Remote Worker via MBG

07/2023 AMT/PTD/PBX/0161/3/4/FR MANUEL DE MISE EN ŒUVRE

🔀 Mitel

Avertissement

Bien que les informations contenues dans ce document soient considérées comme pertinentes, Mitel Networks Corporation (MITEL ®) ne peut en garantir l'exactitude.

Les informations sont susceptibles d'être modifiées sans préavis et ne doivent pas être interprétées de quelque façon que ce soit comme un engagement de Mitel, de ses entreprises affiliées ou de ses filiales.

Mitel, ses entreprises affiliées et ses filiales ne sauraient être tenus responsables des erreurs ou omissions que pourrait comporter ce document. Celui-ci peut être revu ou réédité à tout moment afin d'y apporter des modifications.

Aucune partie de ce document ne peut être reproduite ou transmise sous une forme quelconque ou par n'importe quel moyen - électronique ou mécanique – quel qu'en soit le but, sans l'accord écrit de Mitel Networks Corporation.

© Copyright 2023, Mitel Networks Corporation. Tous droits réservés.

Mitel ® est une marque déposée de Mitel Networks Corporation.

Toute référence à des marques tierces est fournie à titre indicatif et Mitel n'en garantit pas la propriété.

SOMMAIRE

1	INTRO	DUCTION	5
	1.1		5
	1.2	DOCUMENTS DE REFERENCE	5
	1.5	RESTRICTIONS	5
2	ARCHI	TECTURE GÉNÉRALE	6
2	PRINC		7
л Л	SVNTH	IÈSE DES DIFFÉRENTES ÉTADES DOUR LE DÉDI OIEMENT DES REMOTE WORKERS	. /
5	CONFL	GURATION GÉNÉRIQUE	10
Ŭ	5 1		10
	5.2	GÉNÉRATION DE LA CLÉ HASH	11
	5.3	CONFIGURATION DU POSTE DISTANT POUR L'ACCÈS À L'IPBX DE RATTACHEMENT MIVOI	CE
		5.3.1 UTILISATION D'UN SERVEUR RCS	12
		5.3.2 CONFIGURATION DE L'URL DIRECTEMENT SUR LE POSTE	13
	5.4		14 45
		5.4.1 LICENCES	15
		5.4.3 REDÉMARRAGE DU MBG	16
		5.4.4 CONFIGURATION AU POINT D'ACCÈS IP DE MIVOICE 5000	17
		5.4.5 PARAMETRAGES SIP COMMUNA TOUS LES POSTES REMOTE WORKER	18 X19
	5.5	CONFIGURATION DU MBG EN WHITE LIST	28
	5.6	CONFIGURATION DE L'APPLICATION TMA (SERVICE POSTES)	29
_	5.7	DEFINITION DES SERVEURS DE TELECHARGEMENT POUR LES REMOTE WORKERS	30
6	PREPA		32
	6.1	DÉCLARATION DES EQUIPEMENTS SIP (POSTES 6800 SIP ET 6900 IP PHONES)	32
		6.1.2 CAS D'UN MBG EMBARQUÉ OU EN MODE CLUSTER AVEC MICOLLAB	3∠ 33
	6.2	CONFIGURATION SPÉCIFIQUE D'UN SOFTPHONE CLIENT MICOLLAB	34
	6.3	PRÉPARATION DU FICHIER CSV REMOTE WORKER À PARTIR DU FICHIER PROVISIONNING) 26
	6.4	GENERIQUE GESTION DES POSTES REMOTE WORKER PAR TMA	30 39
		6.4.1 PRÉREQUIS	39
	6.5	6.4.2 DÉPLOIEMENT À PARTIR DU SERVEUR DU TÉLÉCHARGEMENT	39
_	0.5		40
7	DEPLC	DIEMENT DES POSTES REMOTE WORKER	41
	7.1	CONFIGURATION DE L'IPBX DE RATTACHEMENT POUR CHAQUE POSTE REMOTE WORKEI	२ ⊿1
		7.1.1 AVEC RCS	41
		7.1.2 SANS SERVEUR RCS	42
8	CONFI	GURATION DES NUMÉROS D'URGENCE POUR LES REMOTE WORKERS FIXES	43
	8.1 8.2		43 44
9	CONFI	GURATION DU MODE OTT POUR LES ACCÈS AUX APPLICATIONS WEB CLIENT ET USER	
PO	RTAL		46
	9.1	PRINCIPE	46
	9.2	SYNTHESE DES DIFFÉRENTES ÉTAPES	48 49
		9.2.2 CONFIGURATION DU TRUSTED PROXY	+o 49
10	CONFI	GURATION DU MODE OTT POUR LE SYSTÈME SIP DECT	50
	10.1		50
	10.1		50

10.2	ARCHITECTURE	50
10.3	CONFIGURATION MIVOICE 5000	51
10.4	CONFIGURATION MBG	51
10.5	CONFIGURATION AVEC OM CONFIGURATOR	52
10.6	CONFIGURATION OMP (OPEN MOBILITY PORTAL)	53
10.7	CONFIGURATION DES ACCÈS XML POUR REMOTE WORKER DECT SIP EN MODE OTT	59
	10.7.1 PRINCIPE	59
	10.7.2 CONFIGURATION	59
10.8	OMM WEB	62

1 INTRODUCTION

1.1 **DÉFINITION**

Cluster : Système téléphonique de la famille MITEL MiVoice 5000 composé de systèmes physiques (Mitel 5000 Gateways, Mitel 500, MiVoice 5000 Server ou C2IC) ou virtualisés (MiVoice 5000 Server) reliés à un MiVoice 5000 Server central, appelé Cluster Server.

Cluster Server : Système MiVoice 5000 Server physique ou virtualisé dédié au pilotage global du Cluster. Ce système peut être dupliqué.

1.2 **DOCUMENTS DE RÉFÉRENCE**

Les documents associés sont disponibles sur le site Mitel.com.

1.3 **GLOSSAIRE**

- MBG : MiVoice Border Gateway
- RCS : Redirection & Configuration Server
- AMC : Applications Management Center Serveur de licence
- ICP : IP Communication Platform (iPBX)

1.4 **RESTRICTIONS**

La fonctionnalité Remote Worker décrite dans ce document s'applique uniquement aux terminaux MiVoice 6800 SIP et 6900 IP phones.

ARCHITECTURE GÉNÉRALE

Exemple d'architecture :

2



Le but est pour un poste 6800 SIP ou 6900 IP phone installé à distance d'avoir quasiment les mêmes fonctionnalités qu'un poste du même type, installé dans le réseau local de l'entreprise.

La connexion du poste distant relié à Internet est routée ensuite via un MBG au réseau local.

Le MBG permettant d'associer l'adresse publique à l'adresse locale de l'iPBX, le poste récupérant ses fichiers de configuration se comporte comme un poste local au site.

Le MBG peut être selon l'architecture :

- Un équipement externe autonome localisé dans la DMZ,
- Intégré (embarqué) dans le serveur MiCollab,
- En Cluster avec MiCollab dans le réseau local,

Son provisionning est assuré selon l'architecture :

- Soit manuellement (MBG Stand alone)
- Soit par le serveur MiCollab.

Lorsque le MiV5000 provisionne un serveur MiCollab situé dans la DMZ, le firewall doit autoriser notamment l'accès au MiV5000.

La résolution des noms de domaine du MBG est assurée par un serveur DNS public.

Une sécurisation est réalisée à partir d'une clé générée dans l'iPBX et est intégrée au chemin d'accès de l'URL permettant aux postes de télécharger leurs configurations.

En configuration multisite, le MBG ne peut se connecter qu'à un seul iPBX MiVoice5000, tous les postes Remote worker devront être déclarés sur cet iPBX.

3 PRINCIPE DE DÉPLOIEMENT

Opérations préalables :

L'URL publique à atteindre est renseignée soit par configuration manuelle au niveau des postes Remote worker soit en utilisant un serveur RCS.

Le poste se connecte, suite à un Factory reset, à l'URL cryptée permettant le déploiement.

Le poste télécharge les fichiers de configuration issus de l'iPBX via le MBG. Fichiers de type aastra.cfg, mac.cfg, software.

Le poste redémarre et envoie son REGISTER.



4 SYNTHÈSE DES DIFFÉRENTES ÉTAPES POUR LE DÉPLOIEMENT DES REMOTE WORKERS

La procédure peut être décomposée en trois types d'action :

- Configuration générique à réaliser par l'installateur,
- Préparation au déploiement à réaliser par l'installateur et l'administrateur réseau par poste,
- Déploiement des postes à réaliser par les Remote Workers ou l'administrateur réseau.

L'ordre chronologique suivant est à respecter :

Configuration générique (Chapitre 5)

Configuration du FireWall

Génération de la clé hash sur MiVoice 5000

<u>Déclaration ou non d'un serveur RCS</u> (utilisé pour la configuration des postes distants pour l'accès à l'iPBX de rattachement MiVoice 5000)

Configuration au niveau MBG

- Licence
- Configuration du Profil réseau
- Configuration au point d'accès IP de MiVoice 5000
- Paramétrages SIP commun à tous les postes Remote Worker

Paramétrages complémentaires MBG

Configuration de la connexion/authentification avec un MBG sur MiVoice 5000

Côté Interface MBG : Côté Web admin MiVoice 5000 : Configuration du MBG en white list

Configuration de TMA sur MiVoice 5000

- Configuration de l'application
- Définition et configuration des Serveur de téléchargement pour les postes Remote Workers

Préparation au déploiement (Chapitre 6)

Déclaration des equipements SIP (postes 6800 SIP et 6900 IP phones)

Cas d'un MBG Standalone

Cas d'un MBG embarqué ou en mode Cluster avec MiCollab

Configuration spécifique d'un Softphone client MiCollab

Préparation du fichier csv Remote Worker à partir du fichier Provisionning générique

Gestion des postes Remote Worker par TMA

- Prérequis Préparation du fichier "csv" à partir du fichier provisionning
- Déploiement à partir du serveur de téléchargement :
 - o Prérequis
 - o Déploiement par TMA embarqué
 - o Déploiement par TMA géré à partir MiVoice 5000 manager

Visualisation/Inventaire des postes remote Worker

Déploiement des postes (Chapitre 7)

Configuration du poste distant pour l'accès au serveur de configuration MiVoice 5000

- Utilisation d'un serveur RCS
- sans serveur RCS

Mise en service de poste Remote Worker

Toutes ces étapes sont décrites dans l'ordre et en détail dans les paragraphes suivants.

5 CONFIGURATION GÉNÉRIQUE

5.1 CONFIGURATION DU FIREWALL

Pour permettre le trafic entre le LAN/DMZ vers Internet, la configuration suivante doit être la suivante au niveau des 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

Configuration des ports de l'accès distant (Box)

Les ports doivent être ouverts au niveau du routeur (Box) distants.

En général, aucune configuration n'est à faire car les flux sortants sont naturellement autorisés par les Box.

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 GÉNÉRATION DE LA CLÉ HASH

La clé hash doit être générée par le MiVoice 5000. Elle est ensuite intégrée dans le chemin de la configuration URL.

Cette clé est unique et est contrôlée par le PBX pour permettre au terminal de télécharger les fichiers.

Menu RESEAU ET LIAISONS>Qualité de service>Chiffrement et paramètres IP

→ (€) № https://192.168.100.160/rhm/m5251	/redirect.htm?onglet=4743	nq2 - Mit 🕅 micollab1 - MiCol 🅅 micollab2 -	MiCol 🛛 MiVoice 5000: × 🛛 🏠 だ
chier Edition Affichage Favoris Outils	?		
MILEL Service	téléphonie	MiVoice 5000	۹
cueil Web Admin	Chiffrement et paramètres IP		
onnés	Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres li	P (4.4.5) 👘 🕻 🏷	
tème	paramètres IP et Chiffrement Certificats		
n de numérotation		D0	
eau et liaisons	octet TOS voix (riexa)	88	
Jalité de service hiffroment et paramètres IP	octet TOS signalisation (nexa)	AU	
nimement et parametres ir	priorite VLAN Voix	0	
canaria et tonalités	priorite VLAN signalisation	6	
s rapides	time to live du datagramme IP		
	Chiffrement signalisation et voix		
	état fonction	INTERDIT	
	dates de validité certificat actif :		
	début 09/12/15 14:26		
	fin 08/12/16 14:26		
	nom de l'autorité de certification :		
	192.168.100.160		
	chiffrement inter-iPBX		
	certificat auto signé	V	
	Régéné	ration du certificat	
	Regent		
	Chiffrement voix (iZxx)		
	état fonction	CLEF INEXISTANTE	
	mise à jour le		
	mode de fonctionnement	ESCLAVE V	
	chiffrement		
	chilfrement		
	Paramètres divers		
	nombre d'entrées ARP	256	
	durée de vie d'une entrée APP sec	600	
	officiement des entrées APP	NON	
	enacement des entrees ARP		
	tempo début alarme rés sec	120	
	tempo debut atamienes sec	30	
XL -R6.2 RC /C201 FRA	Génération du bash	NON	
5/16 15:10:59	deneration du nash		
RL INTERSITE ETABLIE 10-0 *			
5/16 15:09:24 BL INTERSITE COUPEE 10-0/0005 *			
5/16 13:25:18			
RL INTERSITE ETABLIE 10-0 *			

• Dans le champ Génération du hash, sélectionner OUI



IMPORTANT : Un message d'avertissement « régénérer le hash va impacter tous les postes Remote worker déployés » est visualisé si l'exploitant demande une régénération du hash.

- Entrer ensuite le mot de passe du compte Webadmin en cours,
- Cliquer sur Confirmation,

Le champ Chemin pour le téléchargement des fichiers : est renseigné en lecture seule.

Le but étant que l'administrateur puisse le copier/coller ensuite dans l'URL d'accès aux fichiers de configuration poste.

5.3 CONFIGURATION DU POSTE DISTANT POUR L'ACCÈS À L'IPBX DE RATTACHEMENT MIVOICE 5000

Comme le poste est déporté, il n'est pas possible de fournir automatiquement l'URL du MBG à atteindre. Deux méthodes sont possibles :

- L'utilisation d'un serveur RCS,
- La configuration de l'URL directement sur le poste à partir de l'interface Web du poste.

Les postes 6900, livrés en sortie usine avec un firmware Minet, doivent être migrés en firmware SIP. Le téléchargement du firmware SIP peut être fait soit au préalable par l'installateur, soit directement via le serveur RCS (pour tous les postes de l'installation, ou unitairement par fichier Mac).

5.3.1 UTILISATION D'UN SERVEUR RCS

Le serveur RCS permet un déploiement simplifié des postes 6800 SIP et 6900 IP phones mais nécessite l'ouverture d'un compte pour y accéder.

5.3.1.1 Ouverture d'un compte d'accès au RCS



Note : Se référer au document relatif à l'ouverture d'un compte RCS.

Redirect Configu	ion & ration Server	
Login		
Usemame:		
Password:		
	Connect Forgot Password?	

Ecran de login au serveur RCS.



5.3.1.2 Configuration de l'accès au serveur de configuration MiVoice 5000 avec serveur RCS

Le service de redirection et configuration (RCS) est un service qui facilite le déploiement des postes 6800 SIP et 6900 IP phones (Se référer à la documentation RCS pour plus de précisions).

URL d'accès au serveur RCS : https://rcs.aastra.com/rcs/login.php

A partir de l'écran d'accueil du RCS

- Dans le menu Servers, indiquer les informations pour atteindre le MBG :
 - Name : Le nom ou l'adresse de l'adresse publique du MBG,
 - URL (Chemin HTTPS) : Le chemin d'accès intégrant :
 - L'hôte représenté soit par le FQDN soit par l'adresse IP publique du MBG et le port associé (4445).
 - la clé hash de l'URL permettant aux postes de télécharger leur fichier de configuration. Voir valeur paragraphe 5.2,

Exemple : https://name_server:4445/hash

• Cliquer sur Save.

DO https://cc.awtra.com/rcs/p.php?inservers D + @ C D0 Med Redirector ×	n * 0
Either Eithen Afflöger Freen Oph I Redirection & Configuration Server Mitel France.R&D Summy Une General Internet	Alouter le pouveau serveur de configuration
Name URL Descripting Descripting Descripting Traverse # 0 AC3514.00 (mil) Imps/less1 int com: 444511725:05406/18795:050978799:034613/bp; 57xii 1 <t< td=""><td>(IPBX): - Name : - URL : https://name_server.4445/hash - Firmware Override : none</td></t<>	(IPBX): - Name : - URL : https://name_server.4445/hash - Firmware Override : none
VML-CS-RW (edit) https://vm-cs-rw.inte/fr4445/93966/f442dha7508305698eccd64b0933htp_67xxi 4	Edit Server: ACS1-LCO
	Name: 22514200 URL: Mtps://west int.com/4445 Brand: Libre V Firmware Override: Hone V
	Save 🎇 Cancel

Firmware override :

- Si l'installation a beaucoup de postes 6900, il est intéressant de migrer automatiquement les postes 6900 de la version Minet en SIP. Cette mise à jour vaudra aussi tant pour les postes 6800 et 6900.

- Prendre un firmware SIP, avec une version minimale 5.0.0.

Il y aura autant d'URL différentes qu'il y a de MiVoice 5000 Server sur lesquelles les Remote workers sont déclarés.



IMPORTANT : Un MBG ne peut être associé qu'à un seul iPBX MiVoice 5000 pour la fonctionnalité Remote Worker.

5.3.2 CONFIGURATION DE L'URL DIRECTEMENT SUR LE POSTE

Se référer au paragraphe 7.1.2.

5.4 **CONFIGURATION DU MBG**

Accès à l'interface MBG

https://mbg_address/server-manager

La configuration au niveau du MBG comporte plusieurs phases :

- Déclaration des licences MBG
- Configuration du profil réseau
 - Menu MiVoice Border Gateway, onglet System configuration>Network profiles
- Redémarrage MBG

Menu MiVoice Border Gateway, onglet System Status

> Configuration du point d'accès IP au MIVOICE 5000

Menu MiVoice Border Gateway, onglet Service Configuration>ICPs

- > Paramétrages SIP communs à tous les postes Remote Worker du MBG
 - Menu MiVoice Border Gateway, onglet System configuration>Settings
- > Paramétrages complémentaires spécifiques Remote Worker
 - Menu Configurations Onglet Overrides.
- > Configuration de la connexion/authentification entre le MBG et l'iPBX.

La plupart des configurations sont identiques quelle que soit l'architecture MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster.

D'autres ne le sont pas et dans ces cas, l'architecture sera reprécisée en début de paragraphe.

Ce chapitre ne décrit la configuration à effectuer côté MBG que pour la fonctionnalité RemoteWorker. Se référer à la documentation du MBG pour plus de précisions sur son utilisation et son administration.

5.4.1 LICENCES

Les licences Teleworkers sont nécessaires pour le MBG.

Menu Menu MiVoice Border Gateway, onglet System>Dashboard

License information					
Availability and usage	License type	Total loca	lTotal 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 Fa	alse			

5.4.2 CONFIGURATION DU PROFIL RÉSEAU



Menu MiVoice Border Gateway, onglet Network>Profiles

- Entrer les valeurs **RTP ICP-side override addresses** : TBC : Adresse du serveur MBG
- Entrer les valeurs **RTP Set-side override addresses** : TBC : Adresse Publique
- Cliquer sur Apply pour la prise en compte des paramètres.
 ICP => IP Communication Platform = MiVoice5000

Redémarrer ensuite le service MBG. Se référer au paragraphe suivant.

5.4.3 REDÉMARRAGE DU MBG

Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster A partir du menu MiVoice Border Gateway, onglet System>Dashboard :

Dans la zone MBG Status :

- Cliquer sur MBG service
- Cliquer sur Stop
- Cliquer sur Start ensuite pour le redémarrage.

Mitel Standard Lin	ux			admin@mbg92fp1.mylab2.loca	
System - Network -	Televolting - 52 th bunking - Remote proxy -	Call recording + Troubleshooting +			
Page underst The Jay 19 2021 14-6	2 17 OVT+122D Insura cibili d'Europa partecial				
Jan. 29, 2021, 9.02 a.m.	Note: Renote provy is not	found in the main 1050 menu indead of the server manager menu on the left.			
April 0, 2021, 0.45 a.m.	Note: As loos streaming in	enabled, you should know that local streaming behaviour has changed in this release. Ple	ase monitor your depoyment and see the NGO documentation to ensure it is working correctly for your environment.		
M03 status					
Network profile	Streaming addresses (IPvd		interface IPs		
Custors mode	Secure 10.145.41.8		WANK IN ARR OF THE		
	Contrast of the second		True		
		MDD service WebRTD News SIP Call recording			
					-
Additional and a second					
	B		h a sa		
	Carrier said / service said	WHEN COMP	100.000	And a start and a start	
	Ocals			(0)	
	0 come				
System metrics.					
				•	
	Lood everage	% CPU	beep.	Diskusepe	
	-			-	
	0.13				
	cores:2	1%	1%	28.7%	
Chattering status					-
+ 100					47
	A	Custered street			

CONFIGURATION AU POINT D'ACCÈS IP DE MIVOICE 5000 5.4.4

Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster

Menu MiVoice Border Gateway, onglet Network>ICPs

Dans la liste proposée, Sélectionner l'iPBX considéré,

Cliquer sur l'icône Crayon (Modification)

ystem +	Netw	VOIK - TEIEW	orking * Simuunking * Remote	proxy • Call recording •	roubleshooting *								Search
updated	: Tue Apr 2	27 2021 14:43:44 G	MT+0200 (heure d'été d'Europe centrale)										
Aug. 22	2019, 10:	59 a.m.	Note: Remote proxy is now four	nd in the main MBG menu instead of th	e server manager menu on the left.								
conne P Infor	nation	our configured ICPs	, or to run a DNS resolution test on configured	hostnames, see the Diagnostics page									
Default for WiNet	Default for SIP	Name	Hostname or IP address	Туре	Installer password	SIP capabilities	Indirect call recording capable	Associated connectors	Associated sets (MiNet/SIP)	Associated trunk rules (pri/sec)			
	۲	acs	1	MIVoice 5000		UDP TCP TLS	×	×	0/14	0/0	1	Û	Θ
)	0	acs 7.0	miw600077	MiVoice 5000		UDP TCP TLS	×	~	0/3	0/0	1	Ť	0
)	0	acs 7.1	.04 ⁰ ⁻ .75	MIVoice 5000		UDP TCP TLS	×	×	0/0	0/0	1	â	Θ
	0	acs but	0.1:3.010.1:	Mi√oice 5000		UDP	×	×	0/0	0/0	1	ŵ	۲
	0	acs cipac	.0.14J.£ ^e .	MiVoice 5000		UDP TCP	×	×	0/0	0/0	1	Û	Θ
)	0	acs r6.5	10.148.91.74	Mi√oice 5000		UDP TCP	×	×	0/0	0/0	1	ŵ	0

Update default ICPs

Renseigner les champs suivants :

Zone Manage ICP

Name : Nom de l'iPBX

/ Manage ICP					
Name Type SIP capabilities	acs 7.2 MiVoice 5000		Hostnam MiNet ins Indirect call rec	ne or IP address staller password cording capable	10.148.91.181
MiVoice 5000 support					
				_	
	Link to this ICP?		Enable		
	XML listen port	4445	TLS?	<	
	XML destination port	4443	TLS?	✓	
2		Save			

Zone Manage ICP

Hostname or IP address : Adresse IP du MiVoice 5000

Type : MiVoice 5000

SIP capabilities : UDP, TCP, TLS > Connexion SIP entre MBG and MiVoice 5000 en TLS (5061)

Zone MiVoice 5000 support

XML listen port : Port public sur lequel le MBG est en écoute (default value 4445).

XML destination port : MiV5000 port (4445 non configurable dans MiVoice 5000).

5.4.5 PARAMÉTRAGES SIP COMMUN À TOUS LES POSTES REMOTE WORKER

Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster

Menu MiVoice Border Gateway, onglet System>Settings

Configurer les champs suivants relatifs aux options de sécurité RTP :

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
- La clé de chiffrement préconisée est :
- AES_CM_128_HMAC_SHA1_80 (default is _32)

Il existe également une option pour le certificat TLS qui doit être Mitel.

Certifi	SIP support	Protocols UDP TCP TCP/TLS	Access profile Public Public Public Public Public	Device → device local streaming Device → trunk local streaming Codec support RTP framesize	□ Restricted to G 729, G.711 (a-law and µ-law) ♥ Dynamic ♥
Inbound	Set-side RTP security SRTP only SRTP or RTP RTP only SRTP only	Accept either SRT server Send only RTP (pl this server	P or RTP inbound to this aintext) outbound from	PRACK support Send options keepalives Options interval Challenge methods	Only behind NAT V 20 Invite Subscribe Refer Prack V
Preferred cipher	AVP+crypto RTP only AES_CM_128_HMAC_SHA1_32			KPML username KPML password Confirm KPML password	
Inbound	ICP-side RTP security SRTP only SRTP or RTP RTP only	Accept only RTP (j server	plaintext) inbound to this	Registration Mode Set-side registration expiry time ICP-side registration expiry time Allowed URI names	Max Set Side 240 Add another
Outbound	SRTP only AVP+crypto RTP only	Send only RTP (pl this server	aintext) outbound from		micollabtest92/p1 mylab2.loc Blank any field you no longer want.
Preferred cipher Tone Injection	AES_CM_128_HMAC_SHA1_32 V			SIP adaptation support SIP adaptation receive pipeline SIP adaptation send pipeline	· · · · · · · · · · · · · · · · · · ·
	Enable	0		Permit weak SIP passwords	0

5.4.6 CONFIGURATION DE LA CONNEXION/AUTHENTIFICATION ENTRE LE MBG ET L'IPBX

✓ Cor

Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster

5.4.6.1 Principe

La connexion entre le MBG et le MiVoice 5000 doit être créée pour :

- Obtenir les devices SIP **Set-side username, Set-side password** et **Icp-side username** configurés dans le MBG. Ces paramètres seront utilisés pour le déploiement par TMA.
- Synchroniser le MiVoice 5000 quand un mot de passe Set-side a été changé dans la MBG.

Le principe d'authentification avec le MBG se déroule en plusieurs étapes :

- Démarrer le service Web
- Ajouter un nouveau client dans le MBG
- Déclarer un nouvel équipement SIP dans MiVoice 5000

5.4.6.2 Procédure détaillée

Avertissement :

Cette procédure se déroule séquentiellement en utilisant alternativement les menus du MBG et de Webadmin MiVoice 5000.

L'ordre des séquences est à respecter impérativement.

Côté Interface MBG :

L'utilisateur doit créer via le menu **Administration>Web services, onglet Add a new consumer** un compte utilisateur que le MiVoice 5000 utilisera pour s'authentifier.

Un compte comporte deux données indispensables à l'étape d'authentification :

- l'Identité du compte (chaîne de 40 caractères maximum) > Champs Name et Consumer ID
- Son code secret (chaîne de 40 caractères maximum) généré et affiché automatiquement par le MBG. > Champ Shared secret.



Côté Web admin MiVoice 5000 :

Menu Abonnés>Terminaux et Applications>MBG

Saisir les paramètres suivants :

- L'adresse IP du MBG,
- L'ID du compte utilisateur (défini sur le MBG),
- Le code secret partagé associé au compte (défini sur le MBG),
- Appuyer sur Entrée

Le bouton Connexion apparait ensuite.

• Cliquer sur ce bouton **Connexion**.

Applications MiVoice Border Gateway	Conf	igure MSL Web Servic	es			MB	G	
Remote proxy services ServiceLink Blades	~	Operation status report Successfully saved new consumer						
Status	» Locatio	n: MSI web services						
Administration	This is to	-f		aliante dint and an annulting to some it				
Web services	This ince	race permits comparation of MSL's w	ved services internace, and the c	clients that are permitted to use it.				
Backup		Manage web service	availability Start Stop					
View log files		Web se	rvice status Enabled					
System information			Access ORE https:// shosalah	ie or ip address=/insireso				
System monitoring	Below ye	ou will find the registered consumers of	of this web service. These are v	endors of web service clients, not active clients thems	elves. For registered clients, see	further below in		
System users	the table	entitled, "Final tokens".						
Shutdown or reconfigure	Add a ne	tw consumer						
Virtualization	Consum	ier information	C 10	Channel annual				
Security	Active	Name	consumer to	Shared secret	KSA Certificate (ii any)			
Remote access	v	Ona	oria	49/25/082065cde168/fa6446da165d30ea4c94a		Modify		
Port forwarding	\checkmark	MiCollab Client Deployment	MiCollabClientDeployment	ad3def11bfeac00ea7c806e6b61687ca090ed130f		Modify		
Web Server	\checkmark	vApp	vapp	22c01bd55bdd688810ef04e0f9ae50f71d293854		Modify Delete		
Certificate Management	1							
Configuration	v	acs1-mq2	acs1-mg2	e/e254f629cae3dc185133a8baeurcdef61e1331		Modiry Delete	— I	
Networks	\checkmark	Miv5000	Miv5000	0eb9978abe1015a33cc58e72e18432bfad0d79e5		Modify Delete		
Accupit	Wob Ad	min	MBC				-	MiVoice 5000
Accueit	Web Au		MBG				🧠 🚺 🔅	
Termin	s aux et A	pplications	Service telephonie>Abonnes	s>Terminaux et Applications>MBG (19.9) ge équipements SIP				Web Admin
Système				Adresse IP du MBG	172 15 0 15			-
Plan de l	numéro	tation		Compte utilizateur (défini eur le MBC)	MW5000			
Discourse	- Calar	adon		Compte utilisateur (denni sur le MBG)	10000		7.61 / 10 170	
Reseau	et liaisor	15		Secret partagé (défini sur le MBG)	0eb9978abe1015a33	cc58e/2e184	32bfad0d/9e	25 ×
Accueils	6				Connexion			
Message	erie et to	onalités						
Liens rap	pides							
				Export du fichier	AUCUN			
i								
1 I I I I I I I I I I I I I I I I I I I								

Le MBG et l'iPBX doivent être synchronisés (même heure).

IMPORTANT : Dans le cas d'un iPBX de type MiVoice 5000 Server, l'OS doit être impérativement au minimum en version 6.7 ou la dernière version des patches OS doit avoir été installée.

Côté Web admin MiVoice 5000 :

Appuyer sur le bouton **Connexion**. Le menu **Service téléphonie>Abonnés>Terminaux et Applications>MBG** présente alors le champ **Code de vérification**.

Côté Interface MBG :

Un jeton (token) temporaire d'authentification a été créé par le MiVoice 5000 sur le MBG (avec une durée de validité d'une heure). Il apparaît dans le menu **Administration>Web services> « Temporary token »**.

• L'administrateur doit alors approuver ce jeton temporaire via le lien Approve .

Blades		Manage web se	ervice availability Start Stop			
Status		w	eb service status Enabled			
dministration			Access URL https:// <hostnar< th=""><th>me or ip address>/mslrest/</th><th></th><th></th></hostnar<>	me or ip address>/mslrest/		
Web services						
Backup	Below you will	I find the registered consum	ers of this web service. These are v	endors of web service clients, not active	clients themselves. For registered cli	ents, see further below in th
View log files	table entitled,	"Final tokens".				
Event viewer	Add a new cor	nsumer				
System information	Consumer Inf	ormation	Commune ID	Channel as anot		(if)
System monitoring	Active	Name	Consumer ID	Shared secret	KSA Certificate (ir any)
System users	V	Oria	oria	497257d82065cde1687fa6446da165d	30ea4c94a	Modify
Shutdown or reconfigure	\checkmark	MiCollab Client Deploy	ment MiCollabClientDeployment	ad3def11bfeac00ea7c806e6b61687ca	090ed130f	Modify
Virtualization		riconab enerit bapiey				<u></u>
ecurity	V	vApp	vapp	22c01bd55bdd688810ef04e0f9ae50f7	1d293854	Modify Delete
Remote arress	\checkmark	acs1-mo2	acs1-mg2	e7e254f629cae3dc185133a8bae0fcde	f61e1331	Modify Delete
Port forwarding	1					
Web Server	V	Miv5000	Miv5000	0eb9978abe1015a33cc58e72e18432b	ofad0d79e5	Modify Delete
Certificate Management						
onfiguration						
Networks	The following t	table shows the list of appr	oved tokens, representing an approv	ed client for this web service.		
E-mail settings	Final tokens					
Google Apps	Consumer	Tok	en ID Secret	Expiry D	escription	
DHCP	There are no	approved tokens at this tim	ne. Note, tokens are created as part	of the OAuth process, they are not create	ed manually. It is up to the client to i	nitiate this process.
Date and Time						
Hostnames and addresses						
Domains						
IPv6-in-IPv4 Tunnel	The following t	table shows the list of temp	orary tokens. These tokens, if appro	ved, can be used for the client to fetch it	s final tokens, used for day-to-day a	uthentication. These tokens
SNMP	require admin	istrator intervention to perr	nit access. If you do not wish to perr	nit access to the client responsible for th	e request, you may either reject the	token, or wait for it to expir
Ethernet Cards	Temporary to	kens				
	Approved	Consumer Tok	en ID	Expiry	Verifier	
Review configuration			I Contractor and a second s	Tue Teb 2, 2010 @ 15:20:40 UTC		Reject
Review configuration	×	Miv5000 ciluv	vekjrpglivw9h1wotw==	Tue, Feb 2, 2016 @ 15:39:40 01C		

• Cliquer sur OK.

	C	and a second									
https://172.15.0.15/s	server-manager/					C Q Rechercher	☆	ê (•	<u>م</u>	9
🕅 Mitel	Mitel S	tandard Linux							Status: 🚺	ajor	
pplications MiVoice Border Gateway Remote proxy services	Configue * Location: MS	re MSL Web Services									0
erviceLink	This interface	permits configuration of MSL's web serv	ices interface, and	the clients that are permitted to use it.							
Blades Status		Manage wo	b service availa Web service s	bility Start Stop							
dministration			Acce	the second s							
Web services Backup View log files	Below you will Add a new cor	find the registered consumers of this w	eb service. These	This will approve the token for use by the client that req Are you sure?	uested it.	or registered clients, see fi	urther below in the table entitled, "Final i	tokens".			
Event viewer	Consumer info	ormation									
System information	Active	Name	Consum			122-1224-	RSA certificate (if any)				
System monitoring System users	1	Una	ona	OK AN	nuler	0306840948			Modif	Ĺ	
Shutdown or reconfigure	×,	MiCollab Client Deployment	MICOIIabo			_caugued130r			Modif	Ľ	
Virtualization	V	vApp	vapp	22c01bd55bdd688810el	f04e0f9ae5	50f71d293854			Modif	<u> ∠ Deleb</u>	4
ecurity Remote access	V	Miv5000	Miv5000	0eb9978abe1015a33cc	58e72e1843	32bfad0d79e5			Modif	Z Delet	2
Port forwarding Web Server	√	acs1-mq2	Mv5000	9be1b54d2fbf33d9e923	f84eb0bd4:	3a692a5beb4			Modif	<u>/ Deleb</u>	<u> </u>
Certificate Management	The following t	table shows the list of approved tokens,	representing an a	oproved client for this web service.							
Networks F-mail settings	Final tokens										
Google Apps	Consumer Mix5000	Token ID 8v2i6kl7ctvda/jocts/lo==		Secret	Expir	ry 29 1902 3-51 p.m	Description	Mor	lify Dana	w Dava	Va
DHCP Date and Time		overoni nyodyjąnaki g –				2.9, 1902, 9102 pill.			ITT ITTE		
Hostnames and addresses											
Domains IPv6-in-IPv4 Tunnel	The following t	table shows the list of temporary tokens	These tokens, if	approved, can be used for the client to fetch its final to	kens, used	l for day-to-day authenticatio	on. These tokens require administrator i	nterventi	on to perm	it access.	If
SNMP	Temporary to	sh to permit access to the client respons ikens	ble for the reques	t, you may either reject the token, or wait for it to exp	ire.						
Ethernet Cards	Approved	Consumer Token II)	Expiry			Verifier				
Review configuration	×	acs1-mq2 94xv+ifht	8szvbs1lfh99a==	Wed, Mar 9, 2016 @ 1	4:20:21 UT	тс	AD	prove	Reie	đ	
Support and licensing											
Help	Mitel Standard	Linux 10.4.10.0									
	MiVoice Border	Gateway 9.2.0.17 ks Corporation									
		A 🛎 👜 🖷 🕅	W						P 10 0) 1/	4:53

Lorsque le jeton temporaire est approuvé, un code **verifier** est généré. Ce code est à entrer dans Webadmin de MiVoice 5000 comme **Code de vérification**.

Côté Interface MBG :

L'exploitant doit copier le code **Verifier** associé à ce jeton temporaire et le coller dans le champ **Code** de vérification dans le menu Service téléphonie>Abonnés>Terminaux et Applications>MBG.

mporary toke	ens						
proved	Consumer	Token ID	Expiry	v	erifier		
1	Miv5000	ciluwekjrpglivw9h1wotw==	Tue, Feb 2, 2016 @ 15:39:40 UTC	5	40515	Reject	
		Dt swiigsko-Midd Sten Communication	tadX D_ micellata1-MiCellatoX Where KB. Troublechoo 155://how/m0533/redirect.htm Service téléphonie MBG Corrections-Romes.comes.formena.er.egelcations.MBG1	bu X Dr MWeice S006: MBG 1991 Adresse (P du MBG Compte Ullistateur (defin sur le MBG Scoreptatus) (defin sur le MBG) Code de vérification Export du fichter	x + 17 15 015 54 15	C Q Redenter MVoice 5000	ى
		M9508-88-2 82-8 80-09 PHL 9/07/4 E 12 14 612	INT TRA XC			Mi	iVoice 5000 eb Admin

Côté Web admin MiVoice 5000 :

Quand le champ **Code de vérification** est saisi côté MiVoice 5000, le MiVoice 5000 confirme au MBG le token d'authentification.

Le MBG alloue alors au MiVoice 5000 un token final d'authentification (une paire Token ID et le secret associé avec une durée de validité d'un an).

🔯 vmbg-lco - Mitel Standard 🗶 🔯 mi	collab1 - MiCollab	× VMware KB: Troublesho	oti 🗙 🕅 MiVoice 5000: M	BG × ∖ +							
♦ https://192.168.100.155/rhm/m5257/re	direct.htm				C ^e Q. Recherch	er		☆自		- ^	⊜ ≡
N vmbg1-mq2 - Mitel Stat	nda × 🕞 MiVoi	ice 5000: MBG × +	_	_						×	
← ▲ https://172.15.0.15/	server-manager/				C ^I Q, Rechercher		☆自	•	^ 9	≡	
Abonnés Terminaux e MBG Système	Mitel St	andard Linux				admin@vmbg1-mq2	int.com	Status: Ma	ijor	Ŀ.	9 🖆
Plan de num Réseau et la Accueils Messagerie Liens rapide Messagerie Bioles Status Administration Web services Backup View log files	Configure Location: MSL This interface p Below you will f tokens".	e MSL Web Services web services ermits configuration of MSL's web services Manage web serv Web	ervices interface, and the client ice availability Start Start Start service status Enabled Access URL https://chost web service. These are vendo	ts that are permitted to us p name or ip address>/msli ors of web service clients,	re it. rest/ not active clients themselves. For	registered clients, see furt	ther below in t	the table entit	led, "Fina	? Î	
Event visear System information System monitoring System users Shuddown or reconfigure Virtualization Security Remote access Port forwarding Web Server	Add a new cons Consumer info Active	unner mation Name Oria MiCollab Client Deployment vApp MivS000 acs1-mq2	Consumer ID oria MiCollabClientDeployment vepp Miv5000 Mv5000	Shared secret 497257d82065cd ad3def11bfeac00 22c01bd55bdd68 0eb9978abe1015 9be1b54d2fbf33d	e1687fa6446da165d30ea4c94a ea7c805e6b51687ca090ed130f 8810ef04e0f9ae50f71d293854 a33cc58e72e18432bfad0d79e5 9e923f84eb0bd43a692a5beb4	RSA certifica	ite (if any)	Modify Modify Modify Modify Modify	Delete Delete Delete	E	
Certificate Management Configuration Networks E-mail settings doogle Apps DHCP Date and Time + startypy, ctr 405/03/16.112, 007/03/10	The following ta Final tokens Consumer Miv5000 acs1-mq2	ble shows the list of approved toker Token ID 8v2i6k/7rtyda/jatts/lg== lvmdwrmSrpwweg2278gora== bble shows the list of temporary toke	ns, representing an approved of Secret tomaq7ivq1 29qehzfrrci ans. These tokens, if approved	tlient for this web service. SotpoltuidBfw== v/vt0jds8q== , can be used for the clien	Expiry Dec. 29, 1902, 3:51 p.m. March 9, 2017, 2:54 p.m. t to fetch its final tokens, used for	Descripti	on M M . These token	odify Renew odify Renew s require adm	Revok		

s:// 192.168.100.155 /rhm/m5257/red	direct.htm				C Q Rechercher			☆自		+	俞
🕅 vmbg1-mq2 - Mitel Stan	ida × 🗖 MiVo	rice 5000: MBG × +	_	_		_	-				X
♦ https://172.15.0.15/se	erver-manager/			C' C	Rechercher		☆ 自	•	⋒	ø	≡
🕅 Mitel	Mitel St	andard Linux			adm	in@vmbg1-mq2	.int.com	Status: N	lajor	G	•
Applications MiVoice Border Gateway Remote proxy services	Configur » Location: MSI	e MSL Web Services	services interface, and the clients t	nat are permitted to use it.						?	
Blades Status Administration		Manage web serv Web	vice availability Start Stop b service status Enabled Access URL https:// <hostnar< td=""><td>ne or ip address>/mslrest/</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></hostnar<>	ne or ip address>/mslrest/							
Web services		find the registered consumers of thi									
Backup View log files Event viewer	tokens".	sumer	is web service. These are vendors	of web service clients, not active clients	themselves. For regist	ered clients, see furt	her below in	the table ent	itled, "	Final	
Backup View log files Event viewer System information	Active	sumer prmation	Consumer ID	of web service clients, not active clients	themselves. For regist	PSA certifica	te (if any)	i the table ent	itled, "	Final	
Backup View log files Event viewer System information System monitoring	Add a new cons Consumer info	sumer rrmation Name Oria	Consumer ID oria	of web service clients, not active clients Shared secret 492257d82065cde1687fa6446da16	5d30ea4c94a	ered clients, see furt RSA certifica	ther below in	the table ent	itled, "	Final	
Backup View log files Event viewer System information System monitoring System users Shutdown or reconfigure	Add a new cons Consumer info	sumer Oria Micollab Cliest Declaument	Consumer ID oria	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da16	5d30ea4c94a	ered clients, see furf	ther below in	Modi	itled, "	Final	
Backup View log files Event viewer System information System users Shutdown or reconfigure Virtualization	E Consumer info	sumer romation Name Oria MiCollab Client Deployment	Consumer ID oria MiCollabClientDeployment	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da1 ad3def11bfac000a7c80566b616 20c0b147c1d4coac.56.00	5d30ea4c94a ?ca090ed130f	RSA certifica	ther below in	Modi	itled, " iv	Final	
Backup View log files Event viewer System onolibring System users Shutdown or reconfigure Virtualization Security	E E	sumer romation Name Oria MiCollab Client Deployment VApp	Consumer ID oria MiCollabClientDeployment vapp	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da16 ad3def11bfeac00ea7c806e5b168 22c01bd55bd6688810ef04e0f9ae5	themselves. For registr 5d30ea4c94a 7ca090ed130f 0f71d293854	red clients, see furl	ther below in	n the table ent <u>Modi</u> <u>Modi</u>	itled, " iv iv iv <u>iv</u> <u>De</u>	ilete	E
Backup View log files Event viewer System monitoring System users Shutdown or reconfigure Virtualization Security Remote access Der fenoralise	E Consumer info	sumer romation Name Oria MiCollab Client Deployment vApp Miv5000	Consumer ID oria MiCollabClientDeployment vapp Miv5000	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da16 ad3def11bfeac00ea7c806e5b6168 22c01bd55bdd688810ef04e0f9ae5 0eb9978abe1015a33cc58e72e1843	themselves. For registr 5d30ea4c94a 'ca090ed130f 1/71d293854 2bfad0d79e5	RSA certifica	tte (if any)	n the table ent Modi Modi Modi	itled, " iv iv <u>De</u> iv <u>De</u>	lete	E
Backup View log files Event viewer System onolibring System users Shutdown or reconfigure Virtualization Security Remote access Port forwarding Web Server	Elevery you will tokens". Add a new cons Consumer info Active V E V V	sumer romation Name Oria MiCollab Client Deployment VApp MivS000 acs1-mg2	Consumer ID oria MiCollabClientDeployment vapp Miv5000 Mv5000	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da16 ad3def11bfeac00ea7c806e5b168 22c01bd55bd688810ef04e0f9ae5 0eb9978abe1015a33cc58e72e184 9be1b54d2fbf33d9e923f84eb0bd4;	themselves. For registr 5d30ea4c94a rca090ed130f 0771d293854 i2bfad0d79e5 ia692a5beb4	red clients, see furt	tte (if any)	Modi Modi Modi Modi Modi	itled, " iv iv <u>De</u> iv <u>De</u>	lete lete	E
Backup View log files Event viawar System monitoring System monitoring System users Shutdown or reconfigure Virtualization Security Remote access Port forwarding Web Server Certificate Management Certificate Management Ermail settings	below you will takens". Add a new come Consumer info Active	sumer romation Name Oria MiCollab Client Deployment vApp MivS000 acs1-mq2 able shows the list of approved toke	Consumer ID oria MiCollabClientDeployment vapp MivS000 MvS000	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da16 ad3def11bfeac00ea7c806e6b6168 22c01bd55bdd688810ef04e0f9ae5 0eb9978abe1015a33cs0e72e184 9be1b54d2fbf33d9e923f84eb0bd4; t for this web service.	themselves. For registr 5d30ea4c94a rea090ed130f if71d293854 22bfad0d79e5 a692a5beb4	RSA certifica	ite (if any)	<u>Modi</u> <u>Modi</u> <u>Modi</u> <u>Modi</u> <u>Modi</u>	itled, " iv iv De iv De iv De	lete lete	E
Backup View log files Event viewer System monitoring System or reconfigure Virtualization Security Remote access Port forwarding Web Server Certificate Management Configuration Networks E-mail settings Google Apps	below you will tokens". Add a new come Consumer info Active The following tt Final tokens Consumer	sumer romation Name Oria MiCollab Client Deployment VApp Miv5000 acs1-mg2 able shows the list of approved toke Token ID	Consumer ID oria MiCollabClientDeployment vapp Miv5000 Mv5000 tns, representing an approved clien Secret	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da16 ad3def11bfac00ea7c806e6b6168 22c01bd55bdd688810ef04e0f9ae5 0eb9978abe1015a33cc58e72e184 9be1b54d2fbf33d9e923f84eb0bd4 t for this web service. Expiry	themselves. For registr 5d30ea4c94a *ca090ed130f 3/71d293854 :2bfad0d79e5 ia692a5beb4	red clients, see fur RSA certifica Descripti	on	Modi Modi Modi Modi	itled, " iv iv <u>De</u> iv <u>De</u>	ilete ilete	E
Backup View log files Event viawar System monitoring System onentoring 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	below you will tokens". Add a new com Consumer info Active The following to The following to The following to The following to The following to The following to The following to	sumer romation Name Oria MicOllab Client Deployment VApp MivS000 acs1-mq2 able shows the list of approved toke Token ID Sv2icki7rtyda/jqrts/lg==	Consumer ID oria MiCollabClientDeployment vapp Miv5000 Mv5000 ens, representing an approved clier Secret tomag7iu32	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446da16 ad3def11bfeac00ea7c806e6b6168 22c01bd55bdd688810ef04e0f9ae5 0eb9978abe1015a33cc58e72e184 9be1b54d2fbf3dd9e923f84eb0bd43 tf or this web service. epituid9fw== Dec. 39, addefw== Dec. 39,	themselves. For registr 5d30ea4c94a /ca090ed130f 0/71d293854 2bfad0d79e5 ia692a5beb4	red clients, see fur RSA certifica Descripti	on	Modi Modi Modi Modi Modi Modi Modi Modi	itled, " iy De iy De iy De	elete elete elete	E
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 Certificate Management E-mail settings Google Apps DHCP Date and Time Hostnames and addresses Domains IPV6-in-IPV4 Tunnel Even	below you will tokens". Add a new come Consumer info Active Active The following tt Final tokens Consumer MyS000 Set mg3	sumer romation Name Oria MiCollab Client Deployment VApp Miv5000 acs1-mq2 able shows the list of approved toke Token ID Bv2i6kl7rtyda/jqrts/lg== Lond.wwEp.com/gaD70gcct	Consumer ID oria MicollabClientDeployment vapp Miv5000 Mv5000 ens, representing an approved clien Secret tymaq7iuq3oty 29qabs/rocy/	of web service clients, not active clients Shared secret 497257d82065cde1687fa6446de16 ad3def11bfeac00a-7c806e6b6168 22c01bd55bdd688810ef04e0f9ae5 0eb9978abe1015a33cc58e72e184: 9be1b54d2fbf33d9e923f84e0bbd4: tt for this web service. vg1tuid8fw== Dec. 29, vd2489, Mext-9,	themselves. For registr 5d30ea4c94a cca090ed130f 3/71d293854 i2bfad0d79e5 ia692a5beb4 1902, 3:51 p.m. 2003, 3:51 p.m.	RSA certifica Descripti	on	Modi Modi Modi Modi Modi Modify Rene Modify Rene	itied, " iy De iy De iy De ww Re	lete lete lete voke voke	E

Côté Web admin MiVoice 5000 :

Une fois le token final d'authentification obtenu du MBG,

le menu **Service téléphonie>Abonnés>Terminaux et Applications>MBG** présente l'ID du token final et la date de fin de validité de celui-ci.

Lorsque la connexion est établie :

Les actions des différents boutons permettent ensuite les actions suivantes :

- Changer paramètres de connexion : Bouton permettant de supprimer tous les paramètres pour permettre de recommencer l'authentification en cas de changement de compte utilisateur, ou un changement de MBG.
- Synchronisation des équipements SIP : Bouton permettant l'import des équipements SIP rattachés à l'iPBX local et déclarés dans le MBG.
- Export équipements SIP du MBG : bouton provoquant la création du fichier devices_mbg.csv.
- **Export du fichier** : Export du fichier **devices_mbg.csv** sur le PC local ; Utile pour les fichiers MAC.

Le fichier **devices_mbg.csv** comporte plusieurs colonnes issues des valeurs définies au niveau du MBG (se référer au paragraphe 6.1) :

- Login : Set-side username (Valeur du Login du Remote Worker)
- NA : Icp-side username (Numéro d'abonnement du Remote Worker)
- **Password** : **Set-side password** (Mot de passe MD5 entre le poste et le MBG)

Se référer ensuite au chapitre 6.4 pour l'exploitation de ce fichier.

🔉 vmbg-lco - Mitel Standard 🗶 🖸	micollab1 - MiCollab 🛛 🗙 🧰 VMware KB: Troubleshoo	oti × 🔯 MiVoice 5000: MBG	× (+	_ 0 ×
♦ ▲ https://192.168.100.155/rhm/m5257	7/redirect.htm		C Q Rechercher	☆自 ♥ ↓ ♠ ♥ ☰
🕅 Mitel servi	ice téléphonie		MiVoice 5000	٩
Accueil Web Admin Abonnés Terminaux et Applications MBG	MBG Service téléphonies-Abonnés>Terminaux et Applications>MBG Connexion Listage équipements SIP	(19.9)		
Plan de numérotation Plan de numérotation Réseau et liaisons Accueits Messagerie et tonalités Liens rapides		Adresse IP du MBG Compte utilisateur (défini sur le MBG Secret partagé (défini sur le MBG) Jeton final Date fin validité authentification Connexion effectuée avec le MBG	172 15 0.15 Mv5000 9be1b54d2fbf33d9e923f84eb0bd43a692a5beb4 Jwndwrn5rywwwg2278gora== 09/03/2017-14-54:05	
MISSOO RE2 RC (CLB) TA 4 1 2 3 3 4 5 5 5 5 5 5 5 5 5 5 5 5 5	Image C Image </td <td>Chan Synchr Export du fichier</td> <td>ger paramètres de connexion onisation des équipements SIP ort équipements SIP du MBG (devices_mbg.csv (09/03/2016</td> <td></td>	Chan Synchr Export du fichier	ger paramètres de connexion onisation des équipements SIP ort équipements SIP du MBG (devices_mbg.csv (09/03/2016	
👌 🧭 🗐 🗖	o 💿 🖭 💌 🗶			FR 🔺 🏴 算 🌒 17:21

5.5 **CONFIGURATION DU MBG EN WHITE LIST**

 \checkmark

Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster

Comme le MBG concentre le flux de tous les usagers à distance, l'adresse IP du MBG doit être mise dans la White list l'iPBX pour éviter Black listage automatique indésirable du MBG par l'iPBX.

Côté Webadmin de l'iPBX

A partir du menu Service téléphonie>Réseau et liaisons>Qualité de service>Sécurité SIP

Définir l'adresse du MBG dans la Whitelist.

Se référer au document MiVoice 5000 - Manuel d'exploitation.

5.6 **CONFIGURATION DE L'APPLICATION TMA (SERVICE POSTES)**

Menu Configuration de l'application

• Cocher les cases comme indiqué :

🗩 vmbg-lco - Mitel Standard 🗶 🗖 m	icollab1 - MiCollab 🛛 🗙 🔤 VMware KB: T	publeshooti × 🔎 MiVoice 5000 - Service Pos × +				- 0	x
◆ ▲ https://192.168.100.155/tma/index.ph	p?module=parametrage		C Rechercher	☆ 自 ♥	+ 1	9	≡
🕅 Mitel 🕴 Servio	ce Postes						
Accueil Web Admin Configuration de l'application Configuration des serveurs Inventaire Gestion des logiciels Configuration des postes Déploiement Export de la configuration des postes Suivi des actions Journal des événements	Configuration de l'application Configuration des postes Chiffrement des fichiers de configuration Gestion des remote workers Valider Annuler	2					
🚱 🧭 🖯 🛪 🗴) 🖄 🙁 🕘 🚯			FR 🔺	• 🖞 🕪	15:13	

Le chiffrement des fichiers n'est pas impératif mais est fortement recommandé.

Dans le cas de TMA embarqué, le serveur FTP embarqué (= « local ») est défini automatiquement dès que la case **Gestion des remote workers** est activée.

5.7 DÉFINITION DES SERVEURS DE TÉLÉCHARGEMENT POUR LES REMOTE WORKERS

Le but est de définir les serveurs de téléchargement dédiés aux postes Remote Worker.

Dans le cas de TMA embarqué :

Le serveur local FTP est automatiquement ajouté pour les postes Remote Worker (voir paragraphe précédent).



2

IMPORTANT : L'iPBX intégrant ce serveur FTP embarqué doit être le même que celui sur lequel sont déclarés les abonnements de type Remote Worker.

Dans le cas de TMA/TMA-EP centralisé dans le MiVoice 5000 Manager :

Définir le ou les serveurs dédiés aux postes Remote Worker.

Note : Si le même serveur doit être utilisé pour les postes locaux et Remote Worker, il doit être déclaré deux fois (une fois pour les postes Remote Worker et une fois pour les postes locaux).



5.7.1 Configuration du serveur de téléchargement pour les Remote Workers

Les informations nécessaires sont les suivantes :

- Nom
- Adresse IP (doit correspondre au PBX sur lequel sont définis les remote workers)
- Port : valeur figée à 21
- Liste du site sur lequel sont déclarés les Remote Workers rattachés au serveur de téléchargement considéré,
- Infos login/mot de passe écriture pour les postes 6xxxi, renseigner par défaut avec les valeurs du serveur FTP embarqué (compte FTP mngt_ftp_67xxi)

Une fois ces informations validées, le serveur apparaitra dans le tableau "Liste des serveurs Remote Workers"

A partir du menu Configuration des serveurs

- Cliquer sur Ajouter un nouveau serveur dans la zone dédiée aux Remote Worker
- Renseigner tous champs nécessaires comme indiqué précédemment,
- Définir la liste des sites iPBX rattachés à ce serveur pour les Remote Workers (bouton **Modifier la liste des sites** dans l'écran précédent),



- Sélectionner uniquement le site de rattachement des Remote Workers
- Enregistrer et Valider.

Une fois ces informations validées, le serveur de téléchargement apparait dans le tableau Liste des serveurs.

- L'action Modifier le serveur permet de modifier les paramètres du serveur
- L'action Supprimer le serveur permet de supprimer le serveur.

6 PRÉPARATION AU DÉPLOIEMENT

6.1 DÉCLARATION DES EQUIPEMENTS SIP (POSTES 6800 SIP ET 6900 IP PHONES)

✓ Non commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster (voir les différents paragraphes suivants).

6.1.1 CAS D'UN MBG STANDALONE

Cette configuration est à effectuer pour chaque poste 68xxi en mode Remote Worker.

Les équipements peuvent également être créés par téléchargement d'un fichier CSV > Menu **System>Bulk provisioning**.

System - Network	Teleworking SIP trunking	- Remote proxy -	Call recording +	Troubleshooting 👻
Dashboard Metrics	21 15:47:28 GMT+0200 (heure d'été d'Euro	pe centrale)		
Connectors	Note: Remote proxy	is now found in the main N	IBG menu instead of the	server manager menu on the left.
Settings				
Trust store	Materia de la sel ateres		I have a large the second states and in	a baba inclusion has a base of in this calculate. Discuss an advance of a data and the MDC data and this to second it is
Bulk provisioning	working correctly for	your environment.	r know that local streamin	g denaviour has changed in this release. Prease monitor your deployment and see the MDG documentation to ensure it is
C Bulk provisioning				
	MiNet CSV import/export	MiNet backup		Choisir un fichier Aucun fichier choisi
		MINet restore		
	SIP CSV import/export	SIP backup		Choisir un fichier Aucun fichier choisi
		SIP restore		

Configuration des postes Remote Worker

Menu MiVoice Border Gateway, onglet Teleworking>SIP

System +	Network - Telewo	rking 👻 SIP trunking 👻	Remote proxy +	Call recording +	Troubleshooting -				Se	arch
Page updated:	Tue Apr 27 2021 15:25:50 GM	/T+0200 (heure d'été d'Europe c	entrale)							
Aug. 22, 3	2019, 10:59 a.m.	Note: Remote proxy	is now found in the m	ain MBG menu instead of	f the server manager menu on the left.					
Below is a list o	f devices for this MBG server									
Note: To con	figure SIP profiles by uploadi	ng a CSV file, please see the B	ulk provisioning page							
Sets per pa	19e	Status		Simple filter						Bulk edit
20		CEnabled Obisabled				Ĵ				
				_						🚧 📢 Pag
SIP profile	information									
+	Est side users and	ICD alds warman	Augustability	Continued ICD	December	I and sharen be between devices	1	Churtes Terrs		
Enabled	Set-side username	ICP-side üsername	Availability	Conligured ICP	Description	Local streaming between devices	Log verbosity	Cluster Zone		~
×	42800	42800	Everywhere	acs	42800 - ABO 42800	Use master setting	Use master setting	Default	1	
~	s.inattend	45800	Everywhere	acs	45800 - Standard InAttend	Use master setting	Use master setting	Default	1	â
\checkmark	o.adrian	42830	Everywhere	acs	42830 - Adrian Okba	Use master setting	Use master setting	Default	1	1
\checkmark	fmartin.lharidon	42825	Everywhere	acs	42825 - Franck-Martin L'haridon	Use master setting	Use master setting	Default	1	8

Dans la zone SIP profil information, cliquer sur + en haut à gauche de la zone SIP profile information.

Dans la fenêtre suivante, configurer les paramètres comme indiqué ci-après :

Configured ICP:

- ICP => IP Connection Point = MiVoice5000
 Set-side username:
- Valeur du Login du Remote Worker
 - Set-side password:
- Mot de passe MD5 entre le poste et le MBG
 - Icp-side username:
- Numéro d'abonnement du Remote Worker

Icp-side password:

- Mot de passe MD5 de l'abonnement MiVoice 5000 **Description:**
- Nom considéré pour l'équipement utile par exemple pour un listage.
 Après avoir renseigné tous les champs, cliquer sur Save.
 Reprendre la procédure pour les équipements SIP suivants.

6.1.2 CAS D'UN MBG EMBARQUÉ OU EN MODE CLUSTER AVEC MICOLLAB

Les postes 6800 SIP et 6900 IP phone Remote Worker ne fonctionnent qu'en mode SSO.

Lorsque le MBG est en Cluster avec MiCollab, les équipements SIP sont provisionnés par MiCollab server. L'identification suivante est réalisée pour tous les abonnés Remote Worker :

Menu MiVoice Border Gateway, onglet Teleworking>SIP

Dans la zone SIP profil information, cliquer sur +

Configurer les champs suivants comme indiqué :

Set-side username: Login

Set-side password: Généré aléatoirement par le serveur MiCollab.

6.2 CONFIGURATION SPÉCIFIQUE D'UN SOFTPHONE CLIENT MICOLLAB

✓ Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster

Ce cas ne concerne que des utilisateurs ayant un poste Remote Worker 6800 SIP ou 6900 IP phone et un poste Softphone Micollab en accès distant.

Pour l'abonnement considéré, le poste distant doit être logué avant le poste Softphone Micollab.

Le chiffrement n'étant pas disponible actuellement sur les Softphones Client MiCollab, il est nécessaire d'effectuer la configuration suivante :

Au niveau du MBG :

Permise mais non imposée

Enabled	\checkmark		Configured ICP	mv5000-lco
Set-side username	65173		Set-side password	•••••
				Password is good
			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 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

Au niveau du Softphone Client MiCollab :

Non chiffrée impérativement

Représentation	Activer SIP Softphone	·
Intégration du calendrier	DN SIP Softphone :	65173 🔹
Notification d'appels Paramètres de discussion	Connexion SIP :	тср 🔹
Gestion des Connaissances	- Softphone va utiliser les	appareils suivants
Notification de connexion	Microphone :	Microphone sur casque (2- USB Teleph 👻
Intégration PIM	Haut-parleur :	Valeurs par défaut 🗸
Paramètres du logiphone	Alertes:	Valeurs par défaut
Affichage Contacts	Contrôle des appels :	Aucune 🗸
Cliquer pour appeler	Caméra vidéo :	QuickCam Communicate Deluxe 🛛 🗸
	Sonnerie	Lire
	└ Vtiliser le télétravaille	eur pour softphone
	Passerelle Teleworker :	10.148.84.31

6.3 PRÉPARATION DU FICHIER CSV REMOTE WORKER À PARTIR DU FICHIER PROVISIONNING GÉNÉRIQUE

Le fichier TMA provisionning 6xxxi@version.xls est disponible sur l'extranet Mitel.

ONGLET/SHEET '68	XX SIP TELEWOR	RKERS'					
Fonction / Function							
Cet onglet est utilisé p	our générer un fichier ".	csv. pour TMA, contenant le	es paramètres requis pour la fonctionnalité Téléworker	par terminal 68xx S	P.'RemoteWorker pou	ur les postes 68xxi	via MBC
TMA permet ensuite de	e charger ce fichier '.cs	v, créant les fichiers MAC m	is dans le répertoire FTP embarqué défini. Se référer	à la documentation M	/IV5000 'XXX'.		
/ This sheet is used to	generate a '.csv' file, fo	r TMA, including the parame	ters required for the feature Teleworker by terminal 68	xx SIP.			
After TMA allows to lo	oad this file '.csv' file, cr	reating MAC files put into the	e defined embedded FTP server. Please refer to the M	iV5000 documentatio	on 'XXX'.		
Rules:							
3 types de données dif	férenciés par la couleur	r de la police / 3 kind of data	differenciated by the font color:				
	- Noir / Black: donnée	par terminal-abonné / data l	by terminal-subscriber				
	- Marron / Brown: Don	né système - même valeur p	oour toutes les adresses MAC / system data - same	alue for all MAC_AD	DRESS		
	- Rouge / Red: donné	es obligatoires - éviter de les	s modifier / compulsory data - avoid to modify them				
Attention / Caution:							
- Merci de ne pas modifi	er le nom de de cette o	onglet / Please do not modify	/ the name of this sheet.				
- Merci de ne pas créer	de ligne avant 'MAC_AI	DDRESS' / Please do not cr	eate any line before 'MAC_ADDRESS'				
Gonorat	ion cov	D:\temp\export_global_cs	/				
General	1011.03V	D. Kompiexpert_global.com					
TE	RMINAL - SUBSCRIB	ER			SYSTEM		
MAC_ADDRESS	Isip line1 user name	Isip 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	9a480
08000F9F7305	7001	7001	password2	public.test.com	public.test.com	public.test.com	9a480
							1
► ► Import_CSV_TMA	🔬 67xxi Global 🔬 67x	xi Specific 🧹 67xxi All 📜 68:	xxi Teleworker / 🖏 🖉 🔢 🖉				

- Renseigner l'onglet 68xxi Teleworker en respectant les règles ci-dessous (règles rappelées également dans ce même fichier).
- Générer ensuite le fichier au format CSV (bouton Generation .CSV)

Les autres onglets concernent les données Globales et Spécifiques relatives à tous les postes 6xxxi SIP Phones. Se référer au document Manuel d'installation des Postes 6xxxi - AMT/PTD/TR/0043.

Règles pour les Remote Workers (rappelées dans le fichier) :

3 types de données sont à différencier par la couleur de la police :

Noir : Données à renseigner pour chaque poste Remote Worker

Marron : Données système à renseigner commune à toutes les adresses MAC

Rouge : Données obligatoires à éviter de modifier.

Exemple :

A	В	С	U	E	F	G	Н
onction / Function	n:						
Cet onglet est utilisé	pour générer un fichier "	.csv. pour TMA, contenant	les paramètres requis po	ur la fonctionnalité T	éléworker par termina	68xx SIP.'Remote	Worker pour les postes 68xxi via MBG
TMA permet ensuite	de charger ce fichier '.cs	v. créant les fichiers MAC	mis dans le répertoire FT	P embarqué défini. S	Se référer à la docum	entation MIV5000 X	XX.
/ This sheet is used t	o generate a '.csv' file, fo	or TMA, including the param	eters required for the fea	ture Teleworker by te	erminal 68xx SIP.		
After TMA allows to	load this file '.csv' file, c	reating MAC files put into the	ne defined embedded FTF	P server. Please refer	r to the MiV5000 doc	umentation 'XXX'.	
ules:							
3 types de données d	lifférenciés par la couleu	r de la police / 3 kind of dat	a differenciated by the fo	nt color:			
	- Noir / Black: donnée	e par terminal-abonné / data	by terminal-subscriber				
	- Marron / Brown: Dor	nné système - même valeur	pour toutes les adresses	s MAC / system data	a - same value for all	MAC ADDRESS	
	- Rouge / Red: donne	ées obligatoires - éviter de l	es modifier / compulsory	data - avoid to modif	fy them	_	
ttention / Caution	:		N				
Merci de ne pas mod	ifier le nom de de cette	onglet / Please do not modi	fy the name of this sheet				
 Merci de ne pas crée 	r de ligne avant 'MAC A	DDRESS' / Please do not o	reate any line before 'MA	C ADDRESS'			
		Diterration at states					
Genera	ation .csv	D:\temp\export_global.cs	V				
Genera	ation .csv	D:\temp\export_global.cs	v				
Genera	ation .csv	D:\temp\export_global.cs	V		SYSTEM		
Genera T MAC_ADDRESS	etion .csv ERMINAL - SUBSCRIB Isip line1 user name	D:\temp\export_global.cs ER Isip line1 auth name	v sip line1 password	sip proxy ip	SYSTEM sip registrar ip	https server	https path
Genera T MAC_ADDRESS 00085D4330B8	ERMINAL - SUBSCRIB	D:\temp\export_global.cs ER Isip line1 auth name 7000	v sip line1 password password1	sip proxy ip 64.101.10.1	SYSTEM sip registrar ip 64.101.10.1	https server 64.101.10.1	https path 9a48085c1b816fd1b512e8b186686a6
Genera MAC_ADDRESS 00085D4330B8 08000F9F7305	ERMINAL - SUBSCRIB Isip line1 user name 7000 7001	D:\temp\export_global.cs ER Isip line1 auth name 7000 7001	sip line1 password password1 password2	sip proxy ip 64.101.10.1 public.test.com	SYSTEM sip registrar ip 64.101.10.1 public.test.com	https server 64.101.10.1 public.test.com	https path 9a48085c1b816fd1b512e8b186686a6 9a48085c1b816fd1b512e8b186686a6

Cliquer sur le Bouton Generation .csv

- 24 MAC_ADDRESS;!sip line1 user name;!sip line1 auth name;sip line1 passwc
- 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
 - booorsr/303;/001;/001;passwordz;punite.cest.com;public.co

Liste complète :

Données à renseigner pour chaque Remote Worker

- MAC_ADDRESS : Adresse MAC des postes 6800 SIP ou 6900 IP phone Remote Worker
- !sip line1 user name : Login de l'abonné (issu du MBG fichier devices_mbg.csv)
- !sip line1 auth name : Login abonné (issu du MBG fichier devices_mbg.csv)
 - En mode SSO : Login abonné
 - Sans mode SSO : Numéro de l'abonné
- **sip line1 password :** Mot de passe Set-side (issu du MBG fichier devices_mbg.csv)

Données systèmes à renseigner identique à toutes adresses MAC

- sip proxy ip : Adresse publique ou nom du MBG
- sip registrar ip : Adresse publique ou nom du MBG
- https server : Adresse publique ou nom du MBG
- https path : Valeur du hash du MiVoice 5000
- keyboard script : URL d'accès à l'iPBX pour les postes Remote Worker

6.4 **GESTION DES POSTES REMOTE WORKER PAR TMA**

6.4.1 PRÉREQUIS

Le fichier CSV est disponible (créé à partir du fichier Provisionning). Se référer au paragraphe 6.3.

6.4.2 DÉPLOIEMENT À PARTIR DU SERVEUR DU TÉLÉCHARGEMENT

6.4.2.1 Principe

L'action consiste à partir du menu **Déploiement** de l'application TMA, d'envoyer sur le serveur de téléchargement dédié aux postes Remote worker les éléments suivants :

- Le certificat CA_Mitel.pem est à déposer (Champ Autre fichier, template, certificat ...)
- Fichier(s) de données spécifiques mac.cfg généré à partir de l'import d'un fichier csv (Champ Fichier (csv) remote workers)



Note : Le menu "Fichier (csv) spécifique" est grisé car inutile pour la gestion des remote workers, ce menu est utile uniquement pour envoyer des fichiers spécifiques sur un serveur de téléchargement pour les postes no Remote Worker.

6.4.2.2 Déploiement par TMA embarqué

Le serveur FTP embarqué doit être actif.

L'action consiste uniquement à générer le fichier remote Worker et à envoyer le certificat:

Pour les autres fichiers, le serveur FTP embarqué contient déjà la bonne version logicielle "postes" et le fichier de données globales associés

A partir du Menu Déploiement :

- Sélectionner le serveur "local" dans la liste des serveurs FTP "Remote Workers",
- A partir du champ **Fichier (csv) remote workers**, importer le le fichier "csv" relatif aux Remote Worker issu du fichier provisionning défini au paragraphe 6.3
- A partir du champ Autre fichier, template, certificat ...), importer le fichier certificat,
- Cliquer sur Valider.

L'action est lancée immédiatement.

Le déroulement de l'action est consultable à partir du menu Suivi des actions et Journal des évènements.

Lorsque l'action est terminé, le message Déploiement réalisé est visualisé.

6.4.2.3 Déploiement par TMA géré à partir MiVoice 5000 manager

A partir du Menu Déploiement

- Choisir un serveur dans la liste des serveurs Remote workers,
- Eventuellement choisir une version logicielle dans la liste "Version logicielle",
- Eventuellement importer un fichier de données globales,
- A partir du champ **Fichier (csv) remote workers**, importer le le fichier "csv" relatif aux Remote Workers issu du fichier provisionning défini au paragraphe 6.3.
- A partir du champ Autre fichier, template, certificat ...), importer le fichier certificat.
- Cliquer sur Valider.

L'action est lancée immédiatement.

Le déroulement de l'action est consultable à partir du menu Suivi des actions et Journal des évènements.

Lorsque l'action est terminée, le message Déploiement réalisé est visualisé.

6.5 **VISUALISATION/INVENTAIRE DES POSTES REMOTE WORKER**

Une fois l'action de déploiement déroulée avec succès, la liste des postes Remote Workers est visualisable à partir du menu principal de l'application TMA, sélectionner le menu **Inventaire**.

Dans le menu **Inventaire**, bouton **Gestion des remote workers**, présentation des listes des postes "remote workers" par site.

hier Edition Affichage F	150/tma/index.php?module=inventory avoris Outils ?		<u>ا + 9</u>	C D	Gestion des te	erminaux - Inv ×		100	Ω û
치 Mitel 🛛	Gestion des termina	x							Maquette2/Multi Utilisateur: M745
Accueil	Inventaire								
Configuration de application	Gamme Données de filtrage	бхххі		V		Modèle			V
Configuration des erveurs	Site	V		Adı	resse IP		Adress	e Mac	
nventaire	Version logicielle Chiffrement	~	~	Dai Rei	ta globale mote Worke	r 🗸	Data s	pécifique	
estion des logiciels	Filtrer								
Configuration des ostes	Q 9 terminaux dont :								
Déploiement	 7 / 9 en version logici 0 / 9 en version logici 2 / 9 dans une autre v 	elle de production C ielle de test Q version logicielle Q	٤ د						
xport de la onfiguration des	Numéro Logué Label	Logout Périodique	Site	Modèle	Version logicielle	Adresse IP	Adresse Mac	Ligne Data globale	Data N° spécifique site
ostes	61100 💙		AXL- 160	6865i	4.2.0.2011	192.168.100.76	00-08-5D-42-AF-09	1	12 11
uivi des actions	62100 💙		ACS- 155	6867i	4.2.0.2011	192.168.100.95	00-08-5D-3F-12-A8	1	10
ournal des	62101 💙		ACS- 155	6737i	3.3.1.8202	192.168.100.87	00-08-5D-30-8E-D1	1	10
Venements	62102 💙		ACS- 155	6730i	3.3.1.4358	192.168.100.86	00-08-5D-11-DB-FC	1	10
onfiguration iPBX	62103		ACS- 155	Sip				1	10
		_	ACS-	Sin				1	10
	62200		155	oip					
	62200 62201 O	st	155 ACS- 155	6873i	4.2.0.2011	172.15.0.15	08-00-0F-9F-74-04	1	10

Dans le cas TMA Embarqué : Une seule liste "local"

L'icône 🗢 est relatif aux postes Remote Workers et indique que le poste est déployé et connecté.

Actions possibles : Visualisation ou Suppression

Visualisation : Fenêtre "Gestion des remote workers "

Liste des adresses MAC des postes "remote worker" qui ont été déployés

Un ou plusieurs postes peuvent être supprimés impliquant une suppression du fichier spécifique en local et sur le serveur FTP

Suppression : Suppression de tous les fichiers spécifiques associés aux terminaux décrits dans la liste en local et sur le serveur de téléchargement.

Une fonction Filtrage est également disponible.

7 DÉPLOIEMENT DES POSTES REMOTE WORKER

✓ Commun aux architectures MBG stand alone, MBG embarqué dans MiCollab ou MBG en Cluster

L'administrateur récupère l'adresse MAC du poste 6800 SIP ou 6900 IP phone destiné à l'utilisateur distant.

7.1 CONFIGURATION DE L'IPBX DE RATTACHEMENT POUR CHAQUE POSTE REMOTE WORKER

7.1.1 AVEC RCS

URL d'accès au serveur RCS : https://rcs.aastra.com/rcs/login.php

A partir de l'écran d'accueil du RCS

- Dans le menu Phones, renseigner les différents champs comme suit :
- Les adresses MAC de chaque poste attaché à l'IPBX défini ci-dessous,
- Entrer le nom du serveur de configuration (iPBX),
- Branding : None
- Firmware Override :
 - o Le poste 6900 peut être migrer du firmware Minet vers le firmware SIP par cet opération
 - Prendre un firmware SIP, avec une version minimale 5.0.0.
- Cliquer sur **Save**.



Le poste distant, suite à un reset usine (en mode SIP) se connectera au serveur RCS et récupérera automatiquement l'adresse du MBG associé à l'iPBX considéré.

7.1.2 SANS SERVEUR RCS

La configuration est à réaliser par l'administrateur ou par l'utilisateur (selon les instructions données par l'administrateur) pour chaque poste en Remote Worker.

Effectuer au préalable un reset factory du poste via le menu **Reinit.>Retour à la configuration usine**. Se connecter à l'interface Web du poste : **https:\\@IP du 6800 SIP ou 6900 IP Phone (en mode SIP)** Dans le menu **Serveur configuration** :

Renseigner les valeurs suivantes :

- Protocol télécharg : HTTPS,
- Serveur HTTPS : Le nom ou l'adresse de l'adresse publique du MBG,
- **Chemin HTTPS** : Le chemin d'accès intégrant la clé hash de l'URL permettant aux postes de télécharger leur fichier de configuration. Voir valeur paragraphe 5.2,

Exemple : https://name_server:4445/3f52a279885152701d8f2f39d9bcfc36/ftp_67xxi

• Port HTTPS : Port correspondant pour la liaison 4445.

Enregistrer alors les paramètres, puis effectuer un simple démarrage du poste. Il peut être nécessaire de désactiver les options DHCP.



Le poste distant, suite à un redémarrage, standard se connectera ensuite à son iPBX de rattachement via le MBG et récupérera ses fichiers de configuration.

8 CONFIGURATION DES NUMÉROS D'URGENCE POUR LES REMOTE WORKERS FIXES

IMPORTANT :

Pour ce paragraphe, se référer parallèlement au document Mitel Gateways et MiVoice 5000 Server – Manuel d'Exploitation pour la configuration du Plan de numérotation, des numéros abrégés et des numéros spéciaux pour les appels d'urgence. Ce document est disponible sur le site Mitel.

8.1 **PRINCIPE**

Pour un travailleur distant l'appel vers un numéro d'urgence doit être effectué vers le service concerné relatif à sa localisation.

Exemple : Si le 18 est composé par le travailleur distant, l'appel est effectué vers le numéro public des pompiers de la région considérée.

Dans le cas où les télétravailleurs sont situés sur différents sites et raccordés via un MBG, la localisation à base adresse IP n'est pas adaptée car dans ce cas tous les abonnés sont vus avec la même adresse IP.



Pour résoudre ce contrainte les numéros abrégés sont utilisés. Les numéros abrégés peuvent être définis selon la hiérarchie administrative.

Pour chaque hiérarchie les numéros abrégés peuvent être définis avec des numéros publics différents.

Pour appliquer ce mécanisme aux numéros spéciaux, la configuration du numéro spécial doit être modifiée dans le menu des numéros spéciaux.

En exemple, si un utilisateur compose le 119, soit le 00130964718 soit le 00130964719 sera appelé, selon sa hiérarchie (localisation) administrative de l'abonné.

De cette manière, un groupe de personnes appartenant à la même hiérarchie administrative peut appeler le même numéro de service d'urgence en composant simplement le même numéro spécial.

Les étapes principales pour permettre les appels d'urgence vers des numéros publics différents et relativement à la localisation sont les suivantes :

- Le principe est de regrouper les abonnés d'un ou plusieurs sites ayant la même localisation géographique dans la même hiérarchie administrative.
- Créer des hiérarchies administratives différentes par région géographique des agences.
- Affecter une hiérarchie administrative identique pour chaque abonnement d'une même agence (Société1/Agence 1 dans l'exemple)
 Cette hiérarchie administrative doit correspondre à la localisation de l'agence des abonnés.

- Définir des numéros abrégés en fonction de la hiérarchie administrative
- Configurer les numéros spéciaux (numéros d'urgence) relatifs au numéro abrégé et les affecter respectivement selon la hiérarchie administrative. Ex :
 - Configurer les numéros spéciaux avec le préfixe de numéro abrégé (Ex: * 3529) combiné avec le numéro précédemment déclaré du service d'urgence à composer (00130964018).
- Déclarer dans l'annuaire des fiches externes le numéro d'appel public des services d'urgence requis de chaque région géographique et leur affecter le même numéro abrégé avec la hiérarchie administrative correspondante à la région concernée.

De cette manière, un groupe de personnes appartenant à la même hiérarchie administrative peut appeler le même numéro de service d'urgence en composant simplement le même numéro spécial.

8.2 **CONFIGURATION**

 Regrouper les abonnés d'une ou plusieurs agences ayant la même localisation géographique dans la même hiérarchie administrative.

Menu Abonnés>Annuaire>Hiérarchies administratives.

Accueil Web Admin		Hiérarchies administratives
Abonnés		Service téléphonie>Abonnés>Annuaire>Hiérarchies administratives (1.1.4)
Annuaire		
Hierarchies administratives		
Système		Hierarchie
Plan de numérotation		Agence HHAI
Réseau et liaisons		 Bureaul
Accueils		Bureau3
Messagerie et topalités		Bureau4
Liens rapides		
Liens rapides		Bureau6
Accueil Web Admin	Abonnement 2	100
Abonnés	Service téléphonie>A	bonnés>Abonnements>Caractéristiques (1.2.3)
Abonnements Caractéristiques		Par son numéro d'annuaire 2100
Système	Caractéristiqu	es Annuaire Terminaux Touches Renvois Domotiques Répertoire Multi-lignes Fonctions
Plan de numérotation	Genre	······································
Réseau et liaisons	Nom	ABO 2100
Accueils Mossagaria et topalités	Fonction	×
Liens rapides	Hiérarchie	STE 0/SERV 0
	Confidentialité	Agence HHA1/Bureau1
	E-mail	Agence HHAI/Bureau3
		Agence HHA1/Bureau4
	SIP URI	Agence HHA1/Bureau5
		Agen
	Localisation	Agence HHA1/Bureau8
	Label	Agence HHA1/Bureau9
	Secrétaire	Agence HHA3/Bureau1

 Déclarer dans l'annuaire des fiches externes le numéro d'appel public des services d'urgence requis de chaque région géographique et leur affecter le même numéro abrégé avec une hiérarchie administrative différente.

Menu Abonnés>Annuaire>Fiches externes

Accueil Web Admin	Modification fiche exter	rne : POMPIER1
Abonnés	Service téléphonie>Abonnés>Ar	nnuaire>Fiches externes>Modification (1.1.2.2)
Annuaire Fiches externes Modification	Nom Prénom	Pompier1
Modification fiche externe : POMPIER1	Genre	MV
Système	Confidentialité	Liste verte 🖌
Plan de numérotation	Numéro abrégé	529
Réseau et liaisons	Numéro	00130964718
Accueils	Numérotation complète	
Messagerie et tonalités	Hiérarchie	Agence HHA1/Bureau1 🗸
Liens rapides	E-mail	Toutes Hierarchies Agence HHA1
		Agence HHA1/Bureau1
	SIP URI	Agence HHA1/Bureau2 Agence HHA1/Bureau3
	Localisation	Agence HHA1/Bureau4 Agence HHA1/Bureau5
	Adresse postale	Agence HHA1/Bureau6

- Configurer les numéros spéciaux avec le préfixe de numéro abrégé (Ex: * 3529) combiné avec le numéro précédemment déclaré du service d'urgence à composer (00130964718).
- Pour appliquer ce mécanisme aux numéros spéciaux, modifier la configuration du numéro spécial (11) 19 dans le menu des numéros spéciaux ci-dessus, comme illustré ci-dessous.
- Modification du numéro spécial avec le numéro abrégé considéré (*3529)

Numéros spéciaux LISTE 1 pour CODE 0						
Service téléphonie>Plan de numérotation>Numéros spécia	uo-Définitio	on des numéros	spéciaux (3.6.2)			
			Numéro 3			
			num etendu jour			
			num etendu nuit			
			ubeue Numéra 4			
			num étendu jour			
			num étendu nuit			
			libellé			
			Numéro (1)5			
			num étendu jour	015		
			num étendu nuit			
			libellé	SAMU		
			Numéro 6			
			num etendu jour			
			num etendu nuit			
			ubelle			
			num étendu iour	017		
			num étendu nuit	017		
			libellé	POLICE		
			Numéro (1)8	(OLIOC		
			num étendu jour	*3529		
			num étendu nuit			
			libellé	POMPIER		
Visu dos pumáros spásioux pour CODE 0						
visu des numeros speciaux pour CODE o						
Service téléphonie>Plan de numérotation>Numéros spéciaux>Visualisat	tion des	numéros s	péciaux (3.6.3)			
	Liste	Nume	ro Numéro	o de jour 📗	Numéro de nuit	Libellé
	0	(11)2	0112			URGENCE
	0	(11)5	0115			SAMU SOC
	õ	(11)0	0110			MAITRAIT
	1	(1)5	015			CAME
	1	(1)7	015			3AMU BOLLCE
	1	(1)/	01/			POLICE
	1	(1)8	*3529			POMPIER

Dans l'annuaire, le même numéro abrégé est associé à deux numéros publics correspondants à deux localisations.

Visualisation des numéros abrègés Service téléphonie>Abonnés>Annuaire>Visualisatio	ns>Numérotatio	n abrégée générale (1.1	.5.3)	ې 🞝 🖨	ን ሬ
	N° abrégé	Numéro	Nom	Autorisé pour	
	(*3) 001	01, 1004001	EXT601	Toutes Hierarchies	
	(*3) 002	0130014512	Nouvel_essai	Toutes Hierarchies	
	(*3) 111		S.Paja	Toutes Hierarchies	
	(*3) 114	208	ABO 208	Toutes Hierarchies	
	(*3) 123		lhl	Toutes Hierarchies	
	(*3) 168	5225	ABO 5225	Toutes Hierarchies	
1	(*3) 209	119	Y.Houmaire	Toutes Hierarchies	
-i-	(*3) 224	01000000001	Abregeos	Toutes Hierarchies	
	(*3) 333	015655 2000	E.ABO 6000	Toutes Hierarchies	
	(*3) 428	4017	Marco	Agence HHA1/Bureau1	
	(*3) 428	00120013705	Camille	Agence HHA1/Bureau2	
	(*3) 443	5600	Test samu	Toutes Hierarchies	
	(*3) 529	00130964718	Pompier1	Agence HHA1/Bureau1	
	(*3) 529	00130964719	Pompier2	Agence HHA1/Bureau2	
	(*3) 530	0'	S.Henri	loutes Hierarchies	
	(*3) 600		ABO 600	Toutes Hierarchies	
	(*3) 650	011000.0000	Abo650	Toutes Hierarchies	
	(*3) 666	0110 100000	ABO 8123455000	Toutes Hierarchies	

Cette configuration peut être répétée autant de fois que les numéros d'urgence sont différents selon la localisation : Pompiers, hôpital, police, etc).

9 CONFIGURATION DU MODE OTT POUR LES ACCÈS AUX APPLICATIONS WEB CLIENT ET USER PORTAL

9.1 **PRINCIPE**

Cette configuration permet aux travailleurs distants d'accéder via Internet en mode OTT et sans VPN aux applications :

- MiVoice 5000 User Portal via MiVoice 5000 Manager,
- MiVoice 5000 Manager Web Client,
- MiVoice 5000 User Portal embarqué.



Note : Concernant Manager User Portal, la fonctionnalité est également disponible pour les utilisateurs déclarés sur les sites en version < 8.0 (et ≥ 6.5).

Le principe est d'autoriser l'accès à ces applications au travers du MBG.

L'accès est réalisé par Internet et en https via une session MBG Controller en mode OTT.

Via Internet, le FQDN de Mivoice 5000 Manager doit être résolu sur l'adresse IP du MBG quand on est sur INTERNET.

Accès au User portal en mode OTT



Le User Portal (MiVoice 5000 Manager ou intégré au MiV5000) est accessible de n'importe où par Internet grâce au FQDN permettant au travailleur distant de programmer les touches du terminal distant.

L'URL est identique dans le mode local ou dans le mode OTT.

Le MBG est utilisé comme proxy pour permettre l'accès depuis Internet. L'adresse IP locale du MBG au doit être déclaré comme proxy de confiance dans le MiVoice 5000 Manager ou Web Admin.

Le User Portal embarqué utilise le port HTTPS 443.

L'accès au User Portal est compatible avec toutes les versions de MiVoice 5000 (R6.5 et versions ultérieures)

L'accès en mode SSO au User Portal n'est pas disponible pour le User Portal embarqué. Disponible uniquement pour le User Portal du MiVoice 5000 Manager.



Note : Dans la version actuelle, la séparation de flux n'est pas compatible avec le User Portal embarqué.



Accès au Web Client MiVoice 5000 Manager en mode OTT

Le Web Client (MiVoice 5000 Manager ou intégré au MiV5000) est accessible pour le travailleur distant, de n'importe où par Internet grâce au FQDN permettant au travailleur distant d'a.

L'URL est identique dans le mode local ou dans le mode OTT.

Le MBG est utilisé comme proxy pour permettre l'accès depuis Internet. L'adresse IP locale du MBG au doit être déclaré comme proxy de confiance dans le MiVoice 5000 Manager ou Web Admin.

Pour les accès admin de la Web Admin, les utilisateurs et les comptes associés doivent être déclarés dans la configuration du Proxy.

9.2 SYNTHÈSE DES DIFFÉRENTES ÉTAPES

9.2.1 CONFIGURATION MBG

Dans le menu Remote proxy/Domain List :

- Cliquer sur +,
- Entrer le WAN-side FQDN du MiVoice 5000 Manager (cas du Web Client ou User Portal) ou du MiVoice 5000 Server (Cas du User Portal embarqué) pour la résolution sur le MBG
- Sélectionner le service MiV5000 Over Internet Access.et cocher la case Enabled.

Exemple : Cas du MiVoice 5000 manager.

🛤 Mitel 🛛	Mitel Standa	ard Linux		
Applications MiVoice Border Gateway	System - Net	work 🕶 Teleworking 👻 SIP	trunking - Remote proxy -	Call recording - Troubleshooting -
Blades Status Administration	Page updated: Fri Apr 1	5 2022 16:48:33 GMT+0200 (Central I	European Summer Time)	
Web services Backup Restore View log files	Remote proxy			
Event viewer System information	Enabled	WAN-side FQDN	Allowed netblocks	Server type
System monitoring System users Shutdown or reboot Virtualization	×	managerjb.frguylab	All	MiV5000 Over Internet Access server with the following user level access enabled: MiV5000 Over Internet Access Admin level access is <i>enabled</i>
Security				

Dans le menu Remote proxy/Users,

Déclarer les utilisateurs et Créer les comptes associés pour les accès admin de la Web Admin.

siem -	Network -	elevoriting + SIP true	king - Remote proxy -	Call recording - Troubleshooting -				Search	h
updated: T	fue Jul 06 2022 11:06	15 GMT=0200 (heure d'été d	(Europe centrale)						
May 12, 25	021, 12:05 p.m.	Note: As local street to ensure it is work	arring is enabled, you should know ing correctly for your environment	w that local streaming behaviour has changed in t	this release. Please monitor you	r deployment and see the MBG	documentation		
temote pro	ay users								
Active	users. Username	Name	Email address	Granted permissions	Creation date	Deferred activation date	Expiry date		
Active	Username na ' Mana	Name M second, off	Email address steve d. ' 1y@ ' '	Granted permissions MV/S00 Over Internet Access admin	Creation date April 22, 2022, 10,14 a.m.	Deferred activation date	Expiry date None	/	8

Dans le menu Remote proxy/Proxy applications

• Visualiser la liste des URLs du service MiV5000 Over Internet Access

MiV5000 Over Internet Access	a50	/userportal	/rhm	User	Admin
			/trf		
			/csv		
			/system		
			/dhcp		
			/dhcp6		
			/tma		
			/annuaire		
			/easyadmin		
			/setup		
			Avebtelephony		

9.2.2 CONFIGURATION DU TRUSTED PROXY

9.2.2.1 Cas du Web Client et User Portal sur MiVoice 5000 Manager

Configurer l'adresse IP du MBG dans les proxys autorisés par le MiVoice 5000 Manager.

Menu Configuration – Onglet Protection.

Se référer au document MiVoice 5000 Manager - Guide Utilisateur

Paramètres	Heures de campagne	Export	Purce	Portée	Acquaire	Certificata	Filtrates	User Portal	Web Client	Serveur de mise à niveau	Surveillance iPRX	Protection
Blocage automati	in a	- Jon							and then	and a stand of miles	and a state of the state	
				-								
vicavel, cette oba	son pour bioquer une aures	ISE IF SVECT	top dieche	ics de login	n.							
Activer le blo	cage automatique											
Line advector IF	a ara blocuía si alla attain	t la nombre	dichara .	da locia da	na la ofricale	da terres ci da						
Cite screese in				ou rogin ou								
Tentative de	e login		-									
Période (mi	inutes)				10							
Activer I	Texpiration du blocage											
Activer I	Texpiration du blocage	ece IP eora	Alterado	arrie la r	ombra dharr	as andrifides r	deserve					
Quand Tex	Texpiration du blocage xpiration est activée, l'adre	sse IP sera	débloquée	après le n	iombre d'heuri	es spécifiées c	i dessous.					
Quand Fee	Texpiration du blocage xpiration est activée, l'adre	sse IP sera	débloquée	après le n	iombre d'heuri	es spécifiées c	i dessous.					
Cuand Fee Déblog	Texpiration du blocage xpiration est activée, l'adre uer après (heunes)	sse IP sera	débloquée	e après le n	nombre d'heure	es spécifiées c	i dessous.					
Cuand Tex Déblog	Texpiration du blocage xpiration est activée. l'adre uer après (heures)	ose IP sera	débloquée	e après le n	nombre d'heur	es spécifiées c	i dessous.					
Cuand Fee	Texpiration du blocage xpiration est activée, l'adre uer après (heures)	ese IP sera	débloquée	e après le n	iombre d'heuri	es spécifiées c	i dessous.					
Cuand Fex	Texpiration du blocage xpiration est activée, l'adre uer après (heures)	sse IP sera	débloquée	e après le n	tombre d'heun 1 tresse IP blog	es spécifiées c	i dessous. Applic	quer				
Cuand Fex Quand Fex Deblog	Texpiration du blocage xpiration est activée, l'adre uer après (heures)	sse IP sera	débloquée	e aprés le n Ad	rombre d'heuri 1 resse IP blog	es spécifiées c	i dessous. Applic	quer				
Activer I Quand Fer Déblog	Texpiration du blocage xpiration est activée, l'adre user après (heures)	sse IP sera	débloquée	e après le n	tombre d'heuri 1 tresse IP blog	es spécifiées c	i dessous. Applic	quer				
Active I Quand Fer Déblog Proxy autorisés Quand un utilisa	Texpiration du Mocage xpiration est activée, l'adre user après (heurse) steur se connecte à travers	sse IP sera	débloquée	après le n Ad utilisera l'	rombre d'heurr 1 tresse IP blog adresse IP du	es spécifiées c	i dessous. Applic	quer				
Activer I Quand Fex Déblog Proxy autorisés Quand un utilisa	Respiration du blocage repiration est activée, l'adre uer après (heures) abur se connecte à travers	sse IP sera	débloquée	après le n Ad utilisera N	rombre d'heure I resse IP blog adresse IP du	es spécifiées c	i dessous. Applic	quer				

9.2.2.2 Cas du User Portal embarqué

Dans la Web Admin, menu Service téléphonie>Système>Sécurité>Sécurité WEB, onglet Proxy autorisé :

• Entrer le ou les adresses des MBG(s) autorisés pour l'accès en mode OTT.

Scurit Web Admin Systems Sourds WBB Pain de numérotation Reseau et liaions Accurit Web Admin Messagerie to tradités Linns rapides Securits WBB Securits Securits WBB Sec	🕅 Mitel 🕴 Servio	ce téléphonie	admin MiVoice 5000
nuese i co	Accueil Web Admin Abonnés Système Sécurité WEB Plan de numérotation Réseu et laisons Accueils Messagerie et tonalités Liens rapides	Securité WEB Intervention force bruite Proxy autoritot Adresse IP foloculon force bruite Adresse IP 4 Adresse IP 5 Adresse IP 5 Adresse IP 6 Adresse IP 1 Adresse IP 1 Adresse IP 1 Adresse IP 2 Adresse IP 3 Adresse	

10 CONFIGURATION DU MODE OTT POUR LE SYSTÈME SIP DECT

10.1 **INTRODUCTION**

Deux outils peuvent être utilisés pour la configuration du système SIP-DECT :

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

2

Note : L'accès en Web sur la borne dite « OMM » est également utilisable mais avec un peu moins de paramétrage avancé que sur l'OMP. Les possibilités réduites dans ce mode peuvent néanmoins suffire dans de nombreux cas

Outils disponibles sur le site de Mitel :

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



10.2 **ARCHITECTURE**



Exemple de configuration



10.3 CONFIGURATION MIVOICE 5000

Déclarer les abonnés considérés.

Se référer aux documents :

- MiVoice 5000 Server Manuel Exploitation
- MiVoice 5000 Manager Guide Utilisateur.

10.4 **CONFIGURATION MBG**

SIP options

Menu MBG>System>Settings>SIP Options

Certificate Mitel V Export root cert @	Protocols Access profile UDP Public ▼ TCP Public ▼ TCP/TLS Public ▼	Device ↔ device local streaming Device ↔ trunk local streaming Codec support Unrestricted ✓
Set-side RTP secures of the secure of the se	nty Accept either SRTP or RTP inbound to this server	PRACK support Send options keepalives Options interval Challenge methods Invite Refer Prack
Outbound SRTP only AVP+crypto ORTP only Preferred AES_CM_128_HMAC_S cipher	Lo our best to send only AV+ + drypto outbound from this server	KPML username KPML password Confirm KPML password
ICP-side RTP secur Inbound SRTP only	rity Accept either SRTP or RTP inbound to this server	Registration Mode Max Set-Side Set-side registration expiry time ICP-side registration expiry time Add another
SKTP or KTP RTP only SRTP only SRTP only AVP+crypto RTP only	Do our best to send only AVP + orypto outbound from this server	fivoip mile.com Blank any field you no longer want.
Preferred AES_CM_128_HMAC_S cipher Tone Injection	HA1_80 V	SIP adaptation support SIP adaptation receive pipeline SIP adaptation send pipeline SIP adaptation send pipeline
Er	nable 🗌	Permit weak SIP passwords

Menu MBG> TeleWorking> SIP

hage ar prome			
Duffle		Connection	
Frome		Connection	
Enabled		Configured ICP	mv5k-site5 💙
Description	plharidon 4474	Availability	Everywhere V
Set-side Authentication		ICP-side Authentication	
Username	plharidon	Username	4474
Password	Change password	Password	Change password
Confirm		Confirm	
Protocol		Media	
PRACK support	Use global setting 💙	Local streaming between device calls	Use global setting 🗸
Options keepalives	Use global setting 🗸	Codec support	Use global setting 🗸
Heartbeat interval		Tone Injection	
Challenge methods	Use primary setting Override		
		Enable	
Set-side RTP security		ICP-side RTP security	
Inbound	Use global setting 💙	Inbound	Use global setting 🗸
Outbound	Use global setting 💙	Outbound	Use global setting 💙
Preferred cipher	Use global setting 🗸 🗸	Preferred cipher	Use global setting

CONFIGURATION AVEC OM CONFIGURATOR 10.5

Cet outil simple permet :

La découverte des bornes connectés au même réseau que son PC

Le paramétrage initial des bornes RFP (adresse IP, masque, gateway...)

- Login par défaut : omm / omm •
- Mot de passe : XXXX •

OM CONFIGURATION / RFP 1 / OMM

DI Mitel						<u>G</u> eneral	Help	Options General User directory Network Interf	ive - Mitel	Networks Corporation/Documents/omc/tg	×
MAC address Docal confo P address Net mask Ref 006.00 ref 12 bb ✓ 152.468.55.01 255.255.255.0 192.168 20 005.00 rfc4.3e.c1 ✓ 192.168.65.101 255.255.255.0 192.168	uter OMM address 2nd .65.253 192.168.65.101 - .65.253 192.168.65.101 -	I OMM addr	TFTP server 0.0.0.0 0.0.0.0	TFTP file nam unused unused	e Tasks Scan Add RFP Clear Lis	ŧ				OK Cancer	
	🕅 Mitel									<u>G</u> eneral <u>H</u> elp	
	MAC address	local config	P address	Net mask	Router	OMM address	2nd OMM addr	TFTP server	TFTP file name	Tasks	
Detail Data 08:00:0f:c4:3e:c1	✓ 08:00:0f:c4:3e:c1	- ž	192.168.65.102	255.255.255.0	192.168.65.253	192.168.65.101	-	0.0.0.0	unused	Scan	
General OpenMobility Other										Add RFP	
Use local config 🌍										Clear List	
IP Address 192.168.65.101										Edit configuration	
Net Mask 255.255.255.0										Copy Configuration	
Router 192.168.65.253										Paste Configuration	
	Detail Data 08:00:0f:c4:3e:c1									Send Configuration	
	General OpenMobility	Other								Factory Reset	
										Remove selected REP	
	OMM address	192.168.65	5.101		DNS addresses	1	92.168.65.253			Sava DED Confin	
	TFTP server address	0.0.0.0			Ri P configuratio					Load DED Confin	
	TFTP file name	unused								Load RPP Conng	
	Syslog server address										
	Syslog server port										

10.6 **CONFIGURATION OMP (OPEN MOBILITY PORTAL)**

Cet outil avancé permet la configuration du système SIP-DECT

- Login par défaut : omm / omm
- Mot de passe: XXXX



OMP STATUS

🕅 Mitel	o Q 🖌				<u>G</u> eneral <u>H</u> elp
Configuration Status System Sites DECT base stations WLAN DECT phones Conference rooms System features Licenses Support	Overview DECT base stations Users Devic System Uptime ID Day(s) Or Licenses Standby OMM Synchronization state OECT base stations DECT base stations DB import/export Downloading new firmware to portable parts Provisioning OMM configuration file processing Emergency location configuration	es Stes ⊂ 3 h 15 min ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	onference Provisioning Provisioning health report Features OM Integrated Messaging & Alerting service User data server MOM control 802.1x state OMM certificate server Provisioning certificate server 802.1x certificate server SIP certificate server	√ √ × × × ×	
Info console					
PARK: 31100723550549	i 4				🚿 10.144.85.59

OMP - SITES

🕅 Mitel	😳 Q 🖌			
Configuration	Overview DECT base stations Us	sers Devices Sites	Conference Provisioning	Provisioning health report
Status	General			
System	Total	2		
Sites	Contains REP(s)			
DECT base stations				
WLAN	Wideband audio G.722	0		
DECT phones	Enhanced DECT security	0		
Conference rooms	Secure real time transport protocol	1		
System features				
Licenses				
Support				

BASIC SETTINGS 1/2

🕅 Mitel	🔯 Q 🖌				
onfiguration	DTMF settings Int	ercom/Push-to-talk	Supplementary services	Conference	Security
Status	Dasic settings Advan	rea seangs	registration trainic snaping	Backup setti igs	RTP Settings
System	General				
Basic settings	Proxy server	195.25.132.163			
Advanced settings	Proxy port	5061			
SIP	Registrar server	195.25.132.163			
Provisioning	Registrar port	5061			
User administration	Degistration period	CO			
Data management	Registration period	80 360			
Sites	Globally routable user agent URL	\checkmark			
DECT base stations	Outbound proxy server				
WLAN	Outbound proxy port	5061			
DECT phones	Transport protocol	Persistent TLS			
Conference rooms					
System features	Local port range				
Licenses	PP user UDP/TCP	5060 5060	Conference room UDP/TCP	4060 406	0
Support	PP user TLS	5061 5061	Conference room TLS	4061 406	1
					·

BASIC SETTINGS 1/2

🛤 Mitel	🔅 Q 🖌				
configuration	DTMF settings	Intercom/Push-to-talk	Supplementary services	Conference	Security
Status	Basic settings	Advanced settings	Registration traffic shaping	Backup settings	RTP settings
System	General				
Basic settings	Proxy server	195.25.132.163			
Advanced settings	Proxy port	5061			
SIP	Registrar server	195.25.132.163			
Provisioning	Registrar port	5061			
User administration	Registration period	3600 86			
Data management	Olebelly systems	-			
Sites	Globally routable user ager	it URL 🔽			
DECT base stations	Outbound proxy server				
WLAN	Outbound proxy port	5061			
DECT phones	Transport protocol	Persistent TLS	✓		
Conference rooms					
System features	Local port range				
Licenses	PP user UDP/TCP	5060 5060	Conference room UDP/TC	P 4060 40	60
Support	PP user TLS	5061 5061	Conference room TLS	4061 40	61

OMP - RFP SETTING

🕅 Mitel	🔅 Q 🖌				
Configuration	DTMF settings	ntercom/Push-to-talk	Supplementary services	Conference	Security
Status	Basic settings Adva	nced settings	Registration traffic shaping	Backup settings	KTP settings
System					
Basic settings	RTP port base	16320			
Advanced settings	Preferred codec 1	G.722			
SIP	Preferred codec 2	G.711-u-law			
Provisioning	Preferred codec 3	G.711-A-law			
User administration	Preferred codec 4	0 720 4			
Data management	Dreferred sector time	0.725-A			
Sites	Preferred packet tille	20	Nacc.		
DECT base stations	Silence suppression				
WLAN					
DECT phones	Receiver precedence on codec negotiation				
Conference rooms	Eliminate comfort noise packets				
System features					
Licenses	Single codec reply in SDP				
Support	Source port filter				

OMP – GENERAL 1/2

🕅 Mitel	🧔 Q 🖌			
Configuration	Branding image URL	OMM certificate server	802.1× certificate serve	er SIP certificate server
Status	General System	undate Provi	sioning certificates	Provisioning certificate server
System	Provisioning URL			
Basic settings	Active		Changing one of the configu	uration file URL settings may cause
SIP	Protocol	HTTPS 💟		
Provisioning	Port		Use default port 🧹	
User administration	Server			
Data management	Path	[/ipdect.cfg, /-	<mac>.cfg, /<park>.cfg</park></mac>
Sites				
DECT base stations				
WLAN	Security			
DECT phones	Validate certificates		low unconfigured trusted certificates	
Conference rooms	Validate expires	V In	port certificates with first connection	
System features	Validate host name	T	_S version	Auto 🕑
Licenses	Security level	High 💟		
Support				

OMP - GENERAL 2/2

🕅 Mitel	o Q 🖌				
Configuration	Branding image URL	OMM certificate serve	r 802.1× certificate	server SIP certifica	ate server
Status	System credentials	Event trigger	User data import	Software update URL	MA.
System Basic settings Advanced settings	Provisioning URL Active	m update Pro	Changing one of the c logout of all users!	on figuration file URL settings may cau	Ise
SIP	Protocol	https 🕑			
Provisioning	Port		Use default port 🛛 🗸		
User administration	Server				
Data management	Path		/ipdect	.cfg, / <mac>.cfg, /<park>.cfg</park></mac>	
Sites					
DECT base stations					
WLAN	Security				
DECT phones	Validate certificates	V	Allow unconfigured trusted certificate	es 🗌	
Conference rooms	Validate expires	V	Import certificates with first connection	in 👘	
System features	Validate host name	v	TLS version	Auto	
Licenses Support	Security level	High 💟			

OMP – ADVANCED SETTINGS

onfiguration	DTMF settings	Intercom/Push	-to-talk	Supplementar	y services	Contere	nce	Securit
Status	Basic settings	Advanced settings		Registration traffic shaping	9	Backup settings		RTP settings
System	General					12000000028		
Basic settings	Remove route header		11			User agent info	1	
Advanced settings	X-Aastra-Id info		~		User agent info -	compatibility mode		
SIP	DNS SRV failover follow	ving registration	10		M	utiple 180 Ringing	7	
Provisioning	Registration failed retry	Simer	120 540			Transaction timer	4000	mee
User administration Data management	Registration timeout retr	y timer	180 840			Blacklist time out	5	min
Sites	Determine remote party	by	P-Asserted-Ide	ntity		Dial terminator		1
DECT base stations . WLAN	Call reject state code (u	ser reject)	406		Cal (de	reject state code vice unreachable)	405	<u> </u>
DECT phones	Session timer		0 840		inc	coming call timeout	100	54C
Conference rooms	SP contact matching		URL					
System features	Evolet MAI automation		2		Funded Mild a	theoristics seried	-	1 440
Licenses	Capitor and Analysis pro-		10		Coproc and a	anan foru beren	00400	
Support	Semi-attended transfer							
	Transfer mode		Bind		Refe	r-to with replaces		

Cocher la case **X-Aastra-id info** en ayant impérativement effectué une pré-affectation DECT-IP sur les abonnements concernés côté MiVoice 5000.

🕅 Mitel	🔅 Q 🤞	/					<u>G</u> ener
Configuration Status System Sites DECT base stations WLAN DECT phones Conference rooms System features Licenses	D 1 det 2 Sta	Name ELIN number fault - eShowroomS	Wideband audio 36 36	Enh. DECT security 36 36	SRTP	Number of RFPs 0 2	Tasks Create Configure Delete Select columns
Support	General Name Emergency location identification number Wideband audio G.722 Enhanced DECT security SRTP	SiteShowroomSRTP	Changing fixed par	y site parameters, may ts in this site.	restart radio		

OMP - SITES

🕅 Mitel	Ø	С	2 🖌								<u>G</u> eneral
Configuration Status System Sites DECT base stations Device list Paging areas Capturing	R 0x0	FP ID 000 C	Name DMM RFP 1	MAC address 08:00.0F.C4:3E:C1 08:00.0F.E0:12:BB	P address 10.144.85.59 10.144.85.60	DECT cluster 1 1	Paging area 0 0	HW type RFP 48 RFP 48	Connection state	Active	Tasks Create Configure Delete Re-enroliment ¥ Fiter Select columns
Export WLAN DECT phones Conference rooms System features Licenses Support											

OMP - SITES & BASE STATIONS 1/2

OMP - SITES & BASE STATIONS 2/2

🕅 Mitel	<u>ଡ</u> ପ	/								<u>G</u> eneral
Configuration	RFP ID Nar	ne N	MAC address	IP address	DECT cluster	Paging area	HW type	Connection state	Active	Tasks
Status	▼ 0x000 OMM RFP	1 08:	00:0F:C4:3E:C1	10.144.85.59	1	0	RFP 48	4	1	
System		100:	00.0F.EU. 12.DD	10.144.00.00	P .	,	N P 40	*	•	Create
Sites										Configure
DECT base stations										Delete
Device list										Re-enrollment
Paging areas										3¢ Filter
Capturing	DECT base station #0x00	0								Select columns
Enrolment	General DECT	WLAN H	ardware							Concol Constilling
Export										
WLAN	Name	C	OMM RFP 1							
DECT phones	MAC address	ſ	08:00:0F:C4:3E:0	21						
Conference rooms	Emergency location	ſ				_				
System features	identification number	. U								
Licenses	Sile	S	SiteShowroomSF	RTP						
Support	Building									
	Floor									
	Room				\sim					
	Conference channel	s								

OMP - DECT PHONES 1/2

🕅 Mitel	🔅 Q 🖌						<u>G</u> eneral
Configuration Status System Sites DECT base stations WLAN DECT phones	Device D IPEI 0x001 03586 001475 ▼ 0x002 10345 093413	Name 7 6 DECT 5235 2 * DECT 5232	Number/SIP user name 5235 5232	User ID 0x001 Fi 0x002 Fi	User rel. type ixed ixed	Active	Tasks Create Configure Delete 36 Filter
Overview Users Devices Conference rooms System features	Device #0x002 - User #0x002 Additional services General SIP In Authentication user name	User monitoring Conf coming calls Conferenc [5232]	iguration data	User service Messaging	Key lock		Wildcard subscription Select columns Change rel. type
Licenses Support	Password Password confirmation VIP Used for visibility checks Fixed port		port 506	1			

OMP - DECT PHONES 2/2

🛤 Mitel	Ø	Q	. /									<u>G</u> eneral
Configuration		User ID	Na	me	Number/SIP use	er name	Login/Add ID	Use	r rel. type	Rel. device ID	Active	Tasks
Status		0x001	DECT 5235		5235			Fixed		0x001	-	
System	~	0x002	[DECT 5232		5232			Fixed		0x002	· · ·	Create
Sites												Configure
DECT base stations												Delete
WLAN												3¢ Filter
DECT phones												Select columns
Overview												
Users	user	#0X002						¥				
Devices	_	Additional service	vices	User n	nonitoring ing calls	Cor	nfiguration data	Use Messar	r service sing	Key lock		
Conference rooms						-						
System features		Name		DECT 523	32							
Licenses		Number/ SIP u	user name	5232								
Support		Description 1										
		Description 2										
		Login/Additior	nal ID									
		PIN										
		PIN confirmati	ion	••••								

10.7 CONFIGURATION DES ACCÈS XML POUR REMOTE WORKER DECT SIP EN MODE OTT

10.7.1 PRINCIPE

Un abonné Remote Worker de type DECT SIP en mode OTT doit être détecté par le MiVoice 5000 en tant que Remote Worker.

Lors du déploiement, est donc nécessaire de fournir à l'OMM la clé d'accès (hash) générée au niveau du MiVoice 5000 pour renseigner les URL relatives aux fonctionnalités XML considérées (liste des appelants, la liste de renumérotation, le menu Serveur, le code d'accès à la fonctionnalité).

Cette action est à réaliser en deux étapes :

- Au niveau de la WebAdmin du MiVoice 50000 : Récupérer la valeur hash indiquant le chemin pour le téléchargement des fichiers concernant les Remote Workers.
- Au niveau de l'OMM : Renseigner la valeur de la clé hash pour les fonctionnalités nécessitant un accès XML.
- Ouverture de l'accès aux répertoires du MiVoice 5000.

10.7.2 CONFIGURATION

Récupération de la clé hash au niveau MiVoice 5000

Menu Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP (4.4.5) – Onglet Chiffrement :

🕅 Mitel 🕴 Servic	e téléphonie		admin MiVoice 5000	
Accuell Web Admin Abornés Système Plan de numérotation Réseau et laisons Coulté de sansanderes IP Accuells Messagerie et tonalités Liens rapides	Chiffrement et paramètres IP (mode basque) Since tristytone-Resau et associo-batti de tance-Chiffrement et parametres I Chiffrement Octo Doc Super	PI44S Chiffrement signalisation et voix chiffrement voix type de chiffrement Chiffrement voix 67x0	Ø ÆES 256 ▼	속 D, O 쇼 확 A C 目 너 빈 면 면
		eas Jona de fonctionnement mise à Jona le éd chiffement Génération du hash - Chemin pour le téléchargement des fichiers	ESCLAVE ▼ AUTORISE (OUI ▼) (/////////////////////////////////	

Copier et sauvegarder la valeur indiquée du hash (uniquement) dans le champ - Chemin pour le téléchargement des fichiers.



IMPORTANT : La valeur du hash est celle indiquée à gauche du champ, avant /ftp_67xx. Dans l'exemple 0d0f346508a57b3722efe61265db3c7.

Configuration de l'URL d'accès au niveau de l'OMM

A partir de l'interface d'exploitation OMM

Menu Configuration>System features>XML applications

XML applications

•

Configuration	D	Name	Server	Active
Status	0 Ci	aller list	SIPProxy	×
Status	1 R	edial list	SIPProxy	×
System	2 Pr	resence		36
07	3 St	erver menu	SIPProxy	A
Sites	4 A	ction URI		36
DECT base stations	5 Fe	eature access codes	SIPProxy	1
	6	all completion		26
WLAN	7 Pa	ark call		34
DECT phones	8	npark call		×
DECT phones	9 Pi	ickup		24
Conference rooms	10 Ta	ake		×
	11 Ci	all forward		*
System teatures	12 Ci	all routing		X
General settings	13	all protection		24
	14 V	oice box		
Feature access codes	15 H	otkey		ж
Alorm triggoro				
Alaminggera				
Digit treatment				
Directory				
Directory (comp. mode)				

• Entrer la valeur du hash en début du champ relatif à URL d'accès Path (and parameters) .

Configuration		D	Name	Server	Active
Status	0		Caller list	SIPProxy	
Sustem	2		Redial list Presence	SIPProxy	*
System	3		Server menu	SIPProxy	4
Sites	4		Action URI		×
DECT base stations	5		Feature access codes	SIPProxy	4
	6		Call completion		×
WLAN			Park call		7
DECT phones	9		Pickup		
Conference rooms			i de la completa de l		
Contelence rooms	XML application #0				
System features					
General settings	General				
Feature access codes	Active	\checkmark			
Alarm triggers	Name	Caller list			
Digit treatment	Protocol	HTTPS 🔽			
Directory	Port	4445 Use	default port		
Directory (comp. mode)	Sanuar	(c)pp			
XML applications	361961	SIPPROXY			
CoA profiles	User name	cg7450			
Licenses	Password				
Support	Password confirmation				
	Path (and parameters)	%HASH CODE%/omm.mghc/?key=2	20&na={number}		
	ок	Cancel			

La même clé Hash doit être renseignée dans les différentes URLs selon la fonctionnalité :

- Liste des appelants (Caller list) : %HASH CODE%/omm.mghc/?key=20&na={number}
- Liste de renumérotation (Redial list) : %HASH CODE%/omm.mghc/?key=18&na={number}
- Menu Serveur(Server menu): %HASH CODE%/omm.mghc/?key=0&na={nombre}
- Code d'accès à la fonctionnalité (Feature access codes) : %HASH CODE%/omm.mghc/?key=0&na={number}&fac={fac}

Ouverture de l'accès aux répertoires du MiVoice 5000

Menu Configuration>System features>Directory

Onglet General

Configuration	D		Туре	A	ctive	
	1	XML			 Image: A second s	XML directory
Status	2	LDAP			*	
System	3 4	LDAP			x	
Sites	5	LDAP			36	
DECT base stations						
WLAN						
DECT phones						
Conference rooms						
System features						
General settings						
Feature access codes	Directory entry #1					
Alarm triggers	General URL					
Digit treatment	Type	YM				
Directory		AND				
Directory (comp. mode)	Active	\checkmark				
XML applications	Name	XML directory				
CoA profiles	Search base					
Licenses	Search type	Surname				
Support	Display type	Surname, given name				
	Server search timeout	10 sec				
	ОК	Cancel				

Onglet URL

General URL	
Protocol	нттру 🕑
Port	4445 Use default port
Server	SIPProxy
User name	
Password	•••••
Password confirmation	
Path (and parameters)	%HASH CODE%/annuaire/i5xi.php?dn={number}
Use provisioning security configuration	
contiguration	

10.8 **OMM WEB**

Accès > https:\\192.168.65.101

DI Mitel SIP-DECT 8.0		
	Sustam	Login
	PARK	1F103A768B
	Password	
		OK

🕅 Mitel	SIP-DECT 8.0			Z Advanced
Status System	Status		Report	
Sites	OpenMobility Manager		SIP.DECT 8 0.HE01DI16	
Base Stations	Untime		1 Day 1:52	
DECT Phones	Licenses		Built-in license for up to 5 DECT base stations	
WIAN	Standby OMM	0	There is no OpenMobility Manager in standby mode configured	
System Eastures	OM Integrated Messaging & Alerting service		~	
Licenses				
Licenses			Base Stations	
Info	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

MILEL	SIP-DECT 8.0			Auvanceu 2 Owr
Status System System Settings	System Settings OK Cancel			
Provisioning		General settings		
SIP	System name	SR-FR-MiVB		
User	Remote access			
Administration	Tone scheme	FR V		
Time Zones		DECT settings		
DR Management	PARK	1F103A768B	(31100723550549)	
DB Management	DECT power limit 100mW			
Event Log	Encryption			
Sites	Restrict subscription duration			
Base Stations	Authenticate before ciphering			
DECT Phones	DECT monitor			
WLAN	Regulatory domain	EMEA	~	When changing the DECT regulatory doma
System Features	DECT authentication code	78280		
Licenses	DECT phone user login type	Number 🗸		
Info	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 upda	te	
	Mode	One by one ~		

🕅 Mitel 🛛	SIP-DECT 8.0			Advanced
Status System System Settings	SIP OK Cancel			
Provisioning		Basic settings		
SIP User	Proxy server	195.25.132.163		
	Proxy port	5061		
Administration	Registrar server	195.25.132.163		
Time Zones	Registrar port	5061		
SNMP	Registration period	3600	sec	
DB Management	Globally Routable User-Agent URL			
Event Log	Outbound proxy server			
Citor	Outbound proxy port	5061		
Giles	Transport protocol	Persistent TLS ~		
Base Stations DECT Phones	Local UDP/TCP port range	5060	- 5060	
	Local TLS port range	5061	- 5061	
WLAN		Advanced		
System Features	Evaluat HMR extension	Advanced		
Licenses	Explicit MMI subscription	86400	-	
Info	Lagran mmi susseignan period	00400	565.	
	Licer agent info _ compatibility mode			
	Dial terminator	u #		
	Dateminate Desistation failed retry Smor	120		
	Registration later rely unter	120	385	
	Registration theory times	180	00%	
	Session timer	4000	565.	
	Disability inter	4000	mise.	
	Discust time out	5	mn	
	incoming call timeout	180	SEC	
	Determine remote party by	P-Asserted-Identity V	leder	
	Multiple 180 Ringing			



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-D	ECT	B.O								9	Advanced	± OMP
Status System Sites Base Stations	Base Sta New Capturing s	unconfigured	I DECT bas	e stations									
DECT Cluster 1 DECT Phones WLAN System Features	Stop 2 Base Stations												
Licenses	DECT Clus	ter 1: 2 Bas	e Stations ID	Name		MAC address	IP	address	HW type	Site	RPN	Refl	ective environment
	1	6	0000	OMM RFP 1		08:00:0F:C4:3E:C1	10	144.85.59	RFP 48	2	00		×
	,	•	0001	-		08:00:0F E0:12:8B	10	144.85.60	RFP 48	2	01		×



Status	Licenses				
System Sites Base Stations	Changing these settings may cause the OpenMobility Manager to be reset. OK Cancel				
DECT Phones					
WLAN System Features		License settings	License settings		
	Installation ID	272266891	272266891		
	License file import	Choisir un fichier Aucun fichier choisi	Choisir un fichier Aucun fichier choisi		
Infe					
IIIO		General			
	License type	Built-in license for up to 5 DECT base stations			
	PARK	1F103A768B	(31100723550549)		
		System			
	Number of DECT base stations	5		Mitel SIP-DECT System License XXX	
		Messaging			
	Receiving text messages (Emergency, Locating alert) and enhanced messaging features	×		Mitel SIP-DECT Messaging & Alerting License Enterprise	
		Locating			
	Number of users allowed to be located	-	Mitel SIP-DECT Locating User License XXX		
	OM Locating application	×	Mitel SIP-DECT Locating Server License		



mitel.com

© Copyright 2015, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.