

MiVoice MX-ONE

MiVoice Border Gateway MBG - Installation Instructions

Release 7.3 SP2

March 29, 2021



Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

®,™ Trademark of Mitel Networks Corporation
© Copyright 2021, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	General	1
Chapter: 2	Application Requirements	2
Chapter: 3	Installation Notes	3
	Licensing	3
	Installing Release 11.0 on a Standalone Physical Server	3
	Installing Release 11.0 in a VMware Environment	3
	Firewall Configuration	3
	MSL Configuration	4
	MBG Configuration	4
	Phone Configuration	7
	Limitations	7
	Known Issues	8
	Upgrade Notes	8
	Appendix - Config Script	8
	Appendix - mitel.cfg Settings	9

General

This document describes how to configure a single standalone MiVoice Border Gateway (MBG) Release 11.0 server to support Mitel 6900/6800 SIP Terminals as Tele-worker devices for MX-ONE.

This document complements MX-ONE document “Mitel 6700i and 6800i SIP Terminals for MX-ONE” and provides instructions how to setup MBG as an Ingate replacement. The principle used here is to configure MBG to have secure communication on the outside towards the home worker terminals and unsecured communication on the inside towards MX-ONE. The proposed solution has the same limitations as the existing Ingate deployment.

Instructions in this document are specific to the above configuration and must NOT be used in any other deployments. For example, MiCollab 7.1 with MBG and MiCollab clients with MX-ONE.

Application Requirements

You must meet the minimum software level requirements for each application listed below so that the applications function correctly with this Release.

Application	Recommended Software Level	Comments
Mitel Standard Linux (MSL)	11.0	Refer to the <i>MBG Installation and Maintenance Guide 11.0</i> located in the Doc Center on the MiAccess Portal.
MX-ONE	7.3	-
6900	5.1 SP5	Release 5.1 SIP extensions
68xxi	5.1 SP5	Release 5.1 SP5
MBG	11.0	-

Installation Notes

The principle used here is to configure MBG to have secure communication on the outside towards the home worker terminals and insecure communication on the inside towards MX-ONE.

Licensing

The only licensing required is a MiVoice Border Gateway base kit (physical or virtual) and Teleworker licenses (1 per 68xxi device + a few floater licenses).

Installing Release 11.0 on a Standalone Physical Server

For installation of MBG on a standalone physical server, refer to the *MBG Installation and Maintenance Guide 11.0*.

Installing Release 11.0 in a VMware Environment

For installation of MBG on a standalone physical server, refer to the *MBG Installation and Maintenance Guide 11.0*.

Firewall Configuration

If MBG is deployed in a demilitarized zone, the following ports need to be opened (above ports needed for communication with the AMC).

- TCP port 5061 between the Internet and MBG for SIP TLS
 - TCP port 5060 between MBG and MX-ONE
 - TCP port 22223 for classic XML logon between the Internet and MBG for SIP XML
 - TCP port 22222 for classic XML logon between MBG and MX-ONE for SIP XML
 - TCP port 22226 for native VDP logon between the Internet and MBG for Configuration Server Access
 - TCP port 22225 for native VDP logon between MBG and the Configuration Server (MX-ONE)
 - UDP port 20000-31000 between the Internet and MBG and between MBG and the LAN for voice
 - TCP port 22 between LAN and MBG for secure shell access
 - UDP port 53 between MBG and the LAN for DNS resolution to a Corporate DNS server
- NOTE:** Do not enable TCP port 5060 or UDP port 5060 between the Internet and MBG.

MSL Configuration

1. Configure your MSL server to use a Corporate DNS server that can resolve any FQDN associated with MX-ONE.
2. Configure your MSL server to allow Remote Access for secure shell from a local network. This access will be needed to run a special setup script.
3. Navigate to Remote Access under MSL Server Manager.
4. Select “Allow access only from trusted and remote management networks” to setup secure shell access.
5. Select “Yes” for administrative command line access over secure shell.
6. Select “Yes” to allow secure shell access using standard passwords.

MBG Configuration

From a new installation of Release 11.0, access the MiVoice Border Gateway User Interface from MSL server-manager and perform the following steps:

1. Go to System Configuration > Network Profile.
 - a. Select Profile and Apply.
2. Go to System Configuration > Settings.
 - a. Enable SIP support for TCP/TLS and TCP.
 - b. Change Codec support to Unrestricted.
 - c. Change Set-side RTP security to Require (to enforce SRTP between the phone and MBG).
NOTE: Optionally, you can disable support for all protocols under Minet Support.
3. Service Configuration > ICPs
 - a. Add your MX-ONE system as type MiVoice MX-ONE with SIP capabilities as UDP, TCP.
 - b. Configure MX-ONE support.
 - c. Check Link to the ICP and Enable.
 - d. Classic XML login:
 - i. Configure the XML listen port as 22223 and check TLS.
 - ii. Configure the XML destination port as 22222 and uncheck TLS.
 - e. Native VDP login:
 - i. Configure the configuration server listen port as 22226 and check TLS.
 - ii. Configure the configuration server port as 22225 and uncheck TLS.
 - f. Configure the configuration server address (the address to MX-ONE).
 - g. Click Save.
4. Do not start MBG yet.
5. Setup MBG with mutual TLS for SIP using configuration script.
6. Connect to the system via ssh (ex: using putty) and login as root.

7. Run the configuration script specifying the MBG Public IP address (i.e the address the Teleworker 68xx phones will connect to) and the MBG local or LAN IP address.

Optionally, you can use the script to modify an existing mitel.cfg or use MBG as a TFTP server for the phones.

To view all options available, run the configuration script without arguments.

```
[root@mssystem ~]# /usr/sbin/configure_68xx_mbg_support.sh
```

Example #1: MBG Public IP is 1.1.1.1 and MBG local IP is 192.168.100.10

```
[root@mssystem ~]# /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip ip_ad-dress --mbg_lan_ip ip_address --generate_certificate
```

```
[root@mssystem ~]# /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip 1.1.1.1 --mbg_lan_ip 192.168.100.10 --generate_certificate
```

```
mbg_wan_ip=1.1.1.1
```

```
mbg_lan_ip=192.168.100.10
```

```
configure_tftp=false
```

```
generate_certificate=true
```

```
force=false
```

creating /root/aastra_tftp, output files will be placed there.

configuring mbg certificate with ip address: 1.1.1.1

Generating a 2048 bit RSA private key

```
.....+++
.....+++
```

writing new private key to '/root/aastra_tftp/mbg_mxone_key.pem'

```
-----
```

writing RSA key

details:

InsertCertificateIntoChain

Subject: /CN=1.1.1.1

Issuer: /CN=1.1.1.1

ReorderCertificateChain:: client certificate found:

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

ReorderCertificateChain:: root CA certificate found:

Subject: /CN=1.1.1.1

Issuer : /CN=1.1.1.1

VerifyCertificateChain:: m_vrCerts.size()==1 rc=1

certificate and key files for set are /root/aastra_tftp/mbg_mxone_cert.pem and /root/aastra_tftp/mbg_mxone_key.pem
done.

Example #2: MBG Public IP is 1.1.1.1, MBG local IP is 192.168.100.10, modify an existing mitel.cfg (transferred to /root

```
[root@mssystem ~]# /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip 1.1.1.1 --mbg_lan_ip 192.168.100.10 --generate_certificate --modify_cfg_template mitel.cfg --ntp_server pool.ntp.org --time_zone_name SE-Stockholm
```



```
mbg_wan_ip=1.1.1.1
mbg_lan_ip=192.168.100.10
configure_tftp=true
generate_certificate=true
force=false
```

will configure tftp directory /root/aastra_tftp to serve up config files
creating /root/aastra_tftp, output files will be placed there.
configuring mbg certificate with ip address: 1.1.1.1
Generating a 2048 bit RSA private key

```
.....+++
.....+++
writing new private key to '/root/aastra_tftp/mbg_mxone_key.pem'
-----
writing RSA key
details:
InsertCertificateIntoChain
Subject: /CN=1.1.1.1
Issuer : /CN=1.1.1.1
```

```
ReorderCertificateChain:: client certificate found:
Subject: /CN=1.1.1.1
Issuer : /CN=1.1.1.1
```

```
ReorderCertificateChain:: root CA certificate found:
Subject: /CN=1.1.1.1
Issuer : /CN=1.1.1.1
VerifyCertificateChain:: m_vrCerts.size()==1 rc=1
```

certificate and key files for set are /root/aastra_tftp/mbg_mxone_cert.pem and /root/mitel_tftp/mbg_mxone_key.pem
creating mitel.cfg from template, configured with MBG's CN ip
sip proxy ip
sip proxy port
sip registrar ip
sip registrar port
sip outbound proxy
sip outbound proxy port
tftp server
sips trusted certificates
sips root and intermediate certificates
sips local certificate
sips private key
https validate certificates
https user certificates
time server disabled
time server
time zone name
sip transport protocol
found URL's pointing to 22222, switching to https and port 22223

appending fixed URLs to config file done.

8. Return to the MiVoice Border Gateway User Interface and click on Dashboard to Start MBG
9. Confirm that Teleworker 68xx phones have access to the public IP of MBG using the Teleworker Network Analyzer tool.
10. Download the tool from Administration – File Transfer and install it on a Windows machine that has network connectivity to the public IP of your system.
11. Launch the application and run a connect test against the public IP.
SIP TLS, Aastra MXL MX-ONE, Voice Traffic (begin) and (end) should return OK.
If any of the above return CLOSED or TIMED OUT, contact your firewall administrator.

Phone Configuration

1. Phone must be staged in the office.
2. Using WinSCP, copy the /root/aastra_tftp/mbg_mxone_cert.pem and /root/aastra_tftp/mbg_mxone_key.pem to a special folder (ex: athome) on your configuration server.
3. Append the settings listed in “Appendix – mitel.cfg Settings” to your mitel.cfg file or used the modified mitel.cfg also available under /root/aastra_tftp.

If needed, update all other files (ex: <model.cfg>) to use https/22222 for classic XML logon or https/22226 instead of http/22225 for native VDP logon.

Limitations

A list of known limitations shared with the InGate solution.

1. Phones must be staged in the office.
2. Phone firmware must be done in the office as a phone firmware upgrade will remove the certificate loaded.
3. Access to internal configuration server cannot be limited/controlled/blocked from the outside.
4. 68xxi must have access to a NTP server for certificate validation.
5. Corporate directory access must be setup with port forwarding on MSL (server-gateway configuration) or the DMZ firewall.
6. If MX-ONE is setup to like lim1.mysystem.com, the MSL server must point to a Corporate DNS to allow proper DNS resolution.

Here is a list of known limitations with MBG

- a. Single dedicated MBG.
 - b. MBG clustering and backup SIP registrar/proxy in the 68xxi configuration files.
 - c. Using FQDN instead of IP address in the 68xxi configuration files.
7. Music On Idle is not supported.

8. MiCollab Meetings Center application which is accessed through the meetings softkey is not supported.

Known Issues

None.

Upgrade Notes

Trials sites that have deployed based on earlier versions of this document, need to run the following command on their system to ensure that all required files are part of a backup.

```
[root@mysystem ~]# db tug setprop config backuplist
/etc/tug/tug.ini.certifi-cates.ini,/etc/tug/tugcerts.ini,/etc/tug/ca-bundle.crt,/etc/tug/mbg_mxone.ini
```

Appendix - Config Script

```
[root@ ~]# /usr/sbin/configure_68xx_mbg_support.sh
```

```
mbg_wan_ip=
```

```
mbg_lan_ip=
```

```
configure_tftp=false
```

```
generate_certificate=false
```

```
force=false
```

```
-----
```

```
--mbg_lan_ip parameter must be specified
```

```
-----
```

```
Usage: /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip ip_address --mbg_lan_ip ip_address
[--tftp] [--generate_certificate] [--force] [--modify_cfg_tem-plate aastra_cfg_file_template] [--ntp_server
fqdn/ip] [--time_zone_name aastra_name_string]
```

```
--mbg_wan_ip - MBG public address
```

```
sets connect to this address and MBG certificate will contain this
```

```
--mbg_lan_ip - MBG private address
```

```
used for SIP udp and tcp communications with ICP
```

```
(udp and tcp are disabled on MBG's public address)
```

```
--tftp - configure this MBG to supply configuration files via tftp
```

```
--generate_certificate - create a certificate using the value supplied for 'mbg_wan_ip'
```

```
--force - override 'certificate already exists' check
```

```
--modify_cfg_template - If set, specified file will be modified.
```

Cfg settings dealing with certs/sip will be adjusted

--ntp_server - If set, specified fqdn will be used for ntp settings.

otherwise 'pool.ntp.org' will be used.

--time_zone_name - If set, specified time zone string will be used for ntp settings.

otherwise 'SE-Stockholm' will be used.

Appendix - mitel.cfg Settings

#-----

MiVoice Border Gateway (MBG) Teleworker features

SIP TLS and SRTP between the phone and MBG

HTTPS used for XML

#-----

MBG is the SIP proxy and registrar

sip proxy ip:MBGIP

sip proxy port:5061

sip registrar ip:MBGIP

sip registrar port:5061

sip outbound proxy:MBGIP

sip outbound proxy port:5061 #5061 or 0(which will attempt SRV and as fall back send to 5061 due to TLS)

Persistent SIP TLS (requires 'sip outbound proxy')

sips persistent tls:1

sip outbound support:1

sip transport protocol:4 #4-TLS

Certificates/keys for sip-tls

sips trusted certificates: mbg_mxone_cert.pem

sips root and intermediate certificates: mbg_mxone_cert.pem

sips local certificate: mbg_mxone_cert.pem

sips private key: mbg_mxone_key.pem

https validate certificates: 1

https user certificates: mbg_mxone_cert.pem

Voice Encryption (SRTP)

sip srtp mode:2

OPTIONAL – Use MBG's TFTP server

#tftp server:MBGIP

#NTP server must be accessible from the home network

time server disabled: 0

Time server1:<NTP server>

Action URI must use HTTPS to port 22223

action uri startup:https://\$\$PROXYURL\$\$:22223/Startup?user=\$\$SIPUSERNAME\$\$

services script: https://\$\$PROXYURL\$\$:22223/Services?user=\$\$SIPUSER-NAME\$\$&voicemailnr=

#-----

NOTE: Similar changes may be required to <model>.cfg or <mac>.cfg files.

