Updating by Repository

01/2020

AMT/PTD/PBX/0155/3/4/EN

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

CONTENTS

1 INTRODUCTION

This document describes how to update the software components of a cluster, MiVoice 5000 Server, Mitel 5000 gateways, compact MiVoice 5000 system through a localised upgrade server, either on the operator's PC (Windows), or on the MiVoice 5000 Manager server PC, or on a public Mitel platform.

1.1 REFERENCE DOCUMENTS

- XD - XL - XS - XS12 - XS6 - MiVoice 5000 Server - Functional description and hardware installation:
  - AMT/PTD/PBX/0150/EN.
- Mitel 5000 Gateways and MiVoice 5000 Server Activation:
  - AMT/PTD/PBX/0151/EN.
- MiVoice 5000 Web Admin XD-XL-XS-XS12- MiVoice 5000 Server - Operating manual:
  - AMT/PTD/PBX/0080/EN.
- MiVoice 5000 Manager Installation manual
  - AMT/PTD/NMA/0040/EN
- MiVoice 5000 Manager User manual
  - AMT/PUD/NMA/0003/EN
- Updating R6.3 security patches on Redhat and CentOS 7.x
  - AMT/PTD/NMA/0062/4/0/EN
- MiVoice 5000 Server/Manager - Upgrading to R6.3
  - AMT/PTD/PBX/0161/1/0/EN

1.2 TERMINOLOGY

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

1.3 DEFINITION

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

2 DESCRIPTION

2.1 INTRODUCTION

This new method is based on the use of an upgrade server on which are stored the software components required to upgrade the software of a Cluster, MiVoice 5000 Server, Mitel 5000 gateways or of a MiVoice 5000 compact.

The upgrade server may be located:

- on the installer's PC,
- on the Mitel public server,
- on the MiVoice 5000 Manager server PC.

➢ **Up to R6.4**

- Each software component is provided with its own package.
  - A software component may be:
    - CentOS
    - Some security patches related to CentOS
    - The iPBX application release
    - The software of a terminal model (there are as many software components as terminal models).

For a software subscription, check the validity of the license.

➢ **As of R6.5**

Simplification of package format

The software release of a Cluster, MiVoice 5000 Server, Mitel 5000 gateways or MiVoice 5000 compact system is only upgraded by Repository using an upgrade server on which the upgrade packages are stored.

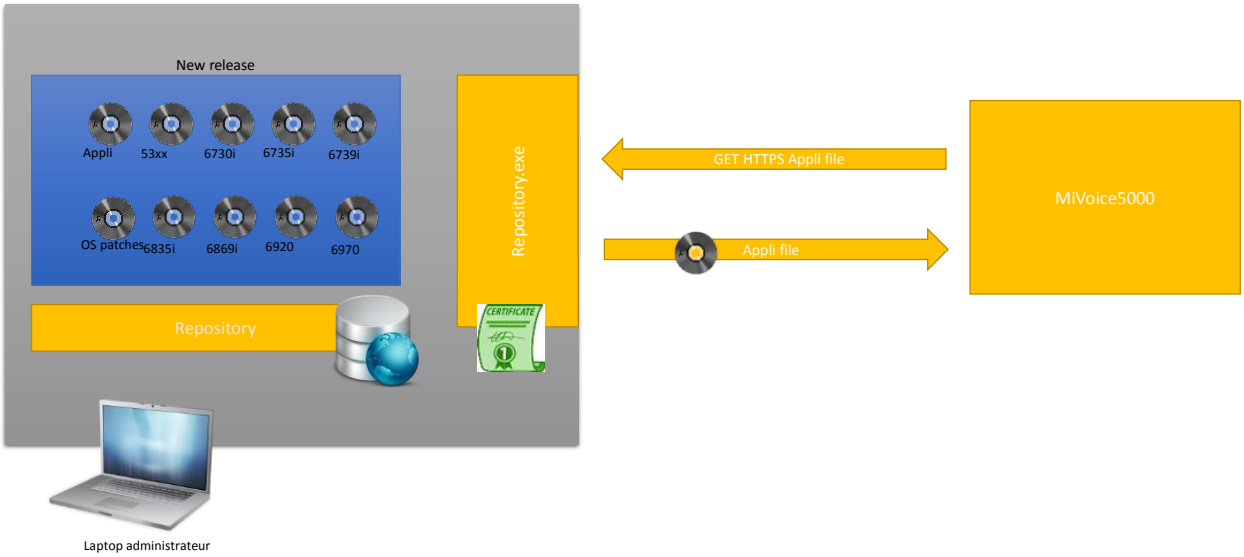
These packages, unlike the previous ones, bring together, in a single compressed file, all the software components necessary for the software upgrade.

A compressed ≥ R6.5 package may be:

- A package containing a new version of MiVoice 5000,
- A package containing a delta batch for a MiVoice 5000 version,
- A package containing the security patches,
- A package containing the terminal software.

In all these types of packages, a tool is also delivered to define the Repository on the installer's laptop disk and install the packages there.

This tool allows an HTTP / HTTPS link to be set up in order to manage the exchanges between the MiVoice 5000 Server when there is no MiVoice 5000 Manager, for instance.


New release
Appli
53xx
6730i
6735i
6739i
OS patches
6835i
6869i
6920
6970
Repository
Repository.exe
CERTIFICATE
GET HTTPS Appli file
Appli file
MiVoice5000
Laptop administrateur

2.2 SYSTEM COMPATIBILITY FOR UPDATES WITH OR WITHOUT REPOSITORY

MiVoice 5000 Servers

<table>
<tr><th>MiVoice 5000 Server
De \Vers</th><th>R6.1</th><th>R6.2</th><th>R6.3 SP+</th><th>R6.4</th><th>≥ R6.5</th></tr>
<tr><td>R6.1</td><td>With or without Repository</td><td>With or without Repository</td><td colspan="3" rowspan="2">Upgrade required with change from OS to CentOS R7.X involving prior data backup</td></tr>
<tr><td>R6.2</td><td></td><td>With or without Repository</td></tr>
<tr><td>R6.3 IP</td><td></td><td></td><td>Without Repository (old method)</td><td>Without Repository (old method)</td><td>Not supported</td></tr>
<tr><td>R6.3 SP1</td><td></td><td></td><td>With or without Repository</td><td>With or without Repository</td><td>Only with Repository with new ≥ R6.5 package</td></tr>
<tr><td>R6.4</td><td></td><td></td><td></td><td>With or without Repository</td><td>Only with Repository with new ≥ R6.5 package</td></tr>
<tr><td>Release ≥ R6.5</td><td></td><td></td><td></td><td></td><td>Only with Repository with new ≥ R6.5 package</td></tr>
</table>

The new package delivered as of R6.5 can be used to upgrade to release **≥** R6.5 a MiVoice 5000 Server R6.3 SP1, R6.4 or **≥** R6.5.

For the old method without repository not described below, refer to the documents relating to these incompatible versions.

Mitel 5000 Gateways

Mitel 5000 gateway From/To	R6.1	R6.2 SP+	R6.3 SP+	R6.4	≥ R6.5
R6.1	Without repository (old method)	Without repository (old method)	Without repository (old method)	Without repository (old method)	Not supported
R6.1 SPX	With or without repository	With or without repository	With or without repository	With or without repository	Repository with new package only
R6.2		Without repository (old method)	Without repository (old method)	Without repository (old method)	Not supported
R6.2 SP2		With or without repository	With or without repository	With or without repository	Repository with new package only
R6.3 IP			Without repository (old method)	Without repository (old method)	Not supported
R6.3 SP1			With or without repository	With or without repository	Repository with new package only
R6.4 IP				With or without repository	Repository with new package only
≥ R6.5 IP					Repository with new package only

The new package delivered in release ≥ R6.5 can be used to upgrade to version **≥** R6.5, a Mitel 5000 gateway R6.1 SPX, R6.2 SP2, R6.3 SP1, R6.4 or **≥** R6.5.

For the old method without repository not described below, refer to the documents relating to these incompatible versions.

Additional comments

MV 5000 Manager automatically adapts the Upgrade function to the software release of the site or the list of selected sites.

For an upgrade from MiVoice Manager, it is still possible to upgrade sites with a release below R6.4 in a heterogeneous multi-site configuration using the old methods.

2.3 NEW FEATURES BROUGHT IN BY R6.5 FOR UPDATE BY REPOSITORY

- The Upgrade Server gives access to CentOS security patches (MiVoice 5000 Server), a new version of the MiVoice 5000, a batch of a version of the MiVoice 5000 or a terminal software package.
- A tool that turns the user's Windows PC into a repository upgrade server.
- With a system release ≥ R 6.4 managed by a MiVoice 5000 manager, the interface has control and status monitoring for each stage and for each site.

3 INSTALLING THE REPOSITORY AND ≥ R6.5 PACKAGES ON THE INSTALLER'S LAPTOP PC

If the repository is installed on the Installer PC, this PC must be on the same network as the iPBXs to be upgraded.

This PC must be in a Windows environment (Windows 7 minimum).

The **R6.5_RC_AXYZ.zip** package provided for the release ≥ R6.5 by Mitel must be decompressed into a local directory of the installer PC.

It is advisable to always use the same directory to facilitate the management of different update releases.

The R6.5 package is valid, no matter the original release and iPBX type (Gateway or Server).

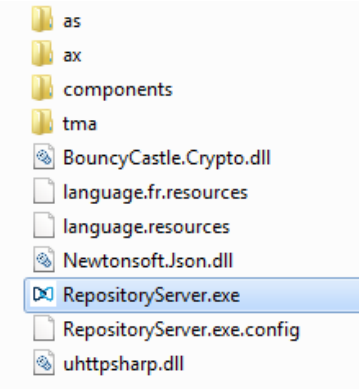
The tool is valid for upgrades to relase ≥ R6.5 only.

This package contains:

- The MiVoice 5000 Server update package
- The Mitel 5000 gateway update package, including the operating system supported by these systems
- The terminal software update TMA package
- A tool for transforming the installer PC into a Repository Server.

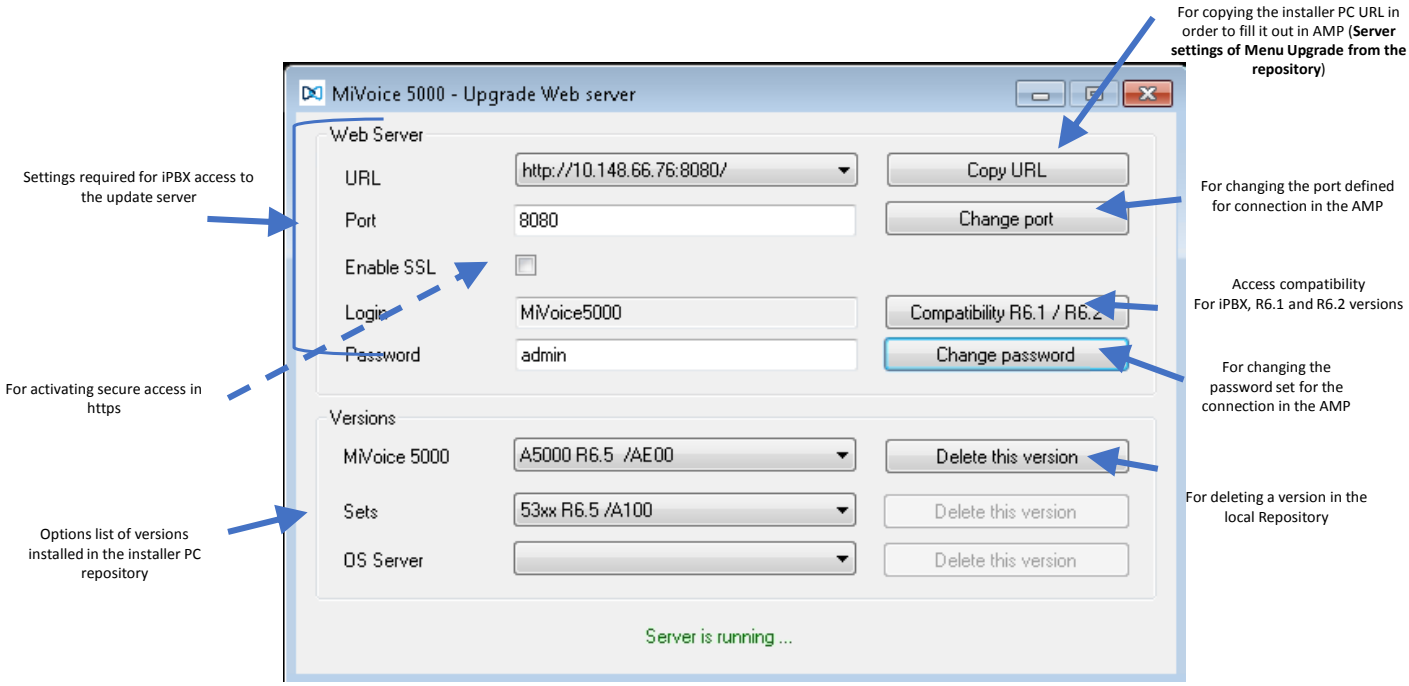
Installation

- Place this **R6.5_RC_XXXX.zip** file in a local directory on the installer PC.
- Decompress this file.
- The decompressed directory is in the form:



- Then run the executable file **RepositoryServer.exe**
- **Note: The message "Alert me when the Windows firewall blocks a new program" may appear. Ignore the message and allow the executable to run.**

The upgrade server management screen opens, allowing the actions described in the figure below:



TMA can access a terminal release even if this release is included in a MiVoice 5000 package.

The MiVoice 5000 Update software offers an option to remove a MiVoice 5000 package, a TMA terminal package or an OS patch package.

This package removal is only available when the package is not part of the MiVoice 5000 package.

The following parameters may be personalised:

- **Password**: password used by the iPBX to access the local installer PC server
- Port: (default value: 8080) port defined in the URL to access the local server
- **Protocol**: HTTP (by default) or HTTPS

When a parameter is changed, its value is stored locally. The tool therefore shows the last value stored locally each time the tool is started.

4 UPGRADING BY REPOSITORY WITHOUT MIVOICE 5000 MANAGER

4.1 PREREQUISITES

Packages for upgrading to release ≥ R6.5 are supported as of release R6.1 (latest service pack) on Mitel 5000 gateway and as of R6.3 (last service pack) on Mitel 5000 Server. Refer to Section 2.2 for compatibility details.

The packages are provided by Mitel and must be retrieved from the PC or dedicated server for the repository.

If the repository is installed on the Installer PC, this PC must be on the same network as the iPBXs to be upgraded.

This PC must be in a Windows environment (Windows 7 minimum).

In release ≥ R6.5, the operating system must be CentOS 7.x for MiVoice 5000 Server and MiVoice 5000 compact. Therefore, it is mandatory to first upgrade to CentOS 7.x if the current operating system version is earlier than CentOS 7.x.

4.2 SUMMARY OF THE STAGES OF THE PROCEDURE

This section gives a summary of the phases of the procedure.

For full details of each phase see the following sections.

- Collect the update packages from Mitel.
- Manual installation of update by Repository packages on the installer PC for a repository on installer PC,
- Enter the IP address of the Repository server in Web Admin.
- Programming, via Web Admin, the date/time of package download on the iPBX concerned
- Programming, via Web Admin, the date/time when these packages will be taken into account on the iPBXs concerned
- Validating the packages on the iPBXs concerned.

If failures occur during these different phases, the actions must be restarted.

4.3 UPDATING THE SYSTEM IPBX APPLICATION RELEASE

Note: When the system's application version is updated, the terminal software type components are also updated on the system according to the rules defined below.

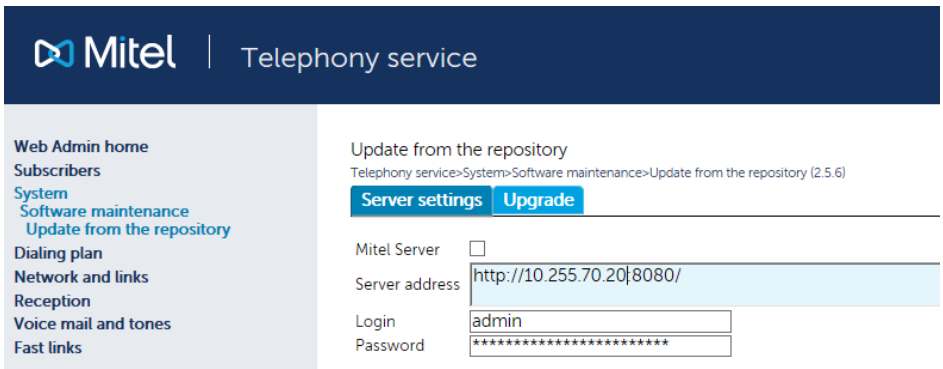
4.3.1 FOR UPGRADING R6.1 - R6.4 TO RELEASE ≥ R6.5:

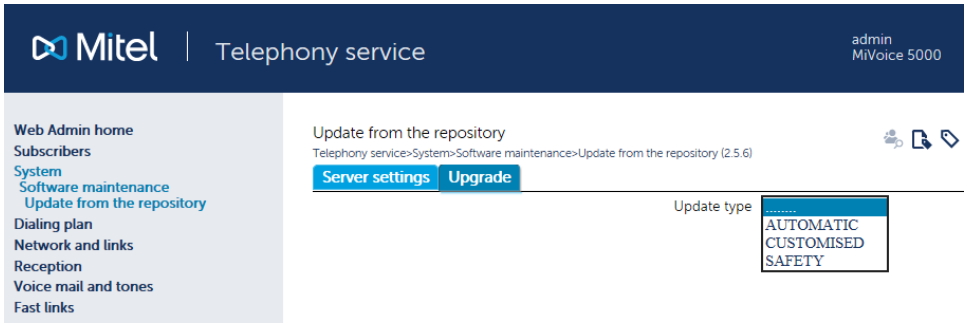
NOTE: For some releases and depending on the MiVoice 5000 Server or Gateway system, update by repository is not applicable. Refer to Section 2.2. For these releases, only the old method (without repository) is applicable. The old method is not described in this document, refer to Operating manual AMT/PTD/PBX/0080 for these releases.

From Web Admin, Menu **Telephony service>System>Software maintenance>Upgrade from repository**:

- In the **Server Settings** tab,
- For a Mitel server, tick the **Mitel server** box.
- If the repository is installed on a server other than Mitel server, untick the **Mitel Server** box.
- Fill in the address of this server as well as the corresponding login/password also defined on the repository server.

If the repository is installed on the installer PC, after launching the tool **RepositoryServer.exe** retrieve the address from the **Copy URL** button. Refer to Section 3.





- In the upgrade tab, for **Update type**, select **Automatic** (this corresponds to downloading the system upgrade package).
  - All the components of the upgrade package are listed.

- The components to be upgraded are automatically selected according to the following rules:
  - Any application or terminal software version above the current version in the system
  - Any component selected in the management MMI from the list of components (Menu **Telephony service** > **Subscribers** > **Terminals and applications** > **Software**)
- The components to be upgraded are automatically **unselected** according to the following rules:
  - Any application or terminal software version equal to the current version in the system
  - Any component not selected in the management MMI from the list of components (Menu **Telephony service** > **Subscribers** > **Terminals and applications** > **Software**)
  - Any terminal software type component included in the system upgrade package

- In the **Software version** field, only the upgrade packages whose version is above or equal to the current version of the system and installed on the upgrade server is displayed.

Note: If no upgrade package is displayed, it means that either the URL or login is incorrect or that the licence is not valid.

- Indicate whether the downloading of the upgrade package to the site concerned is **immediate** or **deferred.** Also specify the maximum time taken to transfer the upgrade package installation script.

Note: By default, in deferred mode, downloading is programmed to start 10 minutes later. If the duration of downloading exceeds the number of hours defined, the downloading process is abandoned.

- For the **Type of switchover** parameter, indicate whether the switchover is **immediate** or **deferred.**

Note: In deferred mode, the programming of switchover takes account of the maximum duration of transfer.

- Check that the **To load** parameter has actually been ticked for application or terminal software type components, then click the **Validation** button.

Downloading the application version to and implementing it on the iPBX

- After the previous action is started and, depending on its configuration, the components are downloaded to the system concerned from the upgrade server.
- These components are taken into account when the system restarts automatically.
- After this restart, validate the active software from the Web Admin welcome banner.

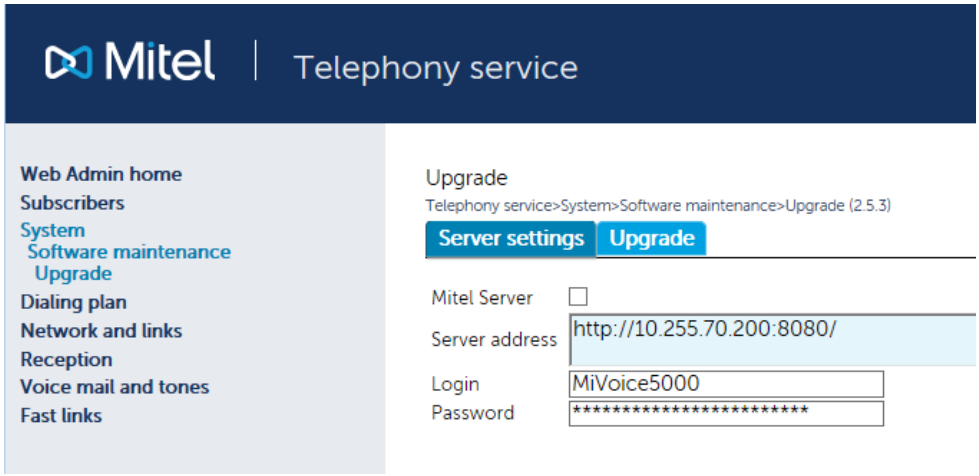
Note: The version of CentOS remains identical after the new application version is installed on an MiVoice 5000 server.

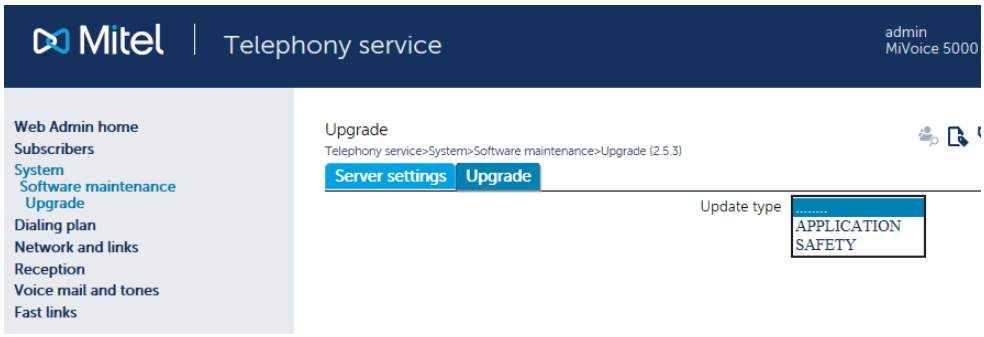
4.3.2 UPGRADING RELEASES ≥ R6.5 N TO RELEASES ≥ R6.5 N + 1:

From Web Admin, Menu **Telephony service>System>Software maintenance>Upgrade**

- In the **Server Settings** tab,
- For a Mitel server, tick the **Mitel server** box.
- If the repository is installed on a server other than Mitel server, untick the **Mitel Server** box.
- Fill in the address of this server as well as the corresponding login/password also defined on the repository server.

If the Repository is installed on the installer PC, after launching the tool **RepositoryServer.exe** retrieve the address from the **Copy URL** button. Refer to Section 3.





- In the upgrade tab, for **Update type**, select **APPLICATION** (this corresponds to the downloading of the IPBX upgrade package).
  - All the components of the upgrade package are listed.
  - The components to be upgraded are automatically selected according to the following rules:
    - Any application type or terminal software release above the current version in the system,
    - Any component selected in the management MMI from the list of components (Menu **Teerminal service** > **Software management**)
  - The components to be upgraded are automatically **unselected** according to the following rules:

  - Any component or terminal software version equal to the current version in the system
  - Any terminal software type component included in the system upgrade package

- In the **Software version** field, only the upgrade packages whose version is above or equal to the current version of the system and installed on the upgrade server are displayed.

Note: If no upgrade package is displayed, it means that either the URL or one of the login parameters is incorrect.

- Indicate whether the downloading of the upgrade package to the site concerned is **immediate** or **deferred.** Also indicate the maximum transfer time.

Note: By default, in deferred mode, downloading is programmed to start 10 minutes later. If the duration of downloading exceeds the number of hours defined, the downloading process is abandoned.

- For the **Type of switchover** parameter, indicate whether the switchover is **immediate** or **deferred.**

Note: In deferred mode, the programming of switchover takes account of the maximum duration of transfer.

- Check that the **To load** parameter has actually been ticked for application or terminal software type components, then click the **Validation** button.

Downloading the application version to and implementing it on the iPBX

- After the previous action is started and, depending on its configuration, the components are downloaded to the system concerned from the upgrade server.
- After this step, the switchover starts immediately or at the programmed time and starts by preparing the new software release.
- After this restart, validate the active software from the Web Admin welcome banner.

Note: The version of CentOS remains identical after the new application version is installed on an MiVoice 5000 server.

4.4 UPDATING OPERATING SYSTEM SECURITY PATCHES

This section only applies to (physical and virtual) MiVoice 5000 Server systems on which CentOs is installed.

For MiVoice 5000 gateway systems, this menu is not applicable because the embedded OS is updated if necessary when the Application is updated.

As of R 6.5, the version of the security patches can be viewed in Menu **Telephony service>System>Info> Software Id**.

Note: The usual method of upgrading the security patches remains valid (see AMT/PTD/NMA/0062).

4.4.1 FOR RELEASES R6.1 TO R6.4

NOTE: Update by repository is not applicable for some releases. Refer to Section 2.2. For these releases, only the old method (without repository) is applicable. The old method is not described in this document, refer to Operating manual AMT/PTD/PBX/0080 for these releases.

From Web Admin, Menu **Telephony service>System>Software maintenance>Upgrade from repository**:

- In the **Server Settings** tab,
- For a Mitel server, tick the **Mitel server** box.
- If the repository is installed on a server other than Mitel server, untick the **Mitel Server** box.
- Fill in the address of this server as well as the corresponding login/password also defined on the repository server.

If the Repository is installed on the installer PC, after launching the tool **RepositoryServer.exe** retrieve the address from the **Copy URL** button. Refer to Section 3.

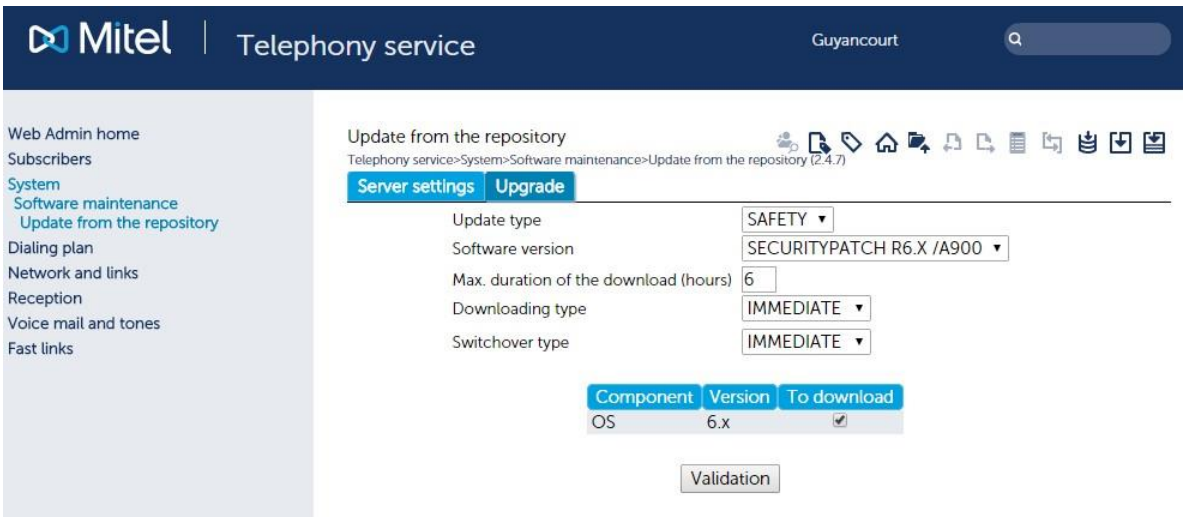
- In the **Upgrade** tab, for **Update type**, select **Security** (this corresponds to downloading the security patch component of CentOS, or the operating system for Mivoice 5000 gateways).
- In the **Software release** field, only the latest security patch installed on the upgrade server is displayed if the upgrade is necessary.
- Indicate whether downloading the operating system security patch or operating system to the site concerned is **immediate** or **deferred.** Also specify the maximum time taken to transfer the security patch installation script. The default value is appropriate in most cases. However, in cluster configuration, this duration can be adjusted according to the number of nodes.

Note: If the duration of downloading exceeds the number of hours defined, the downloading process is abandoned.

- For the **Type of switchover** parameter, indicate whether the switchover is **immediate** or **deferred.**

Note: In deferred mode, the programming of switchover takes account of the maximum duration of transfer.

- Check that the **To load** parameter is actually ticked, then click the **Validation** button.



Downloading the security patches of the operating system on the iPBXs and taking them into account on the iPBXs

- After the previous action is started and, depending on its configuration, the installation script is downloaded to the system concerned from the upgrade server.
- When running this script, the OS security patches are downloaded and installed locally on the system concerned from the upgrade server.
- The security patches (packages) of the upgraded CentOS are taken into account after the system restarts automatically.
- The new operating system for MiVoice 5000 Gateways is taken into account when the system automatically restarts.
- After this restart, validate the active software from the Web Admin welcome banner.

4.4.2 FOR RELEASES R6.5 AND HIGHER

From Web Admin, Menu **Telephony service>System>Software maintenance>Upgrade from repository**:

- In the **Server Settings** tab,
- For a Mitel server, tick the **Mitel server** box.
- If the repository is installed on a server other than Mitel server, untick the **Mitel Server** box.
- Fill in the address of this server as well as the corresponding login/password also defined on the repository server.

If the Repository is installed on the installer PC, after launching the tool **RepositoryServer.exe** retrieve the address from the **Copy URL** button. Refer to Section 3.

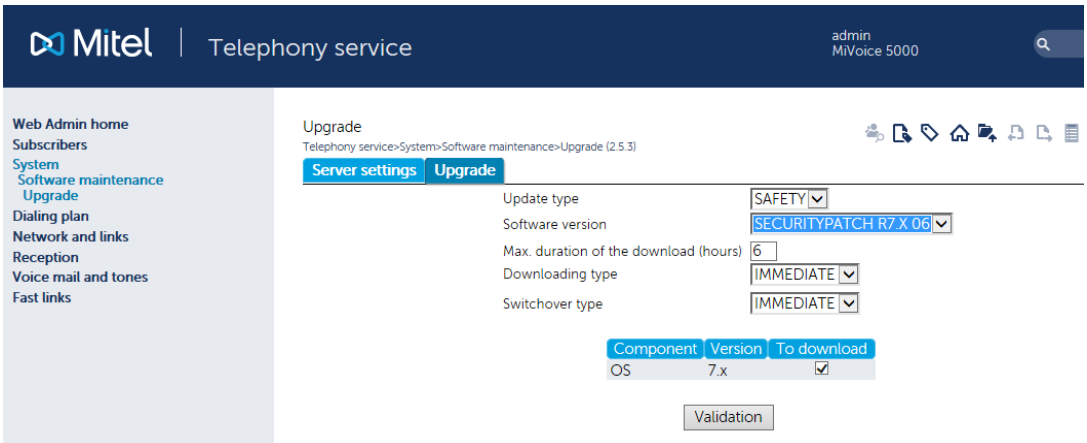
- In the **Server settings** tab, check that the **Server** is ticked (by default).
- In the **Upgrade** tab, for **Update type**, select **SAFETY** (this corresponds to downloading the security patch component of CentOS on MiVoice 5000 Servers).
- In the **Software release** field, only the latest security patch installed on the upgrade server is displayed if the upgrade is necessary.
- Indicate whether the downloading of the operating system security patch to the site concerned is **immediate** or **deferred.** Also specify the maximum time taken to transfer the security patch installation script. The default value is appropriate in most cases. However, in cluster configuration, this duration can be adjusted according to the number of nodes.

Note: If the duration of downloading exceeds the number of hours defined, the downloading process is abandoned.

- For the **Type of switchover** parameter, indicate whether the switchover is **immediate** or **deferred.**

Note: In deferred mode, the programming of switchover takes account of the maximum duration of transfer.

- Check that the **To load** parameter is actually ticked, then click the **Validation** button.



Downloading the security patches of the operating system on the iPBXs and taking them into account on the iPBXs

- After the previous action is started and, depending on its configuration, the installation script is downloaded to the system concerned from the upgrade server.
- When running this script, the OS security patches are downloaded and installed locally on the system concerned from the upgrade server.
- The security patches (packages) of the upgraded CentOS are taken into account after the system restarts automatically.
- The new operating system for MiVoice 5000 Gateways is taken into account when the system automatically restarts.

5 UPGRADING WITH UPGRADE SERVER LOCATED ON MIVOICE 5000 MANAGER

5.1 PREREQUISITES

Packages for upgrading to releases **≥** R6.5 are supported as of release R6.1 (latest service pack) on Mitel 5000 gateway and as of R6.3 (last service pack) on Mitel 5000 Server.

The Manager version must be **≥** V3.5.

5.2 GLOBAL UPDATE

In this architecture, the terminal service is deactivated on each system, and the TMA integrated into MiVoice 5000 Manager is used to manage the terminals, especially to update the terminal software.

MiVoice 5000 Manager Upgrade Services allow:

- Sites to be upgraded to releases **≥** R6.5 via the MiVoice 5000 Manager using the menu **Immediate Actions>Upgrade**
- MiVoice 5000 Server and Compact operating system security patches to be installed via MiVoice 5000 Manager using the menu **Immediate Actions>Upgrade**.

In R6.5, the update versions may be different between the different nodes and the Cluster server by respecting the following rules:

- The Cluster Server version must be higher or equal on all the nodes.
- If an update of a node is requested in a version above that of the Cluster Server, the Cluster will also be selected for update in that version.
- If the administrator ticks only the Cluster server checkbox, the action will only be launched on this Cluster server.

Note: When a cluster is partially upgraded, the administrator can continue the upgrade operation by selecting the same configuration. In this case, the menu automatically selects the cluster equipment that had not been upgraded previously. The operation is complete when all nodes are upgraded.

The management of the models managed on each iPBX is available from Web Admin before R6.5 and in TMA (Terminal Service) as of R6.5.

5.3 SUMMARY OF THE STAGES OF THE PROCEDURE

The processing described below does not concern iPBXs ≥ R6.4 which benefit from an upgrade operation control and monitoring service.

This section gives a summary of the phases of the procedure.

For full details of each phase see the following sections.

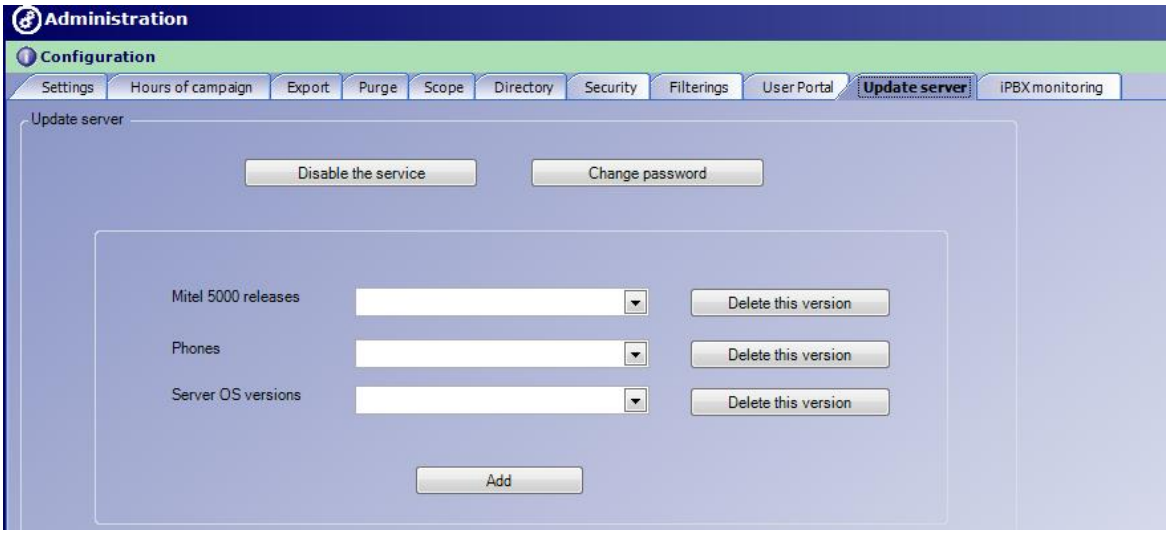
- Activating the upgrade server located on the MiVoice 5000 Manager server
- Installing the packages on the MiVoice 5000 Manager upgrade server
- Programming, via MiVoice 5000 Manager, the date/time of package download on the iPBXs concerned
- Programming, via MiVoice 5000 Manager, the date/time when these packages will be taken into account on the iPBXs concerned
- Validating the packages on the iPBXs concerned.

If failures occur during these different phases, the actions may be restarted.

5.3.1 ACTIVATING THE UPGRADE SERVER LOCATED ON THE MIVOICE 5000 MANAGER SERVER

From MiVoice 5000 Manager, Menu **Administration>Configuration**

- Select the **Upgrade server** screen.
- Click **Activate service**.



- Enter two times the password used to log on to the upgrade server, then click **OK**.

Note: The password is freely defined by the user.

An information message indicates that the new password associated with the login has been taken into account.

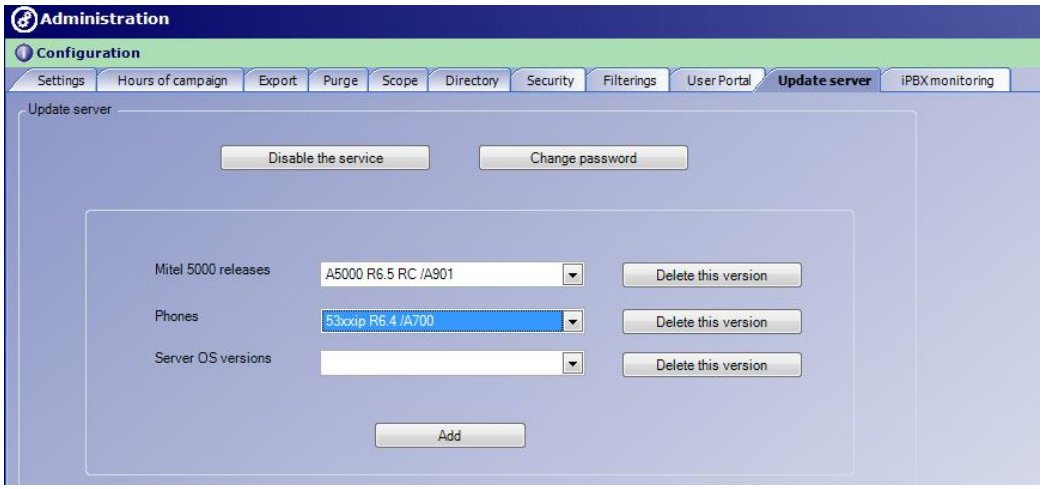
The upgrade server is enabled, allowing the installation of packages related to iPBXs, terminals and operating system patches.

5.3.2 INSTALLING THE PACKAGES ON THE MIVOICE 5000 MANAGER UPGRADE SERVER

5.3.2.1 Welcome screen

With the upgrade server enabled, the screen has 3 fields with an options list:

- **Versions of Mitel 5000**,
- **Terminals**,
- **Operating system versions**.



Note: During a first installation, all these fields are empty.

The **Add** button is used to download and install new versions on the Upgrade server.

The **Delete** this version button is used to delete a package from the Repository upgrade server.

5.3.2.2 Downloading and installation

As of R6.5, the package for an upgrade is a single compressed file (**.zip**):

- **R6.5_RC_AXYZ.zip** containing software updates for Mitel 5000 iPBXs (Gateway and Server) and terminal software.
- **SECURITYPATCH_R7.X_05.zip** containing the security patch upgrade for the MiVoice 5000 Server and Compact systems.

From the previous screen:

- Click **Add**.
- Select **R6.5_RC_AXYZ.zip** or **SECURITYPATCH_R7.X_05.zip** type file in the directory concerned from the file manager.
- Click **Open**.

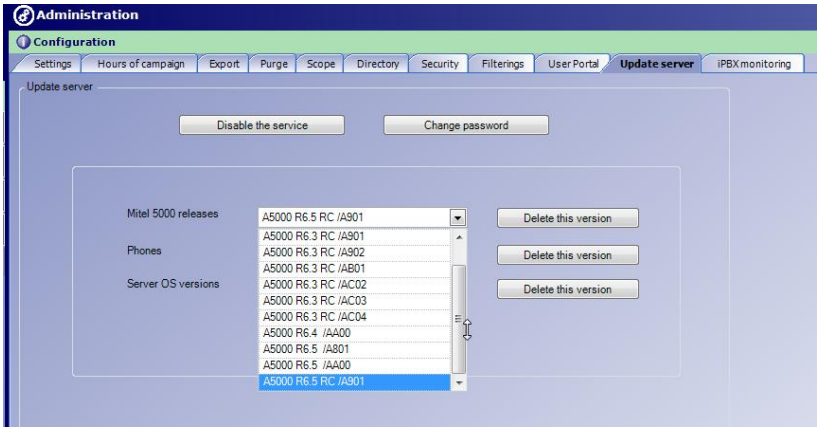
This file is then downloaded to the MiVoice 5000 Manager upgrade server.

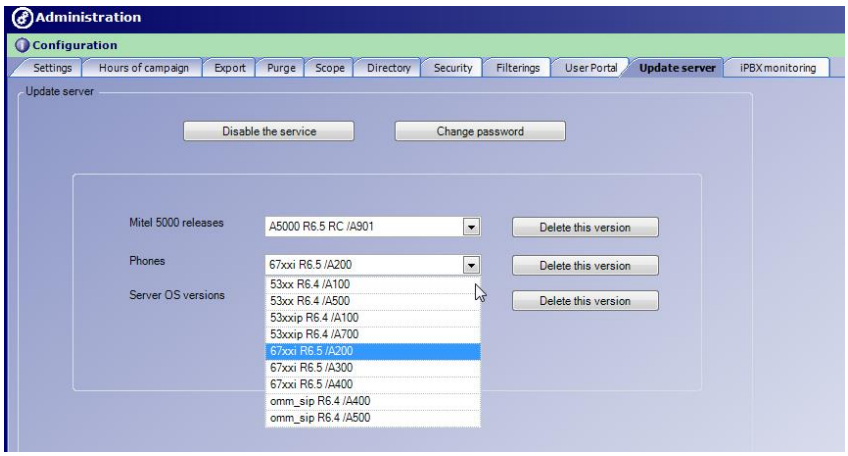
- Wait for the message which indicates that the **software package has been successfully installed**.
- Click **OK**.

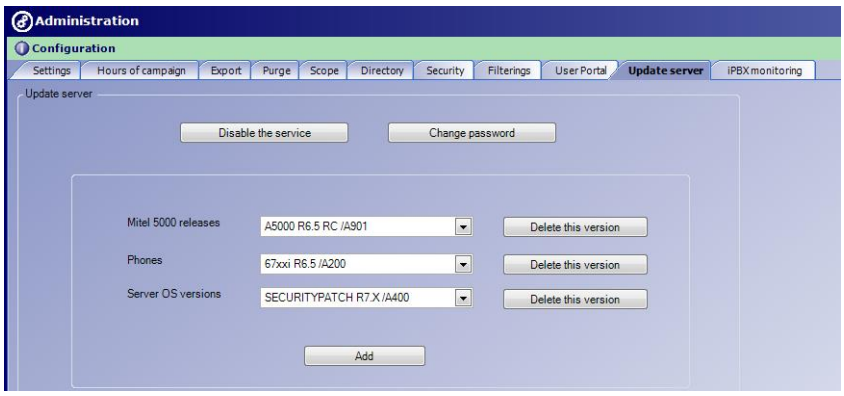
The Operations log also shows the package installation.

Once the download is complete, the new versions will be available in the options completing those previously loaded:

Examples







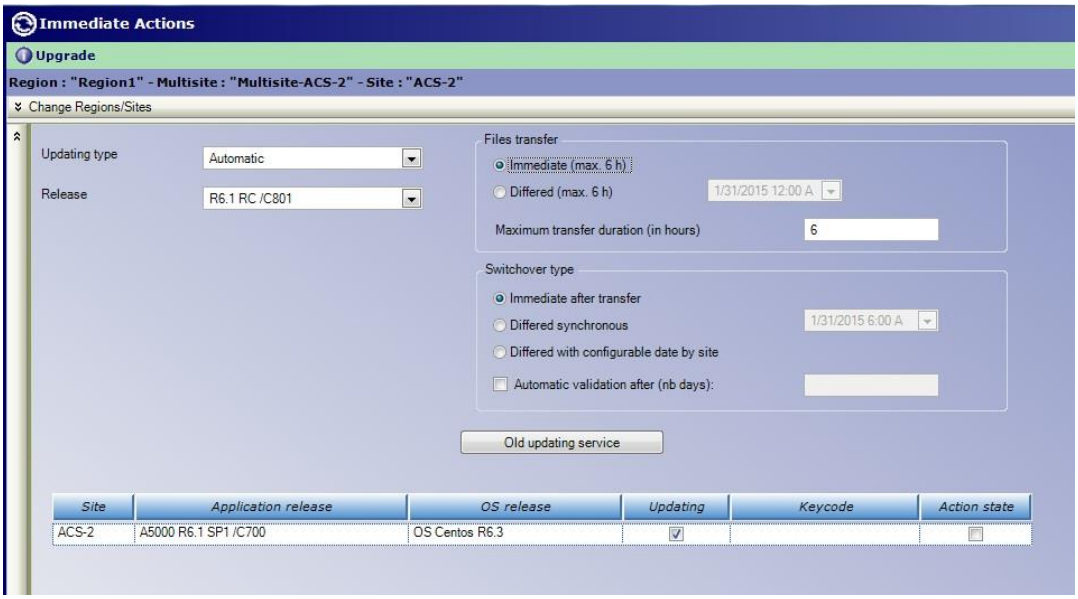
The **Delete this version** button is used to delete a package from the Repository upgrade server.

5.3.3 UPGRADE

From MiVoice 5000 Manager, Menu **Immediate actions>Upgrade,**

5.3.3.1 Consideration

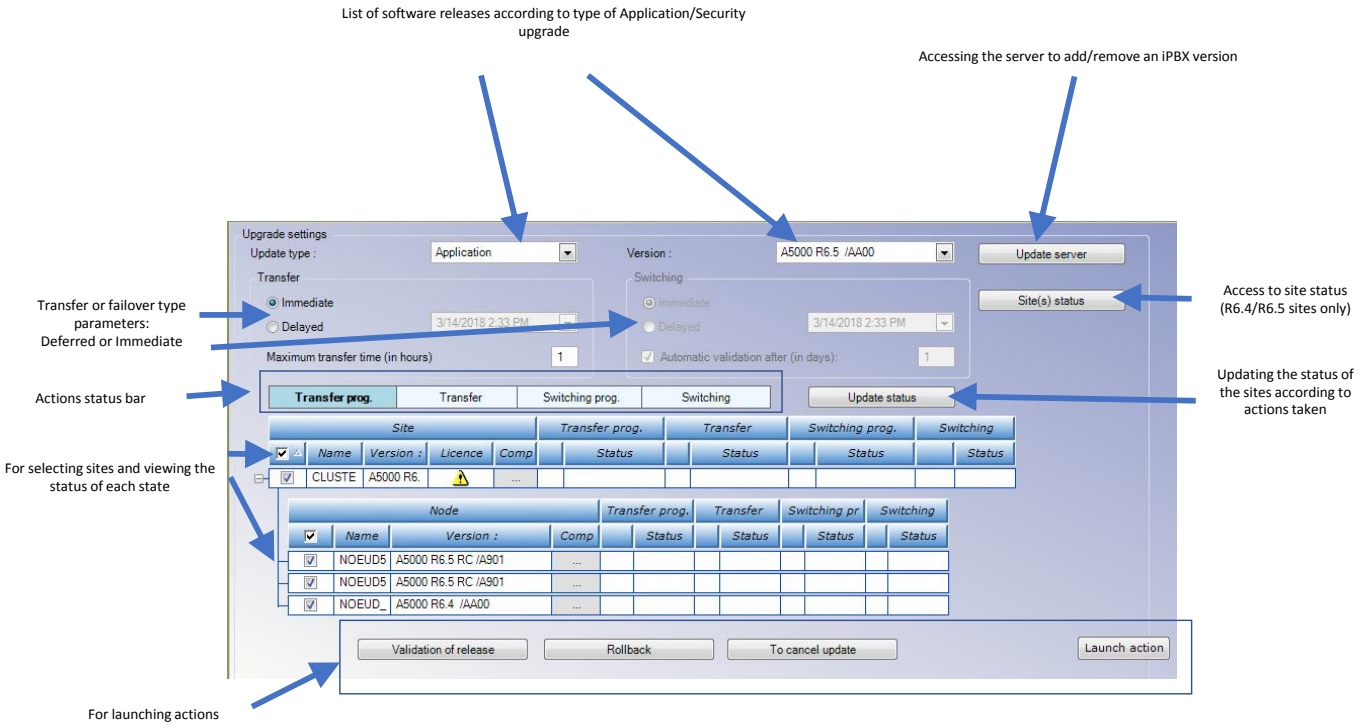
If the version of one or more of the sites is < R6.4, the screen shows the old interface, for memory:



In these cases, for the procedure, refer to document AMT/PUD/NMA/0003 for releases < R6.4.

If all sites are in a release ≥ R6.4; the screen is the one described in the paragraph below.

5.3.3.2 *Description of the upgrade screen (All Sites with version ≥ R6.4)*



Updating type: Application (iPBX software and/or terminals) or Security (OS patches)

Release:

Only releases above the current release are proposed.

Update status: for updating the status of the sites according to the action in progress

Action status bar

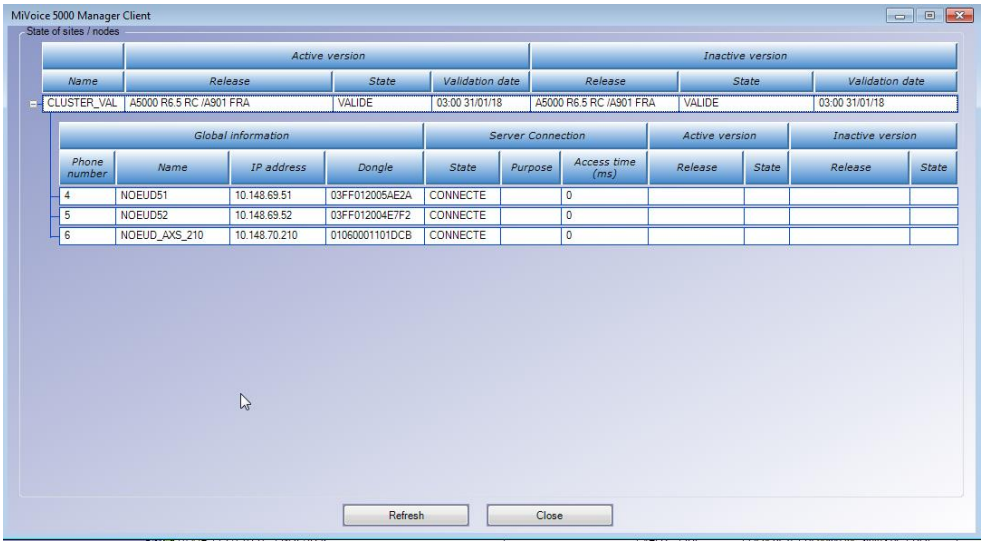
These different fields are used to view the progress of actions. The colour of the field indicates its status:

- **Blue**: the action is ready to be started.
- **White**: the action remains to be started.
- **Grey**: action completed.

Transfer or switchover actions can be initiated immediately or delayed:

Upgrade server: gives access to the upgrade server, so a release can be added or removed. This screen is also accessible in the **Upgrade server** tab of Menu **Administration> Configuration**.

Site(s) status: for viewing the status of sites (active and inactive release):



- **Refresh**: refreshes the status if necessary.
- **Close:** closes the display window

Note: The status of the sites is also accessible from Menu Administration>Network Topology menu, via the Cluster/Nodes Status button.

For the buttons, see Section 5.3.3.3.

5.3.3.3 *Upgrading IPBXs software releases (Application)*

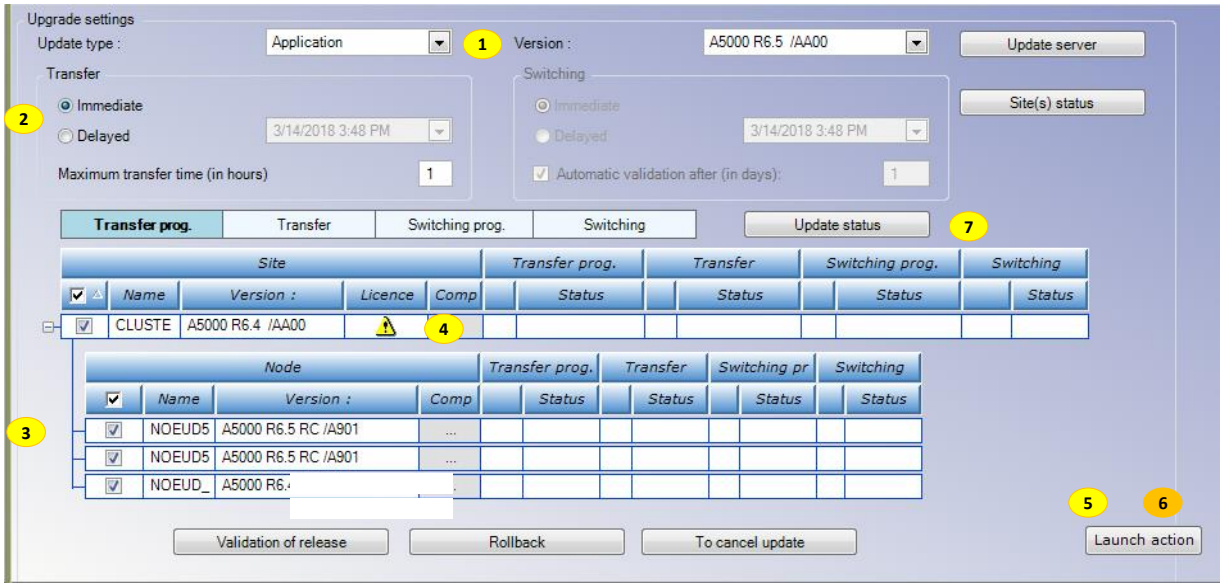
Note: Refer to Section 5.3.3.1 for the presentation of this main screen.

A step can only be scheduled if Step n-1 has been successfully completed (in this case, switchover after transfer).

NOTE: The steps must be followed in the order described below. A step can only be scheduled if Step n-1 has been successfully completed (in this case, switchover after transfer).

From MiVoice 5000 Manager, Menu **Immediate actions>Upgrade,**

- Select the system to be updated.



Step 1

The first step concerns the procedure for transferring the software from the upgrade server (Repository).

1. In the **Update type** field, select **Application** or **Safety**, and select the version for the upgrade (**Version** field).
2. In the **Transfer** section, indicate whether the downloading of the application version to the site(s) in question is **Immediate** or **Delayed.** Also indicate the maximum time taken to transfer the application version component.
3. Tick the box or boxes of sites to be upgraded.

Note: For a cluster:

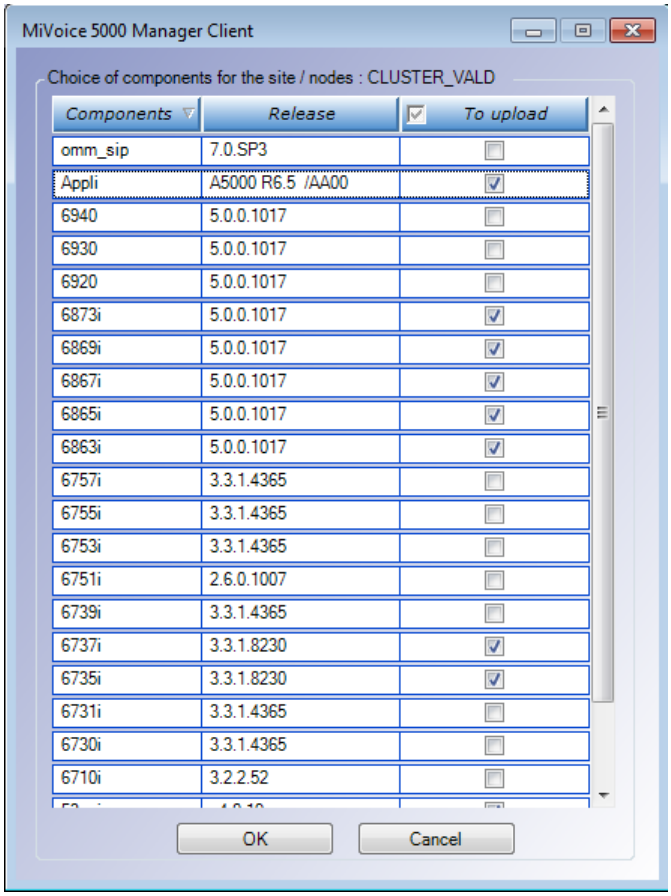
- **If the checkbox of a node is ticked requesting an update to a version above that of the Cluster Server, the checkbox of the Cluster will be automatically ticked, the rule being that a Cluster cannot have a version < that of a node.**

4. **Optional** > Click on the **Component** checkbox of the sites in question for the choice of components.

   The administrator can selectively manage components update site by site (Site list or Cluster).

   - Click on the **Component** box of the site in question.

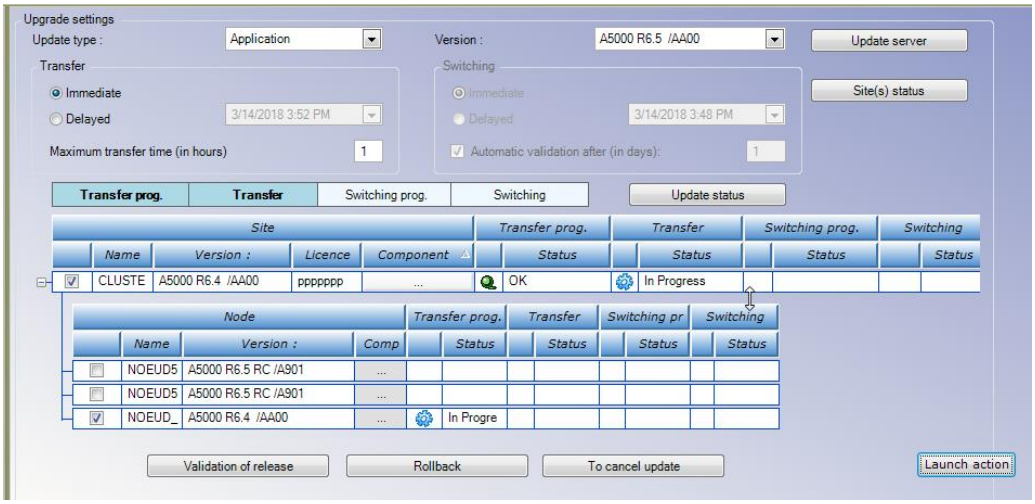
   In the same example, the component selection window is as follows.



   - Click on the boxes concerned and confirm with **OK**.

5. Start the transfer by clicking **Launch action**.
6. The display shows the progress of the transfer to the iPBX. If the status is NOK, restart the action with the same **Launch action** button.

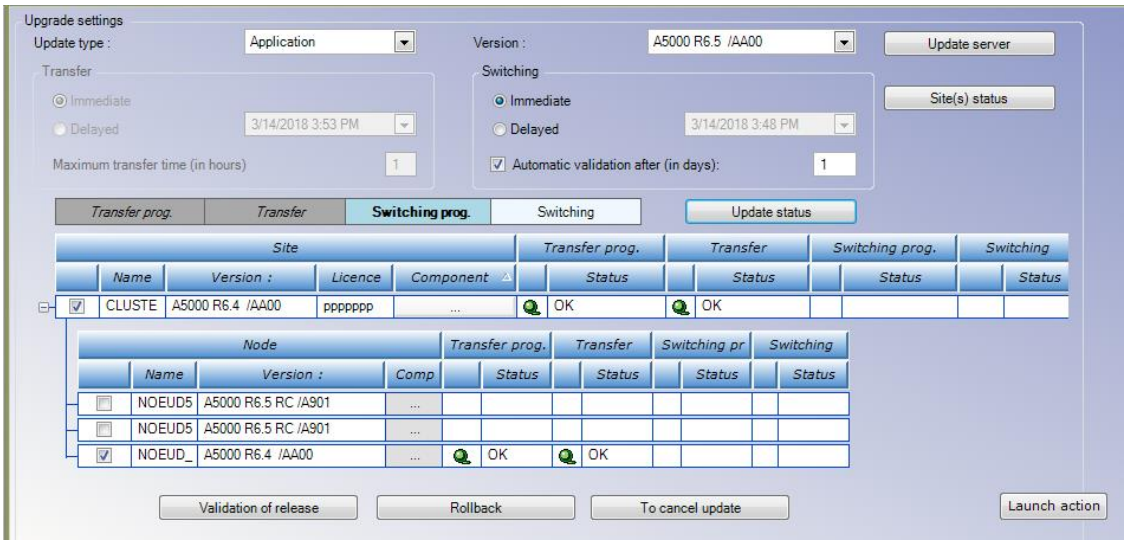
Intermediate status of the first step



7. The **Update status** button is used to refresh the status in order to know the progress status.

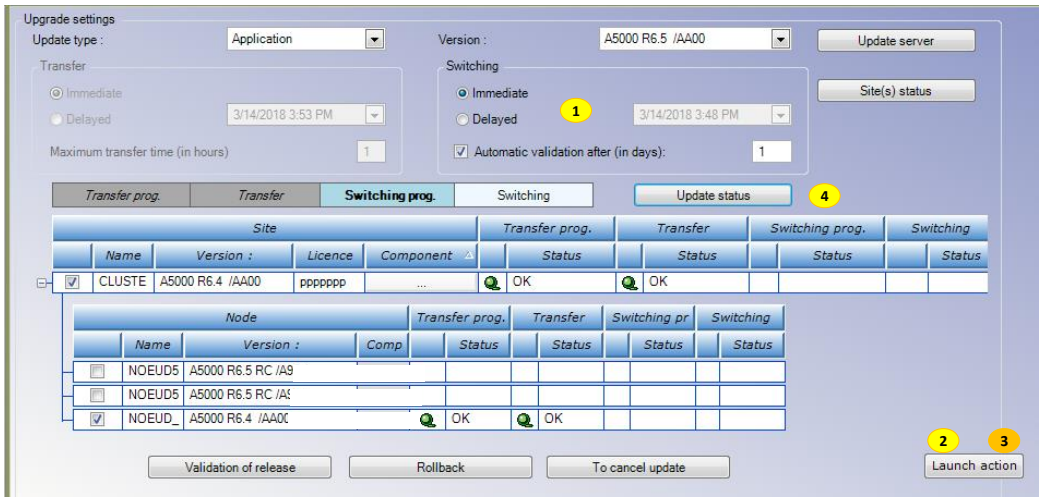
To restart the action on the faulty sites, click **Launch action**.

Final status of the first step



To move to step 2, all actions must be completed and have the status OK.

Step 2



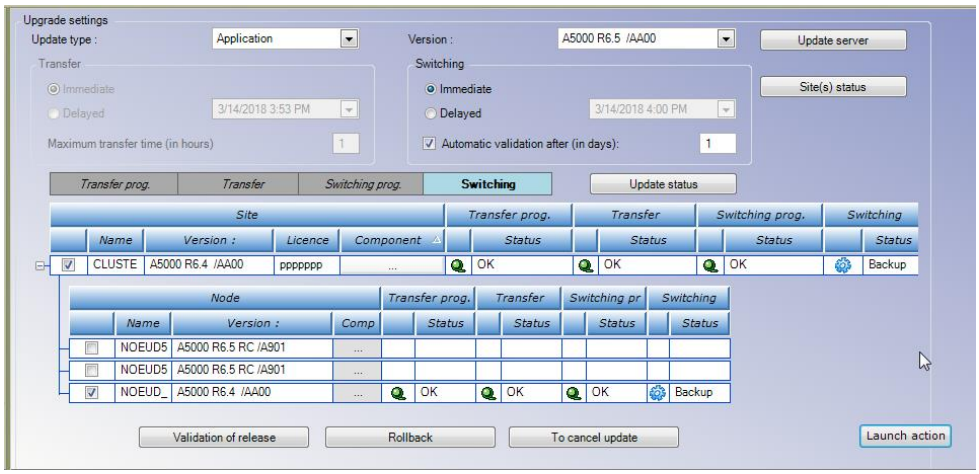
The second step concerns switchover:

1. In the **Transfer** section, indicate whether the switchover to the active status of the application version on the site(s) in question is **Immediate** or **Delayed.**

- Enter the licenses of the sites concerned in the **License** field if the icon is displayed (optional but strongly recommended).
- If applicable, tick **Automatic validation after (in days)**.

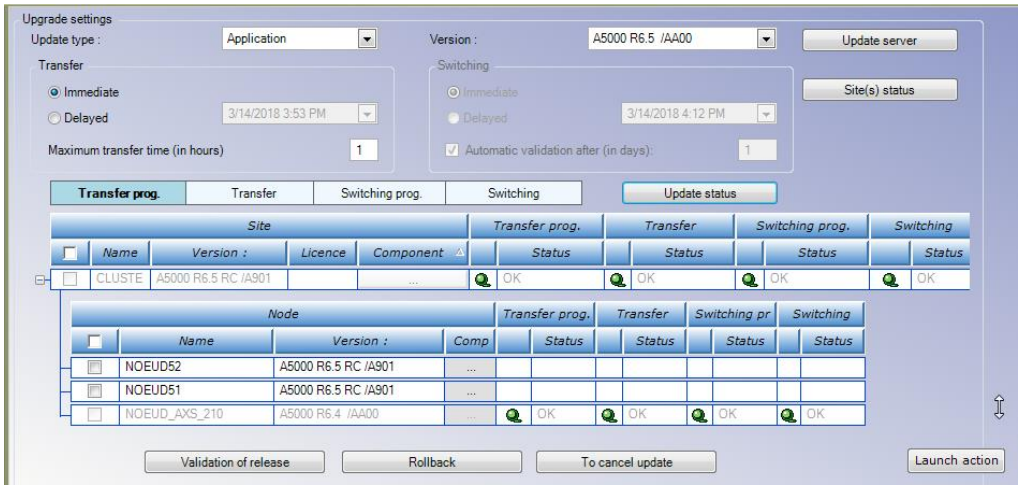
2. Start the transfer (immediate or delayed) by clicking **Launch action**.
3. The display shows the progress of the transfer to the iPBX.

Intermediate status



4. The **Update status** button is used to refresh the status in order to know the progress and restart the transfer procedure.

Final status



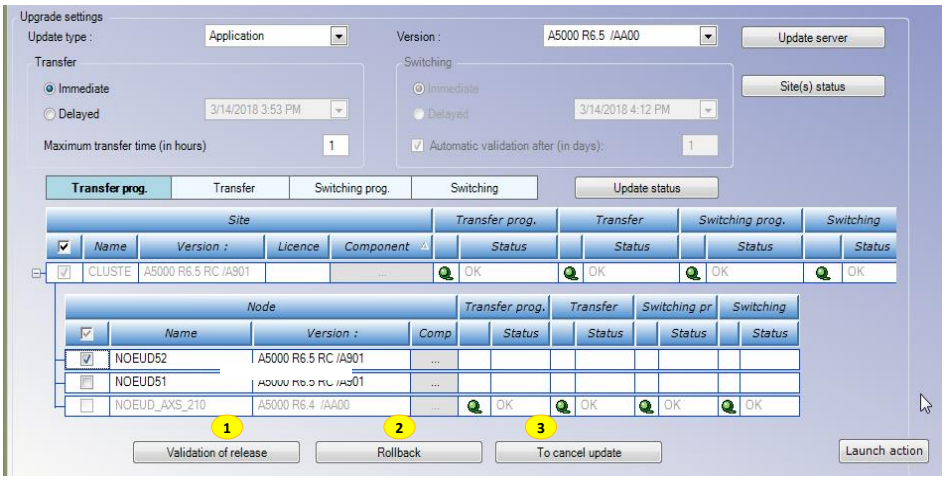
- An automatic restart of the system(s) in question allows the new application version to be taken into account and it switches to **TEST** mode on each system.
- The status of the sites can be viewed by clicking the **Status of the site(s)** button.

- After this restart, validate the active software from the Web Admin welcome banner for each iPBX or using the **Validation of release** button described below.

Note: Validation may be automatic if programmed during the upgrade operation.

Note: The version of CentOS remains identical after the application version is installed on an MiVoice 5000 server.

Other commands



The following buttons, after transfer, respectively allow:

1 The **Validation of release** button allows immediate validation on all iPBXs (cluster or non-cluster configuration) without any intervention on each iPBX or Cluster, unlike **Launch action** which implies taking the release into account from Web Admin for each iPBX.

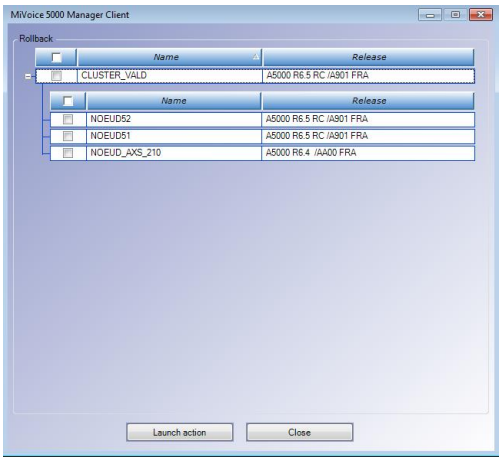
2 **Rollback** button

This button is used to restore the last software release validated but only if the release is in test mode.

For a cluster, rollback is carried out on the cluster server and nodes. If no release is in test mode, this is indicated by the report of the action in the operations log.

For a site list, rollback can be selectively launched by ticking the boxes of the IPBXs concerned:

- Click **Rollback**.
- Select the site(s) concerned.
- Click **Launch action**.



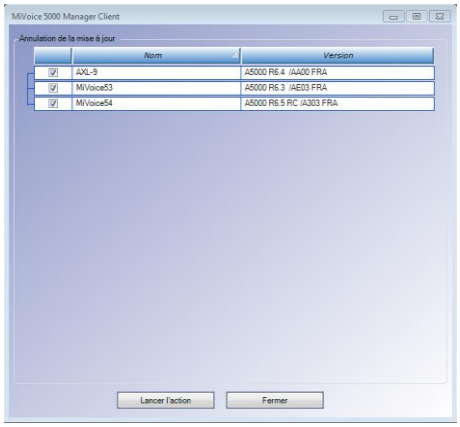
IMPORTANT: after the **Rollback** action, the site must be imported.

3

To cancel Update button:

This button is used to cancel a programmed deferred update. The update is cancelled, no matter the type of update (old method or by repository). If no update has been programmed on the system, this is indicated by the report of the action in the operations log. This action can be performed on several sites by selecting them from the proposed list.

- Click the **To cancel Update** button:
- Select the site(s) concerned.
- Click **Launch action**.

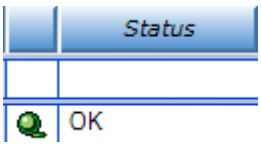


Additional actions on ergonomics

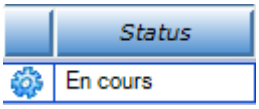
Depending on the progress, the colour of the **Transfer prog./ Transfer/Prog. Switching/Switching** fields change.

The **Update status** button is used to refresh the table indicating the sites and their status:

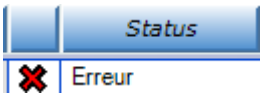
- Action successfully completed



- Actions in progress:



- The action has failed.



In case of failure, solve the problem (Network connection, licenses, etc.) and restart the action.

5.3.3.4 *Upgrading operating system (security) patches*

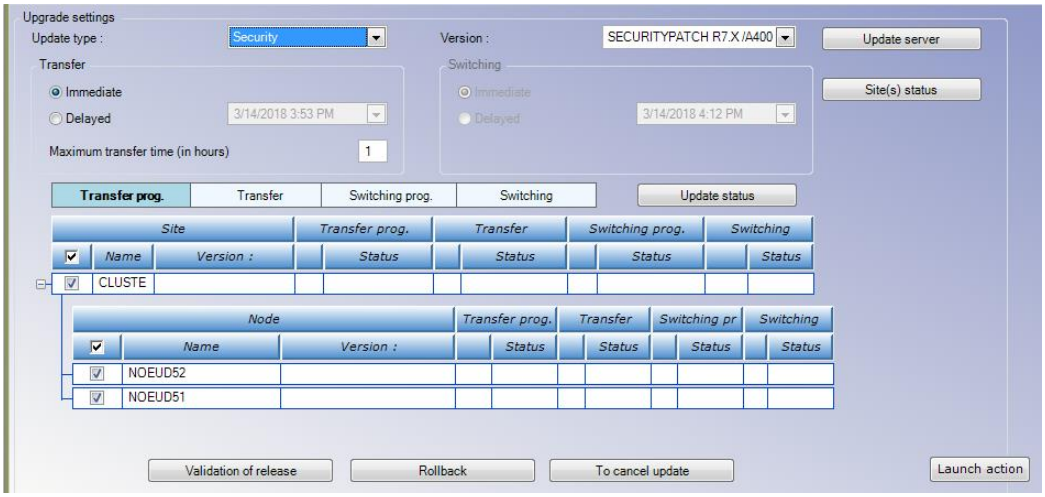
As of R6.5, the version of the security patches can be viewed in the main screen of MiVoice Manager:

Note: On the iPBX AMP, the patch version can also be viewed in Menu Telephony Service>System>Info> Software Id.

From MiVoice 5000 Manager, Menu **Immediate actions>Upgrade,**

- Select the cluster server or the site on which the CentOS security patch must be upgraded on the multi-site network.

Note: Refer to Section 5.3.3.1 for the presentation of this main screen.



Step 1

The first step concerns the procedure for transferring the security patch from the upgrade server (Repository).

- In the **Update type** field, select **Security** (this corresponds to downloading the security patch component of CentOS or MiVoice 5000 gateway operating system).
- In the **Version** field, select the version of the security patch component of the operating system to be downloaded on the site(s) concerned.

Note: All the security patches installed on the upgrade server are displayed. Only the most recent one can be selected.

- In the **Transfer** section, indicate whether the download is immediate or delayed. Also indicate the maximum transfer time.
- Tick the box or boxes of sites to be upgraded.

NOTE: The sites to be updated must have an active and validated software release. If the version is a TEST version and therefore not validated, the action will not be taken into account (Failure).

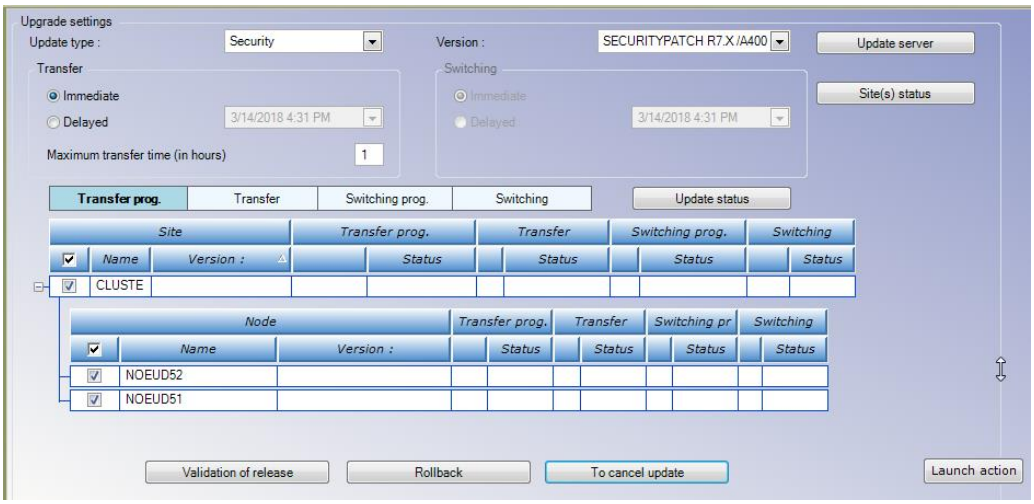
Note: Only MiVoice 5000 Server or Compact sites/nodes are available in the list (CentOS).

Note: If the duration of downloading exceeds the number of hours defined, the downloading process is abandoned.

Note: In deferred mode, the programming of switchover takes account of the maximum duration of transfer.

- Click **Start action**.

Final status (Example)



Step 2

The second step concerns switchover:

1. In the **Transfer** section, indicate whether the transfer to the site(s) in question is **Immediate** or **Delayed.**
2. Start the transfer (immediate or delayed) by clicking **Launch action**.
3. The display shows the progress of the transfer to the iPBX. If the status is NOK, restart the action with the same **Launch action** button.

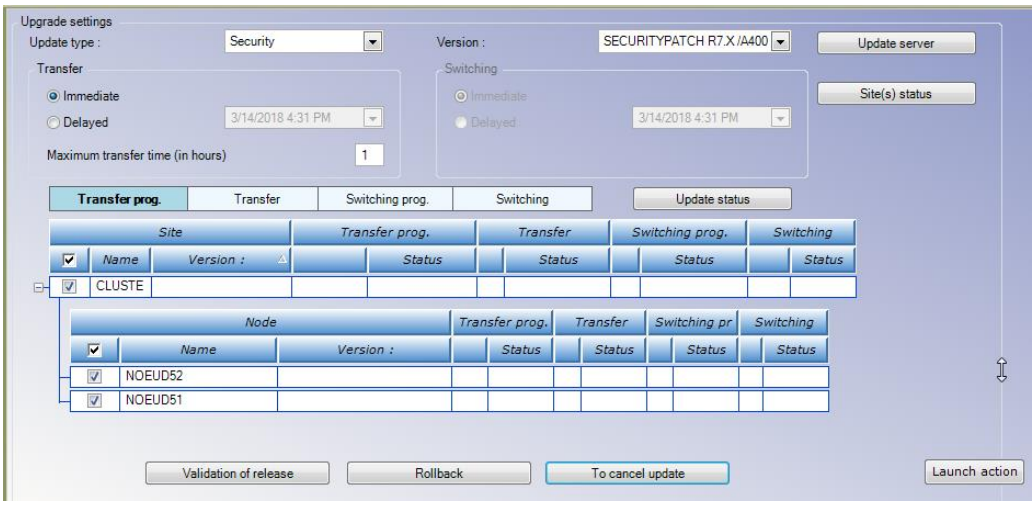
To cancel Update button:

This button is used to cancel a programmed deferred update. The update is cancelled, no matter the type of update. If no update has been programmed on the system, this is indicated by the report of the action in the operations log. This action can be performed on several sites by selecting them from the proposed list.

- Click the **To cancel Update** button:
- Select the site(s) concerned.
- Click **Launch action**.
- The **Update status** button is used to refresh the status in order to know the progress and restart the transfer procedure.

Final status

Example



- The Rollback and Validation of release buttons do not concern the security patch update and therefore have no action in this context.

Note: In the final status and after checking that the patches have been correctly updated, it is advisable to click "Cancel update".

A system with redundant Cluster

- Update patches on the **Master** Cluster machine.
- Wait for the end of the **Master** machine update as indicated above.
- On this same screen, click **To cancel Update**.
- Switch over to the **Slave** Cluster machine.
- Update the patches on the **Slave** Cluster machine following the same procedure as for the **Master** Cluster machine.

6 MANAGEMENT OF TERMINAL SOFTWARE BY TMA ON MIVOICE 5000 MANAGER

For this procedure, also refer to the document AMT/PTD/TR/0014 - TERMINAL INSTALLATION MANUAL - FULL VERSION.

6.1 PREREQUISITES

The packages must have been made available on the upgrade server.

6.2 MODEL MANAGEMENT

Model management is available in Menu **Telephony>Terminal management**.

This list of managed models is taken into account in the software update and provisioning actions (TMA EP):

- sending only files related to managed models to FTP servers.
- For software update, only the update is sent to the PBX for the managed models.

Models must be managed on a site-by-site basis.

- Select the site concerned.
- Tick the terminal models to be managed for this site.

Note: By default, all these boxes are ticked.

When the administrator disables the management of a component (6xxxi, 53xxip or 53xx), TMA deletes the corresponding software in the TMA folder. This deletion concerns all locally stored terminal packages and embedded FTP servers (production and deployment) managed by TMA.

- Click **Validate**.

A message then indicates that the modification of the list of models managed by this site has been updated.

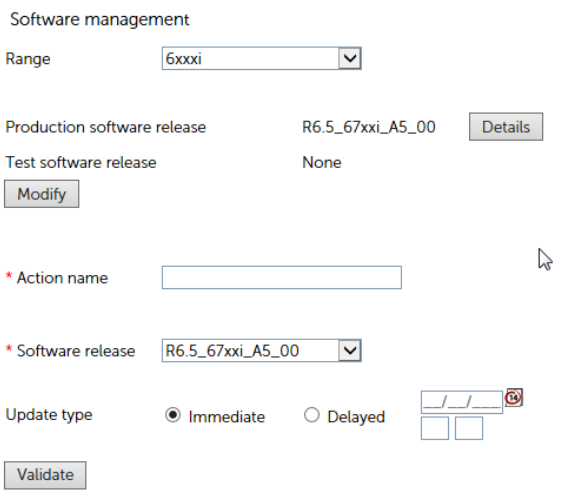
- Click **Return**.

Follow the same procedure for the other sites.

6.3 UPDATING THE TERMINAL SOFTWARE RELEASE

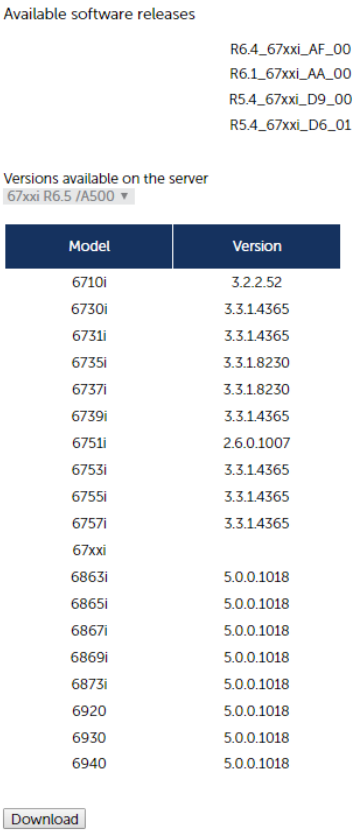
Menu **Telephony>Terminal Management>Software Management**

- Select the range and possibly the model.



- Click **Change**.

- Click **Add versions**.
- Select the version in question from the options **Versions available on the server**.



- Check the boxes for the terminal model to be updated.

- Click **Download.**

Downloading starts.

Then close the window; the download result is displayed:

Software management

Region IDF
Multisite VALD
Range 6xxxi
Model all models
Production software release
Test software release

Add software releases
Add versions (packages lower than R6.5)
Delete a software release
Configure the production software release
Configure the test software release

Filter details:
3 terminals with :

- 0 / 3 in production software release
- 0 / 3 in test software release
- 3 / 3 in an other software release

Phone number	Logged	Label	Periodical logout	Site	Model	Software release	IP address	MAC Address	Line	Global data	Specific data	Site number	Node
50300	✔			CLUSTER_VALD	6865i	5.0.0.1018	10.148.70.237	00-08-5D-42-AF-0F	1			5	
50301	✔			CLUSTER_VALD	6867i	5.0.0.1018	10.148.70.236	00-08-5D-43-31-20	1			5	
50302	✔			CLUSTER_VALD	6731i	3.3.1.4365	10.148.70.235	00-08-5D-11-A0-84	1	05		5	

1 / 1

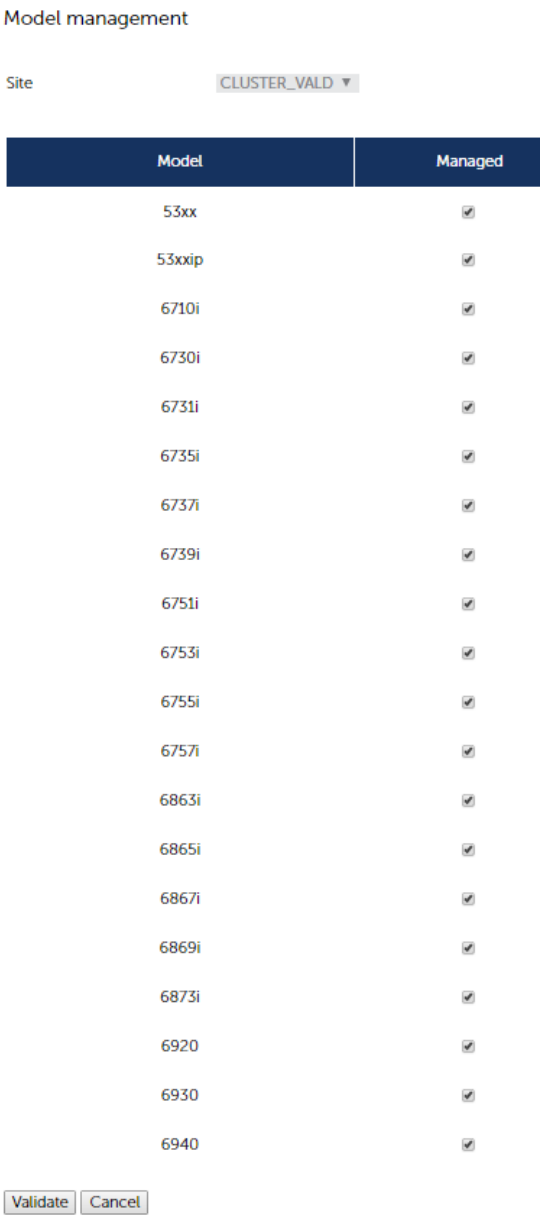
Back

For the rest of the procedure, configuration of the software version (production and test), refer to the document AMT/PTD/TR/0014 - TERMINAL INSTALLATION MANUAL - FULL VERSION or as of R7.0, to the document AMT/PTD/TR/0043 -. Installing and Managing Terminals Mitel 6700, 6800 SIP Phones and MiVoice 6900 IP Phones.

6.4 DELETING A TERMINAL SOFTWARE RELEASE FROM THE IPBXS

Menu **Telephony>Terminal management>Model management**

- Select the site concerned.
- Untick the boxes corresponding to the deletion.



- Click **Validate**.

NOTE: **The terminal software is immediately removed after validation.**

7 MANAGEMENT OF TERMINAL SOFTWARE BY THE TMA EMBEDDED ON IPBX

If the embedded TMA is activated on a Cluster Server, nodes, Mitel 5000 Gateways, MiVoice 5000 Server or MiVoice 5000 compact, different methods can be used to install a new TMA package containing all the terminal software.

7.1 STANDARD UPGRADE OF A SYSTEM AND ITS ASSOCIATED TMA PACKAGE

During a standard upgrade of the software release of a Cluster, MiVoice 5000 Server, Mitel 5000 gateways or MiVoice 5000 compact system, all the terminal software included in the iPBX upgrade package are installed on the iPBX in a new TMA package.

Note: The old TMA packages available in the iPBX are kept.

7.2 INSTALLING A NEW TMA PACKAGE MANUALLY

When a new TMA package is manually installed via the Web Admin terminal service, the terminal software are installed as follows:

- The software with the status ***installed*** or ***to be installed*** on the iPBX's list of terminal software components (Menu **Terminal service > Model management**) are installed on the iPBX, in a new TMA package.
- All the terminal software with the status ***not installed*** are not installed on the iPBX in the new TMA package.
- The old TMA packages available in the iPBX are kept.

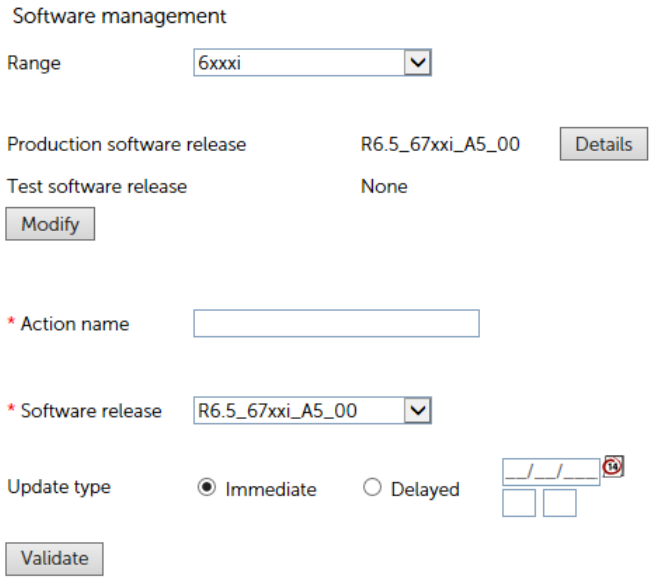
7.3 UPGRADING TERMINAL SOFTWARE DURING AN APPLICATION VERSION UPDATE VIA THE REPOSITORY SERVER

A new TMA package n is created when the application version of the Cluster Server, Nodes, Mitel 5000 Gateways, MiVoice 5000 Server and MiVoice 5000 compact systems are updated by directory.

- The new TMA package **n** is created as follows:
  - The terminal software available in the new application version, with the status ***installed*** or ***to be installed*** and a version above those available in the iPBX, are copied to the new TMA package **n**.
  - The terminal software available in the previous TMA package n-1, with the same release as those available in the new application version, are copied to the new TMA package n.
  - The previous TMA package **n-1** is then deleted.

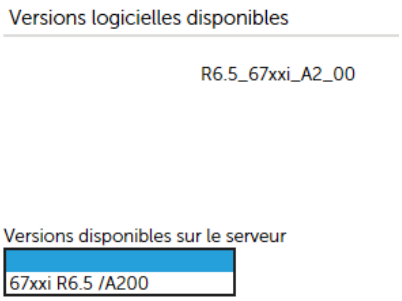
When new terminal software is updated in the iPBX without updating the iPBX application version, this new terminal software package is copied to the current TMA package.

When terminal software is deleted from the list of terminal software components available in the iPBX (Menu **Terminal service** > **Software management**), this terminal software is deleted from the current TMA package.

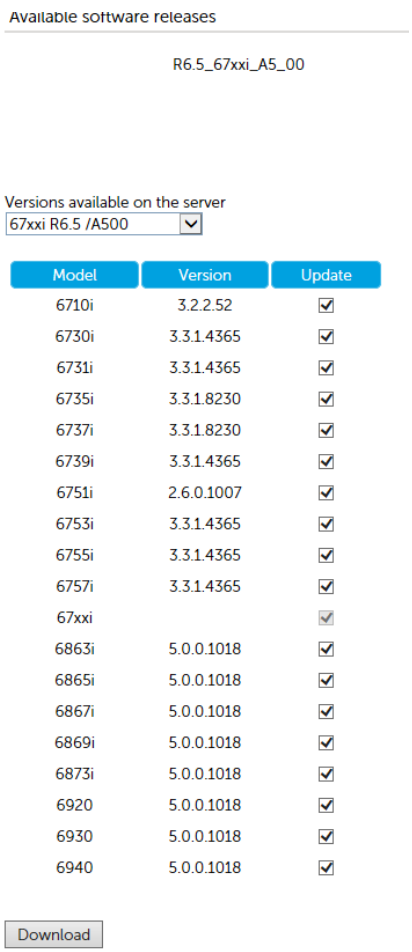


- Click **Change**.

- Click **Add versions**.



- Select the version in question from the options **Versions available on the server**.



- Click **Download.**

Downloading starts.

7.4 DELETING A TERMINAL SOFTWARE RELEASE FROM THE IPBXS FROM WEB ADMIN

From Web Admin, Menu **Terminal service > Model management**

This action is used to:

- Locally uninstall from the system all unused terminal software in order to gain some disk space on the system
- Keep in the system deployment area only the terminal software required to deploy the Mitel 6000 SIP Phones available at the end-customer's,
- Keep the Mitel OMM software of the DECT base stations in the system's TFTP area.

NOTE: In this architecture, the terminal software releases are updated from the terminal software packages installed via the TMA integrated into MiVoice 5000 Manager.

- Untick the terminal software releases to be deleted then click **Validation**.

NOTE: The terminal software is immediately removed after validation.

8 MANAGING THE MITEL OMM-SIP SOFTWARE

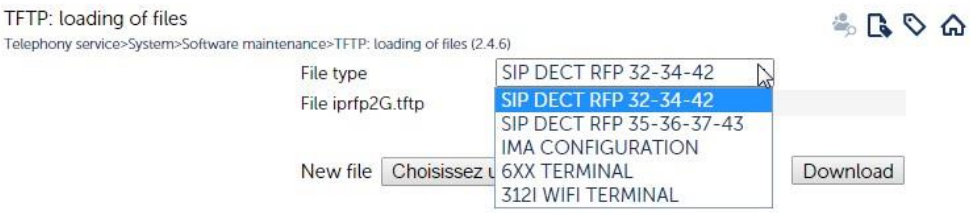
The management of the OMM-SIP software depends on whether or not it is taken into account on the list of terminal components available in the iPBX (Menu **Telephony service** > **Subscribers** > **Terminals and applications > Software**).

8.1 THE MITEL OMM-SIP SOFTWARE MANAGED ON THE LIST OF SOFTWARE COMPONENTS

Note: As of R6.3, in OMM R6.1 the software is included in the software associated with the new terminals.

The Mitel OMM-SIP software is managed as follows:

- During a first installation in release ≥ R6.5, the OMM-SIP software (5.x) is installed by default on the iPBX and managed on the list of terminal software components available in the iPBX (box ticked).
- Once the Mitel OMM-SIP software is managed on the list of components (box ticked):
  - The ***Version*** field may display the current Mitel OMM-SIP software release or the information **TO BE INSTALLED** (new Mitel OMM-SIP release to be installed).
  - The Mitel OMM-IP software is no longer managed manually in Menu Telephony service > System > Software maintenance > TFTP > Loading of files. The DECT-IP input is not proposed in the options.



Note: The only exception to this rule: after a first installation in R6.3, the Mitel OMM-IP software may be managed manually via this menu.

- The Mitel OMM-SIP software may also be managed manually in Menu Telephony service > System > Software maintenance > TFTP > Loading of files. All the Mitel OMM-SIP components (DECT SIP RFP software, IMA configuration, terminal A6xx software) may be manually installed on the iPBX via this MMI. After any of these components is manually installed, the TFTP label appears in the Version field.

- The Mitel OMM-SIP software can be updated through standard update or update by repository, even if this software had been previously installed manually (TFTP label appears in the Version field and Status field is ticked).
- After the iPBX application version is updated through standard update or update by repository, the Version label displays the installed new Mitel OMM-SIP software release again.

- After the Mitel OMM-SIP software is deleted from the list of terminal software components available in the iPBX, (box unticked then validation), the DECT SIP RFP software and terminal A6xx software are deleted from the iPBX.

Note: The Mitel OMM-SIP software can still be managed manually in Menu Telephony service > System > Software maintenance > TFTP > Loading of files.

8.2 MITEL OMM-SIP SOFTWARE NOT MANAGED ON THE LIST OF SOFTWARE COMPONENTS

Once the Mitel OMM-SIP software is no longer managed on the list of components (box unticked), the Mitel OMM-SIP software management procedure is as follows:

- The Mitel OMM-SIP software must be managed manually via Menu Telephony service > System > Software maintenance > TFTP > Loading of files. All the Mitel OMM-SIP components (DECT SIP RFP software, IMA configuration, terminal A6xx software) may be manually installed on the iPBX via this MMI.
- Mitel OMM-SIP software not available on the TFTP server
  - The Mitel OMM-SIP software is not updated after the iPBX application version is updated via update by repository.
  - The Mitel OMM-SIP software is updated after the iPBX application version is updated via standard update.
- Mitel OMM-SIP software available on the TFTP server
  - The Mitel OMM-SIP software is not updated after the iPBX application version is updated via standard update or update by repository.

9 REDUNDANT SYSTEMS

9.1 UPGRADING THE APPLICATION

With or without MiVoice 5000 Manager, the (APPLICATION) software release must be upgraded on the master machine. Refer to Section 4 or 5 as appropriate.

For a redundant system without MiVoice 5000 Manager, also refer to document AMT/PTD/PBX/0083.

9.2 UPGRADING OS PATCHES

Without MiVoice 5000 Manager

When a MiVoice 5000 server is redundant, the operating system (SECURITY) patches must be updated twice (on each server).

To identify operating system patch versions on the secondary server, the administrator must switch to that secondary server to access this information.

See also document AMT/PTD/PBX/0083.

With MiVoice 5000 Manager

The software release (APPLICATION) must be upgraded on the master machine. See Section 5.

A redundant system

- Update patches on the **Master** machine.
- Wait for the end of the **Master** machine update as indicated in Section 5.3.3.4 Upgrading operating system (security) patches.
- In the final screen for tracking the upgrade, click **Cancel Update**.
- Switch over to the **Slave** Cluster machine.
- Update the patches on the **Slave** Cluster machine following the same procedure as for the **Master** machine.