

Remote Worker via MBG

04/2023

AMT/PTD/PBX/0161/3/3/EN
IMPLEMENTATION MANUAL



Warning

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

The information may be changed without notice and should never be interpreted as a commitment on the part of Mitel, its affiliates or subsidiaries.

Mitel, its affiliates and subsidiaries shall not be held liable for any errors or omissions made in this document. This document may be reviewed or re-edited at any time in order to add new information.

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

© Copyright 2023, Mitel Networks Corporation. All rights reserved.

Mitel® is a registered trademark of Mitel Networks Corporation.

Any reference to third-party trademarks is made for information purpose, and Mitel does not guarantee the ownership thereof.

CONTENTS

1	INTRODUCTION	5
1.1	DEFINITION	5
1.2	REFERENCE DOCUMENTS	5
1.3	GLOSSARY	5
1.4	RESTRICTIONS	5
2	GENERAL ARCHITECTURE	6
3	DEPLOYMENT	7
4	SUMMARY OF THE DIFFERENT DEPLOYMENT STEPS FOR REMOTE WORKERS	8
5	GENERIC CONFIGURATION	10
5.1	CONFIGURING THE FIREWALL	10
5.2	GENERATING THE HASH KEY	11
5.3	CONFIGURING THE REMOTE PHONE FOR ACCESS TO THE IPBX ATTACHED TO MIVOICE 5000	12
5.3.1	USING AN RCS SERVER	12
5.3.2	CONFIGURING THE URL DIRECTLY ON THE PHONE	13
5.4	CONFIGURING THE MBG	14
5.4.1	LICENCES	15
5.4.2	CONFIGURING THE NETWORK PROFILE	15
5.4.3	RESTARTING THE MBG	16
5.4.4	CONFIGURATION AT THE MIVOICE 5000 IP ACCESS POINT	17
5.4.5	SIP SETTINGS COMMON TO ALL REMOTE WORKER PHONES	18
5.4.6	CONFIGURING THE CONNECTION/AUTHENTICATION BETWEEN THE MBG AND THE IPBX	19
5.5	CONFIGURING THE MBG IN WHITE LIST	28
5.6	CONFIGURING TMA (PHONE SERVICE)	29
5.7	DEFINING THE DOWNLOAD SERVER FOR REMOTE WORKERS	30
6	PREPARING THE DEPLOYMENT	32
6.1	DECLARING SIP DEVICES (6800 SIP AND 6900 IP PHONES)	32
6.1.1	STANDALONE MBG	32
6.1.2	INTEGRATED MBG OR MBG IN CLUSTER MODE WITH MICOLLAB	33
6.2	SPECIFIC CONFIGURATION OF A MICOLLAB SOFTPHONE CLIENT	34
6.3	PREPARING THE REMOTE WORKER CSV FILE FROM THE GENERIC PROVISIONING FILE	36
6.4	REMOTE WORKER MANAGEMENT BY TMA	39
6.4.1	PREREQUISITES	39
6.4.2	DEPLOYING FROM THE DOWNLOAD SERVER	39
6.5	DISPLAY/INVENTORY OF REMOTE WORKER PHONES	40
7	DEPLOYING REMOTE WORKER PHONES	41
7.1	CONFIGURING THE ATTACHED IPBX FOR EACH REMOTE WORKER PHONE	41
7.1.1	WITH RCS	41
7.1.2	WITHOUT RCS SERVER	42
8	CONFIGURING THE EMERGENCY NUMBER FOR FIXED REMOTE WORKERS	43
8.1	PRINCIPLE	43
8.2	CONFIGURATION	44
9	OTT MODE CONFIGURATION FOR CLIENT AND USER PORTAL WEB APPLICATIONS ACCESS	46
9.1	PRINCIPLE	46
9.2	SUMMARY OF THE DIFFERENT STEPS	48
9.2.1	MBG CONFIGURATION	48
9.2.2	PROXY TRUSTED CONFIGURATION	49
10	OTT MODE CONFIGURATION FOR SIP DECT SYSTEM	50
10.1	INTRODUCTION	50
10.2	ARCHITECTURE	50
10.3	MIVOICE 5000 CONFIGURATION	51

- 10.4 CONFIGURATION MBG51
- 10.5 CONFIGURATION WITH OM CONFIGURATOR52
- 10.6 OMP CONFIGURATION (OPEN MOBILITY PORTAL)53
- 10.7 CONFIGURATION OF XML ACCESS FOR REMOTE WORKER DECT SIP IN OTT MODE59
 - 10.7.1 PRINCIPLE59
 - 10.7.2 CONFIGURATION59
- 10.8 OMM WEB.....62

1 INTRODUCTION

1.1 DEFINITION

Cluster: MITEL MiVoice 5000 telephony systems comprising physical devices (Mitel Mitel 5000 Gateways, Mitel 500, MiVoice 5000 Server or C2IC) or virtual devices (MiVoice 5000 Server) connected to a central MiVoice 5000 Server, called Cluster Server.

Cluster Server: physical or virtual MiVoice 5000 Server systems dedicated to global Cluster control. This system can be duplicated.

1.2 REFERENCE DOCUMENTS

Related documents are available at Mitel.com.

1.3 GLOSSARY

MBG : MiVoice Border Gateway

RCS : Redirection & Configuration Server

AMC : Applications Management Center (Licence server)

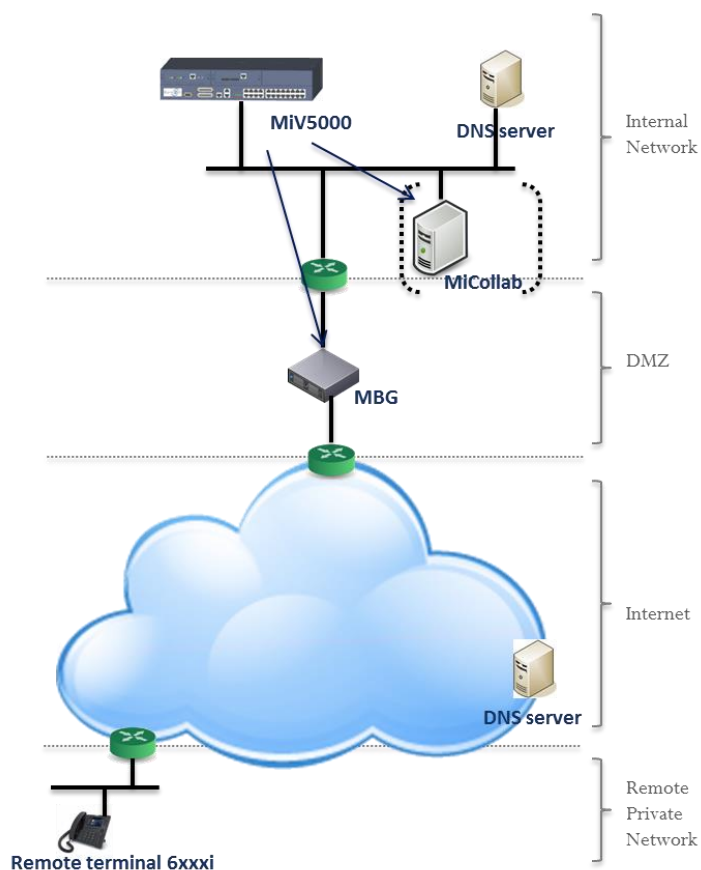
ICP : IP Communication Platform (iPBX)

1.4 RESTRICTIONS

The Remote Worker feature described in this document applies to MiVoice 6800 SIP and 6900 IP phones only.

2 GENERAL ARCHITECTURE

Sample architecture:



The aim is for a remote 6800 SIP or 6900 IP phone to have almost the same functions as a similar phone installed on the company's local area network.

The connection from the remote phone connected to the Internet is then routed via an MBG to the local area network (LAN).

Since the MBG allows the public address to be associated with the local address of the iPBX, the phone retrieving its configuration files behaves like a local phone on the site.

Depending on the architecture, the MBG may be:

- A stand-alone external device located in the DMZ
- Integrated (embedded) in the MiCollab server
- Clustered with MiCollab on the local area network

It is provisioned according to the architecture:

- Either manually (standalone (MBG))
- Or by the MiCollab server.

When MiV5000 is provisioning a MiCollab server located in the DMZ, the firewall must allow access to MiV5000.

MBG domain name resolution is handled by a public DNS server.

Security is provided by a key generated in the iPBX and is embedded in the path of the URL allowing the phones to download their settings.

In a multi-site configuration, the MBG can only connect to one MiVoice 5000 iPBX, all remote worker phones must be declared on this iPBX.

3 DEPLOYMENT

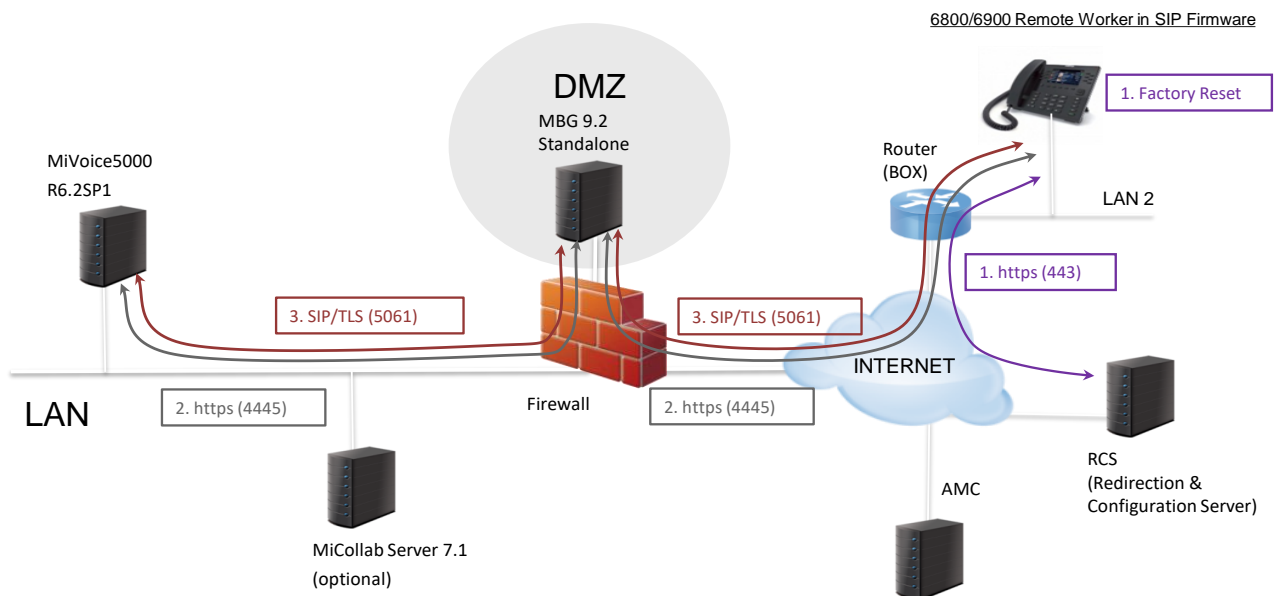
Preliminary operations:

The public URL to be reached is entered either manually by the remote worker or via an RCS server.

After a factory reset, the phone connects to the encrypted URL for deployment.

The phone downloads the configuration files from the iPBX via the MBG. File types: aastra.cfg, mac.cfg, software.

The phone restarts and sends its REGISTER.



4 SUMMARY OF THE DIFFERENT DEPLOYMENT STEPS FOR REMOTE WORKERS

The procedure can be broken down into three:

- Generic configuration, by the installer
- Preparing the deployment, by the installer and the network administrator for each phone
- Deploying the phones, by the remote workers or the network administrator.

The chronological order to be respected:

Generic configuration (Chapter 5)

Configuring the firewall

Generating a hash key on MiVoice 5000

Declaring an RCS server (used to configure remote terminals for access to the iPBX attached to MiVoice 5000)

MBG configuration

- Licence
- Configuring the network profile
- Configuration at the MiVoice 5000 IP access point
- SIP settings common to all Remote Worker phones

Additional MBG settings

Configuring the login/authentication with an MBG on MiVoice 5000

On the MBG Interface:

On the MiVoice 5000 web admin:

Configuring the MBG in white list

Configuring TMA on MiVoice 5000

- Configuring the application
- Defining and configuring the download server for remote worker phones

Preparing the deployment (Chapter 6)

Declaring SIP devices (6800 SIP and 6900 IP phones)

Standalone MBG

Integrated MBG or MBG in Cluster mode with MiCollab

Specific configuration of a MiCollab softphone client

Preparing the Remote Worker csv file from the Generic Provisioning file

Remote Worker management by TMA

- Prerequisite - Preparing the "csv" file from the provisioning file
- Deploying from the download server:
 - Prerequisites
 - Deployment by integrated TMA
 - Deployment by TMA managed from MiVoice 5000 manager

Display/inventory of remote worker phones

Deploying terminals (Chapter 7)

Configuring the remote phone for access to the MiVoice 5000 configuration server

- Using an RCS server
- without RCS server

Activating a remote phone

All these steps are described in order and in detail in the following paragraphs.

5 GENERIC CONFIGURATION

5.1 CONFIGURING THE FIREWALL

To allow traffic from the LAN/DMZ to the Internet, the following configuration must be made on the ports:

Port Range	Direction	Description
TCP 4445 (HTTPS)	Internet -> DMZ (MBG)	https connection between 68xxi and MBG (download configuration files, XML features)
TCP 4445 (HTTPS)	DMZ (MBG) -> LAN	https connection between MBG and MiV5000 (download configuration files, XML features)
TCP 5061 (SIP/TLS)	Internet -> DMZ (MBG)	SIP connection between 68xxi and MBG
TCP 5061 (SIP/TLS)	DMZ (MBG) -> LAN	SIP connection between MBG and MiV5000
UDP 20000 to 31000	Internet -> DMZ (MBG) DMZ (MBG) -> LAN	Range of SRTP ports configured in MBG settings

Configuring the remote access ports (Box)

The ports must be open on the remote router (Box).

In general, no configuration is required as outgoing flows are naturally allowed by the boxes.

Port Range	Direction	Description
TCP 4445 (HTTPS)	Lan (BOX) -> Internet	https connection between 68xxi and MBG (download configuration files, XML features)
TCP 5061 (SIP/TLS)	Lan (BOX) -> Internet	SIP connection between 68xxi and MBG
UDP 40000 to 51000	Lan (BOX) -> Internet	Range of SRTP ports configured in 68xxi settings

5.2 GENERATING THE HASH KEY

The hash key must be generated by MiVoice 5000. It is then integrated into the URL configuration path. This key is unique and is controlled by the PBX to allow the phone to download the files.

Menu **NETWORK AND LINKS>Quality of service> Encryption and IP parameters**

Web Admin home
Subscribers
System
Dialing plan
Network and links
Quality of service
Ciphers and IP settings
Reception
Voice mail and tones
Fast links

Ciphers and IP settings
Telephony service>Network and links>Quality of service>Ciphers and IP settings (4.3.5)

IP parameters and ciphering Certificates

bytes TOS voice (hexal) 88
bytes TOS signaling (hexal) A0
VLAN voice priority 6
VLAN signaling priority 6
time to live of the IP datagram 64

Signalling and voice ciphering
function state LOCKED
dates of active certificate validity :
start 02/02/16 13:58
end 01/02/17 13:58
name of the certification authority :
192.168.100.161
voice terminals ciphering ☐
self signed certificate ☒
Certificate regeneration

Voice ciphering (7xx)
function state LOCKED
updated on: ed:
encryption FORBIDDEN
Generation of keys (CMEK and CMSK)

Miscellaneous settings
ARP inputs number 256
time to live of the ARP input sec 600
ARP entries deletion NO
time-out network alarm start sec 120
time-out network alarm end sec 30
Hash generation NO

XL - R62 RC / C101 FRA
02/02/16 14:04:45
* BUFTIC MUFACI_SERVER CONNECTED
02/02/16 14:03:54

- In the **Generate hash** field, select **YES**.



IMPORTANT NOTE: A warning message "regenerating the hash will affect all deployed remote worker phones" is displayed if the operator requests for hash regeneration.

- Then enter the password of the current Webadmin account.
-

The **File download path**: field is set to read only.

The aim is for the administrator to be able to copy/paste it in the URL used to access the phone configuration files.

5.3 CONFIGURING THE REMOTE PHONE FOR ACCESS TO THE IPBX ATTACHED TO MIVOICE 5000

Since the phone is remote, it is not possible to automatically provide the URL of the MBG to be reached.

Two methods are possible:

- Using an RCS server
- Configuring the URL directly on the phone from the phone's web interface.

6900 phones, factory delivered with Minet firmware, must be upgraded to SIP firmware. The SIP firmware can be downloaded either beforehand by the installer, or directly via the RCS server (for all the phones in the installation, or individually by Mac file).

5.3.1 USING AN RCS SERVER

The RCS server can be easily used to deploy 6800 SIP and 6900 IP phones but requires an access account.

5.3.1.1 *Opening an RCS access account*



Note: refer to the document on opening an RCS account.



RCS server login screen.



5.3.1.2 Configuring access to the MiVoice 5000 configuration server with RCS server

The redirection and configuration service (RCS) is a service that facilitates the deployment of 6800 SIP and 6900 IP phones (refer to the RCS documentation for details).

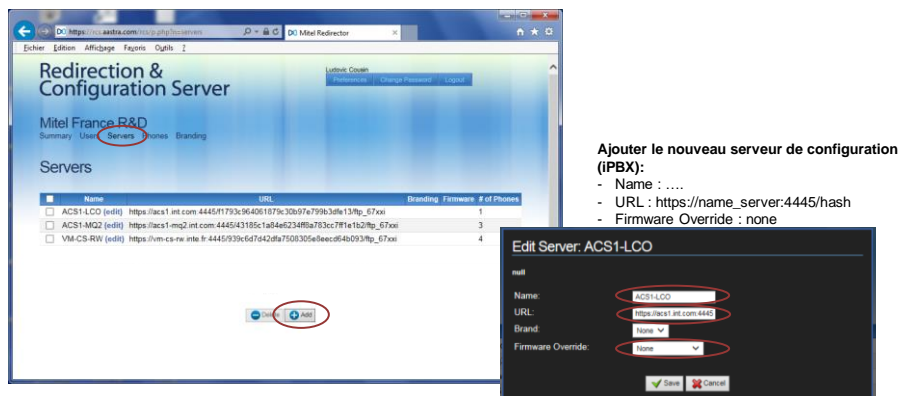
RCS server access URL: <https://rcs.aastra.com/rcs/login.php>

From the RCS welcome screen

- In the **Servers** menu, enter the information to reach the MBG:
 - **Name:** MBG name or public address
 - **URL (HTTPS path):** Access path, including:
 - The host, represented either by the FQDN or by the MBG's public IP address and associated port (4445)
 - The URL hash key enabling the phones to download their configuration file. See the value in Section 5.2.

Example: `https://name_server:4445/hash`

- Click **Save**.



The screenshot shows the 'Redirection & Configuration Server' interface. The 'Servers' tab is selected, displaying a table of servers. A red circle highlights the 'Add' button at the bottom. To the right, a text box lists the steps to add a new server: 'Ajouter le nouveau serveur de configuration (iPBX):' followed by 'Name :', 'URL : https://name_server:4445/hash', and 'Firmware Override : none'. Below this, the 'Edit Server: ACS1-LCO' dialog box is shown with fields for Name, URL, Brand, and Firmware Override, each with a red circle around it.

Firmware override:

- If the installation has a lot of 6900 phones, it is interesting to automatically upgrade the 6900 phones from the Minet version to SIP. This update will also apply both to 6800 and 6900 phones.
- Take SIP firmware 5.0.0 minimum.

There will be as many different URLs as there are MiVoice 5000 Servers on which remote workers are declared.



IMPORTANT NOTE: An MBG can only be associated with one MiVoice 5000 iPBX for the Remote Worker function.

5.3.2 CONFIGURING THE URL DIRECTLY ON THE PHONE

See Section 7.1.2.

5.4 CONFIGURING THE MBG

Accessing the MBG interface

https://mbg_address/server-manager

Configuration on the MBG comprises several phases:

- Declaring the MBG licences
- Configuring the network profile
 - Menu **MiVoice Border Gateway, System configuration>Network profiles** tab
- Restarting the MBG
 - Menu **MiVoice Border Gateway, System Status** tab
- Configuring the MiVoice 5000 IP access point
 - Menu **MiVoice Border Gateway, Service Configuration>ICPs** tab
- SIP settings common to all MBG Remote Worker phones
 - Menu **MiVoice Border Gateway, System configuration>Settings** tab
- Additional settings specific to Remote Worker
 - Menu **Configurations Overrides** tab.
- Configuring the connection/authentication between the MBG and the iPBX

Most configurations are the same regardless of whether the MBG is stand-alone, embedded in MiCollab or clustered.

Others are not and in these cases, the architecture will be clarified at the beginning of the paragraph.

This chapter describes the configuration on the MBG only for the Remote Worker function. Refer to the MBG documentation for further details on its use and administration.

5.4.1 LICENCES

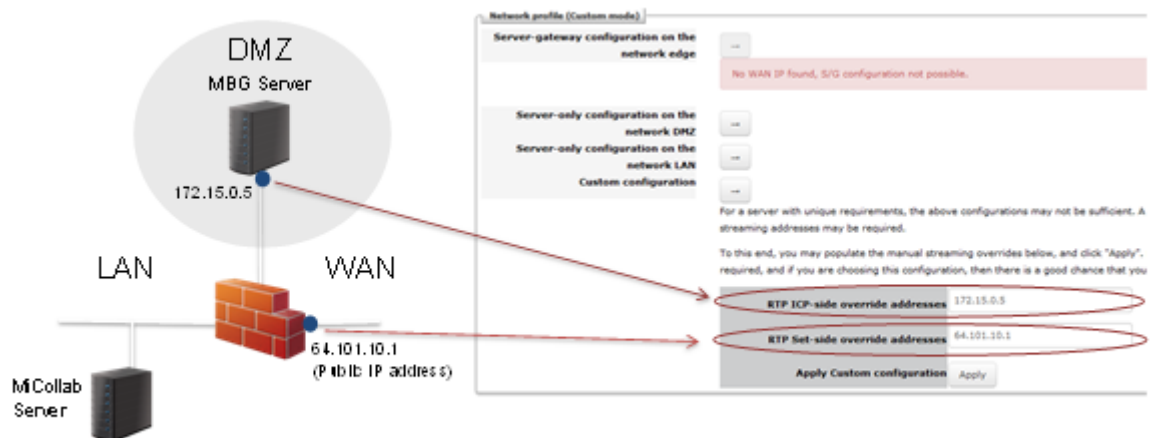
Teleworkers licences are required for the MBG.

Menu **MiVoice Border Gateway, System>Dashboard** tab.

License information				
Availability and usage	License type	Total local	Total local in use	
	Teleworker licenses	50	3	
	Tap licenses:	0	0	
	SIP Trunk licenses:	10	0	
	Transcoding licenses:	0	0	
Virtualization support	True			Expiry July 26, 2016
IPv6 support	Licensed	Enabled		
	False	False		

5.4.2 CONFIGURING THE NETWORK PROFILE

Menu **MiVoice Border Gateway, Network>Profiles** tab



- Enter the **RTP ICP-side override addresses**:
TBC: MBG server address
- Enter the **RTP Set-side override addresses**:
TBC: Public address
- Click **Apply** to apply the settings.

ICP => **IP Communication Platform** = MiVoice5000

Then restart the MBG service. See the following sections.

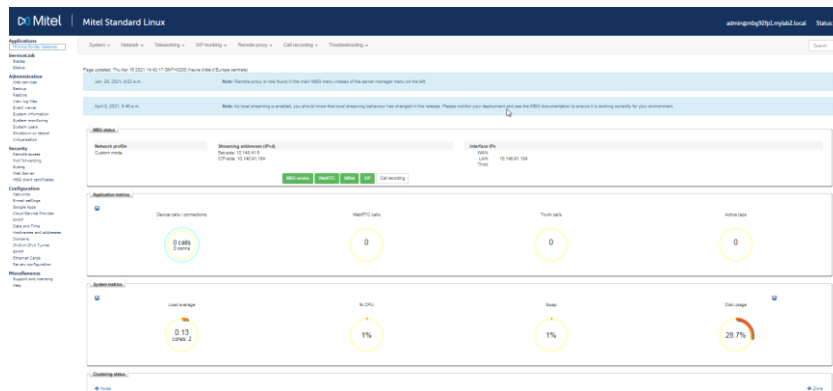
5.4.3 RESTARTING THE MBG

✓ Common to standalone MBGs , MBGs embedded in MiCollab or clustered MBGs

From Menu **MiVoice Border Gateway, System>Dashboard** tab:

In the **MBG Status** area:

- Click **MBG service**.
- Click **Stop**.
- Click **Start** to restart it.



5.4.4 CONFIGURATION AT THE MIVOICE 5000 IP ACCESS POINT

✓ Common to standalone MBGs, MBGs embedded in MiCollab or clustered MBGs

Menu **MiVoice Border Gateway, Network>ICPs** tab

From the list, select the iPBX in question.

- Click the Pencil icon (modify).

System ▾ Network ▾ Teleworking ▾ SIP trunking ▾ Remote proxy ▾ Call recording ▾ Troubleshooting ▾

Page updated: Tue Apr 27 2021 14:43:44 GMT+0200 (heure d'été d'Europe centrale)

Aug. 22, 2019, 10:59 a.m. Note: Remote proxy is now found in the main MBG menu instead of the server manager menu on the left. > Dismiss

To test connectivity to your configured ICPs, or to run a DNS resolution test on configured hostnames, see the [Diagnostics](#) page.

ICP Information

Default for MINet	Default for SIP	Name	Hostname or IP address	Type	Installer password	SIP capabilities	Indirect call recording capable	Associated connectors	Associated sets (MINet/SIP)	Associated trunk rules (pri/sec)			
<input checked="" type="radio"/>	<input checked="" type="radio"/>	acs	10.148.91.181	MiVoice 5000		UDP TCP TLS	✗	✗	0 / 14	0 / 0			
<input type="radio"/>	<input type="radio"/>	acs 7.0	10.148.91.181	MiVoice 5000		UDP TCP TLS	✗	✓	0 / 3	0 / 0			
<input type="radio"/>	<input type="radio"/>	acs 7.1	10.148.91.181	MiVoice 5000		UDP TCP TLS	✗	✗	0 / 0	0 / 0			
<input type="radio"/>	<input type="radio"/>	acs but	10.148.91.181	MiVoice 5000		UDP	✗	✗	0 / 0	0 / 0			
<input type="radio"/>	<input type="radio"/>	acs cipac	10.148.91.181	MiVoice 5000		UDP TCP	✗	✗	0 / 0	0 / 0			
<input type="radio"/>	<input type="radio"/>	acs r6.5	10.148.91.74	MiVoice 5000		UDP TCP	✗	✗	0 / 0	0 / 0			

Fill in the following fields:

Manage ICP area

Name: iPBX name

Manage ICP

Name	<input type="text" value="acs 7.2"/>	Hostname or IP address	<input type="text" value="10.148.91.181"/>
Type	<input type="text" value="MiVoice 5000"/>	MINet installer password	<input type="text"/>
SIP capabilities	<input type="text" value="UDP, TCP"/>	Indirect call recording capable	<input type="checkbox"/>

MiVoice 5000 support

Link to this ICP?	<input type="checkbox"/>	Enable	<input type="checkbox"/>
XML listen port	<input type="text" value="4445"/>	TLS?	<input checked="" type="checkbox"/>
XML destination port	<input type="text" value="4443"/>	TLS?	<input checked="" type="checkbox"/>

Manage ICP area

Hostname or IP address: MiVoice 5000 IP address

Type: MiVoice 5000

SIP capabilities: UDP, TCP, TLS > SIP connection between MBG and MiVoice 5000 in TLS (5061)

MiVoice 5000 support area

XML listen port: Public port on which the MBG is listening (default value: 4445).

XML destination port: MiV5000 port (4445 not configurable in MiVoice 5000).

5.4.5 SIP SETTINGS COMMON TO ALL REMOTE WORKER PHONES



Common to standalone MBGs , MBGs embedded in MiCollab or clustered MBGs

Menu **MiVoice Border Gateway, System>Settings** tab

Configure the following fields for RTP security options:

SIP Support:

- UDP: Disable
- TCP: Public
- TCP/TLS: Public
- Set-side RTP security inbound: SRTP only
- Set-side RTP security outbound: SRTP only
- ICP-side RTP security Inbound: SRTP or RTP
- ICP-side RTP security Outbound: AVP+crypto

The recommended encryption key is:

- AES_CM_128_HMAC_SHA1_80 (default is _32)

There is also an option for the TLS certificate, which must be from Mitel.

The screenshot shows the 'SIP options' configuration page. It is divided into several sections:

- SIP support:** Includes a 'Certificate' dropdown set to 'Mitel' and a 'Protocol' section where 'UDP' is disabled and 'TCP' and 'TCP/TLS' are set to 'Public'.
- Set-side RTP security:**
 - Inbound:** 'SRTP or RTP' is selected.
 - Outbound:** 'SRTP only' is selected.
 - Preferred cipher:** 'AES_CM_128_HMAC_SHA1_32' is selected.
- ICP-side RTP security:**
 - Inbound:** 'SRTP or RTP' is selected.
 - Outbound:** 'SRTP only' is selected.
 - Preferred cipher:** 'AES_CM_128_HMAC_SHA1_32' is selected.
- Device -- device local streaming:** Includes checkboxes for 'Device -- device local streaming', 'Device -- trunk local streaming', 'Codec support' (set to 'Restricted to G.729, G.711 (a-law and u-law)'), and 'RTP frame size' (set to 'Dynamic').
- PRACK support:** Includes a checkbox for 'PRACK support', 'Send options keepalives' (set to 'Only behind NAT'), 'Options interval' (set to '20'), and 'Challenge methods' (set to 'Refer' and 'Prack').
- KPML:** Includes fields for 'KPML username', 'KPML password', and 'Confirm KPML password'.
- Registration Mode:** Includes a dropdown for 'Registration Mode' (set to 'Max Set-Side'), 'Set-side registration expiry time' (set to '240'), 'ICP-side registration expiry time', and 'Allowed URI names' (set to 'micollabtest02p1.mylab2.loc').
- SIP adaptation support:** Includes checkboxes for 'SIP adaptation support', 'SIP adaptation receive pipeline', and 'SIP adaptation send pipeline'.
- Permit weak SIP passwords:** Includes a checkbox.

5.4.6 CONFIGURING THE CONNECTION/AUTHENTICATION BETWEEN THE MBG AND THE IPBX

✓ Common to standalone MBGs , MBGs embedded in MiCollab or clustered MBGs

5.4.6.1 Principle

The connection between the MBG and the MiVoice 5000 must be created in order to:

- Obtain the SIP devices **Set-side username**, **Set-side password** and **lcp-side username** defined in the MBG. These parameters will be used for deployment by TMA.
- Synchronise MiVoice 5000 when a "set-side password" has been changed in the MBG.

The principle of authentication with the MBG consists in:

- Starting the web service
- Adding a new client in the MBG
- Declaring a new SIP device in MiVoice 5000.

5.4.6.2 Detailed procedure



Warning:

This procedure takes place sequentially using the MBG and MiVoice 5000 Webadmin menus alternately.

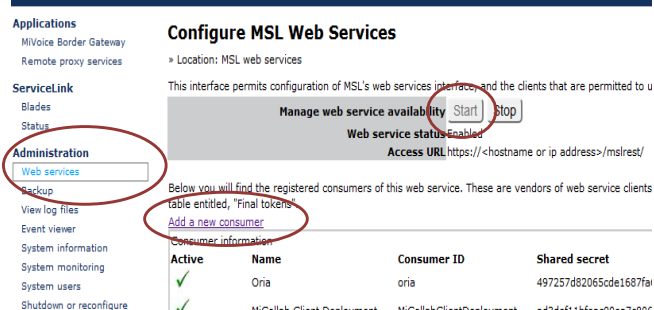
The order of the sequences must be respected.

*On the **MBG Interface**:*

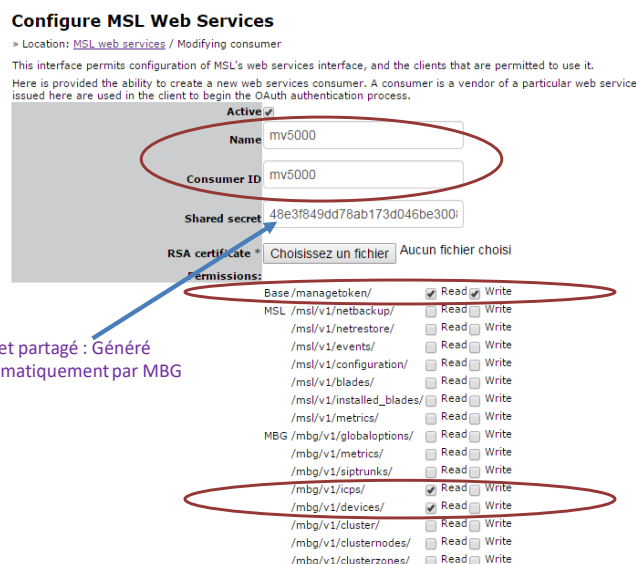
The user must create via Menu **Administration>Web services**, **Add a new consumer** tab a user account that MiVoice 5000 will use to authenticate itself.

An account contains two pieces of data that are essential for the authentication stage:

- the account ID (40-character string maximum) > **Name and Consumer ID** fields
- Its secret code (40-character string maximum) automatically generated and displayed by the MBG. > **Shared secret** field.



Démarrer le service Web
Ajouter un nouveau client > Add a new consumer



Secret partagé : Généré automatiquement par MBG

On the MiVoice 5000 web admin:

Menu **Subscribers>Terminals and Applications>MBG**

Enter the following settings:

- MBG IP address
- User account ID (defined on the MBG)
- Shared secret code associated with the account (defined on the MBG)
- Press Enter.

The **Login** button then appears.

- Click the **Login** button.

MBG

Applications

MiVoice Border Gateway

Remote proxy services

ServiceLink

Blades

Status

Administration

Web services

Backup

View log files

Event viewer

System information

System monitoring

System users

Shutdown or reconfigure

Virtualization

Security

Remote access

Port forwarding

Web Server

Certificate Management

Configuration

Networks

E-mail settings

Configure MSL Web Services

✓ **Operation status report**

Successfully saved new consumer

> Location: MSL web services

This interface permits configuration of MSL's web services interface, and the clients that are permitted to use it.

Manage web service availability Start Stop

Web service status Enabled

Access URL https://<hostname or ip address>/mlrest/

Below you will find the registered consumers of this web service. These are vendors of web service clients, not active clients themselves. For registered clients, see further below in the table entitled, "Final tokens".

[Add a new consumer](#)

Active	Name	Consumer ID	Shared secret	RSA certificate (if any)	
✓	Oria	oria	497257d82065cde1687fa6446da165d30ea4c94a		Modify
✓	McCollab Client Deployment	McCollabClientDeployment	ad3def11bfacc0ea7c806e6b61687ca090ed130f		Modify
✓	vApp	vapp	22c01bd55bd688810ef04e0f9ae5071d293854		Modify Delete
✓	acs1-mq2	acs1-mq2	e7e254f629cae3dc185133a8bae0fdef61e1331		Modify Delete
✓	Miv5000	Miv5000	0eb9978abe1015a33cc58e72e18432bfad0d79e5		Modify Delete

Accueil Web Admin

Abonnés

Terminaux et Applications

MBG

Système

Plan de numérotation

Réseau et liaisons

Accueils

Messagerie et tonalités

Liens rapides

MBG

Service téléphonie>Abonnés>Terminaux et Applications>MBG (1.9.9)

Connexion

Listage équipements SIP

Adresse IP du MBG: 172.15.0.15

Compte utilisateur (défini sur le MBG): Miv5000

Secret partagé (défini sur le MBG): 0eb9978abe1015a33cc58e72e18432bfad0d79e5

Connexion

Export du fichier: AUCUN

MiVoice 5000 Web Admin

The MBG and iPBX must be synchronised (same time).



IMPORTANT NOTE: For a MiVoice 5000 Server iPBX the OS version must be at least 6.7, or the latest version of the OS patches must be installed.

On the *MiVoice 5000* web admin:

press the **Login** button. Menu **Telephony Service>Subscribers>Terminals and Applications>MBG** then displays the **Verification Code** field.

On the *MBG* Interface:

A temporary authentication token has been created by MiVoice 5000 on the MBG (valid for one hour). It appears in Menu **Administration>Web services> "Temporary token"**.

- The administrator must then approve this temporary token via the **Approve** link.

Blades

Status

Administration

Web services

Backup

View log files

Event viewer

System information

System monitoring

System users

Shutdown or reconfigure

Virtualization

Security

Remote access

Port forwarding

Web Server

Certificate Management

Configuration

Networks

E-mail settings

Google Apps

DHCP

Date and Time

Hostnames and addresses

Domains

IPv6-in-IPv4 Tunnel

SNMP

Ethernet Cards

Review configuration

Miscellaneous

Support and licensing

MBG

Manage web service availability
Start Stop

Web service status Enabled

Access URL https://<hostname or ip address>/mslrest/

Below you will find the registered consumers of this web service. These are vendors of web service clients, not active clients themselves. For registered clients, see further below in the table entitled, "Final tokens".

[Add a new consumer](#)

Active	Name	Consumer ID	Shared secret	RSA certificate (if any)
✓	Oria	oria	497257d82065cde1687fa6446da165d30ea4c94a	Modify
✓	MiCollab Client Deployment	MiCollabClientDeployment	ad3def11bfeac0ea7c806e6b61687ca090ed130f	Modify
✓	vApp	vapp	22c01bd55bdd688810ef04e0f9ae50f71d293854	Modify Delete
✓	acs1-mq2	acs1-mq2	e7e254f629cae3dc185133a8bae0fcdef61e1331	Modify Delete
✓	Miv5000	Miv5000	0eb9978abe1015a33cc58e72e18432bfad0d79e5	Modify Delete

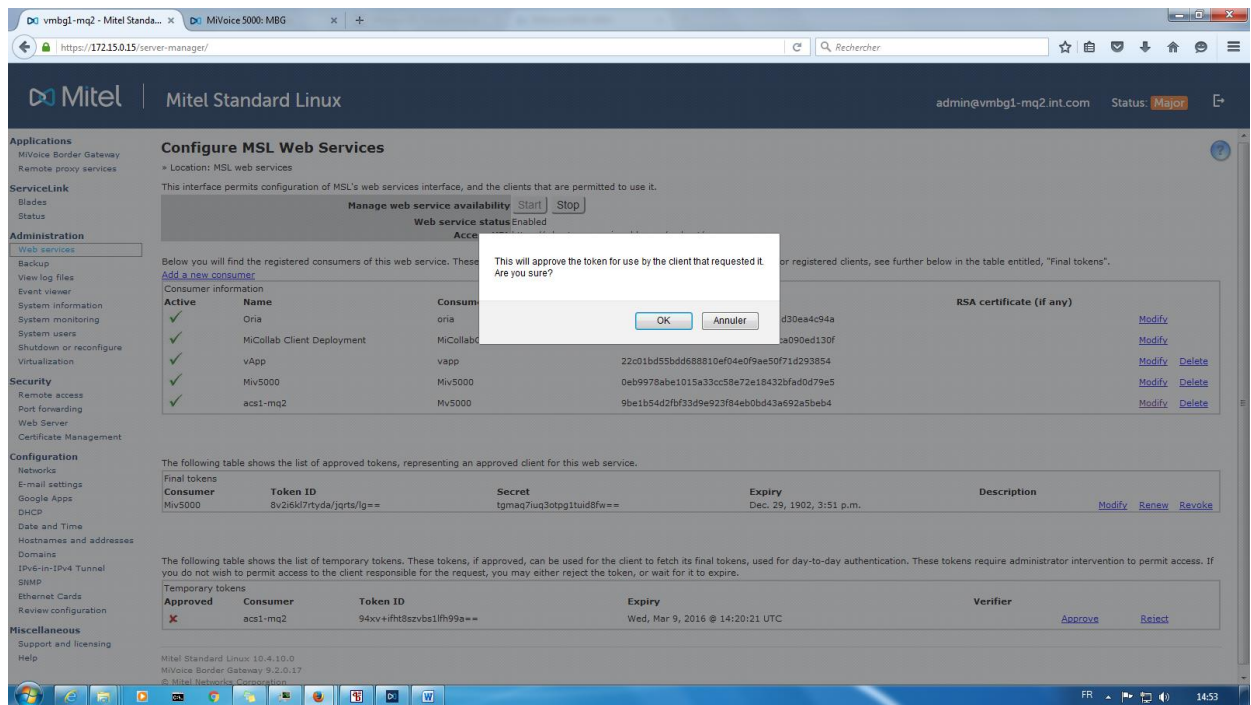
The following table shows the list of approved tokens, representing an approved client for this web service.

Consumer	Token ID	Secret	Expiry	Description
There are no approved tokens at this time. Note, tokens are created as part of the OAuth process, they are not created manually. It is up to the client to initiate this process.				

The following table shows the list of temporary tokens. These tokens, if approved, can be used for the client to fetch its final tokens, used for day-to-day authentication. These tokens require administrator intervention to permit access. If you do not wish to permit access to the client responsible for the request, you may either reject the token, or wait for it to expire.

Approved	Consumer	Token ID	Expiry	Verifier
✗	Miv5000	ciluwekjrpqliw9h1wotw==	Tue, Feb 2, 2016 @ 15:39:40 UTC	<div style="display: flex; align-items: center;"> <div style="display: flex; gap: 10px;"> Approve Reject </div> </div>

- Click **OK**.



When the temporary token is approved, a **Verifier** code is generated. This code must be entered in MiVoice 5000 Webadmin as **Verifier Code**.

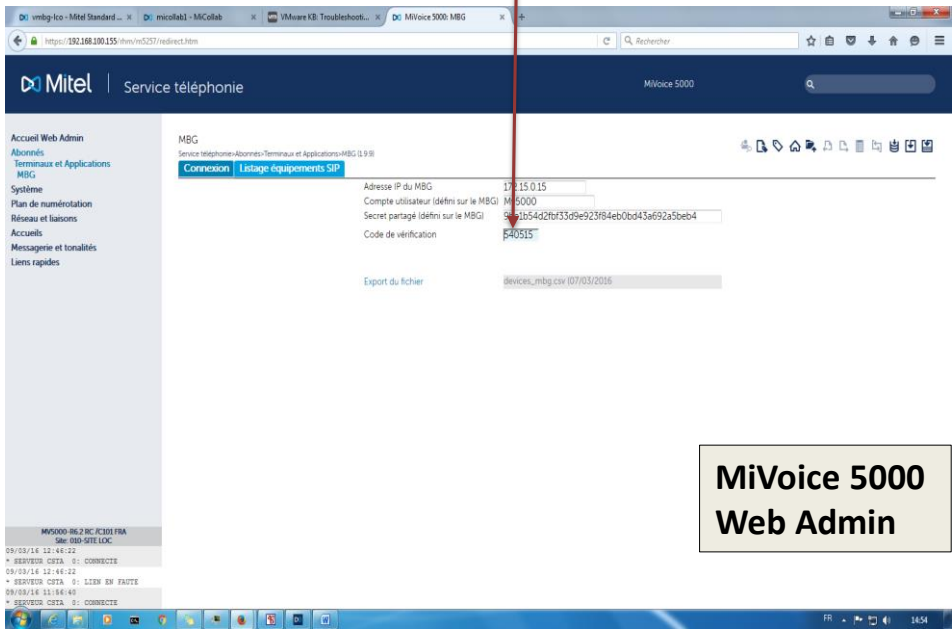
On the **MBG Interface**:

The operator must copy the **Verifier** code associated with this temporary token and paste it into the **Verifier Code** field in Menu **Telephony Service>Subscribers>Terminals and Applications>MBG**.

The following table shows the list of temporary tokens. These tokens, if approved, can be used for the client to fetch its final tokens, used for day-to-day authentication. These tokens require administrator intervention to permit access. If you do not wish to permit access to the client responsible for the request, you may either reject the token, or wait for it to expire.

MBG

Temporary tokens				
Approved	Consumer	Token ID	Expiry	Verifier
✓	Miv5000	ciluwekjrpglivw9h1wotw==	Tue, Feb 2, 2016 @ 15:39:40 UTC	540515 Reject

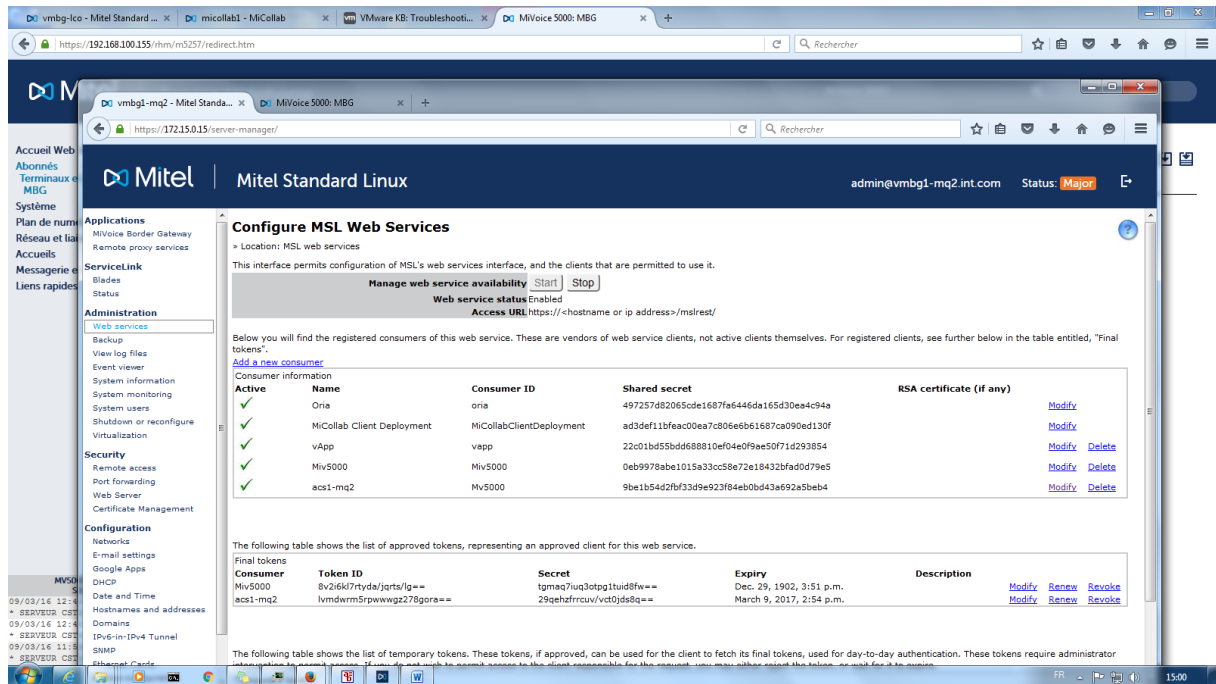


**MiVoice 5000
Web Admin**

On the *MiVoice 5000* web admin:

When the **Verifier Code** field is entered on MiVoice 5000, MiVoice 5000 confirms the authentication token to the MBG.

The MBG then assigns to MiVoice 5000 a final authentication token (a Token ID pair and the associated secret code with a validity period of one year).

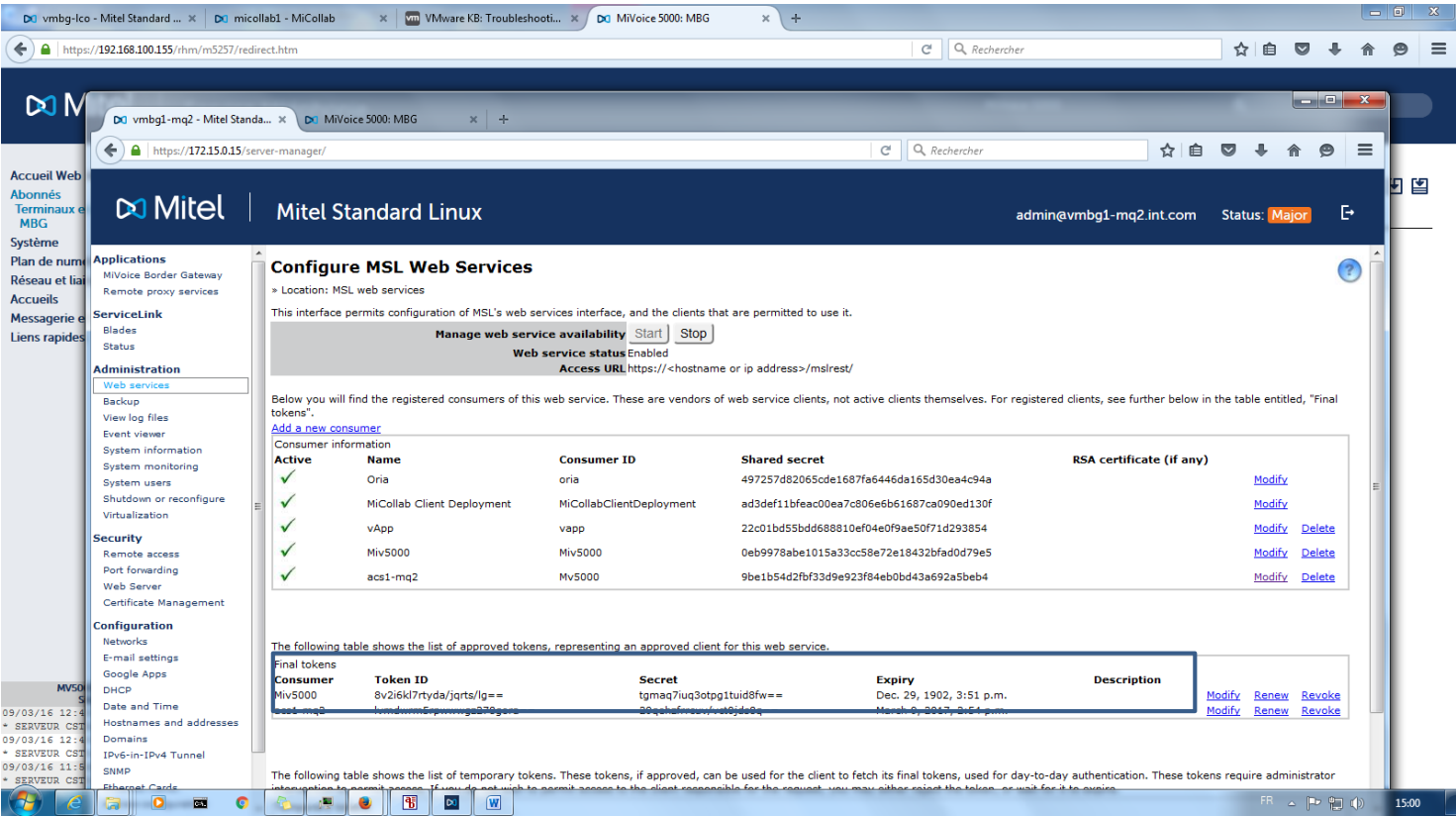


The screenshot shows the Mitel Standard Linux web administration interface. The main content area is titled "Configure MSL Web Services". It indicates that the web service status is "Enabled" and provides a link to manage its availability. Below this, there is a table of registered consumers.

Active	Name	Consumer ID	Shared secret	RSA certificate (if any)	
✓	Oria	oria	497257d82065cde1687fa6446da165d30ea4c94a		Modify
✓	MiCollab Client Deployment	MiCollabClientDeployment	ad3def11bfeac00ea7c806e6b61687ca090ed130f		Modify
✓	vApp	vapp	22c01bd55bd688810ef04e0f9ee5071d293854		Modify Delete
✓	Miv5000	Miv5000	0eb9978abe1015a33cc58e72e18432bfad0d79e5		Modify Delete
✓	acs1-mq2	Mv5000	9be1b54d2fb33d9e923f84eb0bd43a692a5beb4		Modify Delete

Below the consumers table, there is a section for "Final tokens" which shows a list of approved tokens.

Consumer	Token ID	Secret	Expiry	Description	
Miv5000	8v2i6k17tyda/jgrts/g==	tgmaq7uq3otpg1tuid8fw==	Dec. 29, 1902, 3:51 p.m.		Modify Renew Revoke
acs1-mq2	lvmdwm5pwwg2278jgors==	29qehzfrucv/vct0jds8q==	March 9, 2017, 2:54 p.m.		Modify Renew Revoke



On the *MiVoice 5000 web admin*:

Once the final authentication token is obtained from the MBG,

Menu **Telephony Service>Subscribers>Terminals and Applications>MBG** shows the final token ID and expiry date.

When the connection is set up:

The different buttons can then be used to:

- **Change the login settings:** For deleting all settings so authentication can be restarted if a user account or an MBG is changed.
- **Synchronise SIP devices:** For importing the SIP devices attached to the local iPBX and declared in the MBG.
- **Export SIP devices from the MBG:** for creating the file **devices_mbg.csv**.
- **Export of the file:** for exporting the file **devices_mbg.csv** to the local PC ; useful for MAC files.

The file **devices_mbg.csv** contains several columns derived from the values defined in the MBG (see Section 6.1):

- **Login: Set-side username** (Remote Worker login value)
- **NA: Icp-side username** (Remote Worker subscription number)
- **Password: Set-side password** (MD5 password between the phone and MBG)

Then see Chapter 6.4 for information on how to use this file.

The screenshot shows the 'SIP equipments list' tab in the Mitel Border Gateway web admin. The configuration fields include:

- MBG IP address: 172.15.0.15
- User account (set by MBG): Mv5000
- Shared secret (set by MBG): 9be1b54d2fbf33d9e923f84eb0bd43a692a5beb4
- Final token: hfeexepds06pedbhdpxzsw==
- Expiry date of authentication: 01/02/2017-16:59:36
- Connection to MBG established

Buttons visible include 'Change connection parameters', 'Complete synchronisation of SIP devices', and 'Export of MBG SIP equipments'. The 'Export of the file' button is circled in red and points to the following table:

	A	B
1	NA	Password
2	6320	RW6300ptf
3	6310	RW6310ptf
4	6400	RW6400ptf
5	6000	RW6000ptf
6	6200	RW6200ptf
7	6300	RW6300ptf
8	6100	RW6100ptf

5.5 CONFIGURING THE MBG IN WHITE LIST

✓ **Common to standalone MBGs , MBGs embedded in MiCollab or clustered MBGs**

As the MBG concentrates the flow of all remote users, the MBG IP address must be put in the iPBX White list to avoid unwanted automatic listing of the MBG by the iPBX.

On the iPBX Webadmin

From Menu **Telephony Service>Network & Links>Quality of Service>SIP Security**

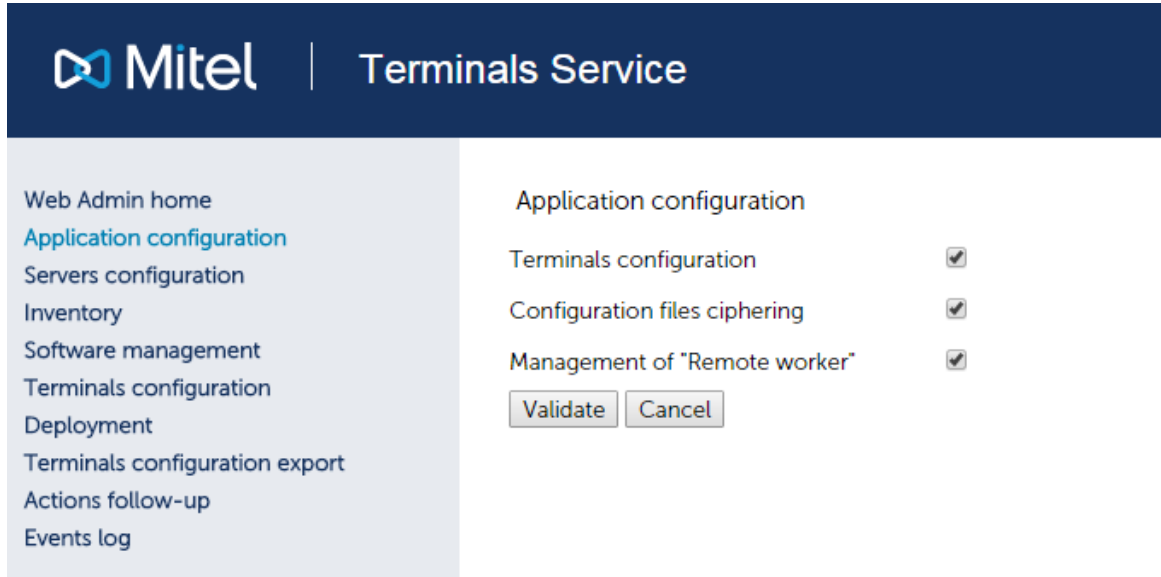
Define the MBG address in the White list.

See iPBX Operating Manual – AMT/PTD/PBX0080.

5.6 CONFIGURING TMA (PHONE SERVICE)

Application configuration menu

- Tick the boxes indicated:



The screenshot shows the Mitel Terminals Service web interface. On the left is a navigation menu with the following items: Web Admin home, Application configuration (highlighted in blue), Servers configuration, Inventory, Software management, Terminals configuration, Deployment, Terminals configuration export, Actions follow-up, and Events log. The main content area is titled 'Application configuration' and contains three items, each with a checkbox: 'Terminals configuration' (checked), 'Configuration files ciphering' (checked), and 'Management of "Remote worker"' (checked). At the bottom of this section are two buttons: 'Validate' and 'Cancel'.

File encryption is not mandatory but is highly recommended.

For the integrated TMA, the integrated (= "local") FTP server is automatically set as soon as the **Remote worker management** box is ticked.

5.7 DEFINING THE DOWNLOAD SERVER FOR REMOTE WORKERS

The aim is to define the download servers dedicated to Remote Worker phones.

For an integrated TMA:

The local FTP server is automatically added for the Remote Worker phones (see previous section).



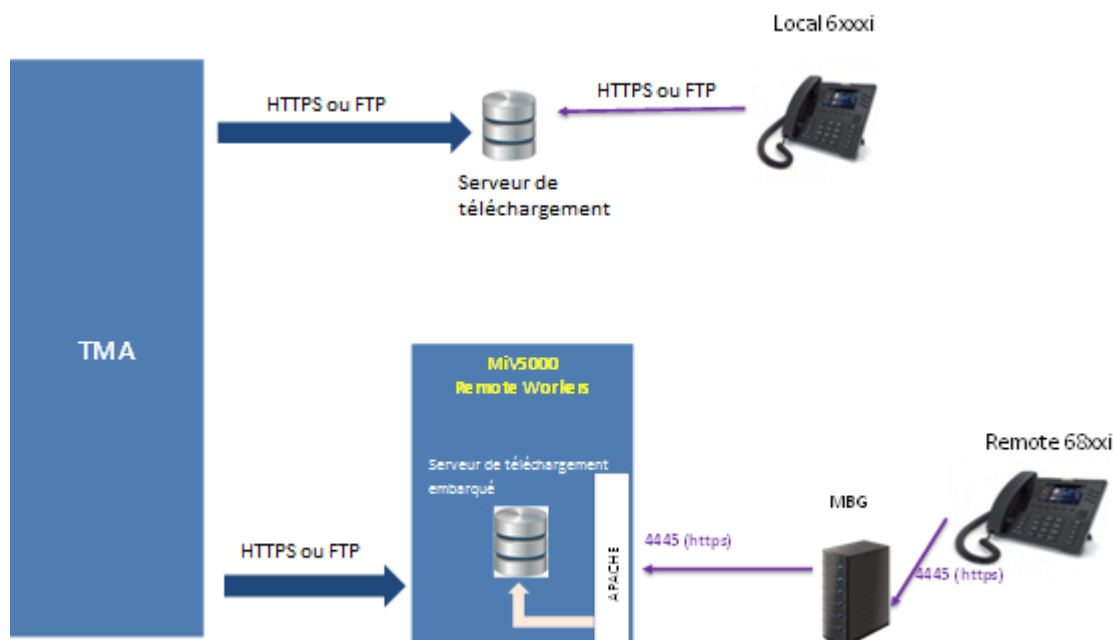
IMPORTANT NOTE: The iPBX integrating this embedded FTP server must be the same one on which the Remote Worker subscriptions are declared.

For the centralised TMA/TMA-EP in MiVoice 5000 Manager:

Define the server(s) dedicated to the Remote Worker phones.



Note: If the same server is to be used for local and remote phones, it must be declared twice (once for remote phones and once for local phones).



5.7.1 Configuring the download server for remote workers

The following information is required:

- Name
- IP address (must match the PBX on which the remote workers are defined)
- Port: value fixed at 21
- List sites on which the Remote Workers attached to the given download server are declared
- Login/password information for 6xxxi phones, entered by default with the values of the embedded FTP server (FTP account mngt_ftp_67xxi)

Once this information is validated, the server will appear on the "List of Remote Workers Servers" table.

From the **Server configuration** menu:

- Click **Add a new server** in the Remote Worker area.
- Fill in all necessary fields as indicated above.
- Define the list of iPBX sites attached to this server for the Remote Workers (using the **Modify the list of sites in the previous screen** button).

Lists management

*Server

Sites list:

Selected

☒ ACS-155

☐ AXL-160

All

None

Inverted selection

Save Reset

* = Required fields

- Select only the site to which the Remote Workers are attached.
- Save and confirm.

Once this information has been validated, the download server appears on the **Server List** table.

- **Modify server** allows you to modify the server settings.
- **Delete server** allows you to delete the server.

6 PREPARING THE DEPLOYMENT

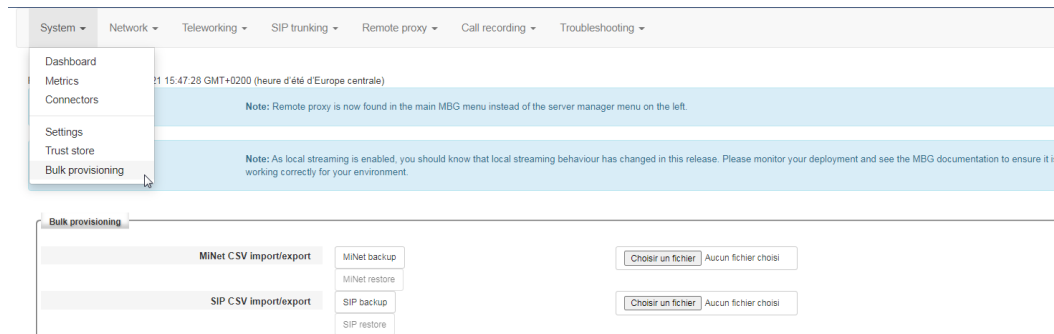
6.1 DECLARING SIP DEVICES (6800 SIP AND 6900 IP PHONES)

✓ **Not common to standalone MBGs , MBGs embedded in MiCollab or clustered MBGs (see the various sections below)**

6.1.1 STANDALONE MBG

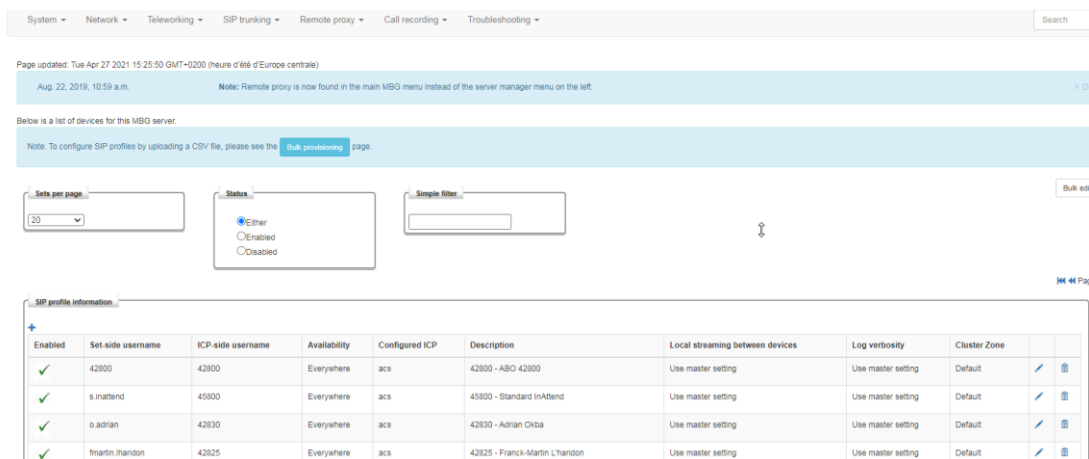
This configuration must be carried out for each 68xxi phone in Remote Worker mode.

Equipment can also be created by downloading a CSV file > Menu **System>Bulk provisioning**.



Configuring Remote Worker phones

Menu **MiVoice Border Gateway, Teleworking> SIP** tab



In the **SIP profile information** area, click **+** on the top left side of the SIP profile information area.

In the next window, configure the settings as shown below:

Configured ICP:

- **ICP => IP Connection Point = MiVoice5000**

Set-side username:

- Remote Worker login value

Set-side password:

- MD5 password between the phone and MBG

lcp-side username:

- Remote Worker subscription number

lcp-side password:

- MD5 password for the MiVoice 5000 subscription

Description:

- Name considered for the device used, for example, for listing.

Fill in all the fields then click **Save**.

Repeat the procedure for the following SIP devices.

6.1.2 INTEGRATED MBG OR MBG IN CLUSTER MODE WITH MICOLLAB

The 6800 SIP and 6900 IP phone Remote Worker only work in SSO mode.

When the MBG is clustered with MiCollab, the SIP devices are provisioned by MiCollab server. The following identification is performed for all Remote Worker subscribers:

Menu **MiVoice Border Gateway, Teleworking> SIP** tab

In the **SIP profile information** area, click **+**.

Configure the following fields as indicated:

Set-side username: Login

Set-side password: Randomly generated by the MiCollab server.

6.2 SPECIFIC CONFIGURATION OF A MICOLLAB SOFTPHONE CLIENT

✓ Common to standalone MBGs , MBGs embedded in MiCollab or clustered MBGs

This case only concerns users with a Remote Worker 6800 SIP or 6900 IP phone and a Micollab Softphone in remote access.

For this subscription, the remote phone must be logged in before the Micollab Softphone.

As encryption is not currently available on MiCollab Softphone Clients, the following configuration is required:

On the MBG:

Allowed but not required

The screenshot shows the 'Manage device' configuration page for a Micollab softphone client. The page is divided into two main columns. The left column contains various settings, and the right column contains authentication and security settings. The 'Set-side RTP security' dropdown is highlighted with a purple oval and is set to 'Allow'. Other settings include 'Enabled' (checked), 'Configured ICP' (mv5000-ico), 'Set-side username' (65173), 'Set-side password' (masked), 'Icp-side username' (65173), 'Icp-side password' (masked), 'PRACK support' (Use master setting), 'Heartbeat interval' (empty), 'Options keepalives' (Use master setting), 'Challenge methods' (Use master setting), 'Description' (65173 - ABO 65173), 'Local streaming' (Use master setting), 'Log verbosity' (Use master setting), 'Enable Detailed Jitter Log' (Use master setting), 'Codec support' (Use master setting), and 'RTP Framesize' (Use master setting).

Enabled	<input checked="" type="checkbox"/>	Configured ICP	mv5000-ico
Set-side username	65173	Set-side password	*****
		Confirm set-side password	*****
Icp-side username	65173	Icp-side password	*****
		Confirm icp-side password	*****
PRACK support	Use master setting	Options keepalives	Use master setting
Heartbeat interval		Challenge methods	Use master setting <input type="button" value="Override"/>
Set-side RTP security	Allow	Description	65173 - ABO 65173
Icp-side RTP security	Use master setting		
Local streaming	Use master setting		
Log verbosity	Use master setting	Codec support	Use master setting
Enable Detailed Jitter Log	Use master setting	RTP Framesize	Use master setting

On the MiCollab Softphone Client:

Configuration d'MiCollab Client

Représentation

Intégration du calendrier

Notification d'appels

Paramètres de discussion

Gestion des Connaissances

Notification de connexion

Intégration PIM

Fenêtre RSS

Paramètres du logiphone

Affichage Contacts

Cliquer pour appeler

☒ Activer SIP Softphone

DN SIP Softphone : 65173

Connexion SIP : TCP

Softphone va utiliser les appareils suivants

Microphone : Microphone sur casque (2- USB Teleph

Haut-parleur : Valeurs par défaut

Alertes: Valeurs par défaut

Contrôle des appels : Aucune

Caméra vidéo : QuickCam Communicate Deluxe

Sonnerie

☒ Défaut ☐ Lire

☒ Utiliser le télétravailleur pour softphone

Passerelle Teleworker :

6.3 PREPARING THE REMOTE WORKER CSV FILE FROM THE GENERIC PROVISIONING FILE

The file [TMA_provisionning_6xxxi@version.xls](#) is available on Mitel's extranet.

ONGLET/SHEET '68xx SIP TELESWORKERS'

Fonction / Function:
 Cet onglet est utilisé pour générer un fichier ".csv", pour TMA, contenant les paramètres requis pour la fonctionnalité Téléworker par terminal 68xx SIP. RemoteWorker pour les postes 68xxi via MBG. TMA permet ensuite de charger ce fichier ".csv", créant les fichiers MAC mis dans le répertoire FTP embarqué défini. Se référer à la documentation MIV5000 'XXX'.
 / This sheet is used to generate a ".csv" file, for TMA, including the parameters required for the feature Teleworker by terminal 68xx SIP. After TMA allows to load this file ".csv" file, creating MAC files put into the defined embedded FTP server. Please refer to the Miv5000 documentation 'XXX'.

Rules:
 3 types de données différenciés par la couleur de la police / 3 kind of data differentiated by the font color:
 - Noir / Black: donnée par terminal-abonné / data by terminal-subscriber
 - Marron / Brown: Donnée système - même valeur pour toutes les adresses MAC / system data - same value for all MAC_ADDRESS
 - Rouge / Red: données obligatoires - éviter de les modifier / compulsory data - avoid to modify them

Attention / Caution:
 - Merci de ne pas modifier le nom de cette onglet / Please do not modify the name of this sheet.
 - Merci de ne pas créer de ligne avant 'MAC_ADDRESS' / Please do not create any line before 'MAC_ADDRESS'

Generation .csv

TERMINAL - SUBSCRIBER				SYSTEM			
MAC_ADDRESS	!sip line1 user name	!sip line1 auth name	!sip line1 password	!sip proxy ip	!sip registrar ip	!https server	
00085D4330B8	7000	7000	password1	64.101.10.1	64.101.10.1	64.101.10.1	9a480i
08000F9F7305	7001	7001	password2	public.test.com	public.test.com	public.test.com	9a480i

Import_CSV_TMA 67xxi Global 67xxi Specific 67xxi All 68xxi Teleworker

- Fill in the **68xxi Teleworker** tab according to the rules below (also listed in this file).
- Then generate the file in csv format (using the **Generate .CSV** button).

The other tabs are for Global and Specific data for all 6xxxi SIP Phones. For more information, refer to the 6xxxi Operating Manual - AMT/PTD/TR/0043.

Rules for Remote Workers (outlined in the file):

3 types of data must be differentiated by font colour:

Black: Data to be entered for each Remote Worker phone

Brown: System data to be entered for all MAC addresses

Red: Mandatory data that should not be modified

Example:

A	B	C	D	E	F	G	H
Fonction / Function: Cet onglet est utilisé pour générer un fichier ".csv", pour TMA, contenant les paramètres requis pour la fonctionnalité Téléworker par terminal 68xx SIP RemoteWorker pour les postes 68xx via MBG TMA permet ensuite de charger ce fichier ".csv", créant les fichiers MAC mis dans le répertoire FTP embarqué défini. Se référer à la documentation MIV5000 'XXX'. / This sheet is used to generate a ".csv" file, for TMA, including the parameters required for the feature Teleworker by terminal 68xx SIP. After TMA allows to load this file ".csv" file, creating MAC files put into the defined embedded FTP server. Please refer to the MIV5000 documentation 'XXX'.							
Rules: 3 types de données différenciés par la couleur de la police / 3 kind of data differentiated by the font color: - Noir / Black: donnée par terminal-abonné / data by terminal-subscriber - Marron / Brown: Donnée système - même valeur pour toutes les adresses MAC / system data - same value for all MAC_ADDRESS - Rouge / Red: données obligatoires - éviter de les modifier / compulsory data - avoid to modify them							
Attention / Caution: - Merci de ne pas modifier le nom de de cette onglet / Please do not modify the name of this sheet. - Merci de ne pas créer de ligne avant 'MAC_ADDRESS' / Please do not create any line before 'MAC_ADDRESS'							
<div> <div>Generation .csv</div> <div>D:\templexport_global.csv</div> </div>							
TERMINAL - SUBSCRIBER				SYSTEM			
MAC_ADDRESS	!sip line1 user name	!sip line1 auth name	sip line1 password	sip proxy ip	sip registrar ip	https_server	https_path
00085D4330B8	7000	7000	password1	64.101.10.1	64.101.10.1	64.101.10.1	9a48085c1b816fd1b512e8b186686a6
08000F9F7305	7001	7001	password2	public.test.com	public.test.com	public.test.com	9a48085c1b816fd1b512e8b186686a6

Cliquer sur le Bouton
Generation .csv

```

23 ;TERMINAL - SUBSCRIBER;;;SYSTEM;;;COMPULSORY;;;;;;;;;;;;;;;;;
24 MAC_ADDRESS;!sip line1 user name;!sip line1 auth name;sip line1 passwo
25 00085D4330B8;7000;7000;password1;64.101.10.1;64.101.10.1;64.101.10.1;9
26 08000F9F7305;7001;7001;password2;public.test.com;public.test.com;publi

```

Full list:

Data to be entered for each Remote Worker

- **MAC_ADDRESS:** MAC address of Remote Worker's 6800 SIP or 6900 IP phone
- **!sip line1 user name:** Subscriber login (from the MBG file devices_mbg.csv)
- **!sip line1 auth name:** Subscriber login (from the MBG file devices_mbg.csv)
 - In SSO mode: Subscriber's login
 - Without SSO mode: Subscriber's number
- **sip line1 password:** Set-side password (from MBG file devices_mbg.csv)

System data to be entered for all MAC addresses

- sip proxy ip: Public address or name of MBG
- sip registrar ip: Public address or name of MBG
- **https server: Public address or name of MBG**
- **https path: MiVoice 5000 hash value**
- keyboard script: iPBX access URL for Remote Worker stations

6.4 REMOTE WORKER MANAGEMENT BY TMA

6.4.1 PREREQUISITES

The CSV file is available (created from the Provisioning file). See Section 6.3.

6.4.2 DEPLOYING FROM THE DOWNLOAD SERVER

6.4.2.1 *Principle*

The action consists in sending the following from the TMA **Deployment** menu to the download server dedicated to Remote worker phones:

- The certificate CA_Mitel.pem must be deposited (in the field **Other file, template, certificate ...**)
- Specific data file(s) mac.cfg generated while importing a csv file (**Remote workers (cs) file** field)



Note: The "Specific (csv) file" menu is greyed out because it cannot be used to manage remote workers; this menu can only be used to send specific files to a download server for non-Remote Worker phones.

6.4.2.2 *Deployment by integrated TMA*

The integrated FTP server must be active.

The action only consists in generating the remote Worker file and sending the certificate:

For other files, the integrated FTP server already contains the correct phone software release and the associated global data file.

From the **Deployment** menu:

- Select the "local" server from the list of "Remote Workers" FTP servers.
- From the **Remote Workers (csv) file** field, import the Remote Worker's "csv" file from the provisioning file defined in Section 6.3.
- Import the certificate file from the **Other file, template, certificate ...** field.
- Click **Validate**.

The action is taken immediately.

The progress of the action can be seen from the **Actions display** and **Events log** menu.

At the end of the action, the message **Deployment completed** is displayed.

6.4.2.3 *Deployment by TMA managed from MiVoice 5000 manager*

From the **Deployment** menu

- Choose a server from the list of Remote Worker servers.
- If possible, choose a software release from the "Software version" list.
- If necessary, import a global data file.
- From the **Remote Workers (csv) file** field, import the Remote Worker's "csv" file from the provisioning file defined in Section 6.3.
- Import the certificate file from the **Other file, template, certificate ...** field.
- Click **Validate**.

The action is taken immediately.

The progress of the action can be seen from the **Actions display** and **Events log** menu.

At the end of the action, the message **Deployment completed** is displayed.


6.5 DISPLAY/INVENTORY OF REMOTE WORKER PHONES

Once the deployment action has been successfully completed, the list of Remote Worker phones can be viewed from the TMA main menu; select the **Inventory** menu.

In the **Inventory** menu, **Remote worker management** tab, the list of remote workers phones is displayed for each site.

For an integrated TMA: There is only one “local” site.

The screenshot shows the Mitel TMA web interface. The 'Inventory' section is active, displaying a list of 9 terminals. The table columns are: Phone number, Logged, Label, Periodical logout, Site, Model, Software release, IP address, MAC Address, Line, Global data, Specific data, Site number, and Node. The data rows show various phone models and their associated IP addresses and MAC addresses. A status icon (a green circle with a white plus sign) is visible next to the phone number 62201.

The  icon concerns Remote Worker phones and indicates that the phone is deployed and connected.

Possible actions: Display or delete

Display: “Remote worker management” window

List of MAC addresses of remote worker phones that have been deployed.

One or more terminals can be deleted, which implies deleting the specific file locally and on the FTP server

Delete: Removing all specific files associated with the terminals described in the list locally and on the download server.

A **Filter** function is also available.

7 DEPLOYING REMOTE WORKER PHONES

✓ Common to standalone MBGs , MBGs embedded in MiCollab or clustered MBGs

The administrator retrieves the MAC address of the 6800 SIP or 6900 IP phone meant for the remote user.

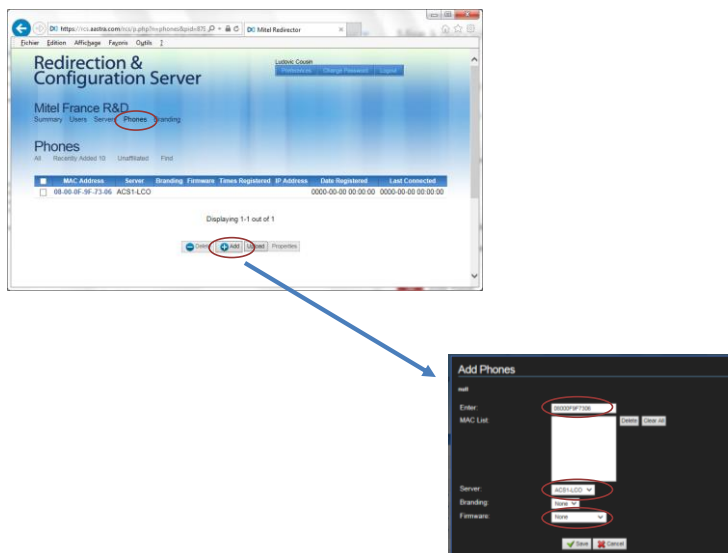
7.1 CONFIGURING THE ATTACHED IPBX FOR EACH REMOTE WORKER PHONE

7.1.1 WITH RCS

RCS server access URL: <https://rcs.aastra.com/rcs/login.php>

From the RCS welcome screen

- In the **Phones** menu, fill in the different fields as follows:
- the MAC addresses of each phone attached to the IPBX defined below.
- Enter the (iPBX) configuration server name.
- Branding: **None**
- Firmware override:
 - The 6900 phone can be upgraded from Minet firmware to SIP firmware through this operation.
 - Take SIP firmware 5.0.0 minimum.
- Click **Save**.



The remote station, after a factory reset (in SIP mode) will connect to the RCS server and automatically retrieve the address of the MBG associated with the iPBX in question.

7.1.2 WITHOUT RCS SERVER

The configuration must be carried out by the administrator or by the user (according to the instructions given by the administrator) for each Remote Worker phone.

First, perform a factory reset of the phone via Menu **Reinit > Reset to factory settings**.

Log on to the phone's web interface: **https://IP address of the 6800 SIP or 6900 IP Phone (in SIP mode)**.

In the **Configuration server** menu:

Fill in the following values:

- **Download protocol:** HTTPS
- **HTTPS server:** MBG name or public address
- **HTTPS path:** Access path including the URL hash key enabling the phones to download their configuration file. See the value in Section 5.2.

Example: **https://name_server:4445/3f52a279885152701d8f2f39d9bcfc36/ftp_67xxi**

- **HTTPS port:** The corresponding port for Link **4445**.

Save the settings then simply restart the phone. It may be necessary to disable the DHCP options.

The remote phone, after a reboot, will then connect to its iPBX via the MBG and retrieve its configuration files.

The screenshot displays the Mitel Configuration Server Settings web interface. The left sidebar contains a navigation menu with options such as Status, System Information, License Status, Operation, User Password, Phone Lock, Softkeys and XML, Keypad Speed Dial, Directory, Reset, Basic Settings, Preferences, Custom Ringtones, and Advanced Settings. The main content area is titled 'Configuration Server Settings' and is divided into two main sections: 'Settings' and 'Auto-Resync'. In the 'Settings' section, the 'Download Protocol' is set to 'HTTPS', the 'Primary Server' is 'sccs-mq2.int.com', the 'HTTPS Path' is '1a0f5c3e4c1a505c70d3c', and the 'HTTPS Port' is '4445'. In the 'Auto-Resync' section, the 'Mode' is 'BOTH', the 'Time (24-hour)' is '0400', the 'Maximum Delay' is '15', and the 'Days' are '0'. There is also a section for 'XML Push Server List (Approved IP Addresses)' with a 'Save Settings' button at the bottom.

8 CONFIGURING THE EMERGENCY NUMBER FOR FIXED REMOTE WORKERS

IMPORTANT:

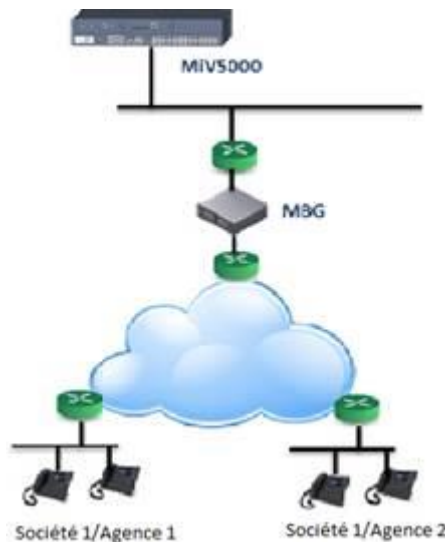
For this section, also see Mitel Gateways and MiVoice 5000 Server - Operating Manual for the configuration of the numbering plan, abbreviated numbers and special numbers for emergency calls. This documents is available on Mitel's website.

8.1 PRINCIPLE

For a remote worker, a call to an emergency number must be made to the right service in relation to their location.

Example: If 18 is dialled by the remote worker, the call is made to the public fire brigade number for the area concerned.

If the remote workers are located at different sites and connected via an MBG, IP-based location is not suitable because in this case all subscribers are seen with the same IP address.



To solve this problem, abbreviated numbers are used. Abbreviated numbers are defined according to administrative hierarchies.

For each hierarchy, abbreviated numbers can be defined with different public numbers.

To apply this mechanism to special numbers, the special number configuration must be changed in the special number menu.

For example, if a user dials 119, either 00130964718 or 00130964719 will be called, depending on the subscriber's administrative hierarchy (location).

In this way, a group of people with the same administrative hierarchy can call the same emergency service number by simply dialling the same special number.

The main steps for making emergency calls to different public numbers based on location are as follows:

- It is all about grouping together, in the same administrative hierarchy, subscribers from one or more sites with the same geographic location.
- Create different administrative hierarchies by the agencies' geographic region.
- Assign an identical administrative hierarchy for each subscription of the same agency (Company1/Agency 1 in the example). This administrative hierarchy must correspond to the location of the subscribers' agency.
- Define short codes according to the administrative hierarchy.

- Configure the special numbers (emergency numbers) for the abbreviated number and assign them respectively according to administrative hierarchy. E.g.:
 - Configure the special numbers with the prefix of the abbreviated number (Example: * 3529) combined with the previously declared number of the emergency service to be called (00130964018).
- Declare the public call number of the required emergency services of each geographic region in the external record directory and assign them the same abbreviated number with the corresponding administrative hierarchy of the region concerned.

In this way, a group of people with the same administrative hierarchy can call the same emergency service number by simply dialling the same special number.

8.2 CONFIGURATION

- Group together, in the same administrative hierarchy, subscribers from one or more agencies with the same geographic location.

Menu **Subscribers>Directory>Administrative hierarchies**.

- Declare the public call number of the required emergency services of each geographic region in the external record directory and assign them the same abbreviated number with a different administrative hierarchy.

Menu **Subscribers>Directory> External records**

- Configure the special numbers with the prefix of the abbreviated number (Example: * 3529) combined with the previously declared number of the emergency service to be called (00130964718).
- To apply this mechanism to special numbers, change the special number configuration (11) 19 in the above special number menu as illustrated below.
- Changing the special number with the abbreviated number concerned (*3529)

Special numbers LIST 1 for CODE 0
Telephony service>Dialing plan>Special numbers>Special numbers definition (3.6.2)

extended day no.
 extend. night no.
 label

Number (1)5
 extended day no.
 extend. night no.
 label

Number 6
 extended day no.
 extend. night no.
 label

Number (1)7
 extended day no.
 extend. night no.
 label

Number (1)8
 extended day no.
 extend. night no.
 label

Number 9
 extended day no.
 extend. night no.

Special numbers display for CODE 0
Telephony service>Dialing plan>Special numbers>Special numbers display (3.6.3)

List	Number	Day number	Night number	Wording
0	(1)2	0112		URGENCE
0	(1)5	0115		SAMU SOC
0	(1)9	0119		MALTRAIT
1	(1)5	015		SAMU
1	(1)7	017		POLICE
1	(1)8	*3529		POMPIER

In the directory, the same abbreviated number is associated with two public numbers corresponding to two locations.

Abbreviated numbers display
Telephony service>Subscribers>Directory>Displays>Com abbreviated dialing (1.1.5.3)

Abbr.numb	Number	Name	Authorized for
(*3) 001	01700011001	EXT601	All hierarchies
(*3) 002	01700011002	Nouvel_essai	All hierarchies
(*3) 111	01700011011	S.Paja	All hierarchies
(*3) 114	208	ABO 208	All hierarchies
(*3) 123		lhl	All hierarchies
(*3) 168	5225	ABO 5225	All hierarchies
(*3) 209	119	Y.Houmaire	All hierarchies
(*3) 224	01700011024	Abregeos	All hierarchies
(*3) 333	01700011033	E.ABO 6000	All hierarchies
(*3) 428	4017	Marco	Agence HHA1/Bureau1
(*3) 428	01700011042	Camille	Agence HHA1/Bureau2
(*3) 443	5688	Test_Sama	All hierarchies
(*3) 529	00130964718	Pompier1	Agence HHA1/Bureau1
(*3) 529	00130964719	Pompier2	Agence HHA1/Bureau2
(*3) 530		S.Henri	All hierarchies
(*3) 600		ABO 600	All hierarchies
(*3) 650	01700011065	Abo650	All hierarchies
(*3) 666	01700011066	ABO 8100	All hierarchies

This configuration can be repeated as many times as the emergency numbers are different in each location: Fire brigade, hospital, police, etc.).

9 OTT MODE CONFIGURATION FOR CLIENT AND USER PORTAL WEB APPLICATIONS ACCESS

9.1 PRINCIPLE

This configuration allows remote workers to access applications via the Internet in OTT mode and without VPN:

- MiVoice 5000 User Portal via MiVoice 5000 Manager,
- MiVoice 5000 Manager WebClient,
- Embedded MiVoice 5000 User Portal.



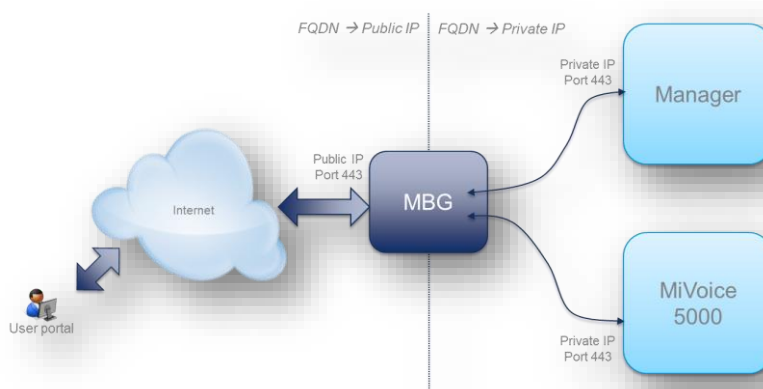
Note: Concerning Manager User Portal, the functionality is also available for users declared on sites in version < 8.0 (and ≥ 6.5).

The principle is to authorize access to these applications through the MBG.

Access is via the Internet and in https via an MBG Controller session in OTT mode.

Via the Internet, the FQDN of MiVoice 5000 Manager must be resolved to the IP address of the MBG when on the INTERNET.

Access to the User portal in OTT mode



The User Portal (MiVoice 5000 Manager or integrated in the MiV5000) is accessible from anywhere via the Internet thanks to the FQDN allowing the remote worker to program the keys of the remote terminal.

The URL is identical in local mode or in OTT mode.

The MBG is used as a proxy to allow access from the Internet. The MBG's local IP address must be declared as a trusted proxy in the MiVoice 5000 Manager or Web Admin.

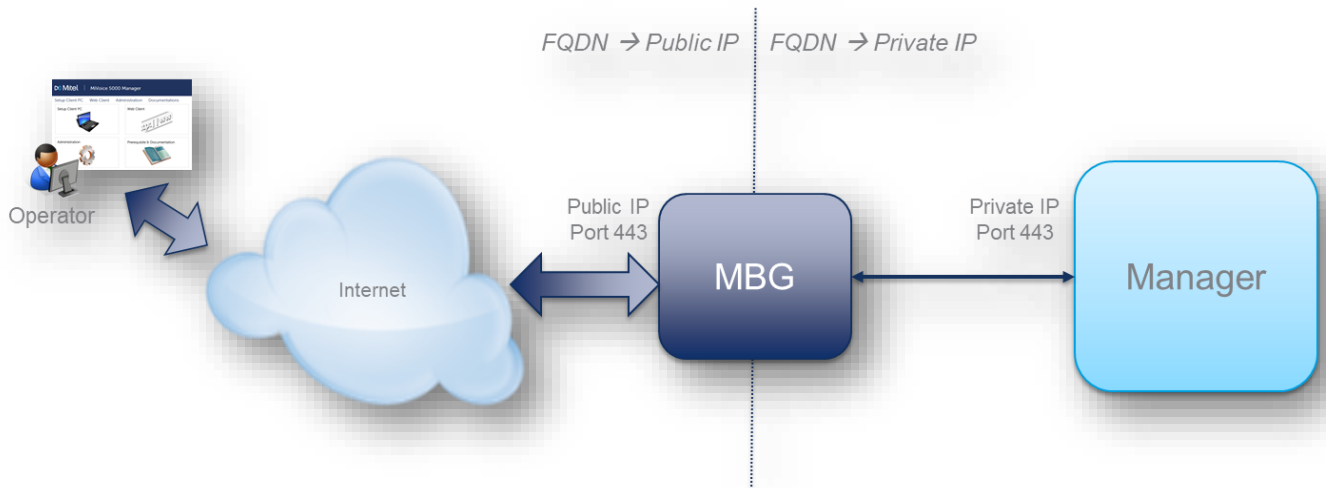
The embedded User Portal uses HTTPS port 443.

Access to the User Portal is compatible with all versions of MiVoice 5000 (R6.5 and later)

Access in SSO mode to the User Portal is not available for the embedded User Portal. Only available for the MiVoice 5000 Manager User Portal.



Note: In the current version, stream separation is not compatible with the embedded User Portal.

Access to the MiVoice 5000 Manager Web Client in OTT mode

The Web Client (MiVoice 5000 Manager or integrated into the MiV5000) is accessible for the remote worker, from anywhere via the Internet thanks to the FQDN.

The URL is identical in local mode or in OTT mode.

The MBG is used as a proxy to allow access from the Internet. The MBG's local IP address must be declared as a trusted proxy in the MiVoice 5000 Manager or Web Admin.

For Web Admin admin access, the associated users and accounts must be declared in the Proxy configuration.

9.2 SUMMARY OF THE DIFFERENT STEPS

9.2.1 MBG CONFIGURATION

In the **Remote proxy/Domain List** menu:

- Click on +,
- Enter the WAN-side FQDN of the MiVoice 5000 Manager (in the case of the Web Client or User Portal) or of the MiVoice 5000 Server (in the case of the on-board User Portal) for resolution on the MBG
- Select the MiV5000 **Over Internet Access** service and tick the **Enabled** box.

Example: Case of the MiVoice 5000 manager.

Mitel

Mitel Standard Linux

Applications

MiVoice Border Gateway

ServiceLink

Blades

Status

Administration

Web services

Backup

Restore

View log files

Event viewer

System information

System monitoring

System users

Shutdown or reboot

Virtualization

Security

System

Network

Teleworking

SIP trunking

Remote proxy

Call recording

Troubleshooting

Page updated: Fri Apr 15 2022 16:48:33 GMT+0200 (Central European Summer Time)

Remote proxy

+

Enabled	WAN-side FQDN	Allowed netblocks	Server type
<input checked="" type="checkbox"/>	managerjb.frguylab	All	MiV5000 Over Internet Access server with the following user level access enabled: MiV5000 Over Internet Access Admin level access is enabled

In the **Remote proxy/Users** menu:

- Declare users and create associated accounts for Web Admin admin access.

System

Network

Teleworking

SIP trunking

Remote proxy

Call recording

Troubleshooting

Page updated: Tue Jul 05 2022 11:05:15 GMT+0200 (heure d'été d'Europe centrale)

May 12, 2021, 12:05 p.m.

Note: As local streaming is enabled, you should know that local streaming behaviour has changed in this release. Please monitor your deployment and see the MBG documentation to ensure it is working correctly for your environment.

Remote proxy users

+

Active	Username	Name	Email address	Granted permissions	Creation date	Deferred activation date	Expiry date		
<input checked="" type="checkbox"/>	mi	Manager	managerjb.frguylab	MiV5000 Over Internet Access admin	April 22, 2022, 10:14 a.m.	None	None		
<input checked="" type="checkbox"/>	mi	Manager	managerjb.frguylab	MiV5000 Over Internet Access admin	April 22, 2022, 2:47 p.m.	None	None		

In the **Remote proxy/Proxy applications** menu

- View the list of URLs of the **MiV5000 Over Internet Access service**

MiV5000 Over Internet Access	a50	/userportal	/htm	User	Admin
			/lrf		
			/csv		
			/system		
			/dhcp		
			/dhcp6		
			/lma		
			/annuaire		
			/easyadmin		
			/setup		
			/webtelephony		

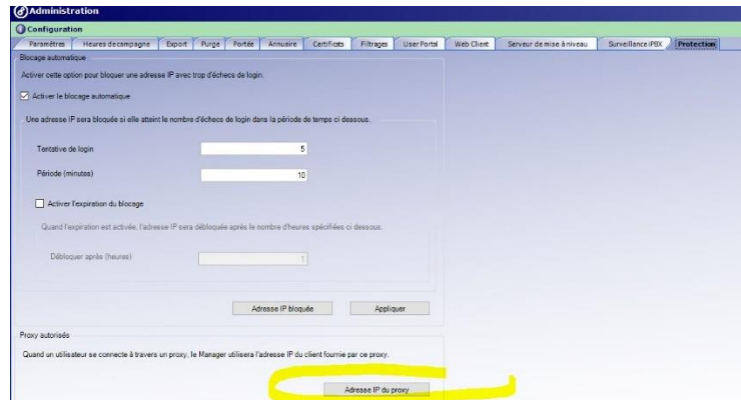
9.2.2 PROXY TRUSTED CONFIGURATION

9.2.2.1 Case of Web Client and User Portal on MiVoice 5000 Manager

Configure the MBG IP address in the proxys authorized by the MiVoice 5000 Manager.

Menu **Configuration – Protection** Tab.

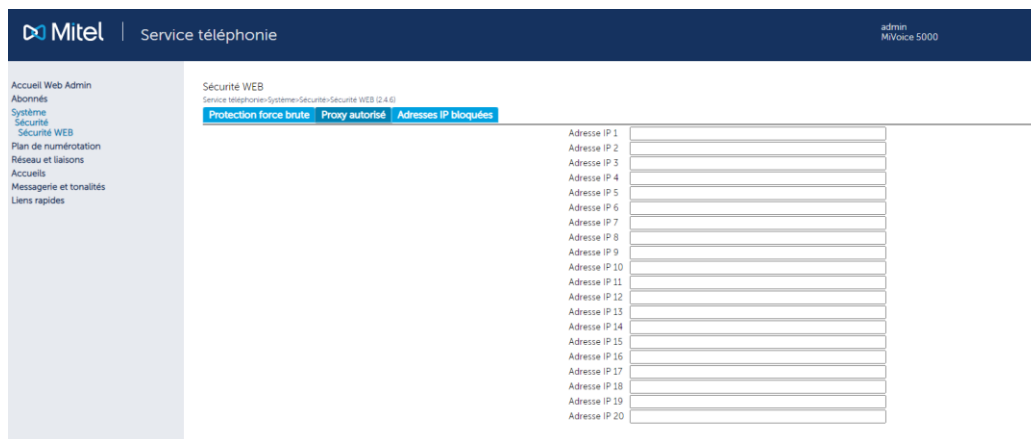
Refer to the document MiVoice 5000 Manager – User Guide



9.2.2.2 Case of the embedded User Portal

In the Web Admin, menu **Telephony service>System>Security>WEB security**, **Proxy authorized** tab:

- Enter the address(es) of the MBG(s) authorized for access in OTT mode.



10 OTT MODE CONFIGURATION FOR SIP DECT SYSTEM

10.1 INTRODUCTION

Two tools can be used for configuring the SIP-DECT system:

- OM Configurator - Open Mobility Configurator,
- OMP - Open Mobility Management Portal.

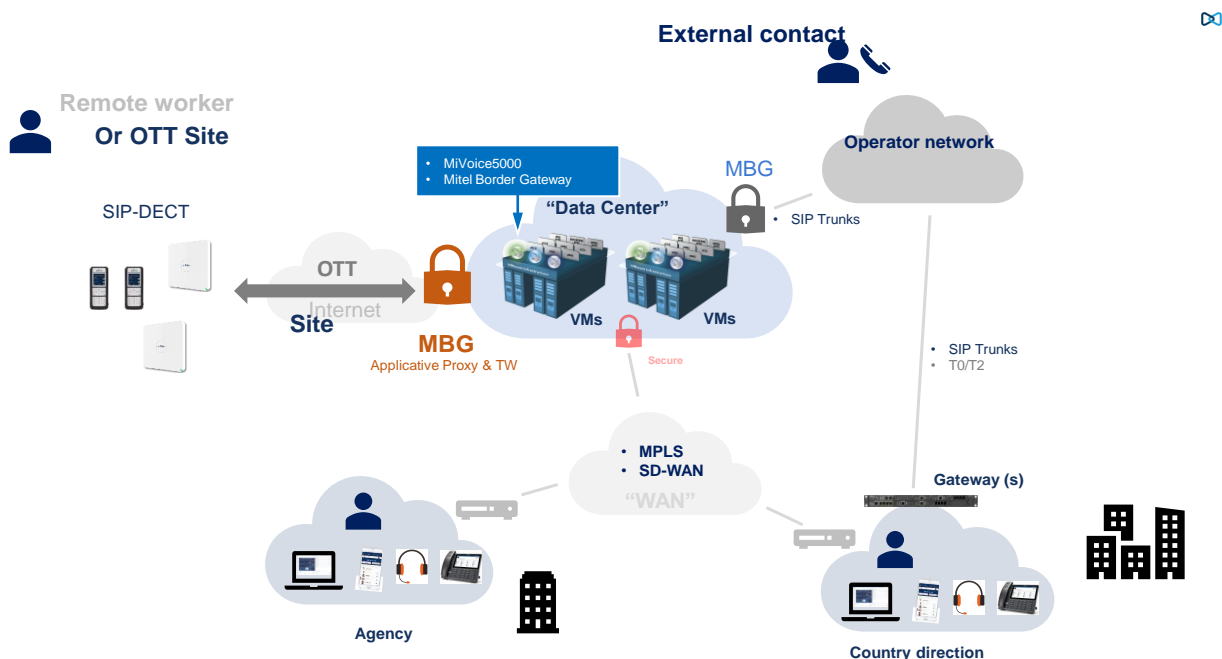
Tools available on the Mitel website:

MiAccess>Software Download Center>SIP DECT>Mitel SIP DECT>Release 8.x SP? menu:

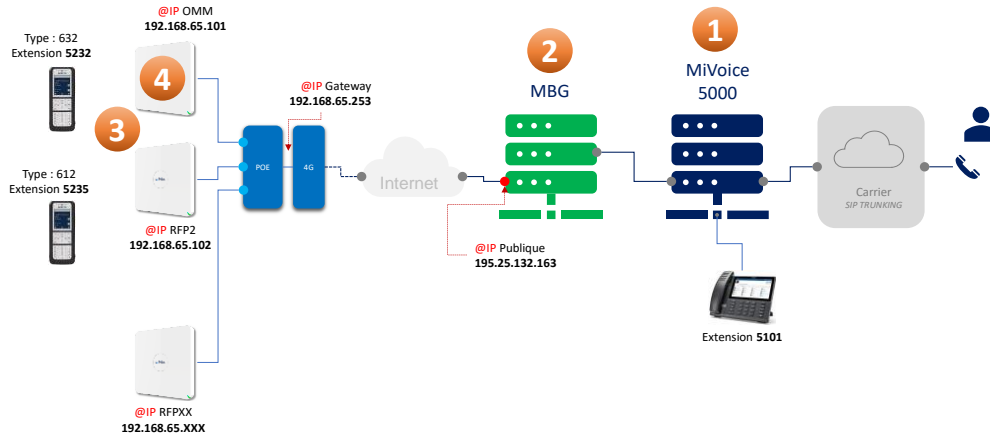
```

iprpf3G.dnld
iprpf4G.dnld
OM_Configurator_Installer_SIP-DECT_8.3.exe
OMCFG_Runtime_Image_Linux.tar.gz
OMCFG_Runtime_Image_Win.zip
OML.war
OMP_Installer_SIP-DECT_8.3.exe
OMP_Runtime_Image_Linux.tar.gz
OMP_Runtime_Image_Win.zip
SIP-DECT.bin
SIP-DECT_CentOS7-B201130_210912.tar.gz
SIP-DECT-MOM-8.3SP1_GI15-0.i686.rpm
  
```

10.2 ARCHITECTURE



Configuration example



10.3 MIVOICE 5000 CONFIGURATION

Declare the considered subscribers.

Refer to the documents:

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

10.4 CONFIGURATION MBG

Menu **MBG>System>Settings>SIP Options**

SIP options

<p>SIP support</p> <p>Protocols: UDP <input type="checkbox"/> TCP <input checked="" type="checkbox"/> TCP/TLS <input checked="" type="checkbox"/></p> <p>Access profile: Public</p> <p>Certificate: Mitel</p> <p>Export root cert ?</p>	<p>Device ↔ device local streaming <input type="checkbox"/></p> <p>Device ↔ trunk local streaming <input type="checkbox"/></p> <p>Codec support: Unrestricted</p>
<p>Set-side RTP security</p> <p>Inbound: <input type="radio"/> SRTP only <input checked="" type="radio"/> SRTP or RTP <input type="radio"/> RTP only</p> <p>Outbound: <input type="radio"/> SRTP only <input checked="" type="radio"/> AVP+crypto <input type="radio"/> RTP only</p> <p>Preferred cipher: AES_CM_128_HMAC_SHA1_80</p>	<p>PRACK support</p> <p>Send options keepalives: Always</p> <p>Options interval: 180</p> <p>Challenge methods: Invite, Subscribe, Refer, Prack</p>
<p>ICP-side RTP security</p> <p>Inbound: <input type="radio"/> SRTP only <input checked="" type="radio"/> SRTP or RTP <input type="radio"/> RTP only</p> <p>Outbound: <input type="radio"/> SRTP only <input checked="" type="radio"/> AVP+crypto <input type="radio"/> RTP only</p> <p>Preferred cipher: AES_CM_128_HMAC_SHA1_80</p>	<p>Registration Mode</p> <p>Set-side registration expiry time: 240</p> <p>ICP-side registration expiry time: Add another</p> <p>Allowed URI names: fvoip.mitel.com</p> <p>Blank any field you no longer want.</p>
<p>Tone Injection</p> <p>Enable <input type="checkbox"/></p>	<p>SIP adaptation support</p> <p>SIP adaptation receive pipeline: ChangeSendonlyToSendrecv</p> <p>SIP adaptation send pipeline: [dropdown]</p>
<p>Permit weak SIP passwords <input type="checkbox"/></p>	

Menu MBG> TeleWorking> SIP

Manage SIP profile

Profile

Enabled ☒

Description plharidon 4474

Set-side Authentication

Username plharidon

Password

Change password

Confirm

Protocol

PRACK support Use global setting

Options keepalives Use global setting

Heartbeat interval

Challenge methods Use primary setting

Override

Set-side RTP security

Inbound Use global setting

Outbound Use global setting

Preferred cipher Use global setting

Connection

Configured ICP my5k-site5

Availability Everywhere

ICP-side Authentication

Username 4474

Password

Change password

Confirm

Media

Local streaming between device calls Use global setting

Codec support Use global setting

Tone Injection

Enable ☐

ICP-side RTP security

Inbound Use global setting

Outbound Use global setting

Preferred cipher Use global setting

10.5 CONFIGURATION WITH OM CONFIGURATOR

This simple tool allows:

- The discovery of the terminals connected to the same network as his PC
- The initial configuration of the RFP terminals (IP address, mask, gateway, etc.)
 - Default login: **omm / omm**
 - Password : XXXX

OM CONFIGURATION / RFP 1 / OMM

Mitel

General Help

	MAC address	local config	IP address	Net mask	Router	OMM address	2nd OMM addr.	TFTP server	TFTP file name	Tasks
<input checked="" type="checkbox"/>	08:00:07:04:12:86	<input checked="" type="checkbox"/>	192.168.65.102	255.255.255.0	192.168.65.253	192.168.65.101	-	0.0.0.0	unused	<div>Scan</div> <div>Add RFP</div> <div>Clear List</div>

Options

General

User directory Jvc - VNA Networks Corporation\Documents\jvc

Network interface 1940\Ethernet Connection (1) 019-LAP

OK Cancel

Mitel

General Help

Detail Data 08:00:07:04:12:86

General OpenMobility Other

Use local config ☒

IP Address 192.168.65.101

Net Mask 255.255.255.0

Router 192.168.65.253

Detail Data 08:00:07:04:12:86

General OpenMobility Other

OMM address 192.168.65.101

2nd OMM address 0.0.0.0

TFTP server address 0.0.0.0

TFTP file name unused

Syslog server address

Syslog server port

DNS addresses 192.168.65.253

RFP configuration file server

Tasks

Scan

Add RFP

Clear List

Edit configuration

Copy Configuration

Paste Configuration

Send Configuration

Factory Reset

Remove selected RFP

Save RFP Config

Load RFP Config

10.6 OMP CONFIGURATION (OPEN MOBILITY PORTAL)

This advanced tool allows the configuration of the SIP-DECT system

- Default login: **omm** / **omm**
- Password: XXXX



Mitel

Login

System name: SR-FR-MIVB

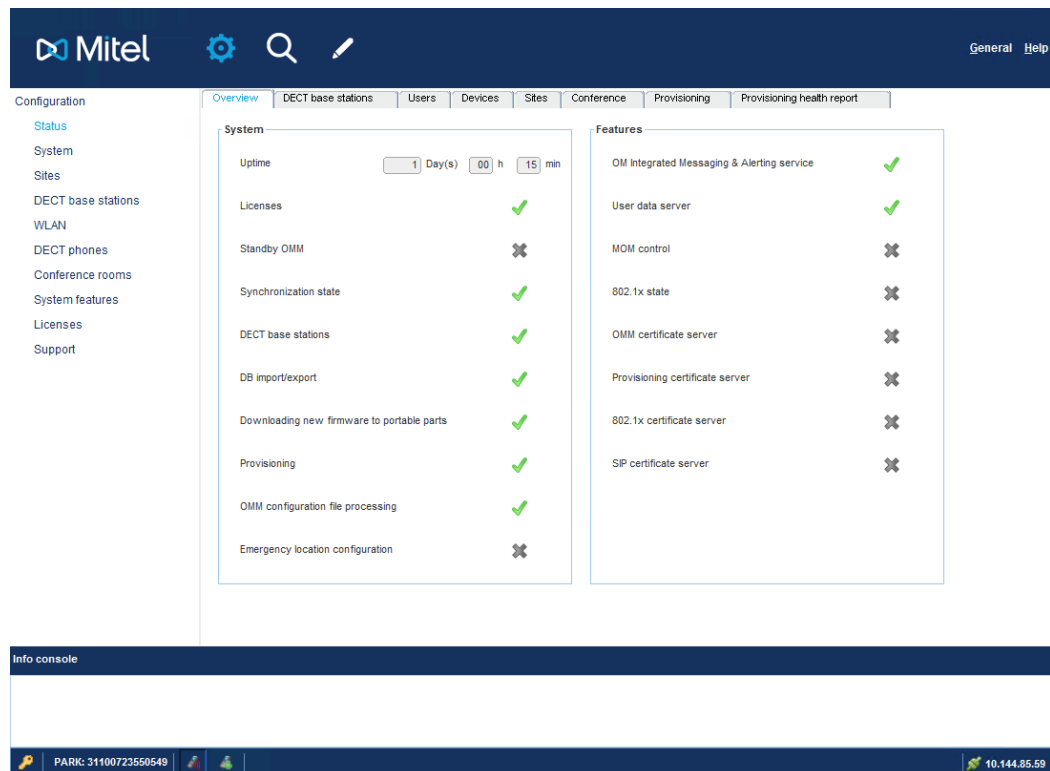
IP address: 192.168.65.101

User name: omm

Password: *****

OK Exit

OMP STATUS



Mitel

General Help

Configuration Overview DECT base stations Users Devices Sites Conference Provisioning Provisioning health report

Status

System

Sites

DECT base stations

WLAN

DECT phones

Conference rooms

System features

Licenses

Support

System

Uptime: 1 Day(s) 00 h 15 min

Licenses: ✓

Standby OMM: ✗

Synchronization state: ✓

DECT base stations: ✓

DB import/export: ✓

Downloading new firmware to portable parts: ✓

Provisioning: ✓

OMM configuration file processing: ✓

Emergency location configuration: ✗

Features

OM Integrated Messaging & Alerting service: ✓

User data server: ✓

MOM control: ✗

802.1x state: ✗

OMM certificate server: ✗

Provisioning certificate server: ✗

802.1x certificate server: ✗

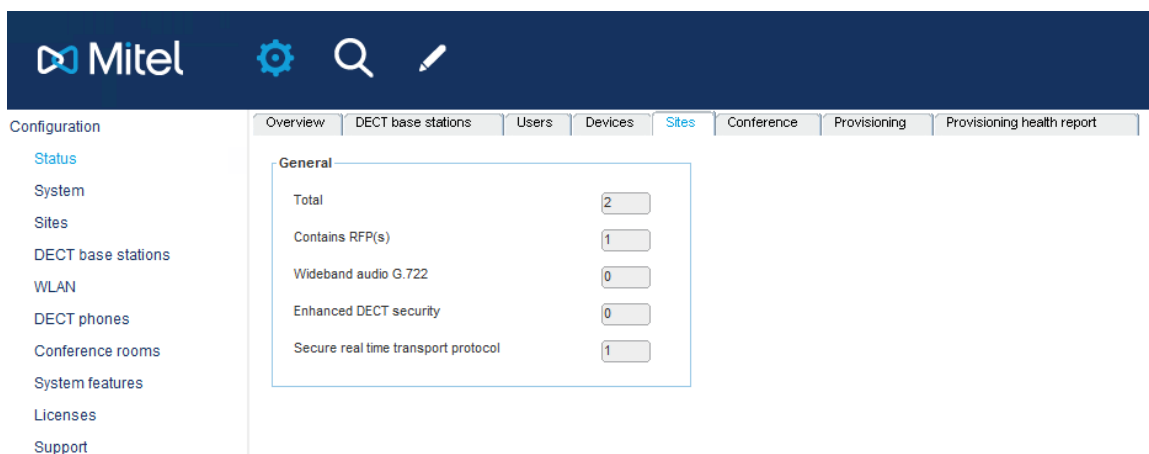
SP certificate server: ✗

Info console

PARK: 31100723550549

10.144.85.59

OMP - SITES



Mitel

Overview DECT base stations Users Devices Sites Conference Provisioning Provisioning health report

Configuration

Status

System

Sites

DECT base stations

WLAN

DECT phones

Conference rooms

System features

Licenses

Support

General

Total: 2

Contains RFP(s): 1




Wideband audio G.722: 0

Enhanced DECT security: 0

Secure real time transport protocol: 1

BASIC SETTINGS 1/2

Mitel



GeneralHelp

Configuration

Status

System

Basic settings

Advanced settings

SIP

Provisioning

User administration

Data management

Sites

DECT base stations

WLAN

DECT phones

Conference rooms

System features

Licenses

Support

DTMF settings

Intercom/Push-to-talk

Supplementary services

Conference

Security

Basic settings

Advanced settings

Registration traffic shaping

Backup settings

RTP settings

General

Proxy server

195.25.132.163

Proxy port

5061

Registrar server

195.25.132.163

Registrar port

5061

Registration period

60

sec

Globally routable user agent URL

☒

Outbound proxy server

Outbound proxy port

5061

Transport protocol

Persistent TLS

Local port range

PP user UDP/TCP

5060

...

5060

Conference room UDP/TCP

4060

...

4060

PP user TLS

5061

...

5061

Conference room TLS




4061

...

4061

BASIC SETTINGS 1/2

Mitel



Configuration

Status

System

Basic settings

Advanced settings

SIP

Provisioning

User administration

Data management

Sites

DECT base stations

WLAN

DECT phones

Conference rooms

System features

Licenses

Support

DTMF settings

Intercom/Push-to-talk

Supplementary services

Conference

Security

Basic settings

Advanced settings

Registration traffic shaping

Backup settings

RTP settings

General

Proxy server

195.25.132.163

Proxy port

5061

Registrar server

195.25.132.163

Registrar port

5061

Registration period

3600

sec

Globally routable user agent URL

☒

Outbound proxy server

Outbound proxy port

5061

Transport protocol

Persistent TLS

Local port range

PP user UDP/TCP

5060

...

5060

Conference room UDP/TCP

4060

...

4060

PP user TLS

5061

...

5061

Conference room TLS

4061

...

4061

OMP – RFP SETTING

Mitel

Configuration: DTMF settings, Intercom.Push-to-talk, Supplementary services, Conference, Security

Status: Basic settings, Advanced settings, SIP, Provisioning, User administration, Data management

Sites: DECT base stations, WLAN, DECT phones, Conference rooms, System features, Licenses, Support

RTP settings

- RTP port base: 16320
- Preferred codec 1: G.722
- Preferred codec 2: G.711-u-law
- Preferred codec 3: G.711-A-law
- Preferred codec 4: G.729-A
- Preferred packet time: 20 msec
- Silence suppression: ☐
- Receiver precedence on codec negotiation: ☐
- Eliminate comfort noise packets: ☐
- Single codec reply in SDP: ☐
- Source port filter: ☐

OMP – GENERAL 1/2

Mitel

Configuration: Branding image URL, OMM certificate server, 802.1x certificate server, SIP certificate server

Status: System credentials, Event trigger, User data import, Software update URL, IMA

System: General, System update, Provisioning certificates, Provisioning certificate server

Provisioning URL

- Active: ☐
- Protocol: HTTPS
- Port: Use default port: ☒
- Server:
- Path: /pdect.cfg, /<MAC>.cfg, /<PARK>.cfg ...

Security

- Validate certificates: ☒ Allow unconfigured trusted certificates: ☐
- Validate expires: ☒ Import certificates with first connection: ☐
- Validate host name: ☒ TLS version: Auto
- Security level: High

OMP – GENERAL 2/2

Mitel

Configuration: Branding image URL, OMM certificate server, 802.1x certificate server, SIP certificate server

Status: System credentials, Event trigger, User data import, Software update URL, IMA

System: General, System update, Provisioning certificates, Provisioning certificate server

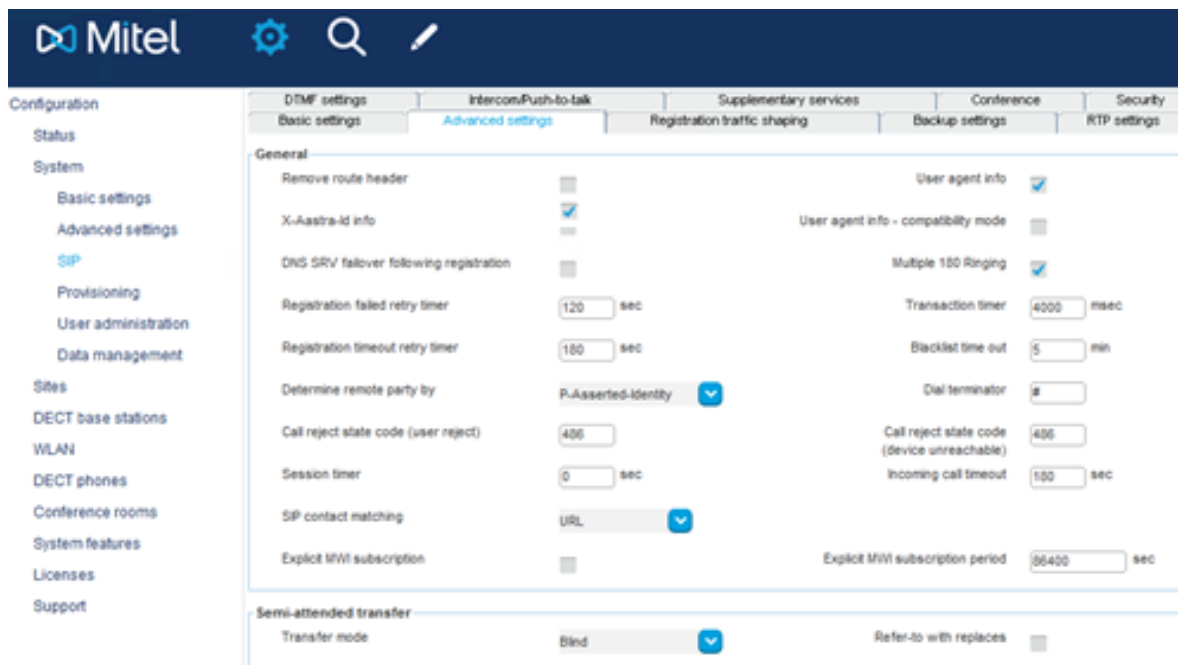
Provisioning URL

- Active: ☐
- Protocol: HTTPS
- Port: Use default port: ☒
- Server:
- Path: /pdect.cfg, /<MAC>.cfg, /<PARK>.cfg ...

Security

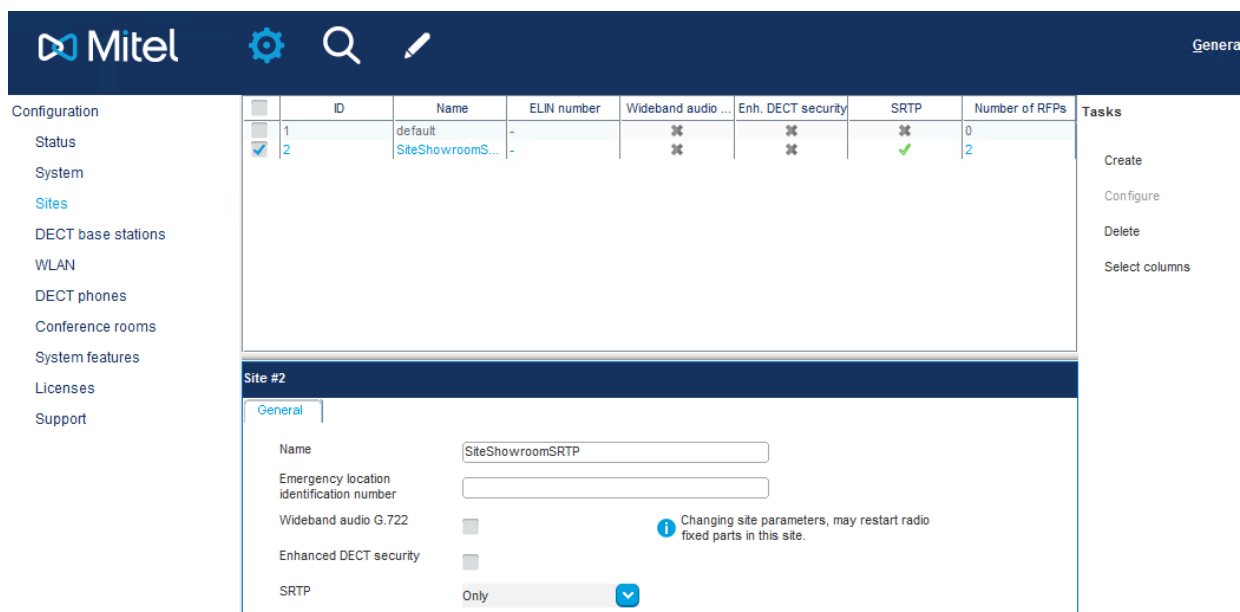
- Validate certificates: ☒ Allow unconfigured trusted certificates: ☐
- Validate expires: ☒ Import certificates with first connection: ☐
- Validate host name: ☒ TLS version: Auto
- Security level: High

OMP – ADVANCED SETTINGS



Check the **X-Aastra-id info** box, having imperatively carried out a DECT-IP pre-assignment on the subscriptions concerned on the MiVoice 5000 side.

OMP - SITES



ID	Name	ELIN number	Wideband audio ...	Enh. DECT security	SRTP	Number of RFPs
1	default	-				0
2	SiteShowroomS...	-			✓	2

Site #2

General

Name: SiteShowroomSRTP

Emergency location identification number:

Wideband audio G.722: ☐

Enhanced DECT security: ☐

SRTP: Only

Changing site parameters, may restart radio fixed parts in this site.

OMP - SITES & BASE STATIONS 1/2

General

- Configuration
- Status
- System
- Sites
- DECT base stations
 - Device list
- Paging areas
- Capturing
- Enrolment
- Export
- WLAN
- DECT phones
- Conference rooms
- System features
- Licenses
- Support

<input type="checkbox"/>	RFP ID	Name	MAC address	IP address	DECT cluster	Paging area	HW type	Connection state	Active	Tasks
<input type="checkbox"/>	0x000	OMM RFP 1	08:00:0F:C4:3E:C1	10.144.85.59	1	0	RFP 48	✓	✓	Create Configure Delete Re-enrollment Filter Select columns
<input type="checkbox"/>	0x001		08:00:0F:E0:12:BB	10.144.85.60	1	0	RFP 48	✓	✓	

OMP - SITES & BASE STATIONS 2/2

General

- Configuration
- Status
- System
- Sites
- DECT base stations
 - Device list
- Paging areas
- Capturing
- Enrolment
- Export
- WLAN
- DECT phones
- Conference rooms
- System features
- Licenses
- Support

<input type="checkbox"/>	RFP ID	Name	MAC address	IP address	DECT cluster	Paging area	HW type	Connection state	Active	Tasks
<input checked="" type="checkbox"/>	0x000	OMM RFP 1	08:00:0F:C4:3E:C1	10.144.85.59	1	0	RFP 48	✓	✓	Create Configure Delete Re-enrollment Filter Select columns
<input type="checkbox"/>	0x001		08:00:0F:E0:12:BB	10.144.85.60	1	0	RFP 48	✓	✓	

DECT base station #0x000

General
DECT
WLAN
Hardware

Name
OMM RFP 1

MAC address
08:00:0F:C4:3E:C1

Emergency location identification number

Site
SiteShowroomSRTP

Building

Floor

Room

Conference channels

OMP - DECT PHONES 1/2

General

Configuration
Status
System
Sites
DECT base stations
WLAN
DECT phones
Overview
Users
Devices
Conference rooms
System features
Licenses
Support

	Device ID	IPEI	Name	Number/SIP user name	User ID	User rel. type	Active
<input type="checkbox"/>	0x001	03596 0014757 6	DECT 5235	5235	0x001	Fixed	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0x002	10345 0934132 *	DECT 5232	5232	0x002	Fixed	<input checked="" type="checkbox"/>

Device #0x002 - User #0x002

Additional services
User monitoring
Configuration data
User service
Key lock

General
SIP
Incoming calls
Conference
DECT
Messaging
Locating

Authentication user name
Password
Password confirmation
VIP
☐
Used for visibility checks
☐
Fixed port
Calculated port

Create

Configure

Delete

Filter

Subscription

Wildcard subscription

Select columns

Change rel. type

OMP - DECT PHONES 2/2

General

Configuration
Status
System
Sites
DECT base stations
WLAN
DECT phones
Overview
Users
Devices
Conference rooms
System features
Licenses
Support

	User ID	Name	Number/SIP user name	Login/Add ID	User rel. type	Rel. device ID	Active
<input type="checkbox"/>	0x001	DECT 5235	5235		Fixed	0x001	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	0x002	DECT 5232	5232		Fixed	0x002	<input checked="" type="checkbox"/>

User #0x002

Additional services
User monitoring
Configuration data
User service
Key lock

General
SIP
Incoming calls
Conference
Messaging
Locating

Name
Number/ SIP user name
Description 1
Description 2
Login/Additional ID
PIN
PIN confirmation

Create

Configure

Delete

Filter

Select columns

10.7 CONFIGURATION OF XML ACCESS FOR REMOTE WORKER DECT SIP IN OTT MODE

10.7.1 PRINCIPLE

A DECT SIP Remote Worker subscriber in OTT mode must be detected by the MiVoice 5000 as a Remote Worker.

During deployment, it is therefore necessary to provide the OMM with the access key (hash) delivered at the level of the MiVoice 5000 to fill in the URLs relating to the proven XML functionalities (list of callers, redial list, server menu , the feature access code).

This action is to be carried out in two steps:

- At the MiVoice 5000 WebAdmin level: Retrieve the hash value indicating the path for downloading the files concerning the Remote Workers.
- At OMM level: Fill in the hash key value for features requiring XML access.
- Open access to MiVoice 5000 directories.

10.7.2 CONFIGURATION

- MiVoice 5000 level hash key recovery

Telephony service menu>Network and links>Quality of service>Encryption and IP parameters (4.4.5) – Encryption tab:

Copy and save the indicated value of the hash (only) in the field - Path for downloading files.



IMPORTANT : The hash value is the one indicated on the left of the field, before /ftp_67xx. In the example 0d0f346508a57b37223efe61265db3c7.

Configuring the OMM level access URL

From the OMM operating interface

Configuration menu>System features>XML applications

Configuration	ID	Name	Server	Active
Status	0	Caller list	SIPProxy	✓
System	1	Redial list	SIPProxy	✓
System	2	Presence		✗
Sites	3	Server menu	SIPProxy	✓
DECT base stations	4	Action URI		✗
WLAN	5	Feature access codes	SIPProxy	✓
DECT phones	6	Call completion		✗
Conference rooms	7	Park call		✗
System features	8	Unpark call		✗
General settings	9	Pickup		✗
Feature access codes	10	Take		✗
Alarm triggers	11	Call forward		✗
Digit treatment	12	Call routing		✗
Directory	13	Call protection		✗
Directory (comp. mode)	14	Voice box		✗
XML applications	15	Hotkey		✗

- Enter the hash value at the beginning of the field relative to Path (and parameters) access URL.

Configuration	ID	Name	Server	Active
<input checked="" type="checkbox"/>	0	Caller list	SIPProxy	✓
<input type="checkbox"/>	1	Redial list	SIPProxy	✓
<input type="checkbox"/>	2	Presence		✗
<input type="checkbox"/>	3	Server menu	SIPProxy	✓
<input type="checkbox"/>	4	Action URI		✗
<input type="checkbox"/>	5	Feature access codes	SIPProxy	✓
<input type="checkbox"/>	6	Call completion		✗
<input type="checkbox"/>	7	Park call		✗
<input type="checkbox"/>	8	Unpark call		✗
<input type="checkbox"/>	9	Pickup		✗

XML application #0

General

Active ☒

Name

Protocol

Port Use default port ☐

Server

User name

Password

Password confirmation

Path (and parameters)

The same Hash key must be entered in the different URLs depending on the functionality:

- Caller list: %HASH CODE%/omm.mghc/?key=20&na={number}
- Redial list: %HASH CODE%/omm.mghc/?key=18&na={number}
- Server menu: %HASH CODE%/omm.mghc/?key=0&na={number}
- Feature access codes: %HASH CODE%/omm.mghc/?key=0&na={number}&fac={fac}

Opening access to the MiVoice 5000 directories

Configuration menu>System features>Directory

General tab

Configuration	ID	Type	Active	
Status	1	XML	✓	XML directory
System	2	LDAP	✗	
Sites	3	LDAP	✗	
DECT base stations	4	LDAP	✗	
WLAN	5	LDAP	✗	

Directory entry #1

General

URL

Type

XML

▼

Active

☒

Name

XML directory

Search base

Search type

Surname

▼

Display type

Surname, given name

▼

Server search timeout

10

sec

OK

Cancel

URL tab

Directory entry #1

General

URL

Protocol

HTTPS

▼

Port

4445

Use default port ☐

Server

SIPProxy

User name

Password

Password confirmation

Path (and parameters)

%HASH CODE%/annuaire/5xi.php?dn={number}

Use provisioning security configuration

☐

OK

Cancel

10.8 OMM WEB

Access > https://192.168.65.101

Mitel SIP-DECT 8.0

Login

System SR-FR-MiVB

PARK 1F103A768B

User name omm

Password *****

OK

Mitel SIP-DECT 8.0 Advanced

Status

System

Sites

Base Stations

DECT Phones

WLAN

System Features

Licenses

Info

Status

General

OpenMobility Manager SIP-DECT 8.0-HF01D16

Uptime 1 Day, 1:52

Licenses Built-in license for up to 5 DECT base stations

Standby OMM There is no OpenMobility Manager in standby mode configured!

OM Integrated Messaging & Alerting service ✓

Base Stations

Total number 2

Connected 2

DECT activated 2

DECT currently active 2

DECT clusters 1

WLAN activated 0

DECT Phones

Total number 2

Subscribed 2

Subscription allowed ✗

Activate firmware update ✓

Loading firmware from Internal

Firmware version [650.602: 7.2] - [602v2: 7.2]

Number of known downloadable DECT phones 1

Number of already updated DECT phones 1

Mitel SIP-DECT 8.0 Advanced OMP

Status

System

System Settings

Provisioning

SIP

User

Administration

Time Zones

SNMP

DB Management

Event Log

Sites

Base Stations

DECT Phones

WLAN

System Features

Licenses

Info

System Settings

OK

Cancel

General settings

System name SR-FR-MiVB

Remote access ☐

Tone scheme FR

DECT settings

PARK 1F103A768B (31100723550549)

DECT power limit 100mW ☐

Encryption ☒

Restrict subscription duration ☐

Authenticate before ciphering ☐

DECT monitor ☐

Regulatory domain EMEA When changing the DECT regulatory doma

DECT authentication code 78280

DECT phone user login type Number

Preserve user device relation at DB restore ☐

WLAN settings

Regulatory domain FR When changing the WLAN regulatory doma

Dynamic Frequency Selection ☐

QoS settings

ToS for voice packets B8

ToS for signalling packets B8

TTL (Time to live) 32

DECT base stations update

Mode One by one

Mitel

SIP-DECT 8.0

Advanced

Status

System

System Settings

Provisioning

SIP

User

Administration

Time Zones

SNMP

DB Management

Event Log

Sites

Base Stations

DECT Phones

WLAN

System Features

Licenses

Info

OK

Cancel

Basic settings

Proxy server

195.25.132.163

Proxy port

5061

Registrar server

195.25.132.163

Registrar port

5061

Registration period

5000

sec

Outbound proxy server

5061

Outbound proxy port

5061

Transport protocol

Persistent TLS

Local UDP/TCP port range

5060

5060

Local TLS port range

5061

5061

Advanced

Explicit MMI subscription

Explicit MMI subscription period

86400

sec

User agent info

User agent info - compatibility mode

Dial terminator

#

Registration failed retry timer

120

sec

Registration timeout retry timer

180

sec

Session timer

0

sec

Transaction timer

4000

msec

Backlist time out

5

min

Incoming call timeout

180

sec

Determine remote party by

P-Asserted-identity

header

Multiple 180 Ringing

Semi-attended transfer mode

Blind

Mitel

SIP-DECT 8.0

Advanced

Status

System

Sites

Base Stations

DECT Phones

WLAN

System Features

Licenses

Info

New

2 Sites

ID

Name

Hi-Q audio technology

SRTP

Enhanced DECT security

1	default	X	X	X
2	SiteShowroomSRTP	X	✓	X

Configure site

When changing site options DECT base stations in this site may be reset.

Site settings

ID

2

Name

SiteShowroomSRTP

Hi-Q audio technology

SRTP

Only

Enhanced DECT security

Mitel

SIP-DECT 8.0

Advanced

OMP

Status

System

Sites

Base Stations

DECT Cluster 1

DECT Phones

WLAN

System Features

Licenses

Info

New

Base Stations

Capturing unconfigured DECT base stations

Stop

2 Base Stations

DECT Cluster 1 2 Base Stations

ID

Name

MAC address

IP address

HW type

Site

RPN

Reflective environment

0000	OMM RFP 1	08-00-0F-C4-3E-C1	10.144.85.59	RFP 48	2	00	X
0001	-	08-00-0F-E3-12-08	10.144.85.50	RFP 48	2	01	X

DECT Phones

New

Import

Search

Subscription

Start

Wildcard subscription

2 min

Start

1 - 2 (2) DECT Phones

Display name

Number/SIP user name

IPEI

DECT 5232	5232	10345 0934132 *
DECT 5235	5235	03586 0014757 6

Status

System

Sites

Base Stations

DECT Phones

WLAN

System Features

Digit Treatment

Directory

Directory (comp. mode)

Feature Access Codes

XML Applications

Licenses

Info

Directory

Order	ID	Type	Name	Server
1		LDAP		
2		LDAP		
3		LDAP		
4		LDAP		
5		LDAP		

OpenMobility Manager SIP-DECT 8.0-HF01D116 - Google Chrome

Non sécurisé | https://10.144.85.59/directory_conf.html?u16=0&u14=0

Configure directory entry

Directory

Active

Type

Name

Search base

Search type

Display type

Server search timeout

Protocol

Port

Server

User name

Password

Password confirmation

Path (and parameters)

Use common certificate configuration

OK

Cancel

Status

System

Sites

Base Stations

DECT Phones

WLAN

System Features

Licenses

Info

Licenses

Changing these settings may cause the OpenMobility Manager to be reset.

OK

Cancel

Licenses

License settings

Installation ID

License file import

General

System

Messaging

Locating