice 5000 User Portal embarqué.

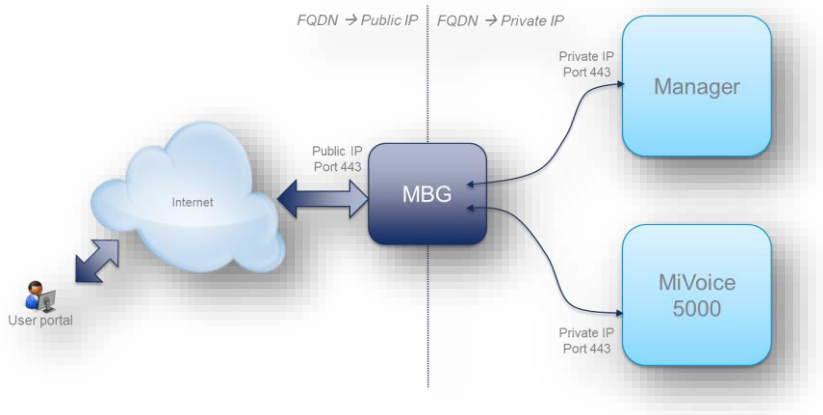
Note : Concernant Manager User Portal, la fonctionnalité est également disponible pour les utilisateurs déclarés sur les sites en version < 8.0 (et ≥ 6.5).

Le principe est d'autoriser l'accès à ces applications au travers du MBG.

L'accès est réalisé par Internet et en https via une session MBG Controller en mode OTT.

Via Internet, le FQDN de Mivoice 5000 Manager doit être résolu sur l'adresse IP du MBG quand on est sur INTERNET.

Accès au User portal en mode OTT



Le User Portal (MiVoice 5000 Manager ou intégré au MiV5000) est accessible de n'importe où par Internet grâce au FQDN permettant au travailleur distant de programmer les touches du terminal distant.

L'URL est identique dans le mode local ou dans le mode OTT.

Le MBG est utilisé comme proxy pour permettre l'accès depuis Internet. L'adresse IP locale du MBG au doit être déclaré comme proxy de confiance dans le MiVoice 5000 Manager ou Web Admin.

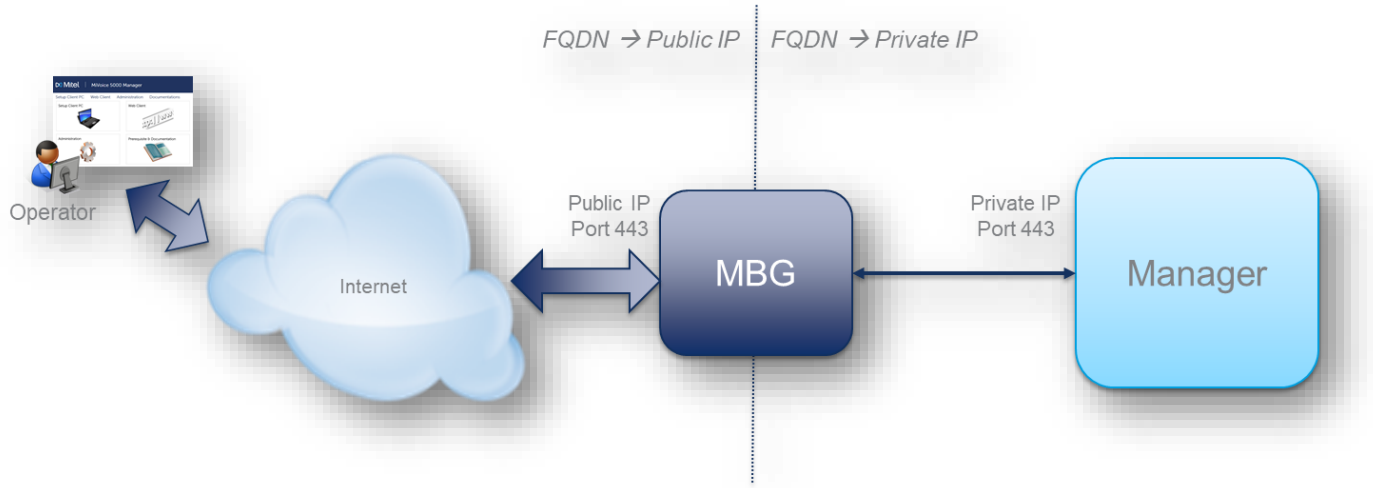
Le User Portal embarqué utilise le port HTTPS 443.

L'accès au User Portal est compatible avec toutes les versions de MiVoice 5000 (R6.5 et versions ultérieures)

L'accès en mode SSO au User Portal n'est pas disponible pour le User Portal embarqué. Disponible uniquement pour le User Portal du MiVoice 5000 Manager.

Note : Dans la version actuelle, la séparation de flux n'est pas compatible avec le User Portal embarqué.

Accès au Web Client MiVoice 5000 Manager en mode OTT



Le Web Client (MiVoice 5000 Manager ou intégré au MiV5000) est accessible pour le travailleur distant, de n'importe où par Internet grâce au FQDN permettant au travailleur distant d'a.

L'URL est identique dans le mode local ou dans le mode OTT.

Le MBG est utilisé comme proxy pour permettre l'accès depuis Internet. L'adresse IP locale du MBG au doit être déclaré comme proxy de confiance dans le MiVoice 5000 Manager ou Web Admin.

Pour les accès admin de la Web Admin, les utilisateurs et les comptes associés doivent être déclarés dans la configuration du Proxy.

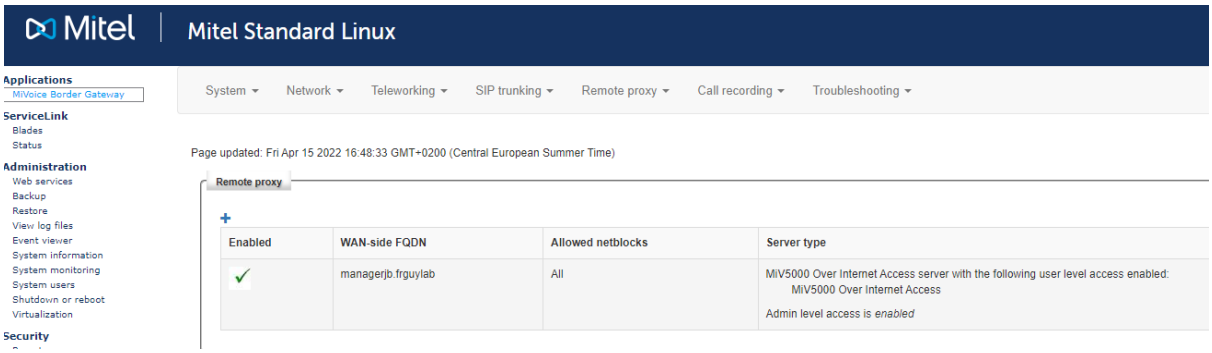
9.2 SYNTHESE DES DIFFERENTES ETAPES

9.2.1 CONFIGURATION MBG

Dans le menu **Remote proxy/Domain List** :

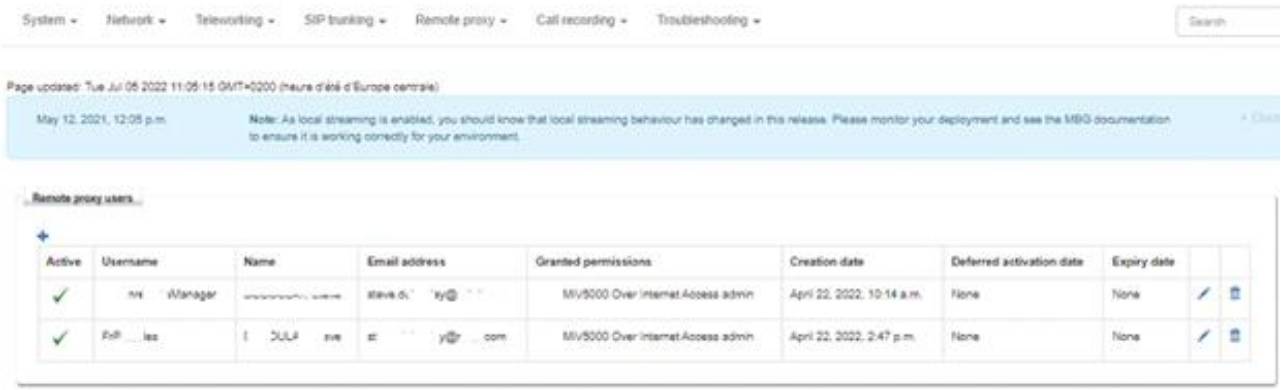
- Cliquer sur **+**,
- Entrer le WAN-side FQDN du MiVoice 5000 Manager (cas du Web Client ou User Portal) ou du MiVoice 5000 Server (Cas du User Portal embarqué) pour la résolution sur le MBG
- Sélectionner le service **MiV5000 Over Internet Access**.et cocher la case **Enabled**.

Exemple : Cas du MiVoice 5000 manager.



Dans le menu **Remote proxy/Users**,

- Déclarer les utilisateurs et Créer les comptes associés pour les accès admin de la Web Admin.



Dans le menu **Remote proxy/Proxy applications**

- Visualiser la liste des URLs du service **MiV5000 Over Internet Access**

MiV5000 Over Internet Access	a50	/userportal	/rhm /frf /csv /system /dhcp /dhcp6 /tma /annuaire /easyadmin /setup /webtelephony		User	Admin

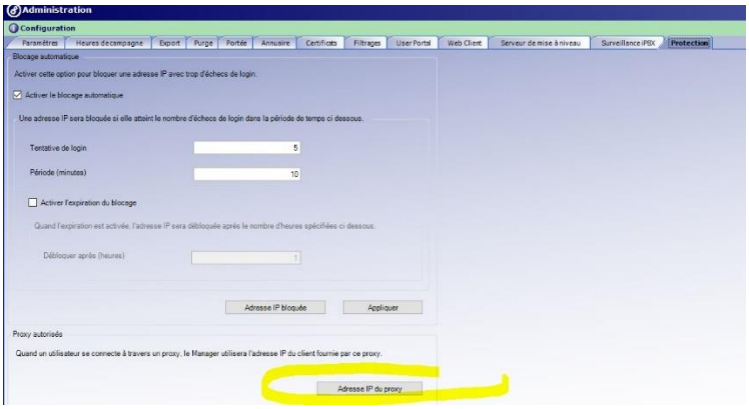
9.2.2 CONFIGURATION DU TRUSTED PROXY

9.2.2.1 Cas du Web Client et User Portal sur MiVoice 5000 Manager

Configurer l'adresse IP du MBG dans les proxys autorisés par le MiVoice 5000 Manager.

Menu **Configuration** – Onglet **Protection**.

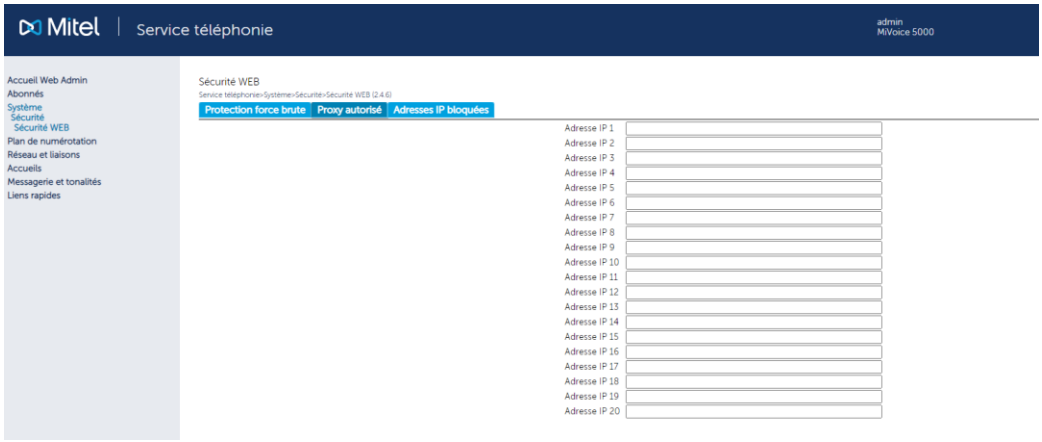
Se référer au document MiVoice 5000 Manager – Guide Utilisateur



9.2.2.2 Cas du User Portal embarqué

Dans la Web Admin, menu **Service téléphonie>Système>Sécurité>Sécurité WEB**, onglet **Proxy autorisé** :

- Entrer le ou les adresses des MBG(s) autorisés pour l'accès en mode OTT.



10 CONFIGURATION DU MODE OTT POUR LE SYSTEME SIP DECT

10.1 INTRODUCTION

Deux outils peuvent être utilisés pour la configuration du système SIP-DECT :

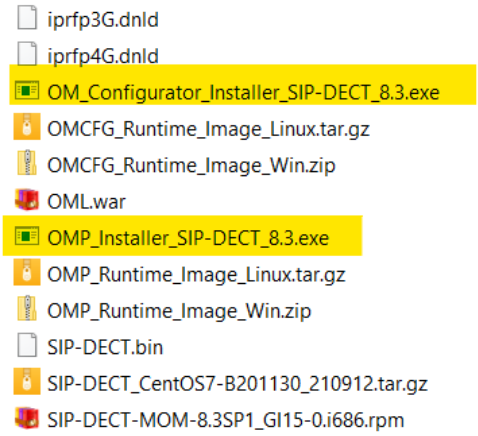
- OM Configurator - Open Mobility Configurator,
- OMP - Open Mobility Management Portal.

.

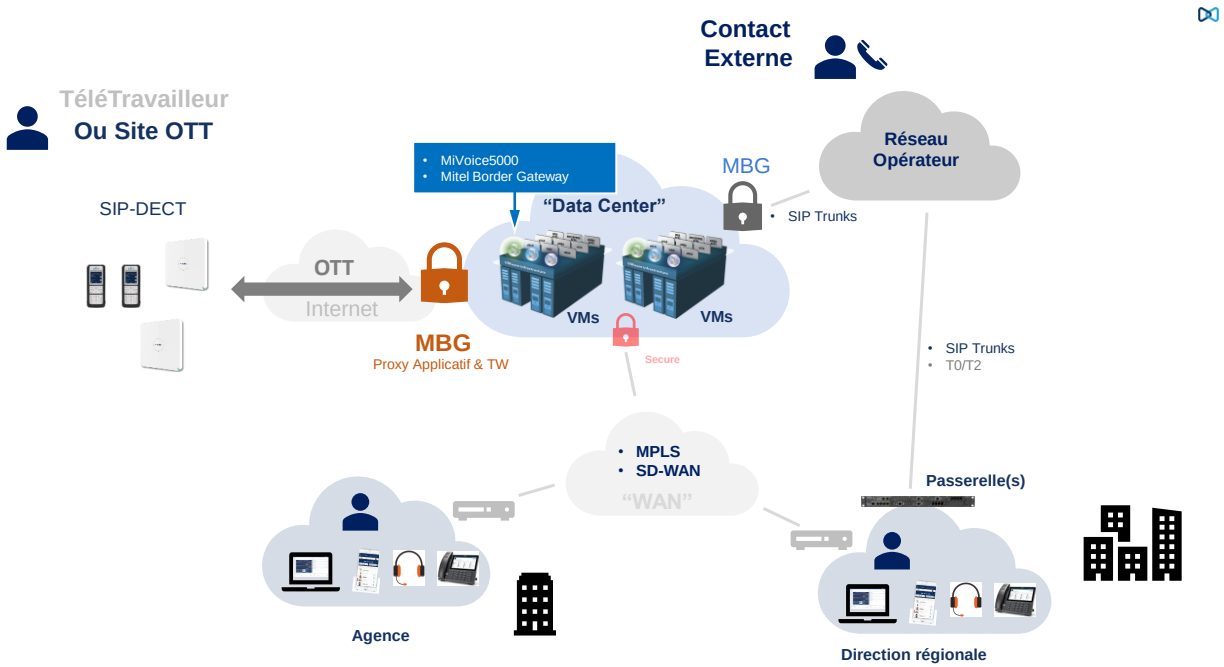
Note : L'accès en Web sur la borne dite « OMM » est également utilisable mais avec un peu moins de paramétrage avancé que sur l'OMP. Les possibilités réduites dans ce mode peuvent néanmoins suffire dans de nombreux cas

Outils disponibles sur le site de Mitel :

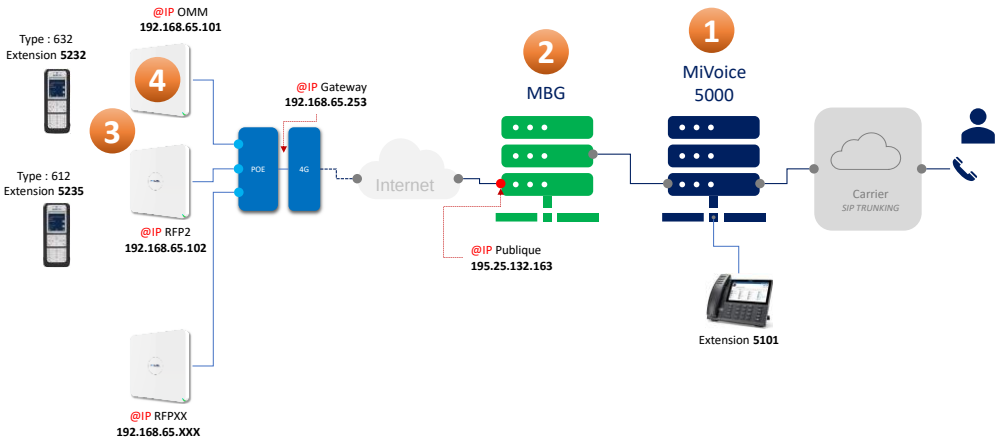
Menu **MiAccess>Software Download Center>SIP DECT>Mitel SIP DECT>Release 8.x SP? :**



10.2 ARCHITECTURE



Exemple de configuration



10.3 CONFIGURATION MIVOICE 5000

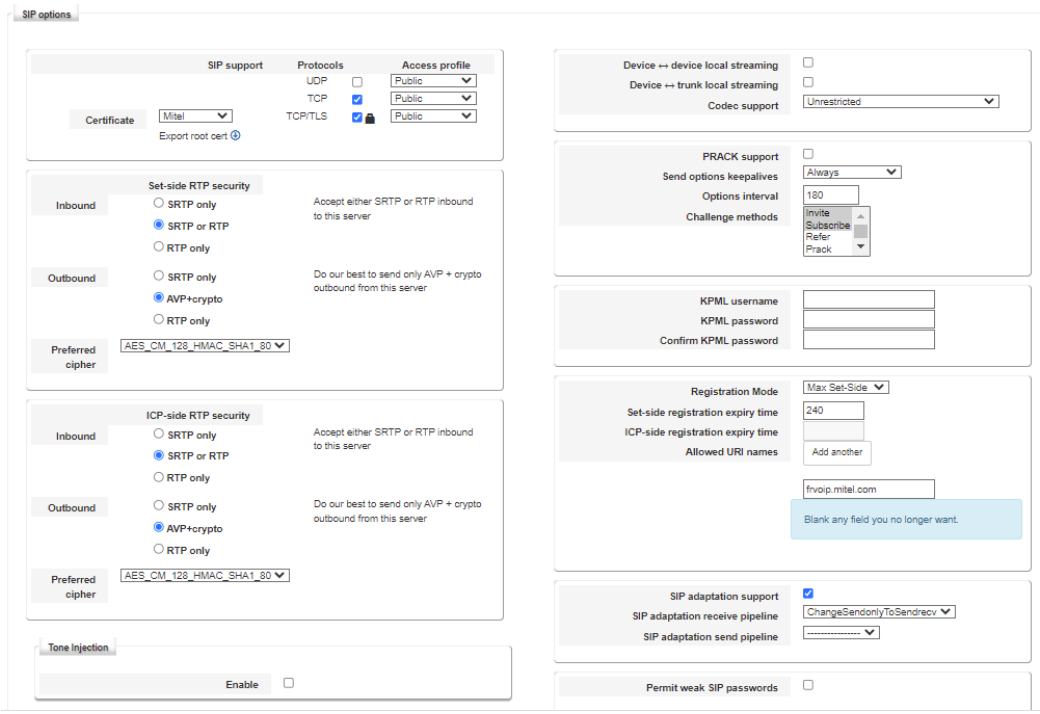
Déclarer les abonnés considérés.

Se référer aux documents :

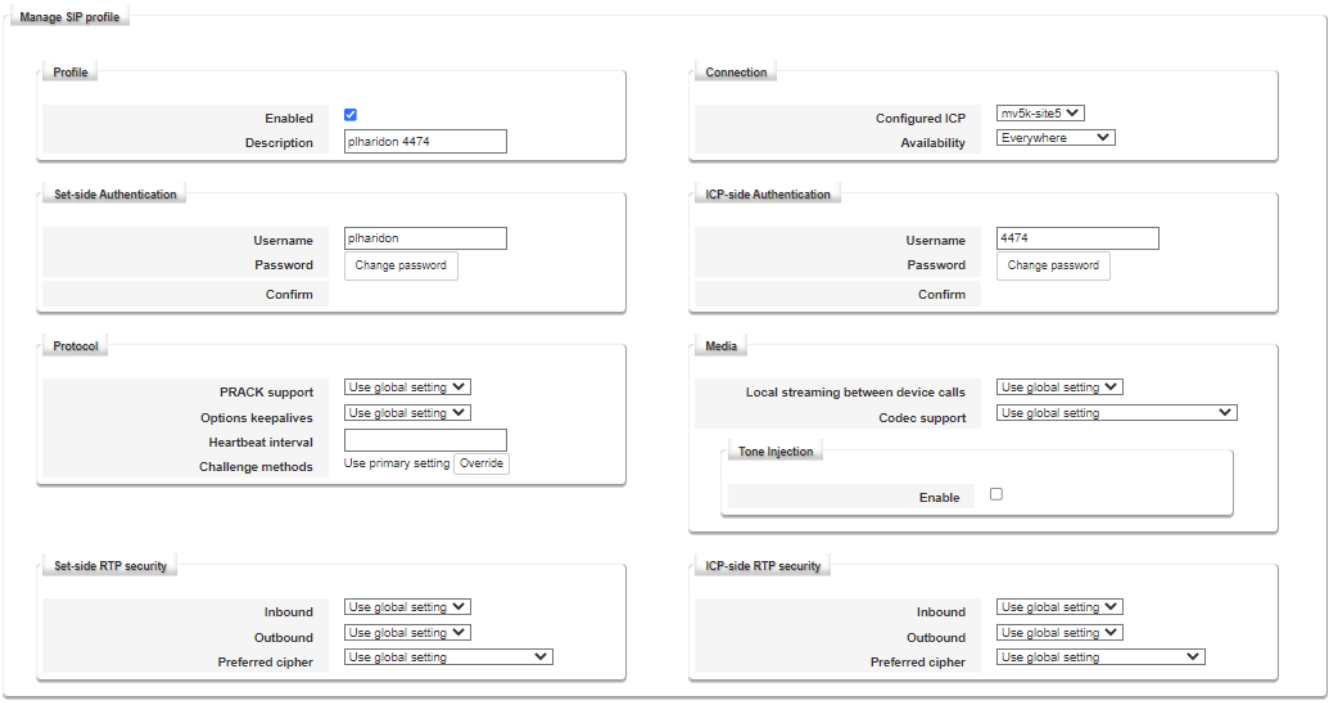
- MiVoice 5000 Server - Manuel Exploitation
- MiVoice 5000 Manager - Guide Utilisateur.

10.4 CONFIGURATION MBG

Menu **MBG>System>Settings>SIP Options**



Menu **MBG> TeleWorking> SIP**



10.5 CONFIGURATION AVEC OM CONFIGURATOR

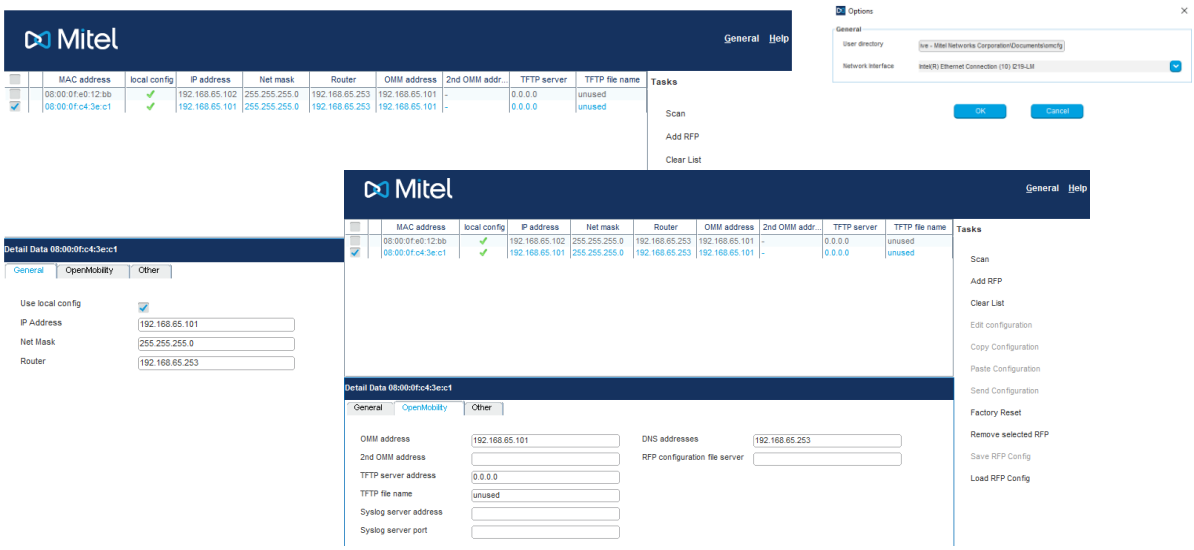
Cet outil simple permet :

La découverte des bornes connectés au même réseau que son PC

Le paramétrage initial des bornes RFP (adresse IP, masque, gateway…)

- Login par défaut : **omm / omm**
- Mot de passe : XXXX

OM CONFIGURATION / RFP 1 / OMM

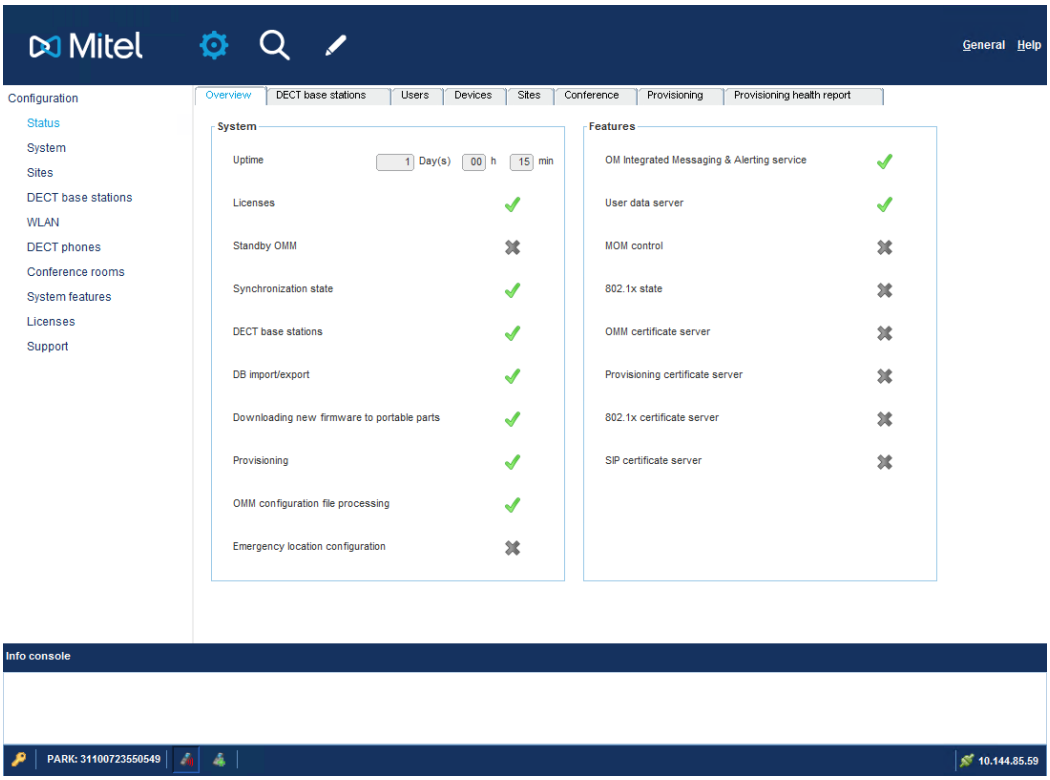


10.6 CONFIGURATION OMP (OPEN MOBILITY PORTAL)

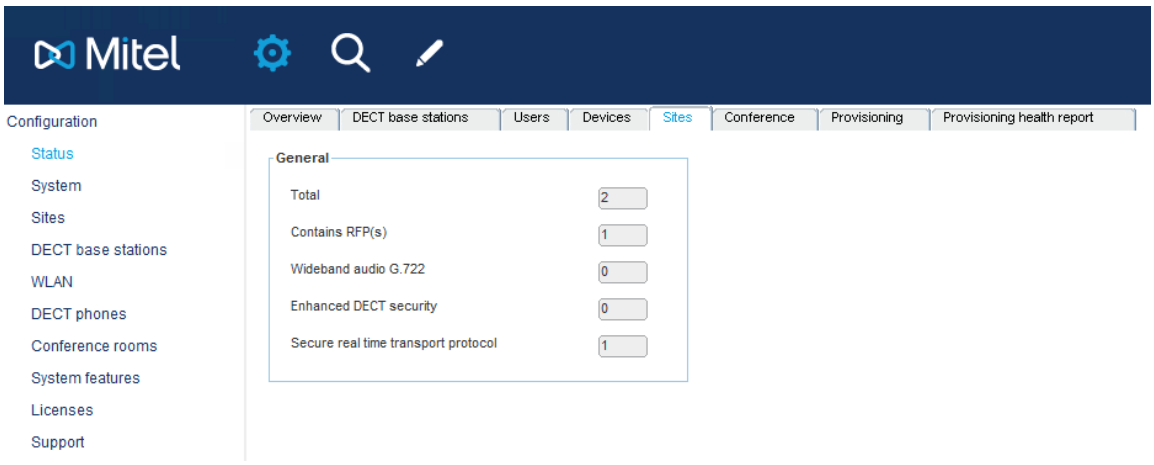
Cet outil avancé permet la configuration du système SIP-DECT

- Login par défaut : **omm** / **omm**
- Mot de passe: XXXX

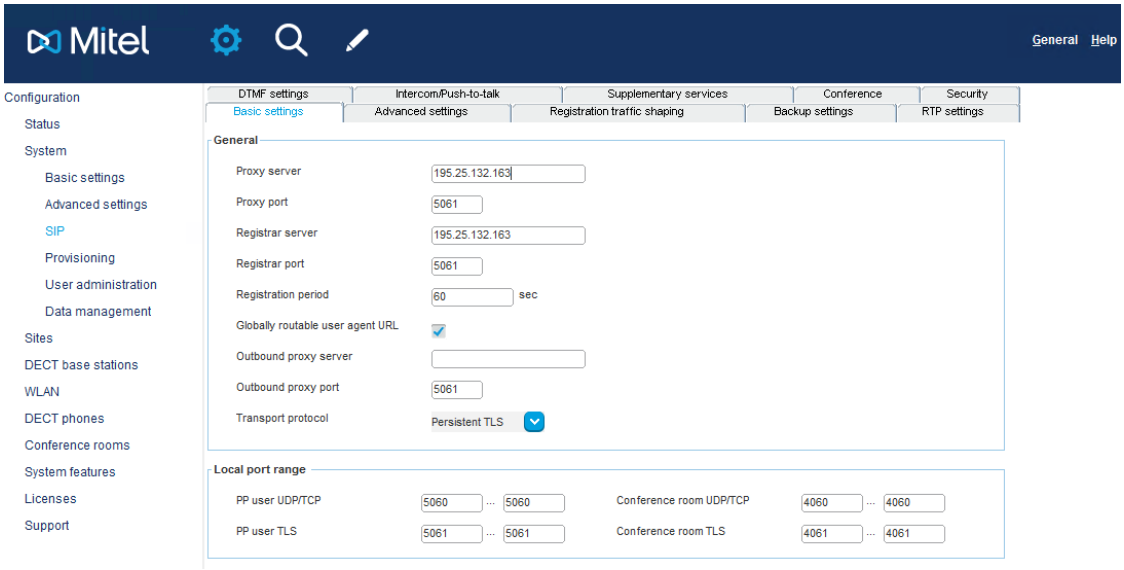
OMP STATUS



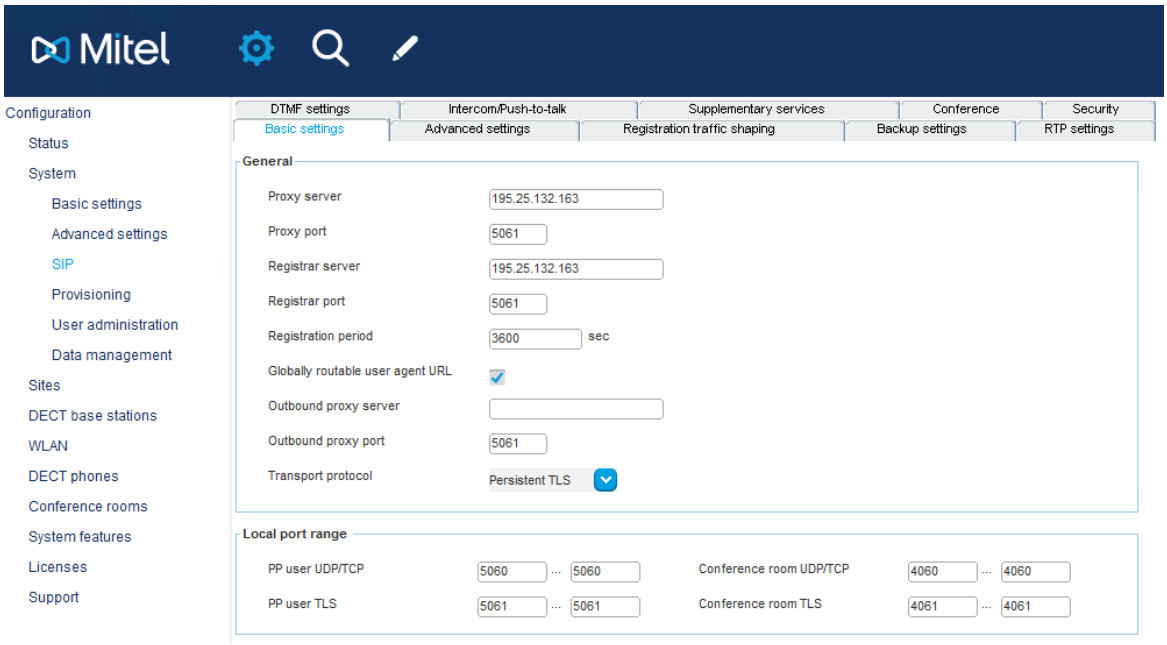
OMP - SITES



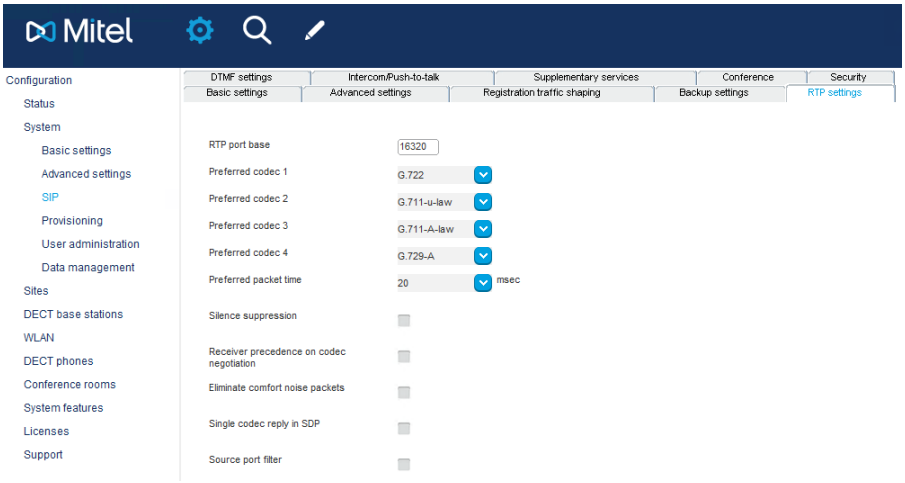
BASIC SETTINGS 1/2



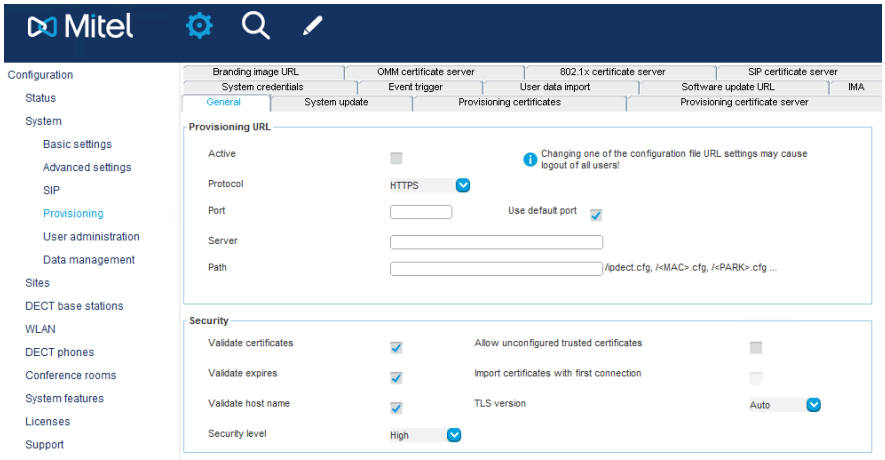
BASIC SETTINGS 1/2



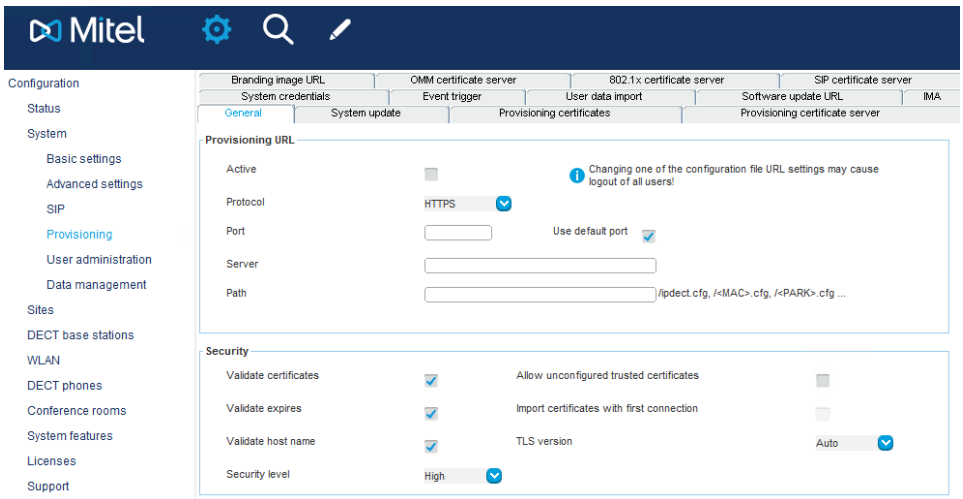
OMP – RFP SETTING



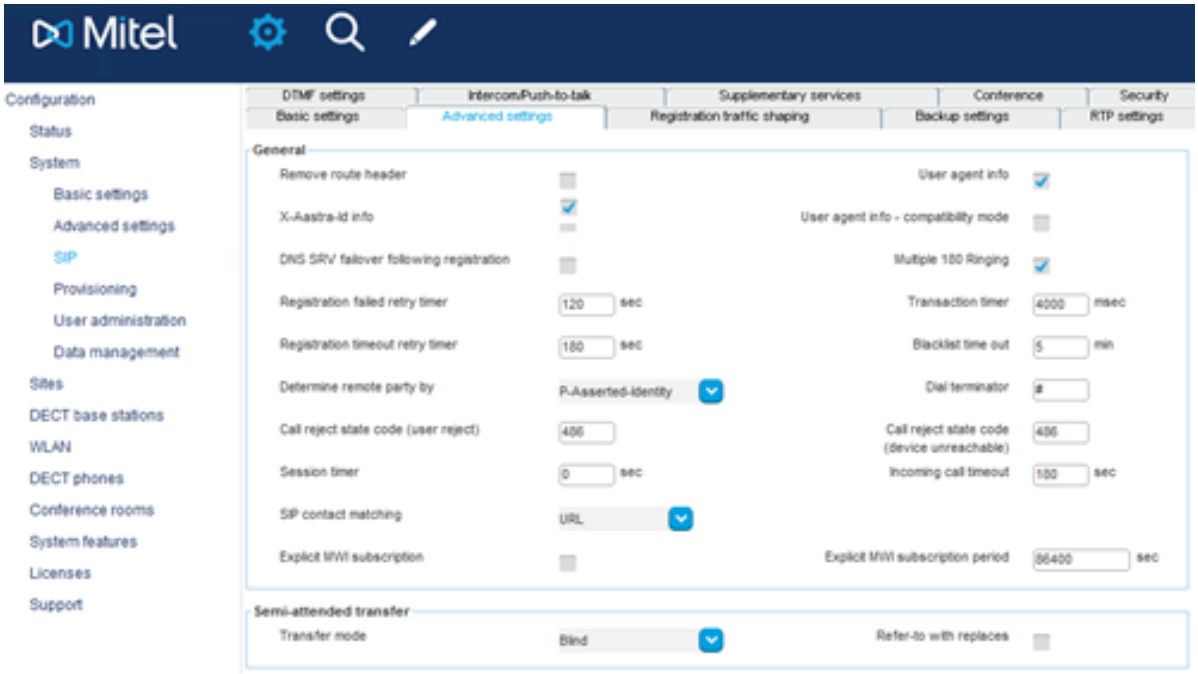
OMP – GENERAL 1/2



OMP – GENERAL 2/2

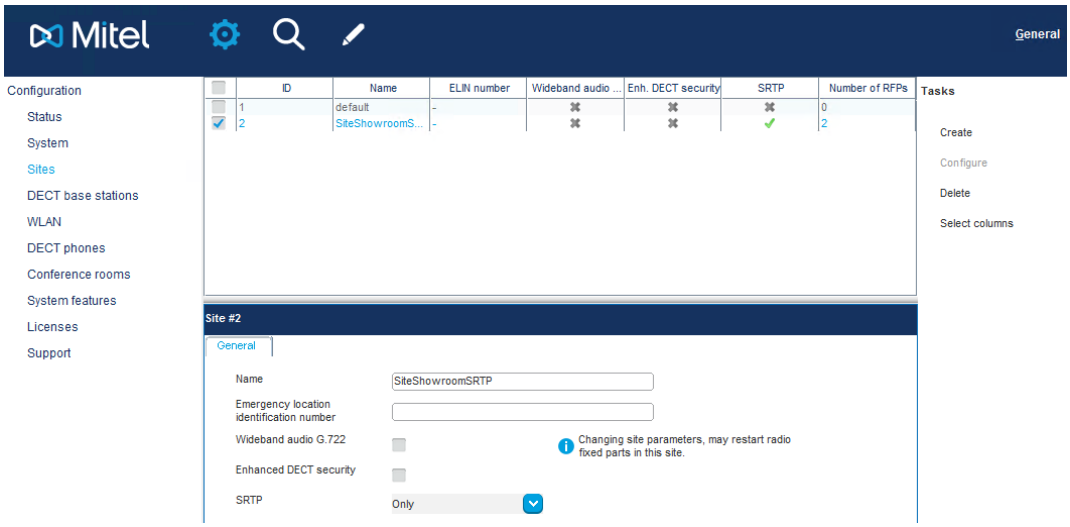


OMP – ADVANCED SETTINGS

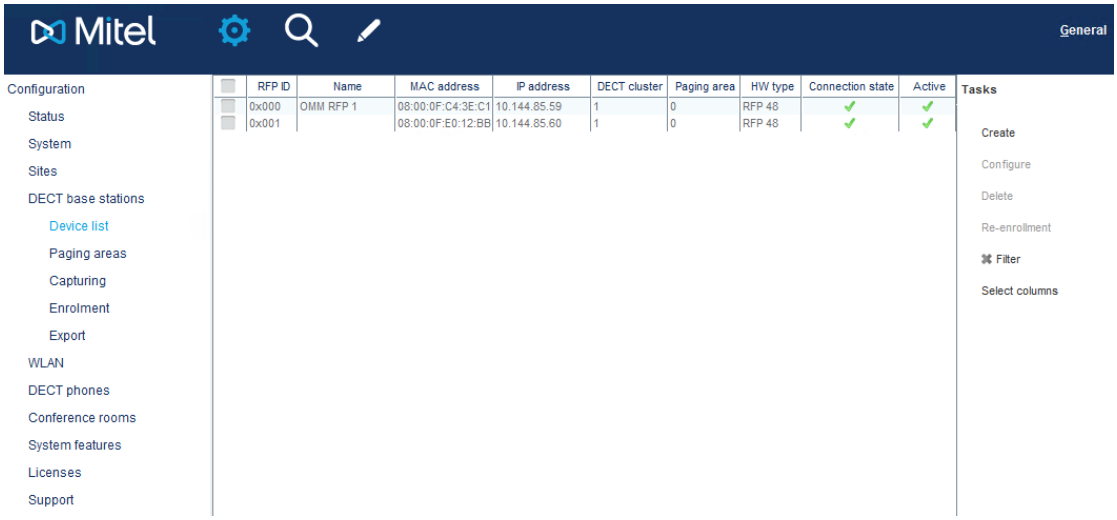


Cocher la case **X-Aastra-id info** en ayant impérativement effectué une pré-affectation DECT-IP sur les abonnements concernés côté MiVoice 5000.

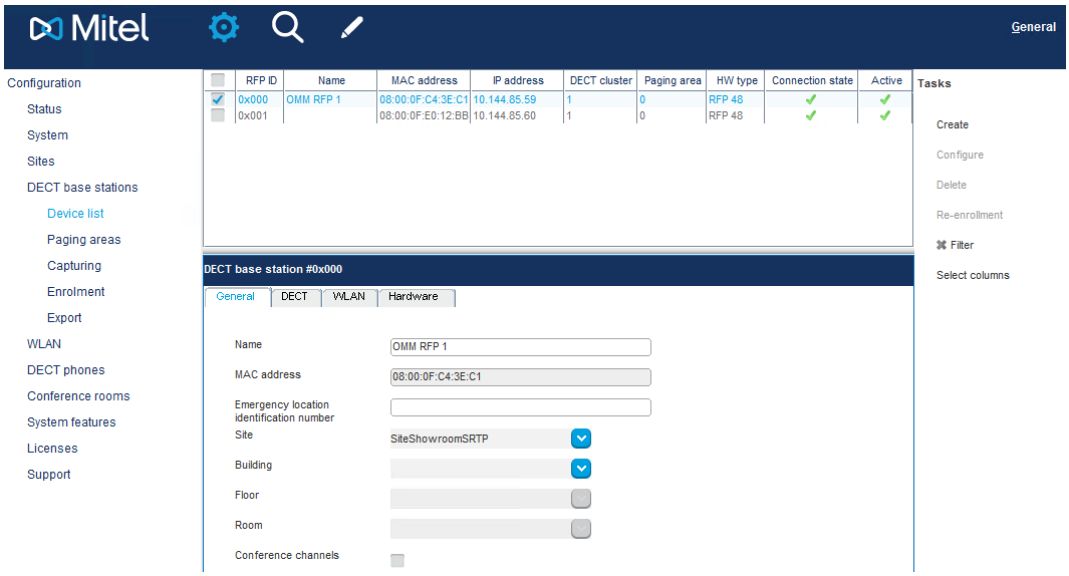
OMP - SITES



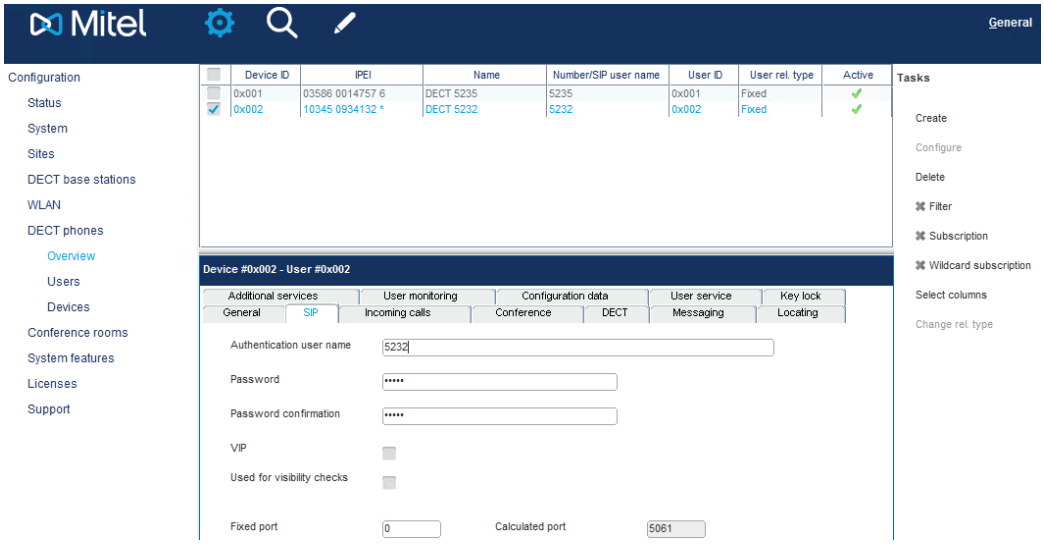
OMP - SITES & BASE STATIONS 1/2



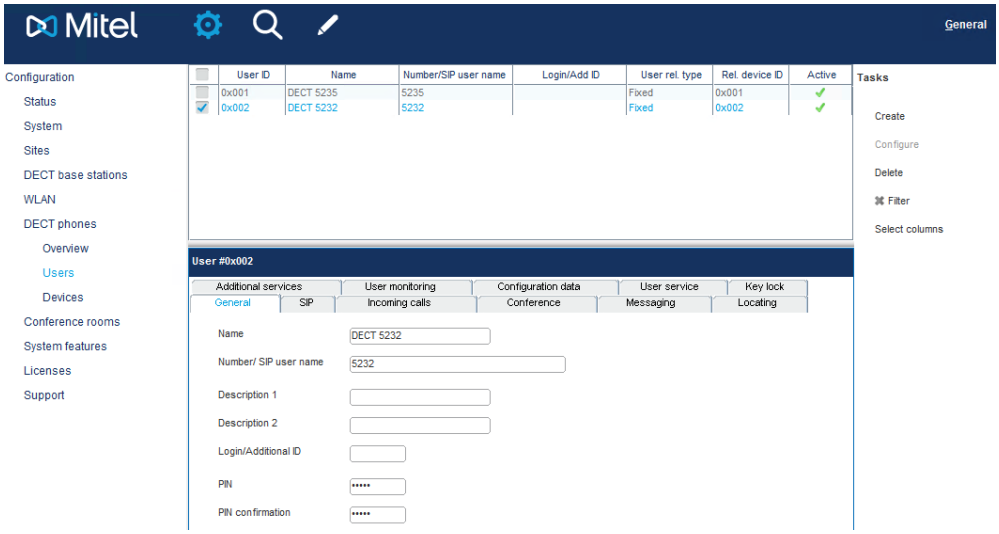
OMP - SITES & BASE STATIONS 2/2



OMP - DECT PHONES 1/2



OMP - DECT PHONES 2/2



10.7 CONFIGURATION DES ACCES XML POUR REMOTE WORKER DECT SIP EN MODE OTT

10.7.1 PRINCIPE

Un abonné Remote Worker de type DECT SIP en mode OTT doit être détecté par le MiVoice 5000 en tant que Remote Worker.

Lors du déploiement, est donc nécessaire de fournir à l'OMM la clé d'accès (hash) générée au niveau du MiVoice 5000 pour renseigner les URL relatives aux fonctionnalités XML considérées (liste des appelants, la liste de renumérotation, le menu Serveur, le code d'accès à la fonctionnalité).

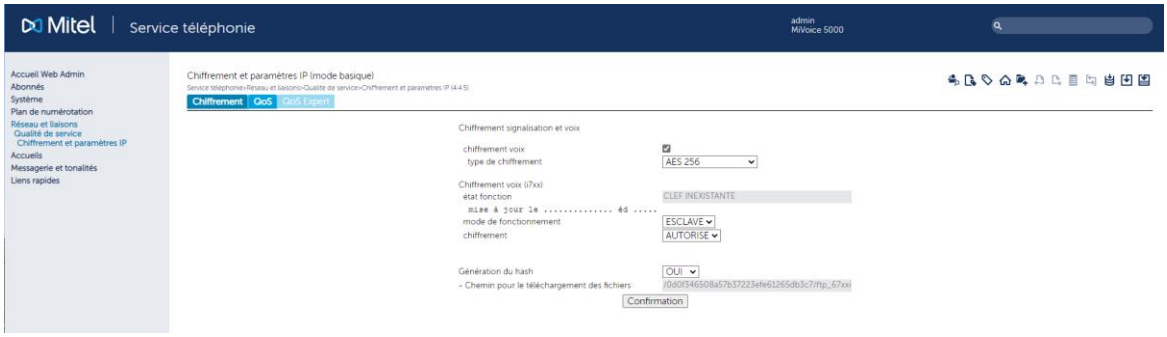
Cette action est à réaliser en deux étapes :

- Au niveau de la WebAdmin du MiVoice 50000 : Récupérer la valeur hash indiquant le chemin pour le téléchargement des fichiers concernant les Remote Workers.
- Au niveau de l'OMM : Renseigner la valeur de la clé hash pour les fonctionnalités nécessitant un accès XML.
- Ouverture de l'accès aux répertoires du MiVoice 5000.

10.7.2 CONFIGURATION

Récupération de la clé hash au niveau MiVoice 5000

Menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP (4.4.5)** – Onglet **Chiffrement** :



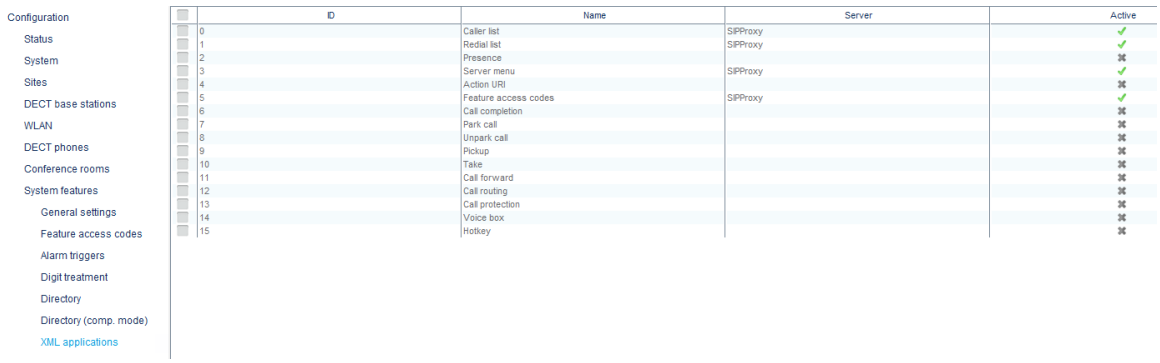
Copier et sauvegarder la valeur indiquée du **hash** (uniquement) dans le champ **- Chemin pour le téléchargement des fichiers**.

IMPORTANT : La valeur du hash est celle indiquée à gauche du champ, avant /ftp_67xx. Dans l'exemple 0d0f346508a57b3722efe61265db3c7.

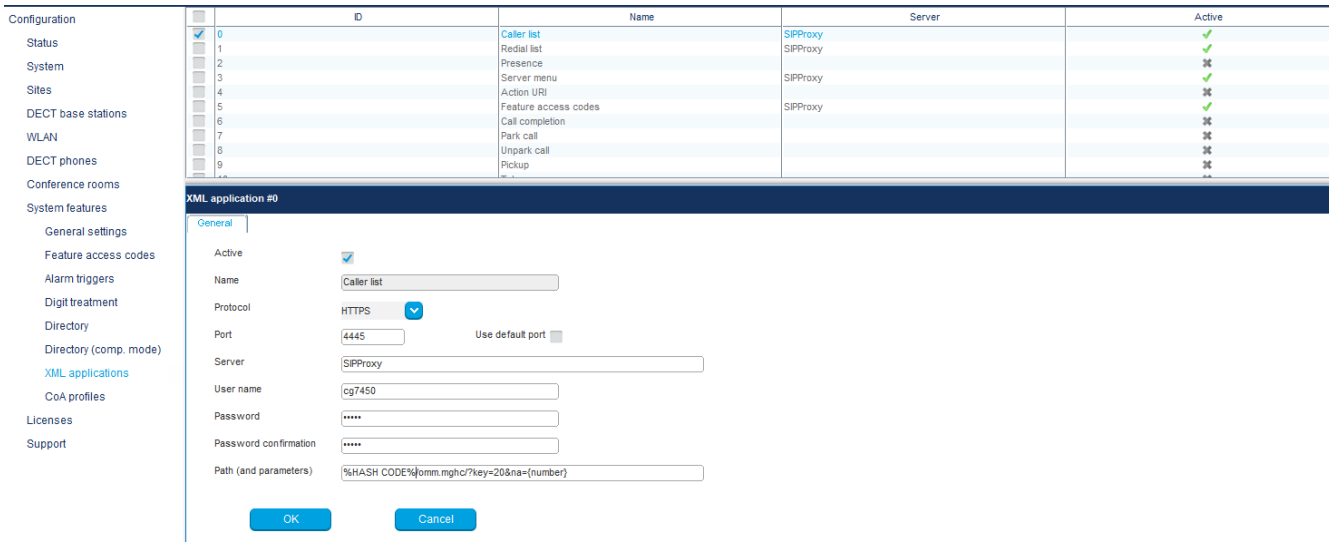
Configuration de l'URL d'accès au niveau de l'OMM

A partir de l'interface d'exploitation OMM

Menu **Configuration>System features>XML applications**



- Entrer la valeur du **hash** en début du champ relatif à URL d'accès **Path (and parameters)** .



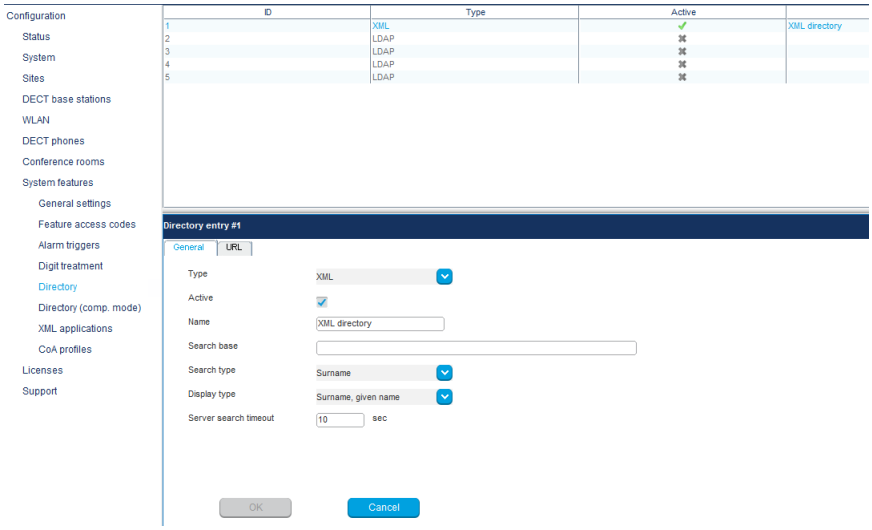
La même clé Hash doit être renseignée dans les différentes URLs selon la fonctionnalité :

- Liste des appelants (**Caller list**) : %HASH CODE%/omm.mghc/?key=20&na={number}
- Liste de renumérotation (**Redial list**) : %HASH CODE%/omm.mghc/?key=18&na={number}
- Menu Serveur(**Server menu**) : %HASH CODE%/omm.mghc/?key=0&na={nombre}
- Code d'accès à la fonctionnalité (**Feature access codes**) : %HASH CODE%/omm.mghc/?key=0&na={number}&fac={fac}

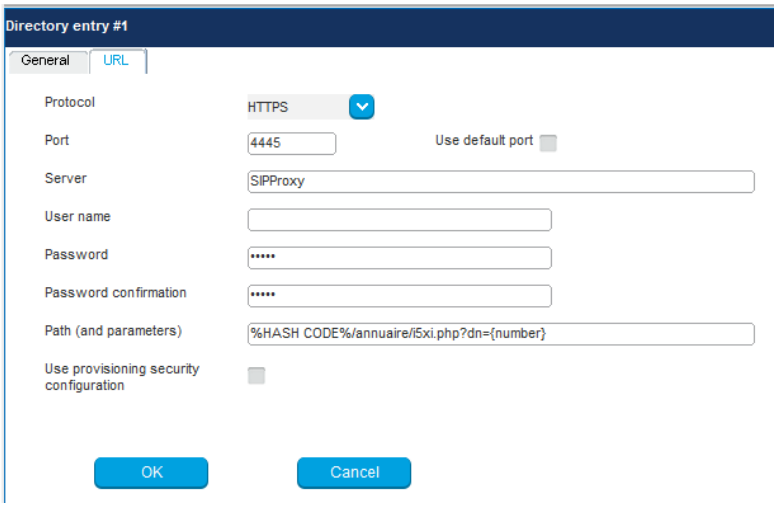
Ouverture de l'accès aux répertoires du MiVoice 5000

Menu **Configuration>System features>Directory**

Onglet **General**

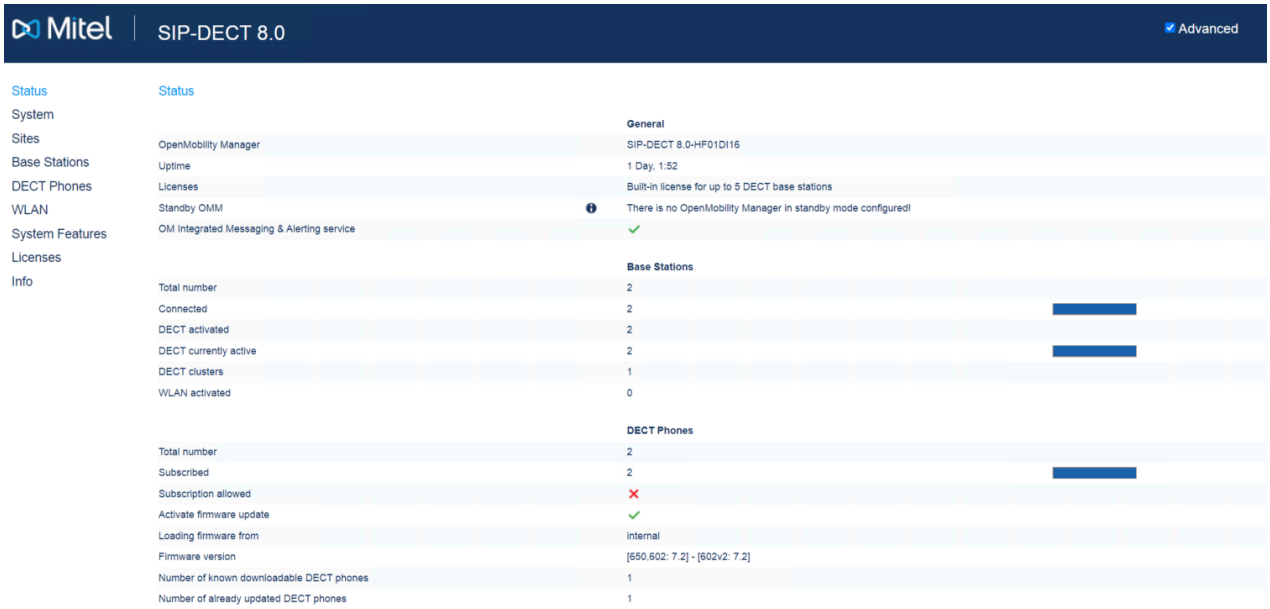


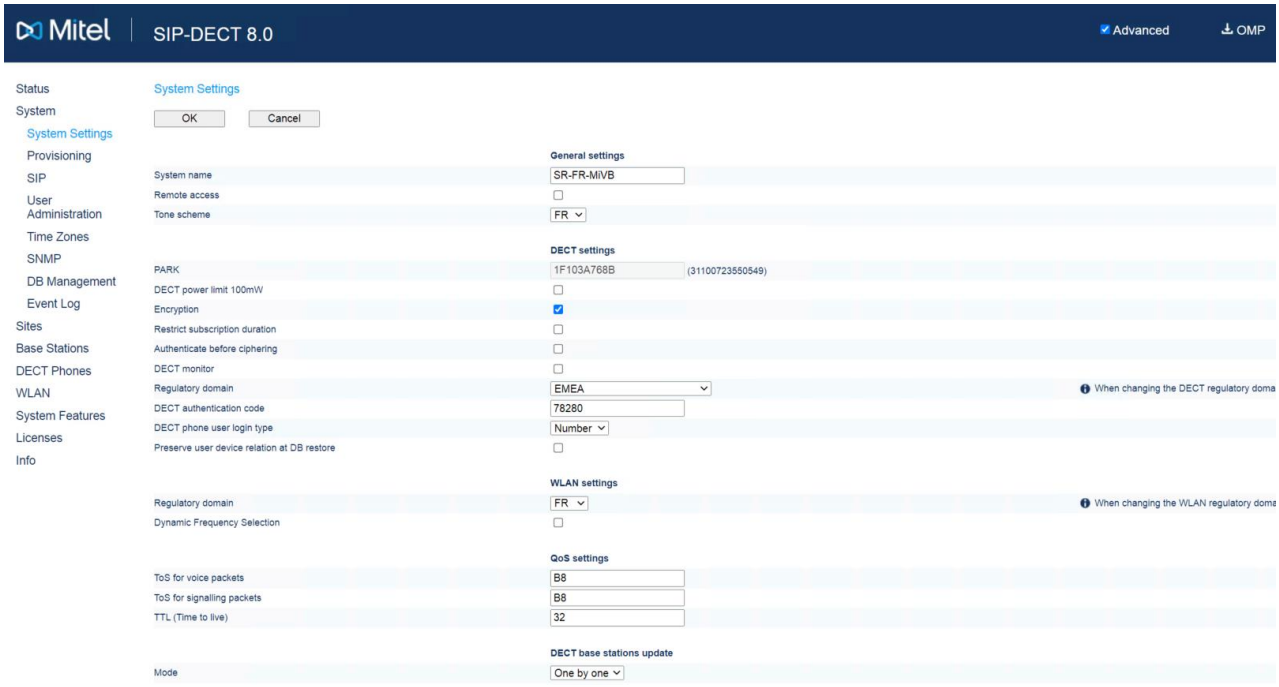
Onglet **URL**

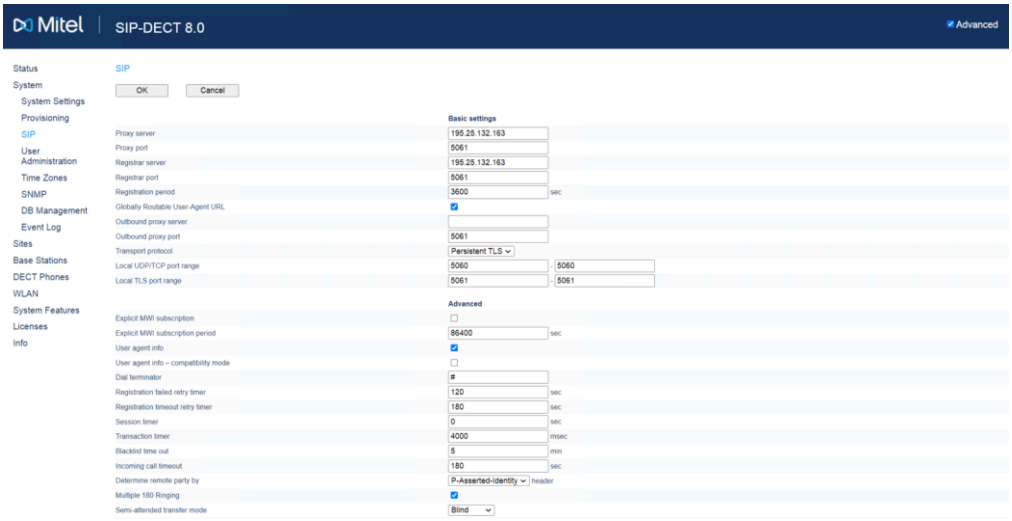


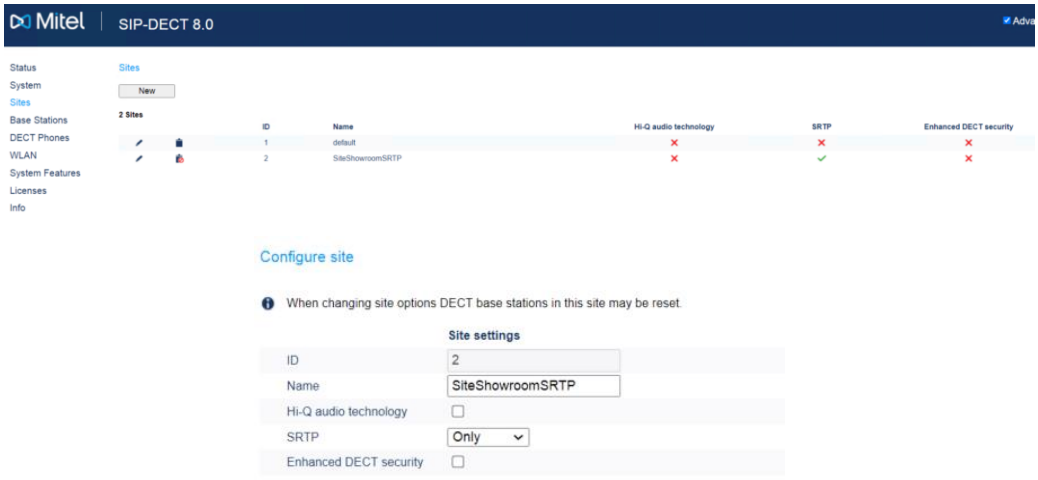
10.8 OMM WEB

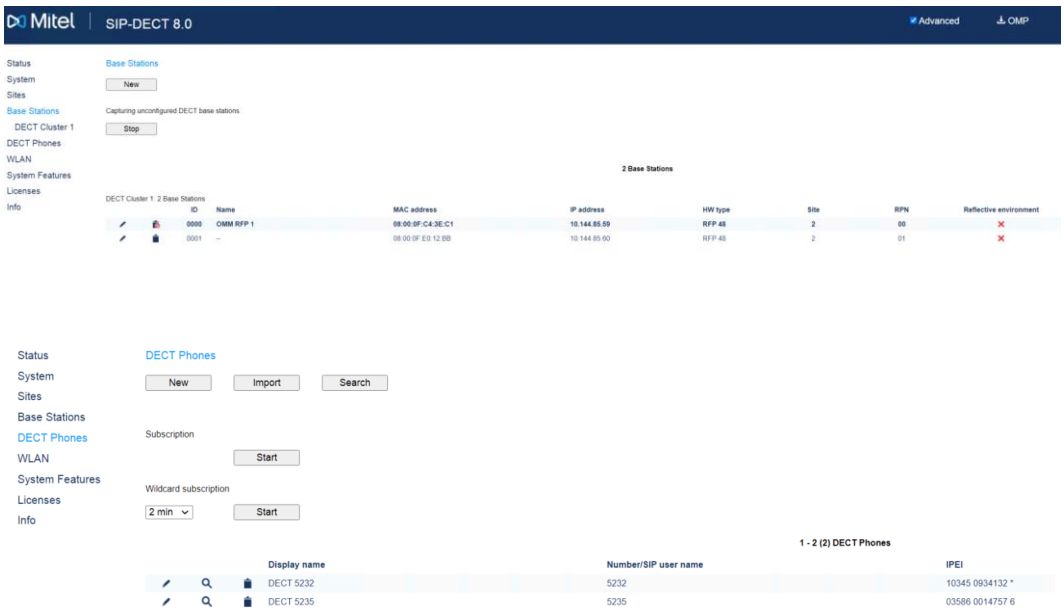
Accès > https:\\192.168.65.101






Mitel
SIP-DECT 8.0
Advanced
Status
System
System Settings
Provisioning
SIP
User Administration
Time Zones
SNMP
DB Management
Event Log
Sites
Base Stations
DECT Phones
WLAN
System Features
Licenses
Info
SIP
OK
Cancel
Basic settings
Proxy server
195.25.132.163
Proxy port
5061
Registrar server
195.25.132.163
Registrar port
5061
Registration period
3600
sec
Globally Routable User-Agent URL
Outbound proxy server
Outbound proxy port
5061
Transport protocol
Persistent TLS
Local UDP/TCP port range
5060
5060
Local TLS port range
5061
5061
Advanced
Explicit MWI subscription
Explicit MWI subscription period
86400
sec
User agent info
User agent info – compatibility mode
Dial terminator
#
Registration failed retry timer
120
sec
Registration timeout retry timer
180
sec
Session timer
0
sec
Transaction timer
4000
msec
Blacklist time out
5
min
Incoming call timeout
180
sec
Determine remote party by
P-Asserted-Identity
header
Multiple 180 Ringing
Semi-attended transfer mode
Blind


Mitel
SIP-DECT 8.0
Status
System
Sites
Base Stations
DECT Phones
WLAN
System Features
Licenses
Info
Sites
New
2 Sites
ID
Name
Hi-Q audio technology
SRTP
Enhanced DECT security
1
default
2
SiteShowroomSRTP
Configure site
When changing site options DECT base stations in this site may be reset.
Site settings
ID
2
Name
SiteShowroomSRTP
Hi-Q audio technology
SRTP
Only
Enhanced DECT security


Mitel
SIP-DECT 8.0
Advanced
OMP
Status
System
Sites
Base Stations
DECT Cluster 1
DECT Phones
WLAN
System Features
Licenses
Info
Base Stations
New
Capturing unconfigured DECT base stations
Stop
2 Base Stations
DECT Cluster 1: 2 Base Stations
ID
Name
MAC address
IP address
HW type
Site
RPN
Reflective environment
0000
OMM RFP 1
08:00:0F:C4:3E:C1
10.144.85.59
RFP 48
2
00
0001
08:00:0F:E0:12:BB
10.144.85.60
RFP 48
2
01
Status
System
Sites
Base Stations
DECT Phones
WLAN
System Features
Licenses
Info
DECT Phones
New
Import
Search
Subscription
Start
Wildcard subscription
2 min
Start
1 - 2 (2) DECT Phones
Display name
Number/SIP user name
IPEI
DECT 5232
5232
10345 0934132 *
DECT 5235
5235
03586 0014757 6