MiVoice 5000 Server

04/2025

AMT/PTD/PBX/0176/3/3/EN

OPERATING MANUAL

Mitel®

Warning

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

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

Neither Mitel nor its affiliated companies or subsidiaries may be held liable for any errors or omissions made in this document. This document may be reviewed or re-edited at any time in order to add new information.

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

CONTENTS

1 ABOUT THIS DOCUMENT

1.1 PURPOSE OF THIS DOCUMENT

This document describes the MiVoice 5000 Web Admin operating interface for MiVoice 5000 Server systems.

1.2 TARGET AUDIENCE OF THIS DOCUMENT

This document is intended for installation technicians responsible for configuring the system and implementing the telephony features introduced in this software release.

1.3 CONTENTS OF THIS DOCUMENT

This manual describes all the tools available to the administrator for configuring iPBXs from a management terminal.

All the user interface screens described in this manual are used to deploy and manage iPBXs.

This manual is composed of chapters, organised according to the tree structure of the user interface as presented on the management console screen.

1.4 TERMINOLOGY

1.4.1 TERMS AND EXPRESSIONS

MiVoice 5000 or MiVoice 5000 Server Telephone switching system hosted by a physical PC or virtual machine.

MiVoice 5000 Manager: Systems management centre

1.4.2 ABBREVIATIONS

CSTA	**C**omputer **S**upported **T**elephony **A**pplications.
DHCP	Dynamic Host Configuration Protocol.
IP	Internet Protocol. This is a protocol used to route packets on networks. IP is an OSI-model level 3 protocol, which offers a single addressing service for all connected terminals.
GDB	**G**NU **D**e**B**ugger
PPP	Point-to-Point Protocol.
MMC	Man Machine Interface (in this document “MiVoice 5000 Web Admin”.
SSO	Single Sign On: function, which enables a user to open one TWP and MiCollab Client session with the login/password, defined for Windows.
TDM	Time Division Multiplexing. Multiplexing through time division. Time is divided into intervals each of which is assigned to a communication channel. This is the principle of signal transport in digital telephony.

1.5 REFERENCE DOCUMENTS

See the technical documentation provided on Mitel.com.

1.6 REMINDER CONCERNING THE LAW ON INFORMATION TECHNOLOGY

It is the responsibility of a PBX user to check that it is used in accordance with the applicable law, standards and directives.

Therefore, the user is reminded that the use of PBXs in the workplace must comply with the specifications, standards and recommendations of the IT law in force.

The user's attention is also drawn to any clauses applicable in laws relating to the confidentiality of calls transmitted by means of electronic communications, which he/she must comply with.

2 ACCESSING THE SYSTEM USER INTERFACE

This first part describes the items required for MiVoice 5000 Web Admin to work correctly.

The second part is devoted to the characteristics of the user interface and, in particular, the different work screen areas.

The third part describes the role of the buttons used on the screens to facilitate parameter input in the corresponding fields, validation, and repetition of tasks and, of course, navigation between the different user interface screens.

2.1 SOFTWARE ENVIRONMENT

For operating system and browser compatibility, please refer to the document **Product Compatibility - MiVoice 5000 releases** provided with the software version of this document.

2.2 USER INTERFACE

Before describing the characteristics of the user interface, it is necessary to explain how to access MiVoice 5000 Web Admin.

2.2.1 ACCESSING MIVOICE 5000 WEB ADMIN

Access to the MiVoice 5000 Web Admin user interface is only via a web browser (see the section “Supported browsers”).

The HTML / HTTPS interface is secure.

Before accessing Web Admin, first validate the certificate provided by Mitel. This procedure is described in the document MiVoice 5000 Server - Installation and Implementation.

2.2.2 ADVANTAGES

The web interface allows access to all the MiVoice 5000 Web Admin screens, to configure Mitel series PBXs.

This interface offers the browsing possibilities available in all web sites: (previous page, next page, define bookmarks, print screens, etc.).

The Web Admin interface also offers the following advantages:

- Repetition function with condition
- Export of current item
- Export of all items in the MMC
- Search by keyword
- Marking sessions
- Access to marked pages
- Presentation in tabs
- Availability of display MMCs on several pages
- Access to screens by menu number
- On-hold messages

These functions are described in detail in the part "Pop-up windows and command buttons”, in this chapter.

2.2.3 HOMEPAGE

2.2.3.1 *Accessing the web page*

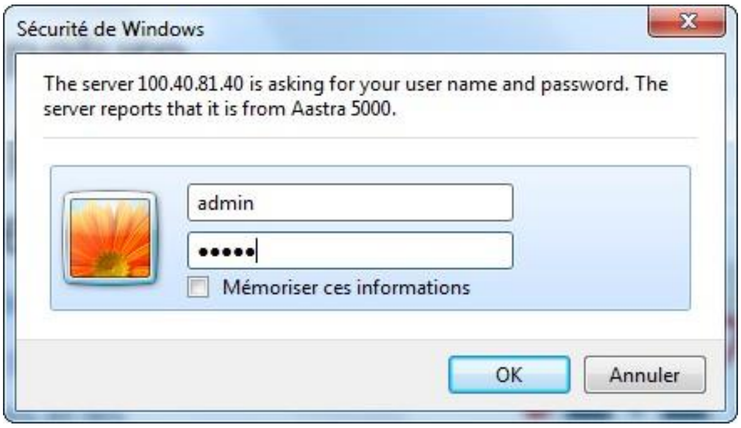
Enter the system IP address in the navigation bar: Example https://122.122.32.32

By default, the HTTPS access port is 443, for optimum connection.

IMPORTANT: After a pre-configuration without IP address setting, access through the web interface is allowed by the system, and Port 433 is configured correctly and associated with the system's canonical IP address (192.168.65.1).

2.2.3.2 *Opening a session*

The identification window opens once the system IP address is entered:



Sécurité de Windows

The server 100.40.81.40 is asking for your user name and password. The server reports that it is from Aastra 5000.

admin

•••••

□ Mémoriser ces informations

Login window (without password policy, see below).

This window allows you to enter a username and a password, which protect access to the screens and system management functions.

The operator is identified when the session is opened. This login is also automatically prompted for at the end of the activity time-out (by default, 10 minutes).

If the operator enters an incorrect password, the entry field is reset. The operator must enter the password again. If the operator wishes to identify himself again while the session is open (change of profile, for instance), he must open a new session.

Note: the default connection settings are admin:admin

Password policy and immediate password change

<u>**During first connection**</u>:

The default password is the one assigned to the administrator. This value must be changed immediately and customised by the user if the administrator has enabled a password policy. See Section 4.4.4.

<u>**Subsequently**</u>:

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

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

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

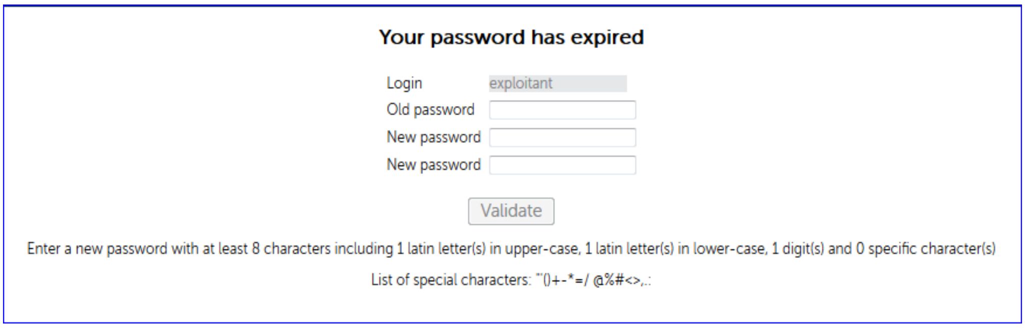
Once you have logged in, the Web Admin home screen is displayed.

Note: By default, if a user makes 5 consecutive incorrect login attempts within 10 minutes, their access to the Web Admin will be permanently locked.

Automatic locking settings and locked IP address management can be configured in Menu System>Security> Web>Security. See Section 4.4.6 – WEB Security. .

Changing the password

If a policy has been defined (see Section 4.4.4), the identification window will look different as follows:



Your password has expired

Login	exploitant
Old password	
New password	
New password	

Enter a new password with at least 8 characters including 1 latin letter(s) in upper-case, 1 latin letter(s) in lower-case, 1 digit(s) and 0 specific character(s)

List of special characters: "()+-*=/ @%#<>,.:

This window then prompts the user, depending on their profile, to change their password according to the syntax rules described in Section 4.4.4.

This window consists of four fields, three of which are input fields:

- The first, non-modifiable, field contains the login used by the operator to log on.
- The second one is for entering the old password: the expired password or the password the operator wishes to change.
- The last two fields are for entering the new password. The same input must be made in both fields.

For it to be valid and thus clear the menu validation button, the old password field must be filled in, the new password must be identical in the last two fields and must respect in terms of length and type of characters the policy (recalled in the last paragraph of the screen) defined in Menu **SYSTEM>Security>Web Admin Password Policy** - See Section 4.4.4.

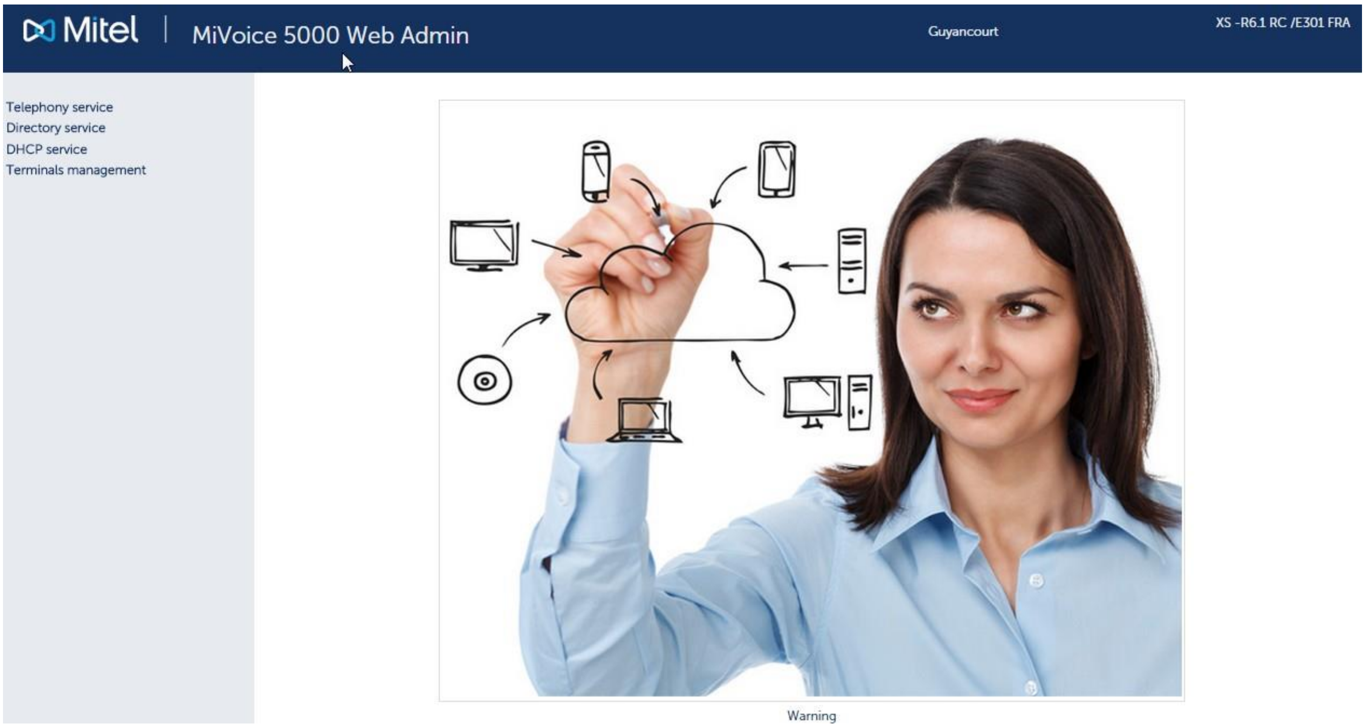
The new password must be different from the old password.

If the screen is called up for a password change, a **Cancel** button is available to return to the Web Admin home screen without changing the password.

If the password has expired, the **Cancel** button is not present as the user has no choice but to enter and confirm a new password.

2.2.3.3 *Welcome screen*

Once the username and password are recognised by the system, the MiVoice 5000 Web Admin welcome screen opens:



Welcome screen

Note: If a Password modification link is displayed on the left side in the menu bar, see Section 2.2.6.
If a red "Warning" message is displayed on the left side in the menu bar, see Section 2.2.4.

The main functions of MiVoice 5000 Web Admin available are:

- **Telephony service**: system management
- **DHCPv4 Service**/**DHCPv6 Service**: management and configuration via DHCP
- **Terminals management**: managing terminals
- **Easy Admin service**: managing directory, calendar and open/closed days

For the DHCP SERVICE, this function is offered to manage the settings of the following devices:

- MiVoice 5300 IP Phone,
- Mitel SIP terminals 6xxxi,
- IP terminals i7xx
- Terminals 312i (WIFI)
- MiVoice Conference terminals,
- TA7102i,

- AG4100 Analog Gateways,
- IP DECT base stations

For the TERMINAL SERVICE, this menu gives access to the TMA integrated into the iPBX.

To enable the terminal service, in Menu **SYSTEM>Configuration>Services** select telephony service then on the line **Terminal service** click **START** in the list area.

For information about the integrated TMA and how it works, see the corresponding documentation.

The TMA, integrated into MiVoice 5000 Server, is used to deploy and manage the following terminals:

- Proprietary MiVoice 5300 IP Phones,
- Mitel 6000 SIP Phones,
- MiVoice 5300 Digital Phones.

Note: After ten minutes of inactivity, the on-going session is automatically closed. More precisely, the http client is disconnected from the system.
This timeout (600 seconds maximum) can be set thanks to the function SYSTEM>Configuration>Management sets>Characteristics (see the chapter “System management”). This timeout concerns telephony service alone.

Refreshing the display

When sessions are opened, it may be necessary to delete cookies and temporary files from the browser in order to obtain a correct display in the web browser.

2.2.4 MITEL LEGAL DISCLAIMER FOR ACCESS TO WEB ADMIN

In order to alert site users to the risks of hacking and security constraints, a warning message for the various operators is displayed in Web Admin.

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

The complete operation mode is described in the Appendix to the document MiVoice 5000 Server - Implementation.

2.2.5 WARNING ABOUT EXPIRING SOFTWARE ASSURANCE

Upgrading to a minor or major software release, or per Delta batch, if subject to a software subscription, is associated with a validity period (Software Assurance or SWA).

Note: Security patches are not affected.

A warning banner for the expiring software assurance may be displayed above the menus in the following cases:

- The software assurance will expire in XY days: number of days remaining before the SWA expires, this information appears as soon as the PBX has less than 30 days of SWA left.
- Software assurance has expired: when the SWA has expired.

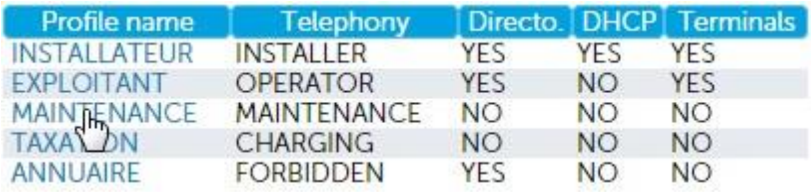
An expiry message will also be shown in the **Upgrade** menus. See Section 4.5.4.

The software assurance (SWA) expiry date is indicated in Menu **SYSTEM>Info>Licences**.

2.2.6 PASSWORDS

Different user profiles have been defined in advance to take into account the needs of each person handling the user interface. These profiles are mainly based on the user's tasks: installer, operator, maintenance technician.

SYSTEM functions (SYSTEM>Configuration>Users) may be used to modify existing profiles or to create new profiles. See Section 4.3.2.



Profile name	Telephony	Directo.	DHCP	Terminals
INSTALLATEUR	INSTALLER	YES	YES	YES
EXPLOITANT	OPERATOR	YES	NO	YES
MAINTENANCE	MAINTENANCE	NO	NO	NO
TAXATION	CHARGING	NO	NO	NO
ANNUAIRE	FORBIDDEN	YES	NO	NO

Predefined user profiles

Depending on the password entered, the user may have restricted access, compared to the description given in this document (some menus will not be accessible).

Applying a security policy on passwords

In this case, the user will have to change their password after it expires.

2.3 POP-UP WINDOWS AND COMMAND BUTTONS

No matter the level on which the user is in the management portal, a lot of tools (search and export functions, list and repeat functions, pop-up windows, navigation bar) are made available to the user to facilitate access to the various input screens, and the search for information. These tools are described in the following sections.

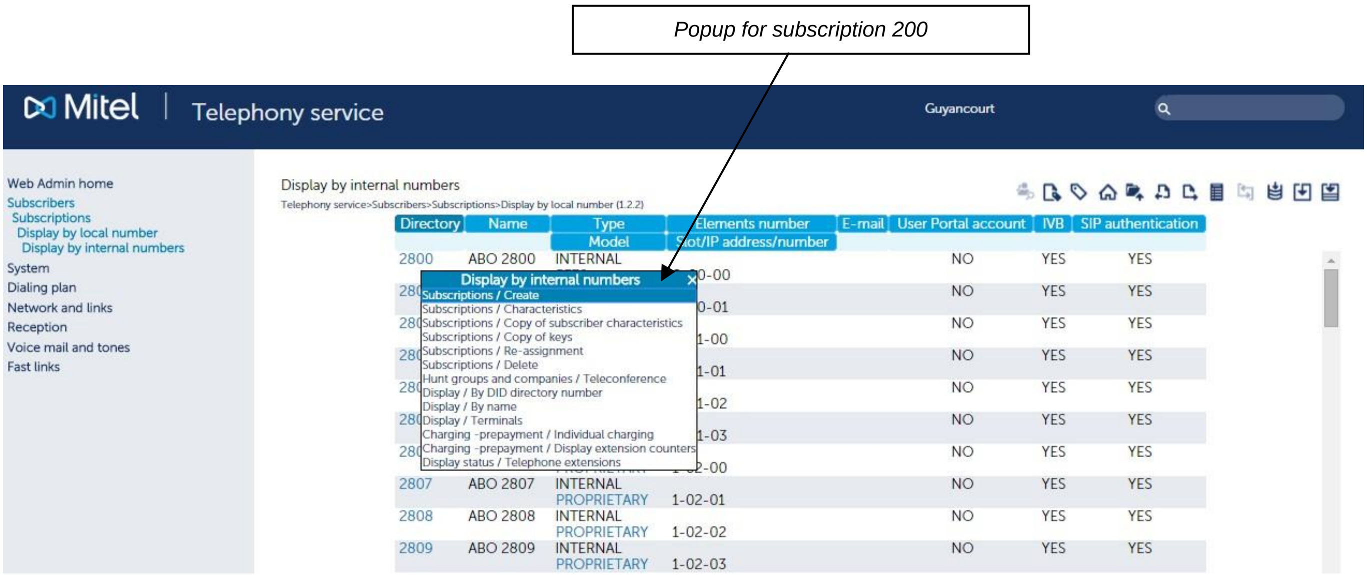
2.3.1 POP-UP WINDOWS

2.3.1.1 *Pop-ups for associated actions or zoom*

The list of zooms associated with a parameter is henceforth displayed in a pop-up window which appears when the corresponding parameter is left-clicked.

The pop-up window is displayed in the position of the mouse and disappears either when a link is activated or during a mouse event outside the pop-up window, or when the red cross in the pop-up title bar is pressed. In these last two cases, when the window is closed, the operator is then outside the initial MMC as if they had not activated the parameter’s hypertext link.

Note that if only one action is available, left-clicking the corresponding parameter does not display the pop-up window but takes you directly to the zoom menu.



Popup for subscription 200

Mitel
Telephony service
Guyancourt
Web Admin home
Subscribers
Subscriptions
Display by local number
Display by internal numbers
System
Dialing plan
Network and links
Reception
Voice mail and tones
Fast links
Display by internal numbers
Subscriptions / Create
Subscriptions / Characteristics
Subscriptions / Copy of subscriber characteristics
Subscriptions / Copy of keys
Subscriptions / Re-assignment
Subscriptions / Delete
Hunt groups and companies / Teleconference
Display / By DID directory number
Display / By name
Display / Terminals
Charging -prepayment / Individual charging
Charging -prepayment / Display extension counters
Display status / Telephone extensions

Display by internal numbers

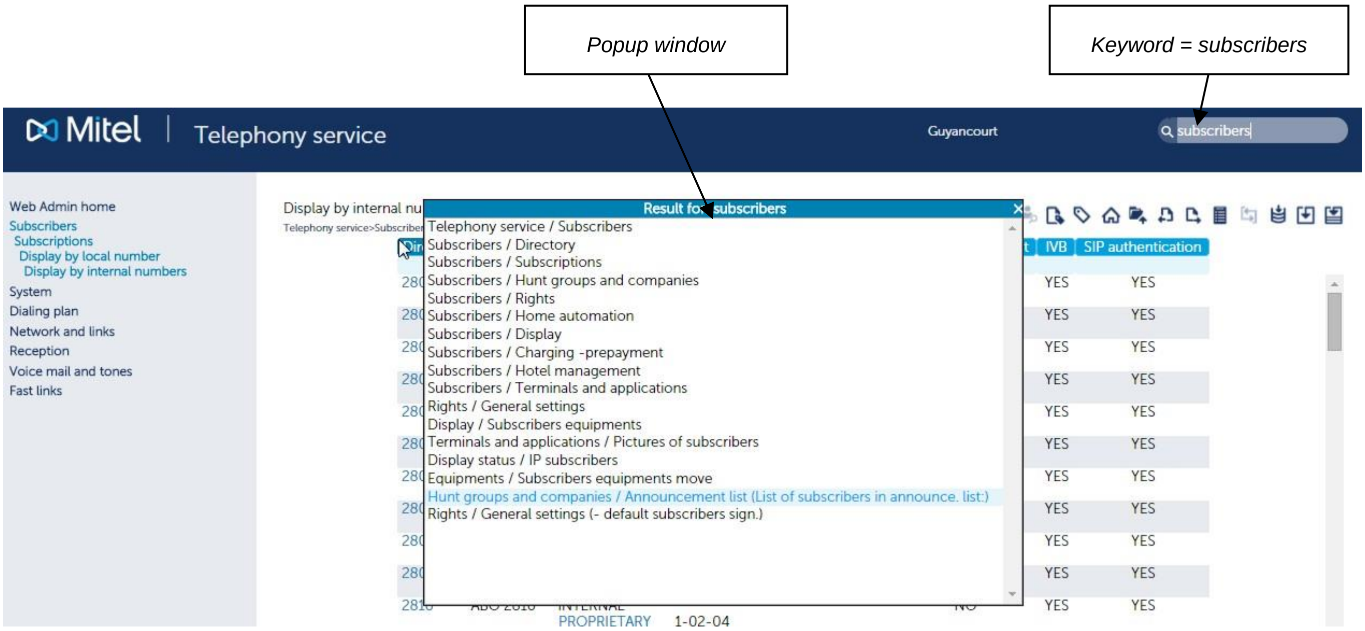
Telephony service>Subscribers>Subscriptions>Display by local number (1.2.2)

Directory	Name	Type	Elements number	E-mail	User Portal account	IVB	SIP authentication
		Model	Slot/IP address/number				
2800	ABO 2800	INTERNAL	0-00		NO	YES	YES
280			0-01		NO	YES	YES
280			1-00		NO	YES	YES
280			1-01		NO	YES	YES
280			1-02		NO	YES	YES
280			1-03		NO	YES	YES
280			2-00		NO	YES	YES
2807	ABO 2807	INTERNAL PROPRIETARY	1-02-01		NO	YES	YES
2808	ABO 2808	INTERNAL PROPRIETARY	1-02-02		NO	YES	YES
2809	ABO 2809	INTERNAL PROPRIETARY	1-02-03		NO	YES	YES

Zooming in on subscription 200

Search by keyword pop-up window

A pop-up window opens, just like during a search by keyword.



Result for subscribers

- Telephony service / Subscribers
- Subscribers / Directory
- Subscribers / Subscriptions
- Subscribers / Hunt groups and companies
- Subscribers / Rights
- Subscribers / Home automation
- Subscribers / Display
- Subscribers / Charging -prepayment
- Subscribers / Hotel management
- Subscribers / Terminals and applications
- Rights / General settings
- Display / Subscribers equipments
- Terminals and applications / Pictures of subscribers
- Display status / IP subscribers
- Equipments / Subscribers equipments move
- Hunt groups and companies / Announcement list (List of subscribers in announce. list:)
- Rights / General settings (- default subscribers sign.)

2.3.2 COMMAND BUTTONS

2.3.2.1 *Switching to Advanced or Basic mode (SIP trunk configuration)*

The icon allows you to switch, for a particular configuration, from basic (simplified) mode to advanced mode (meant for installers who want a more comprehensive configuration).

The icon represents the mode to which you change when you click on it.

The mode change is currently only available in the SIP bundle configuration (Menu Telephony service>Network and links>Network>Trunk groups>Characteristics):

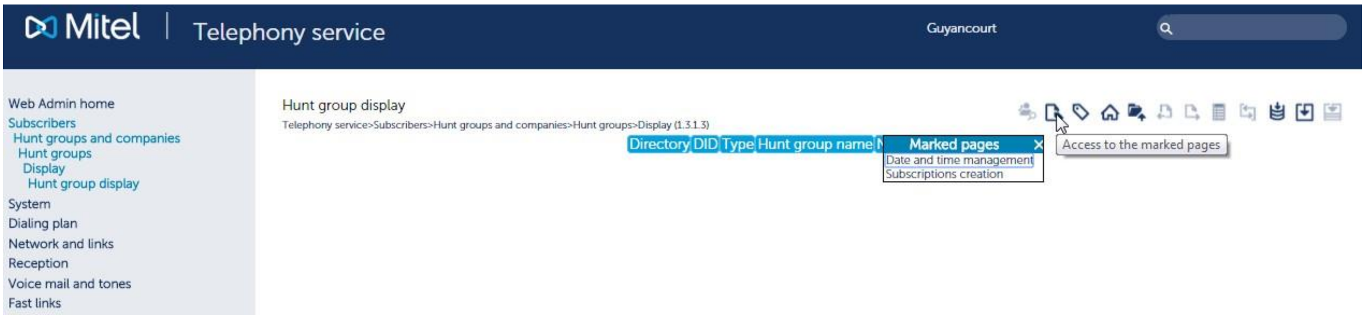
In basic mode, a simplified frame is offered with the minimum parameters needed to quickly and easily configure the trunk.

In advanced mode, more fields are proposed and they allow a more extensive and comprehensive configuration.

2.3.2.2 *Marking pages / accessing marked pages*

The button is used to mark pages while browsing, and to store the various screens visited. It is possible to store a maximum of 9 bookmarks. Beyond this, the oldest bookmark is erased and replaced by the new one.

To access the marked pages, click the button then, in the marked pages pop-up window, select the menu to be started.



Example of marked pages

Note: The bookmarks are kept as long as the web session is open. The pages are not preserved when the session is closed.

2.3.2.3 *Returning to the telephone service welcome screen*

The button is used to return to the **TELEPHONY SERVICE** welcome screen.

2.3.2.4 *Going back one level*

The button is used to move back one level in the MMCs.

2.3.2.5 *Moving to the previous or next item*

The button is used to return to the previous item.

The button is used to move to the next item.

These scroll arrows are used to select the next or previous item on the same screen. The arrows remain greyed out if they are inactive in the context.

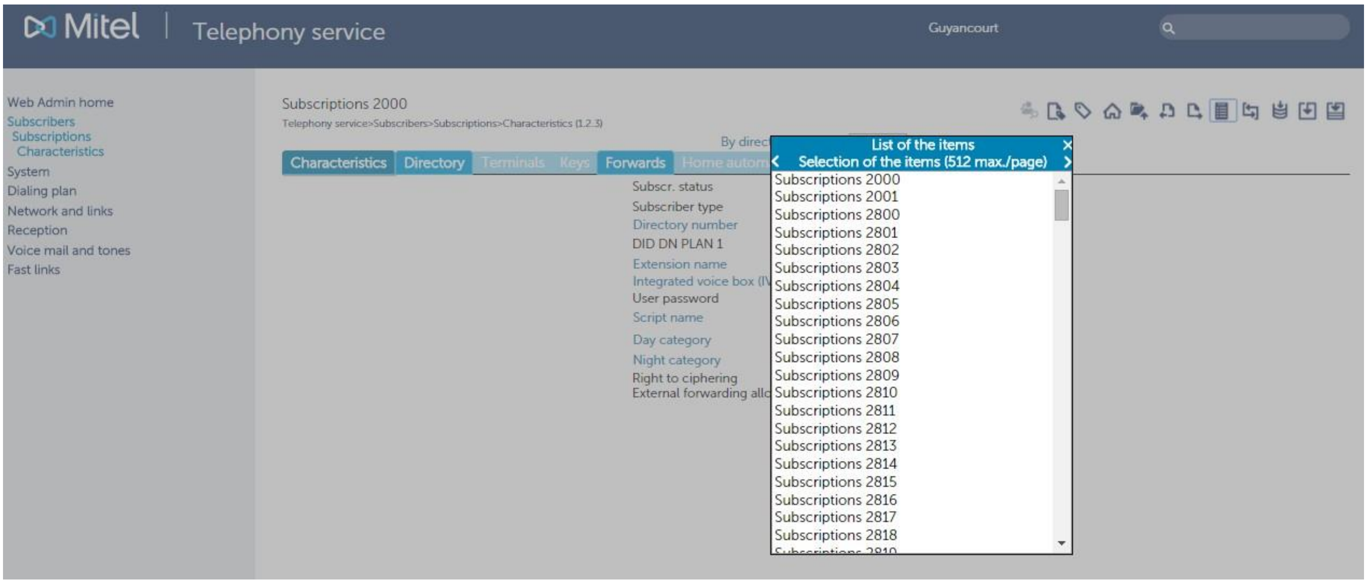
2.3.2.6 *Loading the list*

The button is used to display, on a page of 512 items, the items managed by an MMC.

This button is coloured when a list exists, and greyed out if it is inactive in the context.

For example, the extension characteristics menu gives the list of existing subscribers as shown in the figure below.

In this window, the two small arrows on each side of the table of items are used to move to the next or previous 512 items. To move to an item, just click it.



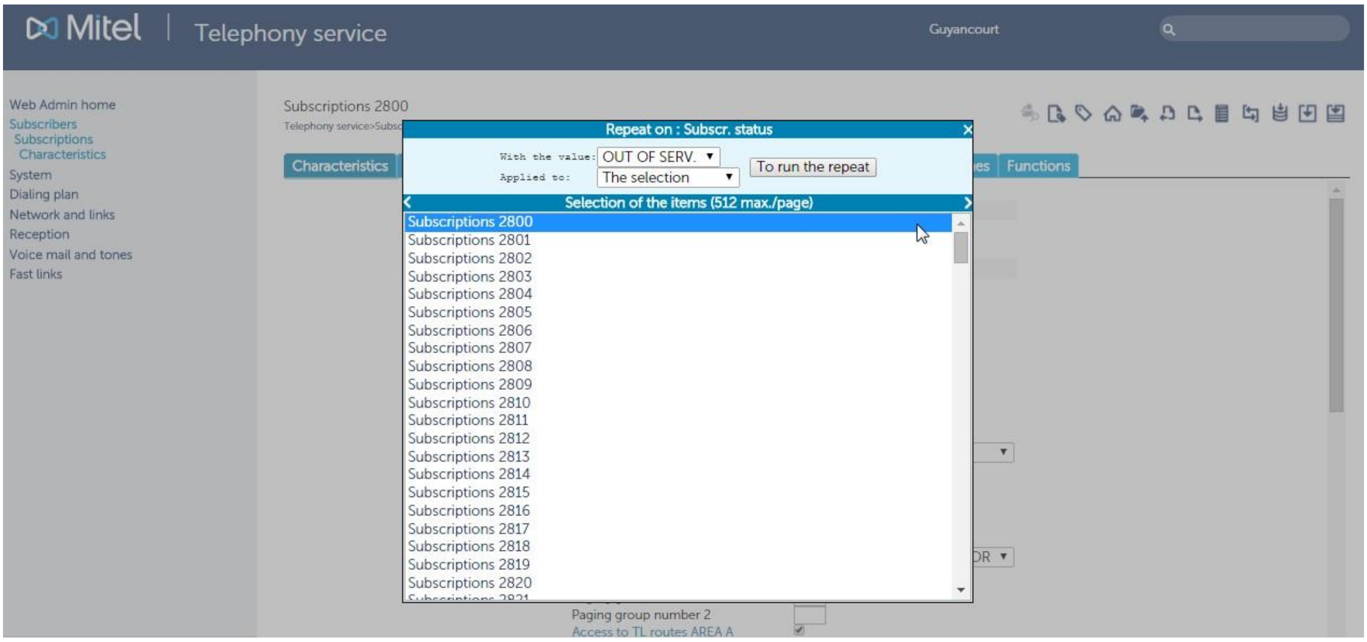
The pop-up window only disappears when the red cross on the title bar is pressed, and any mouse action outside the window is disabled.

Note: In Internet Explorer 6, the parameters display area is totally hidden when the pop-up window is diaplayed.

2.3.2.7 *Repeat function*

This function is accessible via the button. If it is inactive in the context, the button is greyed out.

This function is used to apply the value of the selected field to the next items or to a set of items selected on the same type of list.



Repeat on : Subscr. status

With the value: OUT OF SERV.

Applied to: The selection

To run the repeat

Selection of the items (512 max./page)

Subscriptions 2800
Subscriptions 2801
Subscriptions 2802
Subscriptions 2803
Subscriptions 2804
Subscriptions 2805
Subscriptions 2806
Subscriptions 2807
Subscriptions 2808
Subscriptions 2809
Subscriptions 2810
Subscriptions 2811
Subscriptions 2812
Subscriptions 2813
Subscriptions 2814
Subscriptions 2815
Subscriptions 2816
Subscriptions 2817
Subscriptions 2818
Subscriptions 2819
Subscriptions 2820

Example of repetition

In this example, the night category value of the first subscriber on the list (200) is modified.

At this stage, the repeat function is used to apply the value **INTERNATIO.** according to two different modes:

- To **SELECTION**
- To **ANY NEXT ELEMENT**.

Apply to: SELECTION

In this case, just make the selection on the list by pointing to the items in question (using the “Maj” and “Ctrl” keys). The selected elements are highlighted in a dark colour. Then click *To run the repeat* to apply the changes. Wait for the hold message to close automatically to close the repetition window.

Note: By default no item is selected.

Apply to: ANY NEXT ELEMENT

In this case, when you click the **Start repetition** button, all the next elements on the list will be modified. Wait for the hold message to close automatically to close the repetition window.

Note: In Internet Explorer 6, the parameters display area is totally hidden when the pop-up window is displayed.

2.3.2.8 *Export current element*

This function is accessible via the button. If it is inactive in the context, the button is greyed out.

This function is used to export information about the current item in a file in .csv format.

For menus organised into several tabs, the button allows you to export one or more tabs in a single "archive" file containing the N CSV files each describing a tab. The archive is in TAR format.

The TAR archive is also created with files possibly related to the exported item. In other words, and as an example, for the tone definition menu, this action allows the retrieval of the announcement "WAV or MP3 file" linked to the tone.

Note: At the moment, this concerns IVB, IVR and tone files only.

Other examples:

In the IVR script management menu (Menu **RECEPTION>IVR Scripts**), this operating mode allows you to retrieve the entire definition of a script in a single operation.

In the tone definition menu (Menu **VOICE MAIL AND TONES>Tones**), this operating mode allows the retrieval of the announcement "WAV or MP3 file" linked to the tone.

The CSV file can easily be modified with the help of a spreadsheet and then imported into the system using Menu **SYSTEM>Software maintenance>Massive import**, thus allowing a speedy iPBX-data update.

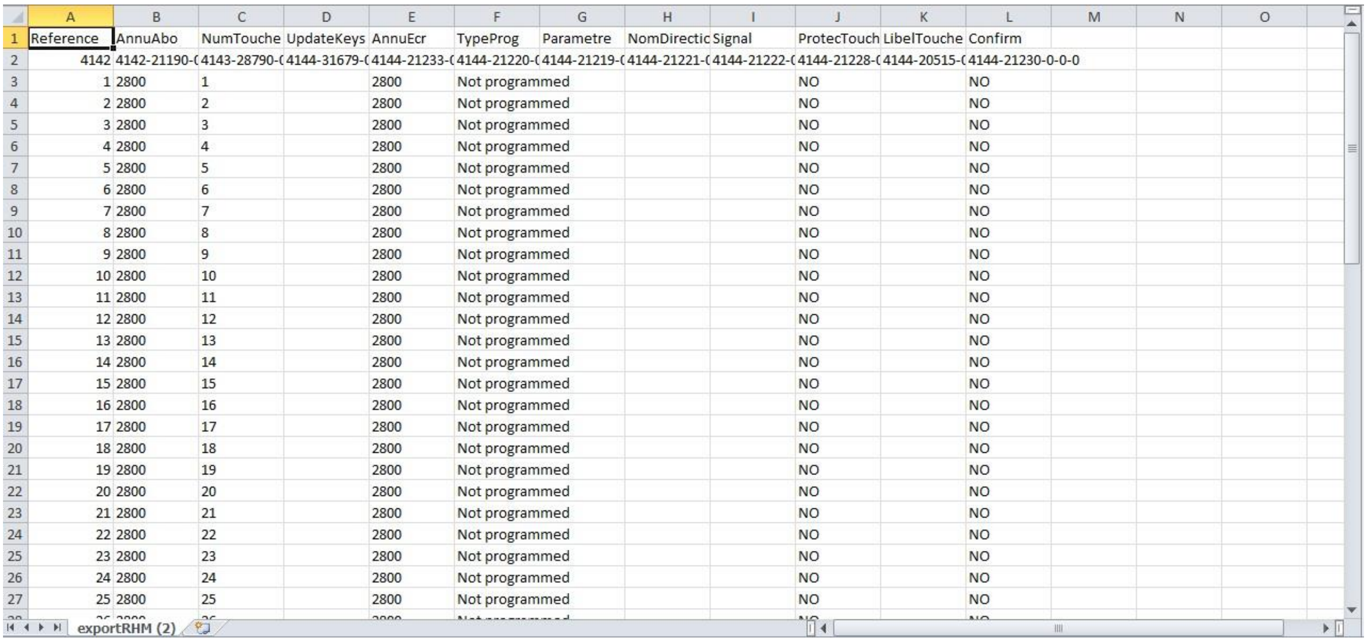
This function is available in all the menus.

For example if the operator is in the edit menu of the programmed keys of Subscriber 200, the individual diskette will only export the keys of Subscriber 200, while the multi-diskette will export all the keys of all the system's subscribers.

From the extension characteristics selection screen, click the **Keys** tab then the button.

An on-hold message appears then closes automatically. The window then opens.

Click **Save file** to save the file so you can use it again later, or click **Open with** to see the content of the export:



	A	B	C	D	E	F	G	H	I	J	K	L
1	Reference	AnnuAbo	NumTouche	UpdateKeys	AnnuEcr	TypeProg	Parametre	NomDirectic	Signal	ProtecTouch	LibelTouche	Confirm
2	4142	4142-21190-(	4143-28790-(	4144-31679-(	4144-21233-(	4144-21220-(	4144-21219-(	4144-21221-(	4144-21222-(	4144-21228-(	4144-20515-(	4144-21230-0-0-0
3	1	2800	1		2800	Not programmed				NO		NO
4	2	2800	2		2800	Not programmed				NO		NO
5	3	2800	3		2800	Not programmed				NO		NO
6	4	2800	4		2800	Not programmed				NO		NO
7	5	2800	5		2800	Not programmed				NO		NO
8	6	2800	6		2800	Not programmed				NO		NO
9	7	2800	7		2800	Not programmed				NO		NO
10	8	2800	8		2800	Not programmed				NO		NO
11	9	2800	9		2800	Not programmed				NO		NO
12	10	2800	10		2800	Not programmed				NO		NO
13	11	2800	11		2800	Not programmed				NO		NO
14	12	2800	12		2800	Not programmed				NO		NO
15	13	2800	13		2800	Not programmed				NO		NO
16	14	2800	14		2800	Not programmed				NO		NO
17	15	2800	15		2800	Not programmed				NO		NO
18	16	2800	16		2800	Not programmed				NO		NO
19	17	2800	17		2800	Not programmed				NO		NO
20	18	2800	18		2800	Not programmed				NO		NO
21	19	2800	19		2800	Not programmed				NO		NO
22	20	2800	20		2800	Not programmed				NO		NO
23	21	2800	21		2800	Not programmed				NO		NO
24	22	2800	22		2800	Not programmed				NO		NO
25	23	2800	23		2800	Not programmed				NO		NO
26	24	2800	24		2800	Not programmed				NO		NO
27	25	2800	25		2800	Not programmed				NO		NO

Key-data export file for Subscription 200

The first line of the file gives the names of the exported parameters.

The second line gives the internal codes of these parameters which will be used to update some parameters during a later import.

The next lines indicate the parameter values for each exported element.

The menus organised into several pages contain an additional column for indicating the page number.

⚠ **IMPORTANT NOTE: During file import, the parameter codes (second line of the file) should not be modified. To prevent a parameter from being updated in the system (for any of the elements), just delete the corresponding column in the file. The lines for the unmodified items can be deleted before the data is imported.**

2.3.2.9 *Export all elements in the MMC*

This function is accessible via the button. If it is inactive in the context, the button is greyed out.

This function is used to export information about the current item in a file in .csv format.

For menus organised into several tabs, the button is used to export one or more tabs into a single "archive" file containing N .csv files which describe each tab. The archive is in TAR format.

For menus with a selection menu and which, thus, define several identical items, a multiple export function was deployed to export all the following items from the one on which the command is run.

As indicated in the previous Section 2.3.2.8, the export function will allow all linked files to be recovered.

The CSV file can easily be modified with the help of a spreadsheet and then imported into the system using Menu **SYSTEM>Software maintenance>Massive import**, thus allowing a speedy iPBX-data update.

The function is available on each selection screen from a list of options, and on each screen with a list of elements.

The example below illustrates export in the home page name definition menu. From the home page definition screen, click the button. At the end of export, a window opens.

Click **Save file** to save the file so you can use it again later, or click **Open with** to see the content of the export:

The first line of the file gives the names of the exported parameters.

The second line gives the internal codes of these parameters which will be used to update some parameters during a later import.

The next lines indicate the parameter values for each exported element.

The menus organised into several pages contain an additional column for indicating the page number.

⚠ **IMPORTANT NOTE: During file import, the parameter codes (second line of the file) should not be modified. To prevent a parameter from being updated in the system (for any of the elements), just delete the corresponding column in the file. The lines for the unmodified items can be deleted before the data is imported.**

2.3.3 IMPORT FUNCTION

2.3.3.1 *Massive import*

For more information, see Section 4.5.5.

Menu **System>Software Maintenance>Massive import** provides an option between a generic massive import and an IVR signature import.

Massive import mode is used to define the item(s) identified through the selection criteria available in the import file. It was therefore not possible, without changing the imported file, to define other items than those exported, unlike the modes explained in the following sections.

The files are in.csv format or in TAR, TAR.GZ or ZIP format for the files stored in the archive.

2.3.3.2 *Importing data in the context*

For the import, the first mode consists in offering the import function directly in the menu defining the imported item.

On these conditions, the .csv file data taken at the input are used to configure the item being edited and not the one defined by the selection criteria available in the import file which are then ignored.

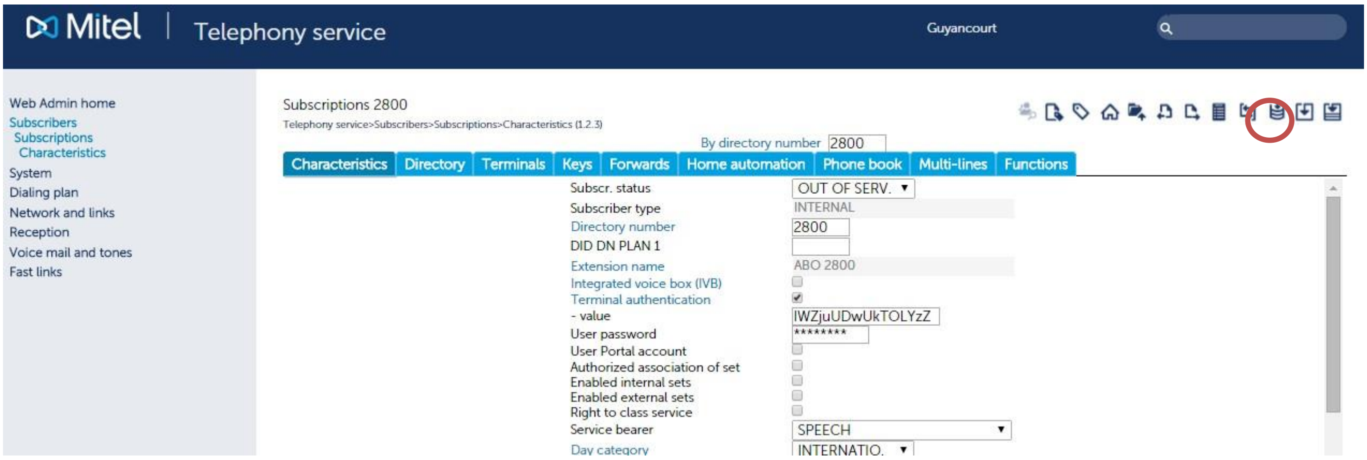
For menus defining several identical items, this operating mode is also used to modify, in only one operation, a series of items (selected when the command is run), taking into account the parameters of the item described in the imported file.

Finally, for the menus organised into several tabs, this command takes at the input a TAR type archive file which describes all the tabs of the menu. These are therefore all modified during this operation.

For instance, it is possible to retrieve from one site the definition of Subscriber 3000 to reimport it into another site as Subscriber 4000.

As shown in the figure below, the import command in the context is active in all the menus with an export command.

The command is activated using the database icon located just before the individual export command in the command bar.

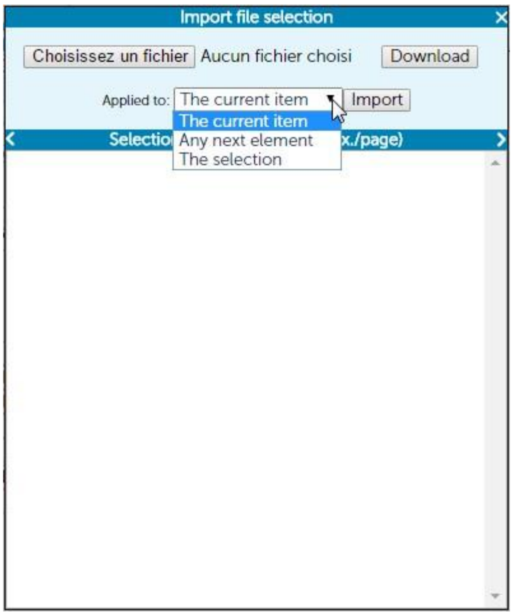


By directory number 2800

Subscr. status	OUT OF SERV. ▾
Subscriber type	INTERNAL
Directory number	2800
DID DN PLAN 1	
Extension name	ABO 2800
Integrated voice box (IVB)	□
Terminal authentication	☑
- value	IWZjuUDwUkTOLYzZ
User password	********
User Portal account	□
Authorized association of set	□
Enabled internal sets	□
Enabled external sets	□
Right to class service	□
Service bearer	SPEECH ▾
Day category	INTERNATIO. ▾

Clicking this icon opens the window below.

The action can be compared to the existing window for the **Repeat** modification icon in the following items concerning the selection of the items which will be modified through import.



In this popup window, the first line is used to select the import file on the internal disk of the client PC. Click the first button on the line to open the file manager and select the file to be imported.

Accepted formats are the same as those used in the import menu:

- CSV file
- TAR archive
- TAR.GZ archive
- ZIP archive.

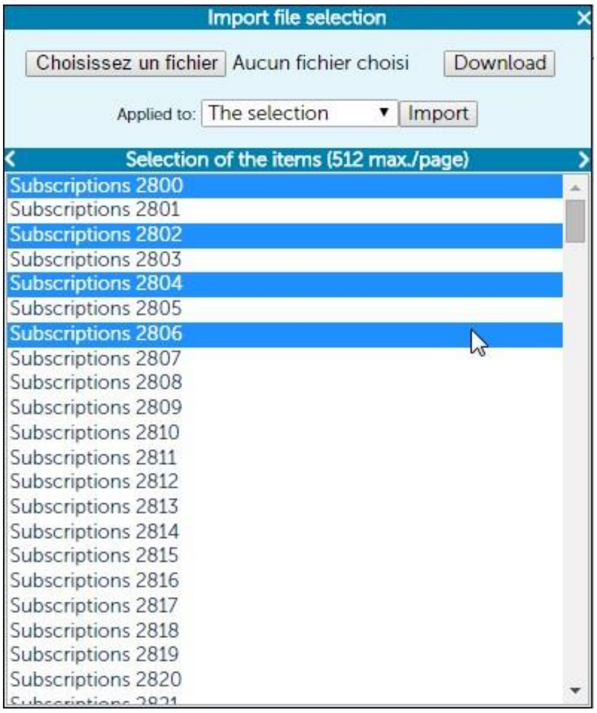
Click the **Download** button to send the selected file to Web Admin without importing it.

In case of error, there are two possibilities:

- Web Admin displays the message **Incorrect format** and cancel the operation.
- The **Import** button on the second line is inactive.

The second line is for selecting the import application mode:

- **The current item**: import is performed on the current item only.
- **Any_next_element**: import is performed on all the next items.
- **The_selection**: import is executed on the items chosen in the lower frame. See the figure below.



Import file selection

Applied to: The selection

Selection of the items (512 max./page)

Subscriptions 2800
Subscriptions 2801
Subscriptions 2802
Subscriptions 2803
Subscriptions 2804
Subscriptions 2805
Subscriptions 2806
Subscriptions 2807
Subscriptions 2808
Subscriptions 2809
Subscriptions 2810
Subscriptions 2811
Subscriptions 2812
Subscriptions 2813
Subscriptions 2814
Subscriptions 2815
Subscriptions 2816
Subscriptions 2817
Subscriptions 2818
Subscriptions 2819
Subscriptions 2820

Click Import.

In return, a popup window opens, just like the one obtained via the massive import commands of the corresponding menu.

2.3.3.3 *Importing files linked to the processed item*

This second import mode is similar to previous mode but allows the related file(s) to be taken into account if any.

The edited item is then entirely defined (with the related files) only through the import command, without any need to download the additional file(s) in a second phase.

For instance, in the IVR script management menu, this operating mode is used in a single operation to define an entire script.

Using the import function in the context, it is possible to create a script from the export of another script.

2.3.3.4 *Import possibilities according to executed import*

	MASSIVE IMPORT MMC	INDIVIDUAL IMPORT IN THE CONTEXT	MULTIPLE IMPORT IN THE CONTEXT
EXPORTING AN ITEM INDIVIDUALLY	Defining the identified item by the selection criteria of the exported item	Defining the edited item using the data on the exported item	Defining the selected items from the data on the exported item
MULTIPLE EXPORT OF SEVERAL ITEMS	Defining the items corresponding to those exported	PROHIBITED	PROHIBITED

2.3.4 SEARCH FUNCTION

Two search modes are available: search by keyword / by screen number.

2.3.4.1 *Search by keyword*

You can perform a search by keyword, by entering a word or part of a word (40 characters maximum) in the search area.

When you click the 🔍 button, the search engine returns in a pop-up window all the links pointing to a screen concerned by the word entered (cf. Section 1.2.1.2).

The principles for use are:

- Upper and lower cases are handled in the same way.
- If a character string contains several words, the search is based on the complete string.
- The search result displays the first 38 occurrences found.
- The search can also be made on a part of the word. For instance, the character string "subscriber" also concerns the occurrence "subscription".

Note: The search engine does not accept accented characters. To be recognised by the search engine, the terms entered in this area should not contain any accents.

The result is displayed in the following order:

- first the menus whose title contains the keyword: the menu and its parent menu are displayed in the format <parent menu>/<found menu>,
- then the menus whose keyword is contained in the label of any of its lines: the line concerned is displayed in brackets.

Note: If there is no result, a "no response" pop-up window opens.

Recommendations for use:

The search engine may return a large number of occurrences of the term entered. It is, therefore, advisable to use search by word only, to obtain a better result.

2.3.4.2 *Search by screen number*

This possibility is offered to an operator who knows the screen numbers and who wishes to access them directly.

The search is made by entering a screen number (without separator or space) in the search area.

Then click the 🔍 button, or press "Enter" to confirm.

Example: enter 22 to search Menu **SYSTEM>Supervision.**

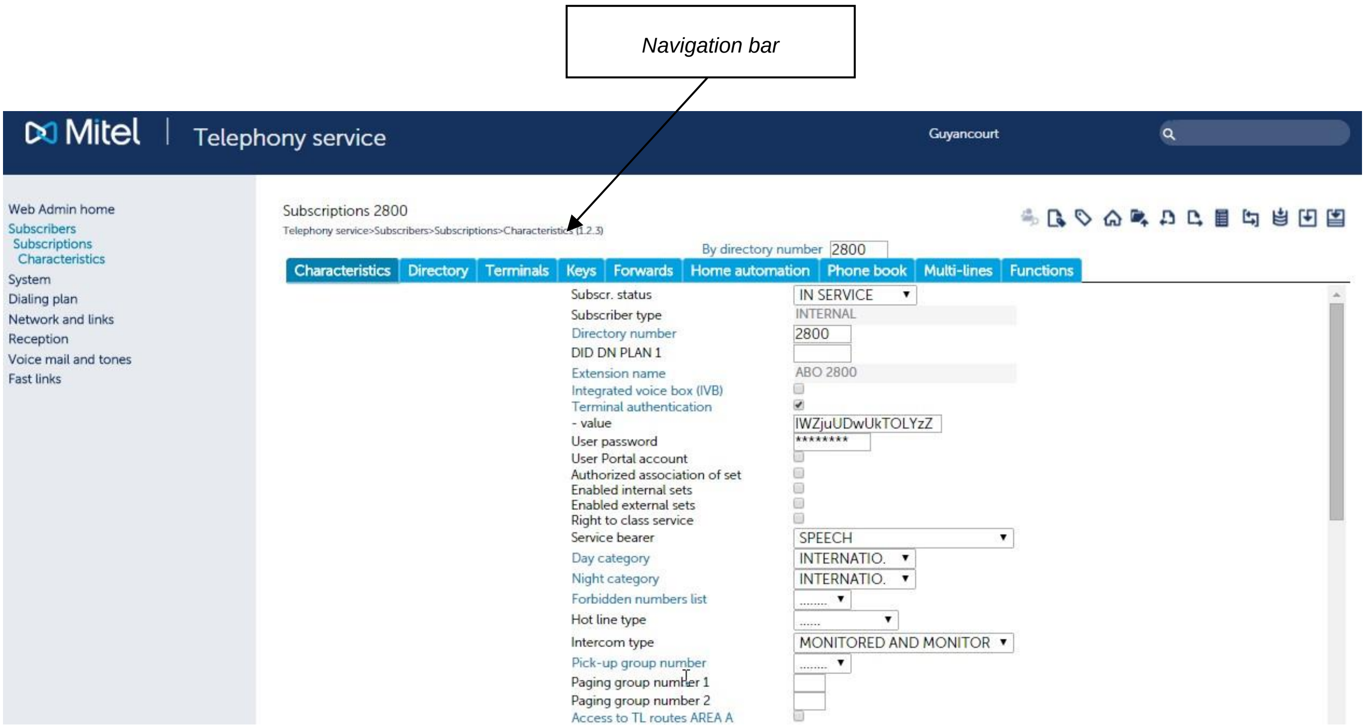
The menu is directly displayed and the search result pop-up window is not displayed.

If the menu does not exist, or is not accessible, the **Telephony service** menu is displayed.

IMPORTANT NOTE: Given the dynamic management of the screens, numbering varies according to the type of configuration declared: multi-company, multi-site, and the type of system (case of the Mitel 5000 Server). The numbers also depend on the operator's access rights which in turn depend on the login / password entered.

2.3.5 NAVIGATION BAR

Under the MMC title and command buttons there is a navigation bar which displays the tree structure taken to reach the MMC and is used to return directly to any of the menus accessed in the process, with a simple mouse click.



Subscriptions 2800

Telephony service>Subscribers>Subscriptions>Characteristics (1.2.3)

By directory number 2800

Subscr. status	IN SERVICE ▼
Subscriber type	INTERNAL
Directory number	2800
DID DN PLAN 1	
Extension name	ABO 2800
Integrated voice box (IVB)	□
Terminal authentication	☑
- value	IWZjuUDwUkTOLYzZ
User password	********
User Portal account	□
Authorized association of set	□
Enabled internal sets	□
Enabled external sets	□
Right to class service	□
Service bearer	SPEECH ▼
Day category	INTERNATIO. ▼
Night category	INTERNATIO. ▼
Forbidden numbers list	.... ▼
Hot line type	...... ▼
Intercom type	MONITORED AND MONITOR ▼
Pick-up group number	.... ▼
Paging group number 1	
Paging group number 2	
Access to TL routes AREA A	□

Navigation bar

An example is given in the figure below for the MMC:
Telephony service>Subscribers>Subscriptions>Characteristics (1.2.3)

Clicking the **Subscriptions** field in the navigation bar takes you directly to this menu.

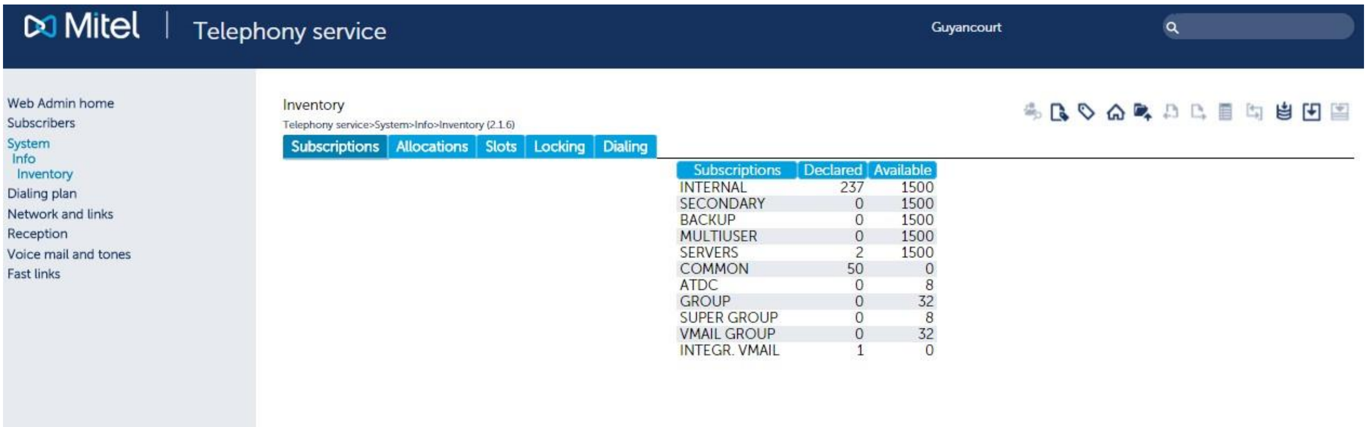
The figures indicated at the end (here 1.2.3) represent the sequence you just need to enter in the search area to move directly in the MMC. In fact, it is the succession of options in the tree structure as it is presented.

2.3.6 PRESENTATION IN TABS

2.3.6.1 *Internal MMC tabs*

Some MMCs display their parameters in form of tabs.

An example of a display menu organised into tabs is the **inventory** menu.



Inventory

Telephony service>System>Info>Inventory (2.1.6)

Subscriptions	Declared	Available
INTERNAL	237	1500
SECONDARY	0	1500
BACKUP	0	1500
MULTIUSER	0	1500
SERVERS	2	1500
COMMON	50	0
ATDC	0	8
GROUP	0	32
SUPER GROUP	0	8
VMAIL GROUP	0	32
INTEGR. VMAIL	1	0

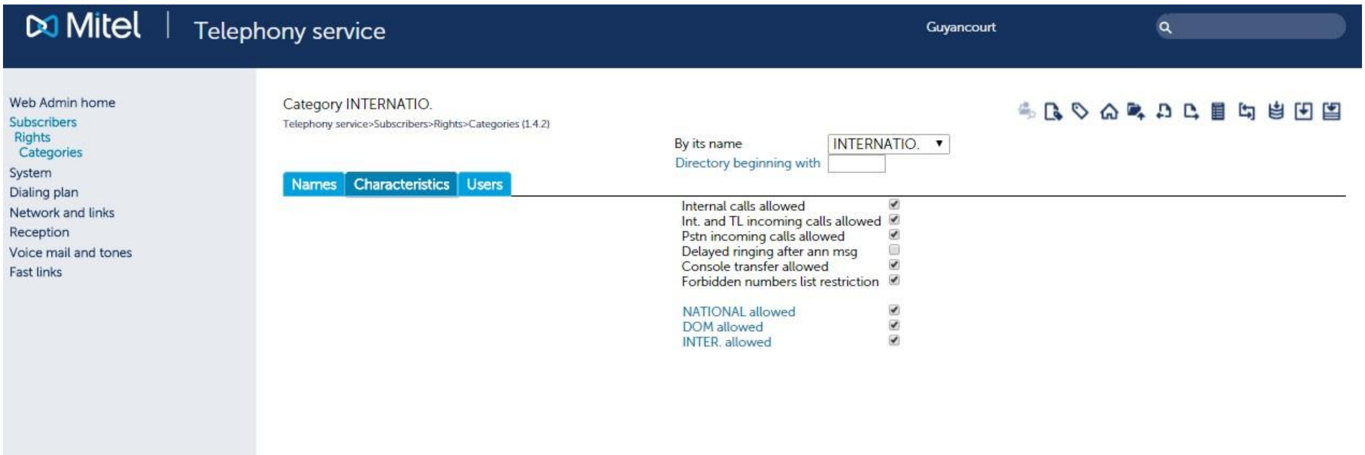
Tabs in the inventory menu

2.3.6.2 *MMC-based tab*

The notion of MMC-based tab is implemented in order to limit the tree structure levels. The aim is to group together as an entity the MMCs handling the same issue and having the same selection menu, if they have any.

An example can be taken with the management of PSTN categories in which the first MMC defines the names, a second one the properties of a category, while the third one gives the list of users in the selected category.

This makes it possible to have a category selection menu, and to display under it the previous three MMCs in form of a tab as shown in the figure below.



Category INTERNATIO.

Telephony service>Subscribers>Rights>Categories (1.4.2)

By its name: INTERNATIO.

Directory beginning with:

Internal calls allowed ☑
Int. and TL incoming calls allowed ☑
Pstn incoming calls allowed ☑
Delayed ringing after ann msg □
Console transfer allowed ☑
Forbidden numbers list restriction ☑

NATIONAL allowed ☑
DOM allowed ☑
INTER. allowed ☑

Tabs in the categories menu

Note: Depending on the selection criteria, all or just one part of the tabs will be accessible.

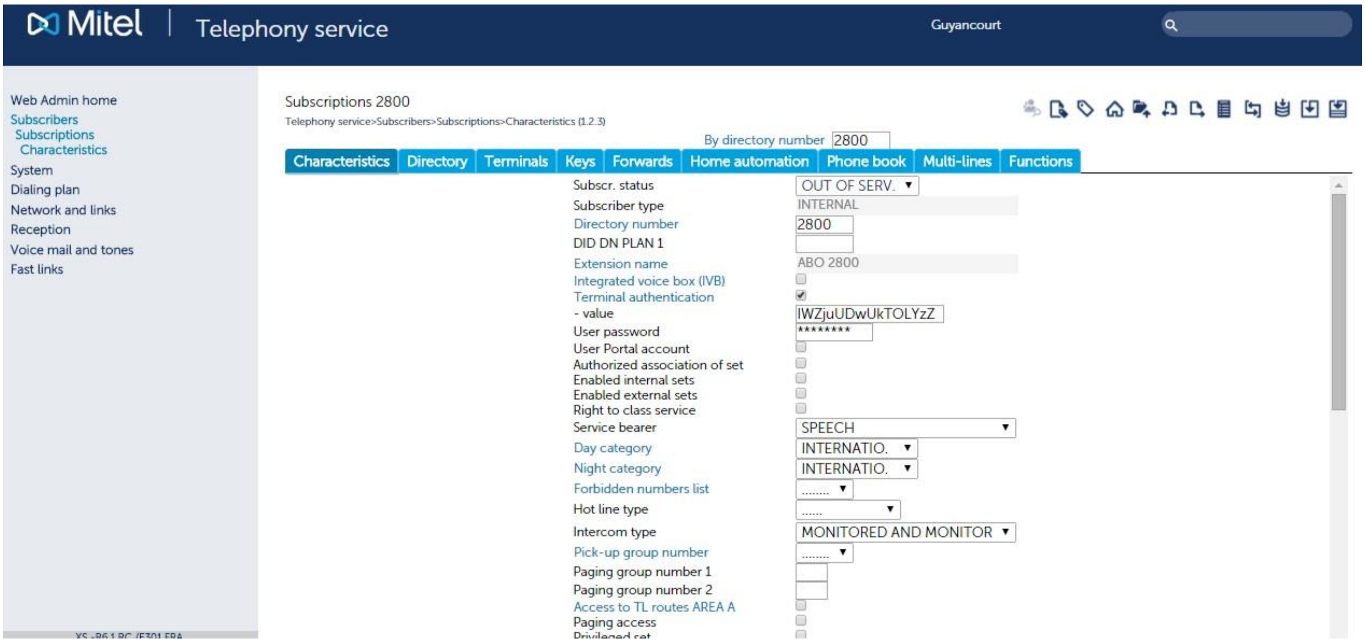
After a tab is opened, emphasis will be laid on the first field of the tab or else on the tab-implementation button.

The session can be generally locked for all the tabs, such that an operator cannot be in the category names menu and another operator in the category definition menu.

The commands “Next” and “Previous” work like before: if a tab is open, the items in the active tab are used.

The tab mode has been implemented for the following MMCs:

- Extension characteristics menu
- PSTN category management menu
- Feature class management menu
- TL class management menu
- Call distribution management menu
- IVS script management menu.



Subscriptions 2800

Telephony service>Subscribers>Subscriptions>Characteristics (1.2.3)

By directory number 2800

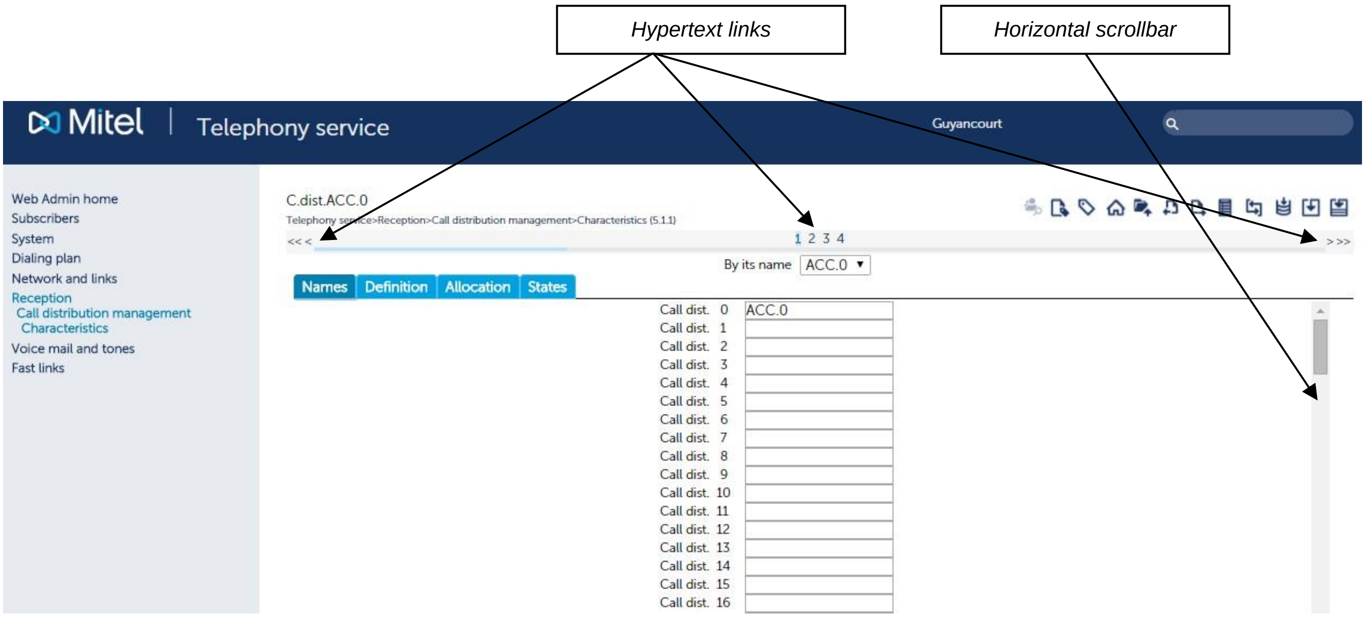
Subscr. status	OUT OF SERV. ▾
Subscriber type	INTERNAL
Directory number	2800
DID DN PLAN 1	
Extension name	ABO 2800
Integrated voice box (IVB)	□
Terminal authentication	☑
- value	IWZjuUDwUkTOLYzZ
User password	********
User Portal account	□
Authorized association of set	□
Enabled internal sets	□
Enabled external sets	□
Right to class service	□
Service bearer	SPEECH ▾
Day category	INTERNATIO. ▾
Night category	INTERNATIO. ▾
Forbidden numbers list	.... ▾
Hot line type	...... ▾
Intercom type	MONITORED AND MONITOR ▾
Pick-up group number	.... ▾
Paging group number 1	
Paging group number 2	
Access to TL routes AREA A	□
Paging access	□
Privileged set	□

Tabs in the menu Subscriptions>Characteristics

2.3.7 INTEGRATING MMCS DISPLAYED ON SEVERAL PAGES

For menus in which the total number of lines exceeds the limit imposed by the system, a page selection bar is added under the command button bar, as shown in the figure below.

The display and input menus are concerned by this enhancement.



C.dist.ACC.0

Telephony service>Reception>Call distribution management>Characteristics (5.1.1)

By its name ACC.0 ▼

Call dist. 0	ACC.0
Call dist. 1	
Call dist. 2	
Call dist. 3	
Call dist. 4	
Call dist. 5	
Call dist. 6	
Call dist. 7	
Call dist. 8	
Call dist. 9	
Call dist. 10	
Call dist. 11	
Call dist. 12	
Call dist. 13	
Call dist. 14	
Call dist. 15	
Call dist. 16	

Display on several pages of an MMC

In this example the total display is broken down into four pages numbered 1 to 4. Page N can be selected by clicking the hyperlink implemented via the corresponding number in this new bar.

The two hypertext links available at the ends of the page selection line are respectively used to go to the first page displayed, the page before the current page, the page after the current page, and the last page of the document. In all cases, the number of the currently displayed page is written without link.

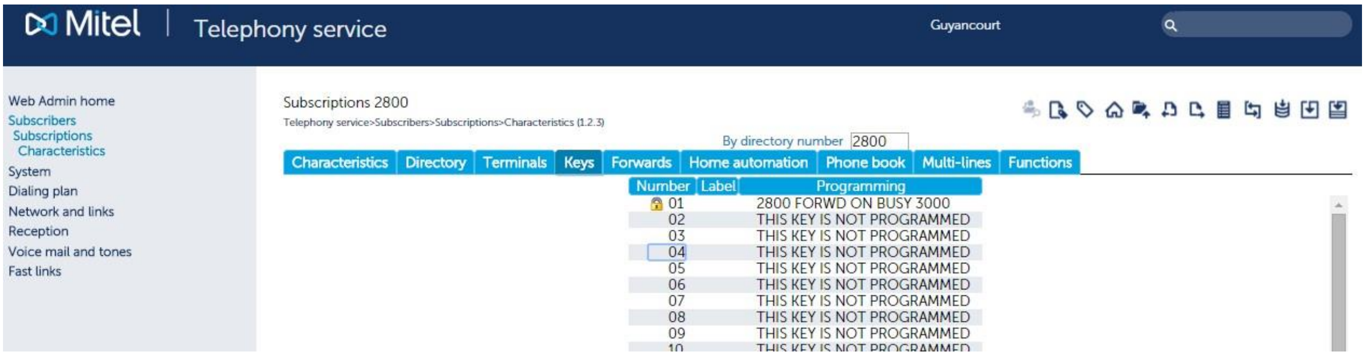
Moreover, a summary drawing of a scrollbar is placed under the page selection numbers. For Internet Explorer, the “black line” represents the area displayed in the entire document. For Firefox, the “black point” represents the location of the end of the page displayed in the entire document.

2.3.8 PROGRAMMED KEY MMC

The key-programming MMC now exists in form of an extension characteristics menu tab.

Moreover, to limit menu sequencing, the previous intermediate menu, which gives the existing key programming and is used to select the key to be programmed, has been integrated into the programming screen in form of a selection table.

The programming type options menu has been enhanced with feature types, and the parameter field is used to enter the additional information presented in form of an ASCII or digital string.



Subscriptions 2800

Telephony service>Subscribers>Subscriptions>Characteristics (1.2.3)

By directory number 2800

Number	Label	Programming
🔒 01		2800 FORWD ON BUSY 3000
02		THIS KEY IS NOT PROGRAMMED
03		THIS KEY IS NOT PROGRAMMED
04		THIS KEY IS NOT PROGRAMMED
05		THIS KEY IS NOT PROGRAMMED
06		THIS KEY IS NOT PROGRAMMED
07		THIS KEY IS NOT PROGRAMMED
08		THIS KEY IS NOT PROGRAMMED
09		THIS KEY IS NOT PROGRAMMED
10		THIS KEY IS NOT PROGRAMMED

Programmed key MMC

In the programming table, a “padlock” icon on the left of the key number indicates a protected key (the “protected key” checkbox has been ticked).

The keys not yet programmed appear in black. The already programmed keys appear in green.

Validating a programming operation automatically updates the display table. If emphasis is on the table, the “Up” and “Down” cursor keys can be used to change from one key to the other. The functions “Next” and “Previous” work on the different subscribers. The “Repeat” function is disabled.

The terminal is deactivated once a program is validated. The terminal is automatically reactivated if the user exits the tab, or by navigating in the subscriber list.

The table below gives the lines visible for each programming type. The lines not mentioned are always visible.

Note: "CCO supervision" key programming is only applicable for proprietary terminals (53xx, 675x) and SIP terminals (6700, 6800 & 6900).

	PARAMETER	DIRECTION	SIGNAL
No programming			
Dialling	PHONE NUMBER		
Cancel all forwarding			
Predefined forward			
Forward on busy	TERMINAL DIRECTORY		
Forward on no answer	TERMINAL DIRECTORY		
Immediate forward	TERMINAL DIRECTORY		
Activate notebook	TIME		
Deactivate notebook	TIME		
Lock			
General stand-by			
Filtering	TERMINAL DIRECTORY		
Do Not Disturb			
Anti-intrusion			
Your number monitoring (CCO)			
External line monitoring	EXTERNAL LINE DIRECTORY	X	X
Filtered call monitoring	TERMINAL DIRECTORY		X
Subscriber supervision	TERMINAL DIRECTORY		X
Privileged intercom (buzz/status)	TERMINAL DIRECTORY		
Phone box			
Tone dialling	PHONE NUMBER		
Your personal external line			
Outside / in hunt group			
Voice mailbox monitoring			X
Messages deposit			
Close room			
Room wake-up			
Open room			
Alarms monitoring			
Call supervision internal			X
Call supervision PSTN incoming 1			X
Call supervision PSTN incoming 2			X
Call supervision Tie-Line incoming			X
Overload signal			X
Reservation signal			X
Console activation			
Hold			
Save/Repeat			

2.3.9 WAIT MESSAGE

2.3.9.1 *Loading windows*

When it takes some time to load or open a window, the window displayed by the navigator includes an animated image that prompts the operator to wait.

This type of wait message may be displayed:

- When a page is opened
- In the MMC parameters input area
- When a tab is opened (the wait image appears in the tab content).

2.3.9.2 *Progress messages*

When it takes some time to modify a parameter or to download a file, a pop-up window opens and prompts the operator to wait. The display is automatic, and the page displayed automatically returns to normal at the end of processing.

Note: When the pop-up is displayed, the operator’s actions are ignored and ineffective.

When a file is downloaded, the message “Wait, work in progress” is replaced by a counter which increments every second.

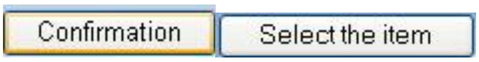
Wait, work in progress

Progress message when subscriptions are being created

2.3.10 OTHER BUTTONS

This paragraph describes the different buttons that facilitate parameter input and navigation between the user interface screens.

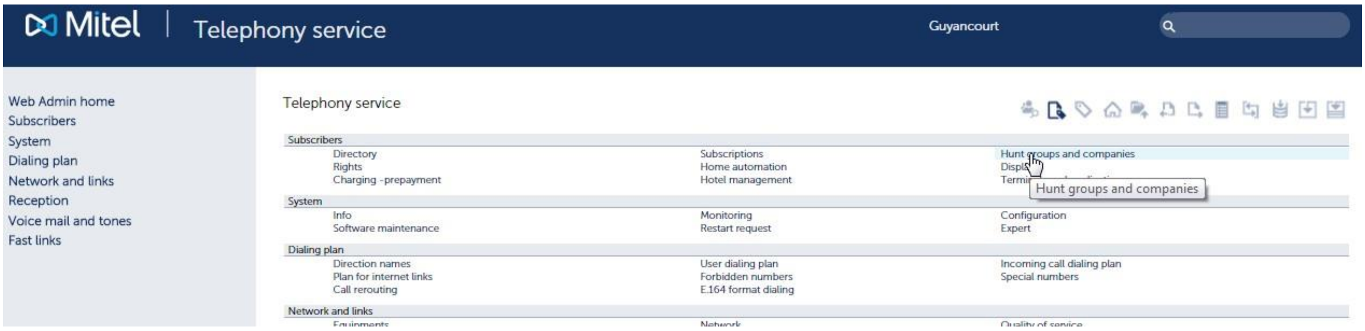
☒: when displayed in certain contexts (error messages, warnings, prohibitions, etc.), this button is used to close an open window or to stop an action in progress.



These buttons are used to validate actions carried out previously: entering parameters, changing a value, choosing an item from a list, etc., depending on the context.

2.3.11 "POP-UP" INFORMATION

When the cursor is moved over the different user interface fields and buttons, bubble type information is displayed if available.

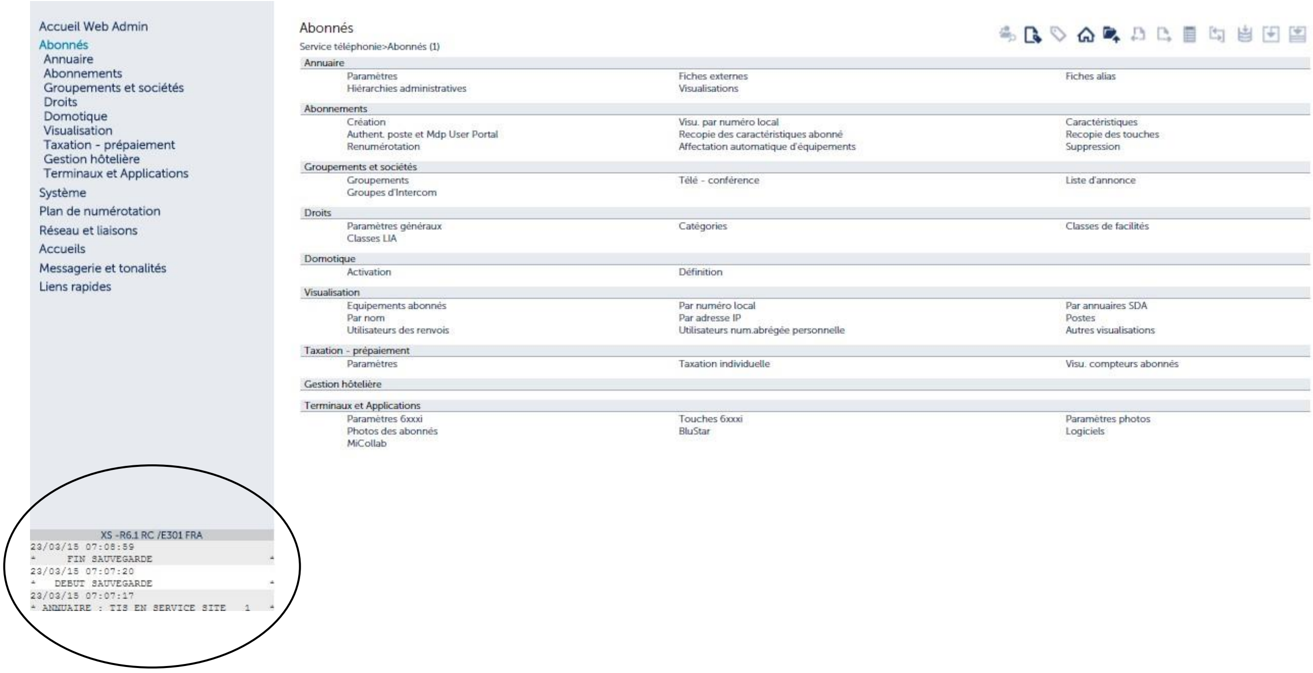


Example of pop-up information

2.3.12 LOGBOOK DISPLAY WINDOW

The permanent window at the bottom left of the screen is used to display the latest items recorded in the logbook.

Clicking the header of this window gives direct access to Menu **System>Monitoring>Display logbook**.



```
23/03/15 07:08:59
*     FIN SAUVEGARDE                *
23/03/15 07:07:20
*   DEBUT SAUVEGARDE                *
23/03/15 07:07:17
* ANNUAIRE : TIS EN SERVICE SITE   1   *
```

3 SUBSCRIBER MANAGEMENT

3.1 INTRODUCTION

Subscriber management includes the following actions:

- Directory management
- Subscription and subscriber management
- Creation of hunt groups and multi-company configuration
- Assignment of rights
- Activation of home automation functions
- Selection of subscriber display modes
- Implementation of charging
- Definition of the special features of hotel management
- Configuring terminals 6xxxi deployable by TMA.

These different subscriber management operations can be performed from Menu **TELEPHONY SERVICE>SUBSCRIBERS**.

3.2 DIRECTORY

Note: For a description of the directory and its different components, see the MIVOICE 5000 operating manual: multi-site management.

Each company has its own characteristics: internal and external directories, forbidden number lists, speed dialling, outgoing and incoming trunk groups, call distribution service, and operator group.

The LDAP directory has the following functions:

- Management of subscriber records (internal numbers)
- Alias record management
- Management of contact records (external numbers)
- Assignment of parameters (attributes) used to complete individual records, including:
- Title
- Function
- The person’s hierarchical position
- Personalisation of subscriber and contact records (additional 10 columns).

Note: The creation of subscriber records (internal records) is directly linked to the creation of the subscribers themselves. For more information, refer to “Subscriber creation” in this chapter.

Definitions:

LDAP (Light Weight Directory Access Protocol) is a protocol used to query and modify directory services. This protocol is TCP / IP based. An LDAP directory is based on a tree structure each node of which is made up of attributes associated with their values.

The directory record is the entry point for subscriber management. It concerns either a natural person or an item to be characterised (fax, corridor set, etc.). It comprises a personal record with one or more directory numbers.

To access the directory functions:

Select Menu **TELEPHONY SERVICE>SUBSCRIBER**>Directory.

3.2.1 PARAMETERS

The management portal handles directory configuration: configuring the directory structure, access rights, the topology of the different directories distributed over the infrastructure and the different synchronisations to make.

Note: Servers accessing the directory implement caching mechanisms in order to optimise processing (search by name, forbidden numbers, abbreviated numbers, SDN).

3.2.1.1 *Connections*

Menu **TELEPHONY SERVICE>SUBSCRIBER>Directory>Settings>Connections**

This menu is used to define the location of the directory to be used later. It is also used to define search priorities in existing databases.

All information about directory records is available in the LDAP directory from this screen.

This menu comprises three tabs:

- Configuration - tab used to define the local or remote LDAP database
- Name resolution - tab used to locate the database used by the Easy Admin
- Numbering service - tab used to deploy the numbering server, for processing abbreviated and forbidden numbers as well as DID number resolution.

Note: For information about multi-site management in the real sense of it, see the document Multisite management.

3.2.1.2 *Configuring directory service broadcast*

The directory service is in charge of search by name and number resolution. It is available on each iPBX, but is only unlocked if authorised by the software licence. If it is unlocked on the iPBX, it can be used locally by the site, but also by other sites if its availability is configured. This availability is configured on the site(s) on which it is active, via Menu **SUBSCRIBERS>Directory>Settings>Connections**.

The directory server is activated for the iPBX in question from the **Directory in use** field of the **Name resolution** tab.

The directory service is active if the box is ticked. If the box is not ticked, another service must be defined in Menu **NETWORK AND LINKS>Multi-sites>Localisation of the services**. Refer to the document "Multi-site Management”.

3.2.1.3 *Location of databases*

The location of the following two databases can be configured:

- The "basic directory exp",
- The directory database used by the Easy Admin service.

The configuration of the "basic directory exp" is decorrelated from the directory database used by the directory service.

3.2.1.3.1 "basic directory exp" database location

Configuration tab of Menu **SUBSCRIBERS>Directory>Settings>Connections**

The "basic directory exp" database is an internal or remote LDAP database.

The following services are connected to this database:

- Easy Admin service: directory display and modification
- Number resolution service: used, in particular for:
    - SDN (DID number resolution)
    - - forbidden numbers (based on administrative hierarchy)
    - - abbreviated numbers.
- XML server: call by name on terminals 6xxxi
- Web Admin telephony service: Directory Configuration.

The location of this database must be configured on each of the sites on the multi-site network, from the **Configuration** tab of Menu:

SUBSCRIBERS>Director> Settings>Connections.

The location of the "basic directory exp" database is configured from the following fields:

- Server type: INTERNAL or EXTERNAL

  This parameter indicates the location of the database.

    - On the site hosting the database, the value of this parameter must be INTERNAL.
    - If the database is not internal on the iPBX, the value of this parameter must be EXTERNAL.
- Server name or IP address:

  Name or IP address of the server hosting the “basic directory exp.” database.

  IP address is the actual local IP address. This database is accessible in LDAP or LDAPS depending on whether or not the TLS parameter has been activated.

  > IMPORTANT NOTE: The LDAPS server connection information must be consistent between the certificate content and the Server Name or IP address field:
  >
  > It is recommended that the FQDN be entered as the main connection information and the IP address as additional information.
  >
  > All server certificates must be generated with the Alternative name field containing both the full domain name and the IP address of the server, in order to successfully set up the TLS connection from MiVoice 5000.
- TLS

When the box is checked, the MiVoice 5000 client connects to the remote LDAP database in LDAPS.

To validate the secure remote connection, the client checks the local certificate store to see if the certification chain that verifies the LDAP server certificate is present.

The LDAPS server certification authorities is imported from the **Certification authorities**tab.

- Port

  Port for LDAP connection (389 is the default value for the LDAP protocol or 636 if the access is secure (TLS ticked)).

- Database or URL:

  Connection point on the LDAP tree.

  The default value for this parameter (ou=local,o=AASTRA,dc=DOMAIN,dc=com) corresponds to a configuration without MiVoice 5000 Manager.

- Login

  LDAP database access login.

  The default login (cn=Manager, dc=DOMAIN,dc=com) corresponds to an account created in the LDAP database during installation.

- Password

  Database access password. Leave the default password proposed: it corresponds to the pre-configured iPBX user account in the LDAP database.

  For a remote database (TYPE OF SERVER = EXTERNAL), configure the access parameters:

- Max. number of answers by request

  This field is used to define the maximum number of requests for displaying search by name.

  Possible values are between **50** and **1500** for MiVoice 5000 Server.

- Customisation

  BASED ON MULTISITE **GLOBAL**

  This parameter defines the location in which the directory record customisation **pbxPerso** branch is declared. Refer to the document "Multi-site Management".

WARNING: In R5.2 and R5.3, this parameter should never be set to GLOBAL.

INTERNAL RECORD REGENERATION

Checkbox. Used to directly regenerate directory records in the (external or internal) LDAP server without using the **Load list** ▤ icon located in Menu **SUBSCRIBERS>Subscriptions /Characteristics>General characteristics**.

After ticking the box, to start the action, click **Validation**.

REDUCED DIRECTORY

It is possible to configure in Web Admin an internal directory database for each iPBX (called reduced directory). This database is used by the SDN service, the directory service and XML proxy when the main directory databases are no longer accessible.

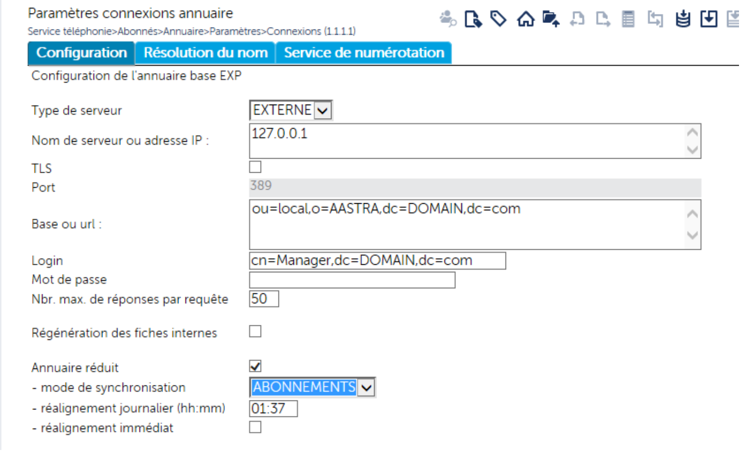
This option is available for all the nodes of a cluster.

This database is synchronised with the main database and contains the directory data corresponding to the site subscribers (local subscribers and backup subscribers).

In Community mode (see Chapter 5) the database contains the directory data of all the Community subscribers.

It is activated from Menu **Telephony service>Subscribers**>**Directory**>**Settings>Connections** – **Configuration** tab.

Note: When the reduced directory database is active, it is only accessible in read only mode. The directory records cannot be modified.



Paramètres connexions annuaire

Service téléphonie>Abonnés>Annuaire>Paramètres>Connexions (1.1.1.1)

Configuration de l'annuaire base EXP

Type de serveur	EXTERNE
Nom de serveur ou adresse IP :	127.0.0.1
TLS	□
Port	389
Base ou url :	ou=local,o=AASTRA,dc=DOMAIN,dc=com
Login	cn=Manager,dc=DOMAIN,dc=com
Mot de passe	
Nbr. max. de réponses par requête	50
Régénération des fiches internes	□
Annuaire réduit	☑
- mode de synchronisation	ABONNEMENTS
- réalignement journalier (hh:mm)	01:37
- réalignement immédiat	□

3.2.1.3.2 Location of the directory database used by the Easy Admin service

Name resolution tab of Menu **SUBSCRIBERS>Directory>Settings>Connections**.

The different sites on which the Easy Admin service is operational (**Directory in use** checkbox ticked) must be configured for access to the network's active database.

This location is configured on the remote databases via the **Configuration** tab of Menu **SUBSCRIBERS>Directory>Settings>Connections**.

The location of the database used by the Easy Admin service is configured from the following fields:

THRESHOLD BEFORE ALARM (IN %)

This field is used to define a threshold before alarm and to display alarm messages when the number of directory records on MiVoice 5000 Server systems is exceeded.

When the threshold is reached, a message is displayed in the logbook to alert the user.

Note: When this limit is exceeded, the call by name and search by name functions name -> number and number -> name are blocked (they stop working).

SEARCH BASE DIRECTORY PRIORITY 0 / 1 / 2

These parameters indicate the location of the databases to be used by the Easy Admin service in the order of priority (0 to 2).

DATABASE FALLBACK EXP

The database used by the Easy Admin service is the management database (defined in the **Configuration** tab).

LDAP

The database used by the Easy Admin service is the LDAP database instance defined by the following parameters.

The description of the parameters used to define an access to a replica of the directory database is the same as the one given above for **Configuration**.

When the server type is LDAP, the operator can configure access to a local database or a remote database.

For a remote LDAP database, access can be secured in LDAPS by ticking the TLS box.

With the TLS box ticked, LDAP access is still available through port 389.

To block this access and use only the secure LDAPS access, go to Menu **SYSTEM>Security>Firewall** and tick **Close port 389**.

- Max number of answers by request

  Field used to define, for each priority 0 to 2 directory database, the maximum number of names proposed during an LDAP request on terminals when users are searching for internal or external names.

3.2.1.3.3 Dialling service

Dialing service tab of Menu **SUBSCRIBERS>Directory>Settings>Connections**.

Ticking the **Service in use** box allows you to define the LDAP database used to resolve problems of abbreviated numbers, forbidden numbers and DID numbers.

This service provides a read access to this LDAP database, possibly secured by a second LDAP database.

By default, the box is ticked (service in use).

The **Broadcast** field contains the following values:

- Internal: the SDN server can only be used for the iPBX concerned.
- Multisite: the server can be used by all the sites on the multi-site network.

If the service cannot be rendered (numbering server not in use or failure upon request prompt):

- The translation of an abbreviated number fails; the call is rejected.
- The list of forbidden numbers cannot be returned; in this case, the external number is authorised by management.

Note: For the specific implementation of this service, refer to the DID number management documentation.

The description of the parameters used to define an access to a replica of the directory database is the same as the one given above for **Configuration**.

When the server type is LDAP, the operator can configure access to a local database or a remote database.

For a remote LDAP database, access can be secured in LDAPS by ticking the TLS box.

3.2.1.4 *Titles*

Menu **TELEPHONY SERVICE>SUBSCRIBER>Directory>Settings>Gender.**

This menu is used to create the gender names which may be used while creating directory records.

3.2.1.5 *Functions*

Menu **TELEPHONY SERVICE>SUBSCRIBER>Directory>Settings>Function**.

This menu is used to create the function names which may be used while creating directory records.

3.2.1.6 *Customisation*

Menu **TELEPHONY SERVICE>SUBSCRIBER>Directory>Settings>Customisation**.

This menu is used to define the additional attributes which will appear in the internal and/or external directory records.

FOR RECORD TYPE

INTERNAL	EXTERNAL

For selecting the type of record to customise.

Select the value then click **Select the item**.

Note: The procedure for defining attributes and configuration fields are the same for the two record types (internal and external).

Up to 10 additional attributes can be defined.

ATTRIBUTE NAME *N*

Attribute name. This name will appear on the records concerned, after the attributes which, by default, are the directory records.

- Type

…..	TELEPHONE	E MAIL	PHOTO

  Attribute type.

Note: The type PHOTO is not operational in this release.

- Comments

  Text field. This comment will appear in the directory database and may be used by some external applications.

- Dialling type

OFFICE	HOME	MOBILE

  Number type for TELEPHONE type attribute.

  The value of this parameter will complete the name display on the terminals.

- Dialable

√

  If the checkbox is ticked, the numbers defined in the field corresponding to this attribute in the records must be directly dialable.

Note: The fields NUMBER TYPE and DIALIABLE are only important for a TELEPHONE type attribute.

- Router mode (Specific SIP URI feature)

  CHECKBOX

  This box is used to activate or deactivate SIP router mode. This mode allows some routing SIP URIs to be entered in external records.

  During a first use or during an upgrade, router mode is deactivated by default.

  This parameter can be modified from any site of a multi-site network, except from a Cluster node.

3.2.1.7 *User accounts*

Menu **TELEPHONY SERVICE>SUBSCRIBERS>Directory>Settings>User accounts** are used to modify the root LDAP and user accounts for the internal database, especially in the absence of an MiVoice 5000 Manager Management Centre.

The modifications are only taken into account if LDAP access is authorised in write mode (condition automatically checked by the system using the interface function with the Easy Admin service).

3.2.1.8 *Root accounts*

By default, the password has the same value as the login indicated.

Authorised characters:

- 24-character password to be entered,
- The characters authorised for the password are "a" to "z", "A" to "Z", "0" to "9" and "_".

Existing passwords are not displayed; they are replaced on display by the characters *, based on the maximum length (24 characters).

3.2.1.9 *User accounts*

These different fields are used to modify the passwords for LDAP user accounts.

The login for the different accounts is not modifiable. The characters authorised for the passwords are:

- 24-character password to be entered,
- The characters authorised for the password are "a" to "z", "A" to "Z", "0" to "9" and "_".

By default, the password has the same value as the login indicated.

The account list is defined in a fixed manner, with the following columns:

Charging application

- Login
- Password

Hotel / hospital application

- Login
- Password

I2052

- Login
- Password

I2070

- Login
- Password

Twp

- Login
- Password

CP

- Login
- Password

MICOLLAB

- Login
- Password

UC360

- Login
- Password

LIFESIZE

- Login
- Password

A340W

- Login
- Password

3.2.2 EXTERNAL RECORDS

External records are used to describe the characteristics of a company's external "contacts".

Five operations are available to manage external directory records: create, edit, delete, view records & view speed dial numbers.

The operations on external records are also available from the Easy Admin Service, Menu **DIRECTORY SERVICE**, of the Web Admin home page.

3.2.2.1 *Creation*

To create an external record, select Menu **SUBSCRIBERS>Directory>External records>Create**.

This screen is used to complete the columns that describe a new external contact.

This information (or administrative attributes) define the identity of the person inside the company.

NAME

Enter the contact's surname.

FIRST NAME

Enter the contact's first name.

GENDER

The drop-down list contains the gender names previously defined in Menu **SUBSCRIBERS>Directory>Settings>Titles**.

Select a value (optional).

VIP

Checkbox. Designates the subscriber's calls as VIP calls. Calls from this subscriber are routed through VIP reception.

CONFIDENTIALITY

This parameter indicates the level of access to the contact directory record:

GREEN LIST	Public access
ORANGE LIST	Limited access inside the company
RED LIST	Access not authorised

Note: In open dialling, the external record must be declared in the Red List.

ABBREVIATED NUMBER

Short number to be dialled, preceded by the access code for the "common abbreviated number" feature, used to call the contact's number (entered in the next field).

The abbreviated number length depends on the number of abbreviated numbers that can be defined on the system. This number is defined in Menu **SUBSCRIBERS>Rights>General settings**. If the number is 1000, for example, the abbreviated number length is 3 digits.

NUMBER

Contact number.

Supported formats are diallable formats (for example 0123456789, 004912345678) and the E.164 format (for example +33123456789, +4912345678).

ENTIRE DIALLING

If the checkbox is ticked, the number indicated in the **Number** field is complete.

Otherwise, it must be completed with a suffix.

Note: This field is only available if an abbreviated number is defined.

NUMBER OF DIGITS TO BE ADDED

For indicating the number of digits to dial after the short number.

Note: This field is only available if the preceding number is not complete (box not ticked).

HIERARCHY

For restricting access rights to the external number from the abbreviated number. Only the subscribers belonging to the selected administrative hierarchy will have access to the abbreviated number.

The drop-down list contains all the administrative hierarchies previously defined on the system via the menu **SUBSCRIBERS>Directory>Administrative hierarchies**.

WARNING: This solution is used to bypass the subscriber's rights (a subscriber without the right to international numbers may call an international number via an abbreviated number).

E-MAIL

For indicating the e-mail address of the external contact.

SIP URI AND ROUTING SIP URI

These fields are used to enter an SIP URI and, possibly, a routing SIP URI in external records.

SIP URIs are limited to 120 characters.

Routing SIP URI is hidden if router mode is not activated in Menu **Subscribers>Directory>Settings>Customisation**.

SIP_URIs must contain only one character "@"; unauthorised characters are "()<>,;:"[]\", and they must end with a "character "." followed by at least two characters.

LOCATION

For giving information, for instance, about the contact's company (name, address, etc.).

The additional fields which may appear on the external record correspond to the attributes previously defined via the menu **SUBSCRIBERS>Directory>Settings>Customisation**.

After entering the parameters, click "Confirmation” to validate the external record creation.

3.2.2.2 *Modification*

To modify an external record, select the menu **SUBSCRIBERS>Directory>External records>Modification**. The screen below is used to select the record to be modified according to several criteria:

The four fields on this screen are used to limit the list of external records proposed for modification.

NAME BEGINS WITH

Beginning of the contact's surname.

FIRST NAME BEGINS WITH

Beginning of the contact's first name.

NUMBER BEGINS WITH

Beginning of the contact's number.

ABBREVIATED NUMBER BEGINGS WITH

Beginning of the abbreviated number associated with the contact.

After entering the selection criteria, click **Select the item**:

Note: If the selection criteria have not enabled a single record to be selected, the << and >> scroll arrows can be used to access the other records.

This screen is used to change one or more parameters associated with an external record.

The description of the fields is the same as the one given for creating an external record (see Section *3.2.2.1*).

All the fields can be modified, including the name of the person.

3.2.2.3 *Delete*

To delete an external record, click **SUBSCRIBERS>Directory>External records>Delete**. The screen below is used to select the record to delete based on several criteria:

The four fields on this screen are used to limit the list of external records proposed for deletion.

NAME BEGINS WITH

Beginning of the contact's surname.

FIRST NAME BEGINS WITH

Beginning of the contact's first name.

NUMBER BEGINS WITH

Beginning of the contact's number.

ABBREVIATED NUMBER BEGINGS WITH

Beginning of the abbreviated number associated with the contact.

After entering the selection criteria, click **Select the item**:

Note: If the selection criteria have not enabled a single record to be selected, the << and >> scroll arrows can be used to access the other records.

On this screen, all the parameters associated with the external record are displayed and greyed out. No input is possible.

To delete a record, click **Confirmation**.

3.2.2.4 *Display records*

Menu **SUBSCRIBERS>Directory>External records>Display**.

This screen is used to define the criteria for selecting the external records to be displayed.

If the fields are completed, the different criteria are entered to define the selection. For example, only the records in which the surname starts with a D, the first name with J and the abbreviated number with 4 may be displayed.

Click **Select the item** to confirm the operation.

Note: Only record display is authorised at this stage.

3.2.3 ALIAS RECORDS

Alias records are internal records of persons without a subscription but who share a terminal with a subscriber.

MiVoice 5000 Web Admin is used to create, modify, delete alias records and view existing alias records using certain filter criteria.

3.2.3.1 *Creating an alias record*

To create an alias record, select the menu **SUBSCRIBERS>Directory>Alias forms>Create**.

This screen is used to describe an alias.

The parameters which will be used by telephony are the last name, first name and number of the main subscriber. The other parameters are for information only.

GENDER

For associating a civil status with the person.

The drop-down list contains the genders declared via the menu **SUBSCRIBERS>Directory>Settings>Genders**.

NAME

Alias name. This name is used for search by name.

FIRST NAME

Alias name. This first name will be used in addition to the last name for search by name.

FUNCTION

For assigning a function with the person.

The drop-down list contains the functions declared via Menu **SUBSCRIBERS>Directory>Settings>Functions**.

E-MAIL

For indicating the person’s e-mail address.

LOCATION

For defining the geographic location of the person in the company.

MAIN SUBSCRIBER NUMBER

Indicates the directory number of the subscription with which the alias shares the terminal.

After entering the parameters, click "Confirmation” to confirm the creation of the alias record.

3.2.3.2 *Modifying an alias record*

To modify an alias record, select the menu **SUBSCRIBERS>Directory>alias forms>Modify**.

The three fields on this screen are used to limit the list of alias records proposed for modification.

NAME BEGINS WITH

Start of the alias last name.

FIRST NAME BEGINS WITH

Start of the alias first name.

NUMBER BEGINS WITH

Start of the number of the main subscriber with which the alias is associated.

After entering the selection criteria, click **Select the item**.

Note: If the selection criteria have not enabled a single record to be selected, the << and >> scroll arrows can be used to access the other records.

The TITLE, LAST NAME, FIRST NAME, FUNCTION, E-MAIL, LOCATION and MAIN SUBSCRIBER NUMBER parameters are those detailed in the previous section (Creating an alias record).

HIERARCHY

The administrative hierarchy of the main subscriber was selected by default while creating the alias record. You can assign another administrative hierarchy to the alias, but this information will not be used.

The drop-down list contains all the administrative hierarchies existing on the system.

LABEL/MAIN SUBSCRIBER LAST NAME

Read only field indicating the last name of the main subscriber.

MAIN SUBSCRIBER FIRST NAME

Read only field indicating the first name of the main subscriber if this has been declared in its internal record.

After modifying the parameters, click "Confirmation” to validate the modification of the alias record.

3.2.3.3 *Deleting an alias record*

To delete an alias record, select the menu **SUBSCRIBERS>Directory>alias forms>Delete**.

The three fields in this screen are used to limit the list of alias records proposed for deletion.

NAME BEGINS WITH

Start of the alias last name.

FIRST NAME BEGINS WITH

Start of the alias first name.

NUMBER BEGINS WITH

Start of the number of the main subscriber with which the alias is associated.

After entering the selection criteria, click **Select the item**.

Note: If the selection criteria have not enabled a single record to be selected, the << and >> scroll arrows can be used to access the other records.

All the parameters in this screen are read only.

To delete a record, click “Confirmation”.

3.2.3.4 *Displaying alias records*

To display alias records, select the menu **SUBSCRIBERS>Directory>Alias forms>Display**.

This screen is used to define the criteria for selecting the alias records to be displayed.

NAME BEGINS WITH

Start of the last name of the aliases to be displayed.

FIRST NAME BEGINS WITH

Start of the first name of the aliases to be displayed.

NUMBER BEGINS WITH

Start of the main subscriber number with which the aliases to be displayed are associated.

After entering the selection criteria, click **Select the item**.

In this example, only the alias records of subscriber 3004 have been requested.

3.2.4 ADMINISTRATIVE HIERARCHIES

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 defined in Menu **SUBSCRIBERS>Subscriptions>Characteristics>Directory information**.

In the external record of a contact with an abbreviated number, the administrative hierarchy refers to the subset of subscribers with access to this contact's abbreviated number. It is defined in Menu **SUBSCRIBERS>Directory>External records>Create** (and **Modification**).

This command is used to describe the administrative hierarchy tree of the iPBX directory, thanks to a graphical tool.

To access this command, select Menu **SUBSCRIBERS>Directory>Administrative hierarchies**.

This screen describes the administrative hierarchy tree.

Icons:

First level node icon.

Second level node icon.

Terminal node icon.

Tree and actions display:

Clicking an item selects this item.

The keypad "up" and "down" arrows are used to move the selection.

Clicking a **+** or **-** icon in front of a node reduces or expands this node. The "left" and "right" arrow keys have the same effect on the selected node.

The "*****" key on the numeric keypad develops all the child nodes of the selected node.

Double-clicking an item or pressing the "**F2**" key when an item is selected changes to edit mode for its label.

In node label edit mode, pressing the "**Enter**" key validates the modification, while pressing the "**Esc**" key cancels the last action taken since the last entry in edit mode.

Buttons:

New	If a node is selected, this button inserts a child node under this node. If no node is selected, it inserts the child node of the first node. In both cases, the insertion is made following the last existing child node.
Delete	Deletes the selected node as well as its descendant.
Save	Saves the tree in the iPBX data.

WARNING: all the changes made since this button was last used (or since entry in the graphic tool) are local and will be lost if they are not backed up).

This button is only active if some modifications have not yet been backed up.

Cancel Cancels all the modifications made since the last backup operation (or since entry in the graphic tool if no backup has been made).
This button is only active if some modifications have not yet been backed up.

⟳ Refreshes the display with the information backed up.

BARRED NUMBERS LIST

For associating a list of forbidden numbers with an administrative hierarchy level. When a list is associated with a hierarchy level, it is associated with all the subscribers attached at this level or any lower level.

The drop-down list contains the names of the declared forbidden numbers lists (the declaration and definition of the forbidden numbers lists is done in the dialling plan.

Note: This parameter appears at the bottom of the screen once a hierarchy level has been selected.

3.2.5 DISPLAYS

3.2.5.1 *External records*

This command is the same as the one described in Section 3.2.2.4.

3.2.5.2 *Speed dial (or abbreviated) numbers*

This screen is accessible from the menu **SUBSCRIBERS>Directory>Displays>Common abbreviated dialling**.

Enter the beginning of the numbers to display (or leave blank to obtain the entire list, then click **Select the item**.

The display then gives all the external records with an abbreviated number.

Only abbreviated number display is authorised at this stage.

It is, of course, possible to limit the display by filling in the field “Abbreviated number beginning with”.

3.3 MANAGING SUBSCRIBERS

Menu **SUBSCRIBERS>Subscriptions**.

This menu includes 9 functions used to:

- Create subscriptions
- Display subscribers from their internal number
- Define (display / modify) subscription characteristics.
- Assign set authentication keys
- Copy a subscriber's characteristics
- Copy keys
- Dial numbers
- Assign terminals automatically
- Delete subscriptions.

Note: In the user interface, just like in this document, the terms Subscriber and User are interchangeable because they have the same meaning.

3.3.1 CREATING SUBSCRIPTIONS

In most cases, for a subscriber, a subscription is defined to which a physical set (or telephone set) is assigned.

It is nevertheless possible to define a subscription, regardless of individual assignment to a set. This assignment may be done in a second phase.

As a rule, assignment consists in defining a subscription/equipment pair. In this case, it is all about a simple subscription. It is also possible to associate several terminals with the same subscription, for example an analogue terminal and a DECT terminal; for this, the subscription must have the property **Authorized association of set** (see General characteristics of a subscription in Section *3.3.3.1*).

Note: Strating from 8.2 SP3, the Do not disturb allowed setting is activated by default for new users. Refer to paragraph 3.3.3.1 – General characteristics

Select the menu **SUBSCRIBERS>Subscriptions**.

Creation of a new subscription requires knowing at least the type of subscriber to define and a directory number available for this subscription.

SUBSCRIBER TYPE

Subscriber type is the first parameter to select. The choice of subscriber type determines the next operations to perform.

Select any of the following subscriber types:

INTERNAL

Internal subscriber. The LOCAL type is proposed by default. Most subscribers are associated with this type of subscription which allows the assignment of a wide range of terminals.

HUNT GROUP

Subscription used to group a set of subscribers who can all be called by the hunt group's call number.

(SUPER) GROUP

Subscription used to group a set of HUNT GROUP type subscribers or associated with a multi-key set.

The number of SUPER GROUP type subscriptions is limited to 8 per iPBX.

MULTIUSER

Subscription sharing the same set as another subscription.

ATDC

Attendant console subscriber. Has special functions (see the chapter "Call distribution”).

AUTOMATED ATTENDANT

An automated attendant (IVS) routes incoming calls to call distribution stations (voice mail box, operator console, predefined numbers, etc). The extension is activated as soon as it is created.

DISA

Server used to set up calls and program features from an external set (not connected to the system)

V MAIL GROUP

For declaring voice mail groups outside the voice mail box and the groups associated with the voice mail box

INTEGRATED V MAIL

Server dedicated to the company’s messaging system

NORMAL MODE CO NF

Teleconference function. Service called from a specific number (see note at the end of the table).

COMMON MODE CO NF

Standard teleconference. Service called from a predefined prefix in the dialling plan (see note at the end of the table)

SYSTEM MODE CON F

Teleconference with reinforced surveillance. For setting up a conference between subscribers belonging to a predefined list (see note at the end of the table).

TELECONFERENCE

Teleconference managed by a conference master who determines the subscribers authorised to participate in the conference (see note at the end of the table).

FIRST DIRECTORY NUMBER

Enter on this line the new subscriber’s number. It must be a number not assigned to another subscriber in the directory.

NUMBER OF SUBSCRIBERS REQUIRED

Enter the number of subscribers to create. By default, the number is set to 1. If the number of subscribers required is above 1, the system automatically creates a series of subscribers from the first directory number indicated. For example:

- First directory number indicated: 6000
- Required number 10
- Subscribers created: 6000 to 6009.

Note: This column is used to create a large number of subscribers while creating the company network.

USER PASSWORD

For more information about user password management, see the USER PASSWORD field in the characteristics tab of Menu SUBSCRIBERS>Subscriptions >Characteristics, in Section .3.3.3.1

The user password displayed is the default password of the PBX. It will be assigned to all the subscribers to be created.

If the proposed "user password" is modified, this new password becomes the default password of the PBX after the subscriptions are created.

After this user password is modified, click Confirmation**.**

The "User password" line is only displayed for the following types of subscriptions: LOCAL, MULTIUSER, ATDC, DISA, AUTOMATIC ATDC.

VERIFY UNIQUE NUMBER IN MULTISITE

When a subscriber is being created, the system checks whether the subscriber exists already in another site, for a multi-site configuration.

If the box is checked, this control is enabled (timeout of about two seconds if control is enabled).

AUTOMATIC CREATION OF DID NUMBER

If the box is checked, a DID (Direct Inward Dialling) number is created which is the same as the internal directory number and prevents creation later in the menu: “Extension characteristics”.

Note: DID is a system which allows direct access from the outside to a subscriber's set without going through the switchboard.

AUTOMATIC CREATION MOBILELINK FUNCTION

If the box is ticked, two keys are programmed in the following order for each subscription (local type) created:

- Key 1 Supervision of main line (CCO). The label assigned to the key is initialised with the subscription number.
- Key 2 MobileLink. The key label is initialised with the MobileLink string only for 6900 SIP phones.

CONFIRMATION

Clicking "Confirmation" validates the content of the screen.

3.3.2 DELETING SUBSCRIPTIONS

Select the menu **SUBSCRIBERS>Subscriptions>Delete**.

SUBSCRIBER TYPE

The list of subscriber types is the same as the one proposed for creation (see Section *3.3.1*).

FIRST DIRECTORY NUMBER

Directory number of the first subscriber to be deleted.

LAST DIRECTORY NUMBER

Directory number of the last subscriber to be deleted For deleting several subscriptions with successive numbers.

Note: If certain numbers between the FIRST and LAST do not belong to the type of subscriber selected, subscriber deletion does not take place. An error message is displayed.

DELETE DIRECTORY RECORDS

If the box is checked, the directory records associated with the subscribers will be deleted from the directory. This action updates the system directory or the multi-site configuration at the same time.

DELETE INTEGRATED VOICE MAILBOX

If the box is checked, the voice mailboxes of the subscribers are deleted.

Otherwise, the messages are kept until the next message deletion audit and will only be accessible if the subscription is created again.

Note: In normal operation mode, check the integrated voice mailbox deletion box.

Click "**Confirmation**" to validate the operation.

DELETE BLUSTAR FILES

If the box is ticked, no matter the origin of the request (including from MiVoice 5000 Manager), the configuration files <N°>_local.cfg and <N°>.cfg associated with the subscribers in question are deleted.

3.3.3 SUBSCRIBER CHARACTERISTICS

Menu **SUBSCRIBERS>Subscriptions> Characteristics**.

This menu proposes different functions used to define the main characteristics of an extension (or subscriber).

IMPORTANT NOTE: For a local subscriber, their subscription is completed when the following items have been defined: directory record, subscriber type, terminal type, characteristics, set model.

Certain functions, such as "General characteristics, are used to individually complete the main parameters associated with a subscription. They are also used to modify or duplicate these characteristics.

3.3.3.1 *General characteristics*

Menu **SUBSCRIBERS>Subscriptions /Characteristics>General characteristics.**

Once the directory number has been entered, click **Select the item**. The "**General characteristics**" screen is used to define all the parameters of a given subscriber.

Note: The number of parameters available in "General characteristics" depends on the type of subscriber declared previously.
For the COMMON MODE CONF or INTEGRATED V MAIL types, there are fewer parameters to enter than for LOCAL, for example.
For the BACKUP type, these are information fields, the configuration of the subscription only being authorised on the reference site.
The number of parameters to enter is limited if feature management is done via feature classes (see the FEATURE CLASS MANAGEMENT parameter in SUBSCRIBERS>Rights>General settings).

SUBSCR. STATUS

IN SERVICE **OUT OF SERV.**

For enabling and disabling the subscriber. To remove a subscriber's card from the system (associated with a fixed TDM set), first disable the sets attached to this card.

When the subscriber has a call set up, "IN COM" is displayed next to the status

Note: If the subscriber is BACKUP type, the SUBSCR. STATUS label is completed by the subscription activation status:
- INACTIVE means that call processing is carried out on the reference subscription site (normal operating state),
- ACTIVE means that the reference subscription site is not accessible and that call processing is carried out on the backup site.
For a detailed description of the Dual Homing feature, see the MIVOICE 5000 operating manual: multi-site management.

DIRECTORY NUMBER

Recalls the subscriber's number in the directory.

Place > In DID management mode by SDN, (specific mode), refer to the document DID Mode Management.

DID DIRECOTRY NUMBER PLAN 1

This field is repeated for each declared plan (8 plans maximum).

It is used for ISDN DID systems: give the MCDU (last 4 digits of the DN) which will reach the set directory number (DID --> set).

EXTENSION NAME

The extension name is made up of 12 alphanumeric characters (for forwarding, the name of the digital Attendant Console or the M7855 Attendant Console is limited to 6 characters).

The name is saved in the LDAP database. It can be used during a call by name.

COMPANY

Name of the company to which the subscriber is attached. The drop-down list contains the names of the companies declared on the system (the companies are declared via the menu **SUBBSCRIBERS>Hunt groups and companies>Multi-company management>Company names**).

Note: This field is only displayed in multi-company configuration.

DEPARTMENT

Name of the department to which the subscriber is attached. The drop-down list contains the names of the departments declared on the system for the selected company (the departments are declared via the menu **SUBBSCRIBERS>Hunt groups and companies>Multi-company management>Department names**).

Note: This field is only displayed in multi-company configuration.

ROOM SET DIRECTORY

Number of the main subscription with which the subscription shares the set.

Note: This field is only displayed for a MULTIUSER type subscription.

INTEGRATED VOICE BOX (IVB)

If the box is ticked, it allows a voice mail box to be assigned to the subscriber.

Not ticking the box results in deletion of the voice mail box, that is, all the messages that it contains, the voice signature, the customised message and the password.

- Class name

  This line is displayed only if the previous box has been ticked. It is used to assign a class to the voice mail box. When a box is created, class 0 (IVB 0) is automatically assigned to the subscriber. The class can be changed later, provided a name had been previously assigned to this class (it is possible to create 10 classes, menu "Name of box classes").

SET AUTHENTICATION KEYS

ABSENT **PRESENT**

Note: Applicable to SIP terminals only.

Information field indicating whether a password is defined for the authentication during recording or during call set up. This authentication is not related to registration, but it may be required any time by the system. The function used to associate an authentication password with the subscription can be accessed via **SUBSCRIBERS>Subscription>Set authentication keys**.

BACKUP SITE

This parameter is only present in a multi-site configuration and for a LOCAL type subscriber.

It allows the subscription to take advantage of the Dual Homing (secure subscription) feature by assigning it a backup site.

Note: The Dual Homing feature is available as of software release R5.1B.

……….	The subscription is not secured.
Site Name	The subscription is secured on the site indicated.

The drop-down list contains all the sites of a multi-site configuration with software release ≥ R5000.1. It should be ensured that the selected backup site is using software ≥ R5.1B.

Note: For a detailed description of the Dual Homing feature, see the MIVOICE 5000 operating manual: multi-site management.

REFERENCE SITE

This parameter is only present in a multi-site configuration and for a BACKUP type subscriber.

It indicates the reference site of the subscription.

Note: For a detailed description of the Dual Homing feature, see the MIVOICE 5000 operating manual: multi-site management.

MULTIUSERS: DEFINED 0, AUTHORIZED

0 = number of multi-users defined already.

To return to 0, firstly erase the multi-user declared. This line is only proposed for analogue or digital sets.

The authorised value cannot be different from 0 if the set features a DID directory number different from its internal directory number.

USER PASSWORD

GENERAL INFORMATION

This 4-digit password is the same for the subscription and for the integrated voicemail.

It can be modified by the user, unlike the previous versions in which it could only be reset.

The types of subscriptions concerned are:

- LOCAL (and multi-line with a unique password)
- MULTIUSER
- ATDC
- DISA (Direct Inward System Access)
- AUTOMATED ATTENDANT

The default user password for the subscription is 0000.

DESCRIPTION OF THE USER PASSWORD FIELD

The value is displayed unencrypted when the password is entered, and then replaced with eight "*" when the field is validated (by pressing the return key or clicking outside the field).

When the user cancels the field (by deleting the "********"), the password is automatically reassigned its default value (value displayed in Menu **Subscribers>Subscriptions>Create**) when the field is validated, and the "********" are displayed.

For multi-line subscriptions, the password can only be modified from the main subscription (which is automatically copied to all the secondary subscriptions). For an ATDC subscription, the password field only appears when the subscription is declared as a multi-line subscription (because the password only applies to the secondary numbers).

For DISA subscriptions, the password remains displayed unencrypted after this latter is validated.

USER PORTAL ACCOUNT

Checkbox

If the option is ticked, the operator allows the subscriber access to the User Portal using a password defined on the next line.

MiVoice 5000 User Portal is a Mitel 5000-integrated application that enables the subscriber to manage their telephone terminal themselves, such as programming their keys or their forwarding.

The User Portal service must be activated (see Menu **Subscribers>Rights>General settings**, **Application** tab).

The User Portal is accessible via a web browser, at this address: https://@iPbx:4446/userportal

- User Portal password

  This field is only visible if the User Portal ACCOUNT option is selected.

  The password input policy is defined in Menu **Subscribers>Rights>General settings**, **Application** tab.

  Creating or modifying the User Portal password sends an automatic e-mail to the subscriber concerned if this option is activated. See Menu **System> Configuration>E.mail**, **User Portal password** tab.

AUTHORIZED ASSOCIATION OF SET

Terminal association is only possible with INTERNAL EXT. ISDN and i2052 VOIP terminals cannot be hosted on a subscription with this characteristic.

Generally, terminal association is not possible on a subscription that does not accept physical terminals (for example, "server", conference subscriptions, etc.).

Note: ISDN and i2052 VOIP terminals cannot be associated with a subscription although they use an INTERNAL EXT subscription.

ENABLED INTERNAL SETS

Checkbox

This parameter is activated by default.

It is useful only if associated with several terminals. The notion of internal terminal represents all the terminals of the subscription inside the company's telephone network.

In contrast, the notion of external terminal represents the terminals defined as EXTERNAL TERMINAL and cannot be reached via the company's network. See the TERMINALS tab.

Parameter activated: All the "internal" terminals receive calls.

Parameter deactivated: No internal terminal receives any call; only external terminals receive calls.

The terminals have typical function information, either in form of a message or an icon: for example INCOMING CALLS DEACTIVATED on a 39i.

WARNING: The operator can deactivate internal and external calls; in this case, the subscription no longer receives any call.

ENABLED EXTERNAL SETS

The same as above but in this case, for external terminals.

On the other hand, external terminals do not have the information if they cannot receive the subscription's calls.

RIGHT TO CLASS SERVICE

This column is only available on analogue sets. CLASS service allows analogue sets to receive the following information about the current call:

- Caller number (if there is no call offering restriction)
- Time and date of the call (only available in V23 mode).

IMPORTANT NOTE: This column only appears for analogue terminals.

SERVICE BEARER

SPEECH	DATA WITHDRAWAL SPEECH	DATA

Indicate to the PBX the type of service used for this set (depends on information type).

DTMF IN BAND

This box, when checked, allows you to specify that DTMF will be sent in-band and not according to RFC 2833 in RTP packets.

This feature only applies to analogue terminals although the typing is at the subscription level.

DAY CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

Select the category assigned to the user.

The authorisations, limitations and prohibitions associated with each category are defined in the menu: Category management.

NIGHT CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

The difference between DAY and NIGHT is the switchover from day to night and vice-versa, which is carried out by the barring calendar (menu : Barring Calendar), in single-company configuration, or in menu : Company/department parameters in multi-company configuration.

ROLE OF MICOLLAB

This options field is displayed when the MiCollab server synchronisation parameters have been defined in Menu **Telephony service>Subscribers>Terminals and applications>MiCollab**. See also Section 3.5.7.

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).

Note: If the Windows login parameter for authentication in Menu Telephony service>Subscribers>Terminals and applications>MiCollab is not ticked and no entry has been made in the user login field in Menu SUBSCRIBERS>Subscription>Characteristics>Directory, the options list remains empty.

MICOLLAB SYNCHRONISATION BUTTON FOR THIS USER

The button is visible if the subscriber has a MiCollab role. Allows for forced synchronisation of the subscriber's MiCollab data.

CLOUDLINK ROLE

Refer to the document **CloudLink - Integration with MiVoice 5000** on the Mitel website.

FORBIDDEN NUMBERS LIST

Used to assign to the subscription a list of numbers that it cannot access. This list can also be configured on a hierarchical/administrative basis via the directory.

Note: The restrictions on the list of forbidden numbers will only be taken into account if the FORBIDDEN NUMBERS LIST RESTRICTION parameter in the category associated with the subscription is checked.

The drop-down list contains the names of the forbidden numbers lists declared via Menu **DIALING PLAN>Forbidden numbers>Forbidden numbers lists names**.

HOT LINE TYPE

…….. **IMMEDIATE** **DELAYED**

For defining the behaviour of the line, for the subscription, when the handset is picked up. This behaviour does not apply to all sets (ISDN, SIP, and H323).

A hotline call can be made in two ways:

IMMEDIATE: An internal or external number is dialled immediately and automatically on off-hooking.

DELAYED: An internal or external number is dialled automatically 5 seconds after off-hooking. This value may be modified from Menu **SYSTEM>Expert>Time-out management**.

- DAY/NIGHT NUMBER

These two fields are only displayed if the "hotline type” has been selected, either “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.
The NIGHT number is used when the system is in night service (calendar applicable).**

Restriction: Only the **day number** will be taken into account for EX GX and TA systems.

INTERCOM 1 GROUP/INTERCOM 2 GROUP

Automatic assignment of GICs by company is configurable and also applies to SIP extensions but not to MiVoice 5000 Server or to Multisite.

Automatic assignment of GICs by company does not apply to the call server or to multi-site and is - I believe - configurable.

INTERCOM groups 0 to 31: supervision and interception by keystroke alone on the digital extension.

INTERCOM groups 32 to 252: same as for 0 to 31 plus interception via the *01 facility. These groups are reserved for subscriber groups: they allow you to intercept a call on behalf of the group.

INTERCOM Group 253 and above (up to 2000): Intercom group with reduced functionality to intercept but not call. Subscriptions belonging to this group can monitor users from any other group. They are not supervised themselves. Applies to Group 253 only.

Subscriptions in the same INTERCOM X group can supervise and be supervised.

PAGING GROUP NUMBER 1

You can assign sets to one or two paging zones so that people can page different parts of the office without disturbing the whole office.

1st case: if the user paging group numbers (called and calling parties) are identical (from 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: if 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.

PAGING GROUP NUMBER 2

See paging group number 1.

OUTGOING PARTITION CLASS

This parameter is only available if partition class management is enabled in Menu **SUBSCRIBERS>Rights>General settings**.

The drop-down list contains the partition classes defined in the system.

INCOMING PARTITION CLASS

This parameter is only available if partition class management is enabled in Menu **SUBSCRIBERS>Rights>General settings**.

The drop-down list contains the partition classes defined in the system.

PRIORITY CLASS

This parameter is only available if partition class management is enabled in Menu **SUBSCRIBERS>Rights>General settings**.

The drop-down list contains the priority classes defined in the system.

ACCESS TO TL ROUTES X

Ticking this box validates access to TL (tie line) directions.

If you want to define a new private direction, first you must create a direction name (menu: **Direction name**) then define this direction (menu: **Access to directions**): a new field, **Access to TL routes "x"**, then appears for the desired area.

Note: Tie-line trunks are not implemented. Consequently, some private directions can be specially configured at the factory for a client (one or more lines then appear on screen).

For example, these 2 lines are displayed:
LINE "ACCESS TO DIRECTION PRIVATEL"

For accessing the PRIVATEL direction. See the screen DIALLING PLAN>User dialling plan>Access to directions.
LINE "ACCESS TO DIRECTION VNC"

For accessing the VNC direction. See the screen DIALLING PLAN>User dialling plan>Access to directions.

Management of up to 64 different tie-line directions, grouped into 8 access zones (geographic or other) by the operator. Access right is, therefore, zone based.

AREA ACCESS A (YES/NO), AREA ACCESS B (YES/NO)

There are as many lines as there are areas defined by the operator.

ACCESS TO PAGING

If this box is ticked, the subscriber has access to three paging types (see descriptions of the paging function in the menu **Direction name** menu and in the menu **Access to directions**).

PRIVILEGED SET

If this box is ticked, the user may call the operator in a privileged manner. It only works with the integrated attendant console.

PICK UP PROTECTION OVERRIDE PICK-UP

If this box is ticked, the user can intercept all calls to all other sets, including calls to sets with a pick up protection feature.

LOCKING ALLOWED

If this box is ticked, the user has the right to 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

If this box is ticked, the user has the right to unlock his set by entering his secret code.

Otherwise, the set remains locked.

USER MOBILE RECORDING

If this box is ticked, the subscriber's mobile (DECT) number may be registered.

PICK UP PROTECTION

If the box is ticked, the set is protected against any pick up, including pick up using a key programmed for the intercom function. Pick-up only applies to users authorised by the parameter: “pick-up protection override".

NIGHT CATEGORY OVERRIDE

If the box is ticked, the user may override their night category using their secret code: for this call, the terminal is switched to day category (secret code = password).

The secret code is not required when in the dialling plan, the direction type is “password require=no”.

CALL FORWARDING PROTECTION

If this box is ticked, the extension is protected against all types of forwarding.

DATA PROTECTION

If the box is ticked, the user can protect himself throughout a conversation from a busy override or from call waiting (protection activated by feature code).

DO NOT DISTURB ALLOWED

If this box is ticked, the user is entitled to use the Do Not Disturb feature (MUTE message on digital sets).

INTRUSION ALLOWED

If the box is ticked, the user can execute a busy override procedure (OFFER) on another set in the busy status 1 (the other set must not have a call waiting).

The aspect of voice mail and charging of busy sets 1 & 2 is handled in the chapters “Network and Links”, section “Trunk characteristics”.

INTRUSION ACCEPTED

If the box is ticked, the set is protected against any busy override (OFFER) but waiting calls are indicated.

LISTENING/INTERVENTION ALLOWED

If the box is ticked, the user can intervene to listen to a call in progress (discrete listening or intervention).

Note: A system parameter is used to authorise the intervention service. The service is only accessible to sets with interactive keys.

LISTENING/INTERVENTION ACCEPTED

If the box is ticked, the user's calls may be listened to.

ENCRYPTION AUTHORISED

If this box is ticked, call encryption will be applied to this user.

MASTER OF CONFERENCE

If this box is ticked, the user may initiate a teleconference (by calling a conference directory number).

Note: The teleconference function is only available for a multi-site configuration with a CCB card.

LOG IN VIA PC ONLY

If the box is ticked, the user may use the login/logout functions on a terminal 6xxxi from a PC application (User Portal or external application).

PRE-EMPTIVE REROUTING TO VOICE MAIL

If the box is ticked, it is used to specify which voicemail to route the call to if the called set and the forwarding set have voicemail boxes.

USE OF DISA FUNCTION

If the box is ticked, calls can be set up and certain features programmed from an external telephone set.

CALL WAITING

Indicates how an “incoming” call is processed when the user is busy.

ACCEPT AND BEEP Normal procedure: the call is placed on hold, and the user is advised.

FORWARD->ON CONSOLE The call is put on hold but forwarded immediately to the ATDC

REFUSED The calling party receives the 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 this box is ticked, the time-out for return to the ATDC on no answer, free or busy set, is changed from the standard value to a special value (see the “Time-out management” screen).

EXTERNAL FORWARDING ALLOWED

If the box is ticked, internal calls can be transferred to an external number.

Forwarding of an external call to another external number is subject to other rights.

Note: In the “Subscribers miscellaneous parameters" screen, tick the box for the parameter “Allow Tk – TK transfers”.
In the Rights>Subscribers miscellaneous settings: Menu "Change other settings", set parameter 282 to 2: forwarding allowed without reading the table of network line forwarding rights and parameter 177 to 1: ISDN-DBX transit allowed (with system reload).

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

If the box is ticked, the user can make a speaker paging call to terminals belonging to any of the paging lists (for digital TDM terminals and terminals 6xxxi equipped with loudspeakers).

NETWORK SHIFT ALLOWED

If the box is ticked, an attempt is made to route the call to “other network” if direct routing and re-routing attempts fail.

NETWORK REROUTING ALLOWED

If the box is ticked, an attempt is made to reroute the call if direct routing attempts fail.

ID SENT PUBLIC NETWORK

AID **IID** **……..**

Used to indicate which number the user wishes to identify himself with to the external correspondent during an outgoing call to the public network.

AID: his own number: AID: the general call number of the system.

ID SENT PRIVATE NETWORK

AID **IID** **……..**

Used to indicate which number the user wishes to identify himself with to the external correspondent during an outgoing call to a private network (for example, tie-line).

AID: his own number: AID: the general call number of the system.

ID SENT CAN BE MODIF. FOR EACH CALL

NO **YES**

If you enter YES, this line enables the user to send either their DID (AID) number or the general number of the system (IID) or nothing to a correspondent, when making outgoing calls from their extension (OPTION interactive key after the prefix or as of R6.2 by prefix before the external number) provided that, in menu “Miscellaneous settings”, NON IDENTIFICATION AUTHORIZED is set to YES.

Note: If the user does not use the OPTION key, the value defined in the previous lines is sent.

PRIORITY SET

If the box is ticked, reserved line seizure is allowed (see the **Trunk group characteristics** menu).

Note: See Appendix for information about these terminals' power-saving function.

RIGHT TO IMMEDIATE FORWARDING

If the box is ticked, immediate forwarding is allowed for any call.

FORWARDING ON BUSY ALLOWED

If the box is ticked, the user is allowed to forward calls if the line is busy.

FORWARDING ON NO ANSWER ALLOWED

If the box is ticked, the user is allowed to forward calls if he is absent.

RING DURATION BEFORE FORWARD

STANDARD **SPECIFIC_1** **SPECIFIC_2** **SPECIFIC_3**

Selection of 4 possible delayed forwarding ring timeouts programmed for a standard configuration duration of 15 seconds (see **Time-out management** menu).

RECORDED CALLS ALLOWED

If the box is ticked, the user is allowed to save the last number dialled.

AUTOMATIC CALLBACK ALLOWED

If the box is ticked, the user may access the “AUTOMATIC CALLBACK” function through the “CALLBACK” function of digital sets or via the “Access to features” screen (Automatic callback activation).

APPOINTMENT REMINDER ALLOWED

If the box is ticked, the user can access the "WAKE-UP” function.

Each user has 4 appointment reminders unless it is a “hotel room set type”, in which case he has just one appointment reminder.

COMMON ABBREV. NUMBERS ALLOWED

If the box is ticked, the user is entitled to use the general abbreviated dialling feature ("DIRECTORY" function on digital sets).

PERSONAL ABBREV. NUMBERS ALLOWED

If the box is ticked, the user is entitled to use his own abbreviated numbers list.

PERSONAL CALLS ALLOWED

If the box is ticked, personal calls are allowed.

TRANSFER BEFORE ANSWER ALLOWED

If the box is ticked, the user is entitled to transfer calls before the called party answers.

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

If the box is ticked, the user can belong to a hunt group.

FEATURES A MANAGER LINE

Checkbox

- LOCATED IN THE SITE
- And in the node
- Line number

Note: These three columns are only displayed in a multi-site configuration.

This user characteristic is used to reserve an outgoing and incoming external line by indicating the TDM network trunk reserved for this subscription. It does not concern VOIP type equipment.

LOGOFF ACCEPTANCE

If this box is ticked, it means that the user can log on to another terminal.

PREDEFINED FORWARDING

Enter the internal or external number to which the user wishes to forward his calls. Forwarding to an external number is only possible if the "Immediate Forwarding Allowed" box is ticked.

The number entered can have a maximum of 17 digits, including direction access prefixes (0, 00).

Note: Other forwarding operations are defined in the dynamic features menu.

HOTEL ROOM SET TYPE

If you tick the box, you authorise personal calls with no password requested, to limit the number of wake-up call requests recorded at any time to 1, and authorise the message deposit feature. This column is used for hotel/motel management.

EXT.LAST CALLERS CALL BACK

Activation of this feature is only valid for the network (display of external number) and for sets with interactive keys.

MAINTENANCE SET

The maintenance set confers the right to the "access restriction" command (manual switching of day/night mode) and to the "billing monitoring".

If the box is ticked, this feature gives access to the functions available on the terminals defined in the menu **RECEPTION>Operators> Settings**.

These functions are accessible via the dynamic keys available on digital sets.

SPOKEN LANGUAGE

This field is only displayed when several languages are defined in the menu **SYSTEM>Configuration>Languages**. It is used to broadcast announcement messages in the user's language (see "**Spoken languages definition**").

WRITTEN LANGUAGE

Selecting the language for the displays on the I-interface stations (G2K, G2KIP): possibility to choose among the languages defined in Menu **SYSTEM>Configuration>Languages**.

USABLE IN CALLS WAITING QUEUE

If this box is ticked, it means that the call may be registered in a queue.

This allows the use of a subscription on which a digital set is "logged" but not necessarily connected or programmed to pile up calls.

BUSY FOR HUNT GROUP ON 1ST CALL

If the box is checked, 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).

EMERGENCY CALLBACK SET

If the box is ticked, the terminal is defined as an emergency callback terminal. Wire multi-line, "DECT" and "without terminal" sets cannot be configured as emergency callback sets.

WARNING: Once a subscriber has been configured as an emergency callback set, its directory number cannot be changed or deleted. The "Correct" command places the cursor on the line "Emergency callback set" so that the function can be set at NO, thus making it possible to change or delete the directory number.

SHARING SET

If this box is ticked, this selection means that the use of the set is shared by several persons (in a hospital room, for instance).

Note: The shared terminal if used by several users (i.e. configured with a short or long signature) should not be declared as prepaid.

SIGNATURE TYPE

This field is only available if the SHARING SET box is ticked.

NONE	Access to the shared set does not require any identification (generally used in a hotel room).
SHORT	Access to the shared set requires a password (generally used for a shared set in a hospital room).
LONG	Access to the shared set requires a login and a password (generally used for a self-service set).

SUBSCRIBER MONITORING (RECORD)

If the box is ticked, a monitoring record is issued at the end of a user’s communication.

CASE OF A MODEM USER

SUBSCRIBER MONITORING (RECORD)

Ticking the box enables you to request for the generation of a monitoring record at the end of a communication with the remote maintenance MODEM.

3.3.3.2 *Directory information*

3.3.3.2.1 Selecting a subscription record

Menu **SUBSCRIBERS>Subscription> Characteristics>Directory**

This screen is used to complete the columns not available while creating a new subscriber. This information, which defines the identity of the subscriber inside the company (or administrative attributes), will later be accessible when the directory is consulted.

This screen is also used to view information about a subscriber whose number is known.

Note: The directory record of a subscription is automatically created when the subscription is created. If this record is deleted subsequently, it is created again automatically by this command unless the subscription in question is BACKUP type.

Note: For a BACKUP type subscription, these are information fields and configuration of the subscription characteristics is only authorised on the reference site.

GENDER

For associating a civil status with the subscriber: Mr, Mrs or Miss (or if necessary, a place called “Conference room”, for a device).

Note: The Gender, Function and Confidentiality columns are defined in Menu SUBSCRIBERS>Directory>Settings.

FIRST NAME

For entering the subscriber’s first name.

VIP

Checkbox. Designates the subscriber's calls as VIP calls. Calls from this subscriber are routed through VIP reception.

FUNCTION

Function exercised by the subscriber in the company. The following functions are available: Assistant, Technician, Engineer, Manager, or other function (…..).

HIERARCHY

The subscriber’s hierarchical position in the company. This attribute will later be used to filter abbreviated numbers and forbidden numbers. Possibly used for charging applications.

CONFIDENTIALITY

Different types of lists are available to indicate the level of confidentiality for the subscriber: green list, orange list, and red list. Membership of any of these lists results in the filtering of certain calls to the subscriber.

E-MAIL

For indicating the subscriber’s e-mail address. This address is used to send a mail associated with a voice message left in the subscriber’s mail box (see the menu **MESSAGES AND TONES**. Notion of e-voicemail).

SIP URI

Field for entering an SIP URI in the Number records. The SIP URI function allows a subscriber to be called via the Internet.

SIP_URIs must contain only one character "@"; unauthorised characters are "()<>,;:"[]\", and they must end with a "character "." followed by at least two characters.

LOCATION

For defining the subscriber’s geographic location in the company.

LABEL

Optional field attached to the notion of abbreviated number, describing the set’s label. If it is entered, this field can be displayed while resolving the number.

ASSISTANT

Possibly for identifying the subscriber’s assistant (information field).

ABBREVIATED NUMBER

For indicating that this number entered is associated with a common abbreviated number on the installation.

USER LOGIN

For assigning a login to a MiCollab user in the LDAP directory when SSO mode is enabled. See Menu **Telephony service>Subscribers>Terminals and applications>MiCollab, Connection** tab, Section **3.5.7**.

This field in UTF8 format must contain a maximum of 120 characters.

In SSO mode, this login can only be deleted if no role is assigned in the subscription: Menu **SUBSCRIBERS>Subscriptions>Characteristics**.

As of R6.2 onwards, this login can be used to access the User portal (see Section 3.9.1.5).

MOBILE

Optional field for the subscriber's mobile number. This setting is configurable and visible for sites running with R8.2 and later.

Note: Customisable attributes can also be used to enter mobile phone numbers. For more information, see Chapter 3.2.1.6 – Customisation.

3.3.3.2.2 Abbreviated numbers display

Menu **SUBSCRIBERS>Characteristics>Directory information**.

ABBREVIATED NUMBER BEGINGS WITH

If this column is completed, only the abbreviated numbers above the number entered will be displayed on the next list.

Otherwise, all the abbreviated numbers will be displayed.

This screen displays the abbreviated numbers previously inserted in the “subscription record characteristics” of the directory record.

3.3.3.3 *Assigning terminals*

Menu **Subscribers>Subscriptions>Characteristics** – **Terminals** tab

Assigning a subscription to a device is not compulsory: the assignment is done automatically by the automatic login function, or manually from a terminal.

Subscription/device assignment is mandatory for the following systems:

- Analogue terminals (Z interface),
- Proprietary DECT,
- ISDN terminal,

It is not mandatory for the following systems:

- 675x,
- 53xx,53xxIP,
- SIP,
- WIFI,
- SIP DECT terminals,
- 67xxi series terminals.

This screen is used to assign a "physical” terminal to a subscriber for TDM terminals.

For other terminals, this is an assignment of a terminal type (e.g. mandatory for SIP DECT).

The notion of physical location does not apply to DECT handsets. It is the reference radio cell that must be entered (obligatory in case of DAS, optional for DECT). DECT management is handled in the chapter "Networks and links”.

Note: For a BACKUP type subscription, these are information fields and configuration of the subscription characteristics is only authorised on the reference site.

PHYSICAL TERMINAL TYPE 1

Options

For an **Associated subscriber** (In Characteristics: Authorised association of set), the maximum number of terminals is four.

TERMINAL TYPES

ANALOGUE

PROPRIETARY

IP_OWNER

SIP

IP DECT

SIP DECT CONFERENCE

RINGER RELAIS

EXTERNAL SET

Only the "Proprietary" type is proposed for an attendant console subscriber.

Note: The list of proprietary terminals can be displayed via Menu SYSTEM>Expert>Proprietary set name listing.

EQUIPMENT NUMBER

This field only concerns the TDM terminals physically connected to an equipment card of the PBX.

In a multi-site environment, the terminal may be an internal terminal, or a remote terminal physically connected to a remote site.

SITE

Name of the site supporting the terminal

NODE

Node number (2 by default)

EQUIPMENT NUMBER

Equipment number (position of the board in the cabinet).

Enter a 5-digit number on this line, indicating:

- First digit: the cabinet number (from 0 to 3)

  0: mother board

1: main cabinet

2: 1st expansion cabinet

3: 2nd expansion cabinet

- Second and third digits: board position number (from 00 to 15). Fourth and fifth digits: board equipment number

  Example: 10802

  This is equipment 02 of the digital extensions located on card 8 of the first cabinet.

SET MODEL

This field is only displayed (greyed out), not modifiable, and indicates the terminal model after connection. The model is automatically recognised.

INFORMATION FIELD (READ ONLY)

The following fields are displayed when the terminal sets up its first connection or makes its first calls.

IP ADDRESS

IP address assigned to the terminal.

RTP PORT

RTP port assigned to the terminal.

ENCODING LAWS

This field indicates the different encoding laws managed by the terminal in question (see Section 6.4).

TERMINAL CAPACITIES

This field indicates the different operating modes managed by the terminal in question, T38, video, encryption.

ACTIVE RINGTONE

For viewing whether the subscriber's terminal rings during a call (box ticked), or does not ring and displays a warning message (box not ticked).

Note: This setting can only be changed via the subscriber's User Portal.

SPECIAL CASES

EXTERNAL TERMINAL TYPE

An external terminal is a terminal not connected to the company's network, but to an operator's network.

It may be a fixed terminal (at home, for instance), or a GSM-type mobile terminal.

Calling the subscription results in a call to the external network.

If the subscriber is associated with a terminal in the company, they may choose the right terminal to receive the calls. See the functions offered by the MiVoice 5000 User Portal.

EXTERNAL NUMBER

Enter the external number used to reach the terminal on the external network.

Do not add the prefix.

This number will contain at least 10 digits, or it will be in E164 format:

For example: 0130969988 or +33 130969988

3.3.3.4 *Programmable keys*

Menu **SUBSCRIBERS>Subscriptions>Characteristics – Keys tab**

Note: "CCO supervision" key programming is only applicable for proprietary terminals (53xx, 675x) and SIP terminals (6700, 6800 & 6900).

For a given directory number, the screen displays the status of programmable keys.

By default, if the key is not programmed, the programming column displays the message **This key is not programmed**.

THIS KEY IS NOT PROGRAMMED

Note: See the documentation on terminals for the list that indicates the number of programmable keys for each set type.

From this screen, click the number of the key to program (or re-program) to edit the corresponding key.

3.3.3.4.1 Set key programming

Note: For a BACKUP type subscription, these are information fields and configuration of the subscription characteristics is only authorised on the reference site.

Number assigned to key

This field available if the terminal is multiline. Select the corresponding line.

Programming type

In the **Programming type** field, select the type you want (see below).

If the key is programmed already, these fields are filled in with the current values.

For programming, depending on the programming type, some additional fields appear below the list of keys.

Parameter

The **Setting** field for certain types allows you to enter the parameter required for the programming type. For some types, it is associated with the additional fields **Direction** and **Signal** (see list below).

Protected key:

The user cannot modify the key if this box is ticked. For some types, default protection is applied.

Update SIP sets

For a terminal 6xxxi, and if key configuration is entrusted to Web Admin (see Menu Subscribers>Terminals>6xxxi settings), the "SIP sets updating" key is proposed; the action updates the terminal keys.

Validating programming

Validating a programming operation automatically updates the display table. If the cursor is on the table, the “up” and “down” cursor keys allow you to change from one key to the other.

Structure

In the programming table, a “padlock” icon on the left of the key number indicates a protected key (the “protected key” checkbox has been ticked).

The keys not yet programmed appear in black. The already programmed keys appear in green.

The functions **Next/Previous**, on the left part of the screen, are used to change to the next/previous subscriber.

The **Repeat** function is disabled by this type of programming.

The terminal is deactivated once a program is validated. The terminal is automatically reactivated if the user exits the tab, or by navigating in the subscriber list.

Table 1: List of programming types and associated fields

PROGRAMMING TYPE	PARAMETER	DIRECTION	SIGNAL
No programming			
Dialling	NUMBER DIALLED		
Cancel all forwarding			
MobileLink			
Predefined forward			
Forward on busy	TERMINAL DIRECTORY		
Forward on no answer	TERMINAL DIRECTORY		
Immediate forward	TERMINAL DIRECTORY		
Activate notebook	TIME		
Deactivate agenda	TIME		
Lock			
General standby			
Filtering	TERMINAL DIRECTORY		
Do not disturb			
Anti-intrusion			
Monitoring your number (CCO)			
External line supervision	EXTERNAL LINE DIRECTORY	X	X
Monitor filtered calls	TERMINAL DIRECTORY		X
Subscriber management	TERMINAL DIRECTORY		X
Privileged intercom (buzz)	TERMINAL DIRECTORY		
Phone box			
DTMF numbering	NUMBER DIALLED		
Your personal external line			
Outside / in hunt group			
Voice mailbox monitoring			X
Messages deposit			
Close room			
Room wake-up			
Open room			
Alarms monitoring			
Call supervision internal ***(attendant console only)***			X
Call supervision PSTN incoming 1 *(attendant console only)*			X
Call supervision PSTN inc 2 ***(attendant console only)***			X

Call supervision tie line inc 2 ***(attendant console only)***			X
Overload signalling ***(attendant console only)***			X
Reservation signalling ***(attendant console only)***			X
Console active ***(attendant console only)***			
Hold			
Save/Repeat			

* Programming options for **Dialling**:

- Complete number: the terminal dials and calls the number entered.
- Incomplete number: the terminal dials the incomplete number entered and lets the subscriber complete the number before starting the call.
- Function code without requesting for a number: the terminal runs the function code command.
- Function code requesting for a number + the full number to be dialled: the terminal runs the function code command with the full number entered.
- Function code requesting for a number + no number to dial: the terminal lets the subscriber enter the full number before running the function code command.
- Function code requesting for a number + a part of the number to dial: the terminal lets the subscriber enter the programmed number before running the function code command.

NOTE: For SIP phones, "Dial" programming with the function code requesting for a number + part of the number to be dialled is not available.

3.3.3.5 *Call forwarding*

Menu **Subscribers>Subscriptions>Characteristics** – **Forwarding** tab

Forwards are characterised by:

- The type of forward (predefined, immediate, on no answer, on busy)
- The call origin (all calls, internal calls, external calls)
- The type of forward recipient (messaging system, internal or external number)
- The recipient’s number (for internal or external number only)
- The locked information (yes/no).

For each subscription, the forwarding type is subject to a right to be defined in Menu **Subscribers>Subscriptions>Characteristics** – **Forwarding** tab.

When a subscription type is forbidden from all forwarding operations (messaging system, modem, ATDC, etc.) the action on the **Forwards** tab remains without any impact.

Programming a forwarding operation via this menu renders it immediately active and deletes any possible forwarding programmed by this terminal.

If predefined forwarding had been programmed and activated, this latter is deactivated but not deleted.

PREDEFINED FORWARD

2 lines in read only mode give the status of forwarding (**Not active, Active, Active Internal, Active External**) and the number of the forward recipient.

IMMEDIATE FORWARD/FORWARD ON NO ANSWER/ON BUSY

For these different forwarding types, the call origin is defined (**all calls**, **internal calls, external calls**). It is possible to define several origins by type of forwarding, even if only one origin is working at a given moment.

For each origin a list of options is presented to determine the type of forwarding recipient:

- ……… : for deleting a programmed forwarding operation
- Voice mail: for forwarding a subscriber to his voicemail
- Number: for forwarding to a number (internal or external).

When the origin is selected, the following two lines appear (for forward to number only):

- Forwarding number: 6 digits maximum for an internal number or 14 digits maximum for an external number (including the prefix used) For forwarding to voicemail, this line is hidden because the system automatically calculates the voicemail directory number.
- Locked forwarding: checkbox indicating that the user cannot modify or cancel their forwarding if the box is ticked.

3.3.3.6 *Personal abbreviated number*

First of all, you have to define the private abbreviated numbers associated with the subscribers.

Then selecting from the private directory will display users of abbreviated numbers.

3.3.3.6.1 Defining personal abbreviated numbers (directory)

From the menu **SUBSCRIBERS>Characteristics>Directory** and by selecting the corresponding directory number.

Note: If a subscriber is not entitled to a private directory, the message “Unproper access right” appears.

Note: For a BACKUP type subscription, these are information fields and configuration of the subscription characteristics is only authorised on the reference site.

10 private abbreviated numbers can be assigned to each directory.

The numbers saved by the subscriber may be complete or the beginning of a number. In this case, the subscriber must complete the number during its use.

3.3.3.6.2 Users of private abbreviated numbers

Menu **SUBSCRIBERS>Display>Personal abbreviated number users.**

This screen is used to display all subscribers with a private directory. For each subscriber identified, the number of private abbreviated numbers declared is indicated (1 to 10), without specifying the numbers themselves.

Note: The assignment of a private directory is subject to a user right entitled “Personal abbrev. numbers allowed”, granted from Menu “Extension characteristics”.

3.3.3.7 *Multiline*

A multi-line subscription is equal to several single-line subscriptions. Each line has its own characteristics.

Menu **Subscriptions>Characteristics>Multi-lines**.

Note: For a BACKUP type subscription, these are information fields and configuration of the subscription characteristics is only authorised on the reference site.

This screen is used to assign one or more secondary numbers to an existing extension number.

The multi-line function is used to differentiate the traffics from the different directory numbers and, thus, manage each number independently (filtering, forwarding, etc.).

Note: An attendant console may have two additional directory numbers, that is three lines in the menu.
When a terminal does not have the corresponding right, the message “Secondary DN not authorized” is displayed.

3.3.3.8 *Display features*

Menu **SUBSCRIBERS>Characteristics>Functions**.

This screen is used to display all the special extension functions not defined in the extension characteristics.

For example, the following functions can be mentioned on this screen:

- Extension belonging to an answering service

- Extension belonging to a hunt group
- Addressee of a forwarded call
- ….

This screen does not allow directory number modification. It displays the configuration of the modifications to make before directory modification.

This menu can also be used to activate or put on standby (deactivate) a terminal belonging to a hunt group.

This feature is offered for the following hunt group types:

- cyclic
- fixed head
- general call
- longest idle time

This feature is not offered for super hunt groups.

3.3.4 TERMINAL AUTHENTICATION AND USER PORTAL PASSWORD

Menu **SUBSCRIBERS>Subscriptions>Terminal authentication and User Portal password**

OPERATION TYPE

Options:

AUTHENTICATING THE TERMINAL	Authentication MD5 passwords generated by the system for all the directory numbers included between the first directory number and the last directory number.
User portal PWD	User Portal access passwords generated by the system for all the directory numbers included between the first directory number and the last directory number.

Note: If SSO mode is enabled, USER PORTAL PWD is not proposed in the options.

SIP DECT R2.1	SIP DECT passwords generated by the system for all the directory numbers included between the first directory number and the last directory number (applicable as of R2.1 for SIP DECT).

FIRST DIRECTORY NUMBER

Directory number of the first subscriber concerned.

LAST DIRECTORY NUMBER

Directory number of the last subscriber concerned.

ACTION

AUTOMATIC GENERATION	Passwords generated by the system for all the directory numbers included between the first directory number and the last directory number.
MANUAL CREATION	The password entered in the MANUAL AUTHENTICATION applies to all the subscriptions between the first directory number and the last directory number.
DELETE	Delete password for all the directory numbers included between the first directory number and the last directory number.
EXPORT	Export in a file ("authpost.csv) of the password for all the directory numbers included between the first directory number and the last directory number.
Mitel OMM EXPORT	Export in a file ("exportomm.csv) of the password for all the directory numbers corresponding to IP DECT or SIP DECT, included between the first directory number and the last directory number. (∗) Applicable as of R2.1 for SIP DECT.

∗ The file generated can be used for manual import from the Mitel OMM (Open Mobility Management) server. For more information about the Mitel OMM import functions, refer to the *DECT over IP Service Installation and Implementation Guide* [5].

MANUAL AUTHENTICATION

This field is only present if the action selected is MANUAL CREATION.

Enter a string with at least 8 alphanumeric characters.

Select the type of action to take, either to define the passwords (automatic/manual) or to delete them (erase) or to export them.

Click **Confirmation** to validate the operation.

If an export has already been carried out, you can download the file generated on the iPBX by clicking the File created link:

Note: If the action applies to a single subscription which is BACKUP type, the system returns an error message.
If the action applies to a set of subscriptions, some of which are BACKUP type, the system will ignore the BACKUP type subscriptions without generating an error message.

3.3.5 COPY OF SUBSCRIBER CHARACTERISTICS

Menu **SUBSCRIBERS>Subscriptions>Copy of subscriber characteristics**.

This screen is used to copy a certain number of an extension’s characteristics to one or more other extensions.

More precisely, this function allows a "reference” subscriber’s characteristics to be copied to several subscribers created beforehand. These "beneficiary" subscribers are identified thanks to a first and last number in the directory.

REFERENCE DIRECTORY NUMBER

Reference directory number (example: subscriber 4000).

FIRST DIRECTORY NUMBER

Number of the first directory on the list (example: subscriber 2795).

LAST DIRECTORY NUMBER

Number of the last directory on the list (example: subscriber 2797).

COPY RANGE

From the following characteristics, select those that will be duplicated, from the reference subscriber to the beneficiary subscriber(s):

- FEATURES

- LIA RTC CATEGORIES (TL PSTN CATEGORIES)

- DISCRIMINATION

- PARTITION

- CUG

- VOICE MAIL CLASS

- INTERCOM GROUP

- PREDEFINED FORWARD

- IMMEDIATE FORWARD

- FORWARD ON NO ANSWER

- FORWARD ON BUSY

Click **Confirmation** to validate the operation.

Note: If the action applies to a single subscription which is BACKUP type, the system returns an error message.
If the action applies to a set of subscriptions, some of which are BACKUP type, the system will ignore the BACKUP type subscriptions without generating an error message.

Note: If the last directory number is not specified, the copy will only be applied to the subscriber indicated by the first directory number.
This function is also applicable to multi-directory subscriptions.
This function also copies the “pre-payment” characteristic, except for the amount paid.

3.3.6 COPY KEYS

Menu **SUBSCRIBERS>Subscriptions>Copy of keys**.

This screen is used to copy all or part of the programming of a reference directory key to other directory subscribers.

REFERENCE DIRECTORY NUMBER

Extension number of the subscriber known as the "reference directory". In this case, the reference directory corresponds to a subscriber whose terminal keys have already been programmed.

FROM KEY

Number of the first key to be copied.

TO KEY

Number of the last key to be copied.

TYPE

C: for **C**all/supervision	**N**: **N**ot used	**P**: **P**ersonal line
M: **M**ail box supervision	**L**: Sup **E**xt. line	**F**: yr calls from... **F**orward to
D: calls to ...coming **F**rom	**M**: mon your **M**ultikey number	**S** : direct access **S**erver
F: **F**eature	**N**: **N**umbering of	**V**: freq. num **V**oice
H: **H**old	**K**: Sa**v**e/repeat	
4 : signal overload	**5**: Signal reservation	**6**: Console active

Only one type of copy can be selected at this stage.

FIRST DIRECTORY NUMBER

Number of the first directory on the list.

LAST DIRECTORY NUMBER

Number of the last directory on the list.

FOR SETS

Indicates the type of set to which the key copy applies. If "…." is selected, it will apply to all types of terminals.

Note: This list can be modified in Menu List of proprietary set names in SYSTEM>Expert.

Select the digital sets concerned by entering the number of keys they have.

FROM KEY

This column is used to transfer the keys of the reference subscription to those of target subscriptions.

DELETION OF THE PROGRAMMING

NO **YES**

This is used to delete the old key programming of called sets.

- YES: the keys concerned are programmed.
- NO: only the un-programmed keys are programmed. The previous programming is kept.

COPY INTERRUPTION IF ERROR

- Box ticked: indicates that the copying procedure stops when an error is detected.
- Box not ticked: the copying procedure continues in the event of an error when programming a key.

Note: If the action applies to a single subscription which is BACKUP type, the system returns an error message.
If the action applies to a set of subscriptions, some of which are BACKUP type, the system will ignore the BACKUP type subscriptions without generating an error message.

3.3.7 REDIALING

Menu **SUBSCRIBERS>Subscriptions>Re-assignment**.

FIRST DIRECTORY NUMBER

Directory number of the first subscriber to be redialled.

LAST DIRECTORY NUMBER

Directory number of the last subscriber to be redialled.

MAIN DIRECTORY NUMBER

New directory number of the first subscriber.

DID DIRECTORY PLAN 1

If the box is ticked, redialling also applies to the DID directory. Enter as "new values" the new number from which the DID directory will be created.

Confirm the parameters to apply the subscription redialling.

Note: If the action applies to a single subscription which is BACKUP type, the system returns an error message.
If the action applies to a set of subscriptions, some of which are BACKUP type, the system will ignore the BACKUP type subscriptions without generating an error message.

3.4 DISPLAYING SUBSCRIBERS

The web interface of MiVoice 5000 Web Admin allows subscriber search using different criteria, depending on the type of information at the user's disposal.

From the menu **SUBSCRIBERS>Display**.

This menu is used to search for a subscriber by equipment number, from internal directories, from DID directories, thanks to the subscriber's name, from the card's IP address, in the list of proprietary sets, or other display criteria.

3.4.1 BY INTERNAL NUMBER

Menu **SUBSCRIBERS>Subscriptions>Display by local number**.

COMPANY SELECTION

Select the company. The drop-down list contains the priority classes defined in the system.

Note: This field is only displayed in multi-company configuration.

DIRECTORY BEGINNING WITH

Beginning of directory number. All directory numbers that start with this digit/ number will be displayed.

SUBSCRIPTION TYPE

…..	BACKUP	GENERAL PURPOSE	list of the types described in subscriber creation

If necessary, select the subscription type to restrict the display to a subscription category.

DISPLAY TERMINALS

NO **YES**

Select this option to display the terminals assigned to the different subscribers selected previously.

After entering all the parameters, click **Select the item** to start searching in the directory.

The **type model** column indicates the subscription type and, where appropriate, the type of associated terminal.

3.4.2 DISPLAY BY DID DIRECTORY

Menu **SUBSCRIBERS>Display>By DID directory**.

This screen is used to display all (or a selection of) the DID numbers assigned already.

PLAN SELECTION (1 TO 8)

For filtering display according to a particular plan. If **.....** is selected, the display concerns all the plans.

DIRECTORY BEGINNING WITH

For filtering display for a directory number range.

DISPLAY OF THE SETS

NO **YES**

For choosing whether or not to display the terminals assigned to subscribers on the list of DID numbers to display.

Then click **Select the item**:

Note: An information line "Incomplete display" appears when more than 1000 subscribers must be displayed (display menu limited to 1000 lines).

3.4.3 DISPLAY BY NAME

Menu **SUBSCRIBERS>Display>By name**.

NAME BEGINS WITH

Indicate here the beginning of the surname of the subscribers to display. If this column is empty, all the directory numbers with a name will be displayed. The list of names will be displayed in alphabetical order.

Click **Select the item**.

3.4.4 DISPLAY BY IP ADDRESS

Menu **SUBSCRIBERS>Display>by IP address**.

MINIMUM IP ADDRESS

Indicate here the first IP address of the subscriber to display.

MAXIMUM IP ADDRESS

If necessary, indicate here the last IP address of the subscriber to display.

Click **Select the item** to validate the operation.

This menu is used to display, for a given address range, all the declared IP subscribers. This list is displayed in the increasing order of subscriber IP address.

3.4.5 SETS DISPLAY

Menu **SUBSCRIBERS>Display> sets**.

SETS RANGE

For selecting the range of owner sets to be displayed.

DIRECTORY BEGINNING WITH

If necessary, for selecting a part of the owner sets to display from the directory number.

Click **Select the item** to validate the operation.

Note: Menu SYSTEM> Expert is used to display all the Mitel terminals, no matter the series.

3.4.6 USERS OF THE FORWARDINGS

Menu **Subscriptions>Display>Users of forwardings.**

This screen is used to select the forwarding type associated with a given number.

TYPE OF FORWARDING

…….	**PREDEFINED**	**IMMEDIATE**	**NO ANSWER**	**ON BUSY**

Select the type of forwarding you want. All subscribers that have activated this forwarding type will be displayed.

Note: If immediate forward replaces active predefined forward, this latter is deactivated but the predefined forward number remains active.

DIRECTORY BEGINNING WITH

Indicate the first subscriber number to be selected.

3.4.7 OTHER DISPLAYS

Menu **SUBSCRIBERS>Display>Other display.**

It is used to select subscribers by the following criteria:

- Shared terminals
- Secured subscriptions (Dual Homing feature)
- Backup subscriptions
- Terminals defined as emergency callback terminals.

3.4.7.1 *Shared terminals*

This command is used to display the list of subscriptions for which the associated set is shared (hospital room, self-service set, for example). Shared set is a subscription characteristic, defined in the menu **SUBSCRIBERS>Subscriptions>Characteristics>General characteristics**.

To display the subscriptions whose terminals are shared, click **Shared sets** from the screen **SUBSCRIBERS>Display>Other display**.

DIRECTORY BEGINNING WITH

Enter a digit (or number).

Used to limit the display of shared terminals to the directory numbers starting with the value indicated.

Click **Select the item**:

The shared sets display table indicates:

- the directory number of the subscription
- type of extension
- the location: cabinet number, board position, board equipment number or IP address,
- the type of signature needed to use the set,
- the subscription numbers (user) and names (names) of the MULTIUSER type subscribers sharing the terminal with the primary subscription,

The star in the last column indicates incoherence in the definitions of the associated shared/multi-users sets:

- the shared set subscription is assigned to no terminal,
- the shared set subscription has no signature and several users are associated with it,
- the shared set subscription has no signature or a short signature, and no associated user.

3.4.7.2 *Display emergency callback sets*

This menu is used to display all the location terminals in case of emergency call.

3.4.7.3 *Secured subscriptions*

This command is only available in a multi-site configuration or Cluster.

This command is used to view the list of secured subscriptions (taking advantage of the Dual Homing feature). The Dual Homing feature is a characteristic of the subscription.

It is configured in Menu**: SUBSCRIBERS>Subscriptions>Characteristics>General characteristics** by assigning a backup site to the subscription.

To display the secured subscriptions, click **Securred subscription** from the menu **SUBSCRIPTIONS>Display>Other display**.

BACKUP SITE

Name of the site on which the displayed subscriptions are backed up.

……….	No selection criteria on the backup site.
Site Name	Only the subscriptions backed up on the site indicated are displayed.

The drop-down list contains all the sites of the multi-site used as backup to at least one secured subscription.

DIRECTORY BEGINNING WITH

Enter a digit (or number): only secure subscriptions in which the directory number starts with this value are displayed.

Choose the display criteria then click **Select the item**:

The secured subscription display table indicates:

- The subscriber's directory number,
- The subscriber's surname,
- The name of the site on which the subscription is backed up,
- The site node number.

The star in the last column indicates that the set associated with the subscription does not support the Dual Homing feature, or that the secured subscription is out of service. In this case, the telephone data of the subscription will not be copied to the backup site (daily or immediate alignment).

3.4.7.4 *Backup subscriptions*

This command is only available in a multi-site configuration or Cluster.

This command is used to display the list of subscriptions used as backup to a subscription on another site.

To display the backup subscriptions, click **Backup subscriptions** from the menu **SUBSCRIPTIONS>Display>Other display**.

REFERENCE SITE

Name of the declaration site of the subscriptions whose backup subscriptions will be displayed.

……….	No selection criteria on the reference site.
Site Name	Only the backup subscriptions of a subscription declared on the site indicated will be displayed.

The drop-down list contains all the sites of the multi-site where at least one subscription is secured on the current site.

DIRECTORY BEGINNING WITH

Enter a digit (or number): only the backup subscriptions in which the directory number starts with this value are displayed.

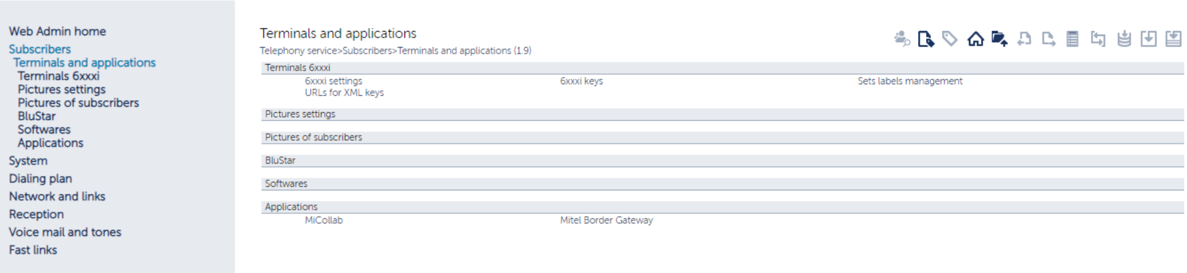
Choose the display criteria then click **Select the item**:

The backup subscription display table indicates:

- The subscriber's directory number,
- The subscriber's surname,
- The name of the site on which the subscription is declared,
- The node number,
- The backup subscription status:
- Inactive indicates normal operation of the subscription on its reference site.
- Active indicates that the reference site of the subscription is no longer accessible and that the backup subscription has been activated on the backup site.

3.5 TERMINALS AND APPLICATIONS

Menu **SUBSCRIBERS>Terminals and applications**



3.5.1 INTRODUCTION

Concerning terminals 6xxxi:

To enable the TMA to manage terminals 6xxxi, this menu offers easy deployment for this type of terminals.
The configuration thus defined will be used as interface for the TMA so it can manage these terminals.
The **Settings** column is used to prepare the deployment phase (associated with the Ctrl + i script) and possibly to automatically configure the systems keys (including the call by name key) and/or dialling plan for terminals 6xxxi.

Blustar 8000 i:

As of R5.4 SP2, BluStar terminal authentication (login/password) may be managed from the iPBX in the following contexts:

- Connection invite login
- Forwarding programming
- IVB authentication
- DND programming.

This 8000i login/password is the login/password of the subscriber defined in the menu **Telephony service>Subscribers>Subscriptions>Characteristics**.

The login / password is not activated by default.

The administrator must tick the corresponding box, if they want, after the different operation types:

- First installation
- Upgrading R6.1 Edition n to R6.1 Edition n + 1
- Upgrading R5.3 SP, R5.4 IP or R5.4 SP1 and R5.4 SP2 to R6.1.

After these operations, the terminals automatically restart with the new release including the authentication function.

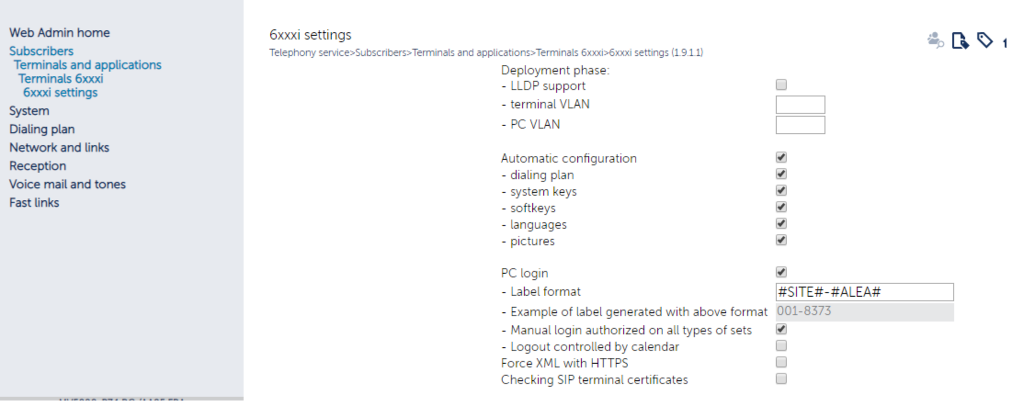
When the administrator ticks the box, the user must log on again to his subscription with the password provided.

The iPBX then performs authentication check on the user's requests.

If some terminals had been disconnected or switched off during the activation, when they are restarted, the corresponding subscriptions are frozen and seen as out of service. They must be unlocked (put into service) in Menu **Telephony service>Subscribers>Subscriptions>Characteristics**.

3.5.2 TERMINALS 6XXXI

3.5.2.1 *6xxxi settings*



6xxxi settings

Telephony service>Subscribers>Terminals and applications>Terminals 6xxxi>6xxxi settings (1.9.1.1)

Deployment phase:
- LLDP support ☐
- terminal VLAN
- PC VLAN

Automatic configuration ☑
- dialing plan ☑
- system keys ☑
- softkeys ☑
- languages ☑
- pictures ☑

PC login ☑
- Label format #SITE#-#ALEA#
- Example of label generated with above format 001-8373
- Manual login authorized on all types of sets ☑
- Logout controlled by calendar ☐
Force XML with HTTPS ☐
Checking SIP terminal certificates ☐

Menu **SUBSCRIBERS>Terminals and applications>6xxxi settings**

DEPLOYMENT PHASEE area

LLDP SUPPORT

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

TERMINAL VLAN/PC VLAN

These parameters are used to define the VLAN dedicated to terminals (6xxxi, 53xxip and i7xx). They are not mandatory on simple networks.

AUTOMATIC SETTING OF SETS area

This area only appears when manual login is enabled.

The **Automatic terminal configuration** area allows the installer not to automatically configure the systems keys (including the call by name key) and/or the dialling plan for MiVoice 6000 SIP Phones).

If the first line is not ticked, the following keys are hidden. On the other hand, it is possible to set to NO the lines ‘*dialing plan*’ and/or ‘*keys*’ and to leave on YES the line ‘*automatic terminal configuration*’.

The "**Programmable keys**" line indicates that the 6xxxi keys can be configured via the iPbX Web Admin settings (Menu **Subscribers>Characteristics>Keys**). Otherwise, only the management centre is authorised to perform this task.

Login via PC

This area with several fields is used to configure the PC login and periodic logout functions.

Log in via PC: This checkbox allows users to log their terminals 6xxxi from a PC (User Portal or an external application if MiVoice 5000 Manager is available). When this box is ticked, a label is automatically generated for terminals 6xxxi.

Label format (20 characters max.) allows you to indicate in the label format the site number as well as a random number (equal in size to the length of its dialling plan). It is necessary to use the keywords **#SITE#** and **#ALEA#** respectively in the description of its label format.

This label can be customised by adding fixed strings or these tags. For example, you can put #alea##alea# if you want to generate a random number twice as long.

This label is used in the automatic generation done by the iPBX. The operator can later change this label for each terminal.

The **Example of label** field (limited to 16 UTF8 characters, i.e. 32 bytes) generated with the above format gives the user an example of a label generated from their label format defined above. This allows the user to check whether the generated string is truncated or not.

The check box **Manual login authorized on all types of sets** allows you to authorise or not the manual login on all terminals connected to the site in question (applies to all types of terminals 6XXXi, 53xx/ip, i/M7xx, etc.). By default, this box is ticked.

The **Logout controlled by calendar** checkbox allows the operator to activate periodic terminal logouts. If this box is unticked, the next 2 fields **(Linked calendar** and **Default value for the new set**) are hidden.

If the **Logout controlled by calendar** box is ticked, the following fields appear:

The **Linked calendar** option allows the operator to choose the calendar defined in the iPBX to which they want to associate the periodic logout function. By default no calendars is selected.

The **Default value for the new set** option allows you to choose the default value for the periodic logout right for any new terminal. By default, this box is ticked; login is activated for all new terminals.

Force XML ON HTTPS

Checkbox used to force XML communication with SIP/XML terminals (6xxxi, SIP-DECT terminals) to secure connection.

The **Force XML with HTTPS**check box is displayed if a certificate has been assigned **for SIP terminal** use from **the Certificates assignment** tab of Menu **SYSTEM>Security>Certificates management**. Refer to Section 4.4.

Box not ticked: the call server uses the http on Port 3197 or HTTPS on Port 4443 (if it is a password request or response to the Mitel OMM request in HTTPS).

Box ticked: the call server will systematically use HTTPS on Port 4443.

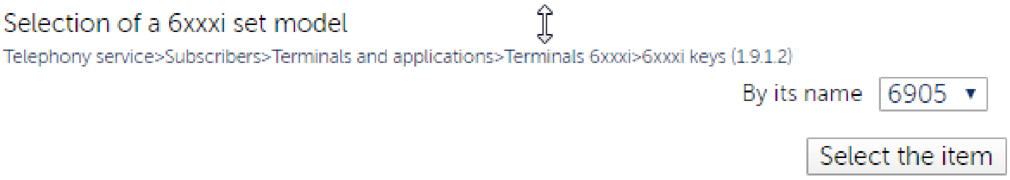
This box is unticked by default.

It is masked on a node as this feature is managed on the cluster server and then replicated on all the nodes connected to this cluster server.

Checking SIP terminal certificates

The Checking SIP terminal certificates checkbox is displayed if a non-self-signed certificate **has been assigned for SIP terminal** use **from the Certificates assignment** tab of Menu **SYSTEM>Security>Certificates management**. Refer to Section 4.4.

3.5.2.2 *6Xxxi keys*



Selection of a 6xxxi set model

Telephony service>Subscribers>Terminals and applications>Terminals 6xxxi>6xxxi keys (1.9.1.2)

By its name: 6905

Menu **SUBSCRIBERS>Terminals and applications>Terminals 67xxi>6xxxi keys** is used to configure **System** keys according to MiVoice 6000 SIP Phone model.

Terminal 6xxxi keys are divided into two categories: **System** keys and **Programmable** keys.

As of release R5.3 SP1, the list of functions is extended and terminal programming is automatic when a MiVoice 5000 Manager is available (see MiVoice 5000 Manager - User Guide).

Systems managed by MiVoice 5000 Manager

In this case, the **System** functions programmed on some **Programmable** keys must be retrieved and reassigned to **System** keys, available according to 6xxxi series terminal model.

Systems without MiVoice 5000 Manager

To be compatible with the previous releases, this menu displays a configuration in which some "**Systems**" functions would have been programmed on some keys in the "**Programmable**" keys area.

As of release R5.3 SP1, only the proposed **System** keys will be configurable.

Procedure:

Select the terminal model from the **By its name** field.

Note: Model 6751i, which does not have any key, is not proposed.

Each programming operation is optional and may only be assigned to one key.

To simplify the programming, the menu is displayed in form of a list of programs that can be activated via a checkbox.

The parameters associated with a program concern the key that will receive this program:

- <Function x> key: label associated with the programming provided by the system according to type of terminal.
- - Key type: system (unmodifiable value)
- - Number: number of this 3-numeric-characters key field (1 to 999)
- - Label: field for 29 alphanumeric characters (upper case and lower case).

The **Label** field is only available for certain keys. It corresponds to the label which will be displayed on terminal 6xxxi. The length of the label displayed on the terminal will depend on its type.

The menu only shows the programs possible for the terminal model chosen.

When a function is activated, the menu searches for the first available key.

When choosing the key type, the menu searches for the first available key of this type. If no key is free, the key field remains blank.

A test is performed while entering the key number to check whether this key is free and whether it is available on this terminal model.

Menu/ident key:

If the terminal is logged on, this key gives access to the following columns:

- Call type
- Active functions: menu used to view all the active functions and possibly to deactivate them (Example: Forward)
- Forward
- Parameters: menu used to access the terminal settings (calls, general, language, forward, Do not Disturb, etc.)
- Voice mail
- Languages
- Logout.

If the terminal is not logged on, this key is used to manually assign a login via the identification columns.

Concerning the **Services** key:

If the terminal is logged on, this key is used to group together and access the following columns:

- Directrory (inside the terminal)
- Caller list
- Voice mail.

Summary by type of terminal

For **Programmable**keys, refer to the MiVoice 5000 Manager User Guide.

MODEL	NR OF SYSTEM KEYS	SUPPORTED KEY PROGRAMMING
6710I	4	Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6730I	4	Menu/ident Services Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6731I	4	Menu/ident Services Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6735I	6	Menu/ident Services Private directory Caller list Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6737I	10	Menu/ident Services Private directory Caller list Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6739I	6	Menu/ident Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding Features in communication (callback, trace, and parking): see Note below.

MODEL	NR OF SYSTEM KEYS	SUPPORTED KEY PROGRAMMING
6753I	4	Transfer Conference Menu/ident Services Private directory Caller list Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6755I	6	Menu/ident Services Private directory Caller list Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6757I	10	Menu/ident Services Private directory Caller list Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6863I	3	Transfer Conference Menu/ident Services Private directory Caller list Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6865I	4	Menu/ident Services Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding

MODEL	NR OF SYSTEM KEYS	SUPPORTED KEY PROGRAMMING
6867I	6	Menu/ident Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding Features in communication (*)
6869I	7	Menu/ident Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding Features in communication (*)
6873I	7	Menu/ident Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding Features in communication (*)
6905	3	Transfer Conference Menu/ident Services Private directory Caller list Call by name Consult mail box directly Forwarding to voice mail Cancel voice mail forwarding
6910	2	Menu/ident Services Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding
6920	7	Menu/ident Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding

		Features in communication (*)
6930	7	Menu/ident Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding Features in communication (*)
6940	7	Menu/ident Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding Features in communication (*)
6970	7	Menu/ident Private directory Call by name Consult mail box directly Voice mail forwarding Cancel voice mail forwarding Features in communication (*)

Note: **For terminals 6739i, 6867i, 6869i, 6873i, 6920, 6930, 6940 and 6970, the Features in communication key does not have any configurable label. Its label will depend on the call phase.**

The programming of this key allows the following actions during phone communications:

- Automatic callback

- Trace

- Parking

3.5.2.3 *Sets labels management*

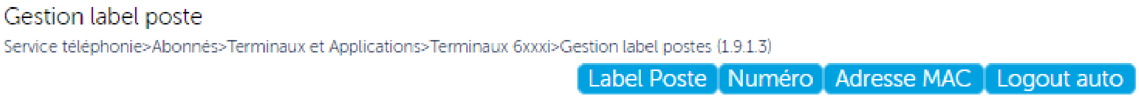
3.5.2.3.1 Set labels display

This menu on the **Subscribers>Terminals and Applications>Terminals 6xxxi>Sets labels management** tree allows you to list the labels of terminals 6xxxi as well as the right to Automatic logout.

Set label beginning with

This menu offers a selection menu allowing the user to enter the label of the entry(entries) they wishe to display.

If no selection criteria are defined, the menu displays all terminals 6xxxi with their labels.



Gestion label poste

Service téléphonie>Abonnés>Terminaux et Applications>Terminaux 6xxxi>Gestion label postes (1.9.1.3)

Label Poste | Numéro | Adresse MAC | Logout auto

The table displays the following details:

- Set label: (20 characters max.) displays the terminal 6xxxi label designated by the MAC address,
- Number: (10 digits max.) directory number associated with the entry,
- MAC address: (12 characters max.) terminal MAC address,
- Automatic logout: display corresponding to the right to periodically logout the terminal in form of a label (YES/NO).

3.5.2.3.2 Modification

If the user clicks in the Set label field of an entry in the display table, they will be taken to a menu where they can make certain changes to that entry:

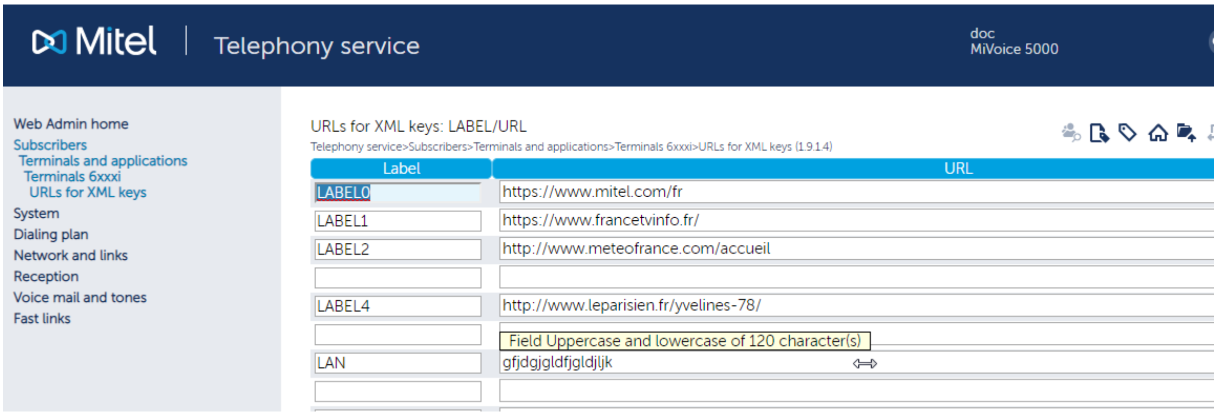
- The Number field allows a directory number to be entered only if the field was previously empty (otherwise the user will get an error diag indicating an "modification not allowed"). This menu only allows you to assign a directory number to an unmarked terminal.
- The Label field allows the terminal label to be changed (the user can thus ignore the label format defined in the 6xxxi settings). There is no uniqueness check on the data entry. The field can also be empty, in which case the item concerned will no longer be identifiable in the PC login function.
- The Automatic logout checkbox allows you to manually configure the periodic logout right for the terminal in question;
- the Delete button: Allows the terminal concerned to be removed from the list of terminals (for a terminal removed from the network).
- The MAC Address field, which shows the MAC address of the terminal concerned in this menu, is read-only.

3.5.2.4 *URLs for XML keys*

This menu allows you to program a type key to access a URL whose address must be specified.

This key is automatically locked. However, unlocking can be done in the **Keys** tab of Menu **Subscribers>Subscriptions>Characteristics**.

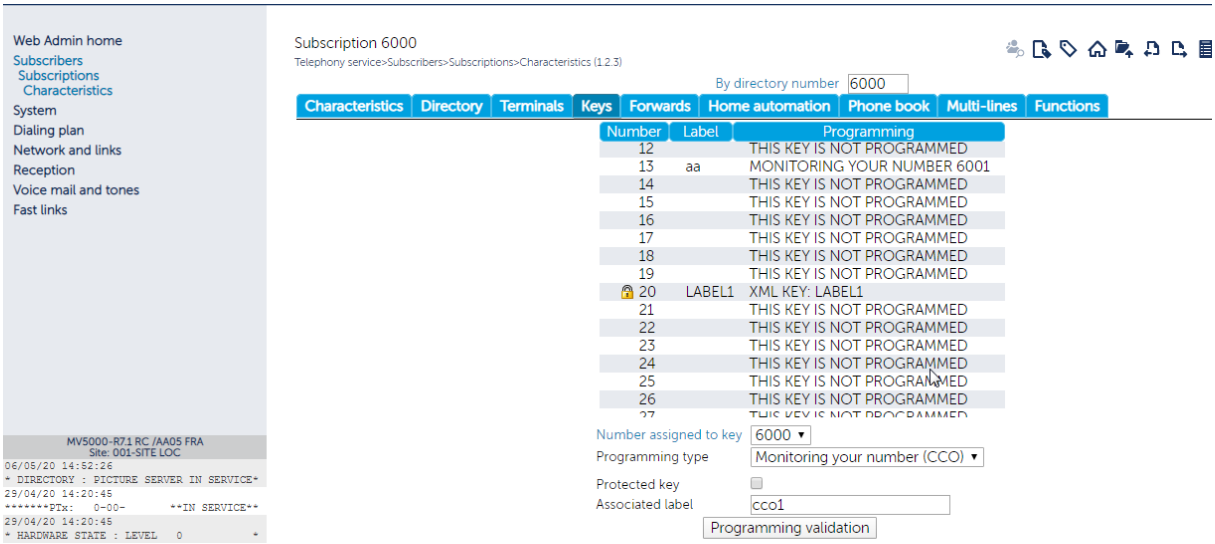
Note : The URL must be absolute to work with the XML keys.



URLs for XML keys: LABEL/URL

Telephony service>Subscribers>Terminals and applications>Terminals 6xxxi>URLs for XML keys (1.9.1.4)

Label	URL
LABEL0	https://www.mitel.com/fr
LABEL1	https://www.francetvinfo.fr/
LABEL2	http://www.meteofrance.com/accueil
LABEL4	http://www.leparisien.fr/yvelines-78/
	Field Uppercase and lowercase of 120 character(s)
LAN	gfjdgjgldfjgldjljk



```
MV5000-R7.1 RC /AA05 FRA
Site: 001-SITE LOC
06/05/20 14:52:26
* DIRECTORY : PICTURE SERVER IN SERVICE*
29/04/20 14:20:45
*******PTx:   0-00-        **IN SERVICE**
29/04/20 14:20:45
* HARDWARE STATE : LEVEL   0           *
```

Subscription 6000

Telephony service>Subscribers>Subscriptions>Characteristics (1.2.3)

By directory number 6000

Number	Label	Programming
12		THIS KEY IS NOT PROGRAMMED
13	aa	MONITORING YOUR NUMBER 6001
14		THIS KEY IS NOT PROGRAMMED
15		THIS KEY IS NOT PROGRAMMED
16		THIS KEY IS NOT PROGRAMMED
17		THIS KEY IS NOT PROGRAMMED
18		THIS KEY IS NOT PROGRAMMED
19		THIS KEY IS NOT PROGRAMMED
🔒 20	LABEL1	XML KEY: LABEL1
21		THIS KEY IS NOT PROGRAMMED
22		THIS KEY IS NOT PROGRAMMED
23		THIS KEY IS NOT PROGRAMMED
24		THIS KEY IS NOT PROGRAMMED
25		THIS KEY IS NOT PROGRAMMED
26		THIS KEY IS NOT PROGRAMMED
27		THIS KEY IS NOT PROGRAMMED

Number assigned to key: 6000

Programming type: Monitoring your number (CCO)

Protected key: □

Associated label: cco1

Programming validation

3.5.3 PICTURE PARAMETERS

Menu **Telephony service>Subscribers>Terminals and applications>Pictures settings** is used to activate internal picture management. They are available in a disk storage area.

Refer to the document Pictures management: Operating manual.

3.5.4 PICTURES OF SUBSCRIBERS

This function must be activated from Menu **Telephony service>Subscribers>Terminals applications> Pictures of subscribers.**

Refer to the document “Pictures management”.

3.5.5 BLUSTAR

Menu **Telephony service>Subscribers>Terminals and applications> BluStar** consists of 3 tabs.

It is used to configure BluStar applications: 8000i, BluStar for PC and BluStar Mobile.

3.5.5.1 *Blustar tab*

Blustar security advanced controls:

- IVB authentication, forwarding, DND: the checkbox is used to activate the authentication of terminal 8000i on IVB, forwarding and Do not Disturb.

3.5.5.2 *Blustar PC tab*

This tab is used to configure the deployment of BluStar for PC:

- Defining the list of BluStar for PC users authorised to use video.
- If necessary, modifying some of the application's configuration file parameters.

The use of this tab is described in detail in the BluStar for PC installation manual – Blustar Mobile tab.

This tab is used to configure the deployment of BluStar for Ipad/Iphone:

- Defining the list of iPad and iPhone users to whom an e-mail will be sent to enable them download the BluStar application
- Managing the users by activating the e-mail transmission function or exporting the configuration files for each subscriber, thus allowing manual transmission of the configuration file
- If necessary, modifying some of the application's configuration file parameters.

3.5.6 SOFTWARE

Menu **Telephony Service>Subscribers>Terminals and applications>Software**

This menu allows you to manage the OMM_SIP software component.

SOFTWARE LIST

The menu indicates the current release of the software if this software is managed.

The software will be taken into account and downloaded next time the iPbx is updated from REPOSITORY.

See **SYSTEM>Software maintenance>Upgrade**.

If unselected, the software is not downloaded and thus reduces the downloading time and the occupied disk space~~.~~

Any modification of the choice of software must be confirmed with the VALIDATION button.

Unselected software components are deleted from the iPbx.

3.5.7 APPLICATIONS

3.5.7.1 *MiCollab*

⚠ **IMPORTANT NOTE: In MiVoice 5000 Cluster configuration, this menu is masked on a Node as this feature is managed on the cluster server and then replicated on all the Nodes connected to this Cluster Server.**

Menu **Telephony service>Subscribers>Terminals and applications>MiCollab** consists of 3 tabs:

- Connection tab
- Roles tab
- Realignment errors tab

Connection tab

This tab is used to define the parameters for connecting to the MiCollab server. This tab also allows immediate synchronisation to this server.

By default, the box is not ticked and no other line is displayed.

If the box is ticked, different fields are proposed, enabling MiVoice 5000 to manage MiCollab server updates:

- - main IP address: MiCollab server IP address (if the syntax is incorrect, an error message is displayed)
- - login: User connection login between MiVoice 5000 and Micollab. This value is not modifiable.
- - password: Password to be defined for the previous connection
- - Windows login for authentication: activating or not activating SSO mode for authenticating Micollab users
- - daily realignment (hh :mm): Field used to define the realignment time-stamping of MiCollab subscriber characteristics updates. Deafult value is 02:59 a.m.
- - last realignment on XX/XX/XXXX at HH.MM: information field indicating the date of last successful realignment.
- Immediate realignment button: button used to start immediate realignment of the MiCollab subscriber update characteristics.

During the realignment phase, a line is displayed to view the progress of the realignment. This line is refreshed every 10 seconds.

The realignment phase may be interrupted by clicking the **Stop realignment** button.

Roles tab

This tab is used to see the different fields, by column, of the role configuration made for MiCollab users.

Index: index value of the role in question.

Label: label of the role stored in UTF8 format but displayed in ASCII format;

Desktop, Softphone columns: a cross indicates whether the items are concerned.

DeskTop refers to the telephone terminal as opposed to the "softphone".

UCA, **AWV, NPM and MBG**: a cross indicates whether the services are concerned.

Realignment errors tab

Directory: subscriber number.

Name: subscriber name.

Role: subscriber's role label.

Mail: a cross indicates whether the e-mail address is defined in the subscriber's LDAP directory.

Login: a cross indicates whether a login is defined in the subscriber's LDAP directory.

Action: type of action required for the MICollab user (creation, modification, change of role, and deletion).

Error: error message received from the MiCollab server (101 characters max.)

3.5.7.2 *MBG*

This menu is for managing terminals 6xxxi with the Remote Worker feature.

Refer to the document R**emote Worker via MBG** on the Mitel Document Center.

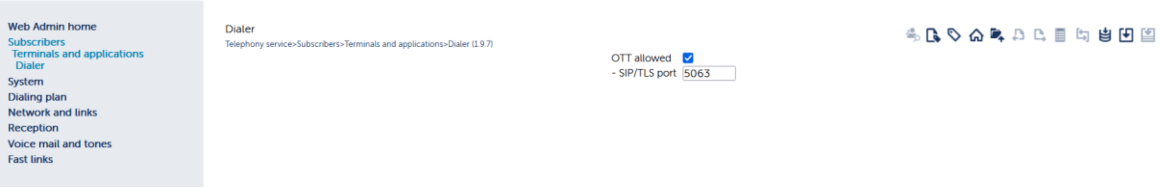
3.5.7.3 *CloudLink*

Refer to the document **CloudLink - Integration with MiVoice 5000** on the Mitel Document Center.

3.5.8 DIALER

Menu **Telephony service>Subscribers>Terminals and applications>Dialer**.

This menu, available from R8.2 SP1, manages the activation of the Mitel Dialer OTT. For more information on the configuration, refer to the document **MiVoice 5000 Server – Subscribers in OTT mode through Embedded SBC**.



Dialer

Telephony service>Subscribers>Terminals and applications>Dialer (1.9.7)

OTT allowed ☑

- SIP/TLS port 5063

OTT ALLOWED

Checkbox. Allos the use of the Mitel Dialer OTT.

SIP/TLS PORT

Field to fill. Only appears if the OTT allowed checkbox is checked.

Default port: 5063

3.6 HOTEL/MOTEL MANAGEMENT

Note: This management function of MiVoice 5000 Web Admin is specifically meant for managing hotel rooms. It is not applicable to other types of establishments with an MiVoice 500 series system.

Menu **SUBSCRIBERS>Hotel management**.

Hotel management is used to configure:

- Occupied rooms
- Unoccupied rooms.

HOTEL / MOTEL MANAGEMENT

If the box is ticked, it becomes possible to configure both types of rooms.

3.6.1 OCCUPIED ROOM

DAY CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

Select a category. The authorisations and restrictions associated with each category depend on the configuration in call distribution management.

NIGHT CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

Select a category. The authorisations and restrictions associated with each category depend on the configuration in call distribution management.

Note: The room open/close functions are managed from the hotel server, available either from the ATDC or via the maintenance set.
The status room occupied / unoccupied depends on HOTEL/MOTEL MANAGEMENT.

3.6.2 UNOCCUPIED ROOM

This screen is accessible via **SUBSCRIBERS>Hotel management**.

DAY CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

Select a category. The authorisations and restrictions associated with each category depend on the configuration in call distribution management.

NIGHT CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

Select a category. The authorisations and restrictions associated with each category depend on the configuration in call distribution management.

Note: The room open/close functions are managed from the hotel server, available either from the ATDC or via the maintenance set.
The status room occupied / unoccupied depends on HOTEL/MOTEL MANAGEMENT.

3.7 HUNT GROUPS

Menu **SUBSCRIBERS>Hunt groups and companies**

A **hunt group** is a set of subscribers grouped together under a common directory number (hunt group directory number) through which they can be called.

The system offers the possibility to create hunt groups distributed differently according to the type of system used.

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.).

i2052 VOIP terminals can be part of a “fixed” hunt group or “cyclic” hunt group, but not a “general call” hunt group (see the definition of hunt group types in the definition of hunt group parameters).

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).

As of R8.2, subscribers who are part of a hunt group can view hunt group calls in the call log. Hunt group calls are displayed with the 👥 icon.

For multi-company operation, the sets must belong to the same company or company 0.

The following functions are available from the menu **SUBSCRIBERS>Hunt groups and companies**:

- Hunt groups (parameters, definition and display)
- Teleconference
- Intercom groups
- Announcement list
- Announcement code list (in a multi-company configuration only)
- Multi-company management (in a multi-company configuration only)

3.7.1 HUNT GROUP PARAMETERS

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Settings.**

This menu is used to define hunt group-related authorisations and the duration of the different ring tones (timeouts) during calls to hunt groups.

ALLOW CALL PICK-UP

If you tick this box, a call intended for a group of sets can be intercepted by dialling the interception code, followed by the group directory number (when the call is intended for the group, and not for a particular set in the group).

This parameter is required in order to put a general call GROUP into service.

ALLOW CALL WAITING BEEPS

If you tick this box, the call waiting beep signal is authorised for the hunt group.

ALLOW NO ACTIVE TERMINAL IN THE HUNTING GROUP

If the box is ticked, the last active terminal in the group may be muted.

Also allows login/logout of a terminal belonging to a group (if it has the right to dislodge itself). May be applied to all groups to which it belongs according to the setting "Ready/Not ready applied to".

DND APPLICABLE TO HUNT GROUP CALLS

This setting is visible if the **Allow no active terminal in the hunting group** box is ticked.

If this box is ticked, it allows “Do Not Disturb” mode to be applied to hunt group members during a hunt group call.

Note : For Dual Homing, if a suscriber in DND mode swiches to its backup site, the DND mode is disabled.

SEND IDENT.

If the caller belongs to a hunt group, the send ID option is as follows:

- NUMBER OF TERMINAL: The caller's number, seen by the called party, is the caller's phone number.
- NUMBER OF HUNT GROUP: The caller's number, seen by the called party, is the hunt group head number.

LAST REDIRECTED DEVICE CSTA OR REDIRECTED NUMBER DISPLAYED

This parameter is mainly used for cascade forwarding while connecting CSTA servers.

- HUNT GROUP/1**ST REDIREC**:
  - HUNT GROUP applies to the CSTA field Last Redirected Device.
  - 1ST REDIREC applies to the displayed re-routed number.
- LAST REDIRECTED BEF.GRP This choice applies to the CSTA field Last Redirected Device and to the displayed re-routed number.
- CALLING NUMBER -TERM.S0: This choice applies to the specific case of S0 terminals, for the CSTA field Last Redirected Device and for re-routed number.

Table 2: Summary of "displays" according to options

OPTIONS	CSTA	TERMINALS	S0
	LAST REDIRECTED DEVICE	REDIRECTED NUMBER DISPLAYED	NUMBER DISPLAYED CALLER / [REROUTED]
HUNT GROUP/1ST REDIREC.	HUNT GROUP NO.	1ST REDIREC. NO.	LAST REDIRECTED NO. BEF GRP / [HUNT GROUP NO.]
LAST REDIRECTED BEF.GRP	LAST REDIRECTED NO. BEF GRP	LAST REDIRECTED NO. BEF GRP	CALLING NO. / [LAST REDIRECTED NO. BEF GRP]
CALLING NUMBER -TERM.S0	HUNT GROUP NO.	1ST REDIREC. NO.	CALLING NO. / [HUNT GROUP NO.]

Behaviour of different terminals according to options

Assuming that: **X** calls **Terminal 1** ….. forwarded to **Terminal D** forwarded to **Hunt group G**.

On the terminals (except terminal S0) are displayed the calling number and a forwarded terminal number (which may be the first or last number, or the hunt group number).

For a terminal S0, this depends on the terminal; on standard terminals, only the calling number is displayed. However, the interface allows the forwarded terminal to be sent.

For CSTA, information is displayed on the hunt group terminal according to type, and information is sent to the CSTA field Last redirected device.

	CYCLIC/FIXED HUNT GROUP/...			GENERAL CALL GROUP	
OPTIONS	HUNT GROUP/1ST REDIREC.	LAST REDIRECTED BEF.GRP	CALLING NUMBER -TERM.S0	HUNT GROUP/1ST REDIREC. CALLING NUMBER TERM.S0	LAST REDIRECTED BEF.GRP
DS	TERMINAL 1	TERMINAL D	TERMINAL 1	TERMINAL 1	TERMINAL D
DS MT	TERMINAL 1	TERMINAL D	TERMINAL 1	TERMINAL 1	TERMINAL D
SIP	TERMINAL 1	TERMINAL D	TERMINAL 1	TERMINAL 1	TERMINAL D
53XX	TERMINAL 1	TERMINAL D	TERMINAL 1	TERMINAL 1	TERMINAL D
ASSOCIATED	TERMINAL 1	TERMINAL D	TERMINAL 1	NA	NA
S0	CALLING = D, REDIRECT = G	CALLING = X, REDIRECT = D	CALLING = X, REDIRECT = G	NA	NA
TAPI	IDEM SUPERVISED TERMINAL	IDEM SUPERVISED TERMINAL	IDEM SUPERVISED TERMINAL	IDEM SUPERVISED TERMINAL*	IDEM SUPERVISED TERMINAL*
VTI-XML CTI	IDEM SUPERVISED TERMINAL	IDEM SUPERVISED TERMINAL	IDEM SUPERVISED TERMINAL	IDEM SUPERVISED TERMINAL *1	IDEM SUPERVISED TERMINAL *1
VTI/ XML VOIP	TERMINAL 1	TERMINAL D	TERMINAL 1	NA	NA
CSTA	HUNT GROUP G	TERMINAL D	HUNT GROUP G	NA	NA

RETURN TO WORK:

- Length of identification code

This field is used to define the length of the work ID code for the hunt group terminal.

  - Default value: 6
  - Maximum value: 19 (limit imposed by charging)

The user dials a special prefix followed by the ID number allowing group calls to be processed by activating or deactivating one of the hunt group terminals. This number may be used to create an ID (signature).

- ACTIVATION INTO GROUP

Work start indicator with activation of the terminal in the hunt group.

  - Box not ticked: when "work start" is activated, a work ID ticket (service ticket) is issued. No activation of the terminal in the hunt group, nor automatic reinsertion into the hunt group when DND mode is used.

Box ticked: When when "work start" is activated, a work ID ticket (service ticket) is issued, and the terminal is activated in the hunt group by generating the ticket activation.

This setting also applies when DND mode is activated. When a subscriber in a hunt group disables DND mode, they are automatically reintegrated into the hunt group.

Note: The end of "work start" also generates a ticket and sets the terminal to standby mode in the hunt group.

READY/NOT READY APPLIED TO

Indicates terminal-based end of work in the hunt group.

LINE: end of work for the line corresponding to the directory number, for a multi-line terminal. Ready/Not ready applies only to the line concerned.

ALL LINES end of work for all the directory numbers of a multi-line terminal. Ready/Not ready applies to all lines and therefore to all groups.

Note: If a subscriber belongs to more than one group and the settings ALLOW LAST ACTIVE WITHDRAWAL and END OF WORK APPLIED TO ALL LINES are ticked, pressing one of the keys of any of the groups, or by code (#48 to deactivate and *48 to reactivate) or from Menu Subscribers>Subscriptions>Characteristics **- Functions tab,** deactivates or reactivates it in all the groups even if it is the last active terminal in any of the groups to which it belongs**.**

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 sets. This corresponds to the time during which a set in the group rings before the next set rings.

EXTENSION IDLE DELAY

Time-out fixed at 2 seconds. This corresponds to the pause between two calls for the same set in a group.

WAIT BEFORE FWD TO OP. CONS.

Time-out fixed at 40 seconds. In the end, the call is taken by the attendant console.

WAITING TIME BEFORE ASSISTANCE

Time-out fixed at 35 seconds. In the end, the call is routed to the assistance number (defined in "Hunt group characteristics”).

WAIT TIME BEFORE ALERTING

Timeout not defined.

% WAITING CALLS

100 % by default.

3.7.2 HUNT GROUP DEFINITION

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Characteristics** tab.

Note: The hunt groups must first be created as HUNT GROUP or SUPER HUNT GROUP type subscribers (Menu SUBSCRIBERS>Subscriptions>create).
The terminal ring time and hunt group global ring duration are defined in Menu SYSTEM>Expert>Time-out.

- If the hunt group selected is a SUPER HUNT GROUP, see Section *3.7.4*.
- If the selected hunt group is of HUNT GROUP type, the parameters displayed are indicated below.

In both cases, the subscribers that make up the hunt group must be declared in the **Composition** tab of Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups**.

After a hunt group is selected by its directory number, the screen displays all the fields required to define a hunt group:

DIRECTORY NUMBER

Hunt group directory number. This must be included in the range of internal numbers and be of the same length (2 to 6 digits).

DID DIRECOTRY NUMBER PLAN 1

This field is reserved for the DID directory number plan.

Enter the operator’s MCDU number within the first plan which will reach the hunt group directory number (DID group relation on the first plan).

HUNT GROUP TYPE

CYCLIC	FIXED HEAD	GENERAL CALL	PAUSE TIME	EMPTY

The hunt group may be **cyclic**: calls are successively routed to each of the terminals in the hunt group in the order in which they were declared in the hunt group. Each new call is routed to the next free set (after the previous call).

The hunt group may be **fixed**: calls are routed on a priority basis, to the first terminal in the group (called group head set). If the first set is busy or is not answering, the second then rings, and so on.

The group may be **general call**: in this case, all the terminals ring simultaneously when an internal or external call (DID or DIR) is made and after 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 checkbox of the parameter ALLOW CALL PICK-UP in Menu **SUBSCRIBERS>Hunt groups and companies>Settings**.

The hunt group may be a longest **idle time** hunt group: in this case, the terminal that rings is the one that registers the least communication time in the hunt group.

The hunt group may be a **super hunt group**: see description of parameters in § *3.7.4*.

The hunt group may be **empty**: in this case, the hunt group does not contain any subscriber.

Note: The "Type of hunt group" column will only be displayed if a directory number had previously been entered on top of the screen.

HUNT GROUP NAME

Information field indicating the hunt group name: SUBSCRIBER + subscriber number.

HUNT GROUP NATURE

TELEPHONY	ISDN DATA	DATA

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 DISTR.

NO by default.

Select YES to have a ticket (ACD 7403 statistics) on the broadcast of an announcement before it reaches the subscriber.

COMPANY

Name of the company to which the group belongs (by default, the hunt group belongs to the company of the first subscriber of the group).

DEPARTMENT

Name of the department to which the group belongs (by default, the hunt group belongs to the company of the first subscriber of the group).

BACKUP SITE

Name of the site on which the displayed hunt groups are backed up.

……….	No selection criteria on the backup site.
Site Name	Only the hunt groups backed up on the site indicated are displayed.

The dropdown list contains all the sites of the multi-site used as backup to at least one secured hunt groups.

⚠ **WARNING:** **For the hunt groups to be properly backed up, the backup site must also be running with R8.2.**

DAY CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

Possible for the delayed ringing hunt group after announcement message, if the category features “DELAYED RINGING AFTER ANN. MSG”.

NIGHT CATEGORY

INTERNATIONAL	INTERNAL	PRIVATE	ADDITIONAL	NATIONAL	REGIONAL

Idem day category. Switching between DAY/NIGHT is carried out by the barring calendar.

CALL WAITING

ACCEPT AND BEEP	FORWARD->ON CONSOLE	REFUSED

Indicates the procedure for handling an external incoming call when the hunt group is busy:

ACCEPT AND BEEP Normal procedure: the call is placed on hold, and the user is advised. After the time-out, the call is forwarded to call distribution. To choose a time-out, see Hunt group parameters>Timeout management.

FORWARD->ON CONSOLE The call is systematically forwarded to the attendant console.

REFUSED The calling party receives the busy tone.

Note: A multi-CCO subscription is only busy if all CCOs are occupied.
To change this status, set "MULTI-KEY EXT. SEEN BUSY ON 1st CALL" to YES in Menu SUBSCRIBERS>Rights>General settings.
See also the section Digital Extension Characteristics: "BUSY FOR HUNT GROUP ON 1ST CALL"

CALL FORWARDING PROTECTION

Click YES to prohibit forwarding to this hunt group.

INTRUSION ALLOWED

Click YES to allow queuing in a super hunt group, with busy hunt group.

RETURN TO CONSOLE ON SPEC. TIME-OUT

If you enter **NO** in case of no answer by the hunt group: return to the Attendant Console (ATDC) is subject to a standard time-out of 40 seconds (see Hunt groups>Hunt group settings).

If you enter YES, the standard time-out value for return to the Attendant Console (ATDC) is replaced by the SPEC. TIMEOUT: REROUT. TO CONSOLE (see SYSTEM>Expert>Time-out).

Note: If the OP GP is absent from the call distribution, the call is returned on special reduced day TIME-OUT.

EXTERNAL FORWARDING ALLOWED

Select YES to enable the “Divert” function for the terminal hunt groups (especially if empty hunt groups used by a call centre are declared).

TRANSFER BEFORE ANSWER ALLOWED

Select YES to allow switchover to help hunt group.

PREDEFINED FORWARDING

Internal or external number to which the hunt group is forwarded: this number contains 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 by a code + hunt group number.

Note: To activate hunt group forwarding, the parameter Predefined forwarding must be enabled (ACTIVE) in the Forward tab of Menu SUBSCRIBERS>Hunt groups and companies>Hunt group>Characteristics (this terminal may or may not belong to the hunt group and must allow “assistant/manager filtering”).

ASSISTANCE NUMBER

Number to which the call will routed after the hunt group response timeout.

GLOBAL RINGING DURATION (SEC)
EXTENSION RINGING DURATION (SEC)
EXTENSION IDLE DELAY (SEC)

These 3 parameters correspond to the timeouts which must be configured according to the needs of the hunt group. Some durations (in seconds) are proposed by default.

WAIT BEFORE FWD TO OP. CONS. (SEC)

Enter a value in seconds, below 3600.

Note: This value, which is used to configure the return to console time-out, is only valid for an EMPTY hunt group.

DELAY BEFORE MUTUAL AID (SEC)
DELAY BEFORE SIGNALING (SEC)

These 2 parameters correspond to the timeouts which must be configured according to the needs of the hunt group. Some durations (in seconds) are proposed by default.

% WAITING CALLS

This parameter (100% by default) indicates the maximum percentage of waiting calls for the hunt group.

3.7.3 HUNT GROUP COMPONENTS

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Composition** tab.

CONSTITUENT DIRECTORY NUMBERS

SUBSCRIBER 1 ……….SUBSCRIBER 100

Directory numbers (2 to 6 digits) of the sets which belong to the hunt group.

The limit is 100 subscribers maximum.

3.7.4 SUPER HUNT GROUP DEFINITION

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Characteristics** tab.

After a hunt group is selected by its directory number, the screen displays all the fields required to define a hunt group.

The description of the general parameters for defining a super group is the same as the one given in the hunt group definition (see Section *3.7.2*).

3.7.5 SUPER HUNT GROUP COMPONENTS

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Composition** tab.

The super group composition parameters are different from those of a hunt group.

The following rules apply to the elements making up a super hunt group:

- The elements making up a super group can only be “cyclic", "fixed head” or "longest idle time" HUNT GROUP type subscriptions or multi_CCO subscriptions (at least one key must be programmed).
- None of them must 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 elements making up 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)

- subscribers 1 to 4

  Directory number.

Note: If the corresponding subscription does not respect the rules indicated above, an error message "incorrect directory number” is 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.

CHANGE LEVEL CRITERION

BUSY SETS Move to level N+1 if all the level N sets are busy.

MAX TIME IN QUEUE 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.

MAXIMUM TIME IN QUEUE (SEC)

This parameter is only displayed if the change level criterion is set to MAX TIME IN QUEUE.

Enter a value in seconds.

3.7.6 DIRECTORY INFORMATION (HUNT GROUP AND SUPER HUNT GROUP)

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Directory** tab

Note: Identical fields for the hunt groups and super hunt groups

This command is used to modify the directory record of a hunt group.

Select the directory number in the **BY DIRECTORY NUMBER** field.

Directory number.

The hunt group's directory record is displayed.

See the description of a directory record in Section *3.3.3.2.1*.

3.7.7 DISPLAY HUNT GROUPS

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Display.**

This menu is used to display all the hunt groups / super hunt groups associated with the following fields:

UNUSED HUNT GROUPS

Shows the number of unused hunt groups.

DIRECTORY

Indicates the hunt group directory number.

DID

Indicates the hunt group DID directory number, if need be.

TYPE

Indicates the type of hunt group: CYCLIC – FIXED HEAD – GENERAL CALL – PAUSE TIME – SUPER GROUP.

HUNT GROUP NAME

Indicates the hunt group name.

NUMBER

Indicates the number of extensions in hunt group.

Note: For a MiVoice 5000 Server, this menu is preceded by a selection menu used to limit the display length.

3.7.8 ACTIVATING FORWARDING FOR A HUNT GROUP

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Forwards** tab

PREDEFINED FORWARD

ACTIVATE

This selection activates forwarding for the hunt group defined in the Predefined forward field of the **Characteristics** tab in Menu **SUBSCRIBERS>Hunt groups and companies>Hunt group>Characteristics**.

NOT ACTIVE

Deactivates the above-mentioned forwarding.

TO NUMBER

Non-modifiable field which gives the number to which the hunt group is forwarded.

3.7.9 DISPLAYING A HUNT GROUP'S FUNCTIONS

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Functions** tab

This tab is used to see the function of each hunt group.

When the hunt group in question is selected, the links to all the management menus involving this hunt group are proposed.

Example:

After the directory number is selected (example `500`):

The following is displayed:

```
Belongs to the super hunt group 600
Predefined forward for 200
```

3.7.10 DISPLAYING THE STATUSES OF HUNT GROUP TERMINALS

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Characteristics** – **Statuses** tab

The **Statuses** tab is only a display menu used to view the status of the terminals that make up the hunt group as well as the dynamic characteristics of the hunt group.

Dynamic characteristics of the hunt group

Overload indicator:

- no overload, no waiting call
- 1 = overload, no waiting call
- 2 = no overload, waiting calls
- 3 = overload, waiting calls

The notion of overload means that a call has exceeded an overload threshold (timeout).

Overload level 1, if a call has waited longer than a given time.

Overload Level 2, if the total number of calls waiting on the hunt group and calls waiting on the terminals, on an individual basis, is equal to the maximum number of admissible number of waiting calls (busy group 2).

Number of terminals / number of calls:

- Number of terminals declared in the hunt group, no matter their status (active, in standby mode, in permanent off-hook position or out of service).
- Number of calls with assistance: if some calls have been waiting for more than a given period, these calls are returned in chronological order to an "assistance" hunt group (if it exists).

Time:

The longest wait time for a call on the queue and the wait time for a call which has the longest ringing time.

Status of hunt group terminals

The number of terminals per hunt group varies according to hunt group type; the maximum number of terminals displayed is 100.

Directory:

Field with maximum 10 numeric characters, representing the extension's directory number.

Name:

Field with maximum 30 alphanumeric characters, representing the name of the subscription declared on the directory server.

Status:

The different dynamic statuses of a terminal in the hunt group are:

- Unknown: if the status returned is different from those indicated below.
- Active and Free: terminal is active and free in the hunt group.

- Active and Busy: terminal is active and busy in the hunt group.
- Stand-By and Free: terminal is in hunt group standby mode and free.
- Stand-By and Busy: terminal is in hunt group standby mode and busy.
- Permanent Off-Hook or Not Connected: terminal is in standby mode and not connected or in perm. off-hook condition (disconnected); the terminal is seen as not active in the hunt group.
- Out of service: set out of service.
- Idle and Free: active terminal in the hunt group is in "trade-union-approved break" (time of inactivity between 2 calls on the same terminal) and free.
- Idle and Busy: active terminal in the hunt group is in "trade-union-approved break, but busy" (personal call).

Note: If no answer is returned during a hunt group status request, the line "Impossible display of states" is displayed in the Status tab.

3.7.11 ANNOUNCEMENT LIST

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Announcement list**

An announcement is a message broadcast to a set of digital terminals 6xxxi fitted with loudspeakers. The requested set of extensions constitutes a group known as an "announcement list" (speaker paging calls).

Mitel-series devices allow the definition of up to 40 announcement lists on loudspeaker.

Each list may contain:

- Either up to 32 subscriptions assigned to fixed digital sets (simple list)
- Or up to 4 announcement lists on loudspeaker within the limit of 32 subscriptions assigned to the terminals.
- Announcement lists 0, 1 and 2 are accessible via the prefixes defined in the dialling plan for features:
- CALL ANNOUNCEMENT LIST 0
- CALL ANNOUNCEMENT LIST 1
- CALL ANNOUNCEMENT LIST 2

Note: Only digital sets with loud speakers can be declared in an announcement list.

An extension can appear on a number of single lists, but all the extensions declared in a list must belong to the same company/department.

By default, the sets are not rung before switchover to the broadcast function (however, this configuration can be modified using table 56, parameter 47).

Menu **SUBSCRIBERS>Hunt groups and companies>Announcement list** is used to choose and summarise all the lists defined already, in the following format:

- LIST NUMBER
- LIST NAME (a declared list must always have a name)
- NO. DNs (the number of users in the list) LIST NOS.
- (the numbers of the lists which are made up of a single list)
- NO. CODES (number of announcement codes allowed to access this list. Update only exists in multi-company configuration).

ANNOUNCEM. HOLD ON SPEAKER AT PICKING-UP

Indicates that the announcement remains on loudspeaker

- Box not ticked: announcement does not remain upon off-hook.
- Box ticked: announcement remains on loudspeaker upon off-hook.

IF CREATION, TYPE OF LIST

SINGLE **COMPOSED**

SINGLE	Selection of single list by list number
COMPOSED	Selection of composed list (composed of x single lists) by list number.

LIST

Clicking a list opens the following fields:

NAME

List name (mandatory).

LIST OF SUBSCRIBERS IN ANNOUNCE.

Subscriber directory number (lines 1 to 32).

Note: A new subscriber cannot be entered if this causes an overflow of the number of subscribers in the list. The number of the composed list generating the refusal is then given in an error message.

3.7.12 ANNOUNCEMENT LIST CODE

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Announcement list code**

This command is used to display all the company/department pairs using an announcement list code.

This screen is used to select announcement list rights.

SELECTION BY NAME

Announcement list code, previously declared in the menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Announcement list code names**.

When **Select the item** is confirmed, the next screen displays the users of an announcement list code. An announcement code contains a set of announcement lists.

An announcement code cannot belong to more than 15 lists.

3.7.13 INTERCOM GROUPS

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Intercom groups**

3.7.13.1 *Names*

Menu **SUBSCRIBERS>Hunt groups and companies>Hunt groups>Intercom groups>Names**

This screen is used to display and modify intercom group names.

- This name can contain up to 16 characters.
- 2000 intercom groups can be defined.

3.7.13.2 *Broadcast*

- This menu is used to optimise the intercom group (or ICG) range.
- BY ITS NAME
- Choose the group you wish to optimise.
- BROADCAST PRIORITY 1
- Eight priority options, from 1 to 8. The data specific to this group is broadcast based solely on the choices made here by the user.
- Options: LOCAL SITE, LOCAL CENTRE, CENTRE EXCEPT SITE, ALL CENTRES, SITE BASED, CENTRE BASED
- SITE BASIS
- Choose the site containing some subscribers included in the ICG group.
- NODE NUMBER
- In a standard, multi-site MIVOICE 5000 system, the node number is 2.

3.7.13.3 *Display*

Menu

SUBSCRIBERS>Hunt groups and companies>Hunt groups>Intercom groups>Display

This screen is used to select an intercom group and, possibly, a sub-group of subscribers belonging to this group.

When **Select the item** is validated, the next screen displays the users declared in the intercom groups.

3.8 MULTI-COMPANY

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company**

3.8.1 DEFINITIONS

A MULTI-COMPANY configuration allows several companies to share the same iPBX (or set of iPBXs in case of multi-site configuration). Each company may have its own characteristics (speed dial, incoming and outgoing trunk groups, answering service and operators).

The table below gives the limits of multi-company management during parameter definition:

	MITEL RANGE (INCLUDING MIVOICE 5000 SERVER)
1 - Companies	32
2 - Departments per company	32
3 - Routing codes	16
4 - Announcement list codes	16
5 – Company profiles	16
6 - Definition of parameters for each company/department pair	

To access the multi-company configuration management menu, select the menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management**.

Note: When the Multi-company Management option of Menu SYSTEM>Configuration>Services is validated, this menu entitled: "Multi-company management" appears on the MiVoice 5000 Web Admin screen.

Multi-company management implies defining the following parameters:

- General settings
- Company names
- Department names
- Routing code names
- Broadcast code names
- Company profile names
- Company/department parameters

3.8.2 GENERAL SETTINGS

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management**.

This screen is used to define the level of communication between the different companies sharing the same equipment: telephony only, data only, or both.

3.8.3 COMPANY NAMES

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Company names**.

This menu is used to declare different companies, and assign them a name.

COMPANY NUMBER

The number of the company. On system start-up, only CMPNY.0 is created (do not modify this field).

NAMED

The name of the company: CMPNY.0 for company no. 0 (this name cannot be used for a new company).

This name can contain up to 16 characters.

For a configuration with two or three companies, CMPNY.0 is the central company (e.g. general services): CMPNY.0 has no prohibition towards other companies.

Note: You must first assign a number to the company so you can assign a name. You must delete the company name before the company number.
A name can only be deleted if the company is no longer used and if no department has been declared within it.

3.8.4 DEPARTMENT NAMES

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Department names**.

This screen is used to define the services that will be provided for each company identified.

DEPARTMENT NUMBER

Department number. On system start-up, only department 0 of company CMPNY.0 is created.

NAMED

The name of the department: this department is named DEPT.0. This name can contain up to 16 characters.

Note: Two different companies can use the same department names. You must assign a number to the department before a name. You can only delete a name provided that the department is no longer being used and has no specific parameter defined on it. You can read the names of other companies' departments.

INDIVIDUAL COMPANIES (Hotel configuration, for example).
You can define individual groups between which internal calls are not allowed to be set up.
To prevent a terminal from calling another terminal in the same department, create a DEPARTMENT NUMBER between 90 and 94 for the COMPANY: a HOTEL for example.
A parameter in menu Rights / Subscribers miscellaneous parameters is used to authorise calls between two terminals, if the calls are set up by an operator.

3.8.5 ROUTING CODE NAMES

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Routing code names**.

The routing code enables the various companies to access the PSTN, using the same prefix (0) on their individual trunk groups.

It is also possible to assign a routing code to a particular department in a company, enabling the department to access a particular trunk group.

NUMBER (1 TO 16)

Routing code names (8 characters maximum for 16 codes).

On system start-up, only the name Code 0 is created for number 1 (do not modify this field).

Note: To make it easier to monitor operations, we recommend that you enter the company name or department name as CODE NAME. A code name can only be deleted if there is no longer any forward declared for the code to be deleted.

3.8.6 BROADCAST CODE NAMES

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Name of broadcast codes list**.

This screen is used to define the announcement code names that will be assigned to each company / department pair declared for the announcement list call (see **DIALLING PLAN>User dialling plan>Access to features**).

NUMBER (1 TO 16)

Names of announcement codes (maximum 8 characters).

On system start-up, only the name Code 0 is created for number 1 (do not modify this field).

Note: To simplify operation administration, it is advisable to enter the name of the company or the name of department for the code name.
A code name can only be deleted if no broadcast is declared on that code.

3.8.7 COMPANY PROFILE NAMES

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Company profile names**.

This screen is used to define the company profile names required to manage wireless TDM (DECT/DAS) accesses.

NUMBER (1 TO 16)

Names of company profiles (maximum 8 characters).

On system start-up, only the name PROFS0 is created for number 1 (do not modify this field).

Note: To simplify operation administration, it is advisable to enter the name of the company or the name of department for the profile name.
A profile name can be deleted subject to the following conditions. There should be:
• no more base station trunk assigned to the company profile,

• no more area profile defined for this company profile, • no more laptop declared in a company/department using this company profile name.

3.8.8 COMPANY/DEPARTMENT PARAMETERS

Menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Company/department settings**.

This screen is used to select the company for which the service parameters must be defined.

COMPANY NAME

CMPNY.0	• • • • •

Select a specific company or all the companies • • • • • . If you have already created other company names, these appear in this field.

Only company CMPNY.0 exists on system start-up in multi-company configuration.

If you select • • • • •, you can modify the parameters of all the companies.

Click **Select the item**.

This screen is used to define the parameters of the departments of one or more companies (for multi-company configuration).

By default, code 0 is assigned to all company/department pairs for routing the 3 outgoing traffic flows.

By default, call distribution service 0 is assigned to all company/department pairs for routing the 3 incoming traffic flows.

AND OF DEPARTMENT

DEPT 0	• • • • •

Select one or more departments • • • • • If you have already created other departments, they will appear in this selection.

Only department DEPT.0 exists on system start-up in a multi-company configuration.

If you select • • • • •, you can modify the parameters of all the departments in a single specified company.

Example:

The system has several company/department pairs with a number of identical parameters (routing code and call distribution service). Common parameters are assigned to these departments first, then specific parameters are assigned to the other departments.

PSTN – TL ROUTE CODE

Code 0 is assigned by default. If you have already created code names, they appear in these selections.

ANNOUNCEMENT LIST CODE

Code 0 is assigned by default. If you have already created code names, they appear in these selections.

PSTN-VIP-TL-INTERNAL CALL DISTRIBUTION

Call distribution 0 is allocated by default. If you have already created call distribution names, they appear in these selections.

IMPORTANT: See definition "TRANSF. ACC. TO CALLED PTY COM-DEPT" in Menu NETWORK AND LINKS>Trunk group selection.

COMMON BELL DN

The common bell directory number can be assigned to an analogue device, with a directory number corresponding to the internal dialling plan.

In multi-company mode, the common bell must belong to the company selected, or company CMPNY 0. The other companies have their bell on an analogue device.

Note: The directory number of the common bell for each company must correspond to the operator forwarding set directory number (see Call distribution / Selection of operator service).

WIRELESS PROFILE

Profile name previously created in Company profile name in Multi-company management.

Note: The wireless profile is used for wireless management.

PSTN ACCESS BARRING CALENDAR NETWORK ACCESS

CAL.1 1

Select a calendar: by default, calendar CAL.1 is created. If you have created other calendar names, they appear in this field.

The barring calendar controls day and night categories, and day and night barring levels for each subscriber.

Reminder: The directory number of the common bell and the barring calendar are not assigned to all the departments in companies ****, but are assigned by the menu corresponding to each company/department.**

3.9 DEFINITION OF RIGHTS

Definition of rights basically concerns subscribers' general parameters, selection of categories, definition of features, and selection of TL class users.

3.9.1 GENERAL SETTINGS

General settings concern subscriber access rights, including in particular the functions available to the terminals, maintenance terminal functions, programming of data copying to the backup sites, ISDN settings and transfer authorisations.

Menu **SUBSCRIBERS>Rights>General settings**.

This menu is divided into 5 tabs:

3.9.1.1 *SSO tab*

LDAP

This section allows LDAP configuration for Single Sign-On (SSO) with both MiVoice 5000 Web Admin and MiVoice 5000 Easy Admin.

- **Server**: server name or IP address
- **Login**: LDAP directory login
- **Password**: LDAP directory password
- **Port**: port number assigned to LDAP access
  - Port 389 by default
  - Port 636 in secure mode
- **Enable TLS**: if checked (recommended), enables secure connection.
- **User attribute**: attribute used for searching in the LDAP/AD database

  Example: sAMAccountName: name of an account (e.g.: Dupontj)
- **DN base**: field for the **Distinguished Name** of the directory branch from which MiVoice 5000 Web Admin users are retrieved.

  It should at least correspond to the root of the directory. Otherwise, indicate a more specific branch.

OPENID CONNECT

This section allows OpenID Connect to be configured for Single Sign-On (SSO) on MiVoice 5000.

- Provider: dropdown list. Identity provider
  - Microsoft Entra ID: the service used for SSO is Microsoft Entra ID.
  - Google: the service used for SSO is Google.
  - Generic: the service used for SSO is a generic service, like Keycloak, ADFS, etc.

Note: For more information on configuring SSO on Microsoft Entra ID, please refer to Appendix 9.1 - Registering MiVoice 5000 PBX in Microsoft Azure.

Note: To use SSO, subscribers must have a valid mail address in their subscriber record.

- **(Client) application ID**: identity provider ID
- **(Tenant) directory ID**: client ID created on the service used for SSO
- **Client secret**: client password created on the service used for SSO

KERBEROS

This section allows Kerberos to be configured for Single Sign-On (SSO) on MiVoice 5000.

- **Domain controller name**: 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.

  Example: ControllerMachine Name.MyDomain.com

- **Default realm**: Input field (100 characters maximum). Domain name associated with the iPBX in the Active Directory configuration of the Kerberos module. This realm is the one specified by the browser client to reach the iPBX User Portal.

  Example: MyDomain.com

- **Keytab file import**: keytab file created on the domain controller. The **Browse** and **Download** buttons are used to locate and import the keytab file. This file is implicitly taken into account in the backup/restore mechanisms.

  Refer to section 9.4.1 to create this file.

SSO FOR USERS

Dropdown list. Selects the SSO mode to use between:

- LDAP
- OpenID Connect
- Kerberos

3.9.1.2 *Subscriber tab*

FORWARDING DEPTH ALLOWED

This parameter provides for cascade mode forwarding (maximum 3 forwarding operations).

By default, the device proposes 2 cascade operations (3 forwarding operations).

TEST ON ROUTED NUMBER

- Box ticked: the forwarded number is tested to check that the origin of the forwarded number is different from the number to which it is forwarded.
- Box not ticked: no test.

PERSONAL CALLS FORBIDDEN

When this box is ticked, personal calls are subject to forbidden numbers lists.

ABBREVIATED/SPECIAL NUMBERS FORBIDDEN

If this box is ticked, general abbreviated numbers are subject to forbidden numbers lists.

MULTI-KEY EXT. SEEN BUSY ON 1ST CALL

If the box is ticked, a subscription set to multi-CCO is always seen as busy when it is on call on a CCO, through the subscriptions monitoring it.

CONFIDENTIALITY ASSOCIATION

By default, the box is unticked.

A confidential association forbids any set in the association from entering an ongoing communication.

A non-confidential association allows you to join a conference by picking up a second terminal in the association.

This selection only applies to:

- A single-key>single-line association (for a multi-key>multi-line association, the association is automatically confidential)
- An association comprising only TDM terminals (an association with at least one IP terminal is automatically confidential)
- Some single-site or multi-site TDM calls.

CHOICE OF THE CTI TERMINAL

This list lets you choose how to select, in an association, the terminal concerned by the CTI actions for making or answering a call from a CTI application connected in CSTA or VTI/XML mode:

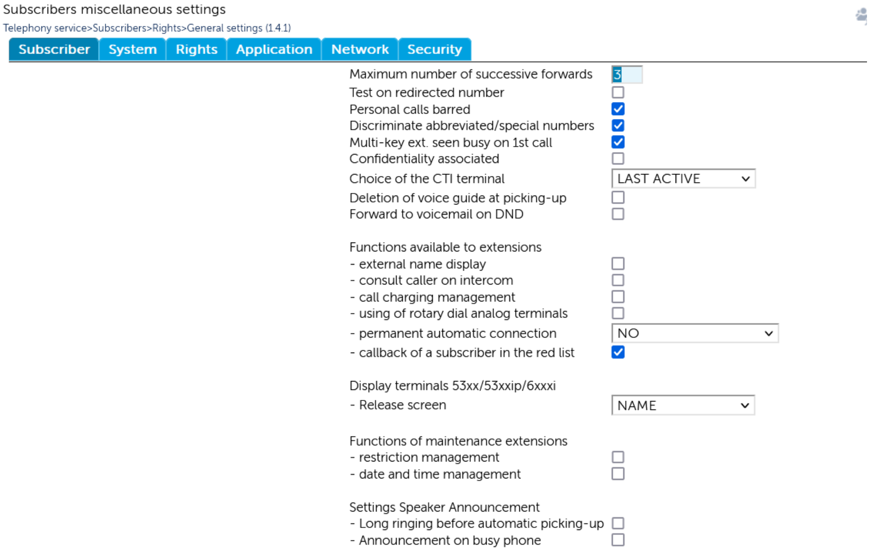
- Last active: in this case, it is the last active terminal in the association.
- Wired terminal: in this case, it is the first wired terminal in the association.

DELETE VOICEMAIL UPON ON-HOOK

- Box ticked: the voice prompt is deleted when the subscriber with activated forward on no answer or no busy off-hooks.
- Box not ticked: no deletion.

FORWARD TO VOICEMAIL ON DND

- Box ticked: transfers an internal call received by a user configured as DND to their voice mailbox. This box is ticked during initial installation.
- Box not ticked: the call received is processed as it was with the previous DND behaviour.



Subscribers miscellaneous settings

Telephony service>Subscribers>Rights>General settings (1.4.1)

Maximum number of successive forwards	3
Test on redirected number	☐
Personal calls barred	☑
Discriminate abbreviated/special numbers	☑
Multi-key ext. seen busy on 1st call	☑
Confidentiality associated	☐
Choice of the CTI terminal	LAST ACTIVE
Deletion of voice guide at picking-up	☐
Forward to voicemail on DND	☐
Functions available to extensions	
- external name display	☐
- consult caller on intercom	☐
- call charging management	☐
- using of rotary dial analog terminals	☐
- permanent automatic connection	NO
- callback of a subscriber in the red list	☑
Display terminals 53xx/53xxip/6xxxi	
- Release screen	NAME
Functions of maintenance extensions	
- restriction management	☐
- date and time management	☐
Settings Speaker Announcement	
- Long ringing before automatic picking-up	☐
- Announcement on busy phone	☐

FUNCTIONS AVAILABLE TO EXTENSIONS

- EXTERNAL NAME DISPLAY

This selection is only significant if the directory server is available. The external caller is displayed by name rather than by number, provided that this name is declared in the server directory.

- CONSULT caller on INTERCOM

Used, when the monitored subscriber receives a call, to see the caller ID before pick-up.

Depending on whether or not this box is ticked, two possibilities will be offered to users when the blinking supervision key is pressed (i.e. the monitored subscriber receives a call):

  - Box not ticked: pick up a call directly when your terminal is idle,

  - Box ticked: first check the monitored caller's ID then pick up or do not pick up the call.

The terminals concerned are proprietary terminals also including, as of R6.1 SP2, Mitel 6800 SIP Phones.

Note: In a multi-site configuration, for proper operation, the box must be ticked homogeneously on all the sites.

- CALL charging MANAGEMENT

If you tick the box, you can view the charging from a digital terminal.

Furthermore, if the MAINTENANCE SET parameter is ticked in the menu Extension Characteristics, the digital set concerned can be used to view the charging function for all sets in the system, and reset the counters. It can also reset these counters.

The requested password can be found in the Password Manager, in the line READ RESET CHARGE UNITS For optimal use, it is better to use a numeric password (*e.g.*: 12345): this type of password can also be used on terminals M510.

- PERMANENT AUTOMATIC CONNECTION

Parameter used to manage permanent automatic headset connection on 53xx/53xxip and 740 terminals.

Possible values:

NO 740 53xx/53xxip 740 and 53xx/53xxip

DISPLAY TERMINALS 53XX/53XXIP/6XXXI

- Release screen

Display options for the type of Office terminal user on the idle screen:

- NAME (default value): the name is displayed if found in the directory, otherwise the number is displayed, preceded by the located "Subscriber" string.
- NO DISPLAY: nothing is displayed (no name, no directory number).
- NAME + NUMBER: displays the name if found in the directory, followed by the directory number. if the name is not found, the number is displayed, preceded by the located "Subscriber" string.

FUNCTIONS OF MAINTENANCE EXTENSIONS

- RESTRICTION MANAGEMENT

Tick the box to authorise day/night switch-over on a digital set.

WARNING: A terminal must be declared as the maintenance terminal or operator console.

- DATE AND TIME MANAGEMENT

This field allows you to create/modify the date and time on an operator console (or maintenance terminal).

Maintenance terminals only have hotel management features.

SETTINGS SPEAKER ANNOUNCEMENT

- Long time-out before off-hook
- Announcement on busy phone

3.9.1.3 *System tab*

COMMON ABBREVIATED NUMBERS

These parameters describe the common abbreviated numbers used in directory records.

- number of numbers

10 **100** **1000** **10000**

The number of abbreviated numbers that can be defined.

- numerous prefixes

If this box is ticked, access to common abbreviated numbers is via different prefixes, based on number ranges.

Note: To be able to tick this box, you must first delete the (unique) access code of the abbreviated numbers in the features, using the menu DIALLING PLAN> User dialing plan>Access to features.

SUBSCRIBER FORWARDED TO THE EXTERIOR

- CHARGING

This parameter is used to assign charging to the caller or forwarded subscriber.

The ticket generated for the external call will mark either the caller or the forwarded subscriber as the call initiator.

Options: CALLER or FORWARDED SUBSCRIBER

Note: This parameter will be taken into account in the next 5 minutes.

- SEND IDENTITY

Moreover, during an external call from the forwarded subscriber this latter receives the caller's ID, either the caller's number of the number of the forwarded subscriber.

Options: CALLING NUMBER or FORWARDED SUBSCRIBER NUMBER

FEATURE CLASS MANAGEMENT

Options

NO **MANUAL YES** **AUTO YES**

If you enter MANUAL YES, the feature classes must have been defined beforehand (menu **SUBSCRIBERS>Rights>Feature classes**).

If you enter AUTO YES, the feature classes are created automatically.

In these two cases, the features are assigned to the subscribers via feature classes in the menu **SUBSCRIBERS>Subscription>Characteristics>General characteristics**.

If NO, the features are individually assigned to each subscriber from the menu **SUBSCRIBERS>Subscription>Characteristics>General characteristics**.

TL CLASS MANAGEMENT

Options

NO **YES**

This field operates in the same way as the Class management field.

PARTITION CLASS MANAGEMENT

If this box is ticked, partition class management is effective. A partition class is defined to limit telephone subscriber access to incoming and outgoing calls. Each class identifies a distinct subscriber community. Up to 64 partition classes can be defined.

Note: These three parameters (feature classes, TL and partition classes must be selected so they can be taken into account by MiVoice 5000 Manager.

DID DIALLING BY SDN

This box must be ticked in case of specific DID number management (see the document Managing DID numbers).

If the box is ticked, the subscriber DID numbers and general DID are taken into account by the SDN server.

NB WITHOUT EXTERNAL PREFIX FOR SIP SET

If this box is ticked, it is possible to transmit an external number without network prefix from an SIP terminal (dialling from a dual-mode GSM-WIFI terminal).

Otherwise, the network prefix is obligatory from the SIP terminals.

EXT CALL ROUTING

Options:

- LOCALISATION SITE (default): the routes used to channel network calls are those on the subscriber's location site.
- SUBSCRIPTION SITE: the routes used to channel network calls are those on the subscriber declaration site.

CHECK PASSWORD WHEN OPENING TAPI SESSION

Indicates the control of TAPI session opening.

- Box ticked: checks the password when a session is opened by TAPI.

The password sent in the "line open" is compared to the password associated with the directory number of the terminal concerned.

- Box not ticked: The line is opened by TAPI without control.

ACD for local calls: priority to D/N calendar

From R8.0, if the box is checked, the local Call distribution be defined based on Calendar. Parameter associated with Call distribution definition. Refer to paragraph 7.1.2.1.

POWER SAVING FUNCTIONS

The implementation of this function is described in the Appendix.

The function is active if the box is ticked. In this case, the ASSOCIATED CALENDAR line is proposed so a calendar can be associated with the power-saving function.

ASSOCIATED CALENDAR

Options of the calendars defined in the menu **CALL DISTRIBUTION>Calendars>Names**.

DUAL HOMING PARAMETERS

Note: These parameters are only available in a multi-site configuration or Cluster.

DAILY ALIGNMENT (HH:MM)

Start time for copying the secured subscriptions telephone data to their backup site.

IMMEDIATE ALIGNMENT OF

……….	No immediate copying.
Site Name	Starts immediate copying to the selected site of the data of all secured subscriptions on this site.
ALL SITES	Starts copying immediately all the relevant secured subscription data on each of the sites backed up from at least one subscription.

The drop-down list contains all the sites connected (at the time of the immediate alignment request), used as backup by at least one subscription.

Once this parameter has been entered, click the "Confirmation" button to validate the immediate alignment request.

3.9.1.4 *Rights tab*

CALL PICK-UP GENERAL NOT ALLOWED

- Box ticked: general call pick-up rejected for all the terminals (except ICG)
- Box not ticked: general call pick-up allowed for all terminals.

CONFERENCE FUNCTION

Applicable to conferences at the iPBX level. These settings are not relevant to the conference feature incorporated in SIP phones.

Indicates the right to a conference.

- Conference function checkbox not ticked: No conference on the iPbx.
- Conference function checkbox ticked: activates the conference function

-TK TK ALLOWED

- If the TK TK allowed checkbox is ticked: One or more external correspondents can be included in a conference (network line TK).
- If the TK TK authorised checkbox is not ticked: Inter-terminal conference is authorised but not conferences with external correspondents.

- SEND TONE

Checkbox

a beep (internal hold tone) is made during the conference.

This line is only displayed if the **Conference function** is authorised.

FORWARDING TO TL SUBJECT TO RIGHT

Indicates that forwarding to TL is subject to a right

- Box not ticked (default value): routing to TL is not subject to a right.
- Box ticked: routing to TL is authorised if the subscriber's feature class allows it.

ALLOW TRANSFER

In this menu, the operator may authorise or not authorise inter-network transfer (TK-TK or TK-IA).

These authorisations may apply according to the deployment mode defined in the TRUNK GROUP CONFIG. field, either generally by LIST NOT USED, or more restrictively by defining a list of trunk group pairs which will be either AUTHORISED or FORBIDDEN.

The list of trunk group pairs is configured in Menu NETWORK AND LINKS>Network>Transfers/transits authorization.

- TK TK

- Box ticked: Network-to-network call transfer is authorised, as well as the CONFIG field. TRUNK GROUPS is displayed, allowing the user to define how to use the list.

- TK TL

- Box ticked: Network-to-TL call transfer is authorised, as well as the CONFIG field. TRUNK GROUPS is displayed, allowing the user to define how to use the list.

TRUNK GROUP CONFIG.

This line is only displayed if at least one of the **TK TK** or **TK IA** checkboxes is ticked.

- LIST AUTHORISATION (default value): The transfer of trunk group pairs is authorised.
- PROHIBITION LIST:The transfer of trunk group pairs is forbidden.
- LIST NOT USED: Transfer is authorised without taking account of the list configuration.

- BY SUBSC. WITHOUT RESTRICTION

Indicator for transfers without barring tests.

- BETWEEN ROOM SETS

This parameter is only active if multi-company configuration is used. It is defined in Menu **Hunt groups and companies**.

If you tick this box, a set can call another set in the same department.

- BETWEEN ROOM SETS VIA OP. CONS.

This parameter is active if multi-company configuration is used: it is defined in menu **Hunt group and companies**.

If you tick this box, the operator console can set up calls between two sets in the same department.

- VIA OP. CONS. TO PRE-PAYMENT SETS

If you tick the box, the attendant console can transfer an outgoing line to a closed prepayment terminal or to a locked terminal.

- OF PERSONAL FORBIDDEN

Indicator that transfers of personal calls are not allowed.

-TO SET WITH PSTN ACCESS ALLOWED

Indicator that call transfers to a set which is entitled to set up calls to the PSTN are not allowed.

3.9.1.5 *Application tab*

PAGING FUNCTION

Indicates the choice of pager mode.

MODE 1: default mode.

MODE: **WITHOUT MEETING FOR INTERNAL CALLS** with meeting for external calls, without meeting for internal calls

int display: caller number for internal calls

ext display: beep no. for external calls + recovery code

MODE 2:

MODE: **WITH MEETING FOR ALL CALLS** with meeting for any call type, without meeting for internal calls

int display: beep no. for internal calls + recovery code

ext display: beep no. for external calls + recovery code

MODE 3:

MODE: **WITH MEETING FOR ALL CALLS** with meeting for any call type, without meeting for internal calls

int display: caller number for internal calls

ext display: beep no. for external calls + recovery code

MODE 4:

MODE: **ALL CALLS** with meeting for any call type, without meeting for internal calls

- int display: caller number for internal calls
- ext display: caller number for external calls

SSO MODE

See also Chapter 9.5.1;

Single Sign On (SSO) allows the user to access multiple applications, including the User Portal, with a single login.

The Login/Password initially entered when logging in to the OS then gives access to other applications.

Note: It is also possible to log on to the User Portal without SSO mode if SSO mode is not enabled.

USER PORTAL SERVICE

Checkbox.

Ticking the **User Portal service** box allows you to force a change of the password on first use.

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

User Portal password policy:

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

- Minimum length
- Minimum number of letters
- Minimum number of digits
- Password validity period in number of calendar days (1 to 180).

  0: Equivalent to Deactivated.

  When the password validity period is modified, the password expiry date is updated for all user accounts if the old expiry date is later than the new date.

  It remains unchanged if the expiry date is earlier than the new expiry date.

- When the password validity period is modified, the password expiry date is updated for all user accounts if the old expiry date is later than the new date.
- It remains unchanged if the expiry date is earlier than the new expiry date.

USER (AUTHORISED SUBSCRIBER) ACCESS TO THE MIVOICE 5000 USER PORTAL

The user must have a PC with a web browser that can access this interface.

Access to the MiVoice 5000 User Portal is subject to the activation of the User Portal account and associated Login/Password.

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 language of the User Portal application is that of the Web browser used.

The application can be accessed in the following ways:

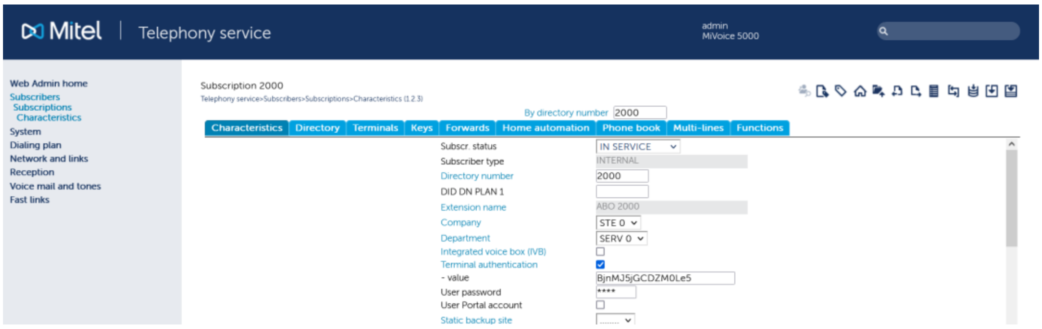
- Either by subscription number,
- Or in SSO mode, if enabled.

The User Portal is accessible via a web browser, at this address **https://@iPbx:4446/userportal** or **https://@iPbx:4446**

The Administrator is advised to communicate this address to the persons using the MiVoice 5000 User Portal.

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. Refer to Section 2.2.4.

Configuring the integrated User Portal account



Subscription 2000

Telephony service>Subscribers>Subscriptions>Characteristics (1.2.3)

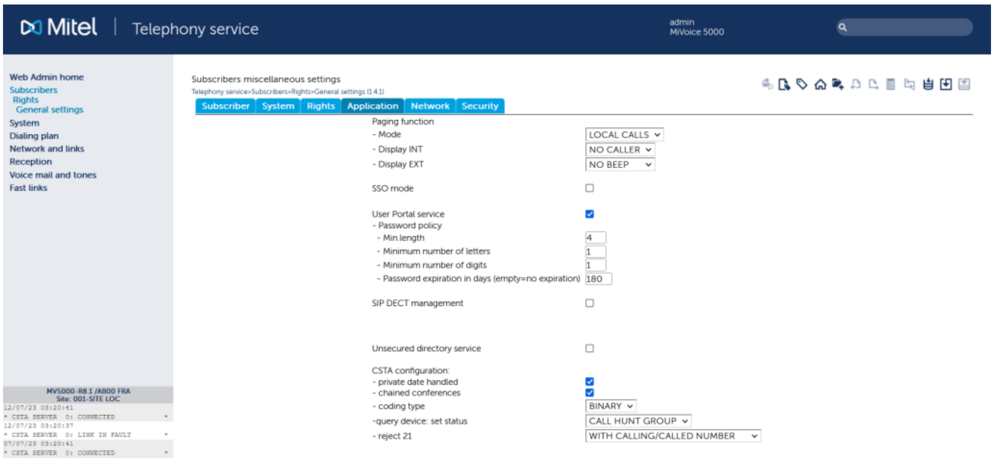
By directory number 2000

Subscr. status: IN SERVICE
Subscriber type: INTERNAL
Directory number: 2000
DID DN PLAN 1:
Extension name: ABO 2000
Company: STE 0
Department: SERV 0
Integrated voice box (IVB): □
Terminal authentication: ☑
- value: BjnMJ5jGCDZM0Le5
User password: ****
User Portal account: □
Static backup site: ....

- In Menu **SUBSCRIBERS> Subscriptions> Characteristics/General characteristics**, in the **User Portal Account** field:

- Box to be ticked if the the operator allows the subscriber access to the User Portal using a password defined on the next line.

- The User Portal service must be activated (see Menu **Subscribers>Rights>General settings**, **Application** tab).



Subscribers miscellaneous settings

Telephony service>Subscribers>Rights>General settings (1.4.1)

Paging function
- Mode: LOCAL CALLS
- Display INT: NO CALLER
- Display EXT: NO BEEP

SSO mode: □

User Portal service: ☑
- Password policy
- Min.length: 4
- Minimum number of letters: 1
- Minimum number of digits: 1
- Password expiration in days (empty=no expiration): 180

SIP DECT management: □

Unsecured directory service: □

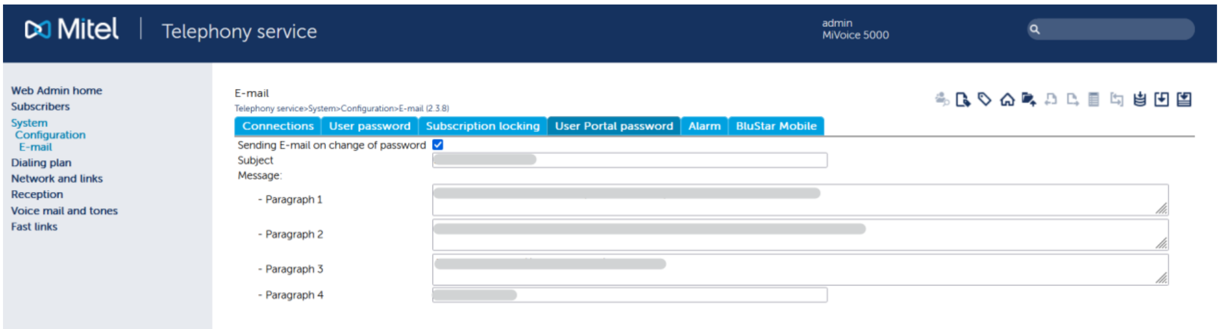
CSTA configuration:
- private date handled: ☑
- chained conferences: ☑
- coding type: BINARY
-query device: set status: CALL HUNT GROUP
- reject 21: WITH CALLING/CALLED NUMBER

```
MV5000-R8.1 /AB00 FRA
Site: 001-SITE LOC
12/07/23 03:20:41
• CSTA SERVER  0: CONNECTED
12/07/23 03:20:37
• CSTA SERVER  0: LINK IN FAULT
07/07/23 03:20:41
• CSTA SERVER  0: CONNECTED
```

This field is only visible if the **User Portal Account** option is activated.

The password entry policy is defined in the following lines in relation to the one defined for the User Portal.

Creating or modifying the User Portal password sends an automatic e-mail to the subscriber concerned if this option is activated in Menu **System>Configuration> E-mail - User Portal Password** tab.



E-mail

Telephony service>System>Configuration>E-mail (2.3.8)

Sending E-mail on change of password ☑
Subject
Message:
- Paragraph 1
- Paragraph 2
- Paragraph 3
- Paragraph 4

MANAGING THE SIP DECT

The OMM login parameters must be defined to allow OMM update.

Tick the checkbox to activate the function.

MAIN IP ADDRESS

Enter the IP address of the main Mitel SIP OMM.

Press Enter to confirm. The following parameters are displayed:

SECONDARY IP ADDRESS

Enter the IP address of the secondary Mitel SIP OMM (if redundant).

SSL PORT

SSL port used (12622 by default)

LOGIN

Mitel OMM access login

PASSWORD

Password

Rules on password syntax:

- Authorised characters: [A-Z]+[a-z]+[0-9]+["#%’()*+,-./:;<=>@_]
- Unauthorised characters: [!$&? [\]^`{|}~]

SYSTEM PARAMETERS CONFIGURATION

If the box is ticked, the system retrieves in the iPBX the information needed to configure Mitel OMM (system settings).

USER CONFIGURATION

If the box is ticked, the realignment will be made to the OMM for the **Users** setting.

CONFERENCE SETTINGS

If the box is ticked, the realignment will be made to OMM for the **Conference**settings.

DAILY REALIGNMENT

Enter the daily realignment time in hh :mm for automatic daily realignment.

The date of last alignment is displayed.

IMMEDIATE REALIGNMENT REQUEST

Click this button to start an immediate realignment.

Errors detected during a realignment process are recorded in the logbook.

UNSECURED DIRECTORY SERVICE

Access to the white pages is via http and is, therefore, not secure. This box allows you to make it accessible or inaccessible.

In first installation, white pages not accessible (box not ticked). The user has the option to make them accessible by ticking the box (unsecured http access).

Following an update or restart in Total mode, white pages accessible (check box). The user has the option to make them inaccessible by unticking the box.

CSTA CONFIGURATION

- PRIVATE DATA HANDLED (CHECKBOX)

- Box not ticked: private data not handled with CSTA
- Box ticked: private data handled with CSTA

- CHAINED CONFERENCES (CHECKBOX)

- Box not ticked: refuse to chain conferences
- Box ticked: accept to chain conferences

- CODING TYPE (OPTIONS)

- ASCII: ascii coding
- BINARY: binary coding (by default)

- QUERY DEVICE: SET STATUS (OPTIONS)

- ALL CALL: terminal status (for any call)
- CALL HUNT GROUP: Status of the terminal compared to the hunt group (by default)

- REJET 21

Options:

- WITHOUT CALLING/CALLED NUMBER: Reject with previous interface
- WITH CALLING/CALLED PARTY NUMBER: reject with interface including the caller/called party number (by default)

3.9.1.6 *Network tab*

ISDN PARAMETERS

ANSWER SET INSTALLATION FWD

Enter in this field the directory number of the terminal or operator console to be authorised to make call transfers (ISDN service complement). This number is unique.

This parameter only concerns systems connected to the ISDN network, having subscribed for the CALL TRANSFER additional service.

In multi-company configuration, only one company can define forwarding. In a single or multi-company configuration, this forwarding must be validated in Menu **Telephony service>Subscribers>Rights>General settings - ISDN settings** field.

ISDN REMOTE CHARGING

This parameter only concerns systems connected to the ISDN network. If you tick the box, the device requests the "cost indication" additional service for each call.

WARNING: There is a charge for this service (1 unit per call), which is an essential service if the customer requires step by step charging. This service can be provided by the Central Office (leave this parameter on NO in this case).

NON IDENTIFICATION AUTHORIZED

Non-identification is a service that concerns installations connected to ISDN and SIP Trunk.

If the box is ticked, the system sends the caller's number with "anonymous indication".

SIGN. DEFAULT SUBSCRIBER SIGN.

ETSI **NUMERIS VN4**

The signalling applicable by default to S0 accesses. This can be redefined individually for each access.

TRANSMISSION OF EMPTY SUU NOT AUTHORISED

Indicates "no transmission of empty SUU".

- Box not ticked (default value): When a terminal makes a call to the public network, if it can receive some SUU, it sends an empty SUU.

- Box ticked: no sending of empty SUU to the network.

IP SETTINGS

- HANDLING OF FAX T.38 COMMUNICATIONS

Supports FAX T.38 and Video communications

- Box not ticked (default value): FAX T.38 is locked

- Box ticked: FAX T.38 is open

- DTMF HANDLED INTO

Options:

- SIGNALLING MESSAGE: DTMF transported functionally via signalling messages.
- RTP PACKET: DTMF transported according to RFC 2833 in RTP packets. PayloadType value (RTP packet header value for DTMF transport). This value must be the same as the one sent by the SIP terminal (trunk or terminal).
- The line "HEADER VALUE (RFC 2833)" only appears if DTMF is managed in the RTP packets.

Decimal values between 96 and 127: default value is 101.

NUISSANCE CALLS TRACKING

Value used to open the nuisance call feature and configure the indication of nuisance calls to the ISDN administrator

- Box not ticked: the nuisance call feature is not offered on the terminals (no service ticket issued). In this case, the following lines are not displayed:
- Box ticked (default value): it is possible to trace nuisance calls.

- OFFERED TO THE ATDC AT THE CALL END: The nuisance call is proposed to the attendant console when the remote terminal on-hooks.

NOTIFICATION TOWARDS ISDN NETWORK

Checkboxes

- FOR THE ATDC: a notification about the nuisance call is sent to the ISDN administrator for the ATDCs.

- FOR PRIORITY TERMINALS: a notification about the nuisance call is sent to the ISDN administrator for priority terminals.

- FOR OTHER TERMINALS

TRANSIT AUTHORIZATION

The fields for this context are linked to the settings made in the menu **NETWORK AND LINKS>Network>Transfer/transit authorisation**.

TRUNK GROUP CONFIG.

Options

- LIST NOT USED (default value): Transit is authorised without taking account of the settings made in the menu NETWORK AND LINKS>Network>Transfer/transit authorisation.
- PROHIBITION LIST:Transit is not authorised if the corresponding trunk group pair is defined in the menu NETWORK AND LINKS>Network>Transfer/transit authorization.

PRE-ANSWER IF TRANSIT

Pre-answer indicator. In case of ISDN transit, the iPBX generates a pre-answer for the caller so he can play back announcements.

- Box not ticked (default value): no pre-answer.
- Box ticked: If it is an internal IP trunk or ISDN trunk and the remote terminal has received a message in progress, pre-answer is generated for the caller so he can listen to announcements.

3.9.1.7 *Security tab*

TERMINAL AUTHENTIFICAT. GENERATION AT CREATION

Ticked or not ticked, this box is used to activate/deactivate the generation of terminal authentication during subscription creation.

The box is ticked by default. Activation or deactivation can also be carried out by pressing Ctrl + I (See document MiVoice 5000 Server – Installation and Implementation).

This word is then used during the following operations carried out by the subscriber:

- Set login,
- Locking,
- Squatt function.

Depending on the security policy defined by the operator, the password to be defined and entered by the subscriber may be simple or complex. The password may be defined in the terminal menu or from the User Portal (see the document MiVoice 5000 Manager Manager - User Guide).

The subscription is frozen after 3 incorrect attempts.

Note: This terminal authentication can then be deleted on a subscription basis, for SIP terminals which do not support MD5.
(*) all Mitel SIP phones support MD5.

PASSWORD POLICY FOR SUBSCRIPTIONS:

Force initial password change: If the box is ticked, the password will be changed: at the end of the validity period indicated, a request is made once, no renewal of the request.

The **Validity period (in days)** field (which appears if the **Force initial password change** box is ticked) is used to define a number of validity days for this initial password between 1 and 30 days. The default value is one day.

The **Force regular renewal** box, associated with the **Validity period of current password** (box ticked), is used to define the validity period between 1 and 90 days.

A Confirmation button appears if any of the previous four fields is modified, in order to validate the settings.

The **Deny easy passwords** box is used to force a more secure password.

The rules are as follows:

Easy passwords: Any 4 digits defined by the administrator.

More complex passwords: In this case the following are forbidden:

- 4 identical digits,
- Sequences of successive ascending or descending digits (examples: 0123, 7890, etc),
- A password that is equivalent to the extension number (for a 4-digits dialling plan),
- The same password as the previous one.

SUBSCRIPTION BLOCKING DURATION (MN)

Duration (in minutes) of the subscription freeze following three consecutive login refusals.

- The default duration is 5 minutes.
- The value 0 indicates a locking operation without unlocking duration (unlocking via Web Admin).
- Only values with multiples of 5 are accepted, the other values are rounded off to a lower value:

0=1=2=3=4: indefinite locking

5=6=7=8=9: locking for 5 minutes ...

By default, the **Force initial password change**, **Force regular renewal** and **Deny easy passwords** boxes are unticked and accessible to installer and manufacturer accounts, via an XML or Web connection.

Depending on available terminal type and display, some messages will be received indicating the next expiry date or an expiration. These messages are also sent to the User Portal.

After these messages, the subscriber must change his password either from the User Portal or from the terminal menus or feature codes.

3.9.2 CATEGORIES

A category groups a set of access rights (external or internal) for both outgoing and incoming calls.

The “Category characteristics” screen is used to manage and modify rights for each category (incoming and outgoing calls).

To create a category, you must first assign a name to the category then go to "Category characteristics" to determine its parameters.

Mitel devices (including MiVoice 5000 Server) propose 16 different CATEGORIES. Each category is designated by a NAME, and can only be managed if its NAME has been declared. By default, 6 CATEGORIES are defined:

- INTERNAL
- PRIVATE
- ADDITIONAL
- NATIONAL
- REGIONAL
- INTERNATIO.

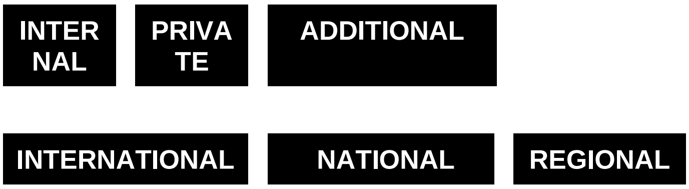
Note: All categories can be modified.
The basic category names are the names allocated to the directions by the operator. Only the defined names are shown in this menu. This means that if a new direction is created, the operator must remember to update the parameter for this direction in all the categories defined. This removes any ambiguity which may arise from the fact that, by default, the "local" direction is named "national" in the plan.

3.9.2.1 *Names*

Menu **SUBSCRIBERS>Rights>Categories>Name**.

This screen is used to display existing categories and define new categories if necessary.

CATEGORY



Categories are used to restrict the dialling features of sets depending on their respective needs.

They are assigned individually to each set. They represent all the rights assigned to subscribers, both for incoming and outgoing calls.

CATEGORY 7

Selection reserved for the creation of an additional CATEGORY.

Note: The NAME of an existing category can be replaced. In this case, the parameters of the category in question are assigned to the new NAME.

Some operating rules:

The category NAME can have no more than 12 alphanumerical characters.

Two categories cannot have the same NAME.

When the category is created, you must choose its parameters by ticking the corresponding boxes in the **Category XXX characteristics** menu.

3.9.2.2 *Characteristics*

Menu **SUBSCRIBERS>Rights>Categories>Characteristics**.

The default configuration is as follows:

RIGHTS	INTERNAL	PRIVATE	ADDIT.	NAT.	REGIONAL	INTERNATIO.
INTERNAL CALLS ALLOWED	YES	YES	YES	YES	YES	YES
INT & TL INCOMING CALLS ALLOWED	NO	YES	YES	YES	YES	YES
INCOMING EXTERNAL CALLS ALLOWED	NO	YES	YES	YES	YES	YES
DELAYED RINGING AFTER ANN MSG	NO	NO	NO	NO	NO	NO
CONSOLE TRANSFER ALLOWED	NO	NO	YES	YES	YES	YES
LOCAL ALLOWED	NO	NO	NO	YES	YES	YES
NATIONAL ALLOWED	NO	NO	NO	NO	YES	YES
INTERNATIO. ALLOWED	NO	NO	NO	NO	NO	YES

Later, the configuration for a category will be the result of the rights you assign to this category.

The call type is compared to the list of user restrictions. If it is in this list:

- During the day, the call is rejected (busy tone).
- At night, if the user is not entitled to override, the call is rejected (busy tone).
- At night, if the user is entitled to override, he is requested to enter his secret code.

S and SIP sets cannot override. For 6xxxi phones, the function is available as of R6.1.

Rights associated with different categories

The categories are to be defined in the **By name** field, in the menu **SUBSCRIBERS>Rights>Categories**.

This screen is used to intervene on the rights associated with the different categories.

After validation, you will obtain the following menu by default (example for the “national” category):

Note: The rights displayed in this menu depend on the previously defined categories.

For each available field, tick the corresponding box to authorise or forbid the use of the function.

INTERNAL CALLS ALLOWED

If you tick the box, the set has access to internal outgoing calls.

INT. AND TL INCOMING CALLS ALLOWED

If you tick the box, the set has access to internal incoming calls.

PSTN INCOMING CALLS ALLOWED

If the box is ticked, pick-up is allowed on calls from the PSTN.

DELAYED RINGING AFTER ANN. MSG

If the box is ticked, this enables the subscriber to connect an answering message to the external caller before the called extension rings (hospital application).

The answering message must be assigned to a tone of the type BEFORE DAY RINGING and/or BEFORE NIGHT RINGING. The duration of the announcement is the parameter ANNOUNCEMENT DURATION BEFORE RINGING in the menu **SYSTEM>Expert>Time-out management**.

CONSOLE TRANSFER ALLOWED

If the box is checked, Outgoing communication transfers from an ATDC are accepted.

BARRED NUMBERS LIST RESTRICTION

If the box is checked, restrictions relative to the lists of forbidden numbers are taken into account.

LOCAL ALLOWED

If the box is ticked, this terminal has access to the direction indicated and can make calls towards this direction.

If not, it cannot call the numbers defined in the dialling plan for the direction in question.

NATIONAL ALLOWED

If the box is ticked, this set has access to the direction indicated and can make calls towards this direction. If not, it cannot call the numbers defined in the dialling plan for the direction in question.

INTERNAT. ALLOWED

If the box is ticked, this set has access to the direction indicated and can make calls towards this direction. If not, it cannot call the numbers defined in the dialling plan for the direction in question.

3.9.2.3 *Display users*

Menu **SUBSCRIBERS>Rights>Categories>Users**.

Select the name of the category you wish to view in the **By name** field.

The display screen presents the users of the category chosen.

Note: An information line "Incomplete display" appears when more than 1000 users must be displayed (display menu limited to 1000 lines).

3.9.3 FEATURE CLASSES

Menu **SUBSCRIBERS>Rights>Feature classes**

You can use this function if you wish to globally manage user rights, that is, if you wish to define a certain number of classes, and assign a class to each subscriber instead of defining a specific set of rights for each subscriber.

When class definitions are modified, the rights of subscribers in this class can also be modified. However, if you modify a subscriber's right and there is no associated class, you must create a new class and then assign it to the user.

By default, the device offers 11 different feature classes which can be modified or deleted: it is advisable to leave the feature classes unchanged.

You can create 53 other classes in the device. Their use must be validated in Menu **SUBSCRIBERS>Rights>General settings**.

In this case, the number of parameters to be entered in Menu **General Characteristics of a subscriber** is limited: all the rights of the subscriber are replaced by a Class No. to be entered in the Feature Category line.

3.9.3.1 *Names*

Menu **SUBSCRIBERS>Rights>Feature classes>Names**.

This screen is used to display all the feature class names (0 to 63).

NUMBER

Feature class numbers 0 to 63: classes 0 to 7, 32, 40, and 41 are created by default.

3.9.3.2 *Characteristics*

Menu **SUBSCRIBERS>Rights>Feature classes>Characteristics**.

This screen is used to define the parameters associated with a feature class (class FAC00 for example).

Note: These rights are described in the paragraph on the characteristics of a subscription. Refer to the paragraph 3.3.3.1 – General characteristics.

The screen below is a continuation of the parameters associated with a feature class.

Note: These rights are described in the paragraph on the characteristics of a subscription. Refer to the paragraph 3.3.3.1 – General characteristics r.

3.9.3.3 *Display users*

Menu **SUBSCRIBERS>Rights>Feature classes>Names>Users**.

This screen is used to display the users of a given feature class.

3.9.4 TL CLASSES

Menu **SUBSCRIBERS>Rights>TL classes**.

TL class definition is used for global management of TL direction accesses per area, and to assign a Tie-Line class to the terminals. Up to 64 TL classes can be defined.

A TL class contains 8 areas (each area being a set of private directions).

Note: In a MULTI-SITE configuration, the "Direction names" screen proposes the creation of 48 private directions which can later be assigned to an area in Menu DIALLING PLAN>User dialling plan>Access to directions>TL and Menu DIALLING PLAN>User dialling plan>Display area composition.

The use of TL classes must be validated in Menu **Rights>Subscribers miscellaneous settings>TL class management**. In this case, the menu **SUBSCRIBERS>Subscriptions>Characteristics** contains the TL class field, and all the access rights for the TL areas are replaced by a class number.

Note: TL: Tie Line: specialised line between PBXs.

3.9.4.1 *Names*

Menu **SUBSCRIBERS>Rights>TL classes>Name**.

This screen is used to display TL classes. The TL class numbers are displayed, from 0 to 63 (classes 0 to 1 are created by default).

3.9.4.2 *Characteristics*

Menu **SUBSCRIBERS>Rights>TL classes>Characteristics**.

This screen is used to define the characteristics of a TL class. The TL class numbers are displayed, from 0 to 63 (classes 0 to 1 are created).

ACCESS TO TL ROUTES X

Tick this box to select the TL route access for the area in question.

Note: Selecting (ticking) the parameter TL CLASS MANAGEMENT in Menu SUBSCRIBERS>Rights>Subscribers miscellaneous settings deletes in Menu SUBSCRIBERS>Subscriptions>Characteristics, all the TL direction access lines and only displays the TL CLASS line.

Note: Initially, users are assigned TL class 7: it gives access to the directions of one and forbids other TL directions.

3.9.4.3 *Display users*

Menu **SUBSCRIBERS>Rights>TL classes>Users**.

This screen is used to display the list of subscribers attached to the selected TL list.

Note: An information line "Incomplete display" appears when more than 1000 users must be displayed (display menu limited to 1000 lines).

3.10 HOME AUTOMATION

Menu **SUBSCRIBERS>Home automation**.

The home automation function is used to manage one or more lamps associated with an analogue set, to indicate delivery of a message, for example.

This function requires a GLM module which, connected parallel to the analogue trunk line, can manage the lamp message function.

This module is configured by means of 3 straps, used to select the DTMF-Q23 codes which switch the lamp on or off, or by a special set incorporating a message lamp and the GLM option.

It is possible to define up to 8 different home automation functions.

This menu is used to:

- Activate the home automation function
- Define the 8 functions.

3.10.1 ACTIVATING THE HOME AUTOMATION FUNCTION

Menu **SUBSCRIBERS>Home automation>Run**.

To activate the home automation function on the system, tick the “Authorise home automation function” checkbox.

3.10.2 DEFINITION

Menu **SUBSCRIBERS>Home automation>Definition**.

This command is used to assign an activation Q23 code and a deactivation Q23 code to a home automation function. The home automation functions are made available for a subscription from the menu **SUBSCRIBERS>Subscription>Characteristics>Home automation** (see description in *3.3.3.6*).

BY NUMBER (1 TO 8)

Function number to be defined.

Click **Select the item**, the different fields for the function are displayed:

NAME OF FUNCTION

Alphanumeric character string

ACTIVATION CODE

Q23 code sent by the device to the set to activate the lamp.

CANCEL CODE

Q23 code sent by the device to the set to deactivate the lamp.

FUNCTION ACTIVATED BY:

OR THE FEATURE

MAIL DEPOSIT **MSG LAMP 0** **MSG LAMP 1** **MSG LAMP 2** **MSG LAMP 3**

List of features that activate the function.

3.11 CHARGING - PREPAYMENT

Menu **SUBSCRIBERS>Charging – Prepayment**

Subscriber charging is part of operation administration. It is based on pre-payment parameters which apply to all the subscribers.

3.11.1 PARAMETERS

Menu **SUBSCRIBERS>Charging – Prepayment>Settings**.

EXTERNAL SERVER USE

If this box is ticked, charging is managed by an external application.

If the box is not ticked, charging may be managed either via an MMC or via an external application.

IN CURRENCY UNIT

CREDIT AND CHARGE UNIT (ROUNDED)

1/10 **1** **10** **100** **1/100** **1/20**

Select the measuring scale before modifying the prepayment counters.

In countries where the monetary unit is divisible by 100, the unit charge can be expressed in hundredths (1/100), rounded off to 5 hundredths (1/20) or to 10 hundredths (1/10).

If the box for the parameter EXTERNAL SERVER USE is ticked, this value cannot be configured and is equal to 1/10.

CUMULATIVE SUM (ROUNDED OFF)

1 **10** **100** **1/100** **1/20** **1/10**

Select the rounding of the accumulated amounts: to round off to the nearest euro, enter 1; to the nearest cent, enter 1/100 etc.

The presentation of the cumulative prepayment sums is displayed on the CHARGING SUBSCRIBER menu, accessible via “SUBSCRIBERS>Charging – prepayment>Individual charging”.

If the box for the parameter EXTERNAL SERVER USE is ticked, this value cannot be configured and is equal to 1.

NO. OF DECIMALS DISPLAYED

Value between 0 and 4.

Defines the display format for the various amounts, independently from the specified value to be rounded off: you must ensure that the request is consistent. In the USA, for example, if the unit charge is rounded off to the nearest cent, 2 decimals must be displayed.

CHARGE UNIT PRICE

Enter in this field the price per charge unit.

If the value 1/100 is selected in the field "Credit and charge unit (rounded)", enter 0.75 to indicate a unit of 75 cents.

EURO/NATIONAL CURRENCY CONVER

The Euro value is given in 6 figures (7 characters with a decimal point).

FUNCTION FOR DIGITAL SETS

- RESET CHARGE PASSWORD

Password which allows subscribers' charging counters to be reset from the maintenance terminal.

3.11.2 INDIVIDUAL CHARGING

Menu **SUBSCRIBERS>Charging – Prepayment>Individual charging.**

DIRECTORY NUMBER

The extension is accessed by its directory number.

Clicking **Select the item** displays the following parameters:

Note: For a BACKUP type subscription, these are information fields and configuration of the subscription characteristics is only authorised on the reference site.

PREPAYMENT

EXTENSION WITH PREPAYMENT

If you tick this box, the prepayment function is assigned to the subscription. In this case, it can be assigned a credit in euros which will be entered: this credit will be reduced for each TU received (communication limitation).

If the box is not ticked, the set is not subject to prepayment; in this case, it is not concerned by a credited amount (no call limitation).

Note: This line is not displayed when the iPbx is configured in management via feature classes. In this case, this line is located in the feature classes characteristics menu.

ACCOUNT CLOSED

If you tick this box, the account corresponding to the subscription is closed.

If you do not tick the box, the account corresponding to the subscription is credited with a sum in euros.

Note: It is possible to close the account even if it has been credited. In this case, the parameters BALANCE and CUMULATED INSTALMENTS are automatically reset (for a customer wishing to settle his bill).

BALANCE

Information field indicating the account balance.

Each time a value is entered in the field AMOUNT TO PAY, the balance increases by this value.

The balance decreases by the amount used up while making calls.

CUMULATED INSTALMENTS

This information field gives the total of the amounts displayed on the line AMOUNT TO PAY.

AMOUNT TO PAY

Enter the amount (maximum 4 digits) of credit the set is allowed. After validation, the sum entered is added to the value of the parameter BALANCE.

Note: If you tick the box ACCOUNT CLOSED, entering a value in the field AMOUNT TO PAY unticks the box.

DATE OF LAST RESET

This field indicates the date (dd/mm) and time (hh/mm) of the last reset of extension counter.

COUNTER VALUE

This field indicates the total number of CUs (Charge Units) received by this extension since last reset.

The **Reset** button is used to reset the counter. The date of last reset is then updated.

Note: In the case of prepayment, the system sends information to the ISDN requesting the continuous retransmission of charges (ISDN SERVICE): the calls made are increased by one TU corresponding to the activation of this service (unless it is part of the subscription).
The prepayment feature is not used with ISDN sets.

3.11.3 DISPLAY EXTENSION COUNTERS

Menu **SUBSCRIBERS>Charging – Prepayment>Display**. **Extension counters**.

COMPANY SELECTION

xxxxxxxx **CMPNY.0**

This field only appears if the multi-company configuration is selected.

Select xxxxxxx to display the extension counters for all companies and departments. If you have already created company names, these are displayed here.

DISPLAYED COUNTERS THRESHOLD

Counter threshold number: the threshold criterion is used to display extension counters whose value is equal to or above the entered threshold value.

DIRECTORY BEGINNING WITH

Enter a digit (or number). All directory numbers that start with this digit (or number) will be displayed.

Clicking **Select the item** displays the following:

EXTENSION COUNTERS

Authorises the display of all the counters for all the extensions connected to the device. You cannot modify this information.

It is now possible to display 15000 extensions on a MiVoice 5000 Server.

The table shows:

- The directory number

- The subscriber number
- The date of the last reset of the charge counter (DAY/MONTH)
- The number of CUs (Charge Units)
- The number of extensions connected to the device
- The total number of CUs for all extensions

Note: The "Incomplete display" line is an information line indicating that a certain number of subscribers are not displayed (display menu limited to 1000 lines).

All directory numbers are in this list, including secondary numbers for multi-line sets and ISDN sets on S0 bus.

3.12 EXTERNAL DIRECTORY SYNCHRONISATION

New Section

Menu **Telephony Service>Subscribers>External directory synchronisation**

This menu is used to synchronise an Active Directory, ADAM, AD LDS or Microsoft Entra Domain Services through LDADP/LDAPS with a MiVoice 5000 Call Server without Manager. External directory synchronisation is subject to a licence and must be unlocked in Menu **SYSTEM>Info>Licences**.

3.12.1 CONFIGURATION

Menu **Telephony Service>Subscribers>External directory synchronisation>Configuration**

3.12.1.1 Connection tab

The Connection tab is used to enter the necessary credentials to access the external directory and initiate an immediate synchronisation.

IP address or FQDN

Field to be filled in. IP address or FQDN of Active Directory.

Port

Field to be filled in. Port number assigned to LDAP access.

- Default port: 389
- Default port for secure mode: 636

DN base

Field to be filled in. Field for the **Distinguished Name** of the directory branch from which MiVoice 5000 users are retrieved.

The DN base should at least correspond to the root of the directory. Otherwise, indicate a more specific branch.

Login/Password

Login and password used to access the LDAP/AD database in read mode. Login and password should preferably be defined by a domain-specific machine account:

- No password expiration date,
- On which rights are limited to read-only.

TLS

Checkbox. If ticked, enables TLS for secure access (recommended). First, add the corresponding root certification authority to the **Trusted Root Certification Authorities** tab of the **Configuration** Menu's **Security** tab.

Synchronization period

Disabled	Daily	Hourly

Dropdown list. Sets the automatic synchronisation rate between the MiVoice 5000 and the external directory.

- If the **Synchronisation period** is set to **Daily**, a field appears underneath to specify the daily synchronisation time in **hh:mm** format.

Once the necessary information has been entered, the **Immediate resynchronization** button appears.

The data to be synchronised must be configured:

- In the Subscriber mapping tab for internal records. Refer to Section **3.17.1.2 - Subscriber mapping (internal records).**
- In the External contacts mapping tab for external records. Refer to Section **3.17.1.3 - External contacts mapping.**

Click Immediate synchronization to start the synchronisation. The **Synchronization** field appears to show the synchronisation progress status.

After the first synchronisation, the menu displays a synchronisation report table, with:

- The date and time of the latest synchronisation,
- The status of the last synchronisation (Success or Failure),
- The number of internal records successfully created,
- The number of internal records edited,
- The number of external records created,
- The number of external records edited,

The synchronisation of the external directory generates an alert in the log. See Section **4.2.1– Logbook display**. If internal records have been created during synchronisation, MiVoice 5000 also sends an email to the administrator to notify them.

For internal records, further configuration is required in Menu **Telephony service>Subscribers>External directory synchronization>Follow-up**. See Section **3.17.2 – Follow-up**.

3.12.1.2 Subscribers mapping (internal records) tab

Filter on external directory

Field to be filled in. Specifies the set of subscribers to include from the external directory for synchronisation, using LDAP search filter format.

Example: (&(objectCategory=person)(objectClass=user))

⚠ **WARNING: If the Filter on external directory field is empty, subscriber synchronisation is disabled.**

Default hierarchy

Dropdown list. Defines the administrator hierarchy to be assigned to subscribers whose hierarchy could not be retrieved during synchronisation.

Two tables list all the attributes affected by the synchronisation of internal records.

- The first table defines the external directory attributes (editable depending on the external directory) retrieved during synchronisation to the MiVoice 5000 directory and their equivalent attributes on MiVoice 5000 Call Server:
  - LDAP reference for resynchronisation (**cleExt** in MiVoice 5000 directory attribute)
  - Name (**displayName** in MiVoice 5000 directory attribute)
  - First name (**displayGn** in MiVoice 5000 directory attribute)
  - Hierarchy (**hierarchySV** in MiVoice 5000 directory attribute)
  - Type (**type** in MiVoice 5000 directory attribute)
  - Function (**function** in MiVoice 5000 directory attribute)
  - User login **userPrincipalName** in MiVoice 5000 directory attribute)
  - Mail (**mail** in MiVoice 5000 directory attribute)
  - Location (**localisationDesc** in MiVoice 5000 directory attribute)
  - Mobile (**mobile** in MiVoice 5000 directory attribute)
  - Picture (**photo** in MiVoice 5000 directory attribute)
- The second table defines the MiVoice 5000 directory attributes retrieved during synchronisation to the external directory and their equivalent attributes on the external directory (editable according to the external directory).
  - DID number **DidNumber** in MiVoice 5000 directory attribute)
  - Main number **MainlineNumber** in MiVoice 5000 directory attribute)

3.12.1.3 External contacts mapping tab

Filter on external directory

Field to be filled in. Field to be filled in. Specifies the set of subscribers to include from the external directory for synchronisation, using LDAP search filter format.

Example: (&(objectCategory=person)(objectClass=contact))

⚠ **WARNING: If the Filter on external directory field is empty, subscriber synchronisation is disabled.**

A table defines the attributes of the external directory retrieved during synchronisation to the MiVoice 5000 directory and their equivalent attributes on MiVoice 5000 Call Server:

- LDAP reference for resynchronisation (**cleExt** in MiVoice 5000 directory attribute)

- Name (**displayName** in MiVoice 5000 directory attribute)
- First name (**displayGn** in MiVoice 5000 directory attribute)
- Phone number number **phoneNumber** in MiVoice 5000 directory attribute)
- Type (**type** in MiVoice 5000 directory attribute)
- Mail (**mail** in MiVoice 5000 directory attribute)
- Location (**localisationDesc** in MiVoice 5000 directory attribute)
- Picture (**photo** in MiVoice 5000 directory attribute)

3.12.2 FOLLOW-UP

Menu **Telephony Service>Subscribers>External directory synchronisation> Follow-up**

This menu groups the subscriber records created during synchronisation between MiVoice 5000 and the external directory, in table form.

Two actions are possible from this table:

- For a record to be kept, enter an existing number from the MiVoice 5000 directory in the **Directory number** field.

⚠ **WARNING: If the directory number entered already has data in its subscriber record, it will be deleted and replaced by data from the external directory after validation.**

- For a record to be deleted, select **YES** from the drop-down list in the **Delete** column.
- After editing the necessary fields, click Validation to:
  - Save the information retrieved from the external directory to existing directory records.
  - Delete the records with **YES** in the **Deletion** column.

4 SYSTEM MANAGEMENT

This management domain is used to:

- Define the device miscellaneous parameters like date and time, device name, etc.
- Enter the key code which gives access to the functions
- View the system hardware and software configurations
- Monitor the system
- Configure the device
- manage and assign security certificates,
- Perform backup, restore and device update operations
- Restart the system
- Deploy investigation tools to solve problems
- Manage the list of Mitel proprietary terminals.

To access this menu, click "SYSTEM" from the system user interface main page.

4.1 DEVICE INFORMATION

Menu **SYSTEM>Info**

This menu is used to:

- Configure the system miscellaneous parameters (date and time, system name)
- Enter the key code and view the authorised functions
- View the system software and hardware configuration
- view the software and hardware configuration of sites in a multi-site configuration
- view the utilisation status of the different elements that can be configured on the system via an inventory function.

4.1.1 DATE AND TIME

NTP server: 2 servers + Security

Menu **SYSTEM>Info>Date and time**

This command allows you to set the system date and time and to define, if necessary, a network synchronisation to one or two time servers.

Note: Changing the date and time is also allowed for the Maintenance profile.

DATE (FORMAT DD/MM/YYYY)

Enter the day (dd) and month (mm), using 2 digits for each value, and the year (yyyy), using 4 digits, depending on the format indicated.

TIME (FORMAT HH:MM:SS)

Enter the hour (hh), minutes (mm) and seconds (ss) using 2 digits for each value, depending on the format indicated.

NETWORK SYNCHRONISATION

If you tick this box, the system updates its DATE and TIME settings at regular intervals using the values retrieved from the NTP server(s) defined in the following field.

- TIME SERVER 1 OR 2

DNS name or IP address of the NTP in question.

- SECURE MODE

This box is used to secure access to this server.

Security is provided by a key (in MD5 or SHA1 format) and a shared secret:

Key: Value between 1 and 65534

Format: MD5 and SHA1

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]).

- STATUS

Information field which gives the NTP server status:

- connected or not connected: status of connection to NTP servers.
- Synchronised, not synchronised: Status of synchronisation to NTP Servers

TIME ZONE:

☞ This parameter is not available for a MiVoice 5000 SERVER.

These parameters enable the system to:

- Manage automatically summer / winter time changes if network synchronisation is not used
- Translate into local date and time the date and time information given by the NTP server if network synchronisation is used.

To define the time zone, select a region then a town located in this region.

- REGION

AFRICA **AMERICA** **ANTARCTIC** **ARCTIC** **ASIA** **ATLANTIC**
AUSTRALIA **EUROPE** **INDIA** **PACIFIC**

- TOWN

The content of this drop-down list depends on the region selected.

4.1.2 PARAMETERS

Menu **SYSTEM>Info>Settings**

This command is used to:

- Choose the language used for progressive print outs (printing out the logbook on a printer)
- Name the system.

DEFAULT SYSTEM LANGUAGE

FRENCH **ENGLISH**

Language used to progressively print out the logbook with a printer.

INSTALL. NAME

Character string (24 ASCII characters) used to identify the system. This character string appears:

- In the navigator title bar, on the top left side
- In the system user interface information frame.

INTEROPERABILITY DATA

Indicator of interoperation between versions.

The value indicates the number of telephone releases separating the version of a site from the oldest version available on the multi-site network.

This line is only proposed in a multi-site configuration.

NONE: no interoperation.

Other values:

- 1 VERSION
- 2 VERSIONS
- 3 VERSIONS
- 4 VERSIONS

The maximum value is 4 versions.

As of R5.3 the minimum release is R4.1, which implies that: -> Releases earlier than R4.1 are no longer managed, so the number of telephone releases separating the current release and the oldest release in a multi-site configuration cannot be above 4.

4.1.3 LICENCES

Menu **SYSTEM>Info>Licences**

Note: For a cluster configuration, additional two tabs are available for the distribution of SIP LINK and MEDIA SERVER licences. In this type of configuration, licences can be distributed to the Cluster Server and to each Node.
See the document "Implementing a MiVoice 5000 Cluster".

This command is used to enter the software key code which gives access to the different management functions and sets the system table size.

For a virtual Mitel 5000 Server, to declare the virtual dongle licence, the fields and steps are different. See the document MiVoice 5000 Server - Implementation.

The licence management screen displays (non-virtualised system):

- A frame containing information about installation and key code
- An information table containing a list of rights (in terms of available functions) and limitations (in terms of sizes) associated with the key code.

IDENTIFICATION NUMBER

Information field indicating the system identification number (code stored in the dongle protection key)

LICENSES SERVER ACCESS

This link opens a new browser window on the Mitel license server.

TYPE OF SYSTEM

Information field indicating the type of system.

SOFTWARE VERSION

Information field indicating the system software release.

KEYCODE

The keycode provided by the installer.

The encoding of the keycode takes account of the previous three parameters and the purchased configuration (size, list of functions).

KEY STATE

This field indicates the current licence status:

- Invalid licence,
- No licence entered,
- Valid licence,
- Licence to be validated,
- Incompatible IP address,
- Incompatible installation code,
- Missing dongle.

Note: for a redundant MiVoice 5000 system, an additional tab on the master machine is used to view information about the slave machine.

4.1.4 SOFTWARE IDENTIFICATION

Menu **SYSTEM>Info>Settings>Software identification**

This command is used to display:

- The software release installed on the CPU card
- The composition of the active directory (production, patches) and its status (validated, test)
- The composition of the inactive directory and its status
- The list of languages available for the MMCs
- The list of languages available on the sets declared on the system (by set type)
- The software releases of the cards.

4.1.5 MULTI-SITE SITES IDENTIFICATION

Note: This command is only accessible in multi-site configuration.

Menu **SYSTEM>Info>Settings>Multisite sites identification**

This command is used to display for each site in a multi-site configuration:

- The type of system
- The software release installed on the system.

The "Site name" column of the displayed table contains, for each site in the multi-site configuration, the site number followed by site name as defined using the menu **NETWORK AND LINKS>Multisites>Definition of centers and sites>Local site and center** on each of the sites.

4.1.6 INVENTORY

Menu **SYSTEM>Info>Inventory**

This command is used to view the system configuration in terms of the number of elements configured and the maximum configuration authorised by, on the one hand, the system capacity constraints and, on the other, the limitations relative to the functions subject to unlocking.

The **Licenses server access** link at the bottom of the screen opens a new browser window on the Mitel license server.

The screen displayed presents the inventory in form of five summary tables.

4.1.6.1 *Inventory of the subscriptions*

INTERNAL	LOCAL type subscribers.
SECONDARY	Secondary directory numbers created by the Multi-line feature.
BACKUP	Backup directory numbers of a local subscriber of another site. These numbers are created automatically on assigning a backup site to a subscriber (Dual Homing function).
MULTIUSER	MULTIUSER type subscribers.
SERVERS	AUTOMATIC ATDC or DISA type subscribers.
GENERAL PURPOSE	Number of sets that can be used at the same time. **Note: the general purpose subscriber is only counted for one subscription.**
ATDC	ATDC type subscribers.
GROUP	HUNT GROUP type subscribers.
SUPER GROUP	SUPER GROUP type subscribers.
VOICE MAIL GROUP	VOICE MAIL GROUP type subscribers.
INTEGRATED V MAIL	V MAIL type subscribers. INTEGRATED.

4.1.6.2 *Inventory of assignments*

MSITE_ANALOG	Analogue terminals declared on the site and connected on another site.
PROPRIETARY MSITE	Proprietary sets declared on the site and connected on another site.
MOBILE DECT	MOBILE DECT type sets.
MOBILE DAS	MOBILE DAS type sets.
PROPRIETARY IP	PROPRIETARY IP terminals (i7xx and MiVoice 5300 IP phone).
SIP	Mitel SIP (6xxxi, 312i) and non Mitel SIP terminals.
IP DECT	IP DECT and SIP DECT terminals.
EXTERNAL SET	Call forking feature
SIP DECT CONFERENCE	Conference management by Mitel SIP DECT
DS_ON_PC	i2052 type sets in VoIP mode.
VTI/XML IP	UCP IP, CC.
H323	H.323 terminals.

4.1.6.3 *Inventory of the declarations subject to unlocking*

The list of licences for IP terminals and the associated terminals is given in Section 4.1.6.3.2.

4.1.6.3.1 Licence for IP or SIP DECT terminals

IP DECT / SIP DECT

IP DECT and SIP DECT terminals require a **MOBILE** licence.

4.1.6.3.2 Inventory of declarations subject to unlocking (MiVoice 5000 server)

Specific lines concerning MiVoice 5000 Server.

MEDIA SERVER	Number of RTP flows for media Server
STANDARD IVBS	Number of standard IVBs
UNIFIED IVBS	Number of unified boxes
XML SGML/ATDC	i2070

The excess column applies only to standard IVB and unified IVB licences.

As of R6.2, it is possible to declare a standard IVB with unified IVB licences within the total number of IVBs <= total number of licences).

4.1.6.4 *Inventory of number declarations*

LOCAL	Local numbers
DID OTHERS	DID numbers defined outside external number blocks.
GENERAL DID	DID corporate numbers defined in the "incoming" dialling plan. **Note: these numbers correspond to the numbers used to access the reception services from outside.**
NAME_BLOCK_NUM	External dialling blocks defined in the "i/c" dialling plan. **Note: as many lines as defined external dialling blocks appear.**

4.2 SUPERVISION

Menu **SYSTEM>Supervision**

This menu is used to:

- Display the logbook
- Delete the logbook
- Display the statuses of the different system components
- Configure traffic observation
- Display and reset traffic observation counters
- Display and reset charging counters
- Know the status of the system in terms of capacity (rate of use of system resources)

4.2.1 LOGBOOK DISPLAY

Menu **SYSTEM>Supervision>Disp. Logbook**

The logbook contains system-operation-related recordings.

The logbook can contain up to 320 recordings.

The logbook lists a certain number of events that occurred during operation: information or error (hardware or software errors or faults):

- Information-type events can be interpreted by the user.
- Software data can be interpreted by the manufacturer.

The logbook can also display service records (by family):

- Agenda/alarm family
- Prepayment family
- Monitoring family
- Features family
- C.Dist family
- Alarms.

Note: When the logbook is saturated (i.e. when the number of messages in the logbook mailbox reaches 40), the logbook switches over to "congestion" mode, which means that the reception of all the messages is no longer guaranteed (some messages may be deleted). The message "Logbook: congestion" is displayed in the logbook. When the logbook returns to normal mode, the message "Logbook: normal lost: xx" appears, specifying the number of messages deleted during the congestion phase.

LOGICAL SECURITY BLOCKS

Automatic system maintenance sees the configuration as a set of hierarchically arranged logical security blocks (SBL). This decomposition allows the system to identify the faulty hardware component in the event of a failure and to react accordingly: following the detection of an error, automatic maintenance can take a defensive action. This involves changing the status of the security block that covers the defective hardware element.

Example: ******LA8 :0, 0, .. ** FAULTY**

The fail-safe action report is recorded in the logbook and contains the following information:

- The type of security block that changed status
- The security block number
- The new security block status

The security block statuses have the following meaning:

NOT EQUIP. The SBL is not equipped in the associated configuration table.

OUT OF SRV The SBL is inaccessible by the software and cannot take part in network operations. This occurs, for example, when the SBL one step up in the hierarchy is faulty.

This status is also the initial status of all SBLs before startup.

DOWNLOAD The processor associated with the SBL is being downloaded.

IN SERVICE SBL participates in normal operation.

FAULTY Error detected in an SBL function. Automatic maintenance has withdrawn this SBL from operational state.

DISABLED The maintenance operator has withdrawn the SBL from operational state, using an operator command.

Other special statuses:

IN PARKING A telephone subscriber did not hang up their phone (off-hook) or a proprietary TDM terminal has been disconnected.

4.2.2 DELETING THE LOGBOOK

Menu **SYSTEM>Supervision>Delete logbook**

PASSWORD

Enter the password then click **Delete logbook**.

If the rights associated with the password are sufficient, the logbook is reset; otherwise, the operation is rejected by the system.

At the end of the operation, the screen displays **Logbook deleted**.

4.2.3 DISPLAY STATUSES

Menu **SYSTEM>Supervision>Display statuses**

This menu is used to display the status of the different system components:

- Subscribers
- IP terminals
- external lines
- Voice resources (VoIP)
- Trunk groups
- Data links
- Cards and equipment
- Portable handsets
- TCP tunnel connections

4.2.3.1 *Extensions*

Menu **SYSTEM>Supervision>Display statuses>Telephone extensions**

This command is used to display a list of extensions (according to status and/or directory number), indicating:

- The extension number
- The extension type
- The extension status
- And, possibly information about the terminal assigned to the extension

STATUS SEARCHED

ANY	Any status
FREE	In service and free
PERMNT	In conversation
BUSY. UNSTABLE	Setting up a call

PERM OFF-HOOK COND.	Analogue sets not on-hooked and/or digital sets not connected
OUT.OF.SERV.	Sets disabled by MMC
NO_CONNECTED	Subscriptions without terminal assignment.
INACTIVE	Inactive BACKUP type subscriptions on the backup site (calls are processed normally on the reference site)

Set status.

DIRECTORY BEGINNING WITH

Digit (or number). All sets with directory numbers associated with this digit (or number) will be displayed.

DISPLAY OF THE SETS

NO **YES**

If you select YES, the terminal type and status will be displayed in addition to information about the user.

Click **Select the item**.

The extension display table indicates:

- the subscriber’s directory number.
- The subscriber type and, on the next line, the terminal type if you had requested for terminal display (the value YES for the parameter DISPLAY OF THE SETS in the previous screen)
- the location: cabinet number, board position, board equipment number or IP address,

Note: This information is only available if terminal display had been requested for (the value YES for the parameter DISPLAY OF THE SETS in the previous screen).

- The subscriber status and, on the next line, the terminal status if you had requested for terminal display (the value YES for the parameter DISPLAY OF THE SETS in the previous screen).

For information on how to view the terminals that use the power-saving function,

See Appendix.

4.2.3.2 *IP terminals*

Menu **SYSTEM>Supervision>Display statuses>IP subscribers**

This command is used to display all IP sets declared on the system on the basis of several criteria (type of set, status of set's applicative session, directory number).

TYPE OF SET

Type of IP set searched for. Only those IP sets of the type selected declared on the system will be displayed.

To view all the IP sets declared on the system, select "**……..**".

APPLICATION SYSTEM

State of the set’s application session. Sets whose application session status is the same as the status selected will be displayed. To display all sessions, select "……..".

CONNECT.	Lists all connected IP sets (no matter the connection mode: optimised or not optimised).
UNCONNECT.	Lists all unconnected IP sets.
……….	Lists all IP sets, no matter the session status.

DIRECTORY BEGINNING WITH

Digit (or number). All IP sets declared on the site associated with directory numbers that start with this digit (or number) will be displayed.

Once the search criteria are selected, click **Select the item**.

For each listed IP terminal, the display is made on 3 lines maximum:

- The first line indicates:
- The directory number associated with the terminal (example: 2000),
- The terminal model (example: i760+ 700)
- The status of the set's application session (example: optimised)
- The CAC centre number (centre containing the main CAC server) or the CAC class number of the IP set if the terminal is part of an IP sub-network belonging to a CAC class.
- The second line (available only in case of call set-up) indicates:
- The name of the site where the IP signalling point is located (example: 002-site2),
- Number of the node where the IP signalling point is located (example: 02),
- The IP address of the login site, for an optimised session
- The third line (available only in case of call set-up) indicates:
- The IP address of the terminal, followed by the UDP port number on which the connection is set up (here: XXX.XXX.XXX.XXX:40000),
- The location number for viewing urgent callback terminals

The location number identifies the geographical area of the subnet for an IP terminal connection. It is used to manage emergency numbers. It may be the same for two closely located subnets.

The IP set display screen also displays a summary line of the application sessions for the sets that meet the selection criteria.

This line shows:

- The total number of IP terminals with optimised connection address
- The number of connected IP terminals
- The number of IP terminals that meet the set type selection criterion.

4.2.3.3 *Media Server resources*

Menu **SYSTEM>Supervision>Display statuses>Media Server resources**

This command is used to display information about the RTP resources used by the Media Server service on MiVoice 5000 Server systems when the announcement, IVR, IVB and conference functions of the Media Server are required on MiVoice 5000 Server.

For each resource, information about interconnected terminals is displayed in addition to the identification information of the resource.

The Media Server resources display table indicates:

ID COLUMN:

Gives the resource ID (0-999)

RESOURCE PORT IP COLUMN:

Gives the IP address and RTP port used by Media Server. The IP address corresponds to the IP address of Mitel 5000 Server PTX board.

USAGE COLUMN:

Indicates the service rendered by the resource taken by the Media Server service:

- TON nnn
- CONF
- IVB
- IVR
- Empty

REMOTE PORT IP COLUMN:

Gives the IP address and RTP port used by the remote resource in communication with Media Server (IP terminal or EIP terminal (Virtual TDM)).

COLUMN NO.:

Corresponds to a resource number assigned by the MMC. Right-clicking inside this column displays detailed information about the resource.

It is possible to view the next or previous resource with these buttons:

Information export is not possible.

The detailed resource information indicates:

STATUS:

Gives the Media Server resource status. This parameter is always displayed. Possible values are**:**

LABEL
INACTIVE
ACTIVE
ACTIVED FOR MESSAGE
ON HOLD
IN WAITING FORCED RELEASE
…………………………………………….

Date OF SEIZURE: Gives the date of seizure of the Media Server resource, in the format DD/MM/YY HH :MM :SS or (MM/DD/YY HH :MM :SS depending on the configuration). This parameter is always displayed.

IP: Resource port Gives the IP address and RTP port used by Media Server. The IP address corresponds to the IP address of Mitel 5000 Server PTX board.

USE: Indicates the service rendered by the resource taken by the Media Server service. This parameter is always displayed.

The possible responses and underlying settings are given in the tables below:

RESPONSE LABELS
MESSAGE FOR USER MESSAGE FOR EXT. LINE
CONFERENCE
IVB
IVR
…………………………………………..

RESPONSE LABELS	UNDERLYING PARAMETERS	
MESSAGE FOR USER MESSAGE FOR EXT. LINE	Use - Tone No.	MESSAGE FOR USER 6
CONFERENCE	Use - Conference Id	CONFERENCE 0
IVB IVR	Use - Session No.	IVB or IVS 0

- TONE No.: This parameter is only displayed if the value of the **Use** parameter is **MESSAGE FOR USER** or **MESSAGE FOR EXT.LINE**. This parameter comprises a zoom command towards the tone definition menu.

IP:REMOTE PORT

Gives the IP address and RTP port used by the remote resource in communication with Media Server (IP terminal or EIP terminal (Virtual TDM)).

CONFERENCE ID

Gives the conference ID. This parameter is only displayed if the value of the **Use** parameter is CONFERENCE.

SESSION N°.

This parameter is only displayed if the value of the Use parameter is IVB or IVS.

MEDIA

This parameter is always displayed. Possible responses are:

RESPONSE LABELS
AUDIO
AUDIO+ENCRYPTION
FAX PASSTHROUGH
FAX PASSTHROUGH+ENCRYPTION
MODEM PASSTHROUGH
MODEM PASSTHROUGH+ENCRYPTION
FAX T.38
VIDEO
………………………………………………..

CODING LAW

This parameter is displayed if the the **Media** is neither **FAX T.38**, nor **VIDEO**.

Possible responses are:

LABELS
G711
G722
G723
G729
P711/PRIV._G711
P723/PRIV._G723
P729/PRIV._G729
…
………………………

- AT TYPE

This parameter is displayed if the the **Media** is neither **FAX T.38**, nor **VIDEO**.

Possible responses are:

LABELS	CODING LAW
A LAW	G711 P711/PRIV._G711
MU LAW	
G723.1	G723 P723/PRIV._G723
G729	G729 P729/PRIV._G729
G729A	
G729B	

G729AB	

DURATION OF PACKETS (MS)

This parameter is displayed if the the **Media** is neither **FAX T.38**, nor **VIDEO**. It gives the packet transmission interval in ms.

Before display, and depending on the encoding law, a multiplier coefficient is applied to the **packetisation** field.

CODING LAW	COEFFICIENT
G711 P711/PRIV._G711	X 1
G723 P723/PRIV._G723	X 30
Other coding laws	X 10

FORCED RELEASE

This button or parameter is only displayed if the **status** of the Media Server resource is different from **IN WAITING FORCED RELEASE**. Pressing this button forces the value **IN WAITING FORCED RELEASE** into the **status** field. This will result in the release of the Media Server resource through audit (5 minutes maximum) and should only be used for a blocked Media Server.

WARNING: Automatic release does not apply to calls made from priority terminals (subscription characteristics).

4.2.3.4 *Inter-iPbx links*

4.2.3.4.1 Connections of TCP tunnel

SYSTEM>Supervision>Display status>Connections of TCP tunnel

This command is used to display the status of TCP tunnel connections.

Note: This command is only available in multi-site configuration. For the TCP connection configuration, see the MiVoice 5000 Operating Manual: multi-site management.

The TCP tunnel display table indicates:

- The connection name
- The directory number associated with the connection
- The status of the connection (connecting, connected, disconnected)
- The number of communicating logical channels

4.2.3.5 *Data links*

Menu **SYSTEM>Supervision>Display statuses>Data links**

This command is used to display the system’s data link status.

The data link display table indicates:

- The data link type
- The directory number associated with the link

- The link status:
- Out of service: out of service and in disabled status,
- Disconnected: in service but busy (terminal OFF, level 2 not set up, etc.),
- Recovery: recovering Level 3,
- Free: in service and waiting for a call,
- In call: in communication (the number of communications is shown by the NO.LC parameter)
- The fifth column "NO.LC" indicates the number of logical channels in communication.

4.2.3.6 *Maintenance*

4.2.3.6.1 Maintenance status

Menu **SYSTEM>Supervision>Display status>Maintenance>Maintenance status**

The maintenance software manages the status of each of the SBLs in the system: a card is an SBL, a piece of equipment on a board is a lower-ranked SBL.

This command is used to display the maintenance status of the system SBLs.

The maintenance status display screen indicates the site's hardware status. The level of site defect determines the level of operation anomalies presented by the system when the maintenance status display request is made. It is an entity that ranges between 0 and 8, where 8 is the most serious defect level. The calculation of this global indicator takes account of the status of each SBL in the system to which weighting coefficients are assigned according to their criticality for the working of the system.

Clicking the ⊞ symbol located on the left side of each card’s slot displays the card’s equipment details:

The Maintenance status display table gives for each card:

- The physical location of the SBL in the following format: cabinet number, card number, and equipment number (if the SBL is a device),
- The SBL card type
- The equipment type, if the SBL is a piece of equipment
- The SBL status.

4.2.3.7 *Mobile location*

Menu **SYSTEM>Supervision>Display statuses>Mobile location**

This menu is used to display the status of each mobile set declared on the system:

- Either for all the mobile terminals (“Mobile basis”) or
- For the mobile terminals attached to a given cell (“Cell basis”).

4.2.3.7.1 Mobile basis

This command is used to display the status and location of all the mobiles.

To access this command, click “**Mobile basis**” from the menu **SYSTEM>Supervision>Display status>Mobile location**.

The list of mobiles is displayed in form of a table, showing:

- The mobile's directory number
- The mobile's reference cell
- The last cell in which the mobile was located: if the cell is internal, the field gives the cell ID; if the cell is remote, the field gives the number of the remote site followed by the cell ID
- The mobile status: LOCAL, MISL., LOST or WAITING_RECORDING.

4.2.3.7.2 Cell basis

This command is used to display, for a given cell, all the mobiles attached to this cell.

To access this command, click "Cell basis" from Menu **SYSTEM>Supervision>Display status>Mobile location**.

SELECT THE CELL

Cell name.

The drop-down list contains a list of cell names declared on the system.

Select a cell name then click **Select the item**.

Note: Selecting "…….." is the same as selecting the first cell name from the drop-down list.

The list of mobiles attached to the selected cell is displayed in form of a table, showing:

- The base station location
- The base station number
- The mobile's directory number
- The site name
- The mobile status: located, busy..

4.2.3.8 *Failed connections*

This command is used to view IP terminals not registered on MiVoice Server.

The list of unregistered terminals is displayed in form of a table, showing:

- The terminal directory number of the unregistered terminal,
- The IP address of the unregistered terminal,
- The MAC address of the unregistered terminal,
- The reason why the registration failed,
- The date and time the registration failed.

Note: The table may contain up to 200 entries. Once this limit has been reached, new entries replace the oldest ones.

The drop-down list is used to select the items to be deleted according to your choice:

- "Select all" selects all unregistered IP terminals,
- "Unselect all" unselects all unregistered IP terminals,
- "Choose selection", for manually selecting unregistered IP terminals.

4.2.4 TRAFFIC OBSERVATION

Menu **SYSTEM>Supervision>Traffic observation**

This menu is used to:

- Configure the observation of traffic on trunk groups
- Display trunk group traffic observation counters
- Display and reset the traffic observation counters for wireless sets
- Display and reset the traffic observation counters for the CAC server.

4.2.4.1 *Definition of trunk group observation*

Menu **SYSTEM>Supervision>Traffic observation>Define trunk group observation**

This command is used to define the parameters of the following trunk group observation parameters:

- The observation frequency
- The observation duration
- An eligibility criterion for sample storage
- The list of observed trunk groups (a maximum of 8 trunk groups can be observed at a given moment).

SAMPLING TIME

10 MIN **20 MIN** **30 MIN** **60 MIN** **1MIN (test)**

Interval between two measurements.

OBSERVATION PERIOD IN HOURS

Total observation period (HH): The observation period is infinite if this field is not filled in.

START DATE

Information field indicating the observation start date.

MINIMUM RATE OF RECORDING

Busy status percentage (in 2 digits) above which samples are stored.

A maximum of 256 samples can be stored. When a total of 256 samples is reached, the oldest samples are deleted by the new samples.

This parameter is used to store only the "significant" samples, to avoid overwriting a significant sample with a non-significant sample.

X RECORDS, RESET

NO **YES**

Note: This field is present only if some samples have been stored.

If you select YES, the stored samples will be deleted.

LIST OF TRUNK GROUPS MONITORED

Lists from 1 to 8 **••••••••** **BRI.TG** **ANA.TG**

Trunk groups to observe.

4.2.4.2 *Display trunk groups observation*

Menu **SYSTEM>Supervision>Traffic observation>Disp. Trunk groups observation**

This command is used to display the observations collected for a particular trunk group or for all trunk groups.

TRUNK GROUP SELECTION

Name of the trunk group to be displayed.

The drop down list contains the names of the trunk groups declared on the system, as well as the field “**.......**”, which means all the trunk groups.

MINIMUM BUSY RATE

Minimum busy rate for sample display.

This rate is only active if trunk group selection is set to "**........**”.

Note: The minimum busy rate selected is only relevant if the value selected is at least equal to the busy rate value requested for storage. (See Minimum rate of recording).

RATE IN ERLANGS

NO **YES**

If you select YES, the busy rate will be displayed in the display screen in Erlangs.

Once the display criteria are selected, click **Select the item**.

The type of display varies, depending on whether a display request applies to one trunk group or all trunk groups:

The observations of a single trunk group are displayed on only one screen: the screen title gives the name of the observed trunk group.

The observations of all trunk groups are displayed in form of a screen by observation date; the << and >> buttons are used to navigate from one date to the other; the title of each screen indicates the date of the observations displayed.

The values displayed in the trunk group observation display table are as follows:

- Way: OUTGOING or INCOMING
- Busy rate: busy rate for lines in the trunk group
- Used: number of calls in the trunk group
- Saturations: number of saturations (counted for outgoing calls only)
- Busy: busy (number of incoming calls for “busy subscribers”)
- Free: number of reception releases
- Conversations: conversation (number of voice communications)
- Quality rate

Busy rate:

Over the duration of observation, this corresponds to the average use of trunks.

This rate is calculated using the following formula:

(total busy rate for all the outgoing or incoming trunk lines) / (observation period)

A line which is 100% busy over the observation period will give a rate of 1 Erlang.

If you select NO, the busy rate will be shown on the display screen in percentage. It will then be calculated using the following formula:

(busy rate for all the trunk service lines *100) / (observation period * number of service lines)

Used

Number of calls which have arrived on the trunk and which lead to the use of a trunk (this is the case once there is a free trunk when the call arrives).

Saturations

Number of calls that arived on the trunk group and which had been rejected because no trunk was free.

Busy

"Used" (calls that lead to trunk seizure) include calls that do not reach a free subscriber (either because the called party is busy or because the caller on-hooked immediately and there was not enough time to present the call to the called extension).

Free

Number of calls released during the observation period.

Conversations

Number of communications (observations), counted during their releases.

Quality rate

This is the rate of response compared to the number of calls presented on the system. This corresponds to (conversations/used)*100.

4.2.4.3 *SIP traffic observation*

Menu **SYSTEM>Supervision>Traffic observation>Trunk groups observation>SIP traffic observation**

This menu contains a table which displays one line for each SIP trunk group on which are indicated:

- The trunk group name as defined in the trunk group name definition menu,
- The SIP link status which may be "CONNECT. " "UNCONNECT." or…. ",
- The number of calls in progress on the trunk group,

The number of authorised calls which is actually the information configured in Menu **NETWORK AND LINKS>Network>Trunk groups>Characteristics**,

- The maximum number of successful simultaneous calls,
- The number of calls rejected because the threshold has been reached,

The lines following this table contain the following information:

- On the first line, the number of licences authorised for all the multi-site or cluster/node iPBXs,
- On the second line, the number of licences assigned to the cluster or node. For standalone mode, this line is hidden as it is equal to the previous line.
- On the third line, the total number of calls rejected since the last reset,
- On the fourth line, the date of the last counter reset.

Note: The last line is a button used to reset the resettable counters: the number of successful simultaneous calls and the number of failed simultaneous calls.

4.2.4.4 *Mobile observation*

Menu **SYSTEM>Supervision>Traffic observation>Wireless observation>Mobile observation**.

This command is used to display for each mobile terminal, the number of incoming calls, with or without roaming.

The title of the screen indicates the observation start date (date on which the counters were last reset).

4.2.4.5 *reset wireless observation*

Menu **SYSTEM>Supervision>Traffic observation> Wireless observation>Reset; Wireless observation**

This command is used to reset the mobile and/or base station observation counters.

MOBILE COUNTERS

If you tick this box, mobile counters (see MOBILE OBSERVATION) are reset upon confirmation.

BASE STATION COUNTERS

If you tick this box, base station counters (see MOBILE OBSERVATION and BASE STATION TRUNK OBSERVATION) are reset upon confirmation.

Tick the corresponding boxes then click "Confirmation”.

This action confirms the counter deletion request and saves the current date as the date of last counter reset for the counter category in question.

4.2.5 CAC SERVER MONITORING

Menu **SYSTEM>Supervision>Traffic observation>CAC server monitoring**

These menus contain all the statistics on calls supervised by CAC.

These statistics are managed by some dynamic counters which give the current/maximum data rates as well as the number of critical calls and rejected calls. These counters can be reset from the menu **SYSTEM>Supervision>Traffic observation>CAC server monitoring**.

The data rates are displayed in kilobits per second.

The active server is the server used to control inter-centre (in multi-site configuration) and/or inter-class flows. Therefore, the active server may refer either to the server declared as main server (normal operation) or the server declared as secondary server (operation on backup server).

4.2.5.1 *Disp. flow towards other centres*

Menu **SYSTEM>Supervision>Traffic observation>CAC server monitoring>Disp. data rate towards other centres**

This command is used to display the current values of the active CAC server counters concerning flows towards other CAC centres.

Only the counters of the centres to which the flow is limited are displayed. These counters are read in the active server

Note: This command is only available in multi-site configuration.

This display screen shows the name of the site where the active server is located and the node number (Node no. 2 for a multi-site MiVoice 5000).

The counter display table shows, for each CAC centre to which the flow is limited:

- The CAC centre name
- The current flow (in kbit/s).

Note: If a centre is attached to a transit centre, its current flow is in fact that of the transit centre. If this is the case, the symbol * is displayed.

- The current maximum flow rate reached since the counters of this type were last reset.

Note: If a centre is attached to a transit centre, its maximum current flow is in fact that of the transit centre. If this is the case, the symbol * is displayed.

- The number of calls in a critical area since the counters of this type were last reset
- The number of rejected calls since these counters were last reset
- Number of rejected video calls
- Maximum data rate towards the centre
- Possible calls: Audio, HiQ, Video (excluding the max. inter-centre data rate)

4.2.5.2 *Disp. flow per class*

Menu **SYSTEM>Supervision>Traffic observation>CAC server monitoring>Disp. data rate per class**

This command is used to display the current values of the active CAC server counters concerning flows for each CAC class defined.

Only CAC class counters with limited flow are displayed. These counters are read in the active server

This display screen shows the name of the site where the active server is located and the node number (Node no. 2 for a multi-site MiVoice 5000).

The counter display table shows, for each CAC class for which the flow is limited:

- The name of the class,
- The current flow (in kbit/s).
- The current maximum flow rate reached since the counters of this type were last reset.
- The number of calls in a critical area since the counters of this type were last reset
- The number of rejected calls since the counters of this type were last reset
- Number of rejected video calls
- Maximum data rate per class (in kbit/s)
- Possible calls: Audio, HiQ, Video (excluding the max. inter-centre data rate).

This column contains the types of calls that can be made according to current data rate, maximum data rates supported, restriction thresholds of the different call types (audio, high-rate audio, video).

4.2.5.3 *Reset the centre counters*

Menu **SYSTEM>Supervision>Traffic observation>CAC server monitoring>Centres counters reinitialization**

This command is used to display all or part of the active CAC server counters concerning flows towards other CAC centres.

Note: This command is only available in multi-site configuration.

Note: The current flow is not a counter and cannot be reset.

The screen shows the name of the site where the active server is located and the node number (Node no. 2 for a multi-site MiVoice 5000).

COUNTRES:MAXIMUM FLOW REACHED

If you tick this box, this counter will be reset after confirmation.

The current maximum audio and video data rates will also be reset.

CRITICAL AREA CALLS COUNTERS

If you tick this box, this counter will be reset after confirmation.

REFUSED CALL COUNTERS

If you tick this box, this counter will be reset after confirmation.

REFUSED VIDEO CALLS COUNTERS

If you tick this box, this counter will be reset after confirmation.

FOR THE CENTRE

Name of the CAC centre whose counters are to be reset.

The drop-down list contains the CAC centre names. To reset the counters for all the CAC centres, select "**……..**".

After selecting the counters to be reset, click "Confirmation” to validate the reset operation.

Note: Already set alarms (returned via the logbook) are not implicitly “also” reset. The end of alarm remains indicated after a few minutes without alert or rejection.

4.2.5.4 *Class counters reinitialization*

Menu **SYSTEM>Supervision>Traffic observation>CAC server monitoring>Class counters reinitialization**

This command is used to display all or part of the active CAC server counters concerning flows by CAC class.

Note: The current flow is not a counter and cannot be reset.

The screen shows the name of the site where the active server is located and the node number (Node no. 2 for a multi-site MiVoice 5000).

COUNTRES:MAXIMUM FLOW REACHED

If you tick this box, this counter will be reset after confirmation.

The current maximum audio and video data rates will also be reset.

CRITICAL AREA CALLS COUNTERS

If you tick this box, this counter will be reset after confirmation.

REFUSED CALL COUNTERS

If you tick this box, this counter will be reset after confirmation.

REFUSED VIDEO CALLS COUNTERS

If you tick this box, this counter will be reset after confirmation.

FOR THE CLASS

Name of the class for which the counters will be reset after confirmation.

Note: If no CAC class is specified, it will be applied to all the CAC classes.

After selecting the counters to be reset, click "Confirmation” to validate the reset operation.

Note: Already set alarms (returned via the logbook) are not implicitly “also” reset. The end of alarm remains indicated after a few minutes without alert or rejection.

4.2.5.5 *CAC servers status*

Menu **SYSTEM>Supervision>Traffic observation>CAC server monitoring> CAC servers status**

For each CAC centre, this command is used to know the site on which the main CAC server is located and the site on which the secondary server is located.

Note: This command is only available in multi-site configuration.

4.2.5.6 *MEDIA SERVER statistics*

Menu **SYSTEM>Supervision>Traffic observation>Media Server statistics**

This menu gives access to the Media Server statistics. The information is displayed in a table.

The first line of the table contains the functional status of the different functions offered by the Media Server (announcements, IVB, IVR and CONF). The two possible statuses are:

ACTIVE: the function is enabled.

INACTIVE: the function is not enabled.

The last three lines of the table indicate the following values for each function offered by the Media Server (announcements, IVB, IVR and CONF):

No used: the current number of channels used (instant value),

Max hold*: maximum number of channels taken (pic)

Failure*: number of failed channel utilisation attempts.

**Since the last counter reset or Mitel 5000 Server restart.*

The last table column (**All**) indicates all the functions offered by the Media Server (for all the applications):

- The current number of channels taken (instant value)
- The maximum number of channels (pic) used since the counters were last reset
- The number of failed channel utilisation attempts.

The first line displayed under the display table gives the number of channels unlocked by the keycode.

The second line under the table gives the date/time the counters were last reset.

The **Reset the counters** button is used to reset the M**ax used and Failure** counters. This button is also used to set the date of last reset to current date/time.

Note: No confirmation is required when the button is pressed.

4.2.6 DISPLAY OF CHARGE COUNTERS

Menu **SYSTEM>Supervision>Disp. Charge counters**

Charge counters measure the calls handled by the system and give information about the cost of the various items configured in the system.

This menu is used to display the charge counters:

- By subscriber
- By department (in multi-company configuration)
- By operator service
- By external network line
- By trunk group

It is also used to reset the counters selectively.

4.2.6.1 *Extension counters*

Menu **SYSTEM>Supervision>Disp. Charge counters**

This command is used to display the extension charge counters since the last extension counter reset.

COMPANY SELECTION

xxxxxxxx **CMPNY.0**

This field is only available in multi-company configuration.

Select to display the extension counters for all companies and departments. If you have already created company names, these are displayed here.

DISPLAYED COUNTERS THRESHOLD

Minimum value for displaying the counters (counters whose value is below the threshold will not be displayed). This value is expressed in number of telephone units.

DIRECTORY BEGINNING WITH

Enter a digit (or number). All directory numbers that start with this digit (or number) will be displayed.

Once the display criteria are selected, click **Select the item**.

The extension counter display table indicates:

- The directory number
- The subscriber name
- The date (DAY/MONTH) on which the extension charge counters were last reset.
- The number of CUs (Charge Units)

4.2.6.2 *department counters*

Menu **SYSTEM>Supervision>Disp. Charge counters**

This command is used to display all the extension counters by company/department.

Note: This command is only available in multi-company configuration.

The department counter display table shows for each department:

- The company name
- The department name
- The number of extensions in the department
- The date (DAY/MONTH) on which the department charge counters were last reset.
- The number of CUs (Charge Units)

4.2.6.3 *Reset counters*

Menu **SYSTEM>Supervision>Disp. Charge counters**

This command is used to reset the charge counters. The reset operation is performed selectively on any type of charge counter.

EXTENSION AND DEPARTMENT COUNTERS

NO **YES**

If you select YES, the extension and department charge counters are reset.

"Department" counters are only significant in multi-company configuration.

OF COMPANY

This field appears in multi-company configuration if you select YES in the previous field. The drop-down list contains the priority classes defined in the system.

AND DEPARTMENT

This field appears in multi-company configuration if you select a company name in the previous field. The drop-down list contains the names of the departments declared for the company.

4.2.7 FILLING STATUS OF TABLES

Menu **SYSTEM>Supervision>Filling status of tables**

This command is used to know the status of the use of each system function table.

This screen displays the filling status of each function table by indicating for each of them the quantity used, as well as its total capacity.

Note: It is important to check availability before offering or selling certain features.

4.3 SYSTEM CONFIGURATION

The functions of the columns in this menu are:

SERVICES:

- Define the system configuration type (single/multi company, single/multi site).
- Start/stop the services that manage the different functions of the system.
- Activate an interface used to manage pictures.

LANGUAGES:

- List the spoken languages for voice prompts and announcements.
- Configure the written languages used to indicate messages on sets.

USERS:

- Manage users from the profiles defining their characteristics and access rights.
- Manage the different codes and access accounts (manufacturer, FTP server for terminal management).

CARDS:

- Manage system cards (CPU cards, general-purpose cards).

OPERATING TERMINALS:

- Manage and configure operating terminal accesses.

ALARMS:

- Configure the alarms.

TICKETS:

- Configure ticket management.

E-MAIL:

- Configure the message servers used by the system to provide e-voicemail services.

MIB SNMP:

- Enter the MIB snmp description parameters.

This menu is accessible by selecting TELEPHONY SERVICE> SYSTEM> Configuration.

4.3.1 SERVICES

The menu **SYSTEM>Configuration>Services** is used to:

- Define the type of configuration (single or multi company, single or multi-site)
- Display the status of the services, start and stop them.
- Activate an interface used to manage an FTP space for terminals.

MULTI-COMPANY MANAGEMENT

If you tick this box, all the multi-company management menus are activated in the user interface.

On start up, the system is set to single-company configuration.

Note: When this box is ticked, it can only be unticked if the single-site characteristics have been previously restored.
• no more company other than Company 0,
• no more service other than Service 0 of Company 0,
• no more routing code other than Code 0,
• no more short code other than Code 0,
To meet these conditions, you will have to make further changes before you can delete the names created.
The change from MULTI-COMPANY to SINGLE-COMPANY is only done in very rare circumstances.

MULTI-SITE MANAGEMENT

If you tick this box, all the multi-site management menus are activated in the user interface.

The working of the system is handled by a certain number of services some of which are started upon installation (see the description of each service below).

With the occasional exception, from the user interface, all the services can be:

- Restarted if they are in the START status
- Stopped if they are in the START status
- Started if they are in the RESTART status.

LDAP SERVICE

STOPPED	START	RESTART

This service gives access to the directory's LDAP base.

This service is started upon installation.

WEB SERVICE

This service gives access to the management portal.

This service is started upon installation.

Note: The web service cannot be stopped from the user interface.

SNMP SERVICE

This service enables the system to respond to external SNMP requests.

This service is not started upon installation.

Note: In SNMP V3 mode, it is forbidden to stop this service (a warning message is returned).

SNMP TRAP SERVICE

This service retrieves SNMP traces of alarms for EX, GX and TA systems.

This service is seen as **Started** even if there is no such system associated in the configuration.

This service is actually started when an EX, GX or TA system is declared.

The **Stopped** status is independent of the presence of an EX, GX or TA system.

SNMP AGENT SERVICE

This service enables the system to issue SNMP alerts (traps).

This service is started upon installation.

SIP SERVICE

This service allows the use of SIP function.

This service is started upon installation.

FTP SERVICE

☞ This parameter is available for MiVoice 5000 Server if the FTP service has been installed in advance while installing the MiVoice 5000 Server application (Ctrl I script) or while it was being reconfigured (standard or TOTAL reconfiguration). Refer to the document MiVoice 5000 Server - Implementation.

This service is used to download software updates and set configurations.

This service is not started upon installation.

TFTP SERVICE

☞ This parameter is available for MiVoice 5000 Server if the TFTP service has been installed in advance while installing the A5000 Server application (Ctrl I script) or while it was being reconfigured (standard or TOTAL reconfiguration). Refer to the document MiVoice 5000 Server - Implementation.

STOPPED START RESTART

This service is used to download software updates for terminals A6xxd, 312i and Mitel IP DECT radio fixed parts (RFP).

This service is not started upon installation.

SSH SERVICE

This service allows you to remotely connect to the system in secure mode.

STOPPED START RESTART

This service is not started upon installation.

SYSLOG SERVICE

☞ This parameter is available for MiVoice 5000 Server if the SYSLOG service has been installed in advance while installing the MiVoice 5000 Server application (Ctrl I script) or while it was being reconfigured (standard or TOTAL reconfiguration). Refer to the document MiVoice 5000 Server - Implementation.

STOPPED START RESTART

This service is used to re-channel traces to one or two IP addresses for gradual display on a remote set.

The forwarding IP addresses are configured from Menu:

SYSTEM>Expert>Processor access>Traces>Settings.

This service is only operational if at least one redirection IP address is defined.

In normal operation, this service is STOPPED.

DHCP SERVICE

☞ This parameter is available for MiVoice 5000 Server if the DHCP service has been installed in advance while installing the MiVoice 5000 Server application (Ctrl I script) or while it was being reconfigured (standard or TOTAL reconfiguration). See the document MiVoice 5000 Server - Implementation.

This service is used to activate the DHCP server incorporated into the DHCP server of the MiVoice 5000 Server PC.

STOPPED START RESTART

For a detailed description of this feature, refer to the *MiVoice 5300 IP Phone and MiVoice 6000 SIP Phone Installation Manual - DHCP Server*.

TERMINAL SERVICE

STOPPED START RESTART

MEDIA SERVER SERVICE

START RESTART

The service offers the following functions:

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

This service is started upon installation. The "STOPPED" option is not authorised for Media Server. If the user asks for this service to stop, the error message "MODIFICATION NOT ALLOWED" is displayed.

WARNING: If the user wishes to stop a service, they must make a standard reconfiguration from the Standard reconfigure shortcut located on the desktop.

As of R5.3 SP1, the conference service is available on MiVoice 5000 Server once the service is activated (no other configuration is necessary). This service will be used once the conference master (except for terminals 6xxxi) is declared on MiVoice 5000 Server (IP or virtual TDM).

NRPE SERVICE

This menu is only visible if the service is active. This is manually validated in Menu **System>Configurations>Alarms>Settings**, or automatically if the iPbx is managed by MiVoice 5000 Manager.

The NRPE service is used to return system resources alarms to the MiVoice 5000 Manager management centre Nagios module.

STOPPED **START** **RESTART**

By default, the service is STARTED if activated.

INTERNET GATEWAY SERVICE

STOPPED **START** **RESTART**

By default, the INTERNET GATEWAY service is stopped.

The operator can access this screen directly from the Internet Gateway configuration menu via a link in the **General Settings** tab.

PROXY LDAP SERVICE

STOPPED **START** **RESTART**

By default, the PROXY LDAP service is stopped.

CLD SERVICE

☞ This parameter is available for MiVoice 5000 Server if the MiVoice 5000 is connected to CloudLink. Refer to the document **CloudLink – Deployment Guide with MiVoice 5000**.

STOPPED **START** **RESTART**

By default, the CLD service is started.

This service is used to restart the CloudLink Daemon service for the MiVoice 5000.

For a detailed description of this feature, refer to the documents **CloudLink – Deployment Guide with MiVoice 5000** and **CloudLink Daemon Solution Guide**.

TEL VPN SERVICE

STOPPED	START	RESTART

By default, the TEL VPN service is stopped.

The operator can access this screen directly from the VPN remote working configuration menu via a link in the **Server** tab.

NTP SERVICE

☞ This parameter is greyed out and only its status is displayed. It is not possible to stop or start it via Web Admin.

☞ Languages

This menu SYSTEM>**Configuration>Languages** is used to list and configure the languages that can be used by the system to present messages to telephone sets (written languages) and only to list spoken languages for tone and announcement broadcasting.

4.3.1.1 *Spoken languages*

Menu **SYSTEM>Configuration>Languages**

This menu is used to view the list of spoken languages that can be assigned to subscribers: the assignment is made via Menu **SUBSCRIBERS>Subscriptions>Characteristics>General characteristics**.

For each of these languages, it is possible to replace the standard tones of the functions with a definable tone. This operation is performed via Menu **VOICEMAIL AND TONES>Tones>Allocation of tones** – languages.

The spoken languages are fixed when the iPBX is first installed (5 at most, 2 by default) and cannot be changed.

To access this command, click **Spoken languages** from the **Languages** menu.

LANGUAGE X

Names of the spoken languages available on the iPBX.

Note: The language selected in the field SPOKEN LANGUAGE 1 serves as default language for the tones.

4.3.1.2 *Written announcements*

Menu **SYSTEM>Configuration>Languages**

This menu allows you to define the list of written languages that can be assigned to subscribers: the assignment is made via Menu **SUBSCRIBERS>Subscriptions>Characteristics>General characteristics**.

To access this command, click **Written languages** from the **Languages** menu.

LANGUAGE X

The drop-down list of each of the fields contains the name of the existing languages not yet selected from any of the other fields.

Note: The language selected in the field WRITTEN LANGUAGE 1 serves as default language for messages.
Only 5 written languages are available.

If a modification is made, the system must be restarted before it is taken into account.

4.3.2 USERS

This menu **SYSTEM>Configuration>Users** concerns the user accounts used to log on to the system's MiVoice 5000 Web Admin and to the Easy Management service.

The functions of the columns in this menu are:

Profiles names / Profiles definition:

- Define the user profiles with some associated rights according to their action field (Telephony, Directory, DHCP, Terminal service and Easy Admin service).

Profiles definition:

- Define user accounts by name, password and associated profile.

System account:

- Modify the account-access, manufacturer and terminal service passwords.

Each profile is associated with:

- A configuration level
- The right to access the directory in write mode (YES or NO)
- DHCP configuration allowed (YES,NO)
- Set download right (YES or NO)

During installation, five profiles are provided by default and can be changed by the administrator:

- INSTALLER
- ADMINISTRATOR
- MAINTENANCE
- CHARGING
- DIRECTORY
- EASY ADMIN

Another predefined profile also exists in the system, but cannot be modified. This is the XML INTERFACE profile, which corresponds to a **MiVoice 5000 Manager** or an **Easy Admin** user.

4.3.2.1 PROFILE NAMES

This menu **SYSTEM>Configuration>Users>Profile names** is used to declare some profile names on the system.

USER PROFILE 1 TO 20

Profile names declared on the system. A maximum of 20 user profiles can be declared.

During installation, the following profiles are declared and can be changed:

PROFILE NAME	ASSOCIATED RIGHTS				
	CONFIGURATION LEVEL	DIRECTORY MODIFICATION	DHCP SERVER CONFIGURATION	SET DOWNLOADING	Easy Admin
INSTALLER	Installer	√	√	√	√
ADMINISTRATOR	Administrator	√		√	√
MAINTENANCE	Maintenance				
CHARGING	Charging				
DIRECTORY	Forbidden	√			
Easy Admin	Forbidden	NO	NO	NO	√

To declare a new profile, enter its name (15 characters maximum) in the first empty field.

4.3.2.2 Profiles definition

Menu **SYSTEM>Configuration>Users>Profiles definition** is used to display and configure/modify the user profiles declared on the system.

The table for this screen shows for each user profile declared on the system:

- The profile name,
- The type of configuration to which the profile has access
- Its right to access the directory (YES or NO)
- Its right to access the DHCP configuration (YES or NO)
- Its terminal download right (YES or NO)
- Its right to modify/update announcement messages.

To modify or configure a profile, click its name, the different services are then proposed.

TELEPHONY SERVICE

INSTALLER **ADMINISTRATOR** **MAINTENANCE**

CHARGING **FORBIDDEN**

Type of configuration authorised for the profile.

DIRECTORY SERVICE

Previously related to the directory service of the Call Server. To allow the directory management, provide rights to the Easy Admin. Refer to the paragraph **4.3.2.4 – Special case of Easy Admin users**.

DHCP SERVICE

If you tick this box, the profile has the right to access the DHCP service.

TERMINAL SERVICE

If you tick this box, the profile is authorised to carry out set downloading.

EASY ADMIN SERVICE

If this box is ticked, the profile XML INTERFACE is allowed to update the announcement messages related to its associated Company/Service.

This profile is associated with the cg7450 account/XML INTERFACE profile which must be configured (with Login/Password) in the **System>Configuration>Users>User definition** menu.

4.3.2.3 *Definition of users*

This menu **SYSTEM>Configuration>Users>Operators definition** is used to display and configure/modify the user accounts declared on the system.

This menu also allows each user to choose whether or not to display the homepage photo in order to minimise the data flow.

The list of user accounts shows for each account name defined:

- The associated profile name
- The associated language (the system’s MiVoice 5000 Web Admin language).

To modify an already defined user account, click the rank number of the number to be modified in the list of user accounts. The definition screen of the user account to modify is displayed. The parameters to modify are the same as the ones described below for creating a new account.

To create a new user account, click the rank number corresponding to an empty line and fill in the following fields.

LOGIN

Character string (16 characters maximum) to be used as login to connect to the system's MiVoice 5000 Web Admin.

PASSWORD

Character string (16 characters maximum) to be used as password to log in to the system's MiVoice 5000 Web Admin.

LANGUAGE

FRENCH	**ENGLISH**	**Dutch**

User interface language associated with the user.

HIDE THE PICTURE ON THE WELCOME PAGE.

Box ticked: No photo on the welcome page

Box unticked: Picture on the welcome page.

PROFILE NAME

User profile name associated with the user account.

The drop-down list contains the names of the user profiles declared in the system.

EXECUTION MODE

- BASIC
- ADVANCED

For a given installer, execution mode may be basic or advanced. It is possible to switch from one mode to the other to configure an SIP trunk. Menu **NETWORK AND LINKS>Network>Trunk groups>Characteristics**

See Section 6.2.1.2.1.

PASSWORD NEVER EXPIRES

Box to be ticked or unticked depending on the policy defined for user passwords:

Box not ticked: No policy

Box ticked: A policy has been defined, and the password will expire at the end of the period defined in Menu **System>Web Admin password policy** and the user concerned is alerted to it by e-mail (text to be entered in the field described below).

Note: If the password policy is enabled, the password entered on the second line of this screen must check this policy even if it is indicated as "never expires".

E-MAIL

A warning text prompting the user to change his password.

When a user account is created or the password is changed, the validity period is set to the current date to force the user to change it the first time he is logging on, if the password is not indicated as "never expires".

Alarm notification by E-mail

Checkbox used to enable or disable alarm notification e-mail by the user.

When the box is checked, an additional field is offered to enter an e-mail address for users (as well as for users defined locally in nodes) even if the Web Admin password policy is not enabled.

This check box is hidden if there is an SNMP Manager in the configuration or when the **Sending E-mail on alarm issuing** checkbox in the **Alarm** tab of Menu **Telephony Service>System>Configuration>E-mail** is ticked.

Company for Easy Admin

Option concerning the selection in the field above **Profile name**.

The user in question is authorised to access the Easy Admin application to manage their messages/advertisements relating to the associated company.

The configuration of the EASY ADMIN profile is indicated in paragraph 4.3.2.2 Profiles definition and 4.3.2.3 Definition of users.

4.3.2.4 *Special case of Easy Admin users*

The configuration phases are as follows:

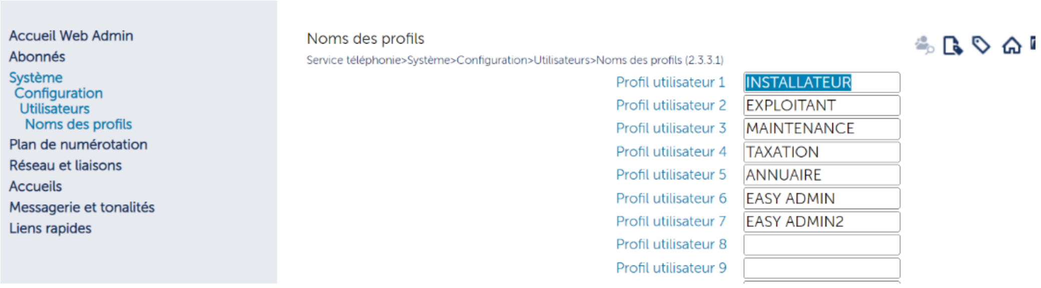
DECLARE THE MULTI-COMPANY.

- Declare the companies and associated services concerned by the Easy Admin service

Menu **Telephony service>Subscribers>Hunt groups and companies>Multi-company management**

- Create or declare a Profile authorized to use the Easy Admin service:

Menu **Telephony service>System>Configuration>Users>Profiles names**



Noms des profils

Service téléphonie>Système>Configuration>Utilisateurs>Noms des profils (2.3.3.1)

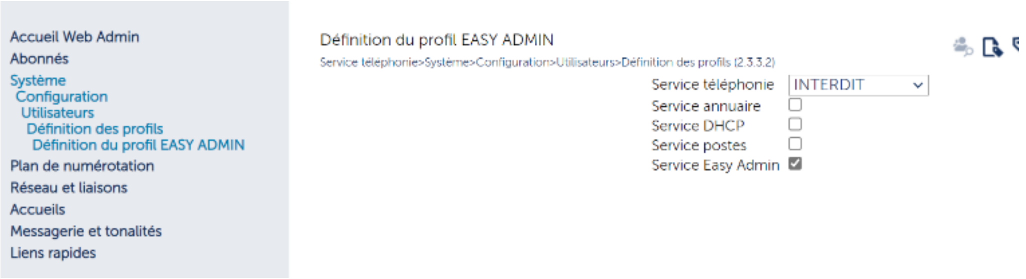
Profil utilisateur 1	INSTALLATEUR
Profil utilisateur 2	EXPLOITANT
Profil utilisateur 3	MAINTENANCE
Profil utilisateur 4	TAXATION
Profil utilisateur 5	ANNUAIRE
Profil utilisateur 6	EASY ADMIN
Profil utilisateur 7	EASY ADMIN2
Profil utilisateur 8	
Profil utilisateur 9	

PROFILES DEFINITION

The configuration of the EASY ADMIN profile is indicated in paragraph 4.3.2.2 Profiles definition and 4.3.2.3 Definition of users.

Menu **Telephony service Menu>System>Configuration>Users>Profiles definition** or direct link from the previous menu.

- Activate the Easy Admin service by ticking the corresponding box.



Définition du profil EASY ADMIN

Service téléphonie>Système>Configuration>Utilisateurs>Définition des profils (2.3.3.2)

Service téléphonie	INTERDIT
Service annuaire	□
Service DHCP	□
Service postes	□
Service Easy Admin	☑

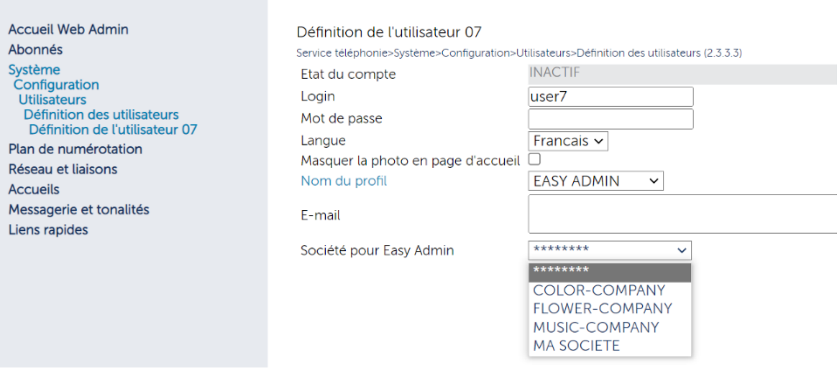
The settings accessible from Easy Admin change according to the configuration of the profile assigned to a user.

- Profiles with the Telephony FORBIDDEN service have basic access to Easy Admin, including:
  - Viewing subscriber, hunt group and IVR records,
  - Modifying subscriber directory information,
  - Managing status in hunt groups,
  - Managing voice messages,
  - Managing calendars.
- Profiles with a selected Telephony service have access to the MiVoice 5000 Easy Admin Pro interface, including, in addition to the above settings:
  - Modifying subscribers’ technical information,
  - Managing subscribers’ keys,
  - Managing subscriber forwarding,
  - Modifying hunt groups’ technical information,
  - Adding and deleting hunt group members.

DECLARE EASY ADMIN USERS BY COMPANY.

- For created users, assign the corresponding profile and associate it with the company in question.

Menu **Telephony service>System>Configuration>Users>Operators definition**



Définition de l'utilisateur 07

Service téléphonie>Système>Configuration>Utilisateurs>Définition des utilisateurs (2.3.3.3)

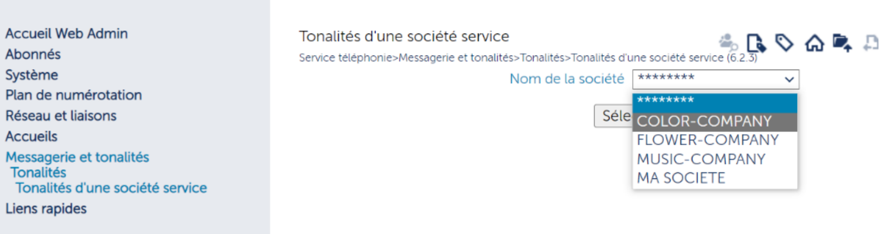
Etat du compte	INACTIF
Login	user7
Mot de passe	
Langue	Francais
Masquer la photo en page d'accueil	□
Nom du profil	EASY ADMIN
E-mail	
Société pour Easy Admin	********

****
COLOR-COMPANY
FLOWER-COMPANY
MUSIC-COMPANY
MA SOCIETE

The registered user will be able to manage all the services of the company in question.

- Declare the Tones specific to each company/department

Menu **Telephony service>Voicemail and tones> Tones>Company/department specific tones**



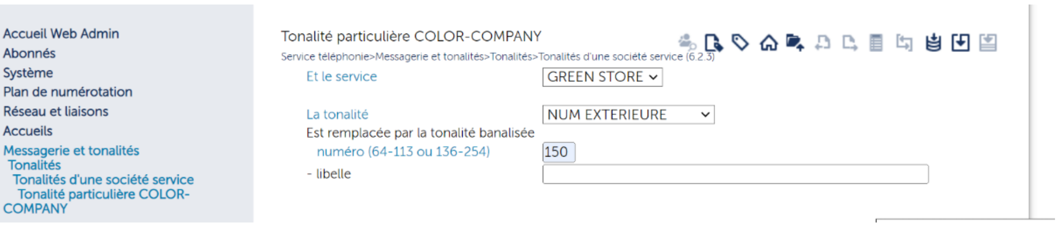
Tonalités d'une société service

Service téléphonie>Messagerie et tonalités>Tonalités>Tonalités d'une société service (6.2.3)

Nom de la société ********

****
COLOR-COMPANY
FLOWER-COMPANY
MUSIC-COMPANY
MA SOCIETE

- Assign to a predefined tone, a dedicated, standard and more explicitly renamed tone, if necessary, for use in Easy Admin.

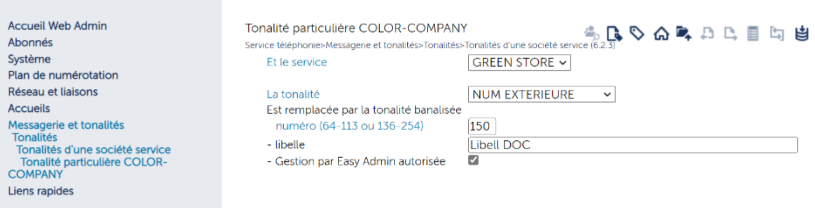


Tonalité particulière COLOR-COMPANY

Service téléphonie>Messagerie et tonalités>Tonalités>Tonalités d'une société service (6.2.3)

Et le service	GREEN STORE
La tonalité	NUM EXTERIEURE
Est remplacée par la tonalité banalisée	
numéro (64-113 ou 136-254)	150
- libelle	

- Then tick the box **Management by Easy Admin.**



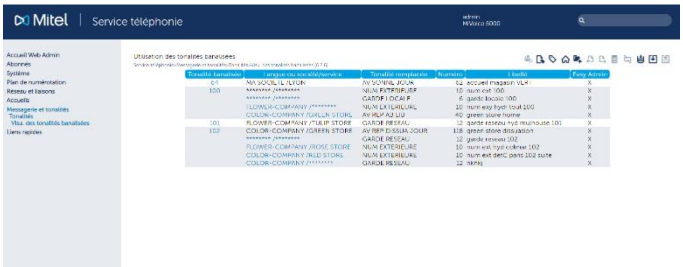
Tonalité particulière COLOR-COMPANY

Service téléphonie>Messagerie et tonalités>Tonalités>Tonalités d'une société service (6.2.3)

Et le service	GREEN STORE
La tonalité	NUM EXTERIEURE
Est remplacée par la tonalité banalisée	
numéro (64-113 ou 136-254)	150
- libelle	Libell DOC
- Gestion par Easy Admin autorisée	☑

In this configuration the **Easy Admin** end user of the company in question will be able to manage (modify, re-record, etc.) this tone with the more explicit label of the announcement in question. Please refer to the document **Easy Admin - User Guide**.

The list of all the tones intended for the Easy Admin service can be consulted in Menu **VOICEMAIL AND TONES>Tones>Display definable tones**.



Utilisation des tonalités banalisées

Service téléphonie>Messagerie et tonalités>Tonalités>Visu. des tonalités banalisées (6.7.6)

Tonalité banalisée	Langue ou société/service	Tonalité remplacée	Numéro	Libellé	Easy Admin
64	MA SOCIETE /LYON	AV SONNE JOUR	62	accueil magasin VERT	X
100	******** /********	NUM EXTERIEURE	10	num ext 100	X
	******** /********	GARDE LOCALE	6	garde locale 100	X
	FLOWER-COMPANY /********	NUM EXTERIEURE	10	num exy hydr tout 100	X
	COLOR-COMPANY /GREEN STORE	AV REP AU LIU	40	green store home	X
101	FLOWER-COMPANY /TULIP STORE	GARDE RESEAU	12	garde reseau hyd mulhouse 101	X
102	COLOR-COMPANY /GREEN STORE	AV REP DISSUA JOUR	118	green store dissuasion	X
	******** /********	GARDE RESEAU	12	garde reseau 102	X
	FLOWER-COMPANY /ROSE STORE	NUM EXTERIEURE	10	num ext hyd colmar 102	X
	COLOR-COMPANY /RED STORE	NUM EXTERIEURE	10	num ext detC paris 102 suite	X
	COLOR-COMPANY /********	GARDE RESEAU	12	hkhkj	X

4.3.2.5 *System accounts*

This menu **SYSTEM>Configuration>Users>System accounts** is used to modify the following accounts or access code:

4.3.2.5.1 Manufacturer access code

MANUFACTURER ACCESS CODE

This code is reserved for MITEL as manufacturer and is not known to the operator. This code is associated with access logins and passwords also solely reserved for Mitel (application access).

Note: For MiVoice 5000 Server, only the application access login and password are to be taken into account, since the OS access account (dedicated Linux PC) remains under the operator's responsibility.

Nevertheless, to increase the security level, it may be modified by the operator. This implies that MITEL will no longer have access to Web Admin in manufacturer mode if it is not communicated.

The choice of modification is made by the operator who may inform Mitel about it.

If this modified access code is forgotten or lost, refer to the document MiVoice 5000 Server – Installation and Implementation, which explains how to recover this access code from a specific mode of the **Ctrl + i** phase.

Authorised characters:

- Modifiable manufacturer's access code, with 4 to 15 characters
- The characters authorised for the password are "a" to "z", "A" to "Z", "0" to "9" and "_".

4.3.2.5.2 FTP accounts for MiVoice 5300 IP Phone and MiVoice 6000 SIP Phone

FTP ACCOUNTS FOR MIVOICE 5300 IP PHONE

The FTP server access accounts are used by TMA to manage terminals (for updating production and test releases as well as for the deployment phase).

Note: Concerning the management of these terminals, refer to the terminal installation manual.

By default, the passwords for all these accounts have the same values as the logins indicated for each account in question.

Authorised characters:

- Modifiable password, with 4 to 25 characters
- The characters authorised for the password are "a" to "z", "A" to "Z", "0" to "9" and "_".

Existing passwords are not displayed; they are replaced on display by the characters *, based on the maximum length (25 characters).

Production and deployment (read)

- Login

- Password

Production and deployment (write)

- Login
- Password

Test (read)

- Login
- Password

Test (write)

- Login
- Password

FTP ACCOUNTS FOR 6XXXI:

Deployment (read)

- Login
- Password

Deployment (write)

- Login
- Password

Production (read)

- Login
- Password

Production (write)

- Login
- Password

Test (read)

- Login
- Password

Test (write)

- Login
- Password

FTP ACCOUNTS FOR BLUSTAR:

Production (read)

- Login
- Password

Production (write)

- Login
- Password

4.3.3 CARDS

Menu **SYSTEM>Configuration>Cards**

This menu is used to:

- Display/modify the settings of IP cards.

For MiVoice 5000 Server only Slot 0-00 is proposed, for the PC network card.

- Then click the access concerned by the IP parameter definition.

The screen then proposes the following fields:

IMPORTANT NOTE: After these settings are defined, click Confirmation so the configuration can be taken into account.

IP ADDRESS

IP address of the PC card configured for the network in question.

If voice and administration networks are separated, this IP address corresponds to the telephony network; see USING AN ADMIN NETWORK.

USING AN ADMIN NETWORK

To dissociate the flows on MiVoice 5000 Server, one or more network cards can be used, depending on the PC configuration.

The administrator may configure the card to be used for each network (telephony or administration):

- The card dedicated to the telephony network must be indicated on top in the first IP address field.
- The card dedicated to the administration network must be indicated in the IP address field, in the Use an admin network area.

By default, the same card is used for both networks. A firewall is integrated into the A5000 Server in order to activate the data flows.

This firewall cannot be configured from Web Admin.

The administrator is responsible for configuring the firewall.

IP ADDRESS

Options list which determine the IP address dedicated to the administration network

FQDN :ADMIN

FQDN value of the iPBX which allows its access through secure connection (https) for the administration network.

UDP PORT

UDP port number of the IP card (value between 2050 and 65000)

Default value: 40000

TCP PORTS: FIRST NUMBER

First number of the IP card TCP port range (value between 0 and 65534). Default value: 41000

- LAST NUMBER

Last number of the IP card TCP port range (value between 0 and 65534). Default value: 41999

The difference between the first and last port number must be at least 500. If this difference is not respected, the second number is automatically updated to restore the difference.

FQDN:

FQDN value of the iPBX which allows its access through secure connection (https) for the telephony network.

Additional local networks*: Ability to add public class sub-networks as LANs on MiVoice 5000 Server.

This field is only taken into account if a **Let's Encrypt** Certificate has been declared on MiVoice 5000 Server.

Format: @IP/mask (*separated by spaces)

V4 and/or V6 IP address

SIP FILTER (REGISTERS/SEC)

~~Field applicable to Mitel 5000 Server only.~~

This field is used to modify the value of the GSI application field (limiting the number of registers per second).

DAYTIME FUNCTION AUTHORISED

This function is used to send the date (DayTime) to the IPS card connected to the system. This value is sent via the network either from the CPU card or the PTX card of the cabinet, according to the IP access configuration:

- For the CPU card, the box is ticked by default, thus giving priority to date transmission through the CPU card.
- For PTx cards, the box is not ticked by default.

4.3.3.1.1 Alarms

Menu **SYSTEM>Configuration>Alarms**

This menu is used to:

- Define the general alarm-processing parameters
- Configure the transmission parameters for each alarm
- Apply a global configuration to all the alarms by type of output device
- Display the current configuration of alarm transmission parameters.

4.3.3.2 *Settings*

Menu **SYSTEM>Configuration>Alarms>Settings**

This menu is used to define the general settings which apply:

- To the processing of alarms returned by the system:
- possible generation of a service record
- addresses of the different output devices
- To the validation of alarms: management of dry loops.
- Configure the alarm thresholds of system resources alarms generated by NRPE

This menu comprises three tabs:

- Alarms management
- Alarms validation,
- NRPE configuration

4.3.3.2.1 Alarms management tab

SERVICE BILLING RECORDING

Checkbox

If selected, all the alarms returned will issue a service ticket.

If not selected, none of the alarms returned will issue a service ticket.

MONITOR TEL. SET

Checkbox

If you tick YES, all the alarms will activate an LED on the attendant console and on all the maintenance terminals.

It is then also possible to request for a call to be sent to the telephone set whose number is indicated in the following field.

- UNTIL THE NUMBER

Number of the set from which the calls will be made.

- AND ACKNOWLEDGED BY CODE

Acknowledgement code on the called set. 4-digit value (authorised characters: 0, 1, …9, #, *).

Note: To acknowledge an alarm that has activated an LED on the attendant console and, thus, stop the flashing LED, you must set the EXT. ACK. alarm of the SUBSCR ACTION SBL to return to key.

TO CENTRALISATION SITE

Checkbox

If selected, all the alarms will be returned to the centralising sites defined by the following parameters SITE 1 and SITE 2.

Note: This parameter, as well as the following parameters (SITE 1, SITE 2), is only available in multi-site configuration.

- SITE 1 / 2

Name of the site(s) to which the alarms will be returned.

The drop-down lists of the parameters SITE 1 and SITE 2 contain the names of sites defined in the multi-site configuration.

SNMP

Options: V1 or V3 (upper security level)

This SNMP option list is used to set the local iPBX to SNMP V1 or V3. The proposed fields will differ according to the selected mode

<u>SNMP V 1 mode</u>

TO SNMP MANAGER 1 / 2 / 3

SNMP manager IP address. If this field is completed, some SNMP traps will be sent to the corresponding SNMP manager for the alarms that meet the criteria defined in the following parameters.

The following 6 fields are only displayed if an IP address is entered.

WARNING: If the iPBX is managed by a MiVoice 5000 Manager, the SNMP manager of the MiVoice 5000 Manager must be configured as SNMP 1 Manager.

- LANGUAGE

Language in which the traps are sent.

- TRAP TYPE

ALARM LOGBOOK	Only the alarms meant for the alarm log will be part of an SNMP trap transmission.
LOGBOOK	Only the events meant for the logbook will be part of an SNMP trap transmission.
ALL	Total of the preceding two cases.

Note: For MiVoice 5000 Manager SNMP manager, it is advisable to select ALL.

- TRANSMIT THRESHOLD

Indicates the alarm severity level as from which a trap will be sent.

…………………	No filtering on the severity level.
WARNING	Transmission of an SNMP trap for alarms whose severity level is at least equal to **warning.**
MINOR ALARM	Transmission of an SNMP trap for alarms whose severity level is at least equal to **minor.**
SEVERE ALARM	Transmission of an SNMP trap for alarms whose severity level is at least equal to **severe.**
CRITICAL ALARM	Transmission of an SNMP trap for **critical** alarms only.

- COMMUNITY

The same community for all the SNMP traps sent to this SNMP manager.

- AGENT IDENTIFICATION

IP address of the agent sending the SNMP trap (value transmitted in the trap).

- NRPE (MANAGER)

This parameter has two functions:

- Activating the NRPE service (see NRPE tab)
- Locally storing the SNMP traps when the link with the server is cut, in order to transmit them in deferred mode

This parameter is activated by default if a MiVoice 5000 Manager is managing the iPbx.

TO AD. X25 NO 1/2:

X25 addresses to which alarms will be returned.

- NUMBER OF ATTEMPTS

Number of authorised attempts.

- ATTEMPTS PERIOD (SEC)

Interval in seconds between two consecutive attempts.

SNMP V3 mode

Rules:

It is forbidden to change to SNMP V3 if the iPBX does not have any dongle ID.

SNMP V3 mode can be assigned on a site or node basis in a cluster configuration.

If the local iPBX is a cluster server, changing to SNMP V3 also results in local management of message transmission to all the nodes so they take this change in configuration into account.

SNMP V3 mode incorporates the following fields from SNMP V1 mode:

- **Language**
- **Trap type**
- **Emission threshold**
- **Agent identification**
- **NRPE**

The fields specific to SNMP V3 mode are as follows:

- **EngineID**: PBX identifier. greyed out text area, given for information only
- **Username for TRAP**: greyed out text area, given for information only
- **Username for GET**: Manager Identifier. greyed out text area, given for information only
- **Secret**: password shared between MiVoice 5000 Manager and the iPBX, so MiVoice 5000 Manager can receive notifications and execute SNMP requests. This attribute can be edited by the user.

  This field is limited to 16 characters. A secret must contain at least 8 characters, with at least one figure and one letter.

  The **Secret** field is initialised with a value randomly generated by the system while changing to SNMP V3 mode or when an SNMP manager is added to an iPBX set to SNMP V3.
- The Security name field gives a default name to each SNMP agent manager. This field is not modifiable.

The security names of SNMP managers assigned by default are: manager1, manager2 and manager3.

When the attribute **secret** is modified in the iPBX, a warning message is sent to MiVoice 5000 Manager.

It is advisable to manage the secret in MiVoice 5000 Manager during centralised management.

It is forbidden to stop the SNMP service in SNMP V3 mode (Menu **SYSTEM>Configuration>Services**). A warning message will be displayed during a request to stop this service.

Changing from SNMP V1 to V3, and vice versa, modifies the option proposed by the **MIB SNMP** menu (see Section 4.3.6).

In case of switchover from one mode to another, MiVoice 5000 Manager is alerted to it by the iPBX concerned. The aim is to prompt MiVoice 5000 Manager to update the site configuration so as to be able to continue managing the iPBX in the updated SNMP mode.

4.3.3.2.2 NRPE configuration tab

NRPE Nagios Remote Plugin Executor

NRPE is a MiVoice 5000 plugin used to return system resources alarms to the MiVoice 5000 Manager management centre Nagios module.

The monitored resources are the CPU load and system disk free space.

NRPE is managed as a system service: see Menu **System>Services**.

It is activated in two ways:

- Manually in the "Alarm management" tab, or
- Automatically when the iPbx is managed by MiVoice 5000 Manager.,

THRESHOLDS BEFORE "WARNING" ALARM (IN %)

For the defined warning values, NRPE generates and sends a warning alarm to MiVoice 5000 Manager:

- **Average CPU load in 1 minute** 15 % by default
- **Average CPU load in 5 minutes** 10% by default
- **Average CPU load in 15 minutes** 5% by default
- **Disk free space** 10% by default

THRESHOLDS BEFORE CRITICAL ALARM (IN %)

For the defined critical values, NRPE generates and sends a warning alarm to MiVoice 5000 Manager:

- **Average CPU load in 1 minute** 30 % by default
- **Average CPU load in 5 minutes** 25% by default
- **Average CPU load in 15 minutes** 20% by default
- **Disk free space** 5% by default

4.3.3.3 *Individualized configuration*

Menu SYSTEM>**Configuration>Alarms>Individualized configuration**

This command is used to configure, for each system alarm, the alarm transmission priority level according to output device. The configuration may apply to:

- A particular alarm
- All the alarms of an SBL group
- All the alarms.

DETECTION IN

LOCAL SITE **OTHER SITE**

Origin of the alarm(s) concerned by the current configuration.

Note: This parameter is only available in multi-site configuration.

BY SBL GROUP

……..	POWER SUPPLY	PROCESSOR	ANAL TRK CARD
DIG TRK CARD	DATA CARD	SUBSCR CARD	VMAIL CARD
ANAL TRK DEV	DIG TRK DEV	DATA DEVICE	SUBSCR.DEV
MANAGEMENT	FALLBACK ACCESS	BILLING	SUBSCR ACTION
DRY LOOP	SUPERVISION	CPU_STARTUP	INTEGRATED BUFFER
EXPORT BUFFER	CAC SERVER		

Name of the SBL group to which the alarm(s) concerned by the current configuration belong(s).

If you select "**……**", all the alarms of all the SBL groups are concerned by the current configuration.

OF ALARM

Name of the alarm concerned by the current configuration.

The drop-down list contains the names of alarms for the selected SBL group.

If you select "**……**", all the alarms of all the alarms of the selected SBL groups are concerned by the current configuration.

ROUTED TO

SET	Calls the set whose number was defined in the alarm parameters
KEY	Activated an LED on the attendant console.
TICKET	Triggers the transmission of an alarm service record.
MAIN	Returns the alarm to the centralising sites (CG or external set) defined in alarm parameters. This value is only available in multi-site configuration.
X25 ADDRESS	Sends the alarm to X25 addresses 1 and 2 defined in alarm parameters.
SNMP TRAP	For generating an SNMP trap, regardless of alarm ticket output, to SNMP managers whose IP addresses are defined in alarm parameters.

Select the configuration criteria then click **Select the item**.

Depending on type, the following information is displayed:

ALARM: "TYPE"

Case of return to X25 address:

NOT TRANS. Alarm not transmitted.

ADDRESS 1 Alarm sent to X25 address 1.

ADDRESS 2 Alarm sent to X25 address 2.

TO 2 ADDR Alarm sent to both X25 addresses.

Case of return to R2 relay:

NOT TRANS. Alarm not transmitted.

RUN Alarm results in the activation of R2 relay.

DESACTIV. Alarm results in the deactivation of R2 relay.

Other cases:

NOT TRANS. Alarm not transmitted.

NOT URGENT Alarm with severity level NOT URGENT transmitted.

URGENT Alarm with severity level URGENT transmitted.

KEYING Alarm with severity level URGENT or NOT URGENT transmitted.

4.3.3.4 *global reset*

Menu **SYSTEM>Configuration>Alarms>Global reset**

This command is used to define default processing for all SBL groups and alarms.

WARNING: Global reset overwrites all previous individualised configurations made.

The possible parameter values on this screen have the following meaning:

NOT TRANS.	Alarm not transmitted.
NOT URGENT	Alarm with severity level NOT URGENT transmitted.
URGENT	Alarm with severity level URGENT transmitted.
KEYING	Alarm with severity level URGENT or NOT URGENT transmitted.
ADDRESS 1	Alarm sent to X25 address 1.
ADDRESS 2	Alarm sent to X25 address 2.
TO 2 ADDR	Alarm sent to both X25 addresses.
RUN	Alarm results in the activation of R2 relay.
DESACTIV.	Alarm results in the deactivation of R2 relay.

DETECTION IN

LOCAL SITE **OTHER SITE**

Origin of the alarms concerned by the reset operation.

Note: This parameter is only available in multi-site configuration.

REPORTED TO SET / KEY / TICKET

NOT TRANS. **NOT URGENT** **URGENT** **KEYING**

Defines for each output the default processing for all SBL groups and alarms (set, key, ticket).

REPORTED TO CENTRAL.

NOT TRANS. **NOT URGENT** **URGENT** **KEYING**

Defines, for return to a centralising site, the default processing for all SBL groups and alarms.

Note: This parameter is only available in multi-site configuration.

REPORT TO X25 ADDRESS

NOT TRANS. **ADDRESS 1** **ADDRESS 2** **TO 2 ADDR**

Defines for the X.25 address output the default processing for all SBL groups and alarms.

RESET CONFIRMATION

YES **NO**

If you select YES, the values selected on the screen are validated.

4.3.3.5 *Configuration display*

Menu **SYSTEM>Configuration>Alarms>Configuration display**

This command displays the current configuration for each alarm.

To access this command, click "Configuration display” from the “Alarms” menu.

DETECTION IN

LOCAL SITE **OTHER SITE**

Origin of the alarms concerned by the display operation.

Select the value you want then click **Select the item**.

For each of the alarms (classified by SBL), the alarm configuration display screen shows:

- The alarm name
- The type of alarm transmission for return to a key
- The type of alarm transmission for return to a set
- The type of alarm transmission for ticket issuing
- The type of alarm transmission for return to a centralising site
- The type of alarm transmission for return to one or two X25 addresses
- The type of alarm transmission for return to an SNMP manager
- The type of alarm transmission for return to R2 relay.

4.3.4 TICKETS

Menu **SYSTEM>Configuration>Tickets**

Tickets are issued by the site’s KITAXE server.

In single-site configuration, the iPBX’s integrated buffer module receives tickets from the KITAXE server, stores them in temporary files according to some configuration criteria, and exports the files to an area where they are made available to an external application.

In multi-site configuration, the MUFACT server centralises the tickets issued by the different sites by connecting to the KITAXE servers of each site. The iPBX’s integrated buffer, on which the MUFACT server is located, receives the tickets from the MUFACT server and manages them in the same way as in single-site configuration.

In Cluster configuration, charging is centralised on the KITAXE server (See note in Paragraphs 4.3.4.5.1 - **General settings** and 4.3.4.5 - Menu **Integrated Buffer)** .

In the event of an outage, in cluster configuration:

- If the Cluster Server is disconnected, the network tickets of the nodes are stored in the nodes.
- Upon reconnection, the tickets are forwarded to the Cluster Server. All tickets are then stored in the Cluster Server BUFTIC.

This menu is used to:

- Configure the ticket output format
- Configure the size of the KITAXE server storage buffers
- Configure MUFACT server connections to the KITAXE server in multi-site configuration
- Configure the integrated buffer.

4.3.4.1 *Billing parameters*

Menu SYSTEM>**Configuration>Tickets>Billing settings**

This command is used to configure the issuing of tickets by the KITAXE server, as well as their format.

------------- CHARGE RECORDS ----------------

USE OF FORMAT 4500

YES	NO

If you select YES, the ticket can either be printed or processed by SMDR.

If you select NO, the ticket will be processed on a PAD link in 6500 format.

STEP BY STEP DEFINITION

SMDR	On a single line in “4500 format”. This value is available if you select the 4500 format.
PRINTER	On several lines in “4500 format”. This value is available if you select the 4500 format.
PAD LINK	If you are using PAD link, records are processed by an asynchronous link connected to the KITAXE or MUFACT server, in "6500 format".
OUTPUT CHANNEL	Billing data output is carried out on the serial port of the main card (UCV), in “6500 format”.

SITE NUMBER OVERRIDDEN IN RECORD

Site number.

When a ticket is issued, the site number of the issuer is indicated on the ticket. This parameter is used to replace this value with a fixed number.

------------- CALL RECORDS ----------------

STEP BY STEP OUTPUT

YES	NO

If you select YES, the call records issued by the KITAXE or MUFACT server are printed out on the printer or on the PAD link, depending on the value of the parameter 4500 OUTPUT FORMAT in the CALL RECORDS column.

Issuing call records on the PAD link requires the integrated buffer to call the KITAXE (or MUFACT) server with sub-address 00.

If you select NO, call records are not issued.

Note: If you select NO, none of the other parameters in the CALL RECORDS column will be available.

OUTPUT FORMAT

SIMPLE FORMAT	(82 characters)	**EXTENDED FORMAT V0**	(112 characters)
EXTENDED FORMAT V1	(128 characters)	**EXTENDED FORMAT V2**	(210 characters)
EXTENDED FORMAT V3	(246 characters)	**EXTENDED FORMAT V4**	(256 characters)

Call record output format. The format determines the number of fields appearing on the record.

TRUNK IDENTIFIED BY

CARD/CHANNEL	Number of the card and equipment channel.
EQUIPMENT	NTL (logic terminal number):

Note: This is the only pertinent mode in a cluster architecture.

Call ID type.

TRUNCATE LAST 4 DIGITS

YES **NO**

If you select YES, the last 4 digits of the number dialled do not appear.

CALL TYPE

INCOM. AND OUTGO.	Incoming and outgoing calls are printed out.
INCOMING	Incoming calls are printed out.
OUTGOING	Outgoing calls are printed out.

Filters the call records to be printed out step by step.

DELETE RECORDS W/OUT CHARGING

YES **NO**

If you select YES, only charged records will be printed out step by step.

WARNING: If you select YES, incoming calls will also be deleted.

INTERNAL CALL RECORD GENERATION

LAST INTERNAL COMPANY

Border company value authorising internal charging according to the parameter value.

Default value: all the companies are called internal companies.

Other values: (among the numbers defined) all companies below or equal to this border company are described as internal; companies above this border company are described as external.

The list of available company names is sorted in an ascending order of company numbers.

This line has a command for zooming to other company parameters:

Note: Deleting a company defined as border company is forbidden in the Company names menu.

DEFINITION OF INTERNAL CHARGING RIGHTS

Default value: no local charging (none of the lines is ticked).

For each of the next lines, tick or untick the box depending on the internal charging rights to apply:

IN THE SAME INTERNAL COMPANY

Charging if the caller and called party belong to the same internal company.

Field always displayed.

IN THE SAME EXRERNAL COMPANY

Charging if the caller and called party belong to the same external company.

Displayed if at least one external company exists.

BETWEEN DIFFERENT INTERNAL COMPANIES

Charging if the caller and called party belong to two different internal companies.

Displayed if at least two internal companies exist.

BETWEEN DIFFERENT EXTERNAL COMPANIES

Charging if the caller and called party belong to two different external companies.

Displayed if at least two external companies exist and the multi-company alias indicator is set to YES.

INTERNAL COMPANY TO EXTERNAL COMPANY (bit 4)

Charging if the caller belongs to an internal company and the called party belongs to an external company.

Displayed if at least one external company exists.

EXTERNAL COMPANY TO INTERNAL COMPANY (bit 5)

Charging if the caller belongs to an external company and the called party belongs to an internal company.

Displayed if at least one external company exists.

--------- DATA RECORDS -----------

STEP BY STEP OUTPUT

YES **NO**

If you select YES, the data records issued by the KITAXE or MUFACT server are printed out on the printer or on the PAD link, depending on the value of the parameter 4500 OUTPUT FORMAT in the CALL RECORDS column.

Issuing records on the PAD link requires the integrated buffer to call the KITAXE (or MUFACT) server with sub-address 10.

If you select NO, records are not issued.

If you select YES, the following field is available.

OUTPUT FORMAT

SIMPLE FORMAT (82 characters) **EXTENDED FORMAT V0** (112 characters)

EXTENDED FORMAT V1 (128 characters)

Data record output format. The format determines the number of fields appearing on the record.

This field is only available if you select YES for the parameter STEP BY STEP OUTPUT.

-----------SERVICE RECORD OUTPUT-------------

OUTPUT FORMAT

SIMPLE FORMAT (82 characters) **EXTENDED FORMAT V0** (112 characters)

EXTENDED FORMAT V1 (128 characters)

Service record output format. The format determines the number of fields appearing on the record.

“AGENDA” / “PREPAYMENT” / “MONITORING” / “FEATURE” / “C.DIST.” FAMILY

For each of the families, this parameter defines the type of output for the corresponding records.

LOGBOOK	For displaying in the logbook all the records concerning the family.
STEP BY STEP	Same function as described above with a link on the output channel or PAD, by means of the KITAXE or MUFACT call with sub-address 30.
STEP BY STEP AND LOG	Same function as described above, with a link on the output channel or PAD by means of the KITAXE or MUFACT call with sub-address 30.
DUMMY	The records for the family in question are not taken into account.

Agenda/alarm family

Wake-up programming, wake-up cancellation, wakeup, no answer to wakeup.

Prepayment family

Prepayment processing: credit, prepayment balance, end of current balance.

Monitoring family

Message output when the TRACE key is pressed (nuisance call).

Message output during a long call .

Feature family

Indicator for validated or cancelled message in home automation function message lamp on set.

C.Dist. family

Message output on the call distribution set in or out of service (or on a set in a hunt group).

-----------MONITORING RECORDS-----------

STEP BY STEP OUTPUT

YES NO

If you select YES, the monitoring records for the subscribers and/or lines are issued according to the criteria defined in the following parameters through a KITAXE or MUFACT call with sub-address 40.

If you select NO, monitoring records are not issued.

If you select NO, none of the following parameters will be available.

---- SUBSCRIBER MANAGEMENT

CALL TYPE

INCOM. AND OUTGO. INCOMING OUTGOING

Call type criterion for monitoring records output.

A record can be issued for each subscriber whose parameter “SUBSCRIBER MONITORING (RECORD)” is set to YES (box ticked) in “SUBSCRIBERS>Subscriptions>Characteristics>General characteristics”.

---- JUNCTOR MANAGEMENT

TRUNK IDENTIFIED BY

CARD/CHANNEL EQUIPMENT

This field determines whether the record is printed with the circuit number or with the card and channel number.

CALL TYPE

INCOM. AND OUTGO. INCOMING OUTGOING

Call type criterion for monitoring records output.

A record can be issued for each phase: Selection, ringing, speech, release, for lines whose parameter “TRANSITION MONITORING (RECORD) is set to YES in “NETWORK and LINKS>Equipment>External line”.

- "SELECTION’’ / "RINGING’’ / ‘’SPEECH’’ / ‘’RELEASE’’

YES NO

Indicates whether a record will be issued, for each of the phases.

-----------MONITORING TICKETS-----------

MONITORING TICKET GENERATION

YES NO

If you select YES, an monitoring ticket is generated for each monitoring counter.

If you select NO, monitoring tickets are not issued.

4.3.4.2 *kitaxe server parameters*

Menu SYSTEM>**Configuration>Tickets>Server kitaxe servers**

This command is used to configure the size of the storage buffers of each record type on the KITAXE server.

NUMBER OF TICKETS (CURRENT) (REQUESTED)

- TELEPHONY / DATA / SERVICE / SUPERVISION / MONITORING TYPE

Size of the storage buffers of the last records.

The maximum total size for all the five buffers is 580 records.

The request is only taken into account after restarting the system, after which the current values are the same as the requested values.

4.3.4.3 *MUFACT SERVER PROFILES*

Menu **SYSTEM>Configuration>Tickets>Mufact server profiles**

This command is used to configure some profiles (maximum 4) which will be used, in multi-site configuration, to connect the MUFACT server to the different KITAXE servers of other sites.

Note: In the last 4 columns of the table:
- "all" means that no filtering has been configured in the profile,
- "filter" means that filtering has been configured in the profile.

The MUFACT profile display table shows for each profile:

- Its number
- Whether the records are subject to acknowledgement
- Whether the records are issued with separators
- Whether filtering takes place on the telephony records
- Whether filtering takes place on the service records
- Whether filtering takes place on the companies
- Whether filtering takes place on the sites

To display and/or modify a MUFACT profile, click its number.

RECORD ACKNOWLEDGEMENT

YES **NO**

If you select YES, the MUFACT server will acknowledge receipt of records from the KITAXE server.

RECORDS ISSUED WITH SEPARATORS

YES **NO**

If you select YES, a start character and an end character are added to the record when it is issued.

TELEPHONE RECORD FILTERING

YES **NO**

If you select YES, you can choose the telephone record filtering you want from the following fields:

By default, no filtering has been defined: the following three fields are set to YES.

- TRANSMIT INCOMING CALL RECORDS

YES	**NO**

If you select NO, incoming call records are not issued.

- TRANSMIT OUTGOING CALL RECORDS

YES	**NO**

If you select NO, outgoing call records are not issued.

- TRANSMIT INTERNAL CALL RECORDS

YES	**NO**

If you select NO, internal call records are not issued.

SERVICE RECORD FILTERING

NONE	**BY INCLUSION**	**BY EXCLUSION**

Filtering type.

By default, no filtering has been defined: all service tickets for all families are issued.

This parameter is used to configure a filter **BY INCLUSION**, by indicating the families for which the records will be issued, or **BY EXCLUSION** by indicating the families for which the records will not be issued.

- FAMILY 1 / 2 / 3 / 4

…….	**WAKE-UP**	**PREPAYMENT**	**SUPERVISION**
FEATURES	**ALARM**	**C.DIST**	

Names of the families to which filtering applies.

CALLER COMPANY FILTERING

NONE	**BY INCLUSION**	**BY EXCLUSION**

Filtering type.

Note: This parameter is only available in multi-company configuration.

By default, no filtering has been defined: all phone tickets for all companies are issued.

This parameter is used to configure a filter **BY INCLUSION**, by indicating the names of the companies for which the records will be issued, or **BY EXCLUSION** by indicating names of the companies for which the records will not be issued.

The filter concerns the caller's company.

- COMPANY 1 / 2 / 3 / 4

Names of the companies to which filtering applies.

The drop-down lists contain the names of companies declared in the system.

CALLED COMPANY FILTERING

NONE	**BY INCLUSION**	**BY EXCLUSION**

Filtering type.

Note: This parameter is only available in multi-company configuration.

By default, no filtering has been defined: all phone tickets for all companies are issued.

This parameter is used to configure a filter **BY INCLUSION**, by indicating the names of the companies for which the records will be issued, or **BY EXCLUSION** by indicating names of the companies for which the records will not be issued.

The filter concerns the called party’s company.

- COMPANY 1 / 2 / 3 / 4

Names of the companies to which filtering applies.

The drop-down lists contain the names of companies declared in the system.

CALLER SITE FILTERING

NONE **BY INCLUSION** **BY EXCLUSION**

Filtering type.

Note: This parameter is only available in multi-site configuration.

By default, no filtering has been defined: all telephone tickets for all sites are issued.

This parameter is used to configure a filter **BY INCLUSION**, by indicating the names of the sites for which the records will be issued, or **BY EXCLUSION** by indicating names of the sites for which the records will not be issued.

The filter concerns the caller’s site.

- SITE 1 / 2 / 3 / 4

Names of the sites to which filtering applies.

The drop-down lists contain the names of sites in the multi-site configuration.

CALLED SITE FILTERING

NONE **BY INCLUSION** **BY EXCLUSION**

Filtering type.

Note: This parameter is only available in multi-site configuration.

By default, no filtering has been defined: all telephone tickets for all sites are issued.

This parameter is used to configure a filter **BY INCLUSION**, by indicating the names of the sites for which the records will be issued, or **BY EXCLUSION** by indicating names of the sites for which the records will not be issued.

The filter concerns the called site.

- SITE 1 / 2 / 3 / 4

Names of the sites to which filtering applies.

The drop-down lists contain the names of sites in the multi-site configuration.

4.3.4.4 CALL FROM BILLING SERVERS

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

In a multi-site configuration, the iPBX connects to the MUFACT server to retrieve billing records. The role of the MUFACT server is to centralise the records issued by the different KITAXE servers.

Therefore, the MUFACT server must know the X25 addresses of the different KITAXE servers on other sites. The MUFACT server connects to the KITAXE servers using the X25 number and a sub-address profile.

This command is used to configure:

- The X25 addresses of KITAXE servers
- The MUFACT profile number for connection
- Filtering by type of records to download.

Note: This command is only available in multi-site configuration, on the site on which the MUFACT server is located. In single-site configuration, the KITAXE server call number is configured in NETWORK AND LINKS>Data links>Servers>MUFACT.

The system is used to define up to 64 accesses to KITAXE billing servers per MUFACT.

CALL NUMBER 1 TO 64

KITAXE server call number.

PROFIL - TEL/PAQ/CIR/SER/SUP/MON

MUFACT profile number to use for connection: types of tickets to download from the KITAXE server.

This field must be filled in as follows:

- MUFACT profile number
- Ticket download filter:
- Each position represents the type of ticket in their order of appearance in the field name.
- A + sign means that correspondent type tickets will be downloaded.
- A - sign means that correspondent type tickets will not be downloaded.

Example: +--+-- means that only telephony and service type tickets will be downloaded.

4.3.4.5 *Integrated buffer*

Menu **SYSTEM>Configuration>Tickets>Integrated buffer**

The role of the integrated buffer is to:

- Receive tickets from a KITAXE server (in single-site configuration) or MUFACT server (in multi-site configuration),
- Distribute tickets in files according to ticket type (a file per ticket type)
- Export these files to an export area for use by external applications.

This menu is used to:

- Configure the integrated buffer
- Enable/disable the integrated buffer
- Configure export parameters (frequency, compression option, etc.)
- Manage the export area (display, purge)
- Export record files manually.

4.3.4.5.1 General settings

Menu **SYSTEM>Configuration>Tickets>Integrated>General settings**

This command is used to:

- Display/change the functional status of the integrated buffer
- Configure the MUFACT server call number.
- Select the record types to back up.

To access this command, click "General settings” from the “Integrated buffer” menu.

STATUS: “CURRENT STATE”

For changing the functional status of the integrated buffer.

••••••••	The functional status of the integrated buffer is not changed.
OPERATIONAL	In service.
SUSPENDED	Out of service.

CURRENT STATE shows the functional status of the integrated buffer: ***in use, suspended***.

Note: You must select the status SUSPENDED if you want to modify the integrated buffer parameters.

IMPORTANT NOTE: For a Cluster configuration:

In a Centralized Charging configuration on a Cluster, the status must remain at In use and the type of tickets to be backed up as telephone tickets must be set to YES.

Bufftic must be in service in the nodes, even if Buftic is not used in charging.

MUFACT CALL NUMBER

MUFACT server directory number.

NUMBER OF RECORD TYPES TO BACK UP

- TELEPHONY / DATA PACKET / DATA CIRCUIT / SERVICE (AND ALARMS) / SUPERVISION / OBSERVATION

NO **YES**

For each record type:

- If you select YES, a file is opened so you can back up the corresponding records.
- If you select NO, these records are not backed up.

4.3.4.5.2 Billing parameters

Menu SYSTEM>Configuration>Tickets>Integrated buffer>Billing settings

For each type of record, this command is used to:

- Define the maximum sizes of temporary files and of the export area
- Define the rate and time of export
- Configure the exported file availability notification option
- Configure the file compression option before export.

BY TYPE

TELEPHONY	**DATA PACKET**	**DATA CIRCUIT**
DEPARTMENT	**SUPERVISION**	**OBSERVATION**

Record type.

Select a record type then click **Select the item**.

Note: The default values are summarised in the table that follow the definition of parameters.

FILE NAME

Information field indicating the type of tickets contained in the file (this character string is used as the beginning of the file name).

Possible values are: TickTel, TickDataPaq, TickDataCirc, TickServ, TickSuperv, TickObserv.

MAX. SIZE OF TEMPORARY FILE (MB)

Maximum size in MB of the integrated buffer storage file for the ticket type concerned. Max. value = 4000.

When this size is reached, the file is exported to the corresponding export area, regardless of the export frequency settings.

MAX. SIZE OF EXPORT ZONE (MB)

Maximum size in MB of the export area reserved for the type of file concerned. Max. value = 4000.

When this value is reached, the newly exported files overwrite the oldest ones.

PERIODICITY OF THE FILES EXPORT

- DAYS PERIODICITY

Number of days between two exports.

- HOURS PERIODICITY

Number of hours between two exports.

Note: The parameters DAYS PERIODICITY and HOURS PERIODICITY are independent of each other. The last field completed cancels the value of the other parameter.

- HOUR OF STARTING (HH:MM)

Time of first export.

NOTIFICATION REQUESTED

If you select YES, a notice of availability is sent to the logbook.

EXPORTED FILES COMPRESSED

If you select **YES**, the file is compressed before being exported. Its extension is then **.gz**.

If you select **NO**, the file is not compressed before being exported. Its extension is then **.arch**.

TYPE OF RECORD	MAXIMUM SIZE OF TEMPORARY FILE (MB)	MAXIMUM SIZE OF EXPORT AREA (MB)	DAYS PERIODICITY	NOTIFICATION	COMPRESSION
TELEPHONY	20	20	1	YES	YES
DATA PACKETS	0	0		NO	NO
DATA CIRCUIT	0	0		NO	NO
DEPARTMENT	0.5	0.5	1	YES	YES
SUPERVISION	0	0		NO	NO
OBSERVATION	0	0		NO	NO

Table 3: Default values of integrated buffer record parameters

4.3.4.5.3 Display of the ticket files

Menu **SYSTEM>Configuration>Tickets>Integrated buffer>Ticket files display**

This command is used to display the list of exported files available in the export area, that is available for external applications.

BY TYPE

ALL **TELEPHONY** **DATA PACKET** **DATA CIRCUIT**

DEPARTMENT **SUPERVISION** **OBSERVATION**

Record type.

Select a record type then click **Select the item**.

For the selected record type or for each type, if you have selected ALL, the display table shows for each file available in the area:

- Its name in the following format: *Type_yyyymmdd_hhmmss.extension*, where:

- *Type* is record type
- *yyyymmdd_hhmmss* stands for record acquisition start date and time
- *extension* is *.gz* if file compression is required, otherwise it *.arch*.
- Export date
- Export time
- Its size.

Date and time concern a ticket file which corresponds to the last information received from the PBX.

4.3.4.5.4 Export of the ticket files

Menu **SYSTEM>Configuration>Tickets>Integrated buffer>Ticket files export**

This command is used to force record file export for use by external applications.

BY TYPE

ALL	TELEPHONY	DATA PACKET	DATA CIRCUIT
DEPARTMENT	SUPERVISION	OBSERVATION	

Record type.

Select a record type then click **Select the item**.

PASSWORD

Enter the password then click **Export of the ticket files**.

Note: The password is the one used to log on to the iPBX Web Admin. If the rights associated with this password are insufficient, the system will reject the file export request.

When the operation is completed, the screen appears:

```
Files: export all
```

4.3.4.5.5 Export zone file deletion

Menu **SYSTEM>Configuration>Tickets>Integrated buffer> Export zone files deletion**

This command is used to delete record files from the export area.

BY TYPE

ALL	TELEPHONY	DATA PACKET	DATA CIRCUIT
DEPARTMENT	SUPERVISION	OBSERVATION	

Record type.

Select a record type then click **Select the item**.

PASSWORD

Enter the password then click "To suppress the files".

When the operation is completed, the screen appears:

```
Files: telephony deleted
```

Note: Deleting files from the export area requires the functional status of the integrated buffer to be SUSPENDED (command: SYSTEM>Configuration>Tickets>Integrated buffer>General settings).

4.3.5 E-MAIL

Menu SYSTEM>Configuration>E-mail

4.3.5.1 *E-voicemail settings*

The e-voicemail function of the iPBX enables the system to send an e-mail to a subscriber to inform him that he has received a voice mail in his integrated voicemail box.

A Modern authentication based on OAuth 2.0 is available if the authentication of POP3 and iMAP4 connections to office365 or ExchangeOnLine servers is not available. See next section 4.3.5.2.

Compatible servers are:

- ExchangeOnLine,
- Office 365,
- Gmail.

Depending on the configuration of his voicemail box class:

- Either no notification is sent,
- Or a simple e-mail is sent, or
- An e-mail is sent with the voice mail as attachment.

To benefit from the e-voicemail service, a subscriber must have an IVB whose class allows this service.

The menu **VOICE MAIL AND TONES>Voice mail>Internal voice mail (IVB)>Voice mail classes** is used to authorise or forbid the e-voicemail service by voice mail box class.

The box class is assigned to the subscriber in **SUBSCRIBERS>Subscriptions>Characteristics>General characteristics**.

The subscriber e-mail address used is that of his directory record.

The menu **SYSTEM>Configuration>E-mail** is used to define the parameters of the message servers used by the iPBX:

- To send an e-mail to a subscriber,
- To receive an acknowledgement of receipt from the subscriber that has read the e-mail.

4.3.5.2 *Authentication types*

As of R7.2 SP1, it is possible to use a new type of identification called Modern Authentication and to define its settings.

The classic authentication for POP3 and iMAP4, and for SMTP should disappear and be replaced with a so-called modern authentication based on the OAuth 2.0 protocol.

This involves setting up authentication for POP3 and iMAP4 connections to office365 or ExchangeOnLine servers.

The aim is to stop having to store a user's password for an application because it can be used and therefore hacked for other applications.

Although for the MiVoice 5000 mail client, the account used is only dedicated to MiVoice 5000, and is therefore not a user account, it is very advisable to set up a modern authentication based on OAuth 2.0.

The **Modern Authentication** field is used to choose whether or not to use modern authentication with Microsoft (required) and Google (preferred) and to retrieve the necessary settings for configuration in the iPBX.

The parameters from these applications are:

- For Microsoft (Tenant ID, Application ID (ClientID), Application Secret (ClientSecret))
- For Google (Client ID, SecretClient).

However, the Not configured option remains available.

4.3.5.3 *Description of the different fields*

E_MAIL ADDRESS

iPBX mail box address on the mail server. This address is the address to which the transmission and reception are made.

MODERN AUTHENTICATION:

List of options:

- Not configured,
- Microsoft OAuth2.0,
- Google OAuth2.0.

Not configured: No modern authentication Then fill in the Transmit and Receive parameters fields.

Microsoft OAuth2.0:

Settings required for modern authentication with Microsoft (required) associated with the Tenant ID, Application ID and Secret fields.

- Register MiVoice 5000 PBX in the Microsoft Azure application to get the following settings used in the OAuth2.0 authentication process. They are listed below:
  - Directory ID (tenant),
  - Application (client) ID,
  - Mute.

Refer to Section 9.1 Registering the MiVoice 5000 PBX in Microsoft Azure.

- Fill in all the fields described previously.

Launch the authorization:

This action is used to obtain the permissions for the account created for Microsoft or Google which redirects to the corresponding authentication web page (Microsoft or Google) to request that the iPBX be allowed to access the mailbox.

If authentication is successful, the **Start authorisation** link disappears and is replaced by the **Clear modern authentication settings** button.

It is then no longer possible to change the settings above the button.

Clicking on this button resets (clears) the modern authentication settings above the button, for reconfiguration if necessary.

Then fill in the **Transmit** and **Receive** parameters fields.

Google OAuth2.0:

Parameters needed for modern authentication with Google (preferred) associated with the (Client ID, SecretClient) fields.

- Register MiVoice 5000 iPBX in the Google application to get the following settings used in the Oauth 2.0 authentication process. They are listed below:
  - Application (client) ID,
  - Mute.

Refer to Section **9.2 Registering the MiVoice 5000 iPBX in Google**.

- Fill in all the fields described previously.

Launch the authorization:

This action is used to obtain the permissions for the account created for Microsoft or Google which redirects to the corresponding authentication web page (Microsoft or Google) to request that the iPBX be allowed to access the mailbox.

If authentication is successful, the **Start authorisation** link disappears and is replaced by the **Clear modern authentication settings** button.

It is then no longer possible to change the settings above the button.

Clicking on this button resets (clears) the modern authentication settings above the button, for reconfiguration if necessary.

Then fill in the **Transmit** and **Receive** parameters fields (see below).

TRANSMISSION SETTINGS (COMMON TO ALL MODES)

These parameters enable the iPBX to send an e-mail to a subscriber.

PROTOCOL: SMTP (GREYED OUT IN CONSULTATION)

SERVER

SMTP message server address

The following two parameters are only to be defined if the SMTP server requires an authentication.

This field can also be entered with a domain name (DNS). This must be complete and correspond to the configuration made in **DNS 1 address** , **DNS 2 address** and **DNS 3 address** in Menu **SYSTEM/Configuration/Cards/IP board settings**.

ENCRYPTED CONNECTION (SSL)

Checkbox which allows the use of an encrypted connection between the iPBX and the mail server used for the e-voicemail function in case of message transmission.

This feature makes it difficult for a third party to intercept exchanges between these two systems.

The default port configuration for the connection with or without SSL for the e-voicemail function, and depending on the protocol, is as follows:

PROTOCOL	WITHOUT SSL (BOX NOT TICKED)	WITH SSL (BOX TICKED)
SMTP	25	465
POP3	110	995
IMAP	143	993

VOICE MAIL ACCOUNT

Name of the iPBX messaging account on the SMTP server.

PASSWORD

iPBX SMTP messaging account password.

Authorised characters: [A-Z]+[a-z]+[0-9]+["#%'()*+,-./:;<=>@_]

Unauthorised characters: [!$&? [\]^`{|}~]

PORT

Field used to define the SMTP server port number.

Check certificate:

Defining whether the certificate of an SSL or StartTLS connection should be verified.
Box ticked: Verification enabled (default setting).

Use modern authentication (Specific to Microsoft and Google modern authentication)

If the box is checked, modern authentication mode is used, associated in emission with the previously declared (Microsoft or Google) account.

RECEIVING SETTINGS (COMMON TO ALL MODES):

These parameters enable the iPBX to receive an acknowledgement-of-receipt e-mail from the subscriber who has read the e-mail received.

Upon receiving the acknowledgement of receipt, the system marks as READ the corresponding voice mail in the subscriber's IVB.

E-MAIL ADDRESS

iPBX mail box address on the mail server. This is the address to which the acknowledgement of receipt is sent.

PROTOCOL

The protocol definition field is used to define the reception settings (POP3 or IMAP).

SERVER

POP3 or **IMAP** mail server address as the case may be

PORT

Field used to define the mail server port number.

ENCRYPTED CONNECTION (SSL)

Checkbox which allows the use of an encrypted connection between the iPBX and the mail server used for the e-voicemail function if a message is received.

For more details, see the above case of message transmission.

VOICE MAIL ACCOUNT

Name of the iPBX messaging account on the mail server.

PASSWORD

iPBX messaging account password.

Authorised characters: [A-Z]+[a-z]+[0-9]+["#%'()*+,-./:;<=>@_]

Unauthorised characters: [!$&? [\]^`{|}~]

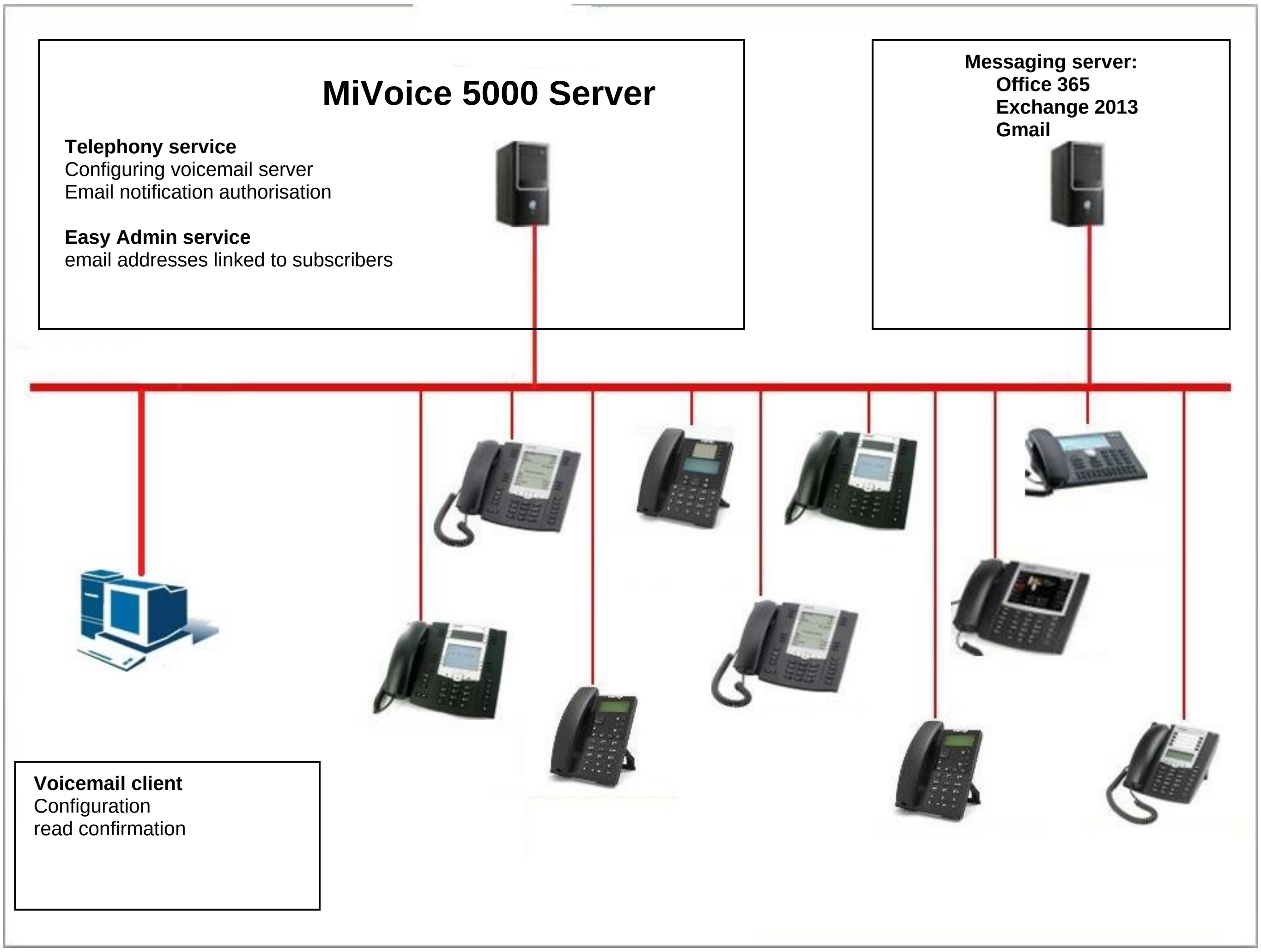
Check certificate:

Defining whether the certificate of an SSL or StartTLS connection should be verified.
Box ticked: Verification enabled (default setting).

Use modern authentication (Specific to Microsoft and Google modern authentication)

If the box is tiecked, modern authentication mode is used, associated in reception with the previously declared (Microsoft or Google) account.

EVOICEMAIL IVB: EXAMPLE OF A SIMPLE CONFIGURATION



TELEPHONY SERVICE

SUBSCRIBER GENERAL CHARACTERISTICS: DECLARING A VOICEMAIL BOX

- Select Menu **SUBSCRIBERS>Subscriptions>Characteristics**
- Tick the **Integrated voicemail box (IVB)** line.
- Select the class name (voicemail box class).

CONFIGURING THE SMTP MAIL SERVER SO AS TO BE NOTIFIED WHEN A MESSAGE IS LEFT

- Select Menu SYSTEM>Configuration>E-mail.

In the **Transmission settings** area:

- Enter the mail server address.
- Enter the account and access password for this server, if necessary.

Note: The "Account" and "Password" fields in the "Transmission settings" part correspond to the mail server access, and not to a subscriber account. It is necessary to indicate whether a password is defined in access to the mail server.

CONFIGURING THE POP3 MAIL SERVER TO ACKNOWLEDGE RECEIPT

- Select Menu SYSTEM>Configuration>E-mail.

In the **Receiving settings** area:

- Enter the e-mail address assigned to the iPBX
- Choose POP3 or IMAP
- Enter the mail server address in the Server field.
- Enter the e-mail account assigned to the iPBX and the associated password.

Note: The "Receiving settings" part enables you to configure the e-mail account associated with the iPBX.
Declaring the values of these fields allows acknowledgement of receipt of the notification e-mail.

CONFIGURING MESSAGE-LEFT NOTIFICATION BY E-MAIL, IN THE IVB CLASS

- Select Menu **VOICEMAIL AND TONES>Voicemail>Internal voicemail (IVB)>Box classes/Characteristics**.
- Select the item corresponding to the voicemail box in question.
- Define the management parameters for this voicemail box (NOTIFICATION/FORBIDDEN).
- Tick the voice message enclosed option if this option is chosen.

Note: The IVB is that of the subscriber's voicemail box on which the message is left (in the previous diagram, subscriber 200).
The "voice message enclosed" option only appears if "Notification" is chosen.

CONFIGURING THE SUBSCRIBER'S E-MAIL ADDRESS

From **Easy Admin Service,** Menu **My subscribers > My internal records** or **My subscribers > My external records**:

- In the subscriber list, select the subscriber concerned,
- Enter this subscriber's e-mail address in the **Mail** field.
- Click **Modify** to save the changes.

EMAIL WITH OUTLOOK 2013, OFFICE 365 AND GMAIL:

CONFIGURING THE SUBSCRIBER'S E-MAIL ACCOUNT ON THE MESSAGING CLIENT

In Outlook:

- Select Menu Tools>Messaging account.
- Select Add a new messaging account.
- Tick the POP3 box.

On the **Internet messaging settings screen (POP3)**:

- Fill in the following fields successively:

Your name	Subscriber account name
E-mail address	Subscriber's e-mail address
Incoming mail server (POP3)	mail server address
Outgoing mail server (SMTP)	mail server address
User name	Subscriber account name
Password	
Store password	

Note: Some columns may be associated with the Outlook configuration fixed by the system administrator. Contact them in this case.

CONFIGURING THE POP3 MAIL SERVER TO ACKNOWLEDGE RECEIPT

In Outlook:

- Select Menu Tools>Options.
- Select the Preferences tab.
- Select the **Mail options button.**
- Select the Monitoring options button.
- Tick the box you want in the area. Use this option to decide how to respond to message-read confirmation requests.
  - Always send a reply.
  - Ask me before sending a reply.

Note: Do not choose the option "Never send a reply" or else the message-read confirmation function would not be activated.

4.3.5.4 *User password, User Portal and Web Admin*

For more information on this tab, see Menu **SUBSCRIBERS>Subscriptions/Characteristics>General characteristics,** Paragraphs 3.3.3.1 and 4.3.2.3 for the definition of the user accounts declared on the system.

This tab is used to enter the content of the mail to be sent by the administrator when the password associated with the subscription and Web Admin login is changed.

SENDING E-MAIL ON CHANGE OF PASSWORD

By default, this box is not ticked. No e-mail is sent if the password is changed.

If the box is ticked the following lines allow the information message to be created:

SUBJECT

40-characters field used to define the subject of the message.

MESSAGE:

This 4-paragraph area is used to define the body of the message, which is broken down as follows:

- 2 paragraphs with 80 characters each.

- 2 paragraphs with 40 characters each (for example for the closing formula and signature).

- SECTIONS 1, 2, 3 AND4

A default, modifiable text is displayed.

The characters are in UTF8 format, allowing the use of accented characters.

The body of the message contains 2 - keywords #PWD#, #NUM#, #LOG#, #PBX#, which are automatically replaced, while creating the mail, with the subscription's password and directory number. These keywords should not be modified.

A mail is sent when the password is modified by the user if the subscription's e-mail address has been entered (personal password modification by the user is not part of mail transmission). A mail is equally sent when the e-mail address is entered (directory tab of the extension characteristics) if the subscription's password is the default password backed up in the file install.conf.

4.3.5.5 *Subscription locking*

Note: For more information about user password management, see Menu SUBSCRIBERS>Subscriptions> Characteristics>General characteristics, in Paragraph 3.3.3.1.

The **SUBSCRIPTION LOCKING** tab is used to enter the content of the mail to be sent by the administrator when the user password associated with the subscription is locked.

SENDING E-MAIL ON SUBSCRIPTION LOCKING

By default, this box is not ticked. No e-mail is sent if the subscription is locked.

If the box is ticked, several lines are displayed so the information message can be created like in the **USER PASSWORD** tab. See the previous paragraph.

Principle of subscription locking

The subscription is locked after the user has made three unsuccessful password input attempts (password frozen on the terminal or IVB).

SUBSCRIPTION LOCKED IN CASE OF INCORRECT PASSWORD

Some telephony functions require a password to be entered.

When three incorrect input attempts are made, the subscription is frozen for 5 minutes for the functions subject to a password.

When the operator freezes the subscription, the **To free the subscription** button appears below the **Subscr. status** line in Menu **SUBSCRIBERS>Subscriptions /Characteristics>General characteristics**.

At the same time, if the **SENDING E-MAIL ON SUBSCRIPTION LOCKING** box is ticked and the subscription has a configured e-mail address, the subscriber in question receives an e-mail with the associated text.

No e-mail is sent when the administrator unlocks the subscription or at the end of a timeout (5 minutes before a new attempt).

BLOCKING AN INTERNAL, MULTI-LINE SUBSCRIBER

All the lines have the same password.

The subscription is locked after three incorrect-password input attempts (cumulative, including IVB).

Unlocking, by the administrator or at the end of the timeout, applies to all the keys.

CLASHES WITH SPECIAL NUMBERS

Certain configurations require that emergency number calls be accessible on locked terminals. Therefore, it is necessary to declare the first digit of emergency numbers (example the digit "1" of "112", "15", etc.). User passwords must not start with the same digit.

A mail may be sent to users whose passwords have been modified.

See Menu **Dialing plan>User dialing plan>Access to public exchange** (Paragraph 5.2.3).

When the "**First digit of urgent numbers**" field is filled out, it is no longer possible to assign this 1st digit when a subscription password is modified; in this case, the error message "**Incorrect beginning**" is displayed. The same constraint is applied to Menu **Subscribers>Subscriptions>Create** for the default password.

4.3.5.6 *Alarm*

The **Alarm** tab allows you to enable or disable the sending of alarm e-mails and to specify their content.

This tab is hidden if there is an SNMP Manager in the configuration.

By default, sending alarm e-mails is not activated.

An alarm threshold (for all operators) can be defined.

- ....: Default value, all alarms are sent if no other option has been selected:
- WARNING,
- MINOR ALARM,
- SEVERE A,LARM
- CRITICAL ALARM.

Alarms are sent by email to operators if:

- There is no SNMP NRPE manager in configuration,
- The local site alarm configuration for routing to SNMP allows alarms to be sent (Menu Telephony service>System>Configuration>Alarms>Configuration display), allowing customisation).
- Sending alarm e-mails is activated,
- Operators have an e-mail address,
- Operators are allowed to receive an alarm notification by e-mail,
- The severity of the current alarm is above or equal to the transmission threshold,
- The e-mail connection settings are filled in.

E-mail alarms are displayed in logbook format and localized in the operators' language.

The different fields proposed are:

Transmit threshold: See above.

SUBJECT

40-characters field used to define the subject of the message. A default, modifiable text is displayed.

MESSAGE:

This 4-paragraph area is used to define the body of the message, which is broken down as follows:

- 2 paragraphs with 80 characters each.
- 2 paragraphs with 40 characters each (for example for the closing formula and signature).

- PARAGRAPHS 1, 2, 3 AND 4

A default, modifiable text is displayed.

The characters are in UTF8 format, allowing the use of accented characters.

The body of these messages contains the keywords #SITE#, #SEVERITY#, #DATE#, #ALARM#, which are automatically replaced when the e-mail is created. These keywords should not be modified.

4.3.5.7 *BluStar Mobile*

The BluStar Mobile tab is used to activate and configure the sending of e-mails to iPad/iPhone users. These latter, upon receiving the e-mail, will be able to download the configuration file allowing them to use the BluStar Mobile application.

To activate the function, tick the **BluStar Mobile E-mail configuration** checkbox. By default, this box is not ticked.

Ticking this box displays the rest of the screen containing a default text. The administrator can personalise the text.

The **#NUM#** variable stands for the subscriber's number.

4.3.6 MIB SNMP

Menu **SYSTEM>Configuration>mib snmp**

This command is used to enter the iPBX snmp MIB description parameters.

NAME

This parameter corresponds to the MIB **sysName** variable.

CONTACT

This parameter corresponds to the MIB **sysContact** variable.

LOCATION

This parameter corresponds to the MIB **sysLocation** variable.

COMMUNITY

The "public" default value authorises read access to the MIB.

MIB ACCESSIBLE TO

ALL MACHINES	No access restriction
MANAGERS AND SUBNET	Accessible by all the managers declared on the network and by all the machines on the same subnet.
MANAGERS ONLY	Accessible by all the managers declared on the network.

In SNMP V3 mode, only the option **MANAGERS ONLY** is proposed.

When returning from SNMP V3 mode to SNMP V1 mode, the field **MIB TO** is reset to **ALL MACHINES** (see also Paragraph **4.3.3.2.1**).

4.4 SECURITY

The **Security** menu contains all the sections for:

- Choice of security level (TLS version),
- Managing certificates (import, generation, assignment, revocation),
- The activation or not of the password policy on MiVoice 5000 products.

4.4.1 SETTINGS

Menu **SYSTEM>Security>Settings**

From R8.0, the TLS 1.0/1.1 level is no longer supported by default but can nevertheless be reactivated from this menu for SIP extensions (67xxi) that do not support the TLS 1.2 level.

The **Security level** drop-down list allows you to choose the following TLS security levels:

- **Standard (recommended),**
- **Compatibility**.

Changing the security level causes the restart of the SIP service (indicated by the message **Wait work in progress.**

By default, during a first installation or an upgrade, the TLS security level is set to **Standard (recommended),**

A message is also indicated to the Logbook.

Note : In very rare cases for which there has been no modification to the configuration of workstations in TMA, the global deployment index is equal to that of production.
In this case if this security parameter is modified, then a TMA action will be automatically launched to increment these indexes (a restart of these workstations will then be carried out).)

4.4.2 CERTIFICATES MANAGEMENT

Menu **SYSTEM>Security>Certificates management**

This menu is used to manage the certificates installed and/or to be installed on the iPBX, depending on the intended use. This menu contains several tabs:

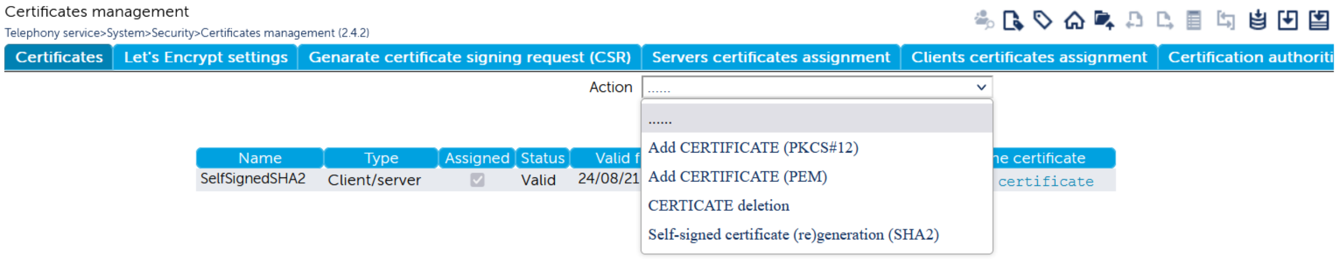
- Certificates tab, dedicated to the management of the certificates database installed on the iPBX, i.e. importing new certificates, (re)generating a self-signed certificate, or deleting existing certificates,
- Let's Encryp settings tab, used to define a domain for Let's encrypt-type trusted certificates specific to the integrated SBC,
- The **Generate certificate signing request (CSR)** tab is used to generate a certificate from a certification authority.
- Server certificate assignment tab, for assigning or unassigning certificates to users during Inter-site link, Web Admin, User Portal, Internet gateway, SIP and LDAP Server exchanges,

- Clients certificates assignment tab, for importing certification authorities from deployed LDAPS servers,

- Certification authorities tab, for importing certification authorities from deployed LDAPS servers deployed,

- Revocation tab, for enabling or disabling certificate revocation management.

4.4.2.1 *Certificates tab*


Certificates management
Telephony service>System>Security>Certificates management (2.4.2)
Certificates
Let's Encrypt settings
Genarate certificate signing request (CSR)
Servers certificates assignment
Clients certificates assignment
Certification authoriti
Action
......
......
Add CERTIFICATE (PKCS#12)
Add CERTIFICATE (PEM)
CERTICATE deletion
Self-signed certificate (re)generation (SHA2)

Name	Type	Assigned	Status	Valid f	ne certificate
SelfSignedSHA2	Client/server	☑	Valid	24/08/21	certificate

This certificate management tab (pkcs12 format) allows the following actions:

- Add/Replace a certificate in PKCS12 format (**.p12)**
- Add/Replace a certificate in **PEM format (.crt)**
- Delete a certificate (unassigned),
- Generate or regenerate a self-signed SHA2 certificate, if the certificate chain does not support SHA2,
- Generate and regenerate a **Let’s Encrypt** certificate.

Note: •Regeneration is forced (anticipated).

In this tab all the certificates available on the iPBX are displayed, with for each certificate:

- The name (entered by the import operator) or self-signed certificate name (SHA2) proposed by default,

- The type of certificate

- The assignment or non-assignment to a deployment (see the Certificates assignment tab),

- The status:

  - Invalid
  - Valid
  - Missing file
  - Expired
  - ----------------
  - Invalid CA
  - CN error
  - Incompatible key

  - OpenSSL error

- The start of validity date
- The end of validity date

By default, the list contains a self-signed SHA2 certificate assigned by default to Web Admin and to the User Portal.

The SHA2 certificate cannot be modified by the operator. It is provided by Mitel and always available. It may be regenerated after a change of configuration, but it remains transparent to the operator.

Clicking the **Detail** box of a given certificate displays an information list with the following fields:

- Comment (fixed by the system for self-signed certificates, or entered for imported certificates),
- Certification authority (CA) to which the certificate is attached,
- Identity (CN): (Possible) Common Name(s) and AltName(s) declared in the certificate as possible DNS values,

  The values **Common Name** and **AltName** stem from the configuration assigned in Menu**System>Configuration>Cards>IP board settings**.
- "Signature" field: Indicate the type of signature affixed on this certificate (sha1/sha256),
- Key size: Indicates the encryption key size (1024/2048 bits).

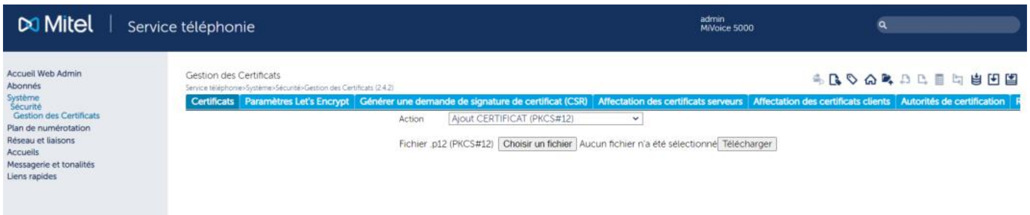
ADD/REPLACE CERTIFICATE,

This action imports a certificate in pkcs12 (**.p12**) or PEM (**.pem**) format. After selecting this option:

- Click Browse on the File line to be imported.
- Search and select to the file in question.
- Click Download.

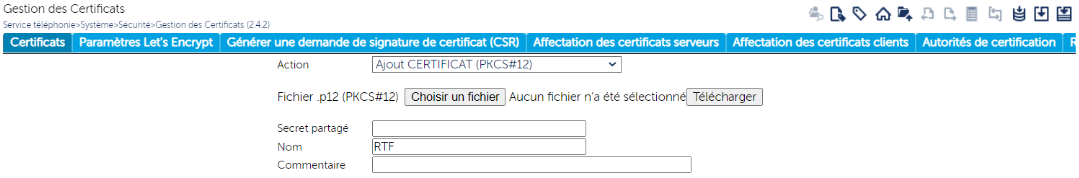
Once the file is downloaded, the different fields must be filled out:

CASE OF PKCS12 FORMAT



Action: Ajout CERTIFICAT (PKCS#12)

Fichier .p12 (PKCS#12) Aucun fichier n'a été sélectionné


Gestion des Certificats
Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.2)
Certificats
Paramètres Let's Encrypt
Générer une demande de signature de certificat (CSR)
Affectation des certificats serveurs
Affectation des certificats clients
Autorités de certification
Choisir un fichier
Télécharger

Action: Ajout CERTIFICAT (PKCS#12)

Fichier .p12 (PKCS#12) Aucun fichier n'a été sélectionné

Secret partagé:

Nom: RTF

Commentaire:

- ***Shared secret*** field appears so you can enter the passphrase used while generating pkcs12. This field is required to end the import of the file in PKCS12 format **.p12**.

  The passphrase is made up of an alphanumeric character string, which indicates the password used to decipher the certificate file.

  The number of characters entered must be between 4 and 20. The characters are clearly displayed during input, then replaced by ******* when the field is validated.

  List of characters authorised for this input field:

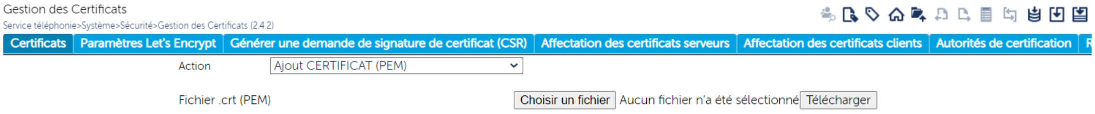
  - 0 to 9
  - A to Z
  - a to z
  - " # ' ( ) - _ @ + = % * > < , . ; / :

- **Name** field: enter the name for this certificate. This field is pre-filled with the imported file name **.p12** (only if this file name does not yet exist among the certificates already installed). This field is required to end the import of the **.p12** file.

- **Comment** field: this comment field is optional and will be attached to the certificate to help the operator identify this latter in case of multiple imports followed by late assignments.

Note: These fields are used by MiVoice 5000 Manager to import a pkcs12 file on an iPBX.

CASE OF PEM FORMAT


Gestion des Certificats

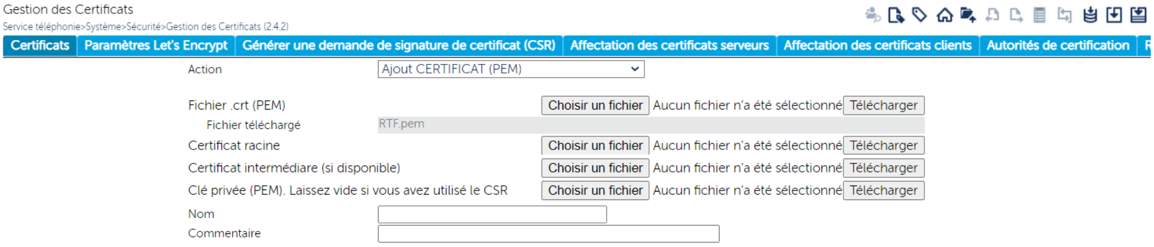
Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.2)

Certificats
Paramètres Let's Encrypt
Générer une demande de signature de certificat (CSR)
Affectation des certificats serveurs
Affectation des certificats clients
Autorités de certification
R

Action: Ajout CERTIFICAT (PEM)

Fichier .crt (PEM) — Aucun fichier n'a été sélectionné

Choisir un fichier
Télécharger


Gestion des Certificats

Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.2)

Certificats
Paramètres Let's Encrypt
Générer une demande de signature de certificat (CSR)
Affectation des certificats serveurs
Affectation des certificats clients
Autorités de certification
R

Action: Ajout CERTIFICAT (PEM)

Fichier .crt (PEM) — Aucun fichier n'a été sélectionné

Fichier téléchargé: RTF.pem

Certificat racine — Aucun fichier n'a été sélectionné

Certificat intermédiare (si disponible) — Aucun fichier n'a été sélectionné

Clé privée (PEM). Laissez vide si vous avez utilisé le CSR — Aucun fichier n'a été sélectionné

Nom

Commentaire

- **.crt (PEM) file**:

- **Root certificate**:

- **Intermediate certificate (if available)**:

- **Private key (PEM). Leave blank if you have used CSR**: if the downloaded certificate comes from a certification authority following the generation of a certificate signing request (CSR) on this server, the private key must remain empty.

- **Name** field: enter the name for this certificate. This field is pre-filled with the name of the imported **.pem** file (only if it does not already exist among the already installed certificates). This field is required to end the import of the **. pem** file.

- **Comment** field: this comment field is optional and will be attached to the certificate to help the operator identify this latter in case of multiple imports followed by late assignments.

In case of an error, the imported file is deleted and will not appear on the list of available certificates.

CERTIFICATE DELETION.

A certificate can only be deleted if it is no longer assigned (see Certificates assignment tab).

If the certificate is no longer assigned, tick the **Deletion** box for each of the certificates to be deleted then click **Validation**.

Even if it is not assigned to any use, the self-signed SHA2 certificate is never listed among the deletable certificates. This certificate is considered as filled out if a certificate is unassigned for Web Admin and User Portal deployments.

SELF SIGNED CERTIFICATE (RE)GENERATION (SHA2)

This action is used to generate a new SHA2 certificate, or to regenerate an already existing certificate.

Once generated or regenerated, the certificate appears on the listing table of the certificates tab.

Note: (Re)generating an already existing self-signed SHA1 certificate does not change the current assignment of this certificate.

Regarding the type of Let's encrypt certificate

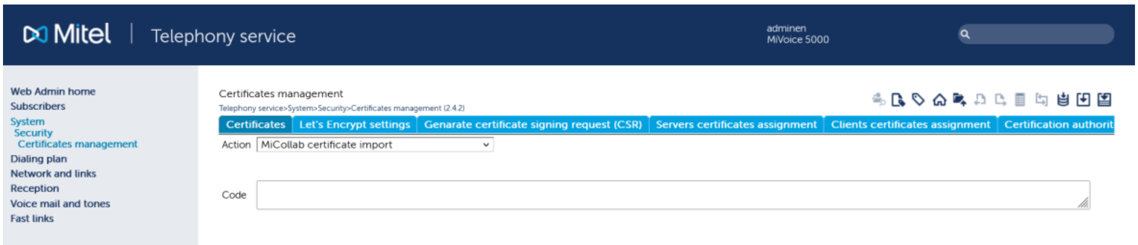
Let's Encrypt certificate compatibility facilitates secure TLS access for MiVoice 5000 systems.

This type of certificate has been added for the integrated SBC, but can be assigned to other services (except for the SIP service which is not offered for technical reasons).

MiVoice 5000 must be accessible from the Internet via an FQDN (**Let's encrypt settings**tab), which is used by Let's Encrypt to generate the certificate (**Certificates**tab) and for exchange via the ACME protocol.

Note: The Session Border Controller (SBC) is used to control and secure the signalling of media streams on video-over-IP or VoIP networks.

IMPORT MICOLLAB CERTIFICATE



Action: MiCollab certificate import

Code

This action allows you to manually import the MiCollab certificate. After selecting this option, a field appears:

- **Code**: field to be filled in. Enter the code generated by MiCollab during certificate generation. The **Validation** button then appears.
- Click **Validation** to have Call Server retrieve the MiCollab certificate.

The certificate:

- Is visible on the list of certificates,
- Can be assigned to a client in the Clients certificate assignment tab.

4.4.2.2 *Let's Encrypt Settings tab*

Menu **SYSTEM>Security>Certificates management**

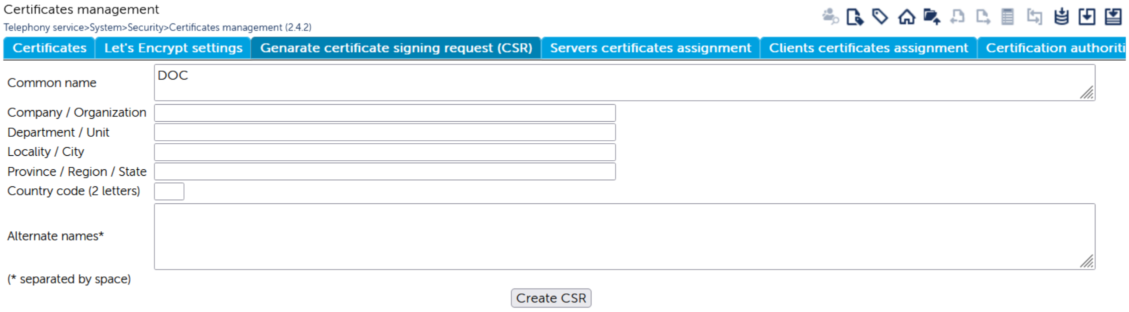
This tab is used to define a domain or other alternative names for some, other than FQDN, which may be Wildcards.

These domains concern the **Let's encrypt** trusted certificates generated or regenerated from the **Certificates**tab.

4.4.2.3 *Generate certificate signing request (CSR) tab*

A Certificate Signing Request (CSR) is a block of encrypted text sent to a Certification Authority (CA) that is required when users request for a certificate, such as an SSL/TLS certificate.

The CSR is required to create the certificate, which will then be distributed and installed on the systems in question.



Certificates management

Telephony service>System>Security>Certificates management (2.4.2)

Certificates
Let's Encrypt settings
Genarate certificate signing request (CSR)
Servers certificates assignment
Clients certificates assignment
Certification authoriti

Common name	DOC
Company / Organization	
Department / Unit	
Locality / City	
Province / Region / State	
Country code (2 letters)	
Alternate names*	
(* separated by space)	

The settings needed for this request must be entered in the following fields:

- **Common name (CN)**:
- **Company / Organization**:
- **Department / Unit**:
- **Locality / City**:
- **Province / Region / State**:
- **Country code (2 letters)**:
- **Alternate names*** (* separated by spaces):
  - ipv4
  - ipv6
  - Fully Qualified Domain Name (FQDN)

A download link is provided to retrieve the CSR file in **.csr** format.

This **.csr** file is then sent to the relevant authority to create the **.pem** file.

Then import the certificate from Menu **SYSTEM>Security>Certificates management - Certificates** tab. Refer to Section **Erreur ! Source du renvoi introuvable.**.

To delete a CSR certificate

- Click the **Delete CSR** button.

Note: If a new CSR certificate needs to be generated when one already exists, the existing CSR certificate must be deleted.

4.4.2.4 *Servers certificates assignment tab*

Menu **SYSTEM>Security>Certificates management**

The different uses proposed in the menu are:

- SIP terminal deployment allows the management of certificates for encryption in the terminals' SIP channel.
- Inter-site link deployment allows the management of certificates for encryption in this type of links (inter-site Movacs or intra-cluster links).
- Web Admin, User Portal and LDAP deployments allow the management of certificates for the encryption pertaining to these access interfaces.
- The use of Internet gateway to access the integrated SBC.

Note: Starting from R8.2 SP3, if the Internet Gateway has no affected certificate, the MiVoice 5000 automatically generates a default certificate for the use of Internet Gateway.

The assignment of a certificate to the LDAP service secures the access to the LDAP server in LDAPS (see 3.2.1.3).

However, the non-secure LDAP service remains active if port 389 is not locked.

Internet gateway assignment allows the Internet gateway to be secured for access to the integrated SBC.

The **Certificates assignment** tab allows assignments or unassignments for the certificates available to the proposed deployments.

This tab contains the following fields:

Available certificates proposes a list of available valid certificates.

Note: The Let's Encrypt certificate is not offered for the SIP service, for technical reasons.

Once the certificate in question is selected, a checkbox area can be used to define its assignment.

A **Validation** button is proposed to validate the change in assignment. This button appears when the first change is made in the assignments of the certificate selected by ticking the box(es).

A table is then displayed, summarising the assignment for each deployment and validity dates.

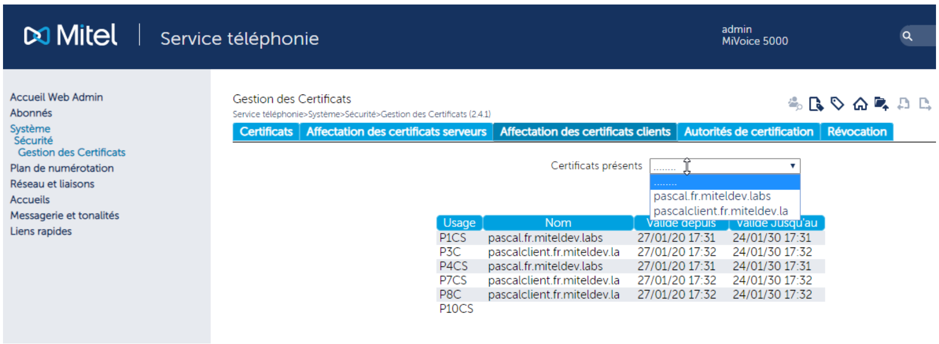
The two Web Admin and User Portal deployments must always have a certificate assigned.

Unassigning a certificate relating to any of these deployments results in an implicit re-assignment of the self-signed SHA2 certificate to this/these deployment(s).

The SHA2 certificate cannot be modified by the operator. It is provided by Mitel and always available. It may be regenerated after a change of configuration, but it remains transparent to the operator.

4.4.2.5 *Clients certificates assignment tab*

Menu **SYSTEM>Security>Certificates management**



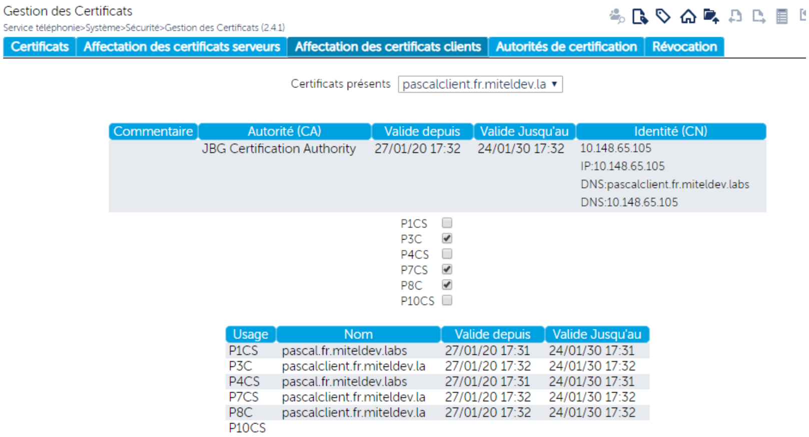
Gestion des Certificats

Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.1)

Certificats présents ....

....
pascal.fr.miteldev.labs
pascalclient.fr.miteldev.la

Usage	Nom	Valide depuis	Valide Jusqu'au
P1CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P3C	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P4CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P7CS	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P8C	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P10CS			


Certificats
Affectation des certificats serveurs
Affectation des certificats clients
Autorités de certification
Révocation

Gestion des Certificats

Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.1)

Certificats présents pascalclient.fr.miteldev.la

Commentaire	Autorité (CA)	Valide depuis	Valide Jusqu'au	Identité (CN)
	JBG Certification Authority	27/01/20 17:32	24/01/30 17:32	10.148.65.105 IP:10.148.65.105 DNS:pascalclient.fr.miteldev.labs DNS:10.148.65.105

P1CS ☐
P3C ☑
P4CS ☐
P7CS ☑
P8C ☑
P10CS ☐

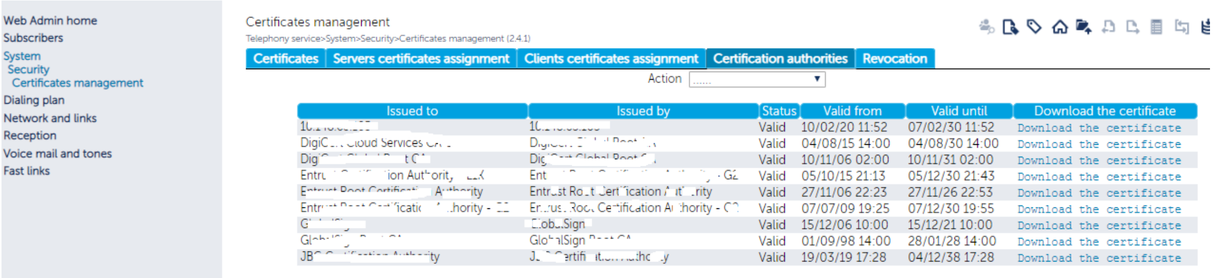
Usage	Nom	Valide depuis	Valide Jusqu'au
P1CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P3C	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P4CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P7CS	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P8C	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P10CS			

⚠ **IMPORTANT NOTE: TLS profiles are not available for the allocation of self-signed SHA2 certificates, to avoid a security gap for the terminals.**

A terminal should not be able to access the PBX via a connection secured by a self-signed certificate when TLS access 5061 is secured with a trusted certificate and MTLS.

4.4.2.6 *Certification authorities tab*

Menu **SYSTEM>Security>Certificates management**



Action ......

Issued to	Issued by	Status	Valid from	Valid until	Download the certificate
[redacted]	[redacted]	Valid	10/02/20 11:52	07/02/30 11:52	Download the certificate
[redacted]	[redacted]	Valid	04/08/15 14:00	04/08/30 14:00	Download the certificate
[redacted]	[redacted]	Valid	10/11/06 02:00	10/11/31 02:00	Download the certificate
[redacted]	[redacted]	Valid	05/10/15 21:13	05/12/30 21:43	Download the certificate
[redacted]	[redacted]	Valid	27/11/06 22:23	27/11/26 22:53	Download the certificate
[redacted]	[redacted]	Valid	07/07/09 19:25	07/12/30 19:55	Download the certificate
[redacted]	[redacted]	Valid	15/12/06 10:00	15/12/21 10:00	Download the certificate
[redacted]	[redacted]	Valid	01/09/98 14:00	28/01/28 14:00	Download the certificate
[redacted]	[redacted]	Valid	19/03/19 17:28	04/12/38 17:28	Download the certificate

Principle

The purpose of a certificate authority is to allow all TLS clients to check the certificates sent by the secure server to which they are connecting (in TLS).

The certification authorities represent a kind of central shop for certificates controlling TLS accesses.

This "shop" contains: CA certificates and possibly self-signed certificates.

How the tab works

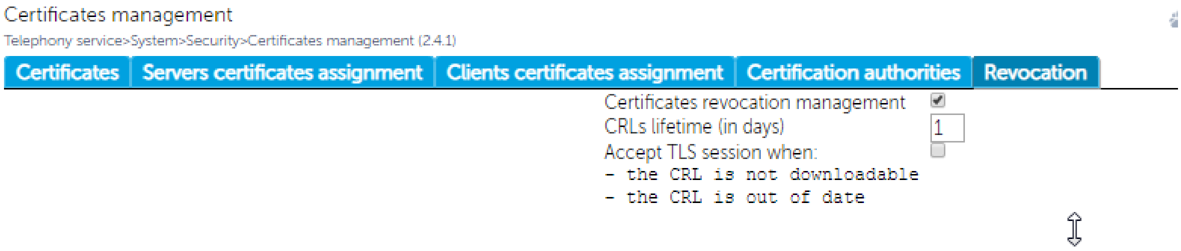
This tab allows you to import to the MiVoice 5000 Server client, the certification authorities of the deployed secure servers.

The certification authority is contained in the PEM file.

Possible actions are the addition or removal of a certification authority.

4.4.2.7 *Revocation tab*

Menu **SYSTEM>Security>Certificates management**


Certificates management
Telephony service>System>Security>Certificates management (2.4.1)
Certificates
Servers certificates assignment
Clients certificates assignment
Certification authorities
Revocation

Certificates revocation management ☑
CRLs lifetime (in days) 1
Accept TLS session when: □
- the CRL is not downloadable
- the CRL is out of date

This menu is for enabling or disabling 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 (checked) on first installation and after an upgrade. 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.

Note: CRL contains its own validity date.

The setting to accept sessions on CRL recovery failure or when the CRL is expired is, by default, disabled (unchecked).

If the administrator ticks this setting, the TLS session is allowed in the cases described above.

When the parameter is unticked, the TLS session is denied when the CRL file is out of date or cannot be found.

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

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),
- Importing the certificates into each MiVoice 5000 using the Server certificates tab of Menu **SYSTEM>Security>Certificate Management**.

4.4.3 ADDITIONAL TLS PROFILES

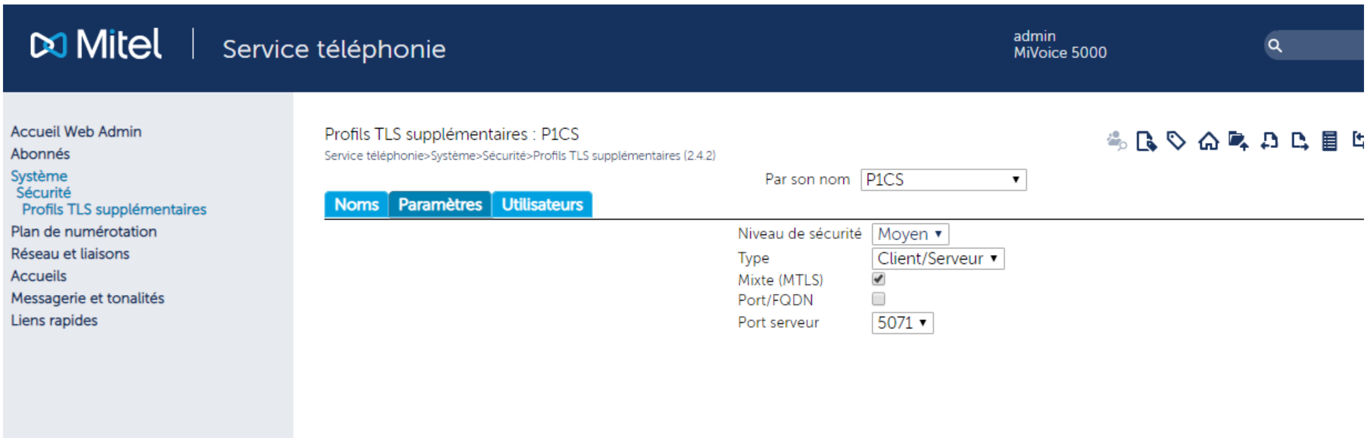
4.4.3.1 *Names tab*

SYSTEM Menu>Security>Additional TLS profiles

This menu allows you to define and configure profiles for secure connections (TLS) for SIP trunks, including :

- Assigning client certificates,
- Assigning specific certificates to a listening port or FQDN (associated with an SNI).

Up to 10 profiles can be defined.



Profils TLS supplémentaires : P1CS

Service téléphonie>Système>Sécurité>Profils TLS supplémentaires (2.4.2)

Par son nom P1CS ▾

Niveau de sécurité Moyen ▾

Type Client/Serveur ▾

Mixte (MTLS) ☑

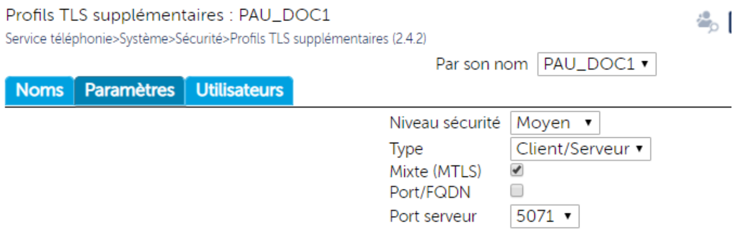
Port/FQDN □

Port serveur 5071 ▾

4.4.3.2 *Settings tab*

SYSTEM Menu>Security>Additional TLS profiles

This tab allows you to configure the settings for a TLS profile using the following fields:



Profils TLS supplémentaires : PAU_DOC1

Service téléphonie>Système>Sécurité>Profils TLS supplémentaires (2.4.2)

Par son nom: PAU_DOC1

Niveau sécurité: Moyen

Type: Client/Serveur

Mixte (MTLS): ☑

Port/FQDN: □

Port serveur: 5071

By its name: Option for selecting the TLS profile to configure.

Security level: Security level of the TLS version selected from the following 3 options:

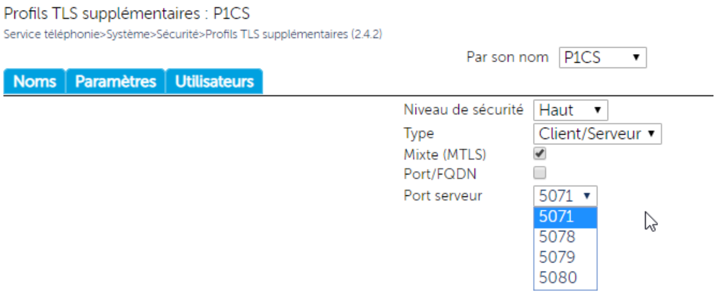
- Medium (default value)
- High
- Basic

Type: Option for defining the type of TLS profile to apply to the connection, which can be:

- Client/ Server: Default value
- Client
- Server

For the Client/Server and Server types, 3 additional lines identify the server configuration:

- Both way (MTLS): Box to be ticked if the TLS connection is bi-directional (MTLS). Checkbox ticked by default.
- Port/FQDN: Tick box to allow the choice of the port from the list or to fill in the FQDN server (for SNI).
  - Box not ticked:
- Server port: List of available and predefined values between Port 5071 and Port 5080. If ports are already used by other TLS profiles, they are no longer available and are not displayed when other profiles are being configured. Example:



Profils TLS supplémentaires : P1CS

Service téléphonie>Système>Sécurité>Profils TLS supplémentaires (2.4.2)

Par son nom: P1CS

Niveau de sécurité: Haut

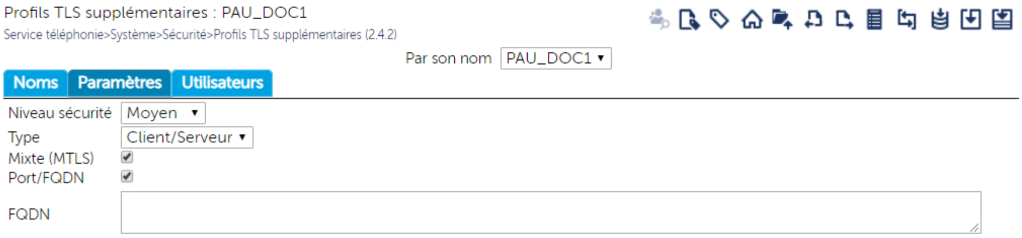
Type: Client/Serveur

Mixte (MTLS): ☑

Port/FQDN: □

Port serveur: 5071

Box ticked:



Profils TLS supplémentaires : PAU_DOC1

Service téléphonie>Système>Sécurité>Profils TLS supplémentaires (2.4.2)

Par son nom PAU_DOC1

Niveau sécurité Moyen

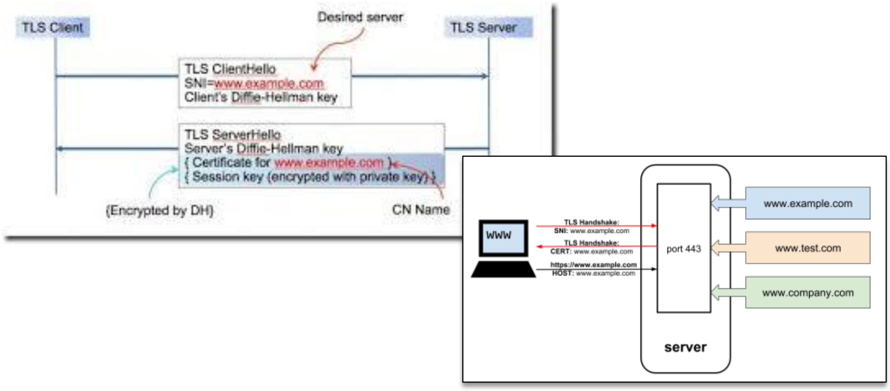
Type Client/Serveur

Mixte (MTLS) ☑

Port/FQDN ☑

FQDN

The **FQDN** field must be filled in to allow identification according to the SNI method described below:



Using an FQDN (SNI method) allows a connection to be accepted on Port 5061, and the certificate assigned to the FQDN to be returned. This full domain name belongs to the iPbx and defines this connection on the trunk.

SNI (server name indication): The SNI TLS protocol extension allows different TLS services to be offered on the same server and specifies the service required to present the correct certificate.

For example, for the domain **BTIPtrunk.mycompany.com**. This full domain name must be declared for use by the trunk operator or by a remote trunk.

If the FQDN cannot be used, for special reasons, a specific port must be used for trunk connection, as different certificates cannot be assigned to the same port without SNI.

The predefined port list is in the range [5071, 5080] and, as a port can only be used by one TLS profile (different certificates cannot be assigned to the same port), the list must contain only free ports.

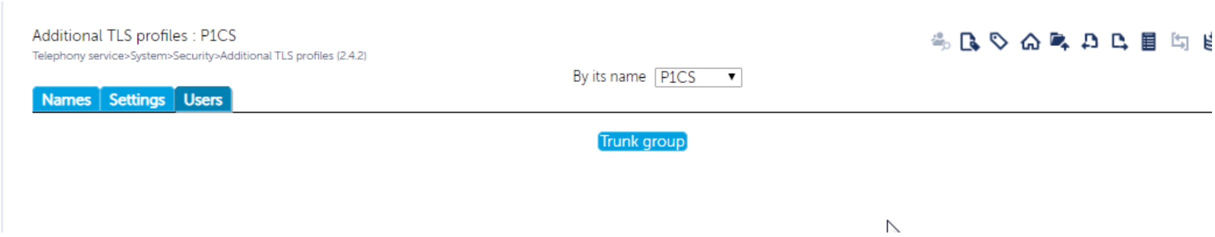
The FQDN is another way of determining the certificate to present on the server side for a TLS connection, based on the FQDN reached by the connection.

When a port is selected, it is not possible to set the FQDN and when an FQDN is set, it is not possible to select a port.

No check is made on the existence of the FQDN, only a syntactic analysis to ensure compliance with the FQDN syntax.

4.4.3.3 *Users tab*

SYSTEM Menu>Security>Additional TLS profiles

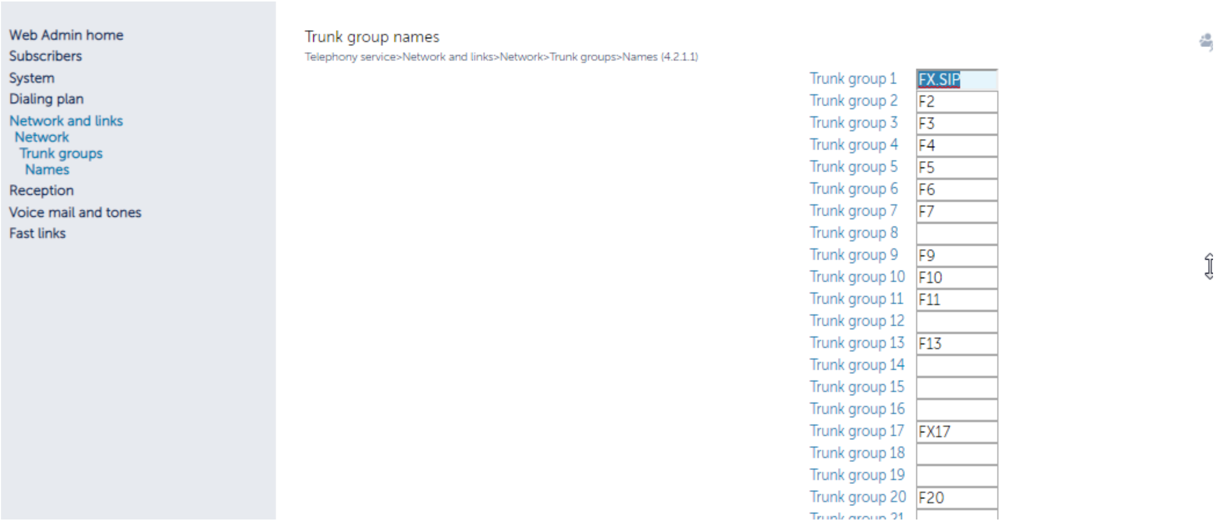


Additional TLS profiles : P1CS

Telephony service>System>Security>Additional TLS profiles (2.4.2)

By its name P1CS

This menu is used to display the trunk group using this profile. Users with the relevant TLS profile (**trunk group** type) are configured from Menu **Telephony service>Network and links>Network>Trunk groups>Characteristics** (advanced mode).



Trunk group names

Telephony service>Network and links>Network>Trunk groups>Names (4.2.1.1)

Trunk group 1	FX.SIP
Trunk group 2	F2
Trunk group 3	F3
Trunk group 4	F4
Trunk group 5	F5
Trunk group 6	F6
Trunk group 7	F7
Trunk group 8	
Trunk group 9	F9
Trunk group 10	F10
Trunk group 11	F11
Trunk group 12	
Trunk group 13	F13
Trunk group 14	
Trunk group 15	
Trunk group 16	
Trunk group 17	FX17
Trunk group 18	
Trunk group 19	
Trunk group 20	F20
Trunk group 21	

4.4.4 WEB ADMIN PASSWORD POLICY

4.4.4.1 *Configuration*

Menu **SYSTEM>Security> Web Admin password policy**

See also Sections 2.2.3.2, 2.2.3.3 and 4.3.2.

In this menu, the first line is used to indicate whether or not the password policy will be enabled. This activation or deactivation is done for all the user accounts.

If the box is ticked, all users will be asked to change their password the next time they log in. This new password will be used for future logins.

Web Admin password policy: box to be ticked or unticked.

If the box is ticked, the following settings must be entered to define a user password syntax policy (INSTALLER, OPERATOR, MAINTENANCE,CHARGING, DIRECTORY, XML INTERFACE):

- minimum password length in terms of 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),
- Number of special characters (0 to 16) it must contain, i.e. any of the following characters: « #'()-_@+=%*<>,.;/:
- Password validity period in number of calendar days (1 to 999).

When the password validity period is modified, the password expiry date is updated for all user accounts if the old expiry date is later than the new date.

It remains unchanged if the expiry date is earlier than the new expiry date.

4.4.4.2 *Mandatory password change during first login (only on standalone, redundant MiVoice 5000 Server and on MiVoice 5000 Server integrated into Mitel EX Controller)*

During first installation, the password policy is activated by default as of R7.2; therefore each user must change their password immediately on first connection. This is applied, regardless of the type of access - Local or SSO mode.

The following users are all concerned:

- INSTALLER,
- OPERATOR,
- MAINTENANCE CHARGING,
- DIRECTORY,
- XML INTERFACE,
- USER PORTAL

Immediate password change is also applied when the user logs in for the first time if they have never logged in before.

The password policy is renewed during an update:

- Retained: Nothing to do
- Activate or deactivate: In the Menu SYSTEM>Security>Web Admin Password Policy (refer to 4.4.4.1).

4.4.5 SECURITY LOG

Menu **SYSTEM>Security> Security log**

This menu is used to view and download the current security log.

The security log displayed in this menu is a partial security log, limited to the last traces, contained in a file of maximum 500 KB (divided into two files).

The MMI security log could directly display the content of the corresponding files, which represents about 1500 traces.

The exportable security file log are text files.

The security log (login/logout and configurations) is stored in the iPBX traces file.

The size of this traces file is:

- 2 MB on MiVoice 5000 Server

It may contain:

- Approximately 16,000 traces on MiVoice 5000 Server

It is circular and saved to disk as compressed files, in a space whose maximum size is configurable in Menu **Telephony service>System>Supervision>Disk space filling** (2.2.7).

By default, the following spaces are assigned to traces:

- 50 MB on MiVoice 5000 Server

Once compressed, the size of the trace files is approx. 120 KB on Call Server, which allows, with the default values of the storage space, to have:

- 415 files, i.e. approx. 6640000 traces on MiVoice 5000 Server,

The compressed trace files can be viewed with TR5000.

The traces, and thus the security log, can also be exported to allow them to be saved over a long period.

To get older logs, it is necessary to export the traces and read them with TR5000 / MAP or to look at the Syslog server side.

4.4.6 SECURITY

Menu **System>Security>WEB security**

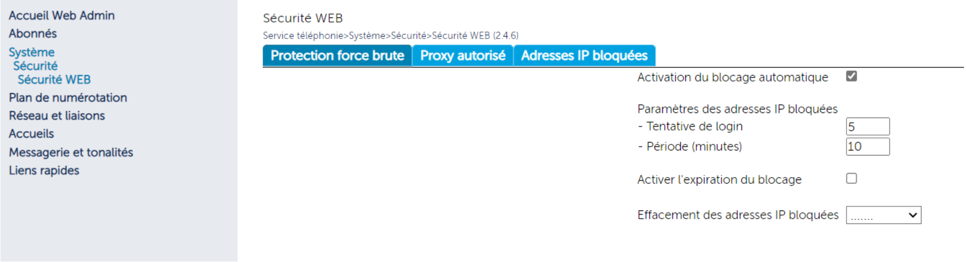
This menu is used to configure the security to be applied when accessing the User Portal in OTT mode.

In OTT mode, the User Portal may be subject to **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.

In case of too many failed connections, the IP address or FQDN is automatically blocked. However, the blocking period is configurable when activated.

4.4.6.1 *Brute force protection tab*



Sécurité WEB

Service téléphonie>Système>Sécurité>Sécurité WEB (2.4.6)

Activation du blocage automatique ☑

Paramètres des adresses IP bloquées
- Tentative de login 5
- Période (minutes) 10

Activer l'expiration du blocage □

Effacement des adresses IP bloquées ....

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 configured duration (in hours).

-**Unlock after (hours):** Default value 1.

Clearing blocked IP addresses: Options.

The **DELETE** option allows immediate deletion (after confirmation).

4.4.6.2 *Trusted proxy tab*

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

4.4.6.3 *Blocked IP addresses tab*

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

The different columns list, by address:

- The locking date and time,
- The target IP address,
- The origin of the attack,
  - **WEB** for MiVoice 5000 Web Admin, Easy Admin or MiVoice 5000 Manager,
  - **User Portal** for MiVoice 5000 User Portal,
- The number of login attempts after locking.

To delete a blocked IP address:

- Select the address concerned from the list.
- A window then opens to confirm the deletion.

4.5 SOFTWARE MAINTENANCE

Menu **SYSTEM>Software maintenance**

This menu is used to:

- Configure and run a system backup operation
- Configure and program a periodic backup operation
- Run a restore operation
- Run an update operation, either by installing a new version, or by installing the current version with patches
- Change massively the configuration of some types of data by importing a data file
- Download to a specific directory dedicated to the TFTP server, the files for IP DECT base stations, terminals A6XXD, and Wifi terminals 312I.

4.5.1 BACKUP

Menu **SYSTEM>Software maintenance>Backup**

This menu is used to:

- Configure and run a system backup operation
- Display the list of backup files available on the system
- Configure and program a periodic backup operation.

4.5.1.1 *Constitution of the backup*

Menu **SYSTEM>Software maintenance>Backup>Backup contents**

This command is used to configure the content of the backup and run a backup operation.

DATA BACKUP

- PABX DATA

These two parameters are not modifiable (the corresponding boxes cannot be unchecked). They correspond to the iPBX configuration data and are the minimum content of a backup.

- DIRECTORY RECORDS

If the box is ticked, the directory records will be backed up.

- ANNOUNCEMENTS

If the box is ticked, spoken announcements will be backed up.

- IVS MESSAGES

If the box is ticked, IVS announcements will be backed up.

CODE BACKUP

If you tick this box, the current software release will be backed up.

Use this option before upgrading the software so as to be able to return to the current release in case of problem.

After entering the backup creation settings, click "Validation” to start the backup operation.

When backup is completed, the backup file name appears in the field EXPORT OF THE FILE.

EXPORT OF THE FILE

Information field indicating the backup file name (for more information about the file name, see Section *4.5.1.2*.)

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

The backup file can then be copied in two ways:

- On the PC via HTTPS
- On an external disk (USB key).

To copy the backup file on the PC, click on the hypertext link available on EXPORT OF THE FILE. The PC operating system then opens the file download window.

To copy the backup file to the iPBX USB key, click **Save on iPBX USB key**. The file is copied to the directory /BACKUP/EXT created by the system if it is not available on the USB key.

Note: If the iPBX USB key is not available, an error message is generated.

4.5.1.2 *List of backup files*

Menu **SYSTEM>Software maintenance>Backup>Backups display**

This command is used to display the list of backup files available on the iPBX.

The backup file display table shows for each file:

- The file name in the following format: Bckp_*X*_*Y*_*yyyymmddhhmmss*.sav where:
- *X* shows whether the backup only contains data (d) or data and code (c+d)
- *Y* is the dongle identifier
- *yyyymmddhhmmss* indicates the backup start date and time
- The backup medium: local or external (USB key)
- The type of backup: d, or c+d
- Backup file backup date (backup end date)
- Backup file backup time (backup end time)
- The file size.

A hypertext link is available on the name of each file from the list used to copy the file on the PC. The PC operating system then opens the file download window.

4.5.1.3 *Programming a periodic backup*

Menu **SYSTEM>Software maintenance>Backup>Scheduling of periodic backups**

This command is used to:

- Configure the content of periodic backups
- Indicate whether the backup file must be saved on an external disk
- Confirm the backup frequency as well as date and time of first backup
- Cancel periodic programming.

The backup creation parameters are the same as the ones described in Section *4.5.1.1*.

SAVE TO EXTERNAL DISK

If you tick this box, the backup file will be copied to the iPBX USB key. The file is copied to the directory /BACKUP/EXT created by the system if it is not available on the USB key.

Note: If the iPBX USB key is not available during validation, an error message is generated.

INDICATE BACKUP FREQUENCY

DAILY	Backup takes place once a day at the time indicated in the HOUR field, as from the day indicated in the DATE field.
WEEKLY	Backup takes place once a week on the day of the week corresponding to the day indicated in the DATE field and the time indicated in the HOUR field, as from the day indicated in the DATE field.

PROGRAM THE FIRST OCCURENCE

DATE (DD/MM/YYYY):

First backup date.

HOUR (HH: MM):

First backup time on the date indicated in the DATE field.

After defining the periodic backup settings, click “Validation” to validate them.

The screen that appears summarises the periodic backup programming parameters. All the fields are information fields.

To cancel periodic programming, click **Cancel**.

4.5.2 RESTORE

Menu **SYSTEM>Software maintenance> Restore**

This command is used to:

- Run or program a restore of the full version (data + application code) or the iPBX configuration (data) from a backup file,
- Delete the current restore programming.

4.5.2.1 *Configuring and programming a restore*

Note: It is not possible to run or program a restore operation if a software upgrade has been programmed.

If no restore or upgrade operation has been programmed, the screen displays by default **Restore type**: **INTERNAL**.

TYPE DE RESTORE

INTERNAL	The backup file to use for restore is on the iPBX.
PC IMPORT	The backup file to use for restore is on the PC.

Select the type of restore you want then click "Validation”.

Case of PC IMPORT:

In this case the file to be downloaded must first be located then downloaded:

FILE TO DOWNLOAD

Name of the backup file to download from the PC.

Use the "**Browse**" button to locate the required file.

Use the "**Download**" button to download the backup file.

Click "**Validation**" to access the restore constitution screen.

INTERNAL:

The screen displayed gives the list of backup files available on the iPBX (either internal or on the external disk).

Click the number of the backup file you want to access the restore constitution screen.

APPLICATION: *VERSION NAME*

Version name indicates the software release corresponding to the backup.

CHOICE OF THE ITEMS TO RESTORE:

Only the items corresponding to the content of the backup file are proposed. They are ticked by default. To restore only certain backup items, uncheck the boxes for the items that should not be restored.

The restore creation parameters are the same as those of backup creation described in Section *4.5.1.1*.

- PABX DATA

This item must be part of the restore operation.

- DIRECTORY RECORDS>ANNOUNCEMENTS>IVS MESSAGES>IVB SIGNATURES>APPLICATIVE CODE

These are optional items:

TYPE OF SWITCH OVER

DEFERRED	The restore operation will be run by the system on the date and time indicated in the DATE and HOUR fields.
IMMEDIATE	The restore operation will be run once you press the “Validation” key.

KEY THE SWITCH HOUR

These fields must be filled in if you select DEFERRED switchover.

DATE (DD/MM/YYYY):

Restore start date.

HOUR (HH:MM):

Restore start time.

After entering the restore creation parameters, click “Validation” to validate them then start the restore operation if you selected IMMEDIATE mode.

Note: For a restore operation concerning the application code, you may be prompted for the keycode during validation.

If you choose DEFERRED mode, the following screen allows you to change or cancel the restore programming.

4.5.2.2 *Modify/dele restore programming*

This screen is displayed in the following cases:

- During access to Menu SYSTEM>Software maintenance>Restore, if a restore operation has already been programmed
- After a deferred restore request is validated.

To modify the restore operation, change the parameters then click **Validation** to take account of the modifications.

To delete the programmed restore operation, tick the **DELETE** checkbox then click **Validation**.

4.5.3 BACKING UP/RESTORING SPECIFIC DATA AFTER A CHANGE OF OPERATING SYSTEM

4.5.3.1 *Backing up specific data after a change of operating system*

The backup indicated in the previous section does not concern certain specific data which require, while upgrading the operating system, a specific script which is independent of the actions taken from the Web Admin menus.

The following specific data is not currently backed up / stored from Web Admin:

- IVB signatures: signature wav/was/avi files
- Left messages– IVB: wav or mp3/was/avi files of left messages.
- Pictures: .png files
- TFTP: TFTP firmware and ima.cfg file
- FTP: Mitel 6000 SIP Phone/MiVoice 5300 IP Phone files from an external TMA (firmware, language and configuration files)

This unique archive (and restore) script is independent of Web Admin, and must be manually started by the user if necessary:

archive_restore.sh

⚠ **WARNING: No choice of the data to be stored/restored is offered by this script.**

This specific data can be stored when MiVoice 5000 Server is working.

When R5.3 is upgraded (to R6.1), this operation may be carried out when Mitel 5000 Server is stopped (command: "service a5000server stop").

During this operation, all the IVB messages and signatures will be backed up regardless of their status (being recorded or already recorded) and regardless of their format (G711/PCM/AVI) or their extension (.wav/.was/.avi).

The backup directory of the message and signature files depends on whether or not Mitel 5000 Server is duplicated:

- Unduplicated MiVoice 5000 Server: "/opt/a5000notdupli/infra/mevo/bvim/"
- Duplicated MiVoice 5000 Server: "/opt/a5000/infra/mevo/bvim/".

This script automatically checks the size of the available storage space compared to the data to be backed up (pictures + IVB messages/signatures).

The script may correct the action taken by the user.

Procedure:

To make this backup, log on as root.

- Select the directory /opt/a5000/infra/utils/bin.
- In the terminal window, enter the command:
  - # chmod 777 archive_restore.sh

- #./archive_restore.sh archive /mnt/backup

This script has three settings:

./archive_restore.sh **function, directory, file**

The parameter **function** is used to specify the type of operation. For data backup, this parameter is **archive**.

The setting directory (**/mnt/backup)** is used to specify a target directory which may be on a local or network disk, or on a USB key. This space must first be created.

The setting **file** is used to specify the source or target archive file name. This parameter is optional for data backup. The default archive filename is **archive_YYYMMDDhhmmss.tar** if it is not specified in the script.

The required space can be estimated via The Web Admin in the Filing of disk space menu (voicemail boxes + pictures + FTP terminals). The file archive.log is used to display the backed up data (in **/opt/a5000/infra/utils/log**).

4.5.3.2 *Restoring specific data after a change of operating system*

The data must also be restored from a specific independent script in Web Admin menus.

This script is located in **/opt/a5000/infra/utils/bin** and is called **archive_restore.sh**

Important notes:

All the old files in the folders concerned will be deleted during the restore operation.

MiVoice 5000 Server is stopped when the script is started and then automatically restarted.

Procedure:

To perform this restore operation, log on as root.

- Select the directory /opt/a5000/infra/utils/bin.
- In the terminal window, enter the command:
  #./archive_restore.sh restore /mnt/backup archive_YYYMMDDhhmmss.tar

This script has three settings:

./archive_restore.sh function, directory, file

The parameter **function** is used to specify the type of operation. For data restore, this parameter is **restore**.

The parameter **directory** (**/mnt/backup**) is used to specify the folder containing the archive file, which may be on a local or network disk or on a USB key. This space must first be created.

The parameter **file** is used to specify the source or target archive file name. For a data restore operation, this parameter indicates the name of the file archive.tar to be restored.

4.5.4 UPGRADE

Menu SYSTEM>Software maintenance>Upgrade

The only method of upgrading the software components of a Cluster or MiVoice 5000 Server is from the repository.

This repository server, on which the upgrade packages will be deposited, is located:

- Either on the operator's (Windows) PC,
- Or on a public Mitel platform,
- Or on the MiVoice 5000 Manager server PC.

Refer to the document **Updating by Repository**.

For upgrades via Repository, it is possible to:

- Receive a notification by e-mail and via the logbook if a new version of MiVoice 5000 is available,
- Receive a notification by e-mail and via the logbook if a security patch is available,
- Automatically install the security patches.

UPDATE CHECKING

Action

Dropdown list. For selecting the MiVoice 5000 action for automatic updates.

- Disabled: MiVoice 5000 does not notify operators when new versions or new security patches are available.
- Notify: MiVoice 5000 notifies operators by email and in the logbook when new versions or new security patches are available.
- Security patch update: MiVoice 5000 notifies operators by email and in the logbook when new versions are available and automatically installs new security patches.

Day

Dropdown list. For setting the day to check for a new MiVoice 5000 version or patch.

Hour of starting (hh:mm)

Field to be filled in. For setting the time to check for a new MiVoice 5000 version or patch.

Note: If operators are unaware of the updates to be made, MiVoice 5000 sends an e-mail and a notification in the logbook every week, according to the day and time scheduled for the check.

4.5.5 MASSIVE DATA IMPORT

Menu **SYSTEM>Software maintenance>Massive import**

Note: See also other import modes in Section 2.3.3 from the icon

IMPORT TYPE

GENERIC

This option is used to import files in .csv format and some archive files in TAR, TAR.GZ or ZIP format.

The import function is used to read an external file in CSV format and, thus, configure all similar items.

These functions can be used to massively modify data on the iPBX:

- Import the modified file to reconfigure the data.
- Perform a massive import during a first installation from the massive creation form (see the appendix to the *Installation and Maintenance Manual*.

The export function is described in 2.3.2.8.

Other import modes are available, depending on context or files relating to the item processed. See Section 2.3.3.

For massive tone import, some IVR and IVB, or the associated file(s) available in the archive are also imported.

IVB SIGNATURES

This option allows massive import of customised greeting messages.

The accepted archive file format is TAR, TAR.GZ or ZIP.

The restrictions are the same for individual import (format, type, size).

A report of the import is displayed (so possible errors can be identified).

Accepted IB signature formats are:

- Number-based format
- First name/Surname based format

<u>Number-based format</u>

<number>_<signature type>_[xxx].<ext>

- <number>: VM number
- <signature type>: Name / AnsRec / AnsOnly
- Name: Signature type Name
- Ansrec: Signature type Answering/recording machine
- AnsOnly: Signature type Answering machine
- [xxx]: option enabling the user to customise the file name
- <ext>: wav or avi

Example: **65010_AnsRec_Service1.wav**

In this example:

- The voicemail box number is: 65010
- Its type is AnsRec: Answering/recording machine
- The remark indicates: Service1
- Sound file format: wav or mp3

First name/Surname based format

<first name>_<surname>_<signature type>_[xxx].<ext>

- <first name>: IVB user's first name
- <surname>: IVB user's surname
- <signature type>: Name / AnsRec / AnsOnly
- [xxx]: option enabling the user to customise the file name
- <ext>: wav or avi

Example: bob_smith_AnsOnly_Agent01.avi

In this example:

- The voicemail box user's first name is: bob
- The voicemail box user's surname is: smith
- Its type is AnsOnly: Answering machine
- The remark indicates: Agent01
- Video file format: avi

Note: It is advisable to use the Number format for a Multi-Directory configuration with the presence of homonyms.
During import processing, a consistency check is made with the directory database.

FILE TO IMPORT

Name of the file to download from the PC.

Use the **Browse** button to locate the required file.

After filling in this field, use the **Download** button to download the upgrade file.

At the end of the download operation, use the “Take account of the data button” to apply the downloaded data to the system.

When the data are taken into account, a report window opens.

The report window presents a table, with lines and columns corresponding to those of the imported file.

Only the lines for which at least one error was encountered during processing are displayed. The message displayed below the table gives the number of lines processed without error and the number of requested processing lines.

The data highlighted in green has been modified or created successfully.

The data displayed in red has not been modified or created. An information bubble is available on the data displayed in red, indicating the reason why it has not been taken into account.

The data displayed in black has not been processed (no processing requested).

4.5.6 LOADING OF FILES

4.5.6.1 *TFTP tab of Menu SYSTEM>Software maintenance>Loading of files*

The tab of this menu is used to download the files for the following devices to a specific directory dedicated to the TFTP server:

- DECT SIP RFP 32-34-42 (File type iprfp2G.tftp) Mitel OMM 4.0 network
- DECT SIP RFP 35-36-37-43 (File type iprfp3G.dnld) Mitel OMM 4.0 network
- IMA CONFIGURATION:
- TERMINAL A6XX ("aafon6xxd.dnld")
- WIFI TERMINAL 312I ("312w.dnld")

The “**Browse**” button gives access to the original directory and is used to select the file to download.

With Mitel SIP DECT RFP 35..43, a version exists already for terminals A6xxd and Wifi terminals 312i; it is displayed in a non-modifiable “**Actual version**” field.

Click "**Confirmation”** after the name of the file to be downloaded to the “**New File**” field is displayed.

If the format for the file to download is incorrect, an error message is displayed.

The TFTP server may be of several types:

- Located on the same PC as MiVoice 5000 Server,
- On a dedicated PC.

Note: The format consistency is checked by detecting the version for terminals A6xxd and 312i files. There is no check for the IP DECT base station software.

4.5.6.1 *Terminal space of Menu SYSTEM>Software maintenance>Loading of files*

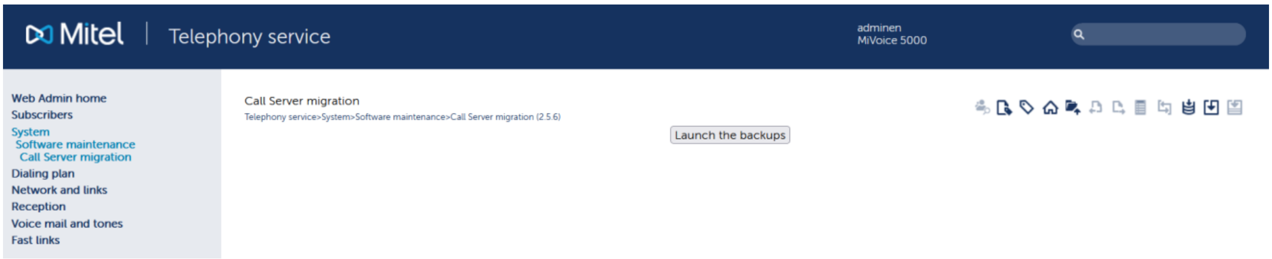
This tab, available as of R7.0, is dedicated to the management and updating of items:

- 6xxxi,
- 53xxip,
- 53xx.

Refer to the Installation and Management Manual of MiVoice 5300 IP/Digital Phones, Mitel 6700 and 6800 SIP Phones, MiVoice 6900 IP Phones.

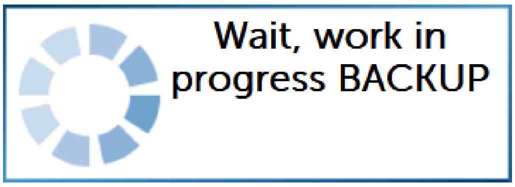
4.5.7 EXPORTING DATA FOR CALL SERVER MIGRATION

Menu **SYSTEM>Software maintenance>Call Server migration**



This menu is used to generate the backup files required for Call Server migration.

Click the **Launch the backups** button to create the backup files required for migration. A pop-up window appears while the backup files are being created.



After a few seconds, the page displays the following backup files:

- The general backup file, with the file name **BCKP_D_CS_MIGRATION.sav**.
- The specific backup file, with the file name **BCKP_S_CS_MIGRATION.tar**.

Click **Export backup file** and variants to download the corresponding backup file.

Click **Delete backup file(s)** to delete the last backup files generated and return to the page for creating backup files.

4.5.8 RESTART REQUEST

Menu **SYSTEM>Restart request**

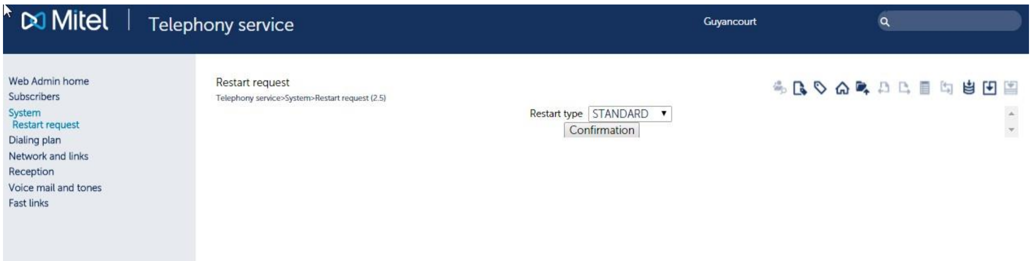
This command is used to:

- Validate the active version if it is being tested (after software upgrade),
- Return to the validated version if the active version is in test and does not run as expected,
- Restart the iPBX application,
- Restart the iPBX application and generate an error file which can be used by MITEL support,
- Restart the iPBX application and the integrated Linux OS,
- Stop the iPBX application and integrated Linux OS.

You may need to restart the system so the modifications to certain configuration data can be taken into account, or after installing a patch.

To access this menu, click "Software maintenance" from the system management main menu.

If you validate the active version, the restart request screen appears as follows:



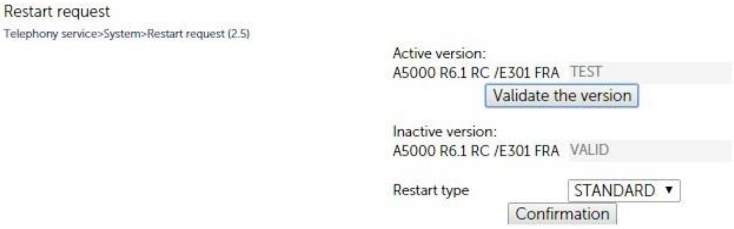
Restart request

Telephony service>System>Restart request (2.5)

Restart type STANDARD

Restart request (1)

If the active version is in test, the restart request screen appears as follows:



Restart request

Telephony service>System>Restart request (2.5)

Active version:
A5000 R6.1 RC /E301 FRA TEST

Inactive version:
A5000 R6.1 RC /E301 FRA VALID

Restart type STANDARD

Restart request (2)

RESTART TYPE

RETURN TO VALID VERSION	The iPBX application restarts with the valid version (currently the inactive directory). The integrated Linux OS is only restarted if the OS versions of the active and passive directories are different. This option is only available if the active version has not been validated.
STANDARD	Only the iPBX application is restarted.

4.5.9 VALIDATING THE ACTIVE VERSION

The restart request screen shows the two software packages available on the system:

- That of the active version in test
- That of the validated inactive version

To validate the tested version, click **Validate the version**.

During the validation phase, the **Validate the version** button is orange in colour:

At the end of the operation, the active and inactive versions are identical and have the status VALID.

4.5.10 RETURINING TO THE VALIDATED VERSION

You can return to the validated version when the active version is in test.

To return to the validated version, select RETURN TO VALID VERSION in the RESTART TYPE field then click “Confirmation”.

The iPBX restarts to the validated version. A wait message then appears.

At the end of the countdown, this screen disappears and the system becomes operational again.

The active version is then the version running prior to the upgrade operation. This version is validated.

The inactive version is the version installed through upgrade, and it is not in test.

WARNING: **This status does not present the backup version in case of problem on the active version. It is advisable to reinstall as quickly as possible a new upgrade provided by the manufacturer, which corrects the malfunctions in the previous version.**

4.5.11 RESTART

To perform a restart, select the type of restart you want then click "**Confirmation**".

The iPBX restarts and a wait message is then displayed:

At the end of the countdown, this screen disappears and the system becomes operational again.

STANDARD:

- In a standard configuration, this action allows the iPBX to restart.
- In a Mitel 5000 Cluster configuration, this action restarts only MiVoice 5000 Cluster Server.

STANDARD WITH THE NODES:

In a Mitel 5000 Cluster configuration, this action restarts the MiVoice 5000 Cluster Server and all associated nodes.

REBOOT OS:

The system is rebooted completely from the OS.

STOP OS:

The system is shut down.

CONFIGURATION RESET:

The system is restarted with the canonical configuration.

STANDARD WITH COREDUMP:

Same as Standard with a trace file available in Menu **Telephony service>System>Expert>Processor access>Debug tools>Errors management**.

4.6 EXPERT

Menu **SYSTEM>Expert**

This menu is used to:

- Deploy investigation tools to solve problems
- Display/change the different call and ringer-related timeouts
- Change the configuration data parameters and identify the changes compared to the original values
- Test some connections
- Manage the list of Mitel proprietary terminals.

4.6.1 PROCESSOR ACCESS

Menu **SYSTEM>Expert>Processor access**

This menu is basically meant for a special investigation requested by Technical Support.

It is used to:

- Deploy investigative tools such as activation of traces, recovery of error files
- Identify excess loads on the card processors
- Access the atomic information of the system configuration via PAS files.

4.6.1.1 *Debug tools*

Menu **SYSTEM>Expert>Processor access>Debug tools**

This menu is used to:

- Manage traces (configuration, export, etc.)
- Recover error files
- Send a Ping request to test the accessibility of a remote device.

4.6.1.1.1 Traces

Menu **SYSTEM>Expert>Processor access>Debug tools>Traces**

This menu is used to:

- Configure traces
- Manually export traces to a file
- Display the configuration
- Display the list of available traces available on the iPBX
- Download the traces files available on the iPBX.

4.6.1.1.1.1 Settings

Menu **SYSTEM>Expert>Processor access>Debug tools>Traces>Parameters**

This command is used to:

- Modify the IP address used to redirect traces to a SYSLOG client,
- Change the current configuration of traces by downloading a configuration file
- Apply the default configuration
- Manually export traces to a file.

SYSLOG SETTINGS

TLS: Checkbox in case of secure connection to Syslog servers. This requires importing the root authority of Syslog servers certificates.

.

IP ADDRESS SERVER 1 AND 2/PORTS

Choice of 2 IP addresses to redirect the traces to one or two remote SYSLOG server(s) in order to send the Security Log.

Processing is done via UDP.

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

☞ The SYSLOG service must be installed on MiVoice 5000 Server. Refer to the document MiVoice 5000 Server - Implementation.

This service must also be activated in Menu **System> Services**.

Messages are sent in real time to the Syslog server(s).

When the session with a Syslog server is lost, there is no repetition of the messages sent. Similarly, a message can be lost, if it is sent in UDP.

To avoid this loss of messages, the Syslog connection mode in TLS may be preferred to standard mode.

The **Test Syslog** button is used to test the connection to these servers.

CONFIGURATION OF TRACES BY FILE

Name of the traces configuration file.

The "**Browse**" button opens a browser used to search for a file on the PC. When the file is found and selected in the browser, the **Download** button can be used to replace the current configuration file with the new one. The new configuration is taken into account once downloading is completed.

The application of a new traces configuration file is generally used for a special investigation and is limited in time. To restore the default configuration at the end of the investigation, click **Default configuration**.

EXPORT TAB

EXPORT OF THE TRACE

The "Export of the trace" button is used to force traces export top a file before the maximum size (512 KB) of the buffer containing the trace on the iPBX is attained (when this size is attained, automatic storage takes place on the system).

EXPORT LAST TRACES FILE

This field indicates on the right the name of the last available traces file, and the title of the left column field is a link that gives access to the downloading of the said traces file.

XX TRACES FILES PRESENT

XX represents the number of traces files stored locally. The link gives access to the trace file listing page corresponding to Menu:

System>Expert>Processor access>Debug tools>Traces>List of trace files

DELETE THESE FILES

Pressing this button definitely deletes the available traces files.

RECOVER TRACES FILES GENERATED BETWEEN:

This command is used to group together in a .tar file all the traces files between two dates/timeslots.

The following fields represent the **start and end dates and time** of the traces files to be recovered.

The CONFIRMATION button generates the **traces.tar** file which can be downloaded via the link on the next menu **EXPORT OF THE FILE.**

4.6.1.1.1.2 Configuration

Menu **SYSTEM>Expert>Processor access>Debug tools>Traces>Configuration**

This menu enables the installer to configure the following trace levels individually:

- INFO
- ERR0201
- WAR
- ERR.

For each trace, select the **ml** name and the corresponding **module** name.

4.6.1.1.1.3 Display the configuration of the traces

Menu SYSTEM>**Expert>Processor access>Debug tools>Traces>Configuration display**

This command is used to display the software modules and severity levels for which the traces are activated.

4.6.1.1.1.4 List of trace files

Menu **SYSTEM>Expert>Processor access>Debug tools>Traces>Display**

This command is used to display the list of the traces files which have been exported either automatically by the system (maximum size has been attained) or manually (**EXPORT OF THE TRACE** in the menu **SYSTEM>Expert>Processor access>Debug tools>Traces>Settings**).

The list of stored files shows for each storage:

- The file name (trace_date_time.tar.gz)
- The date and time of storage
- The file size.

Click the name of an archive to download the archive for possible transmission to Technical Support.

4.6.1.1.2 Dump IP

4.6.1.1.2.1 General information

The **Dumpip** function is used to capture the traffic sent and received on the CPU interface (Port 5).

The corresponding menu is possibly used to filter and modify the capture according to one of the profiles proposed (or type of dump; see below for the proposed options).

The capture files are in **.pcap** format and can be used by various tools, including Wireshark (not supplied)

Menu SYSTEM>Expert>Processor access>Debug tools>Dump IP>Configuration.

Description of the fields:

Type of dump:

The different possible Dump types:

- SIP
- GENERIC

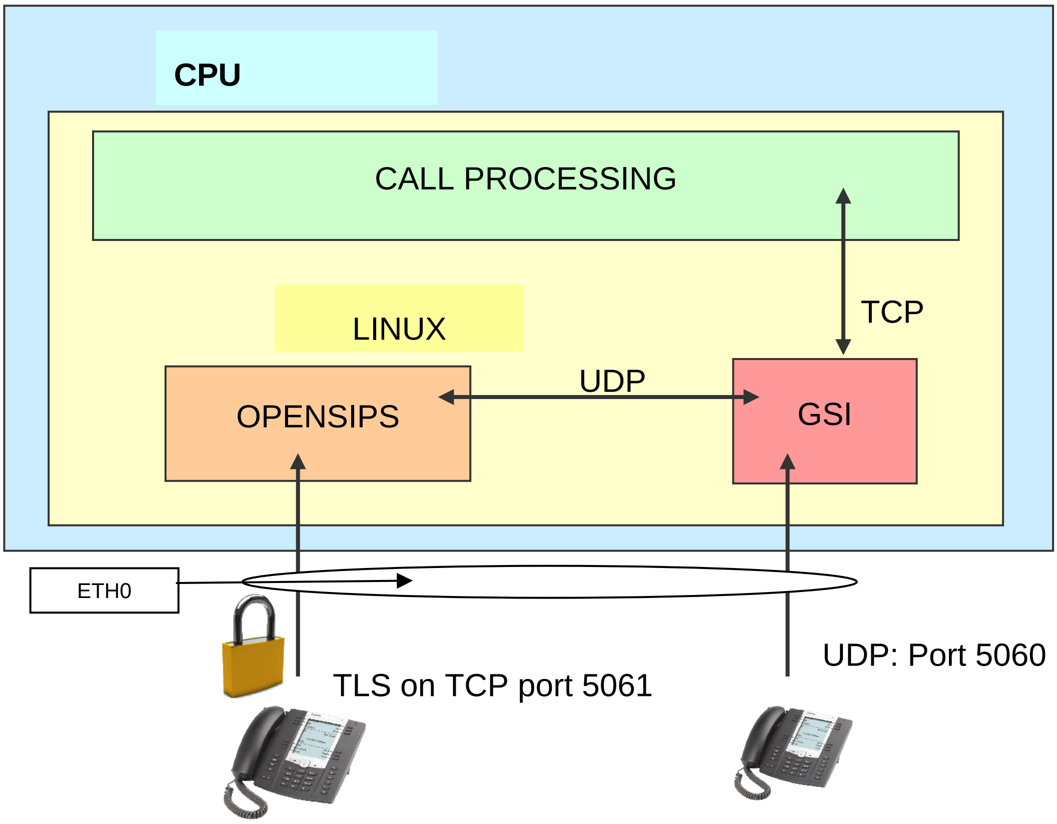
Note: When a filter input field is proposed, its syntax is that of the TCPDUMP tool (for the syntax, refer to the various web sites about this tool).
The filter entered by the operator is not stored and must be entered again each time capture is started.

SIP

This option, which corresponds to the SIP profile, is used to capture the encrypted/unencrypted SIP signalling traffic.

SIP signal processing is presented in the diagram below: the GSI serves as a gateway between system call processing and the devices communicating in SIP mode. It translates proprietary signalling messages to SIP messages and vice-versa.

If the calls are encrypted, signal encryption/decoding is handled by OPENSIPS.



The following dump interfaces are available:

- INTERNAL: capturing the SIP packets exchanged on the internal loopback IP address (127.0.0.1), that is the packets exchanged between the software modules of the CPU, GSI and OPENSIPS. It is all about unencrypted SIP messages corresponding to the encrypted messages exchanged with encrypted SIP terminals.

- ETHERNET 0: capturing the SIP messages sent and received on the ETH0 interface of Linux: everything circulating on port 5 of the microswitch. It is all about encrypted and unencrypted SIP messages exchanged with encrypting and non-encrypting SIP terminals.

- ALL: both traffics mentioned above are captured.

Note: On the INTERNAL interface, the packets are exchanged using the standard loop-back address 127.0.0.1. To facilitate the reading of traces, a different IP address is assigned to the two modules during the capture (GSI/OPENSIPS).

GENERIC

This option, which corresponds to the generic profile, is used to capture the traffic on the CPU port.

The dump interface options are the same as for the SIP (see above).

In summary:

In general, the most frequently used configurations will be:

- GENERIC / ETHERNET 0: for capturing the entire data and signal traffic only sent and received by the system (excluding voice over IP)

- SIP / INTERNAL: for unencrypting encrypted SIP signals

Running captures

After configuring dumps, click the button **Run the dump to run the capture**.

The resulting file can be viewed in Menu **SYSTEM>Expert>Processor access>Debug tools>IP dump>Display**.

After the capture is started, only one button **Stop the dump** is displayed in the configuration menu used to stop the action.

Note: During start or stop, if the command is not correctly executed, the message "system error" is returned to the operator.

Erase all dump files button

If no capture is started, this button can be used to erase all the already stored capture files, to avoid keeping unnecessary traces.

Storing capture files

If this area is filled up, the oldest captures are automatically erased to avoid exceeding the storage capacity.

4.6.1.1.2.2 Displaying Dump ip

Menu **SYSTEM>Expert>Processor access>Debug tools>Dump IP>Display**

This column is used to display and/or download the capture files.

On the displayed page, each line presents a capture file, its date and size.

- Select the file concerned to download it to a directory you want so you can then use it.

The files are compressed and timestamped. They contain the capture in .**pcap** format (example: **dumpip_00001_20101005175155.tar.gz**).

4.6.1.1.3 Errors management

4.6.1.1.3.1 Errors display

Menu **SYSTEM>Expert>Processor access>Debug tools>Errors display**

Serious errors such as system failures are logged and stored in error files.

This command is used to display the list of error files.

The list of stored files shows for each storage:

- The file name (crash-date+time.tgz)
- The date and time of storage
- The file size.

Click the name of an archive to download the archive for possible transmission to Technical Support.

4.6.1.1.3.2 Core-dump creation

Telephony service>System>Expert>Processor access>Debug tools>Errors management>Core-dump creation

- For the PBX software
- For the SIP gateway
- For the SNMP agent

- For Media Server
- For the Utils

4.6.1.1.4 Troubleshooting

In case of technical issues with the MiVoice 5000, this menu gathers the system information from the machine and the MiVoice 5000 Server.

The retrieved data for troubleshooting are listed below:

- Configuration
- Network (IP address, ports)
- System resources -Mem, cup, tasks)
- Disk resources
- Logs
- Traces
- Errors
- Advanced QoS
- Yum history

Check the boxes of the data to retrieve. Click the **File creation** button to generate **the trouble.tar** file, which gathers all the requested data.

The **trouble.tar file** appears on a ne like. Click the **Export of the file** hyperlink to download the file.

4.6.1.1.5 Ping request sending

Menu **SYSTEM>Expert>Processor access>Debug tools>Ping request sending**

This command is used to send a Ping request to a remote device to check that it is accessible via the network.

TO IP ADDRESS

IP address to which the request is sent.

Once this field is completed, the following field appears on the screen.

WITH IP CARD

Location of the IP card to be used to send the ping request to the IP address mentioned above. The drop-down list contains all the IP card slots in the cabinet.

Once this field is completed, the following fields appear on the screen.

DATA SIZE

Size of the IP packet that will be sent. The default value is 32. Possible values are between 32 and 1024 bytes.

TIME TO LIVE OF THE IP DATAGRAM

Packet service life (maximum number of routers crossed to reach the target). The default value is the value used by the PTx cards. Possible values are between 1 and 255.

WAITING PERIOD (MS)

"*Pinged*" equipment response timeout. The default value is 1 second. Possible values are between 100 and 65500 ms.

After entering the parameters, click "Confirmation" to start the request.

The results of the ping request are presented in form of a table of all the basic requests sent by the system, and a statistical summary.

The table indicates for each basic request sent by the system:

- The IP address of the target equipment
- The size in bytes of the IP packet sent
- The transmission and reception time in milliseconds (if the response time is very short, the IP card cannot know it with precision; it is then indicated by an upper base station)
- The return TTL (generally , the target sets the TTL value to 255 before returning the IP packet; the number received is therefore 255 less than the number of routers passed through on the way back)

Note: The character "*" shows that the target equipment's response was not received within the WAITING PERIOD.

The statistical summary indicates:

- The IP address of the source equipment (iPBX) and the IP address of the target equipment
- The number of packets sent, received and lost for all the basic requests
- The minimum, maximum and average packet transmission time.

Note: The time indicators only take into account the packets received within a period known to the system.

4.6.1.1.6 Integrated debug

Menu **SYSTEM>Expert>Processor access>Debug tools>Integrated debug**

This menu is used to manage the light debugger integrated into the iPBX, by proposing to:

- Create or delete a breakpoint
- Activate or deactivate a breakpoint
- Create a breakpoint for a limited number of times
- List breakpoints and their status
- View a disassembled code

This menu is used to configure at most 16 breakpoints.

For a breakpoint, the possibilities for configuring the action to take on arriving on this breakpoint are:

- Displaying registers
- Displaying call stacks (the depth is configurable)
- Displaying the content of the stack (the depth is configurable)
- Display the content of a memory area (in bytes, word, dword, ASCII, byte+ASCII)

Note: The iPBX's integrated debugger does not work simultaneously with GDB.

This screen is used to:

- View all the set breakpoints, as well as the processing operations to be performed upon arriving on these breakpoints.
- Select a breakpoint (by clicking the link available in the first column) to edit its characteristics.

No. (**breakpoint number**)**:** Value between 1 and 16. Represents a breakpoint,

Address: hexadecimal value (format : 0x12345678), representing the breakpoint address; this field is empty if no breakpoint is configured.

The following columns are not filled in unless the breakpoint address exists.

Status: field representing the status of the breakpoint (active or inactive)

Iteration: displaying the number of iterations made (5 characters) compared to the number of requested iterations (5 characters completed by some '0s'). If the number of requested iterations is indefinite, the 5 characters are replaced by the character '–'. *Example: 00002/00010 means that 2 iterations have been made out of 10 iteration requests, 5/----- means that 5 iterations have been made.*

Memory: if the display of a memory area is configured on arriving on this breakpoint, @MEM/Tlll type information is displayed. With:

- @MEM: memory address in 0x12345678 format, or name of a register
- T: export type: B (byte or byte + ASCII), W (Word), D (Double Word), A (ASCII)
- lll: length to be displayed in decimal (de 000 to 999)

Stack: displaying the digit corresponding to the depth of the stack to be displayed on arriving on this breakpoint (between 1 and 999). The character '*' is displayed if the display of the entire stack is requested. If this parameter is not configured, a 'space' character is displayed.

Registers: the character '*' is displayed if register display is configured on arriving on this breakpoint.

Calls stack: displaying the digit corresponding to the depth of the call stack to be displayed on arriving on this breakpoint (between 1 and 20). If this parameter is not configured, a 'space' character is displayed.

DEFINING A BREAKPOINT

Selecting an item in the selection menu gives access to the configuration of this breakpoint in the terminal input menu.

This menu presents the following lines:

Code address: Field with 8 upper-case characters; the authorised characters are [0 .. 9] and [A .. F]. This field is used to enter the address at which the breakpoint will be placed.

The address is entered and displayed in hexidecimal format, but the characters 0x are neither displayed nor authorised for input. The address cannot be entered if a debug script is being executed because these two debug methods are exclusive. It is not possible to enter two breakpoints with the same code address. It is automatically activated during breakpoint creation.

The following lines are only displayed if a code address is entered.

Assembler: a set of 6 lines which present the assembler code from the address entered. This is used to check that the breakpoint is correctly placed compared to the listing.

Active: shows whether the breakpoint is active or inactive. This field is a checkbox for web terminals.

Number of iterations: This field presents in brackets the current number of iterations obtained. The input field is used to specify the number of required iterations.

When the number is reached, the breakpoint is deactivated. If this number is not entered (default value) this means that the number of iterations is indefinite. The values authorised for this field are between 1 and 65500.

Number of steps: This field is used to specify the number of instructions to be executed in step-by-step mode after reaching this breakpoint.

The values authorised for this field are between 1 and 10. Leaving this field empty (default value) means that no step-by-step mode will be used.

The lines which follow 'traced elements' are optional and are used to configure the display of particular items upon arriving at the breakpoint.

Registers: indicates whether register output is requested upon arriving on this breakpoint. This field is a checkbox for web terminals.

Stack: indicates whether stack output is requested upon arriving on this breakpoint. This field is a checkbox for terminals.

- Depth: this line is only displayed if the stack is required. The input field is used to specify the stack depth to display. If this number is not entered, this means that the entire stack will be displayed (default value). The values authorised for this field are between 1 and 999.

Calls stack: indicates whether call stack output is requested upon arriving on this breakpoint. This field is a checkbox for web terminals.

- Depth: this line is only displayed if the call stack is required. The input field is used to specify the number of calling functions to display. The values authorised for this field are between 1 and 20 (default value).

Memory: indicates whether output from part of the memory is requested upon arriving on this breakpoint. This field is a checkbox for web terminals.

- Address: Field with 8 upper-case characters; the authorised characters are [0 .. 9] and [A ..Z]. This field is used to enter the name of a register, or a memory address. The address is entered and displayed in hexidecimal format, but the characters 0x are neither displayed nor authorised for input. The authorised registers are EAX, EBX, ECX, EDX, ESI, EDI, DS, ES, SS, FS and GS. If a register is entered, the memory will be displayed at the address contained in the register. This line is only displayed if memory display is required.

- Type: This line is only displayed if memory display is required. The input field is a list with the following choices: byte, word, double word, ascii, byte + ascii. This indicates the memory display format.

- Length: This line is only displayed if memory display is required. The input field is used to specify the number of items to display. The values authorised for this field are between 1 (default value) and 999.

All the values entered in this menu are stored in the MMC variables and will be written in the file dbg.conf when exiting this menu or while changing from the next or previous breakpoint. After reading the file, the debug ML is alerted to the fact that it must update its breakpoint configuration by rereading the file thanks to dbgi_set_config interface procedure.

4.6.1.1.6.1 Managing the file dbg.conf

Access to the file **dbg.conf**, which contains the breakpoint configuration, is via the interface procedures offered by the Keyfile ML.

The names of the keys and sections used are described in the common file dbg_litteraux.h available under COM_SAFE.

The MMC handles only the break points associated with the CMSTART process. Moreover, only breakpoints 1 to 16 are analysed.

Each time a key or section is written, the MMC adds a comment line indicating the modification date for this key or section.

During the break point writing phase, all the keys of the associated section are deleted and only the keys required to describe this new breakpoint are created.

Example of the content of a file dbg.conf:

```
[break 1]
# Key modified on 02/11/2009 at 09:11:29
Process = CMSTART
# Key modified on 02/11/2009 at 09:11:29
Address = 0x46001500
# Key modified on 02/11/2009 at 09:11:29
State = 1
# Key modified on 02/11/2009 at 09:11:29
Passcounts = 6000
# Key modified on 02/11/2009 at 09:11:29
Dump = reg, stack, bt, mem
# Key modified on 02/11/2009 at 09:11:29
Stack Size =
# Key modified on 02/11/2009 at 09:11:29
Backtrace = 20
# Key modified on 02/11/2009 at 09:11:29
Memory address = eax
# Key modified on 02/11/2009 at 09:11:29
Memory type = byte
# Key modified on 02/11/2009 at 09:11:29
Memory size = 0x64
```

4.6.1.1.7 Debug script

Menu **SYSTEM>Expert>Processor access>Debug tools>Debug scripts**

This command is used to activate/deactivate a debug script when required by Technical Support which will provide, if necessary, the right debug script as well as the instructions to start the script, stop the script and export the generated traces.

SCRIPT FILE

Name of the file to download. Use the **Browse…** and **Download** buttons to download the script provided.

SCRIPT OF

Information field indicating the date and time of the current file containing the debug script.

A check is made when Debug is started. The script will not be executed if a breakpoint exists in the file **dbg.conf**.

Follow the instructions from Technical Support to start/stop debug mode.

4.6.1.2 *Processor load measurement*

Menu **SYSTEM>Expert>Processor access>Processor load measurement**

SAMPLE DURATION IN SECOND

Time during which the measurement must be taken (maximum (120 s).

After entering the parameters, click "Confirmation” to start the measurement.

The result is displayed at the end of the end of the measurement period:

- The processor load of the selected card is expressed in percentage (*100) of free time during the measurement period.
- The free time is the average value of the processor’s free time during the measurement period.
- The minimum free time is the lowest value of the processor’s free time observed during the measurement period.

Note: The value MINIMUM FREE TIME is only available for real PTX cards.

4.6.1.3 *Format of PAS files*

Menu **SYSTEM>Expert>Processor access>Format of pas files**

PAS files are data files which describe the installation configuration.

For a given PAS file, this command is used to display the internal address, type of access and length of each of its table.

SELECTION OF DESCRIPTOR

PAS file identifier.

The drop-down list contains all the PAS file descriptors.

FROM TABLE

First table number (hexadecimal value) in the PAS file to take into account for display. If this field is not filled in, the start rank will be rank 0.

Select the criteria then click **Select the item**.

The PAS file name is displayed in the screen title.

The selected PAS file display table shows for each table with a rank above or equal to the selected “FROM TABLE” value:

- Its number
- Its location address in the memory
- Its type, if it is an access table
- The key type, if it is a table of access by key (nothing for simple key, "double" for double key)
- The number of sub-tables, in case of double index
- The number of items on the table
- The length of each item.

4.6.1.4 *Display of PAS files*

Menu **SYSTEM>Expert>Processor access> Display pas files**

This command is used to view the address and value of the items on a given table for a given PAS file.

SELECTION OF DESCRIPTOR

PAS file identifier.

The drop-down list contains all the PAS file descriptors.

AND OF THE TABLE

Number of the table to be displayed (hexadecimal value). If this field is not filled in, table 0 will be displayed.

START RANK

Rank of the first item to display. If this field is not filled in, the start rank will be rank 0.

END RANK

Rank of the last item to display. If this field is not filled in, the end rank will be the rank of the last item on the table.

Select the criteria then click **Select the item**.

The display screen presents information about the required table.

Note: To display the previous or next tables, use the << and >> buttons.

The PAS file name is given on the screen title, as well as that of the displayed table.

The selected PAS file display screen shows for the table displayed and its table index, if applicable:

- The internal address

- The table type, if it is an access table
- The key type
- The number of sub-tables
- The number of items
- The length of each item.

The display screen of the table displayed shows for each item with a rank between the values “START RANK” and “END RANK”:

- Its rank
- Its internal address
- Its value

For a key code table, the screen displays both the address and the value of the key code and the address and value of the structure associated with the key code.

Double index tables are presented in the same way as single index tables: the number indicated is the result of the multiplication of the 2 indexes.

For key code tables and tables with two indexes, the key code section of the table which is common to x elements in the sub-table is repeated for each element (customised abbreviated number, etc.).

4.6.2 TIMEOUT

Menu **SYSTEM>Expert>Timeout**

This command is used to display and change the different call and ringer timeouts and durations.

To access this command, click "Timeout” from the “Expert” menu.

The timeout management screen is organised into four timeout/duration groups:

- Time in seconds
- Time in 1/10 sec.
- Time in 1/100 sec.
- Time in minutes.

TIME IN SECONDS

DIALLING TIME-OUT

Timeout activated on off-hook without dialling. At the end of the timeout, the set receives a busy tone.

Default value: 22 seconds

TIME-OUT BEFORE PERM. OFF-HOOK COND.

Time-out activated after the DIALLING TIME-OUT, or on an attempted call to a busy set, after reception of the busy tone.

At the end of this time-out, the set goes to the forced release state (forced release corresponds to a request to on-hook).

Default value: 10 seconds

DELAYED HOT LINE TIME-OUT

Timeout activated on set off-hook by a subscriber for whom a DELAYED hot line is defined (see SUBSCRIBERS>Subscriptions>Characteristics>General characteristics).

End of timeout triggers transmission of the number associated with the delayed hot line.

Default value: 5 seconds

RECORDED CALL TIME-OUT

Timeout activated when the set goes off-hook. End of timeout triggers automatic transmission of a number that has been stored with the help of the feature STORED CALL (see DIALLING PLAN>User dialling plan>Access to features>By feature).

Default value: 5 seconds

TRANSFER TO PARK TIME-OUT

Timeout activated when a call is parked. If the call is not picked up before the end of the time-out, it is released (if it is an internal call) or rerouted to the operator (if it is an external call).

Default value: 120 seconds

INTERNAL CALL RINGING DURATION

Timeout activated on a call to a set internal to the system. Corresponds to the time during which the ringing signal is transmitted, before transition to the line lockout phase.

Default value: 40 seconds

DID CALL RINGING DURATION

Timeout activated on a DID call to a set with no reply The call is rerouted to the attendant at the end of the timeout.

Default value: 40 seconds

SPEC. TIMEOUT: REROUT. TO CONSOLE

Value of timeout before return to the ATDC.

AUTO CALLBACK TO CALLER RING. DURAT.

Time-out is activated on call-back to a busy terminal, and corresponds to the caller terminal ringing time.

Default value: 15 seconds

ANNOUNCEMENT DURATION BEFORE RINGING

Time-out activated on presentation of an external call to a set. It is used to connect an announcement message before the set rings (hospital configuration).

Default value: 8 seconds

RINGING DURATION BEFORE DELAYED FORWARD

The following four parameters are used to configure four different ringing durations before deferred forwarding. A ring tone can be assigned to a subscriber using the menu **SUBSCRIBERS>Subscriptions>Characteristics>General characteristics**.

- STANDARD RINGING

Default value: 15 seconds

- SPECIFIC RINGING NOS. 1 / 2 / 3

Default value: 15 seconds

MAXIMUM DURATION WITHOUT ROUTING (BIS):

Timeout for automatic PSTN routing during which the telephone translation server is not called.

The minimum and maximum timeouts are 5 and 120 seconds respectively. The timeout must be a multiple of 5 seconds.

Any value between 5 and 120 may be entered, but this value is automatically rounded off to the multiple (below or above) of 5 seconds.

The default value corresponds to a 120 seconds timeout by default.

RECOVERY HOLD COMMUNICATION ON ENQUIRY CALL FAILURE:

Timeout for resuming a call on hold upon enquiry call failure also applies in case of call diversion.

Timeout expressed in seconds.

No value: automatic resumption of a call on hold upon enquiry call failure, after 5 seconds (500), is reserved for terminals supervised by TAPI or CSTA; upon failure after an attempted call diversion, the failure screen is displayed without timeout.

Values between 5 and 600 seconds: automatic resumption of a call on hold when an enquiry call fails, after the timeout applicable to all terminals upon failure after an attempted call diversion, the failure screen is displayed and the configuration data contains the timeout value at the end of which the call is resumed.

CHARGING INDICATION DELAY

Timeout activated on transition to conversation mode. At the end of this timeout the user receives a series of beep signals so he can hang up if the parameter CHARGE INDICATION is set to YES in the routing characteristics concerned.

TIME IN TENTHS OF A SECOND

INTERNAL CALL RING. DURATION ON

Duration of a full internal call ringing cycle. Associated with the following time-out, this particular time-out is used to calibrate the ringing tone of a set called by an internal extension.

Default value: 2.5 seconds

INTERNAL CALL RING. DURATION OFF

Duration of the internal call ringing cycle timer off. Associated with the previous timeout, this particular timeout is used to calibrate the ringing tone of a set called by an internal extension.

Default value: 2.5 seconds

EXTERNAL CALL RING. DURATION ON

Duration of a full external call ringing cycle. Associated with the following two timeouts, this particular timeout is used to calibrate the ringing tone of a set called by an external extension.

Default value: 1.5 seconds

OUTGOING RINGING DURATION OFF 1

Duration of the first external call ringing cycle timer off. Associated with the next and previous timeout, this particular timeout is used to calibrate the ringing tone of a set called by an external extension.

Default value: 3.5 seconds

OUTGOING RINGING DURATION OFF 2

Duration of the second external call ringing cycle timer off. Associated with the previous two timeouts, this particular timeout is used to calibrate the ringing tone of a set called by an external extension.

Default value: 3.5 seconds

CALL WAITING BEEP DELAY

Length of the beep signal for a waiting call.

Default value: 0.3 seconds

DELAY BETWEEN CALL WAITING BEEPS

Timeout between 2 "CALL WAITING" beeps.

Default value: 20 seconds

TIME IN HUNDREDTHS OF A SECOND

ROTARY DIAL SET FLASH TIMER

Duration from which a line opening may be interpreted as a FLASH on a rotary dial set.

Default value: 180ms

DTMF SET FLASH TIMER

Duration from which a line opening may be interpreted as a FLASH on a DTMF set.

Default value: 180ms

DIGIT PULSE DELAY (MAX)

This corresponds to the length of a digit pulse for a rotary dial set.

Default value: 80ms

Maximum value: 100ms

ROTARY DIAL SET ON-HOOK ACKNOWLEDGE

The minimum on-hooking time for a rotary dial set.

Default value: 400ms

DTMF SET ON-HOOK ACKNOWLEDGE

Minimum on-hooking time for a DTMF set

Default value: 400ms

TIME IN MINUTES

TRUNK AUDIT FREQUENCY

Trunk audit frequency. The system therefore tests the lines at regular intervals: if the line is not connected to an internal terminal or to another line, the system releases it.

Default value: 30 minutes

LONG CALL RECORD

The length of the call which leads to the transmission of a long call record.

HOLD OF NETWORK COMMUNIC. IF FAULT

Depending on the value of the **AUTOMATIC RELEASE OF TRUNK** field (see below) and if terminal type is TDM, some beeps will be sent at the end of call holding.

Line displayed for multi-site configuration only.

Default value = 60: network calls are held for 1 hour. **Value 0**: network calls are not held.

Other values: timeout value for call on hold.

Timeout expressed in minutes based on 5 minutes in the table. The values entered are rounded off to a tenth below for any value of the units between 1 and 4. Possible values are between 5 and 1440 minutes (24 hours).

MAXIMUM DURATION OF CONFERENCES

Wait timeout before conference circuits are released

Default value = 60, which corresponds to one hour wait time before the conference circuit is released.

Other values: Timeout expressed in minutes based on 10 minutes in the table. The values entered are rounded off to a tenth below for any value of the units between 1 and 4, and to a tenth above for any unit value between 5 and 9. Possible values are between 10 and 720 minutes (12 hours).

AUTOMATIC RELEASE OF TRUNKS

Box ticked: the trunks are automatically released on the trunk groups for which the anti-gossip function is activated. Two configurations are associated with this release (interruption):

For the application of this function to trunk groups, see the field **FORCED TRUNK RELEASE** in the menu **Telephony service>Network and links>Network>Trunk groups** – **Characteristics** tab.

⚠ **WARNING: Automatic release does not apply to calls made from priority terminals (subscription characteristics).**

Box not ticked: no automatic trunk release

Lines appear if this box is ticked:

DURATION BEFORE WARNING (MIN)

Wait time before warning about trunk release

Timeout based on n x 5 minutes.

This timeout corresponds to the timeout between audits and not the timeout before release.

- Default value: 60 minutes
- Minimum value: 5 minutes*
- Maximum value: about 18 hours

WARINING BEFORE CUTTING (SEC)

Associated with the previous field, this allows the definition of the warning timeout transmitted to users before the trunk is released (before cutting). This timeout is based on 1 second.

WARNING: Beeps are made for TDM terminals only. If the terminal is an IP terminal, there is no beep even if the trunk is released.

- Default value: 120 seconds
- Minimum value: 10 seconds (transmission of a sequence of 3 beeps)
- Maximum value: 300 seconds (5 minutes)

4.6.3 DCF PARAMETERS

Menu **SYSTEM>Expert>DCF settings**

DCF settings are configuration data settings.

WARNING: DCF settings may only be modified under the control of Technical Support.

This command is used to modify the system configuration data.

NUMBER (IN DECIMAL) OF THE DCF

Index of the configuration data to be modified.

Enter the value then click **Select the item**:

VALUE IN DECIMAL

Current value in decimal of the configuration data.

VALUE IN HEXADECIMAL

Current hexadecimal value of the configuration data.

Note: The value may either be changed in decimal or in hexadecimal.

4.6.4 DCF DIVERGENCE / INIT. VALUES

Menu **SYSTEM>Expert>DCF divergence/init. values**

This command is used to display the configuration data that has been modified compared to the initial data.

The display table indicates for each modified configuration parameter:

- Its number
- Its initial value in decimal and hexadecimal ()
- Its current value in decimal and hexadecimal ()

4.6.5 SETS NAMES

Menu **SYSTEM>Expert> Sets names**

Mitel terminals are identified by the range to which they belong, a reference and a name.

This command is used to manage the list of Mitel proprietary terminals. The actions available are:

- creation of a new reference in a range,
- renaming of an existing reference,
- deletion of a reference.

RANGE

Range name: **M4/5/6/7xx - 53xx – 53xxIP – 6xxxi – APPLICATION SIP – BluStar – BluStar PC – BluStar Mobile – DECT SIP – MiCOLAB CLIENT – SIP /EX/GX/TA**

REFERENCE (HEXA)

Reference of the Mitel terminal in hexadecimal.

OR REFERENCE (DECIMAL)

Reference of the Mitel terminal in decimal.

To create a new terminal reference, select the range to which it belongs and the reference to create, then click **Select the item**

To modify or delete a terminal reference, select the range to which it belongs and its reference, then click **Select the item**

NAME TO BE ASSIGNED

Character string (20 maximum).

If the selected reference exists, this field contains the name of the set, otherwise it is empty.

ACTION

MODIFY	Modifies the name of a listed Mitel terminal.
CREATE	Adds a new Mitel terminal reference.
DELETE	Deletes a Mitel terminal reference.
………….	No action.

4.6.6 SETS NAMES LISTING

Menu **SYSTEM>Expert> Sets names listing**

This command lists all types of Mitel terminals.

4.6.7 TERMINALS MANAGEMENT DATA

Menu **SYSTEM>Expert>Terminals Management Data**

This menu has three tabs for viewing the terminal version and data index information.

- Production version data,
- Test version data,
- Terminal download server data.

For production and test data, the **Global index** column is used to compare the values with those in Menu **Terminals management**. In case of inconsistencies, restart the actions in the **Terminals management** menu.

4.7 GATEWAYS CONFIGURATION

This menu is meant in the MiVoice 500 solution for the installation and configuration of EX Controller and GX Gateway.

Refer to the document **Mitel EX Controller, GX Gateway, Mitel AG4100 and TA7100 – Installation and Configuration**.

4.8 CONFIGURE OPERATING MODE

This menu is used to configure the iPbx operation mode for a multi-site environment.

The operator has two options:

STANDALONE

Standalone mode is the default configuration which allows the iPbx to work independently or to be included in a multi-site system.

NODE

Node mode should only be chosen under the responsibility of the technical support.

In this mode, the iPbx is part of a large network which can be extended to 2000 iPbxs.

5 NUMBERING PLAN

This management domain is used to define:

- The directions
- The user dialling plan (translation, by the system, of a number dialled by a user and routing to the right direction)
- The dialling plan for incoming lines (translation, by the system, of an incoming call and routing to the right direction in case of transit)
- The list of forbidden numbers, for barring access to a certain number blocks according to subscribers
- abbreviated numbers, for access to emergency services (special abbreviated numbers)
- The number translations that allow calls to be rerouted, either systematically (if a subscriber moves to another site, for instance), or upon inaccessibility (for a “vital” subscriber, for instance, who must be reachable at any time), or even according to caller number (rerouting a call to a call distribution service according to geographic origin, for example).

A default dialling plan is provided when the iPBX is installed. It may be modified or recreated after a reset. This latter operation must be used with precaution and requires special rights (password required).

Menu **DIALLING PLAN**

5.1 DIRECTION NAMES

Menu **DIALLING PLAN>Direction names**

This command is used to define the different call routing directions.

Each direction is given a name (8 characters): a direction without a name cannot be managed because it does not exist.

The system can manage up to 64 private directions.

Default directions are pre-defined during installation. Some of them cannot be modified because they are used by the dialling plan provided by default. To modify them, you must first delete all their references in the dialling plan.

• PSTN incoming:	NETWORK
• Local outgoing /81h:	NATIONAL
• Regional 5 outgoing /89h:	REGIONAL
• International outgoing /83h:	INTER.
• Emergency calls /8bh:	EMERGENCY

The other fields are used to create additional directions.

A paging access is considered as a direction which must have a trunk group and a route assigned to it.

There are two types of paging:

- Direct: calling a person's beeper by dialling a prefix, followed by the beeper number
- Automatic: automatic paging is activated when a set with paging rights and forwarded to its own number is called.
- If it is an internal call, the caller number is forwarded to the beeper. The holder of the beeper calls this number from any set in the system. This type of search is also called "without meeting".
- For an external call, the caller line is parked, and the holder of the beeper carries out the parked call recovery request. This type of search is also called "with meeting".

Depending on the device, different dialling plans must be translated out according to the type of call.

AUTO DIRECT PAGING

Direction name.

Note: An access prefix must be defined for direct paging (see DIALLING PLAN>User dialling plan>Access to directions).

AUTO PAGING INTERNAL CALLS

Direction name.

AUTO AUTO PAGING EXTERNAL CALLS

Direction name.

CONSULTATION CALL OVER TRUNK

This indicates the direction name without a route. Its prefix is assimilated to a direction prefix which is used to define various number lengths.

For the definition of external consultation call parameters, see command: NETWORK AND LINKS>Network>Translators>Operations behind PBX.

PACKET CIRCUIT COUPLER

Direction to declare if a special action is required on outgoing AID management (NETWORK AND LINKS>Network >AID handling> Outgoing handling).

OPERATORS

Direction to declare if a special action is required on outgoing AID management (NETWORK AND LINKS>Network >AID handling> Outgoing handling).

SIGNIFICANT DIAL NUMBERS

Direction to declare if a special action is required on outgoing AID management (NETWORK AND LINKS>Network >AID handling> Outgoing handling).

VOICE MAIL

Direction to declare if a special action is required on outgoing AID management (NETWORK AND LINKS>Network >AID handling> Outgoing handling).

5.2 USER DIALLING PLAN

Menu **DIALLING PLAN>User dialling plan**

The user dialling plan indicates the analysis made by the system concerning a number dialled by a particular user. It describes:

- Access to internal numbers
- Access to features
- Access to public exchange
- Access to directions (public and private)
- Access to operations during a call (definition of suffixes).

When the system is installed, a default plan is provided, which depends on the country’s dialling plan.

This menu is used to modify the user dialling plan.

Note: The values displayed in the screens in this section are shown as examples.

5.2.1 ACCESS TO EXTENSIONS

Menu **DIALLING PLAN>User dialling plan>Access to extensions**

This command is used to define internal number blocks.

NUMBER OF DIGITS

In standard configuration, an internal number has three digits, from 200 to 799 (note: 798 is the common bell number and 799 is the modem number).

Consecutive directory numbers are assigned automatically to the existing sets on initial start-up (TOTAL RESET). The internal number length and the number block to create during installation are parameters of the file INSTALL.CONF.

Possible values: 3 to 6.

Note: To change the internal number length, you must first delete the number blocks.

NUMBER OF DIGITS TO DELETE

The number of digits not included in a directory number seen by the extension MMC. This line is to be filled in for an internal dialling plan more than 6 digits long.

RANGE 1

This line contains ranges 2, 3, 4, 5, 6, and 7, corresponding to internal numbers in the default plan provided.

A block is defined by the first digits in the number. A range is a set blocks.

Example: RANGE 1, enter 2-7 on this line for the six blocks.

As a standard, and according to number length, enter:

- 2 for (20 to 29) or (200 to 299),
- 3 for (30 to 39) or (300 to 399),
- 4 for (40 to 49) or (400 to 499),
- 5 for (50 to 59) or (500 to 599),
- 6 for (60 to 69) or (600 to 699),
- 7 for (70 to 79) or (700 to 799.

You can enter other numbers, for example, 32 for 320 to 329.

RANGE 2 TO 46

These lines are used to increase the number of internal dialling plan ranges.

Note: If the internal directory numbers are changed, all the numbers must be of the same length, including:
• subscribers,
• additional directories,
• operators,
• common bells (including internal relay),
• hunt groups,
• remote maintenance modem.
To change the numbering length, you must follow up the operation with an AUTO RESET.

5.2.2 ACCESS TO FEATURES

Menu **DIALLING PLAN>User dialling plan>Access to features**

This menu is used to display and modify the features access codes.

The characters authorised for feature access codes are:

0, 1, 2, 3, 4, 3, 6, 7, 8, 9, *, #.

Note: The features directory can be fully modified.

Access to features can be displayed and/or modified in three ways:

- Displaying all the features (by feature)
- Displaying a given feature (by prefix)
- Displaying the short number feature.

5.2.2.1 *By feature*

Menu **DIALLING PLAN>User dialling plan>Access to features>By features**

This command is used to:

- Display all the features on the same screen
- Modify the access codes

PACKET CIRCUIT COUPLER CALL

Packet circuit coupler internal directory number. This number must be consistent with the internal dialling plan.

CANCEL FORW. FROM FORWARDED SET

Deactivates assistant-manager type forwarding.

To activate this feature, use the "ASSISTANT-MANAG. FORWARD (ACTIVATE)" feature.

CALL WAITING (VIEW)

This code is used for putting a call on hold. The equivalent code features in the suffix plan for consultation calls. You are advised to make these two codes identical.

RECORDED CALL (RECORD) / (DELETE) / (USE)

Registering: for recording an incoming call number so it can be used later.

Delete: for deleting the recorded number.

Use: for dialling the recorded number.

BROADCAST CALL LIST 0/1/2

Possibility to call a group of digital or 6xxxi phones using the loudspeaker. The call is broadcast on all free digital terminals, including those on the corresponding announcement list (announcement lists are defined in **SUBSCRIBERS> Hunt groups and companies> Announcement list**).

EXTENSION BROADCAST CALL

Call recorded on a digital or 6xxxi phone with activation of its loudspeaker (direct switchover to conversation).

NUISANCE CALL

A message is recorded in the logbook.

SINGLE VOICE MAIL CALL

Enables a user to directly access his own voicemail box, or the voicemail system.

VOICE MAIL CALL

Call to a voicemail box in answering mode

OPERATOR CALL

Operator extension number.

PAGING SERVICE CALL WITHOUT ANSWER

A pager is used to alert a user with a beeper that somebody has tried to reach him. In this mode, the user leaves a message on his correspondent’s receiver.

PAGING SERVICE PAGING SERVICE CALL WITH ANSWER

A pager is used to alert a user with a beeper that somebody has tried to reach him. In this mode, a call will be set up between the user and his correspondent.

CHOICE FOR CTI TERMINAL (ACTIVATION)

This feature is used to choose the sound terminal (by feature code) for a CTI terminal in an association.

The choice applies to all the subscription lines.

In previous releases, it was the last communicating sound terminal that was automatically chosen, or the wired terminal of the association.

The two fields proposed are used to enter (create and modify) activation prefixes and cancel the feature.

The feature codes for this feature are:

- *09 for activation
- #09 for deactivation

OVERRIDE ALL FORWARDS

Possibility to reach a forwarded or filtered terminal directly.

VOICE ANNOUNCEMENT (ACTIVATE) / (DEACTIVATE)

Enables the user to activate/deactivate the voice prompt for his account.

CALL PICK-UP IN A HUNT GROUP

Enables a set to pick up a call ringing on another set that is part of the same hunt group.

CALL PICKUP GENERAL

Enables a set to pick up a call ringing on another set that is part on the installation.

CALL PICKUP COMMON BELL

Enables a user to pick up a call presented to a common bell system.

MESSAGE LAMP (ON) / (OFF) / (INTERNAL OFF)

For activating/deactivating an indicator lamp on a set (hotel room type) from another set (hotel reception type) to indicate that messages have been left (on/off).

The "internal off" feature enables the set user (hotel room) to switch off the LED.

CONSULT MAIL BOX DIRECTLY

Allows users to consult their mailbox directly.

LOGIN (ACTIVATE) / (DEACTIVATE)

Feature offered to all users declared on digital or IP sets, enabling them to move to another set and find their rights and features. Any multi-site subscriber with a subscription associated to a digital or IP set may log on/off with any other digital or IP set on the multi-site configuration.

DIRECT ACCESS MESSAGES

Enables a user to listen to spoken announcements.

MESSAGE NO 0 SHORT CALL

Enables a user to listen to message 0 with direct access.

SET LISTENING

Allows a set to listen to another set without being heard. This feature is activated for the set to be listened to. This function is enabled once an authorised set calls the set being listened to.

PASSWORD MODIFICATION

Enables a user to order from his set the modification of his secret code (used for login, set unlocking, etc.).

DO NOT DISTURB (ACTIVATE) / (DEACTIVATE)

A user who does not want temporarily to be disturbed by the telephone ringer and, thus, does not want to receive calls can activate/deactivate the “Do not disturb” function. Within the period when this feature is activated, internal callers receive a busy signal and external callers are routed to an operator.

DIRECTORY NUMBER (CHECK)

Used to check a set’s directory number.

REDIAL (USE) / (DELETE)

Enables a set to redial on demand the last internal or external number dialled.

SPECIAL NUMBERS (LIST 0,…LIST9)

Used to associate an access code with each of the special numbers lists. If a code is associated with a list, the numbers on that list will be accessible via the access code, followed by the abbreviated number defined in the menu “DIALLING PLAN> Special numbers”.

COMMON ABBREVIATED DIALLING

For accessing the common abbreviated numbers defined in the directory records.

Depending on the value of the setting **NUMEROUS PREFIXES**, in Menu **SUBSCRIBERS> Rights>General settings**, you can either define a single prefix or one prefix per range. In this case, the last digit of the prefix must be that of the block.

COMMON ABBREV. PERSONAL ABBREV. NUMBER (RECORD) / (DELETE) / (USE)

Enables users to manage (save a number, delete a number) and use a list of 10 personal abbreviated numbers.

OVERRIDE NECESSARY

Used to ring the set even if it is forwarded.

PARKING

For putting an internal or external call on hold, with a view to resuming it later from any other set on the installation.

PARKING (RESUME) / TAKE

For resuming a parked call.

EXTERNAL TERMINAL (ACTIVATION/DEACTIVATION)

Code used to activate or deactivate call reception on external terminals.

DYNAMIC PROTECTION (ACTIVATE)

The user can protect the ongoing call or the next outgoing call against any third-party entry or on-hold operation.

The protection is automatically deactivated at the end of the protected call.

AUTOMATIC CALLBACK (ACTIVATE) / (DEACTIVATE)

For activating/deactivating the automatic callback of a subscriber found busy.

FORWARDING (CANCEL ALL)

Cancelling all forwarding operations.

ASSISTANT-MANAG. FORWARD (ACTIVATE)

Enables a user with the "secretary" function to activate forwarding of calls meant for another terminal ("director") to his own terminal.

To deactivate this feature, use the feature "CANCEL FORW. FROM FORWARDED SET".

FORWARD ON NO ANSWER (ACTIVATE) / (DEACTIVATE)

Re-routing all calls to the forwarding set on no answer.

FORWARD ON BUSY (ACTIVATE) / (DEACTIVATE)

Re-routing all calls to the forwarding set on set busy. Forwarding can only concern external calls:

- FOR EXTERNAL CALLS (ACTIVATE)

Re-routing external calls to the forwarding set on set busy.

PREDEFINED FORWARD (ACTIVATE) / (DEACTIVATE)

Forwarding for which the addressee is programmed by the operator.

Predefined forwarding can be defined for all calls, for internal calls only or for external calls only, using three different access codes. The same deactivation code is used for the three types of predefined forwarding.

- FOR INTERNAL CALLS (ACTIVATE)

Re-routing internal calls to the forwarding addressee.

- FOR EXTERNAL CALLS (ACTIVATE)

Re-routing external calls to the forwarding addressee.

- OF HUNT GROUP (ACTIVATE) / (DEACTIVATE)

Re-routing calls meant for a hunt group to the forwarding addressee.

IMMEDIATE FORWARD (ACTIVATE) / (DEACTIVATE)

Re-routing calls systematically to the forward set. Forwarding can be carried out for all calls or by call origin.

- FOR INTERNAL CALLS (ACTIVATE) / (DEACTIVATE)

Re-routing internal calls systematically to the forward set.

- FOR EXTERNAL CALLS (ACTIVATE) / (DEACTIVATE)

Re-routing external calls systematically to the forward set.

FORWARDING TO VOICE MAIL

Forwarding calls to voicemail.

- IMMEDIATE

Forwarding calls immediately to voicemail.

- DEFERRED

Forwarding calls to voicemail on no answer.

- ON BUSY

Forwarding calls to voicemail when the set is busy.

SIGN OFF HUNT GROUP

Enables a user belonging to a hunt group to leave the hunt group.

SIGN ON HUNT GROUP

Enables a user to return to the hunt group to which he belongs.

GO BACK TO CALLING PARTY

Enables a set to return an exterior call to the user that had transferred the external call to it.

AGENDA (ACTIVATE) / (DEACTIVATE)

Possibility offered to a user to ring his set at a programmed time (feature code + HHMM). Up to 4 requests can thus be stored per set.

Possibility to wake up a room set. Only one request can be stored at a time per set.

The programming can be cancelled selectively or globally:

- Selective cancellation: (feature code + HHMM) Hotel room or Meeting call type.
- Global cancellation: (feature code + 9999) Hotel room or Meeting call type.

SUBSTITUTION

This feature enables a user to find on any set on the installation certain rights of his set (access to the public switched network, forwarding and agenda programming, personal abbreviated numbers).

MANUAL TEST OF JUNCTORS

Not initialised. Only fill in if necessary.

WORK IN HUNT GROUP (START) / (END)

Used during work start or end to issue a service record in the “Call distribution” family, and a CSTA event.

The user dials the activation code, followed by the CSTA ID. The length of this identifier can be configured in the menu “SUBSCRIBERS>Hunt groups and companies>Hunt groups>Settings”.

LOCK (ACTIVATE) / (DEACTIVATE)

Enables a user to lock (and unlock) his set's access to the public switched network.

Certain set categories can be locked permanently (they cannot unlock themselves).

5.2.2.2 *By prefix*

Menu **DIALLING PLAN>User dialling plan>Access to features>By prefix**

This command is used to view and modify a specific feature. It is also used to configure certain special emergency type numbers, such as 15, 17 and 18 in France, which must initiate the call without waiting for additional digits.

Enter the feature access prefix then press “Enter” to confirm.

The screen is used to modify an existing feature, or to create a new feature using an access code not yet used.

ACCESS CODE

Characters allowed: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,'*', '#'.

This field is used to enter the access code for the feature requested.

RUNNING PROGRAM

This second line, not modifiable by the operator, shows the current definition of the prefix in the description tables.

DESIRED PROGRAMMING

Note: These field are only displayed if the feature code is modifiable.

FEAT.

The drop-down list contains all the feature labels.

Select the feature you want.

To configure an emergency special number, select a SPECIAL NUMBERS LIST X list.

TYPE

RUN	CANCEL	USE	DISPLAY

One or more of these values are available in the drop-down list, depending on the selected feature.

Select the type you want.

To configure an emergency special number, select the UTILISATION type.

STANDARDS VALUES MODIFYING

NO **YES**

Select YES to configure an emergency special number.

If you enter YES, the following 2 lines appear.

LAST DIGIT PRESERVED

NO **YES**

Select YES to configure an emergency special number.

SIGNATURE

NO **YES**

Password request. Only used for certain specific features.

ACTION

Type of action to take. The content of the drop-down list depends on access code context. Possible values are:

……..	Displays the selected value.
MODIFY	Modifies the feature selected (by access code) according to the parameters entered.
DELETE	Deletes the feature selected (by access code).
CREATE	Creates a new feature for an unused access code.

Note: When one of the two standards values lines is modified, the prefix in the previous list (By feature) is deleted.

Example: *Create 3 special prefix numbers (emergency) 10, 11 and 12 (to release 13 .... 19) and retain the last digit. When you dial 10, the number stored as 0 in list 0 is dialled.*

5.2.2.3 *Speed dialling*

Menu **DIALLING PLAN>User dialling plan>Access to features>Speed dialling**

This number translation feature enables the user to access a long number by dialling a shorter number. (32 number ranges can be programmed in this way).

It applies to an internal dialling plan with more than 6 digits.

If programmed by the operator, this feature is available for all users.

DIGIT TO TRANSLATE

Enter the format for the short numbers to be dialled by the users in n(lg) format, where:

- n is the 1 or 2-digit number

- lg is the total length of the short number.

Validating with the "Enter" key refreshes the screen and displays the speed dialling definition parameters.

NUMBER OF DIGITS TO DELETE

Number of digits to be deleted: 1 to 9.

DIGITS TO ADD

Sequence of digits to add.

COMPLETED BY CALLER

NO **YES**

If you select YES, the number is completed by the caller’s number so rerouting can be managed according to call origin.

Example of speed dial programming:

Digit to translate	7(5)
Number of digits to delete 1	
Digits to add	821761
Completed by caller	NO

The user dials 7MCDU: 7 is deleted and 821761 is added. The number 7MCDU is therefore analysed as 821761MCDU, regardless of the calling party directory number.

5.2.3 ACCESS TO PUBLIC EXCHANGE

Menu **DIALLING PLAN>User dialling plan>Access to public exchange**

This screen differentiates business calls from private calls, for purposes of charging and access restrictions.

Note: Before programming the access codes for the public exchange (for example: 00 for business calls and 01 for personal calls), you must first delete the access codes (directions: NATIONAL, INTERNAT, REGIONAL), the private numbers and the business call codes, then program the codes and the private numbers: this does not apply if you keep the 0 for business calls and the 8 (or 80) for example for personal calls.

BUSINESS CALLS

Access code for external business calls.

The default access code for external calls is 0, but may be 0 to 99.

PERSONAL CALLS

Access code for external personal calls (0 to 99).

The set must feature a personal access code (SECRET CODE).

Personal calls are not subject to charging according to category. They can be forbidden according to lists of forbidden numbers.

DEFAULT DIRECTION

NATIONAL **INTER.** **REGIONAL**

The default direction is selected by the iPBX when no direction prefix (or specific direction number) is detected in the number which follows the public exchange access code.

DEFAULT LENGTH

Number of digits by default.

FIRST DIGIT OF URGENT NUMBERS

This field is used to define the first digit of the PSTN emergency numbers (in France, this digit is 1 (15 for ambulance, 17 for police, etc.). These numbers must be accessible from a locked set that requires a password after dialling the network access code. It must be able to recognize whether the first digit dialled is the start of an emergency number, and if so, to bypass the password requirement.

This field is for a specific configuration allowing locked terminals to dial 0 + 1x. It is not advisable to use it because the constraint is that the password should not start with this prefix. It is advisable to use special numbers 1x, configured by default; see Section 5.6.1.

When the "**First digit of urgent numbers**" field is filled out, it is no longer possible to assign this 1st digit when a subscription password is modified; in this case, the error message "**Incorrect beginning**" is displayed.

See Menu **SUBSCRIBERS>Subscriptions /Characteristics>General characteristics**, Section 3.3.3.1

NO. OF USERS WITH PASSWORD TO CHANGE

Information field indicating the number of users whose first password digit is the same on the first emergency number digit.

NEW START OF THEIR PASSWORD

This field only appears if the parameter NO. OF USERS WITH PASSWORD TO CHANGE is not 0.

Note: To see the list of users concerned so as to inform them about the changes made to their password, click “Display the subscriptions to modify” BEFORE making the change. The list is displayed in form of a table:

Enter the first digit of the password for these users and click “Confirmation” to validate the modification.

5.2.4 ACCESS TO DIRECTIONS

Menu **DIALLING PLAN>User dialling plan>Access to directions**

This command is used to assign an access code and a number length to each outgoing direction declared in the system.

It is also used to assign specific numbers to a direction: number whose length is different from the dialling length for this direction.

BY ITS NAME

NATIONAL **REGIONAL** **INTER.** **TIE L00**

Select a direction from the drop-down list then click **Select the item**.

Note: If other directions have been created via Menu DIALLING PLAN >Direction names", they will appear on the drop-down list.

5.2.4.1 *Access to national*

Menu **DIALLING PLAN>User dialling plan>Access to directions**

NATIONAL access corresponds to the direction “Local outgoing /81h” whose name is NATIONAL on the direction display menu (command: DIALLING PLAN>Direction names").

DIRECTION DEFINED DOWNSTREAM OF

NETWORK **INTER.**

Used to define a tree structure for the dialling plan.

LENGTH OF NEXT NUMBER

Number of digits the iPBX waits to receive before transmitting the dialling signal on the network, and before switching to the conversation phase:

- A digit indicates a closed dialling plan
- An asterisk indicates an open dialling plan

SPECIFIC NUMBERS

Specific numbers are "NATIONAL" direction numbers whose length is different from the length defined above.

For each specific number block to define, enter on a line the beginning of the number, followed by the number of digits for this number in brackets.

Example 1: 07(*): all the numbers starting with 07 and which have an undefined length.

Example 2: 10(4): all numbers starting in 10 are considered as 4 digit numbers.

Example 3: 112 (3): the number 112.

Example 4: 310-1(4): all numbers starting with 310 and 311 are considered as 4 digit numbers.

Note: A zero in brackets means that the prefix is invalid.

There are 119 lines for defining specific numbers, (numbers which have a different length from the initial value so as to be accepted and transmitted to the public network without delay).

Note: In certain configurations (for USA, for example), it is possible to have 2 packets of 120 ranges. There is an extra line for selecting one of the two packets.

Codes * and # are authorised for specific numbers (for example, *21* (13).

Only the first digits of a specific number are definable: the number in brackets allows the system to connect to the network as soon as it receives the number of digits indicated.

5.2.4.2 *Access to REGIONAL*

Menu **DIALLING PLAN>User dialling plan>Access to directions**

REGIONAL access corresponds to the direction “Regional 5 outgoing /89h” whose name is REGIONAL in the direction display menu (command: DIALLING PLAN>Direction names").

This direction is used to access the regions and comprises only specific numbers.

DIRECTION DEFINED DOWNSTREAM OF

NETWORK **INTER.**

Used to define a tree structure for the dialling plan: the direction code must consist of the rest of the direction code defined upstream.

ACCESS CODE

Code which follows the direction code defined upstream. If this field is not completed, the code will be the same as that of the direction defined upstream.

SPECIFIC NUMBERS

For each specific number block to define, enter on a line the beginning of the number, followed by the number of digits for this number in brackets.

Example: 0590(10): all numbers starting in 0590 are considered as 10 digit numbers.

5.2.4.3 *ACCESS TO INTERnaT.*

Menu **DIALLING PLAN>User dialling plan>Access to directions**

INTERNATIONAL access corresponds to the direction “International outgoing /83h” whose name is INTER. in the direction display menu (menu: **DIALLING PLAN>Direction names**").

DIRECTION DEFINED DOWNSTREAM OF

NETWORK

Used to define a tree structure for the dialling plan: the direction code must consist of the rest of the direction code defined upstream.

This parameter is used to define the international direction from the national direction in the export configurations for which national access is through the code 0 and international access through the code 00:

- "NATIONAL" access is defined downstream of "NETWORK" with the access code 0.
- "INTERNATIONAL" access is defined downstream of "NATIONAL" with the access code 00.

ACCESS CODE

Code which follows the direction code defined upstream. If this field is not completed, the code will be the same as that of the direction defined upstream.

TONE AFTER ACCESS CODE

If you select YES, a tone is heard after dialling the access code.

PASSWORD REQUEST

If you select YES, the user must enter a password for a night category override.

LENGTH OF NEXT NUMBER

Number of digits the iPBX waits to receive before transmitting the dialling signal on the network, and before switching to the conversation phase:

- A digit indicates a closed dialling plan
- An asterisk indicates an open dialling plan

DIRECTION OBTAINED ON TIME-OUT

The option YES is reserved for export.

SPECIFIC NUMBERS

Specific numbers are "INTERNATIONAL" direction numbers whose length is different from the length defined above.

Note: If the dialling plan is defined as open (value “*" in the LENGTH OF NEXT NUMBER field, specific numbers are not entered.

For each specific number block to define, enter on a line the beginning of the number, followed by the number of digits for this number in brackets.

5.2.4.4 *Access to TL 0*

Menu **DIALLING PLAN>User dialling plan>Access to directions**

TL 0 access corresponds to private direction 1, whose name is TL 0 in the direction display menu (menu: **DIALLING PLAN>Direction names**).

ACCESS RESTRICTION, BELONGS TO

AREA A	AREA B	AREA C	AREA D
AREA E	AREA F	AREA G	AREA H

The areas are used to configure access restrictions for a subscriber (see subscriber description screen: SUBSCRIBERS>Subscriptions>Characteristics>General characteristics).

Select an AREA: A to H.

ACCESS CODE

Enter an access code for the TIE LINE concerned.

TONE AFTER ACCESS CODE

If you select YES, a tone is heard after dialling the access code.

PASSWORD REQUEST

If you select YES, the user must enter a password.

LENGTH OF NEXT NUMBER

Number of digits the iPBX waits to receive before transmitting the dialling signal on the network, and before switching to the conversation phase:

- A digit indicates a closed dialling plan
- An asterisk indicates an open dialling plan

DIRECTION OBTAINED ON TIME-OUT

The option YES is reserved for export.

SPECIFIC NUMBERS

Specific numbers are private TL 0 direction numbers whose length is different from the length defined above.

Note: If the dialling plan is defined as open (value “*" in the LENGTH OF NEXT NUMBER field, specific numbers are not defined.

For each specific number block to define, enter on a line the beginning of the number, followed by the number of digits for this number in brackets.

5.2.5 SUFFIX DEFINITION

Menu **DIALLING PLAN>User dialling plan>Suffix definition**

A suffix is a code to be entered during a call to perform an action. The suffix must be preceded by a flash (R key).

This command is used to define a suffix for each operation. Operations are actions that can be taken from a telephone set during a call.

Suffixes are defined by default in the system and can be modified by the operator. A suffix is made up of one or two characters (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, #).

RECOVERY FROM ON HOLD (CODE 1)

After setting up a consultation call and carrying out a broker's call operation, you can return to one call and release the other.

BROKER'S CALL (CODE 2)

After setting up a consultation call, you can recover each call alternately (broker's call).

CONFERENCE (CODE 3)

After setting up a consultation call, you can recover the two calls simultaneously in the conference mode.

AUTOMATIC CALLBACK (CODE 5)

On an internal call to a busy set, there is a function you can set for automatic call-back.

INTRUSION (CODE 8)

On an internal call to a busy set, you can intrude on the existing conversation (third party intrusion) but both parties hear the intrusion.

DISCRETE INTRUSION (CODE 7)

Discrete intrusion: the correspondent on the called party set does not hear your conversation (discrete intrusion is only possible after the intrusion procedure).

END OF INTRUSION (CODE 9)

This operation ends an intrusion or discrete intrusion.

ANSWER WAITING CALL

This field is used to consult a call received during another conversation.

NUISANCE CALL (CODE # ∗)

This field is used to record in the logbook an internal or external incoming call. For an ISDN call, program configuration parameter 309.

Note: A record can also be sent to the operator if the iPBX has an ETSI trunk group.

PAGING

This field is used to run the pager function with a consultation call.

SUFFIX FOR EXTERNAL ENQUIRY CALLS

- RECOVERY FROM ON HOLD

This field is used to recover a call on hold during conversation after an external consultation call.

- OPERATION A TO I

This field is used for special operations after an external consultation call. To use these operations, see Menu **NETWORK AND LINKS>Network>Translators>Operations>Operations behind PBX.**.

5.2.6 DISPLAY OF THE PLAN

Menu DIALLING PLAN>**User dialling plan>Display of the plan**

This command is used to display the “user” dialling plan using different filters:

- In tone
- For a plan for a range of DNs
- For "direction” numbers
- For "feature” numbers
- For wrong numbers (unused directory numbers).

FOR NUMBERS BEGINNING WITH

Enter zero, one or more digits.

Note: If no value is entered in this field and the type selected is …….., the entire “user" plan will be displayed.

OR TYPE

• • • • • • • • **DIRECTION** **FEATURE** **WRONG NUMBER**

Select the filter you want.

Note: If the two fields are completed, the resulting filter is a combination of both filters.

Click **Select the item** to validate the filter.

The "user" plan display screen is a table that gives for each dialling plan range:

THE COLUMN…	INDICATING:
FEATURE/DIRECTION	- Direction name if the number range corresponds to a direction - Feature name if the number range corresponds to a feature - “Wrong number" if the number range is not used
TYP/LG/LCR	- Name of the tone to be sent to the caller if necessary (type) - Total number length (lg) expected if the number range corresponds to a direction - Call-related action (lcr) if the number range corresponds to a feature; possible values are: • activate • cancel (deactivate) • use

5.2.7 RESET OF THE PLAN

Menu **DIALLING PLAN>User dialling plan>Access to directions>Reset of the plan**

This command is used to delete the "user” dialling plan before creating a new plan.

Resetting the plan resets:

- The features directory
- The access prefixes
- The special abbreviated numbers
- The internal dialling plan ranges.

USE THIS COMMAND WITH PRECAUTION.

PASSWORD

Enter the password then click "Reset user plan".

Note: The password is the one used to log on to the iPBX Web Admin. If the rights associated with this password are insufficient, the system will reject the dialling plan reset.

When the operation is completed, the screen appears:

Reset done

5.2.8 DISPLAY AREA COMPOSITION

Menu **DIALLING PLAN>User dialling plan>Display area composition**

When a private direction is configured (**User dialling plan>Access to directions**) it is assigned to an area. The areas are used to configure access restrictions for a subscriber (see subscriber description screen: **SUBSCRIBERS>Subscriptions>Characteristics>General characteristics**).

This command is used to display, for each area, all the private directions assigned to it.

For each of the areas to which at least one private direction has been assigned, the list of assigned directions is displayed.

5.3 INCOMING CALL DIALLING PLAN

Menu **DIALLING PLAN>Incoming call dialling plan**

The incoming call dialling plan is used to define the analysis made by the system for incoming calls from the network (DID and TL).

This menu is used to modify and display the incoming call dialling plan.

5.3.1 INTERNAL DIALING

Menu DIALLIING PLAN>**Incoming call dialling plan>Internal dialling**

This command is used to define the length of the DID numbers received, as well as the specific number ranges that do not meet this length criterion (incoming TL calls).

DEFAULT NUMBER OF DIGITS

Enter the number of digits received for DID directory numbers: by default, 4 digits. You can also enter a 2- or 3-digit number so as to match the internal dialling plan.

For PSTN access, which always forwards the MCDU (last four digits of the telephone number), associate an incoming digit translator with the trunk group in order to delete the first one or two digits in the number: the number of default digits must be equal to the length of the translated number.

NUMBER OF DIGITS TO DELETE

The number of digits presented to the iPBX for deletion.

Consequently, the total dialling length corresponds to the sum of the DEFAULT NUMBER OF DIGITS + NUMBER OF DIGIT TO DELETE.

SPECIFIC NUMBERS (1-8)

These fields are used to define up to 8 number ranges the length of which is different from the one defined through the parameter DEFAULT NUMBER OF DIGITS.

Enter the specific numbers in form of a prefix, followed in brackets by the expected number length.

OPERATOR CALL

Operator set DID number (used for export configurations only).

CALL NUMBER OF TEST DEVICE

Number not used. A testing device can be called by a DID number (reserved for a specific application).

CALL NUMBER TO LINK SERVER

Multi-site circuit setup prefix.

Note: This parameter is only available in multi-site configuration.

5.3.2 ACCESS TO PUBLIC EXCHANGE

Menu **DIALLING PLAN> Incoming call dialing plan>Access to public exchange**

This command is used to define access to the transit public network.

ACCESS CODE

Enter the code used to access the PSTN in transit. It is better to make this access code the same as the one used in the extension plan for simplicity purposes.

Validating with the "Enter" key refreshes the screen and displays the access definition parameters.

DEFAULT DIRECTION

NATIONAL	**REGIONAL**	**INTER.**

Same principle as for the extension plan.

DEFAULT LENGTH

10 digits: same principle as for the extension plan.

5.3.3 ACCESS TO DIRECTIONS

Menu **DIALLING PLAN>Incoming call dialling plan>Access to directions**

This command assigns to each direction defined via the menu **DIALLING PLAN>Direction names**:

- A prefix
- A dialling tone after the prefix
- A dialling length
- Specific numbers.

These characteristics are used by the iPBX to split incoming transit between two directions.

BY ITS NAME

NATIONAL	**INTER.**	**REGIONAL**	**TL0**

If other directions that require an access code have been created through Menu **DIALLING PLAN>Direction names**, they will appear on the drop-down list.

Select a direction from the drop-down list then click **Select the item**.

The screen masks are the same as the ones proposed for the definition of access to directions on the user plan ("DIALLING PLAN>User dialling plan>Access to directions”), but no default value is provided.

The operator has to program the tables for each of the directions to enable the iPBX to manage call transit.

5.3.4 ANSWERING SERVICES

This menu is currently not proposed if DID by SDN is enabled (Menu **Subscribers>Rights>General settings**).

DID number management must be carried out from MiVoice 5000 Manager. Refer to the document “DID number management”.

Menu **DIALLING PLAN>Incoming call dialling plan<Answering service**

Answering services are numbers that give direct access to:

- Call distribution services
- Operator services
- The packet switch
- The link server in multi-site configuration.

The system allows the definition of up to 64 DID corporate numbers.

This command is used to display the DID corporate numbers defined on the system. It is also used to create these numbers and create new ones.

The list of DID corporate numbers shows, for each number, the company and department associated with this number, as well as its use.

The character * in the column "Handled by" indicates that handling depends on the caller’s number.

Note: COMPANY – DEPARTMENT names are only displayed in multi-company configuration.

To modify an already defined number, click the rank number of the number to be modified on the list of DID corporate numbers. The definition screen of the DID number to modify is displayed. The parameters to modify are the same as the ones described below for creating a new number.

To define a new DID corporate number, click a rank number corresponding to an empty line.

RECEIVED DIGITS

Enter the MCDU (last four digits of the telephone number) of the incoming call according to the handling that will be carried out by the iPBX (see the field Routing). This number must not already be used elsewhere and must be compatible with the internal ranges of the incoming dialling plan.

Validating with the "Enter" key refreshes the screen and displays the DID number definition parameters.

Note: A general DID corporate number cannot be declared if the directory number has already been assigned.

CHECK NB OVERCHARGED

Field allowing the configuration of a call rejection on numbers accessible only via an overcharged (Audiotel) service.

A field for entering 20 numeric characters.

FREE ANNOUNCEMENTS

When the box is ticked, the free-waiting-time service is activated.

The caller is then charged when the called party off-hooks (like for a normal call without welcome message).

COMPANY

Note: This parameter is only available in multi-company configuration.

The drop-down list contains the company names defined on the iPBX.

Select the company associated with the received digits.

DEPARTMENT

Note: This parameter is only available in multi-company configuration.

The drop-down list contains the names of the departments declared on the iPBX for the selected company.

Select the department associated with the received digits.

ROUTING

C.DIST	OP GP1	OP GP2	-----	OP GP15	DPS MODE	LINK SERVER

A call received with the number declared on the RECEIVED DIGITS line is routed to one of the following:

- A call distribution service
- An operator group (OP GP1 to OP GP15)
- The packet switch
- A LINK SERVER, for a multi-site configuration using dynamic links

RECEPTION SERVICE

This parameter only appears on the screen if the CALL DISTRIBUTION SERVICE value is selected for the ROUTING parameter.

The drop-down list contains the names of the call distribution services declared in the system.

Select the name of a call distribution service.

VIP RECEPTION SERVICE

This parameter only appears on the screen if the CALL DISTRIBUTION SERVICE value is selected for the ROUTING parameter.

The drop-down list contains the names of the call distribution services declared in the system.

Select the name of a VIP call distribution service.

HANDLED ACCORDING TO CALLER

NO **YES**

This parameter is used to route incoming calls by called number and caller number.

If you select YES, the system routes incoming calls with certain numbers to a call distribution service or operator group (a concatenation of the calling party number and the called party number): n this way, you can centralise incoming calls according to where they come from.

The values of the two parameters that follow determine the re-routed number format (see command “DIALLING PLAN>Call rerouting>Update”).

NUMBER OF DIGITS OF CALLING PARTY

Note: This parameter only appears if you select the value YES for the parameter HANDLED ACCORDING TO CALLER.

Number of caller number digits which will be used to form the rerouting number.

Enter a digit from 1 to 8 (default value = 4).

Example: caller number = ABPQMCDU

- By default, ABPQ is kept for rerouting number formatting
- For the value 2, it is AB that will be kept.

NUMBER OF DIGITS OF CALLED PARTY

Note: This parameter only appears if you select the value YES for the parameter HANDLED ACCORDING TO CALLER.

Number of called number digits which will be used to form the rerouting number.

Enter a digit from 0 to 4 (default value = 4).

Example: Called number = MCDU

- By default, MCDU is kept for rerouting number formatting
- For the value 2, it is DU that will be kept.

5.3.5 DISPLAY OF THE PLAN

Menu **DIALLING PLAN>Incoming call dialling plan>Display of the plan**

This command is used to display the “incoming” dialling plan, either in full or for a number range.

FOR NUMBERS BEGINNING WITH

Enter zero, one or more digits.

Note: If no value is entered in this field, the "incoming" dialling plan field will be displayed in full.

Click **Select the item**.

The "incoming" dialling plan display screen is a table that gives the same type of information as the "user" plan display screen.

5.3.6 RESET OF THE PLAN

Menu **DIALLING PLAN>Incoming call dialling plan>Reset of the plan**

This command is used to delete the "incoming" dialling plan before creating a new plan.

USE THIS COMMAND WITH PRECAUTION.

PASSWORD

Enter the password then click "Reset incoming dialling plan".

Note: The password is the one used to log on to the iPBX Web Admin. If the rights associated with this password are insufficient, the system will reject the dialling plan reset.

At the end of the operation, a screen appears, indicating that the plan has been reset.

5.3.7 EXTERNAL NUMBER RANGES

Menu **DIALLING PLAN>Incoming call dialing plan>External dialing ranges**

This menu is currently not proposed if DID by SDN is enabled (Menu **Subscribers>Rights>General settings**).

DID number management must be carried out from MiVoice 5000 Manager. Refer to the document “DID number management”.

If DID numbering by SDN is not enabled:

External number ranges are used to automatically assign a DID number to subscribers if the “Automatic creation of DID numbers” box is ticked while creating subscribers (see the menu **SUBSCRIBERS>Subscriptions>Create**).

Defining external number ranges creates a correspondence between public number ranges and internal number ranges.

5.3.7.1 Names

Menu **DIALLING PLAN>Incoming call dialing plan>External numbering range>Names**

This command is used to declare external number ranges.

EXTERNAL RANGE 1 TO 4

Enter the dialling range name to declare (8 characters).

5.3.7.2 Characteristics

Menu DIALLING PLAN>Incoming call dialling plan>External numbering range>Characteristics

This command is used to configure the declared external number ranges.

BY ITS NAME

The drop-down list contains all the names of the external numbering ranges declared previously.

Select the name of the range to configure then click **Select the item**.

If the range is not already configured, the operator is asked to enter the name of the plan and the DID directory start number before the external numbering range definition screen is displayed. These parameters are defined below in the description of the external numbering range definition screen.

1. Select the name of the plan for which the range will be defined:

2. Press "Enter" to validate then enter the first DID directory number for the range:

3. Press “Enter” to confirm.

The external numbering range definition screen is displayed. (If you have already configured the range, this screen is displayed directly after you have selected the external numbering range.).

PLAN

The drop-down list contains the names of the internal dialling plans defined using the menu **NETWORK AND LINKS>Network>AID handling>Definition of the internal plans**.

Select the plan for which the range will be defined:

- TYPE OF PLAN

This information field indicates the type of plan selected.

DID DIRECTORY NUMBER

The following three parameters concern DID directory numbers.

- BEGIN

Indicate the first DID directory number to define for the external numbering range.

- END

Indicate the last DID directory number to define for the external numbering range.

- NUMBER OF ELEMENT

This information field gives the number of DID directory numbers for the external numbering range.

PUBLIC RANGE

- BEGIN

Indicate the first public number to define for the external numbering range.

- END

This information field indicates the last public number for the external numbering range.

ASSOCIATED TO THE LOCAL RANGE:

- BEGIN

Indicates the first internal number to be associated with the public range.

- END

This information field indicates the last internal number for the external numbering range.

5.3.7.3 *Display*

Menu **DIALLING PLAN>Incoming call dialling plan>External dialling range>Display**

This command is used to display, for a given plan, the declared external numbering ranges.

TYPE OF PLAN

Select the type of plan to view external numbering ranges.

……..	No particular type; you can select it with the parameter OR PLAN NAME
PSTN/TL	PSTN or TL type plan.
PSTN	PSTN plan only.
TL	TL plan only.

OR PLAN NAME

For selecting a plan by name instead of by type.

The drop-down list contains the names of the internal dialling plans defined using Menu **NETWORK AND LINKS>Network>AID handling>Definition of the internal plans**.

Select a name.

When you fill in any of the above fields, click **Select the item**.

The external numbering range display screen is a table that gives each external numbering range defined:

NAME

Name of external numbering range.

DID RANGE

DID directory number range defined for external numbering range.

EXTERNAL NUMBER

First external number defined for the external numbering range.

TYPE

Type of internal dialling plan for which the external dialling range is defined.

PLAN

Name of the internal dialling plan for which the external dialling range is defined.

LOCAL RANGE

Internal number range that will be associated with the external numbering range for automatic creation of DID numbers during subscriber creation.

5.4 PLAN FOR INTERNET LINKS

INTERNET LINK. SIP trunk used for SIP URI calls.

5.4.1 ACCESS TO ALL DOMAINS

This menu is used to define the general internet direction that gives access to all domains.

In a cluster configuration, this menu is only available on the cluster server.

The option only proposes the private directions with a defined name, which are not used in the following menus:

Subscriber dialling plan,

- Network dialling plan,
- Routes,
- AID handling
- Plan for internet links/ Access to specific domains.

The value " **……"** indicates that the access direction to all domains is not defined and does not allows this latter to be deleted.

Selecting another value available on the list allows you to define the access direction to all the domains.

5.4.2 ACCESS TO SPECIFIC DOMAINS

This menu is used to define the internet directions that give access to specific domains.

In a cluster configuration, this menu is only available on the cluster server.

A select **by name** menu is used to choose the direction to configure.

The option only proposes the private directions with a defined name, which are not used in the following menus:

- Subscriber dialling plan,
- Network dialling plan,
- Routes,
- AID handling
- Plan for internet links/ Access to all domains.

If the value "**……**" is displayed, this means that there are no longer any available private directions. Create a new direction in the **Direction name** menu.

If at least one direction is available, pressing the **Select the item** button displays the domain configuration menu.

This menu displays 200 Domain/IP address lines with 50 characters maximum.

One line may contain one IP address or domain name.

In a cluster, the list is automatically updated in the nodes by the replication mechanism.

5.4.3 DISPLAY OF THE PLAN

This menu is used to list all the internet directions with, for each access direction to specific domains, all the associated domains.

In a cluster configuration, this menu is only available on the cluster server.

5.4.4 RESET OF THE PLAN

This menu is used to fully reset the plan for internet links.

In a cluster configuration, this menu is only available on the cluster server.

This menu is operator-account-password-protected.

If the password is correct while the operation is validated by pressing the **Reset plan button for internet links**, the MMC:

- Deletes the routing for the directions:
- Access to all domains,
- Access to specific domains on the internal iPBX.

Deletes direction associations:

- Access to all domains,
- Access to specific domains in internet link type trunks (reset to "…." of the associated direction field) on the internal iPBX.

Re-assigns to area A the TL restrictions of all the directions found in the definition of internet link plan:

- Access to all domains,
- Access to domains.

At the end of the reset operation, the menu displays **Reset made**.

5.5 FORBIDDEN NUMBERS

Menu **DIALLING PLAN>Forbidden numbers**

Barred numbers are external numbers that can be forbidden for subscribers either individually or for all the subscribers of an administrative hierarchy.

Barred numbers are defined in the form of lists. You can define up to 50 lists of 100 numbers.

Each entry in a forbidden 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 numbers is forbidden for a subscriber in day and/or night service in the following conditions:

- The list is associated with the subscription.
- The day and/or night service category associated with the subscription takes into account the restrictions linked with the forbidden numbers lists.

The association of a list of forbidden numbers with a subscription is done via Menu **SUBSCRIBERS>Subscription>Characteristics>General characteristics**.

The association of a list of forbidden numbers with an administrative hierarchy is done via Menu **SUBSCRIBERS>Directory>Hierarchic administration**.

The parameters for acceptance by a category of the restrictions linked with the forbidden numbers lists is configured via Menu **SUBSCRIBERS>Rights>Categories>Characteristics**.

Note: When a list of forbidden numbers is directly associated with a subscription, number control is done only in relation to this list: even if lists are associated with administrative hierarchy levels concerning the subscription, no control is done in relation to these lists.

Menu **DIALLING PLAN>Forbidden numbers** is used to declare and define the list of forbidden numbers:

To declare forbidden number lists, click "**Forbidden numbers lists names**" from Menu **DIALLING PLAN>Forbidden numbers:**

LIST 1 TO 50

Name of the forbidden numbers list (8 characters maximum).

To declare forbidden number lists, click "**Forbidden numbers definition**" from Menu **DIALLING PLAN>Forbidden numbers**.

FOR THE LIST

Name of the list to define. The drop-down list contains the names of the forbidden numbers declared on the system.

Select the name of the list to define, then click **Select the item**:

NUMBER 0 TO 99

Enter in these fields the numbers to be forbidden by this list: a maximum of 22 digits for each number, including direction access codes.

The number entered can be closed or open: in this case, all numbers starting with these digits are forbidden numbers.

USA configuration:

It is possible to use "all digit" characters. These characters are the letters A, B, C and D. Example: 00134AB7 bars all numbers beginning with 0134 and having 7 as their seventh digit (for example 00134007, 00134017, 00134267, 00134597, etc.).

**Any of the letters A, B, C and D can be used by the operator.
Example: 00134AB7 is the same as 00134AA7, 00134CD7, 00134DD7…**

Note: letters must not be used in the code which determines the direction concerned.

REFUSED NUMBERS LIST

This menu is used to create and manage a list of rejected numbers for incoming external calls. The list may contain up to 1000 rejected numbers.

For a Multisite, the list can be drawn up from any site in the Multisite.

The number must be an external number.

If the calling number is contained in the list, the call is rejected and not presented to the attendant console.

The numbers are sent at the same time to the LDAP database.

Format number: String of 20 characters

Authorised characters: **0** to **9** ( ) **+ ' ' ;**

Description: Information field not required.

5.6 SPECIAL NUMBERS

DIALLING PLAN> Special numbers

Special abbreviated numbers are used to call emergency services, and are not forbidden by category. They must not appear on the forbidden lists.

The special numbers are organised by lists. A special number is made up of the access prefix for the list on which it is defined (**DIALLING PLAN>User dialling plan>Access to features)** followed by its rank on the list.

The lists are used to define the number translations to apply to the special numbers.

A special number may require number translations that differ according to the geographic location of the caller, especially in a multi-site configuration. To allow this different management, a code is associated with each location and a set of special number lists can be associated with each code. For a description of location management, see the *MiVoice 5000 operating manual*: *Multi-site management*.

Note: In a multi-site configuration, the special numbers must be configured on the site containing the CAC server. It is advisable to use the site copy tool for copying the lists of special numbers applicable to each site.

A special number (for a given location code) can have two different number translations for the day period and the night period.

A maximum of 200 number translations can be defined. This can be, for example, 10 lists of 10 number translations for two different location codes.

The SPECIAL NUMBERS menu is used to:

- Define the names of the location codes,
- Define the lists of special numbers for each location code,

- Display the list of special numbers defined for a given code,
- Define and associate an abbreviated number with a special number in the case of remote worker subscribers (e.g. teleworking) depending on their geographic location. Refer to the manual Remote Worker via MBG.
  The combination of emergency numbers and general short codes allows emergency numbers to be defined according to the administrative hierarchy directly related to the location.

The emergency short code dialled at one of the sites is a special number for reaching the public emergency service number for that site.

5.6.1 DEFAULT CONFIGURATION OF SOME SPECIAL NUMBERS

The following special numbers are predefined by default:

CODE	LIST	NUMBER	DAY NUMBER	LABEL
0	0	2	112	EMERGENCY
0	0	5	115	EMS
0	0	9	119	MALTREAT
0	1	5	15	EMS
0	1	7	17	POLICE
0	1	8	18	FIRE SERVICE

- The numbers 0112, 0115, 0119, 015, 017 and 018 are associated with the EMERGENCY service.
- The prefix 11 is associated with list 0 of the special numbers.
- The prefixes 15, 17 and 18 are associated with list 1 of the special numbers by retaining the last digit.

5.6.2 SPECIAL NUMBER CODE NAMES

DIALLING PLAN>Special numbers>Special numbers code names

This command is used to define the names of the codes associated with the geographic locations.

Note: The definition of the names of the special numbers codes is done on the site containing the CAC server.

CODE NUMBER 0

Name of CODE 0 (value created by default)

Note: When the location of the terminal can be obtained (especially in dual homing), the code corresponding to Geographical Location 0 is used. In general it is Code 0 but in the case of the cluster, each node has a different location and must therefore point to a different code.

CODE NUMBER 1 TO 49

Names of the codes associated with the different geographic locations.

5.6.3 SPECIAL NUMBERS DEFINITION

Menu **DIALLING PLAN>Special numbers>Special numbers definition**

This command is used to define the translation of the special numbers for each code defined previously.

Note: The definition of the special numbers is done on the site containing the CAC server. If no CAC server is activated, the definition of the lists of special numbers only concerns Code 0 which will be the only one used locally for number translation.

FOR THE CODE

Special numbers code name.

The drop-down list contains all the names of the codes defined previously.

AND THE LIST

Name of the list of the numbers to define.

Once the definition criteria have been selected, click **Select the item**.

NUMBER (*N*) 0 TO 9

N represents the prefix defined in the access to the features.

Examples:

FOR THE FOLLOWING FEATURE CODES…	… THE ABBREVIATED NUMBERS (BY LIST) ARE:		
	LIST 0	LIST 1 (∗)	LIST 2
Special numbers (list 0)	NUMBER (11) 0	NUMBER (1) 5	NUMBER (2) 0
Special numbers (list 1)	Extended day No.	Extended day No.	Extended day No.
Special numbers (list 2)	Extended night No.	Extended night No.	Extended night No.
	Label	Label	Label
	NUMBER (11) 1	NUMBER 6	NUMBER (2) 1
	Extended day No.	Extended day No.	Extended day No.
	Extended night No.	Extended night No.	Extended night No.
	Label	Label	Label

∗: the abbreviated numbers on List 1 are defined "By prefix" in access to features (see Section *5.2.2.2*).

EXTENDED DAY NO.

Enter in this field the full number to dial during the day: maximum of 18 digits, including direction access codes.

Specific configuration for locating teleworkers behind an MBG

It is also possible to enter speed dial numbers (example above: *3000) in the configuration of special numbers. This is to be able to handle emergency calls for teleworkers who are configured behind an MBG and, therefore, cannot be located and make emergency calls corresponding to their actual geographical location. Refer to the document Remote Worker via an MBG.

EXTEND. NIGHT NO

Enter in this field the full number to dial during the night: maximum of 18 digits, including direction access codes.

LABEL

Enter in this field a name (maximum 7 characters) which corresponds to the number stored. This name is internal to MMCs and is only displayed on the digital set when the number is called.

Note: Switchover from day number to night number (and vice versa) is controlled by the barring calendar (common to all subscribers in single-company configuration, by company in multi-company configuration), or by a maintenance set (if the barring management right is granted to maintenance sets).

5.6.4 SPECIAL NUMBERS DISPLAY

Menu **DIALLING PLAN>Special numbers>Special numbers display**

This command is used to view the special numbers defined for a given code.

FOR THE CODE

Name of the special numbers code to view.

The drop-down list contains all the names of the codes defined.

Select the code you want then click **Select the item**. The following window opens:

Note: The << and >> scroll arrows are used to view the special numbers for the other codes.

5.7 CALL REROUTING

Menu **DIALLING PLAN>**CALL REROUTING

This menu is used to translate the number that the telephone translation server uses to reroute calls, either systematically or on no answer. A number translation may concern a specific number or a number range identified by a dialling start.

5.7.1 UPDATE

Menu **DIALLING PLAN>**CALL REROUTING>UPDATE

This command is used to create and/or change rerouting operations.

OPERATION TYPE

CREATE	MODIFY

CREATE	Creates a rerouting operation. The iPBX must be reset when a rerouting operation is created.
MODIFY	Modifies the parameters of a rerouting operation. If no rank number is set, it is the rerouting of the lowest rank number for the feature concerned that is selected.

FEATURE

EXTERNAL CALL	FUNCTIONAL FORWARDING 1	FUNCTIONAL FORWARDING 2
VITAL EXTENSION	PRIVILEGED SUBSCRIBER	DID NUMBER

EXTERNAL CALL	Rerouting by translating a PSTN or TL number to a PSTN, TL, or internal number.
FUNCTIONAL FORWARDING 1	Systematic rerouting by translating an internal number to a PSTN, TL, or internal number.
FUNCTIONAL FORWARDING 2	Rerouting for an unknown internal number – translation of an internal number to a PSTN, TL, or internal number.
VITAL EXTENSION	Rerouting for an inaccessible internal number or a TTS number – translation of an internal number to a PSTN, TL, or internal number.
PRIVILEGED SUBSCRIBER	Reserved.
DID NUMBER	Combined rerouting for a DID number, used to supervise various OP GP call distribution services according to the calling party number (calling and called party: ISDN).

IN MODIF: UPDATE: NUMBER BEGINNING WITH

This field is not significant during creation.

During modification, indicate a complete number or the start of numbers to modify. This value is not obligatory but can be used to directly access the rerouting operation to modify.

RANK REROUTING

This field is not significant during creation.

The rank number, is set automatically on creation and is used to call a record for a possible modification. This value is not obligatory but can be used to directly access the rerouting operation to modify.

Note: If you fill in the previous two fields, the most significant is the number or number start, and the rank is used if necessary, in addition to the number start.

Fill in the relevant fields then click **Select the item**.

5.7.1.1 *Create rerouting*

Menu **DIALLING PLAN>Call rerouting>Update**

If the operation type “CREATE” has been selected, fill in:

NUMBER TO BE REROUTED

Enter the number to be translated.

Validating with the "Enter" key refreshes the screen and displays the rerouting definition parameters.

The proposed definition screen varies according to the selected feature:

DEFINITION SCREEN	FOR FEATURES:
Number to be rerouted: 34 Replaced by: Number of digits to be added: 0	FUNCTIONAL FORWARDING 1 FUNCTIONAL FORWARDING 2 VITAL EXTENSION
Number to be rerouted: 0013969 Replaced by:	EXTERNAL CALL

Number of digits to be added: 0 Or handled by:	
Number to be rerouted: 027000 Replaced by: Or handled by:	DID NUMBER

REPLACED BY

Enter the number resulting from the translation.

NUMBER OF DIGITS TO BE ADDED

Identifies the number range concerned by this rerouting:

- 0 means that the number to be rerouted is complete and rerouting only concerns this number.
- n means that rerouting concerns the number range starting with the value “Number to be rerouted", and completed by n digits.

OR HANDLED BY

…… **C.DIST** **OP GP1** **OP GP2** … **OP GP15** **IVR**

Select the department you want for rerouting.

Note: If you complete this field, it replaces the value possibly entered in the field "Replaced by".

5.7.1.2 *Modify rerouting*

Menu **DIALLING PLAN>Call rerouting>Update**

If the operation type “MODIFY” has been selected, fill in the following fields:

- Number to be rerouted: 0145454545
- Replaced by: 4545
- Number of digits to be added: 0
- Or handled by:

The screens proposed for rerouting modification are the same as the creation screens, but the fields initially contain the values for the rerouting operation being modified.

5.7.2 PROCESSING

Menu **DIALLING PLAN>**CALL REROUTING> PROCESSING

Processing of rerouting defines whether rerouting is systematic or is activated on failure. Processing configuration concerns external calls only: for the features FUNCTIONAL FORWARDING 1, FUNCTIONAL FORWARDING 2 and VITAL EXTENSION, processing is not configurable (see the description of the FEATURE setting).

FOR DIRECTION NATIONAL

DIRECTLY Systematic rerouting

ON FAILURE	Rerouting on congestion.

SEARCH VIA DIRECTORY

This box must be ticked in case of specific DID number management of DID numbers (see the document Managing DID mode).

FOR DIRECTION INTERNATIONAL

DIRECTLY	Systematic rerouting
ON FAILURE	Rerouting on congestion.

FOR DIRECTION REGIONAL

DIRECTLY	Systematic rerouting
ON FAILURE	Rerouting on congestion.

FOR DIRECTION EMERGENCY

DIRECTLY	Systematic rerouting
ON FAILURE	Rerouting on congestion.

FOR DIRECTION TL 0

DIRECTLY	Systematic rerouting
ON FAILURE	Rerouting on congestion.

Note: The NATIONAL, INTERNAT, and TL directions are automatically determined according to the numbers to be rerouted that are created: 0 NATIONAL, 00 INTERNATIONAL and 8 TL. If no rerouting operation is created for a direction, the corresponding field does not appear on the processing configuration screen.

- CALL REROUTING AFTER TRANSLATION

Indicator specifying whether or not STT is implemented after a translation obtained via a vital subscriber.

Default value, box not ticked: existing processing; STT is implemented after a translation obtained via a vital subscriber.

Box ticked: STT not implemented after a translation obtained via a vital subscriber.

5.7.3 DISPLAY

Menu **DIALLING PLAN>Call rerouting> Display**

This command is used to display, by feature, the rerouting operations defined in the system.

FEATURE

EXTERNAL CALL	FUNCTIONAL FORWARDING 1	FUNCTIONAL FORWARDING 2
VITAL EXTENSION	PRIVILEGED SUBSCRIBER	DID NUMBER

EXTERNAL CALL	Rerouting by translating a PSTN or TL number to a PSTN, TL, or internal number.
FUNCTIONAL FORWARDING 1	Systematic rerouting by translating an internal number to a PSTN, TL, or internal number.

FUNCTIONAL FORWARDING 2 Rerouting for an unknown internal number – translation of an internal number to a PSTN, TL, or internal number.

VITAL EXTENSION Rerouting for an inaccessible internal number or a TTS number – translation of an internal number to a PSTN, TL, or internal number.

PRIVILEGED SUBSCRIBER Reserved.

DID NUMBER Combined rerouting for a DID number, used to supervise various OP GP call distribution services according to the calling party number (calling and called party: ISDN).

Select the feature type you want.

NO. TO BE REROUTED STARTS WITH

For defining a number range to be displayed.

If this field is not completed, all rerouting operations for the selected feature will be displayed.

Fill in the relevant fields then click **Select the item**.

The list of rerouting operations corresponding to the request is displayed in form of a table.

RANK	NO. CAL. REROUT	REPLACED BY:
0	00237373737373	01234

5.8 E.164 NUMBERING

Menu **DIALLING PLAN>Dialling parameters of E164 format**

This command is used to define the E.164 numbering parameters.

COUNTRY CODE

iPBX location country code.

INTERNATIONAL / NATIONAL PREFIX

Prefixes used to translate E.164 format to diallable format.

6 NETWORKS AND LINKS

This management domain is all about configuring the items required to set up calls (signals and voice) and transfer data.

Call rerouting from a subscriber to the switched telephone network (TDM network) is defined by different parameters: the assignment of an external direction, the selection of a route (direct or circuitous) and the selection of a trunk.

It is also possible to set up calls by connecting to an IP network.

Multi-site configuration, which must also be defined in this domain, is described in another document - Multi-site management.

Menu **NETWORK AND LINKS**

This menu proposes five major functions used to:

- Manage external lines and subscriber equipment
- Define network characteristics (trunk group, routing)
- Define various aspects of multi-site management
- Configure the quality of service
- Configure links and data.

6.1 EQUIPMENT

Menu **NETWORK AND LINKS>Equipments**

This screen is used to display all the functions available in terms of external line equipment.

Note: For a MiVoice 5000 SERVER, many restrictions exist concerning the use of these functions, especially in the Equipment part of external line and subscriber equipment management.

6.1.1 DECT MANAGEMENT

Menu **NETWORK AND LINKS>Equipments>DECT management**

Working principles:

The geographic area is divided into radio areas.

1 area is managed by 1 or more base stations (3 maximum) placed at the same point (distance of 30 cm).

Optimising the quality of calls in the radio areas optimises the base stations’ transmission and reception according to various factors:

- The areas to cover
- The traffic load
- The features assigned to users
- Electromagnetic disturbances

Definitions:

Coverage area: area in which a wireless terminal (portable set) can make and receive calls.

Radio area: area in which a base station transmits and receives signals.

Cell: a set of base stations, or a base station entity used to locate portable terminals.

The menus proposed for DECT use the tree logic: first the topology must be defined, then the resources and finally the mobiles concerned.

6.1.1.1 *Names of cells*

Menu **NETWORK AND LINKS>Equipments>DECT management>Names of cells**

This screen is used to display the names of the cells associated with the DECT. It allows you to declare the cells that were defined during deployment. The maximum number of cells is fixed at 128 (for single-site configuration) and 254 (for multi-site configuration).

6.1.1.2 *DECT parameters*

Menu **NETWORK AND LINKS>Equipments>DECT management>DECT settings**

This screen is used to define the parameters associated with the DECT.

PARI VALUE 0

9 digits maximum (the PARI number can be found on the iPBX approval label).

MOBILES RECORDING

- RANDOM VALUE / RS VALUE

9 digits maximum 2 random values (must not be the same) registered in the mobile by the iPBX when the mobile was registered on the DECT network.

From this point onwards, the iPBX regularly checks the values registered in the cordless handsets (the values are calculated from these two parameters) in order to authorise or refuse use of the DECT network.

Enter a value lower than 4294967295 (FFFF FFFFh). The value of the random number has no significance. However, in a multi-site configuration the number must be identical in all locations where the mobiles are to be registered.

- PASSWORD

Password used while registering a cordless handset.

- RECORDING CODE

Recording code length. The recording code consists of the last digits of the directory number, possibly completed with the first digits of the record password.

DIR. BEGINNING ASSIGNED TO PLL

4 digits maximum, 999 by default. The base stations are connected to the iPBX via an S0 Basic Rate Interface. One PLL (D channel) is used for signalling and downloading to the base stations. PLL directory numbers are comprised of digits recorded in this parameter followed by the base station declaration order number.

Example: 999000, 999001, 999002, etc.

SEARCH FOR MOBILE ON LOCAL SITE

NO **YES**

Indicates whether the cordless handset must be searched for on the local site or on another site.

OR IN ANOTHER SITE

…………

Name of the site where the cordless handset must be searched for.

OR IN THE LOCAL CENTER

NO YES

Indicates whether the cordless handset must be searched for on the local centre or on another centre.

OR IN ANOTHER CENTER

....

Name of the center where the cordless handset must be searched for.

OR IN THE LIST

....

Select the (BROADCAST) list on which the cordless handset must be searched for.

CLOCK SYNCHRON.

This parameter is used to configure the synchronisation of DECT clocks.

3 possible selections: "Priority master", "Not priority master", “Slave”.

- Case of single-site configuration: the default value for a site is “Priority master” (this is supposed to be a standalone site).
- Case of multi-site configuration: in simplex mode, a single iPBX is set to "Priority master” and provides the DECT synchronisation signal for the entire multi-site network. Other iPBXs are configured as "Slaves". In duplex mode, two iPBXs are masters (one "Priority master” and the other “Non priority master”) and can provide the DECT synchronisation signal for the entire multi-site network, while other sites are configured as “Slaves”.

Note: For a multisite network, additional parameters appear, making it possible to define the list of sites on which the mobile terminals will be registered.

6.2 NETWORK

Menu **NETWORK AND LINKS> Network**

This menu includes 9 functions used to:

- Define trunk groups
- Configure then view routing operations
- Define off-net operators
- Manage signalling
- Take the AID into account
- Define the translators,
- Authorise transfers.

Note: IP operators are managed from Menu NETWORK AND LINKS>Network>Trunk groups>Characteristics, by selecting an SIP type trunk group.

6.2.1 TRUNK GROUPS

Menu **NETWORK AND LINKS>Equipment>Trunk groups**

6.2.1.1 *Names*

Menu **NETWORK AND LINKS>Network>Trunk groups**

This screen is used to define the various trunk groups on the installation.

TRUNK GROUP N (1 TO 61)

Name assigned to trunk group n (maximum 8 characters): this definable trunk group number varies according to the system used (see the table below).

Additional fields are available to create further trunk groups.

Note: A trunk group with no name cannot be managed as it does not exist.

	MITEL RANGE
No. of trunk groups which can be managed by the system	61
Trunk group defined by default	
	SIP.TG

Example: Create two additional trunk groups:

On a free location, type "NET.TG" then Enter. This trunk group is for "manager lines" only (analogue trunk lines only)

In a free field, type "PAG.TG" then Enter. This trunk group is for "Paging" only (analogue trunk lines only).

Note: When you create a trunk group, you must define its characteristics and the external trunks it will contain.

The trunk group created must contain a set of homogeneous lines

- **same type,**
- **same signalling.**

6.2.1.2 *Characteristics*

Menu **NETWORK AND LINKS>Network>Trunk groups>Characteristics**

BY ITS NAME

Select the trunk group you want to work on: if you have created a trunk group by name, this is displayed when you make the selection.

After choosing the trunk group name, click **Select the item** to obtain the menu **Characteristics of trunk group**.

6.2.1.2.1 Characteristics of a VoIP trunk group

Menu **NETWORK AND LINKS>Network>Trunk groups>Characteristics**

This menu is used to define the characteristics of a Voice over IP trunk group as well as all the SIP trunk parameters.

An SIP trunk group corresponds to an SIP operator.

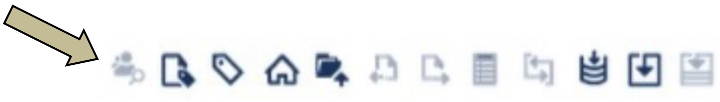
By default, only one SIP trunk group **SIP. TG** is defined by the system.

This menu has the icon used to change, for the configuration of an SIP trunk, from basic (simplified) mode to advanced mode (for installers who want a more comprehensive configuration).

In basic mode, a simplified frame is offered with the minimum parameters needed to quickly and easily configure the trunk.

In advanced mode, more fields are proposed and they allow a more extensive and comprehensive configuration.

This icon is displayed on the top left side of the screen:



Clicking this icon triggers the switchover. Advanced settings are shown in italics.

In this section the parameters are identified in italics on a grey background.

Basic or advanced configuration mode, for a given installer, can also be used from Menu **System>Configuration>Users>Operators definition**.

In the **By its name** option, select **SIP.TG**.

PHYSICAL TYPE

In the **Physical type** option, select **Voice over IP**.

NATURE

Trunk group type option:

BOTHWAY **OUTGOING** **INCOMING**

By default, the trunk group is declared as BOTHWAY.

TYPE OF SIGNALLING

Signalling type option to be assigned to the trunk group:

- MOVACS: Proprietary IP signalling (reserved to the SVL-IP)
  - H.323: Signalling allowing interconnection with H323 type IP networks
  - SIP: Signalling allowing interconnection with SIP type IP networks.

AT TYPE

Signalling sub-type option to be assigned to the trunk group:

Note: The list of basic/advanced parameters differs according to this sub-type.

- STANDARD (default value)
- ROOM STATUS

The dedicated ROOM STATUS trunk group does not contain any trunk lines. In this case, a charge record is printed out if an unsuccessful line seizure attempt is made on this trunk group (Hotel configuration).

- INTERNET LINK. SIP trunk used for SIP URI calls.
- VOICE MAIL. Trunk connected to external voicemail via an SIP trunk.
- INATTEND: Trunk connected to INATTEND via an SIP trunk.
- MICC: Trunk connected to MICC via an SIP trunk.
- CLOUDLINK: Trunk connected to CLOUDLINK via an SIP trunk (refer to the document CloudLink - Integration with MiVoice 5000, on the Mitel website).

Routing of external calls

In a multi-site configuration, MiCC-B agents can be located in various sites/locations. Selecting the **Routing of EXT calls** list enables you to route agents' outgoing calls via their local trunk, as required.

ADVANCED CHARACTERISTICS

After choosing the signalling characteristics, click **Characteristics** to obtain the following fields:

COMPANY

CMPNY.0 **• • • • •**

Option displayed if multi-company configuration is used. On system startup, the trunk belongs to CMPNY. 0

To modify this field go to the DEPARTMENT field and select **.......**.

This value is not assigned to the trunk group. All trunk groups must belong to a new COMPANY/DEPARTMENT pair, or to the CMPNY.0/DEPT.0 pair. If you have created company names, these appear on this line.

Select the company assigned to this trunk group.

DEPARTMENT

DEPT.0 0 **• • • • •**

Options. If the multi-company operation is used. On system start-up, the trunk group belongs to department DEPT.0 of company CMPNY.0.

The **........** field which means "for all other departments" (default department) is only used for changing the company. If you have already created departments for the various companies, these will appear on this line.

Use the space bar of your terminal to select the departments assigned to this trunk group.

SIGNALLING TYPE

This information field indicates the configuration made on the previous trunk group configuration screen.

LINK STATUS

Information field showing the current link status.

TRUNK GROUP USED FOR "ROOM STATUS"

Box to be ticked if the trunk group is used for this feature.

PROTOCOL

Option in advanced mode only: UDP, TCP or TLS

with TLS profile: This link allows you to define the TLS profile to use for this trunk. This link points to Menu **Telephony Service menu>System>Security>Additional TLS Profiles** used to access the TLS profile configuration. This link can be used if you start by creating a trunk in this menu and then want to associate it with a TLS profile (configured or not) to complete and finalise the access security on this trunk.

Then choose the profile to be used from the list.

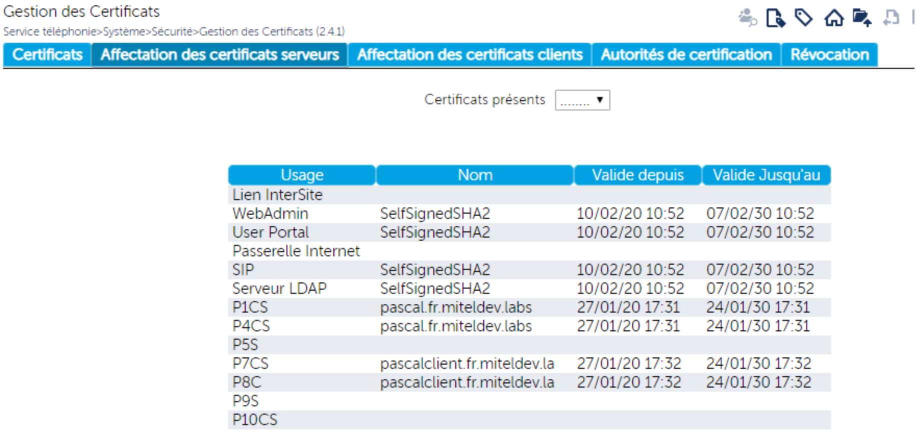
The list only shows profiles that are fully configured and in particular if the assignment of certificates (servers and clients) has been finalised (Menu **Telephony service>System>Security>Certificates management**).

When a specific profile is selected, the system signals the restart of the SIP service for that trunk with the profile:

WARNING: **Restarting the SIP service is necessary (network/SIP router configuration) and should be done at the time when it will cause the least disruption to communications.**

In the example, 5 profiles are proposed concerning the configuration made on the **Certificate** side:

In the example on the **Servers certificate** side



Gestion des Certificats

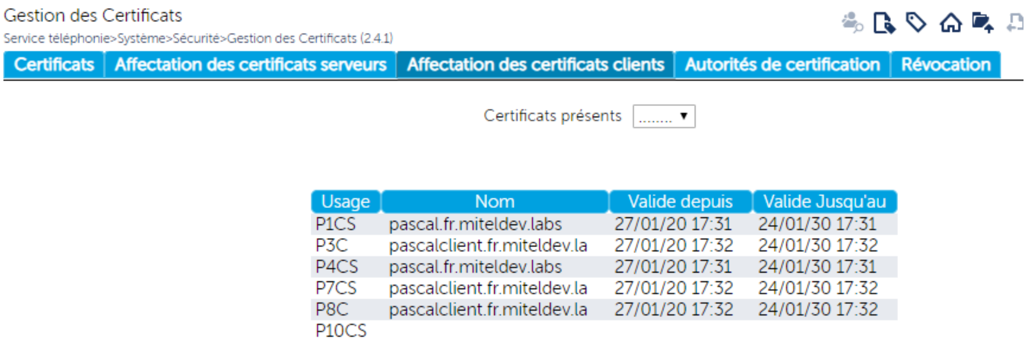
Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.1)

Certificats
Affectation des certificats serveurs
Affectation des certificats clients
Autorités de certification
Révocation

Certificats présents .... ▾

Usage	Nom	Valide depuis	Valide Jusqu'au
Lien InterSite			
WebAdmin	SelfSignedSHA2	10/02/20 10:52	07/02/30 10:52
User Portal	SelfSignedSHA2	10/02/20 10:52	07/02/30 10:52
Passerelle Internet			
SIP	SelfSignedSHA2	10/02/20 10:52	07/02/30 10:52
Serveur LDAP	SelfSignedSHA2	10/02/20 10:52	07/02/30 10:52
P1CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P4CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P5S			
P7CS	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P8C	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P9S			
P10CS			

In the example on the **Clients certificates** side


Gestion des Certificats
Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.1)
Certificats
Affectation des certificats serveurs
Affectation des certificats clients
Autorités de certification
Révocation

Certificats présents .... ▾

Usage	Nom	Valide depuis	Valide Jusqu'au
P1CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P3C	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P4CS	pascal.fr.miteldev.labs	27/01/20 17:31	24/01/30 17:31
P7CS	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P8C	pascalclient.fr.miteldev.la	27/01/20 17:32	24/01/30 17:32
P10CS			

SIPS COMPATIBILITY

In the case of TLS protocol**(only**), this check box allows more secure exchanges between MiVoice 5000 and SIP trunks using the SIPS protocol.

Box ticked: Integration takes place during SIP trunk configuration.

SIPS (SIP Secure), is an extended SIP protocol associated with TLS (Transport Layer Security).

SIPS guarantees end-to-end security for signalling.

This configuration is native on MiVoice 5000 for all TLS/SIP connections, but some SIP trunk operators impose the use of SIP protocol only (SIPS not taken into account).

This parameter, therefore, allows the protocol to be adapted (activated/deactivated) according to the SIP trunk configuration. By default, SIPS is active.

By default, SIPS support is ticked.

PROXY NO. 1

IP address or name of the remote SIP proxy (carrier) to which the frames will be sent.

- Port

The SIP port used by remote proxy No.1.

PROXY NO 2

IP address or name of the remote SIP proxy (carrier) to which the frames will be sent if Proxy No. 1 fails to answer after 3 attempts.

Note: The attempt is made systematically on Proxy No. 1 for each call.

- Port

The SIP port used by remote proxy No.2.

DOMAIN / REALM (OPTIONAL)

IP address or name of the domain to which the remote point you wish to reach belongs. The SIP message headers will use the domain/real and not Proxy No. 1 or No. 2.

This parameter may be used for authentication at certain carriers'.

Example of domain: operator.com

- Port

SIP port used for **domain/realm**.

LOCAL PROXY

NO | **NAT SBC PROXY** | **YES**

This field is used to indicate the proxy type in order to process requests:

YES: shows that the NAT proxy is local and not a MITEL proprietary solution.

In this case, enter the IP address and the corresponding port allowing the identification. Only initial requests from the IP address will be accepted.

NAT SBC PROXY: shows that the NAT proxy is local and a MITEL proprietary solution.

In this case, enter the IP address and the corresponding port allowing the identification. Only initial requests from the IP address will be accepted.

Note: For the port used if the proxy is internal: The default value is 5064 if the local proxy is NAT SBC PROXY; otherwise, it is 5060. This line only appears if an IP address is defined.

CHECK PROXY

NO: in this case, the proxy is not local (no NAT proxy) and the following ID check option can be chosen:

- ………… : No checking (of physical address)
- IP ADDRESS: checks that the SIP message comes from a configured IP address
- IP ADDRESS + PORT: checks the registration IP address

ASSOCIATED DIRECTION

This option is proposed, no matter the type of trunk group (outgoing, incoming, bothway).

The default value is "……", indicating that no internet direction is associated.

The drop-down list only proposes directions which belong to the plan for internet links and which are not already used for other trunks.

The access direction to all the domains can only be selected if the value for the setting **Local proxy** is not **NO** (the value recommended in this case is **NAT SBC PROXY**), or else an error message is displayed.

Local/INTERNET proxy incompatibility.

The value "**….**" (deleting the Trunk/Direction association) can only be restored if there are no longer any defined routes.

Otherwise, the following error diagnosis is displayed:

Value: ………

INTERNET direction in routing

The setting **Audit during speech** is activated with management through **MSG INVITE** and a frequency of **3600** seconds.

For the management of identity transmission, the settings **call ID (From/PAI/PPI/RPID)** proposes two options:

- SIP URI (default value, which corresponds to the IID/AID value for standard SIP trunks) or
- IDENTIFIER

No matter the selected value, the setting **number (From/PAI/PPI/RPID) in E.164 format** is not significant and is, therefore, hidden for this trunk group sub-type.

IDENTIFIER

Field indicating the iPBX username.

REGISTERING

Checkbox used to declare the authorisation account of the SIP trunk set up on the remote carrier.

The identifier account is active throughout the timeout period mentioned in the **Expiration timeout (sec)** field. The recording is reset to half of the timeout interval.

The different statuses detected by the iPBX are:

  - Unknown
  - Registered
  - Carrier refusal
  - Not configured
  - No answer from carrier
  - In progress.

- Register in proxy:
  - Box ticked, the registration is made on Proxies 1 and 2 or on the previously declared domain name.
  - Box not ticked, registration is made on the server declared in the Registration server field.

AUTHENTICATION

(CLIENT ACCOUNT /LOGIN AND PASSWORD)

Field used to authenticate to the carrier. This authentication is not related to recording, but it may be required any time by the carrier.

- SIP client
- SIP server client

PUBLIC NAME OF SIP ACCESS POINT

Field used to send the domain name instead of IP address in the FROM and CONTACT fields of SIP requests for outgoing calls.

SPECIAL PARAMETERS FOR SIP SIGNALLING

AUDIT DURING SPEECH

Checkbox

MSG INVITE ***MSG INFO*** ***MSG OPTIONS*** ***MSG UPDATE***

*This field is used to choose the type of SIP request sent during communication, depending on the next field (**Audit frequency**), to ensure the availability of the remote device.*

The minimum audit frequency with the INVITE request is 3600 seconds. It is 10 seconds for other requests.

AUDIT OUT OF SPEECH (OPTIONS)

PRINCIPLE

A special **OPTIONS** message is transmitted by the iPBX and is used to audit the operator's proxy out of speech.

This way, the PBX is dynamically informed whether or not the operator's proxy is available. This allows immediate overflow to another trunk if the operator's proxy is unavailable.

If this service is activated (**AUDIT OUT OF SPEECH (OPTIONS**) checkbox ticked), the iPBX sends regularly (30s by default) an **OPTIONS** message to the operator's proxy.

Proxy 1 alone is configured:

If Proxy 1 is available and returns a message called **200 OK**, calls will be channelled to it.

Otherwise, after 5 attempts to reach Proxy 1 (Proxy 1 Out of Service) calls will no longer be sent to the SIP trunk but will overflow directly via another trunk (if configured).

After 30 seconds (default value), the iPBX checks again whether Proxy 1 is available, via the **OPTIONS** message.

Proxy 1 and Proxy 2 are configured:

If Proxy 1 is available and returns a message called **200 OK**, calls will be channelled to it.

Otherwise, after 3 attempts to reach Proxy 1 (Proxy 1 Out of Service), the **OPTIONS** message is sent to Proxy 2.

If Proxy 2 is available and returns a message called **200 OK**, calls will be directly channelled to it.

Otherwise, after 3 attempts to reach Proxy 2 (Proxy 2 also Out of Service) calls will no longer be sent to the SIP trunk but will overflow directly via another trunk (if configured).

After 30 seconds (default value), the PBX checks again whether Proxy 1 and Proxy 2 are available, via the **OPTIONS** message.

FORCED TRUNK RELEASE

***Box ticked**: the "anti-gossip" function is enabled for this type of trunk group.*

*A link is associated with this line, enabling the user to go directly to the automatic trunk release line of Menu **TELEPHONY SERVICE>System>Expert>Time-out** to finish configuring the anti-gossip function.*

***Box not ticked**: anti-gossip function disabled.*

Note: This line is not displayed for trunk groups with H323 or MOVACS signalling.

⚠ **WARNING:** ***Automatic release does not apply to calls made from priority terminals (subscription characteristics).***

TRANSMISSION OF ROUTED NUMBERS

Choice of transmission of the corresponding SIP field to the rerouted number:

- *DIVERSION*
- *HISTORY INFO*

Both of them are supported for reception.

IDENTITY SENDING MANAGEMENT

Checkbox used to choose whether or not to send the ID.

CALL IDENTIFIER (FROM)

- *RECORDING ID: corresponds to the IDENTIFIER field*
- *IID/AID: configured in AID processing. An associated box is used to indicate whether the From number is in E.164 format.*

PRESENTATION/RESTRICTION

- *No*
- *P AssertedID: sending the corresponding header*
- *P-PreferredID: sending the corresponding header*
- *PAI and PPI: sending the corresponding header*
- *Remote-Party-ID: sending the corresponding header*

CALL IDENTIFIER (PAI/PPI/PAI,PPI/RPID)

- *IID/AID: an associated box is used to indicate whether the PAI number is in E.164 format.*
- *IDENTIFIER*

SENDING ANONYMOUS INTO FROM

Box to be ticked if anonymous is sent into From if IID/AID is the call identifier (From).

UPDATE OF NAME/NUMBER (UPDATE)

Box to be ticked to transmit the request to update the corresponding header (during the call or ringing phase).

An associated box is used to indicate whether the PAI number is in E.164 format.

IDENTITY RECEPTION MANAGEMENT

Field used to choose whether or not to send the ID.

ID CALLING IN:

- *FROM*

- *PAI or PPI or RPID*

NAME MANAGEMENT

Box ticked: When a call comes in via an SIP trunk, the name of the external directory record corresponding to the number is displayed on the terminal.

FORWARDING MANAGEMENT:

Fields allowing the configuration of two forwarding types for the trunk groups with SIP signalling:

- Immediate forward / forward on busy

- Forward on no answer

Tick the box, respectively for each forwarding type, to activate it.

By default, these forwarding operations are not managed (box not ticked).

VOICE MAIL

This field is used to indicate whether or not the trunk will be connected to an SIP messaging system.

The Subscription line is displayed if the box is ticked.

Subscription

This field is used to indicate whether to manage a subscription to the MWI service. Possible options are:

- *NO: no subscription to the MWI service*
- *WITH IDENTIFIER: a subscription to the MWI service is made using the identifier defined on the "Identifier" line of this menu.*

*The option **WITH IDENTIFIER** is only accepted if an identifier had been previously entered on the "Identifier" line; otherwise an error message "**INVALID IDENTIFIER**" is displayed.*

- *- Run out (sec). This field is used to configure the duration of expiration of an MWI service subscription request. A duration ranging from 20 seconds to 65534 seconds (~ 18 hours) can be entered in this field.*
- *- status. This field shows the status of MWI service subscription requests.*
  - UNKNOWN
  - RECORDED
  - CARRIER REFUSAL
  - NOT CONFIGURED
  - NO ANSWER FROM CARRIER
  - CARRIER REFUSAL
  - DURING
  - SUBSCRIBED

This line is hidden if the "Voicemail" line is not ticked and if the value for the "- subscription" line is NO.

next MWI subscribe at ????????. This line presents the transmission time for the next MWI service subscription request.

MESSAGE LEAVE EXPIRED (SEC)

Validity period entered in the EXPIRES field of the MWI (Message Waiting Indicator) service subscription message.

LOCAL GENERATION OF TONES

If the box is not ticked, the line below is proposed.

ON HOLD MANAGEMENT / FORCE IP ADDRESS TO 0

Choice of the values entered in the attributes of the SDP layer of on-hold INVITE requests.

If the box is ticked, the announcements/tones are managed by MiVoice 5000:

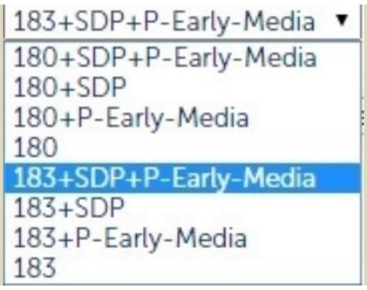
SUPPORT PRACK (100REL)

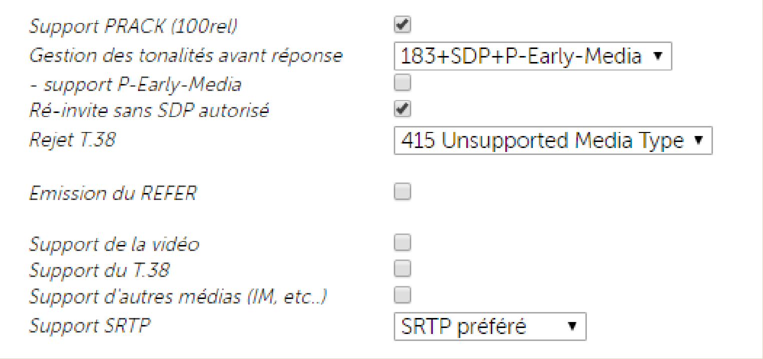
To be ticked if the operator supports the PRACK message in SIP.

Checkbox ticked by default.

MANAGEMENT OF TONES BEFORE ANSWER

- *- support P-Early-Media: shows for an outgoing call that the iPBX supports the P-Early-Media SIP field. This field is used to manage the announcement/tones generated by the network before starting to communicate.*
- *- on transit*

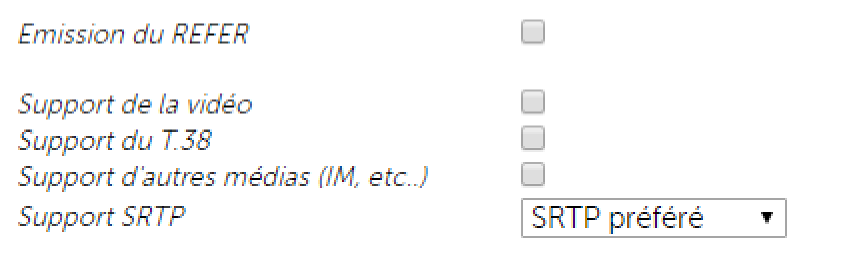




Support PRACK (100rel)	☑
Gestion des tonalités avant réponse	183+SDP+P-Early-Media ▼
- support P-Early-Media	☐
Ré-invite sans SDP autorisé	☑
Rejet T.38	415 Unsupported Media Type ▼
Emission du REFER	☐
Support de la vidéo	☐
Support du T.38	☐
Support d'autres médias (IM, etc..)	☐
Support SRTP	SRTP préféré ▼

RE-INVITE WITHOUT ALLOWED SDP

Choice to be made for an incoming call, with transit for the call, if you wish to transmit (play back) the tone/announcement from the requested network.



Emission du REFER □

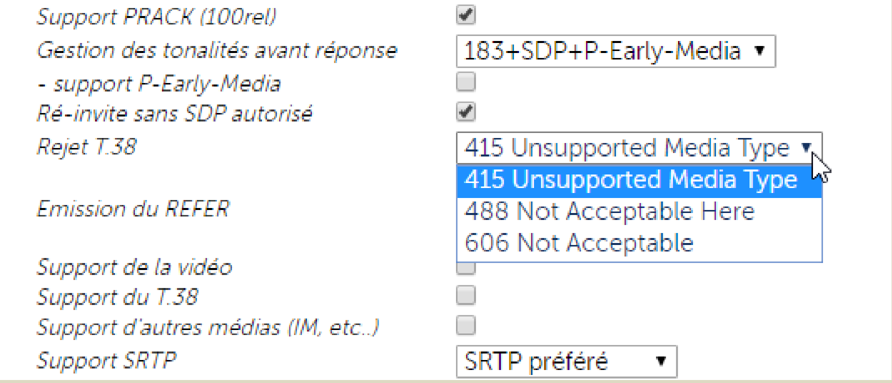
Support de la vidéo □

Support du T.38 □

Support d'autres médias (IM, etc..) □

Support SRTP: SRTP préféré ▼

Reject T38



Support PRACK (100rel) ☑

Gestion des tonalités avant réponse: 183+SDP+P-Early-Media ▼

- support P-Early-Media □

Ré-invite sans SDP autorisé ☑

Rejet T.38: 415 Unsupported Media Type ▼

Emission du REFER

Support de la vidéo

Support du T.38 □

Support d'autres médias (IM, etc..) □

Support SRTP: SRTP préféré ▼

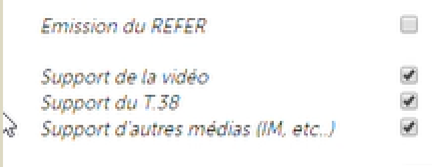
REFER sending*: indicates that the operator or the device behind the SIP trunk can handle the transfer using the REFER method.*

Support of video*:*

Support of T.38*:*

Support of other medias (IM, etc.) *:*

Before



Emission du REFER □

Support de la vidéo ☑

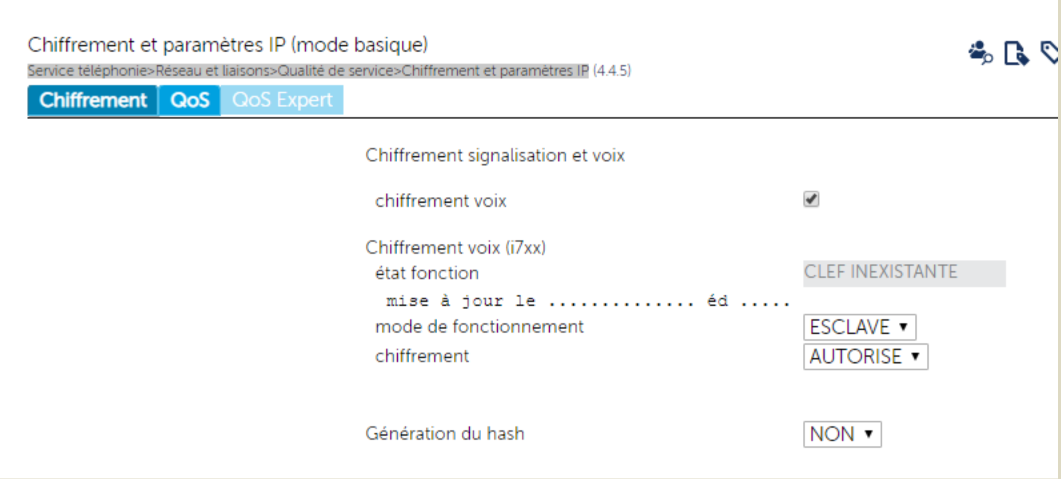
Support du T.38 ☑

Support d'autres médias (IM, etc..) ☑

After

SRTP support*:*

This line only appears if the voice encryption setting is tcked (active) in Menu ***Telephony Service>Network and links>Quality of service>Ciphering and IP settings****.*



Chiffrement et paramètres IP (mode basique)

Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP (4.4.5)

Chiffrement signalisation et voix

chiffrement voix ☑

Chiffrement voix (i7xx)

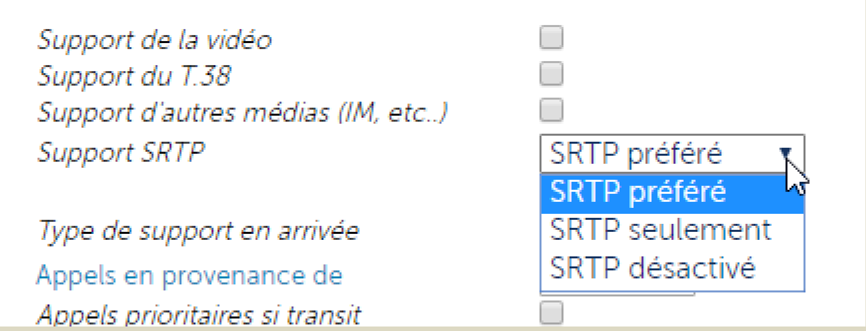
état fonction CLEF INEXISTANTE

mise à jour le .... éd .....

mode de fonctionnement ESCLAVE

chiffrement AUTORISE

Génération du hash NON



Support de la vidéo ☐

Support du T.38 ☐

Support d'autres médias (IM, etc..) ☐

Support SRTP SRTP préféré

Type de support en arrivée

Appels en provenance de

Appels prioritaires si transit ☐

Option used to configure the SRTP protocol:

- *Preferred SRTP: Default value*
- *SRTP only:*
- *SRTP disabled:*

BEARER TYPE INCOMING

CCBT + CCBNT *CCBT* *CCBNT*

The call is rejected if the terminal requested is not of the same type as the calling party terminal (see the field Bearer type outgoing).

CALLS FROM

This setting is used to display the origin of a call on the digital terminal: name of the network or private direction (private direction names are defined in Menu DIALLING PLAN>Direction names).

For a trunk in service, this setting cannot be on the field ....

PRIORITY CALLS IF TRANSIT

Box to be ticked to authorise priority line seizure in an outgoing trunk or on an inter-site link in the same way as a priority subscriber.

SEARCH DID NUMBERS

INCOMING DIGIT TRANSLATOR NUMBER

Enter in this field the incoming digit translator number. This can be used for DID to translate the number received from the network into an internal number. This way, a DID directory number does not have to be given for each user.

This function can also be used for a transfer to a remote PBX.

Reject of numbers not assigned:

Field used to define the processing operation for a network call, if the subscriber does not exist:

- *Box ticked: The communication is terminated.*
- *Box not ticked: the call is forwarded to an attendant console.*

***Search via directory**: This box must be ticked in case of specific DID number management (see the document Managing DID numbers).*

PRE-ANSWERING MESSAGE, CALLER CHARGED

These headings concern incoming and bothway trunk groups only.

Recorded announcement connection is only effective if network tones are declared accordingly (see **VOICE MAIL AND TONES>Tones**).

IF CALLED PARTY FREE OR BUSY 1

Checkbox: The call is connected to the pre-answering message and a charge record is printed in real time, if the user status is free or busy 1.

IF CALLED PARTY BUSY 2

Checkbox: The call is connected to the pre-answering message and a charge record is printed in real time, if the user status is busy 2.

IF NUMBER NOT ASSIGNED

Checkbox: The call is connected to the pre-answering message and a charge record is printed in real time, if a call number is not assigned.

TRANSFER TO

- C.DIST
- OP GP1 to OP GP15
- IVR
- Disabled

Depending on your selection, the call can be handled in two different ways after the no answer time-out for a DID call:

- If you have selected "C.DIST" this call will be handled by the call distribution service according to the applicable calendar (for more information on call distribution, see the chapter on call distribution management).
- If you have selected "SVOPx" this call will be handled by the operator service in which the ATDC has priority (for more information on operator services, see the chapter on call distribution management).
- If you have selected "IVR", this call will be processed by the IVR.

CALL DISTR NAME

C.DIST.0 0

This column only appears if you selected C. DIST in the previous field (selection of the answering service defined for call handling).

TRANSFER ACC. TO CALLED PTY COMP-DEPT CALLED PTY COMP-DEPT

*Invisible if the **Transfer to** parameter is disabled.*

Checkbox: A DID call which is not answered is always forwarded to the call distribution service corresponding to the requested company/department extension.

WARNING: If a loop back is made on the same call distribution service, and if the terminals of this service are on standby or in busy state, there is a security forwarding to ACC.0 (see the call distribution document).

TRUNK GROUP ID (TEL. RECORD)

Value to be entered, used for telephone record handling to group together the various trunks which provide access to a single operator (maximum 3 digits).

TRUNK GROUP SUPERVISION

Checkbox used to validate or invalidate the generation of alarms for the trunk group in question.

The box is ticked by default (supervision active upon creating the trunk group or during an upgrade from an earlier release.

MAX. NUMBER OF SIMULTANEOUS CALLS

Field used to define the maximum number of simultaneous calls on the trunk group. Value between 0 and 65534.

CAC IP ADDRESS / CENTER – CAC CLASS

Information fields.

The address (configured manually or automatically after a call) enables the CAC server to identify trunk calls.

6.2.1.3 *Display users*

Menu **NETWORK AND LINKS>Network>Trunk groups>Display users**

This screen is accessible via NETWORK AND LINKS>Network>Trunk groups>Display users.

This screen is used to display the users declared for a given trunk group.

The scroll bars on top and on the right side of the << and >> screen are used to navigate to see other users.

6.2.2 ROUTES

Menu **NETWORK AND LINKS>Network>Routes**

A route is defined by 4 parameters:

- FOR ROUTING CODE (only available in multi-company management)
- TO DIRECTION
- VIA ROUTE TYPE (routing)
- ON TRUNK GROUP

The **To direction** field proposes all the directions with a name.

- If a non-internet direction is selected, the On trunk group field does not propose any Internet link trunk group sub-type.
- If an internet direction is selected, the On trunk group field proposes:
  - The unique trunk group (if it exists) which is associated with this same direction in the Associated direction field
  - The value ".....” if no trunk group corresponds to the above criteria.

6.2.2.1 *Route selection*

Menu **NETWORK AND LINKS>Network>Routes**

This screen is accessible via NETWORK AND LINKS>Network>Routes.

This screen is used to select the type of route whose characteristics need to be defined.

- In single-company management, the routing code is not requested; it is automatically set at 0.
- In multi-company management, this code is a definition parameter for a company/department pair.

If we take the case of 2 totally independent companies, each having several departments, and with each department having its own trunk resources (trunk line groups), the simplest solution is to assign a routing code to each company. The company name can then be assigned to this routing code.

Similarly, it is possible to privilege a department of a company by giving only this department access to a particular trunk group. This department will then have its own routing code to reach the trunk group reserved for it.

Note: Two routing codes are assigned to this company/department pair: one to access the public network, the other to access the private network.

SETTING UP AN OUTGOING CALL

At initialisation, the system configures three directions: REGIONAL, NATIONAL and INTERNATIONAL via the DIRECT 0 route on the FT0-ETSI trunk group.

FOR ROUTING CODE

CODE 0

This parameter is only displayed if multi-company configuration is used. Code 0 is automatically assigned to the three routes of the trunk group.

TO DIRECTION

Select a direction for the direct routing.

VIA ROUTE TYPE

DIRECT 0	DIRECT 1	PROXIMITY 0	PROXIMITY 1	REROUTING 0	REROUTING 1

REROUTING 2	REROUTING 3	REROUTING 4	REROUTING 5
REROUTING 6	REROUTING 7	OTHER NETWRK 0	OTHER NETWRK 1
OTHER NETWRK 2	OTHER NETWRK 3	MANAGER LINE	. . . .

The route defines the possible variants according to trunk group saturation:

DIRECT

The direct route is the one which is normally used to route the call. Each direction must always have a direct route.

There are 2 possible direct routes.

If the direct routes do not have a line available, and depending on the calling user's rights, it may be possible to overflow onto other trunk groups:

REROUTING

This concerns selecting a line in another trunk group which belongs to the same network. For example: TL-->TL, PSN-->PSN, (traffic +).

There are 8 possible types of overflow routing.

OTHER NETWRK

This concerns selecting a line in another trunk group which belongs to another network, typically TL-->PSTN.

There are 4 possible types of "other network" routing.

MANAGER LINE

This type of routing is used to isolate "manager lines" in a particular trunk group (only available to those subscribers with specific authorisation).

PROXIMITY

Type of routing to use for setting links on inter-site trunk groups in service.

There are 2 options.

The above points are explained in the following examples:

TL direction

Direct routing is on the TL.

In the event that the trunk group is saturated, there is an alternative route on the public network (network change) subject to the user right "NETWORK SHIFT ALLOWED".

Public direction (long distance)

Direct routing is on the traffic + trunk group.

In the event that the trunk group is saturated, there is an alternative route on a normal public network line (rerouting), subject to the user right "NETWORK REROUTING ALLOWED".

Successive TL rerouting on TRAFFIC+ and PSN

This case may be processed by being less rigorous with regard to the terms and by firstly defining rerouting on traffic + and then changing networks to the public network.

In this case, "NETWORK SHIFT ALLOWED" and "NETWORK REROUTING ALLOWED" are applied successively.

A digit translation can be applied to each change in routing (see OUTGOING DIGIT TRANSLATOR).

Example:

Direct_1 is associated with a France Télécom trunk group and direct_2 is associated with a British Telecom trunk group. If no command is given, the France Télécom trunk group will be used as priority. However, an external command can request that this seizure order be reversed for reaching the United States or any other country, according to a calendar known to the external application (see the LCR documentation).

ON TRUNK GROUP

The trunk group field is automatically updated each time one of the first 3 parameters is modified as long as a route has already been defined. A route is erased by deleting the automatically updated trunk group route.

A complete list of trunk groups is only displayed if no route has been defined. The only other option is the **.....** trunk group. . To change the trunk group, the route must be deleted by selecting the **......** trunk group and then selecting the required trunk group.

This function helps prevent the user making mistakes, particularly the mistake of inadvertently modifying the trunk group field when reading the characteristics of the route.

6.2.2.2 *Defining a routing path*

Menu **NETWORK AND LINKS>Network>Routes**

After entering the parameters, click "Advanced characteristics" to move to the next screen.

The heading of this screen indicates the route selected: (the code if in multi-company configuration, the direction, the route, and the trunk group).

The following characteristics must then be defined:

FOR ROUTING CODE

CODE 0

This field indicates the routing code assigned to the "COMPANY/DEPARTMENT" pair.

TONE TYPE

BY FREQUENCY **BY PULSE** **DTMF/DP**

VIA IMPULS THEN FREQ **VIA IMP THEN IMP**

This field is used to define the network tones detection mode.

- DTMF: PSTN on TRK
- DP: TL or PCM in signalling code L0
- VIA IMP AND/OR REQ: both types of toneS are accepted.
- VIA IMPULS THEN FREQ: type of tone reserved for export.
- VIA IMP THEN IMP: two consecutive pulses.

TRANSMIT TYPE

DTMF **DECADIC** **SOCOTEL 1**

This field defines the dialling signal transmission mode on the network line, in accordance with the Central Office exchange characteristics (DTMF or PD).

SEND CALLING PARTY NO. (EMERGENCY)

NO **YES**

Field available for the EMERGENCY direction only.

Selecting YES sends the caller number to the path concerned for EMERGENCY direction.

DIAL TONE

NO **YES**

If you enter YES, this indicates that the system waits for reception of a dial tone before transmitting the dialling signal: case of analogue or digital (PCM) and automatic tie-line with L0 or specific signalling).

1ST SERIES OF DIGITS TO INSERT

This field is used to transmit the first prefix (if used) associated with the direction to the PSTN, (national or international prefix).

In the case of a TL or PCM link between 2 PBXs, the seize prefix for these directions can also be sent, taking account of the programming selection made in Access to directions.

Pause codes A and B can be inserted for certain export requirements.

SECOND TONE

NO **YES**

If you enter YES, this indicates that the system waits for the dialling tone to be received after the first prefix has been transmitted before transmitting the rest of the dialling signal.

2ND SERIES OF DIGITS TO INSERT

This field defines a second possible prefix associated with a direction.

Note: This field is used for export and behind the iPBX.

THIRD TONE

NO **YES**

Presence of a third tone (this option is for a future use or possibly for export).

OUTGOING DIGIT TRANSLATOR NUMBER DEPART

An outgoing digit translator is used for special routing. Enter the outgoing digit translator number (digit translators are defined in "NETWORK AND LINKS> Network> Translators).

This option can be used particularly in the case of a change of network, when the dialling carried out by the user must be modified.

CHARGE INDICATION

NO **YES**

If you select YES, a series of Beep signals will be sent to the user prompting him to hang up at the end of the charge indication timeout (this parameter is defined in “SYSTEM>Expert>Timeout”).

LIMIT NO. OF C CODE REROUTINGS

NO **YES**

In the case of multiple transit routing, enter YES, to avoid loop backs in rerouting.

Note: This field is displayed if a "Paging" direction has been defined.

STATUS DETECTION

NO **YES**

This field is only displayed if, in the case of routing to a "Paging" direction, the field is set at YES by default.

It authorises the detection of the ringing tone and/or the busy tone: to be configured according to the type of "Paging" device connected.

This field is always set at NO for directions which do not have this option.

OFF NET CARRIERS

Enter the name of the off-net carrier used for routing.

Definition:

An off net carrier is a carrier which can be accessed via a local operator.

IMPORTANT NOTE: To assign a carrier in a route, the route must have a number.

6.2.3 ROUTE DISPLAY

Note: Route display can be used to supervise outgoing routes. It cannot be used to modify their characteristics.

Menu **NETWORK AND LINKS>Network>Route display**

This screen is used to display the different routes declared and their respective parameters.

Definitions:

Call routing is based on the definition of a direction, a route and a trunk group.

- The route determines the priority of outgoing calls
- The trunk group corresponds to all the lines or time slots allowing calls to be routed to a network or external access according to a given signal.

TRSF means the translator number.

The scroll bars on top and on the right side of the << and >> screen are used to navigate to see other paths.

OUTPUT FORMAT IN MULTI-COMPANY MANAGEMENT

In multi-company management, the display screen is preceded by a field which allows you to select the routes for a routing code or for a given company.

Menu **NETWORK AND LINKS>Network>Routes>Route display**

FOR A ROUTE CODE

CODE 0

Code 0 is displayed by default. Following this, if you have created other code names, these appear on this line.

Note: For the routing code to work correctly, the field "For a company" must be set at x x x x x.

OR FOR A COMPANY

xxxxxxxx

Selecting this field means "used by other companies" (default company): it allows the display of routes for code 0 or for codes xx.

If you have created company names, these appear on this line.

Choose the name then click "**Select the item** to validate the choice.

The heading on the next screen indicates that the routing is displayed for code 0.

- The first part of the menu repeats the various uses of a routing code (only the significant lines are displayed)
- The second part describes the routing for the code selected.

The scroll bars on top and on the right side of the << and >> screen are used to navigate to see the trunk group types declared.

6.2.4 OFF NET CARRIERS

Menu **NETWORK AND LINKS>Network>Off net carriers**

The management of off-net carriers covers five different operations: naming, defining characteristics, subscription settings, viewing the subscription and viewing the routing.

6.2.4.1 *Names of off net carriers*

Menu **NETWORK AND LINKS>Network>Off net carriers>Names**

This screen is used to enter the names of off-net carriers according to the following rules.

CARRIER N (1 TO 16)

Enter a name using up to 8 characters for each carrier n (maximum 16 names).

Note: A carrier with no name cannot be managed as it does not exist for the system.

A carrier can only be deleted if the following conditions are met:

- It no longer has any route.
- It no longer appears on a route.
- It no longer has any subscription or secret code.

6.2.4.2 *Off net carrier definition*

Menu **NETWORK AND LINKS>Network>Off net carriers>Definition**

This screen is used to select an off-net carrier in order to define its characteristics.

BY NAME

Select the name of the off-net carrier you wish to define.

Then click **Select the item** to confirm your choice and move to the next screen.

This screen presents the characteristics of an off-net carriers:

SCENARIO NUMBER

Enter the number by which the scenario is identified (description of the sequence of operations requesting that information be sent with DTMF signalling).

OFF NET NUMBER

Enter the remote off net carrier number (maximum 20 digits).

MODE OF CALLED NUMBER

DTMF	**IID**	**AID**

Select a forwarding type.

Note: DTMF signalling is used on analogue trunk groups.

IID and AID signalling are used on ISDN trunk groups.

TYPE OF SUBSCRIPTION NO.

INDIVIDUAL	**IID**	**SOC-DEPT**

Select a subscription number type.

- INDIVIDUAL transmits the subscription number on the line.
- IID transmits a company's general number.
- SOC-DEPT is used to transmit a different number for each company-department.

MODE OF SUBSCRIPTION NUMBER

DTMF	**IID**	**AID**

Select a forwarding type (see the definitions in the field above).

TYPE OF CONFIDENTIAL CODE

INDIVIDUAL	**IID**	**SOC-DEPT**

Select a code type (see the definitions in the field above).

IID transmits the company number (single-company configuration).

TX MODE OF CONFIDENTIAL CODE

DTMF **IID** **AID**

Select a forwarding type (see the definitions in the field above).

ANSWER SIGNAL MANDATORY

YES **NO**

Specify the carrier answer on an ISDN trunk line.

The scroll bars on top and on the right side of the << and >> screen are used to navigate to see the operators declared.

6.2.4.3 *Subscription settings*

Menu **NETWORK AND LINKS>Network>Off net carriers>Subscription settings**

This screen is used to select an off-net carrier so as to act on the subscription parameters.

The parameters to complete for off-net carrier subscriptions depend on whether the configuration is multi-company or single-company.

6.2.4.3.1 Multi-company configuration

Menu **NETWORK AND LINKS>Network>Off net carriers>Subscription settings**

Note: In multi-company configuration, you can assign a different subscription number and confidential code for each company-department.

FOR COMPANY

Enter the company name.

Note: Use *** to validate all the companies.**

AND DEPARTMENT

Enter the department name.

Note: Use *** to validate all the company departments.**

SUBSCRIPTION NUMBER

Enter the carrier subscription number (maximum 10 alphanumeric characters).

CONFIDENTIAL CODE

Enter the carrier confidential code number (maximum 10 alphanumeric characters).

6.2.4.3.2 Single-company configuration

Menu **NETWORK AND LINKS>Network>Off net carriers>Subscription settings**

SUBSCRIPTION NUMBER

Enter the carrier subscription number (maximum 10 alphanumeric characters).

CONFIDENTIAL CODE

Enter the carrier confidential code number (maximum 10 alphanumeric characters).

The scroll bars on top and on the right side of the << and >> screen are used to navigate to see the operators declared.

6.2.4.4 *Display carrier subscript.*

Menu **NETWORK AND LINKS>Network>Off net carriers>Display subscription**

This screen is accessible via NETWORK AND LINKS>Network>OFF NET operators.

Displaying subscriptions (multi-company configuration)

This screen is used to display the list of subscriptions for a given off-net carrier.

Note: A carrier name can only be deleted if this list is empty: in this case, there are no more subscriptions belonging to the selected carrier.

The scroll bars on top and on the right side of the << and >> screen are used to navigate to see the subscribers by operator.

6.2.4.5 *Single-company route display*

Menu **NETWORK AND LINKS>Network>Off net carriers>Routing display**

This screen is used to select the routes to be displayed. Two selection criteria are available. Apply either of the criteria:

FOR ROUTE CODE

Select the corresponding code.

OR FOR A COMPANY

If applicable, select the company in multi-company configuration.

Then click **Select the item** to confirm the choice and move to the next screen used to display the routes declared by the off net carrier.

Note: A carrier name can only be deleted if this list is empty: in this case, there are no more subscriptions belonging to the selected carrier.

The scroll bars on top and on the right side of the << and >> screen are used to navigate to see the operators declared.

6.2.5 SIGNALLING

Menu **NETWORK AND LINKS>Network>Signalling**

This menu contains all the functions associated with network signalling.

6.2.6 ACTIVATION

Menu **NETWORK AND LINKS>Network>Signalling>Activation**

The following screens are used to activate only the signalling used for each type of network card present in the system.

Note: Only VoIP signals are presented on a MiVoice 5000 Server.

6.2.7 AID HANDLING

Menu **NETWORK AND LINKS>Network>AID handling**

When a call is made through the ISDN network, two items of information, called "originating numbers" may be transmitted to identify the origin of the call.

The first one, an optional item called **AID** (Additional Installation ID), contains the Caller identity supplied by the calling PBX.

The calling PBX provides this information item:

- Either the DID number at which the calling set may be called back directly. This DID number is called "AID".
- Or the general number of the system (the number of the operator switchboard) if the calling set is not a DID or does not wish to give its DID number. This general operator number is called "IID" in MIVOICE 5000 server jargon.

The following screens are used to handle all caller identification numbers, all cases of callback, and identification of calls from other networks.

6.2.7.1 *Definition of the internal plans*

Menu **NETWORK AND LINKS>Network>AID handling>Internal plans definition**

This screen is used to select the internal plans to be defined. For each plan selected, you also have to choose the type of plan: PSTN or TL.

6.2.7.2 *Composition of internal plans*

Menu **NETWORK AND LINKS>Network>AID handling>Internal plans composition**

This screen is used to assign directions to the plans declared in the system. On system reset, the carrier directions are configured for plan 1.

Note: Unless a direction is allocated to a plan, it will not appear in the list of available directions for all MMCs.
If you want to change a specific direction which belongs to a plan, that direction must not be in use.

6.2.7.3 *Convert internal plan*

Menu **NETWORK AND LINKS>Network>AID handling>Conversion internal plan - network**

This screen is used to select an internal plan and possibly to specify a trunk group.

Note: You cannot enter two exceptions for one direction.

If you change the direction, this deletes the former exception and creates a new exception with the same parameters (there is no change of the network plan or network address nature).

If you select the direction **........**, this deletes the exception.

6.2.7.4 *CONVERT INTERNAL PLAN - NETWORK PLAN*

Menu **NETWORK AND LINKS>Network>AID handling>Conversion internal plan - network**

This screen is used to select a network plan and possibly to specify a trunk group.

Click **Select the item** to confirm your selection and move to the next screen.

6.2.7.5 *IID*

Menu **NETWORK AND LINKS>Network>AID handling>IID**

If DID dialling via SDN is enabled (Menu **Subscribers menu>Rights>General settings, System** tab), DID number management must be performed from MiVoice 5000 Manager. Refer to the document “DID number management”.

DID number management must be carried out from MiVoice 5000 Manager. Refer to the document “DID number management”.

The purpose of these screens is to enter the IIDs which can, for incoming calls:

- Be associated by default with the plan or internal address nature and, possibly, with the trunk group delivering the call
- Be associated with each outgoing call according to the called party, the caller, and, possibly, the outgoing trunk group.

Note: The IID is the corporate number of the attendant consoles, and it can differ from the IID (Installation Identification) defined when the subscription to the ISDN public network access was taken out.

The entry menu is composed of an area with three lines repeated 16 times.

NDI X: INTERNAL PLAN

Select the internal plan with which the IID is associated.

Example: Plan 1, then validate.

OR DIRECTION

Select the direction with which the IID is associated.

NUMBER

Enter on this line the IID (maximum 28 digits). Do not enter 0.

RESTRICTED PRESENTATION

YES **NO**

Select YES to restrict the presentation of IID numbers.

6.2.7.6 *AID prefix*

Definition:

The AID (Additional IDentification) contains the caller identity supplied by the calling PBX.

The AID is the DID number which may be displayed on the set of the called party and which will allow future callback. To do this, define the outgoing prefix on the public network.

Example: 0, line seizure prefix, followed by 00 for the "International" direction.

By default, you must select an internal plan by name.

Menu **NETWORK AND LINKS>Network>AID handling>AID prefix definition**

This screen is used to select the internal plan concerned by the definition of prefixes.

Click **Select the item** to confirm your selection and move to the next screen.

When you have selected an internal plan, the following prefix entry screen is displayed.

No checks are made on the use of the screens for defining handling during the deletion of an exception or of the default setting.

However, you can only delete the default setting when all the exceptions have been deleted.

If you delete the direction or the prefix, this also deletes the exception.

Note: You cannot enter two exceptions for one direction.

6.2.7.7 *Outgoing handlings*

Menu **NETWORK AND LINKS>Network>AID handling>Outgoing handling**

Handling AID/IID outgoing calls consists in indicating in the "Caller Identity" information the DID number of the calling set (known as the AID), or the corporate number of the attendant consoles, (known as the IID).

The type of handling carried out depends on three parameters:

- The internal plan or direction of the calling entity
- The internal plan or direction of the called entity
- In some cases, the outgoing trunk group (infrequent)

As a result, this function is composed of three screens in cascade.

This first screen is used to enter the plan or direction of the caller.

Given the possible dependency of the various types of handling, there are several fallback levels available:

- Specified calling party plan and non-specified calling party direction
- Specified calling party direction with all possible cases for specifying the called party and, in some cases, the trunk call

Click **Select the item** to confirm your selection and move to the next screen.

Note: Set the index from 0 to 15, defined in the section “IID”, on the line IID NUMBER.

Click "Advanced characteristics" to move to the next screen.

6.2.7.8 *Incoming handlings*

Menu **NETWORK AND LINKS>Network>AID handling>Incoming handlings**

If the "Caller identity" information is filled in, the handling of the AID/IID incoming calls will concern this number.

The "Called party identity" can only be filled in by the remote PBX. In this case, the iPBX only receives the IID forced by the carrier. The handling of the AID/IID iPBX incoming calls will concern this number.

This function starts with a selection screen which is used to chose the internal plan for which the handling will be defined.

A second criterion used for very specific cases is the selection of the incoming trunk group (by default the screen takes the 0FEH "joker" value specified by the table) (infrequent).

Select an internal plan.

Click **Select the item** to confirm your selection and move to the next screen.

The screen area containing the last five columns to be filled in is repeated according to the number of directions belonging to the plan selected.

You cannot enter two exceptions for one direction.

The last four lines of the area appear once a direction is correctly entered. Furthermore, the last line is only displayed if the associated IID field is empty (handling is only applied to a received IID and not to a simulated IID).

If there is no IID, this indicates that the IID which is possibly received from the network is retained. On operator request, it can be handled in the same way as the received AID.

6.2.7.9 *Displays*

Menu **NETWORK AND LINKS>Network>AID handling>Displays**

This menu shows the available display actions.

6.2.7.10 *Outgoing handlings*

Menu **NETWORK AND LINKS>Network>AID handling>Displaying>Outgoing handlings**

The purpose of this screen is to display the existing keys in the table which defines the outgoing handling. This means ordering and displaying the existing keys taking into account the default rule.

Sorting is carried out according to the criteria in the following order:

- The calling party plan and its directions
- The called party plan and its directions
- The trunk group.

Each of the lines summarises the handling associated with each of the keys defined, taking account of the priority rule, which is respected by telephony processing.

IID: indicates the index number of the IID.

TRL AID: indicates the digit translator number.

6.2.7.11 *Incoming handlings*

Menu **NETWORK AND LINKS>Network>AID handling>Displays> Incoming handlings**

The purpose of this screen is to display the list of existing keys, taking account of the fallback rule.

Sorting is carried out according to two criteria in the following order:

- The plan and its directions
- The trunk group.

IID: indicates the index number of the IID which may be used.

PREF AID: indicates whether a prefix is added, YES or NO.

TRL AID: indicates the number of the digit translator which may be used.

Note: The prefix added for a given direction will normally be the prefix defined for the direction, and if the prefix is not defined, the prefix defined will normally be for the plan the direction belongs to. Handling is carried out even if the direction is not defined explicitly as an exception at the level of the previously described screens.

6.2.7.12 *Conversion internal plan - network*

Menu **NETWORK AND LINKS>Network>AID handling>Displays>Internal plan - network**

6.2.7.13 *Conversion network plan - internal*

Menu **NETWORK AND LINKS>Network>AID handling>Displays>Network plan - internal**

6.2.8 TRANSLATORS

Menu **NETWORK AND LINKS>Network>Translators**

Digit translator management concerns:

- Translations to be carried out of the called numbers for a given routing (direction, route, trunk group)
- Translations of the calling number (AID) to be sent to the network
- Translations to be carried out of the called numbers on an incoming trunk group
- Translations of the calling number (AID) received from the network
- Translation of operations carried out behind the PBX into telephone events (Flash, dialling)

6.2.8.1 *Outgoing: called party number*

Menu **NETWORK AND LINKS**>NETWORK>TRANSLATORS>OUTGOING: CALLED PARTY NUMBER

The outgoing digit translators are used in the case of TL transit or a network change.

The called party number is assigned to the trunk group in the routing definition on this trunk group. Access is by the digit translator number (0 to 47).

Select a translator number, in our example No. 1.

Click **Select the item** to confirm your selection then move to the next screen and define the following parameters:

DIGIT TO TRANSLATE

The digit to translate (10 characters) indicates the start of the numbering which must be deleted. AND DIGITS indicates the new numbering which must be inserted in place of the deleted numbering.

Letters can also be used. Each letter indicates a random digit of rank i (example: 1A3 includes numbers 103, 113, 123, ..., 193).

The letters contained in the digit to be translated must start with the letter A and then continue in alphabetical order.

The letters which figure in the translated item must also exist in the item to be translated.

TO DIRECTION

List of directions.

AND DIGITS

This indicates the characters which end in the number of digits transmitted, noted between brackets.

Example 1:

- deletion of the first 3 digits and transmission of the last 2
- digit to translate ABC
- digit translated (2)

Example 2:

- addition of 2 digits at the start of the numbering, independent of the numbering itself
- digit to translate A
- translated digit 12A(8)

The line FOR ROUTE CODE is only available in multi-company configuration. The trunk group seizure prefixes are not part of the numbering. On system start up, the translation is zero.

- Digit to translate 1234
- To direction NATIONAL
- and the number 1234(18)

An empty translation is allowed but the brackets are always mandatory.

6.2.8.2 *Outgoing: calling party number*

Menu **NETWORK AND LINKS>Network>Translators>Outgoing: calling party number**

Select a translator number, in our example No. 1.

Click **Select the item** to confirm your selection then move to the next screen and define the following parameters:

- Digit to translate (8 characters)
- to plan (list of plans)
- or to direction (list of directions)
- and digits (16 digits)

Note: See explanations "Outgoing: called party number".

6.2.8.3 *Incoming: called party number*

Menu **NETWORK AND LINKS>Network>Translators> Incoming: called party number**

Incoming digit translators are used particularly for DID, when the MCDU (last four digits of the telephone number) received from the public network must be modified or truncated.

The incoming digit translator is associated with a trunk group and identified by its number in the trunk group characteristics.

Access is by the digit translator number (1 to 48).

Select a translator number, in our example No. 1.

Click **Select the item** to confirm your selection then move to the next screen and define the following parameters:

Letters are used following the same rules as for outgoing translations.

DIGIT TO TRANSLATE

Enter the MCDU number (digits or letters) to be translated.

RESULTING DIGITS

This line appears when a value has been entered on the previous LINE.

Enter the digit to replace the digit to be translated.

Example:

- "internal" user directory number 5300 to 5499
- DID call number 01 30 14 13 00 to 01 30 14 14 99: (digits received 1300 to 1499)
- digit to translate: 13AB Resulting digits: 53AB or 1A -> 5A

or:

- digit to translate: 14AB Resulting digits: 54AB or 1A -> 5A

1A and 5A contain the 2 hundred units, and the last 2-digit group (DU) is transparent.

The DU of the internal directory number must be the same as the DU of the DID directory number.

Note: An incoming digit translator is used for DID or TL if the digit received does not correspond to the internal or DID directory number.
An ISDN DID number must never be translated (except for a transit operation), to ensure that the caller number (AID) is sent correctly by the PBX.

6.2.8.4 *Incoming: calling party number*

Menu **NETWORK AND LINKS>Network>Translators> Incoming: calling party number**

These translators are used to translate the IID/AID received from the network (to be added in the incoming processing).

DIGIT TRANSLATOR NUMBER

Indicate the translator number you wish to work with (the translator number you indicated previously).

There are 48 digit translators, each featuring 16 digits to translate

Letters are used following the same rules as for outgoing translations

Click **Select the item** to confirm your selection then move to the next screen and define the following parameters:

DIGIT TO TRANSLATE

Enter the digit to be translated.

TO PLAN

PLAN 1

Enter the relevant dialling plan.

OR TO DIRECTION

• • • • • • | **NETWORK** | **NATIONAL** | **REGIONAL** | **INTERNATIONAL**

Select the direction which will receive the digits to be translated.

Note: …….. means all directions.

AND DIGITS

Enter the digit to replace the digit to be translated (16 digits).

Note: The first part of the received number (excluding the prefix) is translated first of all. Then the last digits, which are not specified, are sent at the end of the operation without being translated.

6.2.9 TRANSFERS/TRANSITS AUTHORISATIONS

Menu NETWORK AND LINKS>Network>Transfers/transits authorization

Definition:

This menu defines the trunk group pairs for which transit or transfer can be allowed or forbidden (depending on the configuration of the general settings):

- Forward an “incoming” call to an external extension A call received from the network that has already been diverted to an external number,
- Transit between 2 PBXs: External call to an external number,

Two tabs:

- Create
- Display/Delete

6.2.9.1 *Creation tab*

Menu **NETWORK AND LINKS>Network>Transfers/transits authorization**

When the trunk group pairs are being configured, two lines in read-only mode are used to give the operating mode for transfers and transits:

TRUNK GROUP CONFIGURATION

The following lines have a direct link to Menu **Subscribers>Rights>General settings** to allow the modification of the trunk group list operating mode:

- For transfer (Right tab)

- For transit (Network tab)

The fields are greyed out and inaccessible.

See Menu **SUBSCRIBERS>Rights>General settings** for how to define the transfer (or transit) authorisation according to trunk group pair:

- AUTHORISATION LIST
- PROHIBITION LIST
- LIST NOT USED

The trunk groups to be declared do not necessarily belong to the internal site: each trunk group must be definable.

PRIMARY: SITE

Enter the name of the primary site in the list.

NODE

Enter the node number (2 digits).

In a multi-site configuration, the current value of the node is 02.

TK GROUP NUMBER

Enter the trunk group number (2 digits).

To know the trunk group number, go to Menu **Telephony service>Network and links >Network>Trunk groups>Names**.

SECONDARY: SITE

Enter the name of the secondary site in the list.

NODE

Enter the node number (2 digits).

In a multi-site configuration, the current value of the node is 02.

TK GROUP NUMBER

Enter the trunk group number (2 digits).

To know the trunk group number, go to Menu **Telephony service>Network and links >Network>Trunk groups>Names**.

6.2.9.2 *Display/delete tab*

This menu gives a list of the trunk group-sites-node pairs identified by a declaration number on the list.

These pairs define the authorised or forbidden transfers and transits according to the choice of use of this list made in Menu **SUBSCRIBERS>Rights>General settings**, **Right** tab for transfers and **Network** tab for transits.

DELETE TRANSFER OF TRANSIT NO X

The menu proposes for each list input a checkbox for deleting the list input.

The transfer/transit number to delete is identified by its order number.

Click CONFIRM to confirm the deletion.

6.3 MULTI-SITE

Note: All the settings associated with the creation and activation of a multi-site configuration. Please refer to the document MIVOICE 5000 - Multi-site management.

6.4 QUALITY OF SERVICE

Quality of de Service (QoS) is the ability to route in good conditions a given type of traffic, in terms of availability, flow rate, transit delay, and rate of packet loss.

Menu **NETWORK AND LINKS>Quality of service**

6.4.1 SPECIFIC ENCODING LAWS

Menu **NETWORK AND LINKS>Quality of service>Specific coding laws**

This menu is used to define at most 4 specific encoding laws, and to configure the video and Fax T38 throughputs.

Specific law name x: The name of a law is defined by an ascii string comprising a maximum of 20 characters.

Note: To define a name, take for instance in an SIP INVITE frame, field "Media Attribute (a):rtpmap: " and copy the ASCII character string after the Payload.

No check is made on the characters entered.

Throughput (kb/s): **Throughput value** for the 4 specific laws. This field is only displayed if the name of the corresponding law has been entered.

The values authorised are between 0 and 65279 (Kbits/s).

No check is made on the values entered.

6.4.2 VOICE OVER IP ENCODING LAW

Menu **NETWORK AND LINKS>Quality of service>Voice over IP coding law**

Choice of different call types

- Call type
- INTERNAL
- NETWORK
- PRIVATE DIRECTION
- MULTISITE SVL-IP
- OTHER SERVERS
- ISDN S0 S2
- CONFERENCE CIRCUITS

- ANNOUNCEMENTS
- VOICE MAIL

For an **INTERNAL** call, the column SET TYPE is displayed.

SET TYPE: **Options** proposed

NON-IP SET	Default terminal. TDM terminal using a VOIP (analogue, digital)
H.323 TERM	Terminal or PC with integrated telephone using the H323 protocol
IP_OWNER	Proprietary IP terminals (i7xx and MiVoice 5300 IP Phone
DS_ON_PC	Dedicated terminal on PC (VoIP mode i2052 SoftPhone)
VTI/XML IP	Servers using multiplexed VTI/XML sessions over IP (UCP, CC, TWP, etc.).
SIP-DECT IP	SIP phone (MiVoice 6000 SIP Phone, Standard SIP SoftPhone and DECT/IP)

IMPORTANT NOTE: Terminal coding law configuration is available by default: during normal operation, the preferred laws are those defined on the PBX and supported by the terminal (see the table below which gives the default values).

For a **NETWORK** call, the Direction column is displayed.

Direction: proposed options

……	Encoding laws defined by default for all the network directions (LOCAL, REGIONAL, INTER, etc.).
NATIONAL	Encoding laws defined for the LOCAL direction only
REGIONAL	Encoding laws defined for the REGIONAL direction only
INTER	Encoding laws defined for the INTERNATIONAL direction only

WARNING: If the default "……" is changed, all "NETWORK" directions without any explicitly defined coding laws are affected.

For a **PRIVATE NETWORK** call, the **Direction** column is displayed.

Direction: Options proposed

……	Encoding law defined by default for all the private directions (TLXX), including for the TL0 direction.
TL X	Encoding laws defined for the TL X direction only

WARNING: If the default "……" is changed, all private directions without any explicitly defined coding laws are affected, including for the TL0 direction.

For a **MULTISITE SVL-IP** call, the **Site** column is displayed.

SITE: Options proposed

……	Encoding laws defined by default for the IP link server (applies to SVL links defined between the local site and all the remote sites). Law G729 20 ms is used by default.
SITE X	Encoding laws defined only for the SVL IP link between the local site and the remote site X.

For a **TONES** call, the TYPE OF MESSAGES column is displayed.

MESSAGES TYPE: **Options** proposed

NETWORK	This profile applies to the VoIPs or media server resources used to broadcast an announcement or a message for an external call (especially for pre-off-hook, network on-hold). G711, G723, G729 and P729/PRIV. G729 are proposed.
SUBSCR	This profile applies to VOIPs or to the media server resources used to broadcast an announcment or a message to an internal call. G711, G723, G729 and P729/PRIV. G729 are proposed.

After making the selection correctly, click **Select the item** to go to the coding law definition screen.

You can define up to 7 different encoding laws. They include:

CODING LAW	COMMENTS
G711/AUDIO G711	
P711/PRIVEE G711	Reserved for the MULTISITE SVL-IP profile
G723/AUDIO G723	
P723/PRIVEE G723	Reserved for the MULTISITE SVL-IP profile
G729/AUDIO G729	
P729/PRIVEE G729	Reserved for the MULTISITE SVL-IP and LOCAL/NON IP profiles
G722/AUDIO G722	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP, LOCAL/PROPRIETARY IP profiles In R5.3 SP1 and later: also applies to the CONFERENCE CIRCUITS profile ASof R 5.4: Applies to NETWORK and SUBSCRIBER profiles
OPUS	Reserved for the NETWORK, PRIVATE_DIRECTION, CONFERENCE CIRCUITS, TONES, VOICE MAIL, INTERNAL/SIP-DECT IP profiles.
G719	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G7221 16 24	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G7221 16 32	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G7221 32 24	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G7221 32 32	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G7221 32 48	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G726 16	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G726 24	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G726 32	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G726 40	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G728	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
G729E	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
BV16	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
BV32	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
GSM	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
GSM EFR	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
ILBC 20	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles
ILBC 30	Reserved for the NETWORK, PRIVATE DIRECTION, LOCAL/SIP-DECT IP profiles

Each encoding law can contain up to 2 sub-laws and can have up to 4 different rates.

CODING LAW	NUMBER OF SUB-LAWS	FROM THE SUB-LAWS BELOW	NUMBER OF POSSIBLE PACKET SIZES	INCLUDING THE FOLLOWING PACKET SIZES
G711/AUDIO G711, P711/PRIVATE G711	2	A LAW, MU LAW	2	10, 20, 30MS
G723/AUDIO G723, P723/PRIVATE G723	1	G723.1	2	30, 60 MS
G729/AUDIO G729, P729/PRIVATE G729 **(1)**	2	A LAW, G729	4	10, 20, 30, 40 MS
G722/AUDIO G722 G719 G7221 16 24 G7221 16 32 G7221 32 24 G7221 32 32 G7221 32 48 G726 16 G726 24 G726 32 G726 40 G728 G729E BV16 BV32 GSM GSM EFR ILBC 20 ILBC 30	0	/	4	10, 20, 30, 40, 50, 60 MS

(1) : For the encoding law Audio G729, it is mandatory to:

- SYSTEMATICALLY mention the two sub-laws G729 and G729A
- Put them in the same order in all the profiles containing this law.

For the OPUS coding law:

- Sub-law and flow rate settings are not programmable.
- Only OPUS-enabled phones can use it.

OTHER INFORMATION ABOUT PROFILES

"ISDN S0/S2" PROFILE

This profile applies to the VoIPs taken for a number dialled from an S0/S2 terminal.

"CONFERENCE CIRCUITS" PROFILE

This profile applies to the VoIPs taken by a 3-way conference bridge.

In R5.3 SP1 and later: This profile also applies to the media server taken to make a 3-way conference.

"OTHER SERVERS" PROFILE

This profile applies to the VoIPs taken for all the servers, except:

- The link server (which has its own "MULTI-SITE" profile)
- The voicemail server (which has its own "VOICEMAIL" profile)

In practice, this profile is rarely used.

RECOMMENDATIONS

- Except for the "NETWORK" and "PRIVATE DIRECTION" profiles, it is very advisable to configure the encoding laws in the same way for all the sites.

DEFAULT VALUE (AFTER A FIRST INSTALLATION)

CALL TYPE	L.1	L.2	L.3	L.4	L5	L6	L.7
Conference circuit	G711 A & U 20 / 30 MS	G729 & 729A 20 / 30 / 40 MS	....	....	....	....	....
Local non-ip terminal	G711 A & U 20 / 30MS	G729 & 729A 20 / 30 / 40MS	....	....	....	....	....
Local DS on pc	G711 A & U 20 / 30MS	G729 & 729A 20 / 30 / 40MS	....	....	....	....	....
Local Vti/xml ip	G711 A & U 20 / 30MS	G729 & 729A 20 / 30 / 40MS	....	....	....	....	....
Local sip-dect ip	G722 20 / 30 MS	G711 A & U 20 / 30MS	G729 & 729A 20 / 30 / 40 MS	....	....	....	....
Local proprietary ip	G722 20 / 30 MS	G711 A & U 20 / 30MS	G729 & 729A 20 / 30 / 40 MS	....	....	....	....
Network	G722 20 / 30 MS	G711 A & U 20 / 30 MS	G729 & 729A 20 / 30 / 40 MS	....	....	....	....
Private direction	G722 20 / 30 MS	G711 A & U 20 / 30MS	G729 & 729A 20 / 30 / 40 MS	....	....	....	....

After an upgrade to R5.3 from an earlier release (R5.2 or R5.1), the configuration of the encoding laws are kept.

Order of priority for coding laws:

To change the order of priority of the coding laws applied:

- On the **Law displacement** line, click:

- The ↑ button to raise the priority of the law;
- The ↓ button to lower the priority of the law.

6.4.3 DISPLAY ENCODING LAWS

Menu **NETWORK AND LINKS>Quality of service>Coding laws display**

G711, G723 and G729 correspond to AUDIO laws G711, G723 and G729.

P711, P723 and P729 correspond to PRIV. laws G711, G723 and G729.

OPUS: Reserved for NETWORK, PRIVATE_DIRECTION, CONFERENCE CIRCUITS, TONES, VOICE MAIL, INTERNAL/SIP-DECT IP profiles.

Clicking a call type gives direct access to the law definition menu for this call type.

6.4.4 NEGOTIATE ENCODING LAWS

Calls are set up in 5 phases:

1. The calling end IP terminal interface presents its list of coding laws *(for TDM terminals the IP interface is the associated VOIP)*.
2. This list is filtered by the law profile associated with the caller type: only common laws are kept and arranged according to the profile configuration. The duration of packets is replaced.
3. The encoding laws associated with the called terminal is recovered.
4. A list of common laws between these two sites is determined, and the laws not authorised by the CAC withdrawn.

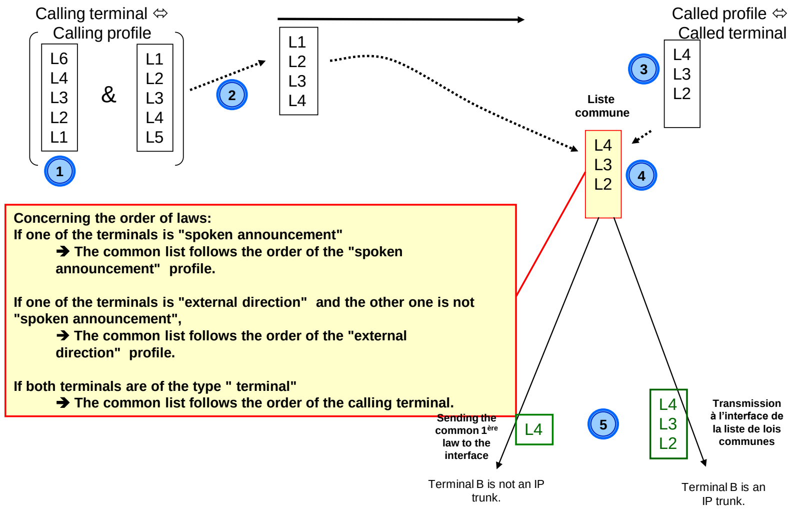
Concerning the order of laws:

- If one of the terminals is "spoken announcement" the common list follows the "spoken announcement":
- If one of the terminals is "external direction" and the other one is not "spoken announcement": the common list follows the "external direction" profile order.
- If both terminals are of "terminal" type and the called party is not associated: the common list follows the "calling terminal" profile order.
- If both terminals are of "terminal" type and the called party is associated: the common list follows the calling terminal profile order.

5. The following are transmitted to the called terminal:
   a. The common list when the call is presented to an IP TRUNK (SIP or H323)
   b. The first law of the common list in the other cases.

The diagram below summarises the negotiation made by the iPBX and specifies the order of laws used to create the common list:

Terminal A calls terminal B



Concerning the order of laws:
If one of the terminals is "spoken announcement"
➔ The common list follows the order of the "spoken announcement" profile.

If one of the terminals is "external direction" and the other one is not "spoken announcement",
➔ The common list follows the order of the "external direction" profile.

If both terminals are of the type " terminal"
➔ The common list follows the order of the calling terminal.

6.4.5 CAC AND LOCATION

The services proposed by the CAC server are as follows:

- Call Admission Control

  The CAC server provides a mechanism for controlling the bandwidth and flows to avoid system overload (which happens when the available bandwidth is insufficient to deal with the required flow).

Note: For a detailed description of this service and the configuration of the CAC server, see CAC Programming Guide.

- Geographic location

  This service is used to:

  - Define special numbers based on geographical location,
  - Route external calls,
  - Manage emergency calls (routing and calling back)

The CAC AND LOCALISATION menu is used to configure these services as well as the items they use, such as breakdown into IP subnets, the definition of the CAC classes and geographic locations.

Menu **NETWORK AND LINKS>Quality of service>CAC AND LOCALISATION**

Definitions:

CAC Centre

A CAC centre is a set of sites grouped together into one or more centres with no IP throughput restriction between them. By convention, the number of the CAC centre is that of the centre where the main CAC server is located.

CAC class

A CAC class represents one or more IP subnets belonging to the same centre.

IP subnet

The IP network is divided into IP subnets so that some flow restrictions between the various subnets can be defined and so that IP sets can be located geographically when making emergency calls.

Note: These definitions apply to multi-site configuration. However, it is possible to define a CAC server in single-site configuration by dividing the network into IP sub-networks to control calls inside the site.

6.4.5.1 *CAC server settings*

Menu **Network and links>Quality of service>CAC and localisation>CAC server settings**

This command is used to:

- Declare the CAC server (primary or secondary)
- Define the services available (location, call control)
- Define the parameters for call control
- Define the centres managed by this server.

ACTIVE: XXXXXXXX, BACKUP: YYYYYYYY

This line is read only. It shows the names of the sites where the CAC server and backup server are located.

SERVER CONFIGURATION

MAIN **SECONDARY** **……..**

Select the CAC server configuration.

MAIN	The CAC server is the main server.
SECONDARY	The CAC server is the backup server.
……..	The CAC server is considered to be inexistent.

IMPORTANT NOTE: This parameter shows the static status of the CAC server (Main or Secondary) whereas the first line displayed on the screen shows the dynamic status of the CAC server (Active or Backup).

SERVICES OFFERED

- GEOGRAPHIC LOCATION

This checkbox is used to manage emergency and external calls; in this case according to the geographic location of the calling set (number translation and routing as close as possible to the calling set).

- CALL CONTROL

This checkbox is used to activate call admission control.

CONTROL BASED ON CLASS

Checkbox to be ticked if class-based control must be activated.

Note: This parameter is only available if the "call control" service is activated.

AUDIO/VIDEO SEPARATION

Checkbox used to activate or deactivate audio/video flow separation.

In separation mode, the text indicates that the saturation concerns audio only.

AUDIO SATURATION BEFORE ALARM (IN %)

In global mode, the field is as follows:

SATURATION BEFORE ALARM (IN %)

Values between 0 and 100.

This setting defines the critical rate which triggers the transmission of messages to the logbook as from a specific bandwidth occupation rate.

Note: This parameter is only available if the "call control" service is activated.

Note: The following columns only appear if the iPBX is used in multi-site mode.

FORCE REALIGNMENT OF MANAGED SITES

YES **NO**

This line allows the operator to generate the sending of an update message to all sites and centres in order to reset all location information (CAC classes, CAC centre, location number) in case of malfunctions.

CENTRES MANAGED BY THE SERVER

CENTRE XXXXXXXX:

YES **NO**

These columns are used to define a list of the centres managed by the CAC server of the local site.

Select YES for the centres managed by the CAC server.

Note: Only the available centres which have no limited throughput for contacting the local centre are proposed (that is, all the centres forming a CAC centre. This means that for a particular centre to be displayed, at least one access must be declared to access that centre (it is not sufficient merely to declare its name or a gateway leading to the centre) and the throughput to this centre must be infinite. The local centre is always proposed on this list.

6.4.5.2 *CAC Classes*

Note: CAC classes are defined only in the sites where the main and secondary servers are located.

6.4.5.2.1 Class names

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation>CAC classes>Names**

The CAC class definition menu is used to define a maximum throughput authorised per CAC class and to specify whether this CAC class manages VoIP header compression. It can be used to define up to:

- 3000 CAC classes, for MiVoice 5000 systems,

The CAC classes are declared on the site hosting the CAC server but are used on all the sites.

The CAC server will be declared on MiVoice 5000 Server and will allow the declaration of 3000 CAC classes.

Interoperation:

Creating more than 254 classes is not prohibited on an older version of MiVoice 5000, but a warning message will be displayed when an operator defines the name of a CAC class ≥ 255 on a MiVoice 5000 Server set to interoperation mode.

A link gives direct access to the management of these characteristics, by clicking the class in question.

6.4.5.2.2 Characteristics of a CAC class

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation>CAC classes>Characteristics**

BY ITS NAME

- Select the class from the options
- Click Select the item to access the configuration menu for this class.

ASSETS: XXXXX, EMERGENCY: YYYYY

This line shows the names of the sites where the CAC server and backup server are located.

VPN OR SBC ATTACHED TO THE CLASS

A list of options offers the configuration of the CAC class to which it is attached (where the VPN server is located).

The classes presented on the list as transit (membership) classes must meet the following conditions:

- They must have a defined global data rate.
- They should not have a specific transit class of their own (no cascade transit), the class will not appear on the list.

For the classes defined as transit class, the line will not appear on the menu. Once attached, this class cannot be attached.

MAXIMUM DATA RATE (KB/S)

This first line only appears in audio/video flow non-separation mode and indicates the maximum data rate authorised for video and audio (in Kbits/s) for the corresponding CAC class. This data rate may be between 0 and 65279 kbit/s. As a CAC class is used to set a limited throughput for a set of IP terminals managed by a CAC server, the throughput MUST be defined. A CAC class with no throughput is considered to be inexistent.

The AUDIO part

MAXIMUM DATA RATE (KB/S)

This line appears in audio/video flow separation mode and indicates the maximum data rate authorised for audio (in Kbits/s) for the corresponding CAC class. This data rate may be between 0 and 65279 kbit/s. As a CAC class is used to set a limited throughput for a set of IP terminals managed by a CAC server, the throughput MUST be defined. A CAC class with no throughput is considered to be inexistent.

VOIP HEADER COMPRESSION

Checkbox indicating whether the transport protocol on the WAN link compresses IP headers.

Note: Flow rate calculation takes into account the size of IP packets: payload + VOIP (RTP/UDP/IP) header, but it does not take account of the transport overhead on the WAN managed by the routers and protocols used (PPP, ATM, Frame Relay, etc.).

HIGH RATE AUDIO CODECS

Checkbox: when unticked, it indicates that the high rate audio codec is not accepted.

When the box is ticked, the restriction threshold is set to 0 (codec authorised until the link is saturated). In this case, the high-rate codec is used without any restriction.

Restriction threshold:

Thresholds are provided in kbits/s. To authorise a high-rate audio codec, the remaining available data rate on the link must be above this threshold. The value of the threshold may be between 0 and 65279 Kbits/s. Leaving the field blank means that the broadband audio codec is not accepted.

The VIDEO part

Checkbox: failing to tick the box means that the video codec is not accepted, neither in intra class nor in inter class.

MAXIMUM DATA RATE (KB/S)

This line appears in audio/video flow separation mode and indicates the maximum data rate authorised for video (in Kbits/s) for the corresponding CAC class. This data rate may be between 0 and 65279 kbit/s. As a CAC class is used to set a limited throughput for a set of IP terminals managed by a CAC server, the throughput MUST be defined. A CAC class with no throughput is considered to be inexistent.

Intra CAC class

- Data rate by comm. (kb/s):
  - Field blank by default when the function is activated: no video flow rate restriction
  - Value 0: intra-class video not allowed
  - Value: maximum value used per call (max. 65279)

Inter CAC class

- Data rate by comm. (kb/s):

By default: reminder (read only) about the default video data rate assigned in the "Specific coding laws" menu.

Other value:

- Field blank by default when the function is activated: no video flow rate restriction
- Value 0: inter-class video not allowed
- Value (in increments of 32): maximum value used per call (max. 65279)

- Restriction threshold:

  The threshold is given in kbits/s. To allow inter-class video, the available data rate on the link must be above this threshold

  - Value 0: default value when the function is activated; no restriction until the link is saturated
  - Value entered: threshold in kbits/s (max.value is 65279). To allow inter-class video, the available data rate on the link must be above this threshold.

6.4.5.3 *High bandwidth laws*

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation>High bandwidth laws**

This menu is used to configure the laws considered as high-speed laws by the CAC which will be filtered when the throughput reaches a certain threshold. The list may be displayed in ascending or descending order, by clicking the column header.

By default, the laws whose data rate is above or equal to 24 kbits/s are considered as high bandwidth laws (box ticked).

6.4.5.4 *Locations*

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation>Locations**

This menu is used to declare the geographic locations and assign them a code that will be used for special number translation. The codes must first be defined via the menu **DIALLING PLAN>Special numbers>Special numbers code names**. Each location will then be associated with an IP subnet, enabling the calling set to be located during a call using its IP address.

6.4.5.4.1 Names

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation> Locations>Names**

To declare the geographic location names, click “Names” from Menu **NETWORK AND LINKS>QUALITY OF SERVICE>CAC SERVICES>Locations>Names**:

LOCATION 0 TO 249

Name of each location.

Up to 250 geographic locations can be defined.

6.4.5.4.2 Characteristics

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation>Locations>Characteristics**

To associate a special numbers code with a location, click "Characteristics" from the "Locations" menu:

BY ITS NAME

Select the name of the location. The drop-down list contains the names of the locations declared.

Click **Select the item**:

ACTIVE: XXXXXXXX, BACKUP: YYYYYYYY

This line is read only. It shows the names of the sites where the CAC server and backup server are located.

SPECIAL NUMBERS CODE

Select the name of the code to associate with the location. The drop-down list contains the names of the locations declared.

6.4.5.5 *Definition of IP subnets*

Menu **NETWORK AND LINKS>Quality of service>CAC and localisation>IP subnets**

The IP network is divided into IP subnets so that throughput restrictions between the various subnets can be defined and so the sets can be located geographically when handling emergency calls.

The IP subnet definition menu is used to create, display or delete an IP subnet.

For each IP subnet, the following location information items are set:

- The subnet centre determined by the IP address used by the IP set to connect.
  This information is used for bandwidth control only. It identifies the CAC server to contact when a call is set up and is used to manage inter-centre flows.

Note: A subnet can only belong to one centre.

- The CAC class.
  A CAC class represents one or more subnets. The CAC class to which the subnet belongs is set when the subnet is declared.

Note: A subnet can only belong to one CAC class. Several subnets can belong to the same CAC class.

- The geographic location associated with the subnet.
  This is used to determine the number translations to apply to the special numbers dialled by a set located on the subnet.

- The site/ node pair to which the subnet is attached.
  It is used to determine the site and routing node (routing tables read) of the special and external numbers dialled by a terminal located on the subnet.

- The location number of the subnet in EMERGENCY configuration only (location terminal) is used to define - on a geographical location basis - a so-called "emergency call-back" terminal:

  - used in the case of SIP operators to send an AID identifying precisely the geographical location

  - Used to call back "non DID" users who have dialled an emergency number.

IP ADDRESS

Enter the IP address of the router or of an IP set.

Click **Advanced characteristics…** to move to the next screen and define the following settings: **MASK**

Select the subnet mask.

ACTION

……….	CREATE	MODIFY	DELETE

Select an action for the mask selected.

CREATE	Creates the subnet defined by the selected IP address/mask pair (the only action possible if the mask entered is not the mask of a subnet already displayed).
MODIFY	Modifies the selected IP address/mask pair (action possible if the mask entered is the mask of a subnet displayed).
DELETE	Deletes the selected IP address/mask pair (action possible if the mask entered is the mask of a subnet displayed).

When the action has been selected press Enter to confirm.

Click "Advanced characteristics…" to move to the next screen and define the following settings:

ASSETS: XXXXX, EMERGENCY: YYYYY

This read only line shows the current status of the CAC server.

IP ADDRESS

Information field indicating the IP address of the selected IP subnet.

MASK

Information field indicating the mask of the selected IP subnet.

CONTAINS IP ADDR IP FROM TO

Information field indicating all the IP addresses contained in this subnet presented by its base stations.

CAC CLASS

Enter a CAC class associated with this subnet. Two read-only lines are displayed indicating the maximum throughput assigned to this class, according to the mode:

In audio/video flow separation mode

- Maximum audio throughput (kb/s)
- Maximum video throughput (kb/s)

In audio/video flow non-separation mode

- Maximum throughput (kb/s)

The "**restriction threshold**" lines only appear if a threshold value is entered. These lines are read-only lines (high-rate audio and video).

The class-related data is accessible when zoomed in by placing the cursor over the class.

LOCATION

Name of the geographic location associated with the IP subnet. The drop-down list contains the names of the locations declared.

- SITE NUMBER / NODE NUMBER / TERMINAL

These lines are used to select a location terminal by IP subnet and indicate the site/ node on which is located the associated subscription, and to show whether this subscription is a "callback terminal for emergency calls".

If the SITE NAME field is empty, the routing site is the local site.

Note: In this menu the lines associated with call control (CAC class) or location (location, site name and terminal) are always shown, regardless of the offered services configured in the CAC server parameters.

6.4.5.5.1 Importing/Exporting IP subnets

IP subnets can be imported and exported using the MMC import/export function specifically designed for IP subnets.

TO EXPORT IP SUBNETS

Menu **Telephony service>Network and links>Quality of service>CAC and localisation>Subnet IP**:

- Click the button.

MiVoice 5000 Web Admin downloads a .csv file containing all the subnets and their configuration.

TO IMPORT IP SUBNETS

Importing subnets requires editing the .csv file retrieved when exporting IP subnets.

- On the .csv file:
  - Open the .csv file in a spreadsheet.
  - If necessary, make the required changes to the configuration of the subnets exported previously.
  - In the Action column, note the commands that MiVoice 5000 Web Admin must carry out during import for each subnet. Three commands are possible.
    - **MODIFY:** if the subnet already exists on the target MiVoice 5000, edit the subnet. configuration on the MiVoice 5000 to apply the configuration saved in the .csv file.
    - **CREATE**: if the subnet does not exist on the target MiVoice 5000, create a new subnet with the configuration saved in the .csv file.
    - **DELETE**: removes the subnet from the list of subnets to be imported on the target MiVoice 5000.

WARNING: Use the correct case for commands in the Action column to ensure proper subnet import.

  - Save the .csv file.
- On MiVoice 5000 Web Admin, import can be carried out in two ways:
  - Via Menu **Telephony service>Network and links>Quality of service>CAC and localisation>Subnet IP**
    - Click the button.
    - Follow the procedure described in Section **2.3.3.2 - Importing data in the context.**

- Menu **Telephony service>System>Software maintenance>Massive import**
  - Check that the Import type field is set to **GENERIC**.
  - Click the button next to **File to import** to open the file manager.
  - Select the .csv file to import.
  - Click **Download**. New fields appear:
  - Tick the **Backup contents** box to generate a backup file before importing the data (recommended).
  - Click **Inclusion of data** to start importing the data.

Note: At the end of the procedure, a pop-up window appears with a report summarising the imported subnets and any import errors. If errors occur, open the .csv file to check for any modification errors or whether the Action column has the correct command.

6.4.5.6 *Data rates towards centres*

Menu **NETWORK AND LINKS>Quality of service>CAC and localisation> Data rates to the centres**

This command is used to define the maximum throughput to centres not managed by the CAC server.

In the drop-down menu, select the name of the centre to be modified. The next screen displays the parameters of this centre. It is possible to change from one centre to the other using the ⇦ and ⇨ command buttons.

ASSET: XXXXX, EMERGENCY: YYYYY

This information line shows the names of the sites where the server and backup server are located.

TO *CENTER NAME*, MAX THROUGHPUT

Maximum throughput authorised for this centre (between 0 and 65279 Kbits/s).

The default flow is infinite (field empty).

Note: Only the available centres not managed by the CAC server are proposed. For a particular centre to be displayed at least one access must be declared to access that centre. It is not sufficient merely to declare its name or a gateway leading to the centre.

OR ATTACHED TO

Shows the attachment centre if the link is not direct (transit centre). The flow applicable is that of the attachment centre.

Example: If the link between centre A and centre C transits via centre B, then the attachment centre is centre B and the flow applicable is that of centre B. The flow for centre B must be defined on the previous line.

Note: Only one transit centre is authorised.

MAXIMUM DATA RATE (KB/S)

This first line only appears in audio/video flow non-separation mode and indicates the maximum data rate authorised for video and audio (in Kbits/s) for the corresponding CAC class. This data rate may be between 0 and 65279 kbit/s. As a CAC class is used to set a limited throughput for a set of IP terminals managed by a CAC server, the throughput MUST be defined. A CAC class with no throughput is considered to be inexistent.

The AUDIO part

MAXIMUM DATA RATE (KB/S)

This line appears in audio/video flow separation mode and indicates the maximum data rate authorised for audio (in Kbits/s) for the corresponding CAC class. This data rate may be between 0 and 65279 kbit/s. As a CAC class is used to set a limited throughput for a set of IP terminals managed by a CAC server, the throughput MUST be defined. A CAC class with no throughput is considered to be inexistent.

VOIP HEADER COMPRESSION

Checkbox indicating whether the transport protocol on the WAN link compresses IP headers.

Note: Flow rate calculation takes into account the size of IP packets: payload + VOIP (RTP/UDP/IP) header, but it does not take account of the transport overhead on the WAN managed by the routers and protocols used (PPP, ATM, Frame Relay, etc.).

HIGH RATE AUDIO CODECS

Checkbox: when unticked, it indicates that the high rate audio codec is not accepted.

When the box is ticked, the restriction threshold is set to 0 (codec authorised until the link is saturated). In this case, the high-rate codec is used without any restriction.

Restriction threshold:

Thresholds are provided in kbits/s. To authorise a high-rate audio codec, the remaining available data rate on the link must be above this threshold. The value of the threshold may be between 0 and 65279 Kbits/s. Leaving the field blank means that the broadband audio codec is not accepted.

The VIDEO part

Checkbox: when unticked, it means that the video codec is not accepted.

MAXIMUM DATA RATE (KB/S)

This line appears in audio/video flow separation mode and indicates the maximum data rate authorised for video (in Kbits/s) for the corresponding CAC class. This data rate may be between 0 and 65279 kbit/s. As a CAC class is used to set a limited throughput for a set of IP terminals managed by a CAC server, the throughput MUST be defined. A CAC class with no throughput is considered to be inexistent.

The principle of centre data rate management is the same as the one adopted for the classes.

When the centre is attached to another centre, the information is read on the attachment centre. Therefore, the configuration of this information for the attached centre does not apply (the following lines on: "Or attached to" do not apply).

DATA RATE BY COMM. (KB/S):

By default: reminder (read only) about the default video data rate assigned in the "Specific coding laws" menu.

Other value:

- Field blank by default when the function is activated: no video flow rate restriction
- Value 0: inter-class video not allowed
- Value (in increments of 32): maximum value used per call (max. 65279)

Restriction threshold:

This line does not appear in audio/video flow separation mode.

The threshold is given in kbits/s. To allow inter-class video, the available data rate on the link must be above this threshold:

- Value 0: default value when the function is activated; no restriction until the link is saturated
- Value entered: threshold in kbits/s (max.value is 65279). To allow inter-class video, the available data rate on the link must be above this threshold.

Note: When the centre is attached to another centre, the information is read on the centre to which it is attached (the lines from VOIP header compression do not appear.)

6.4.5.7 *Displays*

This menu contains the different CAC services display screens.

6.4.5.7.1 Display by IP address

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation>Location> Display by IP address**

ADDR. IP ADDR. BEGINNING WITH

All subnets with an IP address beginning with the digits entered will be displayed. Leave blank to display all IP subnets.

Click **Select the item** to go to IP subnet display.

The IP subnet addresses are displayed in ascending order. The following information is displayed for each subnet:

- IP subnet address
- CAC class to which the subnet belongs
- Name of the geographic location associated with the subnet,
- Name of the routing site for the special numbers dialled from a set on the subnet
- The location number for the urgent callback terminals

6.4.5.7.2 Display by location set

Menu **NETWORK AND LINKS>Quality of service>CAC services>Displays> Display by location set**

DIRECTORY BEGINNING WITH

Directory numbers are displayed in ascending order. For each directory number, information about IP subnets, site node and emergency call terminal is displayed.

6.4.5.7.3 Display by location

Menu **NETWORK AND LINKS>Quality of service> CAC and localisation>Location>Display by location**

FOR LOCATION

All the subnets associated with the location selected will be displayed.

Click **Select the item** to go to IP subnet display.

The IP subnet addresses are displayed in ascending order. The following information is displayed for each subnet:

- IP subnet address
- Name of the site and routing node of the special numbers dialled from a terminal on the subnet.

6.4.5.7.4 Classes display

Menu **NETWORK AND LINKS>Quality of service>CAC and localisation> Classes display**

This screen is used to display the parameters of all the CAC classes. It contains, in particular, the transit class, the different data rate settings of the CAC class definition menu. Clicking a class name displays then gives you access to the menus from which the information came.

The maximum data rate equals the maximum audio data rate + the maximum video data rate.

A zoom (activated by clicking) is available on a class to display the associated parameters.

6.4.5.7.5 Displaying class users

Menu **NETWORK AND LINKS>Quality of service>CAC and localisation>Displays>Display of classes users**

This screen is used to define the selected class.

FROM THE CLASS

Select the class from which the display starts.

SEARCH

IN ORDER	**DEFINED NUMBER**	**AVAILABLE NUMBER**

IN ORDER	Displays all CAC classes in order.
DEFINED NUMBER	Displays the CAC classes used by IP subnets. The associated IP subnets are displayed below the corresponding class.
FREE NUMBER	Displays the CAC classes not used by IP subnets.

Click **Select the item** to change to the next screen which gives the following items on the table displayed:

- The list of classes
- The IP subnets using these classes (the IP subnets are shown as follows: IP address / mask length)
- The maximum audio and video data rate associated with the classes indicated in case of non-separation of audio/video flows
- The maximum audio data rate associated with the classes indicated in case of separation of audio/video flows
- The maximum video data rate associated with the classes indicated in case of separation of audio/video flows
- The high-rate audio threshold defined by class
- The video threshold defined for the class indicated in case of non-separation of flows

A zoom (activated by clicking) is available on a class whose IP network is declared, to display the associated parameters.

6.4.5.7.6 Data rates to the centres display

Menu **NETWORK AND LINKS>Quality of service>CAC and localisation>Displays>Data rates to the centres display**

This menu displays all the centres with a declared inter-centre gateway.

In the configuration with audio/video flow separation, the data rates are displayed in 2 columns (1 for audio and the other for video). In this mode, the video threshold column does not exist.

A zoom (activated by clicking) is available on one of the centres to display the associated parameters.

6.4.6 ENCRYPTION AND IP SETTINGS

This menu is accessible via **NETWORK AND LINKS>Quality of service** and contains the following tabs:

- Ciphering
- QoS
- Qos Expert (accessible in advanced mode by selecting the icon)

6.4.6.1 *Ciphering tab*

This tab is used to manage the settings by equipment type:

- Signal and voice encryption (TLS*) between 2 iPBXs
- Signal and voice encryption (TLS*) between MiVoice 5300 IP Phones (MiVoice 5300 SIP Phone/MiVoice 6000 SIP Phone and an iPBX.
- The Voice encryption checkbox used to enable or disable the SRTP for:
- TLS and TDM terminals behind a VOIP card (Voice encryption licence required),
- Allow the built-in SBC, when enabled, to use SRTP for non-SRTP terminals or equipment during an external call.
  In this case, the SRTP/RTP gateway established by the SBC requires activating encryption and voice encryption licences.
  Also refer to the document SBC Service integrated on MiVoice 5000 Server and Mitel 5000 Compact on the documentation site on Mitel.com.
- In this case, a list of options is proposed:
  - AES 256
  - AES 128 (default value)
  - AES 256 only

In the event of an upgrade from < R7.2 to ≥ R7.2, if encryption was enabled, AES 128 is still proposed by default.

For a first installation (release ≥ R7.2), the default value is AES 256.

SRTP AES256 is supported by the following terminals or components:

- 6867i
- 6869i
- 6873i
- 6900 Series

- MiCollab without MBG
- MiVoice 5000 Server.

- Voice encryption for terminals i7xx, by making it possible to automatically generate CMEK and CMSK keys **.**

*** TLS**: Transport **L**ayer **S**ecurity, secure exchange protocol on the internet.

The **Encryption** function is subject to a licence and must be unlocked in the Menu **SYSTEM>Info>Licences**.

The corresponding subscription must equally be authorised for encryption: checkbox in Menu **SUBSCRIBERS>Subscriptions>Characteristics**.

⚠ **IMPORTANT NOTE: Refer to the document "Call encryption”.**

Each site has its own certificate.

This set may be:

- Either generated automatically by the iPBX (self-signed certificate), or
- Imported via Menu NETWORK AND LINKS>Quality of service by the operator, in form of a file in PKCS12 format (example: pbx.p12) from an external authority.

DESCRIPTION OF PARAMETERS AND FIELDS

---------- SIGNAL AND VOICE ENCRYPTION --------------

Note: This area only concerns MiVoice 5300 IP Phone/6xxxi for the sites in question.

The **Voice ciphering-terminal** box is displayed if a certificate has been assigned for SIP terminal use from the **Certificates assignment** tab of Menu **SYSTEM>Security>Certificates management**. See Section 4.4.

---------- VOICE ENCRYPTION (I7XX) --------------

Note: This area concerns terminals i7xx only.

For terminals i7xx, VOICE ENCRYPTION is a resource that can be shared in a multi-site configuration. To use the resource of another site, the service must be located on the site hosting this resource (menu **NEETWORK AND LINKS>Multi-sites>Localisation of the services>Other services**).

Encryption is performed using the 128 bits AES protocol.

The following conditions must be fulfilled to allow voice encryption on the IP network.

- The encryption function must be unlocked on the master and slave iPBXs.

- The PTx cards used for encryption must be compatible.
- The encryption keys (CMEK and CMSK) must be generated on the iPBX declared as master; then these keys must be sent to all (slave) iPBXs on the multi-site network.
- In a single-site configuration, the iPBX must be declared in master mode.
- In a multi-site configuration, each iPBX must be declared in master or slave mode (the slave mode is configured canonically).

The operator MUST enter the secret encryption keys. Otherwise, no call will be encrypted.

The codes are only entered on the iPBX declared as master in the multi-site configuration, then sent (in encrypted form) from the master iPBX to all the (slave) iPBXs in the multi-site configuration.

This transmission is recorded in the logbook.

After the codes have been entered, it is no longer possible to reread them. However, the date and edition of the last modification are displayed.

It is possible to declare another master iPBX after cancelling the previous one; the screens do not control these modifications.

From the master site, the operator can suspend the encryption on the entire multi-site network or on a site-by-site basis.

Basically, all sites can encrypt calls but it is possible on each site to forbid encryption locally.

FUNCTI. STATUS

UPDATED ON: ……….. ED: …

This line is read only.

If the (CMEK and CMSK) keys have been automatically generated by the iPBX, the date of update and edition are displayed.

The generation is effective and the functional status indicates: “In service”

Date on which the encryption keys were last updated by the operator (dd/mm/yy – hh: mn).

Upon each update, the edition is incremented by 1. By default edition is on: ‘….’

WORKING MODE /ENCRYPTION

SINGLE-SITE CONFIGURATION

In a single-site configuration, the iPBX is by default declared in master mode.

Encryption parameters:

ALLOWED: encryption is allowed on the single-site network.

FORBIDDEN: encryption is not allowed on the single-site network.

MULTI-SITE CONFIGURATION

In a multi-site configuration, only one master must be declared, information uniqueness is not controlled.

By default, the operating mode is set to: Slave.

MASTER SITE: ………….. **NODE: …**

Number and name of the site declared as master

Master node number

This is a read only line and only appears in multi-site mode.

MASTER “CIPHERING” SETTING

Ciphering=LOCAL AUTHORIZATION

The master site allows local encryption and disallows it on other sites.

Ciphering=GENERAL FORBIDDING

The master site forbids encryption in the entire multi-site configuration

Ciphering=GENERAL AUTHORIZATION

The master site distributes the code to and allows encryption in the entire multi-site configuration.

SLAVE “CIPHERING”

Ciphering=FORBIDDING

The slave site disallows encryption locally.

Ciphering=AUTHORIZATION

The slave site allows encryption locally.

HASH GENERATION (REMOTE WORKER):

This menu is for:

- Managing terminals 68xxi with the Remote Worker feature,
- Managing the Mitel Dialer OTT for Call Server in R8.2 SP1 or later.

Refer to the document:

- **Remote Worker via MBG** for the RemoteWorker feature,
- **MiVoice 5000 Server – Configuring the Mitel Dialer OTT via SBC** for the Mitel Dialer OTT.

⚠ **WARNING: Regenerating the hash will impact all deployed terminals.**

6.4.6.2 *QoS*

This tab allows:

- VLAN configuration,
- The configuration of the DSCP field, in decimal value, on a service basis for signalling, voice and video.

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

DESCRIPTION OF PARAMETERS AND FIELDS

VLAN VOICE PRIORITY / VLAN SIGNALING PRIORITY

This information is meant for updating terminals 6xxxi. This must also be used to update the information for terminals i7xx and MiVoice 5300 IP Phone via integrated DHCP. These settings are transmitted to IP terminals via the iPBX (from the file **aastra.cfg**).

The VLANS priority is conveyed in the 802.1q tag priority field.

The default value recommended by MITEL for voice and signalling priority fields is: 6

CONFIGURING DSCP SERVICES

DSCP: Differentiated Services Code Point

As of R7.0, this field replaces the ToS field in IPv4 and uses the Traffic Class field in IPv6.

This value is is intrinsic data for the IP message used to determine the priority of the IP packet containing this value, compared to other IP messages passing through the IP network.

The iPBX generates different types of IP messages (a marking message for voice, a message for signalling and a message for video (MiMvoice 5000 Server and Media server only).

The iPBX assigns a value for the DSCP that is specific to the transmitted IP message.

The DSCP field is configurable for up to 100 ports.

The values below are used to modify the setting of the DSCP field used for the different media. The equivalent value of the TOS bit in hexadecimal is given with reference to the old TOS-based mode:

DSCP TELEPHONY SIGNALLING (DECIMAL) / TOS (HEXA)

Default value, in decimal, used for RTP and RTCP packets. This value may be between 0 and 63.

DSCP VOICE (DECIMAL) / TOS (HEXA)

Default value, in decimal, of the Traffic Class field of an IP packet, conveying a signalling TCP segment. This value may be between 0 and 63.

6.4.6.3 *Qos Expert (advanced mode)*

This tab available in **Advanced** mode (by selecting the icon) allows the current configuration of the DSCP by port.

Note: Port-based configuration overrides service-based configuration.

The various fields allow port-based DSCP configuration rules to be set up (up to 100).

Configuration rules are classified by increasing port number

- Port MIN: Port number [1, 65534]
- Port MAX: Port number [Min Port, 65534] or empty
- Protocol: UDP or TCP
- DSCP Decimal: [0, 63]
- DSCP Binary: 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.

Port value constraints and consistencies

In this advanced mode of port-based DSCP configuration, ports can take any value between 1 and 65534 and can, thus, clash with the service-based DSCP configuration. (QoS tab).

On MiVoice 5000 Servers, this concerns SIP signalling ports and audio ports.

Here is the list, by service.

For DSCP signalling:

- 5060 (UDP and TCP) for SIP signalling
- 5061 (TCP) for SIP signalling
- 5062 and 5064 on MiVoice 5000 Server only for SBC.

For DSCP voice on MiVoice 5000 Server only

- The range [40000, 40999] used by the media server,
- The range [20000, 27999] (default values, modifiable in Menu Network and Links>Internet Gateway), used by the SBC.

For DSCP video on MiVoice 5000 Server only

- The range [40000, 40999] used by the media server (same range as for voice).

Adding a port-based configuration

- Fill in the different fields.
- Click New.

- 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.

Note: No tests have been carried out on the overlap of port ranges. It is, therefore, important not to set a different DSCP value for the same given port range;
Example 1:
Port min = 1; Port max = 100; DSCP value = 46 Port min = 2; Port max = 200; DSCP value = 47 → OK

Port min = 1; Port max = 200; DSCP value = 46 Port min = 2; Port max = 100; DSCP value = 47

And therefore Port 101 to 200; DSCP value = 46 → OK

Example 2:
Port min = 1; Port max = 100; DSCP value = 46 Port min = 1; Port max = 100; DSCP value = 47 → NOK

WARNING: In the Comment field, do not use the character ! as it is not recognised by the system.

Modifying a port-based configuration

- Select the line concerned.
- Enter the new values.
- Click Modify.

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.

6.4.6.4 *SIP security*

Menu **NETWORK AND LINKS>Quality of service> SIP security**

The SIP router, an integral part of Mitel 5000, provides the following services:

- Routing messages to/from a terminal/trunk (no mater the protocol: TLS, TCP or UDP) from/to the GSI
- Processing instant messages
- Defending against DoS (Denial of Service attack), Malicious Call and DDoS (Distributed Denial of Service attack)

- Defending against Brute Force

6.4.6.5 *Security parameters tab*

SECURITY LEVEL

This first parameter is used to configure the deployed level of safety. Options list, possible values:

- None: if the security level (Level "None") is not activated, the white and black lists are not taken into account for IP address filtering. Moreover, the following lines on this screen are hidden.
- Self-protection: for the "self-protection" level the Black list and White list serve as a filter.

DoS parameters

- Threshold: variation range of 10 to 5000
- Window (seconds): range from 2 to 10
- Period: options
  - 30 seconds
  - 5 minutes
  - 30 minutes
  - 1 hour
  - 1 day
  - 1 week
  - infinite.

DDoS parameter

- Threshold: variation range of 10 to 5000
- Window (seconds): range from 2 to 10

DELETING THE DoS BLACKLIST

The DELETE option empties the DoS blacklist.

6.4.6.6 *Whitelist tab*

For entering the 100 IP addresses used on the white list.

6.4.6.7 *DoS backlist tab*

This tab is used to display, at a given time T, the IP addresses that are not trustworthy, preceded by the registration date and time.

Possible action on the list is the deletion of the entire list in the "Security settings" tab.

The deletion of only one address from the black list is accessible via the hypertext link of the first column.

The deletion of several addresses from the black list is accessible via the Repetition command.

6.4.6.8 *Blacklist Force Brute*

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

Three list columns: date and time, target IP address, and origin of attack.

Deletion by the operator is not possible. The address in question can only be deleted after 5 minutes.

6.5 DATA LINKS

Introduction:

The purpose of this chapter is to describe the user interfaces used to define and manage these links between the various terminals or servers of a single-site or multi-site MiVoice 5000 system.

To set up a “data” call between a source terminal and a destination terminal it is therefore necessary to define:

- The identity and characteristics of each link element (local or remote)
- The characteristics of the transmission modes between the different interfaces (network types, protocol, direction, acknowledgement)

The data link main menu is accessible via **NETWORK AND LINKS>Data links**.

The following functions are available from this menu:

- Link management
- Access lists
- Symbols
- Routes
- Remote identifiers
- Servers
- EAS (External application server) users
- TCP/IP-X25 gateways
- Settings

6.5.1 LINK MANAGEMENT

Menu **NETWORK AND LINKS>Data links>Link management**

Any subscriber wishing to transfer packets via the packet switch must be the subject of a declaration which assigns a directory number of the iPBX packet dialling plan.

This may involve:

- An internal server (AFISER, SERVTL, KITAXE, EAS, MUFACT, SERGIC, SRVRHM, TELBOR, BUFTIC)

A directory number comprises up to 8 digits. The first character can be either the letter A or B: in this case, the remaining characters must be digits.

Links with a directory number beginning with either the letter A or B cannot be called by a user, (often used when a CP1 link is created or for the constituent links of a hunt group).

When a subscriber has several links which provide identical services, these links can be grouped together in a hunt group (known as “partial" hunt group).

The hunt group then also receives a directory number distinct from the numbers assigned to links entering into the composition of the hunt group.

Due to the type of bus of the connecting interface on the LD4 card, the “S interface” subscribers are a special type and require a specific form of management: therefore, they cannot be part of a hunt group.

The subscribers associated with the simple links are the subject of a declaration which specifies the characteristics of the equipment connected to the iPBX: either on real accesses (CA1, CS1, CP1 cards), or on a so-called fictitious access (case of the AFISER server).

These characteristics can be divided into two sets:

1. A set including all characteristics common to all subscribers, that is, link identity and link type.

2. A set grouping the characteristics which define link type.

6.5.1.1 *Link characteristics*

Menu **NETWORK AND LINKS>Data links>Link management>Link characteristics**

Links are set up via the IP network

This screen is used to select a link in order to define its characteristics.

BY EQUIPMENT NUMBER: (BY DEFAULT 00 ON MIVOICE 5000 SEVER).

BY DIRECTORY NUMBER

Selecting a link by its directory number (from 1 to 8 characters): the first character is either a number, or A or B; the other characters are necessarily numbers.

By default, the links do not have a directory number. The data directory plan is open and completely independent of the telephony directory: the same number can be assigned on both sides.

BY GROUP

Selecting by the hunt group name defined in the "Hunt group name" menu. This selection enables modifications to be made to links in the same hunt group.

Note: Whenever no selection criterion is specified, the first link on the first card is selected automatically.

For an ISDN link, the subscriber must be created on both sides:

1. Telephony with a CIRCUIT directory number, using the screen “Add/Delete extensions” if there are several directories on the bus,

2. packet with a PACKET directory number using the "Assign directory Nbs. to ISDN accesses" screen: several ISDN data subscribers can be assigned to the same access.

The parameters corresponding to the ISDN subscriber can then be modified using the LINK CHARACTERISTICS screen.

6.5.1.1.1 Links via the IP network

Menu **NETWORK AND LINKS>Data links>Link management>Link characteristics**

Select the IP link then click **Select the item** to move to the next screen.

6.5.1.2 *Display by directory*

Menu **NETWORK AND LINKS>Data links>Link management>Display by directory number**

This screen display of the connections contained in the iPBX: it is a consultation screen and not a modification screen.

NUMB. directory number assigned to the link

SLOT cabinet, card, equipment

TYPE type of link

NAME name assigned to the link

GROUP name of the group to which the link belongs

TEL NO. telephone directory number (circuit) corresponding to the terminal when the link is ISDN/S0 type.

Note: To display the dynamic status of data links, you can also consult the screen "Status of data links".
For a multi-company configuration, the department is displayed in place of the phone number.

6.5.1.2.1 Display users

Menu **NETWORK AND LINKS>Data links>Link management>Display users**

This display shows the users of the selected hunt group, in this instance, Circuit or Packet type routing.

6.5.1.3 *Categories*

Menu **NETWORK AND LINKS>Data links>Link management>Categories**

Categories allow access restrictions for incoming and outgoing subscribers to be specified.

These restrictions are based on the French packet numbering plan prefixes that are:

- 0--> international PSDN access
- 1 6 --> national PSDN access
- 7 --> free
- 8--> PSTN modem access
- 9 --> local access

Each subscriber must have a category.

6.5.1.3.1 Names

Menu **NETWORK AND LINKS>Data links>Link management>Categories>Names**

CATEGORY N (FROM 0 TO 15)

Give a name to each category (up to 8 alphanumeric characters): the iPBX displays the names of the 16 categories proposed.

Note: A category list can be managed only if its name has been declared. Initially, no list is defined.

6.5.1.3.2 Definition

Menu **NETWORK AND LINKS>Data links>Link management>Categories>Definition**

After choosing the category, click "Select the item" to move to the next screen, which gives the characteristics of the selected category. It is used to define access restrictions.

1 - INCOMING ACCESS

ALLOWED **PSDN** **FORBIDDEN**

ALLOWED	All incoming calls are allowed on the link.
PSDN	Only calls with the calling number beginning with a number from 0 to 6 are allowed on the link.
FORBIDDEN	Incoming calls are not allowed on the link (including local calls).

2 - PSDN OUTGOING ACCESS

ALLOWED **NATIONAL** **INTERNATIONAL** **FORBIDDEN**

ALLOWED	Outgoing calls with a number beginning with prefixes 0 to 6 are allowed.
NATIONAL	Outgoing calls with a number beginning with prefixes 1 to 6 are allowed.
INTERNATIONAL	Outgoing calls with a number beginning with the prefix 0 are allowed.
FORBIDDEN	All outgoing calls are forbidden (including local calls).

6.5.1.3.3 Display users

Menu **NETWORK AND LINKS>Data links>Link management>>Categories>Display users**

This screen shows the users of the selected category.

6.5.2 ACCESS LISTS

Menu **NETWORK AND LINKS>Data links>Access lists**

In order to limit accesses to a subscriber, it is possible to allocate the subscriber a list of access rights.

These access rights concern external calls from PSDN (i.e.: those with the "caller address" field beginning with a digit between 0 and 6). The iPBX allows such a call only if this corresponds to an item in the list associated with the link (barring on the incoming call).

6.5.2.1 *Names*

Menu **NETWORK AND LINKS>Data links>Access lists>Names**

A list item comprises:

- Either a calling number: in order to be accepted, the first digits of the "caller address" field of the call packet must be the same as the calling number defined in the "caller address" field of the list. This can be longer, if necessary, and comprise an "additional number".

- Or a password comprising 8 ASCII characters: to be accepted, the call data in the call packet must match the password defined in the screen.

- Or a combination of both, i.e. a caller number and a password: for the call to be accepted, the previous two conditions must be met.

ACCESS LISTS N (FROM 0 TO 15)

Give a name to each access list (up to 8 alphanumeric characters): the iPBX displays the names of the 16 categories proposed.

Note: An access list can be managed only if its name has been declared. By default, no list is defined.

6.5.2.2 *Definitions*

Menu **NETWORK AND LINKS>Data links>Access lists>Definition**

BY NAME

Choose the access list.

After choosing the access list, click "Select the item" to move to the next screen and define the following settings:

CALLING NUMBER

A remote number which has the right to contact the iPBX (15 digits maximum).

If the call comes from PSDN, the calling number must be complete. If the number is local, it must include the digit 9 (local prefix).

PASSWORD

Enter a name with 8 alphanumeric characters (this field must be complete).

Note: CREATING A 5-NUMBER BLOCK: an additional block is created by selecting the “S” function if any blocks remain available.
ADDING, DELETING A LIST ITEM

Items are displayed in the order in which they were created.
An item is added by filling in any empty item displayed on the screen: this will be considered as the last one whatever its position.
To delete an item, you must delete either its calling number or its password.

6.5.2.3 *Display users*

Menu **NETWORK AND LINKS>Data links>Access lists>Display users**

This display shows the users of the selected list, in this instance, data links.

6.5.3 SYMBOLS

Menu **NETWORK AND LINKS>Data links>Link management>Symbol management**

The operator can define symbols in order to facilitate dialling for users (100 symbols from 00 to 99).

A symbol represents, in short form, the entire dialling command that an asynchronous data terminal user would have to give to make their call (class of service, dialling, CUG, reverse charge call, etc.).

In addition to its ease of use, a symbol allows caller restrictions to be overridden from a category and CUG point of view. Thus, a subscriber not having PSDN international access can use a symbol to reach a specific call party abroad.

6.5.3.1 *Symbol characteristics*

Menu **NETWORK AND LINKS>Data links>Symbol management>Characteristics**

BY NAME

Enter the name of the symbol.

SEARCH

Allows you to sort by different criteria: in the order, defined number, available number.

Select the symbol then click **Select the item** to move to the next screen used to define the following settings:

NAME

This comprises 1 to 6 alphanumeric characters and must begin with a letter.

It constitutes the criterion for existence of the symbol and it is therefore the modification of this field that allows the symbol to be created or deleted.

USED BY COMPANY

CMPANY 0

If the iPBX is declared MULTICOMPANY, this additional line appears.

Use of a SYMBOL can be reserved for the links of one company only or can be common to all companies.

A symbol belonging to company number 0 (CMPNY 0) can be used by all links.

CLASS OF SERVICE

VIDEOTEX **ASCII TERMINAL**

The same symbol can be used by a terminal in ASCII mode and a terminal in VIDEOTEX mode. The class of service associated with the symbol can only be used by a terminal in VIDEOTEX mode.

It can have the following values:

VIDEOTEX The user wishes to use his/her terminal in VIDEOTEX mode to dialogue with a server.

ASCII TERMINAL The user wants to use their data terminal in ASCII mode. In this case, the iPBX automatically controls switchover of the terminal to this mode.

CLOSED GROUP NUMBER (CUG)

This specifies the closed group of users with which you wish to reach the call party.

The CUG value is between 0 and 15, given that the value 0 designates the CUG common to all users and that it is possible not to enter any CUG (empty field). In this case, the usual number is used.

The user of the symbol may not belong to this outgoing CUG (override of restrictions).

MINITEL FUNCTION KEYS HANDLED

Selecting "YES" corresponds to the "*" information of VIDEOTEX mode dialling. The Minitel function keys must not be converted because the call party manages these keys according to VIDEOTEX encoding.

The "NO" setting therefore indicates that the call party does not know how to manage the Minitel function keys with VIDEOTEX encoding. Conversion into ASCII is then performed by the iPBX.

REVERSE CHARGING

The "YES" setting indicates that the call generated by the iPBX has the additional reverse charging service.

DIALLING

This comprises 1 to 15 digits specifying the call party to be reached.

ASSOCIATED CALL ESTAB. DATA

This is an optional setting. It can comprise up to 12 ASCII characters specifying the data that the iPBX inserts in the call packet transmitted to the call party.

6.5.3.2 *Display symbols*

Menu **NETWORK AND LINKS>Data links>Symbol management>Display**

This display allows the main characteristics of all existing symbols to be viewed. It links the symbol's name with its number (these numbers are between 00 and 99, that is a maximum of 100 symbols).

MULTI-COMPANY OPERATION

CMPNY.0	**• • • • •**

Select the name of a company. Select **......** to view all declared companies.

6.5.3.3 *Display users*

Menu **NETWORK AND LINKS>Data links>Symbol management>Display users**

This display shows the users of the selected symbol, in this instance, of PAD, Video PAD or incoming PSTN type data links.

6.5.4 ROUTES

Menu **NETWORK AND LINKS>Data links>Routes**

Menu **NETWORK AND LINKS>Data links>Routes>Definition**

CREATING A ROUTE

To create a route, the type "EMPTY" must first be selected in the selection menu. Then, the route type chosen must be defined in the input menu. From this time on it will be recognised by the iPBX and can be displayed by simply entering its type in the selection menu.

DELETING A ROUTE

A route is deleted by assigning it an "EMPTY" type. All existing prefixes for the route must previously be deleted.

MODIFYING THE ROUTE

To modify a route, first delete the old prefix then return to the selection menu to enter the edit menu for the new route.

This screen is used to create, modify or delete a route by selecting it using various criteria.

BY ITS PREFIX

A numeric field of 9 digits maximum.

WARNING: The value of route 0 as local is 9 (default prefix).

BY ITS RANK

Rank is a numeric field between 0 and 63 (64 possible routes).

BY ITS TYPE

• • • • • •	**INTERNAL**	**PACKET**	**CIRCUIT**	**TRANSLATION**	**EMPTY**	**IP TUNNEL**

Select a type of route (64 types of possible routes).

If more than one criterion is specified, the prefix overrides both other criteria (whether they are filled in or not), the route number is considered as outgoing rank in the search for the type of route specified.

To summarise, the first two criteria are used to select a known route, the third is to facilitate search when only route type is known.

Note: When selecting a route by the EMPTY type, the first available route is number 8, defined by default as CIRCUIT type.
If you do not choose any criterion, the first empty route is displayed.

Select the route then click "Select the item" to move to the next screen used to define the following settings:

DIRECTORY NUMBER

This is the directory number of the associated link (or link group) on which the call packet will be routed.

It comprises a maximum of 4 characters, the first one can be either a digit or one of the letters A or B, the other characters must be digits.

BACK-UP ROUTE

It allows the rank of the route used for back-up to be defined (values from 0 to 63).

REMOTE IDENTIFIER NAME

IDENT_0	TCP CONNECTION	• • • • • •

Select the remote identifier defined in the "Names of remote identifiers" menu.
The "CXTUN02" item is to assign connection names to the selected tunnelling link.

-- DEFINED PREFIXES -------------------------------------

This section displays the prefixes associated with the route.

Examples:	- Local routing	→ prefix 9
	- Packet routing →	prefixes 0, 1, 2, 3, 4, 5
	- Circuit prefixes →	7X (X = 0 to 9)

ACCESS TYPE

PSTN	NATIONAL	INTERNATIONAL

This allows the network access type for this route to be defined.

PREFIX

A prefix is a sequence of 9 digits describing the dialling to be analysed: it cannot belong to different routes.

ACTION

CREATE	DELETE	MODIFY

Allows you to create, modify or delete prefixes for this route: to enter a prefix, the route must exist (non-empty type).

Note: In case of route translation, the following fields are displayed:
NEW DIALLING PLAN" route translation can be used only to back up a route. Once translated, the called number undergoes complete analysis.
1-15 digit number which is added before the numbering provided by the caller after having possibly deleted certain digits.
Example: Main/secondary route, backup by route translation.
NUMBER OF DIGITS TO DELETE: number of digits to be deleted from the called number.

6.5.4.1 *Display*

Menu **NETWORK AND LINKS>Data links>Routes>Display**

With this menu, you can display all existing prefixes for a type of routing specified at selection.

For each prefix found, a reminder of route characteristics is displayed.
Moving between "next" and "previous" changes the type. The EMPTY type is not considered in this cycle but can be selected at entry.
There are five types of routing:

- EMPTY routing
- LOCAL routing
- CONSIST. INTERNAL routing
- PACKET routing
- CIRCUIT routing
- TRANSLATION routing
- IP TUNNEL routing

WARNING: Local routing 0 with prefix 9 is the default value.

6.5.5 REMOTE IDENTIFIERS

Menu **NETWORK AND LINKS>Data links>Remote identifiers**

Remote identifiers are used in the case of data calls in X25 packet mode on 64 Kbit/s switched circuits.

They are used:

- For an outgoing call: the circuit mode route definition must be filled in by entering the complete circuit call number to be set up, and the X25 characteristics of the link reached.

- For an incoming call: the X25 characteristics of the calling equipment must be obtained by using the circuit calling number (if this exists). These characteristics are then applied to the X25 link (of the CP1 card) selected. If the calling number is unknown, use the characteristics of the number 0 remote identifier (the default remote identifier).

6.5.5.1 *Names of remote identifiers*

Menu **NETWORK AND LINKS>Data links>Remote identifiers>Names**

REMOTE IDENTIFIER N (FROM 0 TO 127)

Assign a name to the remote identifiers (8 alphanumeric characters): the number of identifiers is fixed at 128.

Note: An identifier can only be used if it has a name.

IMPORTANT NOTE: The remote identifier 0 (IDENT_0) is reserved in arrival: it is dedicated to the SBS PSDN (synchronous unmarked PSDN output).

6.5.5.2 *Definition*

Menu **NETWORK AND LINKS>Data links>Remote identifiers>Definition**

BY NAME

Choose the name of the remote identifier to define.

Select the identifier then click **Select the item** to move to the next screen.

This screen is divided into three parts:

- REMOTE IDENTIFIERS

- X25 PARAMETERS

- LEVEL 2 IDENTITY

------------------------REMOTE IDENTIFIERS---------------------------------

CIRCUIT NUMBERING

Outgoing, this field is MANDATORY, its value is 1 to 15 digits. It corresponds to the directory number to be transmitted to an ISDN T0 access (Numeris BRI) to set up the 64 Kbit circuit (do not forget to put 0 before the complete number), 0 is the external prefix for setting up a circuit call.

Incoming, the number corresponds to the directory number of the caller associated with the identifier (do not forget that if the caller is in the Paris region, NUMERIS (ISDN) adds a "1" before his/her number, so enter 1 ABPQMCDU).

SUB-ADDRESS

Value 1 to 4 digits, this field is optional. This value can be used only in the case of a call via NUMERIS (ISDN).

NETWORK TYPE

INTERNAL **PSDN** **CIRC EXT LINK** **INTER NETWORK**

You must select one of these settings.

The iPBX often modifies the (caller and called party) addresses contained in the X25 packet in order to compensate for differences in the dialling plans of interconnected iPBXs. This modification depends on a parameter called "Remote packet network type".

INTERNAL	Prefix 9 is added followed by the subscriber number in the "caller address" field of the transmitted packets
PSDN	Prefix 9 is added in the "called address" field of the call packets received from PSDN and it is added in the "caller address" field of the packets transmitted to PSDN.
INTER NETWORK	Used in multi-site operation. Do not modify the numbering.
CIRC EXT LINK	Same as PSDN for the "called address" field in the packets received. But in addition, the external prefix associated with the identifier in the "caller address" field is added.

EXTERNAL PREFIX

This field is optional for an incoming identifier, it allows the prefix to be added before the calling number so that a complete number can be given to the caller.

COMPANY

DEPARTMENT

These two fields are linked to multi-company configuration.

------------------------X25 PARAMETERS-----------------------

OUTGOING CUG (0 . . . . . . 15)

Indicates the list of values of the closed user group to which the link belongs.

MODIFY GROUP NUMBER

Allows the Outgoing CUG number to be modified.

INCOMING CUG (0 . . . . . . 15)

Same principle as outgoing CUG.

MODIFY GROUP NUMBER

Allows the Incoming CUG number to be modified.

NUMBER OF EQUIPPED LOGICAL CHANNELS

Value between 0 and 250, mandatory.

It gives the total number of virtual circuits that can be set up on the 64 Kbit/s circuit.

NR. OF OUTGOING LOGIC CHANNEL

Value between 0 and 250, mandatory.

This is the number of logical channels reserved for making incoming calls to the iPBX on the link.

NR. OF INCOMING LOGIC. CHANNEL

Value between 0 and 250, mandatory.

This is the number of logical channels reserved for making outgoing calls to the iPBX on the link.

PACKET WINDOW

Value between 1 and 7, mandatory.

It gives the number of data packets that the iPBX can send in anticipation without waiting for acknowledgement from the remote user. A value "2" is recommended.

This mandatory field indicates the maximum data field size in data packets.

MAX. PACKET DATA FIELD SIZE

128 **256** **512** **1024**

LOGICAL CHANNEL 0 USAGE

This field is mandatory. If you tick YES, the 0 logical channel can be used to set up a virtual circuit.

LINK BEHAVIOR

VARIABLE **DCE** **DTE**

This mandatory field specifies link behaviour with respect to level 3 packet processing, in particular, for the logical channel selection mechanisms.

There are three possible settings:

DCE	Indicates that the iPBX must behave like a network
ETTD	Indicates that it must behave as a terminal (notably for PSDN access).
VARIABLE	Indicates that link behaviour depends on the direction in which the switched circuit is set up, the caller is DTE and the called party is DCE.

REVERSE CHARGING ACCEPTED

This field is mandatory. If the box is not ticked, the iPBX will refuse calls for which reverse charging is requested.

EXTENDED FORMAT X25/84

This field is mandatory. The YES setting indicates that the remote user (called party) accepts extended packet format specified in the X25/84 recommendations and also diagnostic packets.

FRAME WINDOW

This field is mandatory, value from 1 to 7.

Gives the number of information frames that the iPBX can send in anticipation.

DEFAULT DATA RATE

	150	300	600	1200	2400
4800	9600	19200	48000	64000	

This allows the default data rate to be set when the subscription is taken out (default 64000).

FAST SELECT ALLOWED

Refer to the PSDN Contract, Packet Level line 7.

Fast select is an optional user service that a DTE can request for a given virtual call.

THROUGHPUT CLASS NEGOTIATION ALLOWED

Refer to the PSDN Contract, Packet Level line 4.

NEGOTIATION OF FLOW CONTROL ALLOWED

Refer to the TRANSPAC Contract, Packet Level line -6.

CALL REROUTING ALLOWED

Refer to the PSDN Contract, Packet Level line 6.

-----------------------LEVEL 2 ID----------------------------

The following columns are used to define this identity.

LINK ID

CERTIFIED LINK ID

⚠ **IMPORTANT NOTE: For an incoming call, by its DID circuit number. This must be declared on the telephony side in the "DID general call number" menu, then perform a Call packet routing. In the case of local calls, the packet switch must be called by its circuit number. This must be declared on the telephony side, in the “Access to features” menu, and a directory number on the packet switch call line given.**

⚠ **IMPORTANT NOTE: For an outgoing call, do not forget to create the corresponding circuit routes in the menu “Routes” / Data links.**

6.5.5.3 *Display remote identifiers*

Menu **NETWORK AND LINKS>Data links>Display users**

This screen shows the users of the selected remote identifier.

6.5.6 SERVERS

A "server" provides MiVoice 5000 services; these services can be configured in the following menus:

6.5.6.1 *Servers*

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

This screen only allows server characteristics to be modified: by definition, a server cannot be created or deleted.

BY ITS NAME

AFISER
Service virtual user.
Link operational test server (sub-addresses 01, 02, 03), it also returns the caller number (sub-address 04).

SERVTL
Telephone status display server for set hunt groups and Attendant Consoles accessible from a PAD link with Videotex emulation.

KITAXE
Charge record distribution server used, for example, by attendant console on PC with the charging management option.
Accessible from a PAD link ("IRIS" card with Attendant Console on PC).

EAS
External Application Server.
Allows management of sets, wake up calls, etc., from a PC running the corresponding application software (Hotel management, Call distribution, etc.).

MUFACT
Multiplexer, billing demultiplexer (Multi-site).
Allows call records to be sent to external PCs according to sorting criteria and the companies they are for. This server calls on the KITAXE server to perform its task.

SERGIC
Server used in multi-site situations. Maximum packet data field size = 1024.

BUFTIC
SERVER BUFFER associated with the integrated buffer.

Server directory number list

SERVER	DIRECTORY NO.	SUB-ADDRESS	COMMENTS
AFISER	010	00	Echo
		01	Absorber
		02	Slow speed character generator
		03	Fast speed character generator
		04	Caller identification
SERVTL	011	1	VMAIL V.24 call
		6	CSTA server call
		7	SRTAPI call
		8	SRTAPI call
		90	Windows attendant console server call
		91	H.323 gateway access server call
		92	SMDI call
		93	Debug server call
KITAXE	012	000	Telephone ticket
		010	Packet data ticket
		020	Circuit data ticket
		030	Service ticket
		040	Supervision ticket
EAS	013		EAI internal server
			External application interface
MUFACT	014		Called by KITAXE
			Multi-site ACD
SERGIC	016		Multi-site server
SERVRHM	017		MMC implicit call from a PAD
BUFTIC	021		Associated with the integrated buffer

Select the server name then click **Select the item** to move to the screen used to define the following settings:

STATUS

DISABLED **IN SERVICE**

The current status of the server is shown in the <name> section.

This field is used to enable>disable the server.

DIRECTORY NUMBER

Corresponds to the directory number indicated in the table entitled "list of server directory numbers”. Example, 010 corresponds to the AFISER server.

CATEGORY

This is the name of the category that is to be assigned to the server; it is defined in the “Category names” menu.

This category defines the outgoing/incoming restrictions which are to be applied to the server, characteristics given in the “Category definition” menu.

REVERSE CHARGING ACCEPTED

NO **YES**

If YES, indicates that the subscriber associated with the server systematically accepts a call requesting charging of the called party (reverse charge or collect call).

ACCESS LIST

Name of the access list defined in the “Access list names” menu which is to be assigned to the server.

This list gives the number of a list of external callers (from PSDN) authorised to communicate with this particular subscriber (barring of incoming calls).

X25 calls are filtered according to either caller number, or a password, or a combination of both of these.

OUTGOING CUG (0 . . . . . . 15)

Indicates the list of values of the closed user group to which the server belongs.

MODIFY GROUP NUMBER

Allows the Outgoing CUG number to be modified.

INCOMING CUG (0 . . . . . . 15)

Same principle as outgoing CUG.

MODIFY GROUP NUMBER

Allows the Incoming CUG number to be modified.

MAX. PACKET DATA FIELD SIZE

Available values are: 128, 256, 512 or 1024. For the SERGIC server, the maximum packet data size is 1024.

NR. OF LOGIC. CHANNELS EQUIPPED (1/250)

Possible values are from 1 to 250, by default it is at 16, these logical channels concerning the server are incoming channels.

NR. OF OUTGOING LOGIC. CHANNELS (0/250)

NR. OF INCOMING LOGIC. CHANNELS (0/250)

IMPORTANT NOTE: The AFISER server offers different services for character generation/elimination. This is the first item to be put into service in the iPBX as connected terminals can then dialog with it, which allows connection, programming and operation of link configuration to be checked.

- Available Services
  - 00--> Absorber/generator
  - 01 --> Absorber
  - 02--> Low speed character generator (1 packet/second)

  - 03--> Fast speed character generator
  - 04--> Provides the caller number.

- Access to a service is obtained by dialling the code corresponding to the service, after the server directory number.

Example: numbering 9 010 04

  - 9 = Local routing number
  - 010 = AFISER directory number
  - 04 = AFISER service number

6.5.6.2 *Eternal application server users*

Menu **NETWORK AND LINKS>Data links>Servers>External applic. server users**

In the table displayed on this screen, the already declared users are displayed.

SELECTION OF USER NO.(1/8)

A digit from 1 to 8 for selecting the user listed in the first part of the display.

Click the user's number to display the management parameters for this user.

USER IDENTIFICATION

Enter a name for the user.

PASSWORD

Enter a password for the user.

ACCESS LIMITED TO ONE COMPANY

Multi-company parameter: tick this box to configure the access for one company only.

ACCESS TO COMPANY CMPNY 0

Multi-company parameter:

RANGE OF MULTI-SITE

Select the range.

ACCESS RIGHT TO COMMANDS:

Tick or untick the commands according to service rights.

- Password modification
- Update system time
- Calendar switchover
- Least Cost Routing management
- Wake up call management

- Category management
- Message lamp management
- Digital set key management
- Read set status
- Set language management
- Hunt group monitoring
- Prepayment management
- Move multi-users
- Confidential code management
- Call distribution management
- Forwarding management
- Subscriptions status management
- Voice mailbox management

6.5.6.3 *CSTA servers*

Menu **NETWORK AND LINKS>Data links>Servers> CSTA servers**

This menu is used to configure the CSTA servers whose connection is password-protected.

Number of CSTA links per user:

- On MiVoice 5000 Server, maximum 6 CSTA links

CHARACTERISTICS TAB

CSTA server number 0 to 63

The first 64 CSTA servers may be associated with a password.

Server password

Enter here the CSTA server password: 16 ASCII characters maximum, upper cases and lower cases.

Recording

Checkbox indicating whether the server type is a call recorder, like the server at ASC. In this case, the CSTA application supports proprietary call recording events.

E.164

Checkbox indicating whether the server manages the treatment of E.164 numbers.

Note : The E.164 setting is independent to the connection mode.

TCP port:

TCP port chosen for the TCP-IP/X.25 gateway. Authorised values: 2001 -> 65534 except for the following port values and system ports used already.
Default assignment of port 3211 to server 00 in NOT DELIMITED mode.

Mode:

NOT DELIMITED: Default value

TPKT:

STATUS TAB

This tab is used to display the status of CSTA servers:

Column 1: server number

Column 2: server type: CTI_CSTA, CTI_CC, CTI_BSS or CTI_ASC

Column 3: Number of sessions on the server

Column 4: Server host site

Column 5: the node of the hosting site

6.5.7 TCP/IP – X25 GATEWAY LINK

Menu **NETWORK AND LINKS>Data links>TCP/IP – X25 gateway**

This screen is used to select a gateway to access TCP/IP – X25 server characteristics. It has five functions.

6.5.7.1 *TCP - X25 address port translation*

Menu **NETWORK AND LINKS>Data links>TCP/IP – X25 gateway>TCP – X25 address port transl.**

DIRECTORY NUMBER

Select the directory number of the gateway link. The field displayed is used to modify the characteristics of a remote server.

It is possible to modify a TCP – X25 Address port translation with the active gateway link; the modification is only taken into account when the gateway link is reactivated.

- If, when the translation is modified the gateway link is free, it will be automatically “disabled” then “reactivated”.
- If when the translation is modified the gateway link is in communication, it is ”disabled’ and then "enabled" automatically as soon as the gateway link becomes free (e.g. modification of a translation with MiVoice 5000 Web Admin; as soon as MiVoice 5000 Manager disconnects, the gateway will be "disabled’ then "enabled" automatically)
- If, when the translation is modified the gateway link is in communication, for the modification to be taken into account immediately, the gateway must be “disabled” then “enabled” manually.

The title displays the link's directory number.

PORT

Maximum 5-digit port number: this number must be more than 2000. If it is nil, the field is considered as empty.

Note: As long as this number has not been entered, the following fields are not displayed.

X25 NUMBER

X25 number of 15 digits maximum (address requested in the call packet).

MODE

By default, NOT DELIMITED mode is assigned.

CALL DATA (VALUES):

ASCII (16 characters max.)

HEXA (00/07)	42 6F 6E 6A 6F 75 72 0D
HEXA (08/0F)	0A ....

X25 call data is stored in the table (PIPD_DONNEES_APPEL) in the form of ASCII characters. Forbidden characters are replaced, for display, by the substitution character "?".

16 remote X25 servers, per gateway, can access call data; the message “FULL TABLE” is shown in case of overflow.

If certain ACSII characters cannot be entered, you can use the corresponding hexadecimal (HEXA). Input in one mode (ASCII or HEXA) automatically updates the other mode (HEXA or ASCII) at line change.

ACTION

Save or delete.

Note: The PORT and X25 NUMBER fields must be filled in for the action to be valid.

The scroll bars on top and on the right side of the << and >> screen are used to navigate to modify the characteristics of another remote server.

6.5.7.2 *Update X25 addresses*

Menu **NETWORK AND LINKS>Data links>TCP/IP – X25 gateway>TCP – Update X25 addresses**

This screen offers a quick means of updating, in just one operation, the correspondences between port ⇔ X25 address for the internal routing plan.

OLD BEGINNING OF X25 ADDR.

Enter the old beginning of X25 addresses (from 9 to 901).

NEW BEGINNING OF X25 ADDR.

Enter the new beginning of X25 addresses (from 9 to 901).

CONFIRMATION

Click the bar to confirm the update.

6.5.7.3 *Display TCP port transl. - X25 addr.*

Menu **NETWORK AND LINKS>Data links>TCP/IP – X25 gateway>Disp. TCP port transl. - X25 addr.**

DIRECTORY NUMBER

Select the directory number of the gateway link.

The screen displays all the X25 numbers associated with the port numbers for the selected gateway link.

6.5.7.4 *X25 – IP address translation*

Menu **NETWORK AND LINKS>Data links>TCP/IP – X25 gateway>X25-IP address translation**

DIRECTORY NUMBER

Select the directory number of the gateway link. The screen displays the following field:

SUB-ADDRESS

2-digit X25 additional number. If the field is empty, the subaddress is 0FFH.

Note: As long as this number has not been entered, the following fields are not displayed.

From this menu you can modify the characteristics of a remote TCP server, but only if the associated gateway link is inactive.

The title displays the link's directory number.

SUB-ADDRESS

2-digit X25 additional number. If the field is empty, the subaddress is 0FFH.

IP ADDRESS

IP address of the LAN station: station to which the gateway should connect when it receives the sub-address.

PORT

Port number (up to 5 digits) of the LAN station to which the gateway should connect when it receives the sub-address: this number must be above 2000. If it is nil, the field is considered as empty.

MODE

By default, NOT DELIMITED mode is assigned.

ACTION

Save or delete.

Note: The PORT and IP ADDRESS fields must be filled in for the action to be valid.

6.5.7.5 *Display X25-IP addr. translation*

Menu **NETWORK AND LINKS>Data links>TCP/IP – X25 gateway>Disp. X25 – IP address translation**

DIRECTORY NUMBER

Select the directory number of the gateway link. The next screen displays the list of TCP servers (IP address and port) accessible from the iPBX through the sub-address, for the selected gateway link.

6.5.8 PARAMETERS

WARNING: Data link parameters may only be modified under the control of Technical Support.

Menu **NETWORK AND LINKS>Data links>Settings**

PARAMETER NO. IN DECIMAL

In this field, enter the number, in decimal, of the parameter to be modified.

TYPE OF VALUE

DECIMAL **DCB**

Indicate the value type.

DECIMAL VALUE

This line is displayed if the value type selected is DECIMAL.

Enter in this field the value of the parameter. Each parameter has a default value.

BCD VALUE

This line is displayed if the value type selected is DCB. Enter the parameter value in Binary Coded Decimal.

CONFIRMATION

After each modification, just click "Confirmation" to validate the operation.

6.6 INTERNET GATEWAY

Menu **NETWORK AND LINKS>Internet gateway**

The SBC provides the following services for trunk calls:

- Signal/media NAT
- Audio/video transport (interface with RTPProxy)
- Defence against DoS (flooding or hacking) and DDoS attacks

The function is not subject to licensing; however, the IPBX keycode must be entered. This command is used to configure the SBC Trunk integrated in the MiVoice 5000 Server solution. This service is used to manage NAT in case of access to an SIP (SIP trunk) operator for which the NAT problems cannot be solved by the operator.

The screen contains four tabs:

- The first one allows the general settings to be modified.
- The second one allows the security settings to be edited.
- The third one allows the white list addresses to be entered.
- The fourth one allows the blacklisted DoS addresses to be displayed, and this list to be partially reset.

For service and port-based DSCP encryption and configuration, see 6.4.6 Encryption and IP settings.

6.6.1 GENERAL SETTINGS

It is the first tab displayed by default. It fixes the general settings of the trunk SBC.

In case of modification, the service is automatically restarted when the operator exits the MMC or the general parameters tab.

If the **Internet gateway** box is ticked,

INTERNET GATEWAY SERVICE

Indicates the service status. Clicking the field name opens the services configuration menu in which the Internet gateway service may be stopped or started.

The general settings tab allows you to configure up to 5 IP addresses.

Addresses 0.0.0.0 and 255.255.255.255 are prohibited.

WORKING MODE

The following options for this parameter are:

- TRUNK SBC

- Chained – LAN element (R8.2 SP2 or later)
- Chained – WAN element (R8.2 SP2 or later)

OTT TERMINALS ALLOWED

Checkbox to allow the use of OTT terminals. Appears in R8.2 SP1 and later versions.

NAT ON PUBLIC INTERFACE

Checkbox for defining whether there is NAT on the public network side.

By default: box unticked.

If this box is ticked:

Public Interface

- Public interface options
- Port (UDP/TCP): 5062 by default (modifiable)

Private Interface

- Private interface options
- Port (UDP) and secure port (TCP): 5066 by default (modifiable)
- WebRTC (UDP/TCP) subscriber port: not applicable with the current version

NAT ON PRIVATE INTERFACE

Checkbox for defining whether there is NAT on the private network side.

By default: box not ticked.

If this box is ticked:

- Enter the IP address or FQDN of the iPBX seen from the SBC
- Default port 5060 (modifiable)

IPBX ADDRESS

- Enter the iPBX IP address or FQDN
- Default port 5060 (modifiable)

Trunk SBC

- Port: 5060 (not modifiable)
- Minimum RTP port (20000)
- Maximum RTP port (28000)

Changing the RTP port on renegotiation: Checkbox

Symmetric RTP support

Options for configuring the type of support for symmetric RTP:

- NO
- FOR EQUIPMENT WITHOUT NAT
- ALWAYS

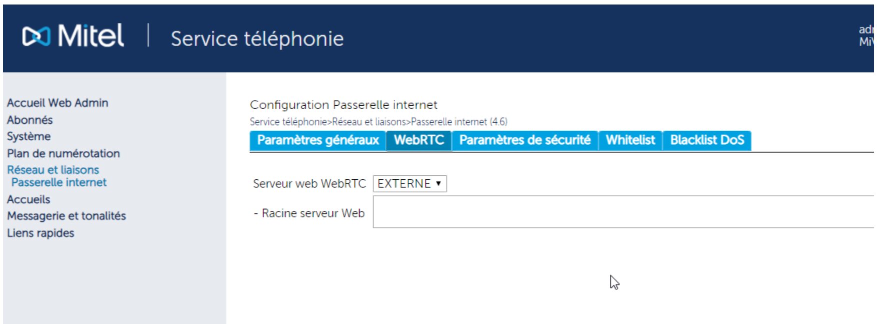
Leave at NO. The other options are not working in this release.

Apply the network topology hiding

For security, this box is checked by default and only concerns exchanges with trunks connected through the on-board SBC.

In the requests/responses sent by the SBC, the addresses of the local network will be masked.

6.6.2 WEBRTC



Configuration Passerelle internet

Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

Serveur web WebRTC: EXTERNE ▾

- Racine serveur Web:

6.6.3 SECURITY PARAMETERS TAB

SECURITY LEVEL

This first parameter is used to configure the deployed level of safety. Options list, possible three values:

- None: if the security level (Level "None") is not activated, the white and black lists are not taken into account for IP address filtering. Moreover, the following lines on this screen are hidden.
- Self-protection: for the "self-protection" level the Black list and White list serve as a filter.
- White list only: for the "whitelist only" level (for SBC only), only the "whitelist" entered by the operator serves as a filter.

DOS PARAMETERS

- Threshold: variation range of 10 to 5000
- Window (seconds): range from 2 to 10
- Period: options
  - 30 seconds
  - 5 minutes
  - 30 minutes
  - 1 hour
  - 1 day
  - 1 week
  - infinite.

DDoS parameter

- Threshold: variation range of 10 to 5000
- Window (seconds): range from 2 to 10

DELETING THE DoS BLACKLIST

The DELETE option empties the DoS blacklist.

6.6.4 WHITELIST TAB

For entering the 100 IP addresses used on the white list.

6.6.5 DOS BACKLIST TAB

This tab is displayed when security is implemented. It is used to see, at an instant T, the non-trustworthy IP addresses, preceded by the registration date and time.

The action possible on the list is deletion in the "Security settings" tab.

6.7 VPN TELEWORKING

Menu **NETWORK AND LINKS>VPN teleworking**

This command is used to configure the OpenVPN service integrated in the MiVoice 5000 Server solution. This service allows a remote worker to connect their BluStar 8000i to their company's telephony network from a remote LAN.

The screen contains 3 tabs:

- **Clients**,
- **Public settings**
- **Server**.

⚠ **IMPORTANT NOTE: As long as the certificate from the certification authority has not been created, no further configuration is possible.**

To configure the service, proceed as follows:

1. First fill in the **Public Settings** tab to define the certification authority.
2. Fill in the **Server**tab.
3. You can then create and manage clients in the **Client**tab.

6.7.1 MANAGE CLIENTS

This client management tab is the default tab shown on the screen.

VALIDITY PERIOD OF CLIENT CERTIFICATES

The default duration is 5 years. It can be odified.

AUTOMATICALLY AVAILABLE CONFIGURATION ARCHIVE

The box is ticked by default. In this case, the configuration archive can be downloaded when the client is created. The value of the **Configuration archive** column is **YES**.

For security reasons it can be unticked: the file then becomes downloadable on demand. The value of the **Configuration archive** column is set to **NO**.

These two parameters are valid for all clients.

6.7.1.1 *Client viewing table*

Each line shows a client. Client information is displayed in different colours, according to the status of the connection:

- green when the client status is connected
- black when the client status is disconnected
- orange when the client status is not configured.

CLIENT NAME

32 characters maximum, consisting of 26 alphabets, 10 digits, a dash (-) and an underscore (_).

VALID FROM / VALID TO

Period of certificate validity

CONNECTION

Indicates the connection status: **NOT CONFIGURED** / **DISCONNECTED** / **DATE and TIME** of connection when the connection is set up.

PUBLIC ADDRESS

Specifies the IP address from which the client connects to the server.

CONFIGURATION DATE

If the client status is different from NOT CONFIGURED, this column shows the configuration date. Date on which the configuration file was downloaded by the terminal.

CONFIGURATION ARCHIVE

By default, the value **YES** / **NO** depends on the value of the settings "**Automatically available configuration archive**" on top of the screen (YES if the box is ticked / NO if the box is not ticked).

To change the value, select the client then select **MODIFY THE CLIENT** (or **MODIFY ALL CLIENTS**) in "Action to be carried out"**.** The line **Available configuration archive** appears: tick or untick the box then click **CONFIRMATION**.

6.7.1.2 *Action to be carried out*

Following the table, the drop-down menu **ACTION TO BE CARRIED OUT** ... allows one of the following actions:

CREATE A CLIENT

Enter the name of the client to be added then click **Confirmation**. If the syntax corresponds to the one defined above, a check request can be made to check that the name is not already assigned.

MODIFY THE CLIENT / MODIFY ALL CLIENTS

These actions define whether or not the configuration archive is automatically available, either for the selected client or for all clients.

DELETE THE CLIENT / DELETE ALL CLIENTS

These actions allow you to delete the selected client or all clients. The client concerned is disconnected if it was connected, the certificate is revoked and the configuration archive is deleted.

GENERATE THE CERTIFICATE / GENERATE ALL CERTIFICATES

These actions allow you to generate the certificate for the selected client or for all clients. The client concerned is disconnected if it was connected, the old certificate is revoked and a new configuration archive is created.

AVAILABLE CONFIGURATION ARCHIVE

This checkbox allows you to define for the selected client (or for all clients) whether the configuration archive is available (downloadable) or not. The change must be confirmed by clicking **Confirmation**.

If the box is ticked, the URL on which the configuration archive is available is:

https://PBX_IP@/bs/client_name.tgz

⚠ **WARNING: The administrator is fully responsible for making this file available on a public network.**

6.7.2 MANAGING PUBLIC SETTINGS

⚠ **WARNING: The settings of this screen can only be modified if the TEL VPN service is stopped (see § Managing server settings).**

SERVER NAME OR IP ADDRESS

Enter the Mitel 5000 Server name or public IP address.

PORT

Enter the default OpenVPN port.

Once any of these areas is modified, the action to be carried out at the bottom of the screen proposes to back up the parameters.

CERTIFICATION AUTHORITY

The following parameters are used to describe the certification authority.

The following fields are free input fields:

- **Country** (max. 2 characters)
- **Region** (max. 128 characters)
- **Town** (max. 128 characters)
- **Organization** (Company name: max. 64 characters)
- **Certificate name** (max. 128 characters)

Once any of these areas is modified, the action to take at the bottom of the screen proposes to back up the parameters.

DATES OF THE CERTIFICATE VALIDITY

The certificate validity dates are assigned by generating the certificate. By default, the validity period is 10 years and is not configurable.

6.7.2.1 *Action to be carried out*

The action to be carried out differs according to the type of change made:

- Back up settings: applies to public server settings
- Back up and generate certificate: applies to the settings of the certification authority.

⚠ **WARNING: Any backup request implies reconfiguring each client.**

6.7.2.2 *Export the certificate*

The **Export the certificate** button makes the certificate file available in PEM format. To download the certificate, click on the link **Download the certificate** which also indicates the name of the certificate.

Generating the authority certificate involves:

- generating the server certificate
- generating each client certificate.

6.7.3 MANAGING SERVER SETTINGS

TEL VPN SERVICE

Indicates the service status. When the field name is clicked a link opens the services configuration menu in which the TEL VPN service may be stopped or started.

⚠ **WARNING: The settings of this screen can only be modified if the TEL VPN service is stopped.**

LOCAL SERVER PARAMETERS

The server IP address must be selected from the list of addresses configured on the server. The port is not modifiable.

CERTIFICATE SERVER NAME

Free-input field.

The fields that appear filled in are taken from the certification authority (public settings).

DATES OF THE CERTIFICATE VALIDITY

The certificate validity dates are assigned by generating the certificate. By default, the validity period is 10 years and is not configurable.

6.7.3.1 *Action to be carried out*

The action to be carried out differs according to the type of change made:

- Settings backup: applies to changing the server IP address.
- Back up and generate certificate: applies to the modification of server certificate name. Generating the certificate does not imply reconfiguring each client.

6.7.3.2 *Export the certificate*

The **Export the certificate** button makes the certificate file available in PEM format. To download the certificate, click on the link **Download the certificate** which also indicates the name of the certificate.

7 CALL DISTRIBUTION MANAGEMENT

This management domain is all about managing incoming calls according to:

- Timeslot (according to a calendar)
- Call origin (PSTN, TL or internal)
- Call number (special treatment for DISA number, for instance).

It also all about defining:

- The operator services on which incoming calls are distributed
- Interactive voice server (IVS) scripts
- DISA scripts
- answering services

Call distribution is managed from the menu **TELEPHONY SERVICE>CALL DISTRIBUTION**.

7.1 CALL DISTRIBUTION MANAGEMENT

Menu **RECEPTION>Call distribution management**

This menu is used to configure and display the different call distribution options available on the iPBX.

☞ For a multi-company configuration, an additional menu **Display by company** is proposed.

A call distribution service defines the way in which incoming calls are answered in three service modes:

- Normal day service
- Reduced day service
- Night service

"Normal day" mode is the normal answering mode for calls in the day period.

"Reduced" mode is the mode used during the day, if the normal day operator groups are deactivated.

"Night" mode is used in calendar night periods and if all the day operator groups are deactivated. (If even one of these operators is present, the "day" mode is used).

The answering service can be defined on an attendant console or on a set. It may be handled by 3 different answering services if the calls are from the public switched network, TLs or internal users (order line).

A day/night calendar which manages the answer mode for incoming calls is associated with each call distribution service. This calendar is defined in “CALL DISTRIBUTION>Calendars” and assigned to call distribution in **CALL DISTRIBUTION>Call distribution management>Definition**.

7.1.1 CALL DISTRIBUTION NAMES

Menu **CALL DISTRIBUTION>Call distribution management>Characteristics, Names** tab

This command is used to display the list of call distribution operations declared already on the system, and to declare new ones.

Like other entities, a call distribution service is defined by a name and cannot be managed or allocated unless it features a name.

This menu is therefore used to define the various call distribution services available in the system. Call distribution service C. DIST .0 is provided on installation.

The system proposes 64 call distribution names (with the possibility of one per company in multi-company configuration).

Each call distribution service is designated by a name and can only be managed if its name has been declared.

This name can contain up to 16 characters.

Note: In the case of multi-company configuration, it is advisable to use the COMPANY NAME for the CALL DISTRIBUTION NAME.

C. DIST. 0

You will find in this field the call distribution service C. DIST. 0 provided upon system installation.

Note: The default call distribution service, C. DIST 0, can be renamed.

CALL DIST. 1 TO 63

Call distribution name (from 0 to 63): these fields are used to create additional call distribution services besides the default one.

7.1.2 CALL DISTRIBUTION DEFINITION

Menu **HOME>Call distribution management>Characteristics, Definition tab**

This command is used to configure the call distribution services declared on the system.

Select the name of the call distribution service to be configured in the drop-down list then click **Select the item**.

7.1.2.1 *Call distribution ACC.0 definition*

This screen is used to define the distribution of incoming calls in the three service modes.

As of R8.0, the local reception can be defined on a Calendar basis by ticking the ACD for local calls: priority to D/N calendar box in the **System** tab of the **Telephony service>Subscribers>Rights>General settings** menu (Se refer to paragraph 3.9.1.3).
This only applies to call distribution services served by a subscriber or hunt group. Please refer to the relevant Release Note.

DAY: ROUTED TO

Name of operator group (OPGP1 to OPGP15), dissuasion message or internal extension (directory number) for day routing.

The definition of DAY ROUTING: ROUTED TO OP GP 1 to OP GP15 corresponds to normal operation (day and night, with the operator console active).

OR TO DIRECTORY NUMBER

Directory number of the set or group of sets assigned to day routing.

REDUCED: ROUTED TO

Name of operator group (OPGP1 to OPGP15), dissuasion message or internal extension (directory number) for reduced day service routing.

The definition of REDUCED SERVICE ROUTING: TO OPGP1 to OPGP15 corresponds to reduced day service. (ATDC deactivated during calendar day periods).

OR TO DIRECTORY NUMBER

Directory number of the set or group of sets assigned to reduced day service routing.

Note: Reduced day service call distribution is also used when the set assigned to day call distribution is busy 2.
If the terminal assigned to reduced day call distribution is busy, calls are routed to the service group defined in the characteristics of the trunk group on which the call is received (see the menu NETWORK AND LINKS> Network> Trunk groups> Characteristics).

NIGHT: ROUTED TO

Select the name of an operator group (OPGP1 to OPGP15), a dissuasion message, or an internal set (directory number) for night routing.

The definition of NIGHT ROUTING: TO OPGP1 to OPGP 15 corresponds to reduced night service (ATDC deactivated during calendar night periods).

OR TO DIRECTORY NUMBER

Directory number of the set or group of sets assigned to night routing.

REFERENCE CALENDAR

Name of the reference calendar to determine the switch-over from reduced service routing to NIGHT routing and vice-versa, when day routing is deactivated.

Note: If the terminal assigned to night call distribution is busy 2, calls are routed to the service group defined in the characteristics of the trunk group on which the call is received (see NETWORK AND LINKS> Network>Trunk groups> Characteristics).

CALL DISTR. AUTHORIZ. BY EXTERIOR

NO **YES**

If you select YES, call distribution may be handled by a remote set in case of no answer (case of networking on a QSIG trunk group; see also “Characteristics of a QSIG trunk group”).

Once you select YES for this field, the screen is refreshed to display the parameters used to configure the distribution of incoming external calls arriving on this call distribution service.

Example:

If the INTERNAL DAY DIRECTORY NUMBER does not answer, the call is forwarded to the remote terminal defined by the field DAY: ROUTED TO #

Moreover, if the parameter RETURN TO INTERN. REDCD. ANSW. S is set to YES and the remote terminal fails to answer, the call is forwarded to the REDUCED INTERNAL DIRECTORY NR. If this latter does not answer, the call is forwarded to the number indicated in REDUCED: ROUTED TO #

DAY: ROUTED TO

Directory number of the remote set that will be assigned to day routing in case of no answer from the internal extension with the same function.

RETURN TO INTERN. REDCD. ANSW. S

NO **YES**

If you select YES, return to reduced internal call distribution is authorised.

REDUCED: ROUTED TO

Directory number of the remote set that will be assigned to reduce service routing in case of no answer from the internal extension with the same function.

RETURN TO BACKUP CALL DISTR.

NO **YES**

If you select YES, return to backup call distribution is authorised.

Note: The emergency answering service is the night forwarding service extension. It is defined by the parameter FORWARD CONSOLE TO DN, in the answering service definition menu.

NIGHT: ROUTED TO #

Directory number of the remote set that will be assigned to night routing in case of no answer from the internal extension with the same function.

RETURN TO BACKUP CALL DISTR.

NO **YES**

If you select YES, return to backup call distribution is authorised.

7.1.3 CALL DISTRIBUTION ALLOCATION (SINGLE-COMPANY CONFIGURATION)

Menu **CALL DISTRIBUTION>Call distribution management>Characteristics, Allocation tab**

This command is used to assign a call distribution service to each type of call and to define the common bell number.

IMPORTANT NOTE: This command is only available in single-company configuration. In a multi-company configuration, call distribution services are assigned in the company/department definition menu SUBSCRIBERS>Hunt groups and companies>Multi-company management>Company/department settings.

https://www.msn.com/fr-fr/feedBy default, the three traffic flows (PSTN + return on no answer of a set in DID + TL + internal) are routed to the same call distribution service (ACC.0). This allocation is only valid for trunk groups or lines which have declared an incoming route on a "call distribution service".

However, it is possible to select a different call distribution service for each type of traffic flow (PSTN, TL, and internal).

PSTN CALL DISTRIBUTION

Call distribution name for calls received from the public exchange (ISDN and ANALOGUE PSTN): the default call distribution service is ACC.0.

VIP CALL DISTRIBUTION

Call distribution name for calls received from the public exchange for VIP calls (configured in an internal or external record with the VIP setting activated): the default call distribution service is ACC.0.

TIE LINE CALL DISTRIBUTION

Call distribution name for calls received from the TL network (tile line): the default call distribution service is ACC.0.

INTERNAL CALL DISTRIBUTION

Call distribution name for calls received from the LAN (internal calls from the ATDC): the default call distribution service is ACC.0.

COMMON BELL DN

Internal directory number of the common bell (this number must be in the subscriber dialling plan):

- Either "798" (on NeXspan S/L/D) corresponding to the integrated bell relay command
- or a directory number of an analogue equipment interface to which an external bell is to be connected

7.1.4 DISPLAY CALL DISTRIBUTION (MULTI-COMPANY)

Menu **CALL DISTRIBUTION>Call distribution management>Characteristics, User tab**

This command is used to display the list of users of a given call distribution service.

Note: Call distribution user display is available in multi-company configuration only.

CALL DISTR NAME

The drop-down list contains the names of call distribution services declared on the iPBX.

Select a call distribution service from the drop-down list then click **Select the item**.

Note: Only the columns with at least one call distribution user are displayed.

The call distribution user display screen shows, for each call type, the company/department pair used. It also shows each DID corporate number whose routing has been defined on this call distribution service, as well as the company/department pair it is using.

DISPLAY ...	MEANING:
******** ********	for all the departments of all the companies
Cmpny 0 ********	for all the departments of “company 0”
Cmpny 0 ********	for the “doc department” of “company 0”

For a given call distribution service, when any of the lines is clicked, the user interface redirects the user to call distribution assignment in the company/department definition menu **SUBSCRIBERS>Hunt groups and companies>Multi-company management>Company/department settings** (multi-company configuration).

7.1.5 CALL DISTRIBUTION STATUS DISPLAY

Menu **CALL DISTRIBUTION>Call distribution management>Characteristics, Statuses tab**

This command is used to know at a given moment the status of each of the call distribution services, and therefore, the resulting overall service.

A call distribution service can be in the following 3 statuses:

- Day
- Reduced
- Night.

CALL DISTRIBUTION

Name of the call distribution service.

TYPE

Current status of the call distribution service.

Possible values are: day, night or reduced.

HANDLED BY

Current routing of calls arriving on the call distribution service.

Possible values are: directory number, attendant console or dissuasion message.

7.1.6 C.DISTR. DISPLAY BY COMPANY

Menu **RECEPTION>Call distribution management>Display by company**

This command is used to display the call distribution services to which calls are routed by type, day of the week and time.

IMPORTANT NOTE: The display of the call distribution services by company/department only appears in multi-company configuration.

COMPANY

********	CMPNY.0

Company name.

The drop-down list contains the names of companies created in the system.

CALL TYPE

PSTN	VIP	TL	INTERNAL

Types of calls for which display is required.

DAY OF THE WEEK

-------	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY	SUNDAY

Day of the week for which the display is required.

TIME HH: MM

Time: HH MM (HH=hour, MM=minute) for which the display is required.

Select the criteria then click **Select the item**. The next screen summarises the use of call distribution services by each of the departments in the company, from the required date (day, time) until the date on which a modification may be made.

Note: The required date and time are indicated in the screen header.

The display screen table indicates for each department that uses a call distribution service on the required date:

- The department name
- The name of the call distribution service used
- The status of the call distribution service
- The routing for the call distribution service
- The expiry date and time of the information displayed.

7.2 IVR SCRIPTS MANAGEMENT

Menu **CALL DISTRIBUTION>IVR scripts**

IVS (or IVR) is the interactive voice response function integrated into Mitel 5000 Server.

Interactive voice response is a special subscriber (AUTOMATED ATTENDANT) to which an IVS script is assigned.

The capacities and occupation rates of message formats are indicated in Menu **System>Supervision>Disk space filling**.

When a call arrives on its number, the associated script presents some messages to the caller.

Depending on the answer given to a message by the caller (in form of Q23 codes corresponding to keys “1”, “2"... «9», «*», «#» on the telephone keypad), either a new message is presented to the caller or an action is triggered such as a transfer to an internal subscriber.

An IVR script is a tree of nodes; each node is associated with an IVR message, that is a sound file or video file on MiVoice 5000 Server.

If the script is multi-lingual, a message per language may be assigned to each node.

The IVS messages on the iPBX are stored in distinct directories for each language, and there is no sharing of files between two languages.

IMPORTANT NOTE: The sound files correspond to the IVR messages that must be recorded in this format: 8 bits WAV, A law, µ law, Mono at 8Khz or mp3. The compression law must be compliant with the law of the country in which the iPBX is used.

On MiVoice 5000 Server, the sound file may be stored in linear PCM format - **16 bits/16 Khz** mono - and the audio file in H264 avi format (baseline profile).

The IVR script management menu is used to manage, modify and delete up to 15 IVR scripts. The IVS can be activated once the scripts are developed. An example of activation is given in *7.2.6*.

Note: Generally, a company uses 1 or 2 scripts, typically a day call distribution service and a night call distribution service, and provides its own recorded announcements with a given studio voice. It is, therefore, advisable to use the company name as prefix for the sound files because two companies are not likely to use the same file. Moreover, this facilitates script and announcement management.

IVR scripts are managed from the following tabs:

- Names: this tab is used to declare the scripts on the system.
- General characteristics: this tab is used to define all the parameters that are common to all the nodes of a script.
- Tree: this tab is used to describe the script nodes.
- Copy: this tab is used to copy a script to another script, for instance, in order to modify it without disturbing the behaviour of the script in operation, or to share announcements between several scripts (see Point *3* in the next paragraph).

The **Users** tab is used to view the users of the script in question.

7.2.1 GENERAL RULES APPLICABLE TO IVS SCRIPT MANAGEMENT

1. A script may exist in one or more languages. Each script may use a maximum of 3 languages, and all the scripts may use a maximum of 8 different languages.

2. In the language name drop-down list, an arrow in front of the language name indicates that this language is used by at least one script:

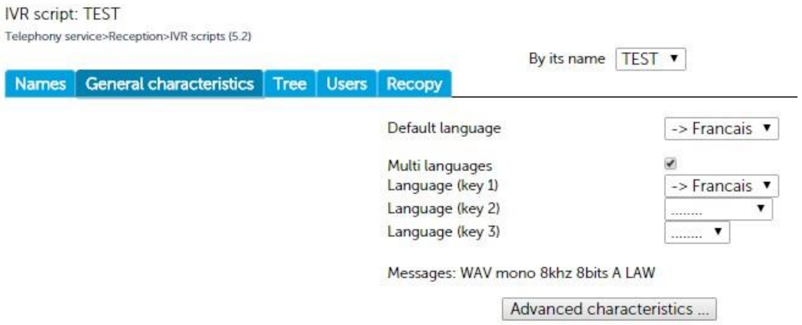
3. An announcement may be used by only one script, except in the special case where a script is copied. This constraint means that if two scripts must present the same announcement to a caller, this announcement must be available in two copies, under two different names. As indicated above, the need to share announcements among several companies is very unlikely due to the consistency of recording voices. On the other hand, within the same company, it is possible that two scripts use the same generic announcements. To avoid this constraint, it is advisable to create a first script then make one or more copies of this script and modify the tree for each copy, according to the needs.

4. When a file name is available in an announcement definition field, there is a hypertext link on the name of the field.

- Left-clicking this link plays back the announcement, provided a .wav or mp3 file player is available on the PC.

- Right-clicking this link saves the announcement on the PC.

5. To be able to untick an option with which an announcement is associated, you must also delete the association with the corresponding announcement. This action is proposed by the graphical interface and illustrated by the following example:



IVR script: TEST

Telephony service>Reception>IVR scripts (5.2)

By its name: TEST ▼

Default language: -> Francais ▼

Multi languages: ☑

Language (key 1): -> Francais ▼

Language (key 2): .... ▼

Language (key 3): .... ▼

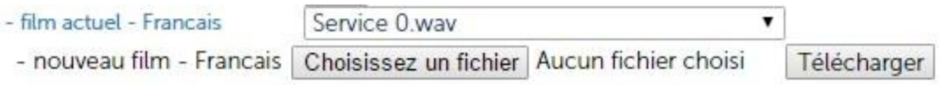
Messages: WAV mono 8khz 8bits A LAW

In this example, the multi-language option has been unticked after being ticked. The "Supp language and associated files" confirmation button is used to validate the action, and the file ***selection langue.wav*** becomes an unused announcement if it is not used elsewhere.

6. The drop-down list of fields used to associated an announcement with a node contain some actions and, possibly, some file names if some announcements are already being used by the script.
The dropdown list is used to check whether or not an announcement has already been associated.

The file names located above the horizontal line correspond to the files used already in the script for the language in question. The ones below the horizontal line are files available on the iPBX but which are not used for the language concerned.

Note: The files used by another script or another language of the script are not available on the drop-down list.

REPLACE THIS MESSAGE BY A NEW	The following download field appears:  - film actuel - Francais Service 0.wav ▼ - nouveau film - Francais [Choisissez un fichier] Aucun fichier choisi [Télécharger] Press the “Browse…” button to open a browser. Select the file you want then click “Download”. **NOTE: all the occurrences for the file will be replaced and not just the ones corresponding to the field in which this choice is made.**

DO NOT USE THESE MESSAGES	Deletes the association of the announcement(s) with the script node **General characteristics** tab: deletes the announcement(s) from the iPBX if there is no other usage occurrence (in any of the scripts). In the **Tree** tab: the announcement is not immediately erased; so, it can be used again by another node. It will be deleted after a new IVR is added or when the PBX is restarted. **Note: if the script is multi-lingual, these actions apply to all the announcements associated with the script node.**

File name	The announcement corresponding to the selected file is associated with the script node.

7. An announcement associated with a LONG MESSAGE node is an announcement through which it is possible to navigate.
   The following navigation codes are available while a LONG MESSAGE type announcement is being broadcast:

- 77: replay message
- 7: rewind for 3 seconds
- 8: pause/play
- 9: fast-forward for 3 seconds
- 99: end of message

7.2.2 DECLARING A SCRIPT

Menu **CALL DISTRIBUTION>IVR scripts – Names tab**

An IVS script is identified by name. To be able to create a script, you must first declare it after giving it a name.

IVS SCRIPT X

Script name (8 characters maximum).

Note: The 15 possible scripts are numbered 0 to 15, the number 10 is excluded.

7.2.3 GENERAL CHARACTERISTICS OF A SCRIPT

Menu **CALL DISTRIBUTION>IVR scripts – General Characteristics tab**

This menu is used to define the general properties applicable to all the nodes of a script (for instance, the choice of languages), as well as the generic behaviour of each of the nodes (actions and associated announcements available to each script node; for instance accesses to the control menu).

BY ITS NAME

Name of the script.

The drop-down list contains the names of the scripts declared in the system.

7.2.3.1 *Languages choice*

DEFAULT LANGUAGE

Option for choosing the language to be used.

- Single-language mode
- Multi-language mode, to broadcast the language selection message and the message associated with the Q23 test if available.

The default value for this field is the iPBX language.

Note: The value selected for the default language is used to manage the language directories on the iPBX and is not necessarily the actual language of downloaded announcements.

MULTI LANGUAGES

If the box is ticked, the script will be available in several languages, provided the corresponding announcements are available.

Once the box is ticked, the language parameters corresponding to multi-language mode are displayed on the screen:

LANGUAGE

These three columns are used to define up to 3 languages for the script.

Note: The value selected for a language is used to manage the language directories on the iPBX and is not necessarily the actual language of downloaded announcements.

CURRENT MESSAGE

This field appears once two languages are chosen. This announcement will be presented to the user so he can choose the script execution language. This announcement is unique (it is not multi-lingual) and is stored in the default language directory.

WARNING: If the default language of the script is changed, the announcement is not copied to the directory of the new default language.

See the description of the values in Paragraph 7.2.1 Point 6.

VIDEO MESSAGES

Box to be ticked if the script accepts some video files. This allows the display of information about the types of files authorised for downloading. In this case, the **avi** line is displayed in the following information columns:

MESSAGES: WAV MONO 8KHZ 8BITS A LAW OR MP3

- wav mono 16khz 16bits PCM

avi

Information indicating the formats that must be respected for message file names.

Note: There is no processing of video file deletion when the Video messages checkbox is unticked.

After entering the parameters, click **Advanced characteristics**… to move to the next screen:

7.2.3.2 *Q23 test and access to control menu*

Clicking **Advanced characteristics …** opens the following columns:

- Conduct a Q23 test at the start of a script to check that pressing a key on the calling device's keypad actually transmits a Q23 code, which is necessary for interactive navigation during script execution

- Give access to the control menu from any script node.
  The control menu gives access to the following 4 operations through the numeric keys on the keypad:

- Playing back the help message (key 1)

- Returning to the beginning of the script (key 2)

- Transferring a call to the ATDC (key 3)

- Returning to the previous node (key 0).

Note: The values for these keys are not configurable.

Q23 TEST

If you tick the box, a Q23 test will be conducted at the start of script execution.

Once the box is ticked, the field used to associate an announcement appears on the screen:

- CURRENT Q23 TEST MESSAGE

See the description of the values in Paragraph 7.2.1 Point 6.

Note: It is advisable to associate an announcement prompting the caller to press a key on his keypad.
This announcement exists only in one language and is downloaded to the default language directory.

MENU OF CONTROL (NAVIGATION BY *)

If you tick this box, the control menu will be accessible using the * key from any script node.

Once the box is ticked, the fields used to associate an announcement with the * key and the help key are displayed on the screen:

- MESSAGE CURRENT CONTROL - LANGUAGE

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

- KEY 1 – HELP MESSAGE (77 7 8 9 99)

Information string indicating the key to use to play back the help message, as well as codes used to navigate in the help message which is a long message.

- CURRENT HELP MESSAGE - LANGUAGE

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

- KEY 2 - RETURN AT BEGIN OF IVS

- KEY 3 - ATD TRANSFER

- KEY 0 – EXIT CONTROL

Information string indicating the key to use for the actions described.

After entering the settings, click **Advanced characteristics**… to move to the next screen:

RETURN TO PREVIOUS NODE BY KEY 0

If you tick this box, the 0 key can be used to return to the previous node from any node of the script.

The box is ticked by default.

HANG UP MESSAGE

This message is optional.

The checkbox is used to activate or deactivate it.

During deactivation, the system proposes to delete the associated files.

- Current message - language

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

INCORRECT INPUT MESSAGE

This message is optional.

The checkbox is used to activate or deactivate it.

During deactivation, the system proposes to delete the associated files.

- Current message - language

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

NO INPUT MESSAGE

This message is optional.

The checkbox is used to activate or deactivate it.

During deactivation, the system proposes to delete the associated files.

If you tick the box, a message will be presented to the caller at the end of the timeout (period of inactivity).

Once the box is ticked, the fields used to associate an announcement with the end of the timeout appear on the screen:

- Current message - language

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

DEFAULT TRANSFER MESSAGE

This message is optional.

The checkbox is used to activate or deactivate it.

During deactivation, the system proposes to delete the associated files.

If you tick the box, a message will be presented to the caller for any type of transfer.

Note: The default transfer message is also associated with any transfer with which no specific message is associated.
- The specific message for transfer to the attendant console may be defined on this screen,
- The messages for other transfers may be associated with the corresponding nodes while describing the script tree.

Once the box is ticked, the fields used to define the default transfer message are displayed on the screen:

- Current message - language

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

TRANSFER TO THE ATD MESSAGE

This message is optional.

The checkbox is used to activate or deactivate it.

During deactivation, the system proposes to delete the associated files.

If you tick the box, a specific message will be presented to the caller for transfer to the attendant console.

If this box is ticked and a **default transfer message** is defined, this message will be presented to the caller.

Once the box is ticked, the fields used to associate an announcement with transfer to a predefined number appear on the screen:

- Current message - language

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

DIAL MESSAGE

Note: The dial message is optional.

If you tick the box, a message will be presented to the caller waiting to dial.

Once the box is ticked, the fields used to associate an announcement with the dial message appear on the screen:

- Current message - language

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

NUMBERING CLOSED BY #

If you tick this box, the number entered when the dial message was broadcast is considered as complete when # is entered.

If the box is not ticked, the number entered is considered as complete when the number of digits dialled reach the internal dialling plan length.

ACTION IN CASE OF FAILURE

Options for the action to take in case of failure:

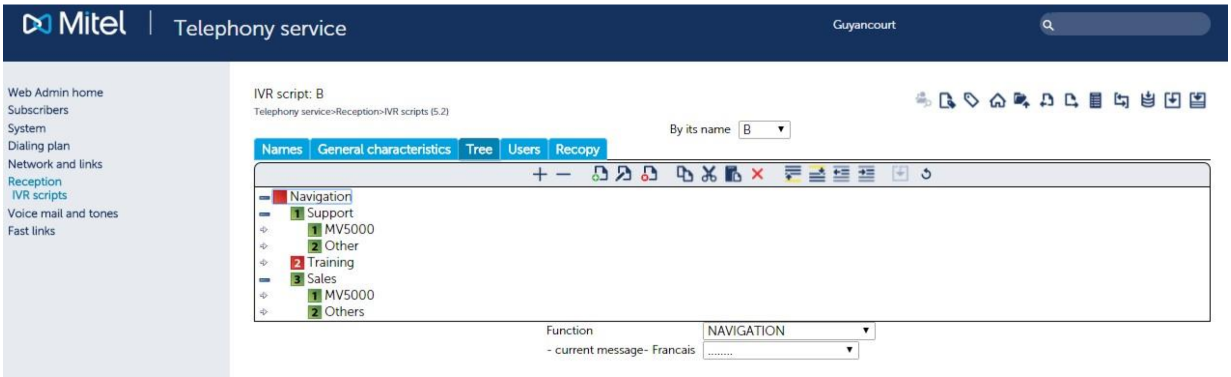
- **TRANSFER TO ATD**,
- **TRANSFER TO SUBSCR.**: In this case, enter the internal subscriber number to be reached.
- Hang-up.

7.2.4 SCRIPT TREE DIAGRAM

Menu **RECEPTION>IVR scripts** – **Tree** tab

This Tab is used to create and/or modify an IVR script using a graphic tool.

7.2.4.1 *Overview of the graphic tool*



IVR script: B

Telephony service>Reception>IVR scripts (5.2)

By its name: B

- Navigation
  - 1 Support
    - 1 MV5000
    - 2 Other
  - 2 Training
  - 3 Sales
    - 1 MV5000
    - 2 Others

Function: NAVIGATION

- current message- Francais: ....

Script tree diagram: graphic tool

The script tree diagram screen is divided into two parts:

The upper part gives a graphic representation of the script tree diagram; this area contains 4 tree-related buttons (see description below).

The lower part, which is only displayed if a tree node is selected, concerns this node; this area contains only one button, 🔄, used to update the tree diagram, taking account of the changes made to the node in the lower part.

Icons:

The icon in front of the name of a node indicates the associated DTMF, that is the key used to access this node while executing the script, for example 3.

There are three exceptions to this rule which are node not accessible via a code:

- The first node of the script whose icon does not contain any character: 🟩
- A child node of a LONG MESSAGE type node: ✓
- A new node which has not yet been backed up: ?

A green icon means that the node definition is complete (parameters and associated announcements).

Note: A TRANSFER type node, the action of which can be carried out with or without an associated announcement (to ATDC, subscriber or voice mailbox), is deemed complete even if it has no associated announcement.

A red icon means that:

- Either the node definition is incomplete
- The tree was not backed up after this node was modified.

- Or the node is a child of a node that does not accept any child node (after a node is moved or after a copy/paste).

Note: The first node on the tree diagram remains red even if its parameters and associated announcements are defined, if at least one obligatory announcement is missing in the general characteristics of the script.

<u>Tree and actions display</u>:

- Clicking an item selects this item and opens the lower part of the screen for this item.
- The keypad “up” and “down” arrows are used to move the selection.
- Clicking ⊞ or ⊟ icon located in front of a node reduces or develops this node. The "left" and "right" arrow keys have the same effect on the selected node.
- The "*" key on the numeric keypad develops all the child nodes of the selected node.
- Double-clicking an item or pressing the "F2” key when an item is selected changes to edit mode for its label.
- In node label edit mode, pressing the "Enter” key validates the modification, while pressing the “Esc” key cancels the last action taken since the last entry in edit mode.
- Pressing "Ctrl+c" copies to a buffer the selected node and its descendant.
- Pressing "Ctrl+v" pastes the content of the buffer as first child node of the selected node.
- It is possible to drag and drop a node with the mouse:
- Select the node.
- Place the cursor on the name of the node.
- Then move the cursor to the target node (the moved node will be inserted as child node of the target node).

WARNING: It is possible, through copy/paste or drag and drop, to create a child node under a node that does not accept any child node. In this case, you have to cancel the operation by deleting the newly pasted or moved node (the nodes that accept child nodes are SURF and LONG MESSAGE).

Pressing "Ctrl+z" cancels the last movement made.

<u>Buttons</u>:

- Buttons used to take actions in the upper part of the screen:

New	If a node is selected, this button inserts a child node under this node. If no node is selected, it inserts the child node of the first node. In both cases, the insertion is made following the last existing child node.
Delete	Deletes the selected node as well as its descendant.
Save	Saves the tree in the iPBX data. **WARNING: all the changes made since this button was last used (or since entry in the graphic tool) are**

	local and will be lost if they are not backed up). This button is only active if some modifications have not yet been backed up. The backup operation assigns a DTMF code to new nodes, starting with the first one available in the branch.
Cancel	Cancels all the modifications made since the last backup operation (or since entry in the graphic tool if no backup has been made). This button is only active if some modifications have not yet been backed up.

Interactive button between both parts of the screen:

↻	Updates the tree with the modifications made in the lower part of the screen.

7.2.4.2 *Description of a script*

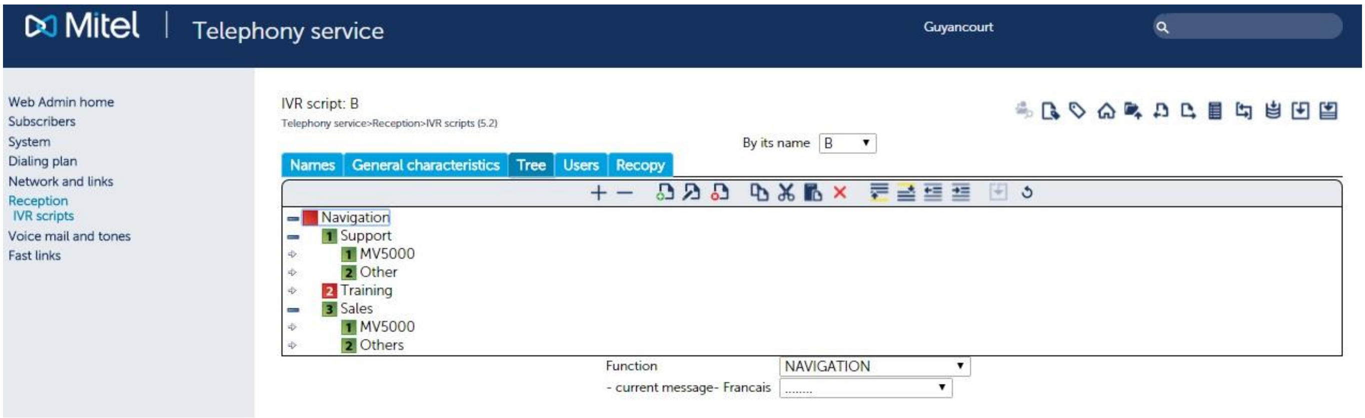
To access a script's tree, click "Script tree diagram" from the IVS script management menu:

BY ITS NAME

Name of the script.

The drop-down list contains the names of the scripts declared in the system.

Select a script then click **Select the item**.



IVR script: B

Telephony service>Reception>IVR scripts (5.2)

By its name: B

- Navigation
  - 1 Support
    - 1 MV5000
    - 2 Other
  - 2 Training
  - 3 Sales
    - 1 MV5000
    - 2 Others

Function: NAVIGATION

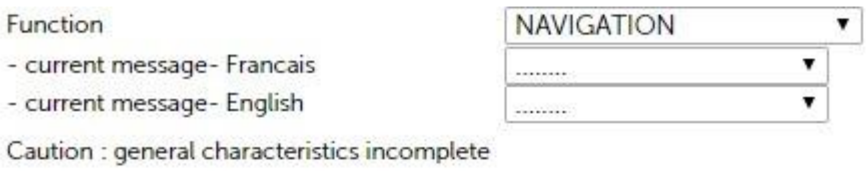
- current message- Francais: ....

Script tree diagram

The tree is modified as described in Paragraph *7.2.4.1*.

To be able to enter a node’s parameters, you must first create and save the node using the **Save** button.

To define the parameters of a node, select the node on the tree. The lower part of the screen opens:



Function: NAVIGATION ▼

- current message- Francais: .... ▼

- current message- English: .... ▼

Caution : general characteristics incomplete

Tree structure of a script: node settings

The parameters that appear on this screen depend on the value of the first parameter FUNCTION.

FUNCTION

Indicates the type of action that will be taken during script execution.

SURF	Accessing one of the child nodes with the help of a key.
LONG MESSAGE	Broadcasting a long message.
GO TO EXISTING NODE	Connecting to one of the tree nodes.
TRANSFER TO ATD	Script output and call transfer to the attendant console.
IVS BOX TRANSFER	Script output and call transfer to the IVS box.
TRANSFER TO SUBSCR.	Script output and call transfer to a number defined in the script.
SUBSCR. BOX TRANSFER	Script output and call transfer to the voice mail box of a number defined in the script.
TRANSFER TO NUMBER	Script output and call transfer to the number entered by the caller.
HANG-UP	Script output.

DTMF CODE

Code for the key that gives access to this node.

Possible values are [1, 2, …9].

Note: Several child nodes of the same node cannot have the same DTMF code.

Note: This field is available for all the nodes, except for the first node of the script and for a long message output node.

- CURRENT MESSAGE - LANGUAGE

This field is available for each of the languages selected for the script.

See the description of the values in Paragraph 7.2.1 Point 6.

Note: This field is available for all the nodes, except for the following node types:
- GOTO TO EXISTING NODE
- TRANSFER TO ATD (messages defined in the general characteristics of the script)
- HANG-UP (messages defined in the general characteristics of the script).

- INTERNAL NUMBER

A subscriber’s number.

This number will the used to transfer the call:

- To the subscriber if the node's function is TRANSFER TO SUBSCR.
- To the subscriber's voice mail box if the node's function is SUBSCR. BOX TRANSFER.

Note: This field is only available for the following node types: TRANSFER TO SUBSCR. And SUBSCR. BOX TRANSFER.

DESTINATION NODE

Name of the connection node on the tree.

The drop-down list contains all the names of the nodes defined already in the script.

Note: This field is only available for the node type GO TO EXISTING NODE.

7.2.5 COPYING SCRIPTS

Menu **CALL DISTRIBUTION>IVR scripts Copy tab**

This command is used to copy an existing script to another one. It is also used to:

- Modify a script and update it without disturbing the working of the IVS
- Share messages (e.g. generic messages) between several scripts: in fact, copy of script is the only case in which two scripts can use the same message without this message having to be copied under two different names.

Note: Scripts from a copy sharing announcements with the source script.

COPY THE SCRIPT

Name of the source script.

The drop-down list contains the names of the scripts declared on the iPBX.

IN THE SCRIPT

Name of the target script.

The drop-down list contains the names of the scripts declared on the iPBX.

Select the scripts then click "Confirm".

WARNING: The content of the target script is overwritten through this operation.

7.2.6 DISPLAY USERS OF AN IVR SCRIPT

Menu **CALL DISTRIBUTION>IVR scripts, Users tab**

This command is used to know the numbers of AUTOMATIC ATDC type subscribers using a given IVR script.

BY NAME

Name of the script.

The drop-downlist contains all the names of the IVR scripts defined on the system.

Select a script then click **Select the item**:

The list of AUTOMATIC ATDC subscribers to which the script is assigned appears.

7.3 OPERATOR MANAGEMENT

Menu **RECEPTION>Operators**

This menu is used to configure the operator services available on the iPBX. It only concerns the attendant consoles integrated in the iPBX.

Note: This menu concerns only the attendant consoles integrated in the iPBX. When the ATDC service is offered by the CC (Web Attendant), this menu is not used.

7.3.1 PARAMETERS

Menu **CALL DISTRIBUTION>Operators>Settings**

This screen is used to configure the general parameters (authorisations, timeouts) of attendant consoles (ATDC).

OPERATOR PARAMETERS

AUTOMATIC CALL DISTRIBUTION

This option is only for class B attendant consoles. If you tick the box, incoming calls are routed to the attendant console with the lowest traffic level.

If you select this option, you can use the interactive keys on the attendant console to activate automatic call-pickup mode.

WARNING: For a multi-site operation, this parameter must be set to all the sites for which the function must be activated, and not just the sites with ATDCs.

- If you tick this box, attendant console connection circuit CC0 is occupied until the called party off-hooks.
- Otherwise, the attendant console connection circuit CC0 is released on transfer. If the called party fails to reply, the call is rerouted to the operator console INCOMING 2 key.
- If you tick the box, the TRK monitoring LED flashes slowly until the called party off-hooks.
- Otherwise, the TRK monitoring LED stays steady on until the called party off-hooks. At the end of the no answer time-out, the LED monitoring the trunk begins to flash rapidly.

OPERATOR GROUP AUDIT ACTIVATED

This parameter is only used in multi-site configuration.

If you tick the box, the attendant console indicates its presence to other sites on the multi-site configuration. Calls to an attendant console can then be routed from another site to this set (for example, if 9 is dialled from another site, it will end up on the attendant console of this site).

SET FORWARDED FROM CONSOLE SETTINGS

ALLOW PREDEFINED FORWARDING

If you tick the box, the forwarding console is authorised to make predefined forwarding on common bell.

To enable forwarding to the bell, the directory number of the common bell must be indicated on the PREDEFINED FORWARD NO. line in the night bell extension characteristics.

ALLOW VARIABLE FORWARDING

If you tick the box, the forwarding console is authorised to make variable forwarding.

ALLOW CALL PICK-UP

If you tick the box, calls to the night console can be intercepted, using an interception code followed by the directory number of the night console.

ALLOW RECEPTION OF INTERNAL CALLS

If you tick the box, the forwarding console is authorised to receive internal calls.

OVERFLOW OF EXTERNAL CALLS ON REDUCED CALL DISTRIBUTION:

- **IF ATDC IS BUSY**:
  - Indicator of ATDC service overflow on busy (checkbox).
  - Default value, box not ticked: no overflow to answering service.
  - Box ticked: authorises the reduced answering service to handle overflow calls when the ATDC service associated with a day answering service is busy (all the ATDCs of an ATDC service taken).

IF ATDC SERVICE DOESN'T ANSWER

- Timeout before prompting the answering service to handle overflow calls if the ATDC(s) does/do not answer.
- Default value, box not ticked: no overflow to answering service.
- Box ticked: overflow to answering service with indication of overflow time on the next line:

OVERFLOW TIMER (IN SEC.) :

Value (in seconds), timeout before turning to the answering service if the ATDC does not answer.

TIMEOUT (EXPRESSED IN SECOND)

NIGHT SERVICE EXT. RING. DURATION

Ringer timeout when the response terminal does not answer.

Forwarding console ringer timeout before automatic activation of predefined forwarding, for the ongoing call (which must be a network call) and all the next calls.

Timeout unit 0.1s

Default value: 120 seconds

SPEC. TIMEOUT REROUT. TO CONSOLE

Timeout (in seconds): at the end of this timeout, a DID call is returned to the attendant console if not answered (set free or busy), if this feature is included in the characteristics of the extension concerned.

Default value: 20

NIGHT SERVICE EXT. RING. DURATION

Timeout (in seconds): At the end of this period, predefined forwarding of the assigned night console to the general night bell is automatically activated when an incoming call is not answered. This forwarding is subject to the right "Allow predefined forwarding" defined above.

Default value: 120

DELAY TIMES (IN 1/100S):

DISPLAY TIMEOUT OF THE IDLE SCREEN

Idle screen (or blank screen) display timeout after release on a digital attendant console.

The timeout is expressed in 1/100 sec, from 0 to 600 based on 0.01 s.

Default value: corresponds to a timeout of 2.5 seconds.

The value 0 allows immediate display.

7.3.2 DEFINITION OF OPERATOR GROUPS

Menu **RECEPTION>Operator>Operator services group**

This command is used to define the contents of each operator group (OP GP). The system has 15 attendant groups: OP GP1 to OP GP15.

Select the name of the attendant console to be defined in the drop-down list then click **Select the item**.

This screen is used to define several operator numbers in a group, as well as the parameters defined below.

OPERATOR NUMBER

Directory number for each operator in the group.

If some ATDC type extensions do exist on the system, this field is pre-completed with the first ATDC number.

The drop-down list contains all the ATDC extension numbers declared on the system.

FORWARD CONSOLE TO DN

Directory number of the forwarding set. By default, the directory number is that of the common bell relay, but this can be replaced by a set or a group of sets designated by their directory number.

Note: When the night console is assigned to a MiVoice 5000 Server, in addition to being entered in the operator service on which the attendant console has been declared, it must be entered in the operator service of this MiVoice 5000 Server hosting it.
This night console may be a remote TDM.

On this PBX, you can also designate a common bell connected to an LA card (subscriber equipment). The default forwarding set number is 798 on MiVoice 5000.

ASSOC. NAME

This field is used to convert the name of the operator group concerned to QSIG signalling.

OP SERVICE IDENTIFICAT. (TEL TICKET)

Information appearing on call records (tickets) identifying the operator service.

7.4 ANSWERING SERVICE

Menu **CALL DISTRIBUTION>Answering service**

The answering service menu (general DID call number management) is part of DIALLING PLAN management and is described in the corresponding chapter in this document. It is accessible via Menu **DIALLING PLAN>Incoming call dialling plan>Answering service**.

7.5 CALENDAR MANAGEEMNT

Menu **RECEPTION>Calendars**

This menu is used to:

- Declare some calendars identified by name
- Define for each calendar some night and day service timeslots for each day of the week
- View declared calendars
- Display the entities that use a given calendar.

Relationship with Easy Admin

Calendar management is also available in Easy Admin, from Menu **Calendar>Closed days** and **Calendar>Opening hours**. Some configuration functions are still reserved for the administrator (Web Admin).

In this case, the configuration is restricted to the calendars used by companies/departments and for this Easy Admin user for call distribution and day/night restrictions.

Therefore, if any changes are made to the Easy Admin application, they are instantly forwarded to Web Admin and can thus be viewed by the administrator. Conversely, if changes/deletions are made in this Web Admin menu, they are instantly transferred to the Easy Admin application.
Please refer to the document **MiVoice 5000 Easy Admin - User Guide**.

7.5.1 CALENDAR NAMES

Menu **RECEPTION>Calendars>Names**

This screen is used to declare the different iPBX calendars. You can declare a maximum of 16 calendars. By default, only one calendar is defined.

CALENDAR 1

Name of the calendar defined by default in the system (maximum 8 characters). The name can be changed (20 characters maximum).

CALENDARS 1 TO 250

250 calendars maximum.

Calendar names (20 characters maximum).

Note: For the power-saving function, refer to Section 9.3.

7.5.2 CALENDAR RANGE DEFINITION

Menu **CALL DISTRIBUTION>Calendars>Ranges definition**

Note: For the power-saving function, refer to the appendix.

For each calendar, you can define 4 timeslots (2 slots in day mode and 2 slots in night mode), independently for each day of the week.

CALENDAR NAME

The drop-down list contains the names of previously defined calendars.

Select the name of the calendar to be configured in the drop-down list then click **Select the item**.

This screen is used to define the day/night switchover timeslots for a given period, whereby a period is defined by a start day and an end day.

You can define 4 timeslots for each period. A maximum of 7 periods can be defined for the same calendar (if each day of the week has a different day/night switch-over range).

FROM (FIRST DAY)

-------	MOND	TUESD	WEDNESDA	THUR	FRIDAY	SATUR	SUNDAY

	AY	AY	Y	SDAY		DAY	

First day of the period for which you want to determine the switch-over ranges.

Note: Only the days not defined for another period (from the 7 possible periods) are proposed.

Once a day is selected for this field, the screen is refreshed to display the parameters used to configure the period.

TO (LAST DAY)

-------	MOND AY	TUESD AY	WEDNESDA Y	THUR SDAY	FRIDAY	SATUR DAY	SUNDAY

Last day of the period.

Note: Only the days not defined for another period and after the first day chosen for the period are proposed.

Each period can consist of four ranges, two DAY ranges and two NIGHT ranges.

FROM (DAY SWITCH HOUR) HH MM

Switchover time for the first DAY range in the format HH MM (HH=hour, MM=minute).

UNTIL (NIGHT SWITCH HOUR)

Switchover time for the first NIGHT range in the format HH MM (HH=hour, MM=minute).

AND FROM (DAY SWITCH HOUR)

Switchover time for the second DAY range in the format HH MM (HH=hour, MM=minute).

UNTIL (NIGHT SWITCH HOUR)

Switchover time for the second NIGHT range in the format HH MM (HH=hour, MM=minute).

Repeat the operation for each period to be defined.

7.5.3 BARRING CALENDER (CASE OF SINGLE-COMPANY CONFIGURATION)

Menu **RECEPTION>Calendars>Barring calendar**

This menu concerns single-company configurations. The principle is the same as for Multi-company configurations.

See 3.13.8 - Section Company/department parameters.

7.5.4 DISPLAY CALENDARS

Menu **RECEPTION>Calendars>Display**

This command is used to display the list of calendars declared on the iPBX as well as their properties.

The following information is displayed for each calendar:

- Its name
- Its current status (Day/Night)
- Its operating mode (Automatic/Anticipated)

- Whether it is assigned to restrictions (Yes/No)
- Whether it is used by a call distribution service (Yes/No).

Note: Automatic mode means that the calendar status results from the ranges defined in Menu CALL DISTRIBUTION>Calendars>Ranges definition. Anticipated mode means that the calendar status has been forced from an entitled terminal (Attendant console or Maintenance console).
This right is activated by ticking the "Restriction management" box in Menu SUBSCRIBERS>Rights>General settings.

7.5.5 DISPLAY USERS

Menu **RECEPTION>Calendars>Display users**

This command is used to display the list of users of a given calendar.

CALENDAR NAME:

The drop-down list contains the names of calendars declared on the iPBX.

Select a calendar from the drop-down list then click **Select the item**.

The next screen is used to display the various uses of the calendar selected.

Note: Only the columns with at least one calendar user are displayed.

BY POWER SAVING

See Appendix.

BY RESTRICTIONS OF

Calendar used by the companies/departments to define the Day or Night switch-over times. The company/department pairs using the calendar are indicated.

Note: The display ****** ****** indicates all departments in all companies.**

BY RECEPTION

Calendar used by the call distribution services to define the Day or Night routing switch-over times. The names of the call distribution services are indicated.

BY DYNAMIC TRUNK GROUP

Calendar used by the dynamic trunk groups to define the parameters for setting up or maintaining the link depending on the time. The names of the dynamic trunk groups are indicated.

7.5.6 CLOSED DAYS

Menu **RECEPTION>Calendars>Closed days**

This menu is used to define days as public holidays/non-working days with regard to the calendars used to route calls to call distribution or hunt group services.

The available calendars are defined in Menu **Calendar names**. See Section **7.5.1 – Calendar names.**

Closed days are displayed in a table with:

- **Calendar**: the calendar associated with the closed day
- **Date DD/MM/YYYY**: date of the current day
- **Label**: name given to the closed day
- **State**: validity of the closed day (**Valid** if the date is in the future, **Expired** if the day has passed).

These days are defined by calendar:

- Either via this menu, by defining the dates and names of public holidays for each calendar,
- Or by importing files containing predefined lists.

The opening and closing hours are defined in Menu **Ranges definition**. Refer to Section 7.5.2 - Calendar range definition.

Delete days: options used to delete:

- Either the expired days
- Or all the days declared and validated.

To delete or modify a given date, go to the corresponding line and delete or modify the values in the fields concerned.

Note: This feature is also available in the EasyAdmin application. In this case, the configuration is restricted to the calendars used by companies/departments and for this Easy Admin user for call distribution and day/night restrictions.

Therefore, if any changes are made to the Easy Admin application, they are instantly forwarded to Web Admin and can thus be viewed in this menu.
Conversely, if changes/deletions are made in this Web Admin menu, they are instantly transferred to the Easy Admin application.
Please see the document MiVoice 5000 Easy Admin - User Guide.

8 VOICE MAIL AND TONE MANAGEMENT

Menu **VOICE MAIL AND TONES**

This management domain is used to:

- Define voice mail parameters
- Configure tones
- Display information about available messages.

8.1 VOICE MAIL

Menu **VOICE MAIL AND TONES>Voice mail**

Generally, a voice mail system is used to receive, record, store play back or transmit voice messages. The messages are left in the voice mail boxes assigned to each system user.

The voice mail box (VMAIL) comprises a set of integrated voice services on a MiVoice 5000 platform:

- Announcement service: transmitting audio announcements (or messages) to a remote terminal
- IVR (Interactive voice response): rendering an audio call distribution service to a remote terminal
- IVB (Integrated interactive voice mail box): offering an interactive voice mail box to each iPBX phone access user.

8.1.1 VOICE MAIL SETTINGS

Menu **VOICE MAIL AND TONES>Voice mail>Definition**

VOICE MAIL CALL NUMBER

Voice mail call number. This number must have be created beforehand (GROUP type (**SUBSCRIBERS> Subscriptions**)).

Note: The default voice mail number is 797.

TYPE OF VOICE MAIL

Type of signalling used by the voice mail system. The following message types are available:

IVB	**XML/IP**	**DTMF**	**XML/IP CTI**	**ISDN S2**	**SMDI**

Note: The subscribers must be part of a hunt group associated with the messaging system (this hunt group must first be created as VMAIL GROUP type subscriber). Only the IVB does not require any hunt group.

AUTOMATIC CALL BACK OF CALLS

INT	**EXT**	**INT+EXT**	**NONE**

Select a configuration for callbacks.

8.1.2 INTERNAL VOICE MAIL (IVB)

Menu **VOICE MAIL AND TONES>Voice mail>Internal voice mail (IVB)**

This menu is used to configure direct access to the integrated voice mail box, without using Q23 codes, for all users on the MiVoice 5000 Server systems.

This configuration is used to offer all subscribers a personal voice mail box and some message recording time.

Note: It is always possible to configure this code, for all the other voice mail types, via the Q23 voicemail settings menu, in Menu *Telephony service>Voice mail and tones>Voice mail>External voice mail*.

8.1.2.1 *Settings*

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Parameters**

VIDEO MAIL (ON MIVOICE 5000 SERVER ONLY)

Box to be ticked when the integrated mail system is managing video.

If the box is ticked, the internal messaging system is configured to use video, and the following lines are presented and used to configure a maximum data rate and minimum data rate for video exchanges with the IVB.

- Minimum data rate, for defining the minimum video data rate which can be used by the IVB,
- Maximum data rate, for defining the maximum video data rate which can be used by the IVB.

Possible data rate values are:

  - 128 kb/s,
  - 384 kb/s,
  - 512 kb/s,
  - 768 kb/s,
  - 1024 kb/s.

The data rates presented on each line respect the following constraints:

  - The minimum data rates presented are strictly below or equal to the current maximum data rate.
  - The maximum data rates presented are strictly above or equal to the current minimum data rate.

- Background video

This field is used to customise the background video broadcast during audio calls.

When the bandwidth is too low, a different, non-configurable file replaces the customised file.

Note: The call is not cut when a new video is loaded.

Downloading is rejected if:

- The file is not in the right format (wav in G711/G722 or avi in H264 baseline profile),
- The file is a video file, but video is not allowed for integrated messaging,
- The maximum IVB size (by default 50 MB on MiVoice 5000 Server) is reached.

CONSULT MAIL BOX DIRECTLY:

- ACCESS TO MENU: Option used to indicate the voicemail box access mode
  - PASSWORD: in this case, the prompt "*Please enter your password followed by a hash*" is made to the user.
  - MAIN: depends on the voicemail box status: announcing the mode, requesting for signature. In this mode, the voicemail box is accessible without pasword (not secure).
  - LISTEN: listening to the first message directly in the "not read" and "read" status, depending on the configured presentation order. In this mode the voicemail box is accessible without password (not secure).

Note: The modification applies to the IVB, that is to all box classes.

NUMBER OF ATTEMPTS

Number of attempts authorised for an operation.

SIGNATURE INCENTIVE DELETION

The signature corresponds to a short personal voice sequence inserted in the greeting message. Ticking the box deletes the prompt to record a signature.

CONFIGURATION TRANSFER

INTERNAL **INT+EXT** **NONE**

Select a transfer configuration. The transfer option is accessible when the voice mail box is being consulted.

PRESENTATION ORDER

UNREAD THEN READ **READ THEN UNREAD** **INCREASING DATE**

Select an order in which the messages will be presented when the voice mail box is consulted.

CALL BACK OF THE DEPOSITE

INT+EXT **NONE** **INTERNAL** **EXTERNAL**

Configure the methods of calling back the person that left the message. Call back of the deposit is available during voice mail box consultation.

MESSAGES DEPOSIT:

- DTMF CODE FOR TRANSFER

Select the multi-frequency detection (DTMF) code for transfer to an attendant console: value 0 or 9.

- LANGUAGE IF EXTERN. CALL

MSG. INTEGRATED **SUBSCR**

Determines whether the language used to broadcast the greeting message is that of the integrated messaging system or the one assigned to the subscriber.

INTERACTIVITY DELETION

Indicator of interactivity deletion on a digital terminal.

Default value, box not ticked: interactivity enabled.

Box ticked: interactivity deleted.

INTRODUCTION OF GREETING OF TYPE "NAME"

These different fields are used to customise the greeting message broadcast before broadcasting the name of a voicemail box. This only concerns the Name type greeting message.

Compatible formats are:

Audio: wav or mp3

Video: avi in H264 (baseline profile)

Note: The call is not cut when a new greeting message is loaded.

The following actions are possible for each language:

- Add new message,
- Replace current message with a new one,
- Delete current message.

For video message customisation, the **Video mail** box must be ticked in this same menu.

Downloading is rejected if:

- The file is not in the right format (wav in G711/G722 or avi in H264 baseline profile),
- The file is a video file, but video is not allowed for integrated messaging,
- The maximum IVB size has been reached.

8.1.2.2 *Voice mailbox classs*

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mail classes**

8.1.2.2.1 Voice mail classes names

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mail classes>Names**

Each voice mail box belongs to a class used to define the general characteristics of the mail box. 10 voice mail box classes can be defined. This menu is used to assign a name to the 10 voice mail box classes.

CLASS 0-1

Classes IVB 0 and IVB 1 are created automatically during total iPBX reset.

CLASS 2-3-4-5-6-7-8-9

Assign a name to these classes.

8.1.2.2.2 Class settings definition

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mail classes>Characteristics**

BY NAME

Select one of the classes created in the previous menu (IVB 0 and IVB 1 are created automatically), then validate with **Select the item**.

Once validated, the following screen is displayed.

This screen is used to define/modify the settings of a class. The parameters are divided into two categories:

- Parameters relating to card physical characteristics
- Parameters relating to telephone operation characteristics.

PHYSICAL PARAMETERS

MAX. NO. OF MESSAGES

Maximum number of messages recorded in a voice mail box (including the greeting messages): from 1 to 100.

DURATION : EXPECTED STEP (IN S.)

Read-only line. The recorded messages are stored by section on the card's Flash memory. The size of these sections depends on the type of Flash memory used. PAS represents the duration of recording per section (expressed in seconds).

MAXIMUM RECORDING DURATION

Maximum duration of a recording in a mailbox for a given class: default value in seconds (from 1 to 3600 seconds).

MAXIMUM MESSAGE DURATION

Maximum duration of a recorded message, expressed in seconds (1 to 3600 seconds).

RECORDED GREETING DURATION

Maximum duration of a customized answering service, expressed in seconds (1 to 360 seconds)

SIMPLE VOICEMAIL GREETING DURATION

Maximum duration of a customized answering service, expressed in seconds (1 to 360 seconds)

NAME ANNOUNCEMENT DURATION

Maximum duration of a customized answering service, expressed in seconds (1 to 35 seconds)

OPERATING PARAMETERS

VIDEO MAIL BOX

Box to be ticked if the voicemail box is a video mailbox. This type of box can be used to record and send audio and video type voice messages.

CALLED STATUS BROADCAST

When a call arrives on a voice mail box, the caller can be informed about the status of the called party (for instance, if the called party has a call in progress, the caller is informed that extension XXXX is engaged).

Tick (or untick) the box to allow (or disallow) the broadcasting of a called extension status message.

E-VOICEMAIL

OPTIONS:

- FORBIDDEN
- NOTIFICATION

Note: The e-voicemail service requires a software key code.
For more information about the e-voicemail service, see the description in the menu: SYSTEM>Configuration>E-mail.

This function is used to send left messages by e-mail.

Selecting **NOTIFICATION** sends an e-mail to the called party (beneficiary of this class), informing them that a voice or video message has been left in his IVB.

This option will work well if you also declare the called party's e-mail address in the integrated directory.

- ENCLOSED MESSAGE

If you tick the box, the voice or video message left in the subscriber's voice mail box will be forwarded as attachment to the e-mail address.

- DELETION OF MESSAGES

This line is only displayed if e-voicemail notification is activated and the addition of e-voicemail message is set (the **JOINED MESSAGE** box is ticked).

If the box is ticked, the voice or video message left in the subscriber's voicemail box is deleted upon receiving the message-read or message-sent notification from the associated e-mail address, as defined in the line below (ON).

- ON

Choice concerning the deletion of voice or video messages:

READING ACKNOWLEDGEMENT or SENDING (see above).

This line is only displayed if the DELETION OF MESSAGES box is ticked.

Note: The scroll arrows and are used to define the characteristics of other voice mailboxes declared.

8.1.2.3 *Mailbox characteristics*

Greetings tab

This tab is used to define the greeting mode and messages for each box:

GREETING MODE

- SIMPLE VOICEMAIL GREETING
- RECORDED GREETING

The following three fields - NAME TYPE GREETING, RECORDED GREETING and SIMPLE VOICEMAIL GREETING - are used to:

- Add a message if there is none (New message),
- Display and/or listen to the current message, by clicking the Current message link,
- Replace the current message.

To download a message:

- Click Browse to locate the file to be downloaded.
- Then click Download to take account of the new message.

Note: After downloading a greeting message, it is possible to replace, but not, delete it.

Compatible formats for downloading:

- Audio: wav or mp3,
- Video: avi in H264 (baseline profile).

Note: The call is not cut when a new greeting message is downloaded.

Downloading is rejected if:

- The file is not in the right format (wav in G711/G722 or avi in H264 baseline profile),
- The file is a video file, but video is not allowed for integrated messaging,
- The file is a video file, but video is not allowed in this IVB class.
- The maximum IVB size has been reached.
- The duration of the greeting is above the maximum duration defined in the box class.
- The voicemail box is currently used by its owner (a special message is displayed to the installer).

GREETING MESSAGE

The proposed options depend on the greeting mode chosen and the greeting messages defined in the **Greeting ….** fields.

Greeting message options:

- Number (default value)

- Name
- Customised (Ans/Reco).

Messages in the box tab

The different columns are used to view the content of each box:

- Number: numbers of the messages left
- Date: date on which the messages were left
- Greeting type: type defined in the Greeting messages tab.

Note: A hypertext link in the greeting type field gives access to the reading of the file in question.

- Status: status of the message received (LEFT or READ)
- Type: Type of message received (audio, video)
- Duration: duration of the message received
- Total: Total duration of all the messages. Information used to check whether the maximum duration has not been reached. This is done in comparison with the maximum duration defined in the box classes characteristics.

8.1.2.4 *Display*

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mail classes>Display**

This function has three display screens:

- Global display
- Messages in a box
- Busy statistics

8.1.2.4.1 Global display

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mail classes>Display>Global display**

This menu is used to display all or part of the integrated voice mailboxes based on different criteria:

FROM NUMBER

A list of the voice mailboxes can be displayed in ascending order, from the directory number of any voice mailbox. Enter a directory number.

FOR THE VOICE MAILBOX CLASS

A list of the voice mailboxes belonging to the same class can be displayed.

FOR THE FUNCTIONAL MODE

A list of the voice mailboxes can be displayed depending on their operating mode:

-------	View all voice mailboxes
RE	View voice mailboxes in Announcement and Recording mode

RS	View voice mailboxes in Announcement mode

Select a voice mailbox operating mode.

FOR THE STATUS

A list of the voice mailboxes can be displayed depending on their status:

-------	View voice mailboxes with space available to receive new messages.
FULL TIME	View voice mailboxes with no more recording space available.
FULL MEMORY	View voice mailboxes with maximum number of authorised messages.
LOCKED	The announcement and recording function is locked. Until the unlocking code is entered (concerning the management of licences in **SYSTEM>Info**), the voice mail operates in announcement mode for all the voice mail boxes declared.

Choose the selection criterion then click **Select the item** to display the next page which contains a sequence of information statistics and a table describing the status of the voicemail boxes.

VOICE MAIL NUMBER:

Indicates the total number of voice mailboxes meeting the selection criteria.

RANGE/VOICE MAIL TOTAL NUMBER :

Indicates the percentage of voice mailboxes meeting the selection criteria out of the total number of voice mailboxes declared.

COLUMNS IN THE TABLE:

NUMBER

Voice mailbox directory number (same as the directory number of the user with this mailbox).

STATUS

Status of the voice mailbox:

AVAIL	Mail box in service (memory space available)
D SAT	Voice mailbox saturated in terms of duration.
M SAT	Voice mailbox saturated in terms of messages.
DISA.	Voice mailbox inaccessible (for example, card disabled)

MODE

Voice mailbox operating mode:

RE	Announcement and Recording mode
RS	Announcement mode

TYPE:

A voicemail box will considered as **UNIFIED** if the associated voicemail box class has e-voicemail notification rights. Otherwise, the voicemail box will be considered as **STANDARD**.

STANDARD	Standard box
UNIFIED	Standard box

GREET.:

Type of voice mailbox greeting message:

STANDARD	Standard message (voice mailbox number)
NAME	Simple customised message (name of mailbox owner)
PERSONAL RE	Detailed customised message (greeting message in announcement and recording mode)
PERSONAL RS	Detailed customised message (greeting message in announcement mode)

GREETING MESSAGE:

Total number of greeting messages for each voice mailbox listed.

MSG LEAVE:

Total number of messages left in each voice mailbox listed.

DURAT.:

Total duration of all messages recorded in the voice mailbox (messages left + greeting messages).

8.1.2.4.2 Messages in a box

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mailbox classes>Display>Messages in a box**

This screen is used to display all the messages contained in a selected voice mailbox.

VOICE MAIL NUMBER

Enter its number to display the messages in a voice mail box.

Click **Select the item** to display the following screen.

On this screen, the recorded messages are of two types:

- first part of menu: greeting messages (maximum of 3 types per voice mailbox)
- second part of the menu: messages submitted

NUM

Message number in the order of arrival.

DATE

Date on which the message was left (dd/mm/yy hh:mm).

ACCESS TYPE

Type of greeting active:

STANDARD	Greeting by voice mailbox number
NAME	Greeting by name
PERSONAL RE	Announcement and recording mode customised greeting
PERSONAL RS	Announcement mode customised greeting

STATUS

Message status (for messages left only):

LEFT	A message has been left but not read
READ	The message left has been read

DUR.

Duration of the message recorded in minutes/seconds.

8.1.2.4.3 Busy statistics

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mailbox classes>Display>Busy statistics**

This screen gives an overview of the occupation status of the memory reserved for the IVB on the compact flash card:

- Display of all recorded messages (greeting messages + recorded messages)
- Display of greeting messages according to type (name, customised)
- Display of recorded messages according to status (read, not read)

8.1.2.5 *Automatic deletion*

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mail classes>Automatic suppression**

An audit is used to manage the time during which the messages left are kept, according to the iPBX configuration.

This “Automatic deletion” function has the following deletion screens:

- Audit start-up criteria
- Selection criteria

8.1.2.5.1 Start-up criteria

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mail classes>Automatic suppression>Start-up criteria**

This screen is used to trigger an audit according to predefined schedules.

Auditing is set to be carried out periodically (hourly or daily) beginning at a start date. If the frequency fields are set at 0, auditing will not be carried out.

FREQUENCY: HOURLY

Indicate the number of hours between 2 audits (HH: from 0 to 23).

FREQUENCY: DAILY

Indicate the number of days between 2 audits (DD: from 1 to 31).

Note: The user must choose only one criterion between 2 previous parameters (tome and day). To avoid any confusion, the web interface does not allow the selection of these two criteria at the same time.

TIME OF START-UP

Indicate the start-up time for the first audit (HH: from 0 to 23).

STATUS

This field displays the current state of the audit, ACTIVE or INACTIVE.

ACTION

•••••• **MODIFY** **CREATE** **DELETE**

This field is used to create or delete an audit. It is also used to change the parameters for running the active audit with new parameters.

8.1.2.5.2 Selection criteria

Menu **VOICE MAIL AND TONES>Voicemail>Internal voice mail (IVB)>Voice mailbox classes>Display>Message selection criteria**

This screen is used to define four conditions for a message to be selected or deleted when the audit starts.

For each condition you can specify 4 criteria: the message status (read or left), the length of time it has been in the voice mailbox (in days), its duration (in seconds) and its service class.

FOR MESSAGE STATUS

••••••	READ	LEFT

••••••	Whatever the message status
READ	Message left and read
LEFT	Message left but not read

AND THE LENTH OF SERVICE (DAYS)

In days. The selected (or deleted) message has reached or exceeded the maximum length of time a message is allowed to remain in the voice mailbox.

AND THE DURATION (IN SECONDS)

In seconds. The duration of the selected (or deleted) message has exceeded the specified limit.

AND THE SERVICE CLASS

Select the name of the class or "------" (whatever the class).

Note: If no criteria are selected in a particular block, the audit will not be run on this block.

8.1.3 EXTERNAL MESSAGING SYSTEM

Menu **VOICE MAIL AND TONES>Voice mail>External voice mail**

In order to successfully complete the installation of your voice mail, you must first configure the iPBX for the voice mail function.

By default, the parameters are predefined to facilitate the configuration.

This menu is specially used to connect voice mail boxes in DTMF mode. It indicates the exchange of information.

Details of the data is not required in order for the system to work correctly.

8.2 TONES

Menu **VOICE MAIL AND TONES>Tones**

Each basic, Mitel-range system can manage announcements and messages whose total duration varies according to the size of the disk. MiVoice 5000 SERVER can access them for the needs of IP subscribers and network accesses.

The announcements and messages can be configured via the management portal (loading and backing up announcements and messages, reading their characteristics, assigning announcement-message tones).

Pre-recorded messages are sound files (.wav or mp3) linked to system tones.

The tones correspond to the different states of a telephone call. A pre-recorded message or music can be linked to each iPBX system tone.

The iPBX can support up to 256 tones (numbered 0 to 255), of two types:

- System tones
- Definable tones whose numbers range between [64, 113] and [136, 254], for customising pre-recorded messages according to the spoken language or company/department pair.

8.2.1 DEFINITION

Menu **VOICE MAIL AND TONES> Tones>Definition**

This command is used to configure the different system tones, and possibly assign them some announcements (messages), by specifying the type of device providing the messages:

For MiVoice 5000 Server, the device is Media Server with the associated message.

Note: Changes in TONE type parameters are only taken into account by proprietary IP terminals after the system is restarted.

IMPORTANT NOTE: The sound files correspond to the announcements that must be recorded in this format: 8 bits WAV, A law or µ law, Mono at 8KHz. The compression law must be compliant with the law of the country in which the iPBX is used.

On MiVoice 5000 Server, sound files can be stored in **16 bit/16 kHz mono**linear PCM format.

INTERNAL

NORMAL DIAL TONE	EXTERNAL DIAL TONE	INTERNAT. DIAL TONE
ROUTE	ON BUSY	INTERNAL ON HOLD TONE
INTRUSION TONE	WARNING	INTERN. RINGBACK TONE
NETWORK RINGBACK TONE	INTERNAL EXT. O.S.	EXTERNAL O.S..
RESTRICTION FAIL	PROGRAM AGENDA TONE	CALL ACCEPTED TONE
CONGESTION TONE	UNKNOWN NUMBER TONE	ENTER PASSWORD
WAKE-UP RECALL	MSG IN BOX	ZERO CREDIT

MINIMUM CREDIT	CONSULT. CALL INTRUS.	SINGLE CALL INTRUSION
CONSULT. CALL NO INTR.	SINGLE CALL NO INTR.	D.N.D ACTIV
VAR FRWD ACTIV	AUTO CALLBACK ACTIV	PREDEF. CBACK ACTIV
DISA PASSWORD	DIRECTORY ENQUIRY	

NORMAL DIAL TONE	Internal tone
EXTERNAL DIAL TONE	Dial tone on external line
INTERNAT. DIAL TONE	International dial tone
ROUTE	Call routing in progress (silence)
ON BUSY	On busy
INTERNAL ON HOLD TONE	Internal on-hold tone
INTRUSION TONE	Interrupt during call
WARNING	Warning
INTERN. RINGBACK TONE	Internal call return
NETWORK RINGBACK TONE	Network call return
INTERNAL EXT. O.S.	Internal extension out of service
EXTERNAL O.S..	External line out of service
RESTRICTION FAIL	Barred number, call disallowed
PROGRAM AGENDA TONE	Programmed reminder
CALL ACCEPTED TONE	Function accepted
CONGESTION TONE	No resource; call cannot be connected
UNKNOWN NUMBER TONE	Number unknown
ENTER PASSWORD	Personal code
WAKE-UP RECALL	Automatic callback requested
MSG IN BOX	Voicemail waiting
ZERO CREDIT	Prepayment empty
MINIMUM CREDIT	Prepayment nearly empty
CONSULT. CALL INTRUS.	Enquiry call with intrusion privilege
SINGLE CALL INTRUSION	Single call with intrusion privilege

CONSULT. CALL NO INTR.	Enquiry call without intrusion privilege
SINGLE CALL NO INTR.	Single call without intrusion privilege
D.N.D ACTIV	“Do not disturb” activated
VAR FRWD ACTIV	Variable forwarding activated
AUTO CALLBACK ACTIV	Automatic callback activated
PREDEF. CBACK ACTIV	Predefined forwarding activated
DISA PASSWORD	Personal code for DISA
DIRECTORY ENQUIRY	Directory enquiry

Select an internal tone.

OR NETWORK

EXTERNAL DIAL TONE	INTERNAL ON HOLD TONE	NETWORK HOLD	BF ANS: EXT FREE
BF ANS: FWD OPCO FREE	AF ANS: EXT FREE	AP REP RVPO FREE	BF ANS: EXT BUSY
AP REP AB OCC	BF DAY RING	BF NIGHT RING	MEET-ME PAGING
BF ANS: DAY DISSUA	BF ANS: NIGHT DISSUA	AF ANS: DAY DISSUA	AF ANS: NIGHT DISSUA

EXTERNAL DIAL TONE	Dial tone on external line
INTERNAL ON HOLD TONE	Internal on-hold tone
NETWORK HOLD	Network on-hold tone
BF ANS: EXT FREE	Ringing before answer on free extension (subscriber or operator)
BF ANS: FWD OPCO FREE	Ringing before answer on free CAP (Central Answering Position) or night console extension number
AF ANS: EXT FREE	Ringing after answer on free extension (subscriber or operator)
AP REP RVPO FREE	Ringing after answer on free CAP or night console extension number
BF ANS: EXT BUSY	Ringing before answer on busy extension
AP REP AB OCC	Tone after answer on busy extension
BF DAY RING	Ringing before answer on day service
BF NIGHT RING	Ringing before answer on night service
MEET-ME PAGING	Awaiting response from person paged
BF ANS: DAY DISSUA	Dissuasion before answer on day service
BF ANS: NIGHT DISSUA	Dissuasion before answer on night service

AF ANS: DAY DISSUA	Dissuasion after answer on day service
AF ANS: NIGHT DISSUA	Dissuasion after answer on night service

Select a network tone.

Note: The tones can be customised in multi-company configuration in the same was as announcements can be customised according to the user's language.

OR TONE NB

Enter the number of a definable tone: 3 digits. These tones are unused on system start-up.

Make the selection then click **Select the item** to display the screen used to define the characteristics of the tone concerned:

SIGNAL TYPE

TONE **MESSAGE** **MESSAGE OR TONE**

Select the signal type.

If the signal type ANNOUNCEMENT OR TONE is selected, the definition screen opens so a tone can be defined, and an announcement listed. The listed announcement will be broadcast if the necessary resources are available, otherwise, the tone will be broadcast.

The tone configuration parameters vary according to the type of signal selected.

ORIGIN NUMBER 1

This parameter is available for TONE and MESSAGE OR TONE signal types.

SILENCE TONE 330 Hz **TONA 440 Hz High** **TONE 440 Hz Low** **TONE 440 + 330 HZ**

Select origin number 1 or modify the existing origin. * INTERNAL MUSIC (1 melody)

PEAK DURATION (UNIT 10 MS)

This parameter is available for TONE and MESSAGE OR TONE signal types.

Number of 10 ms units for defining peak duration.

TROUGH DURATION (UNIT 10 MS)

This parameter is available for TONE and MESSAGE OR TONE signal types.

Number of 10 ms units for defining trough duration.

ORIGIN NUMBER 2

This parameter is available for TONE and MESSAGE OR TONE signal types.

UNDEFINED SILENCE TONE 330 Hz **TONA 440 Hz High** **TONE 440 Hz Low**

Select origin number 2 or modify the existing origin.

* INTERNAL MUSIC (1 melody)

PEAK DURATION (UNIT 10 MS)

This parameter is available for TONE and MESSAGE OR TONE signal types.

Number of 10 ms units for defining peak duration.

TROUGH DURATION (UNIT 10 MS)

This parameter is available for TONE and MESSAGE OR TONE signal types.

Number of 10 ms units for defining peak duration.

ANNOUNCEMENT FROM

This parameter is available for MESSAGE and MESSAGE OR TONE signal types.

VM	EXTERNAL MUSIC	ANALOG EXTENS.

The origin of the announcement.

MESSAGE

This setting is available for MESSAGE and MESSAGE OR TONE signal types, if the message is provided by MiVoice 5000 server

ADD A NEW MESSAGE	For downloading a new message and assigning it to the selected tone. **Note: The number of message that VM box can support is 255. If this number is reached, the ADD A NEW MESSAGE action can no longer be used. Therefore, you only need to assign an unused message to the tone, and choose the action REPLACE THIS MESSAGE BY A NEW. The unused announcements can be displayed via the menu VOICEMAIL AND TONES>Messages>Display.**

REPLACE THIS MESSAGE BY A NEW	For downloading a new message and replacing all occurrences of the previous message with this new one. The old message is erased from the VMAIL. **WARNING: If other tones are using the previous message, they will be changed to use the new message.**

File name	The message which corresponds to the selected file or radio stream is associated with the tone. The list contains all the messages available on the VMAIL or Media Server, and recorded network streams. Adding choice to "Message" field.

If you select ADD A NEW MESSAGE or REPLACE THIS MESSAGE BY A NEW, a downloading field appears:

New Message Browse... Download

Press the “**Browse…**” button to open a browser.

Select the file you want then click **Download….**

Note: A hypertext link on the name of this field is used:
• by right-clicking, to save the message on the PC,
• by left-clicking, to listen to the message provided that a .wav or mp3 file reader is available on the PC.

The formats authorised for audio announcements are:

- G711, A-law if the iPBX is set to A-law

- G711, µ law if the iPBX is set to µ law
- in 16-bit/16 kHz mono linear PCM format on MiVoice 5000 Server only.

⚠ **WARNING: The file name extension must be .wav or mp3.**

ORIGIN SITE

This parameter is available for the MULTISITE ANNOUNCEMENT type signal.

Select an origin site.

ORIGIN NODE

This parameter is available for the MULTISITE ANNOUNCEMENT type signal.

Enter a numerical value from 2 to 99.

Note: The MMC does not check whether there is a device in the node site specified. For an internal site, the node number is forced to 2.

DEVICE NUMBER (IN DECIMAL)

This parameter is available for the MULTISITE ANNOUNCEMENT type signal.

Enter a numerical value from 0 to 767.

NUMBER OF AUTHORIZED CONNECTIONS

This parameter is available for the MULTISITE ANNOUNCEMENT type signal.

Enter a numerical value from 0 to 32.

8.2.2 ALLOCATION OF TONES - LANGUAGES

Menu **VOICE MAIL AND TONES>Tones>Allocation of tones – languages**

Tones and languages are assigned automatically during first installation from the list of spoken languages (accessible via the command **SYSTEM>Configuration>Languages> Spoken languages**). The first language on the list is assigned to the system tone, and the other languages to the definable tones.

This screen is used to replace the standard tone of a function with a definable tone, for a given language (64-113 or 136-254). This requires that the messages be available for downloading.

FOR LANGUAGE

-----------	FRENCH	ENGLISH

Select a language.

AND TONE

INTERNAL ON HOLD TONE	EXT. INTERNAL O.S.	EXTERNAL O.S.	RESTRICTION FAIL
PROGRAM WAKE-UP	CALL ACCEPTED TONE	CONGESTION TONE	NUM. DOES NOT EXIST.
INV. TO BE SIGNED	WAKE-UP RECALL	MSG IN BOX	ZERO CREDIT
MINIMUM CREDIT	CONSULT. CALL INTRUS.	SINGLE CALL INTRUSION	CONSULT. CALL NO INTR.

SINGLE CALL NO INTR.	D.N.D. ACTIV	AUTO CALLBACK ACTIV	PREDEF. CBACK ACTIV

Select the tone to be modified.

IDENTIFIED BY THE NUMBER

A number linked to the tone previously selected is displayed. To select a tone not in the above list and for definable tones (dual criteria company-dept/language), enter the tone number in three digits

IS REPLACED BY DEFINABLE TONE

NUMBER (64-113 OR 136-254)

Enter the number of the definable tone (3 digits) which will replace the tone selected.

8.2.3 COMPANY/DEPARTMENT SPECIFIC TONES

Menu **VOICE MAIL AND TONES> Tones>Company/department specific tones**

This screen enables you to replace network tones with definable tones (single-company or multi-company configuration).

TONE

EXTERNAL DIAL TONE	INTERNAL ON HOLD TONE	NETWORK HOLD	BF ANS: EXT FREE
BF ANS: FWD OPCO FREE	AF ANS: EXT FREE	AP REP RVPO FREE	BF ANS: EXT BUSY
AP REP AB OCC	BF DAY RING	BF NIGHT RING	MEET-ME PAGING
BF ANS: DAY DISSUA	BF ANS: NIGHT DISSUA	AF ANS: DAY DISSUA	AF ANS: NIGHT DISSUA

Select the network tone to be allocated to the definable tone.

IS REPLACED BY DEFINABLE TONE

NUMBER (64-113 OR 136-254)

Enter the number of the definable tone (3 digits) which will replace the tone selected.

In a multi-company configuration, the following additional parameter will have to be completed:

AND DEPARTMENT

Select a department in the company.

In a multi-company configuration, the message corresponding to an item (subscriber, hunt group) associated with the company/department pair 0/0 does not replace the previous message associated with another company/department.

This makes it possible to mutualise some items in different call distribution services while keeping specific messages.

8.2.4 DIRECT ACCESS MESSAGES

Menu **VOICE MAIL AND TONES> Tones>Direct access messages**

This screen is used to establish correspondence between a direct message and a definable tone. Listen to the message by dialling a prefix (see Voice mail parameters).

FOR MESSAGE XXXX DEFINABLE TONE NO.

Enter the definable tone number (1 to 126).

Note: Several messages can use the same tone. A direct access message can reach an announcement or a tone directly (for example, a local speaking clock).

LISTENING TIME (SEC)

Message listening time, 8 seconds by default (5 to 600).

8.2.5 TONES DISPLAY

Menu **VOICE MAIL AND TONES>Tones>Tones display**

This command is used to display the characteristics of all the system tones.

Each table indicates for each tone defined on the system:

- The number of the tone
- Its name
- Its type
- The name of the file, for an announcement
- The tone definition parameters (see *8.2.1*).

8.2.6 DISPLAY DEFINABLE TONES

Menu **VOICE MAIL AND TONES>Tones>Display definable tones**

This screen is used to display the list of definable tones of a single company.

Note: In single-company configuration, the company name displayed is not significant.

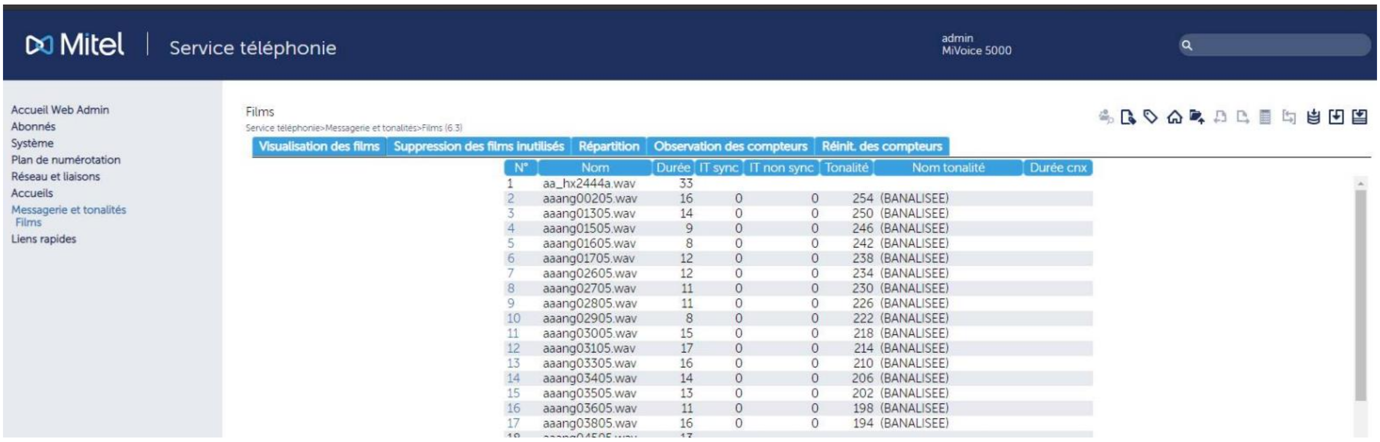
In this example, the definable tones used by CMPNY 0 are:

- Tone 065 is reserved for INTERNAL ON HOLD TONE.
- Tone 152 is reserved for EXTERNAL NUM.
- The other tones apply to all the services:
- Tone 136 is reserved for EXTERNAL NUM.
- Tone 137 is reserved for NETWORK HOLD.

The **Easy Admin** column indicates whether the tone can be managed by this application for customising announcement messages by Company/Department. See the corresponding sections and documents.

8.3 MESSAGES

Menu **VOICE MAIL AND TONES>Messages**



Films

Service téléphonie>Messagerie et tonalités>Films (6.3)

N°	Nom	Durée	IT sync	IT non sync	Tonalité	Nom tonalité	Durée cnx
1	aa_hx2444a.wav	33					
2	aaang00205.wav	16	0	0	254	(BANALISEE)	
3	aaang01305.wav	14	0	0	250	(BANALISEE)	
4	aaang01505.wav	9	0	0	246	(BANALISEE)	
5	aaang01605.wav	8	0	0	242	(BANALISEE)	
6	aaang01705.wav	12	0	0	238	(BANALISEE)	
7	aaang02605.wav	12	0	0	234	(BANALISEE)	
8	aaang02705.wav	11	0	0	230	(BANALISEE)	
9	aaang02805.wav	11	0	0	226	(BANALISEE)	
10	aaang02905.wav	8	0	0	222	(BANALISEE)	
11	aaang03005.wav	15	0	0	218	(BANALISEE)	
12	aaang03105.wav	17	0	0	214	(BANALISEE)	
13	aaang03305.wav	16	0	0	210	(BANALISEE)	
14	aaang03405.wav	14	0	0	206	(BANALISEE)	
15	aaang03505.wav	13	0	0	202	(BANALISEE)	
16	aaang03605.wav	11	0	0	198	(BANALISEE)	
17	aaang03805.wav	16	0	0	194	(BANALISEE)	

The possibilities offered by the user interface in this part are basically information display functions and possibly the deletion of unused customised messages.

8.3.1 DISPLAY

Menu **VOICE MAIL AND TONES>Messages>Announcement display**

This screen is used to display the list of existing messages, by indicating their equipment number (virtual VMAIL card) and the following information:

Num.: message number

Name: message name

DUR: message duration in seconds

IT SYNC: number of TSs reserved for synchronised messages

IT NOT SYNC: number of TSs reserved for unsynchronised messages

TONE: number of tones using the message

TONE NAME: name of the tones using the message

CONN DUR.: time message heard.

Note: If you click the message number (on which there is a hypertext number), you can obtain specifications on the nature of the message via tone definition.

8.3.2 REMOVE UNUSED ANNOUNCEMENTS

Menu **VOICE MAIL AND TONES>Messages>Remove unused announcements**

This tab allows you to delete custom messages to free up memory space or when they are no longer in use.

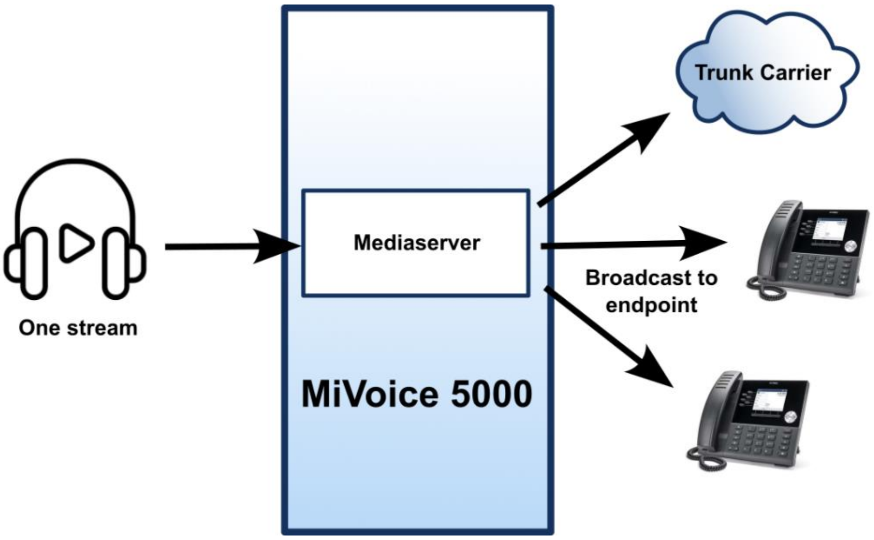
To be deleted, these messages must no longer be assigned to a signal. Refer to Menu **Voice mail and tones> Tones>Definition.**

Messages declared as default messages (canonical values) cannot be deleted.

8.4 WEB RADIOS

Menu **Voice mail and tones> Web Radios**

This screen allows you to view, add and delete radio streams from the MiVoice 5000 Server. Up to 20 radio streams can be added.



The list contains the following information:

Label: radio stream name

URL: radio stream URL

Important: The radio stream address must be in MP3 format to work.

Check certificate: validity of radio stream certificate,

Volume (%): radio stream volume,

Cache (ms): radio stream cache,

Listen: radio stream listening button.

To add a new network stream:

- Fill in the Label field. After validation, the URL field can be modified.
- Fill in the URL field. After validation, the Volume (%) and Cache (ms) fields are accessible.
- The Volume (%) and Cache (ms) fields are automatically filled in but can be modified.

Note: If the radio stream is not available, the radio stream broadcasts silence.

To delete a network stream:

- Delete the contents of the Label field of the desired network stream.

- The rest of the line is automatically deleted.

9 APPENDICES

9.1 REGISTERING THE MIVOICE 5000 PBX IN MICROSOFT AZURE

⚠ **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, please refer to the Microsoft Azure documentation: https://learn.microsoft.com/fr-fr/azure/?product=popular

For the Microsoft account, register the MiV5000 application on the Azure portal:

https://portal.azure.com/

- When registering a new application:
  - Enter the redirection URL in the following format:
    - For SSO of the User Portal: https://[MiVoice5000FQDN]:4446/sso-oidc
    - For the SSO of the Mitel Dialer: https://[SBC FQDN]:4445/sso-oidc
    - For mails: https://[MiVoice5000FQDN]/system/MiVoice5000Mail.htm
- Create a client secret for the application.
- For SSO configuration:
  - 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”.
- For email configuration:
  - This is not specific to OAuth2, but in order to establish an SMTP, POP or iMAP connection, on the OutlookOnLine side, the mailbox must be configured to accept SMTP, POP and IMAP connections.

    Administrator rights may be required to grant these permissions.

For SSO configuration, continue with the procedure in Menu **Telephony service > Subscribers > Rights > General settings**, **SSO** tab. See Section **3.14.1.1 – SSO tab**.

For email configuration, return to Menu **SYSTEM>Configuration>E-mail** in the iPBX for the rest of the procedure. Refer to Section **4.3.5.3 Description of the different fields**.

9.2 REGISTERING THE MIVOICE 5000 IPBX IN GOOGLE

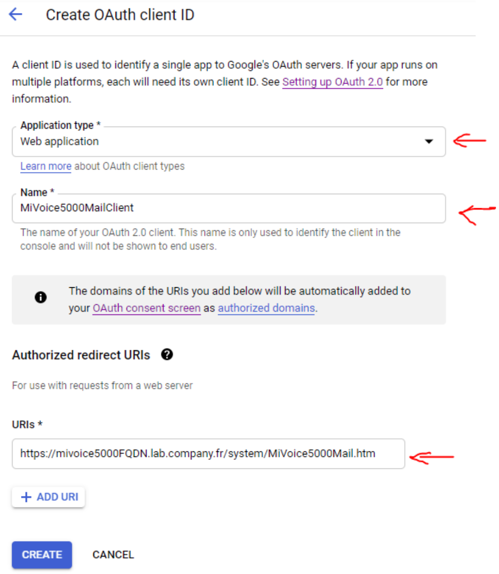
WARNING: The menus and labels indicated in this document are provided as examples to describe the procedure and are subject to changes specific to Google Cloud Portal.

For the Google account, register the MiV5000 application on Google Cloud Portal:

https://console.cloud.google.com/

Fill in the different fields proposed.

Then select the **Create identifiers**tab, the **OAuth client ID** column.



Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See Setting up OAuth 2.0 for more information.

Application type *: Web application

Learn more about OAuth client types

Name *: MiVoice5000MailClient

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

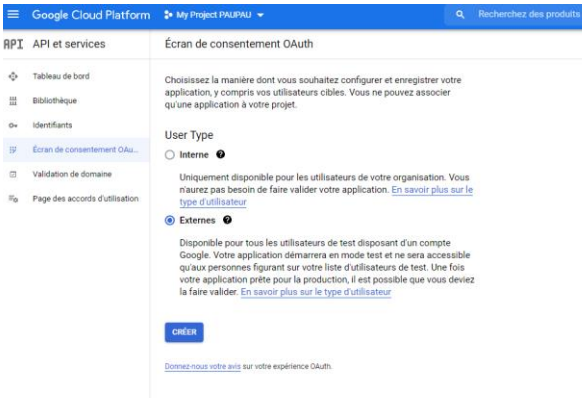
The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.

Authorized redirect URIs

For use with requests from a web server

URIs *: https://mivoice5000FQDN.lab.company.fr/system/MiVoice5000Mail.htm

Select the user type.



Écran de consentement OAuth

Choisissez la manière dont vous souhaitez configurer et enregistrer votre application, y compris vos utilisateurs cibles. Vous ne pouvez associer qu'une application à votre projet.

User Type

○ Interne

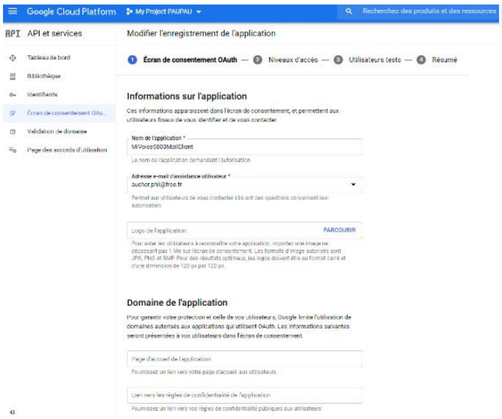
Uniquement disponible pour les utilisateurs de votre organisation. Vous n'aurez pas besoin de faire valider votre application. En savoir plus sur le type d'utilisateur

● Externes

Disponible pour tous les utilisateurs de test disposant d'un compte Google. Votre application démarrera en mode test et ne sera accessible qu'aux personnes figurant sur votre liste d'utilisateurs de test. Une fois votre application prête pour la production, il est possible que vous deviez la faire valider. En savoir plus sur le type d'utilisateur

Donnez-nous votre avis sur votre expérience OAuth.

In the following screens, fill in the different fields.



Modifier l'enregistrement de l'application

1 Écran de consentement OAuth — 2 Niveaux d'accès — 3 Utilisateurs tests — 4 Résumé

Informations sur l'application

Ces informations apparaissent dans l'écran de consentement, et permettent aux utilisateurs finaux de vous identifier et de vous contacter.

Nom de l'application * : MiVoice5000MailClient

Le nom de l'application demandant l'autorisation

Adresse e-mail d'assistance utilisateur * : bucher.phil@free.fr

Permet aux utilisateurs de vous contacter s'ils ont des questions concernant leur autorisation

Logo de l'application

Pour aider les utilisateurs à reconnaître votre application, importez une image ne dépassant pas 1 Mo sur l'écran de consentement. Les formats d'image autorisés sont JPG, PNG et BMP. Pour des résultats optimaux, les logos doivent être au format carré et d'une dimension de 120 px par 120 px.

Domaine de l'application

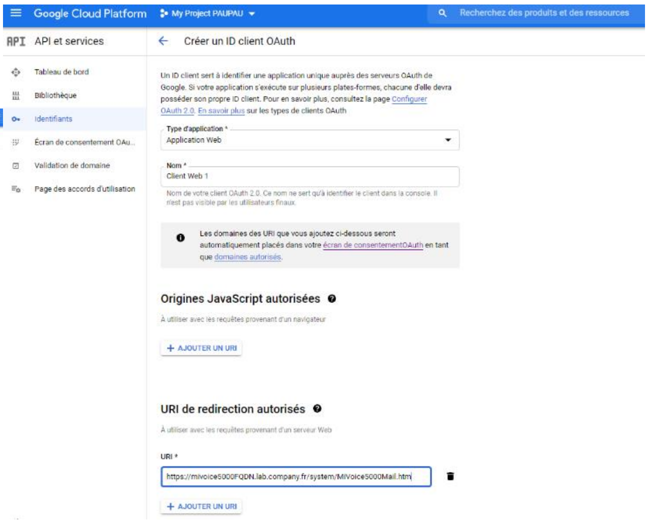
Pour garantir votre protection et celle de vos utilisateurs, Google limite l'utilisation de domaines autorisés aux applications qui utilisent OAuth. Les informations suivantes seront présentées à vos utilisateurs dans l'écran de consentement.

Page d'accueil de l'application

Fournissez un lien vers votre page d'accueil aux utilisateurs

Lien vers les règles de confidentialité de l'application

Fournissez un lien vers vos règles de confidentialité publiques aux utilisateurs



Créer un ID client OAuth

Un ID client sert à identifier une application unique auprès des serveurs OAuth de Google. Si votre application s'exécute sur plusieurs plates-formes, chacune d'elle devra posséder son propre ID client. Pour en savoir plus, consultez la page Configurer OAuth 2.0. En savoir plus sur les types de clients OAuth

Type d'application * : Application Web

Nom * : Client Web 1

Nom de votre client OAuth 2.0. Ce nom ne sert qu'à identifier le client dans la console. Il n'est pas visible par les utilisateurs finaux.

Les domaines des URI que vous ajoutez ci-dessous seront automatiquement placés dans votre écran de consentementOAuth en tant que domaines autorisés.

Origines JavaScript autorisées

À utiliser avec les requêtes provenant d'un navigateur

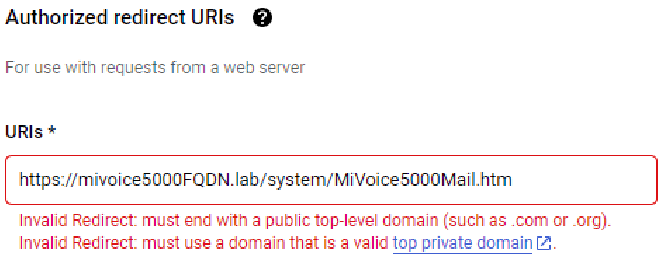
URI de redirection autorisés

À utiliser avec les requêtes provenant d'un serveur Web

URI * : https://mivoice5000FQDN.lab.company.fr/system/MiVoice5000Mail.htm

In the **URI redirection authorised** field , enter the URI which must be complete and correspond to the following domain for MiVoice 5000:

https://mivoice5000FQDN.lab.company.fr/system/MiVoice5000Mail.htm.



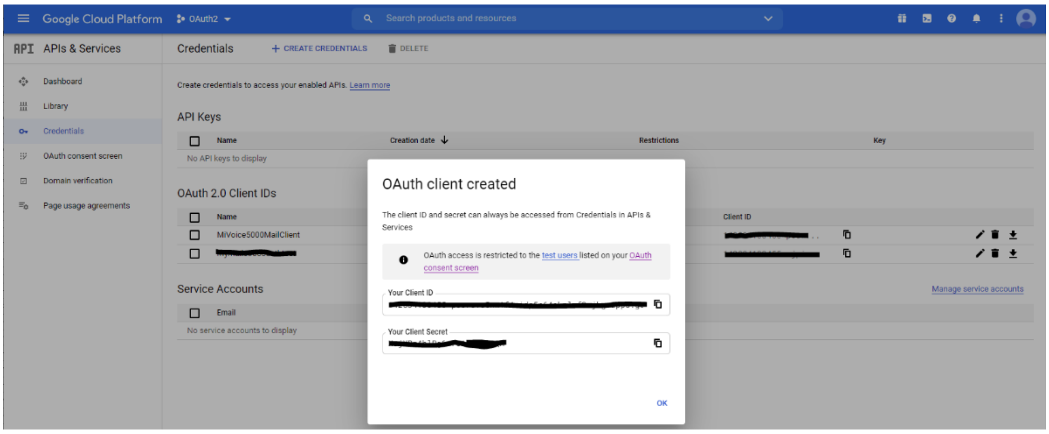
Authorized redirect URIs

For use with requests from a web server

URIs * : https://mivoice5000FQDN.lab/system/MiVoice5000Mail.htm

Invalid Redirect: must end with a public top-level domain (such as .com or .org).
Invalid Redirect: must use a domain that is a valid top private domain.

Once the OAuth client has been created, save the Client ID and Client PIN:



Credentials

Create credentials to access your enabled APIs. Learn more

API Keys

☐	Name	Creation date ↓	Restrictions	Key
	No API keys to display			

OAuth 2.0 Client IDs

☐	Name	Client ID
☐	MiVoice5000MailClient	[redacted]
☐	[redacted]	[redacted]

Service Accounts

☐	Email
	No service accounts to display

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

OAuth access is restricted to the test users listed on your OAuth consent screen

Your Client ID: [redacted]

Your Client Secret: [redacted]

Then return to Menu **SYSTEM>Configuration>E-mail** in the iPBX for the rest of the procedure. Refer to Section 4.3.5.3 Description of the different fields.

9.3 REGISTERING THE MIVOICE 5000 IPBX IN 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.

9.4 IMPLEMENTING THE POWER-SAVING FUNCTION ON MIVOICE 5000 SERVER SYSTEMS

To reduce the power consumption on Mitel 5000 gateways iPBXs, the power-saving function is used to configure a calendar on the basis of which a certain number of terminals are switched off or powered up:

- When the calendar changes to night mode, the terminals are switched off (Power Saving On).
- When the calendar changes to day mode, the terminals are powered up (Power Saving Off).

Activation or deactivation is on a port by port basis on cards.

Power supply is not cut if:

- The terminal is communicating
- The firmware is being updated on the terminal
- The terminal is logging onto a subscription

The terminal is restarted:

- At the time specified by the calendar
- When the iPBX restarts
- When an update operation starts on the terminal.

The terminals do not all restart at the same time, to avoid too much power consumption.

Common terminals

The configuration (activating or not activating the power-saving function) is general for all these terminals and associated with the characteristic of the common subscriber.

Hunt groups

For hunt groups, the function is applied on terminals set to this mode (Menu **Telephony service>Subscribers>Right>General settings**), except for priority terminals.

For virtual TDM terminals, the power-saving function is also activated on Mitel 5000 Server.

By default, all the terminals connected to these cards are concerned, except attendant consoles and night consoles.

The power-saving function can be prohibited for certain terminals by transferring an already existing right to the associated subscription: "Priority terminal".

Terminals on which the power-saving function has been applied are seen as "NOT SUPPLIED".

All the terminals are powered up when the iPBX is started.

The terminals change to power-saving mode next time the calendar associated with the power-saving function changes to night mode.

Changes in the power-saving function status (On/Off) are indicated by a message in the logbook and through the transmission of an alarm-type service ticket.

It is possible to force power supply to the terminals:

- From Web Admin, by manually performing a transition: switching OFF / switching ON on the subscriptions or on the devices concerned.
- From MiVoice 5000 Manager or MiVoice 5000 Web Admin, which proposes an action resulting in the sending of an OFF/ON request on the subscriptions concerned (see the MiVoice 5000 Manager User Guide).
- Power is then supplied to the terminal until the calendar switches to NIGHT mode.

VIRTUAL TERMINALS

To manage virtual TDM terminals, MiVoice 5000 (subscriber declaration) (terminal connection) sites must have consistent power-saving function calendars.

9.4.1 RECOMMENDATIONS

It is advisable to keep the terminals working, including outside opening hours, especially backup terminals, the answering service, corridor terminals, lift terminals, isolated sites, secretariats and, possibly, managers, in order to allow access to the phone (especially for emergency calls) in case of unexpected presence of a person. It is advisable to inform users about the implementation of the power-saving function and about the list of terminals that remain available, even outside opening hours.

9.4.2 DECLARING A CALENDAR

The menu **Reception>Calendars>Names** is used to create a calendar (among the 16 possible calendars) for the power-saving function and to assign it an 8-character name.

The calendar is created without timeslot. Therefore, its default status is "Day".

9.4.3 DEFINING TIMESLOTS

The menu **Reception>Calendars>Calendar range definition** is used to define a specific calendar, the "Day" / "Night" switchover timeslots for each day of the week.

Select the calendar in question for the power saving function.

For the description of the different fields, see Section **Erreur ! Source du renvoi introuvable.**.

9.4.4 ACTIVATING THE POWER-SAVING FUNCTION AND ASSOCIATING THE CALENDAR

In Menu **Subscribers>Rights>General settings**, the two lines below are associated with the power-saving function:

- The power-saving function line is used to activate/deactivate the function via a checkbox.
- The associated calendar option is used to assign a calendar to the power-saving function. This line is only displayed if the previous line is ticked.

Principle:

When the iPBX is started, all the terminals are powered up by default; the power-saving function is, therefore, deactivated.

As a result, when the function is activated from this menu:

- If the status of the associated calendar is "day", no message is sent (logbook and alarm ticket).
- If the status of the associated calendar is "night", the messages are sent (logbook and alarm ticket).

On the other hand, when the function is disabled:

- If the status of the associated calendar has been "day", no message is sent (logbook and alarm ticket).
- If the status of the associated calendar has been "night", power up the terminals again, and the activation message is sent (logbook and alarm ticket).

When the associated calendar is modified, if the Day/Night status of the new calendar is different from the status of the previous calendar, the messages are sent (logbook and alarm ticket) with the status of the power-saving function corresponding respectively to the Night/Day status of the new calendar.

9.4.5 PRIORITY TERMINALS

9.4.5.1 *Rights managed according to subscription*

If the rights are not managed according to feature classes, Menu **Subscribers>Subscriptions>Characteristics** is used to inhibit the power-saving function for the terminals associated with the subscription on which the "priority terminal" right is ticked.

Note: When the right is modified, there is no status change for the subscription. Therefore, if the right is activated when there is no power supply to the terminal, it remains so unless the subscription/equipment status is changed manually (this forces power supply to the terminal). Next time the calendar changes to day mode the TEL software forces power supply to the terminal, no matter the value of the right.
This right may (or may not) be defined on the COMMON subscriptions. Thus, ALL the terminals logged onto this subscription are protected (or not), against the power-saving function.

9.4.5.2 *Rights managed according to features classes*

If the rights are managed according to feature classes, Menu **Subscribers>Rights>Feature classes** is used to inhibit the power-saving function for terminals whose subscription has a feature class in which the "priority terminal" right is ticked.

Note: When rights are modified in a feature class there is no status change on the subscriptions having this class. There is no status change either on a subscription

whose feature class is changed. Therefore, for terminals without power supply, if the right is activated via the feature class assigned to their subscription, the terminals remain without power supply unless the status is manually changed on the subscriptions/devices linked to this feature class. Next time the calendar changes to day mode the TEL software forces power supply to the terminal, no matter the value of the right. A feature class is also associated with COMMON subscriptions. This way, all the terminals logged onto the COMMON subscription are protected or not protected against the power-saving function, depending on the configuration in the feature class associated with the COMMON subscription.

9.4.6 VIEWING THE CALENDARS ASSIGNED TO THE POWER-SAVING FUNCTION

Menu **Reception>Calendars>Display** gives the status and assignment of all the Day/Night switchover calendars.

The power-saving column indicates whether or not a calendar has been assigned to this function.

9.4.7 DISPLAYING USERS OF THE POWER-SAVING FUNCTION

The **By power saving** field of Menu **Call distribution>Calendars>Display users** displays the user function(s) of this particular calendar.

9.4.8 DISPLAYING THE STATUSES OF USERS OF THE POWER-SAVING FUNCTION

Menu **System>Supervision>Display status>Telephone extensions**

When power supply to a terminal is cut, the status of the terminal changes to PERMANENT OFF-HOOK.

The status **NOT SUPPLIED** is not displayed for the subscription and cannot be used as search criterion in this menu.

Single-association subscriptions

For single-association subscriptions, the **PERMANENT OFF-HOOK** telephone status of a terminal is displayed for the subscription. For example:

- If the terminal is disconnected:
  - Subscription status = PERMANENT OFF-HOOK
  - Terminal status = PERMANENT OFF-HOOK
- If the terminal is connected but without power supply:
  - Subscription status = PERMANENT OFF-HOOK
  - Terminal status = NOT SUPPLIED.

Therefore, it is possible to limit a search, with the status PERMANENT OFF-HOOK as search criterion.

Multi-association subscriptions

For subscriptions with multiple associations, the status of the subscription depends on the status of all the terminals. The method described previously cannot be used to display the subscriptions with at least one terminal not concerned by the power-saving function (for instance, an analogue terminal or a terminal declared on an LN16 …).

The most appropriate method of displaying all the terminals in power-saving mode is to:

- List them by criteria: searched status equals "ANY" + "Sets display"
- Then make a search using CTRL+F: NOT SUPPLIED on the page displayed on the navigator.

9.4.9 VIRTUAL TERMINALS WITH DUAL HOMING

To manage virtual TDM terminals with dual homing, the calendar associated with the power-saving function must be consistent between the MiVoice 5000 Server on which the subscriptions are declared and the Mitel 5000 gateways used to connect the terminals.

The principle is to copy the calendar using the Export/Import method described below.

The calendar must be correctly declared on MiVoice 5000 Server.

On MiVoice 5000 Server:

- Log on to Mitel 5000 Server.
- From Menu Call distribution>Calendars>Display, note the name of the calendar associated with the power-saving function.
- Display the timeslots of this calendar.
- Export the current item to a file with the 💾 icon.

On Mitel 5000 Gateways:

- Log on to the iPBX:
- Create the calendar associated with the power-saving function at any level but with the same name as on the IPBX (Menu Call distribution>Calendar>Name).
- Start a massive import operation from Menu System>Software maintenance>Massive import.
- Select the file created during the export to iPBX.
- **Then "**Download**"**
- **Then "**Inclusion of data**"**.
- From Menu Subscribers>Rights>General settings, activate the power-saving function and associate the copied calendar.

9.5 SSO MODE WITH KERBEROS COMPLEMENTS

WARNING: The security certificate must be installed on the Client PC. Refer to the appendix to the MiVoice 5000 Server - Implementation Manual.

9.5.1 SSO USING KERBEROS PROTOCOL

9.5.1.1 *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.

9.5.1.2 *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.

9.5.1.3 *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.

9.5.2 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.