MiVoice 5000 Server

04/2025

AMT/PTD/PBX/0177/1/2/FR

MISE EN SERVICE

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.

SOMMAIRE

1 INSTALLATION DU MIVOICE 5000 SERVER (NON REDONDÉ SANS DOUBLE ATTACHEMENT)

Ce chapitre décrit les tâches nécessaires à l'installation de l'application MiVoice 5000 Server non redondé et sans double attachement. Pour le MiVoice 5000 server redondé se référer au document MiVoice 5000 Server et Cluster Server - Redondance.

Si le système redondé ou non doit être configuré avec double attachement, se référer au document Rocky Linux et Double attachement.

Note : Le double attachement consiste à utiliser deux interfaces reliées par deux câbles distincts. Dans ce cas, on utilise une interface virtuelle " bondx " (mode bonding), la seule vue du réseau et qui permet de basculer de l'une à l'autre des interfaces physiques en cas de dysfonctionnement de l'une d'entre elles.

1.1 PRÉ-REQUIS IMPORTANT

A partir de R8.0, le système d'exploitation Rocky Linux et, doit être installé au préalable sur le PC (installé par défaut en usine). La version précise est indiquée dans la release note.

Se référer au document Rocky Linux et Double Attachement.

La déclaration et la configuration réseau du PC doit avoir été réalisée (contacter éventuellement l'administrateur réseau).

Le PC doit être connecté au réseau sur lequel il est dédié (câble réseau connecté).

Dans un environnement virtualisé, une VM est disponible sur le serveur de téléchargement de Mitel.

1.2 INSTALLATION DE L'APPLICATION MIVOICE 5000 SERVER SUR UN SYSTÈME NON VIRTUALISÉ

1.2.1 LANCEMENT DU SCRIPT D'INSTALLATION DU MIVOICE 5000

- Se loguer sur la machine avec le compte root et le mot de passe Mitel5000
- Monter l'image iso (ACS_A5000_R8.2_AXYY.iso) récupérée du site Mitel. Se référer en annexe au paragraphe **4.1 – Montage d'une image ISO**.

Une fois l'image iso montée :

- Lancer le script d'installation du MiVoice 5000 à la racine de l'arborescence :

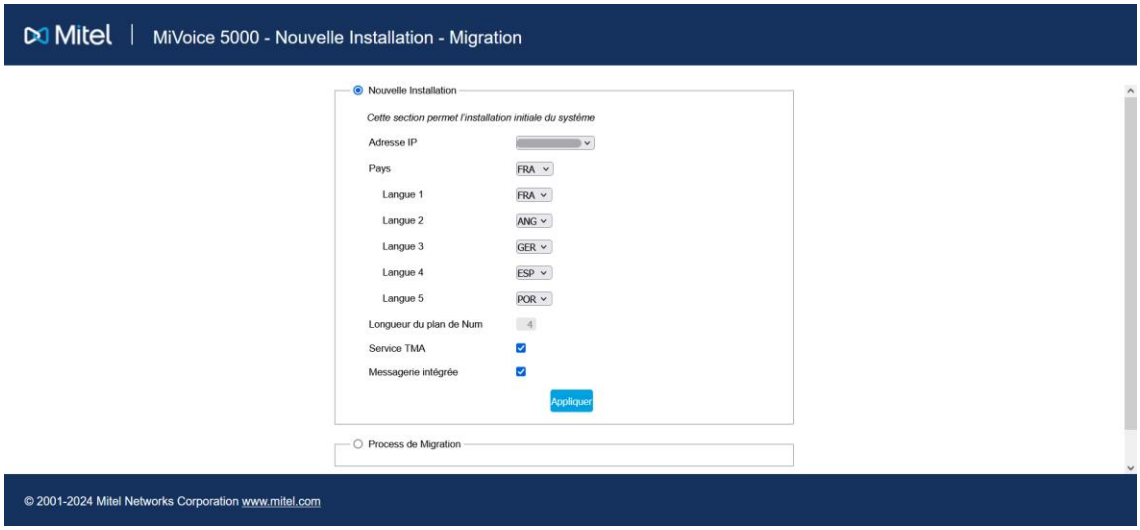
  #**./install_a5000_server.sh**

Le script se déroule ensuite automatiquement sans intervention de l'utilisateur.

1.2.2 INSTALLATION SUR UN SYSTÈME NON VIRTUALISÉ VIA L'OUTIL D'INSTALLATION RAPIDE

La suite de l'installation est à réaliser à partir de l'outil d'installation rapide du MiVoice 5000, accessible à l'adresse **http://Adresse IP ou FQDN**, où **Adresse IP ou FQDN** représente l'adresse IP ou le FQDN du futur MiVoice 5000 Call Server.

La section **Nouvelle installation** s'affiche par défaut.



Remplir les champs suivants :

- **Adresse IP** : Liste déroulante. Permet de sélectionner les adresses IP disponibles pour le MiVoice 5000 Call Server.
- **Pays** : Localisation du MiVoice 5000 Call Server
- **Langue 1 à 5** : Langues applicables sur le MiVoice 5000 Call server, par ordre de priorité
- **Longueur du plan de Num** : Nombre de chiffres pour la structure des numéros téléphoniques locaux du MiVoice 5000 Call Server

- **Service TMA** : Case à cocher. Si cochée, inclut le service TMA au MiVoice 5000 Call Server.
- **Messagerie intégrée** : Case à cocher. Si cochée, inclut la messagerie intégrée au MiVoice 5000 Call Server.

Cliquer sur le bouton **Appliquer** pour lancer l'installation avec les paramètres renseignés. L'installation dure quelques minutes.

Après l'installation, l'outil lance automatiquement la Web Admin du MiVoice 5000 Call Server.

ATTENTION : Après installation, l'outil d'installation rapide n'est plus accessible.

1.3 INSTALLATION DE L'APPLICATION MIVOICE 5000 SERVER DANS UN ENVIRONNEMENT VIRTUALISÉ

1.3.1 DÉPLOIEMENT DE LA MACHINE VIRTUELLE

1.3.1.1 Dans un environnement VMWare

A partir de l'image **ova** fournie par Mitel, suivre la procédure suivante :

- Dézipper le contenu du fichier zip dans un espace disque local ou réseau. Cet espace doit être accessible depuis le vSphere client du Serveur ESX où la VM MiVoice 5000 Server doit être installée. Cet espace doit être accessible depuis le vSphere client du Serveur ESX où la VM MiVoice 5000 Server doit être installée.
- Se connecter via le vSphere client à la machine Serveur ESX
- Sélectionner le fichier **.ova**.
- Cliquer ensuite sur le bouton **Suivant**.
- Vérifier les détails du modèle déployé puis cliquer ensuite sur le bouton **Suivant**.
- Vérifier et éventuellement modifier le nom de la VM puis cliquer ensuite sur le bouton **Suivant**.
- Sélectionner le format de disque.

Note : Les paramètres Nombre de cœurs et Taille de RAM de la VM peuvent être modifiés si nécessaire en fonction de la charge à partir du menu Modifier les paramètres de machine virtuelle, Onglet Matériel.

- Choisir le réseau.
- Cliquer sur le bouton **Terminer** pour démarrer le déploiement de la VM.
- Attendre la fin du déploiement puis cliquer sur le bouton **Fermer.**
- Sélectionner la VM puis la démarrer en cliquant sur la flèche verte.
- Cliquer sur l'onglet **Console**
- Se loguer root (mot de passe par défaut : **Mitel5000**).

ATTENTION : Pour la saisie, le système est en Anglais et clavier initial est en AZERTY. Le pavé numérique n'est pas activé.

En fonction de la langue désirée, taper les commandes suivantes

- Vers le Français :

  # localectl set-keymap fr

- Vers l'Anglais :

  localectl set-keymap us

1.3.1.2 Dans un environnement KVM

Contenu de l'archive au format tgz

L'archive au format tgz contient :

- Le fichier disque (.**qcow2**)
- Le fichier XML des caractéristiques systèmes (.**xml**)
- La signature MD5 des fichiers précédents (.**md5**)

Contenu de la VM

- 1 vCPU
- 1 GB de RAM
- 10 GB de disque

Déploiement de la VM

Note : L'extraction des fichiers de l'archive TGZ doit se faire obligatoirement sous Linux, sur la machine cible qui possède les paquetages KVM.

A partir de l'archive au format **tgz** disponible sur le serveur de téléchargement Mitel, suivre la procédure suivante :

Copier l'archive dans un répertoire sur le serveur KVM sur lequel la VM MiVoice 5000 Server doit être déployée.

Note : La partition dans laquelle sera copiée l'archive, doit posséder au moins 10 Go de disponible

Se placer dans le répertoire dans lequel l'archive a été copiée et extraire les fichiers de l'archive par la commande "**tar xzf A5000_SAAS-KVM_RY.X**_xyz.tgz".

Copier le fichier disque (.qcow2) dans le répertoire /var/lib/libvirt/images

Copier le fichier (.xml) dans le répertoire de travail /tmp

Taper la commande **virsh net-list -all** afin de lister les interfaces réseaux déclarées sur cette machine Linux pour la virtualisation KVM.

Editer le fichier XML des caractéristiques systèmes (.xml) qui se trouve sous /tmp et adapter la VM aux caractéristiques de la machine et en particulier les interfaces réseaux **saaslan** et **saaswan**

Installer la VM avec la commande suivante :

virsh define /tmp/ MV5000.xml

Démarrer la VM avec la commande suivante

virsh start MV5000

Configurer la VM en démarrage automatique avec la commande suivante :

virsh autostart MV5000

Se connecter à la VM (login : c2ic et password : c2ic)

virsh console MV5000

login : c2ic

password : c2ic

Note : Pour sortir de la console virsh, utiliser les touches Ctrl+5. Ne pas utiliser le pavé numérique.

Se reporter ensuite au paragraphe Configuration des interfaces réseau par le User menu**.**

1.3.1.3 Dans un environnement HyperV & Azure

- Récupérer le ZIP compatible HyperV & Azure et y extraire le fichier disque .vhd
- Envoyer dans le cloud Azure le fichier disque .vhd en utilisant une des méthodes documentées par Microsoft Azure :
  - Microsoft Azure Storage Explorer,
  - PowerShell et AzCopy.
- Depuis le portal Azure créer la VM grâce au fichier disque :
  - Se référer à la documentation pour le dimensionnement CPU/mémoire.

Se reporter ensuite au paragraphe Configuration des interfaces réseau par le User menu**.**

1.3.2 CONFIGURATION DES INTERFACES RÉSEAU PAR LE USER MENU

Lancer la commande :

/opt/a5000/infra/utils/bin/utd/usermenu.sh

Le menu de configuration est alors lancé. Répondre aux différentes questions comme indiqué ci-dessous :

```
CONFIGURATION
YOU CAN ACCESS THE MIVOICE 5000 SERVER FROM HTTPS://
1) REBOOT             6)  STANDARD             11) KEYBOARD
2) NETWORK            7)  BACKUP-SPECIFIC      12) LANGUAGE
3) FIREWALL           8)  RESTORE-SPECIFIC     13) LOGOUT
4) PASSWORD           9)  IDENTIFICATION
5) UPDATEOS-SECURITY  10) CONFIG-RESET
SELECT AN OPTION AND PRESS ENTER: 2 ---------------> (TAPER 2)

NETWORK CONFIGURATION MENU
1) IP-ADDRESS         3)  DNS                  5)  BRIDGE
2) ROUTES             4)  HOSTNAME             6)  QUIT
NETWORK - SELECT MENU : 1 ---------------> (TAPER 1)

CURRENT CONFIGURATION
LANA=192.168.1.101/24
LANB=
```

Configuration de LANA (et éventuellement LANA2 ou LANB pour les services SBC)

```
CONFIGURE NETWORK
1) LANA
2) LANA2
3) LANB
4) LANC
5) QUIT
SELECT INTERFACE : 1----------------> (TAPER 1 POUR LANA)
```

Note : L'interface LANA2 correspond à l'adresse virtuelle de l'interface LANA.

```
CONFIGURING LANA
IP ADDRESS [Y] ? 10.10.10.10 ---------> (RENSEIGNER L'ADRESSE IP
 CONSIDÉRÉE)
NETMASK [Y] ? 255.255.255.0 ----------->(RENSEIGNER LE MASQUE CONSIDÉRÉE)
APPLY Y/N [N] ? Y
```

Taper **Return** pour confirmer

Le script est lancé.

A la fin, le menu suivant est affiché (après avoir taper **Return**) :

```
SELECT INTERFACE :
1) LANA
2) LANA2
3) LANB
4) LANC
5) QUIT
SELECT INTERFACE : 3 ----------------> (TAPER 3 POUR QUITTER)
```

Note : Dans le cas où l'interface LANB doit être configurée, sélectionner 2) LANB pour la configurer en suivant la même procédure que pour LANA. Cette configuration peut éventuellement être effectuée ultérieurement.

Configuration de la passerelle par défaut (LANA)

À partir de l'écran précédent :

```
NETWORK CONFIGURATION MENU

NETWORK - SELECT MENU :
1) IP-ADDRESS          3) DNS                          5) BRIDGE
2) ROUTES              4) HOSTNAME                6) QUIT
NETWORK - SELECT MENU : 2 ---> (TAPER 2 POUR ACCEDER A MENU DE CONFIGURATION DE LA
 PASSERELLE)

ROUTE CONFIGURATION MENU
1) SHOW                3)ADD                       5) APPLY
2) DEFAULTGW           4)DELETE                   6) QUIT
ROUTES - SELECT MENU : 2 ---> (TAPER 2 MENU DE CONFIGURATION DE LA PASSERELLE)

ENTER DEFAULT GATEWAY : 10.10.10.1

1) LANA
2) LANB
SELECT INTERFACE : 1----------------> (TAPER 1 POUR LANA)

ROUTES SELECT MENU
```

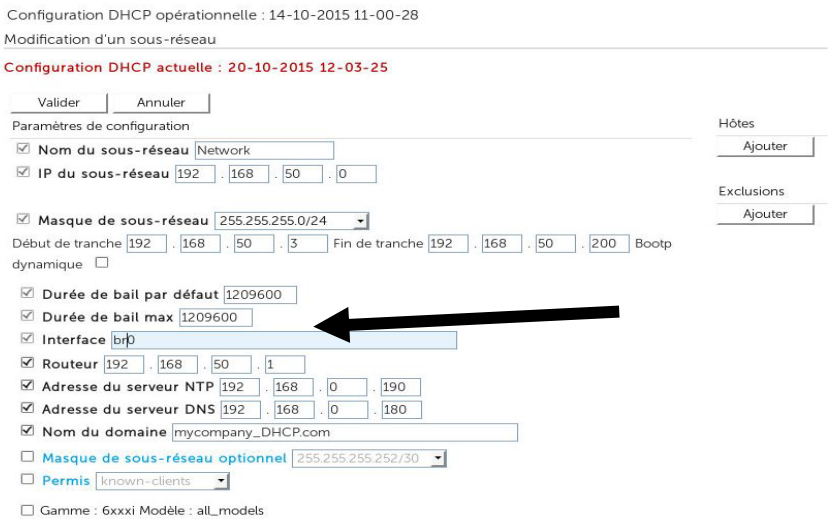
```
1) SHOW                3)ADD                    5) APPLY
2) DEFAULTGW           4)DELETE                 6) QUIT
ROUTES - SELECT MENU : 5 ---> (TAPER 5 POUR CONFIRMER)

LE SYSTÈME REDÉMARRE
RESTARTING NETWORK (VIA SYSTEMCTL) : [OK]

ROUTES SELECT MENU
1) SHOW                3)ADD                    5) APPLY
2) DEFAULTGW           4)DELETE                 6) QUIT
ROUTES - SELECT MENU : 6 ---> (TAPER 6 POUR QUITTER)

NETWORK CONFIGURATION MENU

1) IP-ADDRESS  3) DNS       5) BRIDGE
2) ROUTES      4) HOSTNAME  6) QUIT
NETWORK - SELECT MENU : 6 ---------------> (TAPER 6 POUR QUITTER)
```

Le menu principal est réaffiché.

Contrôle et modification de la configuration du DHCP

Pour la procédure détaillée, se référer au paragraphe Modification de la configuration du serveur DHCP à partir de Web Admin**.**

Dans le menu **DHCP - Exploitation "- Modification d'un sous-réseau :** L'interface **eth0** doit être remplacée par **br0**).



1.3.3 INSTALLATION SUR UN SYSTÈME VIRTUALISÉ VIA L'OUTIL D'INSTALLATION RAPIDE

La procédure d'installation via l'outil d'installation rapide est la même que pour les systèmes non virtualisés.

Se référer au paragraphe **1.2.2 – Installation sur un système non virtualisé via l'outil d'installation rapide**.

1.4 ACCÈS À L'INTERFACE D'EXPLOITATION (WEB ADMIN)

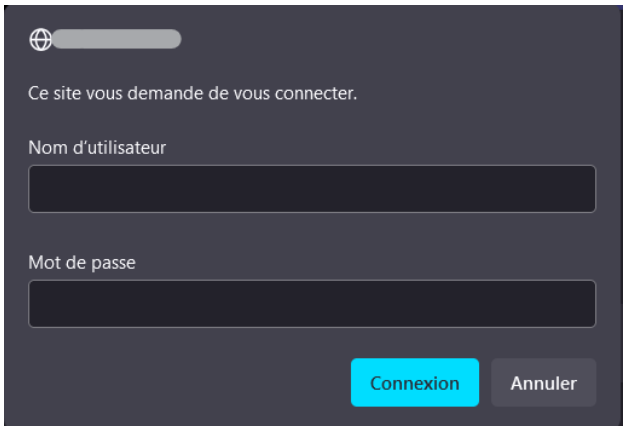
La console d'exploitation est reliée au même réseau que l'iPBX (port LAN de la carte mère).

- Accéder au navigateur Web installé sur la console d'exploitation (Internet Explorer par exemple),
- Entrer l'adresse IP définie pour le système : https://@IP (mode d'accès sécurisé).

Note : Adresse définie lors l'installation de l'OS correspondant à l'adresse IP de la carte réseau du MiVoice 5000 Server.

- Des fenêtres relatives à la sécurité concernant ce mode d'accès "**https**" sont ensuite successivement affichées, répondre "**OUI**" dans chacune d'elles,
- Le navigateur Web (cas de Internet Explorer) affiche une alerte de sécurité lors de la connexion à la Web Admin, cette alerte peut être désactivée Se référer à l'annexe de ce document paragraphe Prise en compte du Certificat de sécurité

Une fenêtre de Login est affichée,



- Entrer le login d'accès par défaut : **admin**
- Entrer le Mot de passe d'accès par défaut : **admin**

Politique de mot de passe et changement immédiat de Mot de passe

Lors de la première connexion :

Le mot de passe par défaut est celui attribué par l'administrateur. Cette valeur doit être immédiatement modifiée et personnalisée par l'utilisateur si l'administrateur à activer une politique de mot de passe. Se référer au document MiVoice 5000 Server - Manuel Exploitation.

Ultérieurement :

L'utilisateur pourra également le changer, à partir de la page d'accueil dans le menu à gauche **Modification du mot de passe** (si la politique est activée).

En cas d'expiration, un message signalera l'obligation de le changer (si la politique est activée).

Toutefois en cas d'oubli de ce mot de passe, l'utilisateur doit recontacter l'administrateur

Une fois l'identification réalisée, l'écran d'accueil de la Web Admin est affiché.

Lors de la première connexion, l'écran d'accueil comporte une page d'avertissement sur les risques de piratage et les contraintes de sécurité :

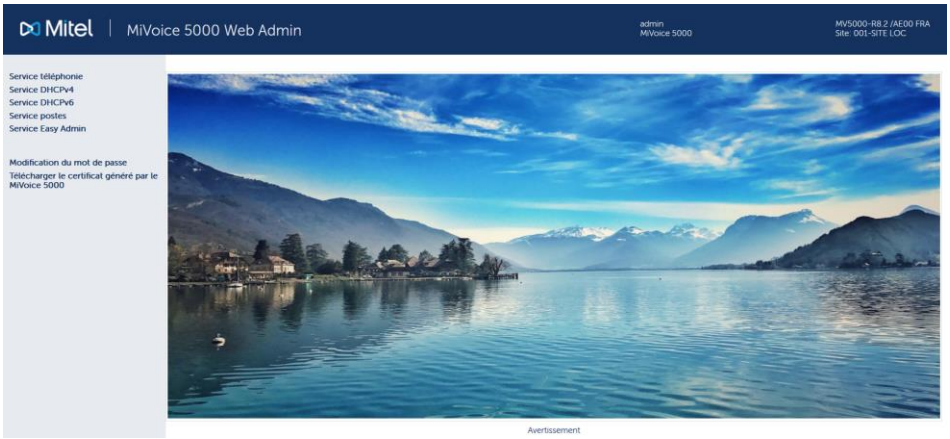
Une fois avoir pris connaissance de ce message,

Cliquer sur un des boutons **Avertissement**,

Dans l'écran suivant rappelant ce message, cocher la case **J'ai pris connaissance de ce texte**,

Cliquer sur **OK** pour confirmer,

L'écran d'accueil de la Web Admin proprement dit est alors affiché permettant d'accéder à l'ensemble des menus :



Pour plus de détails sur l'affichage de ce message d'avertissement, se reporter au paragraphe Avertissement légal MITEL pour l'accès à la Web Admin.

Menu **Télécharger le certificat**

Ce menu est un lien pour le téléchargement du certificat autosigné SHA2 fourni par Mitel.

Le certificat permet de sécuriser la connexion entre les interfaces la Web Admin et le User Portal avec le MiVoice Manager notamment.

Le certificat affecté peut être également externe.

La gestion et l'affectation des certificats est réalisée à partir du Menu **SYSTEME>Sécurité**.

Se référer aux documents suivants dans les chapitres relatifs aux aspects Sécurité/Certificats :

- MiVoice 5000 Server - Manuel d'Exploitation
- MiVoice 5000 Manager Guide Utilisateur

Ce lien apparait systématiquement lors d'une première installation ou suite à une migration vers R8.X pour des sites ou nœuds (Configuration Cluster) dont la version initiale est inférieure à R8.X.

Ce lien n'apparait plus si un certificat (SHA2 Mitel ou externe) a été téléchargé dans l'iPBX soit en local soit à partir du MiVoice 5000 Manager.

1.5 DÉCLARATION DES LICENCES POUR MIVOICE 5000 SERVER VIRTUALISÉ OU PHYSIQUE

À partir de la version R5.2 SP1, Le MiVoice 5000 Server peut être virtualisé. Dans ce cas, le dongle est également virtuel et est livré avec le package du MiVoice 5000 Server.

Pour une première installation, la licence n'est pas obtenue directement et dépend d'un code d'installation à générer à partir de la Web Admin.

Ce code d'installation est propre à chaque iPBX.

Il doit être généré dans un premier temps par l'installateur (à partir de la Web Admin).

Ce code ayant été généré, deux modes d'obtention de la licence sont proposés :

- **Mode automatique** (à partir de R5.3 SP1 minimum), permettant un accès direct et automatique au serveur de licence qui fournit en retour et en temps réel, les licences,
- **Mode manuel**, en se connectant manuellement au serveur de licence Mitel. Le code d'installation peut être regénéré à dans les conditions indiquées au paragraphe 1.5.3 - Précautions d'emploi.

1.5.1 MODE AUTOMATIQUE

A partir de R5.3 SP1, un nouveau mode de connexion direct au serveur de licence Mitel est proposé par le bouton **Obtention clé de déverrouillage**, dans le menu T**ELEPHONIE>SYSTEME>Info>Licences**, afin de récupérer de manière automatique la clé de licence, associée au code d'installation, directement dans l'iPBX.

Le principe est de récupérer automatiquement la clé de licence associée à une installation MiVoice 5000 Server virtualisé, via une requête http sur le serveur Mitel SLS.

La licence est automatiquement prise en compte par l'IPBX et les fonctions considérées sont déverrouillées et visualisables dans dans le menu T**ELEPHONIE>SYSTEME>Info>Licences**.

Ce mode n'est utilisable que si le MiVoice 5000 Server virtualisé dispose d'un accès à Internet, associé à une résolution DNS correcte.

Pour tous les installateurs qui souhaitent isoler leur réseau du réseau Internet, le mode manuel est à appliquer. Se référer au paragraphe 1.5.2 – Mode Manuel**.**

Procédure d'obtention des licences en mode Automatique

Dans le Menu **TELEPHONIE>SYSTEME>Info>Licences,** renseigner successivement :

- Le Numero d'identification,
- Adresse IP de la machine virtuelle,
- Numéro NDI de l'installation.

IMPORTANT : Tous ces champs doivent être impérativement renseignés.

Le numéro NDI saisi pour définir le code d'installation d'un MiVoice 5000 Server contient le numéro d'un accueil ou d'un abonné dans le format transmis par l'opérateur (avant transformation).

Note : Ce champ doit être préfixé avec des 0 lorsqu'il contient moins de 8 chiffres.

- Cliquer ensuite sur le bouton **Generation code d'installation**,

Le cadre code d'installation indique alors la valeur du code d'installation,

- Cliquer sur le bouton Obtention clé de déverrouillage,

La connexion au serveur de licence est alors effectuée automatiquement et quelques instants après, les licences sont reçues et prises en compte par l'iPBX.

Effectuer ensuite un rafraichissement (Bouton **Actualiser** ou **F5**) de la fenêtre du navigateur. Les licences considérées sont alors dans l'état **AUTORISE** dans le tableau correspondant.

Si, ultérieurement, les caractéristiques du système Adresse IP et Numero NDI sont modifiées, le code d'installation sera à regénérer en se référant au paragraphe Précautions d'emploi.

1.5.2 MODE MANUEL

Note : Utiliser de préférence Internet Explorer pour accéder à la Web Admin ; Ceci permettra plus facilement de recopier les valeurs demandées pour générer la licence. Voir ci-après Code installation.

Dans le Menu **TELEPHONIE>SYSTEME>Info>Licences,** Renseigner successivement :

- Le Numero d'identification,
- Adresse IP de la machine virtuelle,
- Numéro NDI de l'installation.

IMPORTANT : Tous ces champs doivent être impérativement renseignés.

Le numéro NDI saisi pour définir le code d'installation d'un MiVoice 5000 Server contient le numéro d'un accueil ou d'un abonné dans le format transmis par l'opérateur (avant transformation).

Note : Ce champ doit être préfixé avec des 0 lorsqu'il contient moins de 8 chiffres.

- Cliquer sur le bouton **Generation code d'installation**,

Le cadre code d'installation indique alors la valeur du code d'installation,

- Dans un nouvel onglet, se connecter au serveur de licence SLS via le lien **https://sls.mitel.com/sls/**,
- Dans le champ **EID / Serial**, rechercher le système par son ID,
- Dans le menu **Activate Product**, saisir le code d'installation pour générer la licence**.**

En retournant dans le même menu, **TELEPHONIE>SYSTEME>Info>Licences**,

- Entrer cette licence dans le champ **cle de déverrouillage** de ce même menu,

Les fonctions considérées sont alors autorisées.

Il est conseillé de conserver cette valeur de licence dans un fichier texte.

Si, ultérieurement, les caractéristiques du système Adresse IP et Numero NDI sont modifiées, le code d'installation sera à régénérer en se référant au paragraphe Précautions d'emploi.

1.5.3 PRÉCAUTIONS D'EMPLOI

Le code d'installation est par définition unique et la clé de déverrouillage générée ne peut donc fonctionner qu'avec un code d'installation.

Si un code d'installation est généré sans obtenir de nouvelle clé de déverrouillage, les fonctions soumises à licence seront fermées dans l'heure qui suit.

Pour permettre de gérer différents cas nécessitants un changement de code d'installation pendant la vie du système et notamment les cas se présentant en astreinte 24/7, il est dorénavant possible de changer de code d'installation sans demande préalable à Mitel.

Suite à ce changement, vous n'aurez plus droits à modification et vous devez impérativement contacter pour justifier les raisons de ce changement (modification opérateur, remplacement physique de la plateforme, modification réseau…).

Après analyse de votre demande, vous serez de nouveau autorisé à modifier le code d'installation.

Lors d'une consultation sur le serveur de licence ("rechercher une clé"), le droit à modifier le code d'installation sur le numéro d'identification concerné est indiqué via les informations suivantes :

- Modification du code d'installation **autorisée**
- Modification du code d'installation **non autorisée**

1.6 RÉINITIALISATION DU CODE D'ACCÈS CONSTRUCTEUR

Contacter le support technique de Mitel.

1.7 IMPORT DES DONNÉES DANS L'IPBX À PARTIR DU FORMULAIRE DE COLLECTE DES DONNÉES

Avant l'import des données, l'administrateur devra effectuer une sauvegarde de la configuration de l'iPBX de façon à pouvoir la restaurer dans le cas où un ou des fichiers .csv n'étaient pas correctement configurés.

L'import des données dans l'IPBX se fait par Web Admin depuis les menus **Service téléphonie**, **Système**>**Maintenance logicielle**>**Import massif** :

- Sélectionner et télécharger le fichier Data.Collecting.zip
- Cliquer sur Prise en compte des données.

La durée de l'import dépend de la quantité de données à télécharger. Des compteurs s'affichent pour indiquer la progression du travail.

- Exemple compteur 12/38 : 15
  - 38 : nombre de fichiers à importer,
  - 12 : numéro du fichier en cours d'import,
  - 15 : ligne traitée dans le fichier en cours d'import.

Un rapport d'installation est généré à la fin de l'import.

1.7.1 RAPPEL DU PRINCIPE

Le formulaire de collecte de donnée contient un onglet spécifique relatif aux paramètres de configuration nécessaire à la phase de Ctrl + i.

Une fois avoir généré les données iPBX, les fichiers suivants sont créés :

- Un fichier DataCollecting.zip contenant les différents fichiers .csv issus de la collecte et utilisés par la Web Admin (exemple : 002.Mitel.DataCollecting.zip).
- Un fichier 7450_Formulaire.xls (version Excel 2003) à importer dans MiVoice 5000 Manager. Il contient les données nécessaires à la configuration des comptes UCP et TWP.

Les fichiers générés sont placés dans le même répertoire que celui où est installé le formulaire.

Des informations supplémentaires sont fournies dans le fichier Excel de collecte de données - onglet Aide.

1.8 CONFIGURATIONS COMPLÉMENTAIRES

1.8.1 DÉMARRAGE ET CONSULTATION DES SERVICES

Le démarrage des services (LDAP, SNMP, GSI, FTP, TFTP, etc.) et la consultation de leur état est à réaliser en utilisant le Menu **SYSTEME>Configuration>Services** de la Web Admin. Se reporter au document MiVoice 5000 Server – Manuel Exploitation.

1.8.2 DÉCLARATION D'UN SERVEUR DE TEMPS NTP

La synchronisation sur un serveur de temps NTP peut s'avérer nécessaire notamment pour certains types de postes.

L'adresse et l'activation du serveur NTP est à effectuer dans le menu "**Système>Administration>Date et heure**" en sélectionnant l'onglet "**Protocole de synchronisation à un serveur de temps**".

2 MISE À JOUR DU LOGICIEL D’UN MIVOICE 5000 SERVER SIMPLEX OU DUPLEX

La méthode de mise à jour du logiciel est exclusivement la méthode par Repository quel que soit le système, avec ou sans MiVoice 5000 Manager.

Se référer au document **Mise à jour par Repository**.

3 CAS DE MISE À JOUR DE VERSIONS < À R8.X VERS R8.2 OU VERSION POSTÉRIEURE

Une procédure de migration vers R8.2 ou version postérieure est obligatoire pour tout système virtuel ou physique dont la version est < à R8.x.

Se référer au document • **MiVoice 5000 Server/Manager, EX Controller et Mitel 5000 Compact Server - Migration vers R8.2+**.

4 ANNEXES

4.1 MONTAGE D'UNE IMAGE ISO

Le point de montage doit exister.

- Entrer les commandes suivantes :

mkdir /mnt/iso

- Copier iso sous /tmp

mount /tmp/CD** /mnt/iso**

4.2 PRISE EN COMPTE DU CERTIFICAT DE SÉCURITÉ

Lors du premier accès à la Web Admin via un navigateur Web (cas de Internet Explorer), une alerte de sécurité est affichée.

Il faut donc indiquer au navigateur Web que l'entreprise est une autorité de certification fiable.

Note : En cas de problème d'accès à Web Admin ou lors d'une réinstallation de certificat, supprimer les certificats précédemment installés sur le poste Client pour cet iPBX.

Dans le cas où, le certificat pour sécuriser les interfaces Administration (accès à la Web Admin) ou End User (accès au User Portal) est généré par le MiVoice 5000, il est impératif d'utiliser le lien **Télécharger le certificat généré par MiVoice 5000** (Page d'accueil Web Admin) pour obtenir ce certificat afin de l'installer sur les PC qui accèdent à l'une de ces deux fonctions (Se référer au paragraphe suivant).

Gestion des certificats avec les navigateurs

Le certificat doit être rajouté manuellement dans Firefox. Pour les autres navigateurs, utiliser le gestionnaire de certificat de Microsoft :

Cliquez sur **Démarrer**, puis dans le champ de recherche, tapez **mmc** et appuyez sur **Entrée**.

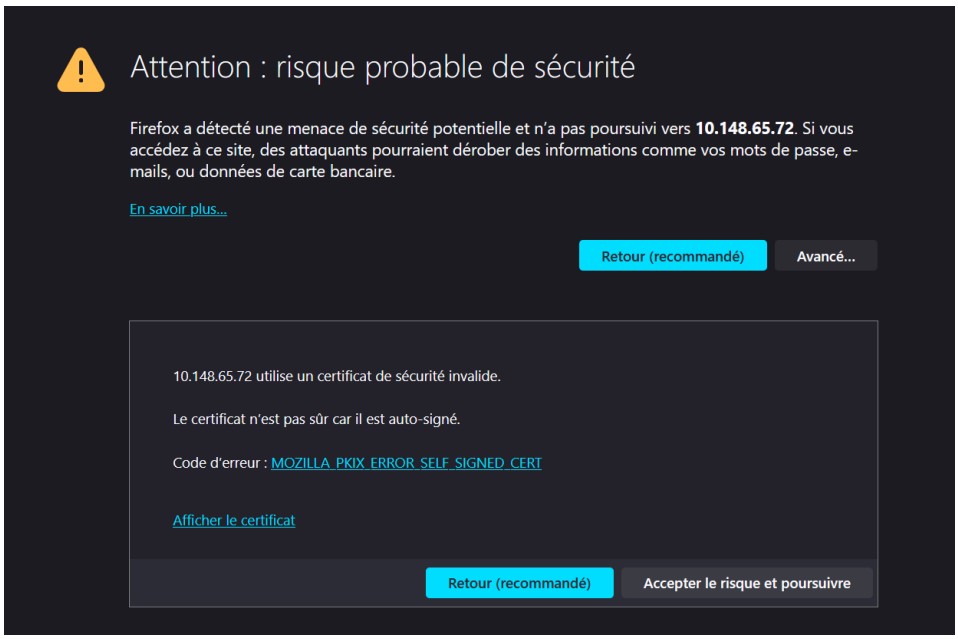
L'écran de gestion est affiché.

4.2.1 POUR LA GAMME MITEL 5000

- Accéder au navigateur Web installé sur la console d'exploitation (Internet Explorer par exemple),
- Entrer l'adresse IP définie pour le système : https://@IP (mode d'accès sécurisé)

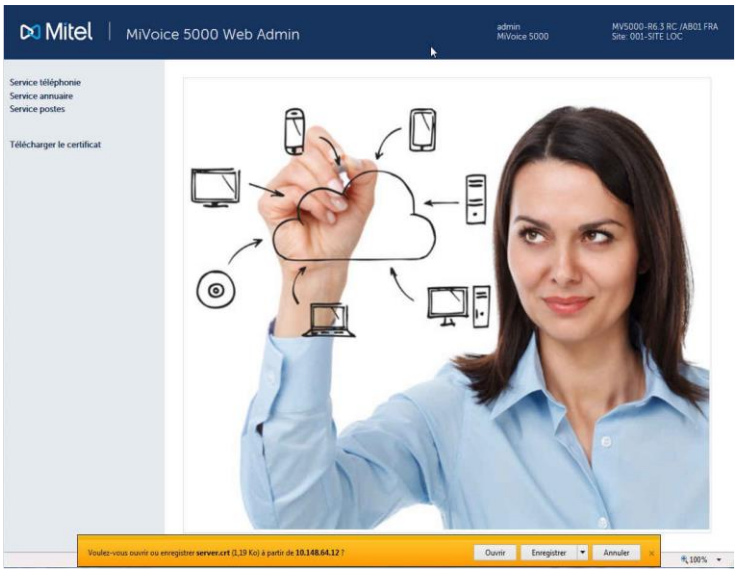
Note : Adresse par défaut en configuration usine : 192.168.65.01

- Un message d'avertissement comme ci-dessous peut suivre après l'entrée de l'adresse :

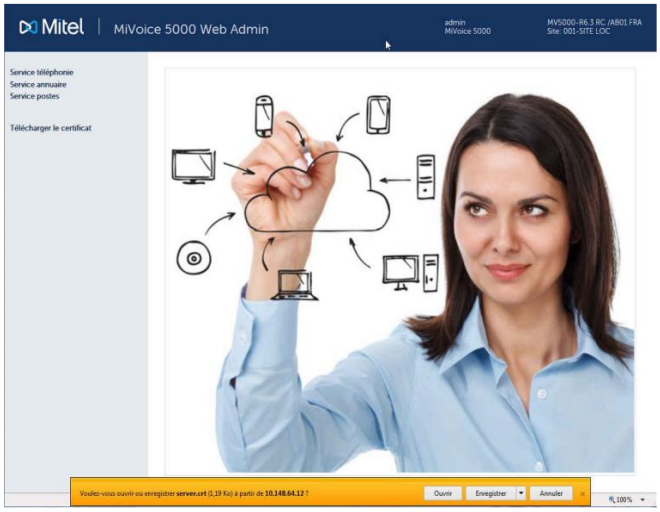


Le message change en fonction du navigateur utilisé.

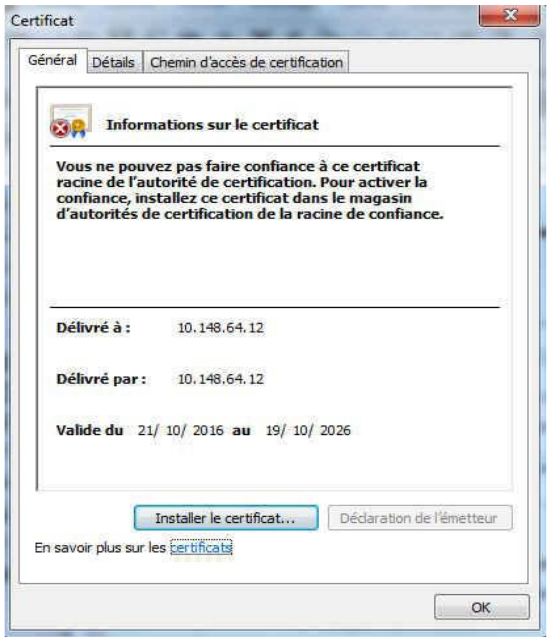
- Cliquer sur le bouton pour poursuivre sur le site,



- Cliquer dans les menus à gauche sur **Télécharger le certificat**,

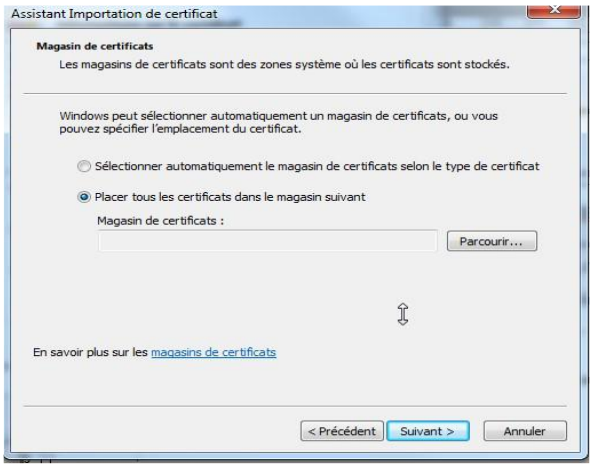


- Cliquer sur **Ouvrir** dans le bandeau affiché en bas,
- Dans l’écran suivant, dans l’onglet **Général**, cliquer sur **Afficher le certificat**,



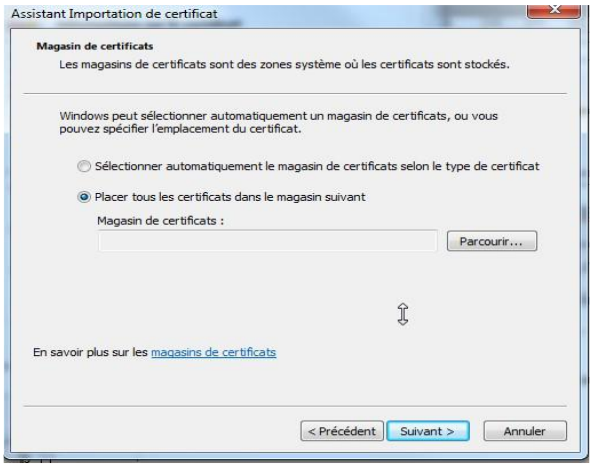
- Cliquer sur Installer le certificat,
- Cliquer sur **Suivant**,

- Cocher la ligne Placer tous les certificats dans le magasin suivant et cliquer sur Suivant,

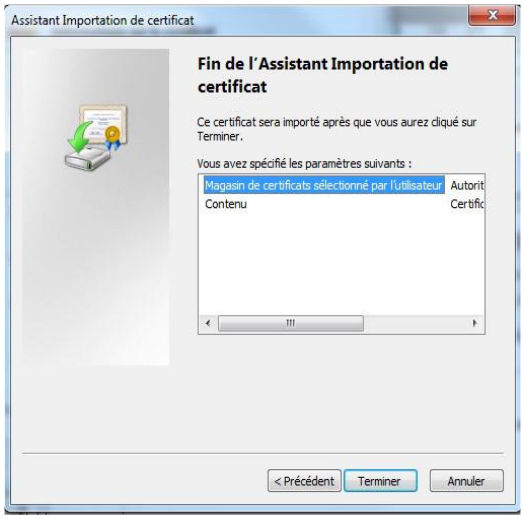


- Sélectionner Autorités de certification racines de confiance et cliquer sur OK,

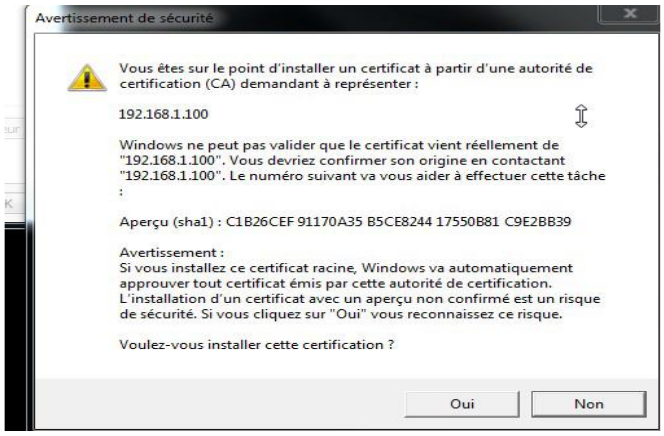
- Cliquer sur **Suivant**,



- Cliquer sur **Terminer**,



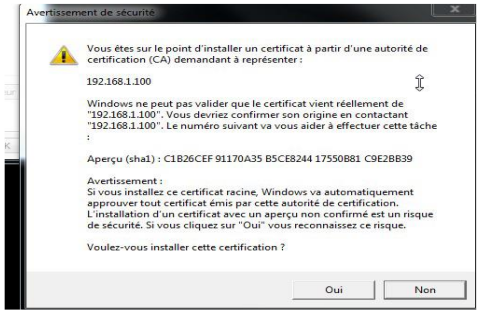
Un avertissement de sécurité est ensuite affiché,



- Cliquer sur **OUI**,

Le certificat est installé.

- Cliquer sur **OK,**



L'installation est terminée.

- Fermer toutes les fenêtres du navigateur,
- Se reconnecter à Web Admin en https://@IP. L’alerte de sécurité n’est plus présentée.

4.3 AVERTISSEMENT LÉGAL MITEL POUR L'ACCÈS À LA WEB ADMIN

Afin d'alerter les exploitants de sites sur les risques de piratage et les contraintes de sécurité, un message d'avertissement à destination des différents opérateurs est affiché au niveau de Web Admin

Ce message est affiché lors de la première connexion à Web Admin ou reste accessible ensuite sous forme de lien s'il n'a pas encore été validé.

Le mode de fonctionnement est le suivant :

Tant qu'un opérateur n'a pas validé le message celui-ci est affiché sur la page d'accueil, un lien permet alors d'afficher la page de validation.

Ce lien (Bouton **Avertissement**) est signalé de manière visible en rouge dans toutes les pages du site en haut à gauche

Dès lors qu'un opérateur a validé ce message, la photo traditionnellement affichée sur la page d'accueil retrouve sa place et seul un lien en bas de la page d'accueil de Web Admin permet de consulter de nouveau ce message.

Page d'accueil avant validation

Si le message d'avertissement n'a pas été validé, la page d'accueil est la suivante :

Deux liens sont disponibles pour appeler et afficher la page de validation de l'avertissement. Tout d'abord dans le haut gauche de la page le texte **Avertissement** sur fond rouge est un premier lien. Le second se situe en bas représenté par le texte **Avertissement**.

Dans les autres pages du site et tant que le message n'a pas été validé un lien **Avertissement** reste affiché dans le haut gauche de la page sur un fond rouge.

Page de validation du message d'avertissement

Dans cette page le lien "Accueil Web Admin" en haut à gauche permet de revenir à la page d'accueil sans valider le message.

Pour valider le message, cocher la case située en dessous du message d'avertissement puis d'appuyer sur le bouton **OK** se trouvant à côté de la case cochée.

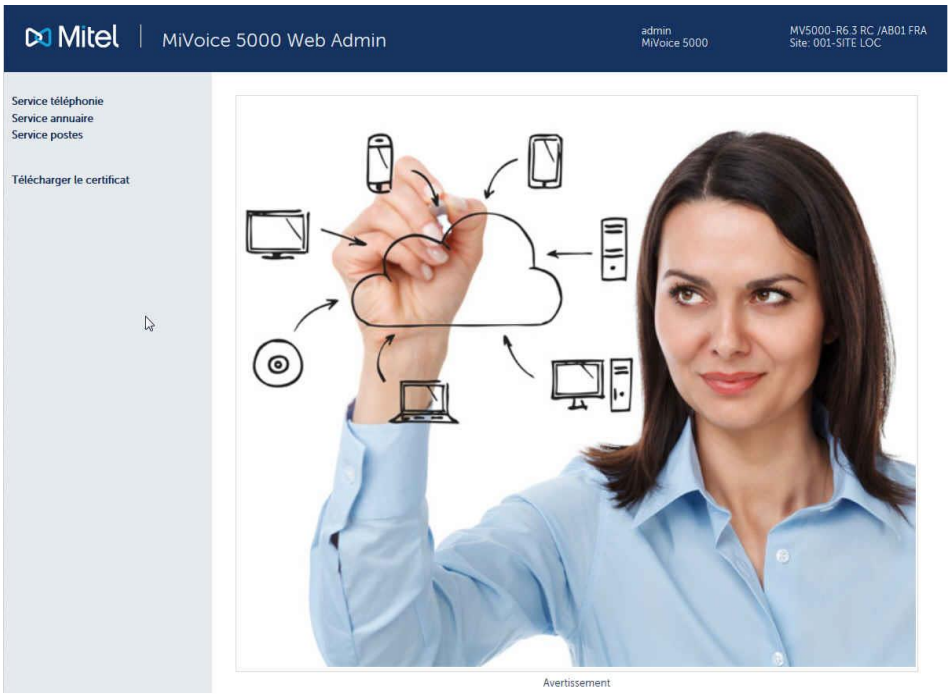
Le login de la personne qui valide l'avertissement ainsi que la date de validation sont mémorisés par le système.

Si la case **J'ai pris connaissance de ce texte** n'est pas cochée, l'appui sur le bouton **OK** ne provoque aucune action.

La validation de l'avertissement est autorisée avant l'expiration de la temporisation de libération console (de base à 10 minutes). Après expiration de cette temporisation la fenêtre de Login est affichée et l'opérateur est automatiquement redirigé vers la page d'accueil de la Web Admin (le login/mot de passe dépend du compte loggé).

Pages de Web Admin après validation

Dans cette page, seul le lien **Avertissement** situé sous la photo permet d'aller dans la page qui affiche l'avertissement.



Dans les autres pages du site, plus aucun lien ne permet d'afficher l'avertissement.

Page de consultation de l'avertissement après validation

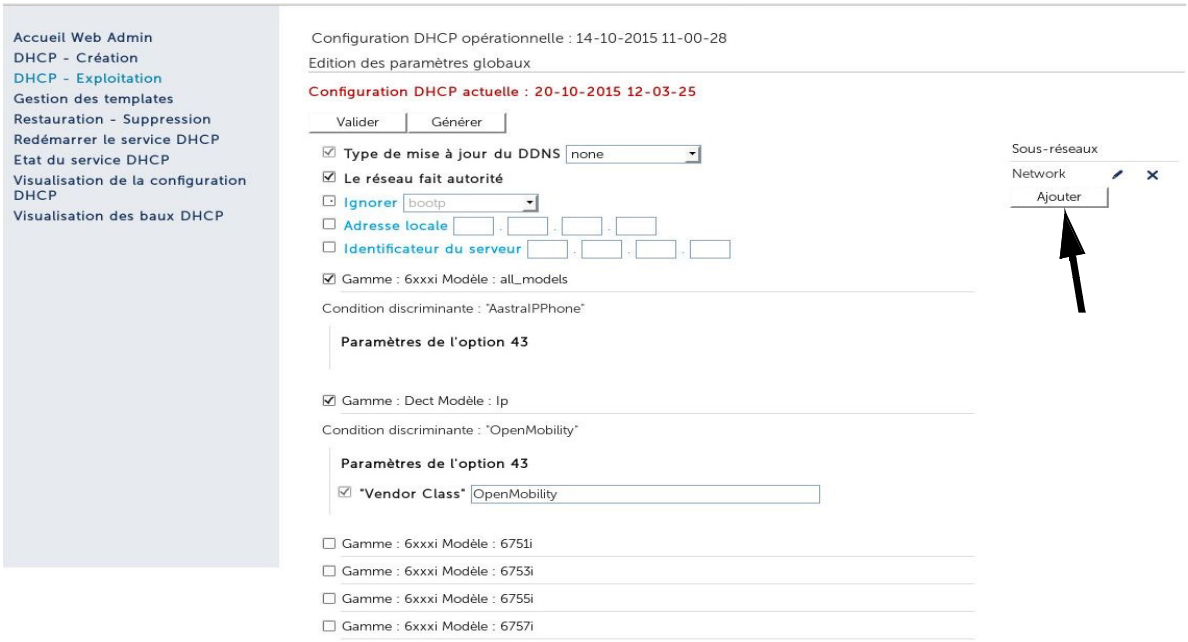
Cette page qui n'offre plus la possibilité de valider l'avertissement offre un seul lien **Accueil** Web Admin permettant de revenir à la page d'accueil du Web Admin.

4.4 MODIFICATION DE LA CONFIGURATION DU SERVEUR DHCP À PARTIR DE WEB ADMIN

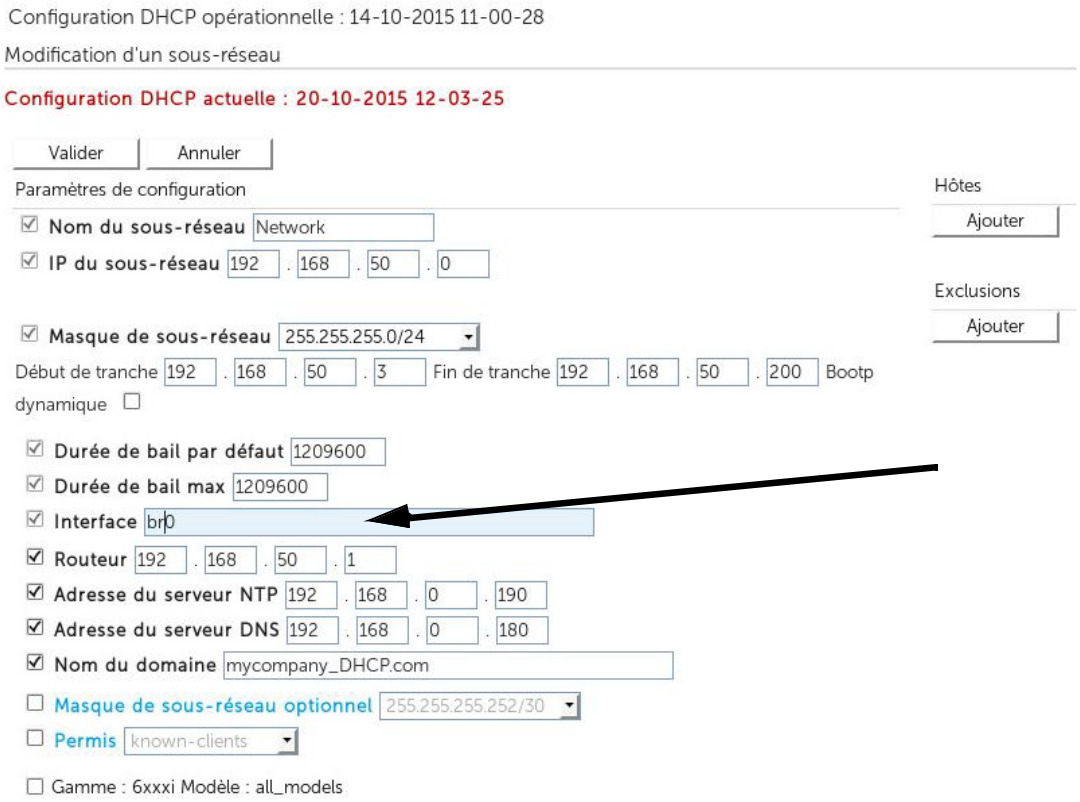
La modification de la configuration du serveur DHCP est nécessaire notamment lorsque l'interface réseau utilisée n'est pas nommé eth0 mais nommée avec autre nom défini pour l'interface réseau de ce serveur.

La modification s'effectue en 5 étapes :

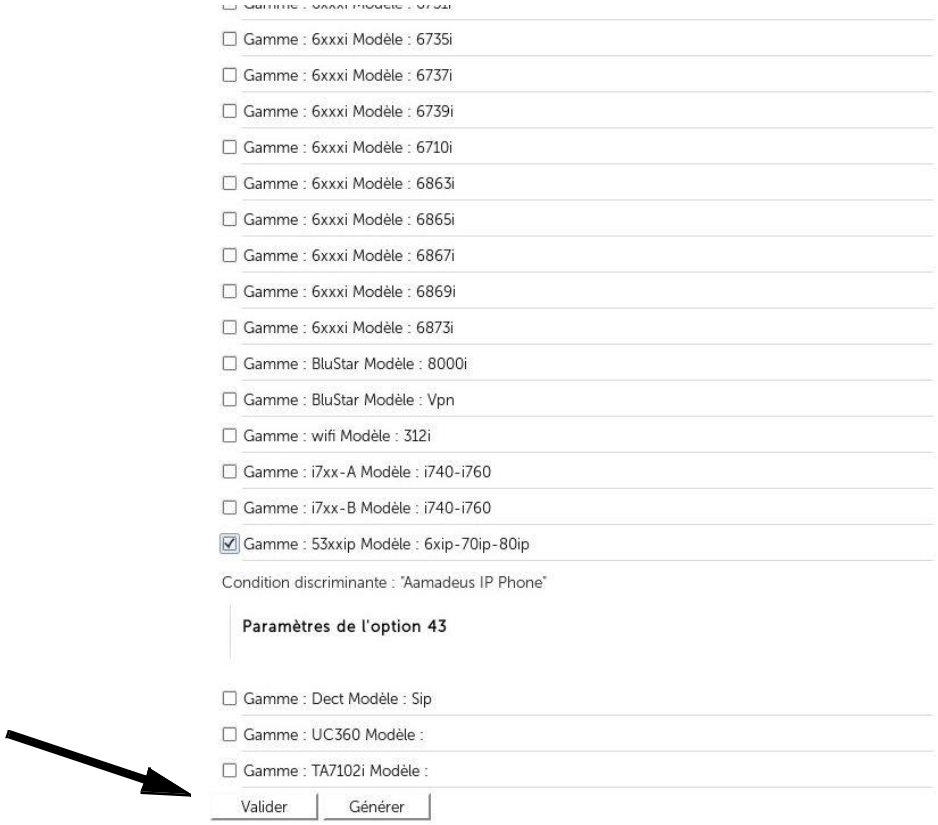
Etape 1 : Menu "**DHCP - Exploitation**" : demander la modification des sous-réseaux (crayon "**network**")



Etape 2 : Menu "**DHCP - Exploitation" - Modification d'un sous-réseau :** Corriger le nom de l'interface ("**eth0**"), à remplacer par le nom défini sur la machine serveur ("**em1**" ou "**br0**" par exemple).

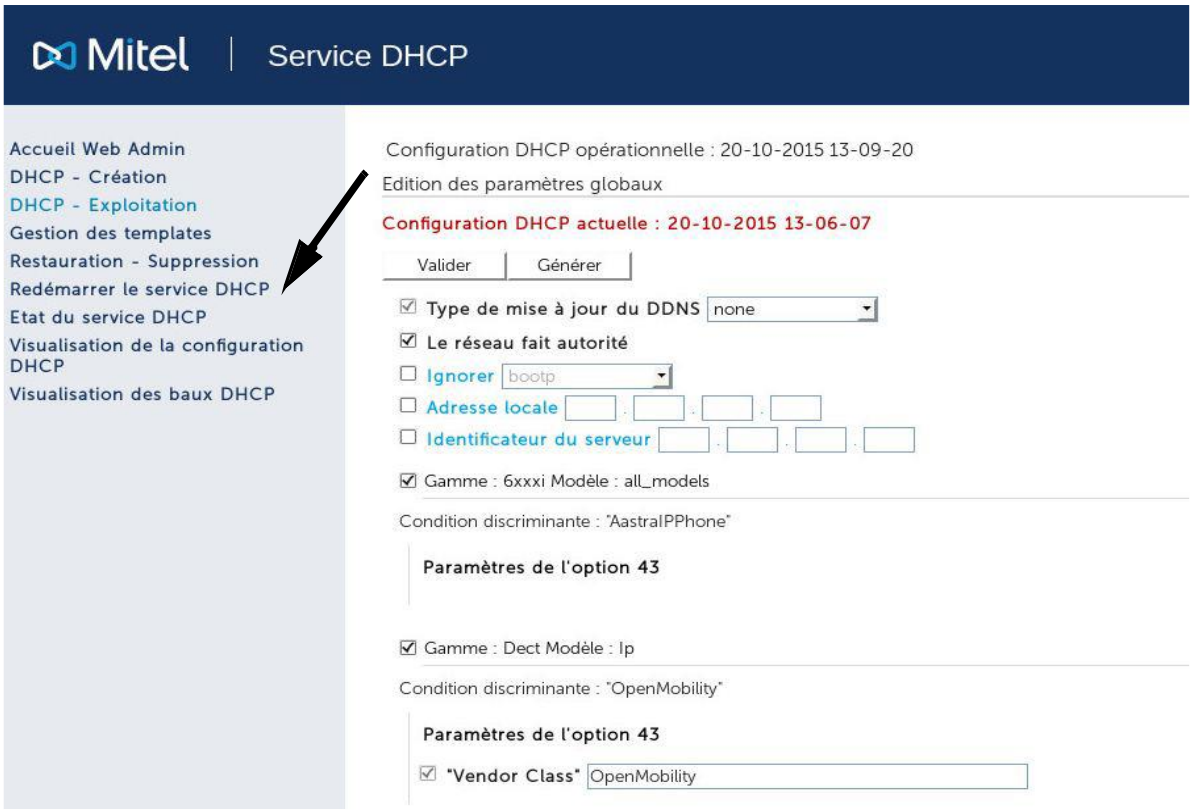


Etape 3 : Menu "**DHCP - Exploitation" - Modification d'un sous-réseau** : Valider la modification en bas ou en haut de la page.


Gamme : 6xxxi Modèle : 6735i
Gamme : 6xxxi Modèle : 6737i
Gamme : 6xxxi Modèle : 6739i
Gamme : 6xxxi Modèle : 6710i
Gamme : 6xxxi Modèle : 6863i
Gamme : 6xxxi Modèle : 6865i
Gamme : 6xxxi Modèle : 6867i
Gamme : 6xxxi Modèle : 6869i
Gamme : 6xxxi Modèle : 6873i
Gamme : BluStar Modèle : 8000i
Gamme : BluStar Modèle : Vpn
Gamme : wifi Modèle : 312i
Gamme : i7xx-A Modèle : i740-i760
Gamme : i7xx-B Modèle : i740-i760
Gamme : 53xxip Modèle : 6xip-70ip-80ip
Condition discriminante : "Aamadeus IP Phone"
Paramètres de l'option 43
Gamme : Dect Modèle : Sip
Gamme : UC360 Modèle :
Gamme : TA7102i Modèle :
Valider
Générer

Etape 4 : Menu "**DHCP - Exploitation**" Demander la re-génération de la configuration DHCP en bas ou en haut de la page. Bouton **Générer**.

Etape 5 : Redémarrer le service DHCP.


Mitel
Service DHCP
Accueil Web Admin
DHCP - Création
DHCP - Exploitation
Gestion des templates
Restauration - Suppression
Redémarrer le service DHCP
Etat du service DHCP
Visualisation de la configuration DHCP
Visualisation des baux DHCP
Configuration DHCP opérationnelle : 20-10-2015 13-09-20
Edition des paramètres globaux
Configuration DHCP actuelle : 20-10-2015 13-06-07
Valider
Générer
Type de mise à jour du DDNS
none
Le réseau fait autorité
Ignorer
bootp
Adresse locale
Identificateur du serveur
Gamme : 6xxxi Modèle : all_models
Condition discriminante : "AastraIPPhone"
Paramètres de l'option 43
Gamme : Dect Modèle : Ip
Condition discriminante : "OpenMobility"
Paramètres de l'option 43
"Vendor Class"
OpenMobility

4.5 CONFIGURATION DU PARE FEU POUR LE MIVOICE 5000 SERVER

Le tableau qui suit donne la liste des ports à ouvrir pour l'installation du MiVoice 5000 Server.

PROTOCOLE	PORTS	APPLICATION
TCP	3198-3199	i2052, i2070, i7xx
TCP	3209	i2052
TCP	3200 et +	Se référer à la liste dans le tableau ci-après
TCP	21	Téléchargement 675xi/53xxip (FTP)
TCP	69	Téléchargement 675xi/RFP (TFTP)
TCP	443	Transfert de fichiers (AM7450)
TCP	389	LDAP
UDP	40000-40078	i2052, i7XX, 675xi, PTx
UDP	30000-30001	53xxip
UDP	5060	675xi, 53xxip, OMM, RFP
UDP	123	Serveur NTP
UDP	67-68	Serveur DHCP
UDP	161-162	Agent SNMP
UDP	1998, 41000-41999	Tunnel Data
UDP	16320-16391	RFP
UDP	8106-8107	RFP
LDAPS	636	En cas de connexion sécurisée à l'annuaire (TLS).

Complément sur liste des ports TCP utilisés par les serveurs internes du MiVoice 5000 Server.

TCP-IP PORT	INTERNAL SERVER OR SERVER ACCESS	SERVER ADDRESS	MODE	CALL DATA
3200-3203	Reserved			
3204	KTAXE Server (records)	012	Non D	
3205	Reserved			
3206	EAS Server (for LCR and TPS)	013	TPKT	“SAESAE”
3207	Reserved			
3208	H.323 Server (for H.323/MOVACS gateway)	01191	TPKT	
3209	Gateway Server for Attendant Console and Software phone on PC (TD/PC)	01190	TPKT	
3210	Reserved			
3211	CSTA Server	011600	Non D	
3212-3216	Reserved			
3217	MUFACT Server (Record multiplexer with communication records and service records, with alarms)	01410030	TPKT	
3218	EAS Server for ACD (For M7403 for instance)	013	TPKT	
3219	Reserved			
3220-3283	Internal Call Server By the TAPI Gateway		TPKT	
3284-3287	Reserved			
3288	MUFACT Server (Record multiplexer with only service records/alarms)	014130	TPKT	
3289-3290	Reserved			
3291	MUFACT Server (Record multiplexer with only communication records)	014100	TPKT	

4.6 UTILISATION DU FORMULAIRE DE CRÉATION DE MASSE

4.6.1 CONSIDÉRATIONS

Ce paragraphe traite uniquement, à partir du formulaire vierge fourni, de la procédure de création en masse des données suivantes :

- Les fiches externes,
- La programmation de touches pour chaque Abonnement (maximum 64),
- Les numéros secondaires pour les abonnés de type Multi-lignes.

Pour les autres fonctions d'exploitation réalisables à partir de la Web Admin, notamment l'export/import et le traitement associé (mise à jour des caractéristiques technique, modification des fiches annuaire internes, modification des fiches annuaire externes, etc), se référer au document MiVoice 5000 Server – Manuel Exploitation dans les chapitres **Fonction Export et Import massif de données**.

4.6.2 INTRODUCTION

Le formulaire Excel permet la configuration massive des systèmes Mitel 5000 en première installation.

Il est préconisé de conserver un exemplaire original de ce fichier au format Excel.

Ce formulaire de base est composé de 3 onglets permettant respectivement la création en masse des éléments suivants :

- Des fiches externes,
- De la programmation de touches pour chaque Abonnement (maximum 64),
- Des numéros secondaires pour les abonnés de type Multi-lignes.

Chaque onglet est à enregistrer séparément au format **.csv** pour générer de manière unique un seul fichier par rubrique.

Les fichiers générés seront à importer un à un lors de la phase **Import massif** à partir de la Web Admin Menu **Système>Maintenance logicielle>Import massif**.

Les données ainsi générées dans le format **.csv** seront compatibles avec le logiciel des Systèmes Mitel 5000 lors de l'import massif. Ces données pourront être ultérieurement traitées comme tout autre fichier de paramètres par la fonction **Export**.

Dans le cas d'un Multisite, un seul fichier de type **.csv** doit être généré (à partir du formulaire Excel) sur le site de référence annuaire pour réaliser l'import massif.

Cette procédure s'applique dans le cas où il n'y a pas de Centre de Gestion MiVoice 5000 Manager sur l'installation.

4.6.3 STRUCTURE ET CONTENU DU FORMULAIRE EXCEL

4.6.3.1 Ergonomie

Le fichier est composé de trois onglets :

- Onglet Création d'une fiche externe
- Onglet Touches Sélection
- Onglet Multi-lignes

Chaque onglet contient respectivement les champs pouvant être renseignés dans le Menu correspondant dans La Web Admin (dans l'exemple **Menu Creation d'une fiche externe**).

Sur chaque onglet :

- Les cellules de la première ligne (ligne 1) indiquent les libellés des paramètres à exporter en correspondance avec les champs à renseigner dans la Web Admin
- Les cellules de la deuxième ligne (ligne 2) indiquent les codes internes invariants de ces paramètres. Ce sont ces codes qui permettent au logiciel du système MiVoice 5000, dans le menu correspondant, l'interprétation des valeurs à prendre en compte lors de l'import au format **.csv**. Dans l'exemple, ci-dessus, tous les paramètres se réfèrent à la valeur 5030 de la cellule **A2** (Code interne du **Menu Creation d'une fiche externe**).
- Les cellules des lignes suivantes (à partir de la ligne 3) sont à renseigner avec les paramètres relatifs à la création de masse. La prise en compte d'une ligne ne sera effective que si la valeur OUI est entrée dans la cellule **Confirmation** relative à cette même ligne.

ATTENTION : Les deux premières lignes ne doivent en aucun cas être modifiées par l'utilisateur.

4.6.3.2 Règles d'utilisation

Le fichier est construit de manière exhaustive à partir de la base des paramètres disponibles dans la Web Admin (valeurs alphanumériques, choix sur listes, dépendances de certaines familles de données).

Toutes les créations doivent être effectuées dans le format Excel.

Sauvegarder systématiquement la dernière version de ce(s) fichier(s) avant la conversion au format **.csv**.

Pour chaque nouvelle création destinée à un nouvel import massif, utiliser uniquement un formulaire vierge (formulaire de base). Ne pas réutiliser un fichier précédent ayant fait l'objet d'un import massif;

Pour les cellules impliquant un choix sur liste, se référer aux choix proposés dans le menu considéré afin d'en respecter la syntaxe (se référer également aux paragraphes suivants).

Les cellules à renseigner doivent être au format texte pour éviter les changements intempestifs liés au paramétrage par défaut du tableur Excel (010 qui devient 10 dans la colonne F de l'exemple précédent).

En fonction de la configuration du système, certaines colonnes n'ont pas besoin d'être renseignées (Monosociété, caractéristiques de l'abonné, droits, etc.)

Certaines colonnes et les cellules associées sont volontairement masquées dans le formulaire d'origine pour en améliorer l'affichage. Ces champs correspondent à ceux non modifiables à partir des menus de la Web Admin.

Les caractères utilisés doivent être de type Alphanumérique (même syntaxe que pour l'exploitation des systèmes Mitel 5000.

Pour les valeurs qui ne sont pas à modifier lors de l'import, renseigner les cellules correspondantes avec le libellé **#NO_CHANGE#**.

Les paramètres relatifs à la création de masse sont à renseigner dans la langue en cours d'utilisation dans la Web Admin (Exemple : en français OUI, NON, Liste rouge. En anglais YES, NO, red list, etc.).

IMPORTANT : Indiquer OUI dans la colonne Confirmation pour chaque ligne à prendre en compte dans la création de masse (avant l'enregistrement au format .csv). Si ces cellules ne sont pas renseignées, elles ne seront pas prises en compte lors de l'import massif.

4.6.3.3 Enregistrement au format .CSV

Une fois l'onglet renseigné,

- Sélectionner Fichier/Enregistrer sous,
- Nommer le fichier,
- Sélectionner le format "CSV (séparateur : point-virgule) (*.csv)"
- Cliquer sur **Enregistrer**.

Le fichier converti est dès lors disponible pour l'import massif à partir de la Web Admin à partir du Menu **Système>Maintenance logicielle>Import massif**.

Note : Si ce fichier doit être encore modifié avant l'import, lors de la réouverture, certains formats seront perdus notamment les valeurs numériques commençant par 0. Dans ce cas, ces cellules devront être ressaisies comme indiqué précédemment. Suite aux modifications effectuées, vérifier systématiquement la valeur des cellules Confirmation pour chaque ligne.

4.6.3.4 Import et Ouverture d'un fichier CSV sous Excel en fichier texte non tronqué

Certains contenus de cellule peuvent être tronquées lors de l'ouverture directe avec Excel d'un fichier CSV.

Dans ce cas, il est préférable d'utiliser la procédure suivante permettant de spécifier comment l'import du fichier CSV doit être réalisé :

- Ouvrir **Excel** à partir du menu **Démarrer**,
- Ouvrir un fichier vierge,
- Sélectionner l'onglet **Données**,

- Sélectionner le choix sur liste **Données externes** et ensuite **A partir du texte** ou **Fichier texte** (peut varier selon la version d'Excel),
- Rechercher le fichier CSV considéré et cliquer sur **Importer**,
- Dans Assistant Importation de texte, cocher la case Délimité et cliquer sur Suivant,
- Cocher la case **Point-virgule** et cliquer sur **Suivant**,
- Cocher la case **Texte**,
- Cliquer sur **Terminer**,
- Cliquer sur **OK**,

Le fichier est ouvert en mode texte sans troncature.

4.6.4 ONGLET CRÉATION D'UNE FICHE EXTERNE

Pour la correspondance avec les choix et valeurs possibles et leur syntaxe se référer au document MiVoice 5000 Server – Manuel Exploitation.

4.6.5 ONGLET TOUCHES SÉLECTION

Cette partie du formulaire permet la configuration de 5 touches par abonné.

Pour la correspondance avec les choix et valeurs possibles et leur syntaxe se référer au document MiVoice 5000 Server – Manuel Exploitation.

Se référer également à la documentation respective des terminaux pour l'information du nombre de touches programmables.

4.6.6 ONGLET MULTI-LIGNES

Pour la correspondance avec les choix et valeurs possibles et leur syntaxe au document MiVoice 5000 Server – Manuel Exploitation.

4.7 CONFIGURATION DU FIREWALL INTERNE DU MIVOICE 5000

En fonction de la configuration nécessaire, l'installateur peut avoir à modifier le firewall interne du MiVoice 5000.

4.7.1 VIA LE FICHIER IPTABLES.CONF

4.7.1.1 Procédure

Créer un fichier **iptables.conf**, en vérifiant que tous les ports nécessaires soient ouverts. Se référer au paragraphe **4.7.1.2 – Exemple de fichier iptables.conf** pour visualiser le contenu d'un fichier iptables.conf type.

Pour intégrer le nouveau fichier **iptables.conf** :

- Se connecter sur le terminal de Linux en **root**.
- Se rendre dans le répertoire **/tmp/.**
- Copier le nouveau fichier **iptables.conf** dans le dossier **tmp**.
- Entrer la commande **dos2unix iptables.conf** pour convertir le fichier **iptables.conf** vers un format Unix.
- Entrer la commande **iptables-restore iptables.conf** pour appliquer la configuration du document **iptables.conf**.
- Entrer la commande **iptables-save > /etc/sysconfig/iptables** pour enregistrer le nouveau fichier **iptables.conf** dans le répertoire adéquat.
- Entrer la commande **systemctl enable iptables** pour activer **iptables** au lancement du Linux.
- Redémarrer le serveur Linux.

4.7.1.2 Exemple de fichier iptables.conf

```
### SEPARATION DE FLUX

*filter
:INPUT DROP [991:382868]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
:syn-tcp-flood - [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT

## TELEPHONY INTERFACE ##
#DHCP:
-A INPUT -i eth1+ -p udp -m udp --dport 68 -j ACCEPT
#TFTP:
-A INPUT -i eth1+ -p udp -m udp --dport 69 -j ACCEPT
#White pages (<=R7.1) + softkeys:
-A INPUT -i eth1+ -p tcp -m tcp --dport 80 -j ACCEPT
#NTP:
-A INPUT -i eth1+ -p udp -m udp --dport 123 -j ACCEPT
#LDAP:
-A INPUT -i eth1+ -p tcp -m tcp --dport 389 -j ACCEPT
#LDAPS (>=R7.0):
-A INPUT -i eth1+ -p tcp -m tcp --dport 636 -j ACCEPT
#MOVACS:
-A INPUT -i eth1+ -p tcp -m tcp --dport 1998:2000 -j ACCEPT
#PICTURE SERVER
-A INPUT -i eth1+ -p tcp -m tcp --dport 3195 -j ACCEPT
#XML:
-A INPUT -i eth1+ -p tcp -m tcp --dport 3197 -j ACCEPT
#VTIXML, i7xx:
-A INPUT -i eth1+ -p tcp -m tcp --dport 3199 -j ACCEPT
#PBX SERVICES:
-A INPUT -i eth1+ -p tcp -m tcp --dport 3207:3216 -j ACCEPT
#CSTA TPKT:
-A INPUT -i eth1+ -p tcp -m tcp --dport 3301 -j ACCEPT
#PBX RESERVED:
-A INPUT -i eth1+ -p tcp -m tcp --dport 3305:3399 -j ACCEPT
#XML & 6xxx WEB update:
-A INPUT -i eth1+ -p tcp -m tcp --dport 4443 -j ACCEPT
#USER PORTAL:
-A INPUT -i eth1+ -p tcp -m tcp --dport 4446 -j ACCEPT
```

```
#SIP:
-A INPUT -i eth1+ -p udp -m udp --dport 5060 -j ACCEPT
#SIPS:
-A INPUT -i eth1+ -p tcp -m tcp --dport 5061 -j ACCEPT
#LDAP Proxy:
-A INPUT -i eth1+ -p tcp -m tcp --dport 5389 -j ACCEPT
#RTP FLOW
-A INPUT -i eth1+ -p udp -m udp --dport 40000:40999 -j ACCEPT
#FTP CONTROL:
#-A INPUT -i eth1+ -p tcp -m tcp --dport 21 -j ACCEPT
#FTP DATA:
#-A INPUT -i eth1+ -p tcp -m tcp --dport 20 -j ACCEPT
#-A INPUT -i eth1+ -p tcp -m tcp --dport 39000:39999 -j ACCEPT

## ADMINISTRATION ##
#FTP CONTROL:
-A INPUT -i eth0+ -p tcp -m tcp --dport 21 -j ACCEPT
#FTP DATA:
#-A INPUT -i eth0+ -p tcp -m tcp --dport 20 -j ACCEPT
-A INPUT -i eth0+ -p tcp -m tcp --dport 39000:39999 -j ACCEPT
#SSH:
-A INPUT -i eth0+ -p tcp -m tcp --dport 22 -j ACCEPT

#SNMP REQUEST:
-A INPUT -i eth0+ -p udp -m udp --dport 161 -j ACCEPT
#SNMP TRAPS:
-A INPUT -i eth0+ -p udp -m udp --dport 162 -j ACCEPT
#LDAP:
-A INPUT -i eth0+ -p tcp -m tcp --dport 389 -j ACCEPT
#LDAPS (>=R7.0):
-A INPUT -i eth0+ -p tcp -m tcp --dport 636 -j ACCEPT
#WEB ADMIN:
-A INPUT -i eth0+ -p tcp -m tcp --dport 443 -j ACCEPT
#TCP-IP/DATA GATEWAY:
-A INPUT -i eth0+ -p tcp -m tcp --dport 3200:3206 -j ACCEPT
-A INPUT -i eth0+ -p tcp -m tcp --dport 3217:3219 -j ACCEPT
-A INPUT -i eth0+ -p tcp -m tcp --dport 3288:3291 -j ACCEPT
-A INPUT -i eth0+ -p tcp -m tcp --dport 3302:3304 -j ACCEPT
-A INPUT -i eth0+ -p tcp -m tcp --dport 3400:3499 -j ACCEPT
#USER PORTAL:
-A INPUT -i eth0+ -p tcp -m tcp --dport 4446 -j ACCEPT
#NRPE:
-A INPUT -i eth0+ -p tcp -m tcp --dport 5666 -j ACCEPT

## SBC INTERFACE ##
#SIP:
-A INPUT -i eth1+ -p udp -m udp --dport 5060 -j ACCEPT
-A INPUT -i eth1+ -p udp -m udp --dport 5062 -j ACCEPT
#RTP FLOW:
-A INPUT -i eth1+ -p udp -m udp --dport 20000:27999 -j ACCEPT

## GLOBAL ##
-A INPUT -p tcp -m tcp --dport 5061 --tcp-flags FIN,SYN,RST,ACK SYN -j syn-tcp-flood
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p icmp -j ACCEPT
-A OUTPUT -j ACCEPT
-A syn-tcp-flood -m limit --limit 2000/sec --limit-burst 2000 -j RETURN
-A syn-tcp-flood -j DROP
COMMIT
```

4.7.2 AVEC LE USER MENU

A partir de 8.2 SP3, il est possible de modifier le firewall interne du MiVoice 5000 via le User Menu. Pour accéder au User Menu :

Lancer la commande **/opt/a5000/infra/utils/bin/utd/usermenu.sh**

Le menu de configuration est alors lancé. Répondre aux différentes questions comme indiqué ci-dessous pour atteindre le menu de configuration du firewall :

```
CONFIGURATION
YOU CAN ACCESS THE MIVOICE 5000 SERVER FROM HTTPS://
1) REBOOT              6)   STANDARD              11) KEYBOARD
2) NETWORK             7)   BACKUP-SPECIFIC       12) LANGUAGE
3) FIREWALL            8)   RESTORE-SPECIFIC      13) LOGOUT
4) PASSWORD            9)   IDENTIFICATION
5) UPDATEOS-SECURITY   10)  CONFIG-RESET
SELECT AN OPTION AND PRESS ENTER: 3 ---------------> (TAPER 3)
```

Le menu suivant s'affiche :

```
FIREWALL CONFIGURATION MENU
1) SHOW                3)   DELETE              5)   DISABLE
2) ADD                 4)   REINIT              6)   QUIT
FIREWALL - SELECT MENU :
```

- Sélectionner **1) Show** pour afficher les règles du firewall.

  Le menu affiche la liste des ports ouverts et fermés du firewall.

- Sélectionner **2) Add** pour ajouter une règle pour le firewall.

  Le menu demande l'interface réseau impacté (LANA, LANB ou LANC), le type de port à ouvrir, et le numéro du port à ouvrir.

- Sélectionner **3) Delete** pour supprimer une des règles du firewall.

  Le menu demande l'interface réseau impacté (LANA, LANB ou LANC), le type de port à ouvrir, et le numéro du port à fermer.

- Sélectionner **4) Reinit** pour réinitialiser le firewall du système.

  Après prise en compte de la demande, le firewall revient à sa configuration par défaut.

- Sélectionner **6) Disable** pour désactiver le firewall du système.

- Sélectionner **7) Quit** pour revenir au menu de démarrage.