

# MiVoice 5000 Manager

06/2017

AMT/PTD/NMA/0040/12/2/EN

INSTALLATION AND CONFIGURATION



## **NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®).

The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries.

Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

©Copyright 2015, Mitel Networks Corporation. All rights reserved.

Mitel® is a registered trademark of Mitel Networks Corporation.

Any reference to third party trademarks is for reference only and Mitel makes no representation of ownership of these trademarks.

# CONTENTS

<b>1</b>	<b>ABOUT THIS DOCUMENT</b>	<b>3</b>
1.1	TARGET AUDIENCE FOR THIS DOCUMENT	3
1.2	REFERENCE DOCUMENTS	3
1.3	LAYOUT OF THE DOCUMENT	4
<b>2</b>	<b>GENERAL DESCRIPTION</b>	<b>7</b>
2.1	PRESENTATION OF THE APPLICATION	7
2.2	OVERVIEW	7
2.3	MANAGED SYSTEMS	7
2.4	GENERAL ARCHITECTURE	7
2.5	IPBX HARDWARE CONFIGURATION	8
2.5.1	HARDWARE CONFIGURATION OF REMOTE IPBXS	8
2.6	PC HARDWARE CONFIGURATION	8
<b>3</b>	<b>CONFIGURING IPBX</b>	<b>11</b>
3.1	IPBX CONFIGURATION FOR AN IP CONNECTION	11
3.2	IPBX CONFIGURATION FOR AN ISDN CONNECTION	11
<b>4</b>	<b>CONFIGURING TICKETS AND ALARMS</b>	<b>13</b>
4.1	CONFIGURING TICKET PROCESSING	13
4.1.1	KEYS TO UNLOCK	13
4.1.2	KITAXE SERVER CONFIGURATION	13
4.1.3	MUFACT SERVER CONFIGURATION	13
4.1.4	RESETTING THE INTEGRATED BUFFER MEMORY	14
4.2	CONFIGURING ALARM PROCESSING (SNMP MANAGER)	15
4.2.1	CONFIGURING SNMP MANAGER	15
4.2.2	ALARM CONFIGURATION	16
4.2.3	ALARM CALLS	17
4.3	ADMINISTRATION PARAMETERS	18
4.4	DOWNLOADING TELEPHONY PARAMETERS	19
<b>5</b>	<b>CONFIGURING RED HAT OR CENTOS</b>	<b>23</b>
5.1	CONFIGURING THE FIREWALL	23
<b>6</b>	<b>INSTALLING AND CONFIGURING THE SERVER PC</b>	<b>25</b>
6.1	INSTALLING THE SERVER PC	25
6.1.1	IMPORTANT PRE-REQUISITE	25
6.1.2	INSTALLING THE MIVOICE 5000 MANAGER APPLICATION	25
6.1.3	INSTALLING THE MIVOICE 5000 MANAGER APPLICATION IN A VIRTUAL VMWARE ENVIRONMENT	27
6.2	CHANGING THE DEFAULT LANGUAGE OF THE MIVOICE 5000 MANAGER APPLICATION IN A VIRTUAL VMWARE ENVIRONMENT	35
6.3	RECONFIGURING MIVOICE 5000 MANAGER IP ADDRESS	35
6.3.1	RECONFIGURATION OPERATIONS ON THE SERVER PC AND MIVOICE 5000 MANAGER CLIENT PC	35
6.3.2	RECONFIGURATION OPERATIONS IN THE LDAP DIRECTORY	38
6.3.3	RECONFIGURATION OPERATIONS IN SNMP MANAGER	38
6.4	INSTALLING NAGIOS	38
<b>7</b>	<b>OVERVIEW OF MIVOICE 5000 MANAGER PORTAL</b>	<b>39</b>
7.1	THE QUICKCREATE APPLICATION	41
7.2	ADMINISTRATION WINDOW	41
<b>8</b>	<b>INSTALLATION ON CLIENT PCS</b>	<b>43</b>
8.1	INSTALLING FRAMEWORK.NET	43
8.2	INSTALLING MITEL CERTIFICATE (AS OF WINDOWS 7)	43

8.2.1	DELETING AN EXISTING CERTIFICATE .....	44
8.2.2	INSTALLING THE MIVOICE 5000 MANAGER CLIENT APPLICATION ON REMOTE CLIENT PCS .....	44
<b>9</b>	<b>ADMINISTRATION FUNCTIONS .....</b>	<b>47</b>
9.1	IMPORTING AN EXTERNAL CERTIFICATE .....	47
9.2	DELETING A CERTIFICATE .....	47
9.3	BACKING UP AND RESTORING THE APPLICATION .....	48
9.3.1	BACKUP .....	48
9.3.2	RESTAURE .....	49
9.4	RESETTING THE MIVOICE 5000 MANAGER DATA CONFIGURATION IN CANONICAL MODE .....	51
9.5	MASSIVE CREATION OF REGIONS AND THEIR SITES .....	51
9.5.1	THE EXCEL FILE .....	51
9.6	OPERATORS' CONNECTION STATUS .....	54
9.7	EXPORTED DATA .....	55
9.7.1	DISPLAYING EXPORTED DATA .....	55
9.7.2	DESCRIPTION OF THE EXPORT DIRECTORIES .....	56
9.8	CONFIGURING EXTERNAL DEVICES .....	58
9.8.1	ADDING A DEVICE .....	58
9.8.2	EXPORTING DEVICE CONFIGURATION .....	59
9.8.3	DELETING A DEVICE .....	59
9.9	MANAGING SECURITY RULES .....	60
9.9.1	PASSWORD FORMAT .....	60
9.9.2	PASSWORD VALIDITY .....	60
9.9.3	RESETTING THE PASSWORD .....	60
9.9.4	INACTIVITY TIMEOUT .....	61
9.9.5	OPERATOR RIGHTS .....	61
<b>10</b>	<b>CONFIGURING MIVOICE 5000 MANAGER FOR THE FIRST TIME .....</b>	<b>63</b>
10.1	DEFINING THE TELEPHONY PARAMETER RANGE .....	63
10.2	CONFIGURING THE DIRECTORY .....	64
10.3	DEFINING ALARMS .....	64
10.4	THE CONFIGURATION OF NETWORK ELEMENTS (REGIONS, MULTI-SITES, SITES) .....	64
10.5	DEFINING A REFERENCE SITE .....	64
10.6	DOWNLOADING IPBX DATA TO MIVOICE 5000 MANAGER .....	65
10.6.1	PREPARING DATA FOR DOWNLOADING .....	65
10.6.2	STARTING THE GENERATION OPERATION .....	65
10.6.3	IMPORTING A SITE .....	66
<b>11</b>	<b>UPGRADE PROCEDURES .....</b>	<b>67</b>
11.1	UPGRADING AN $\geq$ V3.3 CONFIGURATION TO V3.4 .....	67
11.1.1	UPGRADING TO V3.4 (MAIN STEPS) .....	67
11.1.2	UPGRADE PREAMBLE .....	68
11.1.3	UPGRADING THE MIVOICE 5000 MANAGER SERVER PC SOFTWARE .....	68
11.1.4	UPGRADING THE NAGIOS SOFTWARE ON THE MIVOICE 5000 MANAGER SERVER PC... 68	68
11.1.5	INSTALL THE NEW MIVOICE 5000 MANAGER CLIENTS .....	68
11.1.6	CHECKING THE LICENCE STATUS .....	68
11.1.7	UPGRADING THE OPERATING SYSTEM SECURITY PATCHES .....	68
11.1.8	RESTART THE MIVOICE MANAGER SERVER .....	68
11.1.9	RESTORING THE DATA ON THE MIVOICE 5000 MANAGER SERVER PC .....	69
11.1.10	UPGRADING MIVOICE 5000 MANAGER CLIENT TERMINALS (AUTOMATICALLY) .....	70
11.1.11	ENTERING THE LICENCES ON THE SERVER .....	70

# 1 ABOUT THIS DOCUMENT

This document describes how to install and configure the non-redundant MiVoice 5000 Manager. It describes the preliminary configuration to be made on iPBXs, and full installation of MiVoice 5000 Manager on the server and client stations.

For redundant configuration of the MiVoice 5000 Manager, refer to the document entitled "MiVoice 5000 Manager Redundancy and Double Attachment" (AMT/PTD/NMA/0046). Redundancy is a mechanism that prevents hardware failures on the MiVoice 5000 Manager platform.



**Note:** The Redundancy and Double Attachment Manual also describes the double attachment process recommended by Mitel for providing secure access to the MiVoice 5000 Manager platform's LAN in all cases.

## 1.1 TARGET AUDIENCE FOR THIS DOCUMENT

This document is meant for network managers, system administrators, network analysts and operators with:

- Basic knowledge of Windows and/or Linux
- Knowledge of Mitel iPBXs and corporate network applications
- Knowledge of how to configure a corporate network
- Advanced knowledge of network architecture, operation and terminology.

## 1.2 REFERENCE DOCUMENTS

Users will find additional information in the following documents:

- [0] MiVoice 5000 Manager – User Guide  
AMT/PUD/NMA/0003/EN
- [1] MiVoice 5000- R5.1 and later Operating manuals
  - MiVoice 5000 Web Admin XD-XL-XS-XS12-MiVoice 5000 Server – Operating manual  
AMT/PTD/PBX/0080/EN
  - Multi-site management  
AMT/PTD/PBX/0081/EN
- [2] MiVoice 5000 Manager Redundancy and Double Attachment  
AMT/PTD/NMA/0046/EN
- [3] Installation Guide for Red Hat  
AMT/PTD/NMA/0041/EN
- [4] Installation Guide for CentOS  
AMT/PTD/NMA/0059/EN
- [5] IAX SERIES - Hardware Installation and Maintenance Manual - AMT/PTD/PBX/0150/EN
- [6] Mitel 5000 Gateways - Implementation Manual - AMT/PTD/PBX/0151/EN
- [7] Pictures management - Implementation manual  
AMT/PTD/PBX/0114/EN
- [8] MiVoice 5000 Manager - Directory configuration  
AMT/PTD/NMA/0061/EN

## 1.3 LAYOUT OF THE DOCUMENT

This document has the following structure:

- Chapter 1 gives information about Mitel documentation and terminology.
- Chapter 2 contains the characteristics of the MiVoice 5000 Manager application.
- Chapters 3 and 4 describe the configuration of iPBX to work with MiVoice 5000 Manager
- Chapter 5 specifies how to configure the operating system to work with MiVoice 5000 Manager
- Chapters 6 to 8 describe how to install the MiVoice 5000 Manager application on server and client PCs.
- Chapter 9 describes the administration functions grouped together in the administration window.
- Chapter 10 describes the items to configure in the MiVoice 5000 Manager application after its installation.
- Chapter 11 describes the processes to update and/or migrate the application

Information on how to configure the directory (declaring the directory in a multi-site configuration, synchronisation with an external directory) is given in the document AMT/PTD/NMA/0061.

## Glossary

<b>MITEL 5000 GATEWAYS</b>	This term refers to all XS, XL and XD PBXs (as of R5.1).
<b>MIVOICE 5000 OU MIVOICE 5000 SERVER</b>	Telephone switching system on a PC running with Linux Redhat (as of R5.1).
<b>XS, XL, XD</b>	MiVoice 5000 range physical gateways (as of R5.1).
<b>MIVOICE 5000 MANAGER OR MIVOICE 5000 MANAGER</b>	Systems management centre
<b>ACL</b>	<i>Access ControlList</i> ACLs are used to authenticate to LDAP databases and to receive filtered information (read and write rights and parameter list) according to configuration.
<b>LSB</b>	<i>Security Logic Block</i> Term used to identify an item supervised by the iPBX. Example: cluster equipment, X25 data card, digital subscriber channel, etc.
<b>BUFTIC</b>	Server associated with the integrated buffer for storing call tickets.
<b>CAMPAIGN</b>	Day-to-day processing operations comprising all the deferred programmed actions, both the occasional and periodic ones.
<b>CLUSTER</b>	IPBXs new architecture using MiVoice 5000 server and several iPBXs attached to it. Each of these iPBX is called a node .
<b>KITAXE</b>	Detailed-billing server. The KITAXE server is located on each site: its function is to collect site tickets and send them to the MUFACT server.
<b>LDAP</b>	<i>Lightweight Directory Access Protocol</i> Standard protocol used to manage administrative data (directory)
<b>TL</b>	Tie Line Specialised line between PBXs

<b>MIB</b>	<p>Management Information Base</p> <p>Database inside each agent. This base contains management information on the equipment concerned. The MIB allows communication between the SNMP agent and SNMP manager.</p>
<b>MULTI-SITE</b>	<p>Name given to a group of iPBXs connected together to offer a distributed switching function. This group shares the same directory (when declared) and has a centralised call server.</p> <p>Refers to two or more networked iPBXs.</p>
<b>MUFACT</b>	<p>The purpose of the MUFACT server (billing multiplexer-demultiplexer) is to collect the tickets issued by each itemised billing server (KITAXE). The multiplexer is located on the centraliser site for itemised billing. It automatically sets up X25 links (Virtual Circuits) with the billing servers (KITAXE) of the sites belonging to the multi-site network.</p>
<b>NODE</b>	<p>Used only in an Cluster architecture. A node can be either Mitel 5000 Gateways or an A500 or a MiiVoice 5000 server.</p>
<b>POOL</b>	<p>Refers to two or more independent and unconnected NeXspan iPBXs.</p>
<b>REGION</b>	<p>Group of several sites. Set of (site or multi-site) cabinets sharing the same telephony parameters and profiles.</p>
<b>REPOSITORY</b>	<p>A place where the entire data is stored:</p> <ul style="list-style-type: none"> <li>• application configuration data</li> <li>• data concerning managed sites</li> <li>• operator data</li> </ul>
<b>PSTN</b>	<p><i>Public Switched Telephone Network</i></p> <p>Ordinary telephone network</p>
<b>DID</b>	<p><i>Direct Inward Dialling</i></p> <p>A system which allows direct access to a correspondent's terminal without passing through the switchboard.</p> <p>The DID number is the public number used to reach a subscriber from an external network</p>
<b>SITE</b>	<p>a Mitel iPBX</p> <p>A site is either a MiiVoice 5000 Server or a Mitel 5000 Gateways.</p>
<b>STANDALONE SITE</b>	<p>Site not belonging to any multi-site configuration. This site is located in a region, on the same level as multi-sites.</p>
<b>IVR</b>	<p>Interactive voice response</p>
<b>F1</b>	<p>M6501 L/R IP PBX (before R5.1)</p>
<b>F2</b>	<p>M6540 IP PBX (before R5.1)</p>
<b>F4</b>	<p>NeXspan 50 and NeXspan 500 (before R5.1)</p>
<b>F5</b>	<p>Mitel Call Server MiVoice 5000 Server (before R5.1)</p>
<b>F6</b>	<p>XS, XL and XD iPBX (before R5.1)</p>





## 2 GENERAL DESCRIPTION

### 2.1 PRESENTATION OF THE APPLICATION

MiVoice 5000 Manager is an administration tool for large MiVoice 5000 networks. This application is used to manage multi-site network configurations but also standalone iPBXs (up to 2000 multi-sites or iPBXs).

MiVoice 5000 Manager offers system management functions as well as day-to-day management services like telephony subscriber management.

### 2.2 OVERVIEW

The MiVoice 5000 Manager administration tool is used to manage many services on the network, including:

- Remote configuration (MiVoice 5000 Web Admin (Web Admin),
- Alarm management (including notifications by e-mail or on an external device)
- Log and event management
- Collection of call records
- Taking network inventory (hardware and software)
- Real-time programming and supervision of individual tasks or groups of tasks
- Directory Management
- Subscriber management
- Terminal management (TMA)
- Supervision (real-time maps)

### 2.3 MANAGED SYSTEMS

Day-to-day management; the following systems are managed:

- XS/XL/XD in system release R5.1 and later
- MiVoice 5000 in system release R5.1 and later

From R2.4 release, MiVoice 5000 Manager manages only R4.2 iPBX and multisites including R4.2 iPBX.

#### **Capacities**

MiVoice 5000 Manager manages the following capacities in system release R5.1 and later:

- Up to 2000 sites or multi-sites
- Up to 300,000 subscribers
- Up to 400,000 directory records
- Number of operators declared: unlimited
- Number of operators connected simultaneously: 80

### 2.4 GENERAL ARCHITECTURE

Remote access to iPBXs is via IP or ISDN.

ISDN connection is via a router.

## **2.5 IPBX HARDWARE CONFIGURATION**

### **2.5.1 HARDWARE CONFIGURATION OF REMOTE IPBXs**

- MiVoice 5000 requires an IP connection, other iPBXs can be connected via IP or ISDN.
- In ISDN connection, the remote iPBX must meet the following specifications:
  - 1 CP1 card (CCP on X500)
  - 1 ISDN access
  - The buffer function for downloading call alarms or records.

## **2.6 PC HARDWARE CONFIGURATION**

The technical characteristics required for the server PC and client PCs are described in the product guide, as well as in the ordering guides, available on Mitel's Extranet.

# **PART I: CONFIGURING CONNECTIONS**



## 3 CONFIGURING IPBX

Site management is via MiVoice 5000 Web Admin (Web Admin).

The iPBXs concerned by the description of programming are:

- Mitel 5000 Gateways (XS, XL and XD)
- MiVoice 5000

### 3.1 IPBX CONFIGURATION FOR AN IP CONNECTION

Refer to documents listed in section 1.2 - Reference documents

MiVoice 5000 Manager is connected to Mitel 5000 Gateways iPBXs or MiVoice 5000 server through an **https** type secure access. Therefore, it is not necessary to create specific ports; you can use the ports declared by default.

### 3.2 IPBX CONFIGURATION FOR AN ISDN CONNECTION

For an ISDN connection, a router is necessary between MiVoice 5000 Manager and the iPBX to manage.

To configure this type of access, refer to document listed in section 1.2 - Reference documents.



## 4 CONFIGURING TICKETS AND ALARMS

### 4.1 CONFIGURING TICKET PROCESSING

#### 4.1.1 KEYS TO UNLOCK

The unlocking operation is required to generate tickets and alarms. A single key can be used to unlock all the functions.

- **Menu: SYSTEM > Info > Licences**

Enter the software key code in the corresponding area.

To download V2, V3 and V4 format tickets, check that the status of the **128-byte > tickets** line is **authorised**.

#### 4.1.2 KITAXE SERVER CONFIGURATION

The KITAXE server must be in service. Its default directory number is 012.

**Menu: NETWORK AND LINKS > Data links > Servers**

Select KITAXE server

Status : IN SERVICE	<input type="text" value="....."/>	-> Choose IN SERVICE.
Directory number	<input type="text" value="012"/>	->Default number

#### 4.1.3 MUFACT SERVER CONFIGURATION

The MUFACT server must be in service. Its default directory number is 014.

**Menu: NETWORK AND LINKS > Data links > Servers**

Choose MUFACT server.

Status : IN SERVICE	<input type="text" value="....."/>	-> Choose IN SERVICE.
Directory number	<input type="text" value="014"/>	->Default number

If management is in multi-site with ticket centralisation:

- **Menu: SYSTEM > Configuration > Tickets > Call from billing servers**

Call number 1	<input type="text" value="980012"/>
Profil - tel/paq/cir/ser/sup/mon	<input type="text" value="1++++++"/>
Call number 2	<input type="text" value="952014"/>
Profil - tel/paq/cir/ser/sup/mon	<input type="text" value="1++++++"/>

-> where 901 is the prefix for the site, and 012 the internal KITAXE server number.

-> where 952 is the remote site prefix, and 014 the remote MUFACT server number (if the tickets are centralised).

#### 4.1.4 RESETTING THE INTEGRATED BUFFER MEMORY

At the end of the configuration, reset the integrated buffer. This reset empties all the tickets stored in the buffer.

- **Menu: SYSTEM > Configuration > Tickets > Integrated buffer > Deletion of files of export zone**

Select the type of tickets to delete, followed by the password.



## 4.2 CONFIGURING ALARM PROCESSING (SNMP MANAGER)

### 4.2.1 CONFIGURING SNMP MANAGER

SNMP traps are used to alert MiVoice 5000 Manager to alarms and status changes transmitted by MiVoice 5000 and Mitel 5000 Gateways.

On MiVoice 5000 iPBXs

Configure the SNMP manager IP address (MiVoice 5000 Manager IP address).

- Menu: **SYSTEM > Setting > Alarms > Parameters> Alarms management tab,**

The SNMP1 agent IP address corresponding to the address of the AM7450 address and the NRPE box (MiVoice 5000 Manager) are indicated in the iPBXs identification.



**Note:** The remaining addresses 2 and 3 may be declared if other SNMP managers must be reached.

Enable or restart the SNMP service and SNMP agent service.

- Menu: **SYSTEM > Configuration > Services**

Multi-company management	<input checked="" type="checkbox"/>
Multi-site management	<input checked="" type="checkbox"/>
Service LDAP	START
Service WEB	START
Service SNMP	START
Service AGENT SNMP	START
Service SIP	START
Service FTP	START
Service TFTP	STOP
Service SSH	STOP

**Testing SNMP traps** (example with IP address 100.100.22.33)

Example for a system identification (MIB known for any SNMP system):

**snmpget 100.100.22.33 sysDescr.0**

Example for the global status of a MiiVoice 5000 (AMT MIB):

**snmpget 100.100.22.33 globalStatus.0**

**4.2.2 ALARM CONFIGURATION**

**Configuring the generation of integrated buffer related alarm tickets**

**Menu: SYSTEM > Configuration > Alarms > Individualised configuration**

Detection in

By SBL group

Of alarm

Routed to

-> To generate a ticket for the following alarms

Click "Select item" to access the following screen.

Alarm: NOT EQUIP.	<input type="text" value="URGENT"/>
Alarm: DOWNLOAD	<input type="text" value="URGENT"/>
Alarm: DISABLED	<input type="text" value="URGENT"/>
Alarm: IN SERVICE	<input type="text" value="URGENT"/>
Alarm: OUT OF SRV	<input type="text" value="URGENT"/>
Alarm: FAULTY	<input type="text" value="URGENT"/>
Alarm: HW FAULT	<input type="text" value="URGENT"/>
Alarm: LOCKED	<input type="text" value="URGENT"/>

## 4.2.3 ALARM CALLS

Alarm calls must be configured on the IPBX which contains the LSB that must generate the call. In the example below, the integrated buffer LSB is taken into account.

### 4.2.3.1 Configuration of call generation

**Menu: SYSTEM > Configuration > Alarms > Individualised configuration**

Detection in	LOCAL SITE
By SBL group	INTEGR. BUFFER
Of alarm	.....
Routed to	X25 ADDRESS
<input type="button" value="Select the item"/>	

Click "Select item" to access the following screen.

Address 1 corresponding to the MiVoice 5000 Manager address.

Alarm: BEGIN AL.	ADDRESS 1
Alarm: END AL.	NOT TRANS.
Alarm: IN SERVICE	NOT TRANS.
Alarm: OUT OF SRV	ADDRESS 1
Alarm: INFO LOSS	ADDRESS 1

### 4.3 ADMINISTRATION PARAMETERS

#### Billing parameters

Menu: **SYSTEM > Configuration > Tickets > Billing parameters**

----- charge records -----

Use of format 4500

Step by step definition

Site number overridden in record

Choose the link

----- call records -----

Step by step output

Output format

Trunk identified by

Truncate last 4 digits

Call type

Delete records w/out charging

Internal call record generation

Last internal company

Choose the correct format

Choose NO if billing software is

These options must be ticked

## 4.4 DOWNLOADING TELEPHONY PARAMETERS

For this procedure, also refer to documents [0] - MiVoice 5000 Manager – User Guide AMT/PUD/NMA/0003/EN, especially for periodic export mode.

**Menu: SUBSCRIBERS > Rights > General parameters**

To correctly download the telephony parameters to MiVoice 5000 Manager, the following parameters must be defined on the iPBX (see 10.6 - Downloading iPBX data to MiVoice 5000 Manager for more information).

Com abbreviated dialing	
- number of numbers	1000 ▾
- numerous prefixes	<input type="checkbox"/>
Subscriber forwarded to exterior	
- Charging	CALLING ▾
- send ident.	CALLING NUMBER ▾
Feature class management	YES ▾
TL class management	YES ▾
Partition class management	<input type="checkbox"/>
DID numbers handled by the Manager	<input type="checkbox"/>
N° without external prefix for SIP set	<input type="checkbox"/>
Subscription lock duration(min)	5
Routing of FXT calls	LOCALISATION SITE ▾

The parameters **Feature class management** and **TL class management** must be set to **YES (AUTO YES)**.

The parameter **Management of partition class** can be selected if management of partition classes and priorities has been configured for all sites.



# **PART II: INSTALLING AND CONFIGURING MIVOICE 5000 MANAGER**





## 5 CONFIGURING RED HAT OR CENTOS

CentOS 7.x must first be installed before installing MiVoice 5000 Manager V3.4 on the server PC.

### Centos environment:

See the document AMT/PTD/NMA/0059 - Centos and Double Attachment - Installation guide.

For a simplified installation, these documents recommend that the firewall be deactivated.

**For Mitel applications, the use of a firewall is, nevertheless, recommended in order to secure the network. In this case, the firewall must be configured in such a way that it will not filter the ports required by the application to work properly.**

This chapter specifies the Red Hat or CentOS configuration elements required for MiVoice 5000 Manager installation.

### 5.1 CONFIGURING THE FIREWALL

Log on as **root**.

Right-click the desktop then click the menu **Open in a terminal**.

Configure the file **iptables** in the directory **/etc/sysconfig**.

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

### Configuring connection ports using a firewall

Connections to ports must be allowed on the Linux server running the portal, the management services and ISDN call automaton (the configurable ports are indicated by \*):

PORTS TO BE AUTHORISED	USE
TCP 22	<b>SSH</b>
TCP 80	<b>HTTP</b>
TCP 443	<b>HTTPS</b>
TCP 25	<b>SMTP (mail transmission)</b>
TCP 8201 - 8220	* <b>Min-maxi VT100 port</b>
TCP 9010	* <b>BUFTIC port (M7430)</b> (file: globalConfig.xml)
TCP 9500	<b>Transit AG_COMM (M7430)</b> (file: globalConfig.xml)
UDP 162	* <b>SNMP (trap manager)</b>
TCP 20911	* <b>Net remoting (webservices)</b> (file: 7450Portail.exe.config)
TCP 90	<b>HTTP #2 Supervision SNMP Nagios</b>
TCP 1234	(local) supervisor socket to ag_superv and the portal
TCP 7430	(local) socket of ag_xml to the portal
TCP 8080	ISDN call_automaton
TCP 389	LDAP connection port
TCP 13888	UCP connection port

## 6 INSTALLING AND CONFIGURING THE SERVER PC

### 6.1 INSTALLING THE SERVER PC

#### 6.1.1 IMPORTANT PRE-REQUISITE

In V3.4, CentOS 7.x must first be installed before installing MiVoice 5000 Manager on the server PC (PC 64 bits mandatory).

See the document AMT/PTD/NMA/0059 - CentOS and Double Attachment - Installation guide.

In a virtual VMware environment a .zip file is available on Mitel's Extranet, for deploying a VM called **AM7450\_33zxyy** (where z is the release, xx the phase, and yy the batch).

This VM contains:

- **OS CentOS 7.x**, pre-configured to support MiVoice 5000 Manager V3.4 (partitioning, packages, etc.)
- Pre-configured **MiVoice 5000 Manager V3.4** (network parameters, NAGIOS, etc.)
- The documentation associated with V3.4, accessible via the **Index Doc** MiVoice 5000 Manager shortcut

The IP address is first configured while installing Red Hat or CentOS. However, it is possible to modify this address once the MiVoice 5000 Manager server is installed. Refer to Section Reconfiguring MiVoice 5000 Manager IP address.



**CAUTION:** When configuring the network, it is essential that the machine name (hostname) does not include the character "." (full stop). Therefore, the default name "localhost.local-domain" should not be used. For example, the name host is acceptable, whereas the name host.domain.com is not acceptable.

#### 6.1.2 INSTALLING THE MIVOICE 5000 MANAGER APPLICATION

Installation on the server PC is done either:

- From the iso image provided on the Extranet Mitel
- From the installation CD-ROM provided.

After Red Hat or CentOS is installed, the server starts in graphic mode. Connect as root with the password defined while installing Red Hat or CentOS.

##### 6.1.2.1 *Intallation from the iso image*

Put the iso image recovered from the Mitel Extranet in a MiVoice 5000 Manager directory ex: /Mitel

1. Check under **/media** that the cdrom file exists. If not, create it using the command: **mkdir /media/cdrom**
2. Mount the iso image with the command:  
**mount -t iso9660 /Mitel/ CD\_7450\_V71A-50.1\_33-RC-A-xx\_xx.iso /media/cdrom -o loop**
3. Start autorun  
**cd /media/cdrom**  
**./autorun**
4. At the end of the installation, enter "q" to quit.
5. Install Nagios package (refer to Installing Nagios)

The portal is active without restarting, as well as the management services and call automaton.  
During a new installation, the next phase is installing the client PC(s).

#### 6.1.2.2 *Installation from the CD-ROM*



**Note:** To activate autorun, use the menus **System > Preferences > Removable peripherals and media** then tick the box **Start programs automatically on new peripherals and media**.

The installation procedure is as follows:

1. Insert the installation CD in the CD drive.
2. Confirm the autorun request or launch the autorun process manually.
3. Autorun starts the installation script comprising the following phases:
  - Selecting a language
  - Consulting the documentation
  - Testing the CD-ROM
  - Checking the prerequisites
  - Installing third-party applications
  - Installing the MiVoice 5000 Manager application.
4. At the end of the installation, type "**q**" to exit the installation.
5. Installing Nagios Extended Status Map (see Section Installing Nagios)

The portal is active without restarting, as well as the management services and call automaton.  
During a new installation, the next phase is installing the client PC(s).

#### 6.1.2.3 *Changing the MiVoice 5000 Manager default language in a non-virtual environment*

Right-Click then a terminal

- Enter the command: **cd /home/scripts\_m7450**
- Enter the command: **./change\_lang\_7450.sh [langue]**

The language code is defined by 2 caracteres (DE, EN, FR, IT, NL, PL)

exemple to change in english: **./change\_lang\_7450.sh en**

### 6.1.3 INSTALLING THE MIVOICE 5000 MANAGER APPLICATION IN A VIRTUAL VMWARE ENVIRONMENT

From a .zip file called **IW460AAXXX33zxyy.zip**, available on Mitel's Extranet, 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 machine on which the MiVoice 5000 Manager VM must be installed.



**Note:** The content of the .zip file must also be burned on a DVD.

- Connect to the ESX server machine via the client vSphere.
- Click the menu **File > Deploy OVF model**.
  - Click **Browse** then select the disk space or DVD on which the file **AM7450\_33zxyy.ovf** is located.
  - Then click **Next**.
  - Check the details of the OVF model then click **Next**.
  - Check the VM name then click **Next**.
  - Select the disk format **Thick provisioned format** then click **Next**.



**WARNING:** VM requires 80 GB hard disk space, dual core and 4 GB RAM.

- Click **Finish** to start deploying the VM **AM7450\_33zxyy**.
- Wait till the end of the deployment operation then click **Close**.
- Select the VM **AM7450\_33zxyy** then start it by clicking the green arrow.
- Click the **Console** tab.
- Log on as root (default password: **Mitel5000**).



**WARNING:** For the input, the initial keyboard layout is **AZERTY** for installation in French, and **QWERTY** for installation in English. The keypad is not activated.

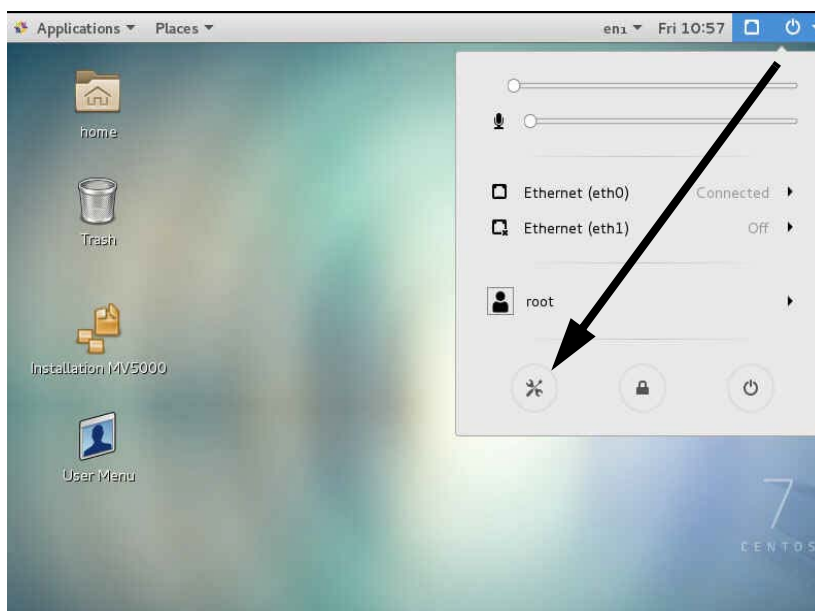
**Modify the system language and keyboard language.**

This stage is necessary if the default languages are not convenient. By default, the languages are English (UK) and English (US) as indicated below.

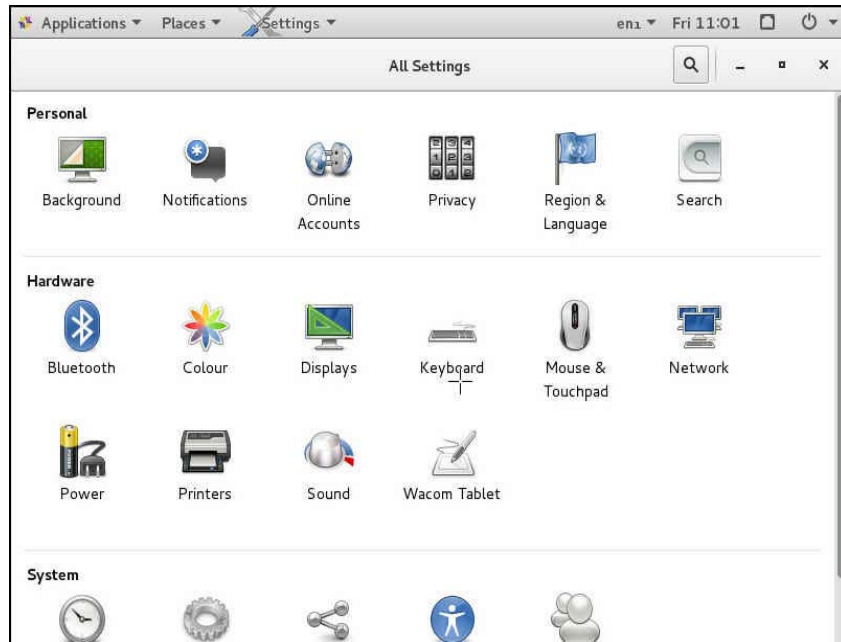


To modify these parameters:

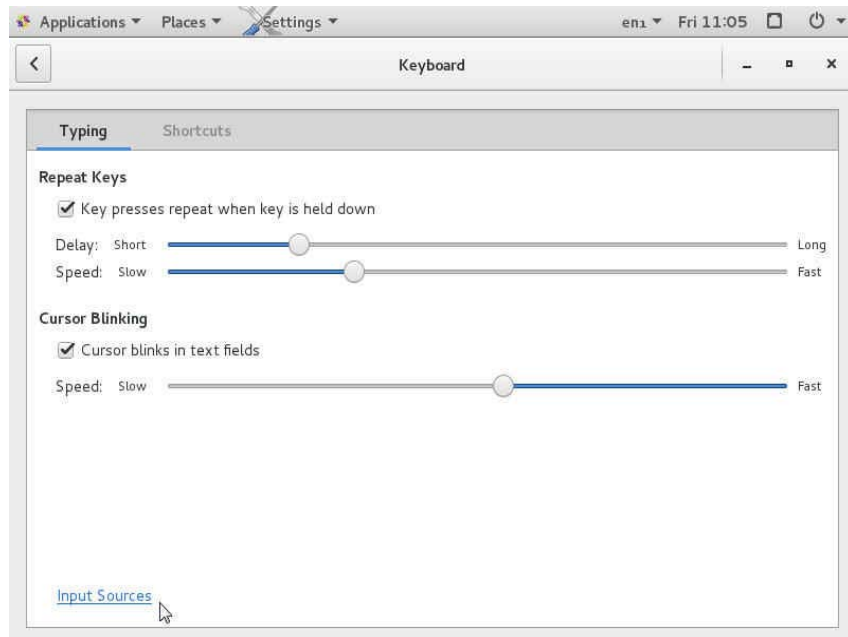
Select the **Tool** icon from the menu on the top right corner:



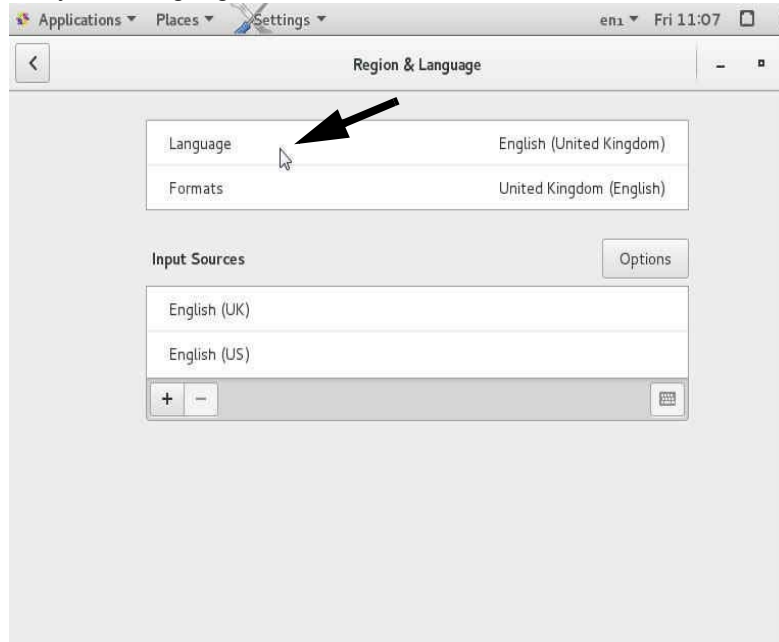
Click **Keyboard** in the **Hardware** menu:



In the screen that opens, select **Input Sources**,



Then select the system language.



In the **language** window choose the language you want (example: French).



Click **Done**

The system proposes to restart. Do not restart immediately by closing the window (**X**)

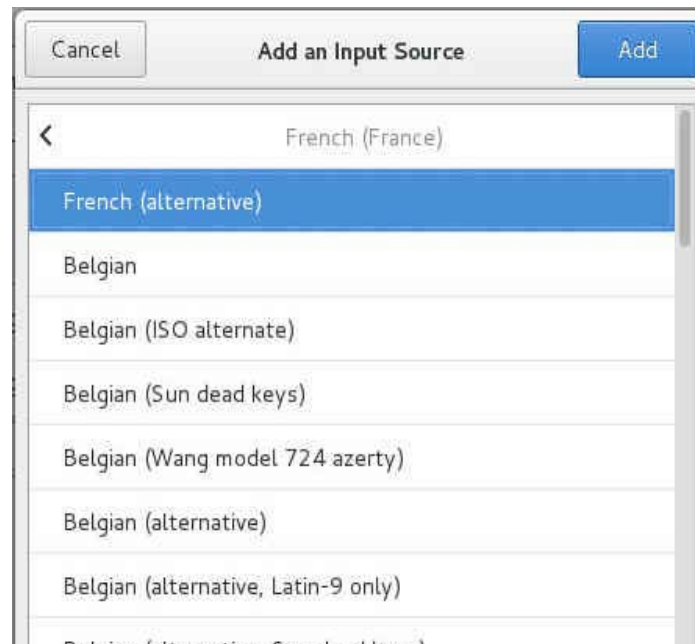


In the **Input Sources** area, select the keyboard language by clicking **+** to display the list of options:



Click the input source a first time (French in the example).

Then click the option concerned for the source input language (French (alternative))



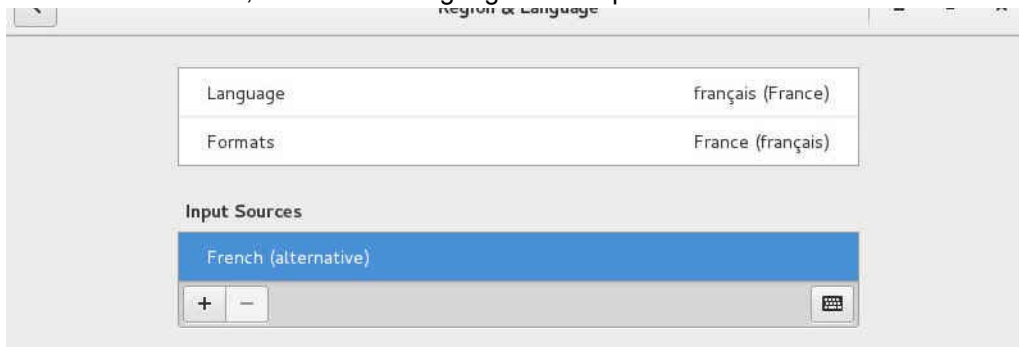
Click **Add**



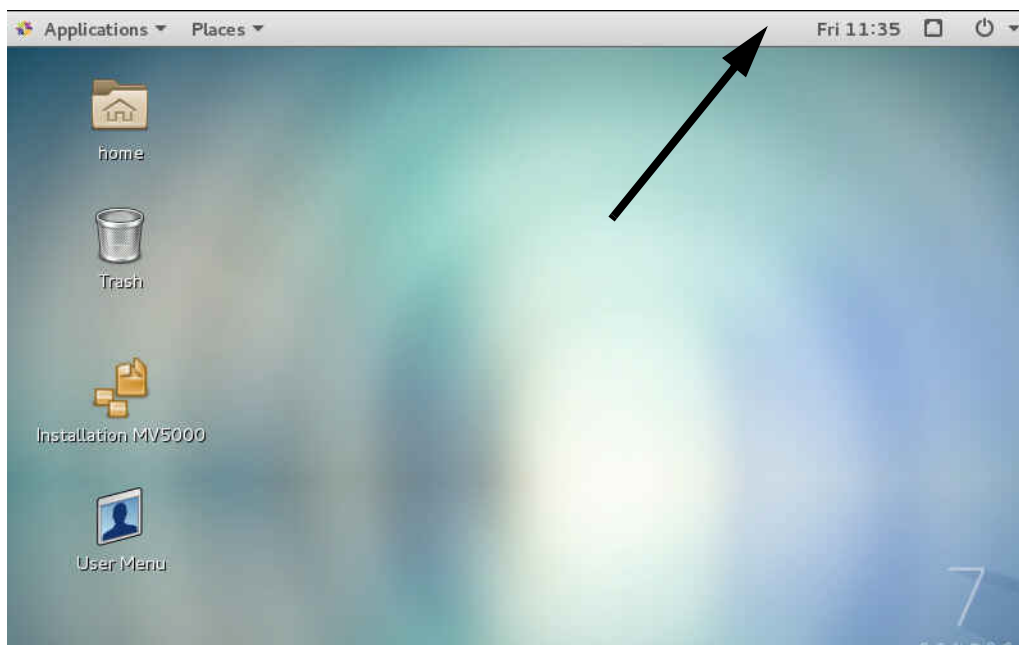
**The new source of input has been taken into account.**

Remove the languages not required by selecting the corresponding lines then on -

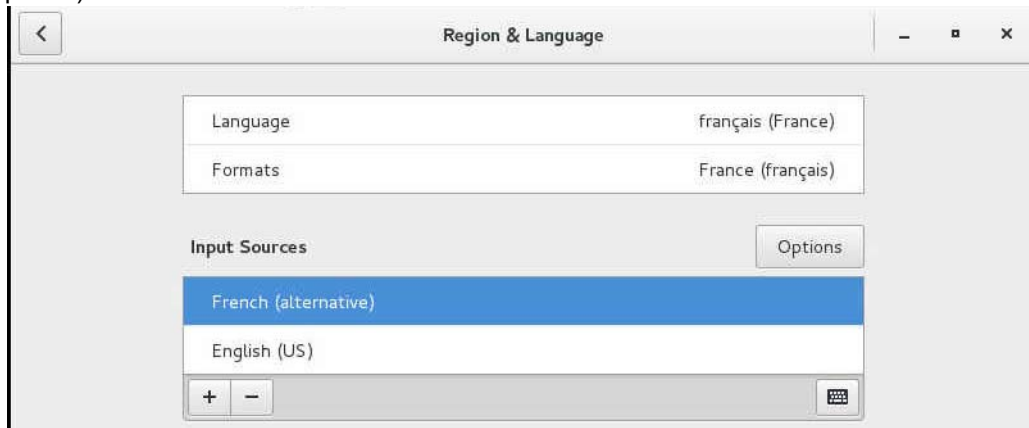
The result is as follows, once all the languages not required have been removed:



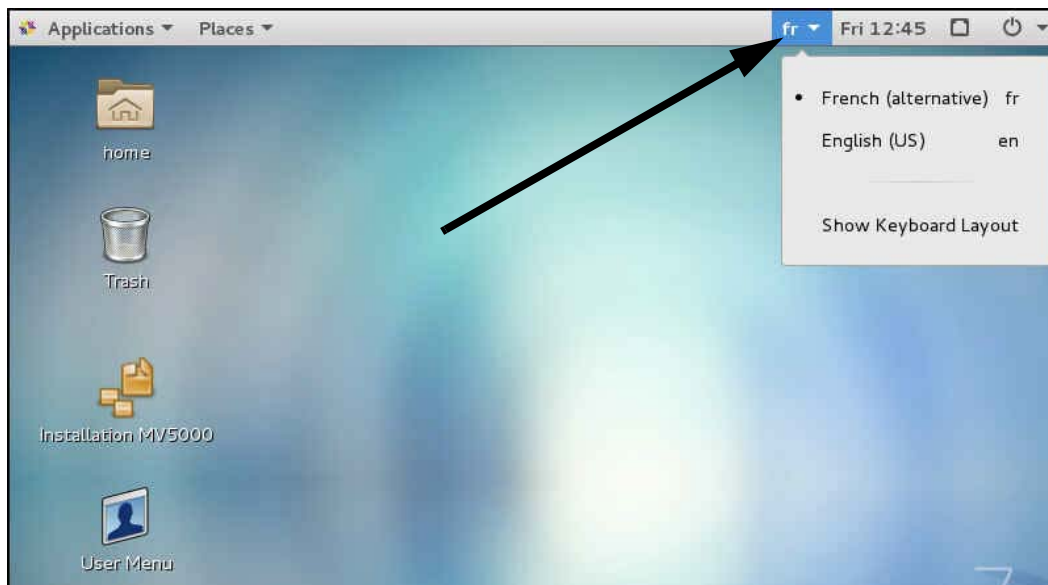
The result is as follows once the languages not required have been removed except one (no options):



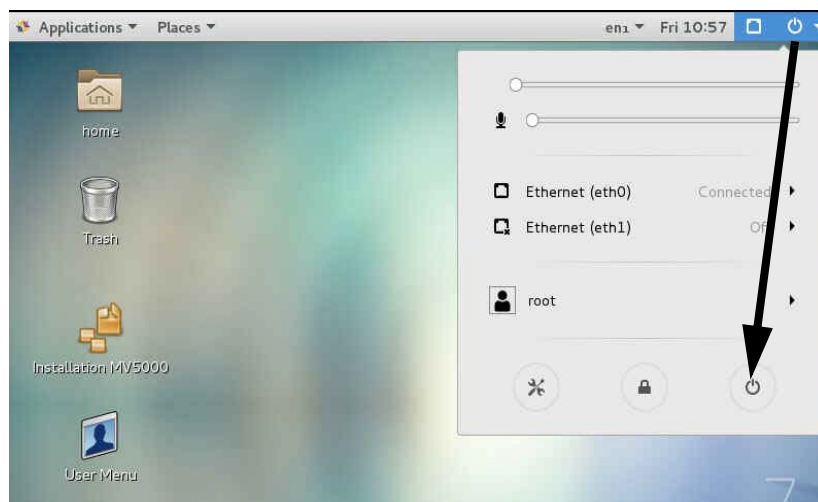
The result is as follows once all but a few languages not required have been removed except one (no options):



An options list is proposed on the welcome screen.



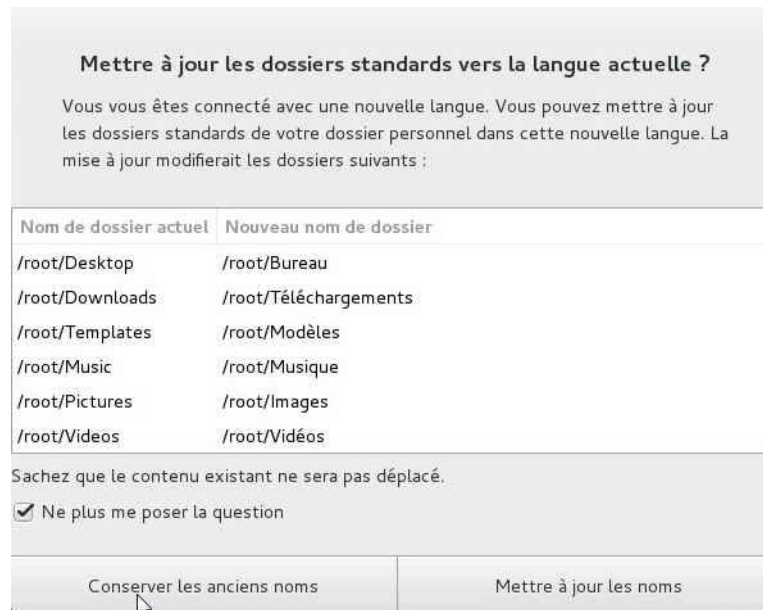
**Restart the system**



Then click **Restart**

Log on as **root** (default password: **Mitel5000**)

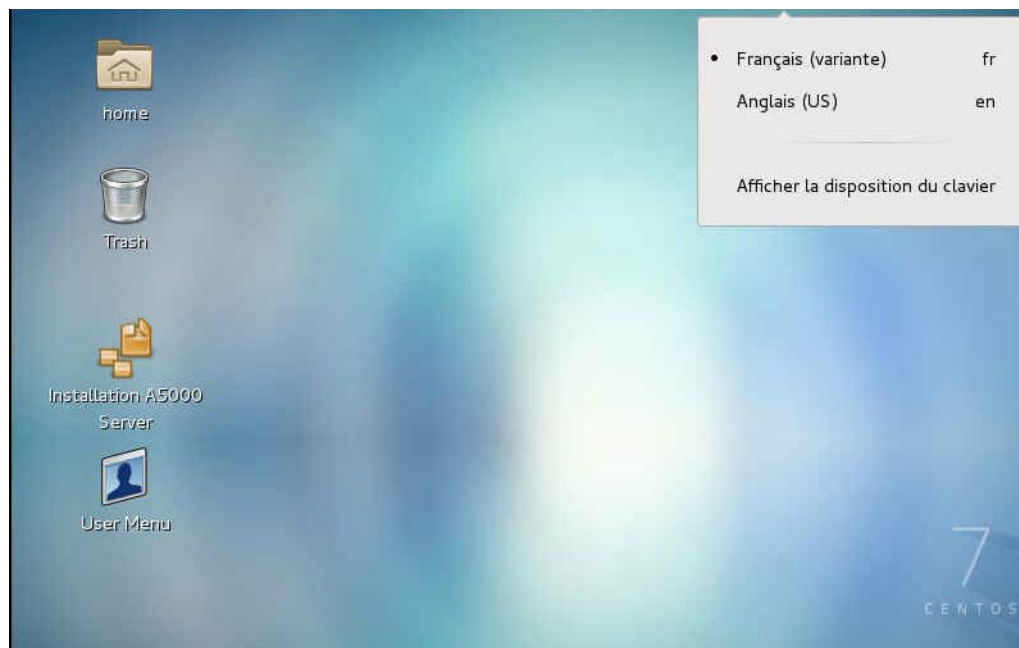
The system displays the following message:



Select **Keep old names** and tick the box **Do not ask me the question again**.

The welcome screen opens with the updated language parameters:

:



**Note :** After installing the VM AM7450\_3xxyy, MiVoice 5000 Manager is automatically installed, in the French configuration.

## 6.2 CHANGING THE DEFAULT LANGUAGE OF THE MIVOICE 5000 MANAGER APPLICATION IN A VIRTUAL VMWARE ENVIRONMENT

This operation is necessary if the installation concerns a country other than France.

- From the client vSphere check that the VM **AM7450\_3.1zxxyy** has been started.
- Log on as root.
- Right-click then **Open a terminal**.
- Type in the following command: **cd /home/scripts\_m7450**
- Type in the following command: **./change\_lang\_7450.sh [langue]**
- The [language] code comprises 2 characters (DE, EN, FR, IT, NL, PL).

Example for changing to French language: **./change\_lang\_7450.sh fr**




## 6.3 RECONFIGURING MIVOICE 5000 MANAGER IP ADDRESS

If necessary, this procedure is used to modify the IP address of the MiVoice 5000 Manager server since this latter is supposed to have been declared while installing Red Hat or CentOS.

Modifying the MiVoice 5000 Manager server IP address also implies:

- Updating the location of the LDAP directory (on MiVoice 5000 Manager)
- Updating the location of SNMP Manager

### 6.3.1 RECONFIGURATION OPERATIONS ON THE SERVER PC AND MIVOICE 5000 MANAGER CLIENT PC

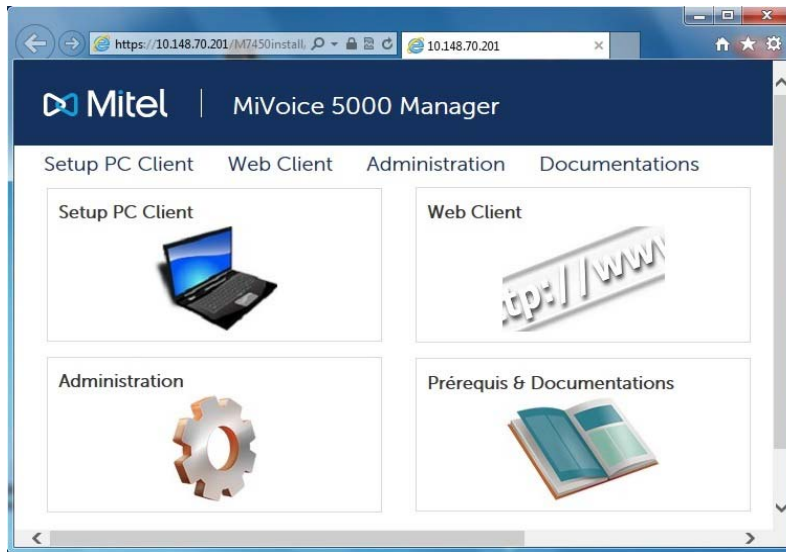
- Log on as **root**
- Select the  icon on the top right side of the desktop,
- Select the  icon,
- Select **Network** in the **Hardware** area.
- In the **Wired** field, select the  icon.
- Select the **IPv4** field.
- Select **Manual** in the options on the top right side.
- Define the (fixed) IP settings of the access concerned in the **Routes** area.
- Click **Apply** to confirm.

Restart the MiVoice 5000 Manager server PC.

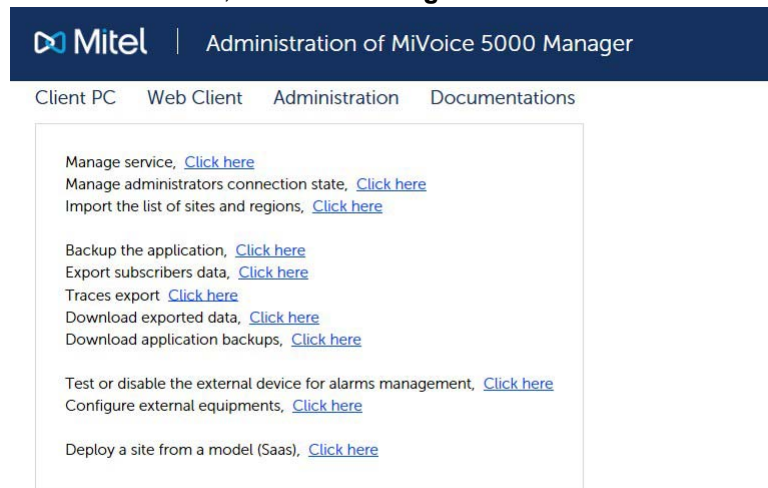
On the client PC, stop the service as follows:

Access Web Admin via the web interface.

From the welcome screen, access the **Administration** window.



In the **Administration** window, select **To manage M7450 service**




Enter the password and login (**M7450/M7450**) to access the service management screen.

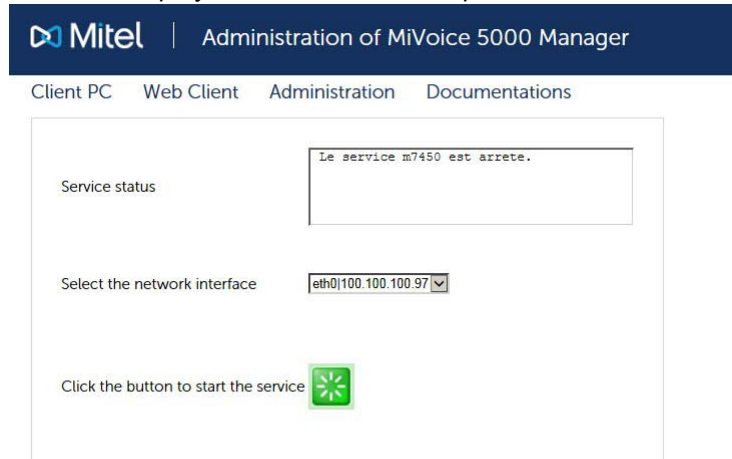




**Note:** The field indicating the MiVoice 5000 Manager server not yet modified is greyed out and, thus, inaccessible.

Then click the  button to stop the service.

The following screen is displayed with a new list of options for the network interface.





Mitel | Administration of MiVoice 5000 Manager

Client PC Web Client Administration Documentations

Service status: Le service m7450 est arrete.

Select the network interface: eth0|100.100.100.97

Click the button to start the service 

In this field, select the new server address and restart the service by clicking .

Restart the MiVoice 5000 Manager client application as indicated in Chapter 10.

## 6.3.2 RECONFIGURATION OPERATIONS IN THE LDAP DIRECTORY

On the MiVoice 5000 Manager side

From the MiVoice 5000 Manager client PC

In the menu **Administration Menu > Configuration > Directory tab**

Enter the new IP address.

On the iPBX site side (from Web Admin)

On each site in the multi-site configuration, reconfigure the IP address for this new connection:

**Menu: SUBSCRIBERS > Directory > Parameters > Connections**

Refer also to Section 4.4.

## 6.3.3 RECONFIGURATION OPERATIONS IN SNMP MANAGER

For each site in the multi-site configuration, restart the identification to reconfigure the new SNMP Manager address. (from Web Admin).

Refer to Section 4.2.

## 6.4 INSTALLING NAGIOS

Nagios is a Java application used for network supervision. This application must be installed in order to recover the traps transmitted by the iPBXs.

Nagios must be installed after the MiVoice 5000 Manager.

The Nagios installation file is provided on the MiVoice 5000 Manager application CD-ROM in a special directory (**CUSTOM\_NAGIOS/**).

Double-click the installation program (**install**) from the Nagios directory (**CUSTOM\_NAGIOS/**) to start installing Nagios.

Restart the system.



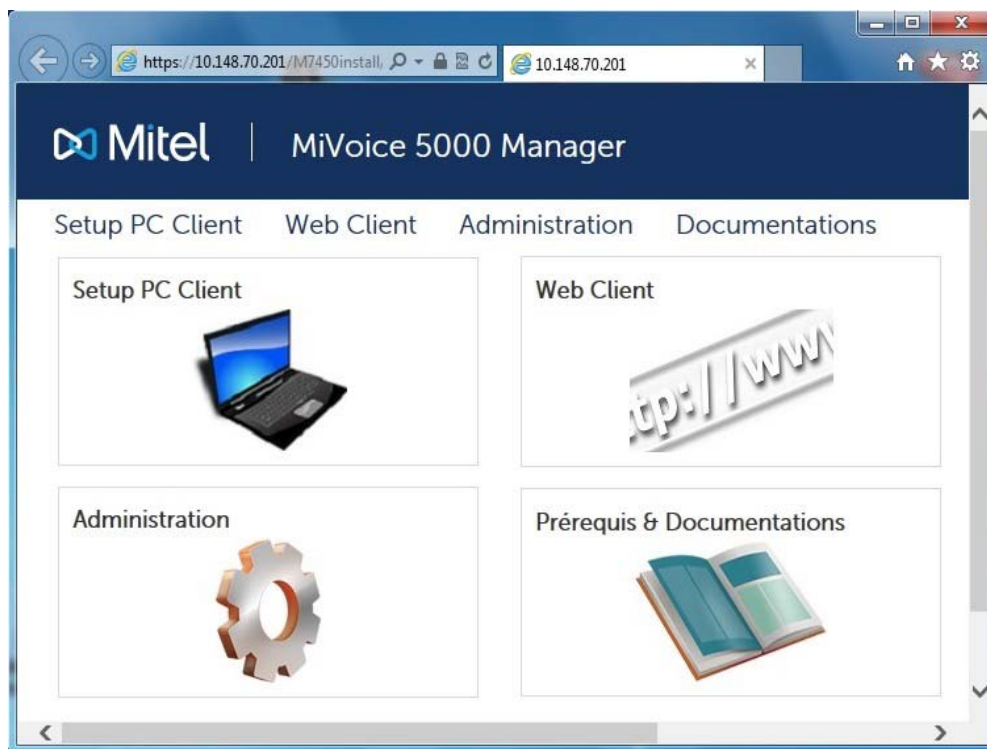
## 7 OVERVIEW OF MIVOICE 5000 MANAGER PORTAL

The MiVoice 5000 Manager portal contains different links used to install and manage the MiVoice 5000 Manager application.

The portal is accessible via a web browser, using the following address:

**https://Server\_IP@M7450install/** , where "Server\_IP@" is the server IP address or name of the server on which the application is installed.

The portal welcome page is as follows:



- **Setup PC Client:** starting or updates the MiVoice 5000 Manager client application.
- **Web Client:** this link is used to start the subscriber management application by profile. This application only allows the management of subscriptions related to a profile.
- **Administration:** opens the Administration window used to install the client application and access administration functions. This access is subject to an operator profile **Login/password**. Depending on the profile (administrator or specific profil), different services are offered (see the section **Managing operators** in the document [0] - MiVoice 5000 Manager – User Guide AMT/PUD/NMA/0003/EN).

- **Prerequisites and documentation:** This link gives access to the following columns:
  - **Prerequisites:** Table giving the software solutions required for the MiVoice 5000 Manager client if they had not been previously installed:
    - **The Manager's root certificate:** this link is used to download the default self-signed certificate provided by MITEL in order to set up a secure "https" connection between the MiVoice 5000 Manager client and the server.  
See Chapter 8 - Installation on client PCs. To install the certificate, click **Recover**.
    - **Framework .NET 4.6:** This option is used to create a **software environment** with Framework .NET. This component is only installed when the product is installed for the first time. If this component is not installed on your PC, click **Recover**.
  - **Site configuration import:** Excel file for massive site configuration
  - **Miscellaneous:**
    - a file describing the MiVoice 5000 Manager MIB. The MIB contains the information on alarms managed by R5.1 systems and later, and allows communication between the agent and SNMP manager.
    - an Excel file (one for R5.1 systems and later, and one for previous-version systems) used to load the exported "inventory.xml" files: a macro retrieves the inventory from the iPBX in question and formats it.
    - The UCP R2.0 proxy used to manage voice mail boxes through the MiVoice 5000 Manager.
    - The UCP R3.0 proxy used to manage voice mail boxes through the MiVoice 5000 Manager.
    - NRPE component for NAGIOS (Win 64) : This is an add on for NAGIOS that allows to execute plugins on a remote server (CC, UCP).

## 7.1 THE QUICKCREATE APPLICATION

This application allows the subscribers management in profile mode.



## 7.2 ADMINISTRATION WINDOW

This access is subject to an operator profile **Login/password**. Depending on the profile, different services are offered (see the section **Managing operators** in the document [0] - MiVoice 5000 Manager – User Guide AMT/PUD/NMA/0003/EN).

The administrator profile has access to all the menu options in the lists below:

### MiVoice 5000 Manager server administration

- (1) >Manage service, Click [here](#).
- (2) >Manage administrators connection state, Click [here](#).
- (3) >Import the list of sites and regions, Click [here](#).
- (4) >I Import Certificate for Client / manager interface and the User Portal, Click [here](#).
- (5) >Backup the application, Click [here](#).
- (6) >Export subscribers data, Click [here](#).
- (7) >Traces export, Click [here](#).
- (8) >Download exported data, Click [here](#).
- (9) >Download application backups, Click [here](#).
- (10) >Test or disable the external device for alarms management, Click [here](#).
- (11) >Configure external equipments, Click [here](#).
- (12) >Deploy a site from a model (Saas), Click [here](#).

1. This option is used to **manage the MiVoice 5000 Manager service**, view its status or stop it. Click the  button to stop the service, or the  button to start it.
2. This option is used to see the **operators connected** to the MiVoice 5000 Manager application and possibly to disconnect them.
3. You can use this option to **update regions and sites**. It is described in Section 9.5 - Massive creation of regions and their sites. This option allows you to recover **exported data**. It is described in Section 9.7 - Exported data.
4. This option is used to download a certificate (provided by the client) in order to secure the Client/manager interface and User Portal. See the section **Importing an external certificate**.
5. This option is used to start a immediat backup of the MiVoice 5000 Manager data in the case for example if the administrator wishes to launch an updating operation.



**WARNING:** This action deletes the last one done in the same day.

6. This option is used to export all the subscriber data managed by MiVoice 5000 Manager. This export file is then available for consultation in a dedicated directory (1 sub-directory per multi-site). Refer to Section 9.7.2.2.
7. This option is used to start a trace export. The file is then available for consultation in the Export directory.

8. This option allows you to recover **exported data**. It is described in Section 9.5 - Exported data.
9. You can use this option to recover **application backups** so as to save them on a device other than the server PC.
10. This option is used to activate or deactivate the external device (alarm box) for managing alarms. See the document MiVoice 5000 Manager User Guide, chapter "Administration functions".
11. This option is used to configure the external devices capable of sending SNMP traps. These devices will be supervised by the NAGIOS application, and the generated alerts are processed using the same rules as alarms from the network iPBX. The creation of configuration files is described in Chapter 9.8 - Configuring external devices.
12. Refer to the document Easy deployment of a MiVoice 5000 Server Client in SaaS mode - AMT/PTD/NMA/0063.

## 8 INSTALLATION ON CLIENT PCS

The client PC must be connected to the internet.

During a first installation, it is necessary to install the plugin SVG and Framework .NET if it is not included by default in the Windows operating system.

Access to MiVoice 5000 Manager is subject to an operator profile **Login/password**. Depending on the profile, different services are offered (see the section **Managing operators** in the document MiVoice 5000 Manager User guide - AMT/PUD/NMA/0003).

### 8.1 Installing Framework.NET



**Note :** Operation necessary if Framework.net 4.6 is not already installed.

From the client PC, log on to the MiVoice 5000 Manager server by entering the address below

**https://Server\_IP@**, where "Server\_IP@" is the server IP address or name of the server on which the application is installed.

- Click **Download** on the **Framework .NET 4.6** line.
- Upon display of the message "**Do you wish to execute or save this file?**", select **Execute**.
- Upon display of the message "**Do you wish to execute this software?**", select **Execute**.

The components are installed. A message is then displayed, indicating the end of Framework installation.

### 8.2 Installing MITEL certificate (as of Windows 7)

The secure connection (https) between the MiVoice 5000 Manager server and the client terminals requires installing an authentication certificate. Installing a certificate is not mandatory but highly recommended.

A self-signed certificate is offered by default by MITEL. If you do not wish to use this certificate but another one instead, see Section 9.1 - Importing an external certificate.

From the client PC, log on to MiVoice 5000 Manager by entering the following address:

**https://Server\_IP\_address**, where "Server\_IP\_address" is the IP address or name of the server on which the application is installed.

Click the **Prerequisites and documentation** link.

In the **Pre-requisites** table, click the Download link from the Manager root certificate line.

- Open the file.
- In the general tab, click Install certificate then **Next**.
- In Windows 8, select the storage location (Current user or local PC).
- Select **Place all certificates in the store**, then click **Browse**.

The store selection screen opens.

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

The **Certificate import wizard** screen re-opens; click **Next**.

- Click **Finish**: wait for the **Security warning** window to open.
- Click **YES**.
- In the window which indicates that the import has been successful, click **OK**.

- The Certificate screen is refreshed; click **OK** to close the window.
- Close all the navigator windows.
- Restart Internet Explorer and log on to the chosen server IP address (a simple **refresh** is not enough).

### 8.2.1 DELETING AN EXISTING CERTIFICATE

From Internet Explorer:

- Select Menu "**Tool/Internet option**", "**Content**" tab, "**Certificates**" button then the "**Trusted root certification authorities**" tab.
- From the list select "Mitel" then click "**Delete**".
- After the warning message, click "**OK**".
- Then click "**Close**" to leave this environment.

The certificate has been deleted.

### 8.2.2 INSTALLING THE MIVOICE 5000 MANAGER CLIENT APPLICATION ON REMOTE CLIENT PCS

Via a web browser, connect to the MiVoice 5000 Manager server by entering the following address:

**https://Server\_IP@M7450install/** , where "Server\_IP@" is the server IP address or name of the server on which the client application installation executable may be recovered.

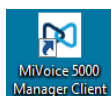
If several MiVoice 5000 Manager servers are managed, choose any of the addresses.

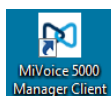
The client will be installed once and for all on the client PC. The MiVoice 5000 Manager Server will then be selected from an options list during Login.

- From the portal welcome page, click **Client PC setup**:



- Click **Run** to install the client application.



- After the client is installed, an icon  is placed on the desktop, and a link created in the **Start** menu.

- The MiVoice Manager Server Login window then opens:



- Enter the IP address or name of the MiVoice Manager concerned.
- The login and password are then required (by default **M7450/M7450**).



**Note :** This is the password for the user logging on to the MiVoice 5000 Manager in question.

- The application is then started, and the welcome page displayed.



The client application is started.

The default password can later be changed from the client application.





## 9 ADMINISTRATION FUNCTIONS

The MiVoice 5000 Manager portal contains different options used to manage the MiVoice 5000 Manager application. These functions concern:

- Downloading a self-signed certificate (in PKCS#12 format) other than the one provided by default by MITEL on the interfaces with MiVoice 5000 Manager,
- Data backup and restore operations,
- Configuration of regions and sites,
- Operator connection management,
- MiVoice 5000 Manager service management,
- External device configuration.

The administrator is responsible for managing the security rules, via a configuration file. Although the portal does not contain any option in this connection, the management of these rules is described at the end of the chapter.

### 9.1 IMPORTING AN EXTERNAL CERTIFICATE

If an encryption certificate other than the one provided by default by MITEL must be used, select the line **Import a certificate for the Client/Manager interface and User Portal** from the **Administration** menu, then click on **Click here**.

- Choose **Browse** to search for the file in question then enter a password if necessary (securing the file).
- Then click **Apply**.

If the file generated is correct, it is then downloaded and stored in MiVoice 5000 Manager. The Web page automatically reloads after a few seconds to display the successful-completion message.

At the same time, the **Manager root certificate** is updated in the Documentation column and prerequisites of the MiVoice 5000 Manager portal welcome page. See Section 8.2 - Installing MITEL certificate (as of Windows 7).



**Note:** The PKCS#12 format is used to store the private keys and certificates in a single encrypted file.

### 9.2 DELETING A CERTIFICATE

From the **Administration** menu:

- Select the line **Import a certificate for the Client/Manager interface and User Portal**, then click on **Click here**.
- The current certificate is indicated in the **Certificate deletion** area.
- Click **Delete** to delete it.

If the self-signed certificate provided by default by Mitel is used, the button is greyed out. This certificate cannot be deleted. Import another one as described in the previous section 9.1 - Importing an external certificate.

A default self-signed certificate is regenerated when an external certificate is deleted.

## 9.3 BACKING UP AND RESTORING THE APPLICATION

### 9.3.1 BACKUP

A daily, automatic backup of the application is programmed by default.

A backup can be also immediately done from the portal **Administration** window, click the link proposed in the option **Backup the application, Click here**.

The backup configuration file is accessible in `"/home/m7450/repository/system"` and is called **back-upportail.xml**.



**Note:** To display the file navigator in Red Hat or CentOS, select **Application > System tools > File navigator**.

By default, back up is programmed to start at 01:00. It can be changed.

This file also contains the last backup date.

The last 31 backups are stored on the server, in the directory `"/home/m7450/backup"`. Each backup is identified by its date.

The backups can be kept 30 days. It can be reduced if necessary by modifying the / file **home/m7450/portail.exe.config**

Modify the line

```
<add key="DELA_SAVE_M7450" value="30"/> (value must be between 3 and 30)
```

To recover the backups:

From the portal administration window, click the link proposed in the option **"To recover M7450 application backups, click here"**.

For a given date, the backup files are:

[config.tar.gz](#): configuration files -> Directory /home/m7450/automate, /home/m7450/portail, /var/www/M7450 and /var/www/webmanagement/data

[m7450.out](#): application data (database)

[repository1.tar.gz](#): Directory /home/m7450/repository/system

[repository2.tar.gz](#): Directory /home/m7450/repository/pabxdata and /home/m7450/repository/Users(except PBXs backup)

[repository3.tar.gz](#): Directory /home/m7450/repository/pabxdata (iPBXs backup)

[repository4.tar.gz](#): Directory /home/m7450/repository/pabxconfig

[repository5.tar.gz](#): Directory/home/m7450/repository/pabxbackup (used in Total mode)

[backup\\_conf\\_ldap.tar.gz & ldap\\_file.ldiff](#): MiVoice 5000 Manager LDAP database backup

[backup\\_nagios.tar.gz](#): Nagios configuration files backup

[selfadmin.tar.gz](#): Self-admin data backup

[syncAd.tar.gz](#): Active Directory synchronisation backup

[tma.tar.gz](#): TMA data backup

[webdata.tar.gz](#): sauvegarde des liens vers les applications Mitel

## 9.3.2 RESTAURE

You can restore via two script sto be run on the server:

- A script for restoring the MiVoice 5000 Manager configuration
- A script for restoring the LDAP database.



**Note:** To open a terminal window in CentOS, from the desktop, right-click and select “Open a terminal”.

- Connect with the login **root**
- Select the directory **/home/scripts\_m7450**
- Launch **su - m7450** command

### For standard restaure without iPBXs backup:

- In the terminal window, type in the command **restaure.sh** parameter management **dd.mm.yyyy**, representing the date of the backup to restore (check). E.g. **"#. /restaure.sh 24.12.2007"**.  
*The duration of the restore operation depends on the size of the configuration..*

### For restaure with iPBXs backup:

- In the terminal window, type in the command **restaure.sh** parameter management **dd.mm.yyyy**, representing the date of the backup to restore (check). E.g. **"#. /restaure.sh -total 24.12.2007"**.  
*The duration of the restore operation depends on the size of the configuration..*



**Note:** The restore script stops the portal automatically. During the operation, the script enumerates the files and data restored.

### **Restoring LDAP data**

- Log on as **root** (or else the LDAP database is not restored).
- Select the directory **/home/scripts\_m7450**
- In the terminal window, type in the command **launch\_restaure\_ldap.sh** parameter management **dd.mm.yyyy** , representing the date of the backup to restore (check). E.g. "**#!/restaure\_ldap.sh 24.06.2013**"



**CAUTION:** In a multi-site configuration containing a directory replica, create the replica after the restore operation (see [0] MiVoice 5000 Manager User guide).

After the restore operations, restart the portal from the administration window.

## 9.4 RESETTING THE MIVOICE 5000 MANAGER DATA CONFIGURATION IN CANONICAL MODE

- If necessary, retrieve the current backups (by moving them, because the reset operation erases these files from the dedicated directory archive).
- Log on as **root**.
- Select the directory **/home/scripts\_m7450**
- Run the canonical reconfiguration script: **./canon.sh**
- MiVoice 5000 Manager restarts with a canonical configuration.

## 9.5 MASSIVE CREATION OF REGIONS AND THEIR SITES

You can perform massive creation of regions and their sites on the server by entering information with an Excel file.

The procedures are:

1. Create regions/sites using the Excel file.
2. Export the content of the file in .xml format.
3. Load the regions/sites on the server from the portal administration window.



**WARNING:** This procedure should only be used for creation. If a big modification must be made, follow the procedure described in Section 6 to recover the existing configuration before modifying it.

### 9.5.1 THE EXCEL FILE

This Excel file is provided on the installation CD. It is also accessible from the Documentation menu of the MiVoice 5000 Manager portal welcome page .

To use it, save it to the hard disk of a Windows PC with Excel.



**Note:** Since it contains macros, this Excel file is not compatible with Open Office.

- Open the .xls file.
- A message is displayed, specifying that the macros have been deactivated. Click on "Activate content". For Excel 2003, see Section 9.5.1.1.
- An **Instructions** tab opens, showing the following three buttons:
  - **Create** button: for creating a region and its sites
  - **Export** button: for exporting the regions/sites file in xml format
  - The **Import** button: for importing the regions/sites file used to recover the existing configuration on the server so as to update it (see Section 6.).

### 9.5.1.1 *Excel file macros (office 2003)*

When a message, indicating that the project macros have been deactivated, appears when the file is opened, change the security level of the Excel application.

1. Close the Excel file used to create regions/sites.
2. Open the Excel application.
3. In the **Tool** menu, select **Macro** then **Security**.
4. In the Security tab, check the **Average security level** option.

When the input file is opened, a message will henceforth indicate that the file contains macros. Click **YES** to execute the macros.

### 9.5.1.2 *Creating regions and sites*

You can create a region without assigning it a site. Nevertheless, to benefit from mass update, each site involved is described in the created tab.

1. From the **Instructions** tab, click **Create**.

A **Create a region** window opens.

2. Enter the name of a new region then click **OK**.

A new tab with the name of the region appears.

3. For each site in the region, fill in the fields defined in the following table (note: do not use the quotation character ") :

CHAMPS	INFORMATION À SAISIR
Name	Site name
Multisite	Site part of a multisite (NO: default value)
Multisite name	This name must be unique in the entire multisite. All sites belonging to the same multisite in this column must have the same name.
Reference site	Only one reference site in a multisite.
Cluster	Cluster mode: YES or NO Choice list
Node	YES or NO Choice list
Cluster name	Choice mandatory when creating a node. The cluster name must be defined.
IP address	Site access IP address
Adress	Site address
Comment	Free text
MMI password	MMI default password
IP address in telephony network	IP address in the telephony network (used for encryption).

4. Check the information.
5. Save the Excel file to complete it later, or start exporting data.

Des controles sont effectués avant enregistrement :

- if a node is created, a cluster must be defined
- an element of a cluster node or a cluster but not both
- a cluster belongs to a multisite. The multisite must have been defined.
- a node can not be a reference site.

### 9.5.1.3 *Exporting the regions/sites file*

1. From the **Instructions** tab, click **Export**.

A backup window allows you to save the file to the location of your choice on the PC. A macro converts the Excel file to two .xml files, with the following default names: region.xml and site.xml

2. Click **Save**.

### 9.5.1.4 *Loading regions and sites to the server*

This loading procedure is done from a PC fitted with a web browser.



**Note:** This can also be done from the MiVoice 5000 Manager client application. See the application's User Guide.

1. Connect to the MiVoice 5000 Manager portal welcome page. Enter the IP address of the server on which the MiVoice 5000 Manager application is installed.
2. In the portal administration window, select the option "**To import the list of regions and sites, click [here](#)**".
3. In the authentication window, enter the username and password.  
A new site and region import window opens.
4. Select the XML files of the regions and sites, using the **Browse...** button, then click **Load**.  
A modification window opens, allowing you to check the creations or modifications made to the configuration. On this list, you can check:
  - The regions added, the regions removed, the regions modified (old name/new name)
  - The sites added, the sites removed, the sites modified (new name/old name, new region/old region, connection parameters, connection).
5. Click **Apply**.

*The following warning message specifies the update modalities.*

#### **Import validation**

<p><b>Attention :</b></p> <p>During the import all datas concerning suppressed sites will be removed.</p> <p>A backup point will be done in order to be able to a roll-back.</p> <p>The server will be re-started in order to take in count the import.</p>
---

Validate


6. Click **Confirm** to start updating the server, followed by automatic restart of the portal.

## 9.6 OPERATORS' CONNECTION STATUS

To see the list of connected operators:

In the portal administration window, click "**To manage operators' connection status, click here**".

The screen displays the following information:

- The connected operator's login
- The IP address of the PC with which he or she connected
- A  button for disconnecting the selected operator. You will be asked to confirm disconnection before the operator's session ends.



## 9.7 EXPORTED DATA

Data is exported from iPBXs as follows:

- For immediate actions: according to the general configuration defined in the **Export** tab of the **Administration/Configuration** menu.
- For campaigns: exports may be redefined in the action parameters while they are created.

### 9.7.1 DISPLAYING EXPORTED DATA

By default, the exported data is stored in the directory **/home/m7450/repository/Export**. The export directory can be redefined in the Export tab of the **Administration/Configuration** menu of the MiVoice 5000 Manager client application (see the MiVoice 5000 Manager user guide).



**Note:** These data are not purged by the MiVoice 5000 Manager.

Exported data can be retrieved from the MiVoice 5000 Manager portal. It can be backed up to the PC.

1. Connect to the MiVoice 5000 Manager portal. Enter the IP address of the server on which the MiVoice 5000 Manager application is installed.
2. From the Portal administration window, select the option "**To recover the exported data, click [here](#)**".
3. In the authentication window, enter the username and password.  
A list of directories is displayed.

### Index of /M7450export

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">Inventory/</a>	13-Mar-2009 01:00	-	
<a href="#">M7450Configuration/</a>	12-Mar-2009 01:01	-	
<a href="#">M7450LogBook/</a>	09-Apr-2009 11:39	-	
<a href="#">TMA/</a>	09-Feb-2009 11:25	-	

**Figure 9.1: Exported data screen**

## 9.7.2 DESCRIPTION OF THE EXPORT DIRECTORIES

### 9.7.2.1 *Billing*

This directory contains the exported directory records and call tickets for the billing applications. The tree structure of this directory is as follows:

Billing ->

- Region name ->
  - Site name (for an isolated site) or multi-site name ->
    - Site or multi-site directory file
    - Ticket file in the form `yyyymmddhhmns.sitename`:
      - yyyy = year )
      - mm = month )
      - dd = days )Download date
      - hh = hour )
      - mn = minute )
      - ss = second )
      - sitename = name of site (isolated or part of a multi-site network).

### 9.7.2.2 *M7450Configuration*

This directory contains three sub-directories:

- **Alarm : XXXXXXXXXXXXXXXX**
- **Operator:** this directory contains the export of the operators file (`operators.xml`). This file is exported each time a user is modified.
- **Site:** this directory contains the site file (`site.xml`) and regions file (`region.xml`). These files are exported upon user request from the export configuration screen.
- **Configuration:** this directory consists of the sub-directories for each multi-site. These sub-directories contain all the exported files:
  - Directory data
  - External contacts
  - Technical records
  - VM records
  - Keys
  - Assignments
  - Forwarding for R5.2 sites or later
  - The files are in ".**csv**" and "**HTML**" format.

### 9.7.2.3 M7450LogBook

This directory contains a backup of the records of portal operations deleted during a purge. During each purging operation, a file is created, whose name is in the format jdo\_yyyymmddhh.xml where yyyy = year, mm = month, dd = day, hh = hour.

If the purge is monthly, the file contains the records of the month prior to the purge.

### 9.7.2.4 PBXLogBook

**This directory contains the exports of the logbook of each iPBX. The tree structure is as follows:**

PBXLogBook ->

- Region name
  - Site name (for an isolated site) or multi-site name ->
    - Logbook files (one file per day) in the format
    - yyyymmddhhmnss.sitename:
      - yyyy = year )
      - mm = month )
      - dd = days ) Logbook date
      - hh = hour )
      - mn = minute )
      - ss = second )
      - sitename = name of site (isolated or part of a multi-site network).

### 9.7.2.5 Inventory

This directory contains exports of iPBX inventories under the following tree structure:

Inventory ->

- Region name
  - Site name (for an isolated site) or multi-site name ->
    - IPBX inventory file (inventory.xml).

### 9.7.2.6 Debug

This directory contains exports of iPBXs diagnostic under the following tree structure:

PBXLogBook ->

- Region name
  - Site name (for an isolated site) or multisite name ->
    - Les fichiers compressés contiennent les fichiers suivants :
      - dumpip
      - errors
      - traces
      - troubleshooting

## 9.8 CONFIGURING EXTERNAL DEVICES

The MiVoice 5000 Manager application is used to process traps from SNMP devices not managed by the application (servers, routers, applications, etc.). If the IP address of the trap sender is known, this trap is taken into account. The severity level is defined on a device by device basis.

This chapter handles the management of configuration files. The use in the application is described in the document [0] - MiVoice 5000 Manager – User Guide AMT/PUD/NMA/0003/EN MiVoice 5000 Manager User Guide.

1. From the MiVoice 5000 Manager portal administration window, select the option "**To configure external devices, click [here](#)**".
2. The following screen is displayed:

**Aastra Management 7450**

Configuration of the external SNMP equipments

Name :  Type:  Address :

Management URL :

Trap severity :

Trap message :

Severity of the successful polling :

Message of the successful polling:

Severity of the failed polling :

Message of the failed polling :

[Click here to go back to the main page](#)

### 9.8.1 ADDING A DEVICE

1. Click **Add**.
2. Fill in the different fields:
  - **Type of equipment** : Select the type of equipment (CC/TWP, ..)
  - **Name**: name assigned to the device (without space or classification mark, and 20 characters maximum). This field is mandatory.
  - **Address**: device IP address. This field is mandatory.
  - **Management Url**: when a management URL is entered here, it is accessible from the alarm log, via the Zoom link (see the chapter Supervision, in the document [0] MiVoice 5000 Manager User Guide).
  - **Severity associated with the trap**: define the severity level (0: OK / 1: Warning / 2: Minor / 3: Major / 4: Critical). The default value is 3.
  - **Severity associated with the trap**: text which will be sent with the trap and used by the MiVoice 5000 Manager application in alarm management. The default message is: " Trap received on device" + name of device.
  - **Severity associated with the success of the polling**: define the severity level (0: OK / 1: Warning / 2: Minor / 3: Major / 4: Critical). The default value is 3.
  - **Message associated with the success of the polling**: If the field is not filled in, the default message is " Ping OK on" + name of device.

- **Severity level associated with the polling failure:** define the severity level (0: OK / 1: Warning / 2: Minor / 3: Major / 4: Critical). The default value is 0.
- **Message associated with the polling failure:** If the field is not filled in, the default message is " Ping NOK on" + name of device.....

*Only the Name and Address fields are mandatory. If the other parameters are not entered, some default values are defined.*

3. Click **Validate** to save the device in the configuration file.

## 9.8.2 EXPORTING DEVICE CONFIGURATION

It is possible to export the configuration of devices into a .csv file, by clicking **Export**. A "Zoom" link then appears at the bottom of the screen. It can be used to view this file in Excel.

## 9.8.3 DELETING A DEVICE

1. From the MiVoice 5000 Manager portal administration window, select the option "**To configure external devices, click [here](#)**".
2. Select the device by opening the **Name** option.
3. Click **Delete** then **OK** to confirm the deletion.

## 9.9 MANAGING SECURITY RULES

The use of the password associated with the login is regularly controlled. The administrator can modify the default parameters by working on:

- The password format
- The period during which the password must be renewed
- The MiVoice 5000 Manager client inactivity timeout.

The value of these parameters may be increased or decreased in the file **/home/m7450/portail/7450Portail.exe.config** (see examples in Section 9.9.4 - Inactivity timeout).

### 9.9.1 PASSWORD FORMAT

The password format must respect the following rules:

- Rule 1: minimum length: 8 characters
- Rule 2: at least 1 lower-case character
- Rule 3: at least 1 upper-case character
- Rule 4: at least 1 numeric character
- Rule 5: no accents or apostrophes
- Rule 6: respect at least 3 of rules 2 to 5.

### 9.9.2 PASSWORD VALIDITY

The password has a default validity period of 90 days. The value may be incremented or decreased. It may also be changed to 0 to cancel the control of validity duration.

During first connection, or after password reset, the operator must change his password.

### 9.9.3 RESETTING THE PASSWORD

- If case of loss of password, for instance, the procedure for resetting the password is as follows:
- Log on as **root**.
- Then type in the command **htpasswd -m /var/www/M7450/.htpasswd M7450**
- Enter the password you want (you are then prompted to confirm it).

#### 9.9.4 INACTIVITY TIMEOUT

If the operator does not take any action on the MiVoice 5000 Manager client for certain period, a logon window prompts him to log on again.

The default value is 10 minutes. The value may be incremented or decreased. It may also be changed to 10 to delete the inactivity timeout. This value is the same for all the MiVoice 5000 Manager clients.

Each disconnection/connection is recorded in the operation log.

#### 9.9.5 OPERATOR RIGHTS

By default, when creating a new operator, the latter is entitled to all managed objects (regions, sites, hierarchy, ...). It is possible to change this behavior so that on the contrary this new operator has no right default on managed objects. In this case, the "isTreeChecked" parameter must be passed to False.

Example of the parameters of the file 7450Portail.exe.config for security rule management:

```
<add key="passwordpolicy"          value="8-1-1-1-3"/>
<add key="inactivityperiod"        value="10"/>
<add key="pwdchangeperiod"         value="90"/>
```





## 10 CONFIGURING MIVOICE 5000 MANAGER FOR THE FIRST TIME

This chapter describes the main MiVoice 5000 Manager configuration phases after it is installed. For details about each phase and use of MiVoice 5000 Manager, see the User Guide (see document [0]).

The following elements must be configured in MiVoice 5000 Manager:

- The telephony parameter range
- The directory base to use and range of the directory
- Alarm definition
- The configuration of network elements (regions, multi-sites, sites)
- The definition of a reference site

To facilitate the downloading of iPBX information on the MiVoice 5000 Manager server, it is also necessary to first configure the elements in the iPBX, such as telephony parameters, directory records, numbering plans, etc.



**Note:** The telephony parameter and the directory configuration applies to system release 5.1. The directory to configure is the LDAP directory.

### 10.1 DEFINING THE TELEPHONY PARAMETER RANGE

#### Menu Administration > Configuration > range tab

Range definition enables you to define a uniform telephony parameter configuration on some or all of the systems managed.

The telephony parameter range may be **Based on multi-site**, **Based on region** or **Global**. It has a major impact on the management of telephony parameters. It must be defined with precaution because, depending on the initial configuration, it cannot be modified later (the range cannot be extended).

Depending on the systems to be managed:

If management concerns only one multi-site, select the range **Based on multi-site**.

If several multi-sites are to be managed but they are not related to each other, also select **Based on multi-site**. Selecting **Based on region** or **Global** would impose the same configuration on all the multi-sites concerned.

In the other cases, if you select **Based on region** or **Global**, the telephony parameters of the first site listed becomes the reference parameters.

Refer also to Section 4.4 - Downloading telephony parameters.

#### Remark concerning stand-alone sites

The difference between a site that is part of a multi-site and a stand-alone site is that there is no telephony management for this latter. Only the administration functions are applicable (backup, restore, etc.).

## 10.2 CONFIGURING THE DIRECTORY

### Menu Administration > Configuration > Directory tab

This tab is used to define the directory range, the parameters for connecting MiVoice 5000 Manager to the LDAP directory, as well as the list of external applications authorised to use the directory.



**CAUTION:** A global directory configuration imposes an identical directory configuration (hierarchy, type, function) on all the multi-sites.

If management concerns only one multi-site, select the range **Based on multi-site**.

Refer also to Section 4.4 - Downloading telephony parameters.

## 10.3 DEFINING ALARMS

### Menu Administration > Configuration > Filter tab

This tab is used to define the alarm severity level beyond which a notification will be sent to the operator and/or an alarm set off and transmitted to an external device (alarm box).

Refer also to Sections 4.2 - Configuring alarm processing (SNMP Manager) and 4.2.3 - Alarm calls.

If the operator has activated alarm notification on the MiVoice 5000 Manager client interface (see Section 9.3 of the User Guide), a beep signal may be activated each time an alarm is received. This configuration applies to all the MiVoice 5000 Manager clients.

For that:

- Change the value below in the file /home/m7450/portail/7450Portail.exe.config:  
<add key ="bipForAlarms" value="false"/> to <add key ="bipForAlarms" value="true"/>
- Restart the m7450 service: service m7450 restart.

## 10.4 THE CONFIGURATION OF NETWORK ELEMENTS (REGIONS, MULTI-SITES, SITES)

### Menu Administration > Network topology

MiVoice 5000 Manager allows the use of several supervision domains called region. A region may contain one or more multi-sites and/or several isolated sites.

It is necessary to create and configure the elements region, multi-sites and sites.



**Note:** Regions, multi-sites and sites can be created on MiVoice 5000 Manager via the massive creation Excel file.

## 10.5 DEFINING A REFERENCE SITE

### Menu Administration > Network topology > Select a region > Select a multi-site.

Defining a reference site enables you to manage homogeneously some data such as telephony parameters.

It is defined in the configuration window of a multi-site.

## 10.6 DOWNLOADING IPBX DATA TO MIVOICE 5000 MANAGER

The generation process is used to transfer iPBx data to the MiVoice 5000 Manager and to configure the MiVoice 5000 Manager management mode on iPBx's. This management mode must be used to operate subscribers from the MiVoice 5000 Manager

This mode allows the iPBX web MMIs to be automatically locked at the end of the operation. The downloaded data will henceforth be used by MiVoice 5000 Manager.



**Note:** The MMIs are those whose parameters may also be managed by the MiVoice 5000 Manager. Once these MMIs's are locked, they can only be viewed.

### 10.6.1 PREPARING DATA FOR DOWNLOADING

This section specifies the elements to check on the iPBXs in order to optimise the data transfer to MiVoice 5000 Manager.

During the generation operation, MiVoice 5000 Manager lists the following iPBX data:

- Telephony parameters
- Number blocks
- ICGs
- Directory records
- Keys
- The physical resources
- DECT cells
- Assignments
- Subscribers
- TWP server
- Call forwarding
- UCP server

For more information on the configuration of these elements, refer to the iPBX operating manuals (see Reference documents).

#### **Telephony parameters**

See on page 19 for how to activate telephony parameter downloading.

#### **Directory records**

All subscribers to be downloaded must have at least one directory record.

### 10.6.2 STARTING THE GENERATION OPERATION

**Menu Administration > Configuration > Network topology > Select a region > Select a multi-site.**

In the multi-site configuration window, click **Generate**.

A wizard type window guides you through the generation operation. At the end of the procedure, a window allows you to lock the iPBX data.

During the generation operation, the availability of the sites configured in MiVoice 5000 Manager is tested. If a site is not accessible or working, there has been no generation, and a message in the log indicates the cause of the failure. Moreover, if the multi-site configuration contains a site not configured in MiVoice 5000 Manager, there has been no generation.

### 10.6.3 IMPORTING A SITE

The function **Import site** enables you to add data from a new site to a multi-site managed already by MiVoice 5000 Manager.

This function allows you, for instance, to gradually create a multi-site in the installation phase (without having all the sites connected and configured right from the beginning).

# 11 UPGRADE PROCEDURES

Upgrading a MiVoice 5000 Manager application requires taking different parameters into account, such as changing the operating system or installing security patches. A contextual analysis is necessary, to define the procedure to use.

This chapter describes the different methods of upgrading a standalone MiVoice 5000 Manager appli

The different upgrade types considered in V3.4 are:

- Upgrading an  $\geq$  V3.3 configuration to V3.4 (with or without security patches upgrading)
- Upgrading an  $<$  V3.3 configuration. In this case, a migration is mandatory with full reinstallation of operating system Centos 7.x. Refer to the document AMT/PTD/PBX/0168.

## 11.1 Upgrading an $\geq$ V3.3 configuration to V3.4

This procedure applies if you wish to upgrade an already operational MiVoice 5000 Manager  $\geq$  V3.3 with a new MiVoice 5000 Manager software V3.4 containing some anomaly corrections or functional upgrades.

The application is upgraded without changing the installed operating system.

### Initial status

- CentOS 7.x 64 bits (with  $x \geq 2$ )
- MiVoice 5000 Manager  $\geq$  V3.3.

### Final status

- Operating system not changed
- MiVoice 5000 Manager V3.4 (new version in this same range)

### Security patches:

Depending on the case:

- Not installed in the initial status > Installation Patches Optional/Recommended for Centos 7.x
- Installed with the initial status but not up to date (a more recent release is available) > Patch upgrade optional
- Installed with the initial status and up to date compared to the most up-to-date release available > No patch upgrade

### 11.1.1 UPGRADING TO V3.4 (MAIN STEPS)

- If necessary, back up the configuration.
- Upgrade the MiVoice 5000 Manager server software.
- Upgrade the Nagios software on the MiVoice 5000 Manager server.
- If necessary, install the new MiVoice 5000 Manager clients.
- Check the licence status.
- Upgrade the operating system security patches (if necessary).

PC Clients already installed will be updated when they are reconnected to the MiVoice 5000 Manager.

## 11.1.2 UPGRADE PREAMBLE

If necessary, back up the configuration.

## 11.1.3 UPGRADING THE MIVOICE 5000 MANAGER SERVER PC SOFTWARE.

To upgrade the server PC, you must be connected as **root**.

It is done with the CD containing the new release. When the CD is inserted in the PC drive, the installation program compares the installed releases and the releases on the CD.

If the release installed is below the release on the CD, the installation takes place automatically (this installation is traced in the installation log file).

If the release installed is above or equal to the release on the CD, the installation program displays an information message and does not perform an update.

## 11.1.4 UPGRADING THE NAGIOS SOFTWARE ON THE MIVOICE 5000 MANAGER SERVER PC

Insert the CD containing the MiVoice 5000 Manager software in the DVD/CD-ROM drive of the server PC then start the file navigator:

Go to Menu **Applications > System tools > File navigator**.

- Go to the **CUSTOM\_NAGIOS** folder.
- Double-click the **install** icon then click **Run in a terminal**.
- Wait for the execution window to close automatically.

## 11.1.5 INSTALL THE NEW MIVOICE 5000 MANAGER CLIENTS.

The portal is active without being restarted, as well as the management services and call automaton. If new clients must be installed, refer to Chapter 8 - Installation on client PCs.

## 11.1.6 CHECKING THE LICENCE STATUS

From a Windows PC, access the web portal via the url **https://Server\_IP@/M7450install/** , where "Server\_IP@" is the server IP address or name of the server on which the application is installed.

- Click the MiVoice 5000 Manager **Client start** link: the client starts automatically (login/password: M7450). The status bar at the bottom of the window must be green and indicate **MiVoice 5000 Manager connected**.
- In Menu **Administration > Unlock** functions, the V3.4 key associated with the dongle ID in the **Master key** field must be entered.

## 11.1.7 UPGRADING THE OPERATING SYSTEM SECURITY PATCHES

If new patches are provided on the Extranet, upgrade the security patches on Redhat and CentOS.

The procedure is described in the version of the document AMT/PTD/NMA/0062 concerning operating system version.

**The upgrade procedure has been completed.**

## 11.1.8 RESTART THE MIVOICE MANAGER SERVER

## 11.1.9 RESTORING THE DATA ON THE MIVOICE 5000 MANAGER SERVER PC

You can restore the application via two scripts to be run on the server:

- One script for restoring the MiVoice 5000 Manager configuration
- One script for configuring the LDAP database.

To open a terminal window in Red Hat or CentOS, from the desktop, right-click and select **Open in a terminal**.

- Log on with the login **m7450** (default password = **aastra78**).
- Select the directory **/home/scripts\_m7450**.

### For standard restore without iPBX backup:

- In the terminal window, type in the command **restore.sh** parameter management **dd.mm.yyyy**, representing the date of the backup to restore (check). E.g. **"#. /restore.sh 24.12.2007"**.

*The duration of the restore operation depends on the size of the configuration.*

### For restore with iPBX backup:

- In the terminal window, type in the command **restore.sh -total** parameter management **dd.mm.yyyy**, representing the date of the backup to restore (check). E.g. **"#. /restore.sh -total 24.12.2007"**

*The duration of the restore operation depends on the size of the configuration.*

*The restore script stops the portal automatically. During the operation, the script enumerates the files and data restored.*

### Restoring LDAP data for upgrading from V2.2 or V2.3:

- Select the directory **/home/scripts\_m7450**.
- In the terminal window, type in the command **launch\_restore\_ldap.sh** followed by the parameter **ddmmYYYY**, representing the date of the backup to restore (check). E.g. **"#. /launch\_restore\_ldap.sh 05.03.2012"**

### Restoring LDAP data for upgrading from V2.1:



**ATTENTION : Do not use the script `launch_restore_ldap.sh` and execute the commands below.**

- Log on as **root** from the backup folder (in the example above, **/home/m7450/backup/05.03.2012**) then run the following commands:

```
service openldap stop
```

```
service openldap initdb
```

```
/usr/sbin/slapadd -c -l ldap_file.ldiff -F /opt/a5000/infra/ldap/conf/slapd.d
```

Go to the directory **/opt/a5000/infra/utills/bin/ldap** and run the command:

```
#!/syncmaster.script
```

### Restoring pictures:

- Select the directory **/home/scripts\_m7450**.
- In the terminal window, enter the command **restorePictures.sh**:
  - `#!/restorePictures.sh`
  - Enter the backup directory name: **/home/m7450/backup**.

Enter the picture filename without extension: **pictures**

### 11.1.10 UPGRADING MIVOICE 5000 MANAGER CLIENT TERMINALS (AUTOMATICALLY)

**For an upgrade from V2.x to V3.4**, client terminals are automatically upgraded when the client is started.

MiVoice 5000 Manager server access from these client terminals is then operational.

### 11.1.11 ENTERING THE LICENCES ON THE SERVER

The previous licences cannot be recovered in V2.4.

- In Menu **Administration > Unlock functions**:
- Enter the V3.4 keycode associated with the master dongle ID to unlock the client functions then click **Validate**.

**MiVoice 5000 Manager is now working.**



