MiVoice 5000 Manager

10/2025

AMT/PUD/NMA/0003/20/0/EN

USER GUIDE

Warning
Although the information contained in this document is considered as pertinent, Mitel Networks Corporation (MITEL ®) cannot guarantee the accuracy thereof.
The information may be changed without notice and should never be interpreted as a commitment on the part of Mitel, its affiliates or subsidiaries.
Mitel, its affiliates and subsidiaries shall not be held liable for any errors or omissions made in this document. This document may be reviewed or re-edited at any time in order to add new information.
No part of this document may be reproduced or transmitted in any form whatsoever or by any means - electronic or mechanical - regardless of the objective, without the written consent of Mitel Networks Corporation.

CONTENTS

1 INTRODUCTION

This document describes how to use the MiVoice 5000 Manager Client application. It presents the application's different menus and functions as of Release 3.1.

For a redundant configuration on MiVoice 5000 Manager, refer to the document "MiVoice 5000 Manager Redundancy". 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 securing access to the MiVoice 5000 Manager platform's LAN in all cases.

For more information about the MiVoice 5000 Manager environment, refer to the documents available on Mitel.com.

Note: The screens presented in this manual are provided for information purposes only. Depending on the configuration installed, the tabs, fields and identifiers may differ from those presented in this manual.

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

Go to the Documentation site on Mitel.com.

1.3 TERMINOLOGY

Web Admin:	**MiVoice 5000 Web Admin.**
CS:	Cluster Server
DHCP:	Dynamic Host Configuration Protocol.
HTTP:	HyperText Transfer Protocol.
HTTPS:	HTTP Secure.
MAN:	Upgrade
Operating system:	Operating System
PBX:	Private Branch eXchange
SIP:	Session Initiation Protocol.
TMA:	Terminal Management Application.
URL:	Uniform Resource Locater.
XML:	eXtended Markup Language.

1.4 DEFINITION

Mitel 5000 Gateways:	MiVoice 5000 series phone system, equipped with specific hardware which normally serves as gateway.
Cluster:	MiVoice 500 telephony systems comprising physical systems (Mitel 5000 Gateways, Mitel 500, MiVoice 5000 Server our MiVoice 5000 compact) or virtual systems (MiVoice 5000 Server) connected to a central MiVoice 5000 Server dedicated to general control, called Cluster Server.
Cluster Server:	physical or virtual MiVoice 5000 Server systems dedicated to global Cluster control. This system can be duplicated.
Node:	Mitel 5000 Gateways, MiVoice 5000 Server, EX Controller or Mitel 5000 system belonging to a Cluster and managed by the Cluster Server.
Updating by repository:	new method of upgrading an iPBX based on the use of an upgrade server on which are stored the software components required to upgrade the software of a Cluster, MiVoice 5000 Server, EX Controller, Mitel 5000 gateways or of a MiVoice 5000 compact.

2 DESCRIPTION OF THE MIVOICE 5000 MANAGER APPLICATION

2.1 PRESENTATION OF THE APPLICATION

MiVoice 5000 Manager is an administration tool for large MiVoice 5000 and Mitel 5000 Gateway 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 site management functions as well as day-to-day management services like telephony subscriber management.

2.2 OVERVIEW

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 e-mail notifications as well as alarm transmission to an external device)
- Log and event management
- Collecting 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 (TMA) management
- Supervision (real-time maps)
- Maintenance (backing up, restoring and upgrading the MiVoice 5000/Mitel 5000 Gateway software).

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 as of system release R5.1

MiVoice 5000 Manager no longer manages iPBXs R4.2 and multi-site configurations including iPBXs R4.2.

Capacities

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

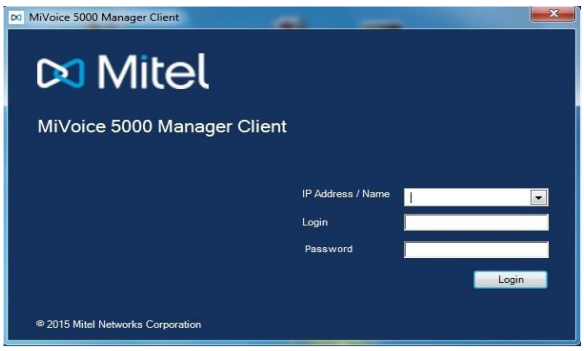
- Up to 2000 sites or multi-sites
- Up to 300,000 subscribers
- Up to 400,000 directory records
- Number of operators declared: unlimited
- Number of operators connected simultaneously: 80

2.4 STARTING MIVOICE 5000 MANAGER

Start the application from the icon 

available on the desktop, or from Menu **Start>All programs>Mitel>MiVoice 5000 Manager Client**.

- The MiVoice Manager Server login window opens:

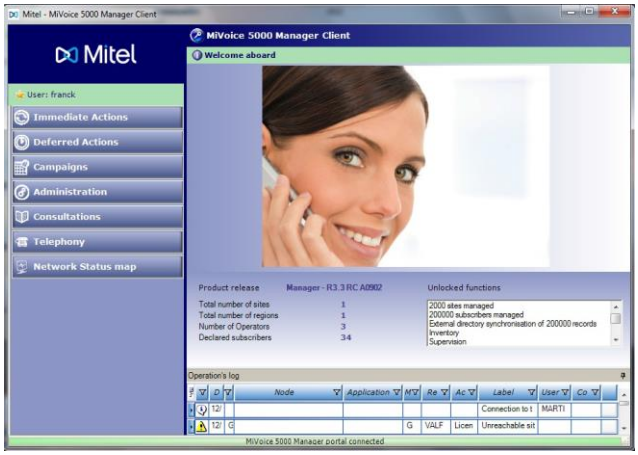


- Enter the IP address or name of the MiVoice Manager concerned.
- The login and password are then required (M7450/M7450 by default).

Note: This is the password for the operator logging on to the MiVoice 5000 Manager concerned.

Note: During the first connection or at the end of the password validity period, a window prompts for a new password. Refer to Section Security policy.

- Once the identification is successful, the application is then started, and the welcome page displayed.



The welcome page opens on the general screen. See Section About MiVoice 5000 Manager....

2.5 CLOSING MIVOICE 5000 MANAGER

To exit MiVoice 5000 Manager, click the cross ❎ on the top right side of the window.

2.6 SECURITY POLICY

When the application is not used for a preset lapse of time, an identification window opens, promoting the user to enter his/her password. The login is greyed out and not modifiable. Only the password corresponding to the login can be used to open the application.

The password format and validity period also follow some predefined rules described below.

2.6.1 PASSWORD FORMAT

By default, the password must respect this syntax:

- Rule No. 1 - minimum length: 8 characters
- Rule No. 2 - at least 1 lower-case character
- Rule No. 3 - at least 1 upper-case character
- Rule No. 4 - at least 1 numeric character
- Rule No. 5 - at least 1 special character, outside of characters with accent and apostrophes
- Rule No. 6 - respect at least 3 of rules 2 to 5.

2.6.2 PASSWORD VALIDITY

The password must be renewed in the following circumstances:

- During first logon, by replacing the password issued by the administrator
- At the end of its validity period (by default 90 days). The user is alerted to the expiration of his/her password 7 days before the end of the validity period and is prompted to change it in the application. When the password expires, the user must immediately change it to be able to log on.
- When the administrator resets the password.

3 MIVOICE 5000 MANAGER LAYOUT

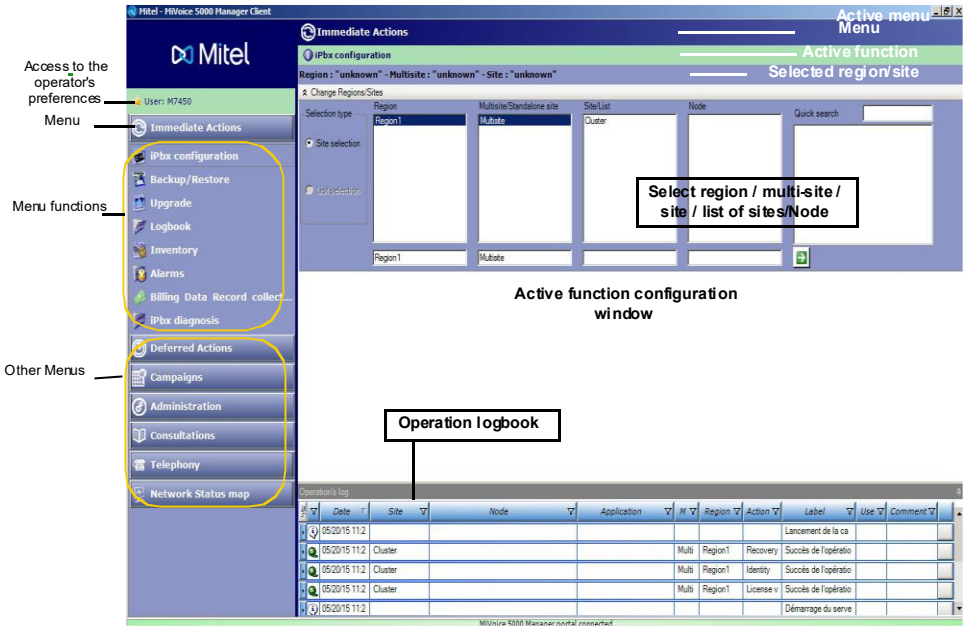
This section describes the organisation of MiVoice 5000 Manager and presents the common windows, menus, buttons and functions listed in the application.

The MiVoice 5000 Manager screen is made up of 3 areas. When a session is opened, these three areas are displayed as follows:

- The space to the left displays, over the entire page length, all the functions arranged according to action groups.
- The upper right space is reserved for configuring the selected function.
- The space at the bottom right displays the last events recorded in the operations log. By default, this display space is present but may be hidden or modified.

Depending on the user's need, the window or each of the three areas may be resized like any Windows window.

The figure below describes the contents of a window:



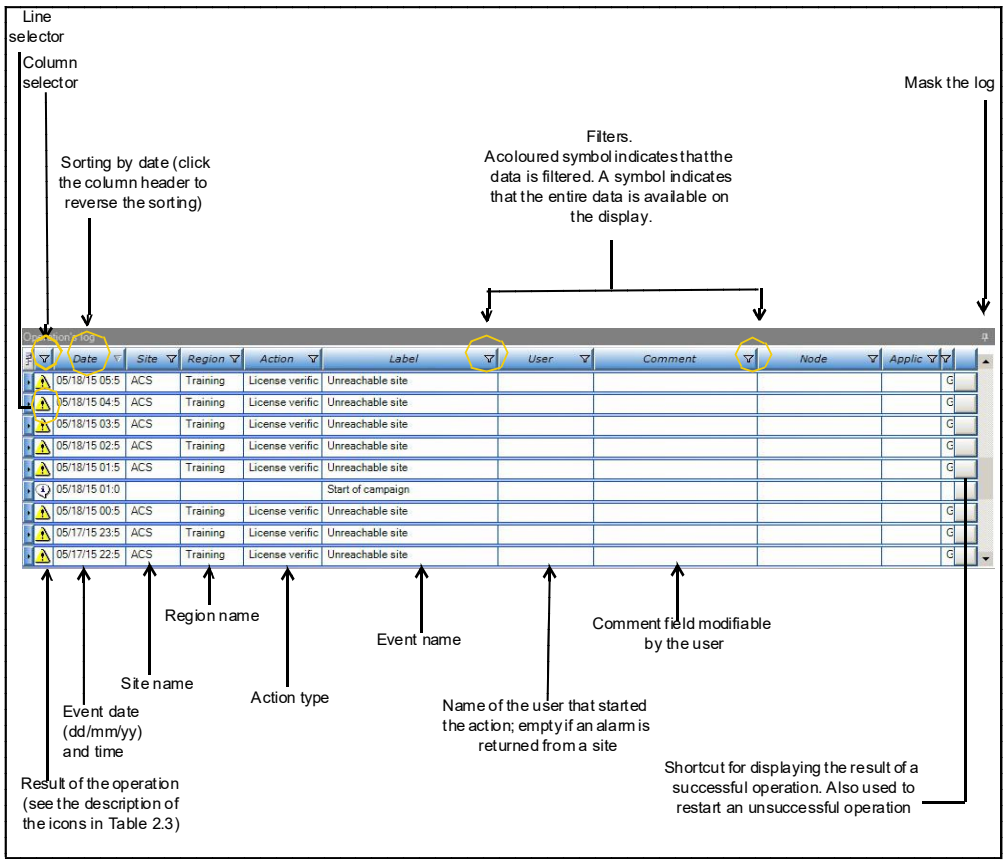
3.1 THE OPERATION LOG WINDOW

The operation log window is present by default in the lower right half of the screen.

Its organisation, the content of the fields and associated menus are described in this section.

The figure below shows an example of the log window of operations offering certain items. The following sections give information about the log configuration.

The operation log window displays a circular log of the last 75 operations. When new events are available in the log, the user is informed about it



MASKING THE OPERATION LOG WINDOW

The operation log window can be masked.

- Click the drawing pin symbol on the top right of the operation log.
- The log window disappears and is replaced by an *Operations log* tab. The window will reappear temporarily each time the cursor is placed on the tab.
- To fix the log window, click the symbol again when the log is displayed.

MASKING/DISPLAYING THE COLUMNS

It is possible to select the columns that must appear in the log window.

- Click the column selector .

The log configuration window is opens. This window allows you to select the fields that will appear in form of columns.

- Tick to select the fields to display in the window. Untick them to hide them.
- Click on the cross to close the column selection window.

Note: A column can also be removed from the display by pulling the column header outside the log display zone. To display it, use the column selector.

MOVING COLUMNS

The columns can be moved in order to reorganise the window display.

- Select the header of the column to move.

This is surrounded by an orange column.

- Press and hold down the left mouse button, then move the column horizontally to the area you want.

Two red arrows allow you to view the target destination.

- At the target destination, release the mouse button. The column is moved.

Note: This movement of columns is possible in all the application tables.

SELECT A LINE

To select a line, click the  symbol located at the beginning of the line. The selected line appears on a yellow background.

Note: Clicking on an end-of-processing notification displays the line concerning the completed event on a yellow background.

MOVING AND RESIZING THE OPERATION LOG WINDOW

You can move the operation log window to any part of the screen.

- Select the window through the *Operation log* title bar.
- Press and hold down the left mouse button then move the window.

In the moving process, a grey line shows the location of the window when the mouse is released.

- Resize the window as you wish, like any Windows window.

The previous size and location are stored in the memory. To return to the previous size and location, double-click the title bar. This action can be repeated and be used, for example, to increase and reduce the size of the window.

FILTERING LOG INFORMATION

Some operation log columns propose a filter menu (see figure).

- Click on the Filter icon ▽ of the column to filter.

A drop-down menu is displayed, proposing the values chosen for the filtering operation. These values depend on the values displayed in the operation log during the filter request and may change according to the values displayed.

- Select one filter option from those proposed.

Filtering is immediate, and the Filter icon turns blue to indicate that filtering exists on this field.

RESULT OF AN OPERATION

The result of an operation is indicated by a symbol. The table below gives the meaning of the symbols:

OPERATION RESULT	MEANING OF THE ASSOCIATED SYMBOL
	Operation successful.
	Operation not successful. The action can be restarted from the operation log.
	Information concerning a change in configuration: operator, site list of sites.
	Note: event needs to be checked (PBX call or internal alarm).

ENTERING A COMMENT

You can use the comment field to make comments about operation log events. Information entered in this field is recorded in the operation log, accessible from the **Consultation** action group and can be used for customised sorting.

SHORTCUTS

You can use these shortcuts to:

-  Open a file associated with an event, such as an inventory, a log or alarms.
-  Re-submit an unsuccessful event. The action will be identical: to modify the parameters, it is necessary to redefine the action.

ACTION REPORTS

When an action is completed, a notification appears on a pop-up screen. The action is recorded in the operation log.

You can display this action in the log window in two ways:

- Click **New notification** in the notification window as long as it is visible. This action updates the log window and the action appears on a yellow background.
- If the pop-up screen is no longer displayed, bring up the scrollbar cursor to the right of the screen to display this action (it does not appear on the yellow background).
- This notification window may be deactivated or activated in the Preferences menu (direct access by clicking the operator's name, preceded by a star).

3.3 SELECTING A REGION / MULTI-SITE / SITE OR LIST OF SITES

Before starting an action, it is necessary to define an action area.

A window used to define this area is available in most of the menus. This window can be displayed or minimised using the ⩔ / ⩓ symbol of the **Change region/sites** title bar. It is used to select a region, multi-site or standalone site, a site in a multi-site configuration or a list of sites to which the action will apply.

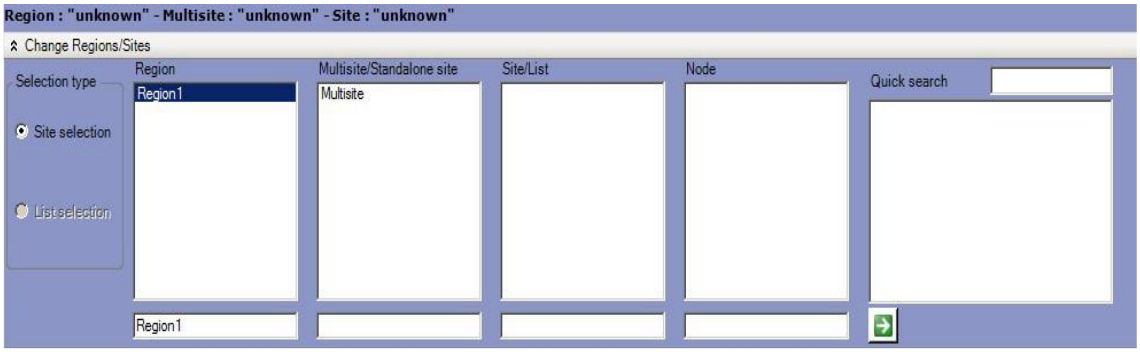
In an architecture in cluster mode, the cluster appears in the Site column and each of the nodes can be selected in the Node column.

Since the selection procedure is the same for all the application screens, it is explained in this section, and forwarding shall be performed in the menus in which it will be required.

The contents of a site list are explained in Section Site list management.

To select an action area:

- If necessary, click the double arrow ⩔ on the *Change region/Sites* title bar to display the selection window below.



- Choose “**Site selection** or “**List selection.**

- The managed regions, multi-sites/ standalone sites, sites or lists of sites appear in their respective areas.
- Click a region, multi-site or standalone site, site or list to select them.
- The selected items are displayed in the areas at the bottom of the list.

Note: If the number of regions, sites or list of sites is too long, enter the first letter(s) of the name in the quick search area. The cursor will automatically be placed on the first name containing the character string entered in the search zone.

- Click on the green arrow  .

The selected action area is displayed above the Change region/sites title bar and the selection made remains valid until the next modification.

PART:

SITE MANAGEMENT

4 IMMEDIATE ACTIONS

This chapter explains how to use the functions offered by the **Immediate actions** menu.

Click the **Immediate actions** menu to display the following actions:

- **iPBX configuration**: for accessing the iPBX via Web Admin.
- **Back up/Restore**: for backing up or restoring data on a site, a multi-site-configuration or a list of sites. Restore is possible on the sites as of R5.1 B.
- **Upgrade**: for upgrading the software release of one or more sites (sites with R5.1 B or later)
- **Logbooks**: for downloading the logbook either to the list of sites, or multi-site
- **Inventory**: gives detailed information about the site for which an inventory has been requested.
- **Alarms**: for downloading alarms occurring on the selected site.
- **Charge data Record collection**: for downloading call records from the site or from a group of selected sites (the information is stored on the server).
- **iPBX diagnosis**: for retrieving the different debug files from a site, a list of sites, a cluster or cluster node.

4.1 IPBX CONFIGURATION

This window gives the user access to a site so as to manage it directly.

4.1.1 USING THE CONFIGURATION FUNCTION

- In the list of **Immediate actions**, click **Configuration**.
- If necessary, select Region/Multi-site / Site or Cluster node.

Note : Only one site or cluster (or cluster node) must be selected for this operation.

- Click the **Connect** button on the top right side of the screen.

The iPBX management screen is displayed.

- Enter the password to access the iPBX management menus.

Note : For information about iPBX management, see the corresponding iPBX operating manuals (see reference documents).

IMPORTANT : Check that you log out at the end of the configuration.

Note : By default, the maximum time for a request is 90 seconds. To change it, edit the PbxProxyTimeout key in the MiVoice 5000 Manager configuration file.

4.2 BACKUP/RESTORE

Refer also to the iPBX operating documents detailed at the start of this document.

4.2.1 BACKUP

4.2.1.1 Contents of a backup

The following types of data can be backed up using this menu:

- Data Backup
  - iPBX configuration data (non-modifiable parameters: minimum content of a backup).
  - Directory Records
  - Spoken announcements
  - IVR announcements
  - IVB signatures
- Application code backup (iPBX application software release)

The backup file can be exported.

At the end of the backup operation, the backup file is located on the iPBX.

4.2.1.2 Using the backup function

- In the list of Immediate actions, click **Backup/Restore**.
- If necessary, select Region/Multi-site / Site or list of sites,

A table indicates the last backup(s) for the selected site or the sites on the list.

- Click Launch action.
- In the Backup options window, tick the data to be backed up then click OK (the Application and PBX data box is ticked by default).

The action is taken into account by Web Admin. For a list of sites, there are as many actions created as there are sites on the list.

- The list of backups is updated once the notification appears.

Data is backed up on the server.

Note : Backup can be run on a list of sites, but data is stored on a site by site basis.

4.2.1.3 Saving the backup locally

The application offers the possibility to save the backed up data locally to the PC hard disk.

- Select from the list of backups the one to be saved to the PC hard disk. It moves to the yellow background.
- Click **Recover**.
- Enter the username and password.
- Define the backup folder and click **Save** to save the backup file there.

4.2.2 RESTORE (IMMEDIATE OR DEFERRED)

4.2.2.1 Restore contents

The following types of data can be restored using this menu:

- iPBX configuration data
  - iPBX configuration data (non-modifiable parameters: minimum content of a backup).
  - Directory Records
  - Spoken announcements
  - IVR announcements
  - IVB signatures
- Application code restore (iPBX application software version)

Note : This menu is used to set either immediate or deferred mode.

4.2.2.2 Using the restore function

- In the list of **Immediate actions**, click **Backup/Restore**.
- If necessary, select Region/Multi-site / Site or list of sites,

A table indicates the last backup(s) for the selected site or the sites on the list.

- Select the backup file that you wish to restore for the site in question
- Click on **Restore**
- On the following screen, indicate the type of data you wish to restore and, if required, tick the **Deferred** box to carry out the restore operation at a later point. If this is the case, indicate the date to be applied.

The action is taken into account by Web Admin. For a list of sites, there are as many actions created as there are sites on the list.

- The list of backups is updated once the notification appears.

For a site managed in multi-site mode

To synchronise the MiVoice 5000 Manager data with the “new” iPBX data, import data from the site:

From the “**Network administration/topology**" menu select the multi-site.

- Click "**Configuration**".
- Then click "**Import**" in the "**To import a new site into the multisite**" area of the site in question.

4.3 UPGRADE

The different types of upgrades concerned in R8.x are:

- Upgrading a configuration ≥ R8.x to ≥ R8.x+1 and only for MiVoice 5000 Server systems. In this case, only Upgrade by Repository is applicable. See the document Upgrading by repository).
- Upgrading from sites < R8.0 to R ≥ 8.x. For MiVoice 5000 Server systems only (including EX Controller). In this case, an upgrade is mandatory with a change of operating system to Rocky Linux. See the Implementation Manual (MiVoice 5000 Server/Manager and EX Controller - Upgrading to R8.x).
- It is no longer possible to upgrade to R8.0 for Mitel 5000 Gateway sites. However, an R6.x or R7.x site can still be upgraded to more recent releases but < R8.0.

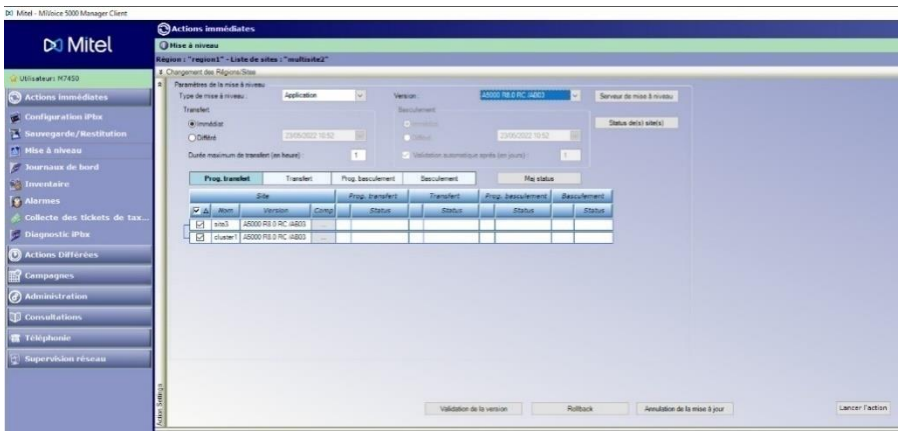
Depending on the type of upgrade version and compatibility, only compatible systems will be shown.

Examples:

Upgrade to R8.x:

In this case:

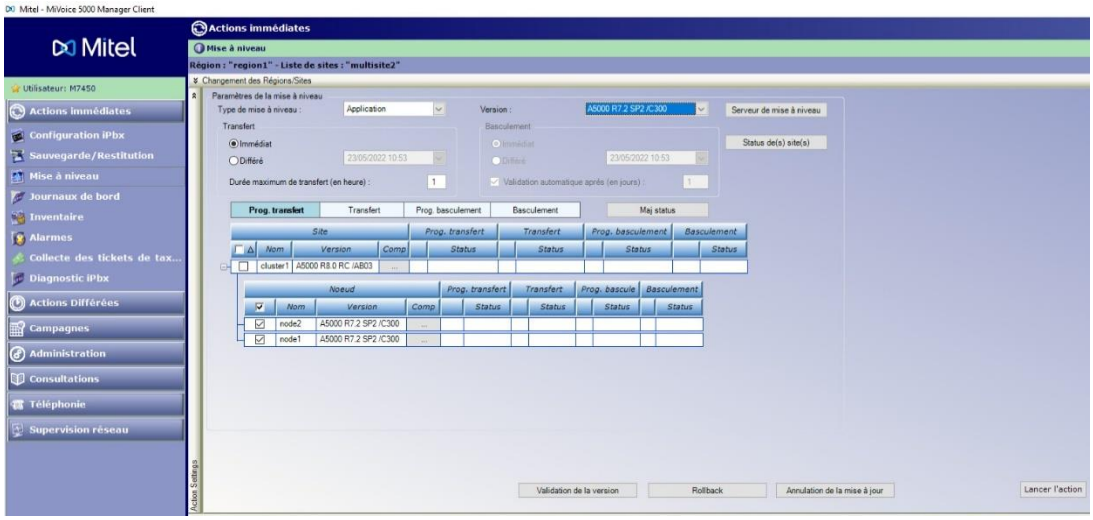
- The cluster is working with R8.x.
- Only compatible nodes (MiVoice 5000 Server ≥ R8.0) are shown and can be upgraded to the selected version ≥ R8.0 from the Upgrade server.



Upgrade in a range < R8.0:

In this case:

- The cluster is working with R8.x.
- Only nodes (< R8.0) are shown and can be upgraded to the release < R8.0 selected from the Upgrade server.



This menu is used to upgrade the software of one or more sites:

- For Mitel 5000 Gateways, the application and system releases are proposed.
- For MiVoice 5000 Servers, only the application release is proposed.

This update can be programmed by site on a date and at a time defined or programmed simultaneously for the sites in question.

- The **Change the list** button is used to change the filter applied to the drop-down lists for the software releases.
- In the list of **Immediate actions**, click **Upgrade**.
- If necessary, select Region/Multi-site / Site or list of sites,
- From the drop-down lists of the different fields, select the releases to be upgraded according to iPBX type.
- In the lower part, tick the sites to be upgraded with the releases in question.
- Enter the licence if necessary. The licence is required while changing a software release (example from V3.x to V3.x+1). In this case, a warning sign is displayed in the **keycode** field.
- For the new release to be automatically validated on the sites, tick **Automatic validation after (nb of days)** then indicate the number of days before switchover, between 1 and 8 days.
- Define the update date for each site or tick the **Simultaneous updates** box if this operation is to be carried out simultaneously for all sites.
- Click **Launch action**. The updates will take place on the dates in question.

Recommendation:

Check that no update or restore is already programmed for the iPBXs. You can view this in the inventory.

Version validation button:

This button is used to validate a test version. For a cluster, validation is carried out on the cluster server and nodes. If there is no test version, this is indicated in the result of the action, in the operations log. This action can only be carried out if a site is selected.

Rollback button:

This button is used to restore the last software release validated if a release is in test mode. For a cluster, rollback is carried out on the cluster server and nodes. If no release is in test mode, this is indicated by the report of the action in the operations log. This function is not available for systems R6.2 and R6.2SP1. This action can only be carried out if a site is selected.

Cancel Update button:

This button is used to cancel a programmed deferred update. The update is cancelled, no matter the type of update (old method or by repository). If no update has been programmed on the system, this is indicated by the report of the action in the operations log. This action can only be carried out if a site is selected.

4.3.1 AUTOMATIC UPGRADE VALIDATION

An automatic validation request generates a deferred action saved in the campaigns. The date of this campaign is then calculated according to this rule: date of next campaign after upgrade + number of days entered.

Until the campaign date, the action may be:

- Viewed: in Menu **Campaigns/Actions by date** or **Actions by site or list**
- Modify: it is possible to modify the date of campaign.
- Cancelled: **note:** in this case, the upgrade must be manually validated on each site.

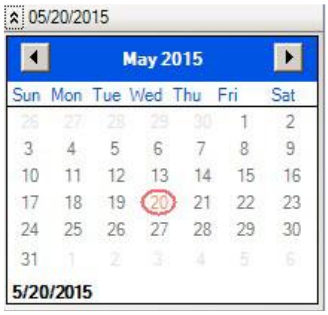
4.4 LOGBOOKS

4.4.1 USING THE LOGBOOK FUNCTION

- In the list of Immediate actions, click Logbooks.
- If necessary, select Region/Multi-site / Site or list of sites (see).
- The logbook content is displayed.

4.4.2 VIEWING DOWNLOADED LOGBOOKS

- Select the Region/Site pair: the logbooks can only be viewed on a site-by-site basis.
- Click on the double arrow in the date bar to view the calendar.



  - The day's date is surrounded by a red circle.
  - The dates in orange colour indicate the dates on which the logbook was downloaded for the site in question.
- Select the date of the log to display.

The logbook for the site is displayed. Depending on the iPBX release, its format may differ. Logbook management tools

4.4.2.1 Finding a character string

This function is used to search for a character string in the logbook. This search applies to the Explanation field (in display-by-table mode).

- Enter the character string in the Search input field.
- Click the  icon.

When the string is found, it is displayed on a blue background.

4.4.2.2 Printing the logbook

The **Print** button is used to print the downloaded logbook on the PC printer.

4.4.2.3 Exporting a logbook

The **Export** button is used to copy the logbook to the PC in form of an Excel file.

4.5 INVENTORY

The inventory function enables operators to check the characteristics of network iPBXs as well as the software solutions installed on them. The information displayed come from the last inventory made.

4.5.1 IMPLEMENTING THE INVENTORY FUNCTION

- In the list of **Immediate actions** , click **Inventory**.
- If necessary, select Region/Multi-site / Site or list of sites (see).
- Click **Start inventory** (button on the bottom right side).
- The action is taken into account by the portal. For a list of sites, there are as many actions created as there are sites on the list.
- Once the task is finished, the operation log sends a notification.
- Check that the operation has been correctly completed. Once the inventory is completed correctly, the site-related information is displayed in the inventory window.

Note : The inventory can be opened for one site, a pre-defined list of sites or a multi-site configuration. If the selection concerns a list of sites or a multi-site configuration, the inventory will provide a combined list of the data relating to all the sites selected.

The information given by the inventory is distributed to the 4 tabs described in the next sections.

4.5.2 SOFTWARE TAB (SINGLE-SITE CONFIGURATION)

The information is distributed across the following display areas (see figures below):

SWITCHOVER AREA:

This area displays the date of the next switchover (date, hour, type and test length.

Mother board area:

This area displays the available software releases (active and inactive) on the iPBXs:

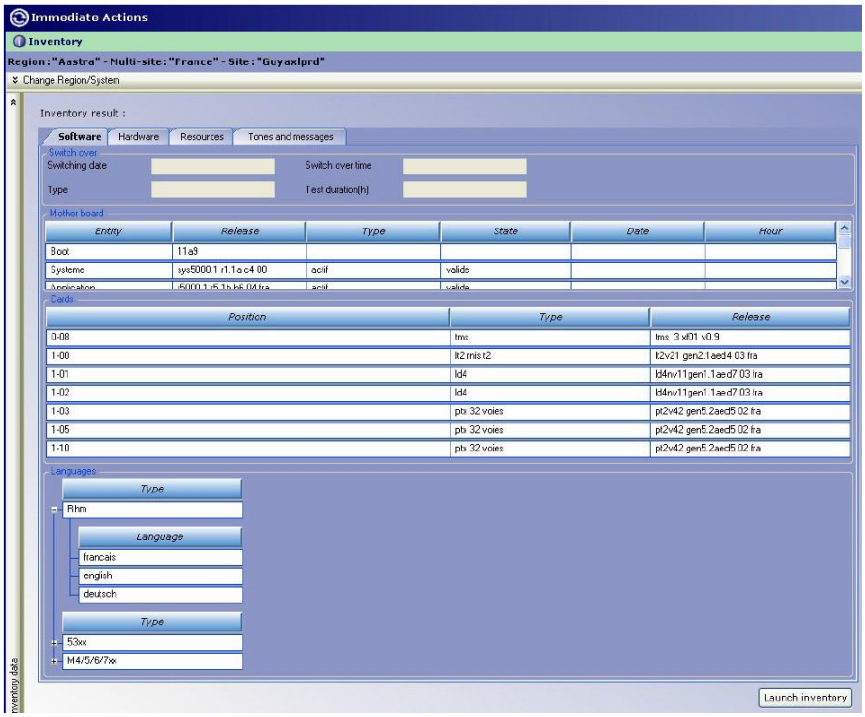
- For the Mitel 5000 Gateways, boot version, system version (active/inactive) and application version (active/inactive)
- For the MiVoice 5000 Server, application version

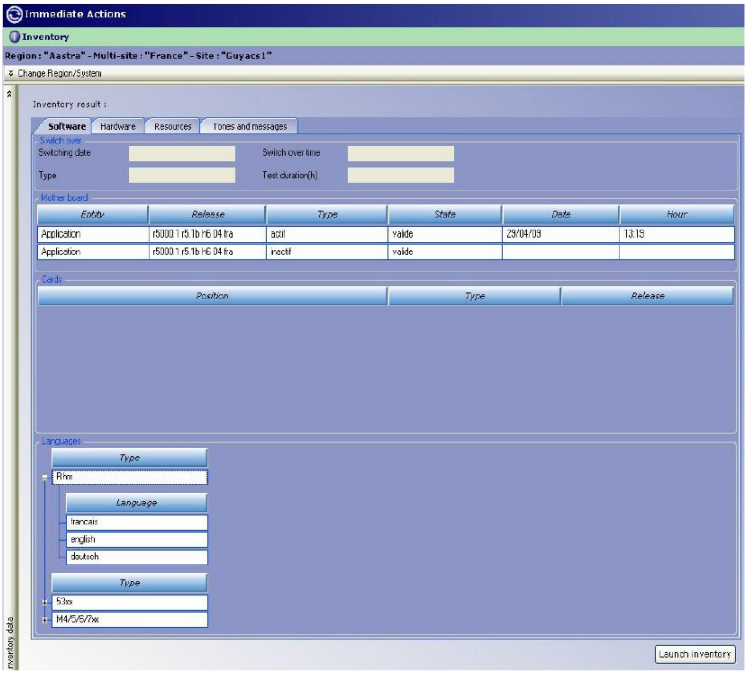
Card area (not applicable to MiVoice 5000 Server)

This area displays the card software and their positions.

LANGUAGE AREA

This area displays the available versions for Web Admin and terminal displays.


Immediate Actions
Inventory
Region : "Aastra" - Multi-site : "France" - Site : "Guyaxlprd"
Change Region/System
Inventory result :
Software
Hardware
Resources
Tones and messages
Switch over
Switching date
Switch over time
Type
Test duration(h)
Mother board
Entity
Release
Type
State
Date
Hour
Boot
11a9
Systeme
sys5000 1 r1.1 a c4 00
actif
valide
Cards
Position
Type
Release
0-08
tmc
tmc 3 xl01 v0.9
1-00
lt2 mls t2
lt2v21 gen2.1aed4 03 fra
1-01
ld4
ld4nv11gen1.1aed7 03 fra
1-02
ld4
ld4nv11gen1.1aed7 03 fra
1-03
pb 32 voies
pt2v42 gen5.2aed5 02 fra
1-05
pb 32 voies
pt2v42 gen5.2aed5 02 fra
1-10
pb 32 voies
pt2v42 gen5.2aed5 02 fra
Languages
Type
Rhm
Language
francais
english
deutsch
Type
53xx
M4/5/6/7xx
Launch inventory
inventory data


Immediate Actions
Inventory
Region : "Aastra" - Multi-site : "France" - Site : "Guyacs1"
Change Region/System
Inventory result :
Software
Hardware
Resources
Tones and messages
Switch over
Switching date
Switch over time
Type
Test duration(h)
Mother board
Entity
Release
Type
State
Date
Hour
Application
r5000 1 r5.1b h6.04 fra
actif
valide
29/04/09
13:15
Application
r5000 1 r5.1b h6.04 fra
inactif
valide
Cards
Position
Type
Release
Languages
Type
Rhm
Language
francais
english
deutsch
Type
53xx
M4/5/6/7xx
Launch inventory
inventory data

4.5.3 HARDWARE TAB (SINGLE-SITE CONFIGURATION AND NOT APPLICABLE TO MIVOICE 5000 SERVER)

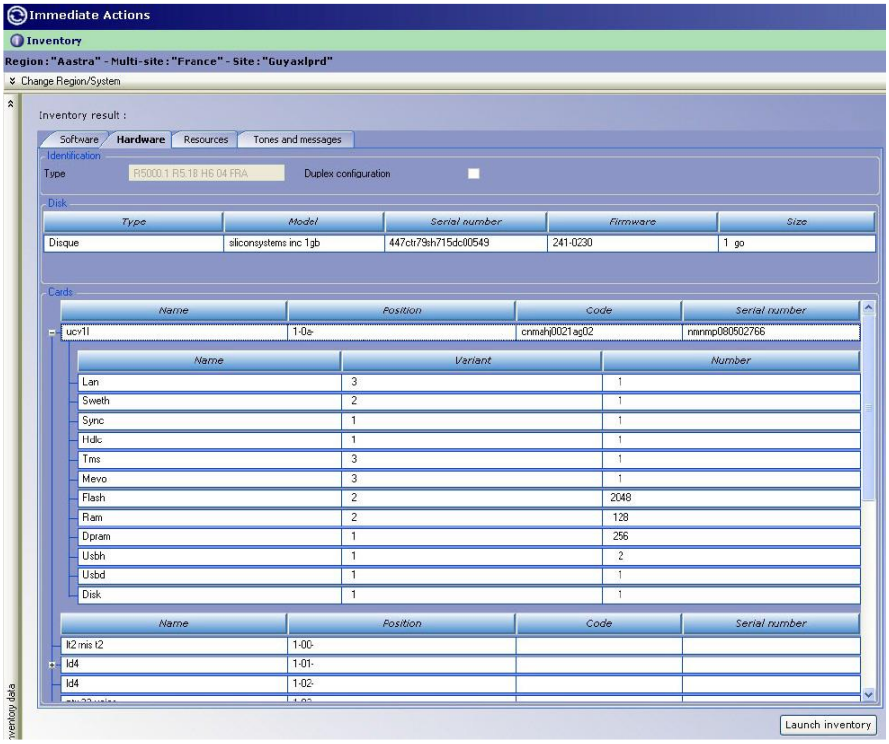
The information is distributed across the following display areas (see figures below):

DISK AREA:

This area displays the characteristics of the Compact Flash card on the CPU card containing the iPBX's software.

CARD AREA:

This area displays the characteristics of the cards in Mitel 5000 Gateways (CPU cards, equipment cards, daughter cards).



4.5.4 RESOURCES TAB (SINGLE-SITE CONFIGURATION)

The information is distributed across the following display areas (see figures below):

SUSBSCRIPTIONS AREA:

This area displays the types of subscription declared on the iPBX.

LOCKED RESOURCES AREA:

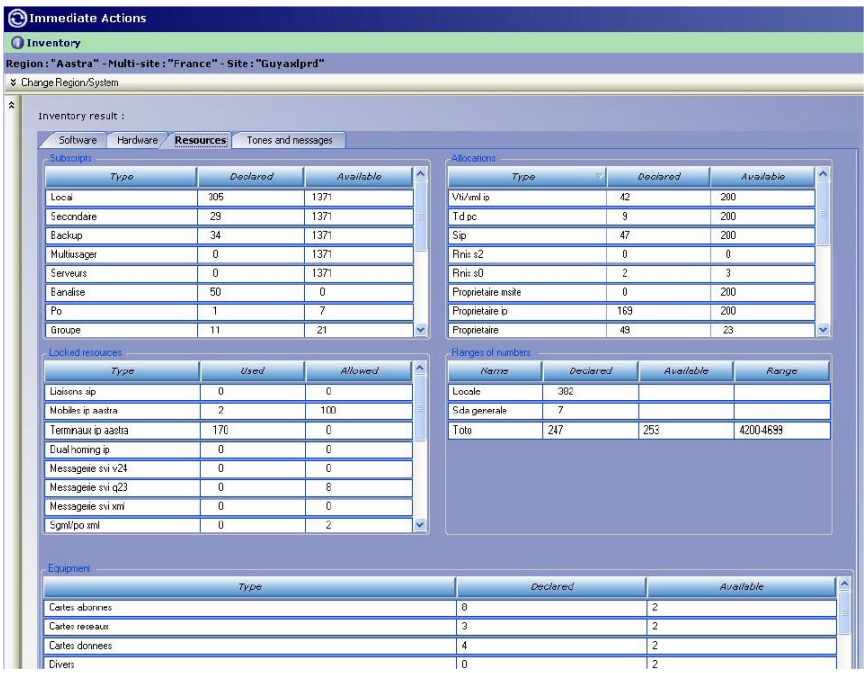
This area displays the available resources in terms of software licences assigned to a site.

ALLOCATIONS AREA:

This area displays the quantity of subscriber numbers declared by number type and segment, if defined.

EQUIPMENT AREA (not applicable to MiVoice 5000 Server):

This area displays the number of cards declared on the site. The cards are grouped together by type.



4.5.5 TONES AND MESSAGES TAB (SINGLE-SITE CONFIGURATION)

The information is distributed to the following display areas:

TONES AREA:

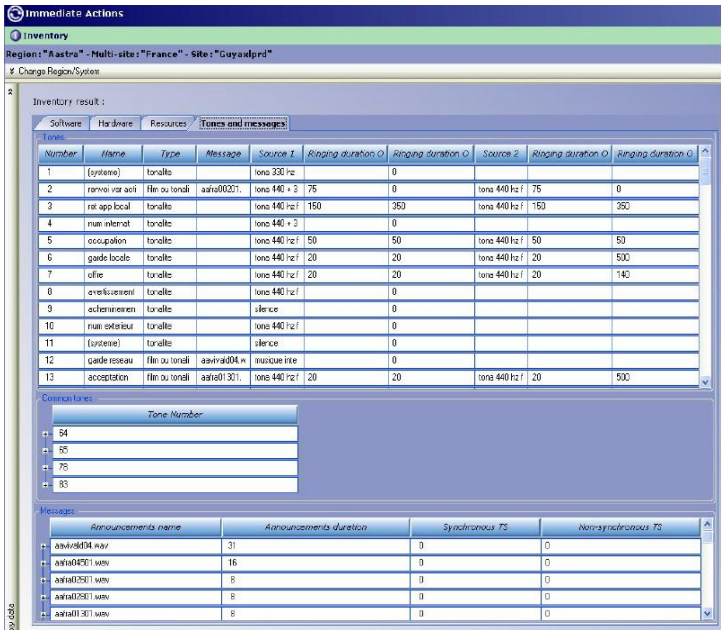
This area displays the types of subscription declared on the iPBX.

EQUIPMENT AREA (not applicable to MiVoice 5000 Server):

This area displays the available resources in terms of software licences assigned to a site.

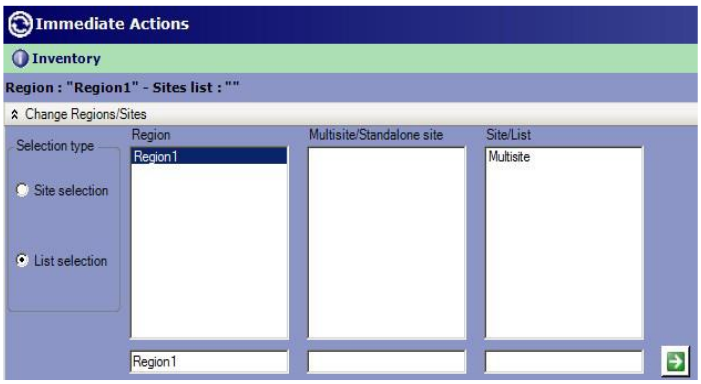
EQUIPMENT AREA (not applicable to MiVoice 5000 Server):

This area displays the number of terminals declared on the site, by type, for each numbering segment.



4.6 INVENTORY OF A GROUP OF SITES

When the user ticks **List selection**, the inventory displays combined data for all the sites in a multi-site configuration or a group of sites chosen from a list.



4.6.1 MULTI-SITE RESOURCES TAB

SUSBSCRIPTIONS AREA:

This area displays the types of subscription declared on the sites in question.

LOCKED RESOURCES AREA:

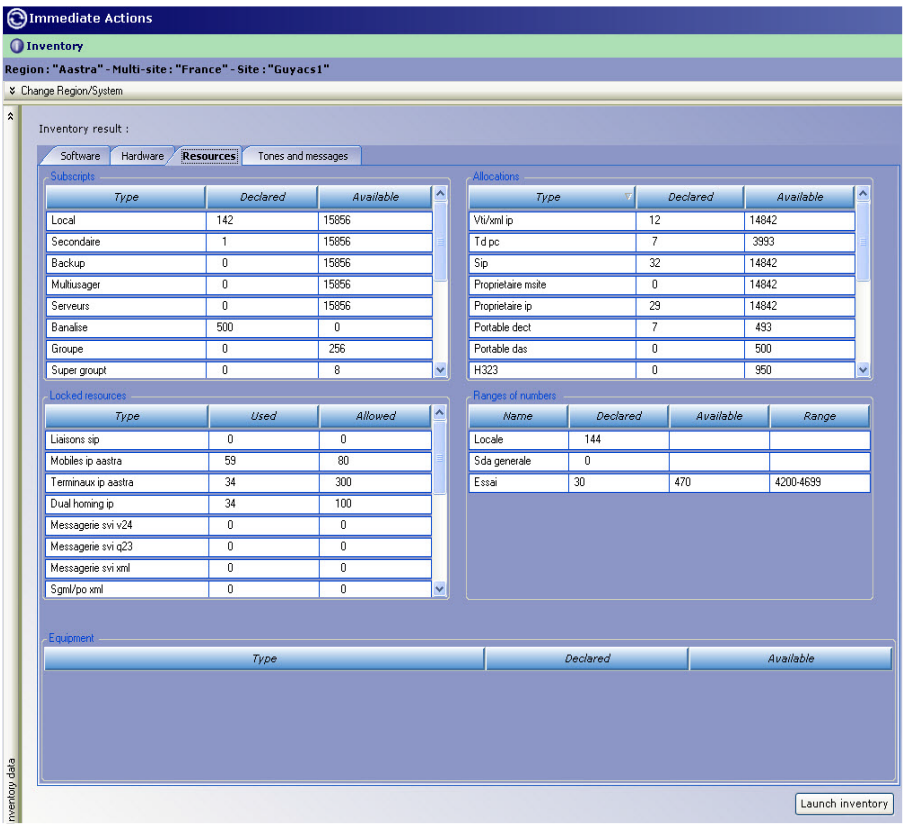
This area displays the available resources in terms of software licences assigned to the sites in question.

ALLOCATIONS AREA:

This area displays the combined quantity of subscriber numbers declared by number type and segment, if defined.

EQUIPMENT AREA (not applicable to MiVoice 5000 Server):

This area displays the total number of cards declared on the sites in question. The cards are grouped together by type.



4.6.2 TABS AND VERSIONS

This area displays the available software releases (active and inactive) for all the sites in question.

4.7 ALARMS

This function is used to display the alarms gradually generated by each iPBX on the network.

Depending on the alarm severity level (see Section Range tab and Filtering tab) an e-mail notification and/or alarm transmission to an external device may be generated.

4.7.1 DISPLAYING ALARMS

- In the list of **Immediate actions** , click **Alarms**.
- If necessary, select Region/Multi-site / Site or list of sites (see).
- The alarms of the day are displayed. You can select a later date by opening the calendar above the alarm display.

The information provided is described in the following table:

Description of the information in the alarms window.

COLUMN	INFORMATION
Symbol	Symbols representing the information type:  The global status of a site or cluster node  The global status of a cluster  The status of services.
Date	Alarm date
Severity level	Alarm severity level: Critical/Major/Minor/OK
Site / Node	Site / node name
Alarm	Name of the alarm returned from the iPBX
Explanation	Description of the alarm
Status	Status of the application or faulty item
Application	Application or faulty item

The background colour represents the alarm severity level.

4.7.1.1 *Update*

This button is used to refresh the display.

4.7.1.2 *Map*

The map button gives access to the Nagvis network supervision application:

- Click Map.
- Enter the operator password.

This application is described in detail in the Section The map application NAGVIS.

4.7.1.3 *Print*

The **Print** button is used to print out the displayed alarm list on the PC printer.

4.7.1.4 *Export*

An export function is used to back up the alarms displayed in .xls format.

4.8 CHARGE DATA RECORD COLLECTION

This function is used to download to the server all the charge tickets generated by each iPBX on the network.

4.8.1 USING THE CHARGE DATA RECORD COLLECTION FUNCTION

- In the list of Immediate actions , click Charge Data Record collection.
- If necessary, select Region/Multi-site / Site or list of,
- *A message informs you about the date of the last upload or indicates that there is no information about the last upload made*.
- Click Launch action.
- The action is taken into account by the portal. For a list of sites, there are as many actions created as there are sites on the list.
- Check that the operation has been correctly completed.

If the administrator has configured an export for the charging unit, by default, any charge ticket collection will be made with export (see the Section Export tab).

Note : Ticket collection can be run on a list of sites, but data is stored on a site-by-site basis.

4.9 IPBX DIAGNOSIS

This action is used to retrieve from the selected iPBXs, the information which will be used to perform a diagnosis.

- In the list of Immediate actions , click iPBX diagnosis.
- Select the region / multi-site / site / list of sites / cluster server, cluster node.
- A message informs you about the date of the last download or indicates whether there is no download information.
- Select the type of diagnosis to download: Trace / TroubleShooting / Dump IP.
- Click Launch action to start a new diagnosis download.
- the result of the operation is displayed in the operation log. The date of last download is updated in the Information field. To retrieve the diagnosis performed, export the downloaded diagnosis.

Note : The Troubleshooting file will only be retrieved for the iPBXs as of R6.1.

4.9.1 EXPORTING DIAGNOSIS FILES

Exporting the diagnosis files lets you transfer to a PC the diagnosis items downloaded during an immediate, deferred action, or during iPBX supervision.

For the selected site, list of sites, cluster server or cluster node:

- In the list of **Immediate actions** , click **iPBX diagnosis**.
- Select Region/Multi-site / Site or Cluster node.
- Click **Export**:
- In the export window, select the date and time from which the file export is required.
- Tick the type(s) of files to be exported.
- Click **Export**:

A .tar.gz file is created and copied to the export directory.

- To view it, enter the login/password.
- The portal export page opens.
- The **tar.gz** file can be opened or saved on the PC.

5 DEFERRED ACTIONS

Deferred actions are used to program periodic and occasional actions. This chapter explains how to create these actions from the **Deferred actions** action group for the following functions:

- **Backup**: backs up the data on a site. Refer to the Section Backup/Restore for the data that can be backed up.
- **Inventory:** downloads device and software information from the network.
- **Charge Data Record collection**: downloads call records from the site or all the selected sites.
- **iPBX diagnosis**: for retrieving the different debug files from a site, a list of sites, a cluster or cluster node.

The schedule and result of deferred actions can be viewed and modified in the action group **Campaigns** (see the Section Managing campaigns).

5.1 USING THE DEFERRED ACTION FUNCTION:

The procedure is the same for all the functions cited above.

- In the list of Deferred actions , click on the action to start.
- If necessary, select Region/Multi-site / Site or cluster.
- In the **Change frequency** window, select any of the following options:
  - **Deferred** for an isolated processing operation.
  - **Periodic** for a periodic processing operation. A display zone called **Frequency** appears.

Deferred processing

- If the Deferred option is selected, enter or select a date in the calendar by clicking the button.
- Click the arrow  .
- In the next window that opens, enter the deferred action name.

Note : It is advisable to use a syntax making it easy to identify the subject of the action (region/site or list, etc.).

- Select the type of deferred action to program.
- Select or unselect the option “Export data at the end of the action”.

This option enables you to overstep the choice made by the administrator in his or her configuration menu (see the Section Export tab).

Note : If the Export option is not required, the data is backed up on the server, in the repository. If Export is required, this data is backed up in the location specified by the administrator in his or her configuration.

- Click **Save** .

A message confirms the submission of the action.

Note : At the end of the campaign, a message is sent by e-mail to the operators whose addresses have been indicated in the operator management module.

Periodic processing

- Define the frequency out of the following options:

- Daily
- Weekly and select the day of the week.
- Monthly then select:
  - The date on the drop-down list
  - The day you want in the month (for example 1st Monday of the month).

- Click the arrow  .
- In the next window that opens, enter the deferred action name.

Note : It is advisable to use a syntax making it easy to identify the subject of the action (region/site or list, etc.).

- Select or unselect, if necessary, the option “Export data at the end of the action”.

This option enables you to override the choice made by the administrator in his or her configuration menu (see the Section Export tab).

Note : If the Export option is not required, the data is backed up on the server, in the repository. If Export is required, this data is backed up in the location specified by the administrator in his or her configuration.

- Select the type of deferred action to program.
- Click **Save** .

A message confirms the submission of the action.

Note : At the end of the campaign, a message is sent by e-mail to the operators whose addresses have been indicated in the operator management module.

6 MANAGING CAMPAIGNS

All the deferred occasional or periodic actions are executed within the framework of daily processing known as a **campaign**. The **Campaigns** menu is used to monitor and modify the processing operations thus planned.
You can monitor and manage campaigns using the following functions:

- **Actions by date**: for monitoring and managing the programmed actions by their processing date for a region.
- **Actions by site or list**: for monitoring and managing the programmed actions for a site or list of sites.
- **Campaign results**: displays the results of deferred actions. Unsuccessful actions can be restarted as immediate or deferred actions.
- **Site maintenance**: used to change a site to maintenance mode, that is to remove it from scheduled actions.

6.1 ACTIONS BY DATE

Actions by date are displayed at the regional level.

- Click the **Selected region** title bar and select the region to take into account.
- Select the date in the calendar.

You cannot select a date prior to the date of the next campaign.

The actions defined for the selected day are presented in form of a table.

Table describing campaigns

COLUMN	INFORMATION
Name	Action name given by the user
Type	Processing type. Possible values: • Backup • inventory • charge Data Record collection • iPBX diagnosis
Site (*)	Site name
List (*)	Site list name
User	Name of the user who programmed the action
Frequency	Defined frequency or date if it is an isolated action. Possible values: • Daily • Weekly • Monthly

(*) These columns are indicated according to the type of action (by date/by site or list).

Note : In the by-date table, the site column and list column appear but only one of them is filled in. If the list of sites is filled in, it is possible to view the lists concerned by displaying the action details.

6.1.1 DELETING AN ACTION

By clicking  the user can delete an action:

- For the date selected in the calendar

  Or

- For all the occurrences relating to the frequency defined while creating the deferred action.

Note : Deleting all the occurrences is the same as deleting this campaign.

6.1.2 MODIFYING AN ACTION

By clicking on  , the user can modify an action. The type of modification depends on the frequency of the action.

- If the action is periodic:
- the modification may concern the date selected in the calendar, or all the occurrences.
- data export at the end of the action may be ticked or unticked (option defined by the administrator in the configuration menu). Refer to Section Configuration.
- If the action is occasional:
  - the frequency may be changed to:
    - daily
    - Weekly
    - monthly.
  - data export at the end of the action may be ticked or unticked (option defined by the administrator in the configuration menu). Refer to Section Configuration.

6.1.3 VIEWING ACTION DETAILS

The user can display the action details by clicking  . This display does not allow any modification.

6.1.4 CAMPAIGN PROPERTIES

(Administrator profile)

In addition to the scheduled actions, the administrator also has the possibility to modify the properties of a campaign:

- Changing the campaign start time
- Inhibiting the campaign, that is stopping any campaign related activity.

6.1.4.1 *Changing the campaign start time.*

This implies occasionally changing the time at which a campaign starts. The campaign start time is defined by the administrator in the configuration menu. Refer to Section Configuration.

In the **Campaign properties area**:

- Open the list of options and select any of the times proposed.
- Click **Validate**.

The time selected will be the time the campaign will start for the chosen date and for all the regions.

6.1.4.2 *Inhibit campaign*

If ticked, this option suspends the campaign for all the regions.

6.2 ACTIONS BY SITE OR LIST

This option is used to monitor and manage the programmed actions for a given site or list of sites.

6.2.1 ACTIONS FOR A SITE

In the **Campaign** list, click Actions by System or List.

- Select a region, a multi-site / site.

Only one site should be selected for this operation.

- The action(s) defined for the selected site is/are presented in form of a table (see Table describing campaigns).

Note : The List column is filled in if the site is part of a list of sites. The other sties are displayed in the action details.

6.2.2 ACTIONS FOR A LIST OF SITES

In the **Campaign** list, click **Actions by System or List**.

- Select a region and a list of sites.
- The actions defined for the selected list are presented in form of a table (see Table describing campaigns).

Note : The sites contained in list are displayed in the Sites in the selected list table.

6.3 CAMPAIGN RESULTS

This function contains the results of deferred actions performed on a region for a given date.

- In the Campaign list, click Campaign results.
- In the calendar, select the date for which you wish to view the results.

  This date must be prior to the last campaign date.
- Select the region from the list of options **Selected region**.

The resulting information is displayed in three parts:

- **Last campaign state** area
- **Mass actions** tab: actions started for a list of sites
- **Individual actions** tab: actions started for a site.

6.3.1 LAST CAMPAIGN STATE

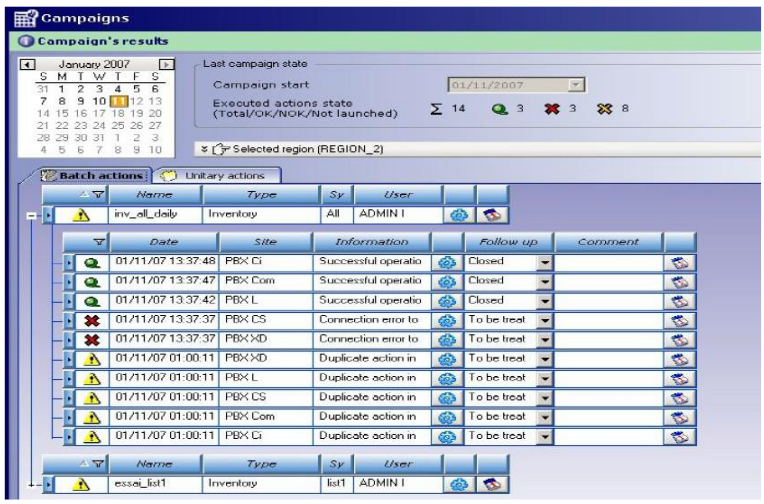
A summary of the selected campaign is presented in this display zone.

- Campaign start date
- Result of executed actions (Total Σ, actions OK, actions NOK)
- Number of actions not started (case of iPBXs under maintenance).

6.3.2 MASS ACTIONS TAB

This tab presents the results in the following form:

- A first line summarises the actions for a list of sites (see Table describing campaigns).
- You can display details of the action per site by clicking the + sign.

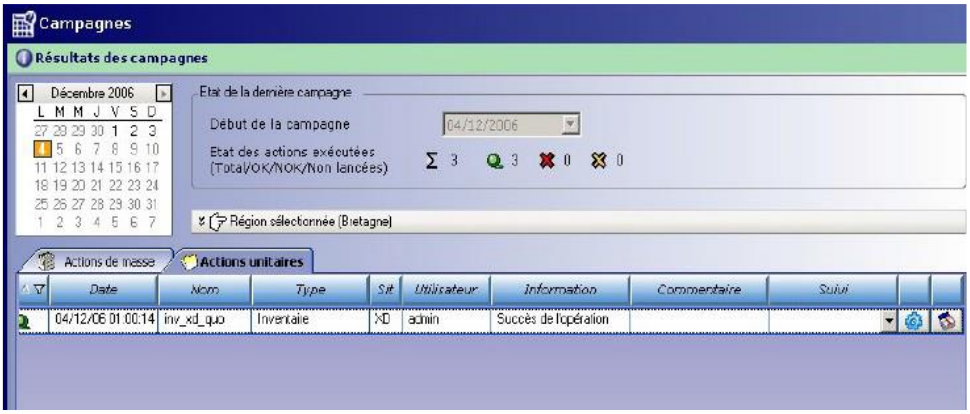


The detail line displays the following information:

- Processing date and time
- Name of the site belonging to the list
- Information: information contained in the operations log
- Follow-up: a list of options is used to assign any of the following three values that facilitate follow-up (sorting on the column):
  - To be processed
  - Taken into account

- Closed

- Comment: free data-entry area. Entering a comment enables you to identify the step to take or to create a group (sorting on the column).



The symbols used in the tables are described in

Table describing campaign symbols

6.3.3 UNITARY ACTIONS TAB

This tab displays the list of actions handled for a site. The information is presented in table form:

- Processing date and time
- Action name given by the operator
- Action type
- Site name
- User name
- Information: information contained in the operations log
- Follow-up: a list of options is used to assign any of the following three values that facilitate follow-up (sorting on the column):
  - To be processed
  - Taken into account
  - Closed
- Comment: free data-entry area. Entering a comment enables you to identify the step to take or to create a group (sorting on the column).

6.3.4 SYMBOLS USED IN THE CAMPAIGN RESULT DISPLAY

The symbols and buttons available in the campaign result display are presented in the table below:

Table describing campaign symbols

SYMBOL/BUTTON	MEANING
	Action completed successfully.
	Action not successful
	Action not executed
	Restart processing in immediate action mode, on a site or group.
	Program processing for a later date, on a site or group.

6.4 SITE MAINTENANCE

This function is used to change one or more network sites to maintenance mode, that is to suspend all programmed actions in the specified period. This function only concerns deferred actions and does not exclude the processing of immediate actions. It is selected on a region.

6.4.1 SETTING A SITE TO MAINTENANCE MODE

- In the **Campaigns** list, click **Sites maintenance**.
- Select a region,
- Click **Add**.
- A **Maintenance mode** window opens. Enter the maintenance parameters:
  - Select site
  - Start date
  - Completion date for a specific maintenance period
  - Tick **No completion date** if this date has not been determined.
  - Click **OK** to confirm or **Cancel** to close the window without updating it.

The selected site is added to the maintenance list.

6.4.2 DELETING A SITE UNDER MAINTENANCE

To remove a site from the list of sites under maintenance, click the symbol  on the list of sites displayed then **OK** to confirm the request.

The scheduled campaigns on this site will be resumed.

6.4.3 MODIFYING THE PARAMETERS OF A SITE UNDER MAINTENANCE

This function allows you to display the maintenance mode definition window so you can change the maintenance start and end dates.

- Click  to open the modification window.
- Enter the new dates.
- Click **OK** to confirm the modification or **Cancel** to close the window without updating it.

7 ADMINISTRATION FUNCTIONS

This **Administration** menu contains the MiVoice 5000 Manager administrative management functions. Some of these functions require administrator rights:

- Configuration: for defining configuration options (reserved for the administrator)
- Operator management : for creating, modifying or deleting users (reserved for the administrator)
- Actions in progress : for displaying on-going actions
- Network topology: for creating or modifying a region, a multi-site configuration or a single site
- Site identification : for identifying a newly created site so it can be managed
- Site list management : for creating site lists so as to allow group processing

Note: A site list is automatically created and associated to each multisite managed by the the MiVoice 5000 Manager. The name of this list is the name of the multisite. It contains all the sites of the multisite (automatic update according to the sites which were added or deleted in the multisite). This list allows a multi-site-based visualisation in several screens, like the inventory, the logbooks and alarm logs.

- Unlock functions : for entering key codes and displaying the unlocked functions (reserved for the administrator)
- **Preferences**: enables a user to change his/her password and manage his/her preferences in terms of ergonomics

7.1 CONFIGURATION

(RESERVED FOR THE ADMINISTRATOR)

In the **Administration** menu, click **Configuration**.

The configuration window contains the following tabs:

- Parameters tab (Servers)
- Campaign hours tab
- Export tab
- Purge tab
- Range tab
- Directory tab
- Security tab
- Filter tab
- User portal tab
- Upgrade server tab
- iPBX monitoring tab

7.1.1 PARAMETERS TAB

The **Parameters** tab has three subtabs:

General parameters tab which allows:

- The IP configuration of MV 5000 Manager
- The configuration of the mail server
- The configuration of NTP time servers

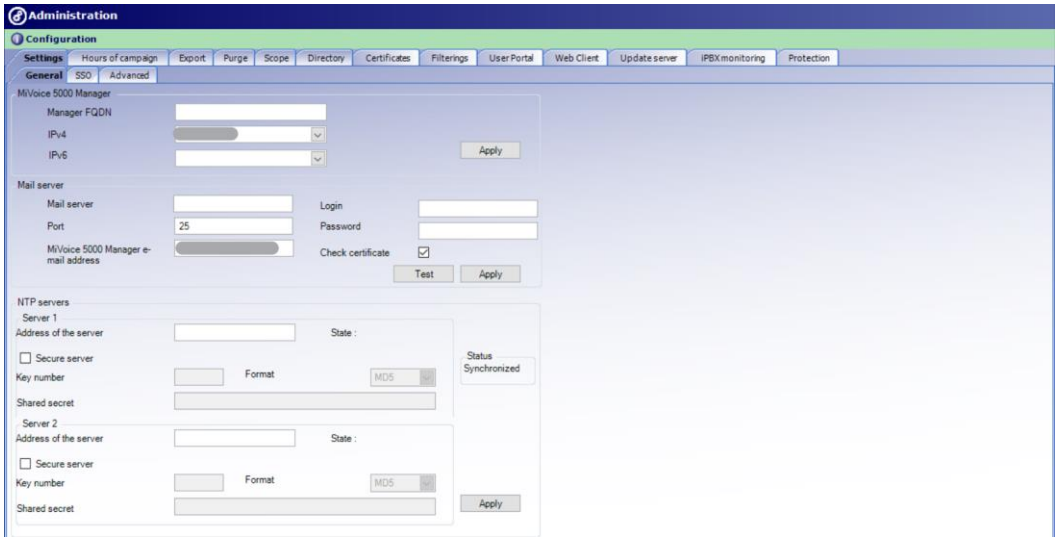
SSO parameters tab which allows:

- The SSO configuration

Advanced parameters tab which allows:

- The configuration of SSO mode
- The configuration of the inactivity time of clients resulting in a disconnection
- Port based DSCP configuration in the Firewall (required for all types of IP exchanges).

7.1.1.1 General parameters:



MiVoice 5000 Manager area:

- **Manager's FQDN**: Indicate the FQDN of MiVoice 5000 Manager. For a self-signed certificate, the server certificate is updated just after this FQDN is modified.

Also refer to document MiVoice 5000 Manager – User Guide - Chapter Installation on Client PCs.

If SSO mode is enabled for the User Portal application (see below), the FQDN defined for this mode is first taken before the one defined in the **MiVoice 5000 Manager Area**. Generally, they should be identical.

- **IPV4**: MiVoice 5000 Manager address in IPv4 format,
- **IPV6**: MiVoice 5000 Manager address in IPv6 format.

Mail server area: This area allows you to define a mail server on MiVoice 5000 Manager.

- **Mail server**: Indicate its IP address or domain name.
- **Port**: Associated port
- MiVoice 5000 Manager **e-mail address**: sender address to be indicated on sent mails.

- **Login/Password**: ID used to access the mail server
- **Check certificate**: If the checkbox is ticked, access will be verified using the authorities available in the **Trusted Root Certification Authorities** tab of the **Security** tab in the **Configuration** menu.

NTP Servers Area: This area allows you to define, if necessary, a synchronisation of the network with one or two time servers in secure or non-secure mode.

For each of Servers 1 and 2:

- **Server address**: DNS name or IP address of the NTP in question.
- **Status**: Information field which gives the NTP server status.
- Secured service:
  - **Box not ticked**: Non-secure access
  - **Box ticked**:

If the NTP server name is specified, this box is used to secure access to this server.

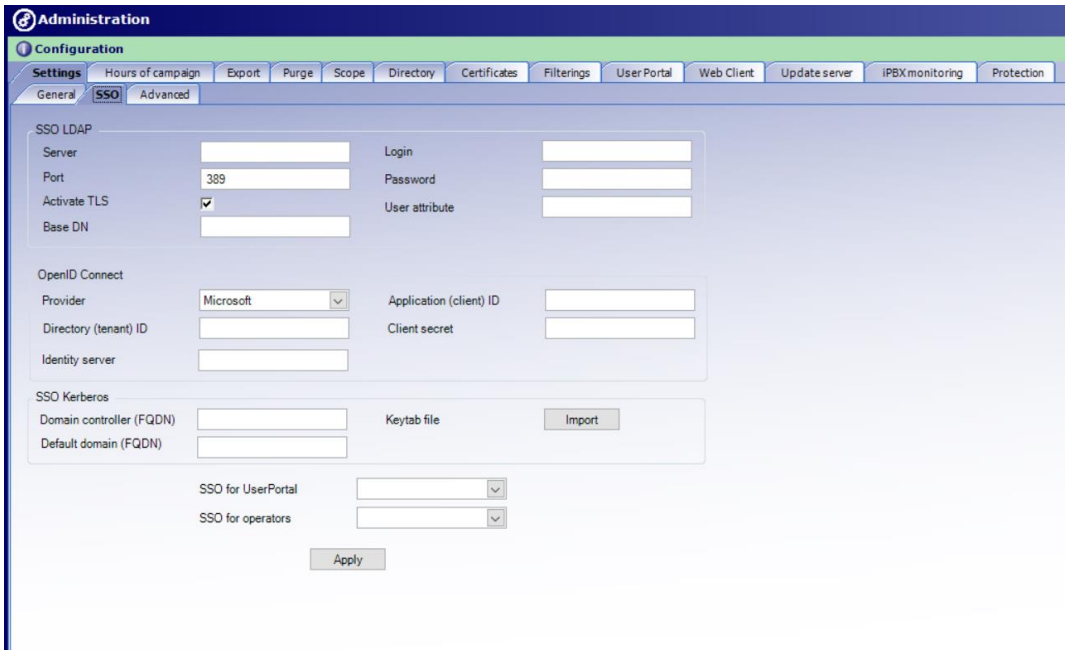
Security is ensured with a key (in MD5 or SHA1 format) and a shared secret:

- **Key number**: Value between 1 and 65534
- **Format**: MD5 or SHA1
- **Shared secret**:
- **In MD5 format**, the number of **shared Secret** characters is limited to 20 (all alphanumeric characters except 0x20 and 0x23).
- **In SHA1 format**, the number of **Shared Secret** characters is limited to 40 (all characters [0, 9] + ([a, f] or[A, F]).

The **Status** area gives information about the synchronisation status.

Synchronisation can take some time.

7.1.1.2 SSO settings



If enabled, this tab is used to configure SSO authentication for operators and User Portal users, enabling them to use their Windows login when connecting to MiVoice 5000 Manager.

There are currently three SSO modes:

- **LDAP SSO** mode for operators and User Portal users,

- **OpenID Connect SSO** mode for User Portal users,
- **Kerberos SSO** mode for User Portal users.

To select an SSO mode for the User Portal or operators, choose an option from the dropdown list.

- For the **SSO for the User Portal** field:
  - **Empty**: SSO mode disabled for the User Portal
  - **Kerberos**: Kerberos SSO mode enabled for the User Portal
  - **LDAP**: LDAP SSO mode enabled for the User Portal
  - **OpenID Connect**: OpenID Connect SSO mode enabled for the User Portal
- For the **SSO for operators** field:
  - **Empty**: SSO mode disabled for operators
  - **LDAP**: LDAP SSO mode enabled for operators

Note: OpenID Connect and Kerberos SSO modes do not apply to operators as they are incompatible with local account access.

LDAP Server Connection Settings

Server: LDAP server name or IP address

Port: Port number dedicated to LDAP access (Port 389 by default and 636 in secure mode).

TLS box:

Box ticked: Access can be secured by ticking this box, after adding the corresponding root certification authority in the **Trusted root certification authorities** tab of the **Security** tab in the **Configuration** menu.

Box unticked: Unsecured access

DN database:

Basic DN

Field corresponding to the **Distinguished Name** of the branch of the directory from which the operators and users of the User Portal are found. It must at least correspond to the root of the directory, otherwise indicate a more specific branch.

Login/Password: Login to access the LDAP/AD database in read mode. This Login/Password should preferably be defined by a specific machine account in the domain without an expiry date (password) and on which rights are limited (read only).

User attribute: Attribute used for searching in the LDAP/AD database.

Example of user attributes:

sAMAccountName: Name of an account (ex: Dupontj)

or

userPrincipalName: Full e-mail address (example: Jean.dupont@mitel.com).

In all cases, the operator accessing MiVoice Manager as a client will have to enter, at each connection, his/her password defined in his/her user domain.

The password policy remains the one defined for the domain in question (syntax, expiry date, etc.).

OpenID Connect Server Connection Settings

WARNING: The preferred provider is Microsoft Entra ID. To get the needed configuration for Microsoft Entra ID, refer to section 17.1 – SSO mode with OpenID Connect.

To configure the OpenID Connect server with Google or another provider, or if you encounter any issues with the configuration, please contact the ProServ team.

In MiVoice 5000 Manager, enter the following information provided by the chosen identity provider:

Provider: identity provider

Directory ID (tenant): identity provider ID. Valid for Microsoft only.

(Client) application ID: client ID created with the chosen provider

Client secret: client password created with the chosen provider

Kerberos Server Connection Settings

Domain controller (FQDN): Input field (100 characters maximum). Full name of the domain controller to which the authentication server connects to check the validity of the kerberos ticket against the uploaded keytab file content.

For example: ControllerMachine Name.MyDomain.com

Default domain (FQDN): Input field (100 characters maximum). Domain name associated with the iPBX in the Active Directory configuration of the Kerberos module.

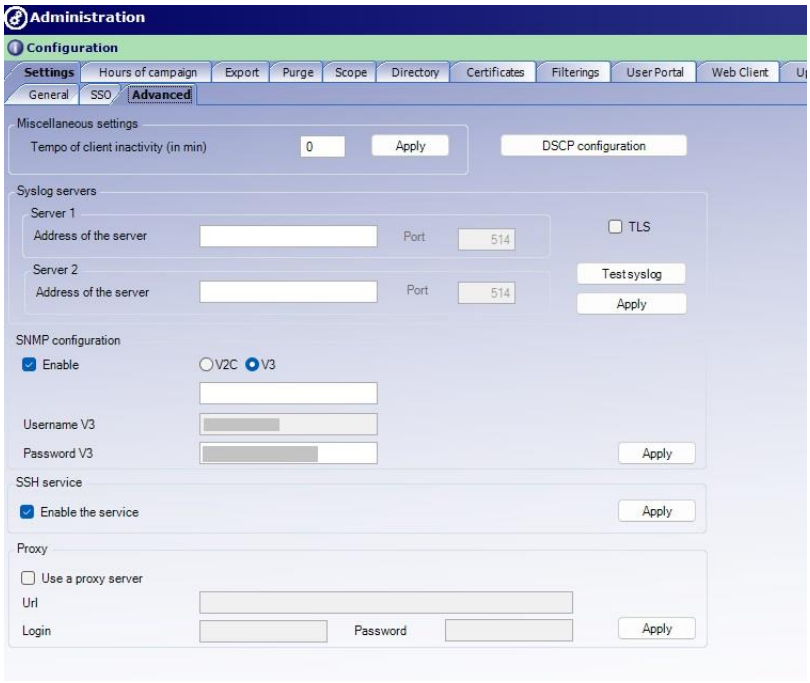
For example: MyDomain.com

Keytab file: keytab file created on the domain controller. The **Browse** button is used to locate and import the keytab file.

WARNING: To create the keytab file, refer to section 17.2 – SSO mode with Kerberos.

At the end of the configuration, click **Apply** at the end of the page to save the modifications.

7.1.1.3 Advanced parameters



Miscellaneous parameters area:

Client inactivity time (in min.):

The inactivity time is generally configurable in MiVoice 5000 Manager and concerns all services.

By default, inactivity time is: **0** (no inactivity processing).

Its value is configurable in minutes (without limits).

When the inactivity time is configured, the user's session is automatically closed as soon as the user no longer acts during the configured time.

The user's screen is blocked by an login window that requires to be filled in again.

Note : The inactivity time can be extended by the system for certain alarms.

Important notes:

For direct access to Web Admin from Manager, the duration of inactivity taken into account is that of Web Admin. Manager does make additional processing in this case.

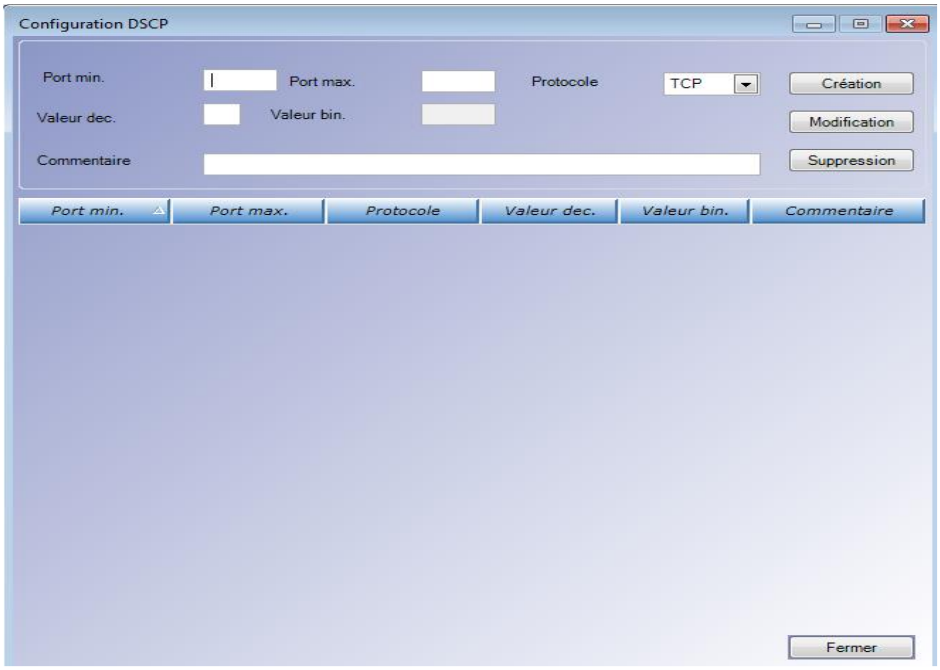
For proxy access to Web Admin from Manager, the inactivity time is shortest between Web Admin and Manager. The HTTPS connection is then closed.

DSCP Configuration button:

Port-based DSCP configuration in the Firewall (required for all types of IP exchanges).

For example, all LDAP, HTTPS or FTP exchanges must be tagged with configurable DSCPs.

This button allows access to the Port-based DSCP configuration window.



By default, no rule is configured.

The different fields allow you to set the rules for port-based DSCP configurations (maximum 100).

Configuration rules are classified by increasing the port number:

- **MIN port**: Port number [1, 65534]
- **MAX port**: Port number [Min Port, 65534] or empty
- **Protocol**: UDP or TCP
- **DSCP Decimal**: [0, 63]
- **Binary DSCP**: Binary conversion corresponding to the decimal value. This is not modifiable.
- **Comment**: String of 20 characters max.

The data can also be sorted by column header.

The configuration data in this menu can be exported or imported in **.csv** format.

Adding a port-based configuration

- Fill in the different fields.
- Click **Create**,
- A line is then created and displayed.

Once created, the configuration rule is applied to the firewall.

Configuration rules are then successively classified by Min. port number.

No tests are performed on the recovery of port ranges. It is therefore important not to set a different DSCP value for the same given port range;

Example 1:

Min port =1 ; Max port = 100 ; DSCP value = 46

Min port =2 ; Max port = 200 ; DSCP value = 47-" **OK**

Example 2:

Min port =1 ; Max port = 100 ; DSCP value = 46

Min port =1 ; Max port = 100 ; DSCP value = 47-' **NOK**

Modifying a port-based configuration

- Select the line concerned.
- Enter the new values.
- Click **Modification**.

The new line is displayed according to its port number.

Deleting a port-based configuration

- Select the line concerned.
- Click **Delete**.

The line is deleted from the list.

Syslog Servers area:

Security logs can be transmitted to one or two remote SYSLOG servers.

The security log contains:

- The login/logout log
- The configuration log.

The fields in this area allow you to enter the address(es) of the remote SYSLOG servers to send the Security Log.

Processing is done in **UDP**. If the **TLS** box is ticked, connection to the servers will be secure.

TLS box: Access can be secured by ticking this box, after adding the corresponding root certification authority in the **Trusted root certification authorities** tab of the **Security** tab in the **Configuration** menu.

If the connection is secure, Port 6514 (default setting) is blocked in the Firewall configuration of this server.

Note : If upon ticking this box the following message is displayed, follow the instructions given:

```
The module is missing. Please install latest security patch (Version 7.X 07 or
higher).
```

Server address and **Port**

The address format is either IP V4, IP V6 or FQDN.

The **Test syslog** button allows you to test the connection once the fields have been filled in.

SNMP Configuration Zone:

SNMP configuration for MiVoice 5000 Manager can be set up using the following settings:

Activate box: tick to enable the SNMP service on Manager.

Choose one of the security levels.

- V2C: requests to the Manager will use SNMPv2c and the community string.
- V3: requests to the Manager will use SNMPv3, the V3 login and secret.

Manager Community and iPbx: editable field. Will be the default community for iPbxs in SNMPv2 and also for Manager if the active mode is V2C.

V3 login: login when using SNMP V3 configuration. Not editable.

V3 password: password when using SNMP V3 configuration.

- After editing the settings, click **Apply** to save the changes.

SSH service zone:

It is possible to enable or disable the SSH service. The SSH service is enabled by default.

After editing the **Enable Service** box, click **Apply** to save the changes.

Proxy zone:

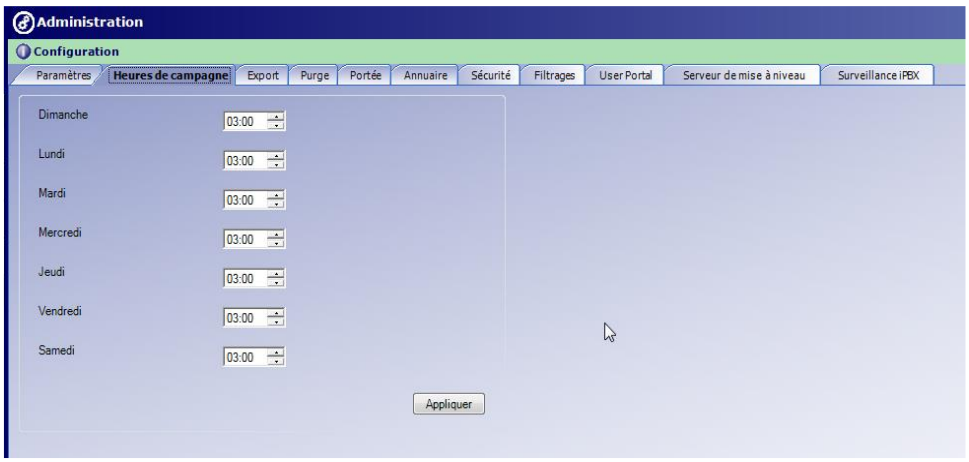
Proxy is used for Mitel licence and repository. Proxy can be set up for MiVoice 5000 Manager using the following settings:

- **Use a proxy server**: tick to open the proxy server settings in Manager.
- **URL**: proxy URL. For example, http://[adresseProxy]:3128
- **Login** (optional): ID used to access the proxy
- **Password** (optional): password used to access the proxy

After editing the settings, click **Apply** to save the changes.

7.1.2 CAMPAIGN HOURS TAB

This tab is used to manage the default campaign start time for each day of the week. This time can be modified from time to time in the **Actions by date** menu of the action group **Campaign**. Refer to Section Actions by date.



7.1.3 EXPORT TAB

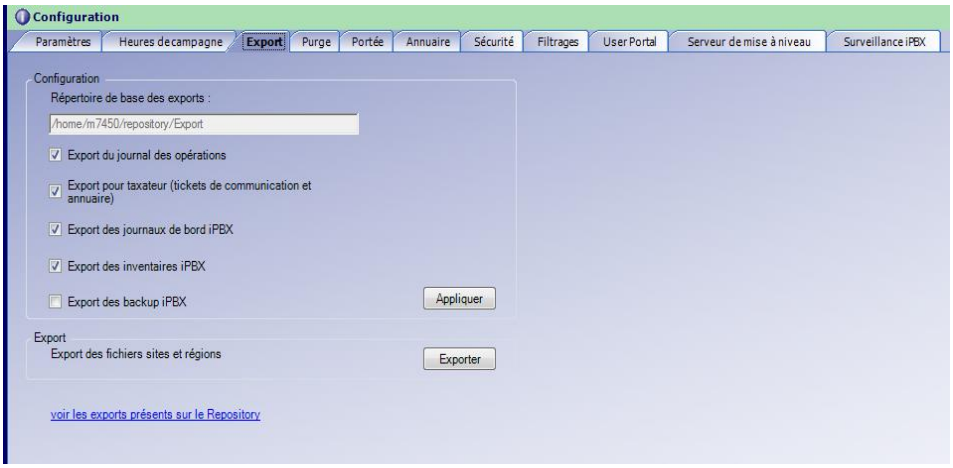
This tab is used to define the required exports and their backup directory (default Red Hat directory: **/home/m7450/repository/Export**). The configuration chosen determines the default exports.

- Select the exports from the following options:
  - Operation log export
  - PBX logbook export
  - Charging unit export (retrieving charge records and the directory)
  - PBX inventory export
  - iPBX backup export
- Click **Apply.**

The configuration modification is saved in the operations log.

Note : This configuration is used without any changes by the immediate actions. While creating deferred actions, it is possible to re-specify whether or not you want an export.

At the end of each processing operation, the data transmitted by the sites is saved in the default directory **/home/m7450/repository/Export** located on the server.



The backup directory for exports is accessible thanks to the link "*see the exports available in the repository*".

- Enter the username and password if prompted (1st access).
- Move further in the tree structure until you reach the export you want. The names of the directories concerned are:
  - *Billing/* for charge ticket export
  - *Debug/* for iPBX diagnosis
  - *inventory*/ for iPBX inventories
  - *M7450Configuration/* for MiVoice 5000 Manager backups
  - *M7450LogBook/* for the operation log
  - *PbxBackups/* for iPBX backups
  - *TMA/* for TMA backup
  - *iPBXLogbook*/ for iPBX logs

Note : The export files are not purged by MiVoice 5000 Manager.

7.1.4 PURGE TAB

The **Purge** tab is used to define the duration of backup for the following functions (the duration is expressed in days):

- Operation log
- Campaign log
- iPBX logbooks
- Alarms
- Call records
- iPBX diagnosis
- Number of iPBX backups

For each backup:

- Enter the number of backup days (the interval is specified for each backup).
- Click **Apply**.

The configuration modification is saved in the operations log.

7.1.5 RANGE TAB

Selecting a range enables you to define a uniform configuration on some or all of the sites generated for phone settings.

The range is chosen in the management centre configuration. The range must be defined with precaution because, depending on the initial configuration, it cannot be modified later (the range cannot be extended).

It is all about defining the telephony parameter range used for subscriber management. This range may be *Multi-site based*, *Region-based or Global*.

The ***Global*** range requires a uniform configuration on all the multi-site configurations managed by MiVoice 5000 Manager.

The ***Region range*** imposes a uniform configuration on all the multi-sites of the region.

In both cases, the reference telephony parameters will be those read on the first multi-site of the region. Therefore, check carefully that the reference site in question is configured with the parameters you want (see Section Presentation of the telephone parameters for the list of parameters concerned).

For a single multi-site, or multi-site configuration without the same characteristics, it is **MANDATORY** to set MiVoice 5000 Manager to ***Based on multi-site*** range.

After selecting the range from the proposed options, click **Apply**.

7.1.6 DIRECTORY TAB

This tab is used to define the parameters for connecting to the LDAP directory used to manage subscribers.

This tab is divided into three areas:

- *Directory* area: for defining LDAP directory connection parameters
- *Administration* area: lists the administrators created in the LDAP directory
- Users area: lists the applications authorised to access the LDAP directory.

7.1.6.1 Directory range

The directory range cannot be modified: it is always in multi-site range.

7.1.6.2 Defining the directory connection parameters

Enter the following connection parameters:

- **IP address**: the IP address of the LDAP directory server is set to 127.0.01. Do not change this default value.
- **TCP port**: connection port set to 389. Do not change this default value.
- **Main branch**: Information on the main branch of the LDAP directory (consultation only).

Case of the local database hosted by MiVoice 5000 Manager

In this case, for access from outside LDAP clients, MiVoice 5000 Manager is a server and gives access to its local database.

Securing LDAPS access to the directory hosted by MiVoice 5000 Manager

If the connection is secure and uses the LDAPS protocol, port 389 must be blocked in the Firewall configuration of this MiVoice 5000 Manager server in LDAPS; this server will support LDAP and LDAPS requests until all clients have been reconfigured in LDAPS.

Once all clients have been configured in LDAPS, the LDAP port 389 dedicated to the unsecured LDAP service can be blocked at the Firewall level on MiVoice 5000 Manager.

7.1.6.3 *Defining directory access profiles*

Administration area

This area lists the administrators declared in the LDAP directory server.

ROOT and CONFIG administrators are declared as default administrators. The **Modify** button is used to modify these administrator passwords.

Users area

This area lists the applications authorised to access the LDAP directory and is used to create other users. A login is created for each application.

Note : Some logins are created by default when the management centre is being installed.

To create a new login, click **Add**. During the creation, a login and password are defined. The directory access rights associated with this login are defined in the Network topology part.

To delete a login, select the login from the list then click **Delete**.

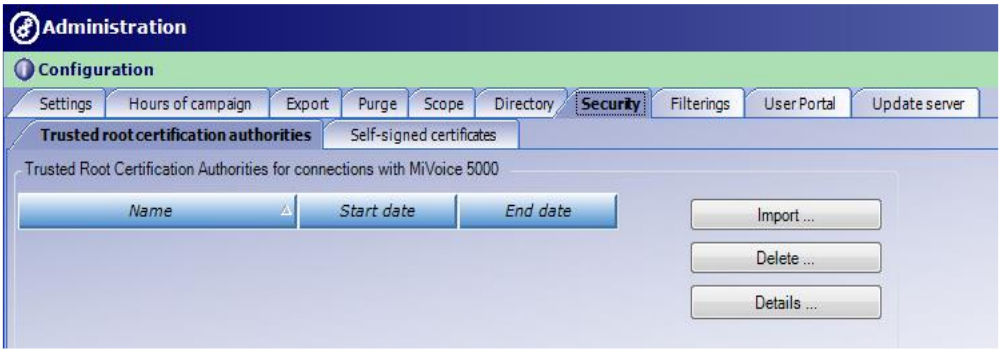
7.1.7 SECURITY TAB

This tab contains two sub-tabs:

- **Trusted root certification authorities** (for authenticating the links between MiVoice 5000 Manager and the iPBXs),
- **Self-signed certificates** (for authenticating the iPBXs on their XML interface with MiVoice 5000 Manager).

7.1.7.1 *Trusted root certification authorities tab*

This tab is used to import or delete a root certificate for authenticating the links between MiVoice 5000 Manager, the iPBXs and other remote servers.



Import This may be a CRT or CER type file.

- Click Import.
- Search and select the CA file concerned,
- Click OK.

The file is added to the list.

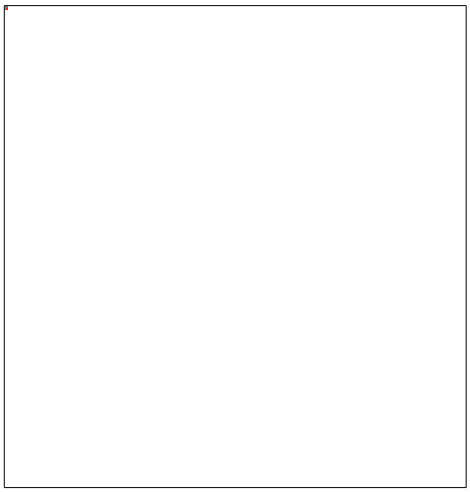
Delete

- Select the line corresponding to the certificate to be deleted.
- Click **Delete**.

After confirmation, the file is deleted from the list.

Details

Button used to access information about the certificate.

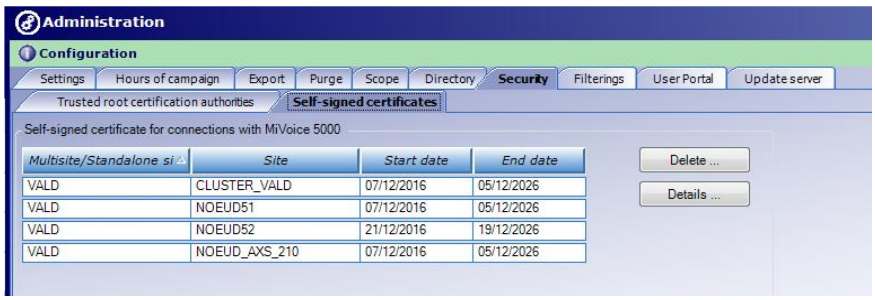


Exporting Manager's certification authority to the sites :

This action allows you to export the certification authority of MiVoice 5000 Manager to iPBX sites. This information will be available in MiVoice 5000 Server and Mitel 5000 Gateways from the **Certification Authorities** tab of Menu **SYSTEMS**>Security>Certificate Management.

7.1.7.2 Self-signed certificates tab

As of release R6.3 the iPBXs contain a self-signed certificate on the XML interface, to communicate with MiVoice 5000 manager. These certificates must be known to MiVoice 5000 Manager.



This tab is used to display and/or delete the self-signed certificates by site.

The **Details** button is used to view a certificate.

Once deleted, MiVoice no longer has access to the site concerned. It will be necessary to transfer the new certificate from this site to restore connection.

See also the sections Configuring a site / a server cluster and Configuring a multi-site network.

7.1.7.3 Certificate revocation tab

This menu allows you to activate or deactivate certificate revocation management.

Revocation management is based on the CRL (Certificate Revocation List) method.

During a TLS connection this revocation consists in:

- Retrieving the list of revoked certificates whose address is available in the server certificate
- Checking that the server certificate is not one of them.

By default, certificate revocation management is enabled (ticked). However, it is only effective if the certificates contain the CRL access point information.

The service life of the CRLs is configurable, between 1 and 15 days, and the default value is 6.

The session acceptance parameter in case of CRL recovery failure or when the CRL expires is, by default, disabled (not ticked).

Note : CRL contains its own validity date.

When the administrator ticks this parameter, the TLS session is allowed in the cases described above.

When the parameter is unticked, the TLS session is rejected if the CRL file has expired or is not found.

Note : CRL management does not take place with a self-signed certificate.

For a cluster configuration, the configuration performed on the Cluster Server is duplicated on all nodes that are in version R7.0 or higher. For previous versions, revocation is not applicable.

Services concerned

The services concerned by certificate check are:

On MiVoice 5000 Server:

- "Access to the repository for upgrading the MiVoice 5000 and OS patches.
- "Access to the repository for upgrading terminals software
- "LDAPS: Accessing an LDAP Server
- "SIP / TLS: certificate certificate sent by SIP terminal (mutual authentication)
- "MOVACS/TLS: Login to link Inersite or intra site
- "MOVACS/TLS: Conrôle of the certificate sent by an iPBX (mutual authentication).
- On MiVoice 5000 Manager:
- "Configuration/HTTPS: Access to the Web Admin of the MiVoice 5000
- "LDAPS: Supervision of a LDAP repliqua
- "Configuration/HTTPS: Access to the Web Admin of the MiVoice 5000 via the proxy

The implementation of the revocation service, which consists in installing in MiVoice 5000 and Mitel 5000 Gateways, a server certificate containing the access point address of the revocation list:

- **"Generating server certificates for each MiVoice 5000 and Mitel 5000 Gateway with the access point address of the revocation list (by the administrator),**

For iPBXs

Import certificates into each iPBX using the **Server certificates** tab of Menu **SYSTEM>Security>Certificate management**.

For MiVoice 5000 Manager

- Import the certificate into MiVoice 5000 Manager using the Manager administration web page:

Once the configuration is done, MiVoice 5000 Manager and MiVoice 5000 will ask to manage the recovery of CRLs when they receive an X.509 certificate. This verification is optimised by the presence of a CRL storage cache with a configurable validity time management.

For a cluster configuration, the configuration performed on the Cluster Server is duplicated on all nodes that are in version R7.0 or higher. For previous versions, revocation is not applicable.

7.1.7.4 Certificate loading tab

This menu allows you to install or update **trusted** certificates on all or part of the iPBXs in a multi-site configuration. These iPBXs must be in version R6.3 or higher.

The **CSV** file must be created as follows:

```
#SERVICES (Intersite, WebAdmin, UserPortal, SIP, LDAP server, Internet Gateway)
1,1,1,1,1,1
#CERTIFICATES
03FF01200433A6,siteldaps.fr.miteldev.labs.p12,secret
```

#SERVICES

A header line dedicated to defining the iPBX services which must use the certificate for installation (Intersite, Webadmin, User Portal, SIP terminals, LDAP server, Internet Gateway),

Put **1** or **0** on the next line to define or not the services to be secured.

These values, in the second line, must be put in line with a comma as separator as in the example above, respecting the order indicated in the first line:

```
(Intersite, Webadmin, User Portal, SIP terminals, LDAP server, Internet
Gateway)
```

#CERTIFICATES

Then one line per iPBX for certificates with:

- The PBX identity (Dongle ID): The ID is system-based.

For a cluster, indicate all the relevant system IDs:

- 1 line per Cluster Server
- 1 line per node

- The name of the PKCS file #12 for this iPBX
- The password for the PKCS file # 12.

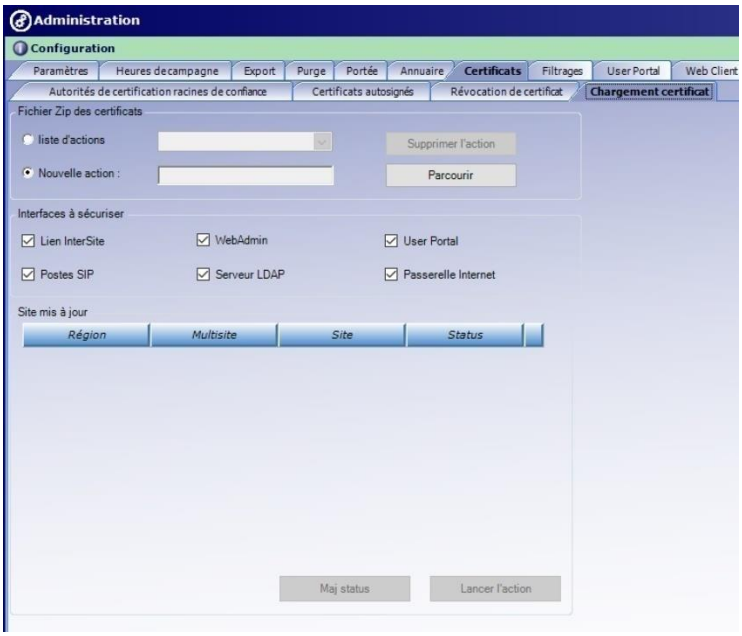
These values must be put in line with a comma as separator as in the example above.

Once created, this file must be compressed as a **Zip** file.

These different files will then be processed from the **Certificate loading** tab, which also allows you to view the status of actions on the sites.

Importing a certificate

- Tick the **New action** box.
- Click **Browse** to select the .**zip** file in question.



The .**zip** file is taken into account and is indicated in the **New action** field.

At the same time:

- the **Updated site** field indicates the list of sites on which the certificates are to be loaded (with respect to the content of the previously created **CSV** file).
- The boxes are ticked or not in the **Interfaces to be secured** area with respect to the content of the previously created **CSV** file.
- Click **Launch action**.

The certificates are then sent to the different sites and the action, automatically time-stamped, will appear in the **Action List** field.

The **Maj status** button can be used to refresh the screen and update the status of current actions.

The **Action list** field allows you to select from a list processed or ongoing actions.

The **Delete action** button allows you to delete an action when it is no longer necessary to keep the associated file (also free up memory space).

All the operations are recorded in the operation log:

7.1.8 FILTERING TAB

The traps (alerts) are sent by an SNMP agent to an SNMP manager. This latter directs them to the management centre which, depending on the defined severity level, may or may not respond to them.

Filtering is used to define the severity threshold beyond which an alarm must trigger the display of an alarm window, the sending of a notification to one or more e-mail addresses, or sending of an alarm to an external device.

In the E-mails tab:

The frame on the left side of the screen gives a list of the operators defined by the administrator in operator management.

- Select an address in the left frame and click the central double arrow to transfer it to the list of recipients.
- To add an e-mail which does not appear on the list, enter it in the space located in front of the "Add recipient" button then click this button to make it disappear from the list of recipients.
- To delete a recipient, select the e-mail address of this recipient in the frame on the right side of the window then click "Delete a recipient"

Filter area:

Define the severity threshold by selecting a value from the list. Beyond the value defined, an alarm window opens and, depending on the case, a notification e-mail is sent to one or more addresses. An alarm may also be sent to an external device.

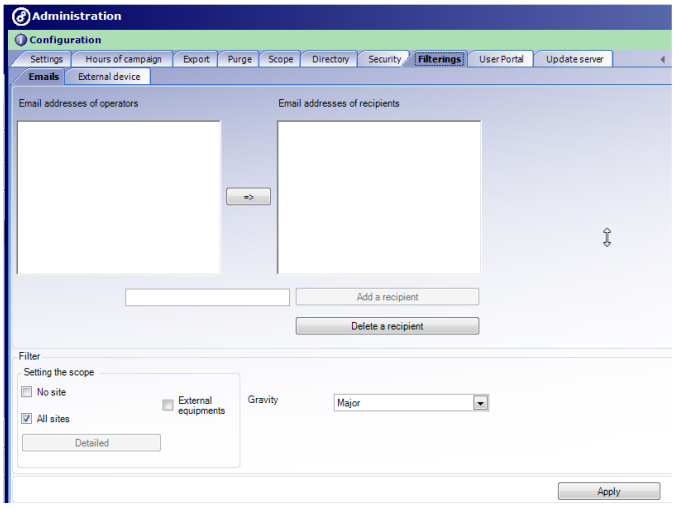
Note : If no operator e-mail address has been defined, the severity threshold taken into account for the alarms window is the one defined in the external system tab (even if it is not physically present).

Possible types are: OK, Warning, Minor, Major, Critical.

Configuring the range:

- **No site**: if ticked, no site will be taken into account.
- **All sites**: if ticked, all sites will be taken into account, depending on the selected filter.
- **External devices**: tick this box to indicate that MiVoice 5000 Manager can receive alerts from other devices than iPBXs. See the section External devices on the map**.** These alerts will be processed by the management centre in the same way as alarms from the managed sites, depending on the selected filter.

If none of these boxes is ticked, click "**Detailed**" to select the site(s) which will be taken into account, according to the selected filter.



In the External device tab:

This screen is used to manage the transmission of alarms to an external device (alarm box type). In addition to the Filter area previously described in the E-mails tab, it contains a "Serial port" field in which must be indicated the location of the port to which the alarm box is connected.

Click **Apply** to confirm the settings.

Note : The settings for a transmission to an external device are activated and deactivated from the portal (see document MiVoice 5000 Manager - Installation and configuration Administration functions).

7.1.9 USER PORTAL TAB

This tab allows you to enable or disable the MiVoice 5000 User Portal in MiVoice 5000 Manager.

By default, the User Portal is activated in MiVoice 5000 Manager. The document MiVoice 5000 User Portal - User Guide explains how to access and use the User Portal.

MiVoice 5000 Manager automatically disables the User Portal service in each iPBX.

7.1.9.1 Disabling the User Portal in MiVoice 5000 Manager

The User Portal tab of Menu **Administration>Configuration** is used to disable the User Portal in MiVoice 5000 Manager, if, for instance, the integrated User Portal is used on the iPBXs.

- Tick **Deactivate** then **Apply.**

The Aastra Phone Suite menu is no longer accessible in the subscription from MiVoice 5000 Manager.

7.1.9.2 Password policy for access to the MiVoice 5000 Manager User Portal

MiVoice 5000 Manager User Portal box:

The **Activate / Deactivate** boxes are used to activate or deactivate the User Portal application.

When SSO is enabled, this feature is deactivated and not used.

User Portal password policy box:

If the above box is ticked, the following settings must be entered to define a syntax policy for User Portal user passwords:

• Minimum password length in terms of the number of characters (1 to 16),

• Number of small letters and/or capital letters which it must contain (0 to 16),

• Minimum number of figures it must contain (0 to 16),

• Minimum number of special characters it must contain (0 to 16): « # ’ () - _ @ + = % * < >, . ; / : ",

- Password validity period in number of calendar days (1 to 999).

  0: Equivalent to **Deactivated**. Default value: 180

Note: The default password validity period is 180 days.

- If the old expiry date is later than the new expiry date, the password expiry date is immediately updated for all user accounts.
- If the old expiry date is earlier than the new expiry date, the password expiry date is updated after the old expiry date is exceeded.

7.1.9.3 Customisation

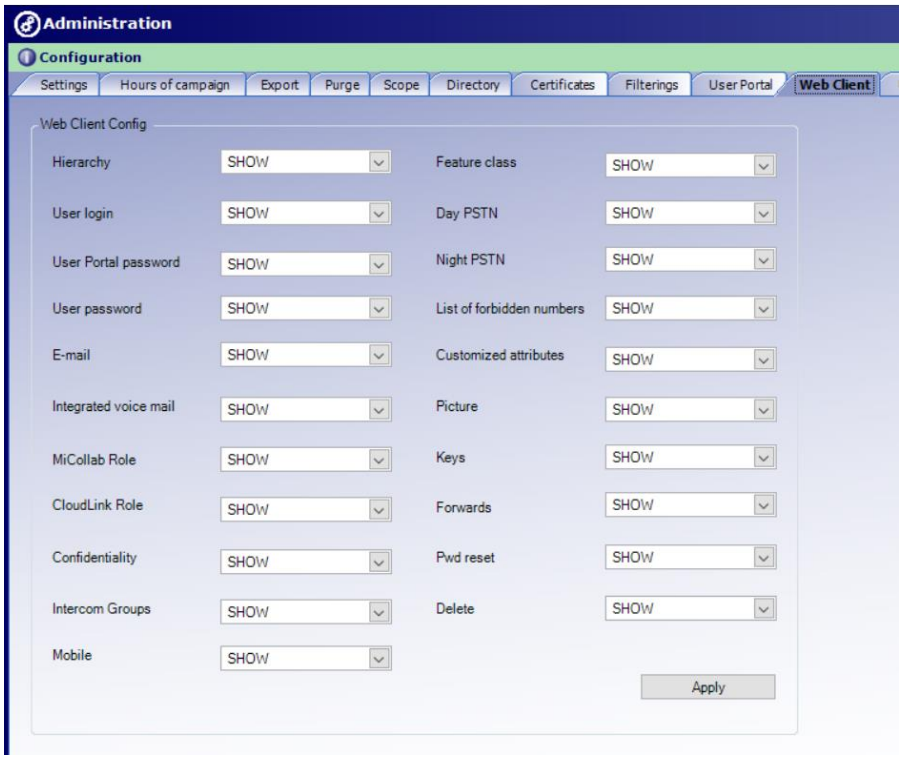
Activate box

Activates the customisation of the User Portal of the MiVoice 5000 Manager.

After activation the option, the administrator must configure the following parameters to change the visual interface of the User Portal:

- **Logo**: Click the **Import** button to open the file manager and select a JPG or PNG file.
- **Name**: Name to display on the banner of the User Portal.
- **Banner color (hex)**: Enter the hex code of the wanted color to change the color of the banner of the User Portal. For example, FF0000 for red.

7.1.10 WEB CLIENT TAB



This tab allows the administrator to define the settings displayed on the Subscriber profiles via the Web Client of MiVoice 5000 Manager.

Each setting is associated with a dropdown list. It is used to choose between:

SHOW: the setting is displayed and can be edited via Web Client Manager.

HIDDEN: the setting is hidden on Web Client Manager.

READONLY: the setting is displayed, but cannot be edited via Web Client Manager.

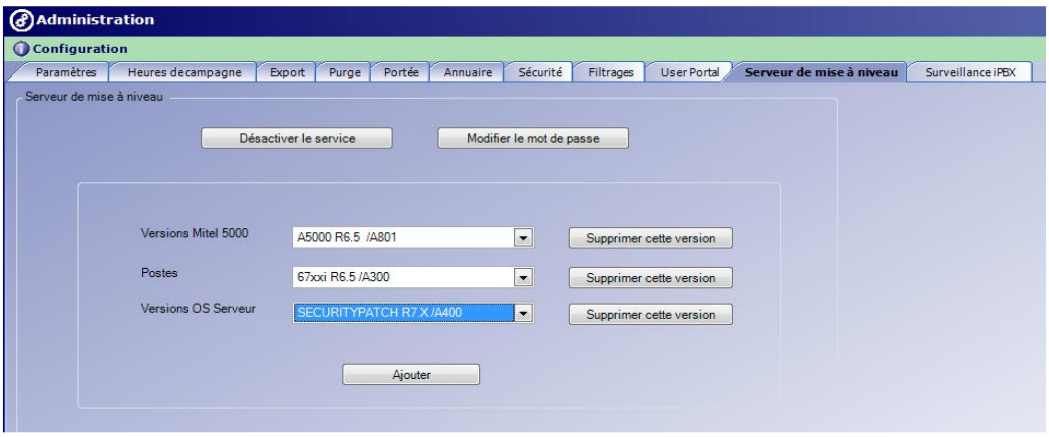
Click **Apply** to save the changes.

7.1.11 UPGRADE SERVER TAB

This tab is used to:

- Enable or disable the software package provision service during an update,
- Enable or disable automatic checks for software updates and security patches available from Mitel servers,
- Manage installed versions in Manager,
- Download new software releases and patches available on Mitel servers via Manager.

The services are disabled by default.

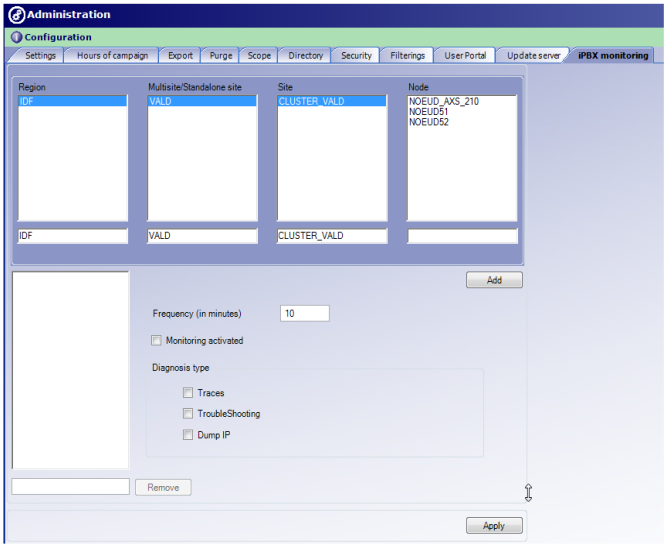


When the administrator activates the service, he is prompted to define the password to access the upgrade server.

Refer to Section Upgrade.

7.1.12 IPBX MONITORING TAB

This tab enables the administrator to define the sites (sites, cluster, cluster node) on which monitoring will be activated.



Note : For a release below R6.1, the diagnostics recovery action will not take place.

- Select individually the sites, server cluster, cluster nodes to be monitored.
- Click **Add**. The site is added to the list (it is possible to remove a site from the list by clicking **Remove** after selecting it).
- Specify the rate of execution: this is the duration, in minutes, between the start of each monitoring operation.
- Tick the type of diagnosis: Traces / TroubleShooting / Dump IP.
- Click **Apply**.

The result of this monitoring operation can then be used from immediate actions, iPBX diagnosis menu.

7.1.13 PROTECTION TAB

This menu is used to configure the security to be applied when accessing the User Portal or Web Client in OTT mode.

In OTT mode, the User Portal or Web Client may be the target of brute force attacks.

The purpose of this configuration is to identify successive failed login attempts from an IP address in order to stop the attack.

By default, when connecting to MiVoice 5000 Manager, the user is allowed 5 attempts within 10 minutes to enter their login and password. After 3 unsuccessful login attempts, MiVoice 5000 Manager locks the user's access for a given period.

Automatic blocking area

Enable auto block: enable by default (Checkbox).

Blocked IP address settings:

- Login attempt: maximum number of attempts allowed (5 by default)

- Period (minutes): maximum period for successive attempts (default 10 minutes).

Enable block expiration

Box ticked: an additional field allows you to unblock the addresses concerned according to the set duration (in hours).

- Unlock after (hours): default value 1.

IP address blocked

This tab is used to display /delete the IP addresses which have attempted to log in or to authenticate and which are considered as suspicious.

The different columns list, by address: the date and time, target IP address, origin of the attack (User Portal or Web Client service in this case).

- Select the address concerned and confirm the deletion.

Trusted proxy area

When a User Portal or Web Client user logs in via a trusted Proxy, the IP address of this Client provided by the Proxy is used. These different fields allow you to enter the addresses of the Proxy(ies) authorising these accesses.

In this window:

Apply: successive addition of trusted Proxy addresses

Address deletion: select the address to be deleted from the list. Click the button at the bottom left to confirm the deletion.

7.2 OPERATOR MANAGEMENT

(RESERVED FOR THE ADMINISTRATOR)

This function enables an operator with administrator rights to define the users authorised to access the **MiVoice 5000 Manager** application, and to define their action perimeter.

7.2.1 OPERATOR PROFILES

Several operator profiles can be defined on the management centre. These profiles define the access rights for the various functions of the application.

The following default operator profiles are available:

- **Administrator**: no restrictions
- **Operator**: access to all functions, except the server configuration, operator management configuration and function unlocking configuration.
- **Telephony**: limited access to the Telephony menu functions.
- **Web**: for accessing directly the web application used to create subscribers by profile.
- **Limited telephony**: limited access to telephony management and subscription management in profile mode. Not authorised: terminal management, Mitel applications and telephony class configuration.
- Supervision: limited access to supervision and logs (logbook, alarm log, operations log).

During installation, a MiVoice 5000 Manager administrator profile is created by default (M7450/M7450). This profile may neither be deleted nor modified.

The administrator can create one or more additional operator profiles (see the section

Managing user profiles.

The table below contains a list of services provided according to different profiles.

	Adminis-trateur	Exploitant	Téléphonie	Web	Téléphonie restreinte	Super-vision
Gestion des opérateurs	√	**(droit sur son mot de passe)**	**(droit sur son mot de passe)**	**(droit sur son mot de passe)**	**(droit sur son mot de passe)**	**(droit sur son mot de passe)**
Gestion de l'annuaire	√	√	√		√ (fiches annuaires seulement)	
Gestion des numéros abrégés	√	√	√		√	
Gestion des abonnés	√	√	√	√ (par interface Quick Create)	√	
Gestion des paramètres téléphoniques	√	√	√		√ (lecture seule)	
Gestion des numéros	√	√	√		√ (n° réservés)	
Gestion des affectations	√	√	√		√	
Installation	√	√				
Exploitation iPbx via RHM	√	√				
Sauvegarde	√	√				
Journaux de bord	√	√				√
Inventaires	√	√				
Gestion des alarmes	√	√				√
Tickets de communication	√	√				
Supervision	√	√				√
Mise à niveau	√					
Déverrouillage des fonctions	√					

User rights must also be defined according to geographic, administrative or community criteria.

- **Geographic rights**: list of regions, multi-site configurations, sites accessible to the user.
- *Assigning a right to a certain level results automatically in the assignment of the right to the levels downstream.*
- **Hierarchical rights**: the list of administrative entities on which the user may perform telephone subscriber management tasks.
- Hierarchical rights can be defined at any level on the administrative heirarchy tree.
- **Community rights**: list of site communities accessible to the user.

Assigning a right to a certain level results automatically in the assignment of the right to the levels downstream.

- **Hunt group management**:

Hunt group management facilitates the administrator's update task. In fact, when the administrator upgrades a group, all the users in the group are updated.

Groups are defined by clicking the **Hunt Group** button, located on the right side of the operator list (see the section **Managing group**). Each user group shares the same geographic, hierarchy or community rights.

To add a user to any of these user groups, the administrator selects the group he is attached to from the **Choice of Group** combo box.

Note : The management of a user group is open to the administrator or to a user with a profile configured with the "Total control" right on user management.

7.2.2 ACCESS TO OPERATOR MANAGEMENT

In the **Administration** menu, click **User management**.

The screen displays the list of existing users, with the following information:

- User name (upward or downward sorting)
- User's first name
- Login issued by the administrator
- The rights granted
- The group, if he is part of a group
- User e-mail address. This address activates the function 'Send notifications by e-mail'. An e-mail is sent in the following cases:
  - When an alarm is returned from an iPBX
  - At the end of campaigns (a report per region).

Note : This sending of e-mail notifications does not apply to web operators.

When a user is selected (the corresponding line appears in yellow), his or her configuration is displayed in the **Details** window. If this window is not visible, click the **Details** bar  .

7.2.2.1 Authenticating a user

A user can be declared and identified in the following ways:

- In **Local** mode: in this mode, user declaration and authentication are managed at the MiVoice Manager level (refer to the section Adding a user in Local mode).
- In **LDAP SSO** mode using the LDAP/Active Directory server authentication service. Login is performed first by connecting to the LDAP/AD directory server followed by authorisation in MiVoice 5000 Manager.

User and group connections are therefore managed with different levels of identification with respect to the information to be entered in MiVoice 5000 Manager:

Info / Actions Type	Login defined in	Authentication defined in	User information Name, e-mail,... defined in	Rights defined in
Local Account	MiVoice Manager	MiVoice Manager	MiVoice Manager	MiVoice Manager
User domain account	MiVoice Manager	LDAP/AD server	LDAP/AD server	MiVoice Manager
LDAP/AD groups	LDAP/AD server	LDAP/AD server	LDAP/AD server	MiVoice Manager

For user groups; they can also be declared in Local mode or from groups also defined in the LDAP/AD server and then associated with groups defined from MiVoice 5000 Manager.

7.2.2.2 *Adding a user in Local mode*

Creating a new user involves several steps:

- Identifying the user
- Assigning geographic rights
- Assigning hierarchical rights
- Defining cs rights

To add a new user, click the **Add** button on the right side of the list.

A profile creation window opens.

- In the ***Identification*** area, enter the following information:
  - User name
  - User's first name
  - User's login: character string defined by the administrator
  - His or her e-mail address
  - A password: this password defined by the administrator is temporary.
  - Define a temporary password for this new user; this password may be modified by the user to whom it is assigned.
    - Tick or leave unticked the box **Password never expires** depending on the security policy to be applied. Refer to Section **Security policy**.
- Defining rights
  - User rights are defined in two ways:
    - Either by using **Hunt group management** (see the section Managing groups) and choosing the group to which the user must be assigned
    - - Or individually as follows:
- To define some geographic rights, click the **Geographic rights** button.

  A window opens with the tree structure for the managed sites.

  By default, an operator has rights in all the regions managed by MiVoice 5000 Manager:

  - Unticking a region prevents any new multi-site created under this region from being automatically assigned to it.
  - Moreover, unticking a multi-site means that any new site added to the multi-site will not be assigned in the user rights.

  In the *Geographic rights* window, tick the regions, multi-sites or sites to assign to the user then click **Apply**.
- To define some hierarchical rights, click the **Hierarchical rights** button.

  A window opens with the administrative entity tree structure.

  By default, an operator has rights over the entire hierarchy of the multi-sites he is managing:

  - Unticking a level N of this hierarchy means that, by default, any new sublevel created under level N will not be assigned to it in terms of its geographic rights.

Note : Only the administrative entities concerning the geographic rights assigned previously are displayed.

Click a multi-site/site to display the administrative entities. Tick the administrative entities to assign to the user then click **Apply**.

Note : Assigning a right to a certain level results automatically in the assignment of the right to the levels downstream.

- To define some community rights, click the **Community rights** button.

  A window opens with the regions / Multi-site / Communities tree structure.

  - Unticking a region prevents any new multi-site created under this region from being automatically assigned to it.
  - Moreover, unticking a multi-site means that any new site added to the multi-site will not be assigned in the user rights.
- In the **functional rights** area, select any of the profiles proposed in the combo box.
- Click **Apply** to validate the creation of a new user.

To close the input window without confirmation, click **Cancel**.

7.2.2.3 *Adding a user declared in an LDAP/AD directory database on a domain*

This feature allows domain operators declared in a directory database (LDAP/AD) to log in SSO mode on MiVoice 5000 Manager, from their Windows Login.

Depending on the configuration of the directory database, the login can be either a short login (Dupontj) or an e-mail address (Dupont.jean@mitel.com), etc.

The user can also be declared as belonging to a group of the domain declared in the directory database without additional configuration (refer to the sectionManaging group.

Directory database search help

If the **Domain user** box is ticked when entering the login, an automatic search is performed in real time from the directory database. A list corresponding to the first letter of the login is then proposed to facilitate the search.

In all cases, the operator accessing MiVoice Manager as a client will have to enter, at each connection, his/her password defined in his/her user domain.

The password policy remains the one defined for the domain in question (Syntax, expiry date, etc.).

Prerequisites

LDAP SSO mode must be configured from the **Advanced** tab in the **Settings** tab of the **Configuration** Menu (box ticked and server and server access settings configured). Refer to Section Advanced parameter.

Procedure

- To add a new user, click the **Add** button on the right side of the list.
- In the lower area, tick the **Domain user** box. The link is then dynamically set up with the directory database configured as a prerequisite.
- Enter the **login** (semi-automatic entry using the list proposed in connection with the established dynamic link).

7.2.2.4 Modifying a user

- On the list of operators, click the line of the operator to be modified. It appears on a yellow background.
- If the **Details** window is not displayed, click the  Details bar located at the bottom of the ***User management*** window to display it.
- Modify the fields concerned.

To modify some geographic, hierarchical or community rights, tick/untick the items to be modified.

Note : Only the login cannot be modified: if you need to change the login, you have to delete the user and create it again with a different login.

- Check the elements modified then click **Apply**.

*To close the input window without confirmation, click **Cancel**.*

Note : The modifications have been saved and will become effective next time the user opens a session.

7.2.2.5 Deleting a user

- Select the user to be deleted from the list of users.
- Click **Delete**.

Note : The user with the default administrator rights (login M7450) cannot be deleted. It may be modified, but its administrator rights cannot be deleted.

- Enter **OK** when prompted to confirm the deletion. To cancel the deletion, click Cancel.

7.2.2.6 Printing the list of users

- To print out the list of users, click **Print**.
- A preview of the list appears.
- If necessary, define the print format (one or more pages per sheet).
- Click the printer symbol to send the print request to the printer connected to the PC.

7.2.2.7 Exporting the list of users

Clicking **Export** lets you display the list of users in .xls format and save it on the PC.

7.2.2.8 Importing the list of users

Clicking **Import** lets you search on the PC a file in .xls format to import into MiVoice 5000 Manager. The **User import** window lets you check and confirm the import.

7.2.2.9 Managing groups

Groups are always local groups and can be linked to a group of the domain controller.

The **Group management** button is used to add and delete user groups with the same rights.

Rules:

- a user is assigned to one group (only one group).
- It is not possible to delete a user group containing at least one group.
- The number of user groups is unlimited.
- The number of users in a group is unlimited.
- A user's rights are limited to those of the group (local or from a directory database).

CREATING A LOCAL USER GROUP

- From the **Group management** screen, click **Add**. It is possible to create a user group from an already created group.
- Enter the name of the new group.
- If necessary, create enter a comment.
- Enter the rights using the **Geographic rights** / **Hierarchical rights** / **Community rights** buttons (see the section Adding a user in Local mode).
- Choose the user profile by selecting it from the **Choice of user type**combo box.
- Click **Apply**.

The new group is displayed on the list of groups.

The groups are classified in alphabetical order; however, the digit in brackets represents the order of creation.

CREATING A GROUP OF USERS DECLARED IN THE DIRECTORY DATABASE

- From the **Group management** screen, click **Add**. It is possible to create a user group from an already created group.
- Enter the name of the new group.
- If necessary, create enter a comment.
- Fill in the **DN LDAP/AD** Group field to set up the link to the group defined in the directory database. The link will then be set up dynamically.
- Enter the rights using the **Geographic rights** / **Hierarchical rights** / **Community rights** buttons (see the section Adding a user in Local mode).
- Choose the user profile corresponding to the functional rights by selecting it from the **Choice of user type** combo box (see the section Operator profiles).
- Click **Apply**.

The new group is displayed on the list of groups.

The groups are classified in alphabetical order; however, the digit in brackets represents the order of creation.

VIEWING A USER GROUP

On the list of groups, click the one to view.

When the users have been assigned to the group, they are listed in the **User list** area.

The rights assigned to the group can be modified. The properties of all the users belonging to the group will then be modified.

DELETING A GROUP

- Select the group to delete in the list.
- Click **Delete** then **OK** to confirm.

Note : It is not possible to delete a group as long as a user is assigned to it.

MODIFYING THE NAME OF A USER GROUP

- Select the profile to modify in the list.
- Modify the name then click **OK**.

Note : Only the name of the group can be modified.

7.2.2.10 Managing user profiles

The **Profiles management...** button is used to add new user profiles or to modify the characteristics of existing ones. A user profile corresponds to a set of functional rights.

CREATING A USER PROFILE

- From the **Profiles management** screen, click **Add**. It is possible to create it from an already created profile.
- Enter the name of the new user profile.
- If necessary, create enter a comment.
- For each of the functions displayed, select the associated right:
  - Total control: the user will have full access to the function.
  - Read only: the user will have read access only.
  - Not accessible: the user will not have access to the function.

The title of the listed functions is displayed by placing the mouse over  .

- Click **Apply**.

The new profile is displayed on the list of profiles.

The profiles are classified in alphabetical order; however, the digits in brackets represent the order of creation (as from 7 since the first 6 digits are default profiles).

Note : The Read_only (6) profile is the only default profile available on the list of profiles. It is modifiable.

VIEWING A PROFILE

On the list of profiles, click the one to view.

When the users or user groups have been assigned to the profile, they are listed in the **Associated lists** area.

The functional rights can be modified. The rights of all the users belonging to the profile will then be modified.

DELETING A USER PROFILE

- Select the profile to delete on the list.
- Click **Delete** then **OK** to confirm.

RENAMING A USER PROFILE

- Select the profile to modify in the list.
- Only the name can be modified.
- Modify the name then click **OK**.

7.2.2.11 *Viewing connected users*

To see the list of connected users, click the link *"See currently connected users"* .

Note : Web operators do not appear on the list of connected operators.

Enter the required administrator password.

An HTML page opens with the following information:

- The user's name (Login)
- The IP address of the PC with which the user connected
- A  button for disconnecting the user in question.

You will be asked to confirm disconnection before the operator's session is closed.

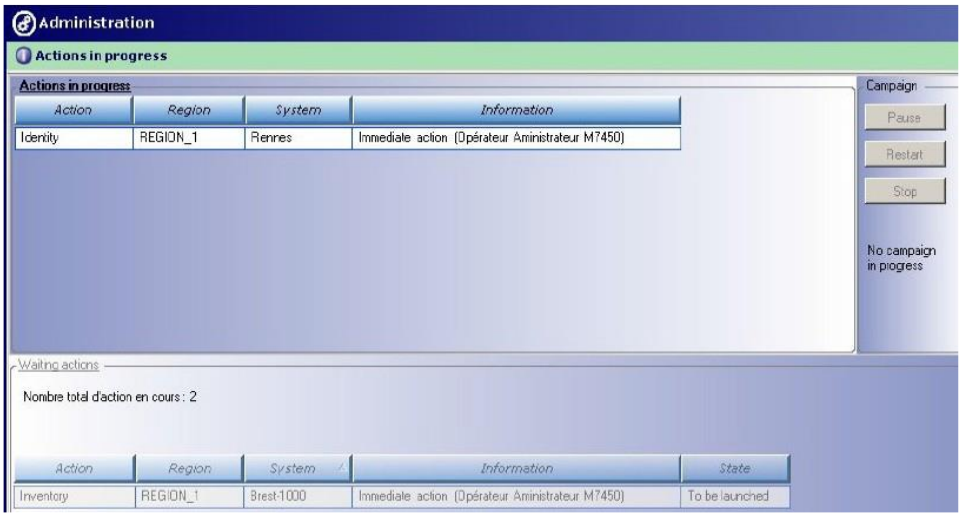
7.3 ACTIONS IN PROGRESS

The **Actions in progress** window displays the actions being handled and actions on standby.

In the **Administration** list, click **Actions in progress**.

The following information is displayed:

- Action type
- Region, multi-site configuration and site concerned
- Information: action name assigned by the user in case of deferred action. If it is an immediate action, the label “immediate action” is displayed. In both cases, the username is specified.
- For standby actions, the information is the same, with in addition the status of the standby action which may be:
  - To be started: action waiting to be executed
  - Pause: a pause has been requested at the campaign level. The status of the actions will change to “To be executed” during resumption.
  - Action in progress: in a campaign, these actions will be executed even if a pause is programmed, because they are part of the sequence of the action already in progress.



Note : Since a maximum of 30 actions in progress can be displayed, it may be necessary to make a selection on region/site to reduce the display.

7.3.1 POSSIBLE ACTIONS ON CAMPAIGN

You must have administrator rights to perform these tasks.

- Pause: this button is enabled when a campaign is in progress. It can then be used to stop deferred actions on standby. However, actions in progress on a site can be completed.
- Resume: this button resumes the processing of the campaign.
- Stop: this button deletes the actions on standby. The actions in progress are completed.

7.4 NETWORK TOPOLOGY

This menu, accessible with an administrator profile, is used to manage network elements. It is used to create or modify regions, and to define multi-site configurations or sites.

It is possible to add a site under a region, a site or a cluster in an existing multi-site configuration, a site in a multi-site configuration to be created.

7.4.1 DEFINITIONS

Region: refers to a group of multi-site configurations or isolated sites (logical group).

Multisite: refers to a group of iPBXs connected together to offer a distributed switching function. A multi-site is characterised by:

- The presence of a single directory
- The definition of identical telephony parameters on all the iPBX
- Uniform number management on all the iPBXs.

Site: refers to an iPBX or MiVoice 5000 comprising one MiVoice 5000 Server and one or more gateways. It also refers to a cluster in a Cluster Server architecture.

Isolated site: site not belonging to any multi-site network. In the site selection window, the standalone site is located under a region, on the same level as multi-sites.

Node: component of a cluster in a Cluster architecture.

7.4.2 RECOMMENDATIONS

Network topology elements are created in the following order:

- Directory configuration (configuration menu)
- Creating regions
- Creating multi-sites
- Creating sites. Creating clusters and their nodes in a Cluster Server architecture
- Creating messaging systems
- Generating iPBX data

Note : To return to the selection page, remember to click Return or Cancel.

7.4.3 CREATING A REGION

(Reserved for the administrator)

To create a region:

- In the **Network topology** window, click the *New region* field.
- Enter the name of the new region then click **Add**.

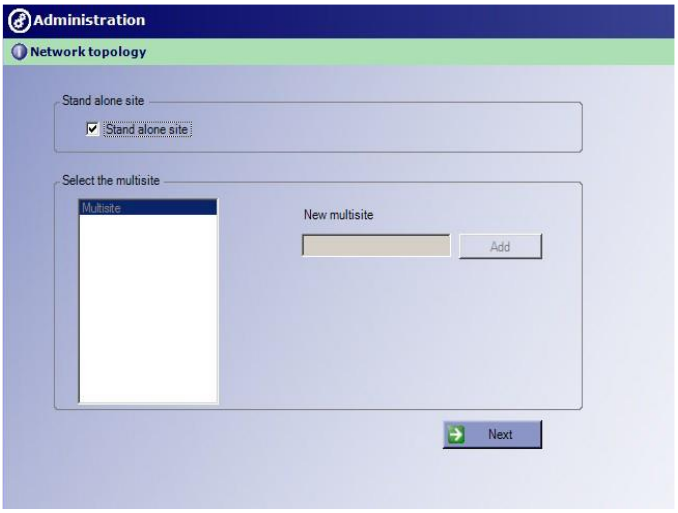
The new region is displayed on the list of regions, and the operations log updated.

7.4.4 CREATING A NEW SITE

To create a new (standalone) site:

- In the list of regions, select the region in which the site will be created.
- Click the **Add** button located under *New site/multi-site/node*.

A site creation window opens.



- Tick the **Standalone site** option then click **Next**.
- The **Identity** and **Advanced configuration** tabs are displayed. Refer to Section Configuring a site / a server cluster.
- Enter the information in the **Identity** and **Advanced configuration** tabs then click **Add**.
- An iPBX identification request window opens. The identification action makes a site operational.
- Click **Identify** to start iPBX identification immediately. Otherwise, click **End** (the identification operation will then be started later).

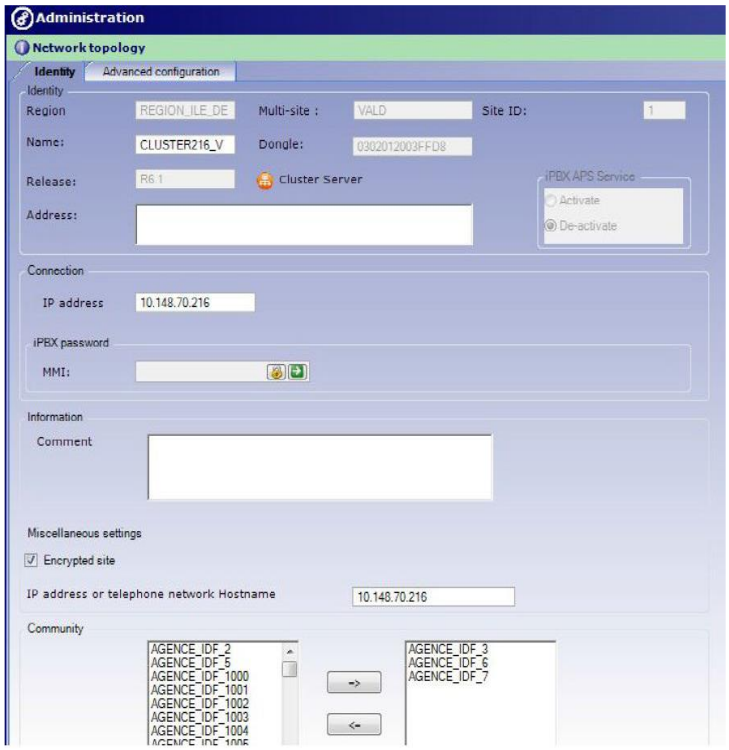
7.4.5 CONFIGURING A SITE / A SERVER CLUSTER

The site configuration window consists of 2 tabs: **Identity** and **Advanced configuration**.

7.4.5.1 Identity tab

This tab contains following areas:

- *Identity* area: displays the site information
- *Connection* area: displays server connection information
- *Information* area: displays additional information about the site
- *Miscellaneous parameters* area:
- *Community* area:



IDENTITY AREA

Region: entered in the previous screen

Name: site / server cluster name

Version: iPBX software release (entered during site identification)

Dongle: dongle number (entered while identifying the site).

In cluster mode, the 

symbol is available on the cluster, the 

symbol is available on a cluster node.

The **Survival node** box is to be used for survival mode operation.

Standalone indicates a standalone site.

Address: optional free input. For locating the site in the region.

iPBX Service User Portal: this area is greyed out and cannot be modified when the User Portal is managed by MiVoice 5000 Manager or when the iPBX release is R5.x. This area can be modified when you want to use the User Portal embedded in the iPBX (iPBX >= R6.1); in this case, click **Activate**. This area does not appear on a cluster node but on the server cluster.

For a multi-site:

- **Multi-site name**: entered while identifying the site.
- **Site ID**: number of the site in the multi-site configuration.

For a standalone site:

- **Multi-site** (for a standalone site): tick this box to add the standalone site to a multi-site network then fill in the following fields:
  - Identifier: name of the multi-site configuration
  - Site ID: number of the site in the multi-site configuration.

CONNECTION AREA

Note : Depending on iPBX type, some fields may not be accessible.

- **IP address or FQDN**: Login parameters for the Administration network. Enter the IP address of the iPBX or the FQDN.
- Mitel 6000 SIP Phone **keys**: Options used to enable or disable Mitel 6000 SIP Phone updates from the User Portal (see the document MiVoice 5000 User Portal - User Guide).

ATTENTION : As of R6.1, this configuration must be carried out on the iPBX. It no longer appears on this MiVoice 5000 Manager screen.

- **iPBX server passwords**: Web Admin access password. This password must be identical to the one created for the account **cg7450** used by MiVoice 5000 Manager. This field is empty by default.
  - The padlock symbol does not allow the entry of a password identical to that of the iPBX in order to realign to it. (The field must be filled out with the same value as on the iPBX).
  - The green arrow opens the menu used to modify the iPBX's Web Admin password for the account used by MiVoice 5000 Manager: **cg7450**.

Note : As of R6.3 a password policy may be defined from AMP. See the iPBX Web Admin in Menu **Telephony service>Systems>Security>User password policy**, and also the document MiVoice 5000 - Operating Manual.

SNMP configuration:

The following information is displayed:

- **V1/V3** radio buttons, to indicate the type of SNMP V3 configuration to be assigned to the iPBX
  - **In SNMP V1 mode**: No field to be filled out (field greyed out and inaccessible)
  - **In SNMP V3 mode**: The fields are as follows:
- **EngineID**: PBX ID, greyed out text area, given for information only,
- **PBX security name**: greyed out text area, given for information only,
- **Secret**: Password shared by MiVoice manager and the iPBX: allows the reception of notifications. This attribute may be modified by the user.

When a PBX is added, no "SNMP" information is provided because the site is not identified. The information will be obtained during identification.

The following operations are possible from the client terminal:

- Activating/deactivating SNMP V3: the SNMP version cannot be modified if the iPBX is a MiVoice 5000 Server cluster node.
- The **Secret** field can only be modified if the iPBX is already set to SNMP V3. The secret is normally automatically generated by the iPBX when SNMP V3 is locally activated on the iPBX.

Note : It is not possible to request for switchover to V3 if a **Secret** input is in progress.

For the syntax of the **Secret** field, the following checks are made:

- Length - between 8 and 16 characters,
- Alphanumeric characters only plus at least one letter and one figure.

If the input does not respect these rules, the user is alerted by an error message.

These modification operations are not immediate. The request is sent to the iPBX, which sends a message once the operation is carried out.

INFORMATION AREA:

- **Comments**: Input area for comments

MISCELLANEOUS PARAMETERS AREA

- **Encrypted site**: When encryption has been enabled on the multi-site architecture, a possibility is offered to disable encryption for the site in question. The area is greyed out if encryption is not enabled in the multi-site architecture.
- The **Download iPBX certificate** button is used to regenerate the certificate on a site.
- **IP address or FQDN of the telephony network**: Field to be completed in case of flow separation (see the document MiVoice 5000 - Separating telephony flows and administration.
- **Community**: Select subscriber communities (see the document Managing DID numbers, in directory characteristics.

COMMUNITY AREA

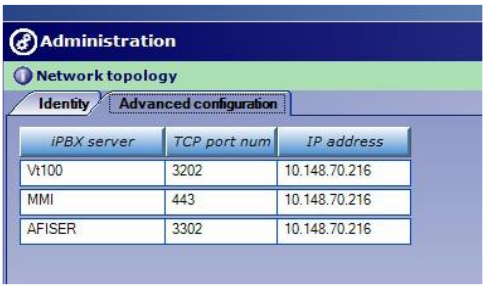
- **Community**: Select the subscriber communities and indicate whether the site is default backup site for managing subscribers in profile mode (see the document Managing DID numbers, in directory characteristics).

7.4.5.2 Advanced configuration tab

The list of iPBX servers is entered by default.

The TCP port and IP address columns are modifiable.

Note : The port to use for the MMC server is 443.



7.4.6 MODIFYING THE CONFIGURATION OF A SITE

A site configuration window is used to modify the parameters of a site, delete the site or execute site identification.

To display the site configuration window:

- Select a region, a multi-site network then a site and click the **Configuration** button.
- The window comprises two tabs: **Identity** and **Advanced configuration**.

7.4.6.1 Identity tab

All the information entered when creating the site can be modified except the name of the region and multi-site network, the dongle number and the software release.

Modify the necessary fields then click **Modify** to take account of the modifications.

7.4.6.2 Advanced configuration tab

To modify the TCP port or IP address of the iPBX:

- Click the area to be modified. It appears on a yellow background.
- After entering the modifications, return to the *Identity* tab then click **Modify** to validate the modification.

7.4.6.3 Deleting a site

- Select a region, a multi-site network then a site and click **Configuration**.

  The configuration window opens.

- In the **Identity** tab, click **Delete**.

  A confirmation request window opens.

- Click **OK** to confirm the deletion.

The site is deleted from the list of multi-site network sites. A notification is displayed, and the operations log updated.

Note : If the site is managed by a voicemail system, the deletion confirmation message indicates it. If the deletion is confirmed, the site is deleted from the list of sites managed by voicemail.

7.4.7 CREATING A NEW MULTI-SITE NETWORK

7.4.7.1 Creating a site in a new multi-site network

- In the list of regions, select the region in which the site will be created.
- Click the **Add** button located under *New multi-site/Site/Node*.
- A site creation window opens.
- Untick the *Standalone site* option to make the *New multi-site* field accessible.
- Enter the name of the new multi-site and click **Add**.

The new multi-site is displayed in the multi-site selection window.

Note : Pressing the Add button does not create the multi-site in the region. The multi-site will be created when the site is being created.

- Click **Next**.
- To create a cluster, see the document Implementing a MiVoice 5000 Cluster Server, or click **NO**.
- The **Identity** and **Advanced configuration** tabs are displayed. Refer to the section Configuring a site / a server cluster for more information on how to use this form.
- Enter the information in the **Identity** and **Advanced configuration** tabs then click **Add**.
- The creation is taken into account, and the operations log updated.
- An iPBX identification request window opens. The identification action makes a site operational.
- Click **Identify** to start iPBX identification immediately.

Otherwise, click **End** (the identification operation will then be started later).

7.4.7.2 Creating a site in an existing multi-site

- Select the region then the multi-site in which the new site will be created.
- Click the **Add** button located under *New multi-site/Site/Node*.
- To create a cluster, see the document Implementing a MiVoice 5000 Cluster Server, click **NO**.
- The **Identity** and **Advanced configuration** tabs are displayed (see the corresponding sections).
- Enter the information in the Identity and Advanced configuration tabs then click **Add**.
- The creation is taken into account, and the operations log updated.
- An iPBX identification request window opens. The identification action makes a site operational.
- Click **Identify** to start iPBX identification immediately.

Otherwise, click **End** (the identification operation will then be started later).

7.4.8 CONFIGURING A REGION

To access the region configuration window, select a region then click the **Configuration** button.

A window opens with the following options: **Apply** / **Delete** / **Cancel**.

7.4.8.1 Renaming a region

In the configuration window, rename the region then click **Apply**.

The region is modified in the list of regions accessible to the user. A notification is displayed, and the operations log updated.

7.4.8.2 Deleting a region

In the region configuration window, click **Delete**.

A confirmation request window opens. Click **OK** to confirm the deletion.

The region is deleted in the list of regions accessible to the user. Deleting a region deletes the objects (multi-site networks, standalone sites, sites, voicemail systems) associated with it.

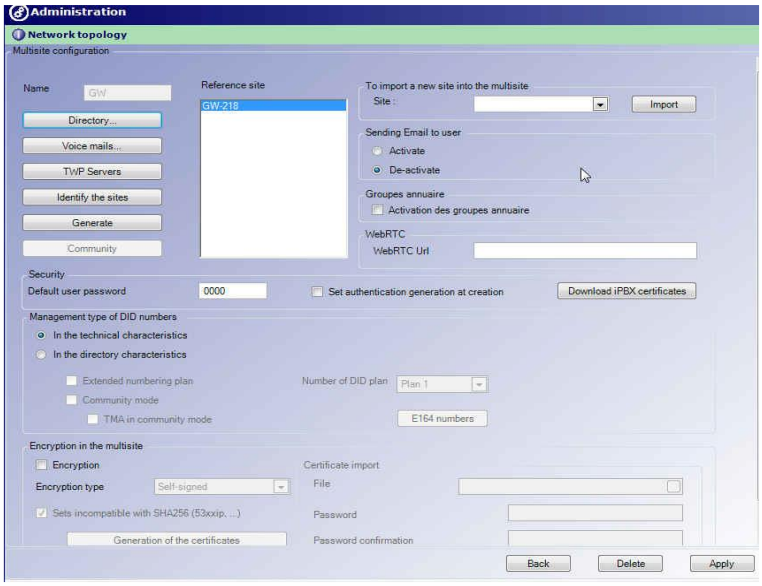
A notification is displayed, and the operations log updated.

7.4.8.3 Configuring a multi-site network

To access the multi-site configuration window:

Select a region, a multi-site then click the  **Configuration** button.

The following window opens.



In this window, it is possible to:

- Define a reference site
- Import a new site into the multi-site
- Define the default user password
- Define the type of DID number management, including or excluding the E164 format configurable from the **E164 numbers** button
- Activate/deactivate e-mail transmission to users
- Enable/Disable groups in the directory
- Enable/Disable the management of technical hierarchies parameters
- Define encryption in the multi-site

The buttons are used to:

- Configure directory access rights
- Configure a voicemail system
- Configure a TWP server
- Identify the sites
- Run a generation action to download iPBX data
- Access the community configuration (see the document Managing DID numbers, in directory characteristics).

The **Return** button is used to return to the network topology screen.

7.4.8.4 Defining a reference site

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

Select a site in the **Reference site** area then click **Apply**.

7.4.8.5 Import a new site into the multi-site

The **Import a new site into the multi-site** area is used to:

- Either import data from a new site declared in the multi-site configuration
- Or import, for a given existing site, the new data if it has been updated.

7.4.8.6 Sending an e-mail to a user

The **Send e-mail to user** area is used to activate or deactivate the **Send e-mail** function. When the feature is enabled and if an e-mail address is entered for the subscriber. See the section **Directory record**, an e-mail is sent in the following cases:

- To send the password for the User Portal (see the document MiVoice 5000 User Portal - User Guide).
- In case of user password assignment:
    - When the subscription is created (individual or massive creation)
    - In case of modification by the operator
- If the user is informed that his password has been frozen after three incorrect inputs.

ATTENTION : During massive import, it may be preferable to disable this feature. On the other hand, if the e-mail transmission function is activated on the management centre, it must be deactivated on the iPBX to avoid double e-mail transmission.

7.4.8.7 *Directory groups*

This function is used to limit access to the LDAP directory (via group definition) during search by name, for Mitel 6xxx SIP phones and proprietary terminals.

When the function is enabled, groups can be managed in the directory parameters (add/delete/list).

Two attributes are available in the definition of an internal record:

- **Subscriber's group membership**: group(s) in which the subscriber is defined
- **Groups accessible for directory search**: group(s) accessible toy the subscriber in the "search by name" function.

In the definition of an alias record or external contact file, only the **Group membership** attribute can be defined.

Moreover, the massive operations will take these attributes into account.

7.4.8.8 *Security*

Default user password: the password is the same for the subscription and the associated IVB. It is pre-defined and may be modified by the administrator (4 digits). This password applies to all the iPBX >= R5.4 of the multi-site network. It is used while creating a local, multi-line, multi-user, DISA, IVR or ATDC type subscription (in this case, it concerns the secondary lines of the ATDC). The area is greyed out if the release of the all multi-site sites is below R5.4.
This password may be replaced at the subscription level and is entered in the technical record.

Generate terminal authentication during creation: If this box is ticked, the subscriptions created automatically contain a password for terminal authentication (iPBX >= R5.4 SP2).

Download iPBX certificates button

As of release R6.3 the iPBXs contain a self-signed certificate on the XML interface, to communicate with MiVoice 5000 manager. These certificates must be known to MiVoice 5000 Manager.

The download operation is automatically started the first time a site is identified or during an upgrade to R6.3.

This button is used to later download, if necessary, all the self-signed certificates available on the sites in the multi-site architecture. The list is available in Menu **Configuration>Security>Self-signed certificates**. Refer to Section tab.

The action is mentioned in the operations log.

7.4.8.9 *Type of DID number management*

The **Type of DID number management** area is used to define the multi-site-based type of DID number management:

- In the technical characteristics
- In the directory characteristics.

See the document Managing DID numbers, in Directory characteristics.

7.4.8.10 Encryption in the multi-site configuration

Prerequisites

MiVoice 5000 Manager, the Cluster (Cluster Server and all the nodes), as well as all the remote sites, must be synchronised via an NTP server:

- Same date
- Same time
- Same minute.

In case of certificate deployment malfunction, check the date/time/minute synchronisation.

In the inter-sites and intra-cluster links.

The following interfaces are concerned:

- Web Admin,
- User Portal,
- MOVACS,
- Terminals.
- The encryption is applied to the entire multi-site configuration and concerns all the R6.3 sites.

While generating certificates, select the option "Generate certificates only for sites already with the encryption property" (seen from MiVoice 5000 Manager).

On the other hand, encryption works between two iPBXs only if it is active on the two iPBXs.

When the feature is enabled, the encryption type must be selected from the options:

- **self-signed encryption**: This type of encryption corresponds to generating a self-signed certificate in each iPBX of the multi-site architecture. In this case, MiVoice 5000 Manager sends the certificate generation command but the certificate is fully managed by the iPBX.

When the certificate expires an expiry alarm is sent to MiVoice 5000 Manager for information, and a new self-signed certificate automatically generated by the iPBX.

- **Through import**: In this case, encryption is carried out by importing the certificate; fill in the **Certificate import** area as follows:
  - On the PC select the file type PKC#12 provided by the relevant authority.
  - Enter the password (twice).
  - Click **Import** to import this certificate into MiVoice 5000 Manager.

  14 days before the expiration of the certificate, the iPBX sends to MiVoice 5000 Manager a daily alarm which counts down the number of days remaining. Upon receiving this alarm, MiVoice 5000 Manager regenerates the certificate. At the end of these 14 days, if MiVoice 5000 Manager fails to regenerate the certificate, an expiry alert is sent to MiVoice 5000 Manager and encryption stops working.

  Terminals not compatible with SHA256 (53xx. ...) : This box must be ticked if some terminals are not sha256 compatible. In this case, the certificates generated are in sha1. Moreover, if the operator imports any certification string containing SHA256, a self-signed certificate is used for the terminals. In case of interoperation with a release below R6.3, the inter-site links also change to self-signed mode.

Generating certificates

after clicking the **Apply** button, this button is greyed out. It is used to generate or broadcast the certificates in the sites of the multi-site. Click **Generate certificates** and select **Generate certificates for all the sites of the multi-sites**.

ATTENTION : Some configurations to be made on the Web Admin side:

- The status of the "Encryption" licence must be "Authorised" on the iPBX.
- Check in Web Admin (Telephony service>System>Configuration >Alarms> Individualised configuration) that the alarms "PersLocAlm" and "IN ALARM" are not set to "NOT TRANS.".

7.4.8.11 Deleting a multi-site network

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

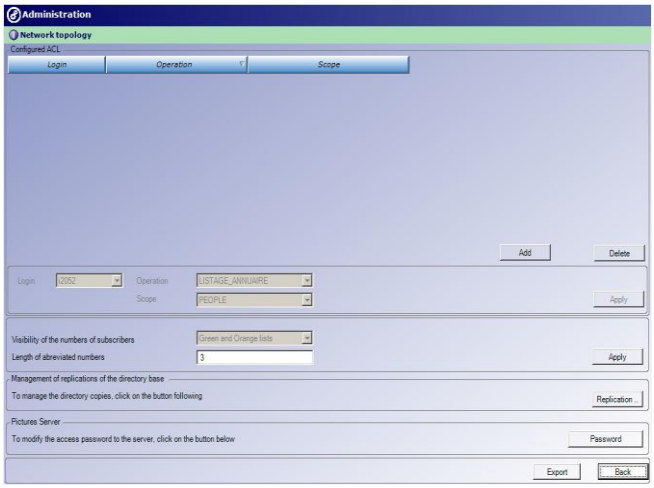
A confirmation request window opens. Click **OK** to confirm the deletion.

The multi-site configuration is deleted from the list of multi-site configurations accessible to the user. Deleting a multi-site configuration deletes the objects and subscribers (sites, voicemail systems) associated with it.

7.4.8.12 Configuring directory access rights

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

The following window is displayed.



This window allows you to configure external applications' access rights for the LDAP directory. A login is created for each application. These logins have already been defined in the **Configuration** part.

ACLs (Access Control Lists) are used to authenticate external applications (charging unit, hotel/motel applications) to the LDAP directory, and to receive filtered information (read/write rights and list of parameters) according to the configuration made.

To configure an access right:

- In the window, click the **Add** button located below the login list.
- The *Login definition* area is activated.
- Define the following parameters:

- **Login**: select the login to define.
- **Operation**: type of operation to which the login has access in the directory:
  - Directory_listing: the right to consult internal and external directory records.
  - Global listing: the right to consult all the directory parameters.
  - Directory modification: the right to modify the directory
  - Global management: no restrictions

- **Range**: LDAP directory branch accessible via the login.
  - People for internal subscribers
  - Contact for external records
  - People and contacts for internal and external records.
- After defining these parameters, click **Apply**.

The configured login is added to the list.

To delete an access right:

- Select a login from the list.
- Click **Delete**.
- Confirm the access right deletion by clicking **OK**.

The login is deleted from the list.

OTHER FIELDS

- **Visibility of subscriber numbers**: for defining the list of records accessible through subscriber search. Possible options: green list or green and orange list.
- **Abbreviated number length**: for defining the length (1 to 4 digits) of the abbreviated numbers used in subscriber and external record management (see Creating an external record).
- **Picture server**: for modifying the picture server access password (see the document Picture Management - Operating Manual).

To configure a directory replica:

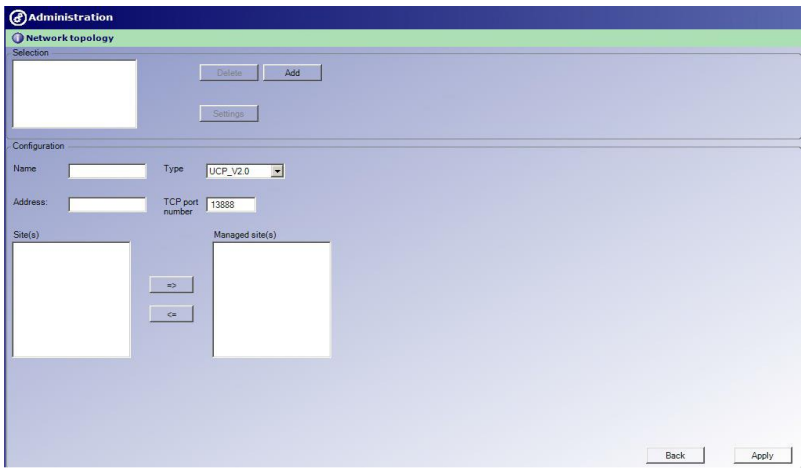
- Click **Replication**… to open the configuration window of LDAP database replicas managed by MiVoice 5000 Manager.
- Click **Add** to configure a new replica. Select the target site for the replica and enter the remote LDAP database password.
- Click **Validate** to start configuring the replica.

7.4.8.13 Configuring the messaging systems of a multi-site configuration

This window is used to assign voicemail systems (UCP) to sites on the selected multi-site configuration, and to configure connection parameters. Possible operations in this window are:

- Adding voicemail
- Modifying voicemail characteristics
- Deleting a voicemail system

In the configuration window, click **Voicemail**.



ADDING VOICEMAIL

- In the *Selection* area, click **Add**.
- Fill in the *Configuration* area fields as follows:
  - Name: voicemail name
  - Type: UCP version
  - Address: enter the voicemail server IP address
  - TCP port: enter the TCP port number
- To define the sites asociated with voicemail during creation, select the sites on the **Site(s)** list then click **=>** to move them to the **Managed site(s)** area (to remove the sites do the contrary).
- Click **Apply** to confirm.

The list of voicemail systems is updated.

MODIFYING A VOICEMAIL SYSTEM

- In the *Selection* area, click the voicemail system to modify.

  Its parameters are displayed in the configuration area.
- Modify the necessary fields then click **Apply** to **confirm**.

DELETING A VOICEMAIL SYSTEM

In the *Selection* area, select a voicemail system and click **Delete**.

The list of voicemail systems is updated. A confirmation message is displayed, and the operations log updated.

LISTING VOICEMAIL PARAMETERS

The settings button is used to update the parameters of voicemail systems managed on the multi-site. It is possible to recover the parameters and/or voicemail boxes declared on the UCP.

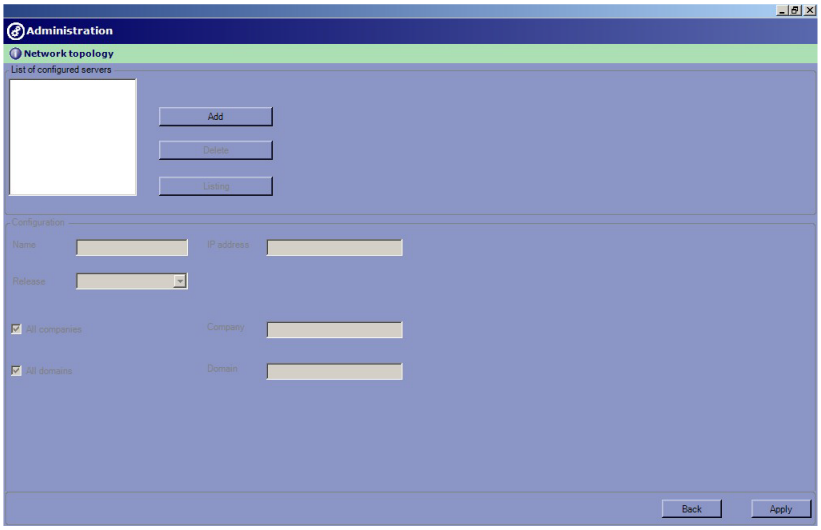
This listing is necessary to take new parameters (IMAP servers, box classes, etc.) created on the UCP into account when voicemail boxes are declared in MiVoice 5000 Manager.

7.4.8.14 TWP server configuration

This window is used to assign TWP servers to sites on the selected multi-site configuration, and to configure connection parameters. Possible operations in this window are:

- Add TWP servers
- Delete a TWP server
- List TWP servers

In the configuration window, click **TWP servers**.



TWP SERVER CONFIGURATION RULES

- Several TWP servers can be defined for a multi-site configuration.
- One TWP server may be shared by several multi-site configurations.
- A TWP server is defined by its IP address.
- One TWP server may be shared by several company/domain pairs.
- Users are defined on each IP address / company-domain pair.
- A phone number is unique in a company/domain.

NOTION OF (TWP) GROUP

- A TWP subscriber may belong to several groups.
- A TWP group is defined for one company/domain pair.
- The company/domain pair is the same for the TWP group and the subscribers it contains.

CONSTRAINTS

The management of a new TWP record for a (main) subscriber is only available:

- For R5.x sites minimum
- In TWP server 3.2 and later.

There is only one TWP subscriber number for the entire IP address / company-domain pairs defined for a multi-site configuration.

The TWP record is proposed for internal subscribers only.

ADDING A TWP SERVER

- In the List of configured servers area, click Add.
- Fill in the *Configuration* area fields as follows:
    - **Name**: server name. The name can be chosen freely and is not necessarily the name of the server hosting TWP.
    - **IP address**: enter the TWP server IP address.
    - **Version**: select the version of the TWP server used.
    - **Company**: Enter the name of the company in question or tick the **Any company** box if the TWP server is generally used.
    - Domain: Enter the name of the domain concerned or tick the **Any domain** box if all the domains are used.
- Click **Apply** to confirm.

The list of TWP servers is updated.

MODIFYING A VOICEMAIL SYSTEM

- In the *Selection* area, click the voicemail system to modify.

Its parameters are displayed in the configuration area.

- Modify the necessary fields then click **Apply** to **confirm**.

DELETING A TWP SERVER

In the **List of configured servers** area, select one TWP server then click **Delete**.

The list of TWP servers is updated. A confirmation message is displayed, and the operations log updated.

The TWP records will be deleted.

LISTING TWP SERVERS

- In the List of configured servers area, click List.
- Tick the box corresponding to the list type:
  - List of parameters (companies, domains, groups)
  - Full list (companies, domains, groups, and users)
- Click **Start** to start listing.

Accessing the TWP server from MiVoice 5000 Manager

On the TWP server, in the Global/Users menu of TWP Admin, create the administrator as follows so MiVoice 5000 Manager can connect to TWP:

- User name: m7450
- Password: m7450

The **Company** field must remain blank.

The **Superuser** box must be ticked.

Further configurations on the TWP server

Apart from the contents of the TWP record defined from MiVoice 5000 Manager, other fields are defined on the TWP server, but they will not be displayed in the TWP record data input:

- PC IP address: for forcing a login without using SSO
- User mail password
- PBX subscription password.

7.4.8.15 Identifying the sites

To manage the created sites, start a site identification operation. This button is used to manage the sites of the configured multi-site.

7.4.8.16 Generation

Generation allows iPBX data to be transferred to the management centre, and iPBX web MMIs to be locked at the end of the operation. The downloaded data will henceforth be managed by the management centre.

In case of serious system failure, this function may be used to realign information between the managed iPBXs and the management centre.

The downloaded data concerns:

- Site configuration
- Telephony parameters
- Number blocks
- ICGs
- Directory records
- Forwarding for R5.2 sites or later
- Keys

- The physical resources
- DECT cells
- Assignments
- Management mode
- The data for the TWP servers defined for the multi-site configuration (R5.x minimum) concerning companies, domains, groups and users.

Some data must be predefined on the iPBXs. The documents "MiVoice 5000 Manager - Installation and configuration" and "Integrated management portal operating manuals" give more information on this topic (see reference documents).

USING THE GENERATION FUNCTION

- In the configuration window, click **Generation**.
- After you have accepted the information message, a wizard window opens. An option allows you to import data from the LDAP directory, click **Import** to start the action.
- Otherwise, click **Next**.
- Before starting the generation procedure, the system must check the configuration of the reference site. Click **Read**.
- A notification is displayed at the end of the operation.
- The generation procedure starts with the downloading of the site configuration. Click **Configure** to run the procedure.
- At the end of the action, the wizard proposes to download the following data.
- For each data type, click **Start** to start the action then **Next** to download the next data.
- The last stage of the procedure (configuring the management mode) allows you to lock the iPBX MMIs on the downloaded data.

Note : In global or regional range configurations, the first generation made will use the parameters read on the reference site as reference for all future multi-sites. If these parameters are incorrect, in the region range, delete the region and restart the operation; in global range delete all the regions and restart the operation. So, you have to check the reference site configuration well before starting the generation operation.

7.4.9 IMPORTING MASSIVE REGION AND SITE CREATION FILES

It is possible, from the client application, to massively create regions and their sites. Before this, you must first enter an input file in Excel format, the content of which a macro changes to xml files.

The use of this function is described in the document *MiVoice 5000 Manager Installation Configuration.*

To import regions and sites:

- From the MiVoice 5000 Manager portal, click the link To import the list of regions and sites.
- Enter the required administrator password (M7450/M7450 by default).
- An HTML page ImportSite opens.
- Select the region and/or site file to import, using the **Browse** button then click **Load**.

7.5 SITE IDENTIFICATION

This screen displays all the sites created but which are not yet operational. To make a site operational, run an identification.

- In the Administration menu, click Site identification.
- Select a region.
- Click the site(s)/node(s) to be identify to display it/them on a yellow background (select several items using the Maj or Ctrl keys).
- Click Start identification.

An operation report appears and is saved in the Operations log.

If the connection fails, check the site identity data (connection type, IP address, etc.) and correct it.

When the site is identified, it then becomes possible to run an inventory (see the section Inventory), and to add it to a list of sites and then perform any action on this site.

7.6 SITE LIST MANAGEMENT

This function is used to create, modify and manage lists of sites per region. A list can be used to execute actions on the logs, alarms, inventories, charge ticket or directory downloads, as well as the iPBX backups defined on the list.

Note : A list of sites is automatically created and assigned to each multi-site configuration managed by MiVoice 5000 Manager. The name of this list is that of the multi-site. It contains all the sites on the multi-sites (updated automatically according to the sites added or deleted on the multi-site). This list allows a multi-site based display in some screens such as inventory, logbooks and alarm logs.

7.6.1 ADDING A SITE LIST

A list of sites can be created in two ways:

- Through the application
- By importing an external file

7.6.1.1 Creating a list through the application

A list of sites can be created in the application as follows:

- Select a region from the **Regions** drop-down list.
- The existing lists for the selected region appear in the **Lists** display zone.
- Click **New list**.

- A dialogue box appears, allowing you to create a list or to import a list file.
- In the **Create a list** zone, enter the name of the list.
- Click **OK**.

The action is taken into account by the portal. Click **OK**. The list of sites appears in the **List name** screen area.

7.6.1.2 Importing lists

New lists are added by importing .txt files from the user PC. Proceed as follows to add a new list of sites.

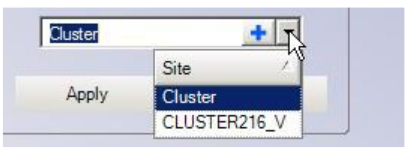
- Check that the file is in .txt format and is located on the PC.
- This file must contain a line per iPBX name, followed by a carriage return (line return). The list will bear the name of the imported file.
- Select a region from the **Regions** drop-down list.
- The existing lists for the selected region appear in the **Lists** display zone.
- Click **New list**.
- A dialogue box appears, allowing you to create a list or to import a list file.
- In the "Import one or more lists" area, click Import.
- A navigation window enables you to select the file on the PC.
- Select the .txt file containing the list of sites and click **Open**.

The iPBXs contained in the list of sites appear in the **Sites** display area.

7.6.2 MODIFYING A SITE LIST

- Select a region from the **Regions** drop-down list.
- The existing lists for the selected region appear in the **Lists** display zone.
- Select the list be modified.
- Click **Modify**.
- Modify using any of the following methods:
  - In the Sites display area which has become is an input zone, enter the modification directly (add, modify, delete a site name). A syntax check is done regarding the sites identified in the region.
  - Select a site using the drop-down list located under the Site area. Click  sign to add the selected iPBX to the list.
- Click **Apply** to confirm the modification.

To delete the modifications made and reset the list, click Cancel.



7.6.3 DELETING A SITE LIST

- Select a region from the **Regions** drop-down list.
- The existing lists for the selected region appear in the **List of sites** display zone.

- Select the list to delete.
- Click **Delete**.
- Answer **YES** when asked whether you really wish to delete the list.

The list is deleted and no longer appears on the list of sites.

7.6.4 PRINTING A SITE LIST

- Select a region from the **Regions** drop-down list.
- The existing lists for the selected region appear in the **List of sites** display zone.
- Select the list to print.
- Click **Print**.

The print request is sent to the PC printer.

Note : A list of sites is automatically created and assigned to each multi-site configuration managed by MiVoice 5000 Manager. The name of this list is that of the multi-site. It contains all the sites on the multi-sites (updated automatically according to the sites added or deleted on the multi-site). This list allows a multi-site based display in some screens such as inventory, logbooks and alarm logs.

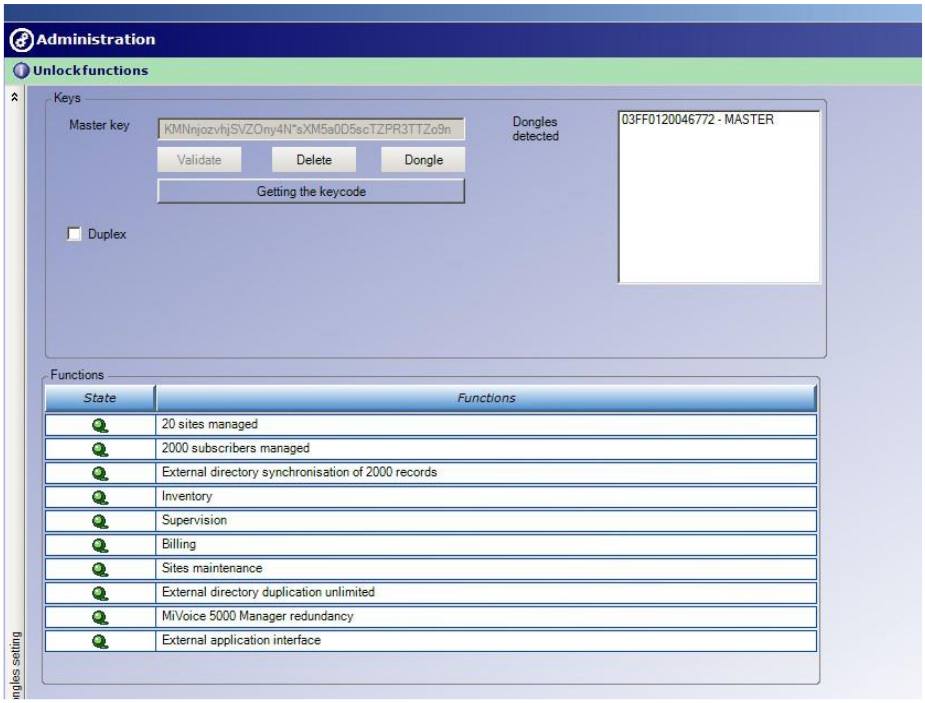
7.7 UNLOCK FUNCTIONS

(RESERVED FOR THE ADMINISTRATOR)

This menu is used to enter the software key code to unlock the functions.

A single key can be used to unlock all the functions.

- In the **Administration** list, click **Unlock functions**.



Tick the **Duplex** option to enter an activation key used to duplicate the management centre.

Note : The key entered for DUPLEX mode can only be checked on the main MiVoice 5000 Manager server. Therefore, it is not advisable to force a switchover in order to check the working of the secondary MiVoice 5000 Manager server and the validity of the DUPLEX key.

7.7.1 UNLOCKING THROUGH A USB DONGLE

- Enter the key number then click **Validate**.

The **Available dongles** area displays the dongle numbers available on the server.

7.7.2 UNLOCKING THROUGH A LOGICAL DONGLE

This type of locking is described in the document **MiVoice 5000 Manager - Installation and configuration**. When the licence is about to expire, a message is sent to the operations log. If the licence is renewed, a new key can then be retrieved by clicking **Obtain key code**.

7.8 PREFERENCES

This function enables a user to modify the password assigned by the administrator, and to modify it again each time it becomes necessary.

It is also used to choose the ergonomics.

To change the password:

- In the **Administration** list, click **Preferences**.
- Click **Modify password**.
- In the input window, enter:
  - The old password
  - The new password
  - Then the new password again to confirm.
- Validate the input by clicking **OK**.

To close without saving the new password, click Cancel.

To change the preference options, tick or untick:

- **Deactivate notification window**: when the box is ticked, the notification pop-up no longer appears at each new event
- **Deactivate alarm window**: this option is used to deactivate / reactivate alarm window display. Refer to the section Alarms**.**
- **Full screen mode**: this option is used to display the application window in full screen mode. The application will retain this display mode for the next connection.

Validate the options chosen by clicking **Apply** then click **OK** to confirm.

Note : You can access this screen directly, no matter your location in the application, by clicking the username in the menu bar on the left side of the screen.

8 CONSULTATIONS

8.1 OPERATIONS LOG

This menu is used to view the entire MiVoice 5000 Manager application log and also includes the security log (Login/Logout).

The amount of information contained in this log depends on the purging periods defined by the administrator in the **Configuration** menu. This log displays the same information as the circular log (see the section

The operation log window).

Operations logs can be sent to one or two remote Syslog servers. See the section

Parameters.

8.1.1 DEFINING DISPLAY CRITERIA

To define the selection criteria:

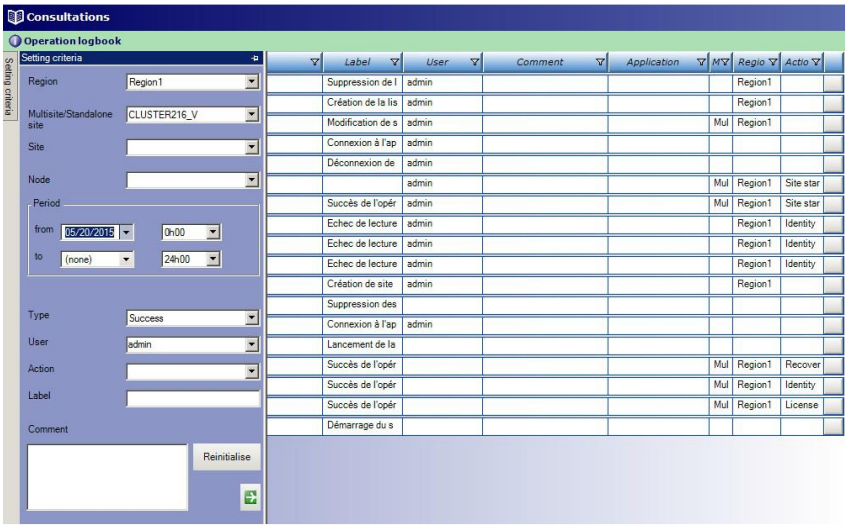
- In the **Operation log** window, click the vertical ***Setting criteria*** tab located on the top left side of the operation log.

A criteria selection panel appears.

Note : Click the drawing pin symbol on the top right side to fix the window.

- If necessary, click **Reinitialize** to reset all the input areas.
- Select the selection criteria from those proposed in the drop-down lists.
- If required, fill in the **Label** and **Comment** areas to select the recordings corresponding to the content of these fields in the operation log.
- Click on the arrow  to validate the selection.

After the selection result is displayed, other selections are possible on the columns with the symbol 
.



8.1.2 PRINTING THE OPERATION LOG

The **Print** button is used to print the operation log on the PC printer.

- Click **Print**.
- A display window opens.
- If necessary, define the print format (one or more pages per sheet).
- Click the printer symbol to start printing.

8.1.3 EXPORTING THE OPERATION LOG

The **Export** button is used to copy the data displayed on the screen to an Excel file.

- Click the **Export** button.
- In the Windows **Save As** window, define the directory to which the file must be copied.
- Enter the name and type of file.
- Click **Save** .

The file is available for another application.

8.2 CAMPAIGN RESULT:

This function is the same as the one contained in the **Campaigns** menu (see the section Managing campaigns).

8.3 ABOUT MIVOICE 5000 MANAGER...

This welcome window appears when the MiVoice 5000 Manager application is opened. It presents the functions managed by the system and the following information:

- The installed product release
- The total number of sites and regions
- The number of users
- The unlocked functions
- The number of managed subscribers.

9 NETWORK SUPERVISION

9.1 DESCRIPTION OF SUPERVISION

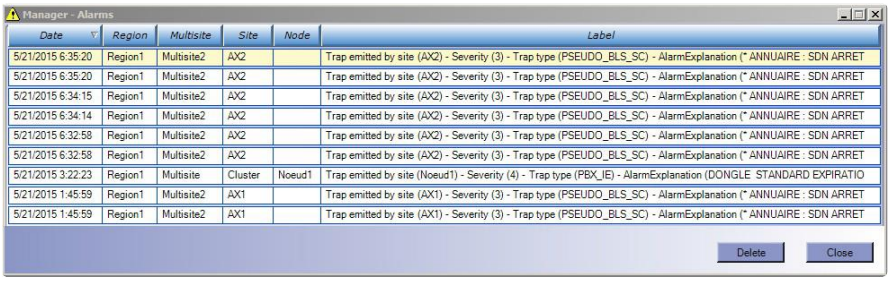
The supervision services brought in MiVoice 5000 Manager management centre are:

- A list of all the alarms by site, or a list of sites from the Immediate actions menu
- Alarm notification on the client terminal in form of an alarm window
- Sending the collected alarms by e-mail or to an external device (alarm box)
- A log of alarms from external devices
- Providing an SNMP supervisor with map (Nagvis)

9.2 ALARM WINDOW

This window opens in the foreground only for alarms with a severity level above the one defined in Menu **Configuration/Filter** to E-mail or external device tab, regardless of whether the alarms come from standalone sites or from external devices.

Note : This alarm window may be deactivated or activated in the Preferences menu (direct access by clicking the operator name preceded by a star).



The **Delete** button is used to delete a selected alarm line from the display window. The event is, however, preserved in the MiVoice 5000 Manager database.

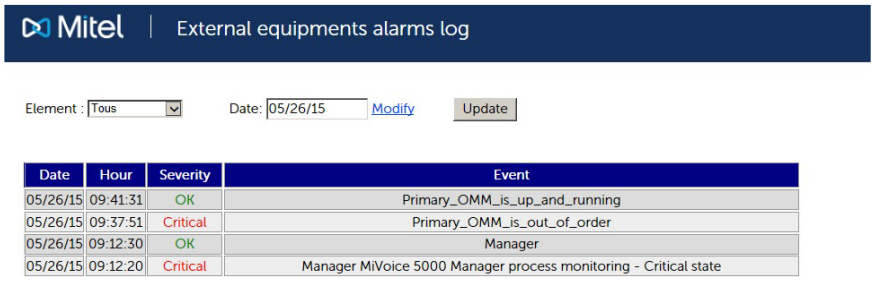
The **Close** button is used to close this window. This will be reopened during the next alarm.

9.3 ALARMS ON EXTERNAL DEVICES

To open the alarm log of external devices:

- Open the **Network supervision** menu.
- Click **Alarms on external devices**.
- Enter the operator password.

The log opens. Here is an example of the alarm logs of external devices:



Date	Hour	Severity	Event
05/26/15	09:41:31	OK	Primary_OMM_is_up_and_running
05/26/15	09:37:51	Critical	Primary_OMM_is_out_of_order
05/26/15	09:12:30	OK	Manager
05/26/15	09:12:20	Critical	Manager MiVoice 5000 Manager process monitoring - Critical state

It is possible to select one item or to display all. These items are configured in the Administration menu of the MiVoice 5000 Manager portal. It is necessary to carry out some settings in MiVoice 5000 Manager. Refer to Section Filtering tab.

The log displays the alarm of the day. To display earlier dates, click **Modify**.

To refresh the window, click **Actualise**.

9.4 THE MAP APPLICATION NAGVIS

Supervision is displayed by the Nagvis application.

To run Nagvis:

- Open the **Network supervision** menu.
- Click **Map**.
- Enter the operator password.

The supervision application starts and this type of window opens.

On top, a menu bar allows you to customise the application (see the section Application menus).
The Nagvis application manages the user rights in such a way that only the multi-sites managed by the user appear.

9.4.1 DESCRIPTION

Each network item is created automatically:

- When the item is created in the Administration/Network topology menu (see Network topology)
- When the external devices are configured (MiVoice 5000 Manager portal administration menu - To configure external devices).
- No matter the card displayed:
- Placing the cursor over an item displays the information about this item.
- Left-clicking an item displays the lower level map (except hardware).

To return to an upper level, click the green arrow on the top left side. To return to the general network view, click the House icon.

Each item contains a colour signal reflecting its status. A round one represents the status of a service, while a square one represents the hardware status.

9.4.2 NETWORK VIEW

The highest level of display shows all the regions managed by the management centre. The view of the map varies according to user rights.

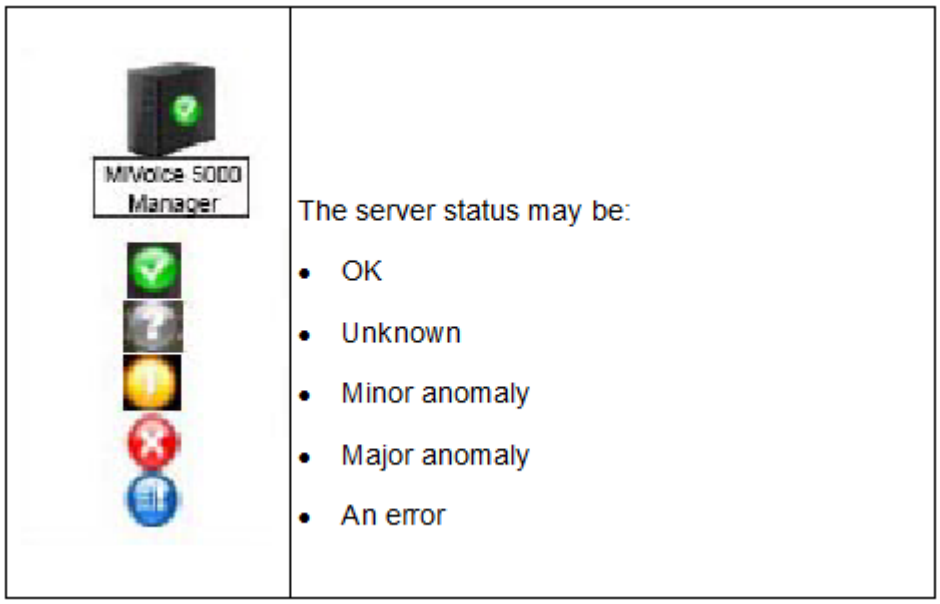
It comprises the following items:

- The management centre
- The regions
- Possibly, the external devices; see the section External devices on the map**.**

The tree of a region can be displayed by clicking the corresponding item. The cards for the multi-sites/sites, clusters and their nodes are thus displayed.

9.4.2.2 *The management centre*

On the map it is represented by the following symbol, accompanied by its status. It represents the service status; there is no hardware status:



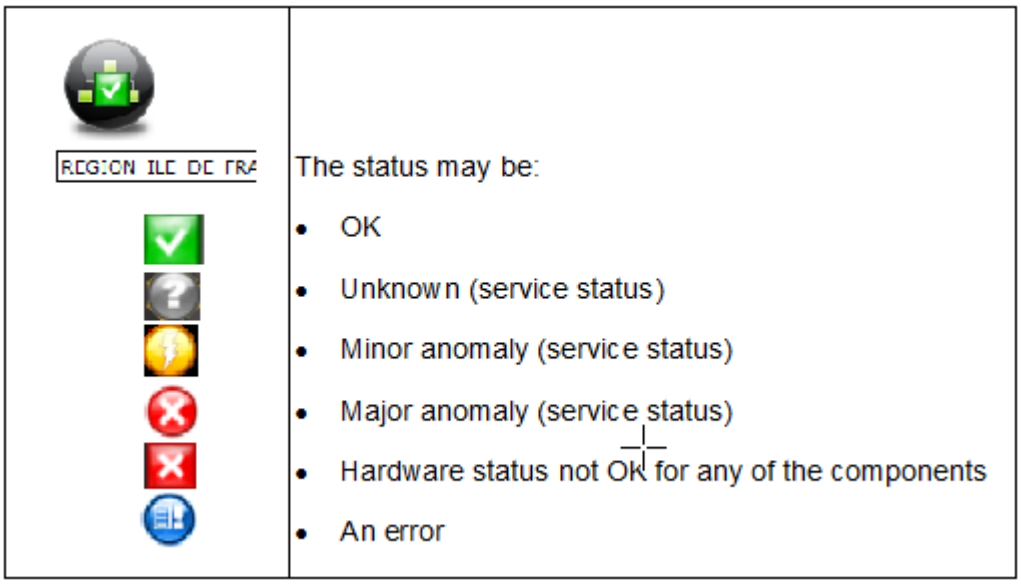
Placing the cursor over the MiVoice 5000 Manager symbol displays its characteristics as well as the status of the different associated services:

The associated services are:

- DISK: checks the disk space of the server's "/" directory
- LOAD: checks the processor load
- LDAP: checks the presence of the "slapd" process
- PORTAL: checks the presence of the "7450Portal.exe" process
- TRAPD: checks the presence of the "snmptrapd" process

9.4.2.3 *The regions*

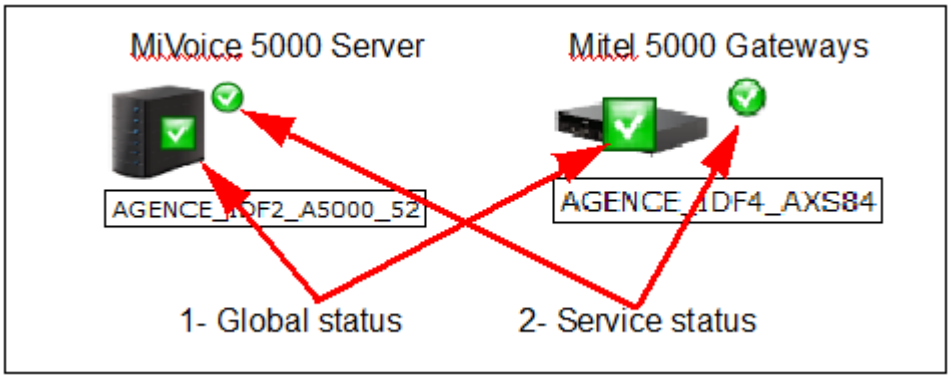
On the map the regions are represented by the following symbol, accompanied by its status. This status is consolidated by its different components:



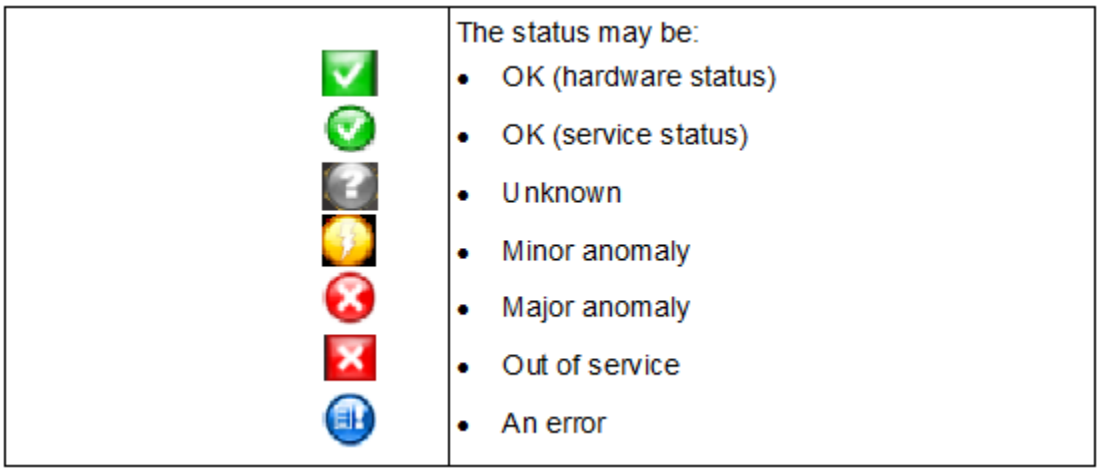
- Place the cursor over the symbol to display the list of items that make up the region.
- Click the symbol of a region to display its map.

9.4.2.4 *Isolated sites*

A site is represented by any of the following symbols:



accompanied by its status:



Site supervision allows access to the following information:

Placing the cursor over the symbol 1- opens a global status window (hardware status + software status).

- Left-clicking the Global status symbol opens a menu equivalent to the Web Admin menu **System> Supervision>Display status>Maintenance> Maintenance status** representing the hardware status.
- Right-clicking the **Global status** symbol opens an **Update statuses** window. This option is used to refresh the map.

Placing the cursor over the symbol 2- opens a service status window.

- Left-clicking the service status opens a Nagios window.

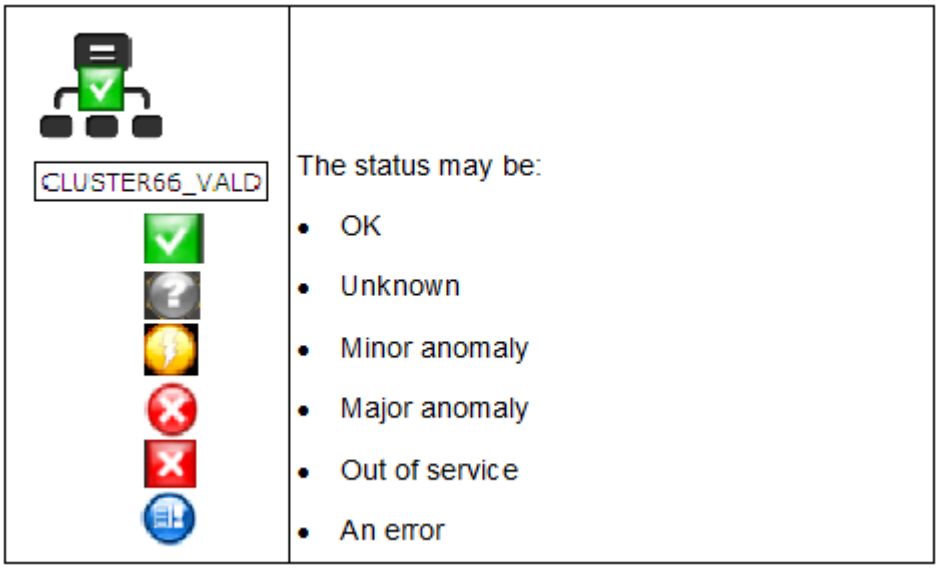
9.4.2.5 *Multi-sites*

From the map of a region, click a multi-site (same symbol as the region) to display its map. The status displayed is a consolidated status of the site statuses.

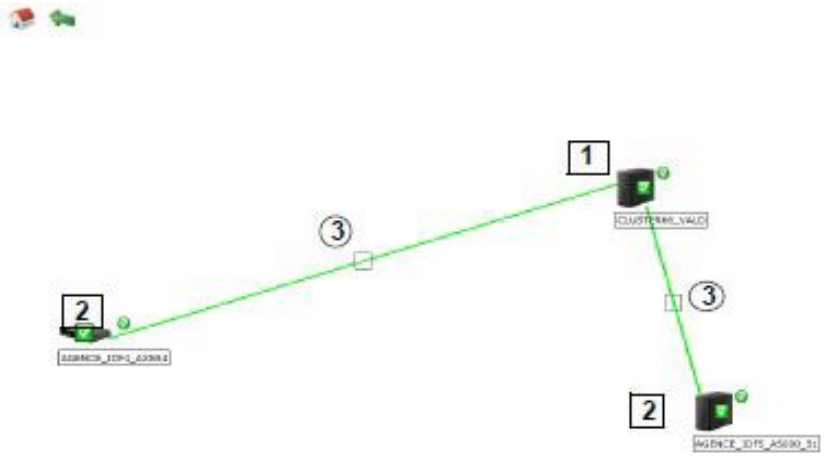
The multi-site is made up of sites or clusters.

9.4.2.6 Clusters

A cluster is represented by the following symbol, accompanied by its status. This is the consolidated status of the cluster server, nodes and links:



- Place the cursor over the cluster to display its components.



- Click the cluster to open the supervision map.
- The map shows:
  - The cluster server with its two information windows (hardware and services)
  - The nodes with the two information windows (hardware and services)

Note : The information provided by the application is the same as the information given in the section Isolated sites.

- The links between the cluster and nodes:
- The colour of the line varies according to the line status.

Placing the cursor over the square displays the service status.

Clicking the square opens the Nagios window.

9.4.3 APPLICATION MENUS

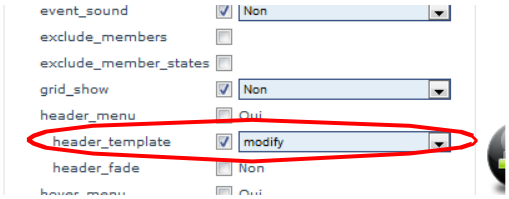
The menu bar proposes the following menus:

- Edit map - reserved for the administrator
- Options - reserved for the administrator
- Personal menu
- Choose a language

9.4.3.1 Edit map

ATTENTION : It is risky to modify this map. If the items are moved and there is a change in the topology, map personalisation is not taken into account for placing the new item. Different items can thus be superimposed.

By default, the **Edit map** menu only contains the **Map options** submenu. To display the other edit options, open this submenu and select the parameter "Header-template", applying the parameter "Modify" to it:



Click Backup to confirm the modification. The Edit map menu displays the submenus.

Lock/unlock all: this option is used to change to edit mode and to move the different items displayed, in order to arrange them at wish. The **Edit Mode!** label is then displayed in red on the menu line.

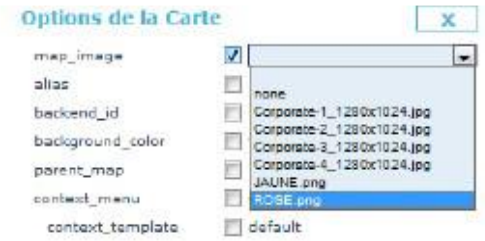
After putting these items in place, click the option again to exit the edit menu and view the characteristics of the map components.

Display/hide grid: displaying the grid allows the different items to be aligned.

Card options:

ATTENTION : any modification must be validated by clicking the Backup button at the bottom of the list.

- To select a screen background (see the section Options), click map_image then select the screen background from the dropdown list that opens:



9.4.3.2 Options

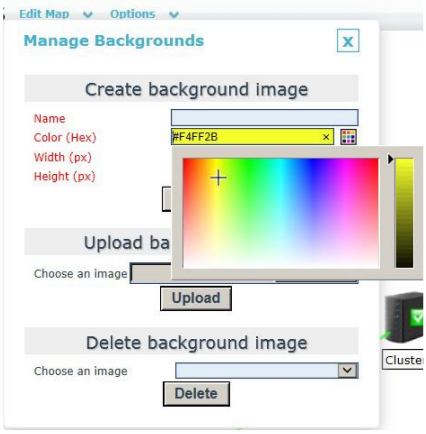
The option **Manage map background** is used to create colour backgrounds, import some images used in the map background, and delete existing map backgrounds.

The map background is taken into account on each map in Menu **Edit map > Map options**.

CREATE MAP BACKGROUND:

This option is used to differentiate, for instance, the colour of the maps.

- Open Menu **Options > Manage map backgrounds**.
- Enter the name of the map background to create.
- Choose the map background colour.
- Enter the width and height according to the size of the screen.
- Click **Create**.



IMPORT MAP BACKGROUND

This option is used to download an image or picture saved on the PC.

DELETE MAP BACKGROUND

From the list of map backgrounds select the one to delete then click **Delete**.

ATTENTION : It is not possible to delete a map background used on a map. It must first be disabled on the map.

9.4.4 EXTERNAL DEVICES ON THE MAP

The external devices must be represented on the network map by a "Devices" symbol. It is automatically created while creating the first external device to be monitored (Menu MiVoice 5000 Manager portal administration menu - To configure external devices).

- Placing the cursor over the hardware displays the hardware status.
- Moreover, placing the cursor over the service icon (on the right side of the hardware) displays the status of these services.
- Clicking a device opens the alarm log for this device.
- During their configuration, the external devices can be defined in different ways:
- Application (TWP, CC, UCP, AMC)
- Generic device (PC, printer)
- Generic server (non-Mitel application).

Here is an example of external device display:

Supervising Mitel applications requires the presence of the component NRPE. This component can be downloaded from the MiVoice 5000 Manager portal - Menu **Others**.

The supervised services are:

- DISK: checks the disk space of all drives
- LOAD: checks the processor load
- MEM: monitors the memory
- Depending on the device, some additional services can be supervised.

PART II:
TELEPHONY MANAGEMENT

10 TELEPHONY

MiVoice 5000 Manager contains a telephony management module used to define and manage directory data, telephony parameters and subscriptions.

Telephony management is shown in a separate window. Operators with a telephony profile only have access to this window. Operators with an Administrator or Operator profile access the subscriber management application by clicking Menu **Telephony** from MiVoice 5000 Manager.

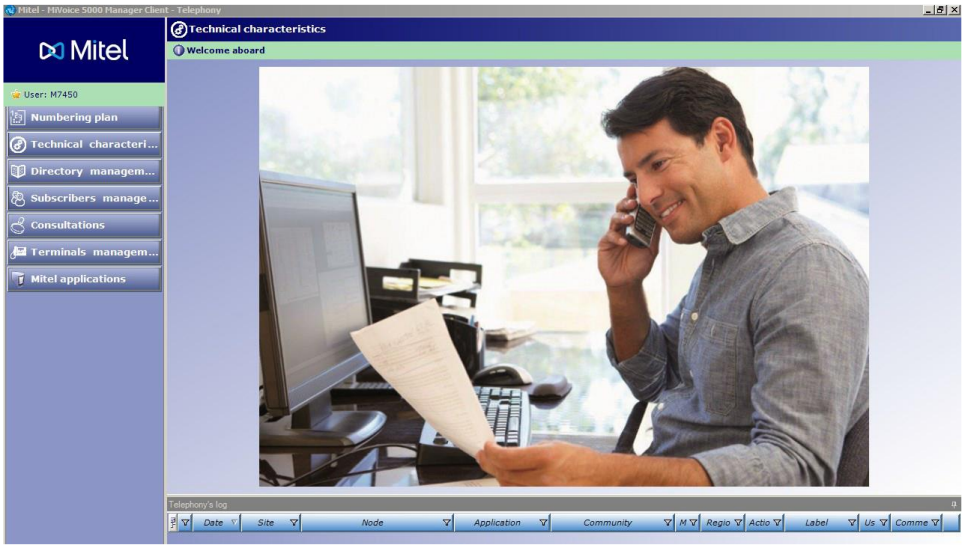
Note : This module applies to MiVoice 5000, XS, XL, XD iPBXs as of system release R5.1.

10.1 DESCRIPTION OF THE INTERFACE

The Telephony window comprises three areas:

- A left column with a list of Telephony window menus
- An upper right area for a screen background
- A lower right area with telephony operations log. This area is available by default, but it may be hidden or resized.

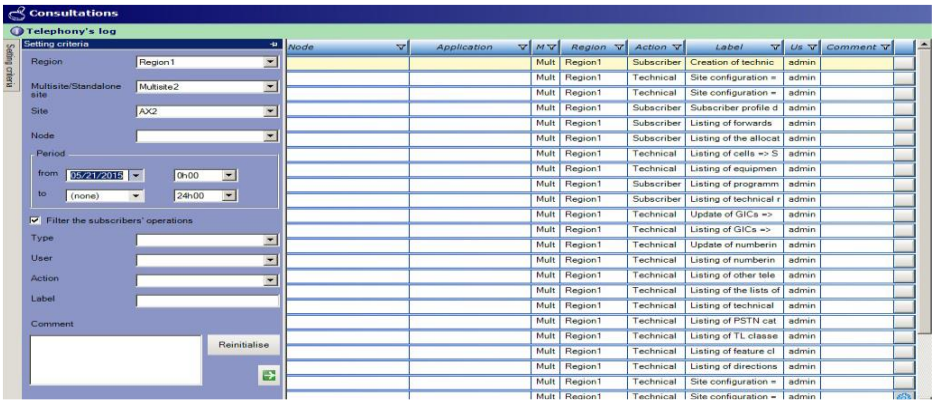
Depending on the user's need, the window or each of the three areas may be resized like any Windows window.



10.3 TELEPHONY LOG

A telephony log is available by default. It only displays telephony management operations. Its window may be opened or minimised.

The telephony operation log window displays a circular log of the last 75 telephony management operations. When new events are available in the log, the user is informed about it.



MASKING THE TELEPHONY LOG WINDOW

The telephony log window can be masked.

- Click the drawing pin symbol on the top right of the operation log.

The log window disappears and is replaced by a *Telephony's log* tab. The window will reappear temporarily each time the cursor is placed on the tab.

- To fix the log window, click again on the symbol when the log is displayed.

MASKING/DISPLAYING THE COLUMNS

It is possible to select the columns that must appear in the log window.

- Click on the column selector .
- The log configuration window is opens. This window allows you to select the fields that will appear in form of columns.
- Tick to select the fields to display in the window. Untick them to hide them.
- Click on the cross to close the column selection window.

Note : A column can also be removed from the display by pulling the column header outside the log display zone. To display it, use the column selector.

MOVING COLUMNS

The columns can be moved in order to reorganise the window display.

- Select the header of the column to move.
- This is surrounded by an orange column.
- Press and hold down the left mouse button, then move the column horizontally to the area you want.
- Two red arrows allow you to view the target destination.
- At the target destination, release the mouse button. The column is moved.

Note : This movement of columns is possible for all the application tables.

SELECT A LINE

To select a line, click the  symbol located at the beginning of the line. The line appears on a yellow background.

Note : Clicking on an end-of-processing notification displays the line concerning the completed event on a yellow background.

MOVING AND RESIZING THE TELEPHONY LOG WINDOW

You can move the operation log window to any part of the screen. To move the window:

- Select the window through the *Telephony log's* title bar.
- Press and hold down the left mouse button then move the window.

In the moving process, a grey line shows the target destination of the window when the mouse button is released.

- Resize the window as you wish, like any Windows window.

The previous size and location are stored in the memory. To return to the previous size and location, double-click the title bar. This action can be repeated and be used, for example, to increase and reduce the size of the window.

FILTERING LOG INFORMATION

Some telephony operation log columns propose a filter menu (see figure).

- Click on the Filter icon of the column to filter.
- A drop-down menu is displayed, proposing the values chosen for the filtering operation. These values depend on the values displayed in the log during the filter request and may change according to the values displayed.
- Select one filter option from those proposed.

Filtering is immediate, and the Filter icon turns blue to indicate that filtering exists on this field.

RESULT OF AN OPERATION

The result of an operation is indicated by a symbol. The table below gives the meaning of the symbols:

OPERATION RESULT	MEANING OF THE ASSOCIATED SYMBOL
	Operation successful.
	Operation not successful.
	Information about a configuration modification
	Caution: event to be checked

ENTERING A COMMENT

You can use the comment field to make comments about telephony log events. Information entered in this field is recorded in the operation log, accessible from the **Consultation** action group and can be used for customised sorting.

SHORTCUTS

You can use these shortcuts to:

-  Open a file associated with an event, such as an inventory, a log or alarms.
-  Re-submit an unsuccessful event. The action will be identical: to modify the parameters, it is necessary to redefine the action.

ACTION REPORTS

When an action is completed, a notification appears on a pop-up screen. The action is recorded in the operation log.

You can display this action in the log window in two ways:

- Click **New notification** in the notification window as long as it is visible. This action updates the log window and the action appears on a yellow background.
- If the pop-up screen is no longer displayed, bring up the scrollbar cursor to the right of the screen to display this action (it does not appear on the yellow background).

10.4 SELECTING A REGION / MULTISITE

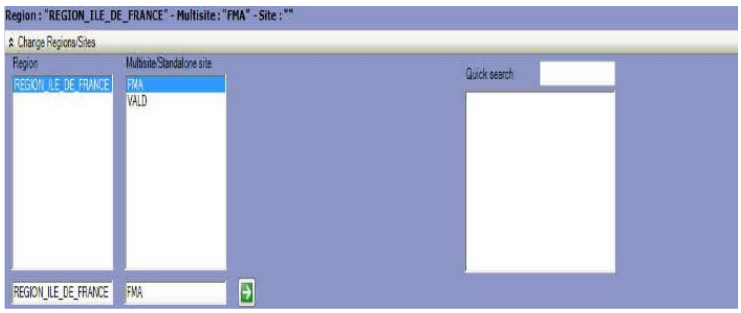
Before starting an action, it is necessary to define an action area.

A window used to define this area is available in most of the menus. This window can be displayed or minimised using the ⩔ / ⩓ symbol of the **Change region/sites** title bar. It is used to select a region, a multi-site configuration or a standalone site to which the action will apply.

Since the selection procedure is the same for all the application screens, it is explained in this section, and forwarding shall be performed in the menus in which it will be required.

To select an action area:

- If necessary, click the double arrow ⩔ on the *Change region/Sites* title bar to display the selection window below.



The regions, multi-site configurations / standalone sites appear in their respective areas.

- Click a region, multi-site / standalone site to select them.

The selected items are displayed in the areas at the bottom of the list.

Note : If the number of regions and sites is too long, enter the first letter(s) of the name in the search area. The cursor will automatically be placed on the first name containing the character string entered in the search zone.

- Click on the green arrow  .

The selected action area is displayed above the **Change region/system** title bar and the selection made remains valid until the next modification.

11 NUMBERING PLAN

This menu is used to display the number blocks defined on the iPBXs and manage a number database.

The number blocks are not managed directly by the management centre; they are obtained through listing on each iPBX. The list of number blocks enables the management centre to determine the available blocks and create subscriptions with directory numbers that are consistent with the numbering plan.

There are two DID number management modes:

- The management mode in the technical records
- The management mode in the directory.

This document describes the DID number management mode in the technical records. The DID number management mode in the directory is described in the document Managing DID numbers in the directory characteristics.

11.1 PRESENTATION OF NUMBER MANAGEMENT

Number management functions are:

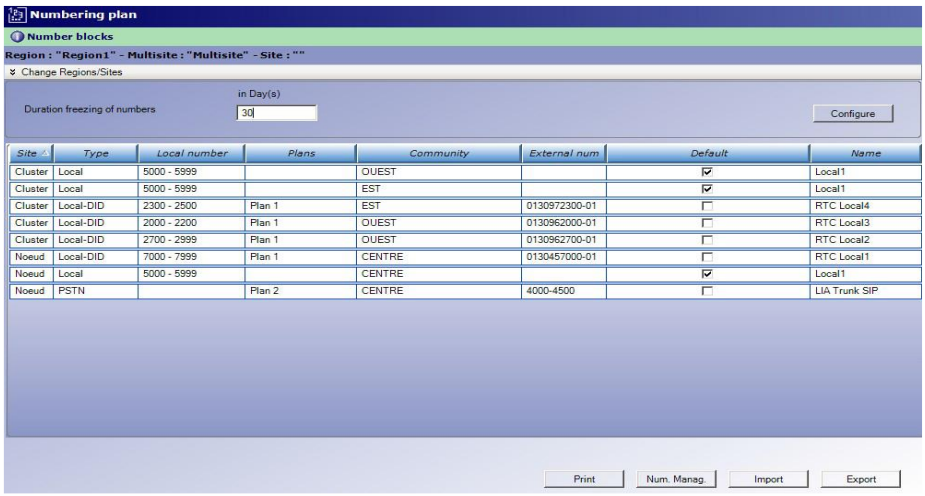
- Viewing the telephone number blocks defined on the network iPBXs
- Reserving, freezing, and releasing telephone numbers

11.2 VIEWING NUMBER BLOCKS

To view the number block list:

- In the **Telephony** window, click **Numbering plan** then **Numbering range**.
- If required, select a region / multi-site configuration.
- The list of number blocks is displayed.

If necessary, click the **List** button to start a list action manually and update the list.



The characteristics of a number block are:

- **Site**: name of the site on which the number block is declared.
- **Type of plan** (internal, PSTN, TL): for distinguishing between PSTN blocks (public numbers), internal blocks (non-DID) and TL blocks (additional numbers on TL).
- **Internal dialling**: internal number block (non-DID).

- **Plans**: number of the internal plan used. This parameter is used to avoid configuring the plan for each subscriber.
- **DID name**: name given to the DID number block.
- **External numbers**: additional numbers which can be associated with internal numbers. This parameter is used to automatically assign an additional DID number to an internal (non-DID) number during internal number configuration. This number may be in E164 format if the prefixes have been set to the new multi-site topology.
- **Public numbers**: numbers that can be dialled on the external network (PSTN or TL) to reach an internal subscriber.
- **Length**: corresponds to the number block range.

11.3 NUMBER MANAGEMENT

Number management is for managing numbers according to their status:

- **Free**: unassigned number
- **Assigned**: number used in a directory record or telephony subscription
- **Frozen**: number kept unavailable during a freeze period (configurable). This status prevents a number from being re-assigned immediately after the directory record is deleted.
- **Reserved**: number kept unavailable by the user to prevent it from being assigned.

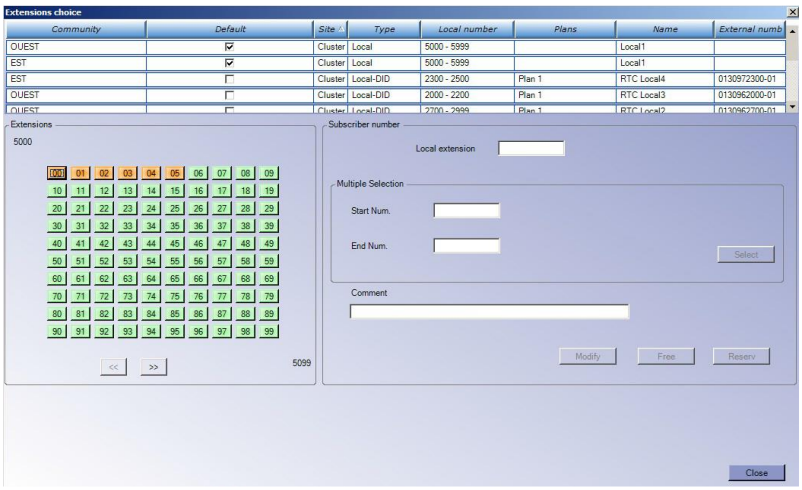
This management is based on the knowledge of the number blocks declared in each managed site.

11.3.1 ACCESSING NUMBER MANAGEMENT

In the **Telephony** window, click **Numbering plan** then **Numbering range**.

- If required, select a region / multi-site configuration.
- Click the **Number Management** button located at the bottom of the table.

The number management window opens.



This window comprises:

- A grid showing the status of the numbers by colour (green: free / red: assigned / orange: reserved). The numbers are presented on the grid by blocks of 100 numbers. Use the buttons << and >> to display the other grids.
- One number status configuration area.

11.3.2 CONFIGURING THE STATUS OF NUMBER BLOCKS

Selecting a number

Click a number in the number grid or enter the number directly in the *Local extension* area.

Selecting a number block

In the *Multiple selection* area, enter the following information:

- **Start Num.** : 1st number on the block
- **End num.**: last number on the block

Click Select to confirm the input.

Reserving a number

Select a number or number block, then click **Reserve**.

The reserved numbers appear in orange on the grid.

Releasing a number

Select a number or number block, then click **Free**.

The released numbers appear again in green on the grid.

Configuring the default number freeze duration

In the number range display window, enter the value (in days) of the freeze duration in the area specified then click **Configure**.

Updating a number

Select a number or number block, then click **Update**.

12 TECHNICAL CHARACTERISTICS

This menu is used to configure the telephony parameters used to manage subscribers. It contains the following parameters:

- Feature classes
- PSTN categories
- TL classes
- Technical hierarchy
- ICG (Interconnection group)
- Partitioning classes
- Priority classes
- Other characteristics.
- White plan

The management centre does not manage all these parameters; some of them are managed on the iPBX and are only proposed on the list. Only the parameters managed by the management centre are broadcast homogeneously over the entire network or part of the network.

12.1 PRESENTATION OF THE TELEPHONE PARAMETERS

Telephony parameters are **descriptions of rights or restrictions** used to define the **characteristics** of a telephone subscriber. They define a subscriber's rights for outgoing and incoming calls and are used by the iPBX switching software.

Defining the telephony parameters on the management centre helps the user manage a telephone subscriber because the parameters are presented to the user in form of a list.

Depending on the range defined in the Administration menu (see the section Site identification, the telephony parameters may apply to a multi-site configuration, a region or the entire network.

Note : If the defined range is global, the region/site selection window is inaccessible.

12.1.1 MANAGED PARAMETERS

The following parameters are managed by the management centre

- Feature classes
- PSTN categories
- TL classes
- Partition classes
- Priority classes
- Technical hierarchy

Creation, modification and deletion operations are possible on these parameters from the management centre. Their transmission is homogeneous on part of or the entire network, depending on the range defined.

12.1.2 PARAMETERS NOT MANAGED

The following parameters are not managed by the management centre and are only proposed as a list:

- ICGs
- Other parameters: written language, spoken language, voicemail box, etc.

These parameters are defined on the iPBXs.

12.2 MANAGING FEATURE CLASSES

A feature class determines all the features and operations a subscriber may use or perform on the equipment (example: appointment reminders, forwarding, etc.).

The classes are identified by their name and a category number between 0 and 63.

12.2.1 DEFINITION OF FEATURES

The list of features below is given for information purpose only and may vary according to iPBX release.

FEATURE	DEFINITION
Access to paging	Right given to a user with a pager to be called via a paging system.
Privileged extension	The user may call the attendant console before other sets on the internal calls queue.
Pick-up protection override	The user may intercept all calls to all other sets, including calls to sets with a pick up protection feature.
Locking allowed	The user may lock his or her set. In this case, certain functions (including external calls, set programming, and personal abbreviated dialling) require the use of a secret code.
Unlocking allowed	The user may unlock his or her set by entering a secret code. Otherwise, the set remains locked.
Mobile recording allowed	The user may register his or her handset.
Pick-up protection	The user may protect his or her set against pick-up, including through programmed intercom key. In this case, pick up is only possible for users with "protection override" right. pick-up".
Night category override	Right given to the user to override his/her night service category using his/her secret code: for this call, the terminal is switched to day service category (secret code = password).
Call forwarding protection	The extension is protected against all types of forwarding.
Dynamic protection	Protects the user throughout a conversation against a busy override or from call waiting (protection activated by feature code).

Do Not Disturb (DND)	The user may use the Do Not Disturb feature (MUTE message on digital sets).
Intrusion allowed	The user may execute a busy override procedure (OFFER) on another set in busy status 1 (the other set must not have a call waiting).
Intrusion accepted	Right given to a user to accept third-party intrusion on a call.
Conference master	The user has the right to set up a conference call then add or exclude participants using a digital set with an interactive keypad.
Encryption authorised	If this box is ticked, call encryption will be applied to this user.
Pre-emptive rerouting to voice mail	If forwarding is set up from a user's set to another set, which is itself forwarded to voice mail, this right enables the user to redirect incoming calls to his/her own voice mail box rather than to the voice mail box of the set on which his/her extension is forwarded.
Use DISA function	Possibility to set up calls and program features from an external call.
Call waiting	Indicates the way in which an incoming call is handled when the user is busy. **- Accept and Beep**: normal procedure: the call is placed on hold, and the user is advised. **- Forward to console**: the call is put on hold but forwarded immediately to the ATDC. **- Refused**: the calling party receives a busy tone. **Note :On a multi-key set, this parameter only applies when all the CCOs are busy.**
Return to console on spec. time-out	If the box is ticked, the time-out for return to the ATDC on no answer, free or busy set is no longer the standard value but a special value.
External forwarding allowed	The user may transfer internal calls to an external number. Forwarding of an external call to another external number is subject to other rights.
Assistant forwarding allowed	This form of forwarding is used for a filtering application. This right makes it possible to activate a forwarding function for another set. All incoming calls to the other set are routed to the intercepting set. This parameter is also used to override call forwarding and DND. It authorises the user to forward a group of sets in predefined forwarding mode.
Broadcast call list	Possibility given to the user for digital DM terminals and 6xxxi terminals fitted with a loudspeaker.
Network shift allowed	The user may select a line in a different type of overflow trunk group if the direct routing trunk group is saturated. Example: Tie Line to PSTN Trunk.

Network rerouting allowed	The user may select a line in the same type of overflow trunk group if the direct routing trunk group is saturated. Example: TRK on TRK.
ID sent to public network	Used to indicate which number the user wishes to identify himself or herself with to an external correspondent during an outgoing call to the public network. **- IID**: his/her own number **- AID**: the general call number of the system **- [...]** : according to the AID/IID configuration defined on the system.
ID sent to private network	Used to indicate which number the user wishes to identify himself/herself with to an external correspondent during an outgoing call to a private network (for example, tie-line). **- IID**: his/her own number **- AID**: the general call number of the system **- [...]** : according to the AID/IID configuration defined on the system.
ID sent can be modified for each call	The digital set user may choose from his/her set (interactive OPTION key after the prefix) to transmit to his/her correspondent during each outgoing call: - To send the IID (his/her DID number) - To send the AID (the system's general number) - To send no caller identification (the call will then be set up with the service complement "no number displayed to called party" on condition that this function is authorised at the level of the installation). **Note :If the user does not use the OPTION key, the value defined in the previous lines is sent.**
Priority set	Allows the user to use reserved lines. The number of priority (reserved) lines is determined at the level of the trunk group. In the event of high traffic levels, the reserved lines are allocated to subscribers with the right to priority calls.
Right to immediate forwarding	The user may forward any call immediately.
Forwarding on busy allowed	The user may forward a call if the line is busy.
Forward on no answer allowed	The user may forward a call if the called party is absent.
Ring duration before forward	Selection of 4 possible delayed forwarding ringing tones programmed for a standard configuration duration of 15 seconds. - Switchboard - Specific (1 to 3)
Recorded calls allowed	The user may program his set to memorise the last number dialled (for this, use feature codes or the "SAVE/REPEAT" key on a digital set).

Automatic callback allowed	If the box is ticked, the user may access the “AUTOMATIC CALLBACK” function through the “CALLBACK” function on digital sets or via the “Access to features” menu (Automatic callback activation).
Appointment reminder allowed	The user may use the <<WAKE-UP>> function (“AGENDA” function on digital terminals). Each user has 4 appointment reminders unless it is a hotel room set type, in which case the user has just one appointment reminder.
Common abbrev. numbers allowed	The user may access the general abbreviated dialling feature ("DIRECTORY" function on digital sets).
Personal abbrev. numbers allowed	The user may use his/her own abbreviated numbers list.
Personal calls allowed	If the box is ticked, personal calls are authorised.
Transfer before answer allowed	Right given to a user to transfer a call to another correspondent during ringing or when a call is waiting.
Transfer with return allowed	If the box is ticked, in the event of an unanswered transferred call, the call returns to the user who initiated the transfer.
Hunt group setting allowed	Right given to a user to become part of a subscriber group.
Logoff acceptance	If this box is ticked, the user may log off from his/her digital set. Another user may then log on to this set.
Hotel room type set	Tick this box to authorise personal calls with no password requested, to limit the number of wake-up call requests recorded at any time to 1, and to authorise the message deposit feature. This option is used in hotels.
Ext. last callers callback	The user of a digital extension may consult the last incoming external calls (on an ISDN) and call back if required. Activation of this feature is only valid for ISDN (display of external number) and for sets with interactive keys.
Maintenance set	Right given to users to access certain system management functions from their sets: - Manual trunk testing - Access to the services offered by the management server.
Extension with prepayment	Right given to a user to have a metering credit. All the outgoing calls made by this user are billed to the user’s account. The credit decreases in real time.
Sharing set	For indicating the set that may receive temporary users.

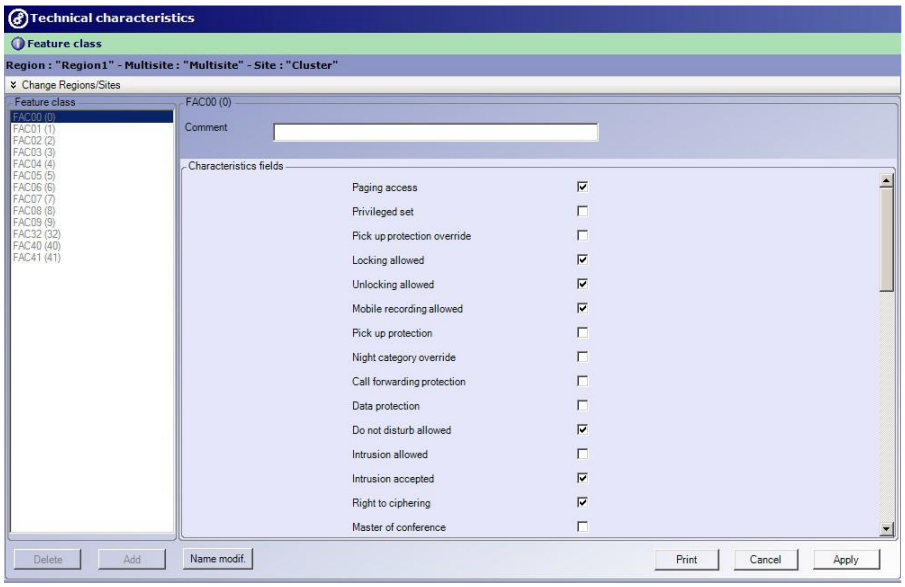
Signature type	Type of identification required from the user for outgoing calls in case of shared sets. Possible types are: - Short: the user must enter his/her secret code (4 digits) for outgoing calls. - Long: the user must dial a code comprising his or her directory number followed by his or her password. - None: the user does not need to authenticate himself/herself.
Busy for hunt group on 1st call	This option is only used to route a call meant for the hunt group if the set is available (generally, a set which features several directory numbers and which belongs to one or more hunt groups).
Log in via PC only	It is possible to define whether the subscriber can log on to a terminal using interactive keys or with the User Portal application only.

12.2.2 VIEWING A FEATURE CLASS

To display a feature class:

- In the *Telephony* window, click **Technical characteristics** then **Feature classes**.
- If necessary, select a region/ multi-site configuration.
- On the *Feature classes*list, click the class to display.

The features defined for the selected class are displayed on the right. The activated features are indicated by a tick.



12.2.3 DEFINITION OF A FEATURE CLASS

You can customise the classes by modifying:

- The comment
- The activation of the various features
- The feature class name.

To modify a feature class:

- In the Telephony window, click Technical characteristics then Feature classes.
- If necessary, select a region/ multi-site configuration.
- On the *Feature classes*list, click the class to modify.
- The features defined for the selected class are displayed on the right.
- Tick (to activate) or untick (to deactivate) the new features.
- To modify the feature class name, click "Name modification" then enter the new name (8 characters maximum). Click OK to confirm. The order number remains the one assigned by default.
- Click **Apply**.

12.2.4 ADDING A FEATURE CLASS

To add a new feature class:

- In the Telephony window, click **Technical characteristics** then **Feature classes**.
- If necessary, select a region/ multi-site configuration.
- Click the **Add** button located under the feature class list.
- An input window opens.
- Enter the name of the new class and, if required, the order number, then click **OK**.

Note : The input is made in upper case. The classes are numbered 0 to 63.

- In creation mode, all the parameters are ticked by default. Untick the parameters to be deactivated.
- If necessary, enter a comment in the *Comments* field then click **Apply** to confirm.
- The new class is displayed on the list. A notification is displayed, and the operations log updated.

12.2.5 DELETING A FEATURE CLASS

To delete a feature class:

- In the Telephony window, click Technical characteristics then Feature classes.
- If necessary, select a region/ multi-site configuration.
- On the *Feature classes*list, click the class to delete.
- Click Delete.

A deletion confirmation request window opens. Click **OK**.

The class is deleted from the list. A notification is displayed, and the operations log updated.

Note : Only the feature classes not used in a telephone subscription can be deactivated. If the class is used, a warning message is displayed.

12.3 MANAGING PSTN CATEGORIES

A PSTN category defines **all the rights and restrictions of a subscriber concerning the external network** (example: local area, national, international call rights, etc.).
PSTN categories are used to restrict the dialling features of sets according to their respective needs. They represent all the rights assigned to subscribers, both for incoming and outgoing calls.
The category is defined on the Management Centre by a description corresponding to a category number between 0 and 63.
The day and night categories of a subscription may be different. The day and night definition is determined by a weekly calendar in which each day of the week is broken down into day and night time bands. The calendar is assigned to a company/service pair and restrictions defined in the day and night categories are applied to all the equipment belonging to that company/service, in accordance with the day and night time bands.

Note : Calendars are managed on the iPBX (see the iPBX operating manuals for more details).

12.3.1 PSTN CATEGORY TYPES

The list of categories below is given for information purpose only and may vary according to system release.

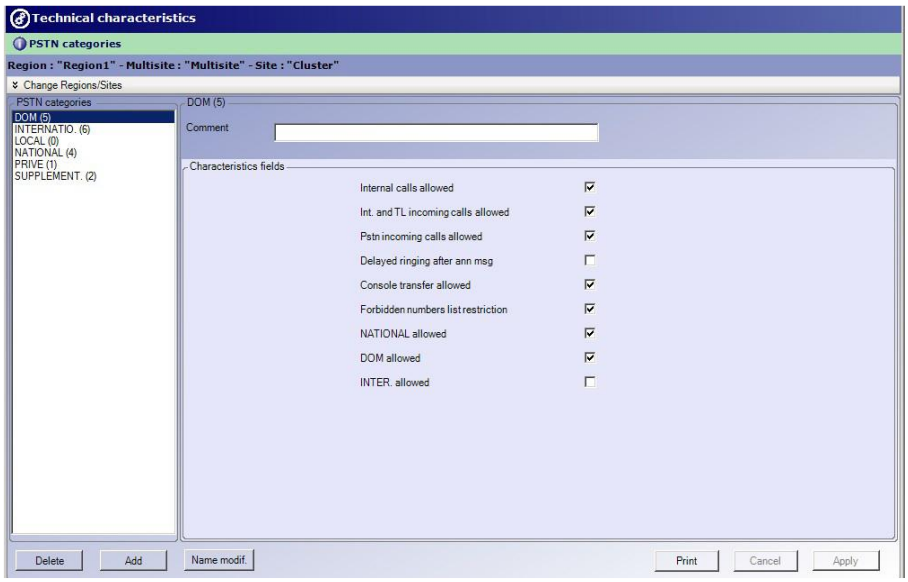
PSTN CATEGORY	DEFINITION
Internal calls allowed	If you tick the box, the set has access to internal outgoing calls. Users cannot receive external calls and cannot call the switchboard (ATDC) by dialling 9.
Int. and TL incoming calls allowed	Incoming internal calls and calls from tie lines are allowed.
External incoming calls allowed	Incoming calls from the public network allowed.
Delayed ringing after ann msg	When this parameter is ticked, the extension only rings after a timeout, to allow the transmission of an offhook signal, followed by a recorded announcement, on the PSTN calling line. This function can be extended to multikey sets and hunt group sets (whether multikey or not). It only applies to internal calls (including calls from the operator) and TL calls.
Console transfer allowed	Access to the public network via the operator is allowed. The operator sets up the call and transfers it to the subscriber.
Barred numbers list restriction	Used to prevent access to the PSTN category for a list of barred numbers. These lists are configured on iPBX's with version R.5.1 B or above only
National access allowed	Outgoing national calls are allowed.
National allowed	Calls to the specified direction allowed.
International access allowed	Outgoing international calls are allowed.

12.3.2 DISPLAYING A PSTN CATEGORY

To display a PSTN category:

- In the Telephony window, click **Technical characteristics** then **PSTN categories**.
- If necessary, select a region/ multi-site configuration.
- In the *PSTN category* list, click the category to display.

The parameters defined for the selected category are displayed on the right. The activated parameters are indicated by a tick.



12.3.3 ADDING A PSTN CATEGORY

To add a new PSTN category:

- In the Telephony window, click **Technical characteristics** then **PSTN category**.
- If necessary, select a region/ multi-site configuration.
- Click the **Add** button located under the category list.

An input window opens.

- Enter the name of the new category and, if required, the order number, then click **OK**.

Note : The input is made in upper case. The classes are numbered 0 to 63.

- In creation mode, all the parameters are ticked by default. Untick the parameters to be deactivated.
- If necessary, enter a comment in the *Comments* field then click **Apply** to confirm the creation.

The new category is displayed on the list. A notification is displayed, and the log updated.

12.3.4 MODIFYING A PSTN CATEGORY

You can customise the PSTN categories by modifying:

- The comment
- The activation or not of the various parameters.

To modify a PSTN category:

- In the Telephony window, click **Technical characteristics** then **PSTN categories**.
- If necessary, select a region/ multi-site configuration.
- In the *PSTN category* list, click the category to modify.
- The parameters defined for the selected category are displayed on the right.
- To modify the PSTN category name, click "Name modification" then enter the new name (8 characters maximum). Click **OK** to confirm.

5. Tick (to activate) or untick (to deactivate) the new categories then click **Apply**.

   The new parameters are taken into account. A notification is displayed, and the operations log updated.

12.3.5 DELETING A PSTN CATEGORY

To delete a PSTN category:

- In the Telephony window, click **Technical characteristics** then **PSTN categories**.
- If necessary, select a region/ multi-site configuration.
- In the *PSTN category* list, click the category to delete.
- Click **Delete**.

A deletion confirmation request window opens. Click **OK**.

The category is deleted from the list. A notification is displayed, and the operations log updated.

Note : Only the categories not used in a telephone subscription can be deleted. If the category is used, a warning message is displayed.

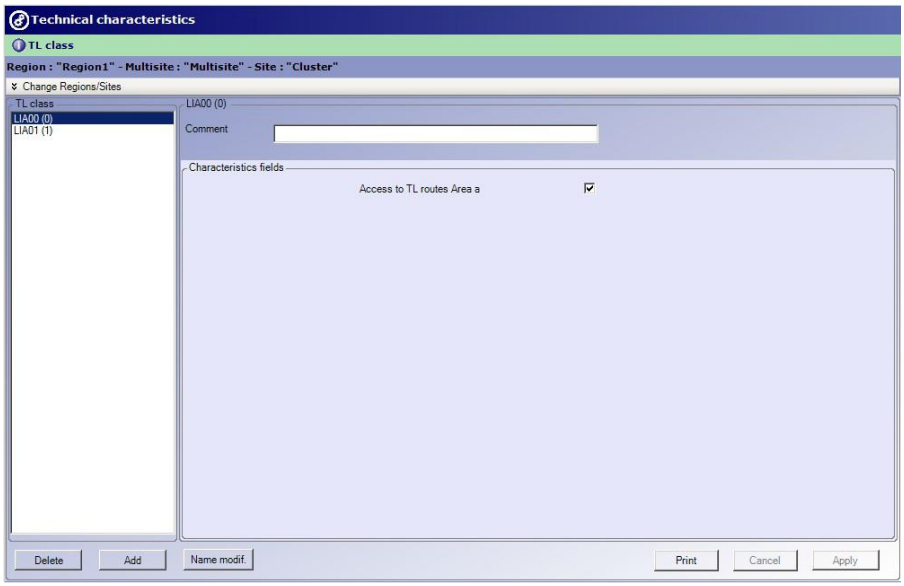
12.4 TL CLASSES

TL class definition is used for global management of TL direction accesses by area, and to assign a Tie-Line class to the sets.

12.4.1 TL CLASS DEFINITION

Depending on the numbering plan, the analysis of some prefixes points to a tie line direction. In a multi-site configuration, 48 private TL directions can be created. These TL directions can be grouped together in 8 restriction areas called “TL restrictions 0 to 7”.

A TL class allows these 8 areas (all the private directions) to be combined in order to assign them to the subscriber. This determines the subscriber’s restrictions with respect to the TL networks.



- Access to TL routes (from A to H)

Access rights for the TL routes in question.

12.4.2 DISPLAYING A TL CLASS

To display a TL class:

- In the Telephony window, click **Technical characteristics** then **TL classes**.
- If necessary, select a region/ multi-site configuration.
- On the *TL classes*list, click the class to display.

The parameters defined for the selected class are displayed on the right. The activated parameters are indicated by a tick.

12.4.3 ADDING A TL CLASS

To add a new TL class:

- In the Telephony window, click **Technical characteristics** then **TL class**.
- If necessary, select a region/ multi-site configuration.
- Click the **Add** button located under the class list.

An input window opens.

- Enter the name of the new class and, if required, the order number, then click **OK**.
- Tick the TL area to specify.
- If necessary, enter a comment in the *Comments* field then click **Apply** to confirm the creation.

The new class is displayed on the list. A notification is displayed, and the operations log updated.

12.4.4 MODIFYING A TL CLASS

To modify a TL class:

- In the Telephony window, click **Technical characteristics** then **TL classes**.
- If necessary, select a region/ multi-site configuration.
- On the *TL classes*list, click the feature class to modify.
- The parameters defined for the selected class are displayed on the right.
- To modify the class name, click "Name modification" then enter the new name (8 characters maximum). Click **OK** to confirm.
- Tick (to activate) or untick (to deactivate) the new areas then click **Apply**.

The modification is taken into account. A notification is displayed, and the operations log updated.

12.4.5 DELETING A TL CLASS

To delete a TL class:

- In the Telephony window, click **Technical characteristics** then **TL classes**.
- If necessary, select a region/ multi-site configuration.
- On the *TL classes*list, click the class to delete.
- Click **Delete**.

A deletion confirmation request window opens. Click **OK** to confirm.

The class is deleted from the list. A notification is displayed, and the log updated.

Note : Only the classes not used in a telephone subscription can be deactivated. If the class is used, a warning message is displayed.

12.5 TECHNICAL HIERARCHY

12.5.1 DEFINING A TECHNICAL HIERARCHY

In the management centre, technical hierarchy refers to the **Company-Department pair defined on the iPBX** as opposed to administrative hierarchy which is used for directory data.

It is defined for a site (or multi-site configuration) of a given region and comprises the following information:

- Company: the associated iPBX company number (integer between 0 and 254 inclusive)
- Department: the associated iPBX department number (integer between 0 and 254 inclusive)

This parameter allows to display and manage the different hierarchies.

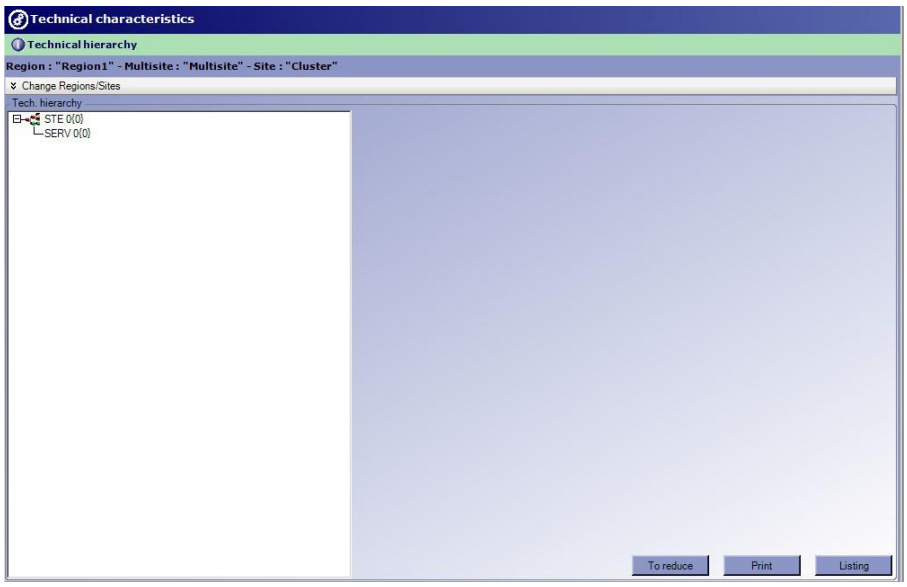
12.5.2 DISPLAYING A TECHNICAL HIERARCHY

To display a technical hierarchy:

In the Telephony window, click **Technical characteristics** then **Technical hierarchy**.

- Select a region, a multi-site configuration.

The technical hierarchy is displayed in form of a tree.



The **List** button is used to manually start an iPBX data listing operation.

12.5.3 MODIFYING A TECHNICAL HIERARCHY

Note: To access these settings, you must first enable the setting Manage Technical Hierarchy Settings in the multisite configuration of the network topology. See Section 7.4.8.3 – Configuring a multi-site network.

The **Edit name** button allows you to change the name of a company or department.

The Technical Hierarchy page displays several editable fields, depending on the multi-site configuration.

- In form of dropdown lists:
  - **PSTN route code**

  - **TIE LINE route code**
  - **Broadcast list code**
  - **PSTN call distribution**
  - **VIP call distribution**
  - **Tie line call distribution**
  - **Internal call distribution**
  - **Wireless profile**
  - **PSTN access barring calendar**
- In form of a field to be filled in:
  - **Common bell directory number**
- The **And of department** field is not modifiable.

Clicking the **Apply** button saves the changes made to the selected department.

Clicking the **Edit all companies** button saves the changes made to all departments within the company.

12.6 ICG

12.6.1 DEFINITION OF ICGS

A GIC or ICG (InterCom Group) consists of extensions that can monitor and pickup each other's calls, or call each other directly.

The number of subscribers belonging to an ICG is limited to 2000.

An ICG is identified by a number on each site.

The subscribers in the same ICG must all belong to the same company or company 0. The company to which the first subscriber assigned to the ICG belongs is imposed.

On a multi-site network, an intercom group may contain the extensions belonging to different sites. However, the function is managed on a single site basis and the subscribers and ICG must be declared on the home site. Company checking is limited to the site subscribers.

Special case of number 253

ICG of number 253 in the iPBX is special: it enables extensions to monitor other extensions without broadcasting their status.

An extension belonging to ICG 253 can program a key to monitor all other extensions belonging to any other ICG. This key is used to pickup calls addressed to the monitored extension, but cannot call this extension.

An ICG 253 extension cannot be monitored (unless it also belongs to another ICG).

An ICG number covers one or more sites and the same number may be assigned to several ICGs.

Example: ICG No. 1 may cover the sites in Toulon and Brest and be defined for sites in Paris and Bordeaux as well.

The list of ICGs for each iPBX is defined through configuration on the Management Centre.

It is possible to manage the name associated with the ICG from the configuration tool. This management operation is used to avoid additional processing on telephony MMIs. On the other hand, modifications are more limited, especially during deletion (since the ICGs assigned to subscribers are not modifiable).

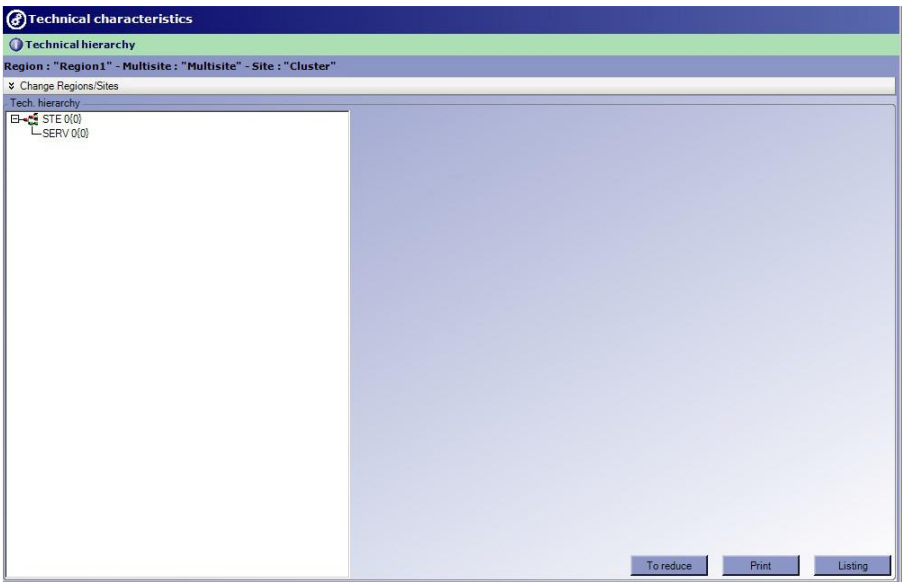
The management of ICGs is, therefore, performed in the management centre and is based on configuration data which lists the ICGs defined on the network iPBXs.

12.6.2 VIEWING INTERCOM GROUPS

To view the ICG configuration on the multi-site:

- In the Telephony window, click Technical characteristics then ICG.
- Select a region, a multi-site configuration.

The ICGs defined on the multi-site are displayed in table form.



The **List** button is used to manually start an ICG listing operation. It is also used to recover a change of configuration on this domain while checking the multi-site consistency of the configuration made. Note that to perform this listing, all the multi-site sites must be operational.

12.7 PARTITIONING CLASSES

12.7.1 DEFINING A PARTITION CLASS

A partition class is defined to **limit and protect telephone subscriber access to incoming and outgoing calls**. The partition class, defined by selecting its description from a list, establishes a macroscopic partition between two large subscriber communities. Two partition classes are assigned to subscribers that determine their rights to communicate with different defined interest groups: one originating partition class (outgoing calls) and one terminating partition class (incoming calls).

Checks are carried out when calls are set up. The calls are authorised by making a logical ET between the caller’s outgoing partition class and the called party’s incoming partition class. The result must be different from 0

The calls are authorised when the parameters defined in the caller's outgoing partition class correspond to those defined.

A partition class is a set of vectors composed of 1 to 8 segments of 1 to 4 bytes.

64 partition classes can be defined.

The following parameters are entered:

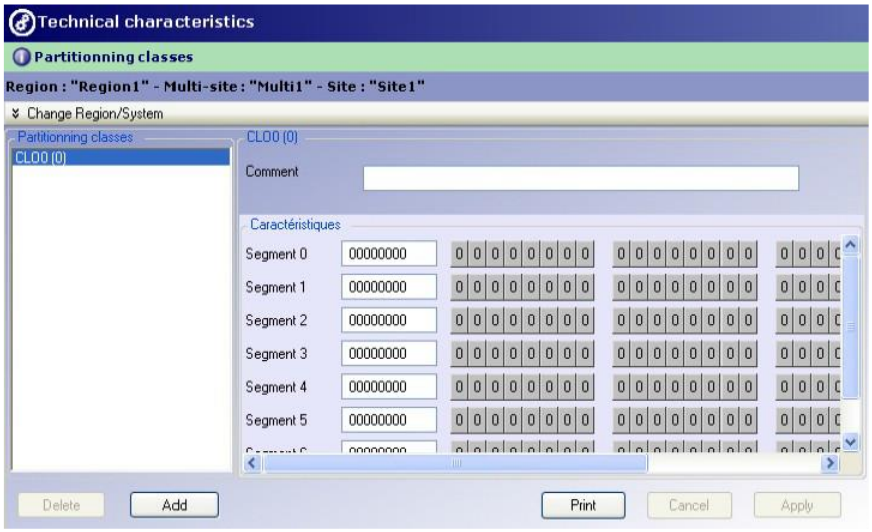
- The label of the partition class
- The number of the class
- A comment.

12.7.2 VIEWING A PARTITIONING CLASS

To display a partitioning class:

- In the Telephony window, click Technical characteristics then Partitioning classes.
- If necessary, select a region/ multi-site configuration.
- On the *Partitioning classes*list, click the class to display.

The parameters defined for the selected class are displayed on the right.



12.7.3 ADDING A PARTITIONING CLASS

To add a new partitioning class:

- In the Telephony window, click **Technical characteristics** then **Partitioning classes**.
- If necessary, select a region/ multi-site configuration.
- Click the **Add** button located under the class list.

An input window opens.

- Enter the name of the new class and, if required, the order number, then click **OK**.
- Enter the values of each segment.
- If necessary, enter a comment in the *Comments* field then click **Apply** to confirm the creation.

The new class is displayed on the list. A notification is displayed, and the log updated.

12.7.4 MODIFYING A PARTITIONING CLASS

You can customise the classes by modifying:

- The comment
- The definition of the various segments.

To modify a partitioning class:

- In the Telephony window, click **Technical characteristics** then **Partitioning classes**.
- If necessary, select a region/ multi-site configuration.
- On the *Classes* list, click on the class you wish to change.

The parameters defined for the selected class are displayed on the right.

- To modify the selected class name, click "Name modification" then enter the new name (8 characters maximum). Click **OK** to confirm.
- Enter the modifications then click **Apply**.

A notification is displayed, and the log updated.

12.7.5 DELETING A PARTITIONING CLASS

To delete a partitioning class:

- In the Telephony window, click **Technical characteristics** then **Partitioning classes**.
- If necessary, select a region/ multi-site configuration.
- On the *Classes*list, click the class to delete.
- Click **Delete**.

A deletion confirmation request window opens. Click **OK** to confirm.

The class is deleted from the list. A notification is displayed, and the log updated.

Note : Only the classes not used in a telephone subscription can be deactivated. If the class is used, a warning message is displayed.

12.8 PRIORITY CLASSES

12.8.1 DEFINING A PRIORITY CLASS

The purpose of priority is, in case of resource saturation, to release some low-priority calls in order to set up a high-priority call. The priority of a call depends on the caller's priorities, expressed by two parameters:

- Activation mode which translates the call pre-emptor character in setup phase and the level of protection against established call pre-emption
- Priority (0 to 5) which translates the priority level assigned to a call for a given activation mode.

Two activation mode / priority pairs are managed by the priority classes:

- Default activation mode / priority which is used if the user does not intervene
- Default activation mode / priority is used if the user intervenes.

64 priority classes can be defined.

The following parameters must be entered:

- The label of the priority class,
- The number of the class
- A comment.

12.8.2 VIEWING A PRIORITY CLASS

To display a priority class:

- In the Telephony window, click **Technical characteristics** then **Priority classes**.
- If necessary, select a region/ multi-site configuration.
- On the *Classes* list, click on the class you wish to display.

The parameters defined for the selected class are displayed on the right.

12.8.3 ADDING A PRIORITY CLASS

To add a new priority class:

- In the Telephony window, click **Technical characteristics** then **Priority classes**.
- If necessary, select a region/ multi-site configuration.
- Click the **Add** button located under the class list.

An input window opens.

- Enter the name of the new class and, if required, the order number, then click **OK**.
- Define the parameters Activation mode and Priority level:
  - Activation mode: list of options
  - Priority level: direct entry.
- If necessary, enter a comment in the *Comments* field then click **Apply** to confirm the creation.

The new class is displayed on the list. A notification is displayed, and the log updated.

12.8.4 MODIFYING A PRIORITY CLASS

You can customise the classes by modifying:

- The comment
- Parameters definition

To modify a priority class:

- In the Telephony window, click **Technical characteristics** then **Priority classes**.
- If necessary, select a region/ multi-site configuration.
- On the *Classes* list, click on the class you wish to change.

The parameters defined for the selected class are displayed on the right.

- To modify the selected class name, click "Name modification" then enter the new name (8 characters maximum). Click **OK** to confirm.
- Modify the necessary parameters then click **Apply**.

The modifications are taken into account. A notification is displayed, and the log updated.

12.8.5 DELETING A PRIORITY CLASS

To delete a priority class:

- In the Telephony window, click **Technical characteristics** then **Priority classes**.
- If necessary, select a region/ multi-site configuration.
- On the *Classes*list, click the class to delete.
- Click **Delete**.

A deletion confirmation request window opens. Click **OK** to confirm.

The class is deleted from the list. A notification is displayed, and the log updated.

Note : Only the classes not used in a telephone subscription can be deactivated. If the class is used, a warning message is displayed.

12.9 OTHER CHARACTERISTICS.

This menu contains other technical characteristics defined on the iPBXs but not managed by the management centre. The characteristics are proposed as listing only.

Integrated voicemail box	List of voicemail boxes that may be assigned to a subscriber (XS/ XL/ XD only)
Directions	List of directions used in the technical characteristics (PSTN, TL)
Written language	Displays the list of languages available for display on digital sets.
Spoken language	Displays the list of languages available for announcements.
Hunt group parameters	Lists the characteristics to be defined for hunt groups. (Refer to the section Managing hunt groups)
IVS scripts	Lists the names of IVS scripts available on the iPBX. These scripts are used for the configuration of IVR type subscribers.
MiCollab role	List of roles available on the iPBX. These scripts are used to configure MiCollab user subscribers.

For each parameter, the **List** button is used to manually list the selected parameter on all the sites of the multi-site.

12.10 WHITE PLAN

The white plan is designed to temporarily change the telephony configuration of certain users by limiting certain features during a crisis period.

The white plan applies for:

- Day and night PTSN accesses
- Day and night TL classes
- Feature classes

It does not affect priority and partitioning classes.

The white plan is defined through a range of parameters which replace the normal operating parameters for this specific period and for the classes in question.

Example: When a white plan is operational some terminals will only be able to make external calls, or receive calls.

The white plan is triggered and managed by MiVoice 5000 Manager only. When this plan is implemented, no declaration is communicated to the various iPBX sites.

You are recommended to assign a single administrator to configure and trigger this plan.

12.10.1 IMPLEMENTING THE WHITE PLAN

The white Plan only applies in a multi-site configuration.

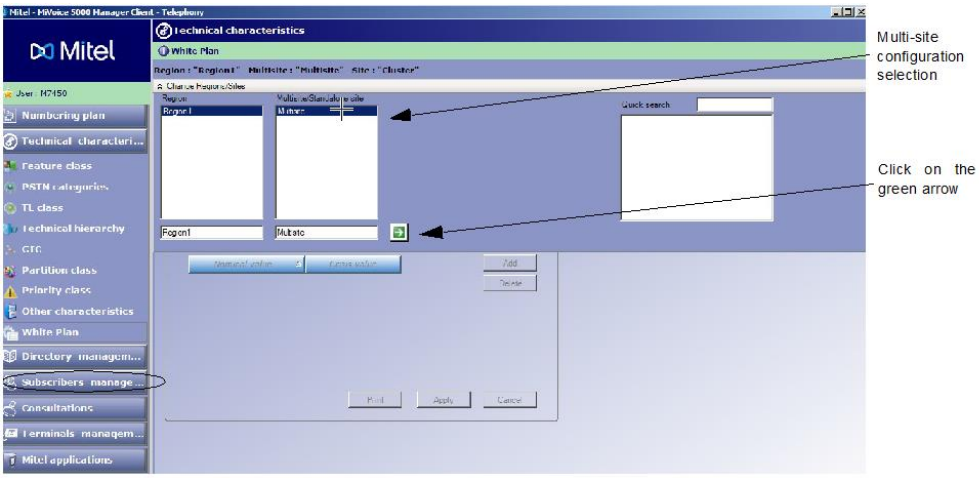
Note : Concerning the changes made when the white plan is activated:

The changes will be effective if they relate to categories not managed by the plan.

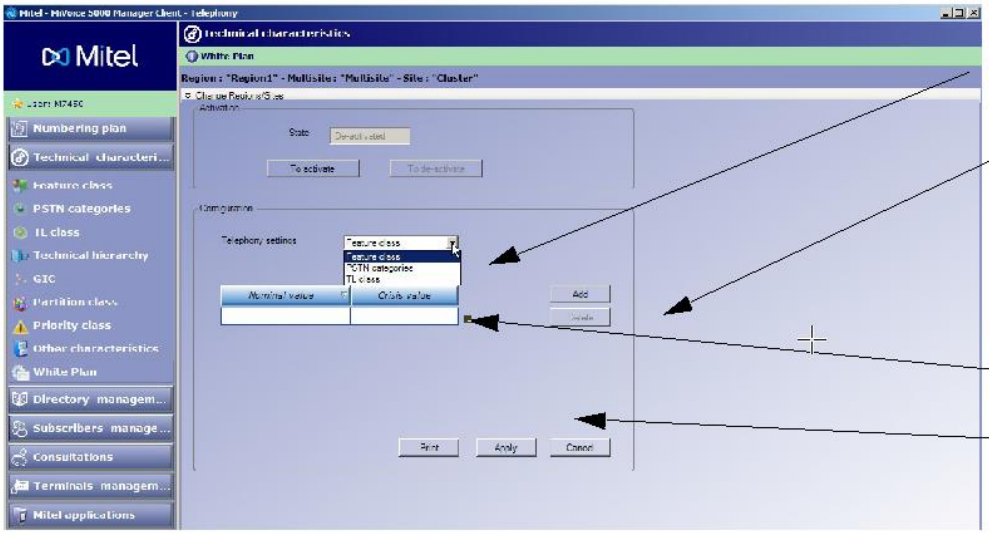
The changes will be lost if they relate to categories concerned by the white plan.

Ensure that, in the **Administration/Configuration** menu, **Range** tab, the **Based on multisite** box is ticked.

- Select the multi-site configuration to which the white plan is to be applied.

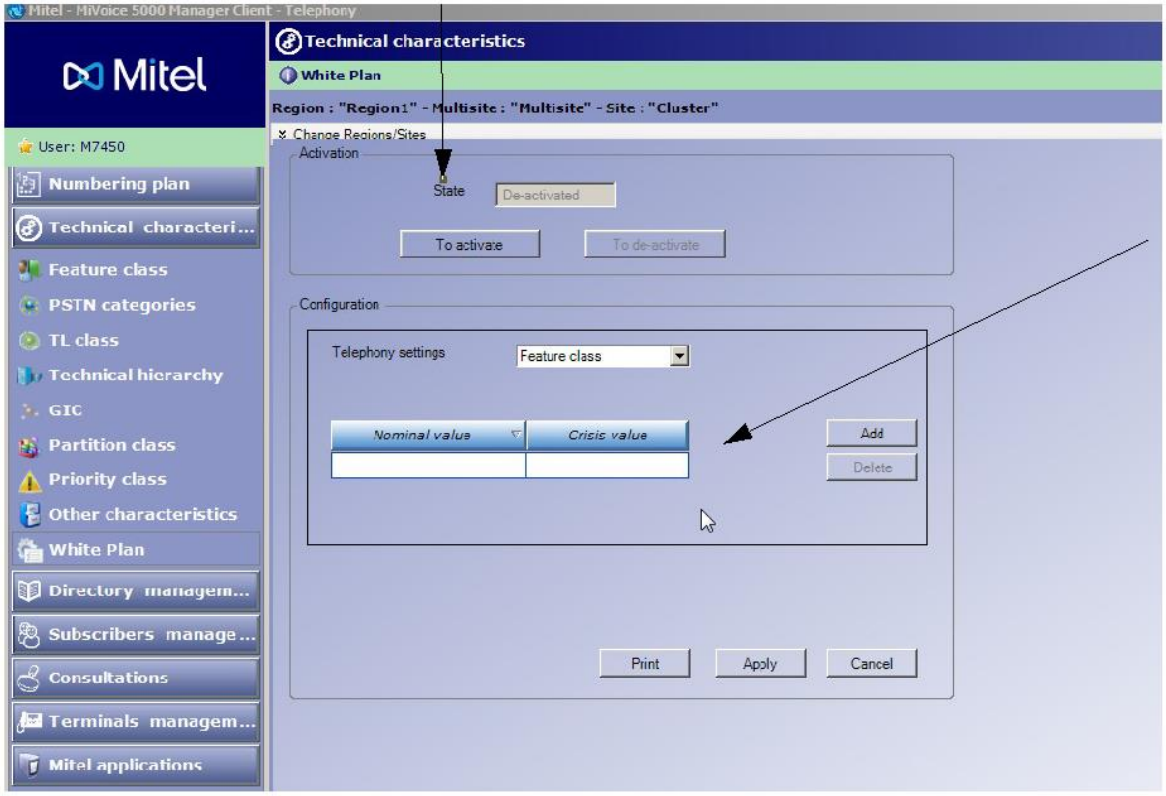


- Select the various telephony parameters to be covered by the white plan.



12.10.2 ACTIVATING THE WHITE PLAN

Once the previous parameters have been defined, the white plan can be implemented by clicking **Activate**.



12.10.3 DEACTIVATING THE WHITE PLAN

On the previous screen, click on **Deactivate**

Once deactivated, the configuration zone is again available.

13 DIRECTORY MANAGEMENT

MiVoice 5000 Manager uses an LDAP directory to manage its subscriber data. Only one directory is used on the entire network. This directory contains all the internal and external directory records. It is customisable in terms of its structure and directory record layout.

Additional information about LDAP directory management can be obtained from the multi-site documentation.

The **Directory management** menu comprises the following elements:

- **Administrative hierarchy**: for managing the directory's administrative organisation
- **Directory parameters**: for defining the values of the options list for directory record parameters
- **Customisation**: for defining the customisable fields of the directory record.
- **External record management**: for managing external contacts.
- **External directory synchronisation**: for synchronising data between the LDAP directory used by the management centre and an external Active Directory type directory database, LDAP database or description file.
- **Directory alias management**

Actions run from these menus are directly executed in the LDAP.

Note : The management of directory parameters and administrative hierarchy is optional. This is notably the case when directory records have been created from an external source during synchronisation.

Note : Servers accessing the directory implement caching mechanisms in order to optimise processing (search by name, barred numbers, abbreviated numbers, SDN).

13.1 ADMINISTRATIVE HIERARCHY

This menu is used to display and manage the administrative structure of the LDAP directory. Possible operations in this menu are:

- Viewing the directory structure
- Modifying an administrative entity
- Deleting an administrative entity
- Adding an administrative entity

For any action on the directory, an execution report is saved in the operation log.

13.1.1 DEFINITION OF ADMINISTRATIVE HIERARCHY

The directory presents a hierarchical structure comprising different administrative entities. An administrative entity may be a company, a department, management, a service, etc.

An entity may have subscribers regardless of its hierarchical level, on condition that it is at a terminating level in the tree structure.

A subscriber's administrative hierarchy refers to the administrative level of the directory to which it is attached. It is identified through a company / administrative department pair.

Difference between administrative hierarchy and technical hierarchy

A telephony subscription may consist of a directory record and a technical record.

Administrative hierarchy is used in the directory record whereas technical hierarchy is used in the technical record. There is no correlation between both hierarchies.

In brief:

- Administrative hierarchy = company / administrative department pair defined in the directory
- Technical hierarchy = company/department pair defined on the iPBX.

Managing barred number lists – function available only as of R5.1B configuration (reference site in R5.1)

Note : For managing barred numbers, refer also to the iPBX operating documents detailed at the start of this document.

Barred numbers are external numbers that subscribers can be barred from calling

- Either individually
- Or for all subscribers within an administrative hierarchy.

Barred numbers are defined in the form of lists. It is possible to define up to 50 lists of 100 numbers.

Each entry in a barred numbers list is either a complete external number (including the access prefix) or the beginning of an external number, the effect of which will be to bar all numbers starting with this entry.

A list of barred numbers can be attached to each administrative hierarchy node. These lists are configured on the iPBXs (parameter not managed by MiVoice 5000 Manager) and can be listed via MiVoice 5000 Manager by clicking the List button on the barred number list group. The names of the different lists retrieved by MiVoice 5000 Manager are displayed here.

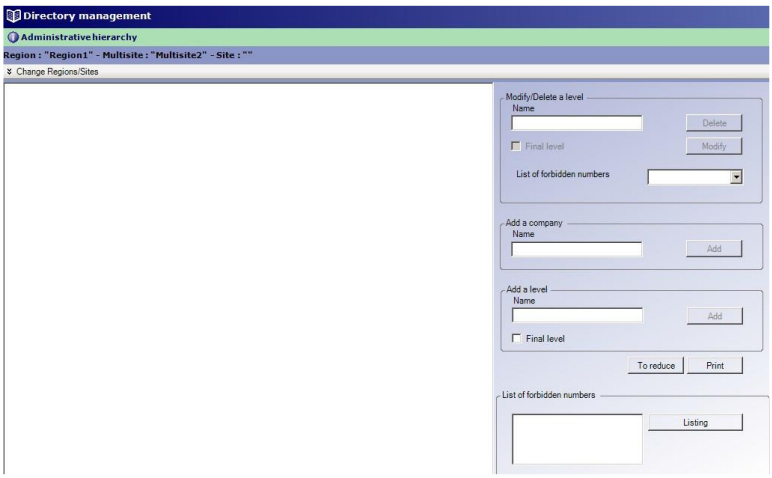
13.1.2 VIEWING AN ADMINISTRATIVE HIERARCHY

To display an administrative hierarchy tree:

In the Telephony window, click Directory management then Administrative hierarchy.

- Select a region / multi-site configuration.

The window with the administrative hierarchy tree defined on this site opens.



Click + to deploy an administrative hierarchy tree.


This symbol shows that the entity is on the first level (**Company** level).


This symbol shows that the entity is on the final level.

13.1.3 MODIFYING AN ADMINISTRATIVE ENTITY

Modifications on an administrative entity may concern its name, its tree level as well as the list of barred numbers for this hierarchy.

To modify an administrative entity:

- On the tree, click an entity to select it.
- If necessary, use the + sign to display the sub-levels.
- Its name appears in the *Modify/Delete level* area.
- Modify the name.
- If the selected entity must be on the last level, tick the *Final level* box.
- If necessary, assign a list of barred numbers. The options list remains greyed out on an R5.1A multi-site (no barred number list management).
- Click **Modify** to confirm the input.

The modification is taken into account. A notification is displayed, and the log updated.

13.1.5 DELETING AN ADMINISTRATIVE ENTITY

- On the tree, click an entity to select it.
- If necessary, use the + sign to display the sub-levels.
- Its name appears in the *Modify/Delete level* area.
- Click **Delete**.

Note : An entity cannot be deleted or modified if it still has subscribers on the same or lower levels.

Note : Deleting a level deletes the attached sub-levels.

13.1.6 ADDING AN ADMINISTRATIVE ENTITY

13.1.6.1 Adding a company

A company is a fist-level entity.

To add a company, enter a name in the **Add a company** field then click **Add**.

The new entity is displayed on the tree.

13.1.6.2 Adding a level

- On the tree, click the entity on which the new entity will be created.
- If necessary, use the +/- signs to display the sub-levels.
- Enter a name in the **Add a level** field.
- Tick the **Final level** box if the entity to be created is on the last level.
- Click **Add**.

The new entity is displayed on the tree.

13.2 DIRECTORY PARAMETERS

13.2.1 DEFINING DIRECTORY PARAMETERS

Directory parameters are defined in the LDAP directory and are made up of the various values presented in form of an options list. They are used in the internal or external directory record.
Accessible directory parameter types are:

- Type (e.g.: Mrs, Mr, Room, Office...)
- Function (e.g.: Manager, Assistant, Salesperson...)
- Group If the attribute "**Activation of directory groups**" is activated in the multi-site architecture, a new type is accessible (see the section Directory groups):
  - Group (example: Shop1, Group1, etc.).

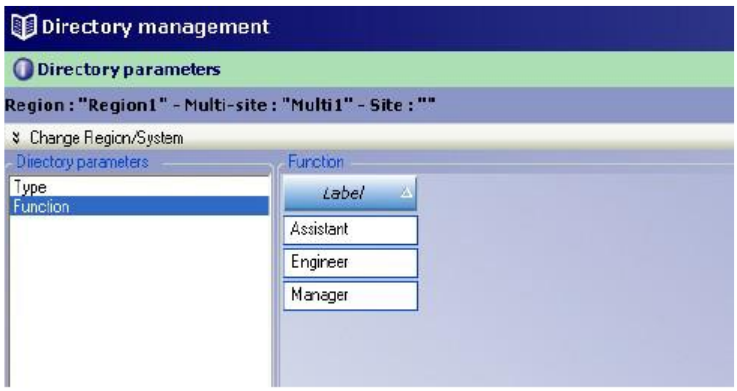
The user cannot create, delete or modify the directory parameters defined in the LDAP directory but, for a given parameter, he or she can define the options list values, add a new value or delete a value.

13.2.2 VIEWING DIRECTORY PARAMETERS

To view the list of directory parameters:
In the Directory management menu, click **Directory parameters**.

- Select a region / multi-site configuration.

The following window is displayed.



- Click on a parameter in the *Directory parameters* list.

The values defined in this parameter are displayed on the right.

13.2.3 ADDING A DIRECTORY PARAMETER

To add a value:

- On the list of directory parameters, click on the parameter to which the new value will be applied.
- Enter the name of the value in the field below the list of values then click **Add**.

Note : The Add button is activated once you start making the entry.

A confirmation message is displayed, and the new value added to the list.

13.2.4 DELETING A DIRECTORY PARAMETER VALUE

To delete a value:

- In the list of values, click on the value to delete.
- Click **Delete**.

A deletion confirmation request window opens; click OK.
A notification is displayed, and the list updated.

Note : You cannot delete or modify a value that is used in a subscription.

13.3 PERSONALIZATION

The directory record proposes a structure comprising:

- **Mandatory** attributes required by the system to work properly.
- **Customisable** attributes which can be added to the internal and external directory records.

This menu is used to define the customisable attributes of the directory record (limited to 10 per record).

This customisation may apply to internal or external directory records.

Depending on the range defined, directory data customisation will be global or multi-site.

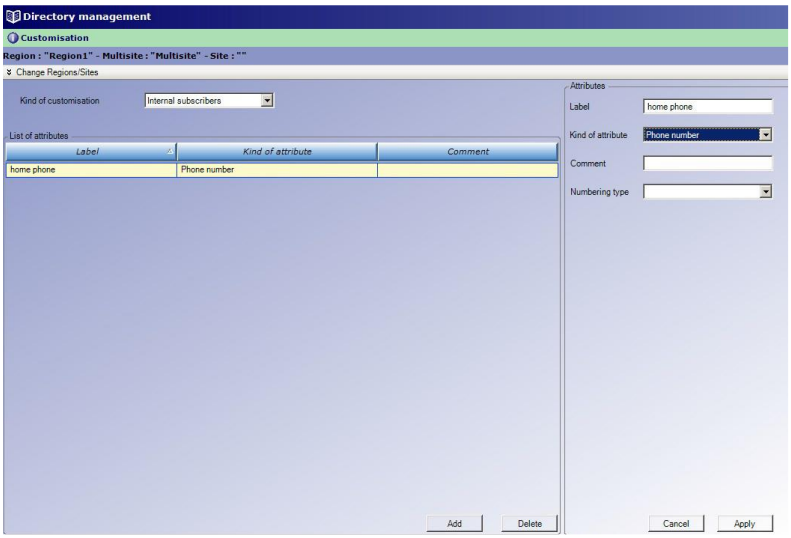
13.3.1 VIEWING THE ATTRIBUTE LIST

To view the customization attribute list:

In the **Directory management** menu, click **Customization**.

- If required, select a region / site.

The following window opens:



- In the *Kind of customization* area, select the directory record types (internal or external records).
- The list of attributes applicable to these records is displayed underneath.
- When an attribute is selected on the list, its parameters appear in the *Attributes* area by the right.

13.3.2 ADDING A CUSTOMISATION ATTRIBUTE

To add an attribute:

- Select a region / site, then choose the type of directory records to be customised in the *Kind of customization* area.
- Click **Add**.

Some empty fields are displayed in the *Attributes* area.

Fill in the following fields:

- **Label**: attribute name (mandatory)
- **Attribute type**: Standard, Phone number, e-mail address or photo.
- **Comment**: free data-entry area

Note : If the selected attribute type is Phone number, the following fields can be filled in:

- **Dialable**: for attributes containing a phone number, this field is used to qualify the number type (Office, Home, GSM, etc.). An icon associated with the number type may be displayed on certain external applications.
- **Dialable number**: if ticked, this field is used to identify the numbers which can be used directly without change of format. External numbers are generally not diallable.
- After defining the parameters, click **Apply**.

A confirmation message is displayed, and the new attribute added to the list.

13.3.3 MODIFYING A CUSTOMISATION ATTRIBUTE

To modify an attribute:

- Select the attribute to modify from the list.

The parameters defined for this attribute are displayed by the right.

- In the **Attributes** part, modify the necessary fields.
- After making the modifications, click **Apply**.

13.3.4 DELETING A CUSTOMISATION ATTRIBUTE

To delete an attribute:

- Select the attribute to delete from the list.
- Click **Delete**.

A deletion confirmation request window opens. Click **OK**.

A notification is displayed, and the list updated.

13.4 MANAGING EXTERNAL RECORDS

This menu is used to manage external records and their abbreviated number.

External records are used to manage contacts outside the enterprise network. The following operations are possible on an external record:

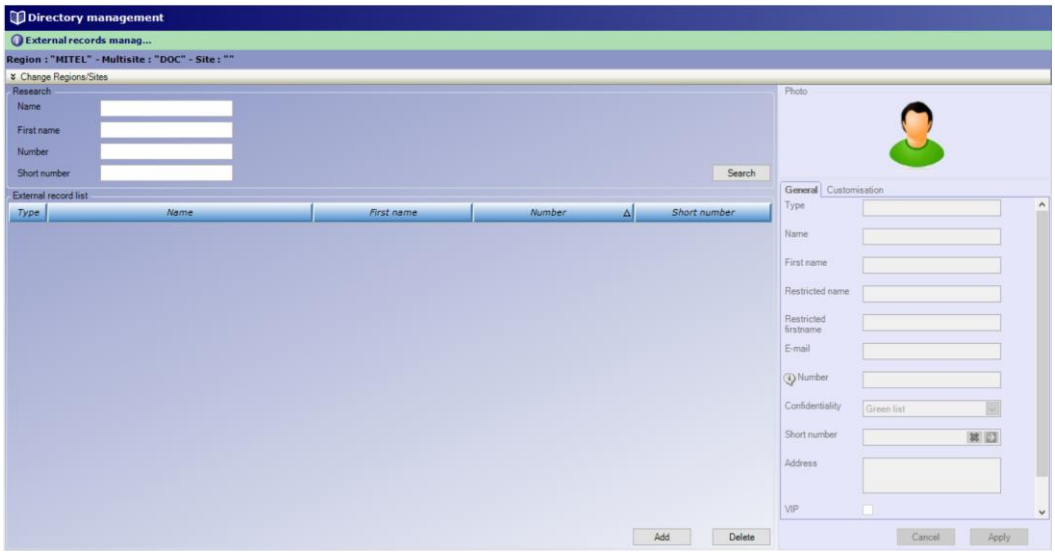
- Create
- View / Modify
- Delete

ACCESS TO EXTERNAL RECORD MANAGEMENT

In the Directory management menu, click External records management.

- Select a region / multi-site configuration.

The following window is displayed.



This window is organised as follows:

- A **search** area in the upper part of the screen
- A **display** area in the lower part of the screen
- An **operation** area on the right side of the screen with two sections:
  - A **Photo** section for the contact photo
  - A section with the **General** and **Customisation** tabs. The MiVoice 5000 Manager displays a third Groups tab if the property Activation of directory groups is enables in the multisite parameters

13.4.1 CREATING AN EXTERNAL RECORD

- Select a region / multi-site configuration.
- Click the Add button located at the bottom of the display area.
- A new record is displayed in the management area.
- The operating area is displayed in form of a folder:

General tab: grouping together the following fields:

Fields with * are compulsory.

- **Type:** options (values defined in the Directory parameters menu)
- ***Name / *First name**: identity of the contact
- **Restricted name / Restricted first name**: entered by the system (this field contains the information in the previous two fields, but without the special and accented characters)
- **E-mail**: contact e-mail address
- **Number**: contact number

  The format for this number may be 10 digits (e.g.: 0123456789) or in E164 format (+<country code number>< +33 123456789).

  For an international number, add the international access code 00491223455678 or use the format E164 +49 1223455678.

  An information bubble on the icon by the right of the Number field indicates the formats possible for external numbers.

Note : This number may be incomplete if an abbreviated number is attached to it. In this case, the external record must be on the red list. The number format will be 013460[4] (incomplete 10 digit number) or 013460[] (incomplete number with undefined length).

- **Confidentiality**: confidentiality enables you to define the list of records accessible through subscriber search. Possible options: green list (public access), red list (access forbidden).
- **Abbreviated number**: see **Managing abbreviated numbers**
- **Address**
- **VIP**: Configures the contact calls as VIP calls
- **SIP Uri**
- **Key**: this attribute is displayed when the record has been created through external database synchronisation.

  This attribute links the subscriber to the External Directory (AD).

  The "Key" attribute can be modified, if necessary, from this field.

  It can also be modified via CSV import.

Personalisation tab: grouping together the personalisation fields

Groups tab:

This tab is only visible if the attribute **Activation of directory groups** is enabled in the property of the multi-site architecture (see the section - Directory groups).

Two multiple choice lists

Available groups: Shows all the groups defined in the directory for the selected multi-site configuration,

Record groups: Group membership of the external record.

By default, no group is associated; the record is said to be "public". This is represented by the item **"***Public***"**

- To add a picture, click the picture icon to open the insertion window.
- Click **Modify** and define the access path to the picture corresponding to this record.
- After entering all the parameters, click **Apply**.

The new class is created and displayed on the list.

13.4.2 SEARCHING FOR AN EXTERNAL RECORD

- If necessary, select a region/site.
- In the *Search* area, define the search criteria:
  - Name
  - The joker character * can be used in place of a character string.
  - First name
  - Number
  - Speed-dial number
- Click **Search**.

The result appears in the display area.

13.4.3 SELECTING AN EXTERNAL RECORD

On the result list, click a record to select it.

The parameters defined for this record are displayed on the right.

13.4.4 MODIFYING AN EXTERNAL RECORD

- Select a record on the result list.

The parameters defined for this record are displayed on the right.

- Enter the necessary modifications then click **Apply**.

13.4.5 DELETING AN EXTERNAL RECORD

- Select a record on the result list.
- Click **Delete**. Confirm the deletion by answering OK to the deletion confirmation request.

The record is deleted.

13.4.6 MANAGING ABBREVIATED NUMBERS

An abbreviated number is a number with 1 to 4 digits used to make a call without dialling the complete telephone number. The abbreviated number length is defined in the **Administration** menu (topology / directory).

Abbreviated numbers are basically used for external records but can also be associated with internal subscriber records.

13.4.6.1 Using abbreviated numbers in the external record

An abbreviated number can be associated with the phone number in the external record.

An administrative hierarchy can be assigned to this abbreviated number. Subscribers attached to a given administrative hierarchy may use the abbreviated numbers defined in this hierarchy. If no administrative hierarchy is associated with the abbreviated number (All hierarchies criterion), the subscriber may use the abbreviated number without restriction and override his or her call rights.

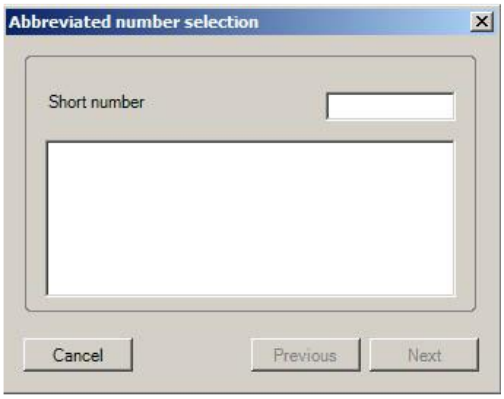
Example: A subscriber with limited call rights internally can make a national call via the associated abbreviated number in the external record.

13.4.6.2 Creating an abbreviated number

An abbreviated number is created in the external record.

- In the external record, *Attributes* area, click the green arrow in the Abbreviated number field.

A new abbreviated number creation window appears.



- Enter a 1 to 4 digits number (depending on the predefined length).
- A list of existing numbers starting with the 1st digit entered appears during the input.
- Click **Next**.
- To define the administrative entities associated with this number, choose the option *Detailed hierarchy list*, tick the associated entities then confirm. Otherwise, select the *All hierarchies* option.
- Click **Validate**.

The created abbreviated number is displayed in the field.

13.4.6.3 *Modifying an abbreviated number*

For a selected external record, click the green arrow in the Abbreviated number field.

The abbreviated number management window appears.

- Modify the abbreviated number then click Next.
- If necessary, modify the administrative hierarchy and click **Validate**.

The abbreviated number is modified.

- Click **Apply** to take this modification into account in the external record.

13.4.6.4 *Deleting an abbreviated number*

- For a selected external record, click the red cross in the Short number field.
- The abbreviated number is deleted.
- Click **Apply** to take this modification into account in the external record.

13.5 EXTERNAL DIRECTORY SYNCHRONISATION

In release 2.3 and later, external directory synchronisation can manage the creation of the directory record and technical, UCP and TWP records.

The configuration required to synchronise an external directory is described in the document **MiVoice 5000 Manager - Configuring the directory**.

13.5.1 USING SYNCHRONISED ELEMENTS

After the elements are synchronised, they can be managed via the management centre. The management operations are run from the **Action** column.

This column displays the type of action taken on the external directory: Creation, modification or deletion of directory records.

13.5.1.1 *Accessing synchronised record follow-up*

- Select a directory record from the list.
- In the **Action** column double-click the action element. The display will differ according to type of action:
  - Creation / Modification: the window opens to the subscriber's directory record. Refer to Section Subscription management.
  - Delete: a deletion confirmation request window opens.

13.5.1.2 *Following up synchronised records*

For a given directory record click the **Management** field then choose one of the criteria proposed: New / Taken into account / Closed.

If you select closed, the subscriber's line is greyed out. The management elements will be deleted during the next purge operation. This way, only the elements that require an additional action from the MiVoice 5000 Manager user are retained in synchronised element Manager management.

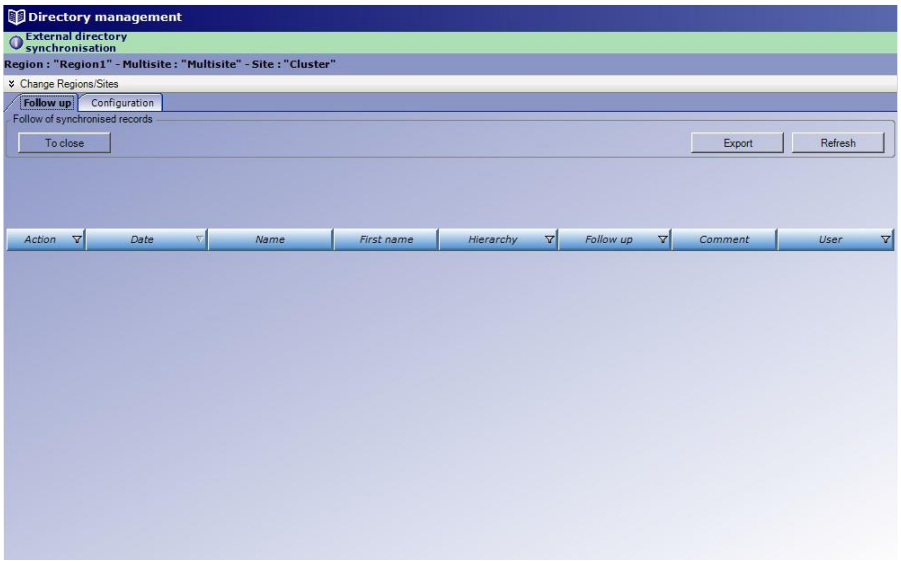
When synchronisation has been configured to create technical, UCP and TWP records, the directory records thus created are displayed on a greyed out background, accompanied by the closed criterion.

13.5.1.3 *Viewing synchronised elements*

In the synchronisation window, click the **Management** tab.

The list of synchronised elements appears.

- Click **Update** to update the display of synchronised elements.



The synchronised elements are presented with the type of action taken in the external database (creation, modification or deletion), the date of update, surname, first name and hierarchy of the corresponding MiVoice 5000 Manager subscription. The management column gives the synchronisation operation management status. The elements in Closed status are purged with the next MiVoice 5000 Manager purge operation Manager (at least once a day). This window also gives access to synchronised element administration and management operations.

13.6 DIRECTORY ALIAS MANAGEMENT

Alias records are internal records of persons without a subscription but who share a set with a subscriber.

The alias record is presented in the same form as the person record but does not have an associated number.

Example:

In the nurses' common room in a hospital department:

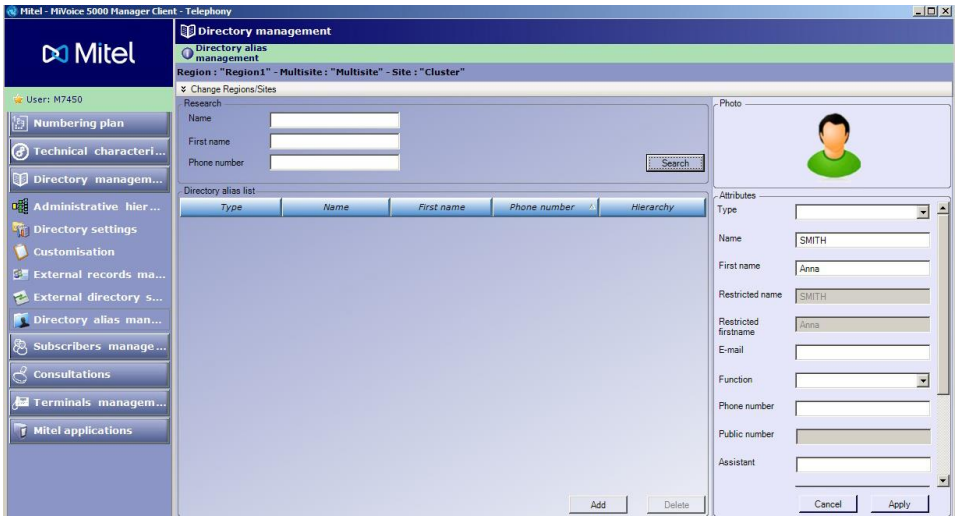
- The telephone set has a single telephone number and therefore a single subscription.
- The main subscription is therefore shared between the nurses declared as Aliases on this number.
- The names of the individual nurses declared on the alias record will be managed on the shared set in the communal area.

For multi-site configurations, the Alias records can only be declared on the supervising MiVoice 5000 Manager.

Mass creation is not possible with this type of record.

13.6.1 CREATING AN ALIAS

Select Menu **Directory management/Directory alias management**.



Note : The Name, First name and Hierarchy fields must be completed.

- Select a region / multi-site configuration.
- Click the Add button located at the bottom of the display area.
- A new record is displayed in the management area.
- The operating area is displayed in form of a folder:

General tab: grouping together the following fields:

Fields with * are compulsory.

- **Type:** options (values defined in the Directory parameters menu)
- ***Name / *First name**: identity of the contact
- **Restricted name / Restricted first name**: entered by the system (this field contains the information in the previous two fields, but without the special and accented characters)
- **E-mail**: contact e-mail address
- **Function:** options (values defined in the Directory parameters menu)
- **Number ***: internal number (mandatory)
- **Public number**: entered automatically
- **Assistant**:
- **Admin. hierarchies**: entered automatically
- **Address**

Personalisation tab: grouping together the personalisation fields

Groups tab:

This tab is only visible if the attribute **Activation of directory groups** is enabled in the property of the multi-site architecture (see the section - Directory groups).

Two multiple choice lists

Available groups: Shows all the groups defined in the directory for the selected multi-site configuration,

Record groups: Group membership of the external record.

By default, no group is associated; the record is said to be "public". This is represented by the item **"***Public***"**

- To add a picture, click the picture icon to open the insertion window.
- Click **Modify** and define the access path to the picture corresponding to this record.
- After entering all the parameters, click **Apply**.

The new class is created and displayed on the list.

13.6.2 SEARCHING FOR AN ALIAS

- If necessary, select a region/site.
- In the *Search* area, define the search criteria:
  - Name
  - The joker character * can be used in place of a character string.
  - First name
  - Number
- Click **Search**.

The result appears in the display area.

13.6.3 SELECTING AN ALIAS

On the result list, click a record to select it.

The parameters defined for this record are displayed on the right.

13.6.4 MODIFYING AN ALIAS

- Select a record on the result list.
- The parameters defined for this record are displayed on the right.
- Enter the necessary modifications then click **Apply**.

13.6.5 DELETING AN ALIAS

- Select an alias on the result list.
- Click **Delete**. Confirm the deletion by answering OK to the deletion confirmation request.

The alias is deleted.

14 SUBSCRIBER MANAGEMENT

MiVoice 5000 Manager allows centralised management of telephony subscribers on the declared network. Telephony subscriber management consists in declaring and configuring telephony subscriptions on managed network iPBXs.

The **Subscriber management** menu contains the following functions:

- Search: for searching for and selecting one or more subscribers for display or management.
- Individual creation: for creating subscribers individually.
- Massive creation: for importing a subscriber database through an Excel file.
- Mass treatment follow-up: for monitoring actions taken on several subscribers.
- Web Client: for accessing directly the web application used to eaasily create subscribers by profile.
- Profiles management: for creating and managing the profiles used to easily create subscribers.

14.1 DEFINITION OF A SUBSCRIPTION

A telephony subscription contains all the information relating to a subscriber number on the network managed by the Management Centre.

All the information concerning a subscriber number and which applies to a particular network element (iPBX, keys, forwarding, voicemail box, etc.) is grouped together, stored and presented by the management centre as a single object called a **Record**.

A telephony subscription comprises all the composite records that refer to the same subscriber number.

A subscription may be composed of the following records:

- Directory record
- Main and/or secondary technical record (possibility of several main records for multi-location subscribers)
- Keys record
- Assignment record (login)
- Voicemail box record
- Forwarding record
- TWP record (only for the main technical record assigned to the main subscription number)

14.1.1 DIRECTORY RECORD

The directory record on the management centre contains all the **administrative information** (example: surname, first name and hierarchy, etc.). It is the entry point for subscriber management.

It comprises obligatory attributes required by the system to work properly as well as optional and customisable attributes.

14.1.2 TECHNICAL RECORD

The main technical record contains the **technical information** required to define a main subscription (subscriber number, technical hierarchy, feature classes, TL and PSTN categories,...). This information is located on the iPBX on which the subscription is declared.

The secondary technical record contains the technical characteristics of a secondary number. It is used for multi-line subscriptions.

14.1.3 KEY RECORD

This record contains the information required to define a subscriber's digital telephone set **key programming**. This information is available in the iPBX and is stored on the management centre.

Note : The creation and use of this type of record is optional.

14.1.4 ASSIGNMENT (LOGIN) RECORD

This record contains the information required to assign resources to subscribers. The assignment operation is used to link a subscription to a resource. This information is available in the iPBX and is stored on the management centre.

Resources consist of physical devices (cluster, card, channel, etc.), logical equipment (mac address, IP address, etc.) and subscriptions on which a subscriber may be logged (multi-user, hunt group, etc.).

There are as many resources records as subscription links with a resource.

Note : The creation and use of this type of record is optional.

14.1.5 VOICEMAIL BOX RECORD

This record contains all the information required to define the voicemail box (UCP) for a subscriber number. This information is available on the voicemail server and is stored on the management centre. It can be associated with a primary or secondary technical record.

Note : The creation and use of this type of record is optional.

14.1.6 FORWARDING RECORD

This record contains all the information needed to program forwarding for a given subscription.

Forwarding is characterised by:

- The type of forwarding (immediate, on busy, on no answer, predefined)
- The call origin (all calls, internal calls, external calls)
- The forwarding destination (voicemail, internal or external number)
- The recipient's number (for internal or external number only)
- For each type, the operator has the possibility to lock the programming so the terminal user cannot program it himself. This locking will be indicated to him/her on the terminal and on the MiVoice 5000 User Portal interface.

14.1.7 TWP RECORD

A TWP record can be assigned to one main number only.

CONSTRAINTS

The management of a new TWP record for a (main) subscriber is only available:

- For R5.x sites minimum
- In TWP server 3.2 and later

There is only one TWP subscriber number for the entire IP address / company-domain pairs defined for a multi-site configuration.

The TWP record is proposed for internal subscribers only.

The following information is needed to define a TWP user:

TWP server area

Server name: declared TWP server options. If only one TWP server has been declared, it is indicated in this greyed-out field (not accessible). This field is mandatory.

Company / domain: declared companies / domains options. If only one pair has been declared, it is indicated in this greyed-out field (not accessible). This field is mandatory. This companies/domains pair belongs to the previously declared TWP server.

Characteristics area

- **User surname and first name**: The surname/first name and e-mail fields will be initialised with the directory record data. The user can modified them if necessary. These fields will be listed when the configuration is imported. They will then be automatically synchronised when the directory record is modified if the surname and first name fields are identical in the TWP record and in the directory record. The synchronisation is performed on a field-by-field basis.
- **Email**. This field is mandatory; it corresponds to the TWP user's e-mail address and will be synchronised with the directory record.
- **Username** (username windows). This field is mandatory. This field is synchronised in case of synchronisation with Active Directory.
- **User login** This field indicates the windows login defined for MiCollab users.
- **Culture**. This field is used to choose the user language from an options screen. This field is mandatory.
- **Mobile**. The user's GSM number. This field is optional.
- **Two free input fields** for 100 characters each. These fields are optional.
- **Activated** field: To be ticked if the user is using TWP caller.

Telephony area

- **Device type** : select the TWP operating mode.
- **IP**: Telephone IP address for the call-recording application. This field is optional.

Groups area

- Area allowing the the groups to be configured according to the configured company/domain.

A TWP subscriber may belong to several groups.

A group is defined for one company/domain pair.

The company/domain pair is the same for the group and the subscribers it contains.

14.1.8 SUBSCRIBER TYPES

Different subscriber types can be defined while creating a subscriber. This choice is decisive for subsequent operations. In fact, depending on the selected subscriber type, the composition of the subscription and the parameters to enter in the technical record will be different.

Note : The list of subscriber types available in the subscriber creation window depends on the types of sites managed (XL/ XS/ XD or MiVoice 5000 Server) and their device release.

14.1.8.1 Internal subscribers

Internal subscriber is the commonest case. Its subscription comprises all record types: directory record, technical record, VM record, assignment record, key records, TWP record, etc.).

Other subscriber types are meant for more specific use, such as server configuration or even subscriber grouping.

14.1.8.2 Specific subscribers

The following subscriber types are meant for specific use. These subscriptions have a specific form and are generally made up of a directory record and a technical record, with specific characteristics.

ATDC subscriber

Subscription for the attendant console (switchboard)

Normal conf.

Teleconference function. Service called from a specific number.

Common conf.

Function used for teleconference services. Service called from a specific prefix.

System conf.

Teleconference with reinforced surveillance. Setting up a conference between subscribers belonging to a predefined list.

Teleconference

Teleconference management function Teleconference managed by an organiser who determines the subscribers authorised to participate in the meeting.

DISA (Direct Inward System Access)

The DISA function allows an external user to find the features of his/her set remotely. It is password-protected.

Interactive Voice Responder (IVR)

An automated attendant routes incoming calls to call distribution services (voice mail box, operator console, predefined numbers, etc). Only on XS/ XL/ XD iPBXs.

This subscriber is characterised by a script number (see technical characteristics).

Sub-group

Subscription used for hunt groups (a set of sets grouped together under a common directory number) to define the hunt group’s call number. Group subscription is used to define the hunt group’s call number. This is a logical subscription (that does not correspond to any device). Refer to Section

Managing hunt groups.

Super Hunt Group

This type of subscription is used to group a set of HUNT GROUP type subscribers or subscribers associated with a multi-key set.

Multi-user

The **multi-user** function is used for a physical set shared by several users and requiring an authentication.

Multi-user subscription is used for shared set users. It is a logical subscription assigned to a set subscription. Refer to Section Managing hunt groups.

Integrated voicemail box (IVB)

Subscription used for integrated voicemail (also known as IVB). Only on XS/ XL/ XD iPBXs.

VM hunt group

Subscription used for a messaging system other than integrated messaging (UCP for example).

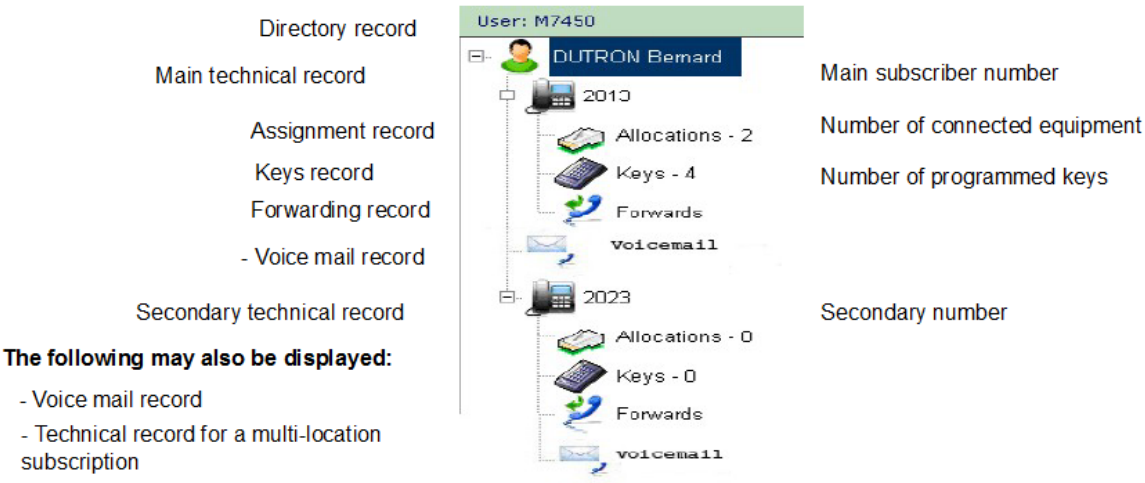
14.2 OVERVIEW OF A SUBSCRIPTION

14.2.1 TOPOLOGY OF A TELEPHONE SUBSCRIPTION

The telephony subscriptions and their various records are presented in graphic and hierarchical form in the subscription topology window.

This logical window is used to quickly access subscriber management by clicking the record to use directly.

The topology of a subscription is as follows:



It available in all the subscription configuration windows.

A **simple** subscription may contain the following records:

- Directory record
- Technical record
- Assignment record
- Key record
- Forwarding record
- Voicemail box record

- TWP record (only for the main technical record assigned to the main subscription number on R5.x sites minimum)

A **multi-line** subscription may contain the following records:

- Directory record
- Main technical record + Secondary technical records
- Assignment record (login)
- Key record
- Forwarding record
- Main voicemail record + (secondary voicemail record)

14.2.2 MIVOICE 5000 USER PORTAL

USER (AUTHORISED SUBSCRIBER) ACCESS TO THE MIVOICE 5000 USER PORTAL

The subscriber must have a PC with a web browser to be able to access this interface.

Access to the MiVoice 5000 User Portal is subject to massive or individual activation by the administrator.

The username and password must be entered. They are assigned by the administrator (see below, depending on the mode). If an e-mail address has been defined for the subscriber in the directory, an e-mail containing their password may be sent to them when their account is activated.

The application language is chosen according to the language defined in the web browser.
The subscriber using this function does not need any specific MiVoice 5000 Manager rights.
The IP address contained in the access path for this webpage is the same as the one for MiVoice 5000 Manager and must be known to the subscriber of the terminal in question.
The Administrator is advised to communicate this address to the persons using the MiVoice 5000 User Portal.
The version of the MiVoice 5000 and/or Mitel 5000 Gateways managed by MiVoice 5000 Manager must be above or equal to R5.1.
The application can be accessed in the following ways:

- Either by subscription number,
- Or by domain login if LDAP SSO mode is enabled,
- Or automatically if Kerberos SSO mode is enabled.

Whichever mode you choose, the first time you log on, the approval charter is displayed so you can read it and confirm that you have read it.

Using a PC with a web browser, log on to MiVoice 5000 Manager by entering the required IP address:

For a single multi-site configuration managed by MiVoice 5000 Manager

https://@IP7450 ou FQDN/userportal
or
https://@IP7450 or FQDN:4446

For several multi-site configurations managed by MiVoice 5000 Manager

https://@IP7450 or FQDN/userportal/?multisite=multisite-name
or
https://@IP7450 or FQDN:4446/userportal/?multisite=multisite-name

Example:
https://10.10.100.111/userportal/?multisite=finistere_sud

Access to the MiVoice 5000 User Portal is subject to massive or individual activation by the administrator.

The login and password are required to access the MiVoice 5000 User Portal. They are assigned by the administrator (see below, depending on the mode).

If an e-mail address has been defined for the subscriber in the directory, an e-mail containing their password and the link connection URL is sent to them when their account is activated.

The application can be accessed in the following ways:

- Either by subscription number,
- Or by domain login if LDAP SSO mode is enabled,
- Or automatically if Kerberos SSO mode is enabled.

14.2.3 SUBSCRIPTION LOG

The log is available in all the subscription configuration windows. It lists all the operations performed on the subscription.

The log is composed of the following information relating to the last modification of the subscription: the date, the nature of the operation and the name of the operator.

14.3 VIEW SUBSCRIPTION DATA

14.3.1 SEARCHING FOR SUBSCRIPTIONS

To facilitate access to managed data, the management centre proposes a multi-criteria search function. The search window is also used to access subscription management.

14.3.1.1 Defining search criteria

To access the search function:

- In the Telephony window, click Subscribers management then Search.
- In the *Search criteria* area, in the *General* tab, define the criteria required:
  - **Region / Multisite / Community / Site** / Position: select the search area from those proposed.
  - **Subscriber name / Subscriber first name/ Subscriber number**: enter the subscriber name, first name and/or number directly.
  - **Technical hierarchy**: select the company or company/department pair concerned. If only the company is identified, the search is made in all records in this company.
  - **Administrative hierarchy**: select the administrative hierarchy.
- If necessary, specify other search criteria:
  - **ICG** in the **General** tab (see the section Other search criteria).
  - **Profile** in the **Global** tab: displays the subscribers who have a specific profile.
  - **MiCollab role**: A list of options used to view the roles assigned for MiCollab users.
  - **Cloudlink role**: A list of options used to view the roles assigned for Cloudlink users.
  - In the **Advanced** tab: **Feature classes**, **PSTN categories**, **TL classes**, **Priority classes**, **Partitioning classes** and the **Set type**, **Set model**, **Set Variant** and **Backup site** options (see the section Other search criteria)
- After defining all the criteria, click **Search** to start the search.

To reset the search and delete all fields, click **Reinitialize**.

The list of subscribers that meet the search criteria is displayed on the right side in **Search result**.

14.3.1.2 Other search criteria

Choice of **ICG** (**General** tab):

The **ICG** options box is greyed out (inaccessible) when no multi-site configuration is selected.

When a multi-site configuration is selected and no site is selected:

- If the multi-site configuration contains a site with a release earlier than R5.1, the option is not available.

When a multi-site configuration is selected but no site is selected, the list of all the ICGs of this multi-site configuration is proposed, and the range indicated.

When a site is selected, the list gives the ICGs for this site.

The different items displayed can be sorted by **Name** or by **Range**.

Options **Set type** and **Set model** (**Advanced** tab):

When no **Set type** is selected, the **Set model** option proposes the terminal ranges supported by the MiVoice 5000 (MiVoice 5000 Server and Mitel 5000 Gateways).

When the terminal type is defined, the **set model** option allows the range to be selected (only for proprietary, proprietary IP or SIP types).

Options **Backup site** (**Advanced** tab):

The Backup site options box depends on other filters of the General tab to display any results:

- The Site options box
- The Community options box, if the Community mode is enabled.

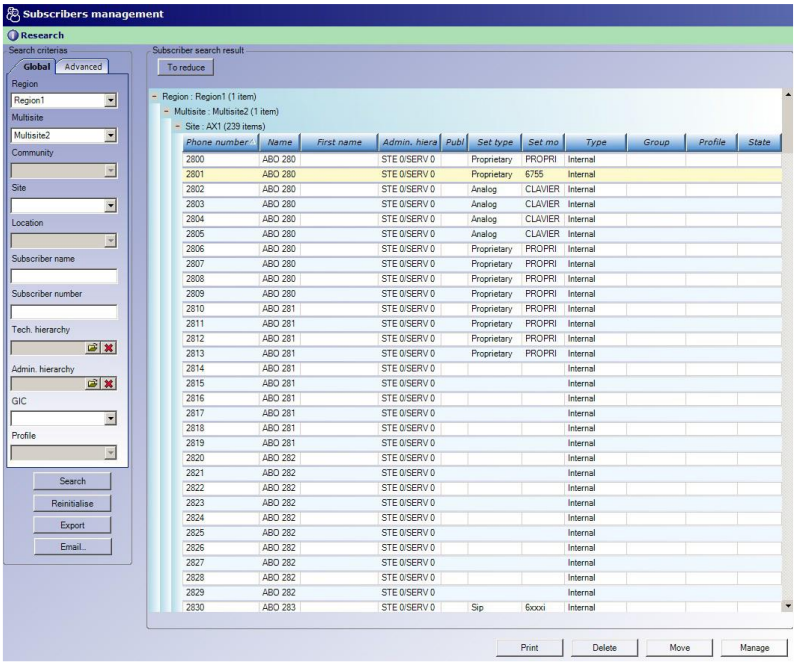
If these options are empty, the Backup site options box also stays empty.

Note : The extension types are not proposed for the search criteria.

14.3.1.4 Search result

The result area is used to display all the subscriptions that meet the defined search criteria. It is divided into two parts: one part, subscribers without number, and another part, telephony subscribers. The results can be sorted in ascending or descending order by clicking the header of each column.

Note : If the search result is too long, it may be necessary to narrow down the search criteria.



14.3.2 SELECTING A SUBSCRIBER

To display, modify or delete a subscriber, it is necessary to select the subscriber.

You can select several subscribers at a time.

- In the search result list, click a subscriber to select it.

  To select several subscribers, click the subscribers to be selected while pressing and holding down the **CTRL** key.

  Selected elements appear on a yellow background.

- After a subscriber (or group of subscribers is selected) the following options are accessible: **Delete**, **Move** or **Manage**.

14.3.3 DELETING A SUBSCRIBER

To delete a subscriber (or a group of subscribers):

- In the search result list, select a subscriber (or a group of subscribers).
- Click **Delete**.

  A deletion confirmation request window opens. Click **OK** to confirm the deletion.

Note : All the subscription records will be deleted.

14.3.4 MOVING A SUBSCRIBER

This function is used to move a subscriber (or group of subscribers) to another site managed on the same multi-site. When this function is activated, a wizard type window opens to guide you through the procedure.

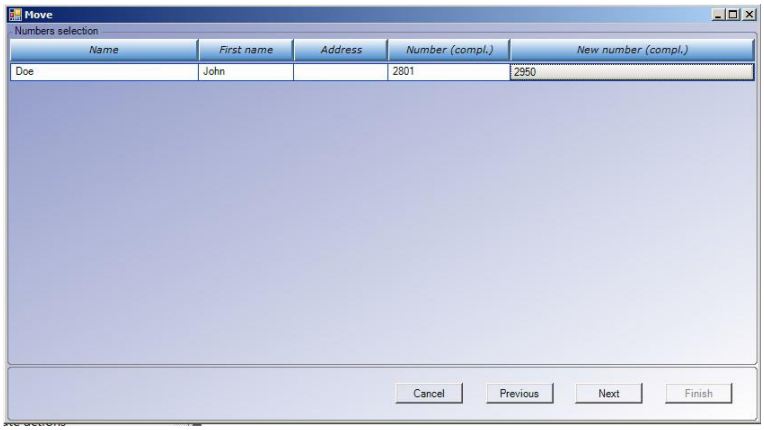
Note : The subscriptions managed in profile mode cannot be moved in this way. It is the Web Client application that is used to manage its movement individually.

To move a subscriber (or a group of subscribers):

- In the search result list, select a subscriber (or group of subscribers) then click **Move**.
- Accept the operation confirmation request.

The **Move** window opens so you can select the destination site.

- Select the destination site then click **Next**.

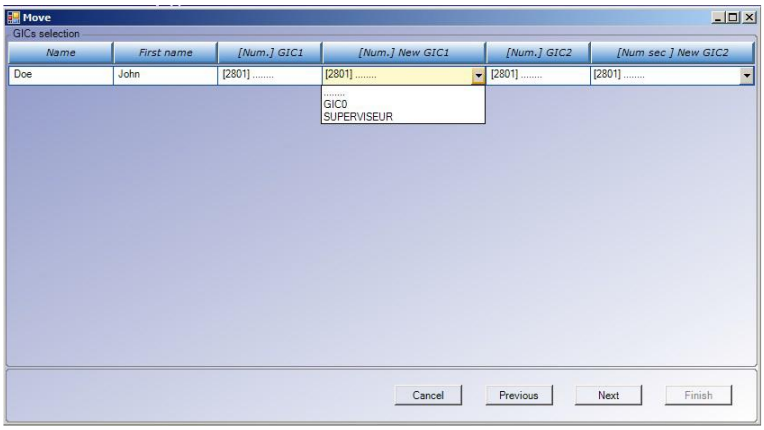


The screen lists information about the directory record to be moved. The following fields can be modified:

- **Address**: optional free
- **New number (compl)**: for modifying the number of the subscriber on the destination site.

The following screen is used to select the ICGs on the destination site.

- Click **Next**.



When a subscriber to be moved is assigned a digital or analogue terminal, the screen "TDM affectation select" is used to possibly modify the type of terminal which will be assigned to the subscriber on the new site. For a transfer to an XS/ XL/ XD site, selecting an "Analogue" or "Proprietary" terminal displays some question marks in the Location column. Click on the area to open the location window: select the location of the terminal on the card then click **Validate**. This location is then sent to the "TDM affectation select" window.

- Click **Next**.

The next screen is used to start the action later or immediately.

In the “R4.x subscriber" field, indicate with a tick whether "The subscriber keeps his or her terminal": in this case, the programmed keys will keep their location on the terminal.

- Click **Finish**. The result of the operation can be viewed on the massive action display screen.

14.3.4.1 Restriction on programmed forwarding

For subscriber transfer, pay attention to the following rules:

- Forwarding is retained when R5.2 subscribers migrate to R5.2.
- Forwarding is lost when subscribers migrate from a release below R5.2 to R5.2.
- Forwarding is lost when R5.2 subscribers migrate to R5.1.

14.3.4.2 Moving a subscription containing a TWP account

When a subscriber is moved, it is possible to keep or not to keep the TWP record. Depending on your choice, tick or untick the **Keep TWP record** option.

Modify the subscription's TWP record if the subscription is moved while changing its number and keeping its TWP record.

14.3.4.3 Moving a subscription to its own backup site

If a subscriber declared with a backup site must be moved to this same backup site as a main subscription, he/she must first be removed from the backup site in question.

14.3.4.4 User password

If a user password has been modified, it is not kept when the subscriber is moved. A new password is assigned: it corresponds to the default user password defined in the multi-site configuration.

While moving an R5.3 site to an R5.4 site: the default user password defined in the multi-site configuration is assigned to the subscriber.

In both cases, the user can receive a notification e-mail if he/she meets the conditions described in the section (Configuring a site / a server cluster).

When an R5.4 site is moved to R5.3, the subscriber loses the user password and is in the subscriber password + IVB password configuration (default iPBX password, i.e. 0000).

14.3.4.5 Case of DID number reassignment

When subscribers are moved from one site to another with a change of number, the DID numbers of the subscriptions must be reconfigured in the technical record:

See the section Creating a primary technical record

Check whether the numbers are correct then confirm the action.

14.3.5 ACCESSING SUBSCRIBER MANAGEMENT

To view or manage one or more subscriber records:

- In the search result list, select a subscriber (or a group of subscribers).
- Click **Manage**.

The subscription window opens so you can view or use the record. See the section Subscription management for more information about the procedure.

Note : If several subscribers are selected, the actions executed on the first subscriber selected will also be applied to the other subscribers selected.

14.4 SUBSCRIPTION MANAGEMENT

(Administrator, User or Telephony). Users with a directory profile have access to subscriptions only in consultation mode.

Managing a subscription involves creating, modifying, and deleting records. A subscription can be managed when:

- A new subscription is created
- An existing subscription is selected.

Note : The screens are presented for information purposes only. Depending on the configuration installed, the tabs, fields and identifiers may differ from those presented in this manual.

14.4.1 CREATING SUBSCRIBERS INDIVIDUALLY.

The **Unitary creation** menu is used to create subscribers individually. It offers a wizard type widow which guides the user through the creation of the different subscription records. At the end of the procedure, a programming action is started to take account of the creation in the system. The following simple subscription creation steps are proposed by the wizard:

- Creating a directory record
- Creating a technical record
- Creating an assignment record (login)
- Creating a key record
- Creating a forwarding record
- Creating a voicemail box record
- Creating a TWP record (main subscription only)

Creating a subscription involves creating at least one directory record:

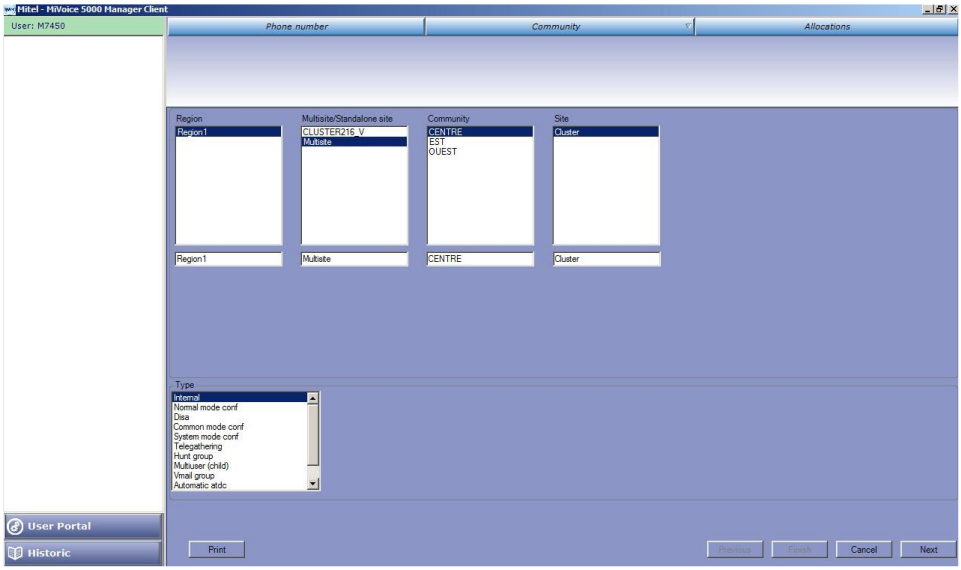
The application also proposes massive subscriber creation via a configurable Excel file. For the massive subscriber creation procedure, see the section **Massive creation**.

USING THE FEATURE FOR AN R5.2 SITE AND HIGHER

The forwarding record is not available for R5.1 sites. The procedures for deploying the other records are the same as for an R5.2 site.

- In the Telephony window, click Subscribers management then Unitary creation.

A creation window opens.



- Select the region / multi-site / site to which the new subscriber will be attached.
- Select the subscriber type then click **Next**.

Note : Depending on the selected subscriber type, different fields will be accessible in the different records.

An empty directory record opens. The fields in this record are described in the section **Directory record**.

- After creating the directory record, the wizard creates the following records:
  - Technical record
  - Assignment record (login)
  - Keys record
  - Forwarding record
  - Voicemail box record.

For each record created, a corresponding symbol appears in the subscription's topology area.

- At the end of the creation operation, click **Program** to confirm the subscriber creation.

The created items are indicated by a green tick. A notification is displayed, and the telephony log updated.

- Click **Finish** at the end of the procedure.

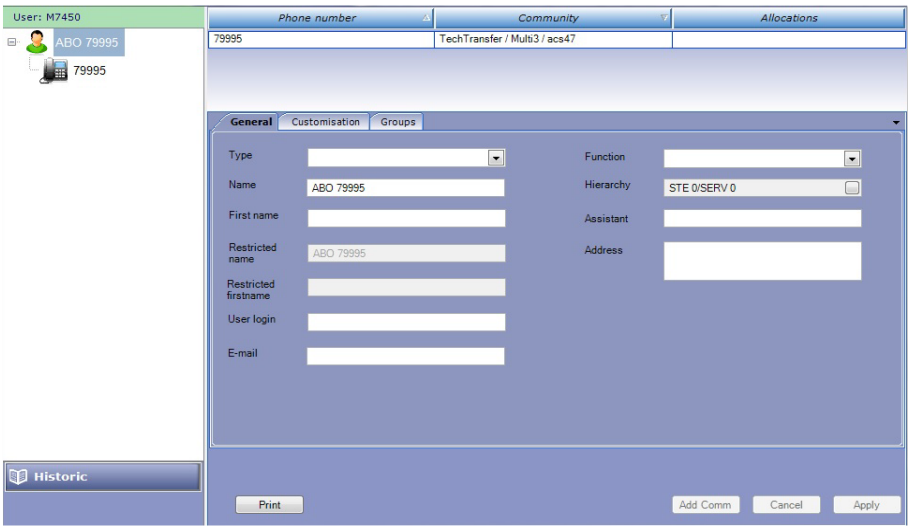
14.4.2 DIRECTORY RECORD

The following operations are possible on a directory record:

- Create
- View / Modify
- Create a multi-location subscriber

14.4.2.1 Description of the directory record

The directory record is organised as follows:



General tab: The fields are as follows:

FIELDS	DEFINITION
Type	Options list defined in the Directory parameters menu Example: Mrs, Mr, Room, Office, etc.
***Name, * First name**	Surname, first name of the subscriber
Restricted name, first name	Entered by the system. These fields contain the information in the previous 2 fields but without special or accented characters.
User login	Used to assign a Windows login to a MiCollab user in the LDAP directory when this mode is activated. This field in UTF8 format must contain a maximum of 120 characters.
Email	E-mail address of the subscriber
Function	Options list defined in the Directory parameters menu Example: Director, manager, assistant...

Key	Entered by the system.
***Hierarchy**	Administrative hierarchy
Address	Information about subscriber location Free input Example: Site, office…
Mobile	Subscriber's mobile phone number. This setting is configurable and visible for sites running R8.2 and later. **Note: Customisable attributes can also be used to enter mobile phone numbers. For more information, see Chapter 13.3 – Customisation**
VIP	Checkbox. Designates the subscriber's calls as VIP calls. Calls from this subscriber are routed through VIP reception.

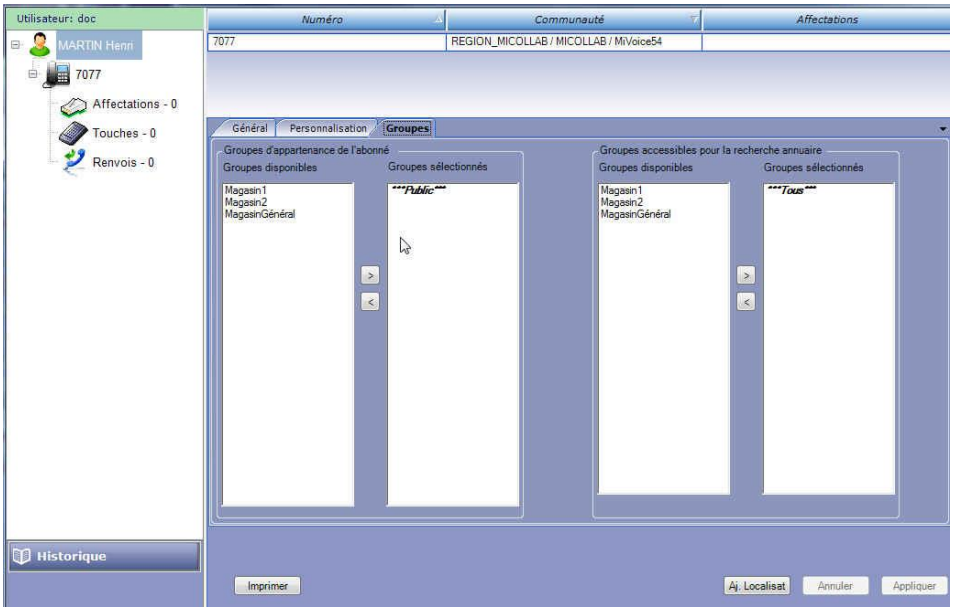
Fields with * are compulsory.

Customisation tab

This area contains customised attributes. They have been defined in the **Customisation** menu.

Groups tab

This tab is only visible if the attribute **Activation of directory groups** is enabled in the property of the multi-site architecture (see the section - Directory groups).



This tab contains two parameters:

- **The subscriber's group membership**: They are selected from all the groups defined in the directory. By default, no group is associated; the record is said to be "public". This is represented by the item **"***Public***"**.

- **Groups accessible for directory search**: They are selected from all the groups defined in the directory. By default, the subscriber sees all the records belonging or not belonging to a group; this is represented by the item ***All***. As soon as a group is added to this list of groups accessible at the same time as the group appears on the list of groups, the item ***Public*** appears indicating that the subscriber will see all the records belonging to the groups available on this list, but also the "public" records, i.e. those not belonging to any group.

14.4.2.2 Creating a directory record

- In the **Telephony** window, click **Subscribers management** then **Unitary creation**.

A new creation window opens.

- Select the region / multi-site / site to which the new subscriber will be attached.
- Select the subscriber type then click **Next**.

The directory record creation window opens. In creation mode, all the records fields are empty.

- Enter the parameters for the directory record. The fields can be filled in as follows:
  - By entering the value directly in a data entry area (name, first name, e-mail, address, etc.)
  - By selecting a value from a list (title, function, administrative hierarchy, etc.)
- After entering all the parameters, click **Next** to continue and access the technical record creation window.

When the directory record is created a symbol, as well as the subscriber's name, appears in the subscription topology window.

After creating a directory record, the operator can complete the subscription with:

- One or more technical records
- For each technical record:
  - One or more directory records (for multi-location subscriptions)
  - One allocation record
  - One key record
  - One forwarding record (only for R5.2 sites or above)
  - One voicemail box record

14.4.2.3 Modify the directory record.

- Select a subscriber.
- In the *Topology* window, click the symbol for the directory record to be modified.
- Modify the necessary parameters fields then click **Apply**.

The modifications are taken into account.

ASSIGNING A SITE FOR DOWNLOADED DATA

For directory records created from a synchronisation with an external source, the **Add localization** button is used to assign a region / multi-site / site to the subscriber (see **Managing abbreviated numbers**).

- Select a subscriber.
- In the **Topology** window, click the symbol for the directory record to be modified.
- Click the **Add location** button, situated at the bottom of the directory record.

A new selection window opens.

- Select a region / multi-site / site and subscriber type then click **Next**.
- Enter the directory record information.
- Click **Apply**.

Note : Adding a location also makes it possible to attach a person with an already existing telephony subscription to another subscription (on the same site or on another site on the multi-site).

SUBSCRIPTION IN PROFILE MODE

Depending on the status of the subscription, a subscription created in profile mode contains any of the following buttons:

- Lock:
  - when the subscription is unlocked (subscription not compliant with its profile), the **Lock** button is used to check the subscription's compliance with its profile.
  - **The Lock** button is used to lock the subscription when it complies with its profile.
- Unlock:
  - This button is used to unlock a locked subscription so it can be modified (without this unlock function, the information defined by profile cannot be modified).

A subscription in profile mode also contains a **Reset profile** button. This button is used to remove a subscriber from profile mode. The subscriber will no longer appear in Web Client.To re-assign him a profile, it will be necessary to perform an upgrade (see the section **Export**), by re-assigning him a profile, then an import (see the section **Importing data**).

For more information about subscriptions created in profile mode, see **Managing subscriptions in profile mode** and **Managing profiles**.

14.4.2.4 Deleting a directory record

The directory record can be deleted from the subscriber selection in the search result window. This deletion will result in the deletion of the entire subscription (including the technical records and voicemail box records).

14.4.3 TECHNICAL RECORD

The following operations are possible on a technical record:

- Create
- View / Modify
- Delete
- Creating a secondary technical record (for multi-line subscriptions)
- Creating an additional number
- Creating a UCP voicemail box record
- Creating a TWP record

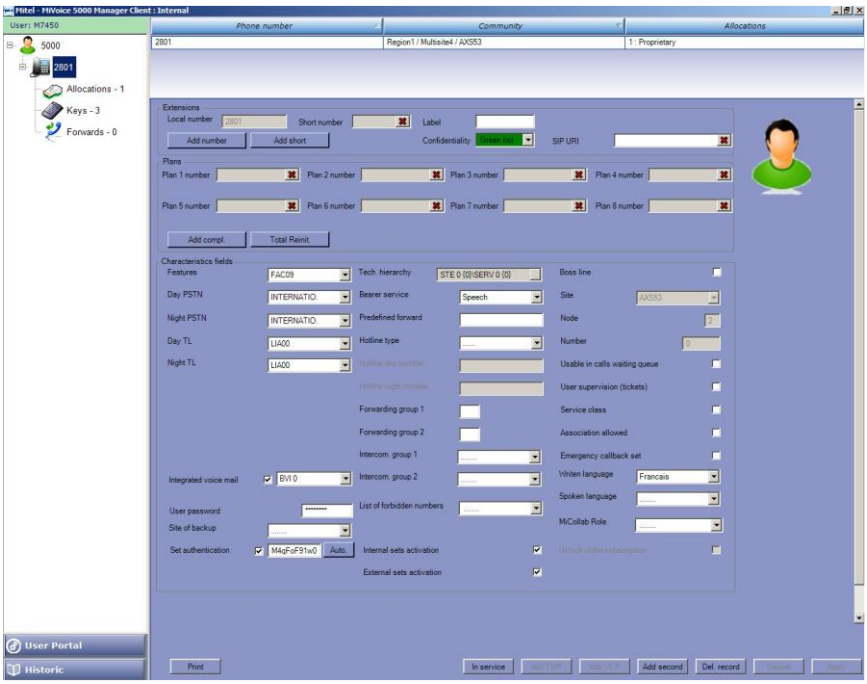
14.4.3.1 Accessing the technical record

In individual creation mode, the wizard proposes the creation of technical record after the directory record is created.

In management mode, click directly the technical record symbol in the subscription topology window.

14.4.3.2 *Description of the technical record*

The technical record is presented as follows:



This window contains the following areas:

- Numbers area

This area includes LDAP directory number record data and information about the numbers. It is used to assign an internal number and abbreviated number, and to define a label and confidentiality.

- **Plan** (Numbering plan) area

This area is used to create additional numbers which will be used to reach a subscriber from an external network (PSTN or TL).

- **Characteristics** (Technical characteristics) area

This area is used to define the subscriber's technical characteristics. It is used to select telephony parameters such as feature classes or PSTN categories, and to define the specific characteristics of the various subscription types. The fields to fill in depend on the type of subscriber selected during creation.

- Picture area

The subscriber's picture, if available, is displayed.

A picture can be modified, deleted or added. For this, click the picture location to open the modification window.

14.4.3.3 *Creating a primary technical record*

In individual creation mode, the wizard proposes the creation of technical record after the directory record is created.

The technical record input phases are:

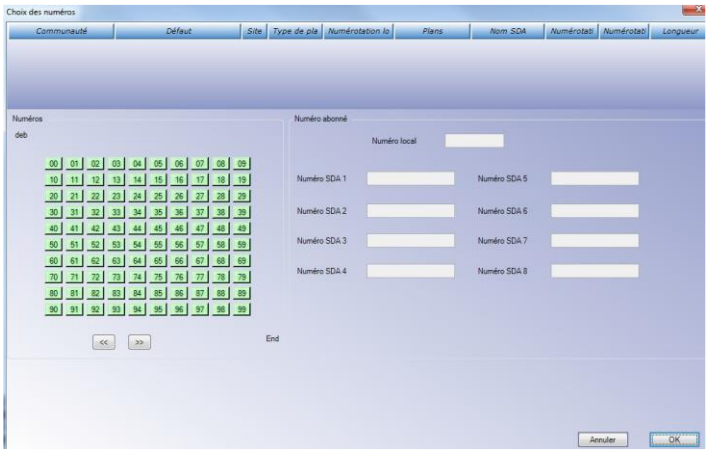
- Creating a subscriber number
- Creating an abbreviated number (optional)
- Entering a label
- Defining confidentiality
- Creating an additional number (optional)
- Defining technical characteristics

ASSIGNING A SUBSCRIBER NUMBER

To assign a subscriber number:

- In the technical record, ***Numbers*** area, click **Add number**.

A number input window opens.



- Select the type of plan to use from the list.
- In the ***Numbers*** area, choose a number block. Use the **>>** symbol to scroll the blocks. The available numbers are indicated in green.
- Click the number you want (or enter the number directly in the ***Local extension*** field by the right).

The number is displayed in the ***Local extension*** field.

Note : If the number is a DID number, it is automatically displayed in the Plans area (Plan 1 No.).

- Click **OK** to confirm.

The subscriber number is created.

CREATING AN ABBREVIATED NUMBER

An abbreviated number may be associated with the active subscriber. The abbreviated number may consist of 1 to 4 digits, depending on the length defined in the Administration menu.

To create an abbreviated number (short number):

1. In the technical record, ***Numbers*** area, click **Add short**.

   An input window opens.

2. Enter the abbreviated number associated with the subscriber.

   A list of existing numbers starting with the 1st digit entered appears during the input.

3. Click **Validate**.

ENTERING A LABEL

The label field is used to enter a label which will be displayed on the telephone set.

DEFINING CONFIDENTIALITY

Confidentiality enables you to define the list of records accessible through subscriber search. Possible values are: green list (accessible to the public), orange list (accessible within the organisation only), red list (access forbidden). This field is mandatory.

CREATING AN ADDITIONAL NUMBER

The **Add number** button is used to create additional numbers which will be used to reach a subscriber from an external network (PSTN or TL).

The procedure for assigning an additional number is the same for a main number.

Note : If the previously created number is a DID or TL number, it is automatically displayed in the Plans area (Plan 1 No.).

DEFINING TECHNICAL CHARACTERISTICS

The fields in this area can be defined:

- By entering the value directly in the data entry area
- By selecting a value from a list
- By activating the parameter through a tick.

The telephony parameters have been previously defined in the Technical characteristics menu.

Note : The list below is given for information purposes only. These characteristics are displayed according to the type of subscriber defined.

CHARACTERISTIC	DEFINITION
Features	For selecting a feature class (a set of rights granted to a subscriber on a device).
Day/night PSTN	For selecting a day PSTN and night PSTN. The difference between DAY and NIGHT is the switchover from day to night and vice-versa, which is carried out by the barring calendar.
Day/night TL	For selecting a day TL class and night TL class. The difference between DAY and NIGHT is the switchover from day to night and vice-versa, which is carried out by the barring calendar.
Priority	For selecting a priority class.
Incoming/outgoing partition	For selecting incoming partition classes (incoming calls) and outgoing partition classes (outgoing call).
Technical hierarchy	Refers to the company/department pair defined on the iPBX.
Service support	Indicates the type of medium assigned to the equipment to select transparent or non transparent routing for an inter-site call or call to an external network (PSTN or TL). Possible types are: **- Voice** The call is routed from the equipment on "speech" or "combined" trunk groups, but not "data" trunk groups. **- Data** The calls is routed from the equipment on "data" or "combined" trunk groups to guarantee transparency. **- Data fallback speech** If the attempt to route the equipment call on "data" and "combined" trunk groups fails, a second attempt to route the call is made using "speech" trunk groups, if necessary.
Predefined forward	Enter the internal or external number to which the user is to be forwarded. Forwarding to an external number is only possible if the "Immediate Forwarding Allowed" option is enabled. The number entered can have a maximum of 17 digits, including direction access prefixes (0, 00).
Hotline type	This option is reserved for the definition of a direct line set (except an ISDN set). A hotline call can be made in two ways: **- Immediate**: an internal or external number is dialled immediately and automatically on off-hooking. **- Time-out**: an internal or external number is dialled automatically 5 seconds after off-hooking.

Day/night number	These fields are only displayed if the "hotline type" has been selected, i.e. “immediate” or “delayed” line. Enter the internal or external number corresponding to the hot line set, on this line. The number entered can have a maximum of 17 digits, including direction access prefixes (0, 00). **Note :The DAY number is used when the system is in DAY or reduced day service.** **Note :The NIGHT number is used when the system is in night service (OP inactive and calendar in force).**
Search group No. 1 - 2	It is possible to assign sets to one or two search areas so users can make searches on different parts of the installation without disturbing other users not located in this area. **- 1st case**: if the user paging group numbers (called and calling parties) are identical (0 to 254), the pager rings (with call end forwarding). **- 2nd case**: if the caller end paging number group is 255, the pager rings (with call end forwarding). **- 3rd case**: the user paging group numbers (called and calling parties) are different and the caller paging group number is not equal to 255, the called extension rings, but the pager does not, despite call end forwarding.
Intercom Group 1-2	Subscriptions in the same INTERCOM group can supervise and be supervised.
Integrated voicemail box	For assigning an integrated voicemail box (IVB) (on XS/ XL/ XD). Not displayed if another messaging system is declared (UCP).
Class	For assigning a class to the voicemail box. When a box is created, class 0 (IVB 0) is automatically assigned to the subscriber.
Reset password **(iPBX < R5.4)**	For resetting the subscriber password to 0000 if the password has been modified (tick the box to reset the password).
Reset IVB password **(iPBX < R5.4)**	For resetting the IVB password to 0000 if the password has been modified (tick the box to reset the password).

User password **(iPBX >= R5.4)**	For assigning to the subscriber a common subscription and IVB password different from the default multi-site password. The user password is used for the following types of subscribers: - Internal - Multi-line (appears only on the main technical record) - Multi-user (for the subscription only) - Automated assistant (for the IVB only) - ATDC (used only in a multi-line subscription, for secondary lines) - DISA (server). **Note :If the subscriber is moved, this password is lost and replaced with the default password defined in the multi-site configuration. An e-mail is sent to the user to give him the new password value (if e-mail notification is enabled in the multi-site configuration and if the subscriber's address is entered in the directory record).**
Unlock subscriber	If the user enters an incorrect user password three times (on the terminal or IVB), the subscription is temporarily locked. This function is used to unlock the subscription (changing the password also unlocks the subscription). The value of the password is not affected.
Right to class service	If ticked, class service allows analogue sets to receive the following information about an on-going call: **- Caller number** (if there is no call offering restriction) **- Time and date of call**
Manager line	If ticked, the manager line is defined in the filter function.
Site / Node / Number	Attachment site.
Association authorised	If ticked, several devices can be assigned to a subscriber.
Password	For defining a password for the DISA function.
Usable in calls waiting queue	- Waiting list
- Subscriber monitoring (record)	If the box is ticked, a monitoring record is issued at the end of a user’s communication.
Emergency callback set	If ticked, the terminal is defined as an emergency callback terminal. Wire multi-line, DECT and without terminal sets cannot be configured as emergency callback terminals.

ATDC type	For selecting the ATDC type. **- Class A**: status display of each interface on a key. **- Class B**: all incoming calls are managed with a single key, and all internal calls with another key. Class A is reserved for configurations with fewer extensions and trunk lines.
Script number	A script defines the IVR tree structure. The caller is thus guided via the menus proposed to him. The scripts are managed by an external remote management tool (M7420 Update). Assign a script number to the IVR subscriber (from 0 to 9 and 11 to 15). **Note :Script number 10 is not allowed (10 is the initialisation value for script nodes).**
Written language	Language command used for displays on digital terminals: this option is used to choose three languages including French, English and German, for example, from N possible languages.
Spoken language	This field is only displayed when several languages are defined in the tones menu. It is used to transmit announcement messages in the user's language.
Room number	In the multi-user function, it is used to assign a user subscription to a terminal subscription.
MiCollab role	For assigning a role to the subscription. If any of the roles (options) is entered in this field, the subscription will correspond to a MiCollab user and may be created or updated during the realignment phases (synchronisation with the MiCollab server) or after adding, modifying or deleting a MiCollab role.
Cloudlink role	For assigning a role to the subscription. If any of the roles (options) is entered in this field, the subscription will correspond to a Cloudlink user and may be created or updated during the realignment phases (synchronisation with the Cloudlink server) or after adding, modifying or deleting a CloudLink role.
Barring ranges **Day / night**	Day / night barring range number for the subscription. Valid only if the site is using release R5.1A.
Barred numbers list	Replaces the barring classes for R5.1B (upwards) site subscribers. For assigning a barred number list to the subscription.
Backup Site	Dual Homing function available to site subscribers as of R5.1 B.
Dynamic SIP DECT backup	For SIP DECT allocations, the subscription is allowed to have a dual homing site according to its location.

Terminal authentication (iPBX >= R5.4 SP2)	Password used by terminals to log on to the IPBX. If a password exists, it is displayed as clear text. The password can be entered (between 8 and 16 hexadecimal characters) or allocated automatically by clicking **Auto**.
User Portal password	Appears if the User Portal integrated in MiVoice 5000 Manager is disabled: the MiVoice 5000 Manager administrator has here the possibility to allow the subscriber to access the User Portal and to generate his/her password. Does not appear when the MiVoice 5000 Manager User Portal is activated since the MiVoice 5000 Manager User Portal button is on the bottom left part of the window.
Activate internal / external terminals	Function activated by default. Concerns incoming calls only. When an external terminal has been declared in the assignment record (example GSM), the user may deactivate any of the (internal or external) subscriber's terminals or even both of them (in this case, there is automatic forwarding to voicemail or to attendant console if the subscriber does not have any voicemail system). A message or information symbol is then returned by the internal terminal, indicating that incoming calls are deactivated. The subscriber may perform the operation for any of his/her terminals from the MiVoice 5000 Manager User Portal.

After entering all the parameters of the technical record, click **Next** to validate the creation.

When the technical record is created an icon, as well as the subscriber’s number, appears in the subscription topology window.

14.4.3.4 Modifying a technical record

- Select a subscriber.
- In the ***Topology*** window, click the technical record to be modified.
- Modify the necessary parameters fields then click **Apply**.

The modifications are taken into account.

14.4.3.5 Deleting a technical record

- Select a subscriber.
- In the ***Topology*** window, click the technical record to be deleted.
- Click the **Del. record** button located at the bottom of the technical record.
- Confirm the deletion by answering **OK** to the deletion request.

The technical record is deleted and no longer appears in the subscription topology.

14.4.3.6 Adding a TWP record for an existing subscription

A TWP record can be assigned to one main number and the **Add TWP** button is proposed for internal subscribers only.

- On the technical record management screen of the subscriber concerned:
- Click the **Add TWP** button located at the bottom of the technical record.
- A window opens so you can enter the subscriber's TWP record.
- Fill in the different fields as indicated in the section **TWP record**.
- Click **Apply** to confirm the account creation..

14.4.3.7 *Adding a voicemail box record for an existing subscription*

A UCP voicemail box may be associated with a main or secondary technical record.

- On the technical record management screen of the subscriber concerned:
- Click the **Add UCP** button, located at the bottom of the technical record.
- A window opens so the UCP record can be entered.
- Fill in the different fields.
- Click **Apply** to confirm the account creation.

14.4.3.8 *Forced synchronisation of an existing subscription with MiCollab, CloudLink or a SIP DECT terminal*

A **Sync. Apps** button is displayed on subscriber profile pages with a MiCollab role, a CloudLink role or a SIP DECT terminal.

Note: The Sync. Apps button appears only for internal subscribers.

On the technical record management screen of the subscriber concerned:

- Click the **Sync. Apps** button, located at the bottom of the technical record.

14.5 ALLOCATIONS MANAGEMENT

Given the separation made between the subscription and terminal in the MiVoice 5000 solution, it is possible to define all the subscriptions regardless of physical terminal assignment. This assignment may be done in a second phase.

The assignment operation consists in defining a subscription/equipment pair.

There are 2 types of assignments:

- **The one carried out by the user** (via the management centre) who specifies the type of equipment to associate with the subscription.
- **The one performed by the subscriber** on the terminal (manual login) who associates a subscription with a device.

EQUIPMENT LIST

The following equipment can be assigned:

- Analogue terminals, including CLASS terminals, modems and faxes.
- Proprietary terminals (digital TDM - 53xx/G2K TDM terminals)
- Proprietary IP terminals (digital IP - 53xxi/G2K IP terminals)
- SIP (Mitel 6000 SIP Phone/BS for PC/IOS or non-Mitel SIP phones)
- IP or SIP DECT
- OMM conference
- Ringer relais
- External terminal (outside the installation, GSM or fixed number, etc.)

From version R8.0 SP2 and relative to sites ≤ 7.2 of the multisite, the Portable DECT assignment is also offered.

EQUIPMENT MANAGEMENT

The equipment can be divided into 3 categories:

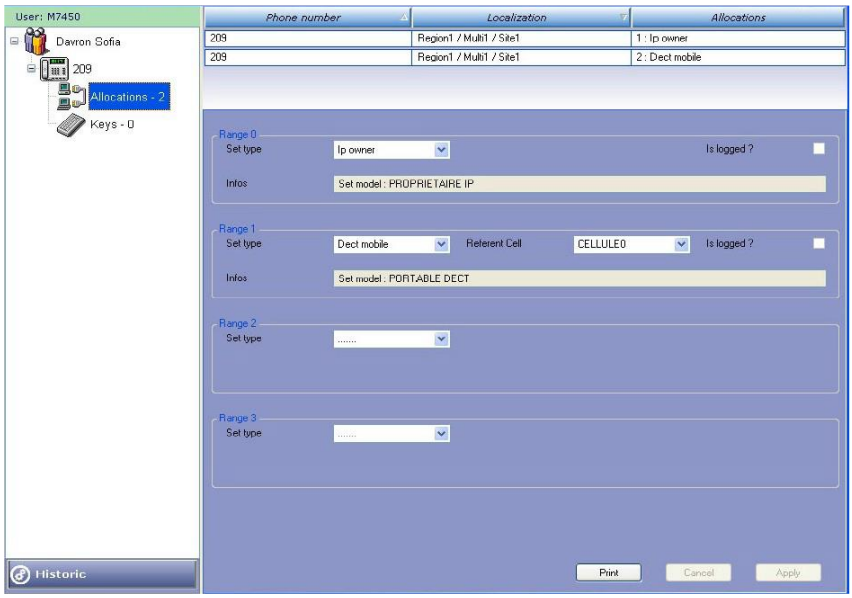
- **Managed equipment**: assignment operations can be performed on the management centre. Fixed TDM sets (analogue, G2K TDM, Office TDM, S0 and S2 sets) are fully managed because it is possible to define the type of set and physical set assigned to a subscription, through the MMC.
- **Partially managed equipment**: assignment operations can be performed on the management centre, but they must be completed through manual actions on the terminal. This applies to IP and DECT sets.
- **Equipment not managed**: assignment operations cannot be performed on the management centre. Manual login on the terminal is necessary.

14.5.1 ACCESSING THE ALLOCATION RECORD

- In individual creation mode, the wizard proposes the creation of allocation record after the technical record is created.
- In management mode, click directly the allocation record symbol in the subscription topology window.

14.5.1.1 Description of the allocation (login) record

The allocation (login) record is presented as follows:



A list of devices (XS, XL, XD) is proposed on the management centre. When a device is added or deleted, a notification is sent to the management centre.

For simple subscriptions, only one terminal is assigned to the subscription.

If the parameter **Association allowed** is ticked in the technical record characteristics, it is possible to assign several devices to the same subscription (up to 4).

In the above example, a subscriber with a fixed terminal and an external terminal.

14.5.1.2 *Creating an allocation*

For a given device:

- Select the set type on the dropdown list.

Information on the set is displayed in the *Info* area.

Note : Depending on the selected set type, the fields to fill in may differ.

- For non-IP sets, the **Localization** field appears and is filled in with the device location on the iPBX.
- If the device is connected already, the **Is logged?** box is ticked.
- Click **Apply** to confirm.

14.5.1.3 *Modifying an allocation*

For a given device, follow the procedures described above by selecting another set type.

If the **Logoff acceptance** feature is activated (see the section **Definition of features**) in the subscription, it is possible to assign a new terminal to this subscription in place of the previous one. Moreover, the set assigned to the subscription may be moved to another subscription. The subscription is said to be **replaceable** if these operations are allowed.

For partially managed sets, there is no specific equipment control. So, if the subscriber changes his or her set and uses the same type of set, the new login will be accepted.

The type of set assigned to a subscriber that is part of a hunt group must be compatible with the type of set used by other subscribers in the hunt group.

DELETING AN ALLOCATION

To delete an assignment, select **[...]** from the set type list then click **Apply**.

14.5.2 MANAGING KEYS

The Keys record is used to program the keys of a **digital, IP or SIP terminal regardless of the terminal used**.

The keys have a logical dialling system and can be placed anywhere (except in special cases). When a set is logged on the subscription, the keys available depend on the set type.

Depending on the model of the terminal logged on to the subscription, the pictures of the terminal and of the associated terminal(s) are displayed in the frame reserved above the **Details** button. DECT terminals and old generation terminal models are not displayed.

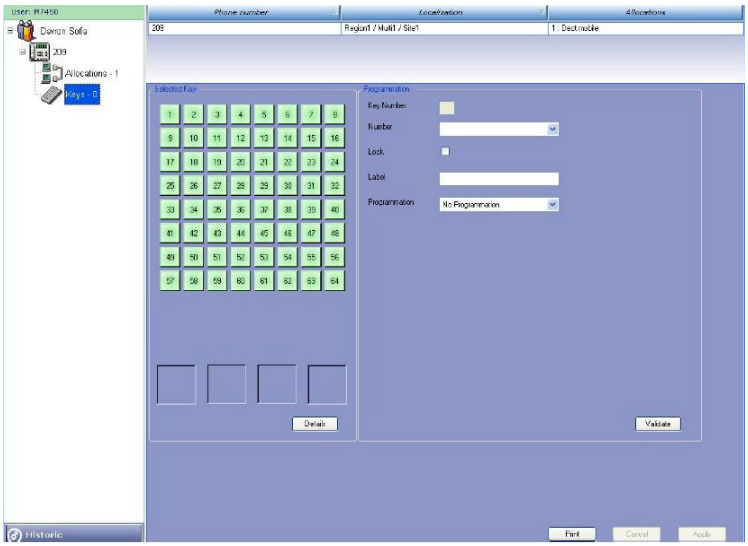
14.5.2.1 *Accessing the keys record*

In individual creation mode, the wizard proposes the creation of keys record after the technical record is created.

In management mode, click directly the keys record symbol in the subscription topology window.

14.5.2.2 *Description of the keys record*

The **keys** record window is as follows:



A table displays the status of programmed keys. Up to 256 keys can be programmed, depending on the site version:

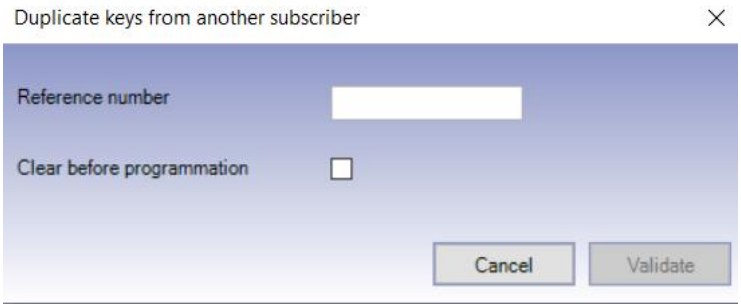
- 64 keys for <R8.1 sites
- 256 keys for ≥ R 8.1 sites

Note: For the site versions with 256 keys (sites ≥ R 8.1), the MiVoice 5000 Manager displays the keys on 4 pages of 64 keys each. To browse through the page, click the >> button to go to the next page, and the << button to go to the previous page.

The pictures displayed can be enlarged by clicking on them.

The **Details** button gives access to a table of programmed keys on the terminal.

The **Duplicate** button opens a new window. The window is used to copy the keys from another subscriber.



- Enter the source subscriber's number in the **Reference number** field.
- If necessary, tick the box **Clear before programming** to clear the current keys of the target subscriber before copying the new keys.

The associated picture makes a correspondent between the numbers of the keys in the table and their location on the terminal.

To program a key:

- Select a key to be programmed from those available (in green).

The already programmed keys are marked in red or blue if they are also locked.

- On the right side, in *Programmation*, fill in the following fields:
  - **Key Number**: Enter the value
  - **Phone number**: Options

- **Lock**: Tick this box to lock the key
- **Label**: Free input
- **Programming**: select the function associated with the key from the function list.

Note : Depending on the programming type chosen, additional input fields may be displayed.

- After entering all the parameters, click **Validate**.
- The key defined is displayed in red (in blue if it is locked).
- Programme the remaining keys in the same way if required.
- Click **Apply** to start programming the key.

A notification is displayed, and the keys log updated.

PROGRAMMING TYPES

- No programming
- MobileLink
- XML
- Dialling
- Cancel all forwarding
- Fixed forwarding
- Forward on busy
- Forward on no answer
- Forward all calls
- Agenda activated
- Agenda deactivated
- Locked
- General standby
- Filtering
- Do not disturb
- Intrusion not allowed
- Your number monitoring
- External line monitoring
- Your calls forwarded to
- For call monitoring
- Your calls from
- Phone box
- Tone dialling
- Your personal external line
- Hunt group I/O command
- Mail box supervision
- Messages deposit
- Client check-out
- Wake-up / Meet me
- Client check-in

- Alarm monitoring
- Call supervision internal
- Supervision of incoming calls 1
- Supervision of incoming calls 2
- Supervision of internal TL calls
- Overload signalling
- Reservation signalling
- Console active
- Hold
- Storage resend

14.5.2.3 Modifying a key

To modify the programming of a key:

- In the keys record, select a key to modify.
- Modify the necessary parameters then click **Apply** and **Apply**.

14.5.3 FORWARDING RECORD

Note : The forwarding record is not available for subscribers of sites with a release below R5.2.

Forwarding is applicable to the following subscriber types:

- Internal subscribers
- Hunt group, super hunt group and VM hunt group
- Automated attendant.
- Forwarding records can be created or modified in several modes:
- **Unitary**: one record for each subscriber type
- **Through mass action**. For the mass action procedure, see the section **Mass modification on subscribers**.
- **Through mass subscriber creation**, using a configurable Excel file. For the massive subscriber creation procedure, see the section **Massive creation**.

14.5.3.1 Forwarding record for internal subscriber

For the internal subscriber, the forwarding record comprises 4 areas which correspond to the type of forwarding to be assigned according to their origin.

Forwarding is characterised by:

- The type of forwarding (immediate, on busy, on no answer, predefined)
- The call origin (all calls, internal calls, external calls)
- The forwarding destination (voicemail, internal or external number)
- The recipient’s number (for internal or external number only)

For predefined forwarding:

Forwarding is to be defined by the operator in the technical record.

If it has been defined, the fields in the **Predefined** forwarding area can only be viewed and correspond to the forwarding characteristics defined by the user on the terminal (either from the terminal, or from the MiVoice 5000 User Portal interface).

Lock box

For each area (except predefined forwarding), this box, when ticked, prevents the terminal end-user from modifying the forwarding operation in question.

This locking will be indicated on the Web Admin and in the MiVoice 5000 User Portal application (by a padlock on the line in question).

14.5.3.2 Forwarding record for trunk group / super hunt group / VM hunt group

For these types of subscriptions, only predefined forwarding may or may not be activated.

The choice of origin is unique: internal and external calls.

14.5.3.3 Forwarding record for automated assistant

For these types of subscriptions, only forwards on busy are proposed.

The three types of origins are proposed in terms of type of recipient.

Locking is available to the operator, for each column (for more information, see the part **Lock** box in the section **Forwarding record for internal subscriber**).

14.5.4 UCP VOICEMAIL BOX RECORD

Possible operations on a voicemail box record are:

- Create
- View / Modify
- Deletion
- Creating a secondary voicemail box record (for multi-line subscriptions)

14.5.4.1 Description of a voicemail box record

- **Characteristics** area: contains the voicemail parameters
- **Email messages options** area: contains information about the unified messaging system if this latter is activated.
- **IMAP** area: contains the definition of IMAP (Internet Message Access Protocol) parameters.

14.5.4.2 Creating a voicemail box record

To create a UCP voicemail box record:

- Select a subscriber.
- In the main technical record, click the **Add UCP** button, located at the bottom of the record.
- A new voicemail box record appears.
- Enter the UCP record parameters. The fields can be filled in as follows:
  - By entering the value directly in the data entry area
  - By selecting a value from a list
- After entering all the parameters, click **Apply** to confirm the creation. A notification appears and the voicemail box record is displayed in the subscription topology.

Note : For a secondary voicemail box record, click the Add UCP button in the secondary technical record you want.

14.5.4.3 Modifying a voicemail box record

- Select a subscriber.
- In the ***Topology*** window, click the voicemail box record to be modified.
- Modify the necessary parameters fields then click **Apply**.

14.5.4.4 Deleting a voicemail box record

IMPORTANT : Before deleting a voicemail box, ensure that all the messages have been deleted because no check is carried out during the deletion.

To delete a voicemail box record:

- Select a subscriber.
- In the *Topology* window, click the voicemail record to be deleted.
- Click the **Del. record** button located at the bottom of the record.
- Confirm the deletion by answering **OK** to the deletion request.

The record is deleted and no longer appears in the subscription topology.

14.5.5 TWP RECORD

The management of a new TWP record for a (main) subscriber is only available:

- For R5.x sites minimum
- In TWP server 3.2 and later.

There is only one TWP subscriber number for the entire IP address / company-domain pairs defined for a multi-site configuration.

The TWP record is proposed for internal subscribers only.

Possible operations on a TWP record are:

- Create
- View / Modify
- Deletion

14.5.5.1 Creating a TWP record

- Select a subscriber.

- In the main technical record, click the **Add TWP** button, located at the bottom of the record. A new TWP record appears.
- Enter the TWP record parameters as indicated in the section **TWP record**.

The fields can be filled in as follows:

  - By entering the value directly in the data entry area
  - By selecting a value from a list

- After entering all the parameters, click **Apply** to confirm the creation.

A notification appears and the TWP record is displayed in the subscription topology.

14.5.5.2 Modifying a TWP record

- Select the subscriber concerned and then his TWP record.
- Modify the necessary parameters fields then click **Apply**.

During a modification, the Server name and Company/Domain fields cannot be modified. To make a change, make a deletion then a creation.

14.5.5.3 Deleting a TWP record

The TWP record can be deleted with the **Delete** button in the TWP record.

If you try to delete a technical record in which there is a TWP record, a message appears prompting you to confirm that you wish to delete the TWP record before deleting the technical record.

14.5.6 MULTI-LINE SUBSCRIBERS

A multi-line subscriber is a digital subscriber with several numbers on the same device. A distinction should be made between two numbers:

- **Main number**: first subscriber number declared
- **Secondary number**: subscriber number assigned to the same item of equipment as the main subscriber number

Multi-line subscribers are managed from secondary technical records or secondary voicemail box records.

A secondary technical record is created from the main technical record in operating mode.

14.5.6.1 Creating a secondary technical record

- Select a subscriber.
- In the *Topology* window, click the primary technical record.
- Click the Add secondary button located at the bottom of the record.

A new empty technical record is displayed.

- The secondary technical record is entered in the same way as for the main technical record; after entering all the parameters, click **Next**.

A window with the list of programmable items opens.

- Click **Program** to confirm the creation.

The created secondary technical record is added to the subscriber's topology area.

A forwarding record is created with the secondary technical record.

14.5.6.2 Modifying a secondary technical record

- Select a subscriber.
- In the **Topology** window, click the secondary technical record.
- Modify the necessary information then click **Apply**.

14.5.6.3 Creating a secondary voicemail box record

A secondary voicemail box record can only be created on an existing subscriber.

To create a secondary voicemail box record:

- Select a subscriber.
- In the *Topology* window, click the secondary technical record.
- Click the Add UCP button, located at the bottom of the record.
- A new voicemail box record appears.
- The secondary voicemail box record is entered in the same way as the main voicemail box record. After entering all the parameters, click Apply.

The created secondary voicemail box record is added to the subscriber's topology area.

14.5.7 MULTI-LOCATION SUBSCRIBERS

A multi-subscriber location is a subscriber with several call numbers on several devices located or not located in the same geographic area. This subscriber can, therefore, be **reached on several sites**. For this, the subscriber must be declared on each site, but these sites must be part of the same multi-site configuration.

A new location is created from the directory record in operating mode. A technical record is created for each location.

To create a new location:

- Select a subscriber.
- In the *Topology* window, click the directory record symbol.
- Click the **Add location** button, situated at the bottom of the directory record.

A new empty technical record is displayed.

- Enter the technical record parameters: subscriber number, confidentiality, technical characteristics, etc.
- After defining all the parameters, click **Apply**.

The created technical record is added to the subscription topology area. The user can complete the subscription with a keys record, an assignment (login) record or a voicemail box record.

14.5.8 MULTI-USER SUBSCRIPTIONS

The **multi-user** function is used for a physical set shared by several users and requiring an authentication. It is often related to the hotel or hospital operations.

The multi-user function is performed on two subscription types:

- **Set subscription** which is assigned to physical terminals in rooms
- **User subscription** which is assigned to users of these rooms.

Set subscription

A set subscription is a standard subscription with special technical characteristics. The following features must be defined:

- Sharing set
- Signature type

User subscription

A user subscription is a specific subscription which has some characteristics of a standard subscription (rights and features) and the following characteristics:

- Room number: association parameter between the user subscription and terminal subscription.
- Password: (4-digit) secret code which the user must enter to make an outgoing call.

The user's directory number may be a DID number and given by the occupant so as to be called from outside. It does not change if the occupant does not change room.

Note : Some standard subscription parameters, such as voicemail box, intercom group, keys, etc., are not accessible to this subscription type.

14.5.8.1 Creating a user subscription

- In individual creation mode, in the subscriber creation window, select a region/multi-site/site, then **Multi-user**.
- Fill in the directory record fields.
- In the technical record:
  - Fill in the Number and Numbering plan area fields.
  - Fill in the Characteristics area fields and more specifically:
    - **Room number**: indicate the terminal subscriber's directory number.
    - **Password**: enter a (4-digit) secret code.
- Click **Next** or **Terminate**.

The screen displays the list of items to be created.

- Click **Program** to confirm the creation.

14.5.9 ADDITIONAL NUMBER MANAGEMENT

14.5.9.1 Creating an additional number

An additional number is used to reach a subscriber from an external network (TL or PSTN). This number works like an alias of the primary subscriber number.

Additional numbers are created from the primary or secondary technical record in creation or operating mode.

Note : The additional number may correspond to the subscriber number if the subscriber number is configured as DID number. In this case, the additional number (Plan 1) is created automatically when the subscriber number is created.

To create an additional number on a primary subscriber number:

- Select a subscriber.
- In the **Topology** window, click the primary technical record symbol.
- In the **Plans**, area, click **Add Compl.**.

A new number input window opens.

- Choose a number block in the **Numbers** area. Use the **>>** symbol to scroll the number blocks. The available numbers are indicated in green.
- Click the number you want. The number appears in the corresponding plan area.

- Click OK to confirm the creation.

Repeat the operation for each additional number to be created in the different plans (maximum of 8 plans).

To create an additional number on a secondary number, repeat the above procedure but click on the secondary technical record in step 2.

14.5.9.2 Deleting an additional number

- To delete the number of one of the 8 plans, click the red cross in the field concerned. The additional number is deleted.
- Click Apply to take this deletion into account.

14.5.10 MANAGING ABBREVIATED NUMBERS

An abbreviated number is a number with 1 to 4 digits used to make a call without dialling the complete telephone number. The abbreviated number length is defined in the **Administration** menu.

An abbreviated number can be assigned to a subscriber. A subscriber's abbreviated numbers are managed in the technical record in creation or operating mode.

To assign an abbreviated number to an internal subscriber, follow the same procedure as for an external contact. However, in this case, the visibility of the abbreviated number cannot be restricted to one or more hierarchies.

14.5.10.1 Creating an abbreviated number

- In the technical record, *Numbers* area, click **Add short**.

An abbreviated number creation window appears.

- Enter the abbreviated number associated with the subscriber then click **Validate**.

A list of existing numbers starting with the 1st digit entered appears during the input.

14.5.10.2 Modifying an abbreviated number

- In the technical record, *Numbers* area, click **Add short**.
- In the abbreviated number window, modify the number then click Next.
- If necessary, modify the administrative hierarchy and click **Validate**.

The abbreviated number is modified.

- Click **Apply** to take this modification into account in the technical record.

14.5.10.3 Deleting an abbreviated number

- In the technical record, *Numbers* area, click **Add short**.
- Click **Apply** to take this modification into account in the technical record.

14.5.11 MANAGING HUNT GROUPS

A hunt group is a **set of terminals grouped together under a common directory number** (hunt group directory number) through which they can be called.

Group subscription is used to define the hunt group's call number. It consists of a directory record and a technical record. It is a logical subscriber (that does not correspond to a device) whose call number is linked to those of members of the hunt group.

14.5.11.1 General rules

- A subscription can only belong to one HUNT type group. However, it can belong to several SUPER GROUP type hunt groups (maximum of 8).
- The super group contains hunt groups or multi CCO subscriptions.
- A hunt group can contain different types of sets (analogue, digital, ISDN, IP, etc.).
- When a set is included in a hunt group, a call interception group number is automatically assigned to the set.
- The last set in a hunt group can be placed on standby, provided that the group is not an answering set group (operator forwarding extension).
- The sets must belong to the same technical hierarchy.
- Maximum number of subscribers per hunt group: 100

14.5.11.2 Hunt group types

There are several types of hunt groups:

TYPE	DESCRIPTION
Cyclic	Calls are successively routed to the various hunt group sets in the order of the declared sets in the hunt group. Each new call is routed to the next free set (after the previous call).
Fixed head	Calls are routed on a priority basis, to the first set in the hunt group (hunt group head set). If the first set is busy or is not answering, the second then rings, and so on.
General call	In this case, all analogue or digital sets ring simultaneously for an internal or external call (DID or DIR), and following an internal transfer. This type of hunt group can be declared as OP FORWARDING SET NUMBER (if de-activating the ATDC). For this type of group to work, tick the AUTHORISE CALL PICK-UP box in the hunt group parameters screen.
Idle time	In this case, the set that rings is the one which registers the least communication time in the hunt group.
Super hunt group	The composition of a super hunt group can be viewed through the MMC. The numbers are registered by the EAI (external interface). A super hunt group can contain both hunt groups and sets.
Empty	In this case, the hunt group does not contain any subscribers.

14.5.11.3 Creating a hunt group subscription

- In individual creation mode, in the subscriber creation window, select a region/multi-site/site, then **Group**.
- Fill in the directory record fields.
- In the technical record:
  - Fill in the Number and Numbering plan area fields.
  - Fill in the Characteristics area fields (see below).
  - Select the subscribers to add to the hunt group (see below).
- Click **Next** or **Terminate**.

The screen displays the list of items to be created.

- Click **Program** to confirm the hunt group creation.

CHARACTERISTICS OF A HUNT GROUP SUBSCRIPTION

The technical record of a hunt group subscription has the following characteristics:

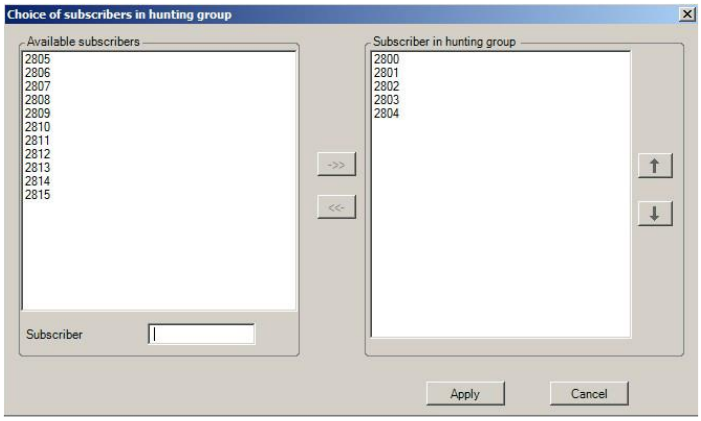
CHARACTERISTIC	DESCRIPTION
Features	See table **Features**
Day/night PSTN	See table **Day/night PSTN**
Backup site	Dual homing feature available to hunt groups as of R8.2. **WARNING: The hunt group's backup site must also be running with R8.2.**
Technical hierarchy	See table **Technical hierarchy**
Type of hunt group	For defining the hunt group type
Hunt group nature	The default hunt group type is TELEPHONY, therefore, all terminal types can be declared in a hunt group. The hunt group type can also be ISDN DATA. In this case, all terminals declared should be of ISDN type (for example, PC with S0 interface, etc.).
Used for pre-call distribution.	If ticked, you will have a ticket (ACD 7403 statistics) upon broadcast of an announcement before it reaches the subscriber.
Predefined forward	Internal or external number to which the hunt group is forwarded: the number entered can have a maximum of 17 digits, including direction access prefixes (0, 00). For all set types (analogue, digital) the predefined forward command is activated by a code + the hunt group number. It is cancelled with a code + hunt group number. **Note :To activate group forwarding, the SET activating this feature must have ASSISTANT FORWARDING ALLOWED set at YES (this set may or may not belong to the hunt group).**
Hunt group ringing duration	Time-out fixed at 40 seconds. This time-out is activated on a call to a hunt group. It defines the global ringing time for sets in the group. This time must not be less than the internal call ringing time. The value of this time-out can be increased according to the number of sets in the hunt group The number of cycles depends on the number of active sets in the group.
Extension ringing duration	Time-out fixed at 15 seconds and activated on a call to a group of terminals. This corresponds to the time during which a terminal in the group rings before the next terminal rings.

Extension idle delay	Time-out fixed at 2 seconds. This corresponds to the pause between two calls for the same terminal in the hunt group.
Time before return to operator console	
Waiting time before assistance	
Wait time before alerting	
% waiting calls	

Selecting hunt group subscribers

- In the Characteristics part, click the **Add** button in the *Subscribers* area.

A selection window appears and displays the list of existing subscribers.



- Select some subscribers from the list of available subscribers (user the MAJ or CTRL keys for multiple selection) and click ->> to include them in the hunt group (do the contrary to remove some subscribers).
- Click **Apply** to save the operation.

To remove some subscribers from a hunt group:

In the *Subscribers*area, select the subscribers to remove then click **Remove**.

14.5.12 MANAGING SUPER HUNT GROUPS

This type of subscription is used to group a set of HUNT GROUP type subscribers or subscribers associated with a multi-key set.

The number of SUPER GROUP type subscriptions is limited to 8 per iPBX.

The description of the general parameters for defining a super group is the same as the one given in the hunt group definition (see the previous section - Managing hunt groups).

The parameters that relate to the composition of a super hunt group are different from those for a hunt group. The following rules apply to the constituent elements of a super hunt group:

- the constituent elements of a super hunt group can only be "cyclic", "fixed head" or "longest time idle" HUNT GROUP type subscriptions or multi_CCO subscriptions (at least one key must be programmed),
- None of them should already belong to 8 super groups.
- They are distributed according to 4 hierarchical levels and each hierarchical level may contain up to 4 subscriptions.
- A subscription can only be defined in a hierarchical level if the lower level is not empty.
- In a multi-company configuration, the elements making up a super group must belong to the same company/department pair as the super group.

Note : In a multi-site configuration, the constituent elements of a super group can be declared on different sites.

A change level criterion is associated with the super group and used to define the conditions in which the calls are routed to the higher hierarchical level.

LEVEL N (1 TO 4)

SUBSCRIBER 1 TO 4

Directory Number.

Note : If the corresponding subscription does not respect the rules indicated above, an "incorrect directory number" error message will be sent by the system.

The system undertakes the controls to ensure rule compliance before validating a component element. This operation may take a few seconds.

Level change criterion

- **Sets busy**: Move to level N+1 if all the level N sets are busy.
- **Max. waiting time**: Move to level N+1 if the maximum time in each of the level N queues has been reached
- **Queue busy**: Move to level N+1 if the queues for level N subscribers are full.

Max. waiting time (SEC)

This parameter is only displayed if the change level criterion is set to MAX TIME IN QUEUE.

Enter a value in seconds.

14.6 MASSIVE ACTIONS

Massive actions concern operations performed on a group of subscribers. It may be creation or modification. A massive processing management menu is used to monitor executed operations.

Massive creation is carried out on maximum 5000 subscribers.

14.6.1 MASSIVE MODIFICATION ON SUBSCRIBERS

Note : Mass modification on subscribers does not apply to subscribers in profile mode.

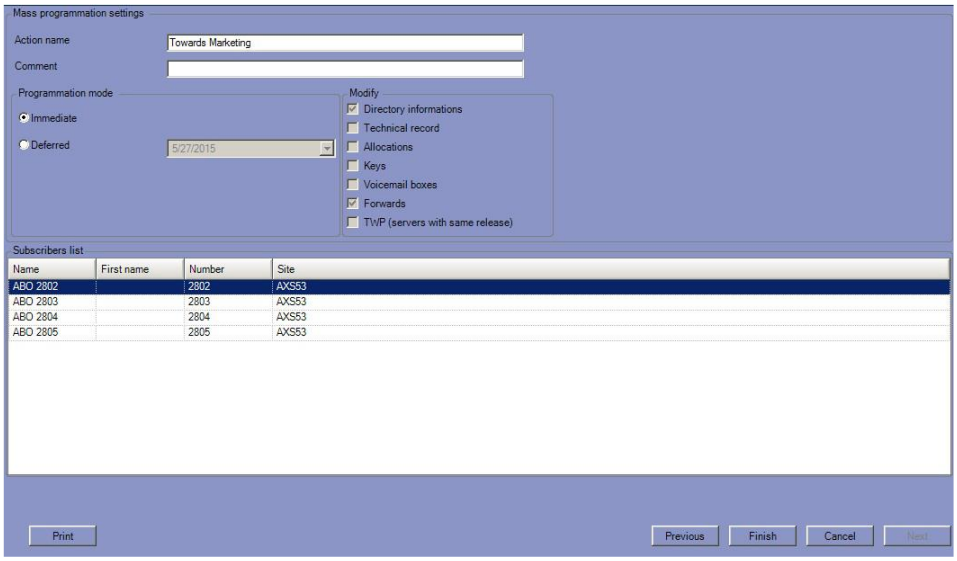
- In the Telephony window, click Subscribers management then Search.
- Carry out a search.
- In the search result list, select a group of subscribers then click Manage.

A warning message is displayed. Click OK to continue with the procedure.

The subscription window opens so you can carry out the operation.

- In each record, enter the necessary modifications. Use the Previous/Next buttons to navigate between the records.
- After entering the modifications, click **Terminate**.

A programming window appears with the list of subscribers concerned.



- In this window, enter the name of the action and possibly a comment.
- It is possible to select immediate or deferred programming.

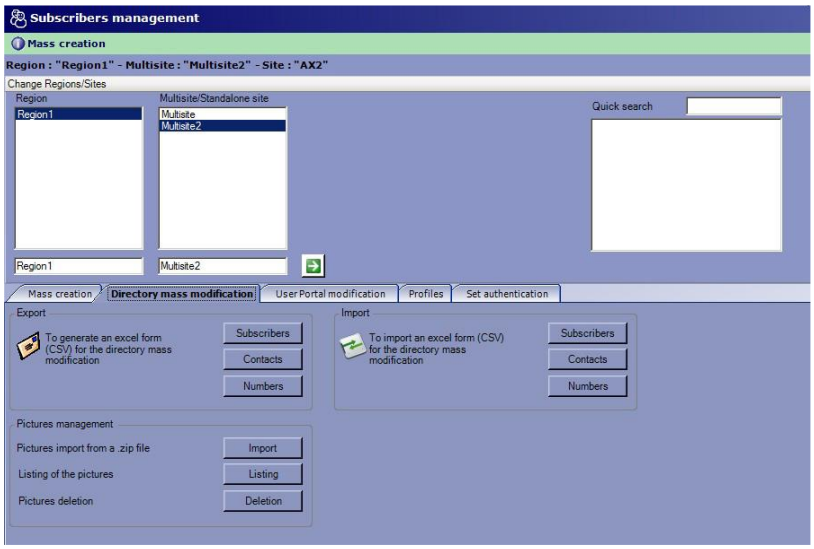
If the **Deferred** option is selected, enter or select a date in the calendar by clicking the button.

- Click **Program** to start the programming operation. A notification is displayed at the end of the operation.

Note : If several subscribers are selected, the actions executed on the first subscriber selected will also be applied to the other subscribers selected.

14.6.2 MASS MODIFICATION ON DIRECTORY DATA (INTERNAL OR EXTERNAL RECORDS / PICTURES)

- In the **Telephony** window, click **Subscribers management** then **Mass creation**. Select a region / multi-site then click the green arrow.
- Click the **Directory mass modification** tab.



14.6.2.1 *Mass modification on (internal or external) records*

- Depending on the type of records to modify, click the Subscriber button (internal records) or Contacts (external records) in the Massive modification group – Export.
- At the end of the export, a web browser opens on a csv file, including all the internal subscribers or external contacts available in the LDAP database for this multi-site. Modify the data you want and back up the file on the local disk.
- Click the Subscribers or Contacts button in the Massive modification – Import group to import the modifications made in the csv file. Select the file saved locally in step 3.

Note : The Shortnumber data in the contacts is for information only and cannot be changed or added by the mass modification form.

14.6.2.2 *Massive modification on pictures*

The massive modification on pictures via MiVoice 5000 Manager is described in the document Managing DID numbers in the directory characteristics.

14.6.3 MASSIVE CREATION

This menu is used to create a set of subscribers or external contacts by entering all the creation information in an Excel file. The entered data is then imported into the application.

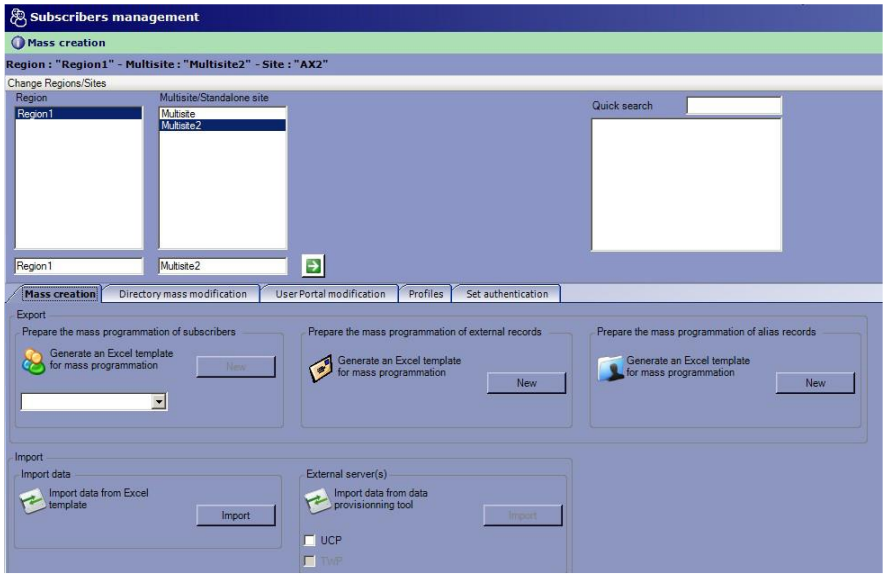
The procedures are:

- Creating subscribers or external subscribers on the Excel file
- Importing data from the Excel file
- Starting programming and creating subscriber records or the corresponding external contacts

14.6.3.1 Implementing mass creation

In the **Telephony** window, click **Subscribers management** then **Mass creation**.

The mass creation window opens.



- In the mass creation window, select a region / multi-site then click the green arrow.
- Click the **Mass creation** tab.
- To open the internal subscriber configuration Excel file, click **New** in the **Prepare the mass programmation of subscribers** area. To open the external contact configuration Excel file, click **New** in the **Prepare the mass programmation of external records** area.
- To import the UCP and/or TWP records from MiVoice 5000 Provisioning collection:
  - First select the site in the **Export** area.
  - In the **External server(s)** area, select **UCP** and/or **TWP** depending on the data to be imported.
  - On the PC, select the file **7450_Form.xls** that corresponds to the site then click **Import**. See the document MiVoice 5000 Provisioning - Operating manual.

14.6.3.2 Creating data on the Excel file

INTERNAL SUBSCRIBERS

The Excel file consists of several tabs corresponding to each subscriber record.

- Directory tab = directory record
- Technical tab = technical record
- Login tab = allocation (login) record
- Keys + PQMCDU tab = keys record

- Forwarding tab = forwarding record
- TWP tabs = TWP record

The information that needs to be entered in the Excel file corresponds to the information in the different subscription records.

- Enter the information in each tab. Some columns such as site selection or directory parameters (type, function) propose an options list.

Note : It is mandatory to enter directory record information.

- At the end of the entry, click **File** > **Save** (or the diskette icon).

The data entered is ready to be imported into the management centre directory database.

14.6.3.3 External contacts

The Excel file contains only one CONTACT tab. Note: this file contains Excel macros: check that the configuration of the Excel application on the PC allows the opening of files with macros (menu: Tools-Macro-Security, Average security level to be selected).

Fill in the different fields corresponding to the information available in the external records.

The Configuration button in the hierarchy input column is used to display the administrative hierarchy in form of a tree to possibly reduce the range of an abbreviated number. By default, the Any hierarchy option is selected. Unselect it to access the selection of a particular node on the tree.

14.6.3.4 Importing application data

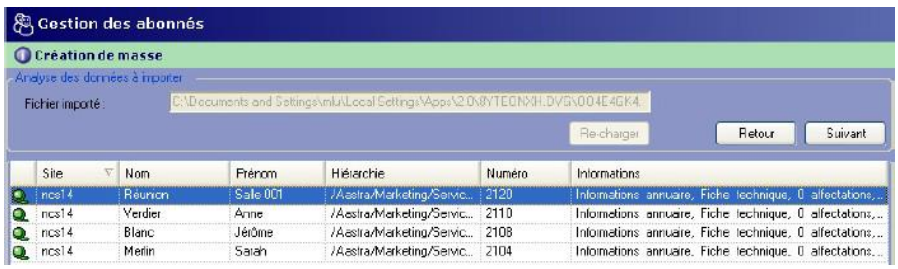
- After entering and saving the data, close the Excel file.
- In the management centre massive creation window, click **Import**.

A navigation window opens so you can select the Excel file with the data to be imported.

- Select the Excel file then click **Open**.

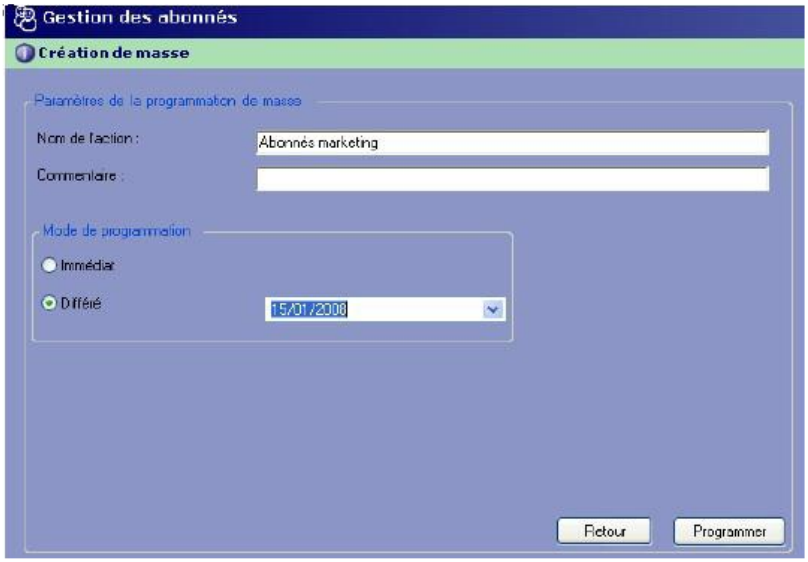
The data is imported and displayed in the management centre.

Note : In case of inconsistencies, a table is displayed with the list of errors. The user must correct these errors in the Excel file before resuming the import procedure.



- Click Next.

A programming window opens.



- In this window, enter the name of the action and possibly a comment.
- It is possible to select immediate or deferred programming.
  - If the **Deferred** option is selected, enter or select a date in the calendar by clicking the button.
- Click **Program** to start the programming operation.

A notification is displayed at the end of the operation.

The subscribers or external records are created in the management centre LDAP directory. All the management operations are possible on these subscribers or external records.

14.6.4 MASSIVE MODIFICATIONS IN MIVOICE 5000 USER PORTAL

This action enables the administrator to massively update the user accounts authorised to use MiVoice 5000 User Portal.

Note : The tab is not available when SSO mode is enabled.

14.6.4.1 Data export

This operation is used to export information about the subscribers of a site in a .csv file in order to update, via Excel, their right to use the MiVoice 5000 User Portal application.

- In the **Telephony** window, click **Subscribers management** then **Mass creation**. Select a region / multi-site then click the green arrow.
- Click the **User portal modification** tab.
- In the **Export** group, click **Subscribers**.
- After the action is taken into account by the portal, the administrator login is required.
- Open the proposed .csv file.
- Fill in the following areas:
  - **action**: not identified during export. Update consists in setting the area to 1 to activate the authorisation to use MiVoice 5000 User Portal, or to 0 to deactivate it.
  - **password**: during export, the password is not communicated. If access to MiVoice 5000 User Portal is activated, the area contains some asterisks or else the area is empty.
  - **mail sent to**: the area is filled in if the e-mail address exists in the subscription. It is possible to enter or modify the address indicated. A confirmation e-mail will be sent to the address indicated. This will not update the subscription.
- Save the .csv file.

14.6.4.2 Importing data

- In the **Telephony** window, click **Subscribers management** then **Mass creation**. Select a region / multi-site then click the green arrow.
- Click the **User portal modification** tab.
- In the **Import** group, click **Subscribers**.
- In the navigation window, indicate the location of the file saved previously after export.
- A control file is generated: it contains the passwords assigned to users and the e-mail addresses to which a notification was sent after access to the application had been authorised. If an e-mail could not be sent to the subscriber because the area had not been filled in, a notification is made there. The administrator must send his password to the user either separately via e-mail, or by updating the control .csv file: e-mail address and action code on 1 for erroneous recordings.

The e-mail received by the user contains:

- the login: the directory number
- the password: it is issued at random by the system.
- the link to the MiVoice 5000 User Portal application, for customising the telephony account.

14.6.4.3 Customising the e-mail sent to the user

It is possible to customise the content of the e-mail sent to the user when activating the MiVoice 5000 User Portal account.

- Go to: **/home/m7450/repository/system** as m7450 (**su - m7450**) administrator.
- First rename the file **selfadmin.sample.html** to **selfadmin.html**.
- Then edit the file **selfadmin.html** and configure it with the variables set out below.

Caution: this file must be in UTF-8 and html format.

- The following variables must be configured and represent:
  - **{0}**: the subscriber's number
  - **{1}**: the password
  - **{2}**: the server IP address
  - **{3}**: the multi-site name.

Example of file:

```
<html>
<head>
</head>
<body>
<div width="100%">
   Your MiVoice 5000 User Portal account has just been activated:
   <ul>
      <li>Login: <b>{0}</b></li>
      <li>Password: <b>{1}</b></li>
   </ul>
   Here is the link to the application:
   <br />
   <a
href="https://{2}/selfadmin/Page_login.aspx?multisite={3}">https://{2}/selfadmin/Page_login.aspx?multisite={3}</
a>
   <br />
   <br />
   This link will give you access to your phone account customisation: configuration of programmable keys,
forwarding, etc.
   <br />
   <br />
   <br />
   Yours cordially,
   <br />
   <br />
   The Administrator
</div>
</body>
</html>
```

14.6.5 MASS PROCESSING OF SUBSCRIBERS CREATED BY PROFILE

The profiles tab is used to massively process the subscribers managed in profile mode (see also

14.7 WEB CLIENT APPLICATION

and Managing profile).

- In the **Telephony** window, click **Subscribers management** then **Mass creation**. Select a region / multi-site then click the green arrow.
- Click the **Profiles** tab.

14.7.1.1 Export

The export function is used to:

- Create subscribers by profile (from a blank Excel file): select **Create (blank file)** then click **Export**.
- Modify the profile for the subscribers managed in profile mode: select **Modify** then click **Export**.
- Export subscribers: select **Migration** then click **Export**:
  - in an installation on which subscribers have not been created by profile, the subscribers can be changed to profile-based management mode by assigning them a profile.
  - After MiVoice 5000 Manager is upgraded from a version below V2.4A, the subscribers can also be changed to profile-based management mode by assigning them a profile.

14.7.1.2 Import

- After entering and saving the data, close the Excel file.
- Click **Import**.

A navigation window opens so you can select the Excel file with the data to be imported.

- Select the Excel file then click **Open**.

The data is imported and displayed in the management centre.

The result of the import is displayed in a table. Detected anomalies are indicated in the **Information** column. It is possible to correct the anomalies in the Excel file before restarting the import procedure.

14.7.2 MASSIVE PROCESSING OF TERMINAL AUTHENTICATION

This tab is used to create or modify terminal authentication in the technical record through massive processing.

- In the **Telephony** window, click **Subscribers management** then **Mass creation**. Select a region / multi-site then click the green arrow.
- Click the **Terminal authentication** tab.

14.7.2.1 Export

The export function is used to create or modify the password.

- Click **Subscribers** in the **Export** display area.
- The corresponding Excel file has 2 columns: the subscriber number and the password (passwordsip).
- If a password exists, it is displayed in clear text.
- The password can be modified (value between 8 and 16 hexa characters).
- To generate the password automatically, enter the **AUTO** character string.
- Save the .csv file at the end of the modification.

14.7.2.2 Import

- Click **Import**.

A navigation window opens so you can select the Excel file with the data to be imported.

- Select the Excel file then click **Open**.

The data is imported and displayed in the management centre.

After the validity of the **passwordsip,** field is checked, a list of subscriptions whose password does not correspond to the expected value is displayed.

The **Return** button reopens the massive processing window. Anomalies can then be corrected in the Excel file before resuming the import procedure.

IMPORTANT : Massive processing of terminal authentication may affect some subscriptions managed by profile if the Excel file requires their modification. In this case, the modified subscriptions are unlocked.

14.7.2.3 Creating data on the Excel file

The Excel file contains several tabs, corresponding to each subscriber record.

- Directory tab = directory record
- Technique tab = technique record
- Login tab = login record
- Keys tab = keys record
- Forward tab = forward record
- TWP tab = TWP record

TABS	TABS COLUMNS
Directory	Surname, First name, Number, **Main number***, Place, Hierarchy, Gender, Function, Address, Username, E-mail, Confidentiality, Assistant
Technique	Plan 1 to Plan 8, Company/Department, ICG 1, ICG 2, IVB classes, Partner set, Class service, Feature classes, Day PSTN Cat. Night PSTN Cat. Day TL Cat. Night TL Cat., Spoken language, Written language, Set Auth. Set Auth. Val., Dep. Partition classes, Incom. partition classes, Priority classes, Forbidden numbers list, CUG class, User password, SIP Uri, MiCollab role, Dyn. bkp SIP DECT, MOM perm. user, CloudLink role, **Backup site**
Login	Resources No.1, Equipment No.1, Resources No.2, Equipment No.2, Resources No.3, Equipment No.3, Resources No.4, Equipment No.4, Resources No.5, Equipment No.5, Resources No.6, Equipment No.6
Keys	Key number (1 to 20), 🔒, **Label**, Key type, Settings, Signal, URL
Forward	Int/Ext No answer, Number, 🔒 Int/Ext On busy, Number, 🔒 Int/Ext Immediate, Number, 🔒 Int No answer, Number, 🔒 Int On busy, Number, 🔒 Int Immediate, Number, 🔒 Ext No answer, Number, 🔒 Ext On busy, Number, 🔒 Ext Immediate, Number, 🔒
TWP	

*Column to be completed only for a subscriber's secondary lines.

Note: The Excel file can contain up to 5,000 lines.

14.7.3 MASSIVE PROCESSING FOR EXTENDED NUMBERING UPGRADE

See the document Upgrading to extended numbering plan.

14.7.4 MASS TREATMENT FOLLOW UP

This menu is used to monitor massive actions taken on subscribers, in creation or operating mode.

The monitoring table contains all the actions defined in the mass creation or mass modification menus. It lists all the operations, both in immediate or deferred processing mode. It gives an overview or detailed view of mass actions.

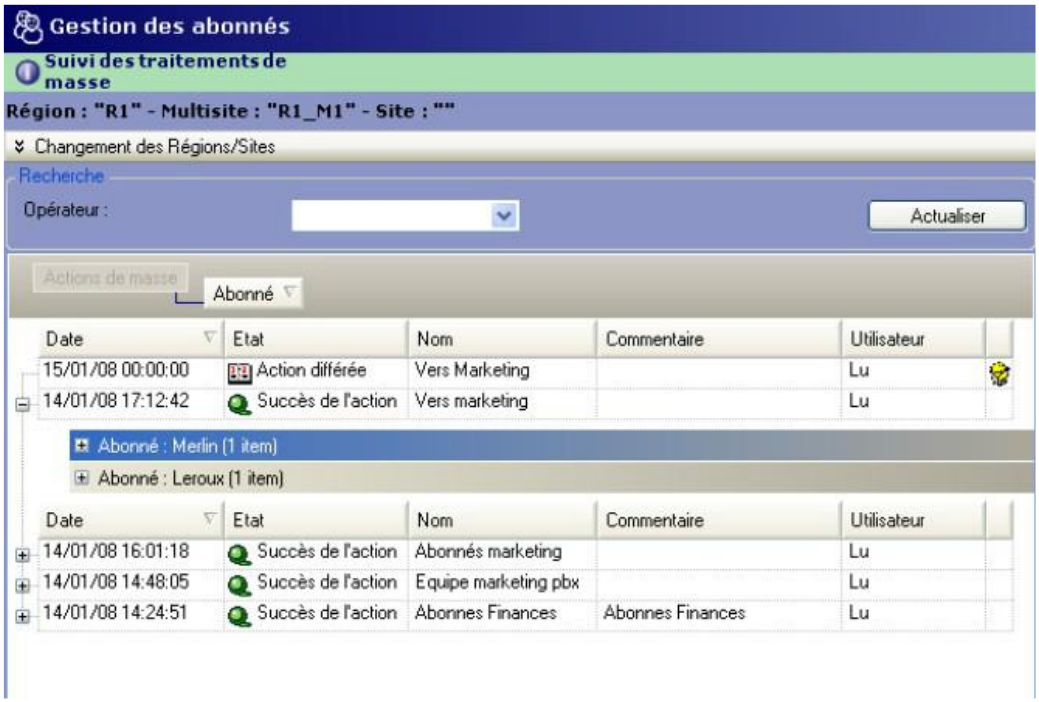
14.7.4.1 Accessing mass treatment

- In the **Telephony** window, click **Subscribers management** then **Mass treatment follow up**.
- Select a region / multi-site configuration.
- If necessary, select an operator from the drop-down list then click **Refresh**.

The list of massive operations performed by the selected user is displayed.

14.7.4.2 Description of the follow-up table

The mass treatment follow up table is as follows:



The + sign located at the beginning of each line is used to see the details of a massive action and the subscribers concerned by the action. More details can be displayed for each subscriber.

The actions are classed by date, status, name and user. Upward or downward sorting is possible, by clicking the header of each column.

The INSERT ICON icon is used to generally launch all failed individual actions.

14.8 WEB CLIENT APPLICATION

IMPORTANT :	**When creating a subscriber manually or automatically by profile (Web management or external sync), the iPBX must be reachable and the subscriber management menus of Web Admin should not be used.** **If this rule is not respected, the creation will not be performed (creation failure) and the operation will have to be repeated.** **In the case of creating profiles by EXTERNAL synchronisation, the possibilities are as follows:** **The creation of technical record can be completed from MiVoice 5000 Manager Client,** **Or** **Deleting the directory record in the MiVoice 5000 Manager means that the next time the external database is notified, the creation will be restarted.**

Logging in when accessing this application is via a local Operator account or a domain account if the feature is activated (see the section Access to operator management).

This menu gives access to the Web Client application for easy creation of subscribers in Profile mode and to change the configuration of some standard subscriber features.

Thanks to this simplified management of subscriptions from the Web Client interface, it is possible:

For standard subscribers:

- To modify some directory features
- To modify some technical characteristics
- To program call forwarding and keys

For subscribers in profile mode:

- To create/modify the technical characteristics
- To create/modify the UCP characteristics
- To create/modify the TWP characteristics
- To create/modify allocations
- To program call forwarding and keys

Any action started in the interface (creation, modification) is considered as mass processing.

If a user programs keys and/or forwarding for his/her phone, this does not result in non-compliance of his/her subscription with regards to his/her profile.

This application is described in the document MiVoice 5000 Manager - Web Client Application.

14.9 MANAGING PROFILES

IMPORTANT : When creating a subscriber manually or automatically by profile (Web management or external sync), the iPBX must be reachable and the subscriber management menus of Web Admin should not be used.

If this rule is not respected, the creation will not be performed (creation failure) and the operation will have to be repeated.

In the case of creating profiles by EXTERNAL synchronisation, the possibilities are as follows:

The creation of technical record can be completed from MiVoice 5000 Manager Client,

Or

Deleting the directory record in the MiVoice 5000 Manager means that the next time the external database is notified, the creation will be restarted.

Profiles are created for two reasons:

- It allows easy and homogeneous subscriber creation. The profile contains the characteristics of the subscription to be created which must no longer be entered during each creation.
- For an external directory synchronisation, the profile allows automatic creation of a technical record and UCP/TWP records.

Note : Subscribers created through external directory synchronisation should not be managed by the Web Client interface. They must be modified from the remote directory database, including the profile.

Profiles are managed (created, modified, deleted) from MiVoice 5000 Manager only.

On the application **Telephony** screen:

- Click **Subscriber management** then **Profile management**.

14.9.1 DEFAULT PROFILE

When defined, the default profile is identified in the table by the  symbol of the **Default profile** column.

It is only obligatory for external directory synchronisation.

To define a default profile, click Define. On the list of profiles displayed, select the profile which will be the default profile then click Validate.

14.9.2 CREATING A NEW PROFILE

To create a new profile:

- Click **Add**. To create a new profile from an existing profile, just select the profile to be copied before clicking **Add.** The selected profile will then serve as a model for creating the new profile.
- In the **Profile** field, enter the name for this new profile: the name can be freely chosen, but the characters **Space** and **Underscore** are not allowed.
- In the **Comment** field, enter a comment which will be displayed in form of information in the application used to manage subscribers in profile mode.
- In the **Directory parameters** area, **Hierarchy** field, select a default administrative hierarchy.
- **Site** and **Managed sites**: if the multi-site architecture comprises several sites, indicate the managed sites by selecting them on the left then clicking the arrow to move them over to the right column.
- For an external directory synchronisation profile: in the **Mapping** area, enter the value of the attribute which characterises the profile in the external directory record (accents are not allowed) then click **Add**.

  The value added concerns the underlined site. If several sites have been selected, create a map for each site.
- Click **Next**.
- The window below displays the technical record pre-filled with default values: depending on the profile to be created, change the default values then select the technical hierarchy and click **Next**.
- Define the associated number range by clicking a line in the **Range** column (or the line with some question marks) then select any of the displayed ranges. Click Select. To be repeated for each site, if necessary.
- Key programming screen: indicate which keys, if any, are to be programmed for this profile see the section **Key management**).
- Programming forwarding: define the forwarding operations to be programmed for this profile and click Lock to prevent the user from modifying the forwarding operation in question (see the section **Forwarding record**).
- To activate the creation of a UCP record and/or a TWP record, select Program a UCP voicemail box and/or Program a TWP user to define their characteristics (see the sections UCP voicemail box record and TWP record).
- Click **Apply**.

  The new profile is added to the profile list.

14.9.3 DELETING A PROFILE

It is forbidden to delete a profile used in a subscription.

14.9.4 MODIFYING A PROFILE

Modifying a profile modifies all the subscriptions associated with this profile.

14.10 ANALOG GATEWAYS

This menu manages EX Controller, GX Gateway, TA7100, and Mitel AG4100. The menu is divided into four tabs:

- The Subscribers tab for viewing and editing the subscribers registered on the gateway,
- The Firmware tab for viewing and updating the gateway firmware releases,
- The Mass actions tab for making backups, reboots, and resets on multiple gateways at once,
- The Mass Gateway Import tab for adding and automatically configuring multiple gateways using a .csv file.

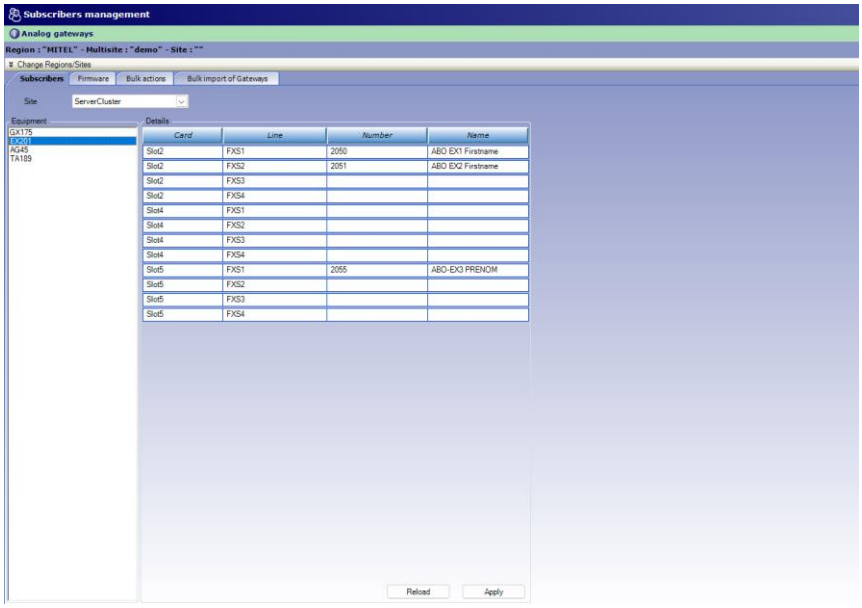
14.10.1 SUBSCRIBERS TAB

Select a site from the dropdown list to display the site's gateways in the **Equipment** section.

Note: The menu displays only the gateways for sites running R8.2 and later.

Select one of the devices from the equipment list to view the gateway's information. The list is displayed in a table format with the following data:

- **Card** (EX Controller only): card slot number
- **Line**: FXS port name
- **Number**: subscriber number associated with the line
- **Name**: subscriber name associated with the line



To modify a line:

- Enter the subscriber number to associate with a line in the **Number** column.
- Click **Apply** to save the changes.

The **Name** column is automatically populated based on the number entered.

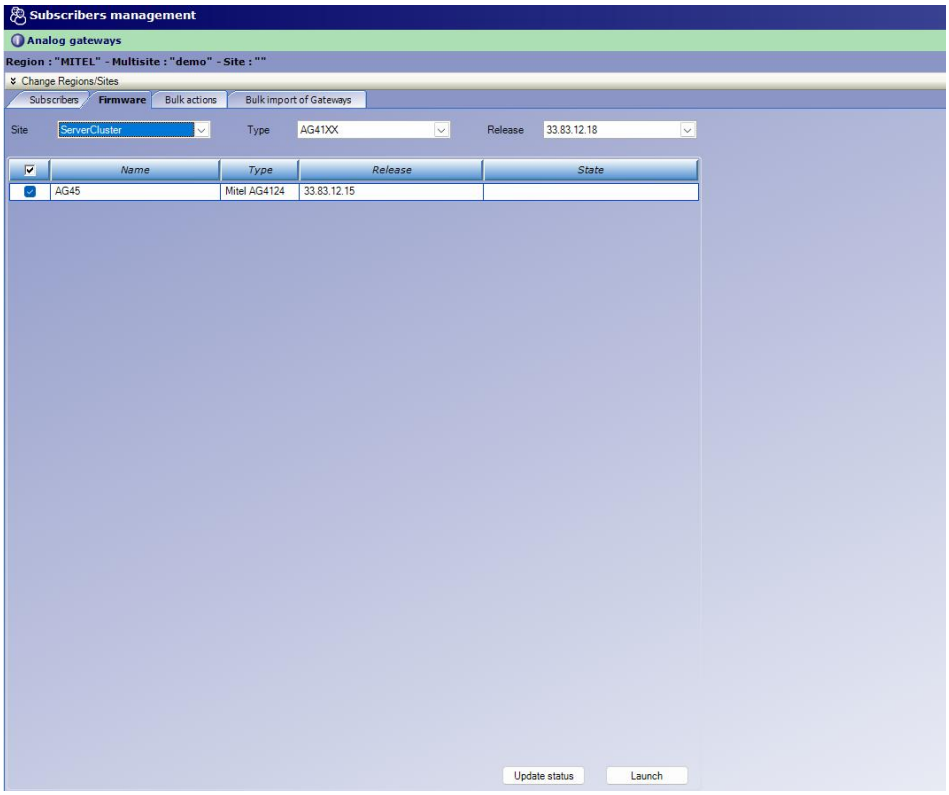
Click the **Reload** button to refresh the page.

14.10.2 FIRMWARE TAB

Select a site from the Site dropdown list to display the site's gateways in the table.

The list is displayed in a table format with the following data:

- **Name**: gateway name
- **Type**: gateway range
- **Version**: release number of the firmware installed on the gateway
- **Status**: gateway status during update



To update one or more gateways:

- From the **Site** dropdown list, select the site containing the gateway(s) to update.
- Select the gateways to be updated. If necessary, use the **Type** dropdown list to filter the gateways.
- From the **Version** dropdown list, select the release to apply for the update.
- Click **Launch** to start updating the gateway(s).

  Gateways take some time to update. Wait for the end of update. The **Status** column shows whether the update has been successful, is in progress, or has failed.
- Click the **Update Status** button to refresh the page and see the changes in the **Status** column.

IMPORTANT NOTE: For an EX Controller, update includes a VM reboot. MiVoice 5000 Web Admin is unavailable during the update.

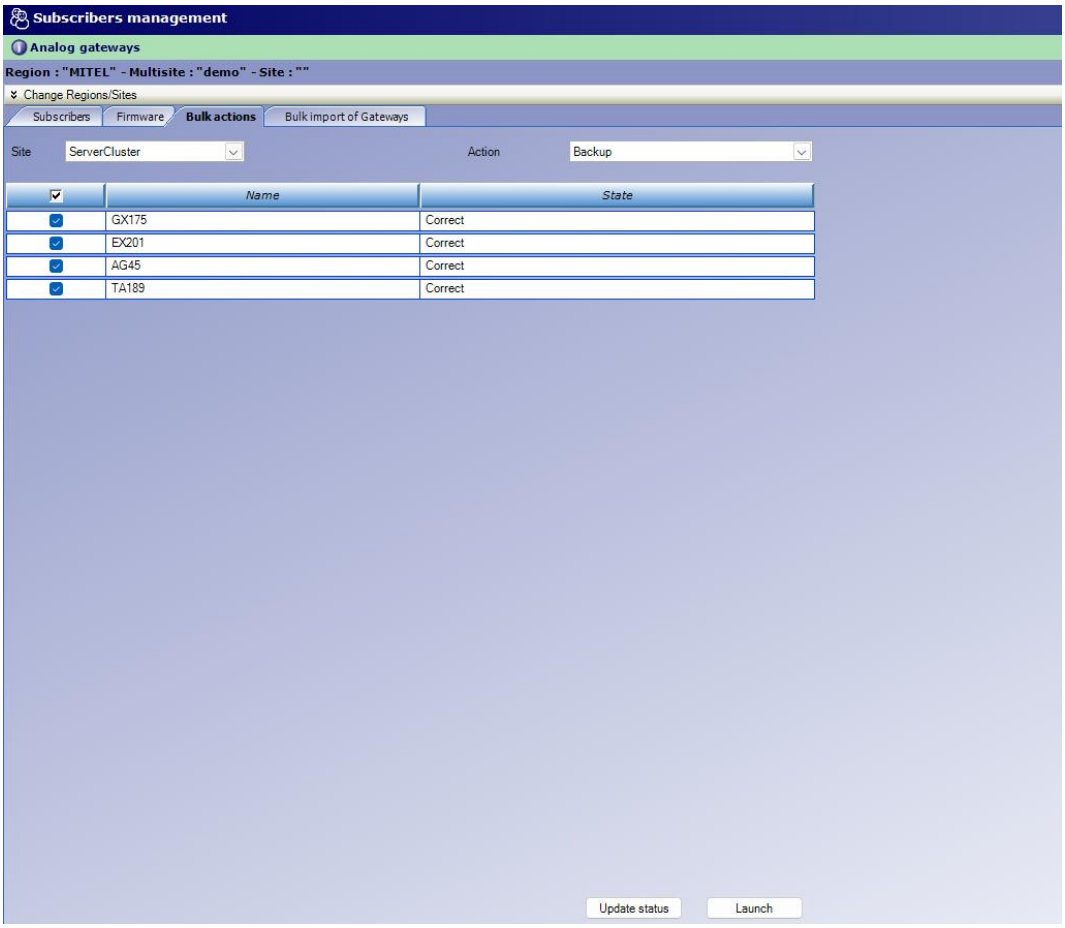
For GX, TA7100, and AG4100, MiVoice 5000 Web Admin remains accessible during the update. Avoid changing the gateways' configuration while an update is in progress.

14.10.3 BULK ACTIONS TAB

Select a site from the Site dropdown list to display the site's gateways in the table.

The list is displayed in a table format with the following data:

- **Name**: gateway name
- **Status**: gateway status during a mass action.

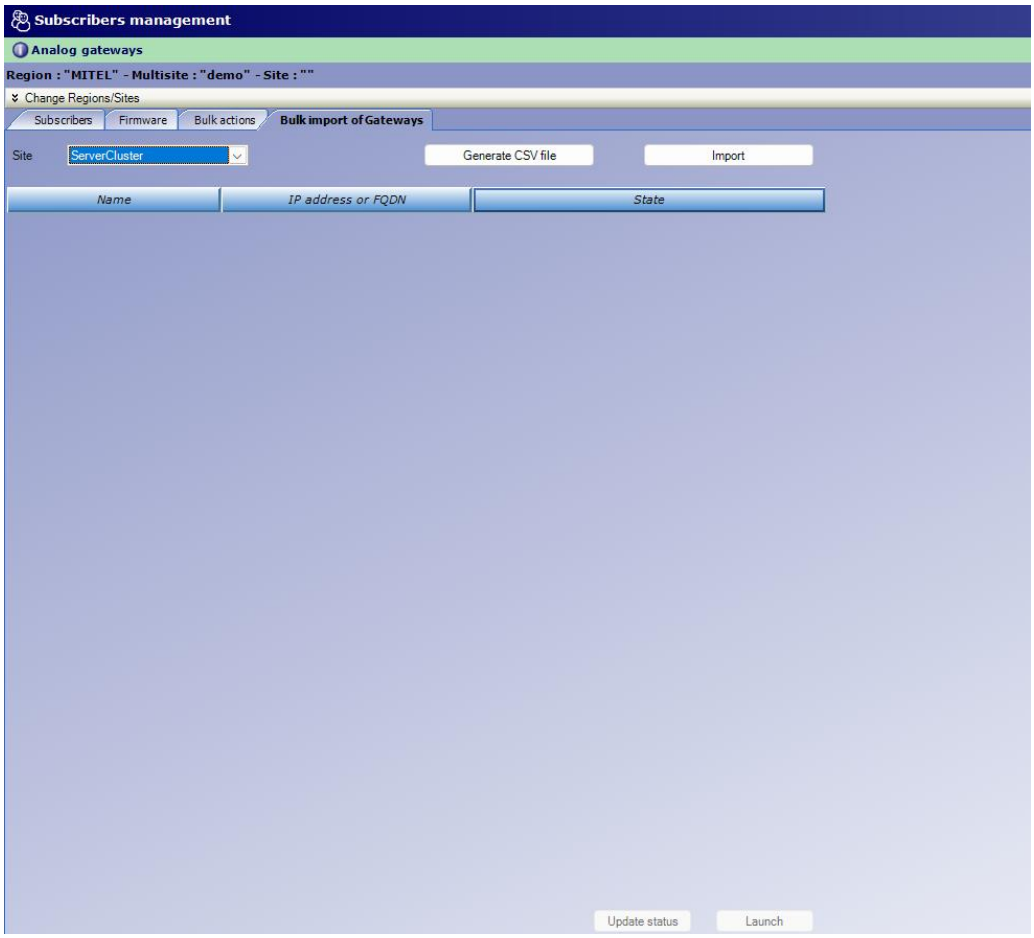


To start a bulk action:

- Select the gateways concerned.
- In the **Action** dropdown list, select the action to take on the selected gateways:
  - Save
  - Restart
  - Reset General settings.
- Click **Launch** to start massive action.

  Gateways take some time to update. Wait for the end of update. The **Status** column shows whether the action has been successful, is in progress, or has failed.
- Click the **Update Status** button to refresh the page and see the changes in the **Status** column.

14.10.4 BULK IMPORT OF GATEWAYS TAB



To import new gateways:

- From the **Site** dropdown list, select the site where new gateways will be imported.
- Click **Generate CSV file** to create a file named **gateways.csv**.

  The gateways.csv file contains 3 columns to fill in:

  - **#Name**: name to give to the gateways to be imported
  - **Address**: IP addresses of the gateways to be imported
  - **Password** (Optional): leave blank
- Enter the information about the gateways to be imported.
- Save the file on the PC.
- Back in MiVoice 5000 Manager, click the **Import** button to open the file manager and select the modified **gateways.csv** file.
- After loading, the list of the gateways to be imported is displayed in a table format with the following data:

  - **Name**: gateway name
  - **IP address or FQDN**: gateway range
  - **State**: gateway status during import.
- Click **Launch** to start massive action.

  Gateways take some time to update. Wait for the end of update. The **Status** column shows whether the import has been successful, is in progress, or has failed.

Click the **Update Status** button to refresh the page and see the changes in the **Status** column.

14.11 CONSULTATIONS

14.11.1 TELEPHONY OPERATIONS LOG

This log only displays telephony management operations (subscriber management, telephony parameters management, etc.).

The amount of information contained in this log depends on the purging periods defined by the administrator in the **Configuration** menu.

14.11.1.1 Defining the display criteria

To define the selection criteria:

- In the **Operation log** window, click the vertical **Setting criteria** tab located on the top left side of the operation log.

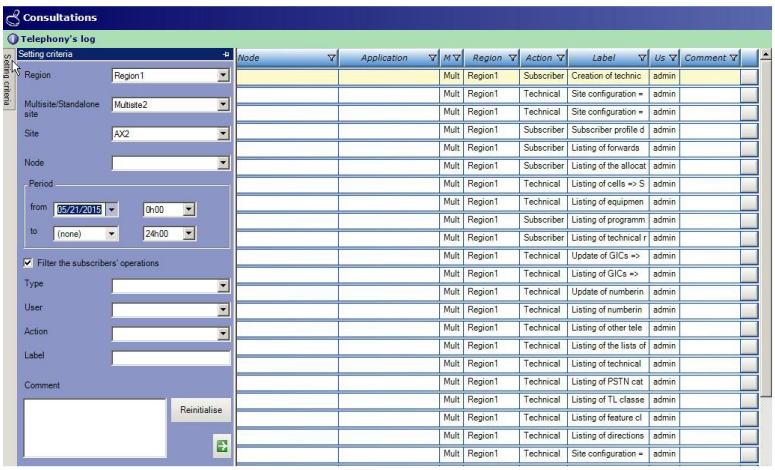
A criteria selection panel appears.

Note : Click the drawing pin symbol on the top right side to fix the window.

- If necessary, click **Reinitialize** to reset all the input areas.
- Select the selection criteria from those proposed in the drop-down lists.
- If required, fill in the **Label** and **Comment** areas to select the recordings corresponding to the content of these fields in the operation log.
- Click the  arrow to validate the selection.

Note : If the result is too long, it may be necessary to narrow down the search criteria.

After the selection result is displayed, other selections are possible on the columns with the symbol 
.



14.11.1.3 Printing the telephony operations log

The **Print** button is used to print the operation log on the PC printer.

- Click **Print**.
- A display window opens.
- If necessary, define the print format (one or more pages per sheet).
- Click the printer symbol to start printing.

14.11.1.4 Exporting the telephony operations log

The **Export** button is used to copy the data displayed on the screen to an Excel file.

- Click the **Export** button.
- In the Windows **Save As** window, define the directory to which the file must be copied.
- Enter the name and type of file.
- Click **Save**.

The file is available for another application.

14.11.2 ACTIONS ON STANDBY

This menu contains all the failed telephony parameter modification actions waiting to be resumed by the system.

The modifications made to the telephony parameters of a site are normally applied to the sites concerned by the defined range.

If some sites are inaccessible during the operation, an error message is displayed, and the action recorded as action on standby.

The management centre will relaunch the actions on standby in order of priority the next time the telephony parameters are modified.

Note : The actions on standby also include subscriber movements.

14.11.3 DOCUMENTATION

This menu opens a link to the Mitel documentation site.

15 TERMINAL MANAGEMENT

TMA (Terminal Management Application) is used to deploy and update the following terminals:

- MiVoice 5300 IP Phones
- Mitel 6000 SIP Phones,
- Terminals 53xx

No specific additional licence is required to use TMA. However, the “Subscriber management” licence must be unlocked in MiVoice 5000 Manager to access the TMA start menu.

See the terminal installation documents available on www.mitel.com.

16 MITEL APPLICATIONS

MiVoice 5000 Manager contains a page that gives quick access to other applications or websites. The list of these applications is defined by the user.

16.1 ACCESSING THE INTERFACE

To open the interface, click **Mitel applications**.

The button on the right side of the page gives the user quick access to the Mitel OMM portal if he/she enters the identification data required of him/her.

Already defined links are displayed in the **Telephony server list** frame.

16.2 ADDING A LINK

To add a link:

- In the **Name** area, enter a name to identify the link.
- In the **Url** area, enter the application access url (http://).
- Click **Add**.

The link is added to the list.

To access the site or web application, just click the name given to the link.

16.3 DELETING A LINK

To delete a link, click the red button  .

The link is deleted immediately.

17 APPENDIX

17.1 SSO MODE WITH OPENID CONNECT

WARNING: The menus and labels in this document are provided as examples to describe the procedure and are subject to changes specific to Microsoft Azure.

For more information on the procedure, refer to the Microsoft Entra ID documentation: https://learn.microsoft.com/fr-fr/entra/identity/.

- When registering a new application:
  - Enter the redirect URL in the format: https://[MANAGER-FQDN]/sso-oidc
- Create a client secret for the application.
- In the Token configuration menu, select Add optional claim and enter the following settings:
  - Type: ID
  - Add the value **upn** in claim.
  - Tick the “Turn on Microsoft graph profiles permissions’ box”.

Continue the procedure in the menu Administration > Configuration, SSO tab. Refer r to the section 7.1.1.2 – SSO tab.

17.2 SSO MODE WITH KERBEROS

WARNING: The security certificate must be installed on the Client PC. Refer to the appendix to the MiVoice 5000 Server - Implementation Manual.

17.2.1 SSO USING KERBEROS PROTOCOL

17.2.1.1 General information

Kerberos is a network authentication protocol that relies on a secret key mechanism and the use of tickets, not plain text passwords, thus avoiding the risk of fraudulent interception of user passwords.

Authentication is configured from an Active Directory environment and must be used when accessing the User Portal.

17.2.1.2 Creating an account in Active Directory

Create an account in Active Directory with the associated login/password (given here as an example):

- Login (example): *kerbmanager*
- Password (example): *mypassword*

These values are then used to create the **keytab** file.

17.2.1.3 Creating the keytab file

The keytab file is generated on Active Directory Server in a Windows PowerShell with the following command:

```
ktpass -princ HTTP/ machine_name@DOMAIN.COM -mapuser kerbmanager@DOMAIN.COM -pass
mypassword -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -out C:\kerberos.keytab
```

The values in red are to be filled in (given as an example here):

- Name of the machine from which the keytab file is imported: `machine_name`
- Domain name: `DOMAIN.COM`

- Encoding type: `AES256-SHA1`

WARNING: The command is case sensitive.

The **Keytab** file allows the Web server to log into Active Directory with the account stored in this **Keytab** file. This account is defined by the Kerberos right in Active Directory to allow active Directory to respond to a Kerberos ticket. This file will then be imported into the iPBX.

17.2.2 CONFIGURING THE WEB BROWSER FOR SSO MODE

For Internet Explorer and Google Chrome, add the following URL or domain name in *Internet Option>Security>Local Intranet>Sites>Advanced:*

Full URL:

As an example, in relation to the previous paragraph

- https://mivoice 5000 manager machine name.integration.com when the User Portal is managed by MiVoice 5000 Manager.
- https://iPBX machine name.integration.com when the User Portal is integrated into the iPBX.

Domain name (*.domain name.com)

As an example, in relation to the previous paragraph

*.integration.com

For Firefox:

- Launch Firefox and in the address bar, enter *about:config* to access the advanced configuration options.
- Add the previous URL or domain name to the variable *network.negociate-auth.trusted-uris*.

It is mandatory to declare the FQDN and not the IP address.

In SSO mode, the access URL for the User Portal is as follows:

As an example, in relation to the previous paragraph

- https://mivoice 5000 manager machine name.integration.com/userportal/ when the User Portal is managed by MiVoice 5000 Manager.
- https://iPBX machine name.integration.com/userportal/ when the User Portal is integrated into the iPBX.

Access to the User Portal is direct in SSO mode, without displaying the notification window.

17.3 SSO MODE WITH MICROSOFT AD FS

WARNING: The menus and labels indicated in this document are provided as examples to describe the procedure and are subject to changes specific to Microsoft AD FS.

For the Microsoft AD FS account, register the MiV5000 application on the Microsoft AD FS application:

- In the folder **AD FS>Application Groups**, create a new group.
- Click on the **[Group – Web API]** line.

  A new window pops up, with several tabs.
- In the **Access control policy** tab:
  - In the **Choose an access control policy** section, select the **Permit everyone** option.
- In the **Issuance Transform Rules** tab:
  - Create a new role, with the option **E-Mail Address** as an **Issued claim**.
- In the **Client Permissions** tab:
  - In the **Permitted scopes** section, check the **allatclaims** and **openid** boxes.