MiVoice Border Gateway
Installation and Maintenance Guide

JANUARY, 2017

RELEASE 9.4

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.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

To obtain the source code of third-party components licensed under the GNU General Public License or Lesser General Public License, please e-mail *gplrequest@mitel.com*.

For a detailed list of third-party license content, see the *Mitel Standard Linux Installation and Maintenance Guide* available at Mitel OnLine.

MiVoice Border Gateway Installation and Maintenance Guide
January 2017

®,™ Trademark of Mitel Networks Corporation
© Copyright 2017, Mitel Networks Corporation
All rights reserved

OVERVIEW 1
Feature Support 2
MBG Standalone Feature Support 2
MBG-MiCollab Feature Support 2
What's New in this Release 3
Release 9.4 3
NETWORK PROFILES 4
Server-Gateway Configuration on Network Edge 4
Server-only Configuration on Network DMZ 5
Server-only Configuration on Network LAN 6
Server-Gateway Configuration with Bridged Interface 7
INSTALLING MIVOICE BORDER GATEWAY SOFTWARE 9
Before You Begin 9
Collect Site Information 9
Installing on a Physical Server 11
Download Software from Mitel Online 11
Build CD/DVDs from the Software 11
Install and Configure MSL Software 12
Install MBG Software on an Online system 12
Install MBG Software on an Offline System 13
Installing in a VMware Virtual Environment 13
VMware Resources 14
Requirements 15
Collect Properties 15
Deploy Virtual MBG Appliance 17
Configuration 20
Installing in a Microsoft Hyper-V Virtual Environment 21
Limitations 21
Disabling the MBG Service 21
Enabling the MBG Service 22
TELEWORKER SERVICE 22
Corporate Location Requirements 22
Hardware 22
Software 23
Communication Platforms 23
Phones/Devices 23
License Requirements 23

Software Assurance 24
Firewall Requirements 24
Support for HTML Applications 24
Remote Location Requirements 25
Phones/Devices 25
Network Parameters 25
Router/Internet Gateway 26
Configure Teleworker Service 26
Configuring the Teleworker Service on MBG 26
Provisioning MiNet Devices 27
Provisioning SIP Devices 29
Bulk Provisioning of MiNet and SIP Devices 30
SIP TRUNKING 32
Other Features 32
Before You Begin 33
Configuration Overview 33
Network Requirements 33
Configuration Example 33
Configure SIP Trunking 34
Configuring the MiVoice Business (3300 Controller) to Support SIP Trunks 34
Configuring the MiVoice Office 250 to Support SIP Trunks 36
Configuring the MX-ONE to Support SIP Trunks 37
Adding a SIP Trunk to MBG 38
Editing a SIP Trunk on MBG 40
Configure DID Routing Rules for SIP Trunking 40
Configuration Example 40
Adding a DID Routing Rule 41
Editing a DID Routing Rule 42
DID Routing Rule Format 43
Valid Characters for DID Routing Rules 43
Sample DID Routing Rules 43
REMOTE PROXY SERVICES 44
Overview 44
Web Proxy 44
Remote Management Service 44
When to Use the Web Proxy 44
Configurations 45
Basic Operation 45
Basic Configuration Overview 47

Split DNS Setup 47
Multiple Account Setup 47
Firewall 48
Requirements for Audio, Web and Video Conferencing 49
DNS 49
Message Flow for Web Traffic 49
Message Flow for Web Conferencing (Collaboration) Requests 51
Firewall 52
Configure LAN Servers on the Web Proxy 53
Configure Users for Remote Management 55
Web Proxy with Multiple LAN Servers 56
Security Certificate Not Trusted 58
SECURE RECORDING CONNECTOR SERVICE 59
Direct Call Recording 59
Indirect Call Recording 59
Requirements 60
Phones/Devices 60
Firewall 60
DHCP for Direct Call Recording 60
Configuration 61
Enrolling the Call Recording Equipment 61
Handling Certificate Requests 61
WEB REAL-TIME COMMUNICATION (WEBRTC) 62
SECURITY 62
Firewall 62
WebRTC Usage Scenarios 62
Anonymous Calls 62
Subscriber Calls 63
ICP Support 63
WebRTC Configuration 63
ICP Configuration 64
Configuring the MiVoice Business to Support SIP Trunks 64
Configuring the MiVoice Business (3300 Controller) to Support SIP Trunks 64
Configuring the MiVoice 5000 to Support SIP Trunks 65
MBG Configuration 66
Configure WebRTC Settings 66
Configure WebRTC Port Ranges (Optional) 69
WEB SERVER CONFIGURATION 69
Downloading the SDK and Opening the Files 69

Adding the Files to the Web Server 70
Implement the Complete SDK 70
Implement Only the JS Files 70

CLUSTERING 71

Cluster Licensing 72

Cluster Hardware 72

DAISY CHAINING MBG SERVERS (TELEWORKING) 73

Setting up Daisy Chained Servers 73

Daisy Chaining to Enforce Strict Firewall Rules 75

UPGRADING SOFTWARE AND LICENSES 76

Upgrading MiVoice Border Gateway Software 76
Upgrading a Physical MBG with CD/DVD or USB 76
Upgrading a Physical MBG with Remote Fresh Installation (RFI) Blade 77
Upgrading a Virtual MBG on VMware 78
Upgrading a Virtual MBG on Hyper-V 79
Upgrading a Cluster Setup 79

Upgrading MiVoice Border Gateway Licenses 81

Supporting Documentation 83

MBG AND EMERGENCY SERVICES 84

APPENDIX A: THIRD PARTY LICENSES 85

ARES DNS library 85

Picojson 85

reSIProcate SIP stack 85

Rtpproxy 86

XMLRPC-C (used by rtpengine): 87

PCRE (used by rtpengine) 87

libvpx 88

Securimage 89

OVERVIEW

The MiVoice® Border Gateway (MBG) is the evolution of the Mitel Teleworker Solution to a platform for the secure deployment of multiple services in a variety of network configurations. MBG provides the following services:

- **Teleworking**: Secure remote MiNET and SIP access for IP phones on the MiVoice Business platform. Also NAT traversal for tenant offices for the Multi-instance MiVoice Business application.
- **Secure Call Recording**: Call recording solution that allows third-party recording equipment to record Mitel encrypted voice streams.
- **SIP Trunking**: An outbound proxy for SIP trunking from internal MiVoice Business platforms to external third-party SIP providers.
- Remote Proxy Services:
  - **Web Proxy Domain**: A reverse proxy that provides access to hosts on a corporate LAN for clients on the Internet.
  - **Remote Management Service**: Provides administrative-level access control to the MiVoice Business and MiCollab management web interfaces using password authentication while restricting access to all other parts of the enterprise network.
- **WebRTC**: A gateway to support browser-based voice and video calling.

This guide provides information about the requirements and installation procedures of the MiVoice Border Gateway.

Note that the MBG interface supports ASCII and UTF-8 encoding, enabling the entry of a wide range of unaccented, accented and special characters.

FEATURE SUPPORT

MBG Standalone Feature Support

FEATURE	MIVOICE BUSINESS	MIVOICE OFFICE 250	MIVOICE MX-ONE	MIVOICE 5000	MIVOICE OFFICE 400
MiNet Teleworker	Yes	Yes	No[1]	No[1]	No[1]
SIP Teleworker	Yes	Yes	Yes[2]	Yes[2]	Yes[3]
SIP Trunking	Yes	Yes	Yes	No	No
Secure Call Recording	Yes[4]	No	Yes[4]	No	No
Remote Proxy Services (administrative interfaces)	Yes	No	No	No	No
WebRTC	Yes[5]	No	Yes[5]	Yes	Yes[5]

1. These platforms only support the SIP protocol, not MiNet.
2. This platform supports MiCollab Client softphones and 68xxi devices as SIP teleworkers.
3. This platform supports MiCollab Client softphones as SIP teleworkers.
4. Contact your CRE vendor to determine which Mitel platforms it supports.
5. These platforms support subscriber WebRTC calls using the Mitel MiCollab Web Client only. MiVoice Business also supports anonymous WebRTC calls.

MBG-MiCollab Feature Support

FEATURE	MIVOICE BUSINESS	MIVOICE OFFICE 250	MIVOICE MX-ONE	MIVOICE 5000	MIVOICE OFFICE 400
MiNet Teleworker	Yes	Yes	No[1]	No[1]	No[1]
SIP Teleworker	Yes	Yes	Yes[2]	Yes[2]	Yes[2]
SIP Trunking	Yes	Yes	Yes	No	No
Secure Call Recording	Yes[3]	No	Yes[3]	No	No
WebRTC	Yes[4]	No	Yes[4]	Yes	Yes[4]

1. These platforms only support the SIP protocol, not MiNet.
2. These platforms support MiCollab Client SIP softphones as SIP teleworkers. They do not support 68xx SIP devices.
3. Contact your CRE vendor to determine which Mitel platforms it supports.
4. These platforms support subscriber WebRTC calls using the Mitel MiCollab Web Client only. MiVoice Business also supports anonymous WebRTC calls.

WHAT'S NEW IN THIS RELEASE

Release 9.4

- **IP Phone Support:** MiVoice Border Gateway now supports the following new IP phones:
  - Mitel MiVoice 6920 IP Phone
  - Mitel MiVoice 6930 IP Phone
  - Mitel MiVoice 6940 IP Phone
  - WebRTC now supports tenanted cloud deployments.
  - Capacity and performance improvements for cloud and large enterprise environments.
- **Improved Logging Capabilities:** The new Logging panel under the Administration menu controls the information that MiVoice Border Gateway logs that is used to troubleshoot issues.

NETWORK PROFILES

MBG provides three preset Network Profiles for streaming addresses. You can choose the profile that applies your particular configuration or you can create a custom profile by manually entering the set-side and ICP-side IP addresses.

The default Network Profiles provide the following preset values:

NETWORK PROFILE	DEFAULT SET SIDE IP ADDRESS FOR RTP STREAMING	DEFAULT ICP SIDE IP ADDRESS FOR RTP STREAMING
Server-gateway on network edge	WAN IP address	LAN IP address
Server-only on network DMZ	Public IP address as seen by the AMC	Public IP address as seen by the AMC
Server-only on network LAN	LAN IP address	LAN IP address

Note: Improper selection of network profile can result in one-way audio or no audio at all.

SERVER-GATEWAY CONFIGURATION ON NETWORK EDGE

In this configuration, the server functions a firewall/Internet gateway with two Ethernet interfaces. One interface is connected to the external network (Internet) while the other is connected to the internal network. The firewall provided by the MBG server is not configurable. All default data traffic initiated inside the network is allowed while data traffic initiated outside the network is denied.

When you select this network profile, the system will program the RTP streaming addresses of the MBG as follows:

- ICP-side streaming address = LAN interface address
- set-side streaming address = WAN interface address

This setup enables you to provide prioritization for voice traffic by programming the maximum capacity of the MBG's WAN links using the "Bandwidth Management" feature.

Although it is technically feasible to install services such as MICOLLAB on the gateway, it is not recommended. For optimum security, services should be located in the DMZ or LAN.

The external (WAN) address of the server MUST be:

- dedicated to the MBG Solution
- publicly routable
- reachable from the Internet and the internal network (that is, the server should **not** reside behind a NAT device)

Note: In the server-gateway configuration, the MBG server is the gateway for MBG traffic.

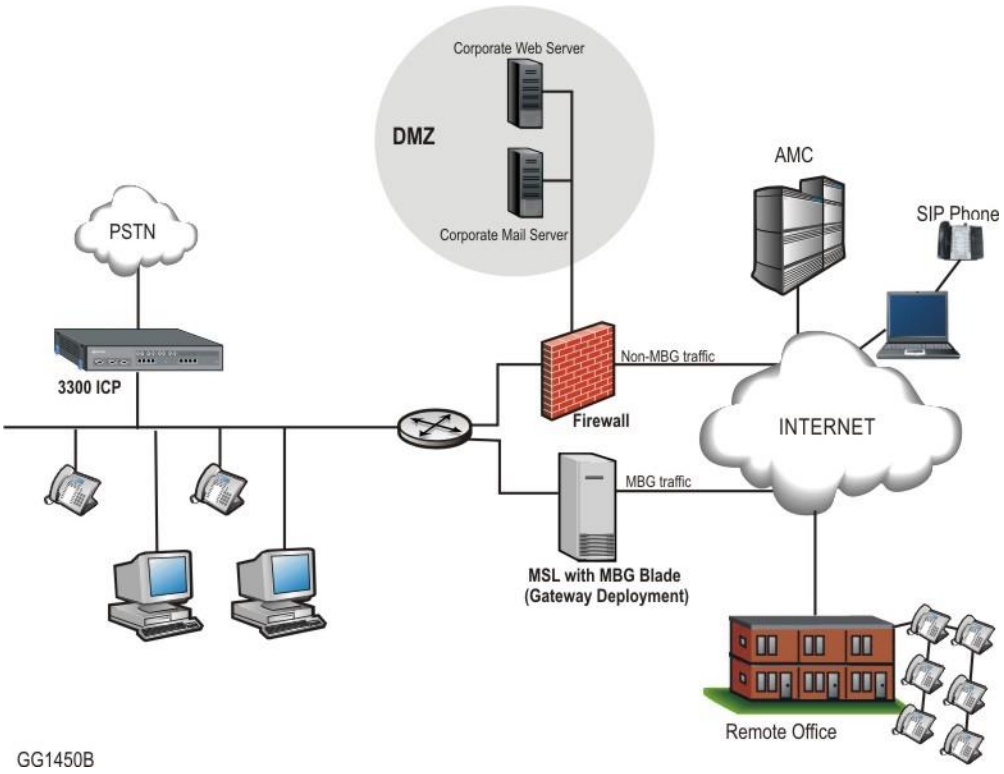


Figure 1. Server-Gateway Configuration

MBG can also be implemented with an existing firewall on the network edge, as illustrated above. In this example, MBG serves as a gateway for MBG traffic while the second firewall handles non-MBG traffic.

SERVER-ONLY CONFIGURATION ON NETWORK DMZ

In this configuration, the server is installed in the Demilitarized Zone (DMZ) of a customer's existing firewall. It acts only as a server and is protected from Internet exposure by the existing firewall.

On the MBG, configure the LAN interface with an IP address that is:

- dedicated to the MBG solution
- private (allocated from the firewall's DMZ network range)
- reachable from the internal network.

On the enterprise firewall, configure the WAN interface with an IP address that is:

- dedicated to the MBG Solution
- publicly routable via the firewall
- reachable from the Internet and the internal network.

When configuration is complete, the system will use the public, post-NAT address of the server for both the set-side and ICP-side streaming addresses of the MBG. To determine this address, access the MSL Server Manager, select Review Configuration and examine the **Internet Visible IP Address** field.

Note: In a DMZ configuration, the firewall is the gateway for all traffic and has three interfaces (WAN, LAN, and DMZ), as shown in Figure 2. (See Firewall Requirements.)

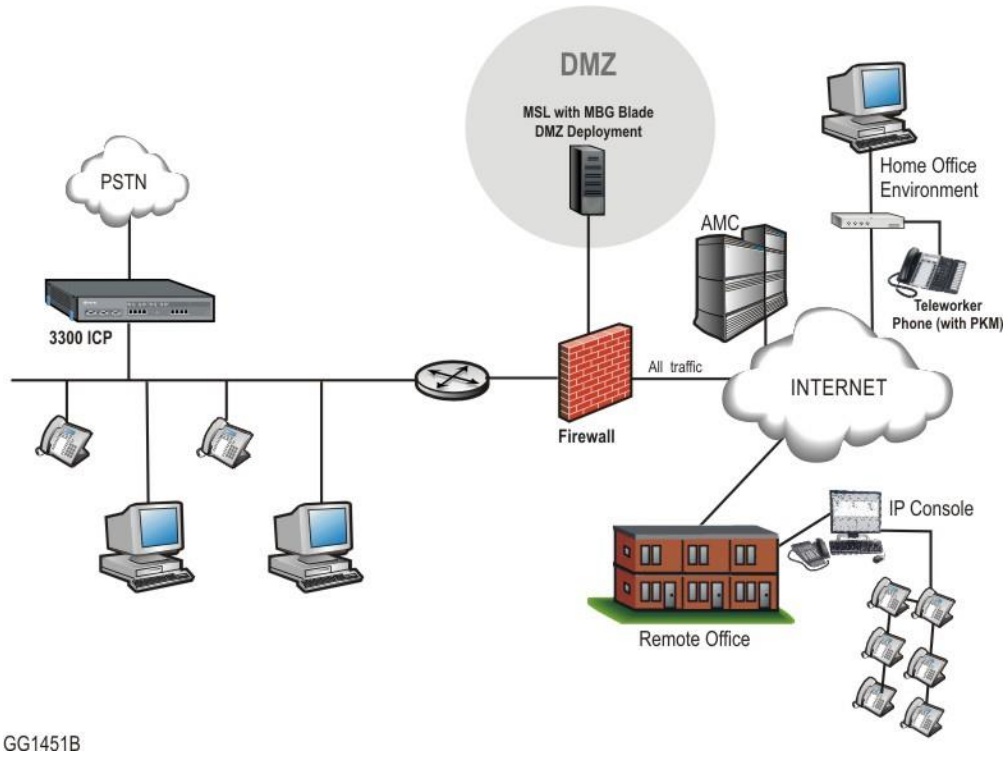


Figure 2. DMZ Configuration

- For Web Proxy configurations see page 43.
- For SRC configurations see page 59.

SERVER-ONLY CONFIGURATION ON NETWORK LAN

In this configuration, the server is installed in the customer's existing network LAN with no exposure to the Internet.

When you select this network profile, the system will use the LAN address of the server for both the set-side and ICP-side streaming addresses of the MBG. This address SHOULD be:

- dedicated to the MBG Solution
- private
- reachable only from the internal network

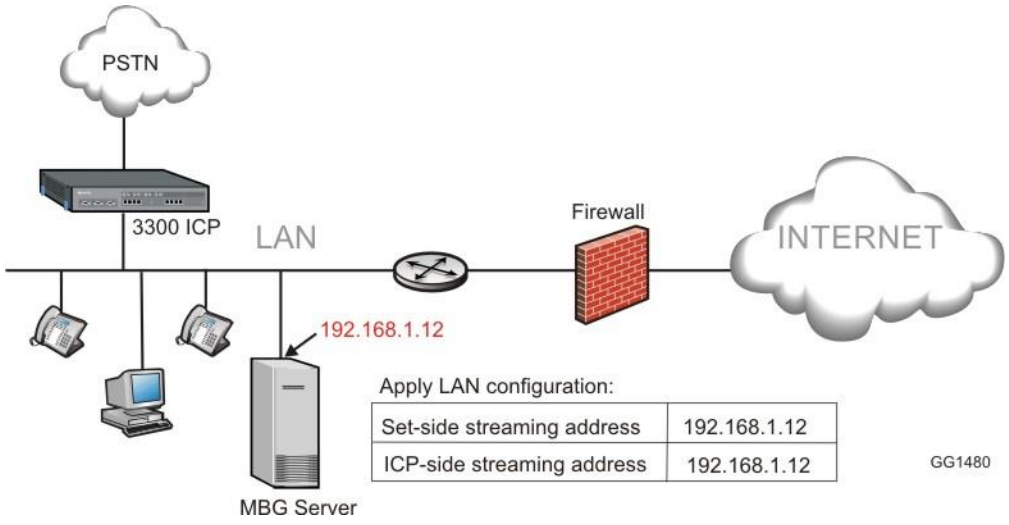


Figure 3. Server-only Configuration

Some examples of deployments that use this configuration are:

- Secure Call Recording (see page 59)
- Daisy Chaining (see page 73)

SERVER-GATEWAY CONFIGURATION WITH BRIDGED INTERFACE

The server functions as a firewall/Internet gateway for VoIP traffic, and as a bridge to the WAN interface of the customer's existing firewall for all other traffic.

When incoming traffic arrives on the server's WAN interface, it is routed to the appropriate network segment. Voice packets are sent directly to the Voice VLAN and data packets are bridged to the firewall's WAN interface. By separating the traffic between the voice and data network segments, QoS for voice calls is improved. This setup also enables a Voice VLAN to be installed into an existing Data VLAN without having to update the firewall rules.

With this network profile, the system programs the RTP and data streaming addresses as follows:

STREAM	INTERNAL OR ICP-SIDE ADDRESS	EXTERNAL OR SET-SIDE ADDRESS
RTP	LAN interface of server	WAN interface of server
Data	Bridged interface of server	WAN interface of server

As part of this configuration, you can prioritize voice over data traffic using the MBG's "Bandwidth Management" feature. Simply program the maximum amount of bandwidth available on the WAN communication links (inbound and outbound). The system employs these settings to establish traffic shaping queues which give priority to voice calls ahead of data traffic.

The external address of the server MUST be

- dedicated to the MBG Solution
- publicly routable
- reachable from the Internet and the internal network (that is, the server should **not** reside behind a NAT device)

To enable this network profile, the server requires at least three network interface cards: one for the LAN connection, another for the WAN connection, and the third for the bridged connection to the

WAN interface of the firewall. As part the Mitel Standard Linux (MSL) installation, you will be prompted to configure the third interface after you have selected the WAN adapter.

The following diagram shows the settings that are applied when the server has a third network adapter that has been configured as a bridged interface and you select **Server-gateway configuration on the network edge**:

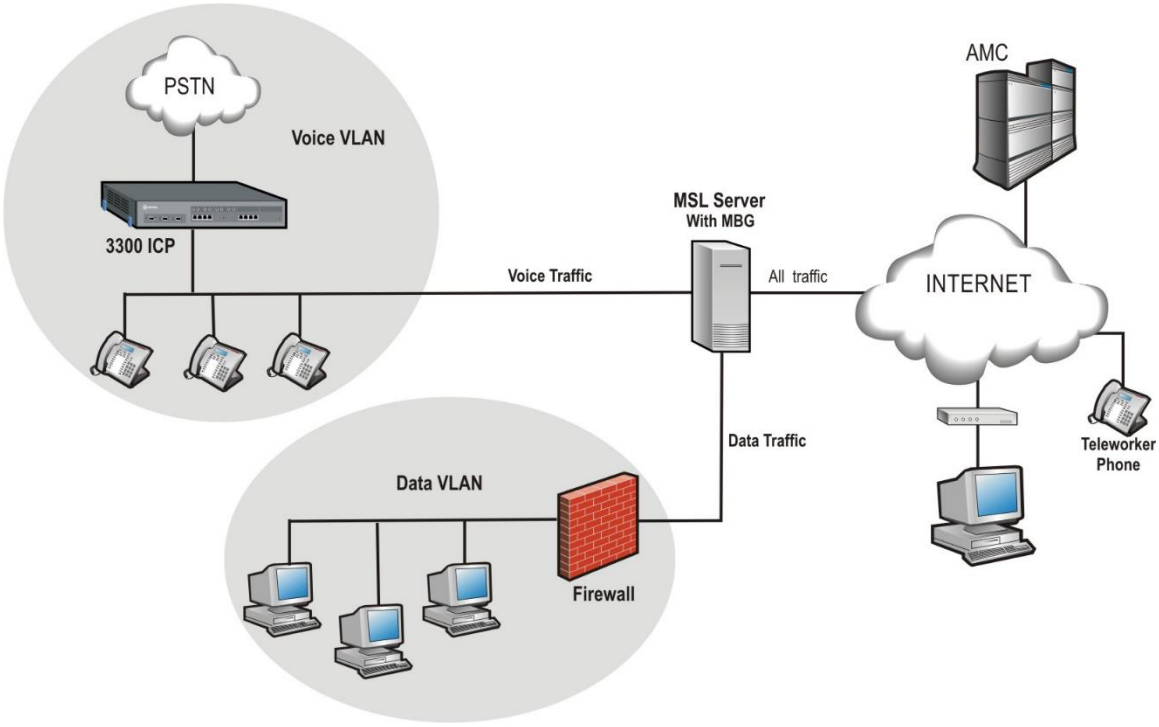


Figure 4. Server-gateway with Bridged Interface Configuration

Note: MSL 9.2 or greater is required to implement “Server-gateway with Bridged Interface” mode.

INSTALLING MIVOICE BORDER GATEWAY SOFTWARE

This section describes the new installation of MBG on the following platforms:

- Physical deployment on a hardware server — page 9
- Virtual deployment in a VMware environment — page 13
- Virtual deployment in a Hyper-V environment — page 21

If you are upgrading from a previous release, see *Upgrading MBG Software* on page 76.

BEFORE YOU BEGIN

1. Review the **MBG Release Notes** available in the Mitel Knowledge Base.
2. Review the **MBG Engineering Guidelines** available at Mitel OnLine.
3. Ensure that corporate and remote sites meet **MBG requirements** (see below).
4. Create an Application Record ID and assign MBG licenses to it.

COLLECT SITE INFORMATION

The following table itemizes the information you will need to enter during software installation and configuration. For efficient installation, gather this information before you start the installation:

ITEM	NOTES	YOUR INFORMATION
Localization		
Time zone setting	Identify the MSL operating system time zone setting. The default is America/New York. The Time zone setting also determines your system telecommunications regional settings.	
Keyboard Type	Identify the preferred keyboard type (default is **us**).	
Application		
Administrator Password	Record the initial administrator password for the MSL server manager interface. This password must be at least six characters long. When you access the server manager, you will be prompted to change this initial password. **Note**: You must enter a password before you deploy the system; otherwise, the system will not boot up.	Initial server manager Administrator Password: _____ Final server manager Administrator Password: _____ It is recommended that you use a strong password that contains all of the following: upper case letter, lower case letter, number, non-alphanumeric character, and be at least seven characters long. Do not use a commonly used word (for example: 'password').
System name	Set the system name (hostname) of	

ITEM	NOTES	YOUR INFORMATION
	the system.	
Domain Name (Optional)	Specify the domain name for the hostname above. The default domain name is "mycompany.local".	
License Key (Optional)	Identify the License Key (ARID) for this system. The ARID is used by the AMC to distribute the system licenses.	
DNS Server (Optional)	Record the IP address of your corporate DNS server. **Note**: If your DNS is supplied by your ISP, leave this setting blank.	
Remote Network Address for server administration (Optional)		
Remote Network Netmask (Optional)		
Network Settings		
LAN IP Address	Record the IP address of the local (LAN) interface. This must be a valid IP address on the local LAN.	
LAN Netmask	Record the Netmask of the LAN.	
WAN IP Address (Optional)	For Network Edge (Server-gateway) deployments, record the IP address of the external (WAN) interface. This must be a valid IP address on external WAN. For LAN only (Server-only) deployments, use an IP address of 0.0.0.0.	
WAN Netmask (Optional)	Record the Netmask of the WAN.	
Alias WAN IP Address (Optional)	Optional second, alias IP address used for applications that require a server with two IPs (like Audio, Web and Video Conferencing).	
LAN (Optional)	Optional network interface that can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.	
Default Gateway IP Address	Record the Gateway IP address. For Server-gateway deployments this gateway typically points to the internet. For Server-only deployments, this gateway typically points to a LAN router.	

ITEM	NOTES	YOUR INFORMATION
Trusted Network Access If the ICP or some of your users are not on the same subnet as the MSL server, you need to classify them as "Trusted Networks" and then allow them access. Both IPv4 and IPv6 networks are supported.		
IP Address	The IP address of the network for which you want to allow access	
Subnet	The subnet mask for the range of IPv4 addresses you wish to allow.	
Router Access	The address of the router/ gateway you will use to access the network (or subnet) to which you are granting access	

INSTALLING ON A PHYSICAL SERVER

This section describes the fresh installation of MBG software on a **physical server** from the MSL Qualified Hardware List.

Download Software from Mitel Online

You can download the MSL and MBG software ISO images from Mitel OnLine and burn CDs or DVDs to take onsite. If the site has limited Internet connectivity, you may also need to perform an offline synchronization with the AMC to retrieve licensing information. (Instructions for offline installation are included in the Installation section.)

To download **MSL** software from Mitel OnLine:

Note: Use HTTP or the Software Download Manager to download software.

1. Log on to Mitel OnLine.
2. Move your cursor over **Technical** and then click **Software Downloads**.
3. Click **MiVoice Border Gateway**. The correct MSL load for your software is included on this page.
4. Click the **MSLx.x.x.iso** link (where x.x.x represents the MSL release number).
5. Select a download method: **HTTP** or the **Software Download Manager**.
6. Select a location on your PC to store the downloaded software ISO images.

To download **MBG** software from Mitel OnLine:

1. Follow steps 1 to 3 in the "To Download MSL software from Mitel OnLine" procedure above.
2. Click the appropriate **MBG** software version.
3. Select a download method: **HTTP** or the **Software Download Manager**.
4. Select a location on your PC to store the downloaded ISO image.

Build CD/DVDs from the Software

For 32-bit installations of MSL, use a CD. For 64-bit installations of MSL, use a DVD.

1. Insert a CD or DVD into the CD/DVD-ROM drive of the maintenance PC.
2. Navigate to the stored .iso image and double-click the file. Your CD/DVD burner builds the software CD or DVD.
3. Label the discs and take them with you to the installation site.

Install and Configure MSL Software

1. Configure the MBG server to boot from either the CD/DVD-ROM drive.
2. Insert the MSL software CD or DVD into the CD/DVD-ROM drive of the MBG server.
3. Refer to the Mitel Standard Linux Installation and Administration Guide to complete the following procedures:
   - Install MSL Software
   - Configure the Server

Install MBG Software on an Online system

These instructions apply when installing MBG on a server that is connected to the Internet. If you have no Internet connectivity, see Install MBG on an Offline System.

1. Upon reboot of MSL, you are prompted to enter your **Application Record ID**. You must enter this number to activate the licensing for the site.
2. If you are using a remote management PC on a different subnet than the MBG server, you may need to add the IP address of the PC to the Trusted Networks listing on the MBG server. See the “Networks” topic in the *Mitel Standard Linux Installation and Administration Guide*. When the required trusted local networks have been configured, proceed to the next step.
3. Open a browser and enter the following URL to access the MSL server manager: **https:**//*<IP address or FQDN of MBG server>***/server-manager**
4. Under ServiceLink, click **Blades**.
5. Click the Install link associated with the MBG blade. The MBG license agreement appears. (To download the blade for installation at a later time, click the Cache link.)
6. Click **Read text** to read the license terms for all software applications. If you agree with the license terms, click **Accept all licenses**, or click **Cancel** to exit the blade installation. After you accept all licenses, a progress indicator appears. **Note**: If you see a “proxy error” message, click **Blades** (in the server manager menu under ServiceLink) to return to the MSL browser screen.
7. To refresh the page for Internet Explorer browsers, use **Click here for automatic update**.
8. When installation is complete, an overview of installed components appears. Click **Clear this report** to return to the Blades panel.

   Navigation links for MiVoice Border Gateway and Remote Proxy Services (Web Proxy and Remote Management) appear in the **Applications** section.
9. In the left-hand menu, under Applications, click **MiVoice Border Gateway**. For MBG configuration instructions, click the Help icon in the upper right corner of the MBG interface. To configure remote phones to operate as teleworker devices, refer to the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.

Install MBG Software on an Offline System

This section describes the fresh installation of MBG 8.x software on a **server** from the MSL Qualified Hardware List that does not have access to the Internet. Ensure that you have downloaded MBG software and burned a CD or DVD as instructed on page 11.

To Offline Sync with the AMC:

1. Upon reboot of MSL, you are prompted to enter your **Application Record ID**. Select **Next**. You are returned to the Linux login prompt.
2. Log in as “admin”. The MSL server console menu is displayed.
3. Select the option to perform **Offline Sync with the AMC**.
4. In the Offline sync screen, select **create**.
5. When prompted, insert a portable storage device and then select **Next**.
6. When prompted, enter your **Application Record ID** and then select **Next**.
7. When prompted, remove the storage device and take it to a PC with Internet connectivity.
8. Insert the storage device in the remote PC and navigate to the storage drive location.
9. Search the main directory for a file called **sync.bat** and double-click it. A script runs that sends your sync information to the AMC and receives license key information in return.
10. To verify the sync, navigate to the **sync.log** file in the **sdata** directory of the storage drive location. Double-click **sync.log** to open and check for “completed successfully” message.
11. Remove the storage device from the remote PC and go back to the MBG server.
12. Select the option to perform **Offline Sync with the AMC**.
13. On the Offline sync screen, select **read**.
14. When prompted, insert the storage device and select **Next**. The MSL server reads the activation information from the storage device and signals successful completion.
15. Select the option to **Exit from the server console**. You have successfully performed an offline activation and your MBG license information is retrieved.
16. Insert the MBG software CD or DVD in the CD/DVD-ROM drive of the server.

Complete the installation by following steps 2 through 10 under Install MBG on an Online system on page 12.

INSTALLING IN A VMWARE VIRTUAL ENVIRONMENT

Virtual MBG (vMBG) allows you to deploy MBG as an appliance within a VMware virtualized environment. Virtual MBG supports the same server configurations as the physical server MBG (see Network Profiles on page 4).

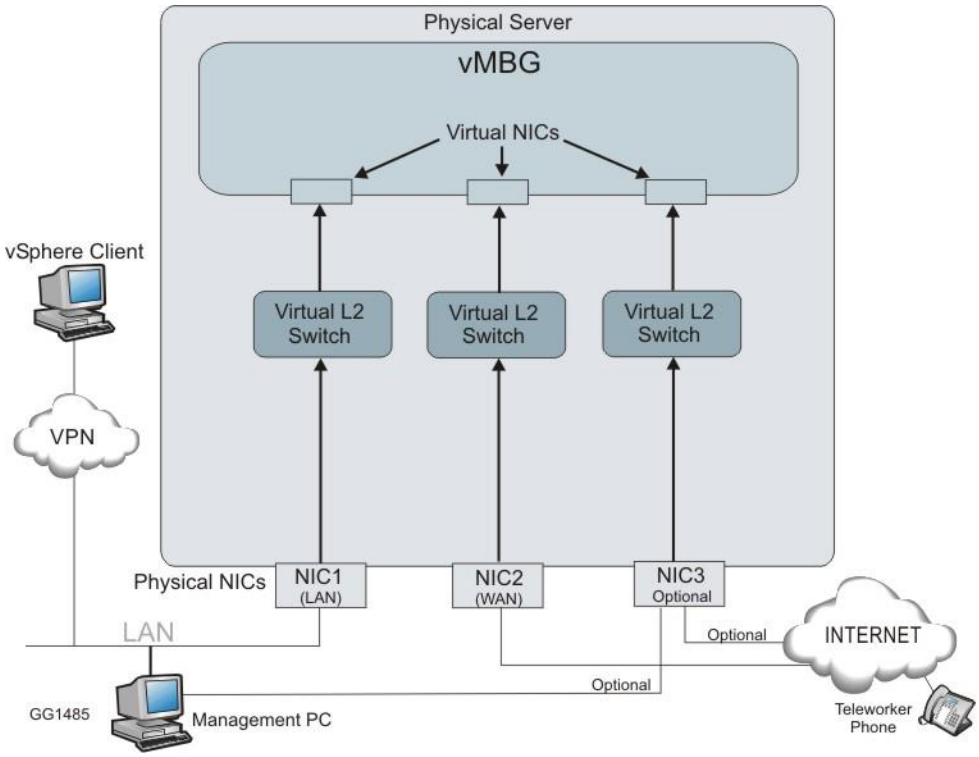


Figure 5. Typical Virtual MBG Appliance

VMware Resources

This section explains the installation of the virtual MBG appliance. Refer to the VMware documentation for a description of the setup and operation of the vCenter Server and the vSphere Client.

Virtual MBG is supported on the following platforms:

- For a list of the VMware vSphere software product versions supported by MBG, see the *Virtual Appliance Deployment Guide* on the Mitel Customer Documentation site at http://edocs.mitel.com/
- See the VMware main documentation page at https://www.vmware.com/support/pubs/ for links to the following information:
  - New Features and Release Notes
  - Hardware and Software Compatibility Information
  - System Administrator Documentation (Main Documentation Set plus additional resources)
  - Optional vSphere Products and Modules
  - Automators and Customizers
- See the VMware Compatibility Guide at http://www.vmware.com/resources/compatibility/search.php for supported hardware platforms.
- For vSphere tutorials and training videos/demos, go to http://www.rtfm-ed.co.uk/vmware-content/vsphere-videosdemos/.

If you experience low transfer speeds though a Virtual MBG that is operating in server-gateway mode, it may be necessary to adjust the Large Receive Offload (LRO) settings,

which are located in the vSphere client application under Configuration > Advanced Settings > Net. For up-to-date information on this issue, check the VMware knowledge base at http://kb.vmware.com/; for example http://kb.vmware.com/kb/1027511.

Requirements

The following requirements apply to virtual MBG installations:

- Refer to the *Virtual Appliance Deployment Guide* available at Mitel Online for:
  - A list of the VMware software product versions supported for use in a Mitel virtualized data center.
  - Details concerning virtual appliance resource requirements, including the number of vCPUs, disk space and memory that must be configured/reserved. The vMBG OVA template enforces these specifications during deployment for each of the two available deployment configurations (vMBG Small Business and vMBG Enterprise).
  - Information on how to configure VMware infrastructure and features, including resiliency, high availability and resource management and the deployment mode.
- Refer to the *MBG Engineering Guidelines* available at Mitel Online for:
  - Capacity constraints, including the maximum number of SIP and MiNET registered devices and concurrent G.711 calls supported for each of the two available deployment configurations (vMBG Small Business and vMBG Enterprise).
- See Appendix B of this guide for details on Offline synchronization. Internet access to allow licensing from the Applications Management Center (AMC). Offline synchronization is not supported with virtual deployments.
- A DNS server that is reachable from the platform.
- The virtual MBG software in an OVA archived file from Mitel. This archive of OVA files contains the OVF 1.0 descriptor and VMDK file.

The following constraints apply:

- Virtual MBG is not supported if you manually install MBG (that is, install the MSL and the MBG software into a VMware virtual machine and then use a virtual MBG Application Record ID to activate the software). Virtual MBG is only supported if you install it from the virtual MBG .ova file.
- Migration of a physical MBG system database backup to a virtual MBG deployment is not supported. Virtual MBG deployments do support application data backup and restore, however.

Collect Properties

The following table itemizes the information you will need to enter during software installation and configuration. For efficient installation, gather this information before you start the installation:

ITEM	NOTES	YOUR INFORMATION
Localization		
Time zone setting	Identify the MSL operating system time zone setting. The default is America/New York. The Time zone setting also determines your system telecommunications	

ITEM	NOTES	YOUR INFORMATION
	regional settings.	
Keyboard Type	Identify the preferred keyboard type (default is **us**).	
Application		
Initial Administrator Password	Record the initial administrator password for the MSL server manager interface. This password must be at least six characters long. When you access the server manager, you will be prompted to change this initial password. **Note**: You must enter a password before you deploy the system; otherwise, the system will not boot up.	Initial server manager Administrator Password: _____ Final server manager Administrator Password: _____ It is recommended that you use a strong password that contains all of the following: upper case letter, lower case letter, number, non-alphanumeric character, and be at least seven characters long. Do not use a commonly used word (for example: 'password').
Hostname	Set the hostname of the system.	
Domain Name (Optional)	Specify the domain name for the hostname above. The default domain name is "mycompany.local".	
License Key (Optional)	Identify the License Key (ARID) for this system. The ARID is used by the AMC to distribute the system licenses.	
DNS Server (Optional)	Record the IP address of your corporate DNS server. **Note**: If your DNS is supplied by your ISP, leave this setting blank.	
Remote Network Address for server administration (Optional)		
Remote Network Netmask (Optional)		
Network Settings		
LAN IP Address	Record the IP address of the local (LAN) interface. This must be a valid IP address on the local LAN. **Note**: You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this IP address from vSphere Client. Right-click on the MiCollab and click **Edit Settings**. Click the **Options** tab, click **Properties** and enter the LAN IP	

ITEM	NOTES	YOUR INFORMATION
	Address.	
LAN Netmask	Record the Netmask of the LAN	
WAN IP Address (Optional)	For Network Edge (Server-gateway) deployments, record the IP address of the external (WAN) interface. This must be a valid IP address on external WAN. For LAN only (Server-only) deployments, use an IP address of 0.0.0.0. **Note**: You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this address from vSphere Client. Right click on the MiCollab and click **Edit Settings**. Click the **Options** tab, click **Properties** and enter the WAN IP Address.	
WAN Netmask (Optional)	Record the Netmask of the WAN.	
LAN (Optional)	Optional network interface that can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.	
Default Gateway IP Address	Record the Gateway IP address. For Server-gateway deployments this gateway typically points to the internet. For Server-only deployments, this gateway typically points to a LAN router.	

For additional information concerning VMware deployments, refer to the *Mitel Virtual Appliance Deployment Guide* available at Mitel OnLine.

Deploy Virtual MBG Appliance

You deploy the virtual MBG vApp as an image in OVF 1.1.0 package format (file suffix of .ova). The virtual MBG .ova file contains the VMware tools, MSL operating system and MBG software as a pre-installed image. The MBG vApp is unique from the other MBG software application files.

Typically, you deploy virtual appliances into the vSphere environment from the vSphere Client application that runs on a Windows PC. However, you can also use the command-line *ovftool* to deploy vApps (from .ovf or .ova files). Both methods involve deploying an OVF Template. You can deploy an OVF template from any local file system that is accessible from the vSphere Client machine or from a remote web server.

To deploy Virtual MBG:

1. Obtain the virtual MBG VMware .ova archive file from Mitel Online:
   - Launch a web browser on the vSphere Client PC.

- Log in to Mitel Online at https://www.ebiz.mitel.com.
- Click Technical and then click Software Downloads.
- Click MiVoice Border Gateway.
- Click the appropriate virtual MBG Software Download version:
  MiVoice Border Gateway Standalone Download - Server and VMware Installs
- Review the Release Notes.
- Verify that the versions of the software and applications are correct.
- Download the required .ova file by clicking the link in the table.
- Select a download method: **HTTP** or the **Software Download Manager**.
- Select a location on your vSphere Client PC to store the downloaded .ova file.

2. Launch the vSphere Client application on the network PC.
- Click Start > All Programs.
- Click VMware > VMware vSphere Client.
- Enter the IP address or hostname of the Hypervisor ESX/ESXi Host server OR enter the IP address or hostname of the vCenter Server.
- Enter your username and password.
- Click **OK**.

3. In the vSphere Client application screen, click **File > Deploy OVF template . . .** The *Deploy OVF Template* screen opens.

4. Do one of the following:
- Deploy from file: if the OVF template file was downloaded to the local computer or to a network share drive, then click **Browse** to locate the file. (On Microsoft Vista systems, select *.ova* in the File Type list.)
- Deploy from URL: if the OVF template file is on the internet or accessible through a web browser; enter the URL of the location of the file.

5. Click **Next**. The *OVF Template Details* screen displays. The Version field identifies the version of the virtual MBG preinstalled software.

6. Click **Next**. The *End User License Agreement* screen displays.

7. Click **Accept** to accept the license agreement, then click **Next**. The *Name and Location* screen displays.

8. Enter a meaningful **name** for this virtual MBG instance or accept the default name. Enter a folder location within the inventory if the vSphere Client is connected to an ESX/ESXi host. Click **Next**. The *Deployment Configuration* screen appears.

9. Choose the required deployment configuration for your site from the drop-down menu: **Small Business** or **Enterprise**. After you select a deployment configuration, user limits and required hardware resources are displayed on the screen. Click **Next**. The following three steps are dependent on your configuration.

10. If you are using the optional vCenter Server, select the appropriate Host/Cluster for this deployment. Click **Next**.

11. If you are deploying virtual MBG in a vCenter Server, select the Resource Pool for the virtual MBG instance. Click **Next**.

12. If multiple datastores are available, select the datastore where the virtual machine files will be stored. Click **Next**. The *Disk Format* screen appears.

13. Select **Thick Provision Lazy Zeroed**. Selecting any other option, such as Thin Provisioning, can cause voice quality issues due to disk sharing. Click **Next**. The *Network Mapping* screen appears.

14. Configure the network mapping. (This screen is only displayed if the network defined in the OVF template does not match the name of the template on the host to which you are deploying vMBG.)

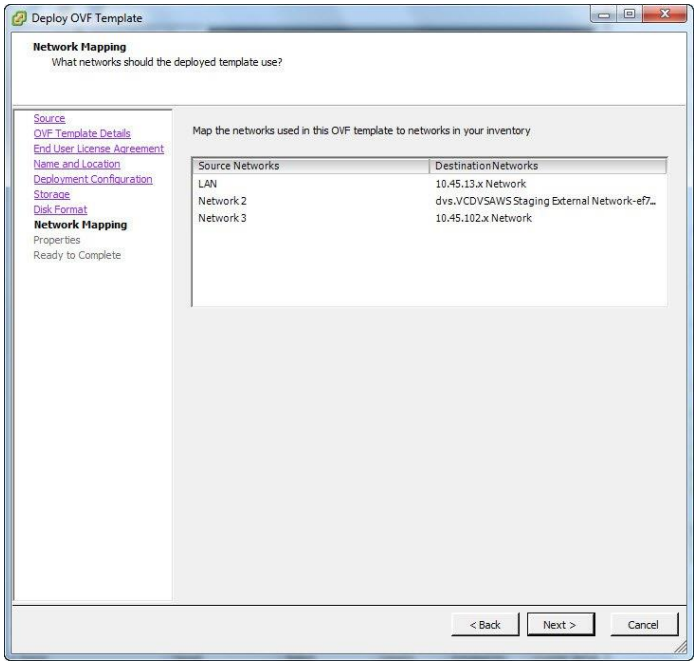


Figure 6. Network Mapping

The required settings are dependent on your deployment configuration:

- **Network Edge (Server-Gateway) Mode**: In this configuration mode, the server functions a firewall/Internet gateway with two Ethernet interfaces. One interface is connected to the internal network (LAN) while the other is connected to the external network (Internet). Select the destination LAN and WAN networks for the OVF template. These are the "Associated Networks" that are assigned in the LAN and WAN IP Pools. You must assign the LAN and WAN destinations to different networks.
- **LAN Only (Server-only) Mode**: In this configuration mode, the server is only connected to the internal network (LAN). For this mode, only select a destination LAN network for the OVF template.
- **LAN (Optional)**: This interface can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.

Contact your Data Center administrator for more details about which network mapping to use.

15. Click **Next**. If you are deploying on vCenter, the *Properties* screen appears. You can use this screen to configure the MSL operating system parameters. Complete the fields in this screen using the information that you gathered above. Mandatory fields are highlighted with a red border.

- You must specify both the LAN IP and WAN IP addresses. Otherwise, the virtual appliance will not power on. If you are deploying the virtual machine in LAN only (server-only) mode set the WAN IP address to 0.0.0.0.
- For Network Edge deployments, ensure that the LAN IP and WAN IP addresses are on different subnets and the Gateway IP address is on the subnet of the WAN IP address.
- You can only use this screen to set the LAN IP and WAN IP addresses for the initial deployment of the appliance. After initial boot-up, you must use the MiCollab server console interface to modify the LAN IP or WAN IP addresses.

Note: To create a blank template for cloning, leave the following fields empty: Administrator Password, Hostname, Domain Name, LAN and WAN IP addresses. After you create the clone, you must complete these fields before you can proceed with deployment. You cannot clone an active (deployed) virtual machine.

16. Click **Next**. The *Ready to Complete* screen appears.
17. Review the information and click **Finish**. vSphere starts the deployment of virtual MBG on the server. A progress bar is displayed.
18. After the dialog indicating that the deployment is complete appears, click **Close**. The virtual MBG vApp appears in the inventory list in the left side navigation pane.

Configuration

1. To launch the MSL server console:
   - right-click on the virtual MBG name in the inventory list and click **Power > Power On**.
   - right-click on the virtual MBG name again and then click **Open Console.** MSL boots and the server console appears. Click inside the console window to continue. To release the cursor for other desktop activities, press CTL + ALT.
2. Do one of the following:
   - If you deployed vMBG on vSphere vCenter and used the Custom Template to configure the MSL Operating System parameters, you can log in to MSL and begin using MBG.
   - If you did not use vSphere vCenter, you must follow the instructions in the *Mitel Standard Linux Installation and Administration Guide* to configure the MSL operating system. You may be prompted to **Install applications from CD/DVD?** Select **No**. If you are unsure if you have the latest version of MBG software, access the Blades panel in the MSL console and check for available upgrades.

Notes:

- If the Mitel Virtualization Framework requires upgrading, the MVF blade will appear on the Blades panel. Install it to take advantage of optional VMware features such as SRM and High Availability.
- If the MSL server lacks direct access to the Internet, you can connect to the AMC by opening a pinhole in your firewall or by configuring a licensing proxy server to perform port forwarding. For implementation details, see the MSL *Installation and Administration Guide* and the *Mitel Virtual Deployment Guide*. Offline synchronization is not supported by virtual deployments.

3. In the left-hand menu of the server manager, under Applications, click **MiVoice Border Gateway**. For MBG configuration instructions, click the **Help** icon in the upper right

corner of the MBG interface. To configure remote phones to operate as teleworker devices, refer to the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.

INSTALLING IN A MICROSOFT HYPER-V VIRTUAL ENVIRONMENT

If you are installing MBG in a Microsoft Hyper-V environment, refer to the *Virtual Appliance Deployment Guide* for hardware and software requirements. After you have done this and created the virtual machine, use the "physical" software installation procedure to install the MBG virtual application.

Limitations

- Although you use the physical software installation procedure to install vMBG, you must assign a virtual product license to the ARID.
- Hyper-V virtual machines that run Mitel Standard Linux (MSL) do *not* support connection of USB devices. Accordingly, the MSL software installation must be performed from the CD/DVD-ROM drive.
- Mitel software must be installed using traditional physical ISO images available from Mitel OnLine. OVA images cannot be used. After creating the virtual machine, use the ISOs to install the MSL operating system and MBG application software as you would on a physical system.
- Once the software has been installed and licensed, Hyper-V must maintain online connectivity to the AMC and is subject to the same Sync Expiry rules in place for VMware-based deployments.
- To achieve the same performance as VMware, a Hyper-V virtual machine requires twice as many virtual processors.

DISABLING THE MBG SERVICE

Disabling the MBG service can be done immediately or can be queued until all currently active calls are completed (“Courtesy Down”).

Note: Calls that are in the “Calling”, “Hold”, or “Transfer” state are not maintained. (In a clustered environment, you can make a node shut down more gracefully by setting its Cluster Weight to zero before disabling. This ensures that the node remains in service until all sets are idle for at least 30 seconds. For more information about setting Cluster Weight, see the MBG online help.)

To shut down immediately:

1. On the MBG main page, click the **System status** tab and then click **Dashboard**.
2. Click **Stop**.
3. Click **OK** to confirm the immediate shutdown.

To shut down after all currently active calls are completed:

1. On the MBG main page, click the **System status** tab and then click **Dashboard**.
2. Click Courtesy Down.
3. Click **OK** to confirm the Courtesy Down shutdown.

ENABLING THE MBG SERVICE

When you access MBG, the web interface opens on Dashboard screen which displays the MBG status, Clustering status, and licensing information.

Note: You must select a Network Profile before you can enable the MBG service. See page 4.

To enable the server:

1. On the MBG main page, click the **System status** tab and then click **Dashboard**.
2. Click **Start**. MBG starts and is enabled.

TELEWORKER SERVICE

This section contains corporate and remote location software, hardware, and connectivity/network requirements necessary to support the teleworker service of the MiVoice Border Gateway Solution.

CORPORATE LOCATION REQUIREMENTS

Hardware

Please refer to the *MSL Qualified Hardware List*, available at Mitel OnLine, for hardware combinations that have been tested in Mitel's labs.

- For deployments of less than 100 sets, select an **entry class** server.
- For deployments of 100 to 500 sets, select a **mid class** server.
- For deployments of 500 or more sets, please contact Mitel Sales Engineering.
- For clustered deployments, each server in the cluster should have the same, or similar, processor capacity.

Software

ITEM	REQUIREMENT
MSL software	To determine the MSL software version(s) required for MBG, review the product Release Notes available in the Mitel Knowledge Base.

Communication Platforms

ITEM	REQUIREMENT
MiVoice Business (3300 ICP)	To determine the MSL software version(s) required for MBG, review the product Release Notes available in the Mitel Knowledge Base.
MiVoice Office 250	
MiVoice MX-ONE	
MiVoice 5000	

Phones/Devices

For a complete list of devices that are supported by MBG and its services, please refer to the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.

License Requirements

MBG licenses are available in various quantities. For detailed licensing information, see Upgrading MiVoice Border Gateway Licenses on page 81.

Each MBG service requires licensing as follows:

- **Teleworking service**: Each teleworker device requires an “MBG Upgrade: TW service” license. Licenses are available in packages of 1, 10, 25 or 50.
- **Secure recording connector service**: You need a quantity of “Secure Recording Connector” licenses equal to the total number of concurrent recording ports you will use. (A “port” corresponds to the recording of a two-party or multi-party conversation.) Licenses are available in packages of 1, 10, or 50.
- **IPv6 service**: For IPv6 interface support, you require one “IPv6 License for MBG.”
- **SIP Trunking service**: For SIP Trunking support, you require one “MBG: 1 SIP Trunking Channel License” for each of the maximum number of simultaneous calls you estimate that you will make.
- **Web Proxy and Remote Management**: No license is required to use these services.
- Transcoding (Compression) Licenses:
  - **For MBG**: You can configure MBG to compress the voice streams to and from remote MiNET devices. You need a compression license for each call that will concurrently run G.729. **Note**: Enabling G.729 transcoding may degrade voice quality. In addition, it increases the load on the server’s CPU which may reduce the number of simultaneous calls the server can handle. If the ICP has the appropriate compression licenses and is programmed to make the licenses available to the remote sets, use these licenses instead.
    You can also configure set-side compression to apply a compression codec to the voice traffic going to remote sets. See the “Configure Transcoding” topic in the MBG online help for more information.
  - **For SRC**: The CRE may request that the voice stream be compressed. In this case, when properly provisioned with compression licenses, SRC automatically applies

compression to the stream that it sends to the CRE. One compression license is required per recorded call. If there are no licenses available, SRC continues to send the voice stream but it is not compressed.

Software Assurance

The Mitel Software Assurance (SWA) Program is a subscription-based service that provides customers with access to new software releases, updates, functionality and product support services for all users (ports) on a given application record. The Mitel Applications Management Center (AMC) manages the entitlement of the Software Assurance Program, determining whether a given application record ID for a customer is entitled to a specific software installation or upgrade. Initial product purchase includes 13 months of Software Assurance. The program can then be renewed for your chosen term. (Note: Discounted rates are applied to multi-year renewals.)

Renewing Software Assurance

Your Authorized Mitel Reseller will contact you before the expiry of your Software Assurance term to assist you with the renewal process. When you have decided upon a renewal term (from 1 day to 4 years), your Mitel Reseller will supply a price quotation. Upon acceptance of the quotation, your Mitel Reseller places your order and your Software Assurance is renewed within minutes. **Note**: If your software assurance plan has expired, you can still renew it, but there will be a re-enlistment fee.

For more information about Software Assurance:

1. Log into Mitel Online.
2. Under Services, click **Software Assurance**.

Firewall Requirements

When using the MBG server behind a firewall, the firewall must have the following capabilities:

- At least **three** physical interfaces:
- Internal network
- External network / Internet
- DMZ
- Must preserve TCP and UDP port numbers used on the external address of the firewall when the packets are passed to the MBG server in the DMZ.
- Must provide static network address translation between an externally visible address and the DMZ address of the MBG server.
- SIP awareness must be disabled.

Note: Firewalls with only two ports are not supported even though they may be able to simulate a DMZ using port forwarding.

For a detailed list of required firewall settings, refer to the *MBG Engineering Guidelines* available at Mitel OnLine.

SUPPORT FOR HTML APPLICATIONS

MBG has the ability to automatically fetch HTML applications from ICPs and make the files available for downloading by teleworker devices. For example, Mitel IP Phones located on the Internet can download a screensaver HTML application from an ICP via MBG.

A list of valid HTML applications in maintained by MBG. This list is updated periodically when MBG fetches the latest versions of the applications from the ICPs.

Notes:
- MBG does not support HTML applications that require continual access to internal network in order to function.
- To facilitate downloading HTML applications from the ICP, firewalls must allow TFTP traffic between the MBG and ICP. Refer to the engineering guidelines for details.

REMOTE LOCATION REQUIREMENTS

To support the teleworking service of MBG, each remote location requires the following components:

- IP/SIP Phone(s) from the list of supported phones.
- Broadband Router (Internet Gateway) that provides NAT and local DHCP.
- Sufficient Internet bandwidth to support any other Internet traffic that uses the same link, such as web browsing. The connection must terminate on an Ethernet device.
- Each remote location also requires a **broadband** Internet connection that provides
  - a bandwidth of at least 50 Kbps, bi-directional, if G.729a compression is enabled at the corporate site, or
  - a bandwidth of at least 100 Kbps, bi-directional, if G.729a compression is **not** enabled at the corporate site.

For bandwidth requirement calculations, refer to the *MiVoice Border Gateway Engineering Guidelines*.

Phones/Devices

The remote location must meet the following requirements:

COMPONENT	DETAILS	NOTES
Supported IP Phones	For a complete list of devices that are supported by the teleworking service of MBG, please refer to the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.	
Supported Mitel peripherals	5305 IP Conference Unit 5310 IP Conference Unit Line Interface Module Cordless Module and Accessories IP Programmable Key Module (PKM)	Some peripherals are listed in the MBG Remote Phone Configuration Guide.
Maximum IP Phones per Remote Site	Bandwidth must be provisioned for all Internet traffic, including applications other than the MBG Solution application. **Note**: Maximum number of sets per remote site may be adversely affected by router performance.	

Network Parameters

COMPONENT	DETAILS	NOTES
Network Parameters	IP Address	Provided by the Internet Gateway
	Subnet Mask	
	Default Gateway IP Address	

	Teleworker Gateway IP Address	Manually programmed into the IP Phone (see the *MBG Remote Phone Configuration Guide* available at Mitel OnLine)

Router/Internet Gateway

In addition to a supported phone, the remote location requires a broadband router (or Internet Gateway) that provides NAT and local DHCP. This device will allow both your phone and PC to share the single IP Address provided by your Internet Service Provider.

Note: MBG is not supported in situations that require specific software to be loaded on the PC to manage the connection. (For example, AOL broadband.)

CONFIGURE TELEWORKER SERVICE

The following procedure describes how to configure the Teleworker Service on MBG and the remote SIP and MiNet devices.

Configuring the Teleworker Service on MBG

To configure the teleworker service on MBG:

1. Access the MSL server manager and click **MiVoice Border Gateway** under Applications.
2. Add the ICPs to MBG:
   a. On the MBG main page, click the **Service configuration** tab and then click **ICPs**.
   b. Click the + sign.
   c. Enter a **Name** of the ICP (for example, ICP1).
   d. Enter the **Hostname or IP Address** of the ICP.

Note: For MiVoice Office 250 systems equipped with a Processing Server (PS-1), enter the hostname or IP address of the PS-1. SIP traffic will then point to the PS- instead of the base MiVoice Office 250.

   e. For **Type**, select the type of ICP:
      - MiVoice Business
      - MiVoice Office 250
      - MiVoice MX-ONE
      - MiVoice 5000
      - MiVoice Office 400
      - Silhouette
   f. (Optional) Enter the **Installer password** for this ICP. The password is supported only on MiNet phones, *not* on MiCollab Client softphones, Spectralink phones, or SIP phones. Valid characters include 0 to 9, *, and #.
   g. Select the **SIP Capabilities** to support: **UDP**; **UDP, TCP**; or **UDP, TCP, TLS**. Ensure that this setting matches the capabilities of the ICP. For example, select **UDP, TCP, TLS** for MiVoice Business or **UDP** for MiVoice Office 250.
   h. (Optional) Select **Indirect call recording capable** to allow MBG to provide a secure recording connector (SRC) service to remote MiNET devices registered on the ICP.
   i. Click **Save**.
   j. Repeat for all other ICPs connected to MBG.

3. (Optional) Configure the default ICP(s) for MBG:
   a. On the MBG main page, click the **Service configuration** tab and then click **ICPs**.
   b. In the ICP listing, locate the ICP that will be your default.
   c. Do one or both of the following:
      - Select the **Default for MiNet ICP**. Select this option only when **Restrict MiNet devices** is disabled on the Settings screen.
      - Select the Default for SIP ICP.
      - You can use the same ICP for both roles.
   d. Click Update Default ICPs.
4. Enable the server:
   a. On the MBG main page, click the **System status** tab and then click **Dashboard**.
   b. In the **MBG status** box, click **Start**. MBG starts and is enabled.

Note: You must select a Network Profile before you can enable the MBG service. See page 4.

5. Provision the teleworker devices:
   - To provision devices using the web interface, see Provisioning MiNet Devices and Provisioning SIP Devices.
   - To provision devices using a CSV file, see Bulk Provisioning of MiNet and SIP Devices.

Notes:
- Following a software upgrade, reconfiguration is not required other than to add new hardware (ICPs or devices).
- After completing the initial installation, run the Basic connectivity test on Diagnostics page. The test confirms connectivity to ICP signaling services such as MiNet, SIP and TFTP.

Provisioning MiNet Devices

MiNet is Mitel's proprietary signaling protocol used to control Mitel IP and TDM devices. MiNet devices in a teleworker environment can take advantage of the same features and functionality as they would when connected directly an ICP.

Note: When using MBG in conjunction with MiNet devices on a MiVoice Business, set the **NAT Address Type** for the devices to **Native** (this setting is located under System > Devices and Feature Codes > Trunks > <trunk number>).

There are three ways to add MiNet devices to MBG:

- Auto-configuration
- Manual Configuration
- Unrestricted Access

Note: In addition to configuring the MiNet devices with the web interface, you can also configure them in a CSV file. For details, see Bulk Provisioning of MiNet and SIP Devices.

Auto-configuration of MiNet Devices

Use this procedure to enable your MiNet devices to connect to MBG automatically.

To program auto-configuration of MiNet devices:

1. On the MBG main page, click the **Service configuration** tab and then click **ICPs**.
2. Do one of the following:
   - To add a new ICP, click the + sign.
   - To update an existing ICP, locate in the list and click ✎.
3. Enter the **Installer password** between five and 10 characters in length. Valid characters include 0 to 9, *, and #.
4. Click **Save**.
5. Repeat for other ICPs as required.
6. On the remote MiNet devices, program the following:
   - For **TELEWORKER GATEWAY**, enter the public IP address of MBG.
   - For **TW INSTALL PW**, enter the Installer Password of the ICP.

Note: Field names vary by device. For valid field names and complete programming instructions, refer to the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.

The programmed remote MiNet devices may now register with MBG. They automatically appear on the MiNet devices screen with default values and a status of "enabled". If the devices are already listed on the ICP, they will be registered automatically. If they are not yet listed, then the ICP will request PINs from the sets in order to complete the registration.

Manual Configuration of MiNet Devices

Use this procedure to manually configure MiNet devices in a teleworker environment. Manually provisioning devices is recommended if you have a limited number of devices.

Note: Complete this procedure only if an installer password (auto-configuration) is not implemented.

To manually provision MiNet devices:

1. On the MBG main page, click the **Service configuration** tab and then click **MiNet devices**.
2. Click the + sign.
3. Select **Enabled** to enable the set and allow it to connect to the ICP
4. Enter the **MAC address** of the phone.
5. Update other fields as required.
6. Click **Save**.
7. Repeat for all MiNet remote devices connected to MBG.

Unrestricted MiNet Devices

Use this procedure to disable the requirement for MiNET devices to authenticate themselves. This enables any MiNet device to register without a password, provided that it is programmed and configured on the default ICP. (See above to program a default ICP.)

Because MBG simply passes the MiNet devices to the ICP for registration, this method should restricted to LAN-based teleworker implementations. It should not be used for MiNet devices located on the Internet.

To enable unrestricted MiNet device access:

1. On the MBG main page, click the **System configuration** tab and then click **Settings**.

2. Under MiNet options, clear **Restrict MiNet devices**.
3. Click **Save**.
4. On the remote MiNet devices, program the following:
    - For **TELEWORKER GATEWAY**, enter the public IP address of MBG.

Note: Field names vary by device. For valid field names and complete programming instructions, refer to the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.

The programmed remote MiNet devices may now register with MBG. They automatically appear on the MiNet devices screen with default values and a status of "enabled".

Provisioning SIP Devices

Notes:

- In addition to configuring SIP devices with the web interface, you can also configure them in a CSV file. For details, see Bulk Provisioning of MiNet and SIP Devices.
- For MiVoice Office 250 implementations, select **Yes** for the **Use Registered Username** value of the SIP phone profile group (this setting located under System > Devices and Feature Codes > SIP Peers > SIP Phone Groups on the MiVoice Office 250).
- For MiVoice Business implementations, add SIP devices to the ICP in a similar fashion to other devices by using either the “User Configuration” or “Multiline IP Set Configuration” form in the MiVoice Business System Configuration Tool.
- MBG cannot disable restricted login by SIP devices. This means is that all SIP devices must be programmed on the MBG before being presented to the ICP.

Manual Configuration of SIP Devices

Use this procedure to manually configure SIP devices in a teleworker environment.

To manually provision SIP devices:

1. On the MBG main page, click the **System configuration** tab and then click **Settings**.
2. Under **SIP Options**, enable **SIP support** by selecting one or more of the following :
    - **UDP**
    - **TCP**
    - **TCP/TLS**
3. For each protocol, choose which interface the SIP connector listens to by selecting an **Access Profile**:
    - **Private**: The SIP connector listens on the LAN interface.
    - **Public**: The SIP connector listens on the LAN and WAN interfaces.
    - **Third interface only**: The SIP connector listens on the third interface only (used when MBG has two LAN interfaces, one of which is connected to a SIP trunk).
    - **WAN-reachable IPs only**: The SIP connector listens on the WAN interface only.
4. Click **Save**.
5. On the MBG main page, click the **Service configuration** tab and then click **SIP devices**.
6. Click the + sign.

7. Select **Enabled** to enable the set and allow it to connect to the ICP.
8. For **Set-side username**, enter the set-side (MBG side) user name for the SIP client you want to authorize.

Note: In Auchan mode, MiVoice Border Gateway usernames must always be associated with a PNI. MBG maps between PNI+DN (set-side username) and DN (ICP-side username). In case of a duplicate DN, MBG will not allow new user creation.

9. For **Set-side password**, enter the set-side password for the SIP client you want to authorize. Then enter the **Confirm set-side password**.

Note: Choose a secure password that is not trivial. Ensure that it contains letters, numbers, and punctuation. (For example, Mitel*Server1!) If you attempt to configure a weak password, you will receive a warning or be prevented from preceding (depending on whether **Permit Weak Passwords** is enabled on the Settings screen). A secure set-side password is required on MBG in case the ICP does not require a strong password.

10. For **ICP-side username**, enter the Username that this SIP client uses to access the ICP.

Note: In Auchan mode, MiVoice Border Gateway usernames must always be associated with a PNI. MBG maps between PNI+DN (set-side username) and DN (ICP-side username). In case of a duplicate DN, MBG will not allow new user creation.

11. For **ICP-side password**, enter the password that this SIP client uses to access the ICP. Then enter the **Confirm ICP-side password**.

Note: Leaving the two preceding fields blanks causes the ICP-side credentials to default to the same values as set-side credentials This may not match the password configured in the ICP, causing connections for this set to be denied. We recommend that you enter both SIP- and ICP-side credentials for more secure authentication.

12. Update other fields as required.
13. Click **Save**.
14. Repeat for all SIP remote devices connected to MBG.
15. On the remote SIP devices, program the following:
    - For **User Name**, enter the set-side username.
    - For **Password**, enter the set-side password.
    - For **SIP Registrar** or **Domain**, enter the public IP address of MBG.
    - For **SIP Proxy** (if applicable), enter the public IP address of MBG.

Note: Field names vary by device. For valid field names and complete programming instructions, refer to the SIP device manufacturer documentation or the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.

The programmed remote SIP devices may now register with MBG. If the devices are already listed on the ICP, they will be registered automatically.

Bulk Provisioning of MiNet and SIP Devices

This procedure enables you to add or edit multiple device records in a CSV file, and then import the file onto MBG. This is handy when you need to add or amend many records at once.

To facilitate this process, you can download a copy of the CSV file for SIP or MiNet devices and use it as a template. After you have finished making updates, you can import the file back onto MBG. Your changes will be merged into the system, with new and updated data overwriting the previous configuration.

The CSV import:

- retains existing information
- merges imported data with existing data (if possible) and broadcasts the data in a cluster (if present)

Both MiNet and SIP devices specify a minimum set of fields that are required in the import. Otherwise many of the columns will use default settings for the other options.

Notes:

- You need Microsoft Excel® 97, Excel 2000, Excel 2003 or higher installed on your client station to read the spreadsheet.
- Save the spreadsheet as a Microsoft Office Excel Comma Separated Value file with a .CSV extension — for example, minet-export.csv.
- The CSV file must be encoded as ASCII or (if special characters are included) UTF-8.
- To designate a field as unmanaged, enter "usemaster" or "0" in place of a real value. For example, if you enter "0" in the Time Format field, MBG will use the default value of 12.
- In addition to editing multiple devices in a CSV file, you can use the **Bulk edit** command on the MiNET or SIP devices screen. Refer to the online help for details.

To download the spreadsheet and update it with device data:

1. On the MBG main page, click the **Administration** tab and then click **File Transfers**.
2. Do one of the following:
   - To export SIP data, click **SIP Backup**.
   - To export MiNet data, click **MiNet Backup**.
3. Click **Save**.
4. Navigate to the folder where you wish to store the file, and click **Save**.
5. Open the file in Microsoft Excel.
6. Enter information that you wish to import for existing and new users. Enter "usemaster" or "0" for unmanaged (i.e. default) fields.
7. Click **Save As**, enter a **File Name**, navigate to the folder where you wish to store the file, and click **Save**.

To import the spreadsheet containing device data to MBG:

1. On the MBG main page, click the **Administration** tab and then click **File Transfers**.
2. Do one of the following:

- To import SIP data, click **Choose file** beside SIP CSV import/export: SIP Restore, browse to the location of the SIP Device Data CSV file (encoded in ASCII or UTF-8), click **Open** and then click **SIP Restore**.
- To import MiNet data, click **Choose file** beside MiNet CSV import/export: MiNet Restore, browse to the location of the MiNet Device Data CSV file (encoded in ASCII or UTF-8), click **Open** and then click **MiNet Restore**.

A message displays indicating whether the import process was successful. Problems can be corrected by re-importing the file.

SIP TRUNKING

MBG can be used as a SIP trunk proxy to connect a Mitel ICP to the Public Switched Telephone Network (PSTN) via the Internet using Voice over IP (VoIP). There are several benefits to using the MBG as a SIP trunk proxy, including:

- NAT traversal of media and signaling
- Media anchoring for the remote provider
- SIP aware firewall (enhancing the Mitel ICP's existing functionality)
- SIP adaptation and normalization to improve interoperability
- Serves multiple roles (outbound proxy for SIP trunking and legacy MBG functionality), reducing the need for non-Mitel equipment

Other Features

MBG also offers the following other SIP Trunk features:

- **T.38**: T.38 is the ITU standard for sending fax messages over IP networks in real time using UDP packets. Operating modes 2 and 4 are supported at 14,400 bps and lower; V.34 is not supported. This feature is transparent to the administrator and does appear on the MBG interface.
- **Multiple Media lines for T.38**: Key to supporting T.38, SIP Trunking via MBG supports the SIP standard for multiple media lines in a call (RFC 3264). The media type can be audio or video and multiple lines of the same media type can be used within the same SIP session. RFC 3264 states: “A typical example for multiple media streams of the same type is a pre-paid calling card application, where the user can press and hold the pound ("#") key at any time during a call to hang up and make a new call on the same card. This requires media from the user to two destinations—the remote gateway, and the DTMF processing application which looks for the pound key entry. This could be accomplished with two media streams, one … to the gateway, and the other … (from the perspective of the user) to the DTMF application.” This feature is transparent to the administrator and does appear on the MBG interface.
- **SIP Trunk Resiliency**: To maintain system availability, the SIP Trunking solution within MBG includes the ability to configure two MiVoice Business endpoints instead of one. The second endpoint is used as a backup in case the primary fails. When the primary recovers, MBG routes new requests to the primary again. This feature is only available to MiVoice Business endpoints that are configured in a clustered environment. It is not supported by MiVoice Office 250s.
- **KPML Digit Suppression**: MBG supports Key Pad Markup Language (KPML) digit detection and suppression. Some manufacturers, such as Blackberry, embed signaling in the voice stream in the form of DTMF tones which can be perceived as a nuisance by the call participants. To remove them, MiVoice Business informs MBG via signaling when the DTMF should be suppressed. MBG then removes the DTMF, reorders the remaining packets, and streams the voice to the endpoints.

BEFORE YOU BEGIN

Prior to implementing SIP trunking functionality, refer to the *SIP Center of Excellence Guide* available at Mitel OnLine for requirements concerning:

- Supported versions of MiVoice Business or MiVoice Office 250 software
- Compatible SIP trunking service providers, SIP devices, gateways/firewalls and SIP-based applications.

CONFIGURATION OVERVIEW

SIP trunks are established between the Mitel ICP (MiVoice Business or MiVoice Office 250) and the SIP trunking service provider, with the SIP trunk proxy located between these components.

Typically, the SIP trunk proxy is placed alongside the firewall, serving as a method to trunk (connect) voice and video traffic between the PBX and the PSTN. The trunks can be used for both incoming and outgoing traffic.

Port usage considerations:

- Port 5060 is typically used for signaling between the Mitel CP and the SIP service provider (confirm with service provider)
- Ports 20,000 to 50,000 are typically used for Real-time Transport Protocol (RTP) via UDP for voice streaming

MBG provides variable packetization solutions. For example, if the RTP packet framesize is set at 20 ms on the Mitel ICP and another value on the SIP service provider, MBG can translate or convert the framesizes in order to facilitate communication between the components. (See the Remote RTP framesize setting.)

Network Requirements

There must be adequate bandwidth to support the voice over IP connections between MBG and the SIP Service Provider. As a guide, the Ethernet bandwidth is approximately 85 Kb/s per G.711 voice session and 29 Kb/s per G.729 voice session (assuming 20ms Packetization).

Note: 20ms Packetization is assumed in these instructions because it is a requirement on the MiVoice Business in Release 4.1. MBG as a proxy can aid with variable packetization conversion between the SIP provider and the MiVoice Business. Subsequent releases of the MiVoice Business may support various packetization schemes.

As an example, for 20 simultaneous SIP sessions, the Ethernet bandwidth consumption will be approximately 1.7 Mb/s for G.711 and 0.6Mb/s for G.729. Almost all Enterprise LAN networks can support this level of traffic without any special engineering. Please refer to the MiVoice Business or MiVoice Office 250 Engineering guidelines for further information.

Note: For high quality voice, the network connectivity must support a voice-quality grade of service (packet loss <1%, jitter < 30ms, one-way delay < 80ms).

CONFIGURATION EXAMPLE

SIP service providers offer SIP trunks that provide flexible and cost-effective WAN solutions for Mitel ICPs. SIP trunking provides basic feature functionality, billing capability, emergency services support, FAX support, and other services.

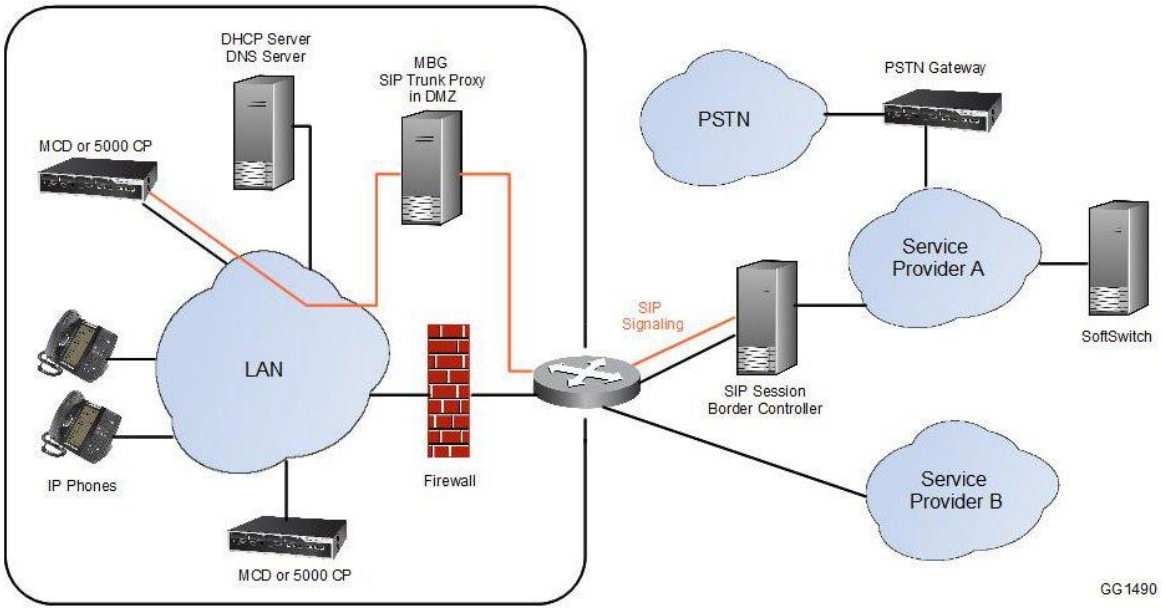


Figure 7. Configuration Example

Note: If you are using MBG in the DMZ behind a third-party firewall, make sure to disable any SIP support in the firewall.

A SIP trunk can have a number of “channels," each of which corresponds with an active media stream. The concept is very similar to that of an ISDN PRI trunk. An ISDN PRI trunk has 23 channels (North America) or 30 channels (outside North America) for media and one or two channels for signaling. All of the ISDN channels can be engaged in calls simultaneously. An equivalent SIP trunking setup would be to have an MBG with 23 or 30 SIP trunk channel licenses. Since one license is used per call, 23 active calls require 23 licenses.

CONFIGURE SIP TRUNKING

1. Configure the Mitel ICP to support SIP trunking via MBG:
   - MiVoice Business (3300 ICP)
   - MiVoice Office 250
   - MiVoice MX-ONE
2. Configure the SIP trunk on MBG

Optionally, configure routing rules to direct incoming SIP trunk calls based on the number dialed rather the SIP username. You can configure multiple routing rules and designate a primary and secondary ICP for each rule. See SIP Trunk Routing by DID.

Configuring the MiVoice Business (3300 Controller) to Support SIP Trunks

To configure an MiVoice Business to support SIP trunking:

1. In the MiVoice Business System Administration Tool, click **View by Category**.
2. Add licenses:
   a. Access the **License and Options Selection** form.
   b. Under Trunking Networking, enter the number of SIP Trunk licenses for your implementation. This is the maximum number of trunk sessions that can be

configured for all service providers and applications connected to the MiVoice Business.

3. Configure the network elements:
   a. Access the **Network Elements** form.
   b. Create a network element for the SIP service provider. Enter a unique Name (e.g. SIPSP). For Type, select **Other**. Select the SIP Peer check box. Enter a SIP Peer Transport value of **UDP** and a SIP Peer Port value of **5060**.
   c. Create a network element for the MBG. Enter a unique Name (e.g. MBG). For Type, select **Outbound Proxy**. Enter an Outbound Proxy Transport Type value of **UDP** and an Outbound Proxy Port value of **5060**.

Note: Confirm the port numbers with your SIP service provider.

4. If non-default SIP port numbers are in use, update the system IP ports:
   a. Access the **System IP Ports** form.
   b. Change the SIP UDP, TCP, and TLS port numbers if necessary.
5. Configure the SIP trunk attributes:
   a. Access the **Trunk Attributes** form.
   b. Select a trunk service number that is available to be changed. Update the configuration to direct incoming calls from the SIP trunks to an answer point in the MiVoice Business. This is consistent with the programming for any incoming trunk on the MiVoice Business.
6. Configure the SIP peer profile:
   a. Access the **SIP Peer Profile** form.
   b. Add a new entry. For SIP Peer Profile Label, enter a name. For Network Element, select the network element created for the SIP service provider. For Outbound Proxy Server, select the network element created for the MBG. For Trunk Service, enter the Trunk Service Number for the trunk updated on the **Trunk Attributes** form. For Use P-Call-Leg-ID Header, select **Yes**.
7. Set up inward dialing modification rules for inbound calls (optional):
   a. Access the **Inward Dialing Modification** form and add one or more new rules to alter the dial strings contained in inbound SIP calls.
   b. Access the **SIP Peer Profile Called Party Inward Dialing Modification** or **SIP Peer Profile Calling Party Inward Dialing Modification** form and associate the inward dialing rule(s) to the network element created for the SIP service provider.
8. Configure an ARS route:
   a. Access the **ARS Routes** form.
   b. Create a route to connect the SIP trunks to the SIP service provider. For Routing Medium, select **SIP Trunk**. For SIP Peer Profile, select the network element created for the SIP service provider. For COR Group Number, enter a Class of Restriction group number.
9. Configure ARS digits dialed (optional):
   a. Access the **ARS Digits Dialed** form.
   b. Add an entry that enables the system to recognize digits and route trunk calls to the SIP service provider using the ARS route. For Termination Number, enter the ARS Route Number.
10. Configure the SIP Peer Profile Assignment for Incoming DID:

a. Access the **SIP Peer Profile Assignment for Incoming DID** form.

b. Add an entry. Associate the range of telephone numbers that have been assigned by the SIP service provider. For SIP Peer Profile Label, select the the SIP Peer Profile Label that you added on the **SIP Peer Profile** form.

11. Update the Class of Service Options:

a. Access the **Class of Service Options** form.

b. Enable the **Public Network Access via DPNSS** field in the class of service for all devices that make outgoing calls through SIP trunks, PRI trunks, LS trunks, and so forth that are connected to SIP Trunks.

Configuring the MiVoice Office 250 to Support SIP Trunks

To configure a MiVoice Office 250 to support SIP trunking:

To create a SIP trunk group:

1. Select **System > Devices and Feature Codes > SIP Peers > SIP Trunk Groups**.

2. Configure a SIP trunk group:

Note: You can create a SIP trunk group from a pre-existing template or by entering data obtained from your service provider. The following procedure illustrates how to create a SIP trunk group with data.

a. Right-click in the right pane. The Create SIP Trunk Group dialog box appears.

b. Click **Create SIP Trunk Group**. The Create SIP Trunk Group Extension dialog box appears.

a. Select the **Starting Extension** number or accept the default (92002).

b. Select the **Number of Extensions** (only one is required).

c. Click **OK** to create the new SIP trunk group.

d. Assign a username and description to the new SIP trunk group. The description can be up to 20 characters and appears in all trunk group lists in the database. The username can be up to 10 characters and appears on display phones.

e. Select the new SIP Trunk Group, and then select **Configuration**.

f. Right-click **IP Address**, enter the address of the SIP service provider, and then click **OK**.

g. Right-click **Operating State**, select **In-Service**, and then click **OK**.

h. Right-click **Port Number**, enter **5060**, and then click **OK**.

3. Configure route sets for the SIP trunk group:

a. Select the new SIP Trunk Group, and then select **Configuration > Route Sets**.

b. Right-click in the right pane and click **Add To Route Sets List** to create a Route Sets element (for example, **1**).

c. In **Hostname**, enter the host name of the MBG.

4. Configure the SIP trunk group settings:

a. Select the new SIP Trunk Group, and then select **Trunk Group Configuration**.

b. For **Day Ring-In Type** and **Night Ring-In Type**, select **Single** and enter the phone number or hunt group pilot number you want to alert.

c. For **Calling Party Name**, enter the name of the SIP service provider.

d. For **Calling Party Number**, enter the calling number of the SIP Service Provider.

5. Program the SIP Peer Trunks:

a. Select the new SIP Trunk Group, and then select **Trunk Group Configuration - Trunks**.
b. Right-click in the right pane and click **Create SIP Peer Trunk**.
c. Select the **Starting Extension** number or accept the default.
d. Select the **Number of Extensions** (only one is required).
e. Click **OK** to create the new SIP peer trunk.
f. Assign a **Label** to the new SIP peer trunk group.

Note: The SIP Peer Trunk belongs to the SIP Trunk Group you created previously.

Configuring the MX-ONE to Support SIP Trunks

To configure an MX-ONE to support SIP trunking:

1. Access the web interface for the MX-ONE Service Node Manager.
2. Add a route:
   a. Select Telephony > External Lines > Route.
   b. Click **Add** to access the **Route - Add** screen.
   c. In the **Type of Signaling** list, select **SIP**.
   d. In the **Profile Name** list, select the name of the endpoint that is to be used for the route. If you cannot find the endpoint for your implementation, select **Default**.
   e. Click **Next ->** to continue.
   f. In the **Route Name** box, enter a name for the route.
   g. In the **Route Number** list, select a route number or accept the default value.
   h. In the **Profile specific settings**, program the endpoint-specific settings.
   i. Click **Apply** and **Done** to return to the **Route** screen.
   j. Locate the route you just added and click the icon to access the **Route - Change** screen.
   k. Select the **SIP** tab, click Advanced and program the SIP-specific settings.
   l. Click **Apply** and **Done** to return to the **Route** screen.
3. Add an external number:
   a. Select Number Analysis > Number Plan > Number Series.
   b. Click **Add** to access the **Number Series - Add** screen.
   c. Select External Numbers.
   d. Click **Next ->** to continue.
   e. In the **External Destination** box, enter the number used to access the SIP endpoint.
   f. Click **Apply** and **Done** to return to the **Number Series** screen.
4. Associate the new external number with the route:
   a. Click Telephony > External Lines > Destination.
   b. Click **Add** to access the Destination - Add screen.
   c. Select Destination.
   d. Click **Next ->** to continue.
   e. Program the following settings:
   - **Destination** - <Destination_Number>

- **Route Name** - <Route_Name>
- Customer Choice - enable

f. Click **Next ->** to continue.

g. Program the following settings:

- Start Position for Digit Transmission - 3
- Type of Seizure of External Line - Immediate
- Show Original A-Number - enable
- Use Original A-Number's Type of Number - enable
- Enable Enhanced Sent A-Number Conversion - enable

h. Click **Apply** and **Done** to return to the **Destination** screen.

Adding a SIP Trunk to MBG

To add a SIP trunk on MBG:

1. On the MBG main page, click the **Service Configuration** tab and then click **SIP trunking**.
2. Click the + sign.
3. Enter a **Name** for the SIP trunk.
4. Enter the **Remote trunk endpoint address** to enable the connection to the SIP service provider. This value can be entered as an IP address or DNS hostname. If the SIP service provider has multiple IP addresses, enter the DNS hostname as a Fully Qualified Domain Name (FQDN). The system will resolve the FQDN into a list of IP addresses and then accept traffic from any of them.

Note: In most cases, the remaining fields can be left at their default values. Update the fields only if unique settings are required by the SIP service provider.

5. Enter the **Remote trunk endpoint port**. The default is port 5060.
6. Select **Accept traffic from any port** to accept incoming requests from any port at the remote trunk endpoint IP address. Clear to accept requests only from the specified IP address and port.
7. Select the **Options keepalives** setting. This setting controls whether SIP Options messages are sent to SIP devices as keepalive mechanisms. Options:
   - **Never** to prevent keepalives from being sent.
   - **Always** to force keepalives to be sent.
8. Enter the **Options interval**. If **Options keepalives** is enabled, this is the interval at which keep-alive messages are sent. The default is 60.
9. Select **Rewrite host in PAI** to change the P-Asserted-Identity (PAI) header contained in outgoing ICP messages to the host IP of the MBG's public interface. Clear to leave the unchanged.
10. Select the **Remote RTP framesize (ms)**. This setting controls the RTP framesize on the set side of MBG. By default, the requested framesize is respected. If you select a non-default setting (e.g. 30 ms), the specified value will be used.

Notes:
- This setting should be changed only if a specific framesize is required on the set side of MBG.
- This setting does not affect the framesize used between MBG and the ICP (MiVoice Business or MiVoice Office 250).

11. Enter the **Idle timeout (s)**. This timer monitors "no traffic" conditions on the trunk. When there is no traffic on the trunk for the selected amount of time (default is one hour), the timer expires and all connections are closed until the next packet is received. The default is 3600 seconds.
12. Select the **RTP address override** setting. This is the interface the MBG server uses to access the SIP trunk provider. If no selection is made, the interface is set in accordance to the configured route to the SIP trunk provider. After updating this setting, restart the system to have the change take effect. For details, see Stop MBG and Start MBG.

Note: Typically, an RTP address override should be used only if your service provider is *not* reachable via the WAN port of MBG.

13. Select **Local streaming** to allow IP phones and devices located behind the same NAT device to communicate with each other directly without going through the MBG server. While this option reduces traffic in the MBG server, it also circumvents the recording of these sets. The default is False (local streaming disabled). The master setting for Local streaming can be programmed in the Configuration Settings.
14. Select the **PRACK support** setting. This setting controls whether the "Provisional Response ACKnowledgement" (PRACK) method is used.
    - **Use master setting** to use the PRACK option programmed in the Configuration Settings. (Default)
    - **Enabled** to enable the trunk to use PRACK.
    - **Disabled** to prevent the trunk from using PRACK.

    If this setting is disabled and the Require header indicates that PRACK is necessary, MBG logs an error and the call will fail. Most peers now support PRACK, which can be useful in interoperability scenarios with the PSTN (see RFC 3262). Disable the setting only if the SIP service provider does not support PRACK.
15. Select the **Log Verbosity** setting. Typically, you would to adjust this setting for troubleshooting purposes. Options:
    - Normal
    - Very Quiet
    - Quiet
    - Verbose
    - Very Verbose
    - **Use master setting** to use the Log Verbosity setting programmed on the Configuration tab. (Default)

Note: Adjust the Log Verbosity setting only when instructed to do so by Mitel Product Support.

16. Enter an **Authentication Username** and **Authentication Password**. Some SIP service providers require authentication of PRACK requests before allowing a trunk connection. Username and password information is provided by the SIP Service Provider and must match the authentication credentials in the SIP Peer Profile form in the MiVoice Business System Administration Tool.
17. (Optional) Enter the DID routing rule mask for this SIP trunk to use. See Configuring DID Routing Rules for more information.

Note: If the trunk does not yet have any rules, a single unprogrammed rule will be listed by default.

18. To save the trunk, click **Save**.

Once the SIP trunk is configured and operational, the following metrics are displayed at the bottom of the page: Calls in progress, Calls per hour, Seconds idle, Active transactions, and Transaction errors (timeout or protocol errors which indicate that something may be wrong with the configuration or connection, or that the provider does not accept the format of our Options (keepalive) messages). The **Trunk Status** field indicates the following:

- Green icon - All trunks connected to both the ICPs (MiVoice Businesses and MiVoice Office 250s) and SIP service providers are "up."
- Yellow icon - Some trunks are down, but at least one trunk connected to an ICP and another connected to a SIP service provider are "up."
- Red icon - A trunking connection cannot be established between the ICPs and the SIP service providers.

Editing a SIP Trunk on MBG

To edit a SIP trunk on MBG:

1. On the MBG main page, click the **Service Configuration** tab and then click **SIP trunking**.
2. Click the sign.
3. In the trunk list, click beside the trunk you want to edit.
4. Edit the SIP trunk options as required.
5. Click **Save**.

CONFIGURE DID ROUTING RULES FOR SIP TRUNKING

Incoming SIP calls are addressed to a SIP username, commonly a Direct Inward Dialing (DID) telephone number. MBG can be configured to map the username (or portion of the username) to a specific ICP (MiVoice Business or MiVoice Office 250). Usernames can be obtained from URIs found in the "Request", "From" and "To" header fields of incoming SIP messages.

Configuration Example

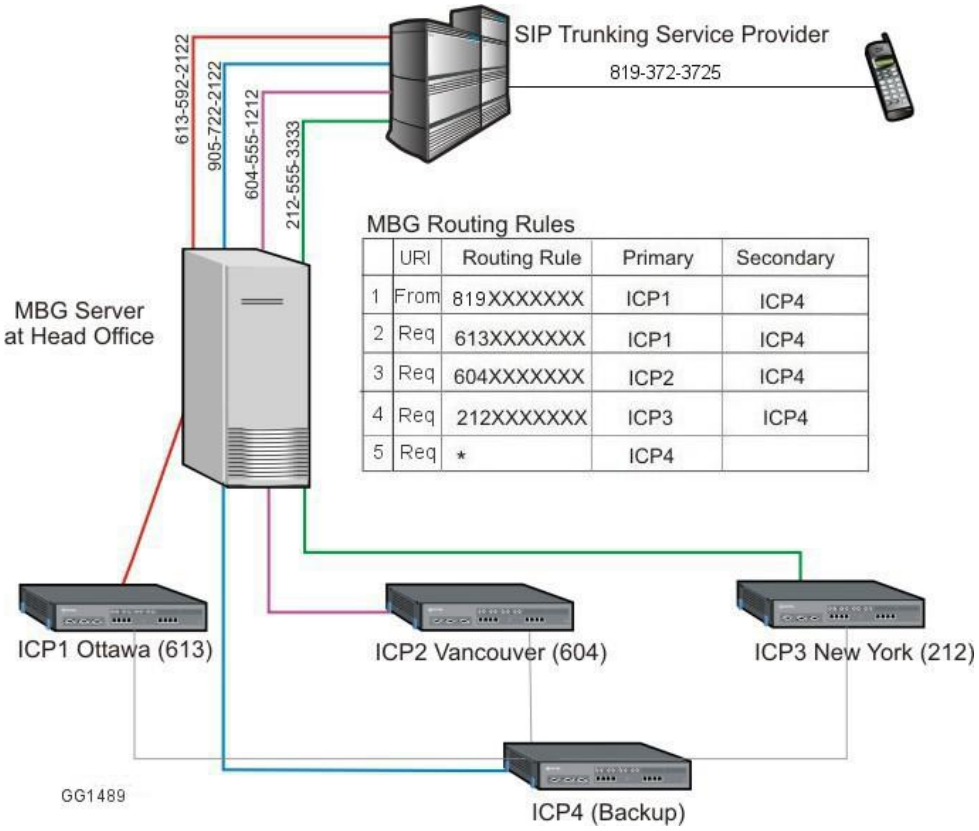
A central data center (CenData) has three geographically remote locations that each have one ICP.

CenData programs their MBG server to perform call routing based on the called number, caller number and original target number:

- **Called Number**: When a match is made on the called number contained in the "Request" header, the call is routed to the appropriate ICP. In this example, ICP1 in Ottawa handles calls destined for area code 613. ICP2 in Vancouver handles calls for 604, and ICP3 in New York handles calls for 212. Their trunk service provider, SipCo, provides the DID numbers.
- **Caller Number**: When a match is made on the caller's number contained in the "From" header, the call is routed accordingly. In this example, the service provider routes calls from mobile phones originating in area code 819 to ICP1. This is useful when the service provider wants to route customer calls though a PBX, enabling the customers to dial office extensions from their mobile phones. It can also be used to route callers based on

their anticipated language needs. For example, you create a rule that routes Puerto Rican callers to an ICP with Spanish-speaking call center agents.

- **Original Target Number**: When a match is made on the address-of-record contained in the "To" header, the call is routed accordingly. This enables you to direct calls based on the original called number, before call forwarding has been applied. For example, you have two data centers, A and B, where B is the backup for A and both data centers have their own DID number. If A goes offline, the service provider will reroute A's calls to B and modify the "Request" header so that it contains B's DID number and a different ICP. Provided that the service provider has left "To" header untouched, you can employ a routing rule to direct the call to its originally intended destination in data center A.



	URI	Routing Rule	Primary	Secondary
1	From	819XXXXXXX	ICP1	ICP4
2	Req	613XXXXXXX	ICP1	ICP4
3	Req	604XXXXXXX	ICP2	ICP4
4	Req	212XXXXXXX	ICP3	ICP4
5	Req	*	ICP4	

Figure 8. SIP Trunking Configuration Example with DID Routing Rules

Using MBG Routing Rule configuration, calls for SIP usernames that begin with 613 or from SIP usernames that begin with 819 are routed to ICP1 in Ottawa. Calls for SIP usernames that begin with 604 are routed to ICP2 in Vancouver, and calls for SIP usernames that begin with 212 are routed to ICP3 in New York. Calls that do not match any of the first four rules will use rule 5 which directs all non-matching calls to ICP4. There is no secondary ICP for this rule.

Adding a DID Routing Rule

You can add DID routing rules at the same time that you create a new SIP trunk, or you can add them to existing trunks.

To add a DID routing rule:

1. On the MBG main page, click the **Service Configuration** tab and then click **SIP trunking**.
2. Click the sign beside an existing trunk or click the + sign to add a new trunk.

3. In the lower section of the screen, locate the place where you wish to add the new rule. Use the following screen tools to sort through the list:
    - **Rules per page**: Specify the number of rules displayed on the page, from 10 to 1000.
    - **Jump to page**: If there are multiple pages of rules, select the page you wish to view.

Note: If the SIP Trunk does not yet have any rules, a single unprogrammed rule will be listed by default.

4. To add the new rule, click + beside an existing rule. A new rule will be added directly below the existing rule
5. Specify the rule parameters:
    - **Match**: Select the match criteria: Request URI, From header URI, or To header URI.
    - **Rule**: Enter the rule, making sure to adhere to the format outlined below.
    - **Primary**: Select the primary ICP to route the call.
    - **Secondary**: Select the secondary ICP to route the call (if applicable).
    - **Description**: Type a description of the rule (optional entry).
6. After you have specified the rule parameters, you can do the following:
    - To move the rule up the list, click ↑.
    - To move the rule down the list, click ↓.
7. Click **Save**.

Editing a DID Routing Rule

You can move a DID routing rule forward or backward in order to adjust its precedence in the list. You can also modify the rule parameters or delete it altogether.

To edit a DID routing rule:

1. On the MBG main page, click the **Service Configuration** tab and then click **SIP trunking**.
2. Click the ✎ sign beside an existing trunk.
3. In the **Routing rules** section of the screen, locate the rule you wish to edit. Use the following screen tools to sort through the list:
    - **Rules per page**: Specify the number of rules displayed on the page, from 10 to 1000.
    - **Jump to page**: If there are multiple pages of rules, select the page you wish to view.
4. After locating the rule you wish to edit, you can do the following:
    - To modify the rule parameters, select and change any of the following: **Match**, **Rule**, **Primary**, **Secondary**, **Description**.
    - To move the rule up the list, click ↑.
    - To move the rule down the list, click ↓.
    - To delete the rule, click 🗑.
5. Click **Save**.

DID Routing Rule Format

The routing rule format is a case-sensitive string of 0-9, +, -, _, *, N, or X characters. In effect, you are programming a "mask" to apply to the username in the SIP request to check for a match. If the SIP request is successfully matched with a routing rule, the call follows the corresponding ICP routing. SIP requests with unsuccessful matches continue through the list of rules until a match is found. If no rule matches, the call is rejected.

Pattern matching is exact. The rule and the dialed number must be the same length and each character in the dialed number must match the character in the rule. (For example, 6135925660" does not match "613 5925660" or "613-592-5660".) An "X" in the pattern will match any single character at that position in the dialed number. An "N" will match any single character at that position from 2-9.

Valid Characters for DID Routing Rules

- **X** refers to any character from 0 through 9
- **N** refers to any character from 2 through 9
- **+** refers to the literal "plus" character that may be used in European telephone numbers
- **-** a routing rule consisting of a single "-" character allows the selected ICPs to make outgoing trunk calls, but since this pattern will never match an actual call, no incoming calls will be routed to those ICPs. When used in conjunction with other digits to make a pattern, "-" refers to the literal "dash" character.
- _ refers to the literal underscore character
- ***** a routing rule consisting of a single "*" character allows any pattern to match.

Note: For effective pattern matching, make sure this type of rule is the final rule in your list, otherwise some patterns will never be checked. When used in conjunction with other digits to make a pattern, it refers to the literal "star" character.

Sample DID Routing Rules

- A routing rule of "613NXXXXXX" matches any 10-digit phone number that starts with "613". When a call is received with a DID number (or SIP username) that matches this pattern, it is sent to the ICP that is configured in this rule.
- A routing rule of "613592XXXX" narrows the matches to any 10-digit phone number that begins with "613592".
- A routing rule of "613-592-XXXX" matches any 10-digit number that begins with "613-592-".
- A routing rule of "*" matches any number.

REMOTE PROXY SERVICES

OVERVIEW

The Remote Proxy Services feature includes two components: the Web Proxy and Remote Management Services.

Web Proxy

The Web Proxy component acts as a reverse web proxy, providing a secure method for Mitel end user web clients to connect with their LAN-based applications. The proxy restricts access to URLs that belong to the administrative and user web interfaces for applications. Valid URLs for each application are listed on the Supported Applications tab.

The Web Proxy is licensed as part of the MBG base bundle. Upgrades from are covered under Software Assurance.

Remote Management Service

The Remote Management component enables you to set permissions for remote administrative users. The permissions define which MiVoice Business and MiCollab management web interfaces the administrators may access while restricting access to all other parts of the enterprise network.

When administrators attempt to log in, they are prompted to authenticate themselves with a username and password. If they fail to authenticate themselves correctly or they are not on the list of configured "Remote Management" users, they will be denied access.

Remote Proxy Services is not intended to be installed on MiCollab servers so it will not be visible for MiCollab installation.

When to Use the Web Proxy

The Web Proxy is meant to provide secure access for Internet-based clients to an Internet-protected server on the LAN. It is intended for deployment on a standalone MBG server in both server-only (DMZ) deployments and server-gateway (Network Edge) deployments. Check your application documentation to see which deployments are supported.

CONFIGURATIONS

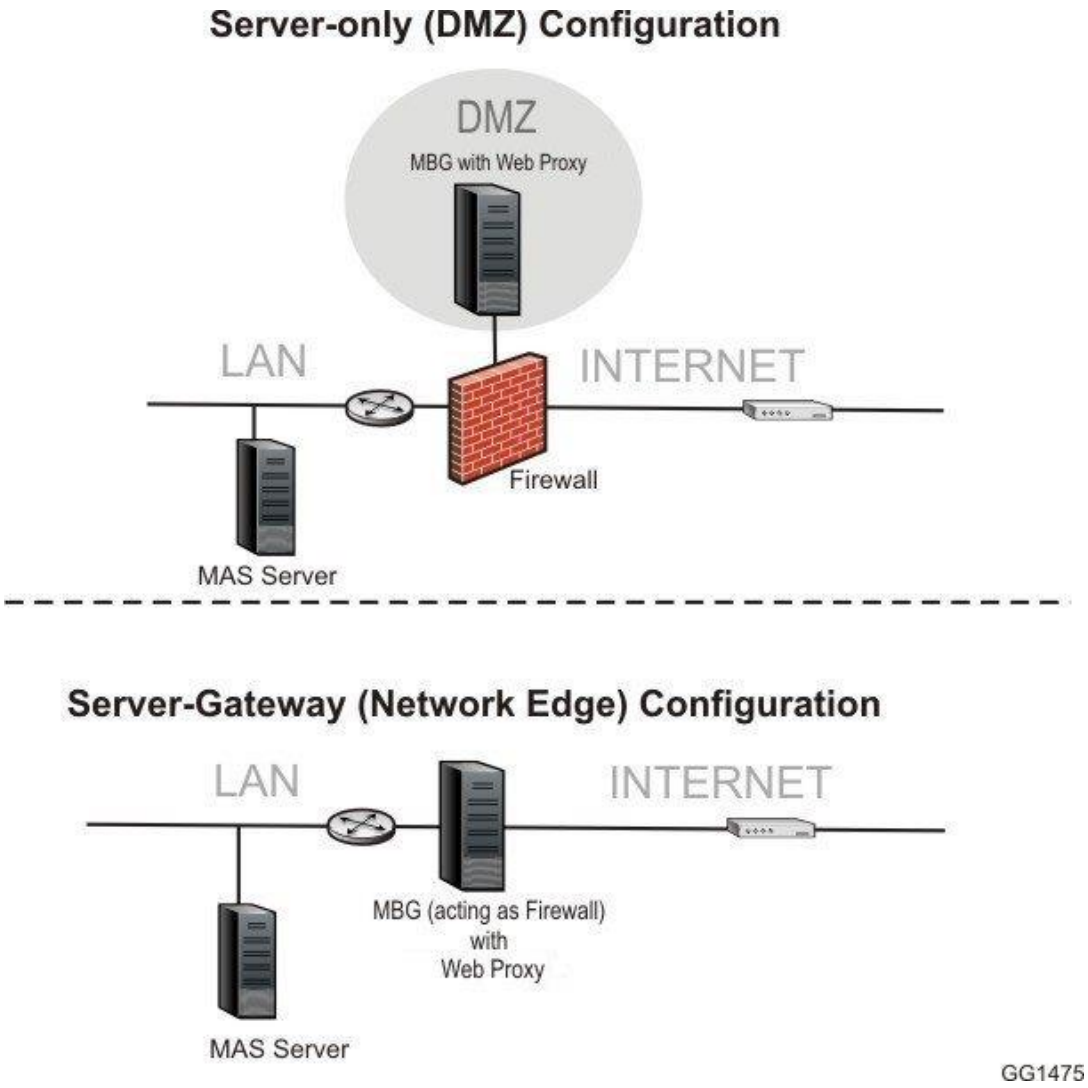


Figure 9. Configurations

BASIC OPERATION

This is an example of the operation of the Web Proxy component when configured in Server-only (DMZ) mode and a MiCollab Mobile Client requests login:

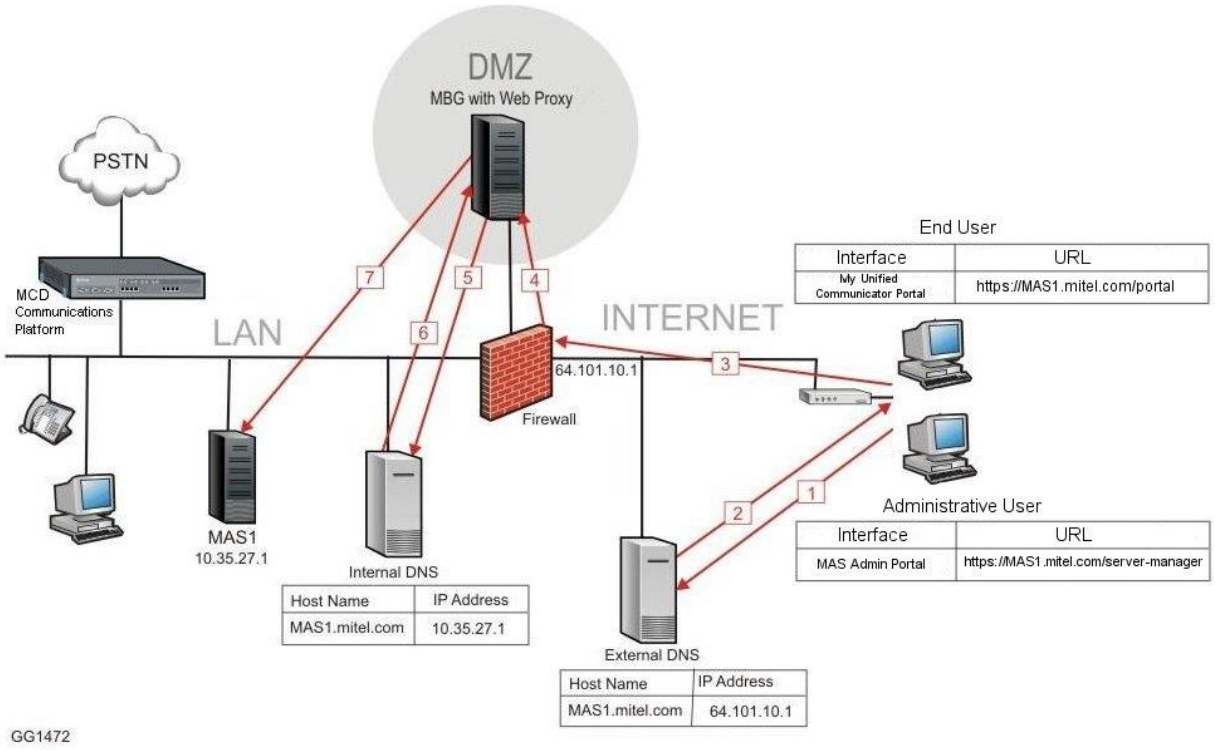


Figure 10. Basic Operation

Note: To be proxied successfully, remote users must enter a valid URL for the resource they are attempting to access. For example, to access Audio, Web and Video Conferencing, users must enter https://mca.mitel.com/awc/, not https://mca.mitel.com. A list of valid administrative and user-level URLs is provided on the Supported Application tab.

1. UC Mobile client requests DNS resolution for **MAS1.mitel.com**.
2. The external DNS server returns the IP address of the corporate firewall.
3. UC Mobile connects to the corporate firewall.
4. The corporate firewall routes the http request to the Web Proxy.
5. The Web Proxy requests resolution for **MAS1.mitel.com**.
6. The internal DNS server provides the IP address of the MAS1 server.
7. The Web Proxy completes the connection to the MAS1 server.
8. The Web Proxy proxies the request to the MAS1 server along with the full URL requested by the client (e.g. MAS1.mitel.com/awc/).

Note: In this example, you must program the IP address of the internal DNS server into the Corporate DNS Settings on the Domains page of the MBG server. If you do not plan to use a separate DNS server for internal name resolution, then you can program the IP address of the MiCollab server directly into the LAN Host FQDN or IP Address field of the Web Proxy interface.

Web Proxy supports the following:

- MiCollab Client Release 3.0
- MiCollab End User Portal
- Web View browser for standalone NuPoint Unified Messaging
- Multiple servers
- Server-gateway (Network Edge) configuration

BASIC CONFIGURATION OVERVIEW

Split DNS Setup

A split DNS setup is one where a single domain is split into two “zones” – an internal zone and an external zone. Internal hosts are sent to an internal DNS server for name resolution and external hosts are sent to an external DNS server. The same DNS query produces different results depending on the source of the request.

To enable the Remote Proxy to work properly, you need to configure the MSL server to resolve the FQDN to the internal address. There are two ways to do this:

1. In the MSL Server Manager, under **Configuration > Domains**, configure MSL as a Corporate DNS Server.
2. In the MSL Server Manager, under **Configuration > Domains**, configure MSL as an Internet DNS server and ensure that a DNS forwarding address is *not* configured. Under Configuration > Hostnames and Addresses, configure the FQDN and IP address of the internal DNS server.

Typically, larger implementations (such as MiCollab) use the first option while smaller implementations use the second option.

Multiple Account Setup

In addition to using split DNS to route traffic, you can configure your hosts with two different accounts. One account is used to connect directly to resources on the internal network while the other is used to connect to the public interface of your enterprise—either the firewall or the MBG in Server-Gateway in Network Edge mode).

Be aware that not all clients support multiple accounts. Typically, you will require an iOS or Android device equipped with a SIP softphone such as the MiCollab Mobile Client.

Example of Split DNS for the Remote Proxy

- External DNS must be programmed to resolve requests for MAS1.mitel.com to the **IP address of the corporate firewall** (IP3 in the following figure) or the IP address of the MBG server in Server-Gateway (Network Edge) mode.
- Internal DNS must be programmed to resolve requests for MAS1.mitel.com to the **IP address of the MiCollab server** on the LAN (IP1).

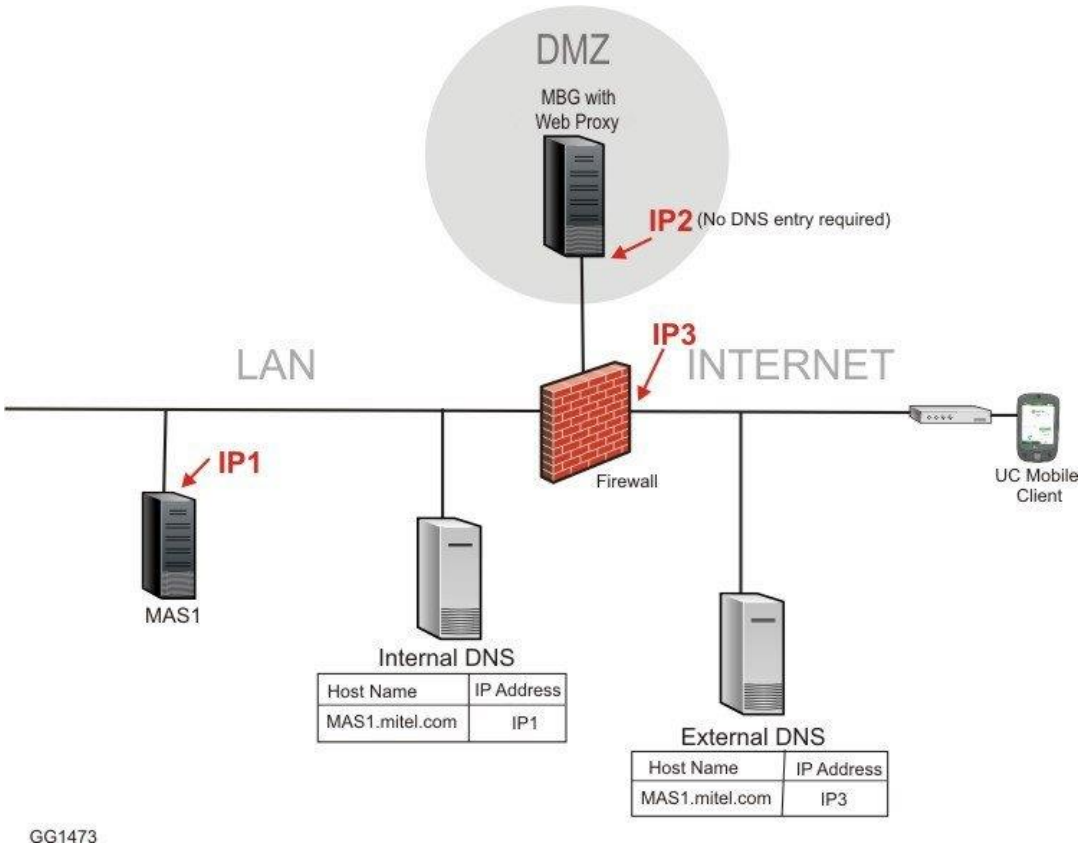


Figure 11. Basic DNS Configuration

Firewall

The corporate firewall must be configured to route client requests received at the firewall (IP3) to the HTTPS port on the Web Proxy (IP address IP2). AMC traffic must also be allowed between the Internet and both the MBG and the MiCollab servers for AMC communications. Audio, Web and Video Conferencing traffic also requires some additional firewall programming. Detailed firewall rules are described on page 52.

REQUIREMENTS FOR AUDIO, WEB AND VIDEO CONFERENCING

Note: When the Web Proxy is deployed in Server-Gateway (Network Edge) configuration, you do not need to configure an AWV (formerly MCA) listening port. When you provide a LAN IP address and two AWV IP addresses, then MSL automatically configures port setup.

The Audio, Web and Video Conferencing (AWV) application has different configuration requirements. A web client may be setting up the conference and inviting participants ("web traffic" request) or it may be joining a web conference, file-sharing session, or video conference ("web conference" request; also called "Collaboration" or "Connection Point"). Both of these requests are made on port 443. To separate the two request types, the firewall (or the MBG server in Server-gateway configuration) must be programmed with two IP addresses for AWV. Firewall rules are then programmed to forward web conference request traffic from the second IP to a programmed port on the Web Proxy (default 4443). The Web Proxy then forwards the traffic to port 4443 on the MiCollab server (IP1).

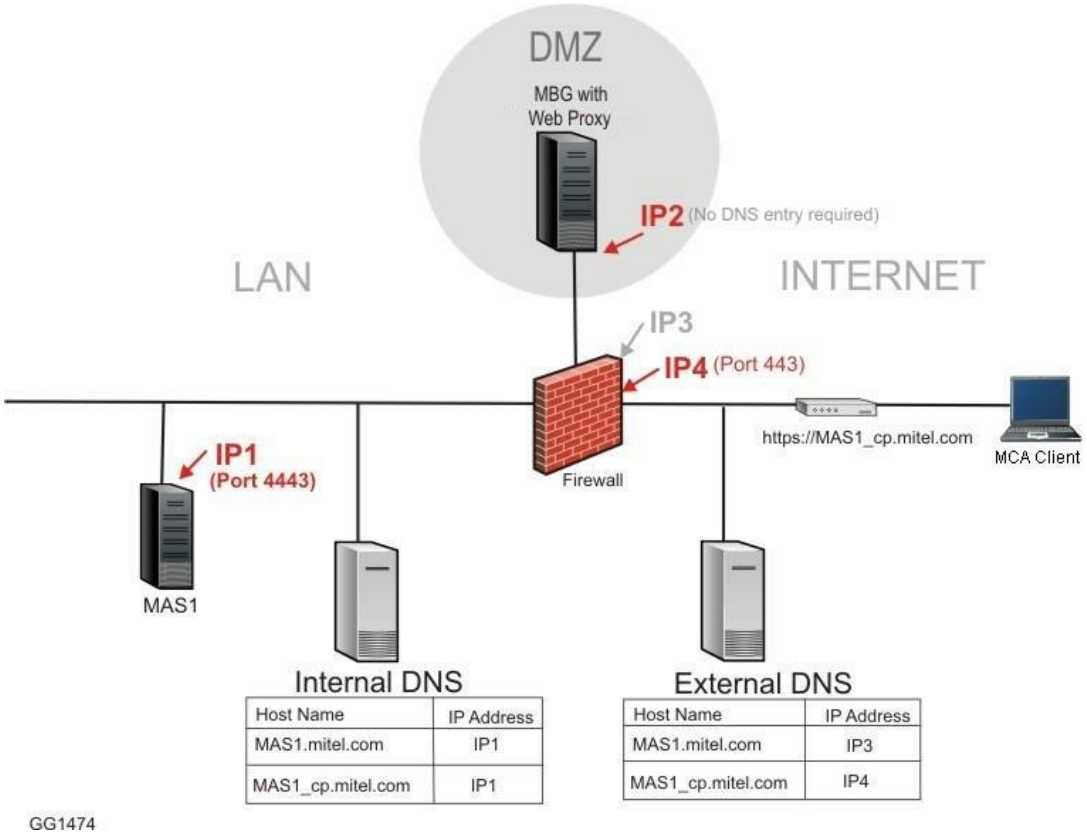


Figure 12. AWV Communications

DNS

In addition to the basic DNS configuration in the last section, external DNS must be programmed to resolve requests for AWV web conference traffic (MAS1_cp.mitel.com) to the second IP address on the corporate firewall (**IP4** in the preceding figure).

Message Flow for Web Traffic

When AWV users set up conferences and send e-mail notices, the message flow is as follows:

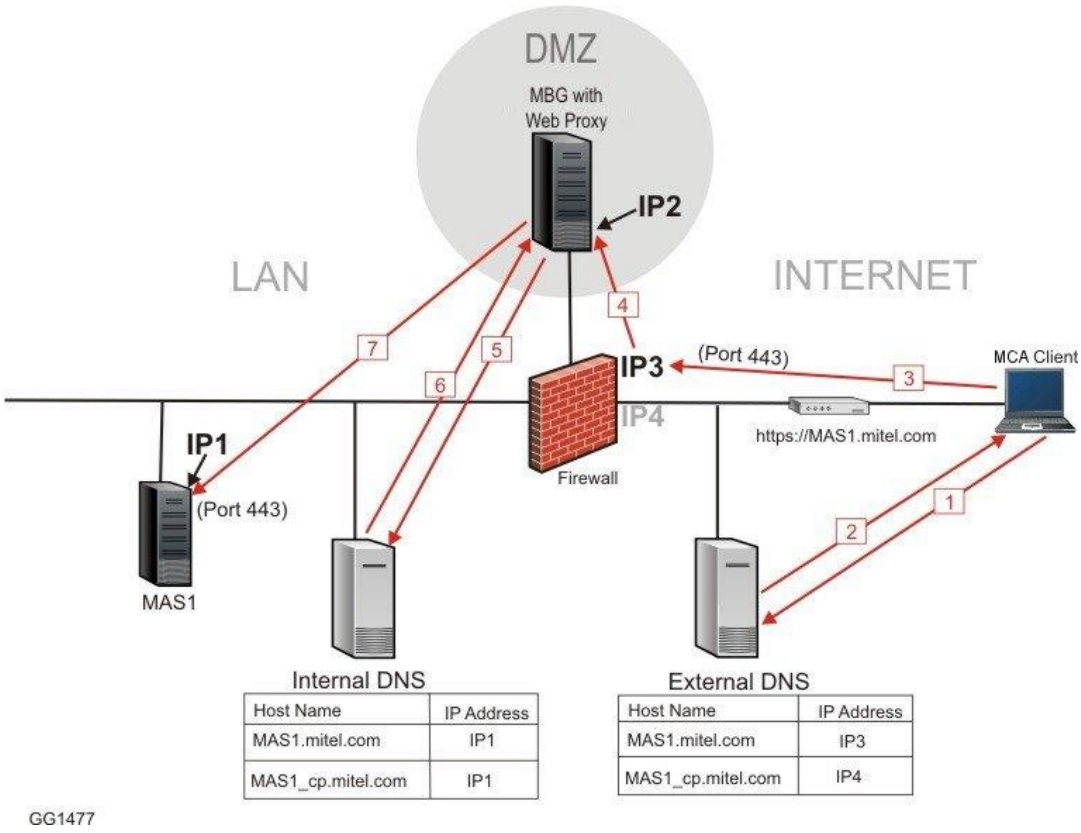


Figure 13. Message Flow for Web Traffic

1. AWV client requests DNS resolution for **MAS1.mitel.com**.
2. The external DNS server returns the IP address of the corporate firewall (IP3).
3. AWV client connects to IP3 on the corporate firewall.
4. The corporate firewall routes the http request to the Web Proxy.
5. The Web Proxy requests resolution for **MAS1.mitel.com**.
6. The internal DNS server provides the IP address of the MAS1 server.
7. The Web Proxy completes the connection to the MAS1 server, port 443.

Message Flow for Web Conferencing (Collaboration) Requests

When AWV conference members share files, desktop, or participate in video conferencing, the message flow is as follows:

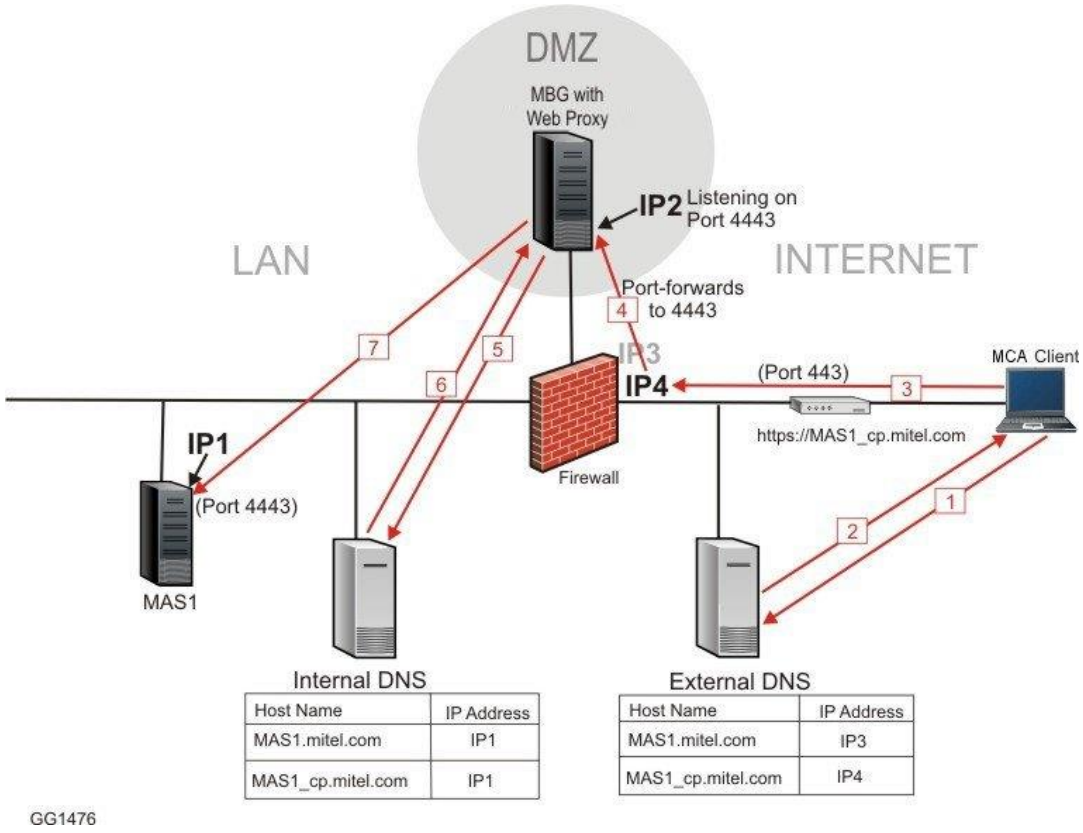


Figure 14. Message Flow for Web Conferencing Requests

1. AWV client requests DNS resolution for **MAS1_cp.mitel.com**.
2. The external DNS server returns the IP address of the corporate firewall (IP4).
3. AWV client connects to IP4 on the corporate firewall.
4. The corporate firewall is programmed to route the http request to the Web Proxy port 4443.
5. Web Proxy, listening on port 4443, sends a request to the internal DNS server to resolve **MAS1_cp.mitel.com**.
6. The internal DNS server provides the IP address of MAS1 server, port 4443.
7. The Web Proxy completes the connection to the MAS1 server, port 4443.

Firewall

The corporate firewall must be configured to forward client requests for Connection Point (also called Web Conferencing or Collaboration) traffic (MAS1_cp.mitel.com) to a port on the Web Proxy (**IP2**) that is programmed to listen for Connection Point traffic (default is 4443) and forward it to Port 4443 on the MAS1 server (**IP1**).

Note: When Web Proxy is deployed in server-gateway (network edge) configuration, MSL automatically configures port settings.

The direction of the arrow indicates permission to initiate new traffic in that direction. These rules assume a stateful firewall that will permit return traffic on an existing established connection.

Program the following firewall rules:

PORT RANGE	DIRECTION	DETAILS
TCP 22 (SSH)	MBG Server → Internet MiCollab Server → Internet	Allow outbound packets (and replies) on TCP port 22 between the MBG Server and the Internet to enable AMC communications.
UDP 53 (DNS)	MBG Server → Internet MBG Server←→ LAN	The server requires DNS to look up the IP address of the Mitel AMC and to the LAN to look up LAN server names. Alternatively, the server can be configured to forward all DNS requests to another DNS server. See the *MSL Installation and Administration Guide* for details.
TCP 443 (HTTPS)	MBG Server ← Internet (IP address IP3) and MBG Server→ LAN	Allow inbound and outbound packets on TCP port 443 between the MBG server and the Internet for AWV web pages (SSL mode). Allow inbound and outbound packets on TCP port 443 between the MBG server and the LAN for AWV web pages.
TCP 4443	MBG Server ← Internet (IP address IP4) and MBG Server→ LAN	Allow inbound packets on TCP port 443 and forward them to port 4443 on the MBG server as well as return traffic. Allow inbound packets on TCP port 4443 between the MBG server and the LAN. Used for ConnectionPoint traffic for external users of Web conferencing.

Note: Since the Proxy obscures the actual originator of all network traffic it handles, responses will be sent back to it, by the same routes (unless the customer's network configuration specifically redirects it). As such, as long as the firewall permits the traffic to be bi-directional, no additional rules should be required to permit that response traffic.

Configure LAN Servers on the Web Proxy

The Web Proxy component of remote proxy services provides a secure interface between applications on the LAN and clients on the Internet. Some examples of clients are the Mobile Client feature of MiCollab Mobile Client, and the web collaboration client of Audio, Web and Video Conferencing.

Use the following procedure to add the WAN-side host name of the LAN server you wish to proxy and configure access to its client and administrative interfaces.

The instructions assume that an external DNS server resolves your WAN-side host name (for example, "MAS1.mitel.com") to the corporate firewall which, in turn, sends HTTP requests to the Web Proxy server. It is also assumed that MSL is configured to use an internal DNS server which resolves the LAN-side host name (also "MAS1.mitel.com") to the actual server on the LAN.

Notes:

- Select the Supported Applications tab to review the requirements to access various applications, including the correct format for administrative and end-user URLs.
- Effective MBG Release 7.1, the Web Proxy is included as a component of Remote Proxy Services and is licensed as part of the MBG base bundle. Upgrades from are covered under Software Assurance.
- The Web Proxy relies on the fully qualified domain name in the HTTP request to map that request to the appropriate LAN server. Access via IP address is not supported.
- If your implementation includes the Mitel Oria system management application, you can provide access to it by selecting "MiVoice Business" as the type of LAN server to be proxied.

To add a LAN server to the Web Proxy:

1. In the server manager, under Applications, click **Remote proxy services**.
2. On the Domain list tab, click **Add new LAN server proxy**.
3. Select **Enabled**.
4. In the **WAN-side FQDN** field, enter the name of the server to which you want to proxy. This is the name that external users will enter in their web browsers to access the LAN host (for example, "MAS1.mitel.com").

Note: The LAN-side host name defaults to the WAN-side FQDN.

5. Select the LAN server and user interface:

LAN SERVER	USER INTERFACE
MiCollab server	• **MiCollab**: Select to forward MiCollab client traffic to the web-based communications portal on the MiCollab server (which will be the WAN-side FQDN). **Note**: This selection includes the required URLs for NuPoint on MiCollab. • **MiCollab Client**: Select to forward MiCollab Client traffic

	(web portal or mobile portal) to the MiCollab server. • **MiCollab NuPoint Unified Messaging**: Select to forward NuPoint client traffic (web view or system admin view) to the MiCollab server. • **MiCollab Audio, Web and Video Conferencing**: Select to forward MiCollab Mobile Client client traffic to the MiCollab server. **Note**: Ensure that the Use HTTPS Only setting is enabled in System Options configuration. Refer to the Configuring Web Conferencing Settings section of the *Audio, Web and Video Conferencing Configuration and Maintenance Manual* for full instructions. • **Google Calendar Integration to AWV**: Select to forward Google Apps traffic (i.e. traffic that includes "google" as part of the FQDN in HTTPS requests) to the MiCollab server. • **Listen port for MiCollab AWV**: If you enable the AWV user interface on the MiCollab server, we recommend that you enter the default AWV port of 4443. This is the port that the Web Proxy listens on for Connection Point (or "Collaboration") traffic. Note that if your MSL network configuration is deployed in Network-Edge mode (server-gateway mode), the AWV listen port entry is not required.
MiVoice Business	This setting provides access to MiVoice Business System Administration Tool interface. **Note**: This setting can also be used to provide access to the Oria system management and customer self-service application.
MiCollab Client	**MiCollab Client**: Select to forward Audio, Web and Video Conferencing (AWV) client traffic to the MiCollab Client server (WAN-side FQDN). **Note**: This setting is for access on standalone MiCollab Client only. Access for the MiCollab version of MiCollab Client is supplied in the MiCollab web-based communications portal.
MiCollab NuPoint Unified Messaging	Select to forward NuPoint UM client traffic (web view) to the NuPoint UM server (WAN-side FQDN). **Note**: This setting is for access on standalone NuPoint UM only. Access for the MiCollab version of NuPoint UM is supplied in the MiCollab web-based communications portal.
generic MSL admin only	Provides access to the MSL interfaces.
Open Integration Gateway	Select to forward Mitel OIG application web service requests (https: only) to the Mitel OIG server within the enterprise network. The WAN-side FQDN for the OIG server used for the remote Mitel OIG application must match the LAN-side FQDN for the Mitel OIG server within the enterprise network.
Oria	This setting provides access to the Mitel Oria system management and customer self-service application.
MiContact CenterOria	This setting provides access to the Mitel MiContact Center application.
MiVoice Call Recording	This setting provides access to the Mitel MiVoice Call Recording application

Note: Only administrative access is available for the MiVoice Business server and the MSL server.

6. To enable administrative access to the LAN server, select **Yes** in the **Do you wish to permit remote administrative access?** field.
7. To restrict access to one or more specific network addresses (that is, to allow only these addresses to access the Web Proxy), select Some from the drop down, click add netblock and then enter an address in the **Network Address** field. Click add netblock again to enter another address.
8. Click **Save**.

To modify or disable an existing proxy:

1. In the server manager, under Applications, click **Remote Proxy Services**.
2. On the LAN server proxy list tab, click **Modify**.
3. Make the required changes (or clear the Enabled check box to disable the proxy) and then click **Save**.

To delete an existing proxy:

1. In the server manager, under Applications, click **Remote Proxy Services**.
2. On the LAN server proxy list tab, click **Delete**.
3. Click **OK**.

Configure Users for Remote Management

The Remote Management component of remote proxy services enables you to set permissions for remote users. The permissions define which MiVoice Business and MiCollab web management interfaces the users may access.

For example, to grant access to the administrative interface of the MiVoice Business, add a new user and select the "MiVoice Business Management - Administration" permission. When users attempt to access the System Administration Tool on the MiVoice Business, they will be prompted to enter their Remote Management username and password in a web-based dialog. MBG will then forward them to the MiVoice Business interface, where they will be prompted to enter their application-level username and password.

Some application services are not supported by the Remote Management component. Details are provided in the following table:

APPLICATION	INTERFACE	REMOTE MANAGEMENT LIMITATIONS	NOTES
MiVoice Business	System Administration Tool	• Cannot perform FTP backups or restores from the MiVoice Business System Administration Tool interface. • Cannot perform MiVoice Business upgrades. • Cannot use System Administration Tool Reach Through to access another MiVoice Business. • Cannot import files.	• Local backups to the client PC are supported. • The MiVoice Business System Administration Tool should be used to perform the following tasks: - basic form updates (add users, change COS, etc.) - enter maintenance commands - download logs
MiCollab	Server Manager	• Cannot perform upgrades. • Cannot access the MiVoice Business System	• Application support is limited to the following: - Users and Services

Administration Tool for a network element (ICP).
- Application support is provided as a technology preview only. See Notes for a list of supported applications.

- Audio, Web and Video Conferencing
- MiVoice Border Gateway
- NuPoint UM
- UC Mobile
- MiCollab Client Service
- Licensing Information

Notes:
- In the current release, you can set permissions to control administrative-level access to the MiCollab Server Manager and the MiVoice Business System Administration Tool. In future releases, it will be possible to set permissions to control administrative- and user-level access to the complete range of Mitel applications.
- To ensure the administrative interfaces display correctly when accessed from a remote location, use a supported browser. For the MiVoice Business System Administration Tool, use Internet Explorer 6.0 and higher; for the MSL Server Manager, use Internet Explorer 7.0 and higher.
- To enable use of the Remote Management component of Remote Proxy Service, the application must be installed on Mitel Standard Linux Release 9.4 or higher.

To add a user to the Remote Management list:

1. In the server manager, under Applications, click **Remote Proxy Services**.
2. On the Users list tab, click **Add new user**.
3. Select **Active**.
4. In the **Username** field, enter the username used for authentication when accessing the application interface.
5. In the **Password** field, enter the user's password used for authentication when accessing the application interface.
6. In the **Confirm Password** field, re-type the user's password.
7. In the **First Name** field, type the user's first name.
8. In the **Last Name** field, type the user's last name.
9. In the **Email address** field, type the user's e-mail address.
10. In the **Add permission** list, select the application interfaces you want this user to access, and then click **Add**. Use Shift+Click and Ctrl+Click to select multiple applications.

Note: In this release, select permissions only for the "Admin interfaces". In a future release, it will be possible to select "User interfaces".

11. To automatically activate the user at a later date and time, enter the **Deferred activation Date** and **Time** in military format.
12. To automatically de-activate the user at a later date and time, enter the **Expiry Date** and **Time** in military format.
13. Click **Save**.

WEB PROXY WITH MULTIPLE LAN SERVERS

The Web Proxy can handle traffic to multiple LAN servers.

The following figure shows a setup with two LAN servers. MAS1 runs the AWV application and MAS2 runs the UC Mobile application. Both applications require communication from external end user web clients. In our example, an AWV client is making a ConnectionPoint request to MAS1_cp.mitel.com. The request is directed to Port 443 at IP4 on the firewall. The firewall is programmed to forward these communications to a programmed port on the Web Proxy (in this example, we have left the "AWV Port" setting at the default of 4443). The Web Proxy then forwards the ConnectionPoint traffic to Port 4443 at IP1 (the MAS1 server).

Requests for web pages (to either server) are processed through IP3 and the Web Proxy determines the recipient using the hostname supplied in the request header.

Note: If both servers were running the AWV application, then the Web Proxy would be programmed to listen for each server's ConnectionPoint traffic on a different port. Also, AWV ConnectionPoint traffic to the second server would require a third IP address on the firewall. Note that this scenario is not possible in Server-gateway (Network Edge) mode as MSL allows only one additional WAN IP address.

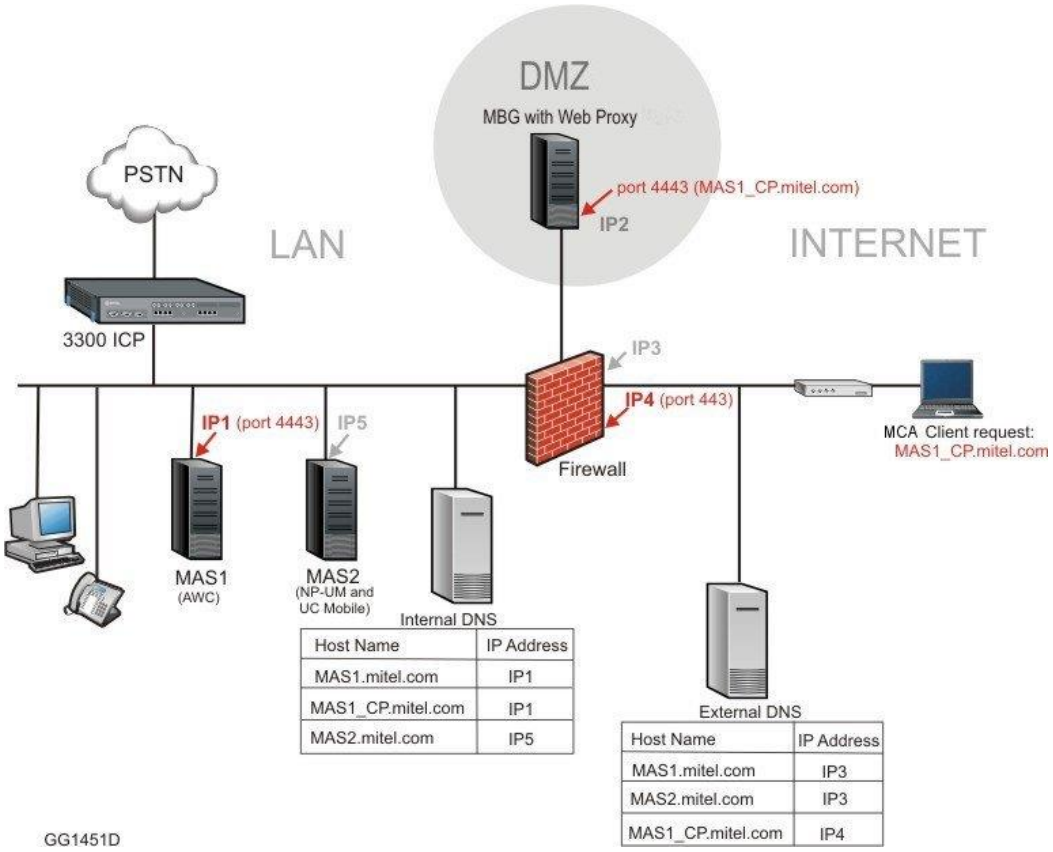


Figure 15. Multiple LAN Servers

SECURITY CERTIFICATE NOT TRUSTED

If your web clients receive a message saying that your site's security certificate is "not trusted" or is "certified by an unknown authority", it means that their browsers are trying to verify the authenticity of the host certificate presented by the Web Proxy server by looking for a digital signature from a trusted Certificate Authority (CA). Each MSL server automatically creates a self-signed certificate (that is, not verified by a CA) which does not appear as a "trusted" site.

To avoid these security warnings, you have a choice of actions:

- You can view/examine the self-signed certificate and accept it as the authentic MSL certificate. Follow the instructions in your web browser.

  OR

- You can purchase a certificate from a trusted third-party Certificate Authority (CA), like VeriSign. Steps to obtain a certificate include:
  - Generate a Certificate Signing Request (CSR) on the Web Proxy server
  - Include the alternate names for each LAN server to be proxied (each virtual host). Check the CA web site for instructions.
  - Submit your request to the CA.

See the Mitel Standard Linux Installation and Administration Guide for detailed instructions.

SECURE RECORDING CONNECTOR SERVICE

The Secure Recording Connector (SRC) service of MBG facilitates the recording of Mitel encrypted voice streams by third-party call recording equipment (CRE). Two configurations are supported, “direct call recording” and “indirect call recording”.

Direct Call Recording

The MiCollab or MBG server is positioned on the LAN between the ICP (typically a MiVoice Business) and the devices to be recorded. The SRC accepts requests from properly authorized Call Recording Equipment (CRE) to establish taps in the voice stream of local devices. These taps are separate (mirrored) streams from the SRC service to the call recording equipment. Both voice and signaling streams pass through the SRC.

Indirect Call Recording

With indirect call recording, the MiCollab or MBG server acts as a “broker” between the Mitel equipment and third-party CREs for adding and removing taps on the remote devices. Instead of being connected to the MBG/SRC, the remote devices are registered directly to ICPs located in branch offices. The ICPs send copies of the signaling to the MBG/SRC while the remote devices send copies of the RTP media streams to the CREs.

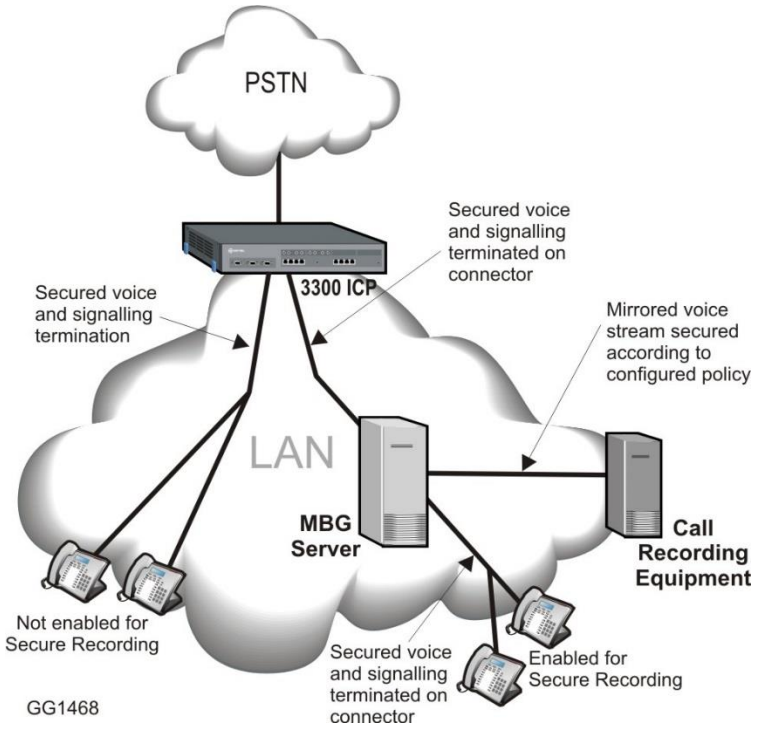


Figure 16. MBG Server with SRC Service (Direct Call Recording)

Notes:

- The SRC service is not limited to recording the prime DN of the telephone; however, the configuration/programming of the CRE may introduce this restriction.
- MBG servers with SRC service can be clustered to provide resiliency, load balancing, and scalability. For information about resilient SRC service, see the Clustering section.
- Indirect call recording is supported on 5300-series and the 6900-series IP Phones using the MiNet protocol, MiVoice Business ICPs with MiVoice Business release 5.0 SP1 or later, and a range of Call Recording Equipment (CRE).
- If your deployment includes a variety of set types, you can implement Indirect Call Recording for the 5300-series sets and the 6900-series sets and Direct Call Recording for all other sets.
- An SRC license is required for each recorded call. So if you anticipate the need to record 20 calls simultaneously, you must purchase at least 20 SRC licenses. In most circumstances, you will not require an SRC license for every set.

REQUIREMENTS

This section contains software/hardware requirements necessary to support the Secure Recording Connector service.

Phones/Devices

For a complete list of devices that are supported by the secure recording connector service of MBG, please refer to the *MBG Remote Phone Configuration Guide* available at Mitel OnLine.

Firewall

The direction of the arrow indicates permission to initiate new traffic in that direction. These rules assume a stateful firewall that will permit return traffic on an existing established connection.

The following connections must be configured:

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 22 (SSH)	Server ←→ Internet	**AMC communications**. Allow outbound packets (and replies) on TCP port 22 between MSL and the Internet to enable server registration, software and license key downloads, alerts and reporting.
UDP 53	Server ←→ Network	**DNS**. Configure MSL DNS to work within network OR Configure a DNS forwarder to your internal DNS server, which needs to resolve sub-domains of mitel_amc.com
TCP 6810	LAN → Server	**Call Recording Support**. To enable a third-party call recording equipment (CRE) server to connect to the SRC control interface on MBG, this port must be enabled.
TCP 6815	Server → ICPs	**Indirect Call Recording support (Optional)**. To enable MBG to connect to the Indirect Call Recording connector on MiVoice Business systems which support it.
UDP 35000 to 36999	LAN → Server	**Voice Recording**. For streaming voice streams from the MBG server to the CRE for recording purposes.

DHCP for Direct Call Recording

DHCP setups vary according to the percentage of total sets that you want to record.

TO RECORD…	YOU CAN USE THIS DHCP SETUP…
A small percentage of total sets	Configure the phones manually as teleworker phones and enter the IP address of the SRC server when prompted for the “Teleworker Gateway IP” address. For more information about configuring phones manually, refer to the *Multi-Protocol Border Gateway Remote Phone Configuration Guide* available at Mitel OnLine.
All sets	Configure the DHCP server in your ICP (such as a MiVoice Business) to supply the IP address of the SRC server to the phones as their ICP and TFTP addresses. OR Enable the pre-configured DHCP server supplied with the MSL server.
A large percentage of total sets	A possible setup for this scenario is to deploy the recorded group on a different subnet from the non-recorded phones. You can use an ICP (such as a MiVoice Business) as the DHCP server for the non-recorded phones and the MSL server as the DHCP server for the recorded phones subnet. Recorded phones will then receive the IP address of the SRC server as their TFTP server and Call Controller (ICP) addresses.

For more information about configuring DHCP in the MSL server, refer to the *Mitel Standard Linux Installation and Administration Guide*.

CONFIGURATION

For SRC configuration instructions, click **Help** in the upper right corner of the MBG interface. For installation and configuration of Call Recording Equipment, refer to the documentation supplied by the CRE manufacturer.

ENROLLING THE CALL RECORDING EQUIPMENT

Both the SRC application and the CRE equipment require a one-time enrollment to establish proper trust relationships. After the SRC service has been started, but **before** the CRE is installed, the administrator must complete the blade enrollment by approving the certificate request using the instructions provided in Handling Certificate Requests.

After the CRE has been installed, the administrator must again complete its enrollment by approving the request from the CRE using the same instructions.

In this way, both the SRC and the CRE have certificates signed by the same Certificate Authority.

HANDLING CERTIFICATE REQUESTS

1. Access the server manager.
2. Under **Security**, click **Certificate Management**. Certificate requests waiting for approval appear under the heading Queued CSRs.
3. Click the Certificate ID link.
4. After confirming the identity of the requester, do one of the following:
   - Click **Approve** to approve the CSR and allow the requester to establish taps.
   - Click **Reject** to remove the CSR from the list. (**Note**: If you reject the request, the requester must regenerate it.)
   - Click **Cancel** to return to the Certificate Management main screen without approving/rejecting the request.

Notes:

- It can take up to two minutes for certificate approval to appear. To refresh the view, under Security, click **Certificate Management** again.
- Most errors that occur during approval are due to duplicate certificate IDs. Check the **Certificate Management** panel for duplicates. If the duplicate existing certificate is not correct, revoke it and repeat your certificate request.

For more information about Certificate Management, see the *Mitel Standard Linux Installation and Administration Guide* available at Mitel OnLine.

WEB REAL-TIME COMMUNICATION (WEBRTC)

WebRTC is an API definition drafted by the World Wide Web Consortium (W3C) that provides browsers and mobile applications with Real-Time Communications (RTC) capabilities.

MBG supports WebRTC for browser-based voice and video calling without the need of plug-ins using Google Chrome, Mozilla Firefox and Opera.

The WebRTC solution consists of the WebRTC gateway, hosted on MBG, and a web-based client application developed with the WebRTC SDK. The SDK is a toolkit which you can use to add communication components to enterprise web pages or applications.

Please refer to MiCollab for a ready-to-use WebRTC-based subscriber mode UC solution that works with MBG.

SECURITY

WebRTC provides secure calling using industry-standard HTTPS and DTLS-SRTP. A standard TLS certificate from a CA that the user's browser trusts is used to authenticate the server. Media is encrypted between the client and gateway.

WebRTC requires clients to use a FQDN to reach the MBG server. URLs containing IP addresses cannot be used. This FQDN must resolve to the set side of MBG – usually the IP reachable from the WAN. The FQDN must appear in the TLS certificate that is installed on the MBG, and the certificate must be signed by a CA that browsers trust.

Firewall

WebRTC requires several port ranges to be opened in your firewall. Refer to the *MiVoice Border Gateway Engineering Guidelines*, section 7.3 *Firewall Configuration for WebRTC Gateway* for details.

WEBRTC USAGE SCENARIOS

Two usage scenarios are available, for "anonymous" and "subscriber" calls. It is possible to use both modes at the same time and for multiple applications to use the same WebRTC gateway. Sample applications are provided on MBG at the URLs /webrtc (subscriber mode) and /webrtc/call.php (anonymous mode). Using the SDK provided, you may embed WebRTC functionality (e.g. click to call) in your own web sites or applications.

Anonymous Calls

In this scenario, an external user initiates a call to the enterprise by clicking a button on a web site and then providing minimal credentials (name and CAPTCHA1 entry). The user, who is known as an "anonymous caller," is directed to an internal service such as a sales or product support hotline. The administrator, not the anonymous caller, specifies the number for the internal service as part of the WebRTC and website configuration.

Once the call is established, an anonymous caller can do the following:

- Mute audio/video
- Toggle a keypad to send DTMF
- Hang up
- Enlarge the video to full screen
- Toggle the self-view
- Anonymous calls can be initiated from the built-in demo portal or from an enterprise website that uses the WebRTC SDK provided with MBG.

Subscriber Calls

In this scenario, an external user logs in to MBG from a browser and then registers with the ICP. The user, who is known as a "subscriber," can perform a variety of tasks, including both placing and receiving calls, while registered. The subscriber, not the administrator, specifies the number of the called party.

To initiate registration, the user logs in with the MiCollab Web Client by entering his or her MiCollab username and password. The MiCollab client then automatically registers to MBG using the right SIP credentials.

Once registered, a subscriber can do the following:

- Mute audio/video
- Toggle a keypad to send DTMF
- Make a call
- Receive a call
- Hang up
- Dial or search in the directory
- Call voicemail (using a specific button)
- Access the company directory from an LDAP database (if configured)
- Feature availability varies by platform and client. For information on MiCollab Client capabilities, see the MiCollab documentation.

ICP Support

Restrictions apply depending on which call mode and ICP you wish to use. These are outlined in the following table:

SUPPORTED CALL MODES	SUPPORTED ICPS
Anonymous	• MiVoice Business • MiVoice 5000
Subscriber	• All (Using MiCollab Web Client)

WebRTC Configuration

To implement the WebRTC application, complete the following steps:

1. **Configure ICP for WebRTC**.
   You must configure a SIP trunk to support anonymous calls. Configuration differs

depending on which ICP you are using, the MiVoice Business or MiVoice 5000.

Note: This step is not needed if you are using only subscriber mode.

2. **Configure MBG for WebRTC**.
   Complete this step for all implementations. As part of this configuration, you must specify whether you intend to host the WebRTC client on a standalone web server or on MBG itself.
3. **Configure Web Server for WebRTC**.
   Complete this step if you are hosting WebRTC client on a standalone web server. It involves downloading the Software Development Kit (SDK) from the WebRTC on MBG, unzipping the SDK to obtain Javascript libraries and PHP templates, and then uploading some or all of these files to your web server.

Note: This step is required only if you are developing your own WebRTC application using the SDK.

ICP CONFIGURATION

Configuring the MiVoice Business to Support SIP Trunks

To enable the ICP to receive WebRTC Anonymous calls, a SIP trunk must be configured between MBG and the call controller.

Configuring the MiVoice Business (3300 Controller) to Support SIP Trunks

Note: The following instructions describe how to set up a SIP trunk without security. Instructions that include the use of SSL certificates will be added in a later release.

To configure a MiVoice Business to support SIP trunking:

1. In the MiVoice Business System Administration Tool, click **View by Category**.
2. Add licenses:
   a. Access the License and Options Selection form.
   b. Under **Trunking Networking**, enter the number of SIP Trunk licenses for your implementation. This is the maximum number of concurrent trunk sessions that can be configured.
3. Configure the network element:
   a. Access the **Network Elements** form and add a new entry.
   b. Configure the following fields:
   - **Name**—Enter a unique name of up to nine characters for the network element (eg. WebRTC). Record the name; you will require it in step 5, below
   - **Type**—Select **Other**.
   - **FQDN or IP Address**—Enter the LAN IP address of MBG, provided that MBG is operating in Server-Gateway mode.
   - **SIP Peer**—Select this check box.
   - SIP Peer Transport—Select UDP.

- SIP Peer Port—Enter 5064.
- SIP Peer Status—Select Always Active.

c. Click **Save**.

4. Configure the SIP trunk attributes:

   a. Access the **Trunk Attributes** form and select a trunk service number that is available to be changed.

   b. Configure the following fields:

   - **Non-Dial-In Trunks Answer Point – Day**—Enter the destination number (answer point) to which incoming WebRTC trunk calls are routed during the Day service. This can be a station, hunt group pilot number, DISA number, or System Speed call number on the ICP.
   - **Non-Dial-In Trunks Answer Point - Night 1**—Enter the same value as specified above.
   - **Non-Dial-In Trunks Answer Point - Night 2**—Enter the same value as specified above.
   - **Trunk Label**—(Optional) Enter the character string to identify the trunk.

   c. Click **Save**.

   d. Record the **Trunk Service Number** that you have modified. You will require it in the next step.

5. Configure the SIP peer profile:

   a. Access the **SIP Peer Profile** form and add a new entry.

   b. Configure the following fields:

   - **SIP Peer Profile Label**—Enter the name of the network element (eg. WebRTC).
   - **Network Element**—Select the network element that you created for the MBG
   - Address Type—Select IP Address.
   - **Trunk Service**—Enter the **SIP Trunk Service Number** that you modified in the previous step.

   c. Click **Save**.

   d. Record the **SIP Peer Profile Label**. You will require it in the next step.

6. Configure the SIP Peer Profile Assignment by Incoming DID:

   a. Access the SIP Peer Profile Assignment by Incoming DID form and add a new entry.

   b. Configure the following fields:

   - **Incoming DID Range**—Enter the destination number (answer point) to which incoming WebRTC trunk calls are routed on the ICP.
   - **SIP Peer Profile Label**—Select the **SIP Peer Profile Label** that you added in the previous step.

   c. Click **Save**.

Configuring the MiVoice 5000 to Support SIP Trunks

To configure a MiVoice 5000 to support SIP trunking, refer to the "Characteristics of a VoIP trunk group" procedure in the Mitel 5000 Gateways and MiVoice 5000 Server Operating Manual.

MBG CONFIGURATION

Complete the following procedures to enable MBG to support WebRTC.

Configure WebRTC Settings

To configure WebRTC settings on MBG:

Note: These values are included in the SDK. If you are implementing WebRTC features on your own site with the SDK, program these values before you download it.

1. On the MBG main page, click the **Service configuration** tab and then click **WebRTC**.
2. Enter or edit the options as required and then click **Save**:

FIELD	DESCRIPTION
Hosting Mode	This setting controls whether the sample WebRTC applications are available on MBG. Selecting **Host WebRTC client locally** enables the URLs /webrtc and /webrtc/call.php on MBG, and selecting **Host WebRTC on a separate server** disables those URLs. Both modes allow external WebRTC applications to be used, but only "Host locally" allows the built-in application to be used. For use as part of the MiCollab solution, select **Host WebRTC on a separate server** to disable the built-in demo applications. In this context, MiCollab Web Client, running on the MiCollab server, is considered a "separate server". This is true even when MBG is embedded with MiCollab. If you will be using the demo applications for subscriber (MiVoice 5000 only) or anonymous (all supported platforms) calling, select **Host WebRTC client locally**. If you will be hosting a WebRTC application off-board from MBG, such as embedded in your web site, select **Host WebRTC on a separate server**. If you select **Host WebRTC client locally**, configuration is complete when you save the WebRTC settings. Users may then initiate a call by entering the following addresses in a web browser: • **Anonymous call mode** https://<MBG-FQDN>/webrtc/call.php?to=<CalledNumber | SipUri> • **Subscriber call mode** (**MiV5000 Only**) https://<MBG-FQDN>/webrtc/index.php If you select **Host WebRTC client on separate server** and employ the WebRTC client that is pre-installed on the MiCollab web server, configuration is complete when you save the WebRTC settings. Users may then initiate a call by entering the following addresses in their MiCollab Web Client: • **Subscriber call mode** <https://<MiCollab-server_FQDN>/ucs/micollab> If you select **Host WebRTC client on separate server** and choose to host the WebRTC client on your enterprise web server, after saving the WebRTC settings, you must download the Software Development Kit (SDK), modify the files contained in the kit to suit your requirements, and then upload the files to your enterprise web server. Users may then initiate a call by entering the following addresses in a web browser: • **Anonymous call mode** https://<standalone-web-server-FQDN>/webrtc/call.php?to=<CalledNumber | SipUri> • **Subscriber call mode** https://<standalone-web-server-FQDN>/webrtc/index.php

	Note: To host the WebRTC client on your enterprise web server, your implementation must include the MiVoice 5000 for subscriber-based calling, or the MiVoice 5000 or MiVoice Business for anonymous calling; other ICPs are not supported.
Enabled	You must disable/enable WebRTC after importing a web certificate to the system.
Mode	Select the call mode(s) that users can employ to initiate calls from their web browsers: - **Anonymous**: Users can initiate anonymous click-to-call sessions from a browser to the call controller. To access this service, the users are required to provide minimal credentials (name and CAPTCHA entry). MBG then directs them to an internal service that has been configured on the Anonymous WebRTC ICP. - **Subscriber**: Users can access the company directory and place calls from a browser using a SIP web phone. To access this service, the users are required to provide their MBG login credentials (set-site username and password). MBG then registers them with an ICP that has been configured on the ICPs screen. - **Anonymous and Subscriber**: Users can initiate both anonymous and subscriber calls.
Webserver shared secret	Choose a strong password to be shared between MBG and the external web server. This value must be set even when the MBG system is configured to function as a web server.
WebRTC ICP	Select the ICP to which WebRTC clients will be directed. Only one ICP can be selected as the destination of WebRTC Anonymous calls. The following ICP types are supported: • MiVoice Business • MiVoice 5000 **Note**: Multiple ICPs are supported for WebRTC Subscriber calls. When a user logs in, he or she provides their MBG login credentials (set-site username and password); MBG then registers the user to the ICP specified by the MBG administrator for that user.
WebRTC protocol security mode	This field controls encryption for WebRTC communications. Two options are available: - **Public only**: Encryption is enabled for WebRTC communications on the public interface of MBG (the Internet) but not the private interface. This mode must be used with MiVoice Business. - **Public and Private**: Encryption is enabled for WebRTC communications on both the public and private interfaces of MBG. Currently, this mode is available only with MiVoice 5000. For encryption to work properly on the public interface of the WebRTC server, you must configure the system with a third-party web certificate. The certificate must contain the FQDN that will be used to access WebRTC on MBG. It may also need to contain a different FQDN for MiCollab or other applications behind the MBG. (Refer to the relevant product documents for more information on certificate requirements.) Failure to install a trusted web certificate results in client applications being unable to connect to WebRTC. Depending on the application, this failure to connect may manifest in subtle ways like registration or call failures.

	1. Add the 3rd-party Web Server Certificate. For instructions, see “Installing a Third-Party Certificate on the MSL Server” in the *MSL Installation and Administration Guide*. **2.** Restart the WebRTC application: **3.** On the MBG main page, click the **Service configuration** tab and then click **WebRTC**. a. Clear the **Enabled** field. b. Click **Save**. c. Select the **Enabled** field. d. Click **Save**.
WebRTC whitelist/blacklist mode	This field controls the operation of the whitelist/blacklist security feature that can be enabled on the WebRTC application. The whitelist consists of "trusted addresses" belonging to ICPs that are configured on MBG. The blacklist consists of "untrusted addresses" belonging to endpoints that are suspected of malicious behavior such as brute force attacks. - **Neither**: The feature is disabled. All addresses are allowed. - **Whitelist and Blacklist**: Addresses on the whitelist (trusted ICPs) are allowed. Addresses on the blacklist (untrusted endpoints) are blocked. An address will be dropped from the blacklist after five hours, provided that it does not engage in suspicious behavior during that time.
Video enabled	Select to enable video in addition to audio. Clear to enable audio only. To take advantage of this feature, both endpoints must support the same codec: VP8 and/or H.264. Otherwise, transcoding must be enabled. When this field is enabled, users will see a video panel on the built-in call web site. If this field is disabled, the video panel will not appear. Not all WebRTC applications support video – refer to the application’s documentation for details.
Transcoding enabled	Select to enable transcoding to/from the codecs supported by WebRTC web clients (VP8 and sometimes H.264) and Mitel devices (G.711 and H.264). Transcoding video can be CPU intensive. To prevent your system from experiencing issues, you may need to instruct your users to limit the number of video calls that they place at any one time. Video transcoding requires a powerful server and its use on MBG Virtual is not recommended. You must enable transcoding if your implementation supports video calls and users are using Opera browser. Transcoding is not required if users use Firefox or Chrome (v52 or higher) browsers as both support the H.264 codec.
LDAP server	If you are using Subscriber call mode in conjunction with the MiVoice 5000, and you wish to look up/retrieve user information from an LDAP database such as Active Directory, enter the address of the LDAP server. For example, to use the LDAP database included with the MiVoice 5000, enter the address of the MiVoice 5000
LDAP DN	Enter the LDAP Distinguished Name.
LDAP login	Enter the LDAP login ID.
LDAP password	Enter the LDAP login password.
Pictures server URL	If you are using Subscriber call mode and wish to retrieve user images from a media server, enter the URL of the server. For example, to use the media server included with the MiVoice 5000, enter https://hostname/photos/local/ as the URL.

	The image files require the following format: <number>.png Where <number> is each user's telephone number.
Voicemail digits	Enter the telephone number required to access the voicemail system. Typically, this is a hunt group number.

Configure WebRTC Port Ranges (Optional)

You can set the range of ports available for use by WebRTC on the public (external) and private (internal) interfaces of MBG. By default, ports 32000 to 32500 are assigned to the public interface, and ports 33000 to 33500 are assigned to the private interface.

For most implementations, you should use the default values; no change is required.

To configure WebRTC port ranges on MBG:

1. On the MBG main page, click the **System configuration** tab and then click **Port ranges**.
2. If required, update the following port ranges:

- WebRTC public starting port
- WebRTC public ending port
- WebRTC private starting port
- WebRTC private ending port

After completing the configuration, double-check all settings. They are critical to the operation of the WebRTC gateway and are included in the Software Development Kit (SDK) that you download for deployment to your web server.

WEB SERVER CONFIGURATION

After configuring MBG to support WebRTC, download the Software Development Kit (SDK) from the WebRTC. The SDK includes the settings you have configured on MBG (WebRTC address and port, WebRTC protocol security mode, Webserver shared secret, etc.) and allows you to deploy the application to your web server, customizing the look and operation of the pages if you desire.

The SDK is provided free of cost but without developer support. If you require support, you must join the Mitel Solutions Alliance. See www.mitel.com/msa for membership information.

Note: These instructions are required only if you are going to embed WebRTC functionality in your own application or website, hosted on a separate server. If you are going to host the application on MBG itself or have chosen “Host on separate server” to use the MiCollab solution, these instructions can be ignored.

DOWNLOADING THE SDK AND OPENING THE FILES

To obtain the SDK:

1. On the MBG main page, click the **Service configuration** tab and then click **WebRTC**.
2. Click Download **SDK**.

The file (webrtc.zip) is downloaded in accordance with your web browser setup.

3. Move to file to a location of your choosing (if necessary), unzip it and examine the contents.

The SDK is an archive (zipped file) that contains:

- JavaScript libraries:
  - **miwebphone.js** is the SIP web phone used with Subscriber call mode.
  - **miwebrtc.js** is proprietary JavaScript required by the default web pages.
  - **sip<-x.x.x>.js** is the SIP stack that is used by miwebphone.js.
  - **jquery.js** is a well-known library required by miwebphone.js.
- PHP templates and their static resources. The templates are dynamic pages containing credentials which may differ according to the user identity or time of use:
  - **index.php** is the default template for Subscriber call mode. It includes a login interface and the SIP credentials required to enable the web phone (miwebphone.js) to work properly. As with any web site, it is the main page that allows dynamic content.
  - **config.php** contains WebRTC settings configured on MBG, which are used to generate dynamic web pages.
  - **call.php** is the default template for Anonymous call mode. It includes ephemeral credentials delivered through CAPTCHA verification. You can make this file "plug and play" by adding a destination number or SIP URI to it. The number/URI must also be configured on the ICP.

ADDING THE FILES TO THE WEB SERVER

There are two ways to implement WebRTC on your web server:

Implement the Complete SDK

To employ this option, simply extract the contents of the SDK onto the web server to a location such as the root directory. The server requires PHP. You can then begin using the standalone service by opening the appropriate URL in the SDK folder location. For example, to initiate a call, you would enter the following addresses in a web browser:

Anonymous call mode—https://<FQDN>/webrtc/call.php?toCalledNumberOrSipUri

Subscriber call mode—https://<FQDN>/webrtc/index.php.

Optionally, you can modify the implementation as follows:

1. Add a reference to the WebRTC in your own web site. To support anonymous call mode, make sure to include the destination number or SIP URI in the URL.
2. Updates the image and audio files. At the very least, hide the Mitel image by adding the "hh=1" parameter to the URL. If you have your own image and audio files, copy them to the appropriate directories and update the CSS accordingly.
3. Modify the PHP content to customize the look and operation of the service. This step is recommended only for experienced web developers.

Implement Only the JS Files

You can build your own web application using only the Javascript files included with the SDK. If your web pages are dynamically created by PHP, you can include the config.php file as in your PHP code. If your implementation does not support PHP, you must manage these parameters manually.

You are required to use the following JavaScript libraries:

- **miwebphone.js** — SIP web phone used with Subscriber call mode.
- **sip<-x.x.x>.js** — SIP stack that is used by miwebphone.js.

- **jquery.js** — well-known library required by miwebphone.js.

Correspondence table of config.php values and miwebphone.js constructor values:

CONFIG.PHP	MIWEBPHONE.JS CONSTRUCTOR
$websocket_secure	'ws_secured'
$websocket_server	'ws_server'
$websocket_port	'ws_port'
$disable_video	'disable_video'
$user_ipbx_server	'pbxIpaddress'

Config.php values used by the web pages but not provided to the constructor:

- $webrtc_mode=1 — Used to enable/disable independently the PHP web pages.
- $enable_captcha=1 — Used to enable/disable the display of the CAPTCHA.
- $websocket_passphrase="MySecret" — Used to generate the ephemeral credentials of anonymous call.
- $webservice_server=https://my.mbg.mydomain.foo/webrtc/api/ — This is the root URL that is used to access web services on MBG, including to retrieve ICP credentials, execute directory searches and display user images.

CLUSTERING

Multiple MBG nodes can be joined together and programmed to balance the connection load, and to provide redundancy and/or scalability for MiNET devices. To set up a cluster initially, two nodes are designated "master" and "slave". The master node can then add nodes to the cluster, applying both a weighting factor for load balancing and a list of “fall-back” servers for resiliency. For more information about cluster capabilities, see the MBG Engineering Guidelines.

Data is shared among the nodes in the cluster, with the master node being the authoritative data holder. In the case of a master node failure, any slave node has the option to take ownership of the cluster.

For configuration information, see Configure a Cluster in the MBG online help.

The following illustration shows a cluster of MBG-SRC servers on the LAN with another MBG server deployed in server-gateway (network edge) configuration. Note that you cannot mix software releases within a cluster (for example, one node running Release 7.1 and another node running Release 8.0 is not supported).

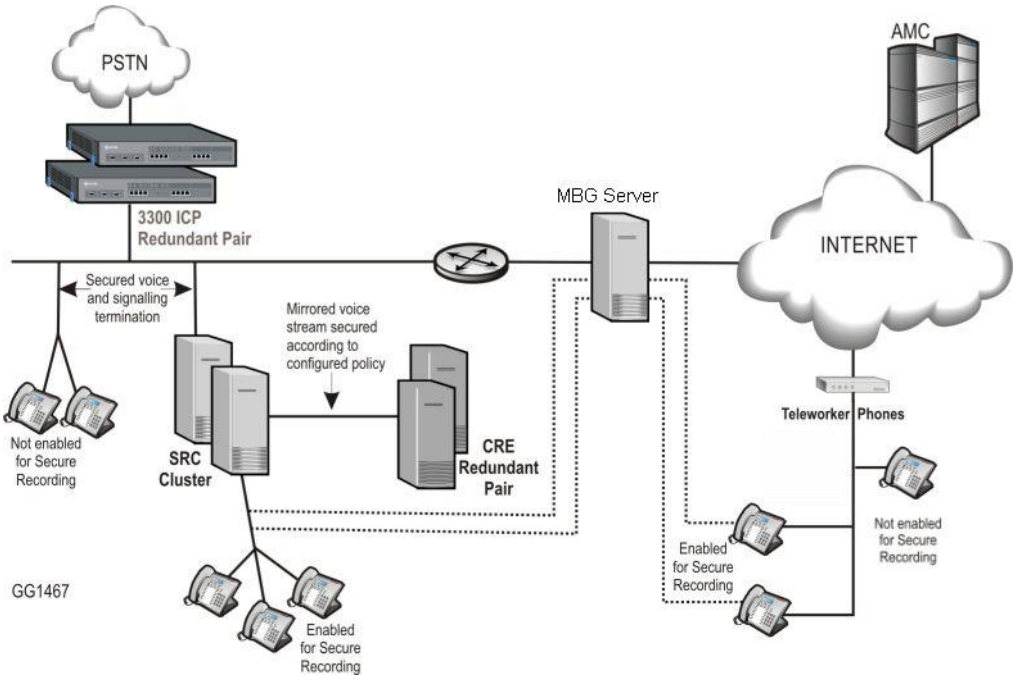


Figure 17. MBG Server with SRC Service (Direct Call Recording)

The setup shown above also illustrates SRC resiliency. When an ICP fails, SRC and its enabled sets fail over to the other ICP in the redundant pair. When an SRC node fails, recording is temporarily disrupted but all enabled sets fail over to another node in the cluster and service resumes for new calls.

Note: The CRE must be capable of connecting to all nodes in the cluster and be able to handle sets moving from node to node.

CLUSTER LICENSING

All nodes in the cluster contribute their licenses to the cluster "pool". Any node that requires a license (for connections, compression, or trunks) takes it from the pool. If the pool does not contain enough licenses to supply the node, the request fails and an alarm is generated. When a node is intentionally removed from a cluster (when the "Leave cluster" button is selected, or when the Master node selects the "Delete" link for that node), the licenses it originally contributed are also removed. Any licenses that it procured from the pool after joining the cluster are returned to the pool. If nodes without licenses are added to the cluster, they will also take from the pool as required. **Note**: Because the license pool "memory" is not maintained during service outages, we recommend that licenses are shared among all nodes in the cluster to avoid the possibility of a non-licensed node becoming the resilient failover server.

CLUSTER HARDWARE

MBG relies on the MSL Qualified Hardware List for hardware compatibility.

Note: With an increasing number of servers in a cluster, inter-cluster communications traffic increases on all nodes. When clustering three or more nodes, we recommend mid class or carrier grade servers that each have the same, or similar, capacity. Although load balancing is performed programmatically, there is also inter-server communication overhead that must be shared equally among nodes.

For more information about cluster weighting, load balancing and redundancy, see the *About Clustering* topic in the MBG online help.

DAISY CHAINING MBG SERVERS (TELEWORKING)

Some of the factors that contribute to latency and communication delay between the corporate and remote offices are:

- long distances (for example, hosting remote sets in Asia from North America)
- large number of remote sets deployed at one or more remote offices

Daisy chaining MBG servers provides a method of decreasing the virtual distance by allowing local streaming access among remote offices.

Multiple standalone MBG servers are daisy chained to an ICP-connected MBG server. The upstream MBG server (closest to the ICP) provides the local streaming feature for all connected MBG servers, allowing all sets connected to these servers to communicate directly without sending the voice stream back through the upstream server.

Notes:

- Licenses are required only on the downstream MBG servers, not on the upstream server.
- Daisy chaining and standard mode of proxying for ICPs are mutually exclusive.

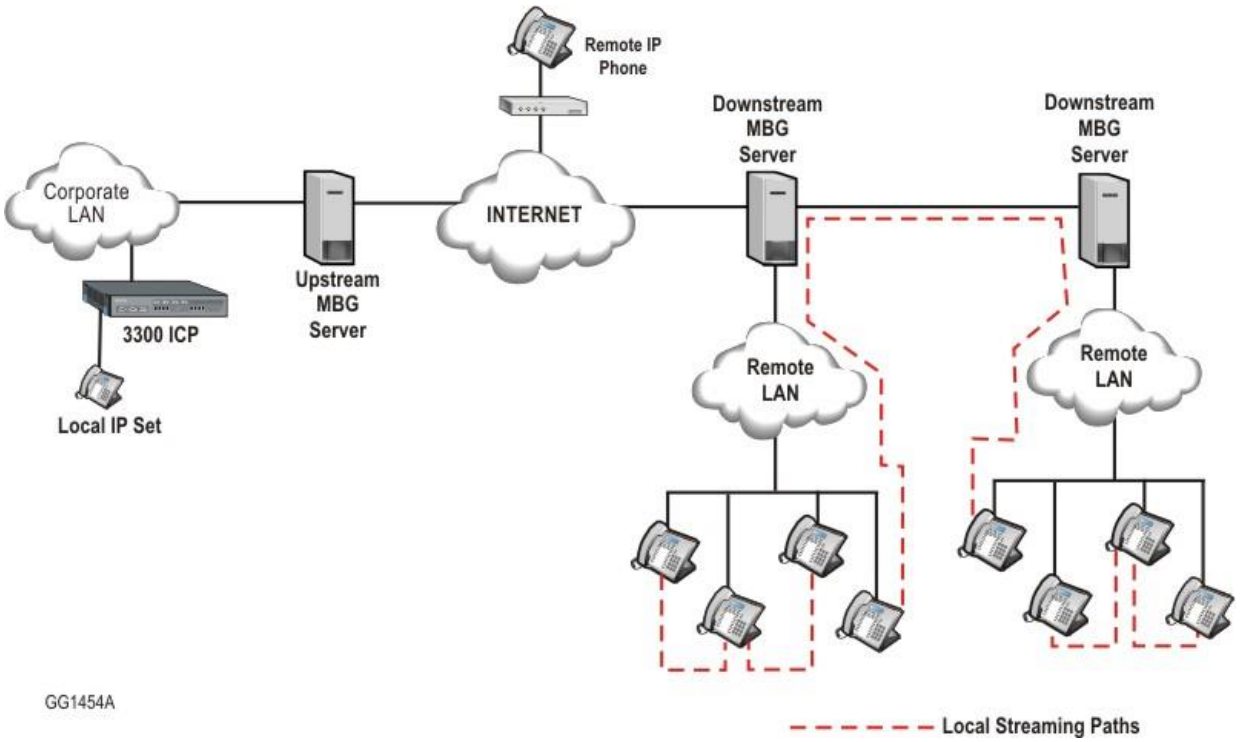


Figure 18. Daisy Chaining

SETTING UP DAISY CHAINED SERVERS

For geographically remote servers:

1. Configure your upstream MBG server as usual (either Gateway or DMZ deployment).

2. On the downstream server, use the MBG web interface to configure the following parameters:
   - On the MBG main page, click the **System configuration** tab and then click **Network profiles**.
   - Click Enter Daiseychain Mode.
   - In the **Daisy-Chain IP address** field, enter the IP address of the upstream MBG server.
   - Click **Save**.

Notes:
- Downstream server can be in either Gateway or DMZ deployment mode.
- Add sets and configuration changes to the upstream server only.

For remote offices with high volume of remote sets:

This scenario can be configured in one of the following two ways:

1. Remote (downstream) office uses an MBG server operating in Gateway mode as the Internet firewall.
2. Remote office has a separate firewall and runs the MBG server in DMZ mode.

In either case the configuration described under *For geographically remote servers* should be done on the downstream server.

Note: There is no restriction on the location of remote sets – they do not have to be on the LAN side of the server. So it is possible (and may be desirable) to have Internet MBG sets also point to the downstream server to maintain local streaming with sets on the remote LAN.

DAISY CHAINING TO ENFORCE STRICT FIREWALL RULES

You can also daisy chain an MBG server in your LAN to another MBG server in your DMZ and apply a strict firewall rule that only allows traffic between the two. (In the normal recommended DMZ deployment, the firewall must be configured less strictly, allowing certain UDP and TCP connections to your internal network.)

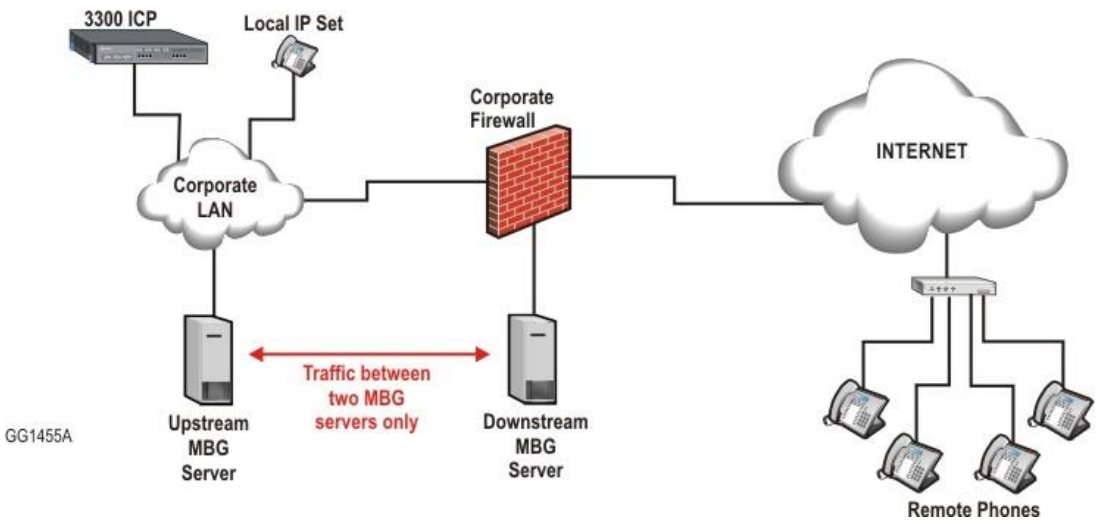


Figure 19. Daisy Chained Firewall Administrator

This configuration places the downstream server in the DMZ and daisy chains it to the upstream server on the LAN. Both servers are configured in DMZ mode (that is, one Network Interface).

The downstream server is configured as described under *For geographically remote servers* on page 73.

Note: Add sets and configuration changes to the upstream server only.

UPGRADING SOFTWARE AND LICENSES

When you upgrade MBG software, the previous version of the software is automatically removed after the upgrade is complete.

Note: For upgrades in a clustered environment, see *Upgrading a Cluster Setup* on page 79.

UPGRADING MIVOICE BORDER GATEWAY SOFTWARE

- If you are upgrading **from a release older than 5.2**, you must upgrade to Release 5.2 before you can proceed. Follow the instructions in the Release 5.2 documentation to upgrade to 5.2 and then follow the instructions below.
- If you are upgrading **from Release 5.2 to Release 6.0 or later**, follow the instructions below.
- It is recommended to upgrade to the latest release of MSL prior to upgrading MBG software. This enables you to take advantage of the latest MSL features such as IPv6 addressing and Virtual MiVoice Business.
- For major software upgrades (e.g. upgrading from MSL 9.x to MSL 10.x), you must perform a fresh installation of MSL and MBG software.

Upgrading a Physical MBG with CD/DVD or USB

You can upgrade from CD/DVD or USB media provided you have physical access to the MBG server.

Note: For major software upgrades, such as the upgrade to MBG 8.0/ MSL 10.0, you must perform a fresh software installation. This entails backing up the database, installing the new MSL version from a CD/DVD or USB flash drive, and restoring the database.

To upgrade a physical MBG with CD/DVD or USB:

1. Obtain the MBG and MSL software from Mitel Online and copy it to CD/DVD or USB media.
2. In the server manager, under Applications, click **MiVoice Border Gateway**.
3. Shut down the MBG service using one of the methods described in Disabling the MBG Service on page 21.
4. Under Administration, click **Backup** and follow the prompts to perform a full system backup to a USB device or network file server.
5. Install the new MSL software:
   a. Configure your system to boot from either the CD/DVD-ROM drive or the USB drive.
   b. Insert the software CD/DVD or USB drive containing the new software.
   c. In the server console, selecting the **Reboot** menu option.
   d. Follow the prompts to install the software. During this process, select the option to **Erase all disks and perform fresh install**.
   e. When prompted, remove the CD/DVD or USB media and then reboot the system.
6. Restore from backup:
   a. After the system has rebooted, you are prompted "Do you wish to restore from backup?" Click **Yes**.

b. Select Restore from removable device.

c. You will be prompted to insert the removable device (USB or CD/DVD) containing the backup file. You can then select the backup file you wish to restore and follow the prompts to install it.

d. After responding to all prompts, click **Next** to restore the backup data. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the **Decryption password**. When the restore completes, MSL reboots the server and activates the restored configuration.

7. After the system has rebooted, log back in to the server console.

8. Select the option to **Register for Service Link** to perform a sync with the AMC.

Note: For details concerning backup, installation and restore process, see the *Mitel Standard Linux Installation and Administration Guide*.

Upgrading a Physical MBG with Remote Fresh Installation (RFI) Blade

This procedure enables you to upgrade a physical MBG from a remote location. Access to the server's media (CD/DVD ROM or USB) is not required.

Notes:

- The RFI blade requires sufficient disk space for a backup. If your system has insufficient disk space, the MBG blade will not be listed on the Blades panel.
- The RFI blade is not intended for virtual deployments and is only available to the MBG application.
- To employ this procedure, your system must be running MSL 9.3 or later.

To upgrade a physical MBG with the RFI blade:

1. In the server manager, under Administration, click **Backup** and follow the prompts to perform a full system backup to a USB device or network file. See the *Mitel Standard Linux Installation and Administration Guide* for detailed instructions.

2. Under Applications, click **MiVoice Border Gateway**.

3. Shut down the MBG service using one of the methods described in Disabling the MBG Service on page 21.

4. Under ServiceLink, click **Blades** and then click **Update List**.

5. Locate the **Remote Fresh Install** blade and click Install link beside it.

6. Accept the software license agreements when prompted.

   The system automatically backs up the database, installs the software, and restores the database. After this process is complete, you are prompted to reboot the server.

7. In the server manager, under Administration, click **Shutdown or reconfigure**, select **Reboot** and then click **Perform**.

   When the reboot is complete, log back in to the server console and confirm that the configuration data has been restored. If there is a problem, restore from the backup you saved in step 1. For instructions, see "Restore on an Operational System" in the *Mitel Standard Linux Installation and Administration Guide*.

8. Select the option to **Register for Service Link** to perform a sync with the AMC.

9. Reinstall the MBG application software blade. See the *Mitel Standard Linux Installation and Administration Guide* for detailed instructions.

10. Under Applications, click **MiVoice Border Gateway**.

11. Click the **System status** tab and then click **Dashboard**.
12. In the **Enabled** field, click **Start**.

Upgrading a Virtual MBG on VMware

The following procedure describes how to perform a fresh software installation, which is required for major software upgrades such as the upgrade to MBG 8.0/ MSL 10.0. The procedure entails obtaining a new OVA file that includes all of the necessary software (VMware tools, MSL, and MBG application), backing up the database, deploying the software, and restoring the database

For a minor software upgrade, such as a Service Pack release, you can update the vMBG version from the Blades panel of the MSL Server Manager.

To upgrade a virtual MBG:

1. Download the vMBG OVA file from Mitel Online to a network drive or vSphere client PC.
2. In the server manager, under Applications, click **MiVoice Border Gateway**.
3. Shut down the MBG service using one of the methods described in Disabling the MBG Service on page 21.
4. Under Administration, click **Backup** and follow the prompts to perform a full system backup to a network file server that supports SFTP (Linux) or SMB/CIF (Windows).
5. Deploy the vMBG OVA file on the host system. See Deploy Virtual MBG Appliance on page 17.
6. In the vSphere client, right-click the newly created vMBG instance and then click **Power > Power On**.
7. Right-click on vMBG again and select **Open Console**.
8. Place the cursor in the console window and click to continue.
9. Click **Next**, select your keyboard layout, and then click **Next**.
10. After the system has rebooted, you are prompted "Do you wish to restore from backup?" Click **Yes**.
11. Do one of the following:
12. Restore from backup:
    a. When the system prompts you with "Do you wish to restore from backup?", click **Yes**.
    a. Select Restore from Network Server.
    b. You will be prompted to select a network interface to use for the restore (LAN or WAN), the address and netmask of the local MSL server, the address, gateway and domain name of the backup server, the folder name containing the backup file, and the username and password required to log in to the backup server.
    c. After responding to all prompts, click **Next** to restore the backup data. When the restore completes, MSL reboots the server and activates the restored configuration.
13. Restore from another running server:
    a) When the system prompts you with "Do you wish to restore from backup?", click **Yes**.
    b) When prompted, select Restore from another running server.
    c) If your system has more than one network adapter, select the adapter to use for the restore procedure. (This will usually be the LAN adapter.)
    d) Enter the local **IP address** of the new server.
    e) Enter the appropriate **subnet mask** for this server.

f) Enter the **IP address** of the existing server.

g) If the two servers are on different IP networks, MSL will prompt for the **gateway IP address** to use to access the existing server.

h) When prompted, enter the “admin” **password** for the existing server.

i) MSL does the following:

- Configuration and application data is backed up from the existing server.
- Configuration and application data is restored to the new server.
- The existing server is shut down.

j) On the new server, the restore is confirmed. Press **Enter** to reboot and activate your restored configuration settings.

14. After the system has rebooted, log back in to the server console.

15. Select the option to **Register for Service Link** to perform a sync with the AMC.

Notes:

- The backup file cannot be restored from a USB drive.
- For details concerning backup, installation and restore process, see the *Mitel Standard Linux Installation and Administration Guide*.

Upgrading a Virtual MBG on Hyper-V

When MBG is installed as a virtual appliance in Hyper-V, the Microsoft Windows native hypervisor, your upgrade options are similar to those that are available for physical servers. For minor release upgrades and Service Pack releases, you should perform a blade upgrade, and for major upgrades you must perform a fresh install and restore.

For more information concerning vMBG on Hyper-V, refer to the Mitel Virtual Appliance Deployment Guide.

Upgrading a Cluster Setup

You will upgrade the master node first, causing a temporary software version mismatch.

Notes:

- Do not attempt to update the MBG or cluster configuration after starting the upgrade process. Any changes you make, such as programming sets or trunks, will be lost when the slaves synchronize with the master.
- As you proceed with the upgrade, the MBG Dashboard will reflect the state of the individual nodes, not of the complete cluster. The nodes will display the same settings once they are synchronized and the upgrade is complete.

Back up the Cluster Nodes:

1. On each node in the cluster, access the MBG main page and do the following:

- Under **Administration**, click **Backup** to perform a full MSL system backup. See the *Mitel Standard Linux Installation and Administration Guide* for detailed instructions.

Upgrade the Master Node:

1. Access the MBG main page on the master node.

2. (Optional) Redirect MiNet sets from the master node to other nodes in the cluster:

Note: The following steps are required only if your implementation includes MiNet sets.

- On the master node, click the **System status** tab and then click **Dashboard**.
- For the master node, click the **Modify node** icon.
- In the **Cluster weight of current node** field, select **0**. Click **Save**.
- Wait for the sets to be redirected.

3. Stop the MBG service:
   - On the **System status** tab of the master node, click **Dashboard**.
   - To stop the service immediately, click **Stop**. To stop the service after calls have completed, click **Courtesy Down**.
4. Upgrade MSL and MBG software on the master node.
5. If you are upgrading from MBG 8.x or earlier to MBG 9.2 or later, set the SSL cipher suite on the master node:

Note: If you are upgrading from MBG 9.0 or 9.1 to MBG 9.2 or later, the following steps are *not* required.

   - On the master node, click the **System configuration** tab and then click **Settings**.
   - In **SSL Ciphers**, select **8.x Compat**. Click **Save**.
6. Start the MBG service:
   - On the **System status** tab of the master node, click **Dashboard**.
   - Click **Start**.

   The **Cluster Status** field on the Dashboard will report a mismatch between major software versions. In this state, partial cluster functionality is available (including license sharing and set load balancing) but configuration updates will not be possible until all nodes have the same software version.
7. (Optional) Redirect MiNet sets back to the master node:
   - On the master node, click the **System status** tab and then click **Dashboard**.
   - For the master node, click the **Modify node** icon.
   - In the **Cluster weight of current node** field, select the original value (eg. **90** or **100**) . Click **Save**.
   - Wait for the sets to be redirected.

Upgrade the Slave Nodes:

1. Access the MBG main page on a slave node.
2. (Optional) Redirect MiNet sets from the slave node to other nodes in the cluster:

Note: The following steps are required only if your implementation includes MiNet sets.

   - On the slave node, click the **System status** tab and then click **Dashboard**.
   - For the slave node, click the **Modify node** icon.
   - In the **Cluster weight of current node** field, select **0**. Click **Save**.
   - Wait for the sets to be redirected.

3. Stop the MBG service:
   - On the **System status** tab of the slave node, click **Dashboard**.
   - To stop the service immediately, click **Stop**. To stop the service after calls have completed, click **Courtesy Down**.
4. Upgrade MSL and MBG software on the slave node.
5. Start the MBG service:
   - On the **System status** tab of the slave node, click **Dashboard**.
   - Click **Start**.
6. (Optional) Redirect MiNet sets back to the slave node:
   - On the slave node, click the **System status** tab and then click **Dashboard**.
   - For the slave node, click the **Modify node** icon.
   - In the **Cluster weight of current node** field, select the original value (eg. **90** or **100**) . Click **Save**.
   - Wait for the sets to be redirected.
7. Repeat steps 1 through 6 for all slave nodes.
8. Wait for the cluster to synchronize.

   The **Cluster Status** field on the Dashboard should report that the nodes are successfully clustered.

Reset the SSL Cipher Suite on Master Node:

Note: The following steps are required only if you are upgrading from MBG 8.x or earlier to MBG 9.2 or later.

1. Access the MBG main page on the master node.
2. Reset the SSL cipher suite on the master node:
   - On the master node, click the **System configuration** tab and then click **Settings**.
   - In **SSL Ciphers**, select **Default**. Click **Save**.

UPGRADING MIVOICE BORDER GATEWAY LICENSES

To purchase additional user or compression licenses:

1. Contact Mitel Customer Services (or your Authorized Partner) and place your order using the part numbers in Table 1.
2. In your AMC account, access the Application Record that applies to this MSL installation. Assign the upgrade products from your License account to the Application Record. The AMC updates your licenses on its regular synchronization OR you can force an immediate synchronization by clicking the **Sync** button on the **Status** page of the server manager.

Table 1. MBG License Part Numbers for 3300 ICP and MiVoice Office 250

PART NUMBER	DESCRIPTION	NOTES

54004571	MBG Base	Every MBG Solution must have this base level of service. Includes: • MBG base software blade • Web Proxy software blade • 1-year Software Assurance - or – • MBG deployed in a virtual environment using VMware virtualization solution (see 54005339, below)
54004572	MBG Upgrade	1 additional client license
54004573	MBG Upgrade	10 additional client licenses
54004574	MBG Upgrade	25 additional client licenses
54004575	MBG Upgrade	50 additional client licenses
54004577	MBG Upgrade	100 additional client licenses
54004578	TW to MBG Upgrade	Upgrade from Teleworker 4.5 to MBG 5.2
54004581	MBG Upgrade	Upgrade from Teleworker 5.0 to MBG 5.2
54004582	MBG Compression	5-session Compression License
54005339	MBG Virtual Appliance	MBG deployed in a virtual environment using VMware virtualization solution
54005340	MBG Virtual Appliance Demo Kit	MBG Virtual Appliance demonstration software
54005472	IPv6 License for MBG	MBG deployed in an Internet Protocol version 6 environment

Table 2. Part Numbers for Secure Recording Connector Licenses

PART NUMBER	DESCRIPTION	NOTES
54003182	SRC Upgrade	1 additional tap license (Note that a single SRC license is used for each recorded call. So if you anticipate the need to record 20 calls simultaneously, you will require 20 SRC licenses. In most circumstances, you will not require an SRC license for every set.)
54003183	SRC Upgrade	10 additional tap licenses
54003184	SRC Upgrade	50 additional tap licenses
54003231	SRC 5-port Compression	5-port compression license (Applies to compression between SRC and CRE - not required for G.729 compression on IP Phones.)
54005314	Upgrade from SRC 2.2 to MBG 6.1	Upgrade license

Table 3. Part Numbers for SIP Trunking Licenses

PART NUMBER	DESCRIPTION	NOTES
54004491	MBG: 1 SIP Trunking Channel License	• SIP Trunking

SUPPORTING DOCUMENTATION

To access Product and Technical Documentation

1. Log on to Mitel OnLine.
2. Point to **Support**.
3. Click Product Documentation.
4. To access IP Phone documentation, point to End User Documents and then click PDF Guides.
5. To access MBG documentation, point to **Applications** and then click **MiVoice Border Gateway**.

To access Mitel Knowledge Base articles

1. Log on to Mitel OnLine.
2. Point to **Support**.
3. Under Technical Support, click **Mitel Knowledge Base**.
4. Click **Mitel Knowledge Base**. The Knowledge Base search engine opens.
5. From the Product list, select **MiVoice Border Gateway** and then click **Search**.

To download MSL software from Mitel OnLine

1. Log on to Mitel OnLine.
2. Point to **Support**.
3. Under Technical Support, click **Software Downloads**.
4. Select MiVoice Border Gateway software.
5. Click the links to download Release Notes and software.

MBG AND EMERGENCY SERVICES

MBG alone is not suitable for providing reliable access to emergency services (for example, 911, 999 or 112). See the following legal disclaimer.

WARNING: MITEL NETWORKS DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT THE SOFTWARE WILL PERMIT OR ALLOW YOU ACCESS TO EMERGENCY CALL SERVICES, SUCH AS 911/999/112 OR SIMILAR EMERGENCY CALL SERVICES (IN THE APPLICABLE TERRITORY WHERE THE SOFTWARE IS USED). MITEL NETWORKS FURTHER DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OR REPRESENTATION THAT, IN THE EVENT SUCH ACCESS IS AVAILABLE, THE SOFTWARE WILL RELAY ACCURATELY OR AT ALL, THE DEVICE IDENTIFICATION NUMBER OR PHONE NUMBER (ALSO KNOWN AS AN AUTOMATIC NUMBER IDENTIFICATION (ANI) OR CALLBACK) OR THE LOCATION (ALSO KNOWN AS AUTOMATIC LOCATION INFORMATION (ALI)) YOU ARE CALLING FROM, TO THE APPROPRIATE EMERGENCY RESPONSE CENTER (ALSO KNOWN AS A PUBLIC SAFETY ANSWERING POINT (PSAP)). MITEL NETWORKS RECOMMENDS THAT THE SOFTWARE NOT BE USED IN CONNECTION WITH OR TO UTILIZE EMERGENCY CALL SERVICES, SUCH AS 911/999/112 OR SIMILAR EMERGENCY CALL SERVICES.

Emergency call routing can be supported as follows:

Note: Emergency call routing in a MiVoice Border Gateway environment is supported with the use of the following equipment ONLY:

- a properly programmed MiVoice Business ICP (release 6.0 or higher).
- a properly programmed Mitel Dual Mode 5220, 5224, 5235, or 5340 IP phone equipped with a properly configured Mitel Line Interface Module (LIM).

IMPORTANT! For resilient operation, the LIM must be configured as a second channel device, with emergency call routing configured on both the primary and secondary ICP.

For other required configuration details see the following **guides at Mitel Online.**

FOR MORE INFORMATION ABOUT…	PLEASE REFER TO THIS DOCUMENTATION…
LIM Configuration	LIM Installation Guide (LineInterfaceModule IG.pdf)
Programming The MiVoice Business ICP For Emergency Call Routing	MiVoice Business ICP System Administration Tool Online Help
Programming Mitel IP Phones With Lim	5220 Dual Mode IP Phone User Guide 5224 IP Phone User Guide 5235 IP Phone User Guide 5340 IP Phone User Guide
Resiliency	MiVoice Business ICP Resiliency Guidelines

APPENDIX A: THIRD PARTY LICENSES

Parts of Mitel Border Gateway are licensed under open-source licenses. By accepting the Mitel EULA, you are also accepting all open-source software terms and conditions.

ARES DNS LIBRARY

Version 2.0, January 2004

Copyright 1998 by the Massachusetts Institute of Technology.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

M.I.T. makes no representations about the suitability of this software for any purpose. It is provided ""as is"" without express or implied warranty.

PICOJSON

Copyright 2011 Kazuho Oku

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY CYBOZU LABS, INC. ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL CYBOZU LABS, INC. OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."

RESIPROCATE SIP STACK

The Vovida Software License, Version 1.0

Copyright (c) 2000 Vovida Networks, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names "VOCAL", "Vovida Open Communication Application Library", and "Vovida Open Communication Application Library (VOCAL)" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact vocal@vovida.org.
4. Products derived from this software may not be called "VOCAL", nor may "VOCAL" appear in their name, without prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL VOVIDA NETWORKS, INC. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DAMAGES IN EXCESS OF $1,000, NOR FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by Vovida Networks, Inc. and many individuals on behalf of Vovida Networks, Inc. For more information on Vovida Networks, Inc., please see http://www.vovida.org.

RTPPROXY

Copyright (c) 2004-2006 Maxim Sobolev sobomax@FreeBSD.org

Copyright (c) 2006-2014 Sippy Software, Inc., http://www.sippysoft.com

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OFSUCH DAMAGE.

XMLRPC-C (USED BY RTPENGINE):

Copyright (C) 2001 by First Peer, Inc. All rights reserved.

Copyright (C) 2001 by Eric Kidd. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PCRE (USED BY RTPENGINE)

PCRE2 LICENCE

PCRE2 is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 10 of PCRE2 is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE2, supplied in the "doc" directory, is distributed under the same terms as the software itself. The data in the testdata directory is not copyrighted and is in the public domain.

The basic library functions are written in C and are freestanding. Also included in the distribution is a just-in-time compiler that can be used to optimize pattern matching. This is an optional feature that can be omitted when the library is built.

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England.

Copyright (c) 1997-2015 University of Cambridge

All rights reserved.

PCRE2 JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg

Email local part: hzmester

Emain domain: freemail.hu

Copyright(c) 2010-2015 Zoltan Herczeg

All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg

Email local part: hzmester

Emain domain: freemail.hu

Copyright(c) 2009-2015 Zoltan Herczeg

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University of Cambridge nor the names of any contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBVPX

Copyright (c) 2010, The WebM Project authors. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of Google, nor the WebM Project, nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SECURIMAGE

Copyright (c) 2011 Drew Phillips

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Mitel
Powering connections
mitel.com

© Copyright 2017, 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.