Mitel 5000 Gateways and MiVoice 5000 Server

08/2019

AMT/PTD/PBX/0151/6/3/EN

IMPLEMENTATION

Warning

Although the information contained in this document is considered as pertinent, Mitel Networks Corporation (MITEL ®) cannot guarantee the accuracy thereof.

The information may be changed without notice and should never be interpreted as a commitment on the part of Mitel, its affiliates or subsidiaries.

Mitel, its affiliates and subsidiaries shall not be held liable for any errors or omissions made in this document. This document may be reviewed or re-edited at any time in order to add new information.

No part of this document may be reproduced or transmitted in any form whatsoever or by any means - be it electronic or mechanical - no matter the purpose thereof, without the prior written consent of Mitel Networks Corporation.

CONTENTS

1 INSTALLING AND IMPLEMENTING MITEL 5000 GATEWAYS

1.1 IMPLEMENTING A NEW MITEL 5000 GATEWAYS INSTALLATION

Since the system has been preconfigured in the factory, the start-up operation only requires configuring the IP parameters on the CPU card unless the installer wishes to use the data collection form (see Section Starting from a USB key containing the data collection file).

Access is provided locally on the COM port of the CPU card, using a NULL MODEM cable (ref.: BHG0024A) connected between the COM port of the CPU card and the PC COM port.

Note: For XD, the card to be used to connect to the COM port is the active UCVD card, and not the IUCVD card or the passive UCVD card.

Procedure

- Open a Hyperterminal window and configure the connection as follows:
  - Bits per second: 115200 bits/s
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: None
- Power on the cabinet and follow the start-up progress on the PC.
- Upon display of “Identification starting”,
- Press **Ctrl** + **I.**
- The screen then displays the different configuration modes.

```
Configuration mode (F/T/S/P/U/E)
- F: Factory mode
- T: Total mode
- S: Standard mode
- P: Password reset
- U: USB provisioning mode
- E : for Exit
```

- Select “**s**" mode then press "**Return**" to enter the network pre-configuration menu.

Note: for USB provisioning mode, see Section Starting from a USB key containing the data collection file.

The system’s default network pre-configuration is displayed on screen.

During a first installation, it is from this screen that the address defined can be used to access iPBX management via Web Admin.

Access is physical via the **LAN** port on the CPU card front panel.

If it becomes necessary to configure administration and telephony flow separation, the address indicated on this screen will be dedicated to the telephony network in association with the one defined for network administration in the **ADMINISTRATION NETWORK** menu.

For this type of configuration, see the specific document: Operating manual for telephony and administration flow separation - AMT/PTD/PPBX/0101.

```
MIVOICE 5000 CONFIGURATION / NETWORK

*-------------------------------------------------*
| ENTER IP ADDRESS: 192.168.65.1       |
| ENTER NETWORK MASK: 255.255.255.0    |
| ENTER GATEWAY: 192.168.65.254        |
| ENTER DNS1:              |
| ENTER DNS2:              |
| ENTER DNS3:              |
*-------------------------------------------------*
Do you want to change configuration Y/[N] : Y
```

- Answer "**y**" and validate with the "**Return**" key to access the different fields.
- Enter successively the system parameters, using the “**Return**” key to change line.
  - The DNS settings must also be entered if necessary.

```
MIVOICE 5000 CONFIGURATION / NETWORK

*-------------------------------------------------*
| ENTER IP ADDRESS: 100.100.40.150     |
| ENTER NETWORK MASK: 255.255.255.192 |
| ENTER GATEWAY: 100.100.40.129        |
| ENTER DNS1: 100.100.40.160 |
| ENTER DNS2: 100.100.40.161 |
| ENTER DNS3 : 100.100.40.162 |
```

After the last line is validated, a summary of the network parameters is displayed for confirmation.

```
MIVOICE 5000 CONFIGURATION / NETWORK
*-------------------------------------------------*
| SUMMARY |
*-------------------------------------------------*
*-------------------------------------------------*
| IPADR = 100.100.40.150     |
| NETWORKMASK = 255.255.255.192        |
| GATEWAY = 100.100.40.129    |
| DNS1: 100.100.40.160 |
| DNS2: 100.100.40.161 |
| DNS3 : 100.100.40.162 |

| NETWORKADR = 100.100.40.128    |
| BROADCAST = 100.100.40.191     |
*-------------------------------------------------*
```

If the summary is not correct:

- Press "**n**" to restart network pre-configuration.

If the summary is correct:

- Press "**y**" then "**Return**", to confirm.

Note : By default, the EIP card(s) is/are automatically assigned an address and is/are automatically activated. The values assigned are IPADR + 1 and IPADR + 2 (in case of two EIP cards)

ATTENTION : This feature may result in IP address clashes. It is advisable to check that the EIP IP address is correct for your addressing plan.

The screen below opens, asking whether the administration network must be configured in case of administration and telephony flow separation.

```
DO YOU WANT TO CONFIGURE MANAGEMENT IP NETWORK ? Y/[N]
```

If this configuration is not necessary, answer "n" and confirm with the "**Return**" key to go to the next screen concerning the service status.

If this configuration is necessary in this phase, See the specific document: Operating manual for telephony and administration flow separation - **AMT_PTD_PBX_0101**.

The status of FTP, TMA and DHCP services can be modified on the following screens:

These services are used by the TMA application, and to manage IP terminals. See Terminal installation manual - AMT/PTD/TR/0014.

```
MIVOICE 5000 CONFIGURATION / SIP SERVICE
 AN EXISTING CONFIGURATION WAS FOUND
*-------------------------------------------------*
| FTP (0/1): 1                  |
| TMA (0/1): 1                  |
| DHCP(0/1): 0                  |
*-------------------------------------------------*
Do you want to change configuration Y/[N] ? Y
```

Note : For the FTP service, it must be set to "1," and then be present in Menu **SYSTEM>Configuration>Web Admin Services (Activation and deactivation)**.

If the answer is YES, "**y**", the following screen can be used to modify the configuration parameters for Mitel 6700 SIP Phone deployment (or to deactivate these services if other deployment solutions are to be used).

```
MiVoice 5000 Configuration / Services
 *-------------------------------------------------*
| FTP :                 1       |
| TMA :                 1                         |
| DHCP :                0       |
*-------------------------------------------------*
Entrer : 1 for DHCP
Do you confirm (Y/N)(Press ENTER to reconfigure)?
```

The values entered must be 0 (deactivated) or 1 (activated).

FTP: value 0 or 1.

This field allows (1 = yes) or disallows (0= no) the use of the integrated FTP server on Mitel 5000 Gateways during first installation. The FTP server must be active (1) in order to be able to use the integrated TMA services.

Default value in factory settings: **FTP = 1**

TMA: value 0 or 1.

This field allows (1 = yes) or disallows (0= no) the use of the integrated TMA server on Mitel 5000 Gateways during first installation (and MiVoice 5000 Server for memory). For management by MiVoice 5000 Manager, the integrated TMA service is inactive since management is centralised for all the terminals on MiVoice 5000 Manager.

Default value in factory settings: **TMA = 1**

DHCP: value 0 or 1.

This field allows (1 = yes) or disallows (0= no) the use of the integrated DHCP service on Mitel 5000 Gateways.

If an external DHCP server is used, the DHCP service is inactive.

If DHCP is on 0, then TERMINAL VLAN and PC VLAN are proposed.

```
MiVoice 5000 Configuration / SIP Mitel 6700 SIP Phone
 An existing configuration was found
*-------------------------------------------------*
| LLDP ENABLED : 0                                |
| TERMINAL VLAN:                    |
| PC VLAN:                                       |
*-------------------------------------------------*
Do you want to change configuration Y/N?  N
```

LLDP ENABLED

This field is used to activate the LLDP in the terminal (1 = yes) or not (0= no).

TERMINAL VLAN and PC VLAN

These parameters are used to define the VLAN dedicated to Mitel 6700 SIP Phones. They are not mandatory on simple networks.

If DHCP is on 1, the screen is displayed.

```
MiVoice 5000 Configuration / SIP Mitel 6700 SIP Phone
 An existing configuration was found
*-------------------------------------------------*|
|| LLDP ENABLED : 0                                |
|
*-------------------------------------------------*
Do you confirm (Y/N)?
```

- If necessary, modify the value of the LLDP field.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

If the DHCP service had been previously installed, this menu can be used to automatically pre-configure the DHCP server for Mitel 6700 SIP Phones and for terminals A53xxip and i7xx.

```
MiVoice 50005000 Configuration / DHCP
*-------------------------------------------------------------------
---------*
| SUBNET MASK :        255.255.255.0                              |
| BEGIN RANGE :        20.1.1.100                                 |
| END RANGE :          20.1.1.199                               |
| GATEWAY :            20.1.1.254                                   |
| TERMINAL VLAN:
|
| PC VLAN:                                                      |
*---------------------------------------------------------------*
Do you confirm (Y/N) (Press enter to reconfigure) ? y
```

SUBNET MASK: subnet mask dedicated to IP and SIP terminals

BEGIN RANGE and END RANGE: address range dedicated to IP and SIP terminals

GATEWAY: IP address of the network gateway dedicated to the IP and SIP terminals

TERMINAL VLAN and PC VLAN: these parameters are used to define the VLAN dedicated to Mitel 6700 SIP Phones and to terminals A53xxip and i7xx. They are not mandatory on simple networks.

- Press "Return" to confirm each input.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

```
WARNING REBOOT
 *-----------------------------------------------------*
| WARNING :                                           |
| Applying changes implies a iPBX restart      |
| *-----------------------------------------------------*
Do you want to apply your change Y(ES)/N(O)/R(ECONFIGURE) ?
```

- If the configuration is not correct:
  - Press "**r**" to restart the preconfiguration.
  - Leave "T" mode and restart with the previous configuration without saving the modifications
  - Press "**n**"; the system restarts with the previous configuration.
- > If the configuration is correct:
  - Press "**y**" and confirm by pressing "**Return**".

The system then restarts automatically, and the its IP network link can be set up via the LAN access.

Start-up is now complete and you can configure the site from the user interface. For terminal management refer to the MiVoice 5300 IP Phone and Mitel 6700 SIP Phone Mitel 53xx Installation Manual - AMT/PTD/TR/0014.

Note : You can modify the factory setting entirely, using T mode after pressing Ctrl + I.

1.2 STARTING FROM A USB KEY CONTAINING THE DATA COLLECTION FILE

Additional information on data collection is provided in the **MiVoice 5000 Provisioning Excel** file - **Help** tab.

1.2.1 REMINDER

The data collection form contains a specific tab for the configuration parameters required for the **Ctrl + I** phase.

The following files are created after the iPBX data is generated:

- **Install.conf** containing the data for the CTRL + I of a managed iPBX (example: 002.Mitel.install.conf).
- **DataCollecting.zip** containing the different **.csv** files from the collection and used by Web Admin (example: 002.Mitel.DataCollecting.zip).
- **7450_Formulaire.xls** (Excel 2003) to be imported into MiVoice 5000 Manager. It contains the data required to configure UCP and TWP accounts.

The generated files are placed in the same directory as the one in which the form is installed.

The generated file **Install.conf** is then copied to a USB key and can be used for the two start-up modes indicated in the sections below.

Depending on start mode (automatic or through **Ctrl + i**), file renaming and the name of the storage directory are different.

1.2.2 BOOTING IN U MODE (USB KEY CONNECTED) USING A SERIAL CABLE ON THE CONSOLE PORT

In this case, the generated **install.conf** file must be copied to the unprotected USB key in a specific directory, with the following access path syntax: **<USBKEYROOT>/aastraprovisionning/SiteNumber.Name.conf**

where **<USBKEYROOT>/aastraprovisionning/** is the directory name and **SiteNumber .Name.conf** the file name.

Example: **aastraprovisionning/020.Site1.conf**

Note : The site number will be transformed to 3 characters if the entry is made with 2 characters. This is to facilitate the classification of directories in Windows.

The file **Install.conf** must be named and copied to the USB key in a directory to be created and named as follows: **aastraprovisionning**.

IMPORTANT : The syntax for the name of this directory must be respected.

How to start in U mode

Prerequisites: the provisioning file must be on the USB key, in the right directory and with the right syntax.

Start the iPBX in Ctrl + i mode (see Section Implementing a new Mitel 5000 Gateways installation), up till the menu used to display the different modes:

```
Configuration mode (F/T/S/P/U/E)
- F: Factory mode
- T: Total mode
- S: Standard mode
- P: Password reset
- U: USB provisioning mode
- E : for Exit
```

- Select "**u**" mode and confirm by pressing "**Return**".
- Enter successively the system parameters, using the **Return** key to change line.
    - The DNS settings must also be entered if necessary.

```
MIVOICE 5000 CONFIGURATION / NETWORK

*-------------------------------------------------*
| ENTER IP ADDRESS: 100.100.40.150    |
| ENTER NETWORK MASK: 255.255.255.192 |
| ENTER GATEWAY: 100.100.40.129       |
| ENTER DNS1: 100.100.40.160|
| ENTER DNS2: 100.100.40.161|
| ENTER DNS3 : 100.100.40.162|
```

After the last line is validated, a summary of the network parameters is displayed for confirmation.

```
MIVOICE 5000 CONFIGURATION / NETWORK
*-------------------------------------------------*
| SUMMARY |
*-------------------------------------------------*
*-------------------------------------------------*
| IPADR = 100.100.40.150     |
| NETWORKMASK = 255.255.255.192       |
| GATEWAY = 100.100.40.129   |
| DNS1: 100.100.40.160|
| DNS2: 100.100.40.161|
| DNS3 : 100.100.40.162|
| NETWORKADR = 100.100.40.128   |
| BROADCAST = 100.100.40.191    |
*-------------------------------------------------*
```

If the summary is not correct:

- Press "**n**" to restart network pre-configuration.

If the summary is correct:

- Press "**y**" then "**Return**", to confirm.

The screen then prompts you to connect the USB to the CPU card.

```
MiVoice 5000 Configuration
*-------------------------------------------------*
| Please connect your usb device then press any   |
| key                                             |
*-------------------------------------------------*
Press C to Cancel
```

- After connecting the key, press any key to continue, or **C** to cancel.

If there are several files in the directory:

- The screen displays the different files available in the directory dedicated to the USB key (maximum 10, displayed in ascending order).

```
More than one provisioning file has been found  |
| Please choose the file you want to use :       |
| - 1 : 001.pbx1.conf                            |
| - 2 : 002.pbx2.conf                            |
| - 3 : 003.pbx3.conf                            |
| - 4 : 004.pbx4.conf                            |
| - 5 : 005.pbx5.conf
```

After you have chosen the file, a summary is displayed with the following message:

```
Do you want to apply your change Y(ES)/N(O)/R(ECONFIGURE) ?
```

Note : If there is only one file in the directory, the summary is displayed directly.

If the configuration is not correct:

- Press "**R**" to restart configuration in "**U**" mode (from the beginning).
- To leave "U" mode and restart with the previous configuration without saving the modifications:
- Press "**N**"; the system restarts with the previous configuration.

If the configuration is correct:

- Press "**Y**" and confirm by pressing "**Return**".
- The system restarts automatically in **Total** mode taking into account the configuration file.
- Remove the USB key.

1.2.3 AUTOMATIC START WITHOUT CTRL + I, TAKING INTO ACCOUNT THE DATA COLLECTION FILE

This other very simplified start mode does not require any link on the serial port and gives remote access, after a T0 access has been configured, to the iPBX via the integrated HSCX modem of the CPU card.

Principle:

The iPBX starts automatically on the USB key (without going through the Ctrl + i phase) taking into account the specific file **install.<dongle_number>.conf** from the iPBX data generation (data collection form).

The initial file from the iPBX data generation (**install.conf**) must be renamed with the syntax indicated below and placed in a dedicated and unique directory called **/aastra_usbconfig/** at the root of the USB key.

This file contains the values used to access the HSCX modem.

Specific format and location of the directory name and of the .conf file

The generated file **install.conf** must be named and copied to a USB key not write-protected in a specific directory, respecting the following syntaxes:

<USBKEYROOT>/aastra_usbconfig/install.<dongle_number>.conf

- **<USBKEYROOT>/aastra_usbconfig/** is the mandatory directory name.
- **install.<dongle_number>.conf** is the name of the renamed file, where <dongle_number> is the exact iPBX dongle ID.
    - Example install.0106000012E9A9.conf.

In this same example after the iPBX is restarted, this file will be renamed *install.0106000012E9A9.conf.done.txt.*

Procedure:

Prerequisites: the provisioning file must be on the USB key, in the right directory and with the right syntax.

Since the iPBX has been stopped:

- Connect the USB key.
- Restart the iPBX.

During the restart phase the USB key is first detected, allowing you to perform the configuration from the data in the file **install.<dongle_number>.conf**.

At the end of this phase:

The file has been renamed so it does not have to be reloaded later (see example below).

- Then configure the T0 access from Web Admin to access the HSCX modem.
- Remove the USB key.

1.3 ACCESSING THE USER INTERFACE (MIVOICE 5000 WEB ADMIN)

Note : Accesses via analogue modem, ISDN modem and ISDN router are described in Section Remote access modes.

1.3.1 ACCESSING THE USER INTERFACE (MIVOICE 5000 WEB ADMIN) VIA THE LAN

The operating console is connected to the same network as the iPBX (CPU card LAN port).

- Open a web browser installed on the operating console (Internet Explorer, for instance).
- Enter the IP address defined in the system: https://@IP (secure access mode).

Note : Default address in factory setting: 192.168.65.01

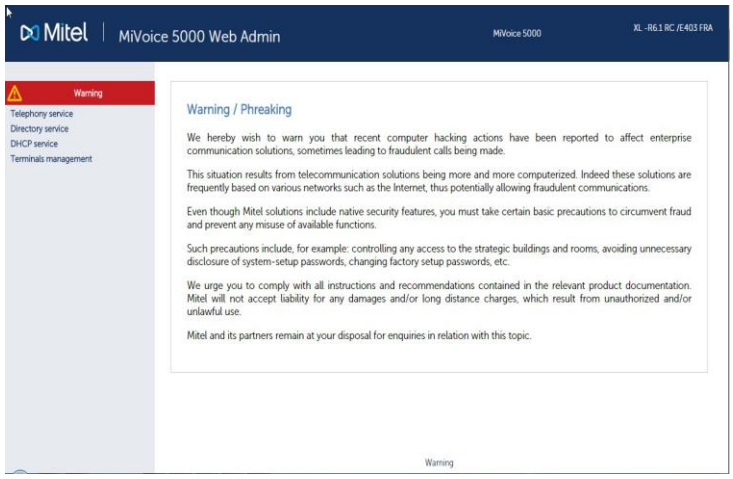
- Some security windows for this "https" access mode are then displayed successively; enter “YES” for each of them.
- The web browser (Internet Explorer) displays a security alert when connecting to Web Admin; this alert can be deactivated. Refer to the appendix to this document, Section Taking the security certificate into account

A login window opens.

- Enter the default access login: **admin**
- Enter the default access password: **admin**

The Web Admin welcome screen is displayed.

The first time you are logging on, the welcome screen displays a page alerting you to the risks of piracy and to the security constraints.



After reading this message:

Click any of the **Warning** buttons.

On the next screen that opens, displaying this message, tick **I have read this text**.

Click **OK** to confirm.

The actual Web Admin welcome screen is then displayed, giving access to all the menus:

For more information about the display of this warning message, see the Section MITEL's legal warning concerning Web Admin access.

Certificate download menu

This menu is a link for downloading the self-signed SHA2 certificate provided by Mitel.

The certificate is used to secure the connection between the Web Admin and User Portal interfaces with MiVoice Manager, in particular.

The assigned certificate may also be external.

Certificates are managed and assigned from Menu **SYSTEM>Security**.

Refer to the following documents in the chapters concerning Security/Certificates:

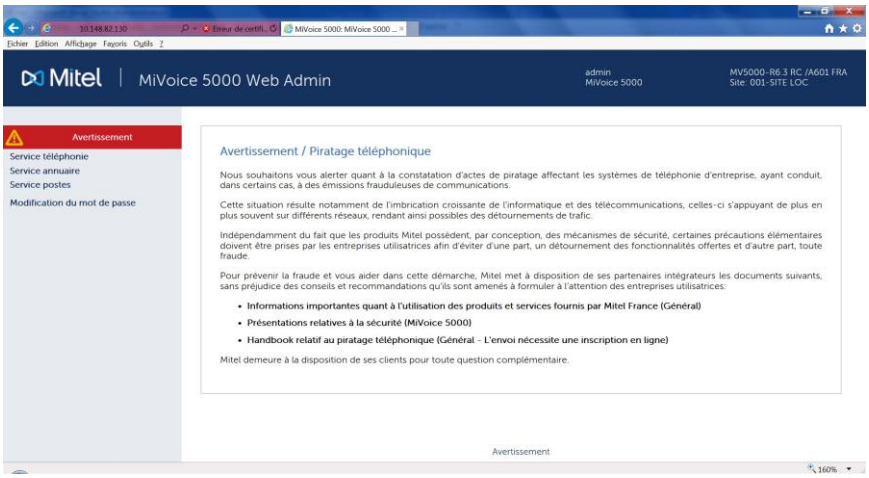
- AMT/PBX/0080 - A5000 Operating Manual
- MiVoice 5000 Manager User Guide

This link appears systematically during a first installation or after upgrading to R7.0 for sites or nodes (Cluster Configuration) whose initial version is below R7.0.

This link no longer appears if a certificate (Mitel or external SHA2) has been downloaded into the iPBX either locally or from MiVoice 5000 Manager.

User password notification message

If a password policy is defined for the user password, the welcome screen may contain an additional **Password modification** menu prompting the user to change his password if it has expired.



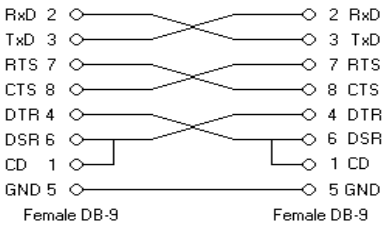
See the document AMT/PTD/PBX/0080, in the section on user password policy.

1.3.2 ACCESSING THE USER INTERFACE (MIVOICE 5000 WEB ADMIN) IN LOCAL ACCESS MODE VIA THE COM PORT (PPP PROTOCOL)

The PPP exchange protocol can set up a network type connection between two systems on a serial point-to-point link.

1.3.2.1 *Connections*

Access is provided on the COM port of the CPU card (ISDN type access), using a NULL MODEM cable (ref.: BHG0024A) connected between the COM port of the CPU card and the PC COM port.



1.3.2.2 *Configuring the serial connection*

Windows PC specifications

A PC with a COM pig.

A modem of the type "**communication cable between two computers**" must be installed. Use Device manager to check the presence of this pseudo modem.

If the modem is not installed, please proceed as follows, for instance for Windows XP.

In Control Panel

- Select "Add hardware".
- After automatic detection, select " **Yes, I have already connected the hardware** " then choose" **Add a new device** " in the window that opens.
- Click "**Next**"
- Tick the option "install the hardware I manually select from a list " then choose "Modem".
- Click "**Next**"
- In the following screen, tick the option "**Do not detect my modem**".
- Click "**Next**"
- Select the modem "**Communication cable between two computers**" then choose a communication port.
- Click "**Next**"

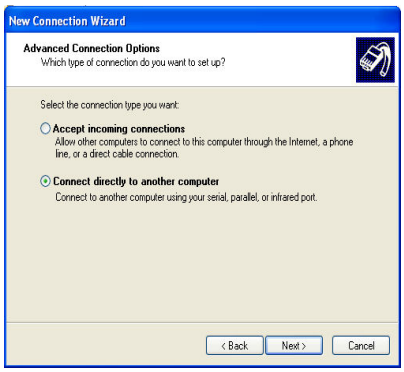
The next screen indicates that the modem is now installed: it is visible in the Device manager.

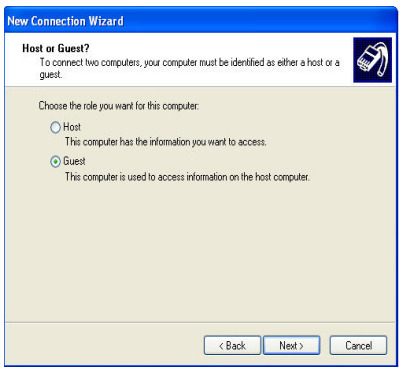
- Click "**Finish**"

Configuring the PPP connection

In Control Panel

- Click "**Network connections**".
- Select "Create a new connection".
- Tick successively the boxes indicated below.





- Enter a name for this network connection.
- Select the device " Communication cable between two computers".
- In the next screen, indicate the restriction on the use of this connection.

The connection is now defined.

Configuring the connection port

The configuration is made in the "**Properties**" menu of the network connection.

- Choose 15200 bits/s

- Tick the option "Enable hardware flow control".

Setting up a connection on the PBX

In the "**Start**" menu, "**Connections**" tab, start the connection to the PBX.

- Login: user
- Password: guest

The PPP connection characteristics are displayed using the Windows ipconfig command. By default, the IP addresses 192.168.0.101 and 192.168.0.102 are used for the system and for the PC.

Note : For a stand-alone PC and if the iPBX IP address is used, IP routing uses the PPP connection as available route to access the IP address provided.

If the PC is located on the same network as the iPBX, it is necessary to disconnect the PC from the network to force routing via PPP connection. In this case, it is more practical to use the IP address "192.168.0.101" of the PPP interface.

For a stand-alone PC and if the iPBX IP address is used, IP routing uses the PPP connection as available route to access the IP address provided.

If the PC is located on the same network as the iPBX, it is necessary to disconnect the PC from the network to force routing via PPP connection. In this case, it is more practical to use the IP address "192.168.0.101" of the PPP interface.

1.3.2.3 *Accessing Web Admin via the serial link*

- Open a web browser installed on the operating console (Internet Explorer, for instance).
- Enter the address dedicated to this access mode: https://192.168.0.101 (secure access mode).
- Some security windows for this "https" access mode are then displayed successively; enter “YES” for each of them.
- A Login window opens, allowing access to Web Admin.

1.4 REMOTE ACCESS MODES

The user interface remote access modes are:

- Access via an analogue modem
- Access via an analogue ISDN modem
- Access via an ISDN router.

1.4.1 ACCESSING THE USER INTERFACE VIA AN ANALOGUE MODEM

From a PC, set up a connection with the external analogue modem via the PC's integrated modem.

Then access the web browser installed on this PC (Internet Explorer, for example).

Enter the IP address, 192.168.0.101, the default value defined for this connection type via the operating console in secure mode:

- **https:// 192.168.0.101** (secure access mode).

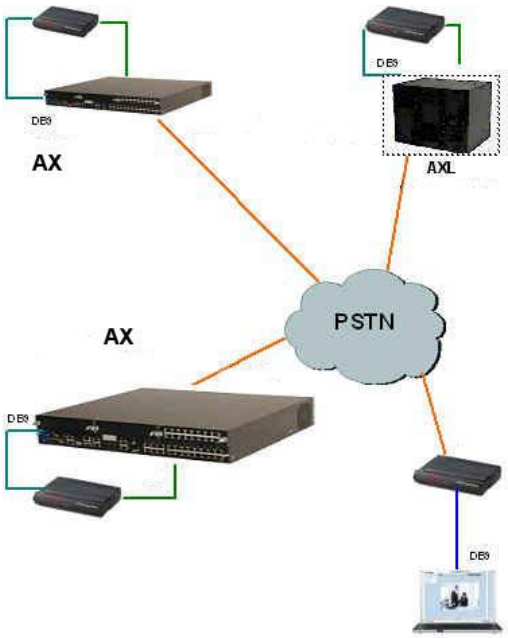
Connections

Only one access per Mitel 5000 Gateways system.

The analogue connection requires an external analogue modem between the gateway and analogue network socket.

Note : Mitel offers at the price a 56k US Robotics analogue modem.

A cable, DB25M, on the modem side - modem - DB9F on the gateway side, is used to connect the modem to the gateway.



Configuring Mitel 5000 Gateways systems

- Assign a DID number.

Modem configuration

- Automatic: controlled by Mitel 5000 Gateway

Hayes commands for analogue US ROBOTICS modem configuration

In case of ppp remote maintenance connection problem on a modem, check your modem's register configuration.

Below is the recommended modem register configuration.

- atS0= 2 off-hook after 2 seconds
- &b1=115200 serial port throughput

To see the register bases, type either **at&v** or **at&i4**.

ATTENTION : Do not forget to back up using at&w

Configuring the PPP connection

In Control Panel

- Click " Network connections ".
- Select Create a new connection.
- In New connection wizard, click Next.
- Tick successively the boxes indicated below:
    - In the Network connection type screen, tick Connection to company network.
    - Click **Next**.
    - In the Network connection screen, tick Remote access connection.
    - Click **Next**.
    - Choose the modem type on the list proposed.
    - Click **Next**.
    - In the Connection name screen, fill in the Company name field.
    - Click **Next**.
    - In the screen **Enter the phone number to dial** , enter the call number for this connection via modem.
    - Click **Next**.
    - In the Connection availability screen, tick All users.
    - Click **Next**.

The PPP configuration has been completed.

In the "**Start**" menu, "**Connections**" tab, start the connection to the PBX.

- Login: **user**
- Password: **guest**

Accessing the Web Admin user interface

Open a web browser installed on the operating console (Internet Explorer, for instance).

Enter the address dedicated to this access mode: https://192.168.0.101 (secure access mode).

Some security windows for this "https" access mode are then displayed successively; enter “YES” for each of them.

A login window opens.

1.4.2 ACCESSING THE USER INTERFACE (WEB ADMIN) VIA AN ISDN MODEM

Configuring Mitel 5000 Gateways systems

In ISDN, since the Mitel 5000 Gateways system is connected to the operator network, you have to:

- Define a subscriber (by default, Subscriber 796).
- Assign an "HSCX modem" terminal type to this subscriber ("terminals allocation).
- Assign a DID number to the iPBX.

Configuring the remote PC

- On the remote operation PC, there must be an “ISDN modem”.

ISDN modem configuration

The ISDN modem is connected (depending on the models) to the serial port or USB port of a PC on the operator ISDN line, or on an S0, S2 bus.

Configuring the ISDN modem access on the Mitel 5000 Gateways system

- S0: Call without ID at Yes (menu 414)

Examples of external ISDN modems: Olitec ISDN USB V2 or V3, Bewan gazel 128 USB, Zyxel omi.net USB.

It is possible to use a PCI card to be integrated in the PC (with driver installation).

Configuring the PPP connection

In Control Panel

Configuring the PPP connection

In Control Panel

- Click " Network connections ".
- Select Create a new connection.
- In New connection wizard, click Next.
- Tick successively the boxes indicated below:
    - In the Network connection type screen, tick Connection to company network.
    - Click Next.
    - In the Network connection screen, tick Remote access connection.
    - Click Next.
    - Choose the modem type on the list proposed.
    - Click Next.

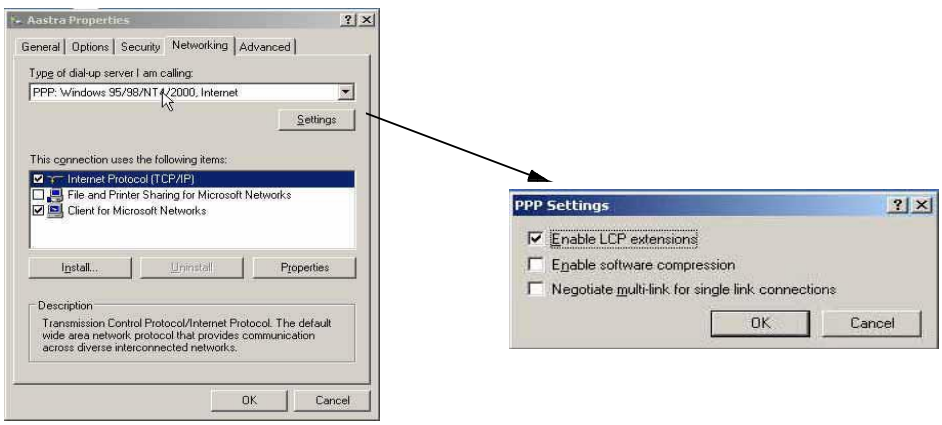
In the **Connection name** screen, fill in the **Company name** field.

- Click **Next**.
- In the screen **Enter the phone number to dial** , enter the call number for this connection via modem.
- Click **Next**.
- In the Connection availability screen, tick All users.
- Click **Next**.

The connection has been configured.

In the "**Start**" menu, "**Connections**" tab, start the connection to the PBX.

- Login: **user**
- Password: **guest**
- Click **Properties** then successively tick the boxes as indicated below in each tab.
  - In the Modem properties tab:
    - Choose the modem type on the list proposed.
    - Enter the call number.
    - In the **Options** tab, tick
    - Indicate connection progress status.
    - Request for a name, a password, etc.
    - Request for a phone number.
    - Choose the callback options.
    - Indicate connection progress status.
  - In the **Security** tab, retain the default value.
  - In the **Network management** tab, select and tick the values accordingly as indicated in the following screen:



  - In the **Advanced** tab, retain the default value.

- Click **OK**.

Accessing the Web Admin browser

- Open a web browser installed on the operating console (Internet Explorer, for instance).
- Enter the address dedicated to this access mode: **https://192.168.1.101** (secure access mode).

Some security windows for this "https" access mode are then displayed successively; enter “YES” for each of them.

A login window opens.

1.4.3 ACCESSING THE USER INTERFACE (WEB ADMIN) VIA AN ISDN ROUTER

In this release (R5.1A), the router must mask the PC address (NAT); the iPBX only sees an IP address on the PPP link (all the others are routed over the LAN port, the connection would not be set up).

1.4.3.1 *CONNECTIONS*

- ISDN cable: router RJ45, LD4X or LT2/LT2N or operator RJ45.
- Ethernet cable: RJ45 -RJ45

PBX CONFIGURATION

- S0 or S2 parameter
- S0: Call without ID at Yes (menu 414)
- S2: Call without ID at yes
- CRC4 management at yes

ACCESSING the Web Admin BROWSER

- Open a web browser installed on the operating console (Internet Explorer, for instance).
- Enter the address dedicated to this access mode: **https://192.168.1.101** (secure access mode).

1.5 MODIFYING THE FACTORY SETTINGS

The system is preset in the factory, but it is possible to fully modify these factory settings on site.

Access is provided locally on the COM port of the CPU card, using a NULL MODEM cable (ref.: BHG0024A) connected between the COM port of the CPU card and the PC COM port.

Note : For AXD, the card to be used to connect to the COM port is the active UCVD card, and not the IUCVD card or the passive UCVD card.

Procedure

On the PC connected to the COM port

- Open a Hyperterminal window and configure the connection as follows:
  - Bits per second: 115200 bits/s
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: None
- Power on the cabinet and follow the start-up progress on the PC.
- Upon display of "Identification starting"
- Press **Ctrl** + **I**
- The screen then displays the different configuration modes.

```
Configuration mode (F/T/S/P/U/E)
- F: Factory mode
- T: Total mode
- S: Standard mode
- P: Password reset
- U: USB provisioning mode
- E : for Exit
```

- Select "**T**" mode to enter the pre-configuration menus.

The system's default network pre-configuration is displayed on screen.

During a first installation, it is from this screen that the address defined can be used to access iPBX management via Web Admin.

Access is physical via the **LAN** port on the CPU card front panel.

If it becomes necessary to configure administration and telephony flow separation, the address indicated on this screen will be dedicated to the telephony network in association with the one defined for network administration in the **ADMINISTRATION NETWORK** menu.

For this type of configuration, see the Operating manual for telephony and administration flow separation - AMT/PTD/PBX/0101.

```
MIVOICE 5000 CONFIGURATION / NETWORK

*-------------------------------------------------*
| ENTER IP ADDRESS: 192.168.65.1      |
| ENTER NETWORK MASK: 255.255.255.0   |
| ENTER GATEWAY: 192.168.65.254       |
| ENTER DNS1:              |
| ENTER DNS2:              |
*-------------------------------------------------*
Do you want to change configuration Y/[N] : Y
```

- Answer "**y**" and validate with the "**Return**" key to access the different fields.
- Enter successively the system parameters, using the **Return** key to change line.

```
MIVOICE 5000 CONFIGURATION / NETWORK

*-------------------------------------------------*
| ENTER IP ADDRESS: 100.100.40.150    |
| ENTER NETWORK MASK: 255.255.255.192 |
| ENTER GATEWAY: 100.100.40.129       |
| ENTER DNS1: 100.100.40.160|
| ENTER DNS2: 100.100.40.161|
| ENTER DNS3 : 100.100.40.162|

*-------------------------------------------------*
```

After the last line is validated, a summary of the network parameters is displayed for confirmation.

```
MIVOICE 5000 CONFIGURATION / NETWORK
*-------------------------------------------------*
| SUMMARY |
*-------------------------------------------------*
*-------------------------------------------------*
| IPADR = 100.100.40.150   |
| NETWORKMASK = 255.255.255.192       |
| GATEWAY = 100.100.40.129      |
| DNS1: 100.100.40.160|
| DNS2: 100.100.40.161|
| DNS3 : 100.10040.162|

| NETWORKADR = 100.100.40.128   |
| BROADCAST = 100.100.40.191    |
*-------------------------------------------------*
```

If the summary is not correct:

- Press "**n**" to restart network pre-configuration.

If the summary is correct:

- Press "**y**" and confirm by pressing "**Return**".

Note : By default, the EIP card(s) is/are automatically assigned an address and is/are automatically activated. The values assigned are IPADR + 1 and IPADR + 2 (in case of two EIP cards)

ATTENTION : This feature may result in IP address clashes. It is advisable to check that the EIP IP address is correct for your addressing plan.

The screen below opens, asking whether the administration network must be configured in case of administration and telephony flow separation.

If this configuration is not necessary, answer "**n**" and confirm with the "**Return**" key to go to the next screen concerning the service status.

If this configuration is necessary in this phase,see the specific document:

Operating manual for telephony and administration flow separation - AMT_PTD_PBX_0101.

The licence number declaration screen is then displayed.

- Enter the corresponding value (optional: it may be entered later from Web Admin.
- Press "**Return**" to confirm, after entering "**y**" or "**n**".

The system's PARI number configuration screen is displayed:

- If you answer YES, "**y**", the next screen allows you to redefine this number.
- Enter the corresponding value.
- Press "**Return**" to confirm, after entering "**y**" or "**n**".

The status of FTP, TMA and DHCP services can be modified on the following screens. Refer to Section Implementing a new Mitel 5000 Gateways installation.

After this series of screens concerning TMA, FTP and DHCP services, the parameter definition screen of Mitel 6700 SIP Phones appears. Refer to Section Implementing a new Mitel 5000 Gateways installation.

After this series of screens concerning terminal Mitel 6700 SIP Phone parameters, the system's general parameters declaration screen opens (name, IID (system identification number)):

```
MIVOICE 5000 CONFIGURATION / Name&IID
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE NAME/IID Y/[N] : Y      |
*-------------------------------------------------*
```

- If you answer YES, "**y**", the next screen allows you to declare the system's general parameters.
- Fill in successively the different fields, using the **Return** key to change line.

```
MIVOICE 5000 CONFIGURATION / Name&IID

*-------------------------------------------------*
| NAME: MIVOICE 5000      |
| IID: 00130927001        |
*-------------------------------------------------*
```

- After the last line is validated, a summary of the network parameters is displayed for confirmation.
- If the values are correct, press "**Return**" to confirm, after pressing "**y**".

The next screen is used to configure the numbering plan length.

```
MIVOICE 5000 CONFIGURATION / NL
*-------------------------------------------------*
| Do you want to configure Numbering lenght Y/[N] ? Y |
*-------------------------------------------------*
```

- Press "**Return**" to confirm, after entering "**y**" or "**n**".

The answer is "**n**", the default value remains 4.

If the answer is "**y**", enter the corresponding values (2 to 10).

The field is used to define the internal number length to take into account (2 to 6). This field is associated with the fields **first**, **last**, **modem**, **IVB**, **hscx**, **common subscriber** and **common bell** defined on the "Subscribers" screen.

```
MIVOICE 5000 CONFIGURATION / NL

*-------------------------------------------------*
| NUMBERING LENGTH: 5     |
*-------------------------------------------------*
DO YOU CONFIRM (Y/N)(PRESS ENTER TO RECONFIGURE)? Y
```

- Press "**Return**" to confirm, after entering "**y**".

The next screen is used to configure call distribution.

```
MIVOICE 5000 CONFIGURATION / Call Dist
*-----------------------------------------------------*
| DO YOU WANT TO CONFIGURE CALL DISTRIBUTION Y/[N]: Y |
*-----------------------------------------------------*
```

- Press "**Return**" to confirm, after entering "**y**" or "**n**".

If the answer is "**y**", fill in successively the different fields, by pressing **Return** to change line.

```
MIVOICE 5000 CONFIGURATION / Call Dist

*-------------------------------------------------*
| SUBSCRIBER: 3005        |
| DID: 4000               |
*-------------------------------------------------*
```

The "**SUBSCRIBER**" field allows you to assign a subscription number as a day number and reduced to reception 0. This number is assigned if it corresponds to an internal subscription which can be added to a call distribution service, or if it corresponds to the number of a subscription that may be on the multi-site network (MiVoice 5000 Server).

The "**DID**" field is used to assign a DID number to call distribution service0. Authorised characters are " 0123456789ABCDE".

- After the last line is validated, a summary of the network parameters is displayed for confirmation.
- If the values are correct, press "**Return**" to confirm, after pressing "**y**".

The following screen is used to configure subscriptions:

```
MIVOICE 5000 CONFIGURATION / Subscribers
*-------------------------------------------------
*
| Do you want to change configuration Y/[N] ? Y |
*-------------------------------------------------
*
```

If the answer is "**y**", fill in successively the different fields, by pressing Return to change line. These fields are described below:

```
MIVOICE 5000 CONFIGURATION / Subscribers

*-------------------------------------------------*
| CREATION (0/1): 0       |
| IVB CREATION (0/1): 1   |
| UNIFIED IVB (0/1): 1    |
| FIRST : 3000            |
| LAST : 3999             |
| DID NUMBERING LENGTH        4       |
| FIRST DID : 3000        |
| FIRST PUBLIC DID : +33(0)136923000  |
| MODEM : 0               |
| IVB :                   |
| HSCX CREATION (0/1): 1  |
| HSCX : 3400             |
| DID HSCX :              |
| COMMON SUBSCRIBER : 3500      |
| COMMON BELL : 3001      |
| ADDITIONNAL SUBSCRIPTIONS : 40      |
| PASSWORD SUBSCRIBER: 0000     |
| GENERATION OF SETS AUTHENTICATION=1 |
```

The **Creation** field may be used to inhibit automatic subscriber creation. This field may take on the values 0 (= creation inhibited) or 1(= creation authorised).

The **IVB creation** field is used to inhibit automatic creation of integrated voice mail boxes for subscribers during automatic creation of subscriptions. This may take on the values 0 (= creation inhibited) or 1 (= creation authorised).

The **Unified IVB** field is used to define some unified voice mail boxes, if available.

The **numbering length** field defined on the previous screen contains the internal number length to take into account (2 to 6). If this value is valid, the fields **first**, **last**, **modem**, **IVB**, **hscx**, **common subscriber** and **common bell** are taken into account. Otherwise, they will be ignored.

Note : If the internal number length (in the internal numbering plan) is different from the internal number length in the incoming numbering plan (default value for the country, not modifiable on this level), the subscribers are created but do not have any DID number.

The field **first** contains the first internal subscription that can be created automatically, while the field **last** contains the last one.

The fields **common subscriber**, **common bell, IVB, modem,** and **hscx** are read in this order and taken into account if they are in the complete block and if this number does not exist already. If this is not the case, or if the field does not exist, they are assigned a default number. If their value is 0, they will not be assigned any number. The only exception is **common subscriber** which must always have a number.

The **DID numbering length** field is used to define the internal number length in the incoming number plan (i.e. DID numbers).

The **first DID** field is used to create the external block 0 associated with the internal number block [first, last]. Authorised characters are " 0123456789ABCDE". For this block to be created, this number must belong to an incoming number plan.

The **first public DID** field is used to associate a public number (format: 0130967000 or +33(0)130967000) with the DID number for block 0. This ASCII string will be truncated to 20 characters.

The **HSCX creation** field is used to create a HSCX subscription. The **HSCX** field is used to define the internal HSCX subscription number. The **DID HSCX** field is used to define the HSCX subscription DID number.

The **additional subscriptions** field indicates the number of further internal subscriptions to create.

Password Subscribers :

This field is used to modify the default subscriber password (0000). The value will be assigned to all subscribers, using Ctrl + i.

This 4-digit password will be used to access the IVB and to deploy Mitel 6700 SIP Phones.

It is the password to be configured in the iPBX (used by default for any subscription created in Web Admin).

This password can be modified later from Web Admin, in Menu **Subscribers>Subscriptions>Create**, or in extension characteristics.

For more details on how to manage this password, see the sections concerning these menus in the document AMT/PTD/PBX/0080.

Generation of sets authentication=1

This field is used to activate/deactivate the generation of a terminal authentication during subscription creation. The default value is 1 = YES => terminal authentication generated during subscription creation. This is the case during a first installation, for instance.

Managing the assignment of numbers to subscriptions:

Create a general-purpose subscription.

If automatic creation is authorised, for each subscriber equipment detected, create a subscription, assign it a DID number (read in the external block), or assign it a voice mail box if creation is authorised. Then update its LDAP directory record with the internal number and possibly DID number. Then assign this subscription to the detected equipment and then go to the next equipment.

After processing all the equipment, if automatic creation is allowed, create as many additional subscriptions as necessary (and as possible). Assign them a DID number (read in the external block) and a voice mail box if automatic creation is authorised, then update their LDAP directory record with the internal number and possibly DID number.

- After the last line is validated, a summary of the network parameters is displayed for confirmation.
- The screen then displays a summary of the configuration made.

```
*-------------------------------------------------*
| SUMMARY:
|
*-------------------------------------------------*
| IPADR = 100.100.40.150  |
| NETWORKMASK = 255.255.255.192       |
| GATEWAY = 100.100.40.129      |
| DNS1 = 100.100.40.160|
| NETWORKADR = 100.100.40.128   |
| BROADCAST = 100.100.40.191    |
| NAME =               XL                         |
| IID =                   |
| FIRST =                3000   |
| LAST =                 3999    |
| DID NUMBERING LENGTH = 5             |
| FIRST DID = 3000        |
| FIRST PUBLIC DID =       +33130980000      |
| IVB =                   |
| NUMBERING LENGTH =   4                          |
| COUNTRY =            FRA                        |
| SPOKEN LANGUAGE= FRA/ANG/GER/ESP/POR       |
| LICENCE =            4LMLMLLMLMLMLMLML     |
| PARI =               123456789                  |
| START UP TYPE =      TOTAL    |
*-------------------------------------------------*
DO YOU WANT TO APPLY YOUR CHANGE Y(ES)/N(O)/R(ECONFIGURE) ? Y
```

If the summary is not correct:

- Press "**r**" to restart the preconfiguration.

  To leave the "T" mode and restart with the previous configuration without saving the modifications:

- Press "**n**"; the system restarts with the previous configuration.

If the summary is correct:

- Press "**y**" if the values displayed are correct and confirm by pressing "**Return**".

The system then restarts automatically, and the its IP network link can be set up via the LAN access.

Start-up is now complete and you can configure the site from the user interface.

Note : You can configure automatic or manual start of the SIP gateway or SNMP agent from Web Admin. By default, the SIP gateway is started, and the SNMP agent activated.

1.6 RETRIEVING THE ORIGINAL MANUFACTURER'S ACCESS CODES

The default manufacturer's password can be reset if the user loses the manufacturer's access code modified from Menu **Telephony/System/Configuration/Users/System accounts**.

Rappel : The manufacturer's access code may be modified to reinforce system security.

Preliminary operation

Contact MITEL's customer service to obtain the values **Enter Identifier** and **Enter Key** which will be required during the procedure described below. You also need to provide the (i-Button) ID number. This number must be provided to MITEL in order to generate the values **Enter Identifier** and **Enter Key**.

Procedure

On the PC connected to the COM port

- Open a Hyperterminal window and configure the connection as follows:
  - Bits per second: 115200 bits/s
  - Data bits: 8
  - Parity: none
  - Stop bits: 1
  - Flow control: None
- Power on the cabinet and follow the start-up progress on the PC.
- Upon display of "Identification starting"
- Press **Ctrl** + **I**
- The screen then displays the different configuration modes.

```
Configuration mode (F/T/S/P/U/E)
- F: Factory mode
- T: Total mode
- S: Standard mode
- P: Password reset
- U: USB provisioning mode
- E : for Exit
```

- Select "**P**" mode to enter the pre-configuration menus.

- In the next screen, enter the values **Enter Identifier** and **Enter Key** provided by MITEL.

```
MIVOICE 5000 CONFIGURATION / NETWORK

*-------------------------------------------------*
| ENTER IDENTIFIER : IPNH123LMNVKGH5U
| ENTER NETWORK MASK : POULKJEPOSD5Q9/P
| *-----------------------------------------------*
PLEASE_ENTER_A_VALID_ID_KEY
```

- Press "**Return**" to confirm.
- Then answer "**Y(es)**" to the next questions to complete the procedure.
- At the end of the procedure, the manufacturer's default login and password are regenerated and can be used again.

The manufacturer's default access code will also be reset in Menu **Telephony/System/Configuration/Users/System accounts**.

The Web Admin access login/password are reset:

- Default access login: **admin**
- Default access password: **admin**

1.7 IMPORTING DATA INTO THE IPBX FROM THE DATA COLLECTION FORM

Before importing data, the administrator must back up the iPBX configuration so as to be able to restore it if one or more **.csv** files had not been configured correctly.

Data is imported into the iPBX via Web Admin from Menu **Telephony service**>**System** > **Software maintenance** > **Massive import**:

1. Select and download the file Data.Collecting.zip
2. Click **Take account of the data**.

The duration of import depends on the amount of data to be downloaded. Some counters are displayed to indicate the work progress status.

- Example of counter 12/38: 15
  - 38: number of files to be imported,
  - 12: number of files being imported,
  - 15: line processed in the file being imported.

An installation report is generated at the end of the import.

Additional information on data collection is provided in the MiVoice 5000 Provisioning Excel file - Help tab.

1.2 ADDITIONAL CONFIGURATIONS

You can configure the services (LDAP, SNMP, GSI, FTP, TFTP, etc.) and display their status from Menu "**Telephony service/System/Configuration/Services**" in MiVoice 5000 Web Admin. See MiVoice 5000 Web Admin operating manual (AMT/PD/PBX/0080).

1.8 VIEWING THE IP ADDRESS IN CASE OF LOSS (OFFLINE)

Access via the web interface will no longer be possible if the system's IP parameter value is lost.

In this case, consultation in serial mode is available from a Windows PC equipped with the "Hyperteminal" application.

Access is provided locally on the COM port of the CPU card, using a NULL MODEM cable connected between the COM port of the CPU card and the PC COM port.

Note : For AXD, the card to be used to connect to the COM port is the active UCVD card, and not the IUCVD card or the passive UCVD card.

- Open a Hyperterminal window and configure the connection as follows:
  - Bits per second: 115200 bits/s
  - Data bits: 8
  - Parity: none

- Stop bits: 1
- Flow control: None

- Restart the cabinet.
- Upon display of "Identification starting"
- Press **Ctrl + I**:
- The screen then displays the different configuration modes.

```
Configuration mode (F/T/S/P/E)
- F: Factory mode
- T: Total mode
- S: Standard mode
- P: Password reset
- U: USB provisioning mode
- E : for Exit
```

- Select "**S**" mode to display the network configuration.
- The screen then displays the cabinet’s network configuration.
- Enter "**N**" in this screen and in the next ones if the configuration should not be modified.

2 UPGRADING A SIMPLEX MITEL 5000 GATEWAY R6.X SYSTEM TO R7.0

2.1 PRINCIPLE

This procedure for upgrading to R7.0

applies to XD, XL, XS, XS, XS12 and XS6 systems already working in R6.x including Pack services (SPx).

The upgrade involves replacing (migrating) the iPBX R6.x Compact Flash with a R7.0 formatted Compact Flash.

For a Duplex XD system, two R7.0 formatted Compact Flash cards are required (one for the active card, one for the passive card).

A new R7.0 licence is mandatory.

This upgrade concerns the following data:

- Application data
- LDAP data
- Voicemail files (announcements, prompts, IVR, signatures and messages left on the IVB)
- Local FTP and TFTP server files (sip_stes folders)
- Software files of terminals managed by TMA.

IMPORTANT NOTE : Network settings (IP addresses, mask, gateway and especially DNS 1, 2 and 3) must be noted before the upgrade because they will be lost during this operation. They must be redefined if they have not changed when starting in Total mode using Ctl + i (refer to Section 2.2.4).

2.2 UPGRADE OPERATION

2.2.1 PRELIMINARY OPERATIONS

For any of the backup or restore operations to be performed correctly, the system checks first that:

- A USB key is correctly connected and recognised,
- The active and inactive software releases are valid,
- The TMA related automatic actions have been taken and completed,
- The available space on the USB key, in case of backup, or on the compact flash card, in case of restore, is sufficient for the action.

In case of error, a dialogue box opens and the requested action is not taken.

The exchange directory created by the software is unique on the USB key. It is called **backup_CF**.

Note: During backup and restore, it is not possible to access or leave messages on the IVB.

2.2.2 BACKING UP DATA ON THE USB KEY (4 GB RECOMMENDED)

2.2.2.1 *Procedure*

To perform the upgrade, first connect a USB key (4 GB recommended) to the iPBX CPU card before accessing Menu **SYSTEM/Software maintenance/ Compact flash migration**.

When this menu is selected, the software searches for the key and analyses its content. The target directory on the key is first emptied of its content, if any, or is created if it does not exist.

If no key is detected, a message indicates that no key has been detected:

No USB key detected

On these conditions, connect a key then exit and return to the menu.

If a key is detected, the window is presented in form of a single button, prompting the operator to back up the data to be upgraded on the key:

Start the backup on the USB key.

Press this button to run the backup on the key. A wait message is displayed during the backup operation.

The backup operation may last several minutes, depending especially on the number of voice messages and the amount of TMA data available on the compact flash card.

When the backup is correctly completed, the following message is displayed:

Operation correctly done

The USB key is automatically deactivated at the end of the backup operation.

The operator can then exit the menu and disconnect the key containing the upgrade data.

In case of error, a dialogue box indicates to the operator that the backup has not been made correctly. In this case, the entire data has not been stored on the key. The key is not automatically deactivated; it will be when the menu is exited.

2.2.2.2 *Error messages*

When data is being backed up on the USB key, the following error messages may be returned to the operator:

- "**Transfer error x**" means that an error occurred while data was being copied in step x.
- "**System error, exit and retry**" means that no key is connected or that the maintenance software cannot execute the backup action.
- "**Forbidden function: version test**" means that the software release is not valid.
- "**Other transfer in progress**" means that automatic TMA actions have not been completed.
- "**Cannot delete**" means that the USB key cannot be deleted before the beginning of backup operations.
- "**Error of directory creation**" means that the target directories cannot be created on the USB key.
- "**Not enough free disk space**" means that the space available on the key is not enough to contain all the backed up data.
- "**Impossible export**" means that the data BACKUP file cannot be created.

2.2.3 REPLACING THE COMPACT FLASH CARD

Stop the iPBX by respecting the following two procedures:

- On the CPU card, press briefly the "SHTD" (shutdown) button and wait for the green "SHTD" LED to go steady on and for all the others to go off.
- Power off the power modules (I/O push button on O). **Then** ⌘ remove the CPU card from the cabinet.
- Remove the old Compact Flash card and replace it with a 4 GB, R7.0-formatted Swissbit Compact Flash card.
- The 4 GB compact flash card must be of "**loaded not started**" type and must not have been started before, so the country and spoken languages can be defined using Ctrl + I.
- Reinstall the CPU card.
- Start the iPBX in Ctrl + i mode (see next section).

2.2.4 START WITH THE NEW 4GB CARD IN TOTAL MODE, USING CTRL + I.

Note: For more information on the use of Ctrl +i, see Section Implementing a new Mitel 5000 Gateways installation.

During the start in TOTAL mode usinig CTRL + i, you must fill in the following fields (just like in the previous configuration):

- **Network configuration** (IP address, subnet mask, gateway and DNS 1, 2 and 3)
- **Country**
- **Languages** (out of the five languages proposed, the first two must be the same as in the previous configuration)

- Licence
- **Services** (FTP, TMA and DHCP).

During this first system start using the 4 GB Compact Flash card with factory-configurations, it is necessary to wait at least for 2 minutes after accessing the Web Admin interface via https, before any operation on the iPBX, especially stopping or restarting the iPBX.

After using Ctrl + I, the duration is 7-10 minutes after Ctrl + I is validated.

Then restore the previous R6.x configuration (see next section).

2.2.5 RESTORING DATA FROM THE USB KEY

2.2.5.1 *Prerequisites*

The cabinet has restarted correctly.

The software release is valid.

The USB key containing the backup is connected.

2.2.5.2 *Procedure*

When it accesses the menu **SYSTEM/Software maintenance/Compact flash migration**, the iPBX detects that all the data to be restored is on the connected USB key.

The button below is then displayed:

Restore the content of the USB key

This unique button is used to start importing data into the iPBX.

Like for the previous case, a progress popup window opens during the restore operation. The restore operation takes place like the backup operation in 6 phases. Here too, the operations may last several minutes. This restore operation takes place in inactive mode. After the restore operation, an automatic reset to restart on the inactive version is made.

At the end of the restore operation and before iPBX reset is activated, if the backup has been made correctly, the following message is displayed:

Operation correctly done

The restored data has been erased from the key, and the key deactivated.

During the iPBX restart phase, the following message is displayed:

Restart in progress please wait xx seconds

In case of error, a dialogue box indicates to the operator that the restore has not been made correctly. In this case, all the data remains on the USB key. The key is not automatically deactivated; it will be when the menu is exited.

The duration of the restore operation is about 6 minutes, depending on the content to be restored and the initial and target software releases.

Then validate the software release.

At the end of the procedure, if everything is correct, disconnect the USB key.

2.2.5.3 *Error messages*

When data is being restored on the compact flash card, the following error messages may be returned to the operator:

- "**Transfer error x**" means that an error occurred while data was being copied in step x.
- "**System error, exit and retry**" means that no key is connected or that the maintenance software cannot execute the restore operation.
- "**Forbidden function: version test**" means that the software release is not valid.
- "**Other transfer in progress**" means that automatic TMA actions have not been completed.
- "**Not enough free disk space**" indicates that the space available on the iPBX compact flash card is not enough to contain all the restored data.
- "**Software restitution failure**" indicates that the data restore operation performed by the maintenance software did not take place correctly.

2.2.6 MANAGING AND VIEWING THE FILLING OF DISK SPACE

Compact card filling information is given in Menu **SYSTEM>Supervision>Filling of the disk space**.

From this menu, it is possible to modify the values assigned to each function, including picture management.

For more information, refer to the Operating Manual AMT/PTD/PBX/0080.

2.3 RESTARTING AND VALIDATING THE NEW VERSION

Rappel : After system restart, it is necessary to refresh the browser screen to access Web Admin. It is advisable to close and reopen it. It may also be necessary to delete cookies and temporary files from the browser to obtain a correct display in the web browser.

After the software is upgraded, the installed version is not automatically validated during switchover. You must validate the new version manually after noticing that it is running satisfactorily.

You can validate it through Menu "**SYSTEM> Restart request**".

IMPORTANT NOTES:

As long as the new version is not validated:

- it remains "**in test**",
- a red frame is displayed in the menu area indicating that the active version is not valid.
- It is possible to return to the previous release (see "**SYSTEM>Restart request**"), but the data modified while the software had not been validated will be lost.

ATTENTION : Restore operation will not be possible on the recovered release.

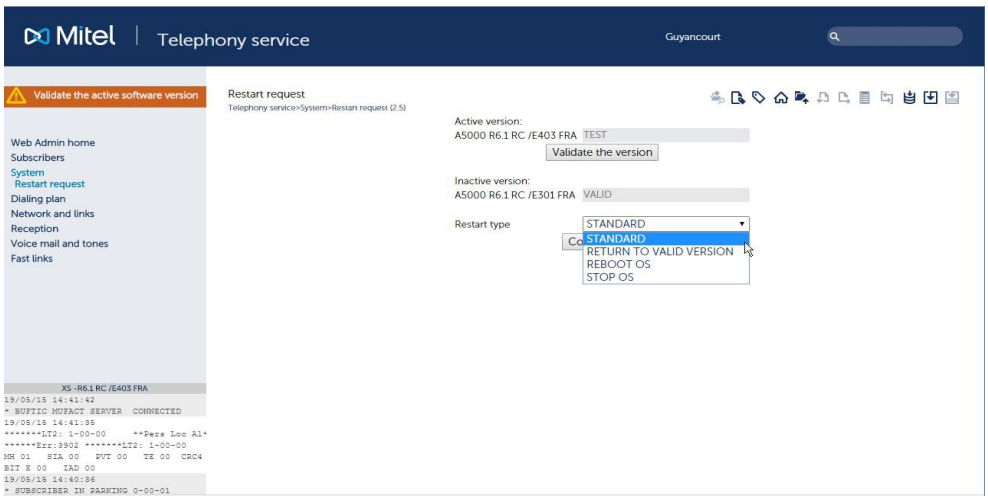
- It is impossible to back up data until the software is validated.

It is advisable to validate the new version as quickly as possible (once you observe a normal operation).

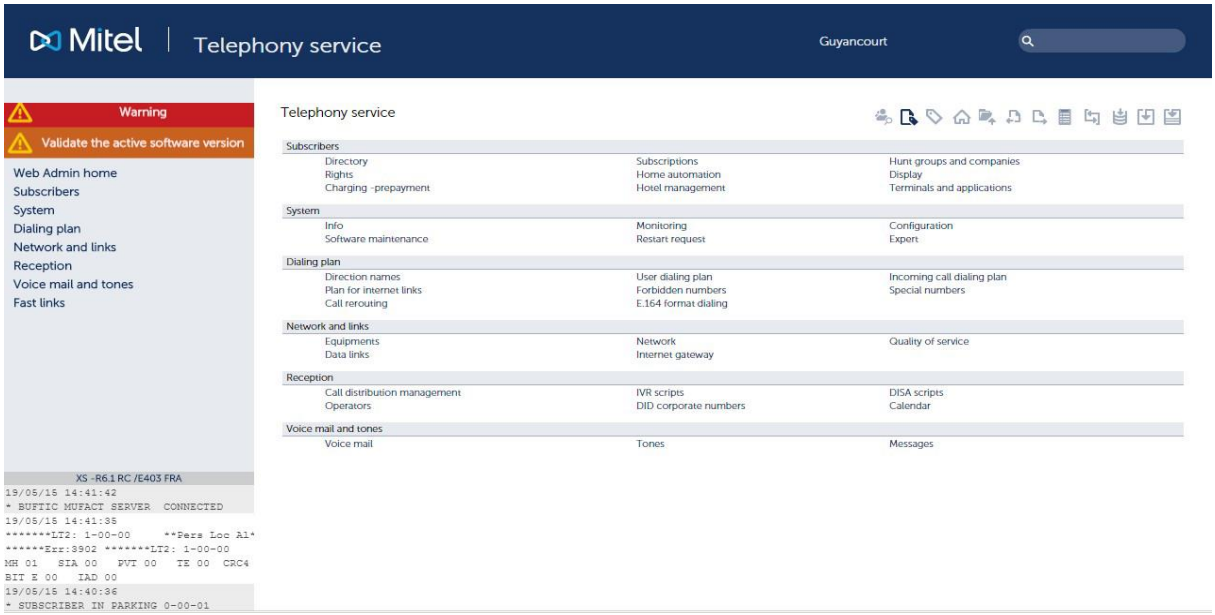
Procedure

Validation and possible cancel requests are proposed in Menu "**SYSTEM/Restart request**" as indicated below.

- To validate the release "**in test**", click "**Validate the version**". The system restarts automatically, declaring the release valid.
- If you do not wish to validate the release "in test" but to return to the previous release, select "Confirm". The system restarts automatically with the previous release.



This menu is also directly accessible via Menu TELEPHONY SERVICE, by clicking the quick link **Validate the active software version**.



For other options, see MiVoice 5000 Web Admin operating manual (AMT/PD/PBX/0080).

3 UPGRADING FROM A SIMPLEX R7.X CONFIGURATION TO R7.X+ 1.

In this case, only the Repository method is applicable. See the document Upgrading by repository AMT/PTD/PBX/0155, Edition 2/ minimum).

4 UPGRADING A DUPLEX XD MITEL 5000 GATEWAY R6.X SYSTEM TO R7.0

For a duplex XD Mitel Gateway system, two R7.0 formatted Compact Flash cards are required (one for the active card, one for the passive card).

The CPU cards must be of UCV2D type.

To upgrade a duplex XD system proceed as follows:

Update the Compact Flash card of the active UCV2D card using the same procedure as for a simplex configuration (see Section Upgrading a Simplex Mitel 5000 Gateway R6.X system to R7.0).

IMPORTANT NOTE : The 4 GB formatted Compact Flash card must be installed on the passive card.
The procedure must be complete, the system restarted and the new version validated on the active card (see Section Restarting and validating the new version).

After the new release is validated on the active card, the system automatically restarts in duplex mode.

- Check the passive card downloading phase, message:

```
"Uc 1-0b passive telechargt",
```

- Wait for the end of the passive card download (several tens of minutes).
- At the end of the downloading operation, the passive card status changes to active,

```
message passive Uc 1-0b in service",
```

- Also check the availability of the following message in the logbook.

```
14:38:47 02/07/08                    2
*Service : duplication       in service*
```

Note: During update, the status of the RUCVD card(s) changes to "IN ALARM".

5 UPGRADING AN XD MITEL 5000 GATEWAY R7.X TO R7.X +1

To upgrade a duplex XD system proceed as follows:

- Update the software of the active UCVD card using the same procedure as for a simplex configuration (see Section Upgrading from a Simplex R7.x configuration to R7.x+ 1.).

IMPORTANT : The procedure must be complete, the system restarted and the new version validated (see Section Restarting and validating the new version).

IMPORTANT NOTE :

The procedure must be complete, the system restarted and the new version validated (see Section Restarting and validating the new version).

After the new release is validated on the active card, the system automatically restarts in duplex mode.

- Check the passive card's downloading phase, message "**passive Uc 1-0b download**".
- Wait for the end of the passive card download (several tens of minutes).
- At the end of the downloading phase, the status of the passive card changes to active, **message** passive Uc 1-0b in service".
- Also check the availability of the following message in the logbook.

```
14:38:47 02/07/08                          2
*SERVICE : DUPLICATION        IN SERVICE*
```

.

Note : During update, the status of the RUCVD card(s) changes to "IN ALARM".

6 INSTALLING MIVOICE 5000 SERVER (NOT REDUNDANT WITHOUT DOUBLE ATTACHMENT)

This chapter describes how to install the non-redundant MiVoice 5000 Server application without double attachment. For the redundant MiVoice 5000 server, refer to AMT/PTD/PBX/0083.

If the redundant or non redundant system must be configured with double attachment, refer to document AMT/PTD/PBX/0059 - Centos 7.x and Double attachment.

Note : Double attachment consists in using two interfaces connected by two separate cables. In this case, we use a virtual "bondx" interface (bonding mode), the only view of the network that allows to switch from one physical interface to the other if any of them fails.

6.1 IMPORTANT PRE-REQUISITE

From R6.3 onwards, CentOS 7.x must first be installed on the PC (in the factory by default).

See the document CentOS 7.x - Double attachment - AMT/PTD/NMA/0059.

The PC network must have been declared and configured (if necessary, contact the network administrator).

The PC must be conected to the network to which it is dedicated (network cable connected).

:

Note : SE Linux and the firewall are deactivated by default when CentOS is being installed from the DVD provided by Mitel.

In a virtual VMware environment a .zip file is available on Mitel's Extranet, for deploying a VM R7.0 called **A5000_A5000_R**7.0_PP_xyzz.

PP: represents the phase (-empty- or SPx)

Xyzz: represents the level/version/phase

Examples:

A5000_A5000_R7.0__AK00.zip

A5000_A5000_R7.0_SPx_C700.zip

This VM contains:

- **CentOS 7.x** preconfigured to support MiVoice 5000 Server R7.0 (partitioning, packaging, etc.),
- MiVoice 5000 Server R7.0: a shortcut on the desktop named **Installation MiVoice 5000 Server** allows its installation.

6.2 INSTALLING THE MIVOICE 5000 SERVER APPLICATION ON A NON-VIRTUAL SYSTEM

- Insert the MiVoice 5000 R7.0 application CD or DVD into the server PC..

- Define a mount point:

  #mkdir /mnt/iso

- Mount the iso image in this directory:

  #mount -o loop ACS_A5000_R7.0_RC_AXYY.iso /mnt/iso

- Launch the installation script:

  #**./first_install.sh**

In the next screen, choose **F5** and press **Enter**

The script is then automatically executed without the user's intervention.

Pre-configuration starts at the end of the script.

Configuring the IP address of the telephony network

```
MiVoice 5000 Configuration / IP Tel
*----------------------------------------*
Select the IP you want to enable for the |||
MiVoice 5000 server (Telephony Network side)

| Enter the choice number or another IP address
|| 0 : 20.1.1.1
|| 1 : Another                          |
*-----------------------------------------------*

Enter your choice: [] ? 0
```

The screen below opens, asking whether the administration network must be configured in case of administration and telephony flow separation.

```
DO YOU WANT TO CONFIGURE MANAGEMENT IP NETWORK ? Y/[N]
```

If this configuration is not necessary, answer "n" and confirm with the "**Return**" key to go to the next screen concerning the country configuration.

If this configuration is necessary in this phase, see the specific document: Operating manual for telephony and administration flow separation - AMT/PTD/PBX/0101.

Country configuration (locating menu labels and displaying sets)

```
MiVoice 5000 Configuration / Country

*-------------------------------------------------*
| Enter Country: GB
*-------------------------------------------------*
Do you want to change configuration Y(es)/N(o) ? n
```

This screen corresponds to the configuration of the country in which the system will be installed. Choosing the country code makes it possible to define the type of encoding law used by the .wav files deployed by the voice functions of the MEDIA SERVER as well as the five default spoken languages.

- If necessary, modify the value proposed, otherwise press "**n**" (to keep the proposed value).

```
MIVOICE 5000 CONFIGURATION / Country
*-------------------------------------------------*
| ENTER COUNTRY: FRA |
*-------------------------------------------------*
| => FRA |
| => ANG                          |
| => GER |
| => ... |
| => ... |
| => TWN |
| => BEL |
| => EXP |
*-------------------------------------------------*
DO YOU CONFIRM (Y/N)? Y
```

- Enter the country code in case of modification.
- Confirm or do not confirm the modification by pressing "y" or "n".

Configuring the spoken languages

The spoken language configuration menu is used to define the 5 spoken languages used by the following MEDIA SERVER service functions:

- Announcement (ANN)
- Voicemail (IVB)
- Interactive Voice Response (IVR)

```
MiVoice 5000 Configuration / Spoken Language

An existing configuration was found

*----------------------------------------

| Enter Language 1 : FRA
| Enter Language 2 : ANG
| Enter Language 3 : GER
| Enter Language 4 : ESP
| Enter Language 5 : POR
*--------------------------------------*

Do you want to change configuration Y/[N]? Y
```

- If the 5 languages defined by default must be modified, press "**y**".

The 5 spoken languages defined by default can be modified on the screen, among the ones proposed.

```
MIVOICE 5000 CONFIGURATION / SPOKEN LANGUAGE
*-------------------------------------------------
 ----------------------*
| ENTER LANGUAGE 1 :FRA
| ENTER LANGUAGE 2 :ANG
| ENTER LANGUAGE 3 :GER
| ENTER LANGUAGE 4 :ESP
| ENTER LANGUAGE 5 :POR
*-----------------------------------------*
|       ANG      CTL      DAN
|       ESP      FIN      FLA
|       FRA      GER      HOL
|       ITA      MDT      MEX
|       NOR      POL      POR
|       SUE      TCH      USA
*--------------------------------------*
DO YOU CONFIRM (Y/N) (PRESS ENTER TO RECONFIGURE) ? Y
```

- For each of the 5 spoken languages, in case of modification, enter the language code.
- Press "**Return**" to validate each spoken language.
- Confirm or do not confirm the modifications by pressing "**y**" or "**n**".

Configuring the licence

```
MiVoice 5000 Configuration / Licence

*-------------------------------------------------*
| Licence:                                        |
*-------------------------------------------------*
Do you want to change configuration Y(es)/N(o) ? n
```

- Enter the corresponding value of the release (optional: it may be entered later from Web Admin).

For a virtual or physical machine, during first installation, if the licence is not known, it is necessary to access Web Admin with Ctrl +i, and to follow the procedure described in Section Accessing the user interface (MiVoice 5000 Web Admin).

- Validate the modifications with the "Return" key, after confirming or rejecting them by pressing "**y**" or "**n**".

Configuring PARI

```
MIVOICE 5000 CONFIGURATION / PARI
 AN EXISTING CONFIGURATION WAS FOUND
*-------------------------------------------------*
| | PARI :                  123456789 |
| *-----------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ?
```

- To modify the system's PARI number, type in "**y**" and enter the corresponding value.
- Press "Return" to confirm this modification.

- Confirm or do not confirm this modification by pressing "y" or "n".

Installing the services

This menu is used to install the following services:

- DHCP
- FTP
- TFTP
- SYSLOG
- Announcement
- IVR
- IVB
- CONF

If you wish to manage any of these services, you must install it in advance. Installing the service enables you to modify its status and configuration later via Web Admin.

The FTP service (accounts and storage directories) is automatically configured when the FTP service is started by Web Admin.

The TFTP service is automatically configured when the TFTP service is started by Web Admin. Menu Telephony service > System > Software maintenance > Tftp: loading of files is only accessible if the TFTP service is installed. This menu is used to place the firmware of terminals A6xxd, 312i and Mitel DECT-IP base stations (RFPs) in the TFTP server storage directory.

The SYSLOG service is configured manually and via the menu: Telephony service > System > Expert Processor access > Debug tool >Traces > Parameters. The IP address configuration is only accessible if the SYSLOG service is installed and if the "step-by-step output" line is validated.

The DHCP service is automatically configured when the DHCP service is started. In a redundant MiVoice 5000 Server configuration, the DHCP service cannot be installed and managed by Web Admin. In this case, it is managed directly by the operating system.

The MEDIA SERVER service comprises the following four functions:

- Announcement: managing announcements and tones (255 announcements and tones maximum)
- IVR: managing the interactive voice response (15 scripts maximum)
- IVB: managing the integrated voicemail boxes (15000 IVBs maximum)
- CONF: managing three-way conferences

ATTENTION : G.711 (A law or µ law), G.729 and G.722 are available and are used by the announcement, IVR, IVB and conference functions of the MEDIA SERVER service.

ATTENTION : G.711 40ms and G.722 40ms are not supported by terminals A53xxip.

```
MIVOICE 5000 CONFIGURATION / MANAGED SERVICE
ACTUAL CONFIGURATION IS:
*-----------------------------------------------*
| DHCP (0/1) :                  0          |
| FTP (0/1) :                   0    |
| TFTP (0/1):                   1    |
| SYSLOG (0/1):                 0    |
| SSH (0/1) :                    0         |
| ANNOUNCEMENT (0/1):           1    |
| IVR (0/1):                    1    |
| IVB (0/1):                    0    |
| CONFERENCE(0/1) :        1    |
*-----------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y/[N]? Y
```

- To install a service, press "y". The next screen is used to modify the value of the DHCP, FTP, TFTP, SYSLOG, SSH, ANNOUNCEMENT, IVR, IVB and CONFERENCE fields. The values entered must be 0 (service not installed) or 1 (service installed).
- If any of the four functions ANNOUNCEMENT or IVR or IVB or CONFERENCE is installed, the MEDIA SERVER service is automatically installed.
- Press "Return" to confirm each modification.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

Configuring service start

The status of the FTP, TMA and DHCP services can be modified so they may or may not be started automatically. If a service is not configured to start automatically, Menu Telephony service > System > Configuration > Web Admin services can be used to start them manually later.

The FTP service is used to download via TMA the firmware and configuration files used by MiVoice 5300 IP Phones and Mitel 6000 SIP Phones and the firmware used by Mitel 53xx phones. See Terminal installation manual - AMT/PTD/TR/0014.

The TMA service is used by TMA, and to manage IP and TDM terminals. See Terminal installation manual - AMT/PTD/TR/0014. The TMA service configuration is accessible via the Web Admin terminal service menu.

The DHCP service allows a lease to be automatically assigned to MiVoice 5300 IP Phones and Mitel 6000 SIP Phones and negotiates with them the standard and specific parameters required to configure them. Refer to the MiVoice 5300 IP Phone and Mitel 6000 SIP Phone Mitel 53xx Installation Manual - AMT/PTD/TR/0014.

```
MIVOICE 5000 CONFIGURATION / SERVICES TO START AUTOMATICALLY
AN EXISTING CONFIGURATION WAS FOUND
*-----------------------------------------------------*
| FTP (0/1) :              0    |
| TMA (0/1) :                   1    |
| DHCP (0/1) :                  0    |
```

- If the answer is YES, "y", the screen below can be used to modify the value of the FTP, TMA and DHCP fields. The values entered may be 0 (automatic service start) or 1 (manual service start via Web Admin).

- Press "Return" to confirm each modification.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

```
MIVOICE 5000 CONFIGURATION / SERVICES TO START AUTOMATICALLY
AN EXISTING CONFIGURATION WAS FOUND
*-------------------------------------------------*
| FTP (0/1) :                  1 |
| TMA (0/1) :                  1 |
| DHCP (0/1) :                 1 |
*-------------------------------------------------*
```

FTP: value 0 or 1.

This field allows (1 = yes) or disallows (0= no) the use of the integrated FTP server on MiVoice 5000 Server during first installation. The FTP server must be active (1) to then use the integrated DHCP and TMA services.

Default value in factory settings: **FTP = O**

TMA: value 0 or 1.

This field allows the use (1 = yes) or non-use (0= no) of the TMA service integrated into MiVoice 5000 Server. For management by MiVoice 5000 Manager, the integrated TMA service is inactive since management is centralised for all the terminals on MiVoice 5000 Manager.

Default value in factory settings: **TMA = 1**

DHCP: value 0 or 1.

This field allows (1 = yes) or disallows (0= no) the use of the integrated DHCP service on MiVoice 5000 Server.

If an external DHCP server is used, the DHCP service is inactive.

Configuring the deployment of Mitel 6700 SIP Phones

If DHCP is on 0 in the previous service start menu, the parameters TERMINAL VLAN and PC VLAN are proposed in the Mitel 6700 SIP Phone configuration menu.

```
MiVoice 5000 Configuration / SIP Mitel 6700 SIP Phone
 An existing configuration was found
*-------------------------------------------------*
|
| LLDP ENABLED : 0                                |
| TERMINAL VLAN:               |
| PC VLAN:                     |
*-------------------------------------------------*
Do you want to change configuration Y(es)/N(o) ?  N
```

LLDP ENABLED

This field is used to activate the LLDP in Mitel 6700 SIP Phone (1 = yes) or not (0= no).

TERMINAL VLAN and PC VLAN: These parameters are used to define the VLAN dedicated to Mitel 6700 SIP Phones. They are not mandatory on simple networks.

If DHCP is on 1 in the previous service start menu, the parameters TERMINAL VLAN and PC VLAN are not proposed in the Mitel 6700 SIP Phone configuration menu.

```
MiVoice 5000 Configuration / SIP Mitel 6700 SIP Phone
 An existing configuration was found
*-----------------------------------------------*
| LLDP ENABLED : 0                              |
*-----------------------------------------------*
Do you confirm (Y/N)?
```

- If necessary, modify the value of the LLDP field.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

DHCP server configuration

If the DHCP service had been previously installed, this menu can be used to automatically pre-configure the DHCP server for Mitel 6700 SIP Phones and for terminals A53xxip and i7xx.

IMPORTANT : This DHCP pre-configuration requires that the deployed network interface be called eth0.

If this is not the case, the DHCP server must be reconfigured from Web Admin, following the procedure described in Section Modifying the DHCP server configuration from Web Admin.

```
Mitel 5000 Configuration / DHCP
*-------------------------------------------------*
| SUBNET MASK :         255.255.255.0           |
| BEGIN RANGE :         20.1.1.100            |
| END RANGE :           20.1.1.199             |
| GATEWAY :             20.1.1.254               |
| TERMINAL VLAN:
|
| PC VLAN:                                       |
*-----------------------------------------*
Do you confirm (Y/N) (Press enter to reconfigure) ? y
```

SUBNET MASK: subnet mask dedicated to IP and SIP terminals

BEGIN RANGE and END RANGE: address range dedicated to IP and SIP terminals

GATEWAY: IP address of the network gateway dedicated to the IP and SIP terminals

TERMINAL VLAN and PC VLAN: These parameters are used to define the VLAN dedicated to Mitel 6700 SIP Phones and to terminals A53xxip and i7xx. They are not mandatory on simple networks.

- Press "Return" to confirm each input.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

Configuring Name & IID

The system's general parameters declaration screen opens (name IID (system identification number)):

```
MIVOICE 5000 CONFIGURATION / Name&IID
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE NAME/IID (Y/N): Y |
```

- If you answer YES, "**y**", the next screen allows you to declare the system's general parameters (11 digits).

```
MIVOICE 5000 CONFIGURATION / Name&IID

*-------------------------------------------------*
| NAME: MIVOICE 5000 |
| IID: 00130927001 |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

- Press "Return" to confirm the modifications.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

Configuring the numbering plan length

```
MIVOICE 5000 CONFIGURATION / NL
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE NUMBERING LENGTH: Y |
*-------------------------------------------------*
```

- Press "**Return**" to confirm, after entering "**y**" or "**n**".

If the answer is "y", enter the corresponding values.

The field is used to define the internal number length to take into account (2 to 10).

```
MIVOICE 5000 CONFIGURATION / NL

*-------------------------------------------------*
| NUMBERING LENGTH: 4 |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

- Press "Return" to confirm the modifications.
- Then confirm or do not confirm this modification by pressing "y" or "n".

Configuring call distribution

```
MIVOICE 5000 CONFIGURATION / Call Dist
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE CALL DISTRIBUTION: Y |
*-------------------------------------------------*
```

- Press "**Return**" to confirm, after entering "**y**" or "**n**".

If the answer is "y", enter the corresponding values.

```
MIVOICE 5000 CONFIGURATION / Call Dist
AN EXISTING CONFIGURATION WAS FOUND
*-------------------------------------------------*
| SUBSCRIBER: 3005 |
| DID: 4000 |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

SUBSCRIBER:

This field allows you to assign a subscription number as a day number reduced to reception 0. This number is assigned if it corresponds to an internal subscription which can be added to a call distribution service, or if it corresponds to the number of a subscription that may be on the multi-site network (MiVoice 5000 Server).

DID:

This field is used to assign a DID number to call distribution service0. Authorised characters are “0123456789ABCDE”.

- Press "Return" to confirm the modifications.
- Then confirm or do not confirm these modifications by pressing "y" or "n".

Configuring subscriptions

```
MIVOICE 5000 CONFIGURATION / Subscribers
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE SUBSCRIBERS (Y/N): Y |

*--------
```

If the answer is "y", enter the corresponding values for the different fields described below.

```
MIVOICE 5000 CONFIGURATION / Subscribers

*-------------------------------------------------*
| CREATION (0/1) : 1          |
| IVB CREATION (0/1) : 1      |
| UNIFIED IVB (0/1): 1        |
| FIRST : 3000                |
| LAST : 3999                 |
| DID NUMBERING LENGTH 4           |
| FIRST DID : 3000            |
| FIRST PUBLIC DID : +33(0)130923000    |
| IVB : 3998                  |
| COMMON SUBSCRIBER : 3500    |
| ADDITIONNAL SUBSCRIPTIONS : 40   |
| PASSWORD SUBSCRIBERS: 0000 |
| GENERATION OF SETS AUTHENTICATION=1   |

*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

CREATION:

This field may be used to inhibit automatic subscriber creation. This field may take on the values 0 (= creation inhibited) or 1(= creation authorised).

The **numbering length** field defined on the previous screen contains the internal number length to take into account (2 to 6). If this is a valid value, the fields **first, last, common subscriber** will be taken into account. Otherwise, they will be ignored.

IVB CREATION:

This field is used to automatically create the voicemail boxes associated with the automatically created subscriptions. This field is only proposed if the IVB function is installed.

UNIFIED IVB:

The **Unified IVB** field is used to define some unified voice mail boxes, if available.

FIRST:

This field contains the first internal subscription that can be created automatically.

LAST:

This field contains the last internal subscription that can be created automatically.

DID numbering length:

This field is used to define the internal number length in the incoming number plan (i.e. DID numbers).

FIRST DID:

This field is used to create the external block 0 associated with the internal number block [first, last]. Authorised characters are " 0123456789ABCDE". For this block to be created, this number must belong to an incoming number plan.

FIRST PUBLIC DID:

The field is used to associate a public number (format: 0130967000 or +33(0)130967000) with the DID number for block 0. This ASCII string will be truncated to 20 characters.

IVB:

This field is used to define the IVB access number. This field is only proposed if the IVB function is installed.

COMMON SUBSCRIBER:

This field is only read and taken into account if it is in the complete block and if this number exists already. If this is not the case, or if the field does not exist, they are assigned a default number. If their value is 0, they will not be assigned any number. The **common subscriber** field must always have a number.

ADDITIONNAL SUBSCRIPTIONS:

This field indicates the number of further internal subscriptions to create.

Password Subscribers:

This field is used to define the default subscriber password.

This same password will be used to access the IVB and to deploy Mitel 6000 SIP Phones.

Generation of sets authentication=1

This field is used to activate/deactivate the generation of a terminal authentication during subscription creation. The default value is 1 = YES => terminal authentication generated during subscription creation. This is the case during a first installation, for instance.

Managing the assignment of numbers to subscriptions:

Create a general-purpose subscription.

If automatic creation is authorised, for each subscriber equipment detected, create a subscription, assign it a DID number (read in the external block), or assign it a voice mail box if creation is authorised. Then update its LDAP directory record with the internal number and possibly DID number. Then assign this subscription to the detected equipment and then go to the next equipment.

After processing all the equipment, if automatic creation is allowed, create as many additional subscriptions as necessary (and as possible). Assign them a DID number (read in the external block) and a voice mail box if automatic creation is authorised, then update their LDAP directory record with the internal number and possibly DID number.

- Press "**y**" and confirm by pressing "**Return**".
- The screen then displays a summary of the configuration made (example).

```
| SUMMARY:
*-------------------------------------------------*
| IPADR = 20.1.1.1          |
| NAME = MIVOICE 5000       |
| IID = 00130927001         |
| FIRST : 3000              |
| LAST : 3999               |
| DID NUMBERING LENGTH 4         |
| FIRST DID : 3000          |
| FIRST PUBLIC DID : +33(0)130923000  |
| IVB : 3998                |
| NUMBERING LENGHT = 4      |
| COUNTRY = FRA             |
| LICENCE = 123456789123    |
| PARI =                    |
| START UP TYPE = TOTAL     |
| DEDICATED SNMPD = Y       |
|     |
*-------------------------------------------------*
DO YOU WANT TO APPLY YOUR CHANGE Y(ES)/N(O)/R(ECONFIGURE) ? Y
```

If the summary is not correct:

- Press "**r**" to restart the preconfiguration (from the first “Choose country” screen).
- If the summary is correct:
- Press "**y**" if the values displayed are correct and confirm by pressing "**Return**".

Restarting the virtual MiVoice 5000 Server PC

On the MiVoice 5000 Server PC:

- Go to Menu **System > Stop**.
- Click the "**Restart**" button.
- Wait for the end of the start operation.

The configuration phase is complete.

Initial installation has been completed and you can now configure the site (see MiVoice 5000 Web Admin operating manual).

6.3 INSTALLING THE MIVOICE 5000 SERVER APPLICATION IN A VIRTUAL ENVIRONMENT

6.3.1 DEPLOYING THE VIRTUAL MACHINE

6.3.1.1 *In a VMWare environment*

From a.zip file called **A5000_A5000_R**7.0_PP_xyzz.zip, provided by Mitel, proceed as follows:

- Unzip the content of the .zip file to a local disk or network space. This space must be accessible from the ESX Server vSphere client on which the MiVoice 5000 Server R7.0 VM must be installed.

Note : The content of the zip file may also be burned onto a DVD.

- Connect to the ESX server machine via the client vSphere.
- Click Menu **File>Deploy OVF model**.
- Click on the **Browse** button and select the disk or DVD space in which the file **A5000_A5000_R7.0_PP_xyzz.ovf** or the file **A5000_A5000_R7.0_PP_xyzz.ova** is located.
- Then click **Next**.
- Check the details of the deployed model then click **Next**.
- Check and, if necessary, modify the VM name then click **Next**.
- Selecting the disk format
  - For ESXi 5 and 6, tick Static provisioning reset immediately.
  - For ESXi 4, tick **Thick provisioned format**.
  - Then click **Next**.

ATTENTION : *The VM requires 90 GB hard disk space, 2 cores and 4 GB RAM.*

Note : The number of cores and size of RAM in the VM can be modified, if necessary, according to the load from Menu Modify virtual machine parameters, Hardware tab.

- Implement mapping according to available network interfaces.
- Click **Finish** to start deploying the VM **A5000_A5000_R7.0_PP_xyzz**.
- Wait till the end of the deployment operation then click **Close**.
- Select the VM **A5000_A5000_R7.0_PP_xyzz** then start it by clicking the green arrow.
- Click the **Console** tab.
- Log on as root (default password: **Mitel5000**)

ATTENTION : The system input language is English, and the keyboard format QWERTY. The numeric keypad is not activated.

Modify the system language and keyboard language.

Depending on the language you want, type the following:

- To French:

  # localectl set-keymap fr

- To English:

  localectl set-keymap us

6.3.1.2 *In a KVM environment*

Content of the archive in tgz format

The archive file **A5000_SAAS-KVM_R7.0_xyz.tgz** contains:

- The disk file (.**qcow2**)
- The systems characteristics XML file (.**xml**)
- The MD5 signature of previous files (.**md5**)

VM content

The VM contained in the archive file has been generated from the following items:

- CentOS 7.x - 64 bits
- A Kick-start "Saas" file
- Two network interfaces (eth0/br0 =>saaslan, eth1=>saaswan)
- RAM=1 GB
- Disk size=10 GB
- 1 VCPU

VM deployment

Note : Files must be extracted from the TGZ archive in Linux, on the target machine with KVM packaging.

From the archive file **A5000_SAAS-KVM_R**7.0_xyz.tgz, available on the Mitel extranet, proceed as follows:

Copy the archive file **A5000_SAAS-KVM_R**7.0_xyz.tgz to a directory on the KVM server on which the MiVoice 5000 Server R7.0 VM must be deployed.

Note : The partition to which the archive file A5000_SAAS-KVM_R7.0_xyz.tgz will be copied must have at least 10 GB space available.

Go to the directory to which the archive files have been copied and extract the archive files using the command "**tar xzf A5000_SAAS-KVM_R**7.0_xyz.tgz".

Copy the disk file (.qcow2) to the directory /var/lib/libvirt/images

Copy the file (.xml) to the /tmp work directory.

Type in the **virsh net-list -all** command in order to list the network interfaces declared on this Linux machine for KVM virtualisation.

Edit the systems characteristics XML file (.xml) located in /tmp and adapt the VM to the characteristics of the machine and, in particular, **saaslan** and **saaswan.**

Install the VM with this command:

virsh define /tmp/ A5000_SAAS-KVM_R7.0_xyz.xml

Start the VM with this command:

virsh start A5000_SAAS-KVM_R7.0_xyz

Set the VM to automatic start with this command:

virsh autostart A5000_SAAS-KVM_R7.0_xyz

Connect to the VM (login: c2ic and password: c2ic)

virsh console A5000_SAAS-KVM_R7.0_xyz

return

login: c2ic

password: c2ic

Note : To exit the virsh console, press Ctrl+5. Do not use the numeric keypad.

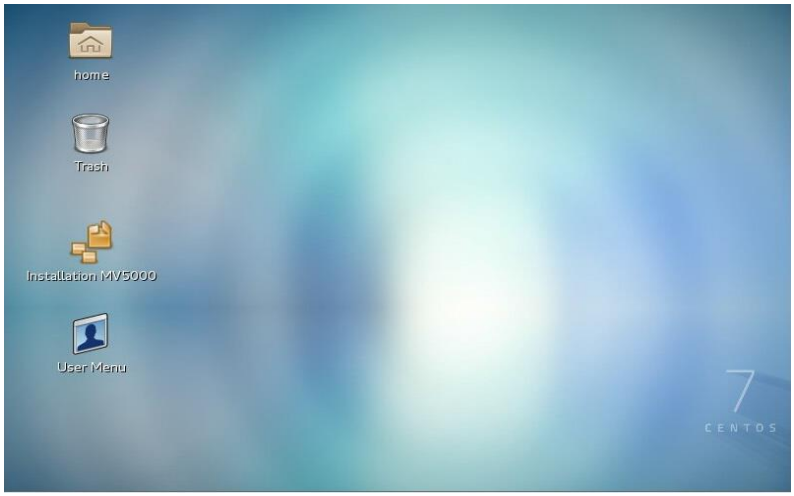
See Section Configuring the network interfaces via the User menu.

6.3.2 CONFIGURING THE NETWORK INTERFACES VIA THE USER MENU

It is necessary to configure the network interfaces.

On the desktop

- Click the **User Menu** icon.



The configuration menu opens. Answer the different questions as follows:

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

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

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

Configuring LANA (and possibly LANB for VPN, SBC services)

```
CONFIGURE NETWORK
1) LANA
2) LANB
3) QUIT
SELECT INTERFACE: 1 ----------------> (PRESS 1 FOR LANA)

CONFIGURING LANA
IP ADDRESS [Y] ? 10.10.10.10 ---------> (ENTER THE IP ADDRESS IN QUESTION)
NETMASK [Y] ? 255.255.255.0 ----------->(ENTER THE MASK IN QUESTION)
APPLY Y/N [N] ? Y
```

Press **Return** to confirm.

The script is run.

At the end, the menu below opens (after pressing **Return**):

```
SELECT INTERFACE:
1) LANA
2) LANB
3) QUIT
SELECT INTERFACE: 3 ----------------> (PRESS 3 TO EXIT)
```

Note : If the LANB interface must be configured (VPN, SBC), select 2 LANB to configure it using the same procedure as for LANA. This configuration may be made later.

Configuring the default gateway (LANA)

From the previous screen:

```
NETWORK CONFIGURATION MENU

NETWORK - SELECT MENU:
1) IP-ADDRESS          3) DNS                      5) BRIDGE
2) ROUTES              4) HOSTNAME              6) QUIT
NETWORK - SELECT MENU: 2 ---> (PRESS 2 TO ACCESS THE GATEWAY CONFIGURATION MENU

ROUTE CONFIGURATION MENU
1) SHOW                3)ADD                     5) APPLY
2) DEFAULTGW           4)DELETE                  6) QUIT
ROUTES - SELECT MENU : 2 ---> (PRESS 2 TO ACCESS THE GATEWAY CONFIGURATION MENU)

ENTER DEFAULT GATEWAY : 10.10.10.1

1) LANA
2) LANB
SELECT INTERFACE: 1 ----------------> (PRESS 1 FOR LANA)

ROUTES SELECT MENU
1) SHOW                3)ADD                     5) APPLY
2) DEFAULTGW           4)DELETE                  6) QUIT
ROUTES - SELECT MENU : 5 ---> (PRESS 5 TO CONFIRM)

THE SYSTEM RESTARTS.
RESTARTING NETWORK (VIA SYSTEMCTL) : [OK]

ROUTES SELECT MENU
```

```
1) SHOW              3)ADD                    5) APPLY
2) DEFAULTGW         4)DELETE                 6) QUIT
ROUTES - SELECT MENU : 6 ---> (PRESS 6 TO EXIT)

NETWORK CONFIGURATION MENU

1) IP-ADDRESS  3) DNS       5) BRIDGE
2) ROUTES      4) HOSTNAME    6) QUIT
NETWORK - SELECT MENU: 6 ---------------> (PRESS 6 TO EXIT)
```

The main menu is displayed again.

Installing MiVoice 5000 Server from the User menu in TOTAL mode

The MiVoice 5000 Server installation script is automatically executed without the user's intervention. Pre-configuration starts at the end of the script.

```
SELECT AN OPTION AND PRESS ENTER:
1) REBOOT              6) UPDATEOS-SECURITY        11) IDENTIFICATION
2) NETWORK             7) TOTAL                    12) KEYBOARD
3) SET-NTP-SERVER      8) STANDARD                 13) LOGOUT
4) PASSWORD            9) BACKUP-SPECIFIC
5) UPDATEOS-FULL       10) RESTORE-SPECIFIC

SELECT AN OPTION AND PRESS ENTER: 7 ---------------> (PRESS 7 TO RESTART IN TOTAL
 MODE)
```

Configuring the IP address of the telephony network Choose the IP address previously configured for LANA

```
MiVoice 5000 Configuration / IP Tel
*-------------------------------------------------------------------------*
| Select the IP you want to enable for the                                 |
| MiVoice 5000 server (Telephony Network side)
|
| Enter the choice number or another IP address                            |
| 0 :10.10.10.10
| 1 :10.10.10.10
| 2 :10.10.10.10
| 3: Another                                                              |
*-------------------------------------------------------------------------*
Enter your choice: [] ? 0
```

IMPORTANT : The choice must be 0 - the default LAN address.

The screen below opens, asking whether the administration network must be configured in case of administration and telephony flow separation.

```
DO YOU WANT TO CONFIGURE MANAGEMENT IP NETWORK ? Y/[N]
```

If this configuration is not necessary, answer "n" and confirm with the "**Return**" key to go to the next screen concerning the country configuration.

If this configuration is necessary in this phase,See the specific document: Operating manual for telephony and administration flow separation - AMT_PTD_PBX_0101.

Country configuration (locating menu labels and displaying sets)

```
MiVoice 5000 Configuration / Country

*-------------------------------------------------*
| Enter Country: GB
*-------------------------------------------------*
Do you want to change configuration Y(es)/N(o) ? n
```

This screen corresponds to the configuration of the country in which the system will be installed. Choosing the country code makes it possible to define the type of encoding law used by the .wav files deployed by the voice functions of the MEDIA SERVER as well as the five default spoken languages.

- If necessary, modify the value proposed, otherwise press "**n**" (to keep the proposed value).

```
MIVOICE 5000 CONFIGURATION / Country
*-------------------------------------------------*
| ENTER COUNTRY: FRA |
*-------------------------------------------------*
| => FRA |
| => ANG                          |
| => GER |
| => ... |
| => ... |
| => TWN |
| => BEL |
| => EXP |
*-------------------------------------------------*
DO YOU CONFIRM (Y/N)? Y
```

- Enter the country code in case of modification.
- Confirm or do not confirm the modification by pressing "y" or "n".

Configuring spoken languages

The spoken language configuration menu is used to define the 5 spoken languages used by the following MEDIA SERVER service functions:

- Announcement (ANN)
- Voicemail (IVB)
- Interactive Voice Response (IVR)

```
MiVoice 5000 Configuration / Spoken Language

An existing configuration was found

*-------------------------------------------

| Enter Language 1 : FRA
| Enter Language 2 : ANG
| Enter Language 3 : GER
| Enter Language 4 : ESP
| Enter Language 5 : POR
*-------------------------------------------*
```

- If the 5 languages defined by default must be modified, press "**y**".
- The 5 spoken languages defined by default can be modified on the screen, among the ones proposed.

```
MIVOICE 5000 CONFIGURATION / SPOKEN LANGUAGE
*--------------------------------------*
| ENTER LANGUAGE 1 :FRA
| ENTER LANGUAGE 2 :ANG
| ENTER LANGUAGE 3 :GER
| ENTER LANGUAGE 4 :ESP
| ENTER LANGUAGE 5 :POR
*-------------------------------------------*
|       ANG      CTL      DAN
|       ESP      FIN      FLA
|       FRA      GER      HOL
|       ITA      MDT      MEX
|       NOR      POL      POR
|       SUE      TCH      USA
*-------------------------------------------*
DO YOU CONFIRM (Y/N) (PRESS ENTER TO RECONFIGURE) ? Y
```

- For each of the 5 spoken languages, in case of modification, enter the language code.
- Press "**Return**" to validate each spoken language.
- Confirm or do not confirm the modifications by pressing "**y**" or "**n**".

Configuring the license

```
MiVoice 5000 Configuration / Licence

*-------------------------------------------------*
| Licence:                                        |
*-------------------------------------------------*
Do you want to change configuration Y(es)/N(o) ? n
```

- Enter the corresponding value of the release (optional: it may be entered later from Web Admin).

For a virtual or physical machine, during first installation, if the licence is not known, it is necessary to access Web Admin with Ctrl +i, and to follow the procedure described in Section Accessing the user interface (MiVoice 5000 Web Admin).

- Validate the modifications with the "**Return**" key, after confirming or rejecting them by pressing "**y**" or "**n**".

Configuring PARI

- To modify the system's PARI number, type in "**y**" and enter the corresponding value.
- Press "**Return**" to confirm this modification.
- Confirm or do not confirm this modification by pressing "**y**" or "**n**".

Installing the services

This menu is used to install the following services:

- DHCP
- FTP
- TFTP
- SYSLOG
- Announcement
- IVR
- IVB
- CONF

If you wish to manage any of these services, you must install it in advance. Installing the service enables you to modify its status and configuration later via Web Admin.

The FTP service (accounts and storage directories) is automatically configured when the FTP service is started by Web Admin.

The TFTP service is automatically configured when the TFTP service is started by Web Admin. Menu Telephony service > System > Software maintenance > Tftp: loading of files is only accessible if the TFTP service is installed. This menu is used to place the firmware of terminals A6xxd, 312i and Mitel DECT-IP base stations (RFPs) in the TFTP server storage directory.

The SYSLOG service is configured manually, via Menu **Telephony Service>System>Expert>Processor access>Debug tools>Traces>Parameters**. The IP address configuration is only accessible if the SYSLOG service is installed and if the "step-by-step output" line is validated.

The DHCP service is automatically configured when the DHCP service is started. In a redundant MiVoice 5000 Server configuration, the DHCP service cannot be installed and managed by Web Admin. In this case, it is managed directly by the operating system.

The MEDIA SERVER service comprises the following four functions:

- Announcement: managing announcements and tones (255 announcements and tones maximum)
- IVR: managing the interactive voice response (15 scripts maximum)
- IVB: managing the integrated voicemail boxes (15000 IVBs maximum)
- CONF: managing three-way conferences

ATTENTION : G.711 (A law or µ law), G.729 and G.722 are available and are used by the announcement, IVR, IVB and conference functions of the MEDIA SERVER service.

ATTENTION : G.711 40ms and G.722 40ms are not supported by terminals A53xxip.

```
MIVOICE 5000 CONFIGURATION / MANAGED SERVICE
ACTUAL CONFIGURATION IS:
*-------------------------------------------------*
| DHCP (0/1) :                      0           |
| FTP (0/1) :                       0     |
| TFTP (0/1):                1      |
| SYSLOG (0/1):              0      |
| SSH (0/1) :                 0          |
| ANNOUNCEMENT (0/1):        1      |
| IVR (0/1):                 1      |
| IVB (0/1):                 0      |
| CONFERENCE(0/1) :          1      |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y/[N]? Y



*-------------------------------------------------*
```

- To install a service, press "**y**". The next screen is used to modify the value of the DHCP, FTP, TFTP, SYSLOG, SSH, ANNOUNCEMENT, IVR, IVB and CONFERENCE fields. The values entered must be 0 (service not installed) or 1 (service installed).
- If any of the four functions ANNOUNCEMENT or IVR or IVB or CONFERENCE is installed, the MEDIA SERVER service is automatically installed.
- Press "**Return**" to confirm each modification.
- Then confirm or do not confirm the modifications by pressing "**y**" or "**n**".

Configuring service start

The status of the FTP, TMA and DHCP services can be modified so they may or may not be started automatically. If a service is not configured to start automatically, Menu Telephony service > System > Configuration > Web Admin services can be used to start them manually later.

The FTP service is used to download via TMA the firmware and configuration files used by MiVoice 5300 IP Phones and Mitel 6000 SIP Phones and the firmware used by Mitel 53xx phones. Refer to the MiVoice 5300 IP Phone and Mitel 6000 SIP Phone Mitel 53xx Installation Manual - AMT/PTD/TR/0014.

The TMA service is used by TMA, and to manage IP and TDM terminals. Refer to the MiVoice 5300 IP Phone and Mitel 6000 SIP Phone Mitel 53xx Installation Manual - AMT/PTD/TR/0014. The TMA service configuration is accessible via the Web Admin terminal service menu.

The DHCP service allows a lease to be automatically assigned to MiVoice 5300 IP Phones and Mitel 6000 SIP Phones and negotiates with them the standard and specific parameters required to configure them. Refer to the MiVoice 5300 IP Phone and Mitel 6000 SIP Phone Mitel 53xx Installation Manual - AMT/PTD/TR/0014.

```
MIVOICE 5000 CONFIGURATION / SERVICES TO START AUTOMATICALLY
AN EXISTING CONFIGURATION WAS FOUND
*-----------------------------------------------------------*
| FTP (0/1) :                0    |
| TMA (0/1) :                     1    |
| DHCP (0/1) :                    0    |
*-----------------------------------------------
DO YOU WANT TO CHANGE CONFIGURATION Y/[N]? Y
```

- If the answer is YES, "y", the screen below can be used to modify the value of the FTP, TMA and DHCP fields. The values entered may be 0 (automatic service start) or 1 (manual service start via Web Admin).

- Press "Return" to confirm each modification.

- Then confirm or do not confirm the modifications by pressing "y" or "n".

```
MIVOICE 5000 CONFIGURATION / SERVICES TO START AUTOMATICALLY
AN EXISTING CONFIGURATION WAS FOUND
*-----------------------------------------------------------*
| FTP (0/1) :                1 |
| TMA (0/1) :                1 |
| DHCP (0/1) :               1 |
*-----------------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y/[N]? Y
```

FTP: value 0 or 1.

This field allows (1 = yes) or disallows (0= no) the use of the integrated FTP server on MiVoice 5000 Server during first installation. The FTP server must be active (1) to then use the integrated DHCP and TMA services.

Default value in factory settings: **FTP = O**

TMA: value 0 or 1.

This field allows the use (1 = yes) or non-use (0= no) of the TMA service integrated into MiVoice 5000 Server. For management by MiVoice 5000 Manager, the integrated TMA service is inactive since management is centralised for all the terminals on MiVoice 5000 Manager.

Default value in factory settings: **TMA = 1**

DHCP: value 0 or 1.

This field allows (1 = yes) or disallows (0= no) the use of the integrated DHCP service on MiVoice 5000 Server.

If an external DHCP server is used, the DHCP service is inactive.

Configuring the deployment of Mitel 6700 SIP Phones

If DHCP is on 0 in the previous service start menu, the parameters TERMINAL VLAN and PC VLAN are proposed in the Mitel 6700 SIP Phone configuration menu.

```
MiVoice 5000 Configuration / SIP Mitel 6700 SIP Phone
 An existing configuration was found
*-------------------------------------------------*
|
| LLDP ENABLED : 0                                |
| TERMINAL VLAN:                |
| PC VLAN:                      |
*-------------------------------------------------*
Do you want to change configuration Y(es)/N(o) ?  N
```

LLDP ENABLED

This field is used to activate the LLDP in Mitel 6700 SIP Phone (1 = yes) or not (0= no).

TERMINAL VLAN and PC VLAN: These parameters are used to define the VLAN dedicated to Mitel 6700 SIP Phones. They are not mandatory on simple networks.

If DHCP is on 1 in the previous service start menu, the parameters TERMINAL VLAN and PC VLAN are not proposed in the Mitel 6700 SIP Phone configuration menu.

```
MiVoice 5000 Configuration / SIP Mitel 6700 SIP Phone
 An existing configuration was found
*-------------------------------------------------*
| LLDP ENABLED : 0                                |
*-------------------------------------------------*
Do you confirm (Y/N)?
```

- If necessary, modify the value of the LLDP field.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

DHCP server configuration

If the DHCP service had been previously installed, this menu can be used to automatically pre-configure the DHCP server for Mitel 6700 SIP Phones and for terminals A53xxip and i7xx.

IMPORTANT : This DHCP pre-configuration requires that the deployed network interface be called eth0.

If this is not the case, the DHCP server must be reconfigured from AMP, following the procedure described in Section Modifying the DHCP server configuration from Web Admin.

```
Mitel 5000 Configuration / DHCP
*-----------------------------------------------------------*
| SUBNET MASK :         255.255.255.0           |
| BEGIN RANGE :         20.1.1.100                    |
| END RANGE :           20.1.1.199                      |
| GATEWAY :             20.1.1.254                      |
| TERMINAL VLAN:                                        |
| PC VLAN:                                             |
*-------------------------------------------------*
Do you confirm (Y/N) (Press enter to reconfigure) ? y
```

SUBNET MASK: subnet mask dedicated to IP and SIP terminals

BEGIN RANGE and END RANGE: address range dedicated to IP and SIP terminals

GATEWAY: IP address of the network gateway dedicated to the IP and SIP terminals

TERMINAL VLAN and PC VLAN: These parameters are used to define the VLAN dedicated to Mitel 6700 SIP Phones and to terminals A53xxip and i7xx. They are not mandatory on simple networks.

- Press "**Return**" to confirm each input.
- Then confirm or do not confirm the modifications by pressing "**y**" or "**n**".

Configuring Name & IID

The system's general parameters declaration screen opens (name IID (system identification number)):

```
MIVOICE 5000 CONFIGURATION / Name&IID
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE NAME/IID (Y/N): Y |
```

- If you answer YES, "**y**", the next screen allows you to declare the system's general parameters (11 digits).

```
MIVOICE 5000 CONFIGURATION / Name&IID

*-------------------------------------------------*
| NAME: MIVOICE 5000 |
| IID: 00130927001 |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

- Press "Return" to confirm the modifications.
- Then confirm or do not confirm the modifications by pressing "y" or "n".

Configuring the numbering plan length

```
MIVOICE 5000 CONFIGURATION / NL
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE NUMBERING LENGTH: Y |
*-------------------------------------------------*
```

- Press "**Return**" to confirm, after entering "**y**" or "**n**".

If the answer is "y", enter the corresponding values.

The field is used to define the internal number length to take into account (2 to 6).

```
MIVOICE 5000 CONFIGURATION / NL

*-------------------------------------------------*
| NUMBERING LENGTH: 4 |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

- Press "Return" to confirm the modifications.
- Then confirm or do not confirm this modification by pressing "y" or "n".

Configuring call distribution

```
MIVOICE 5000 CONFIGURATION / NL
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE NUMBERING LENGTH: Y |
*-------------------------------------------------*
```

- Press "**Return**" to confirm, after entering "**y**" or "**n**".

If the answer is "y", enter the corresponding values.

```
MIVOICE 5000 CONFIGURATION / Call Dist
AN EXISTING CONFIGURATION WAS FOUND
*-------------------------------------------------*
| SUBSCRIBER: 3005 |
| DID: 4000 |
*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

SUBSCRIBER:

This field allows you to assign a subscription number as a day number reduced to reception 0. This number is assigned if it corresponds to an internal subscription which can be added to a call distribution service, or if it corresponds to the number of a subscription that may be on the multi-site network (MiVoice 5000 Server).

DID:

This field is used to assign a DID number to call distribution service0. Authorised characters are " 0123456789ABCDE".

- Press "**Return**" to confirm the modifications.
- Then confirm or do not confirm the modifications by pressing "**y**" or "**n**".

Configuring subscriptions

```
MIVOICE 5000 CONFIGURATION / Subscribers
*-------------------------------------------------*
| DO YOU WANT TO CONFIGURE SUBSCRIBERS (Y/N): Y |

*-------------------------------------------------*
```

If the answer is "y", enter the corresponding values for the different fields described below.

```
MIVOICE 5000 CONFIGURATION / Subscribers

*-------------------------------------------------*
| CREATION (0/1) : 1          |
| IVB CREATION (0/1) : 1      |
| UNIFIED IVB (0/1): 1        |
| FIRST : 3000                |
| LAST : 3999                 |
| DID NUMBERING LENGTH 4          |
| FIRST DID : 3000            |
| FIRST PUBLIC DID : +33(0)130923000   |
| IVB : 3998                  |
| COMMON SUBSCRIBER : 3500   |
| ADDITIONNAL SUBSCRIPTIONS : 40       |
| PASSWORD SUBSCRIBERS: 0000      |

*-------------------------------------------------*
DO YOU WANT TO CHANGE CONFIGURATION Y(ES)/N(O) ? Y
```

CREATION:

This field may be used to inhibit automatic subscriber creation. This field may take on the values 0 (= creation inhibited) or 1(= creation authorised).

The **numbering length** field defined on the previous screen contains the internal number length to take into account (2 to 6). If this is a valid value, the fields **first, last, common subscriber** will be taken into account. Otherwise, they will be ignored.

IVB CREATION:

This field is used to automatically create the voicemail boxes associated with the automatically created subscriptions. This field is only proposed if the IVB function is installed.

UNIFIED IVB:

The **Unified IVB** field is used to define some unified voice mail boxes, if available.

FIRST:

This field contains the first internal subscription that can be created automatically.

LAST:

This field contains the last internal subscription that can be created automatically.

DID numbering length:

This field is used to define the internal number length in the incoming number plan (i.e. DID numbers).

FIRST DID:

This field is used to create the external block 0 associated with the internal number block [first, last]. Authorised characters are " 0123456789ABCDE". For this block to be created, this number must belong to an incoming number plan.

FIRST PUBLIC DID:

The field is used to associate a public number (format: 0130967000 or +33(0)130967000) with the DID number for block 0. This ASCII string will be truncated to 20 characters.

IVB:

This field is used to define the IVB access number. This field is only proposed if the IVB function is installed.

COMMON SUBSCRIBER:

This field is only read and taken into account if it is in the complete block and if this number exists already. If this is not the case, or if the field does not exist, they are assigned a default number. If their value is 0, they will not be assigned any number. The **common subscriber** field must always have a number.

ADDITIONNAL SUBSCRIPTIONS:

This field indicates the number of further internal subscriptions to create.

Password Subscribers:

This field is used to define the default subscriber password.

This same password will be used to access the IVB and to deploy Mitel 6000 SIP Phones.

Generation of sets authentication=1

This field is used to activate/deactivate the generation of a terminal authentication during subscription creation. The default value is 1 = YES => terminal authentication generated during subscription creation. This is the case during a first installation, for instance.

Managing the assignment of numbers to subscriptions:

Create a general-purpose subscription.

If automatic creation is authorised, for each subscriber equipment detected, create a subscription, assign it a DID number (read in the external block), or assign it a voice mail box if creation is authorised. Then update its LDAP directory record with the internal number and possibly DID number. Then assign this subscription to the detected equipment and then go to the next equipment.

After processing all the equipment, if automatic creation is allowed, create as many additional subscriptions as necessary (and as possible). Assign them a DID number (read in the external block) and a voice mail box if automatic creation is authorised, then update their LDAP directory record with the internal number and possibly DID number.

- Press "**y**" and confirm by pressing "**Return**".

- The screen then displays a summary of the configuration made (example).

```
| SUMMARY:
*-------------------------------------------------*
| IPADR = 20.1.1.1          |
| NAME = MIVOICE 5000       |
| IID = 00130927001         |
| FIRST : 3000              |
| LAST : 3999               |
| DID NUMBERING LENGTH 4         |
| FIRST DID : 3000          |
| FIRST PUBLIC DID : +33(0)130923000  |
| IVB : 3998                |
| NUMBERING LENGHT = 4      |
| COUNTRY = FRA             |
| LICENCE = 123456789123    |
| PARI =                    |
| START UP TYPE = TOTAL     |
| DEDICATED SNMPD = Y       |
|     |
*-------------------------------------------------*
DO YOU WANT TO APPLY YOUR CHANGE Y(ES)/N(O)/R(ECONFIGURE) ? Y
```

If the summary is not correct:

- Press "**r**" to restart the preconfiguration (from the first “Choose country” screen).

If the summary is correct:

- Press "**y**" if the values displayed are correct and confirm by pressing "**Return**".

Wait for the end of the script (**Configuration ended**) then press **Return**.

Restart the VM from the User menu so the configuration can be taken into account.

```
SELECT AN OPTION AND PRESS ENTER:
1) REBOOT              6) UPDATEOS-SECURITY        11) IDENTIFICATION
2) NETWORK             7) TOTAL                12) KEYBOARD
3) SET-NTP-SERVER      8) STANDARD                 13) LOGOUT
4) PASSWORD            9) BACKUP-SPECIFIC
5) UPDATEOS-FULL       10) RESTORE-SPECIFIC
SELECT AN OPTION AND PRESS ENTER: 1 ---------------> (PRESS 1 TO RESTART)
```

Wait for the end of the (**Configuration ended**) script then close the script window.

- Wait for the end of the start operation.

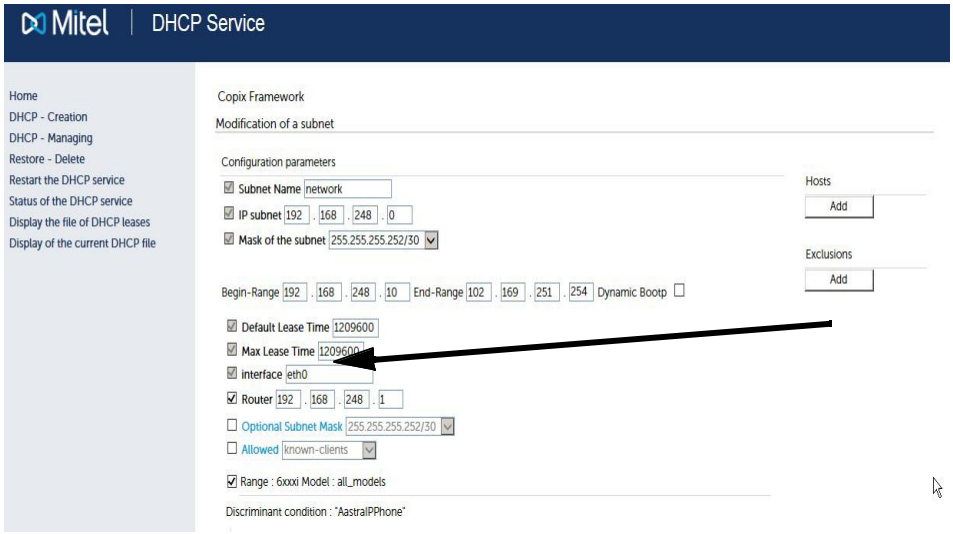
The configuration phase is ended, and the desktop is displayed again with all the MiVoice 5000 Serve icons.

Initial installation has been completed and you can now configure the site (see MiVoice 5000 Web Admin operating manual).

Checking and modifying the DHCP configuration

For more details, see Section Modifying the DHCP server configuration from Web Admin.

In Menu **DHCP - Management "- Modify a subnet:** The **eth0** interface must be replaced with **br0**).



6.4 ACCESSING THE (WEB ADMIN) USER INTERFACE

The operating console is connected to the same network as the iPBX (CPU card LAN port).

- Open a web browser installed on the operating console (Internet Explorer, for instance).
- Enter the IP address defined in the system: https://@IP (secure access mode).

Note : Address defined while installing the OS corresponding to the IP address of the MiVoice 5000 Server network card.

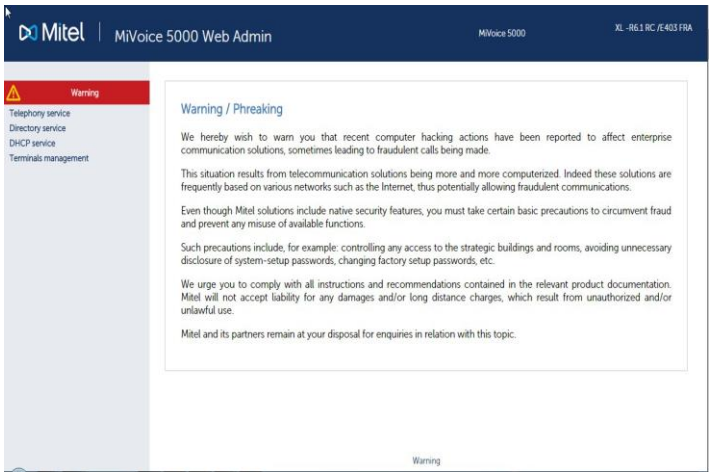
- Some security windows for this "**https**" access mode are then displayed successively; enter “**YES**” for each of them.
- The Web browser (Internet Explorer, for instance) displays a security alert when connecting to Web Admin, this alert can be disabled. Refer to the appendix of this document paragraph Taking the security certificate into account.

A login window opens.

- Enter the default access login: **admin**
- Enter the default access password: admin

The Web Admin welcome screen is displayed.

The first time you are logging on, the welcome screen displays a page alerting you to the risks of piracy and to the security constraints.



After reading this message:

Click any of the **Warning** buttons.

On the next screen that opens, displaying this message, tick **I have read this text**.

Click **OK** to confirm.

The actual Web Admin welcome screen is then displayed, giving access to all the menus:

For more information about the display of this warning message, see Section MITEL's legal warning concerning Web Admin access.

Certificate download menu

This menu is a link for downloading the self-signed SHA2 certificate provided by Mitel.

The certificate is used to secure the connection between the Web Admin and User Portal interfaces with MiVoice Manager, in particular.

The assigned certificate may also be external.

Certificates are managed and assigned from Menu **SYSTEM>Security**.

Refer to the following documents in the chapters concerning Security/Certificates. :

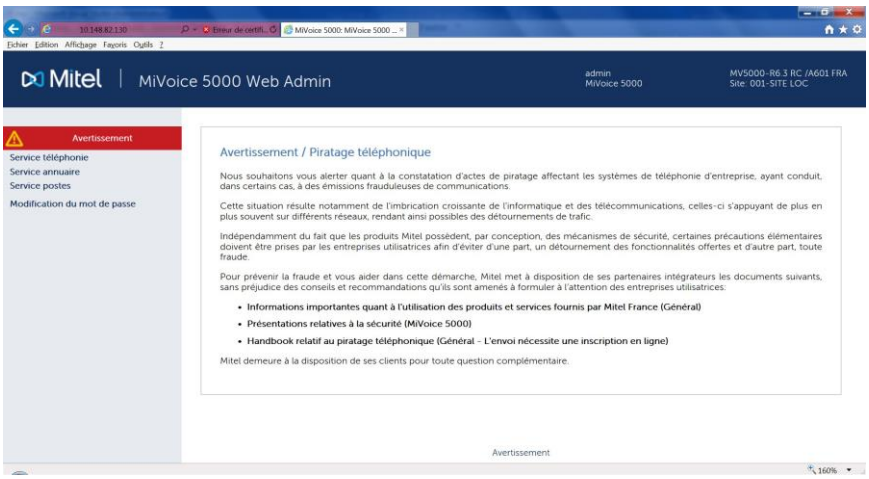
- AMT/PBX/0080 - A5000 Operating Manual
- MiVoice 5000 Manager User Guide

This link appears systematically during a first installation or after upgrading to R7.0 for sites or nodes (Cluster Configuration) whose initial version is below R7.0.

This link no longer appears if a certificate (Mitel or external SHA2) has been downloaded into the iPBX either locally or from MiVoice 5000 Manager.

User password notification message

If a password policy is defined for the user password, the welcome screen may contain an additional **Password modification** menu prompting the user to change his password if it has expired.



See the document AMT/PTD/PBX/0080, in the section on user password policy.

6.5 DECLARING THE LICENCES FOR VIRTUAL OR PHYSICAL MIVOICE 5000 SERVER

MiVoice 5000 Server may be virtualised in R5.2 SP1 and later. In this case, the dongle is equally virtual and is delivered with the MiVoice 5000 Server package.

For a first installation, the licence is not obtained directly and depends on the installation code to be generated from Web Admin.

This installation code is specific to each iPBX.

It must first be generated by the installer (from Web Admin).

Two methods of obtaining the licence are proposed after this code is generated:

- **Automatic mode** (as of R5.3 SP1 minimum): this allows direct and automatic access to the licence server which returns the licences in real time.
- **Manual mode** (currently available): connecting manually to the Mitel licence server. The installation code can be regenerated from R5.4 on the conditions indicated in Section Precautions for use.

6.5.1 AUTOMATIC MODE (R5.3 SP1 MINIMUM)

As of R5.3 SP1, a new method of connecting directly to the Mitel licence is proposed by the **Getting the keycode** button, in Menu T**ELEPHONY>SYSTEM>Info>Licences**, in order to automatically obtain the licence key, associated with the installation code, directly in the iPBX.

It is all about automatically retrieving the license key associated with a virtualised MiVoice 5000 Server installation via an http request on the Mitel server (**https://support.mitel.fr/akop/genlicence.php**).

The licence thus returned is automatically taken into account by the iPBX, and the functions concerned are unlocked and displayed in this same menu.

This menu can only be used if the virtual MiVoice 5000 Server has an internet access, associated with a correct DNS resolution.

Manual mode must be applied for all users wishing to isolate their network from the internet (see Section Manual mode).

How to obtain licences in automatic mode

In Menu TELEPHONY>SYSTEM>Info>Licences,, enter successively:

- The identification number
- The IP address of the virtual machine
- Installation IID number.

IMPORTANT : All these fields must be filled in.

The IID number entered to define the installation code of an MiVoice 5000 Server contains the number of an answering service or subscriber in the format sent by the operator (before translation).

Note : This field must have the prefix 0 when it contains less than 8 digits.

- Then click the **Installation code generation** button.

The installation code frame then gives the value of the installation code.

- Click Getting the keycode.

Connection to the licence server is then automatically set up and shortly thereafter the licences are received and taken into account by the iPBX.

Refresh the browser window (using the **Actualize** or **F5** button). The status of the licences in question is then **AUTHORISED** in the corresponding table.

It is advisable to make a call from outside to check the validity of the key immediately.

If later the characteristics of the IP address and IID number system are modified, the installation code will be regenerated following the procedure described in Precautions for use.

6.5.2 MANUAL MODE

Note : It is better to use Internet Explorer to access AMP; this will make it easier to copy the values required to generate the licence. See Installation code below.

In Menu TELEPHONY>SYSTEM>Info>Licences,, enter successively:

- The identification number
- The IP address of the virtual machine
- Installation IID number.

IMPORTANT : All these fields must be filled in.

The IID number entered to define the installation code of an MiVoice 5000 Server contains the number of an answering service or subscriber in the format sent by the operator (before translation).

Note : This field must have the prefix 0 when it contains less than 8 digits.

- Then click the **Installation code generation** button.

The installation code frame then gives the value of the installation code.

- Log on to the licence server **https://support.mitel.fr/akop/genlicence.php** and enter this installation code.

This server then generates the actual licence for the function requested for during the order.

- Save this licence using the **Export .txt file** link.

Return to the same menu **TELEPHONY>SYSTEM>Info>Licences**.

- Enter this licence in the **keycode** field of this same menu.

The functions in question are then authorised.

It is advisable to make a call from outside to check the validity of the key immediately.

It is advisable to store this licence value in a text file.

If later the characteristics of the IP address and IID number system are modified, the installation code will be regenerated following the procedure described in Precautions for use.

6.5.3 CHECKING THE VIRTUAL DONGLE VALIDITY

A check is made periodically on activities passing through the IP access and the IID number for the ID of this type of dongle.

As from the 30th day, the logbook gives a message about inactivity on any of these accesses.

If no activity is detected for the next 30 days, the licence is cancelled.

6.5.4 PRECAUTIONS FOR USE

The installation code is unique, and the generated keycode can only work with an installation code.

If an installation code is generated without obtaining a new keycode, the functions that require a licence will be closed within the next one hour.

To manage the different cases that require a change of installation code during the life of the system and, in particular, the cases encountered 24/7, it is now possible to change the installation code without asking Mitel first.

After this change, you will no longer have the right to make any modification and you must first contact Aastra to explain why you need to make any modification (change of user, physical replacement of the platform, network modification, etc.).

After analysing your request, you will again be authorised to modify the installation code.

During a search on the AKOP licence server ("search for a key"), the right to modify the installation code on the identification number concerned is indicated via the following information:

- Modification of installation code **allowed**
- Modification of installation code **not allowed**

Reminder: the IID number is the installation number, and you must check that it is regularly called up. If this is not the case, some error messages will appear after one month in the logbook (as of R5.4) then the functions will be locked.

6.6 RESETTING THE MANUFACTURER ACCESS CODE

The default value of this code may be established if the user has changed it from Menu **Telephony>System>Configuration>Users>system accounts** and if the user has lost or forgotten it.

Rappel : The manufacturer's access code may be modified to reinforce system security. In this case, neither the user nor the manufacturer (Mitel) will have access to Web Admin in manufacturer mode (see the document AMT_PTD_PBX_0080 for information about password management).

Preliminary operation

Contact Mitel's customer service to obtain the values Enter Identifier and Enter Key which will be required during the procedure described below. You also need to provide the (dongle) ID number. This number must be provided to Mitel in order to generate the values **Enter Identifier** and **Enter Key**.

Procedure

On the desktop hosting MiVoice 5000 Server:

- Copy the "**Reconfigure Standard**" icon, rename this icon to "**Reconfigure CTRL+ i**".
- Right-click the icon to enter the "**Properties"** menu.
- Select the "**Launcher**" tab.
- In the "**Command**" field, delete the **"-standard**" string.

The string must be as follows:

```
./conftools/upd_config.sh -dontquit -config
```

- Close the **"Properties**" window.
- Click the "**Reconfigure CTRL+ i"** icon.
- The screen then displays the different configuration modes.

```
Configuration mode (F/T/S/P/E)
- F: Factory mode
- T: Total mode
- S: Standard mode
- P: Password reset
- E : for Exit
```

- Select "**P**" mode to enter the pre-configuration menus.
- In the next screen, enter the values **Enter Identifier** and **Enter Key** provided by Mitel.

```
MIVOICE 5000 CONFIGURATION / NETWORK

*-----------------------------------------------*
| ENTER IDENTIFIER : IPNH123LMNVKGH5U
| ENTER NETWORK MASK : POULKJEPOSD5Q9/P
| *---------------------------------------------*
PLEASE_ENTER_A_VALID_ID_KEY
```

- Press "**Return**" to confirm.
- Then answer "**Y(es)**" to the next questions to complete the procedure.

At the end of the procedure, the manufacturer's default login and password are regenerated and can be used again.

Restart the MiVoice 5000 Server application, so this reset operation can be taken into account.

The manufacturer's default access code is also reset in Menu **TELEPHONY>SYSTEM>Configuration>Users>System accounts**.

The Web Admin access login/password are reset:

- Default access login: **admin**
- Default access password: **admin**

6.7 IMPORTING DATA INTO THE IPBX FROM THE DATA COLLECTION FORM

Before importing the data, the administrator must back up the iPBX configuration so as to be able to restore it if some .csv files had been wrongly configured.

Data is imported into the iPBX via Web Admin from Menu **Telephony service** >**System** > **Software maintenance** > **Massive import**:

- Select and download the file Data.Collecting.zip
- Click Take account of the data.

The duration of import depends on the amount of data to be downloaded. Some counters are displayed to indicate the work progress status.

- Example of counter 12/38: 15
  - 38: number of files to be imported,
  - 12: number of files being imported,
  - 15: line processed in the file being imported.

An installation report is generated at the end of the import.

6.7.1 REMINDER

The data collection form contains a specific tab for the configuration parameters required for the Ctrl + i phase.

The following files are created after the iPBX data are generated:

- A DataCollecting.zip file, containing the different .csv files from the collection and used by Web Admin (example: 002.Mitel.DataCollecting.zip).
- 7450_Formulaire.xls (Excel 2003) to be imported into MiVoice 5000 Manager. It contains the data required to configure UCP and TWP accounts.

The generated files are placed in the same directory as the one in which the form is installed.

Some additional information is provided in the data collection Excel file - Help tab.

6.8 ADDITIONAL CONFIGURATIONS

6.8.1 STARTING AND VIEWING THE SERVICES

You can configure the services (LDAP, SNMP, GSI, FTP, TFTP, etc.) and display their status from Menu "**SYSTEM>Configuration>Services**" in Web Admin. See MiVoice 5000 Web Admin operating manual (AMT/PTD/PBX/0080).

6.8.2 DECLARING AN NTP TIME SERVER

It may be necessary to synchronise an NTP server, especially for some terminal types.

The NTP server address can be defined, and NTP activated in Menu "**System>Administration>Date and time**", by selecting the tab "**Time server synchronisation protocol**".

7 UPGRADING SIMPLEX OR DUPLEX MIVOICE 5000 SERVER SOFTWARE

The software update method is exclusively the Repository method, regardless of whether the system is with or without MiVoice 5000 manager.

See the document Upgrading by repository AMT/PTD/PBX/0155, Edition 2/ minimum).

8 APPENDICES

8.1 TAKING THE SECURITY CERTIFICATE INTO ACCOUNT

A security alert is displayed the first time Web Admin is accessed via a web browser (Internet Explorer).

Therefore, you have to indicate to the web browser that the company is a reliable certification authority.

Note : If you have any problem accessing Web Admin or while reinstalling a certificate, delete the certificates previously installed on the Client terminal for this iPBX.

If the certificate which secures the Administration interface (Web Admin access) or End User interface (User Portal access) is generated by MiVoice 5000, the **Download link for the certificate generated by MiVoice 5000** (Web Admin welcome page) must be used to obtain this certificate in order to install it on the PCs accessing any of these two functions (see next section).

Managing the certificates with the browsers

The certificate must be manually added in Firefox. For the other browsers, use the Microsoft certificate manager:

Click **Start**, then in the search field, type in **mmc** then press **Enter**.

The management screen opens:

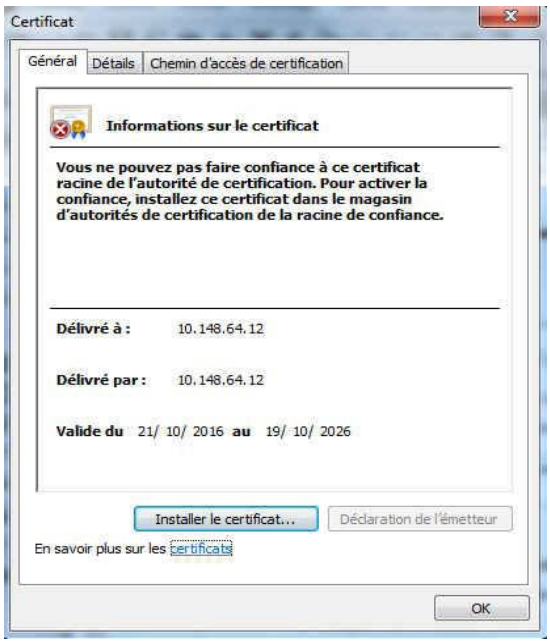
8.1.1 FOR THE MITEL 5000 RANGE

- Open a web browser installed on the operating console (Internet Explorer, for instance).
- Enter the IP address defined in the system: https://@IP (secure access mode).

Note : Default address in factory setting: 192.168.65.01

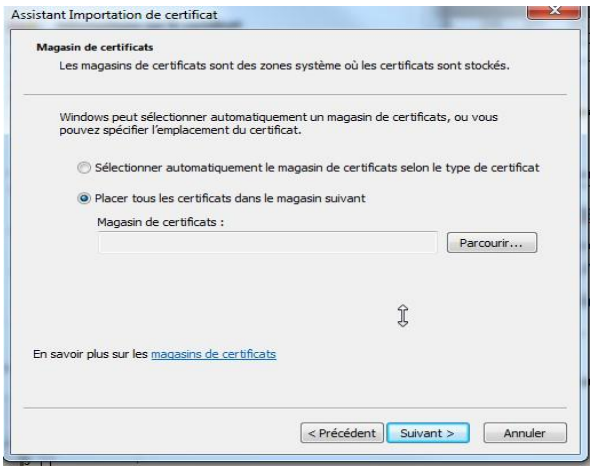
After the warning message below, click **Continue** with this site (not recommended).

- In the menus by the left, click **Download the certificate**.
- Click **Open** in the banner displayed below.
- On the next screen, in the **General** tab, click **Display the certificate**.



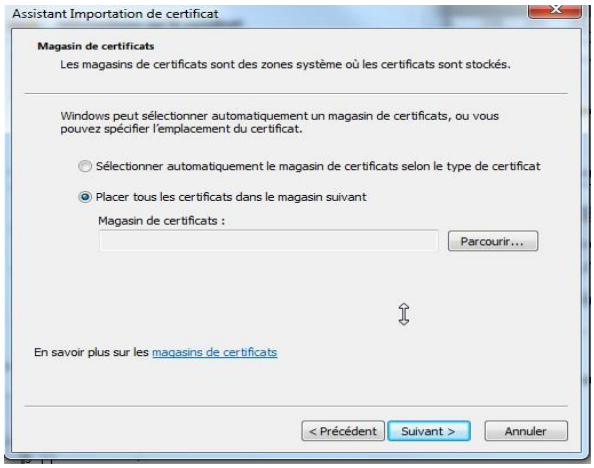
- Click **Display certificate**.
- Click **Next**.

- Tick the line **Place all certificates in the next store**, then click **Next**.

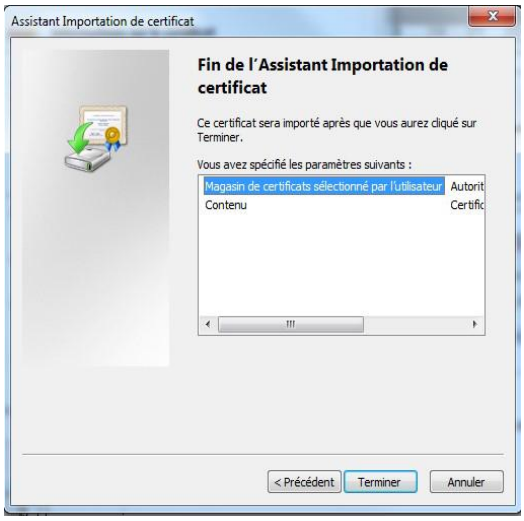


- Select **Trusted root certification authorities**, then **OK**.

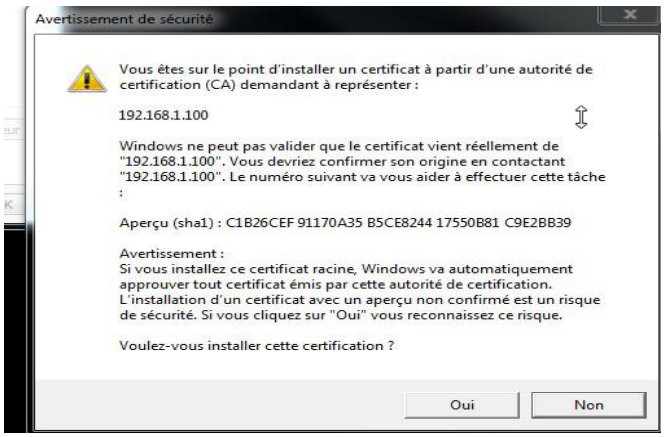
- Click **Next**.



- Click **Finish**.



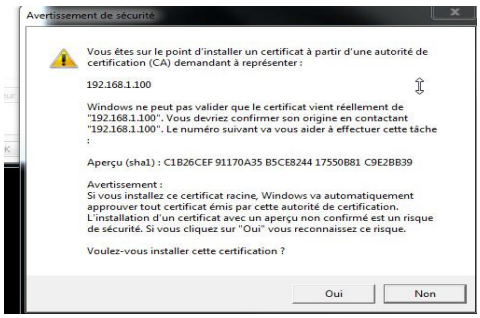
A security warning is then displayed.



- Click **YES**.

The certificate is installed.

- Click **OK**.



The installation has been completed.

- Close all the navigator windows.
- Log on to Web Admin via https://@IP. The security warning is no longer available.

8.2 MITEL'S LEGAL WARNING CONCERNING WEB ADMIN ACCESS

To alert site users to the risks of piracy and the security constraints, a warning message to the different users is displayed on Web Admin.

This message is displayed when you first log on to Web Admin, or remains accessible later in form of a link if it has not yet been validated.

It works as follows:

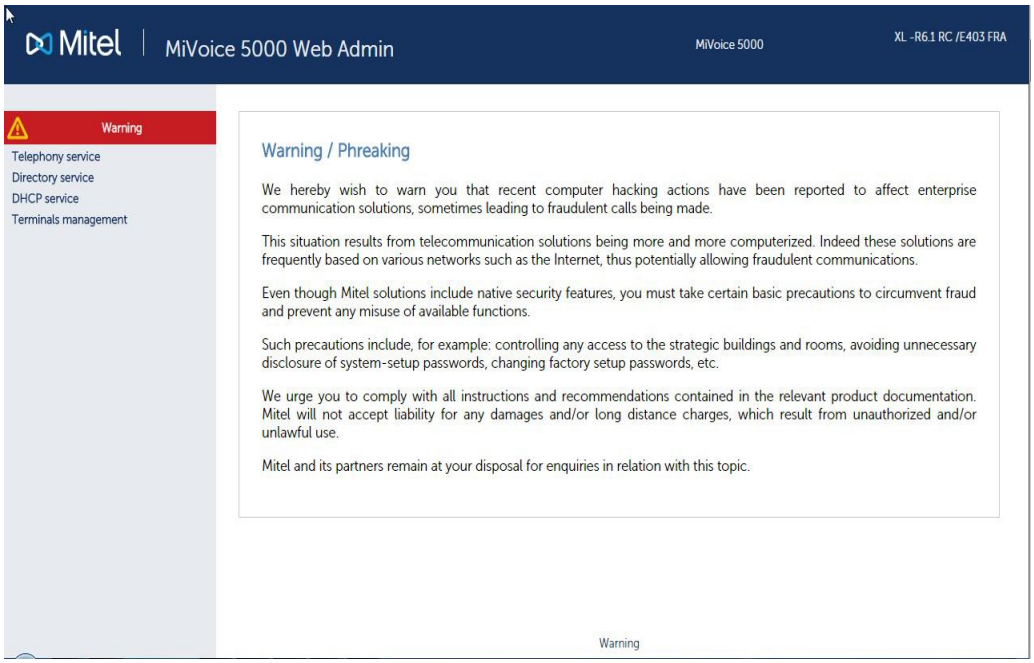
As long as a user has not validated the message, the message is displayed on the welcome page; a link is then used to display the validation page.

This link (**Warning** button) is visibly displayed in red on all the pages of the site, on the top left side.

Once a user validates this message, the picture normally displayed on the welcome page finds its place, and only a link at the bottom of the Web Admin welcome page can be used to view this new message.

Welcome page before validation

If the warning message has not been validated, the welcome page is as follows:



Two links are available to call up and display the warning validation page. First of all, on the top left side of the page the **Warning** text on a red background is a first link. The second one is located at the bottom, represented by the **Warning** text.

On the other pages of the site and as long as the message has not been validated a **Warning** link remains displayed on the top left side of the page, on a red background.

Warning message validation page

On this page the "Web Admin welcome" link on the top left side can be used to return to the welcome page without validating the message.

To validate the message, tick the box located below the warning message then press the **OK** button located by the checkbox.

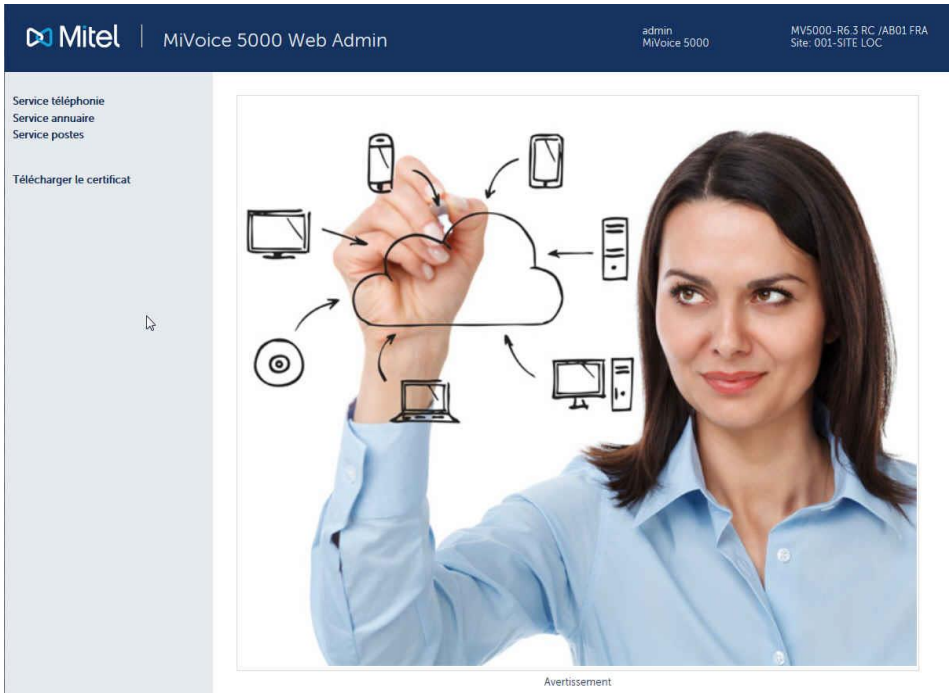
The login of the person validating the warning, as well as the validation date, is stored by the system.

If the **I have read this text** checkbox is not ticked, no action is taken if you press the **OK** button.

It is authorised to validate the warning before the end of the console release timeout (basically 10 minutes). At the end of this timeout the login window opens and you are automatically returned to the AMP welcome page (the login/password depends on the account logged onto).

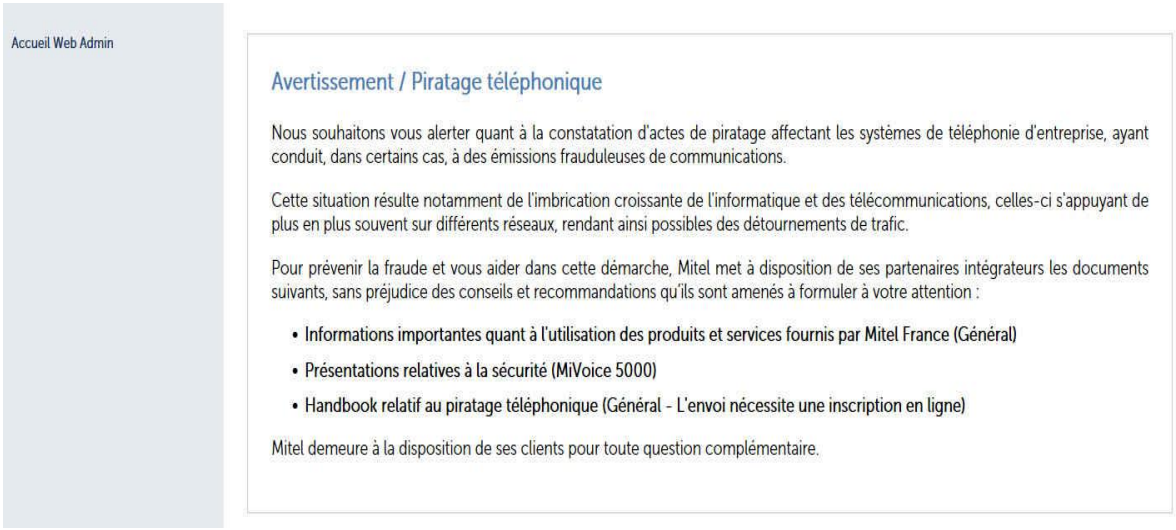
Web Admin page after validation

On this page, only the **Warning** link located under the picture can be used to go to the page which displays the warning.



On the other pages, no link can be used to display the warning.

Warning display page after validation



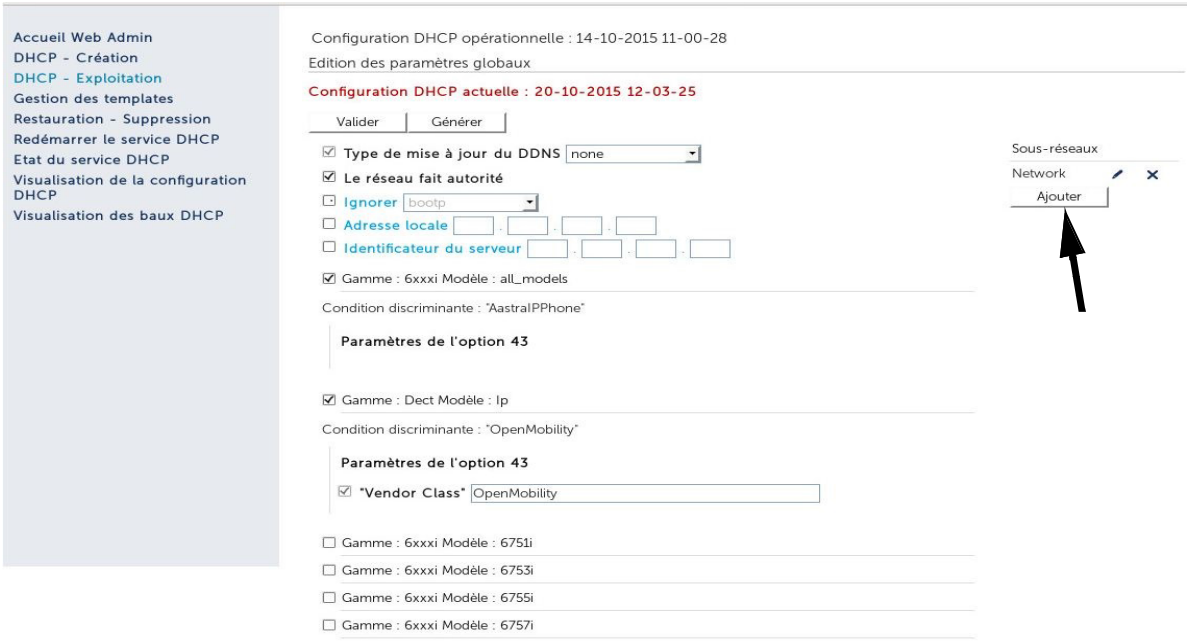
This page, which no longer offers the possibility to validate the warning, offers only one Web Admin **Welcome** link used to return to the AMP welcome page.

8.3 MODIFYING THE DHCP SERVER CONFIGURATION FROM WEB ADMIN

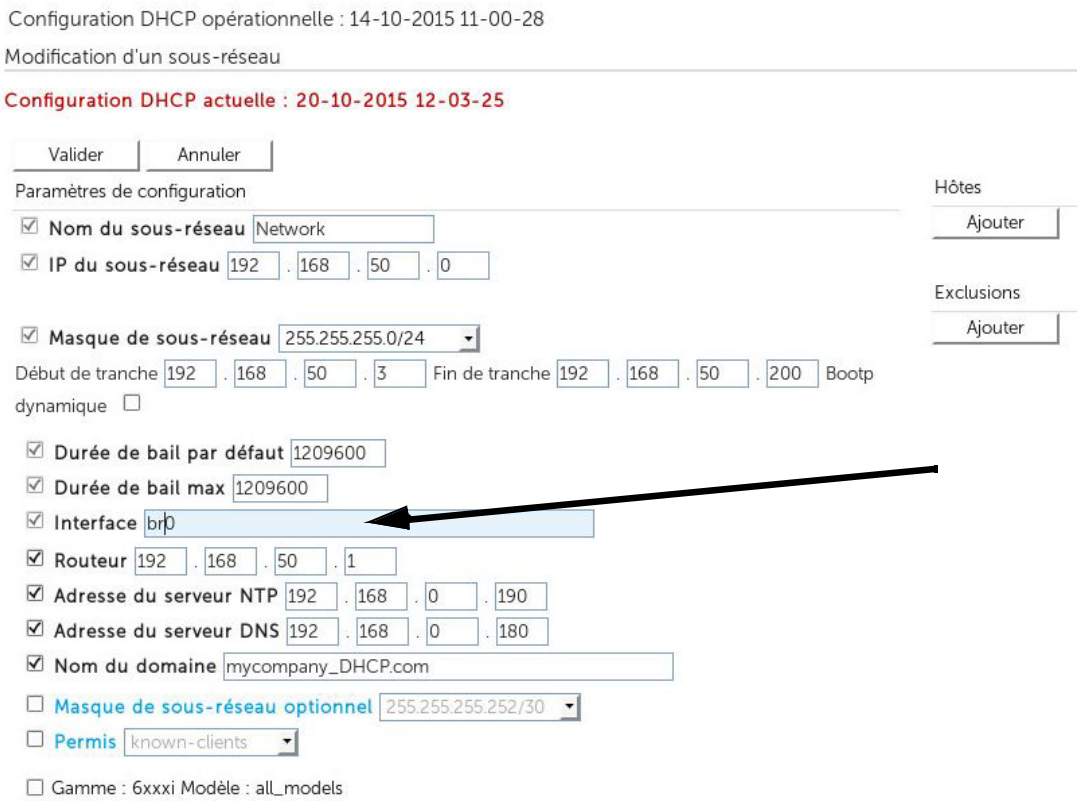
Modifying the DHCP server configuration is necessary when the network interface used is not called eth0 but has another name defined for this server's network interface.

The modification is made in five phases:

Phase 1: “**DHCP - Operation**” menu: request the modification of subnets (**"network**" pencil)



Step 2: In Menu “**DHCP - Management” - Modify a subnet:** Correct the interface name ("**eth0**") , to be replaced with the name defined on the server PC ("**em1**" or "**br0**" for example).



Step 3: In Menu “**DHCP - Management” - Modify a subnet**: Check the modification at the bottom or on top of the page.

Step 4: "**DHCP - Management**" Ask for the regeneration of the DHCP configuration at the bottom or on top of the page. **Generate** button.

Phase 5: Restart the DHCP service.

8.4 CONFIGURING THE FIREWALL FOR THE MIVOICE 5000SERVER

The following table gives the list of ports to open for MiVoice 5000 Server installation.

Protocole¤	Port(s)¤	Application¤
TCP¤	3198-3199¤	i2052/i2070/i7xx¤
TCP¤	3209¤	I2070¤
TCP¤	β200·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¤	NTP·Server¤
UDP¤	67-68¤	DHCP·Server¤
UDP¤	161-162¤	SNMP·Agent¤
UDP¤	1998/41000-41999¤	Tunnel·DATA¤
UDP¤	16320-16391¤	RFP¤
UDP¤	8106-8107¤	RFP¤

Additional items on the list of TCP ports used by the internal servers of MiVoice 5000 Server.

TCP-IP Port	INTERNAL SERVER or Server ACCESS	Server Address	Mode	Call Data
3200 to 3203	reserved			
3204	KITAXE Server (records)	012	Non D	
3205	reserved			
3206	EAS Server (for LCR et 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 to 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 to 3283	Internal server called by the TAPI Gateway		TPKT	
3284 to 3287	reserved			
3288	MUFACT Server (record multiplexer with only service records / alarms)	014130	TPKT	
3289 to 3290	reserved			
3291	Server MUFACT (record multiplexer with only communication records)	014100	TPKT	

8.5 USING THE MASSIVE CREATION FORM

8.5.1 CONSIDERATIONS

This section only describes how to massively create the following data, from the blank form provided:

- External data
- Programming keys for each subscription (maximum 64)
- Secondary numbers for multi-line subscribers.

For other management functions available from Web Admin, especially export/import and the associated processing operation (update of technical characteristics, modification of internal directory records, modification of external directory records, etc.), see the chapters **Export function and Massive data import** in the MiVoice 5000 Web Admin operating manual (AMT/PTD/PBX/0080).

8.5.2 INTRODUCTION

The Excel form allows massive configuration of Mitel 5000 systems during first installation.

It is advisable to keep an original copy of this file in Excel format.

This basic form comprises 3 tabs allowing respectively the massive creation of the following items:

- External records
- Key programming for each subscription (maximum 64)
- Secondary numbers for multi-line subscribers.

Each tab is saved separately in **.csv** format to generate a single, unique file per column.

The generated files will have to be imported one by one during the **Massive import** phase from the Web Admin menu **System/Software maintenance/Massive import**.

The data thus generated in **.csv** format will be compatible with the Mitel 5000 systems during massive import. This data may later be processed as any other parameter data type, using the **Export** function.

For a multi-site network, only one **.csv** file must be generated (from the Excel form) on the reference directory site for massive import.

This procedure applies if there is no MiVoice 5000 Manager Centre on the installation.

8.5.3 STRUCTURE AND CONTENT OF THE EXCEL FORM

8.5.3.1 *Structure*

The file comprises three tabs:

- External record creation tab
- Selection keys tab
- Multi-lines tab

Each tab contains respectively the fields that can be completed in the corresponding Web Admin menu (in the example, **Creation of external record**).

On each tab:

- The cells on the first line (line 1) indicate the labels of the parameters to be exported, corresponding to the fields to be completed in Web Admin.
- The cells on the second line (line 2) indicate the invariable internal codes for these parameters. These codes are used by the MiVoice 5000 system software, in the corresponding menu, to interpret the values to be taken into account during import in **.csv** format. In the above example, all the parameters refer to value 5030 in the cell **A2** (internal code of the menu **Creation of external record**).
- The cells on the following lines (as from line 3) are to be filled in with massive creation parameters. A line will only be taken into account if the value YES is entered in the **Confirmation** cell for this same line.

ATTENTION : The first two lines should never be modified by the user.

8.5.3.2 *Instructions for use*

The file is created exhaustively from the parameters database available in Web Admin (alphanumeric values, options list, dependences of certain data families).

All creations must be made in Excel format.

Back up systematically the latest version of these files before converting them to **.csv** format.

Use only a blank form (basic form) for each new creation meant for a new massive import. Do not re-use an old file already subjected to massive import.

For cells involving an options list, see the options offered in the menu in question so as to respect the syntax (see also the next sections).

The cells to be filled in must be in text format, to avoid random changes resulting from the default settings of Excel (010 which becomes 10 in column F in the previous example).

Depending on the system configuration, some columns do not need to be filled in (single-company, extension characteristics, rights, etc.).

Some columns and associated cells are hidden intentionally in the original form, to improve display. These fields correspond to those not modifiable from Web Admin menus.

The characters used must be alphanumeric characters (the same syntax as for Mitel 5000 system management).

For values which must not be modified in import, fill in the corresponding cells with the label **#NO_CHANGE#**.

The massive creation parameters must be entered in the language currently used in Web Admin (example: in English YES, NO, red list, etc.).

IMPORTANT : Enter YES in the Confirmation column for each line to be taken into account in massive creation (before saving it in .csv format). If these cells are not filled in, they will not be taken into account during massive import.

8.5.3.3 *Backing up the file in .csv format*

After filling in the tab:

- Select File/Save As.
- Name the file.
- Select the format "CSV (separator: semicolon) (*.csv)"
- Click **Save** .

The converted file is then available for massive import from Web Admin in Menu **System/Software maintenance/Massive import**.

Note : If this file still needs to be modified before import, when re-opened, some formats will be lost, especially the numeric values starting with 0. In this case, these cells must be filled in again as indicated previously. After the modifications, check systematically the value of the Confirmation cells for each line.

8.5.3.4 *Importing and opening a .csv file in Excel as a non truncated text file*

Some contents of the cell may be truncated when a .csv file is directly opened with Excel.

In this case, it is preferable to use the following procedure to specify how to import the .csv file:

- Open **Excel** from the **Start** menu.
- Open an empty file.
- Select the **Data** tab.
- Select the **External data** option then **From the text** or **Text file** (depending on the Excel version).
- Search for the .csv file then click **Import**.
- In the Text importation wizard, tick the Delimited box then click Next.
- Tick the **Semi-colon** box then click **Next**.
- Tick the **Text** box.
- Click **Finish**.
- Click **OK**.

The file is opened in non-truncated text mode.

8.5.4 EXTERNAL RECORD CREATION TAB

For correspondence with the possible options and values, as well as their syntax, see MiVoice 5000 Web Admin operating manual (AMT/PTD/PBX/0080).

8.5.5 SELECTION KEYS TAB

This part of the form is used to configure 5 keys per subscriber.

For correspondence with the possible options and values, as well as their syntax, see MiVoice 5000 Web Admin operating manual (AMT/PTD/PBX/0080).

Refer also to the respective terminal documentation for information on the number of programmable keys.

8.5.6 MULTI-LINES TAB

For correspondence with the possible options and values, as well as their syntax, see MiVoice 5000 Web Admin operating manual -(AMT/PTD/PBX/0080).