MiVoice 5000 Server

04/2025
AMT/PTD/PBX/0177/1/2/EN
IMPLEMENTATION MANUAL

Warning

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

The information may be changed without notice and should not be interpreted in any way whatsoever as a commitment on the part of Mitel, its affiliated companies or subsidiaries.

Neither Mitel nor its affiliated companies or subsidiaries may 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 or by any means whatsoever - be it electronic or mechanical - no matter the purpose thereof, without the prior written consent of Mitel Networks Corporation.

CONTENTS

1 INSTALLING MIVOICE 5000 SERVER (NON-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 the document MiVoice 5000 Server and Cluster Server - Redundancy.

If the redundant or non redundant system must be configured with double attachment, refer to the document “Rocky Linux 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 switching from one physical interface to the other if any of them fails.

1.1 IMPORTANT PRE-REQUISITE

As of R8.0, Rocky Linux must first be installed on the PC (installed in the factory, by default). The specific version is indicated in the release note.

Refer to the document “Rocky Linux and Double Attachment”.

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).

In a virtual VMware environment, a zip file is available on the Mitel download server.

This VM contains:

- The operating system, preconfigured to support MiVoice 5000 Server R8.X (partitioning, packaging, etc.).
- To install it, log in and run the command:

  su c2ic

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

1.2.1 LAUNCHING THE INSTALLATION SCRIPT OF THE MIVOICE 5000

- Log in to the PC as root, with the password Mitel5000.
- Mount the iso image (ACS_A5000_R8.0_RC_AXYY.iso) retrieved from the Mitel website. See in the appendix, Section 4.1.

Once the iso image is mounted:

- Go to the directory containing the installation script:

  /mnt/iso/inst5000

- Run the installation script at the root of the tree:

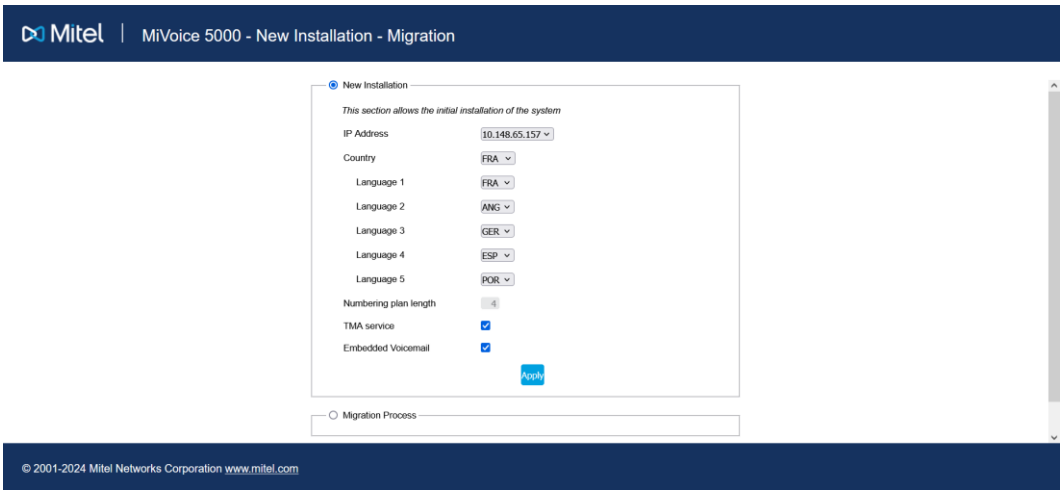
  #**./install_a5000_server.sh**

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

1.2.2 INSTALLATION ON A NON-VIRTUALIZED SYSTEM USING QUICK INSTALL

The remaining installation operation should be carried out using the MiVoice 5000 Quick Install, accessible at **http://IP_Address or FQDN**, where **IP_Address or FQDN** is the IP address or FQDN of the future MiVoice 5000 Call Server.

The **New installation** section is displayed by default.



Enter the following data in the fields:

- **IP address**: dropdown list. For selecting the IP addresses available for MiVoice 5000 Call Server
- **Country**: location of MiVoice 5000 Call Server
- **Languages 1 to 5**: languages applicable on MiVoice 5000 Call Server, in order of priority
- **Dialling plan length**: number of digits for the structure of internal phone numbers of MiVoice 5000 Call Server

- **TMA service**: checkbox. If ticked, includes the TMA service on MiVoice 5000 Call Server
- **Integrated messaging**: checkbox. If ticked, includes the integrated messaging on MiVoice 5000 Call Server.

Click **Apply** to start installing with the settings entered. The installation takes a few minutes.

After installation, the tool automatically launches the Web Admin of MiVoice 5000 Call Server.

WARNING: After installation, the quick install tool is no longer accessible.

1.3 INSTALLING THE MIVOICE 5000 SERVER APPLICATION IN A VIRTUAL ENVIRONMENT

1.3.1 DEPLOYING THE VIRTUAL MACHINE

1.3.1.1 *In a VMWare environment*

From the **ova** image 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 vSphere client of the ESX Server on which the MiVoice 5000 Server VM must be installed. This space must be accessible from the vSphere client of the ESX Server on which the MiVoice 5000 Server VM must be installed.
- Connect to the ESX server machine via the client vSphere.
- Select the **.ova** file.
- Then click **Next**.
- Check the details of the deployed model then click **Next**.
- Check and, if necessary, modify the VM name then click **Next**.
- Select the disk format.

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.

- Choose the network.
- Click **Finish** to start deploying the VM.
- Wait till the end of the deployment then click **Close**.
- Select the VM 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 initial keyboard AZERTY. The numeric keypad is not activated.

Depending on the language you want, type in the following commands

- For French:

  # localectl set-keymap fr

- For English:

  localectl set-keymap us

1.3.1.2 *In a KVM environment*

Content of the archive in tgz format

The archive in tgz format contains:

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

VM content

- 1 vCPU
- 1 GB RAM
- 10 GB disk space

VM deployment

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

From the archive in **tgz** format, available on the Mitel download server, follow the procedure below:

Copy the archive to a directory on the KVM server on which the MiVoice 5000 Server VM must be deployed.

Note : The partition to which the archive 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_RY.X**_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/ MV5000.xml

Start the VM with this command:

virsh start MV5000

Set the VM to automatic start with this command:

virsh autostart MV5000

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

virsh console MV5000

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**.**

1.3.1.3 *In a HyperV & Azure environment*

- Retrieve the HyperV & Azure compatible ZIP and extract the .vhd disk file.
- Upload the .vhd disk file to the Azure cloud using one of the methods documented by Microsoft Azure:
  - Microsoft Azure Storage Explorer,
  - PowerShell and AzCopy.
- From the Azure portal create the VM using the disk file:
  - Refer to the documentation for CPU/memory capacity.

See Section Configuring the network interfaces via the User menu**.**

1.3.2 CONFIGURING THE NETWORK INTERFACES VIA THE USER MENU

Run the command:

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

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

```
CONFIGURATION
YOU CAN ACCESS THE MIVOICE 5000 SERVER FROM HTTPS://
1) REBOOT             6)   STANDARD             11) KEYBOARD
2) NETWORK            7)   BACKUP-SPECIFIC      12) LANGUAGE
3) FIREWALL           8)   RESTORE-SPECIFIC     13) LOGOUT
4) PASSWORD           9)   IDENTIFICATION
5) UPDATEOS-SECURITY  10)  CONFIG-RESET
SELECT AN OPTION AND PRESS ENTER: 2 ---------------> (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) LANA2
3) LANB
4) LANC
5) QUIT
SELECT INTERFACE: 1 ---------------> (PRESS 1 FOR LANA)
```

Note : The interface LANA2 refers to the virtual IP address of the LANA interface.

```
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 you have pressed **Return**):

```
SELECT INTERFACE:
1) LANA
2) LANA2
3) LANB
4) LANC
5) 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
```

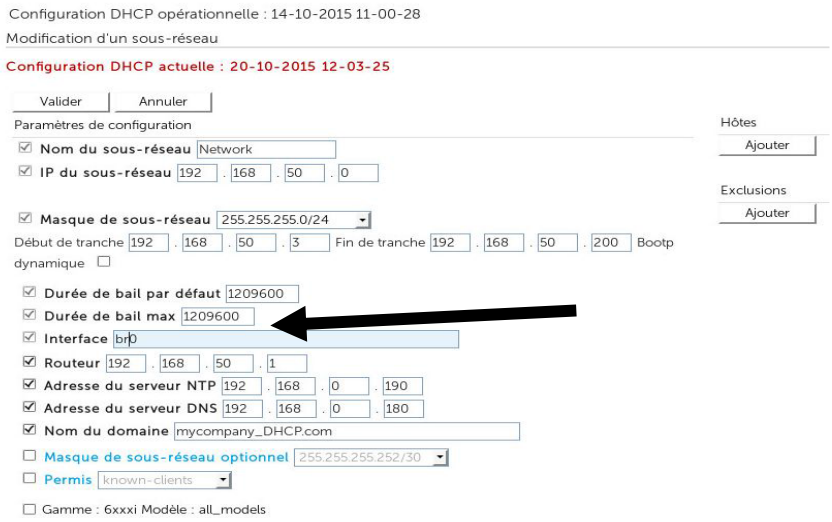
```
1) SHOW                3)ADD                      5) APPLY
2) DEFAULTGW           4)DELETE                  6) QUIT
ROUTES - SELECT MENU : 5 ---> (PRESS 5 TO CONFIRM)

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.

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**).



1.3.3 INSTALLATION ON A-VIRTUALISED SYSTEM USING QUICK INSTALL

The installation procedure using Quick Install is the same as for non-virtualised systems.

Please refer to Section **1.2.2 – Installation on a non-virtualised system using Quick Install**.

1.4 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**

Password policy and immediate password change

During first connection:

The default password is the one assigned to the administrator. This value must be changed immediately and customised by the user if the administrator has enabled a password policy. Refer to the document MiVoice 5000 Server - Operating Manual

Subsequently:

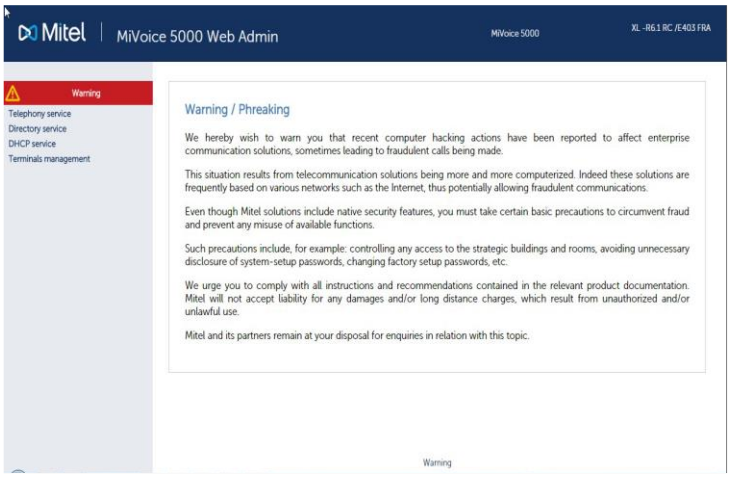
The user will also be able to change it, from the home page in the menu on the left **Password modification** (if the policy is enabled).

If it expires, a message is displayed indicating that it must be changed (if the policy is enabled).

However, if the user forgets the password, they must contact the administrator again.

Once you have logged in, the Web Admin home 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 the 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:

- MiVoice 5000 Server - Operating Manual
- MiVoice 5000 Manager User Guide

This link appears systematically during a first installation or after upgrading to R8.X for sites or nodes (Cluster Configuration) whose initial version is below R8.X.

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.

1.5 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 on the conditions indicated in Section Precautions for use.

1.5.1 AUTOMATIC MODE

As of R5.3 SP1, a new method of connecting directly to the Mitel licence is proposed by the **Getting the keycode** button, in the 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 SLS.

The iPBX thus automatically takes into account the licence, and the requested functions are unlocked and displayed in the menu T**ELEPHONY>SYSTEM>Info>Licences**.

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.

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.

1.5.2 MANUAL MODE

Note : It is better to use Internet Explorer to access Web Admin; 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.

- Click the **Installation code generation** button.

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

- In a new tab, log in to the SLS license server through the link **https://sls.mitel.com/sls/.**
- In the **EID / Serial** field, search the system through its ID.
- In the **Activate product** menu, enter the installation code.

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 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.

1.5.3 CHECKING THE VIRTUAL DONGLE VALIDITY

Periodic checks are carried out on the activity passing through the IP access, and the IID number related to the ID of this type of dongle.

Staring from the 30th day, a message is sent to the logbook mentioning the inactivity of one of these two accesses.

If no activity is detected in the next 30 days, the license is removed.

1.5.4 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 subject to a licence are closed within 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 Mitel 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 consultation on the 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 appear in the logbook after one month then the functions are locked.

1.6 RESETTING THE MANUFACTURER ACCESS CODE

Contact Mitel technical support.

1.7 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.

1.7.1 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.

1.8 ADDITIONAL CONFIGURATIONS

1.8.1 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 the document MiVoice 5000 Server – Operating Manual

1.8.2 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**".

2 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.

Refer to the document Updating by repository.

3 CASE OF UPGRADING FROM VERSIONS < R8.X TO R8.X

A procedure for upgrading to R8.x is mandatory for any virtual or physical system below R8.x.

Refer to the document **MiVoice 5000 Server/Manager and EX Controller - Upgrading to R8.x**.

4 APPENDICES

4.1 MOUNTING AN ISO IMAGE

The mounting point must exist.

- Enter the following commands:

mkdir /mnt/iso

- Copy iso under /tmp

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

4.2 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:

4.2.1 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:
- 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 the 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 browser windows.
- Log on to Web Admin via https://@IP. The security warning is no longer available.

4.3 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 displayed:

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 Web Admin 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

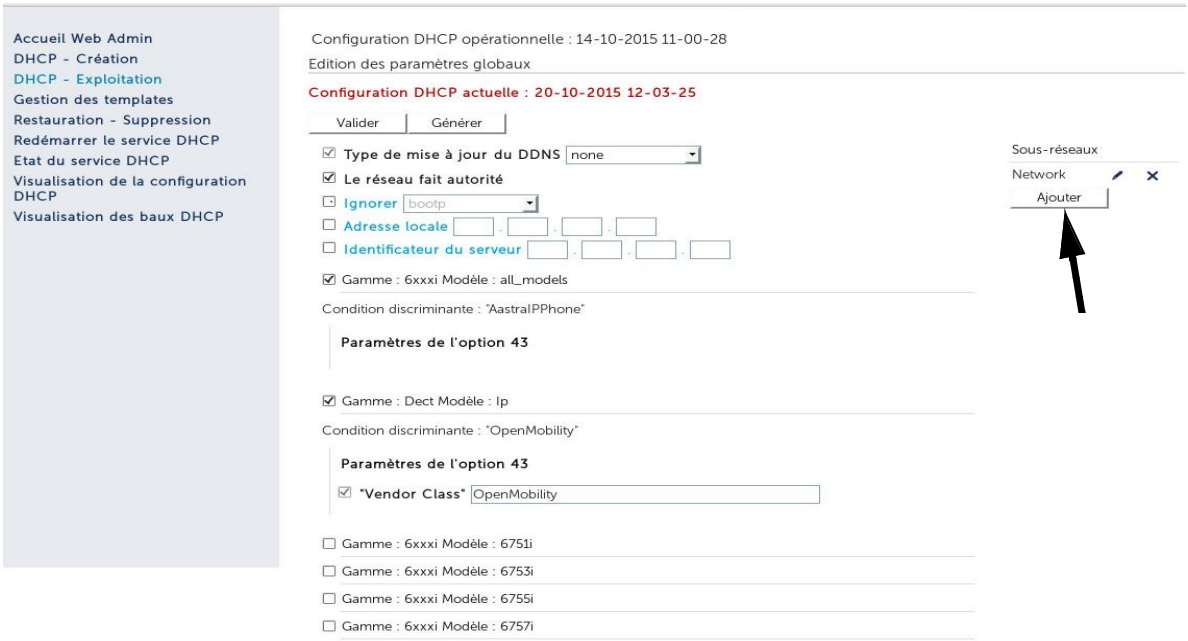
This page, which no longer offers the possibility to validate the warning, offers only one Web Admin **Welcome** link used to return to the AMP welcome page.

4.4 MODIFYING THE DHCP SERVER CONFIGURATION FROM WEB ADMIN

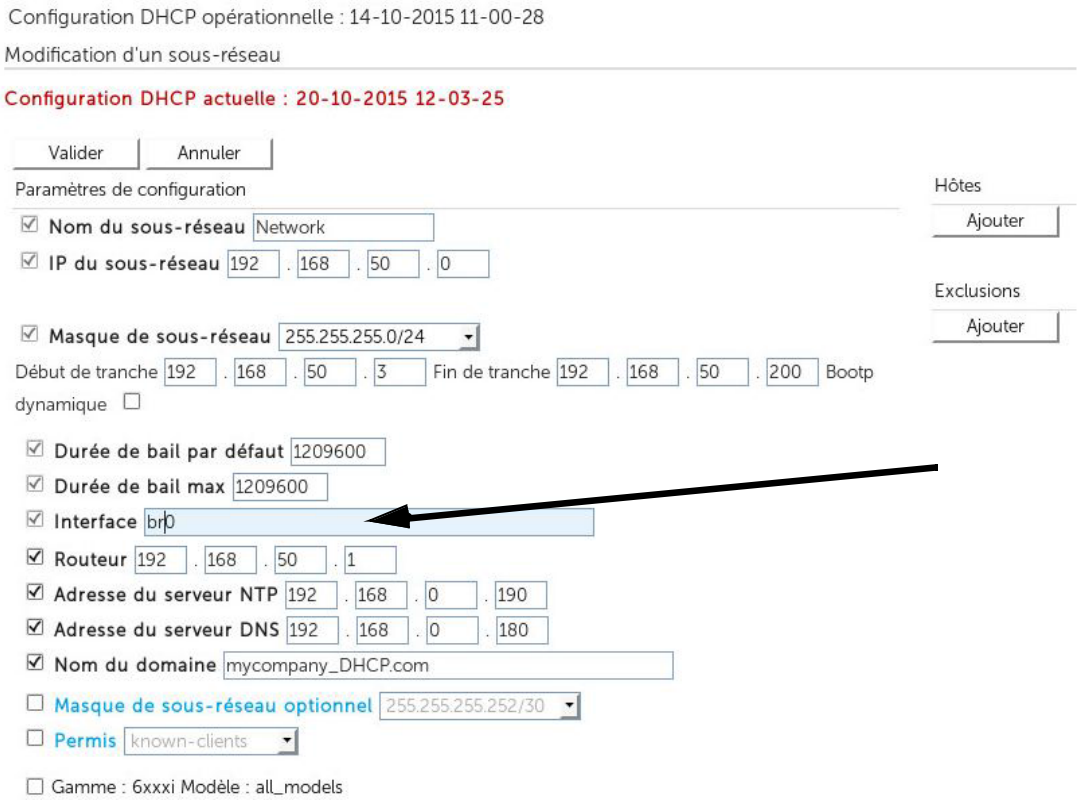
Modifying the DHCP server configuration is necessary when the network interface used is not called eth0 but has another name defined for this server's network interface.

The modification is made in five phases:

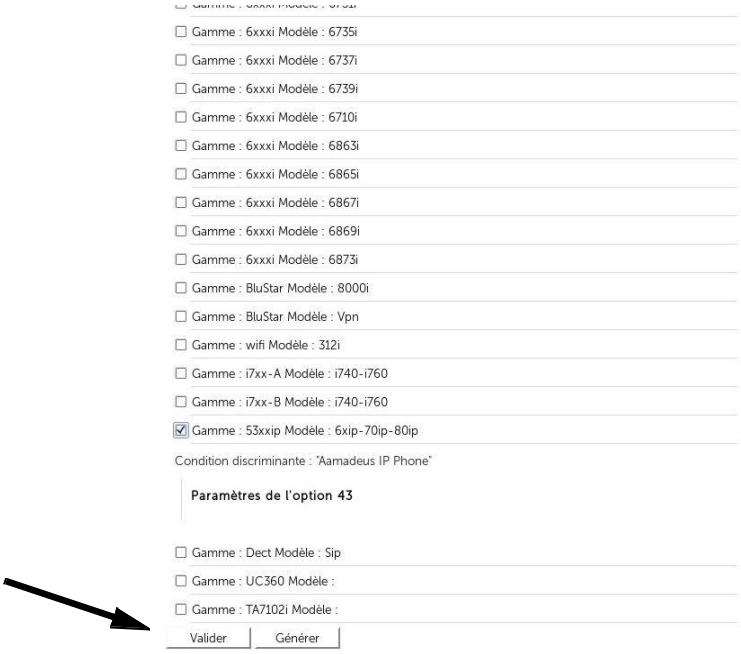
Phase 1: “**DHCP - Operation**” menu: request the modification of subnets (**"network**" pencil)



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).

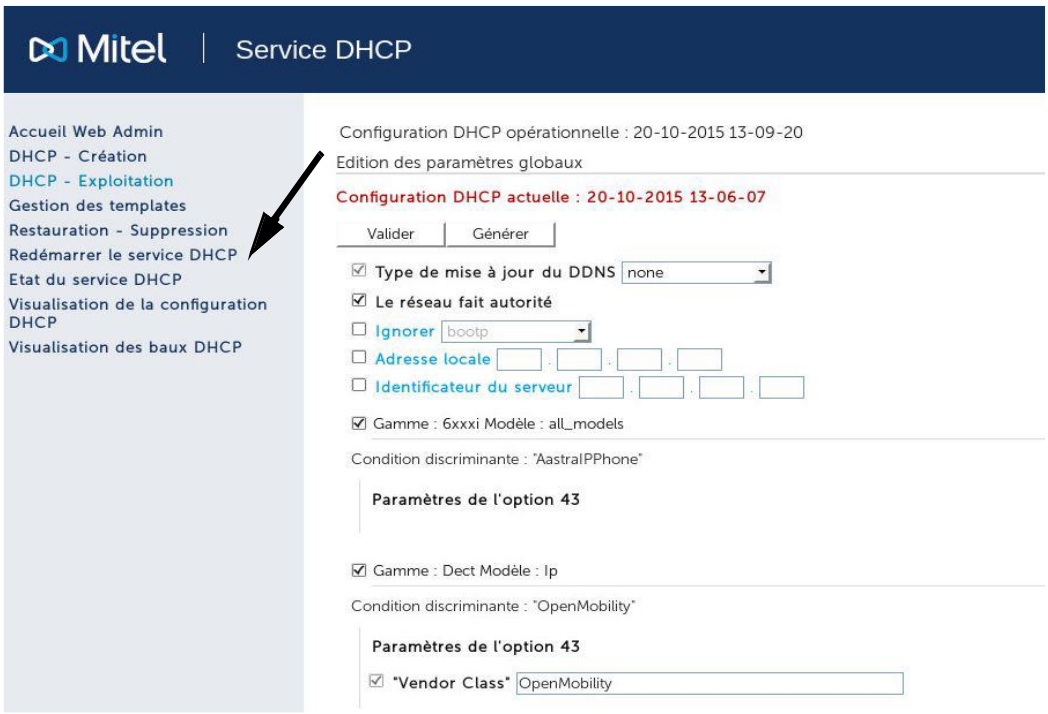


Step 3: In Menu “**DHCP - Management” - Modify a subnet**: check the modification at the bottom or on top of the page.



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.



4.5 CONFIGURING THE FIREWALL FOR MIVOICE 5000 SERVER

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

PROTOCOLE	PORTS	APPLICATION
TCP	3198-3199	i2052, i2070, i7xx
TCP	3209	i2052
TCP	3200 et +	Refer to the list in the table below.
TCP	21	675xi/53xxip Download (FTP)
TCP	69	675xi/RFP Download (TFTP)
TCP	443	File Transfert (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
LDAPS	636	In case of a secure connection to the directory (TLS).

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

4.6 USING THE MASSIVE CREATION FORM

4.6.1 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 Server operating manual.

4.6.2 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.

4.6.3 STRUCTURE AND CONTENT OF THE EXCEL FORM

4.6.3.1 *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.

4.6.3.2 *Instructions for use*

The file is created exhaustively from the settings database available in Web Admin (alphanumeric values, options, 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 settings 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.

4.6.3.3 *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.

4.6.3.4 *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.

4.6.4 EXTERNAL RECORD CREATION TAB

For the correspondence with the possible options and values and their syntax, refer to the document MiVoice 5000 Server - Operating Manual.

4.6.5 SELECTION KEYS TAB

This part of the form is used to configure 5 keys per subscriber.

For the correspondence with the possible options and values and their syntax, refer to the document MiVoice 5000 Server - Operating Manual.

Refer also to the respective terminal documentation for information on the number of programmable keys.

4.6.6 MULTI-LINES TAB

For the correspondence with the possible options and values and their syntax, see MiVoice 5000 Server - Operating Manual.