A MITEL
PRODUCT
GUIDE

MiCollab Engineering Guidelines

Release 9.5
May 2022

Mitel
Powering connections

Notices

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

Trademarks

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

®,™ Trademark of Mitel Networks Corporation

Contents

Introduction 1

This chapter contains the following sections:

This document provides guidelines for implementing MiCollab solutions. You will find the following information in this document:

- System Overview
- Deployment Configurations
- System Requirements
- Capacities, Performance, and Constraints
- Upgrade, Migration, and Conversion Considerations
- Application-specific Guidelines

1.1 Obtaining Product Information

1.1.1 Accessing Customer Documentation

To access MiCollab product documentation:

1. Log on to Mitel MiAccess (formerly known as **Mitel Connect**).
2. From the left menu, select **Doc Center**.
3. Click **APPLICATIONS** > **COLLABORATION**> **MICOLLAB**.

> **Note**:
>
> For PBX related documentation, navigate to **Business Phone Systems** > **On Site**.

1.1.2 Accessing the Knowledge Management System

To access the Knowledge Management System:

1. Log on to **Mitel MiAccess** (formerly known as **Mitel Connect**).
2. From the left menu, select **Knowledge Management System**.

   The Knowledge Base search engine opens.
3. Enter your application name in search area and click the **Search** icon.

1.2 Obtaining MiCollab Software Downloads

Refer to *MiCollab Installation and Maintenance Guide* for instructions on how to download the MiCollab software package.

What’s New in MiCollab Release 2

For the list of new functionalities, see the MiCollab What's New Guide, in the Mitel Customer Documentation site, the Document Center.

System Overview 3

MiCollab is a software solution that provides co-residency features for applications that use the MSL operating system. MiCollab supports co-residency of the following applications:

- MiCollab Client
- Mitel Standard Linux
- MiCollab Client Deployment
- Suite Application Services
- MiCollab Audio, Web and Video Conferencing
- NuPoint Unified Messaging
- MiVoice Border Gateway (MBG)
- MiVoice Border Gateway (MBG) with Secure Recording Connector (SRC) in LAN Mode (server-only)

Note:

The MBG Web Proxy is only supported when it is installed on a second MBG server that is located in the DMZ.

Note:

(MiVB only): The Speech Auto Attendant option is only supported if NuPoint Unified Messaging is the only installed application. This restriction applies to both the MiCollab server and MiCollab Virtual Appliance. Although all applications are installed in the MiCollab Virtual Appliance OVA, if you only apply NuPoint licenses (à la carte) then it is considered a single application installation.

Note:

The MiCollab server must never be directly connected to the Internet, but the MiCollab server should always be isolated from the Internet by an MBG and/or a properly configured firewall.

Deployment Configurations 4

This chapter contains the following sections:

4.1 MiCollab Server or MiCollab Virtual Appliance Deployments

You can deploy MiCollab Server or MiCollab Virtual Appliance in the following configurations:

MiCollab in LAN with a second MBG Server in DMZ: This configuration has MiCollab located in the Local Area Network (LAN) connected to a second MBG server in the Demilitarized Zone (DMZ). Two variants of this configuration are supported:

- **MiCollab with second MBG Web Proxy in the DMZ (2 Server)** consists of a MiCollab on the corporate LAN with Web Proxy in an MBG server in the DMZ (see page 4). Remote web browser users connect to the MiCollab server through the Web Proxy.
- **MiCollab with second MBG / Teleworker/ Web Proxy in DMZ (2 Server)** consists of MiCollab on the corporate LAN with Teleworker and Web Proxy on a MiCollab server located in the DMZ (see page 8). The Teleworker service is installed on both the MiCollab and MBG systems. The Teleworker service in the MiVoice Border Gateway (MBG) is used to support the teleworkers in the DMZ. The Teleworker service in MiCollab is only used to remotely manage the Teleworker phones that are configured on the MBG server. The Web Proxy service is also installed in this configuration.

Table 1: MiCollab in LAN Mode (Server only)

License Software Package	License Components	Platform			
		MiVoice Business	**MiVoice Office 250**	**MiVoice Office 400**	**MiVice 5000 And Mivoice MX-One**
#1 MiCollab Software Base PN 54005441 Or #1 Virtual MiCollab Software Base PN 54005442	NP-UM	Yes	Yes	No	Yes
	SAA	Yes	No	No	No
	MiCollab AWV	Yes	Yes	Yes	Yes
	MiCollab Client	Yes	Yes	Yes	Yes
	MBG Secure Recording Connector (LAN devices only)	Yes	No	No	No
#2 MiCollab Client Add-on PN 54005445	MiCollab Client	Yes	Yes	Yes	Yes

Note:

The following restrictions apply to MiCollab deployments:

- The majority of the applications included in MiCollab are designed to run on the LAN. For this reason, MiCollab is not supported in the DMZ.
- In configurations where multiple MiCollab servers are deployed, each server must be managed separately. A single point of management for multiple MiCollab servers is not supported in this release.
- The MBG Web Proxy is not supported directly on a MiCollab server or MiCollab Virtual Appliance deployment. MBG Web Proxy is only supported when it is installed on a second MBG server that is located in the DMZ. In this deployment, the Web Proxy on the MBG server allows clients on the internet to connect through the network firewall to a MiCollab system on the LAN.

4.2 MiCollab Configuration with Web Proxy on a Second MBG Server

The majority of MiCollab applications are designed to run on the LAN (for example, NuPoint Messenger). For this reason, MiCollab is not supported in the DMZ. To support applications that have clients on the web, such as AWV, you require a web proxy running on a second MBG server in the DMZ to protect the MiCollab server in the LAN from Internet exposure.

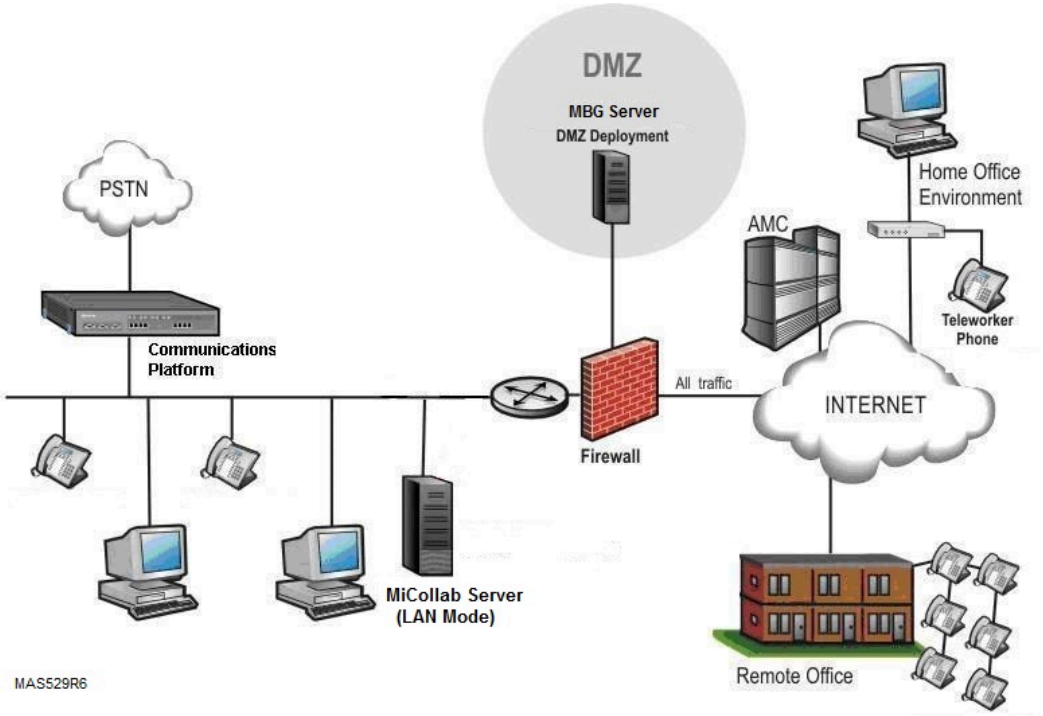
4.2.1 MBG Teleworker with Web Proxy

To support Teleworkers, use MiCollab in LAN Mode (server-only) with Web Proxy on a second MBG server in the DMZ,

In a DMZ configuration, as shown in the following figure, the **firewall** is the gateway for all IP network traffic with the internet. See Firewall Config for MiCollab in LAN with Web Proxy for details. See the *MBG with Web Proxy documentation* on the Mitel Customer documentation site for MBG configuration details.

This configuration provides a secure method for remote web browser users to connect with a MiCollab system located on the corporate LAN. Remote web browser users connect to MiCollab in the LAN through the Web Proxy.

Figure 1: MiCollab in LAN Mode with MBG and Web Proxy in DMZ



4.3 MiCollab AWV with Web Proxy

From MiCollab Release 8.0 onwards, there are two different configuration methods for providing access to the AWV application (installed on the MiCollab Server) from outside of the customer firewall. Previous software releases required the use of two external IP addresses, however with MiCollab Release 8.0 onwards, it is now possible to use a single external IP address.

4.3.1 Configuration with two external IPs

The AWV application uses two components, both of which will need to accept client connections:

- Web Browser access for web conferencing and user portal.
- Connection Point access for collaboration client.

Within the AWV settings, the External port is configured with 443. This directs the external clients to reach the Connection Point using port 443. The result is, the connection to both server components from external locations will request that they are to be reached on port 443.

To separate the two types of requests (because they are both using port 443), the firewall must have two IP addresses for AWV (one IP address for web conferencing and a second IP address for web collaboration client communication to Connection Point).

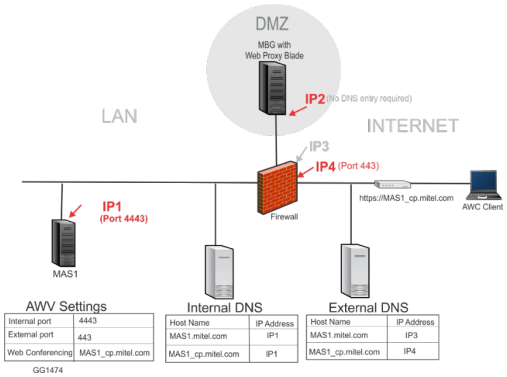
Firewall rules are then programmed to forward traffic from the second IP to a programmed port on the Web Proxy (default 4443). The Web Proxy then forwards the traffic to port 4443 on the MiCollab server (IP1 in the following figure). In addition to the basic DNS configuration in the last section, external DNS must be programmed to resolve requests for AWV Connection Point traffic (MAS1_mca.mitel.com) to the second IP address on the corporate firewall (IP4 in the following figure).

Note:

The configuration method using two external IP addresses is helpful in preventing connectivity issues that may arise when AWV Clients are behind a corporate firewall with rules for outgoing traffic, where those rules may only allow web-based ports to be reached at a remote location.

For example, a remote user is more likely to be able to make a connection to a server outside of their network using port 443, than port 4443.

Figure 2: MiCollab AWV External IP address Handling with Web Proxy (two external IPs)



4.3.2 Configuration with single external IP

The AWV application uses two components, both of which will need to accept client connections:

- Web Browser access for web conferencing and user portal.
- Connection Point access for collaboration client.

In the AWV configuration with one external IP address, the External Port is configured with 4443. This directs the external clients to reach the Connection Point using port 4443. The result is, the connection to the web conferencing portal will be requested on port 443, and the connection to the Connection Point component will be requested on port 4443.

Because two different ports are used, one External IP address can be used for both components.

The Firewall rules are programmed to forward the traffic to port 4443 on IP1 to port 4443 on MiCollab server (see the following figure).

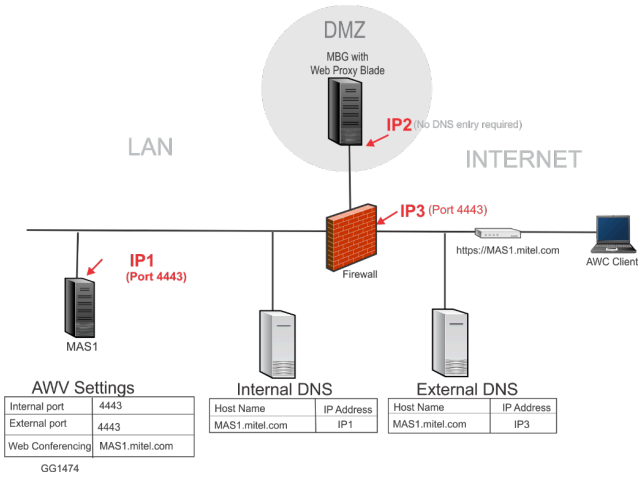
Note:

Ensure that the **Use HTTPS Only** setting is enabled in **System Options** configuration. Refer to the *Web Conferencing Settings* topic in the MiCollab AWV administrator online help.

Note:

The single IP address configuration will avoid the additional usage of a dedicated IP address (useful when IP addresses are costly or simply not possible), however it should be noted that some external users sitting behind a firewall with restricting outgoing traffic rules at ports other than 80 and 443 may experience connectivity issues.

Figure 3: MiCollab AWV External IP address Handling with Web Proxy (single external IP)



4.3.3 MiCollab Client with Web Proxy

A “MiCollab with MiCollab Client in LAN mode (server-only)” configuration requires an MBG server in the DMZ to provide a web proxy. The MBG application on the MiCollab server only provides a single point of provisioning to the MBG server.

4.3.4 Firewall Config for MiCollab in LAN with Web Proxy on 2nd MBG Server in DMZ

The corporate firewall must be configured to route web browser requests received at the firewall to the programmed HTTPS port on the Web Proxy. AMC traffic must be allowed between the Internet and both the web proxy MBG server and the MiCollab server for AMC communications.

MiCollab AWV traffic requires some additional firewall programming. The corporate firewall must be configured to forward client requests for Connection Point traffic to a port on the Web Proxy that is programmed to listen for Connection Point traffic (default is 4443) and forward the traffic to Port 4443 on the MiCollab server.

Firewall rules must be set up to allow communication between the MiCollab applications, the AMC, the ICP / CP, IP / SIP phones, and the Internet. The direction of the arrows in the following tables indicates permission to initiate 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 for MiCollab in LAN with Web Proxy on second MBG server in DMZ:

Table 2: Firewall Settings for MiCollab with Web Proxy (No Teleworker)

PORT RANGE	DIRECTION	DETAILS
TCP 22 (SSH)	Web Proxy Server → Internet MiCollab Server → Internet	**AMC Communications**. Allow outbound packets (and replies) on TCP port 22 between the Web Proxy and MiCollab Server and the Internet to enable AMC communications (i.e., enable server registration, software and license key downloads, alerts and reporting).

PORT RANGE	DIRECTION	DETAILS
TCP 80 (HTTP)	Web Proxy Server ← Internet	**Web Browser Access**. Allow inbound packets and replies on TCP port 80 between the Web Proxy server and the Internet. Used for remote web browser pages; will be redirected to TCP port 443 (HTTPS).
TCP 443 (HTTPS)	Web Proxy Server ← Internet Web Proxy Server → LAN	**Web Browser Access**. Allow inbound and outbound packets on TCP port 443 between the Web Proxy server and the Internet for web pages (SSL mode). Allow inbound and outbound packets on TCP port 443 between the Web Proxy server and the LAN for web pages.
TCP 4443 (default – can be configured in web proxy)	Web Proxy Server ← Firewall Web Proxy Server →LAN	**MiCollab AWV Collaboration Client**. Allow inbound packets on TCP port 443 (default is 443, for single IP allow inbound packets on TCP port 4443) and forward them to configured port (default 4443) on the Web Proxy server as well as return traffic. Allow inbound packets on TCP port 4443 between the Web Proxy server and the LAN. Used for Connection Point traffic related to MiCollab AWV Web Collaboration.
UDP 53 (DNS)	MiCollab Server → Internet Web Proxy Server → Internet	**Domain Name System**. The server requires DNS to look up the IP address of the Mitel AMC. Alternatively, the server can be configured to forward all DNS requests to another DNS server. See the *MSL Installation and Administration Guide* for details.

PORT RANGE	DIRECTION	DETAILS
TCP 443 (HTTPS)	MiCollab Server → Internet MiCollab Server → Internet	**Mobile Client Deployment**. Used to send deployment tokens and the configuration download URLs to the Mitel redirect deployment servers. **MiTeam Integration**: Used to connect with Mitel's Cloud-based MiTeam solution located on the Internet.
TCP 443 (HTTPS)	MiCollab Server ← Internet	**Remote Server Management**. *(Optional)* Allow inbound and outbound packets on TCP port 443 between the MiCollab Server and the Internet to allow remote management of the server, if required. HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface.

4.3.5 MSL Server Security Certificate – Trusted or Self-Signed

If a web browser displays a security alert warning indicating the MSL server's security certificate is "not trusted" or is "certified by an unknown authority", it means that the web browser is trying to verify the identity of the MSL server. Each MSL server automatically creates a self-signed certificate that is typically "not trusted" by web browsers.

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

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

OR

- You can obtain a trusted certificate from a trusted third-party Certificate Authority. Click **Web Server Certificate** in the server manager panel of the MSL server.

4.4 MiCollab with MBG Teleworker & Web Proxy Configuration

You can use a MiCollab server in LAN mode to manage Teleworker services that are running on a MiVoice Border Gateway (MBG) server located on the Network-Edge or in

the DMZ. To support this configuration, you install the MiCollab server with MBG in the LAN and install the MBG server with Teleworker in the DMZ.

Note:

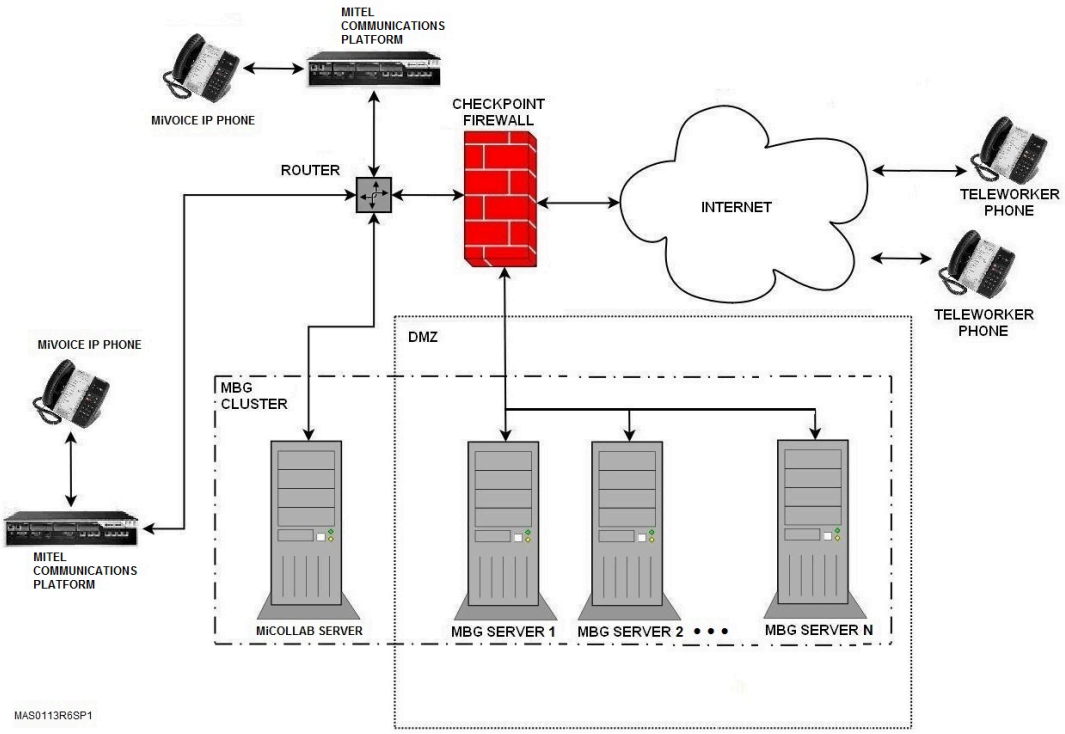
MiCollab server in LAN mode have an MBG proxy for any external connection. MiCollab on the LAN with no MBG is for internal connection only.

The follwoing figure shows an example of a MiCollab server deployed on the LAN and clustered with multiple MBG servers in the DMZ.

Clustering allows you to remotely manage the Teleworker services in the DMZ from the MiCollab server in the LAN. The MiCollab server (master) must have the Teleworker service installed and the MBG servers must have the Teleworker and Web Proxy Services installed. However, Teleworker phones are not supported on the LAN. You only use the Teleworker service on the MiCollab server to remotely manage the Teleworker phones on the MBG servers.

You can cluster multiple MBG servers in this configuration to support additional Teleworker capacity or to provide resiliency for the Teleworker phones. See *Install MiCollab Server in LAN Mode with an External MiVoice Border Gateway Server* in the *MiCollab Installation and Maintenance Guide* for instructions on how to configure the cluster.

Figure 4: MiCollab with MBG Teleworker & Web Proxy



The following table shows Firewall Settings for Teleworker in DMZ below indicates the Firewall settings needed for Teleworker service in addition to the settings in Firewall Settings for MiCollab with Web Proxy (No Teleworker). Some settings are the same as the settings defined in Firewall Settings for MiCollab with Web Proxy (No Teleworker).

Table 3: Firewall Settings for Teleworker in DMZ

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 22 (SSH)	MBG Server → Internet	**AMC communications**. Allow outbound packets (and replies) on TCP port 22 between the MBG Server and the Internet to enable server registration, software and license key downloads, alerts and reporting.
UDP 53 (DNS)	MBG Server → Internet	**Domain Name System**. The server requires DNS to look up the IP address of the Mitel AMC. Alternatively, the server can be configured to forward all DNS requests to another DNS server. See the *MSL Installation and Administration Guide* for details.

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 443 (HTTPS)	MBG Server ← Internet	**Remote Server Management**. *(Optional)* Allow inbound and outbound packets on TCP port 443 between the MBG Server and the Internet to allow remote management of the MBG server, if required. HTTPS access to allow remote management of the MBG server must be also be explicitly enabled from the server manager interface.
TCP 6800, 6801 and 6802	MBG Server → LAN MBG Server → ICP(s) MBG Server ← Internet	**MiNET Call Control**. Allow incoming and outgoing packets for TCP ports 6801 (MiNET-SSL) and 6802 (MiNET-Secure V1) between the MBG server and the Internet. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNET), 6801 and 6802 between the MBG server and the LAN and the MBG server and the ICP(s). The LAN rule can be omitted if there are no IP sets on the LAN, but ensure that the ICP(s) can communicate with the server's **public** address.
UDP 20,000 to configured upper bound* (SRTP)	MBG Server ← Internet MBG Server ← LAN	**Voice Communications**. Allow incoming SRTP on UDP ports 20000 – configured upper bound* from all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.
UDP 1024 to 65,535 (RTP)	MBG Server → LAN MBG Server → Internet	**Voice Communications**. Allow outgoing SRTP on UDP ports greater than, or equal to 1024 from the server to all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 6809	MiCollab Server → MBG Server	**MiCollab remote management of Teleworker**. This port allows a MiCollab server admin to remotely manage the Teleworker service in the DMZ. The MiCollab server manager panel indicates Remote Teleworker Solution. Teleworker Clustering must be enabled on the MiCollab server and MBG server.
TCP 3998, 6881	Internet → MBG Server	**SAC Connection Support**. Allow incoming TCP from the Internet to the MBG server, on ports 3998 and 6881, to support applications and web browsing, respectively, on the 5235, 5330, 5340 and Navigator sets. There is an additional LAN rule that follows this to complete the support.
TCP 6881	Internet → MBG Server	**MiNET MiVoice 69xx Avatar support**. Allow incoming TCP from the Internet to the MBG server on port 6881 to support avatars on MiVoice 6920, 6930, 6940 phones.
TCP 80	MBG Server → MiCollab Server	**MiNET MiVoice 69xx Avatar support**. Allow MBG to connect to the MiCollab server to retrieve avatars for MiVoice 6920, 6930, 6940 phones. (Optional).
UDP 5060	Server ←→ LAN Server ←→ Internet	**SIP Support**. If the SIP connector is enabled, then this port is required for non-encrypted SIP signaling between MBG and the set, between MBG and the ICP, and for SIP trunking support.
TCP 5060	MBG Server ←→ Internet MBG Server ←→ ICPs	**SIP TCP Support**. Open this port for SIP signaling over TCP between the MBG server and remote SIP devices that use TCP on port 5060. This port may also be opened between MBG and the ICPs.

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 5061	MBG Server ←→ Internet MBG Server ←→ ICPs	**SIP TCP/TLS Support**. This port is required for SIP signaling between the MBG server and remote SIP devices that have been configured to use TCP/TLS on port 5061 (the default client configuration). This port may also be opened between the server and the ICPs.
TCP 6806	Internet → MBG Server	**IP Console Support**. Open TCP port 6806 to support presence status updates.
TCP 6807	Internet → MBG Server	**IP Console and MiVoice Business Console Support**. Open TCP port 6807 to support presence status updates.

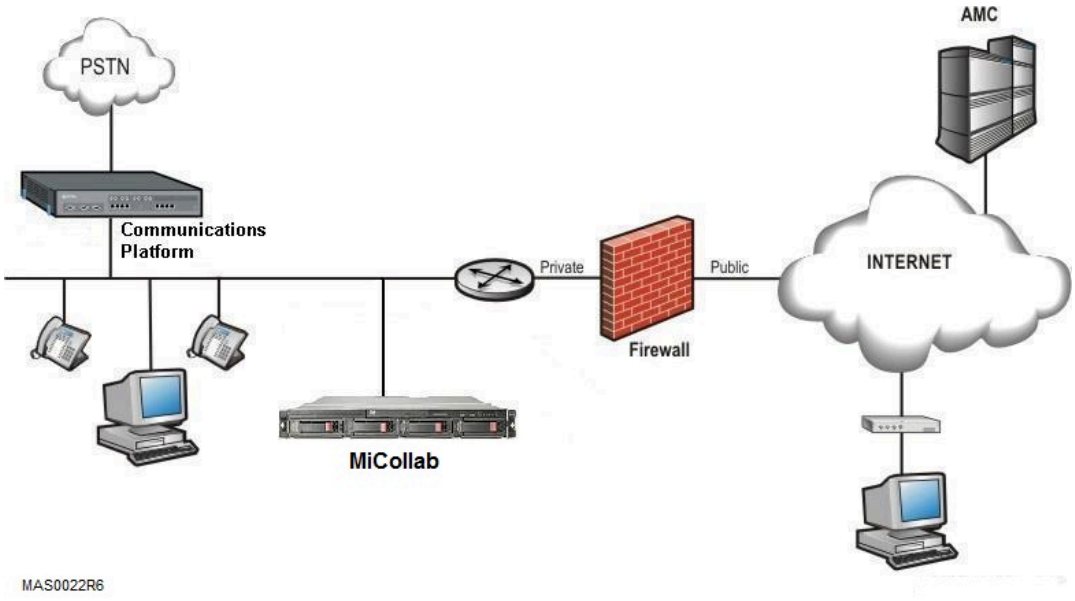
* Configured upper bound for SRTP on UDP ports is controlled by a setting in the Teleworker Solution Advanced panel. You must reserve four ports per set that you wish to support. Thus, to support 1000 sets, 4000 ports are required, from 20000 to 24000, and those ports must be open in the firewall configuration of any firewall that the Teleworker server is installed behind.

4.5 MiCollab in LAN Mode (Server-only)

In this mode, the MiCollab server is located on the local area network and acts as a "server only". It is not generally accessible from the Internet, making allowances only for outgoing connections to resolve DNS, and to communicate with the Applications Management Center (AMC) for synchronization. The MiCollab Ethernet adapter (or Network Interface Card) is configured as "Local" network adaptor with a non-routable IP address. Multiple Ethernet adaptors cannot be bonded together to present a single interface. This configuration requires the base license package #1 that is listed in MiCollab in LAN Mode (Server only) MiCollab in LAN Mode (Server only).

The following figure shows a MiCollab server in LAN mode connected to a supported Mitel communications platform.

Figure 5: MiCollab Server in LAN Mode



Important:

If you want to deploy the AWV application in LAN mode, appropriate port forwarding must be configured in the firewall, to enable external web conferencing and collaboration. If AWV is part of a bundle, but you are not deploying it, then this rule does not apply. For more information about AWV firewall settings, see Conferencing Firewall Settings (MiCollab in LAN Mode).

Note:

The Teleworker application in the MiCollab system on the LAN cannot be used to control teleworker phones.

4.5.1 Deploying Conferencing Clients with MiCollab in LAN Mode

AWV can operate behind a firewall on a private corporate network. The firewall must provide Network Address Translation (NAT) to allow external connections to AWV and to allow connections by external clients and Web browsers. The firewall must also provide NAT connections (originated by the MiCollab server) to external using a Domain Name System (DNS) server.

Consider the following when configuring AWV with two external IPs.

- AWV must be behind a firewall or router that allows port mapping.
- You must have two external IP addresses available for AWV.
- Have two domain names (or subdomains) available when using address translation.
    - External IP address 1, port 443 must be routed to Internal IP address 1 port 443.
    - External IP address 2, port 443 must be routed to Internal IP address 1 port 4443 (default).

Consider the following when configuring AWV with single external IP.

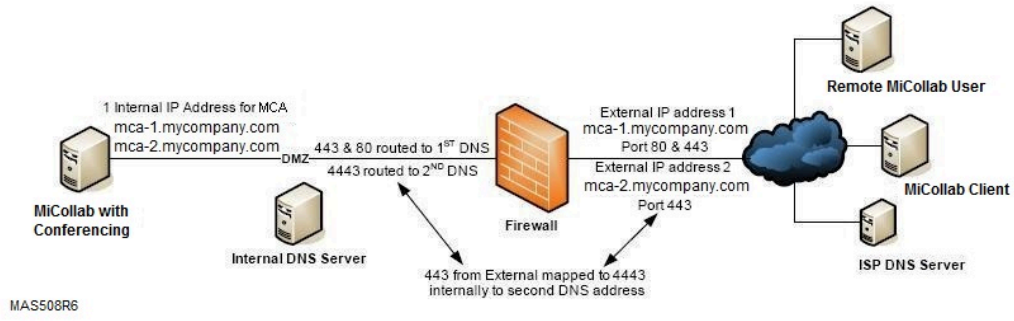
- AWV must be behind a firewall or router that allows port mapping.
- You must have one external IP address available for AWV.
- Have one domain name (or subdomain) available when using address translation.
    - External IP address, port 443 must be routed to Internal IP address 1 port 443.
    - External IP address, port 4443 must be routed to Internal IP address 1 port 4443 (default).

Note:

Ports 443 and 4443 are the default values in AWV. These port values are configured in the Web Conference Settings page of AWV. For single external IP, set the value to 4443 in external and internal port, when configuring Web Conference Settings.

In the following example with two external IPs, the firewall does not rewrite the source address. The DNS is split. Everyone uses the external name. Inside the firewall, it resolves to the internal address. Outside the firewall, it resolves to the external address. To configure this, set the MiCollab server name to the external name.

Figure 6: AWV Firewall Configuration



4.5.2 Deploying Secure Recording Connector Services with MiCollab in LAN Mode

Mitel Applications Suite supports Secure Recording Connector (SRC) services in the following deployment configurations:

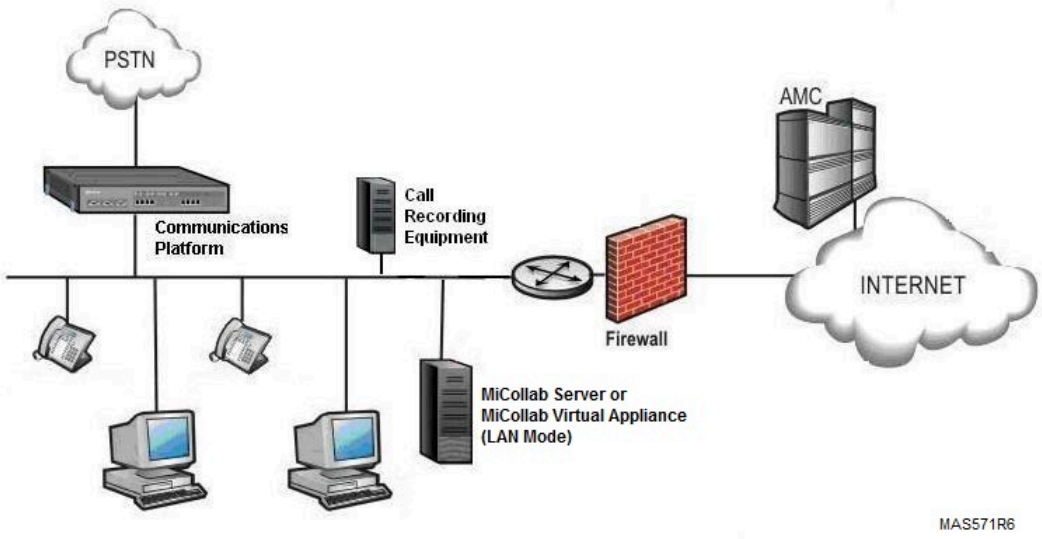
- MiCollab Server or MiCollab Virtual Appliance in LAN Mode
- MiCollab or MiCollab Virtual Appliance in LAN Mode ***with*** MBG Server in Network Gateway Mode
- MiCollab or MiCollab Virtual Appliance in LAN Mode ***with*** MBG Server in the DMZ

The Secure Recording Connector (SRC) service facilitates the recording of Mitel encrypted voice streams by third-party call recording equipment (CRE). The SRC service accepts requests from an authorized CRE to establish “taps” in the voice stream. These taps are separate (mirrored) streams from the SRC service to the call recording equipment.

4.5.2.1 MiCollab Server or MiCollab Virtual Appliance in LAN Mode

In this configuration, MiCollab is installed in LAN mode with the MiCollab Server Software Base Package #1 (PN 54005441) or MiCollab Virtual Appliance Software Base Package (PN 54005442). These packages include the MBG application. The MBG application on the MiCollab platform provides SRC services for the devices on the LAN only. SRC services are not supported for teleworker devices.

Figure 7: MiCollab Server or MiCollab Virtual Appliance with SRC in LAN Mode

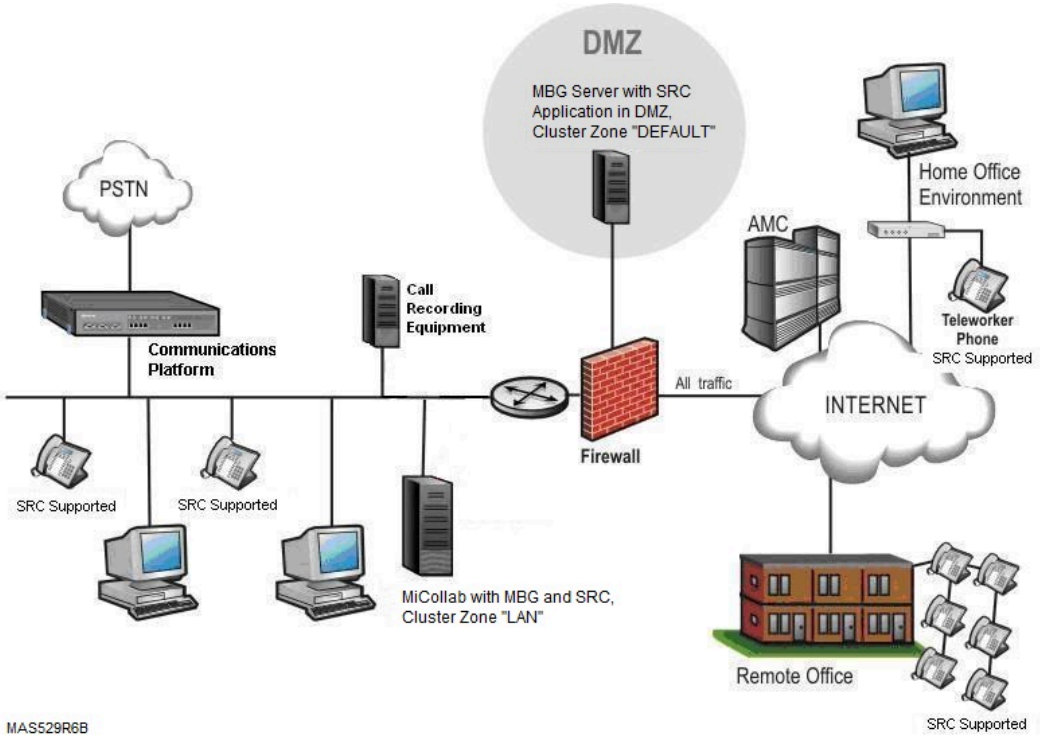


4.5.2.2 MiCollab Server or MiCollab Virtual Appliance in LAN Mode with MBG Server in DMZ

In this configuration, you deploy MiCollab or MiCollab Virtual Appliance in the LAN. A separate MBG server is installed in the DMZ. The teleworker and SRC licenses are shared with an MBG server in the DMZ. The MBG application on the MiCollab platform provides the SRC services for the LAN devices, and allows you to manage the teleworker devices that are supported by the MBG server in the DMZ.

The standalone MBG server in the DMZ provides the teleworker and SRC services for all WAN devices. Cluster zoning is used to minimize the teleworker and call recording licensing requirements on the LAN side. You must create a cluster and then divide it into two zones: MiCollab server in a “LAN” zone and MBG in the “Default” WAN zone, the teleworker and call recording licenses are shared between the MiCollab and MBG servers. The devices in the “LAN” zone each consume one call-recording license (when in use) but no teleworker licenses. Teleworker devices in the “Default” WAN zone each consume one Teleworker license, and if required one call recording license (when in use).

Figure 8: MiCollab/MiCollab Virtual Appliance with SRC in LAN Mode with MBG Server with SRC in DMZ



The following conditions apply to the configurations show in the above figure:

- These configurations are supported for both MiCollab Server and MiCollab Virtual Appliance deployments.
- The MiCollab server and MBG server must be running the same version of the MBG application.
- The MiCollab Server and MBG server must be joined in a cluster. When you create the MBG cluster, you must create a “LAN” zone and place the MiCollab server within it. The MBG server must be in a separate “Default” zone. Refer to *“Install MiCollab Server in LAN Mode with a MiVoice Border Gateway Server”* in the *MiCollab Installation and Maintenance Guide* for instructions on how to create the MiCollab-MBG cluster.
- Teleworker sets must be recorded on the MBG server. If you select the Teleworker option in MiCollab for a device, regardless of call recording option setting, the device is automatically placed in the Default cluster. If you do not select the teleworker option for a device, the device is automatically placed in the LAN cluster zone. Teleworker calls cannot be proxied through to the MBG application on the LAN.
- For the configuration shown the above figure:

  In the **MiVoice Border Gateway/Dashboard/Network profiles** tab of the MBG Server Manager interface, the Network Profile (streaming addresses) must be set to *“Server-only in DMZ”* mode.
- You must add teleworker devices through the MiCollab User and Provisioning application. If Teleworker devices are added to the system through the MBG application, the MiCollab database will not be updated with the set data. These orphan services consume call recording licenses and are counted and displayed in the MiCollab server manager licensing page.
- Refer to the MBG online help in the MiCollab Server Manager for instructions on how to provision devices with secure call recording.

4.5.3 MiCollab is not supported in the DMZ

Most of the applications available for MiCollab are designed to run on the LAN (except for Teleworker). For a summary of the supported applications, platforms, and deployment modes, see MiCollab in LAN Mode (Server only).

For this reason, MiCollab is not supported in the DMZ. Use the standalone MiVoice Border Gateway to deploy Teleworker in the DMZ for large sites.

For a complete listing of application Firewall port settings see MiCollab in LAN Mode Firewall Settings.

4.5.4 MiCollab in LAN Mode Firewall Settings

In LAN mode, firewall rules must be set up to allow communication between the applications, the AMC, the ICP, IP phones, and in some cases, the Internet.

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

Table 4: Conferencing Firewall Settings (MiCollab in LAN Mode)

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP22 (SSH)	Server → Internet	Allow outbound packets (and replies) on TCP port 22 between the MiCollab and the Internet to enable server registration, software and license key downloads, alerts and reporting.
TCP80 (HTTP)	Server ← Internet (IP Address 1) AND Server ← LAN	Allow inbound packets (and replies) on TCP port 80. Used for communication between Web server and Client.
TCP 443(default - port value is configurable in the Web Conference Settings page of AWV). (HTTPS)	Server ← Internet (IP Address 1) AND Server ← LAN	Remote server management and Web pages of AWV when set for SSL mode. If AWV is not set to SSL mode, this port should be closed or limited to specific hosts that have remote management capability.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 443 (HTTPS)	MiCollab Server → Internet Server → Internet	Used to send MiCollab Client Deployment tokens and the configuration download URLs to the Mitel redirect deployment servers. Used to connect with Mitel's Cloud-based MiTeam solution located on the Internet. The MiCollab server requires bi-directional access to the MiTeam solution on the Internet at the following top-level MiTeam FQDNs: miteam.micloudoffice.com and api.micloudoffice.com. Because Internet access is required, MiTeam is not available to Dark Data Centers. Note that in a private cloud these FQDNs will be different.
TCP 4443(default-port value is configurable in the Web Conference Settings page of AWV)	Server ← LAN	Allow outbound packets and replies from internal users and port 4443. Used between internal users for Web conferencing.
	Server ← Internet (IP Address 2)	Allow outbound packets and replies from external users on port 443 (default is 443, for single IP allow outbound packets on TCP port 4443 or configured internal port) and redirects them to port 4443 on the server. Used between external users for Web conferencing.

Table 5: NP-UM Firewall Settings (MiCollab in LAN Mode)

PORT RANGE	DIRECT	PURPOSE & DETAILS
TCP 22 (SSH)	Server → Internet	**AMC communications**. Allow outbound packets (and replies) on TCP port 22 between the MSL Server and the Internet to enable server registration, software and license key downloads, alerts and reporting.
UDP 53 (DNS)	Server → Internet	**Domain Name System**. The server requires DNS to look up the IP address of the Mitel AMC. 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)	Server → Internet Server → Internet	**Mobile Client Deployment**: Used to send deployment tokens and the configuration download URLs to the Mitel redirect deployment servers. **MiTeam Integration**: Used to connect with Mitel's Cloud-based MiTeam solution located on the Internet.
TCP 443 (HTTPS)	Server ← Internet	**Remote Server Management**. *(Optional)* Allow inbound and outbound packets on TCP port 443 between the MSL Server and the Internet to allow remote management of the server, if required. HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface.

Table 6: MiCollab Client Firewall Settings (MiCollab in LAN Mode)

PORT RANGE	DIRECTION	PURPOSE & DETAILS
MiCollab Server		

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 22 (SSH)	Server → Internet	**AMC communications**. Allow outbound packets (and replies) on TCP port 22 between the MiCollab Server and the Internet to enable server registration, software and license key downloads, alerts and reporting.
TCP 80 (HTTP) and 443(HTTPS)	Server ← LAN	Web services interface
TCP 5060	Server ←→ Internet Server ←→ ICPs	**SIP TCP Support**. Open this port for SIP signaling over TCP between the server and remote SIP devices that use TCP on port 5060. This port may also be opened between the server and the ICPs.
TCP 5061	←→ Internet Server ←→ ICPs	**SIP TCP/TLS Support**. This port is required for SIP signaling between the server and remote SIP devices that have been configured to use TCP/TLS on port 5061 (the default client configuration). This port may also be opened between the server and the ICPs.
TCP 6800, 6801, and 6802	ICP(s) ← LAN	MiNET
MBG 6801, 6802	ICPs ← Internet	MiNET
UDP 50000 to 50511	ICP(s) ← Internet ICP(s) → Internet	Voice (not on server).
UDP 20000 to 30999	MBG ← Internet MBG → Internet	Voice

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 389	Server → LAN	LDAP
TCP 636	Server ← LAN	LDAP
TCP 36008 (SSL)	Server → Internet	Websocket proxy. This connection is used by the MiCollab Client Mobile clients for real-time notifications.
TCP 443 (HTTPS)	MiCollab Server → Internet MiCollab Server → Internet	**Mobile Client Deployment**. Used to send deployment tokens and the configuration download URLs to the Mitel redirect deployment servers. **MiTeam Integration**: Used to connect with Mitel's Cloud-based MiTeam solution located on the Internet.
MBG Server		
TCP 443	MBG Server ← Internet	MiXML
TCP 36008	MBG Server ← Internet	Websocket proxy
TCP 36007	MBG Server ← Internet	SIP
TCP 36006	MBG Server ← Internet	HTTP (NuPoint)
TCP 36005	MBG Server ← Internet	HTTP

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 6801 and 6802	MBG Server ← Internet	Secure MiNET
UDP 20000 to 309999	MBG Server ← Internet MBG Server → Internet	Voice
UDP 50098 to 50508	MBG Server ← Internet MBG Server → Internet	Voice

4.6 Network Edge Deployments for MiVoice Business/Office 250

The deployment configurations described in this section are supported for MiVoice Business or MiVoice Office 250 platforms only. They are not supported for MiVoice Office 400, MiVoice MX-ONE, or MiVoice 5000 platforms.

There are two network edge deployment variants:

- **MiCollab in LAN Mode with MBG and Web Proxy Server in Network Edge Mode**: This configuration has MiCollab located in the Local Area Network (LAN) connected to a second MBG server on the network edge (see Figure 9).
- **MiCollab in Network Edge Mode (Server Gateway)**: In this configuration, MiCollab is installed on an internet-facing server with firewall capability (see page 18). This configuration supports all MiCollab applications and uses MSL firewall with preconfigured filtering and port forwarding to secure the LAN.

The above deployment configurations can also support SIP trunking and Secure Recording Connector services. SIP trunking is supported by the MBG application installed on the MBG server in the Network Edge or on the MiCollab server in the Network Edge. SRC is only supported for sets on the LAN.

Note:
Call Recording of TW sets is supported. MiVCR would connect to the MBG in the DMZ and the MBG on the MiCollab MBG on the LAN.

The following tables summarize the deployment configurations and required licenses:

Table 7: MiCollab in Network Edge Mode

Licensed Software Package	License Components	Platform	
		MiVoice Business	MiVoice Office 250
#1 MiCollab Software Base PN 54005441 Or #1 Virtual MiCollab Software BasePN 54005442	NP-UM	Yes	Yes
	SAA	Yes	No
	MiCollab AWV	Yes	Yes
	MiCollab Client	Yes	Yes
	MBG Teleworker Service	Yes	Yes
	MBG Secure Recording Connector	Yes	No
	SIP Trunking Service	Yes	Yes
#2 MiCollab Client Add-on PN 54005445	MiCollab Client	Yes	Yes

4.6.1 MBG Teleworker with Web Proxy

To support Teleworkers use one of the following configurations:

- MiCollab in LAN Mode (server-only) with Web Proxy on a second MBG server in the DMZ,
- MiCollab in LAN Mode with Web Proxy on a second MBG server on the network edge, or
- MiCollab in Network Edge Mode with MiVoice Border Gateway (MBG) on the same server. See Figure 10 for an example.

Note:
The MBG Web Proxy is not supported directly on a MiCollab server or a MiCollab Virtual Appliance deployment in either LAN mode or Network Edge mode.

An MBG server with web proxy installed in the Demilitarized Zone (DMZ) or on the network edge protects the MiCollab in the LAN from Internet exposure. In a DMZ configuration, as shown in Figure 1, the firewall is the gateway for all IP network traffic with the internet. In a Network Edge configuration, as shown in Figure 9, the MBG server acts as a firewall/gateway for the MiCollab applications. See Firewall Config for MiCollab in LAN with Web Proxy for details. See the MBG with Web Proxy documentation on the Mitel Customer documentation site for MBG configuration details.

These configurations provide a secure method for remote web browser users to connect with a MiCollab system located on the corporate LAN. Remote web browser users connect to MiCollab in the LAN through the Web Proxy.

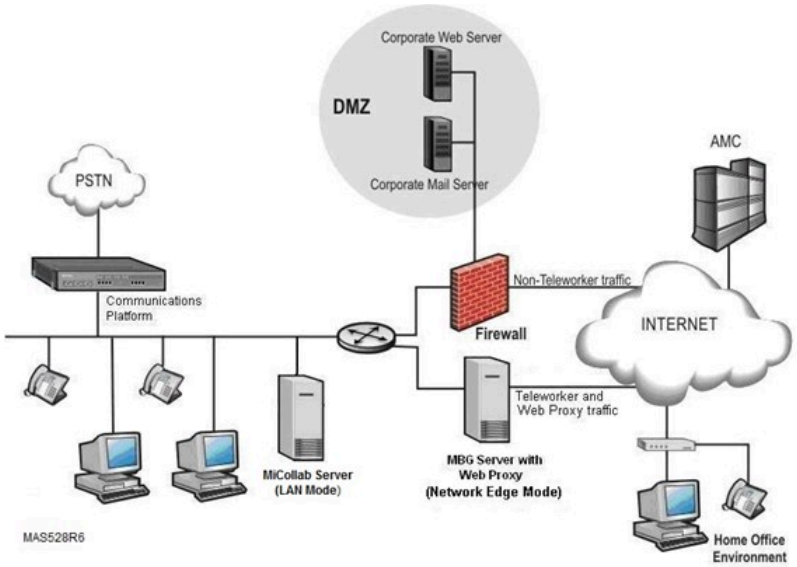


Figure 9: MiCollab in LAN Mode with MBG and Web Proxy in Network Edge Mode

4.6.2 MiCollab in Network Edge Mode (Server-Gateway)

Network Edge (Server-Gateway) mode can be used to deploy any of the MiCollab applications. In this mode, MiCollab must have direct Internet access, which is required by the MBG Teleworker and MiCollab Client applications. If there is no requirement for these applications, the preferred deployment is to have MiCollab in LAN (Server-only) mode on the corporate LAN behind a firewall.

Network Edge (Server-Gateway) mode requires two Ethernet adaptors. One adapter is configured as "Local" for connection to the local network, and one is configured as "WAN" for connection to the Internet. The WAN network adapter has a publicly-routable IP address; accessible to both the Internet and the internal network (that is, the server should not reside behind a NAT device). This configuration requires base license package #1.

Figure 10illustrates the preferred deployment of MiCollab server on the Network Edge. MiCollab is used in conjunction with the corporate firewall. The MiCollab system acts as a firewall/gateway for MiCollab applications while the corporate firewall controls business data traffic. If your voice/telephony network and your data network are separate, the MiCollab Local network adapter should be directly on the voice/telephony network as the MiCollab applications are performing telephony functions.

Note:

When using teleworker in conjunction with LAN-facing applications, customers must ensure that they review the configuration in relation to their corporate security policy. Some customers may choose to deploy teleworker on a separate server in their DMZ.

Note:

Although, MiCollab Client is supported in a Network Edge (server gateway) mode, it should never be directly connected to the Internet. The MiCollab server should always be isolated from the Internet by an MBG and/or a properly configured firewall.

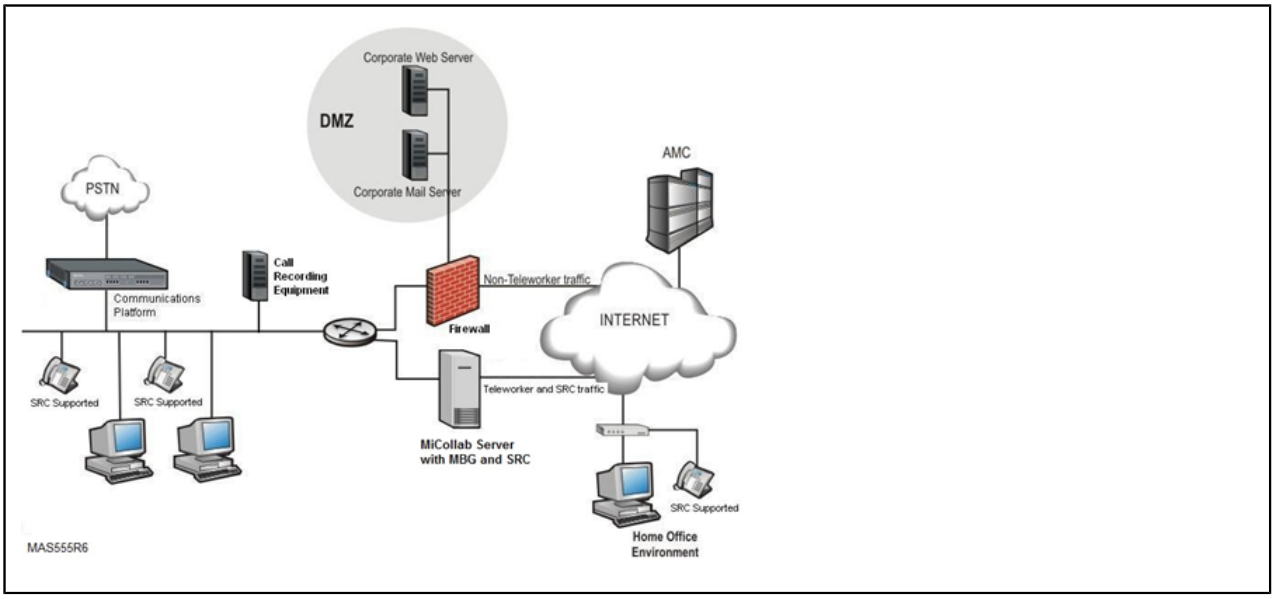


Figure 10: MiCollab Server in Network Edge (Server-Gateway) with LAN Firewall

Figure 11illustrates the preferred deployment of MiCollab Virtual Appliance on the Network Edge.

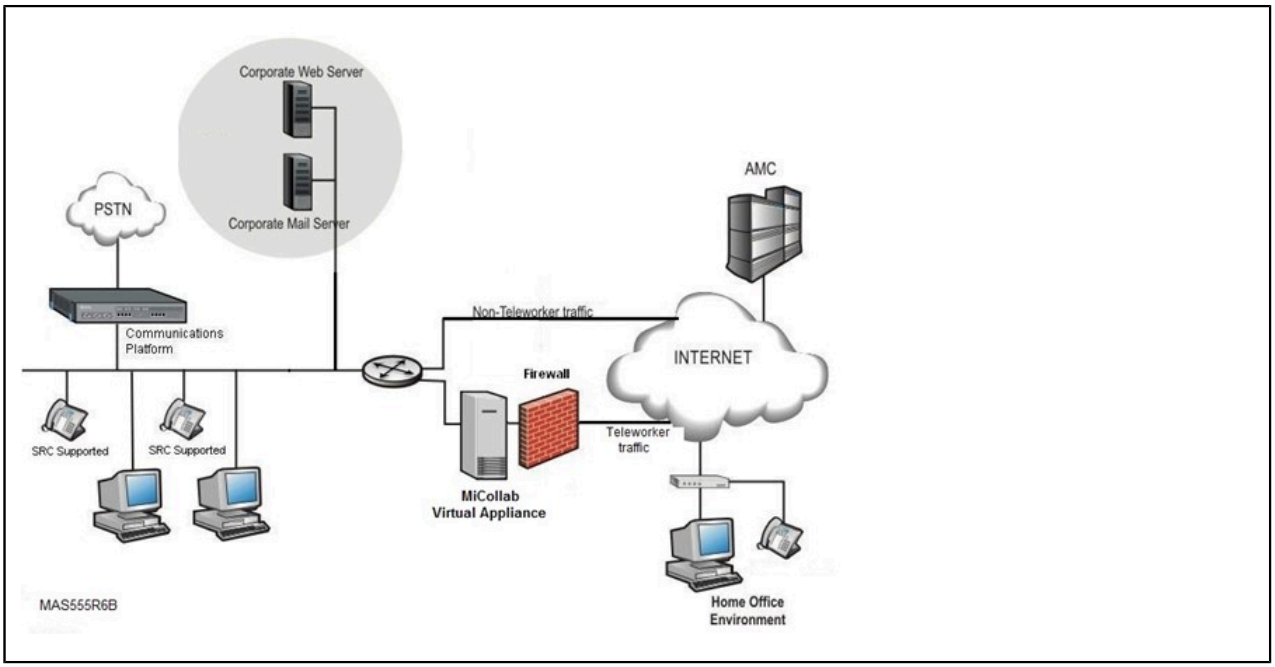


Figure 11: MiCollab Virtual Appliance in Network Edge (Server-Gateway) with LAN Firewall

4.6.3 Security Considerations

Network Edge deployment implies certain security considerations that may not be amenable to all customers. For such customers, a two-server configuration may be more in line with their IT network security policies.

Figure 12 illustrates another example of Network Edge (Server-Gateway) mode. MiCollab is used as the corporate firewall.

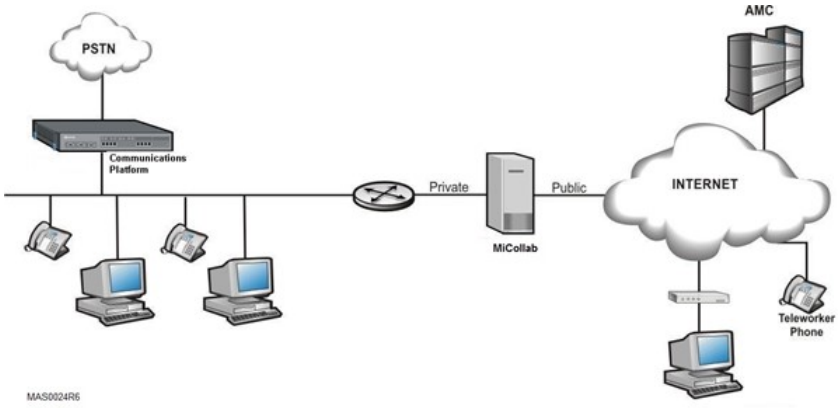


Figure 12: Network Edge (Server-Gateway) Configuration Example

4.6.4 Deploying AWV Clients in Network Edge Mode

To deploy MiCollab in Network Edge mode with conferencing, there are two different configuration methods for providing access to the AWV application (installed on the MiCollab Server) from outside of the customer firewall. Previous software releases required the use of two external IP addresses, however with MiCollab Release 8.0, it is now possible to use a single external IP address.

Configuration with two external IPs

Using two external IP is the default option. Obtain two external IP addresses from your Internet Service Provider (ISP). These IP addresses are used for the AWV web server interface and the conference functions. In Network Edge mode, the MiCollab server resides on the network edge between the LAN and the Internet. The MSL firewall is located on MiCollab between the LAN and the Internet and is pre-configured to port forward from the second external alias IP address (conference functions) to the first external alias IP address (AWV service).

You enter the two external IP address for the WAN adapters when you configure MSL operating system on the MiCollab server. Refer to the *MiCollab Installation and Maintenance Guide* for instructions.

Within the AWV settings, the External port is configured with 443. This directs the external clients to reach the Connection Point using port 443. The result is, the connection to both server components from external locations will request that they are to be reached on port 443. The user must have the outbound traffic enabled for the CP port 4443 when sitting behind a firewall. For example, inside corporate LAN.

Configuration with single external IP

In the AWV configuration with one external IP address, the External Port is configured with 4443. This directs the external clients to reach the Connection Point using port 4443. The result is, the connection to the web conferencing portal will be requested on port 443, and the connection to the Connection Point component will be requested on port 4443.

Because two different ports are used, one External IP address can be used for both components.

4.6.5 Deploying MiCollab Client on a MiCollab Platform in Network Edge Mode

MiCollab mobile clients make use of a websocket connection to MiCollab to support real-time notifications of missed calls and other events. To enable this functionality, a persistent connection is made from the device via TCP port 36008 to the MiCollab on the Network Edge. Ensure that TCP/36008 is allowed to pass through the corporate firewall, if applicable.

The following Collaboration ports are accessible via the WAN interface when MiCollab is deployed in Network Edge mode (server-gateway):

TCP/80 – HTTP (default with MSL)

TCP/443 – HTTPS (default with MSL)

TCP/5060 – SIP proxy and TCP/80 (HTTP) are used by internal MiCollab Client PC clients (on the LAN) to connect to the MiCollab Server

or

TCP/36005-TCP/36007 are used by external MiCollab PC clients (teleworkers on the intranet) to connect to the MBG service that is configured on the MiCollab Server

TCP/5061 – TLS (default port used by the MiCollab Mobile Client)

TCP/36008 – Web socket proxy (required for mobile phone, for example Android Client).

Note:

To support Teleworker MiCollab Client clients, MBG service must be configured on the MiCollab in Network Edge mode.

Note:

For MiCollab Client for iOS users with a softphone, ensure that the softphone is deployed correctly to avoid one-way audio conditions. In the Client Deployment profile, set the MBG SIP host to a FQDN which always resolves to the public IP address of the server (and not the LAN IP Address), or WAN IP address. If MBG SIP host is not set to the server hostname, the new FQDN needs to be added in **Allowed URI names** in MBG (**System Configuration** > **Settings** > **SIP options**). For more information, see *MiCollab Client Deployment Online Help*.

Figure 13 shows the port usage for the MiCollab Client application when MiCollab is deployed in Network Edge Mode. Refer to Table 8 for a description of the port usage and firewall settings.

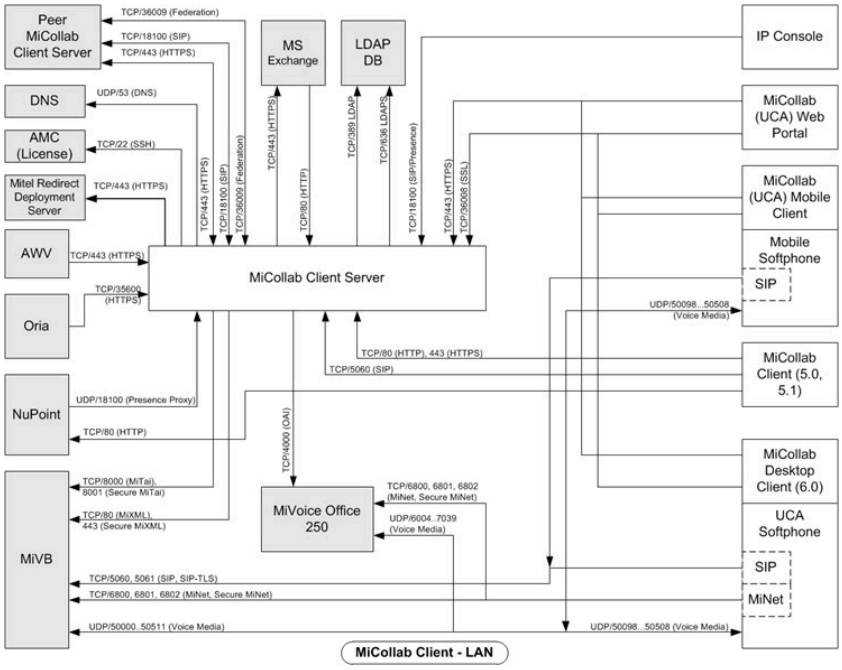


Figure 13: MiCollab Client Port Usage for MiCollab in Network Edge Mode

4.6.6 MiVoice Border Gateway Application as Internet Gateway

You can deploy the MiCollab server with the MiVoice Border Gateway application as the Internet gateway and firewall. The following figure shows an example of this configuration using the MiVoice Border Gateway application and a MiVoice Business.

MBG requires two network interfaces and two addresses for this configuration. The external address must:

1. Be a static address that does not change
2. Be directly attached to a NIC on the MSL server
3. Be reachable from the public network/Internet
4. Be reachable from the internal network/LAN
5. Not be subject to NAT or behind another firewall

The interface may be configured via DHCP, PPPoA, PPPoE, or similar technology, but the address it receives must always be the same.

Note:

Warning: If the external address changes, all teleworker phones must be reprogrammed with the new address.

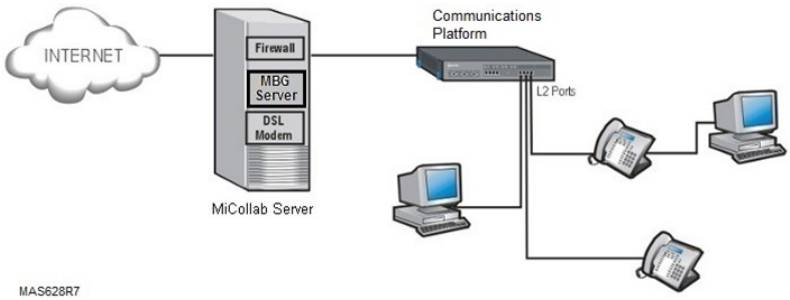


Figure 14: MBG Application as Internet Gateway (No Enterprise Firewall)

An enterprise can take advantage of the DSL, authenticated DHCP, and PPPoE/PPPoA capabilities of the MSL server. MSL additionally provides NAT for all devices at the enterprise, a stateful packet filter firewall, and optional port-forwarding.

Note:

PPPoA support is limited in the current release. Mitel UK Product Support recommends the use of a D-Link DSL 300T modem at the enterprise site if PPPoA connectivity is required in gateway mode. Configure the modem to provide DHCP on the internal interface, and use DHCP on the MiCollab server to configure the public interface. The modem acts as a bridge. PPPoA routers that provide NAT will not work here.

4.6.7 Additional Local Networks

Additional internal networks or subnets that require access to the MiVoice Border Gateway application can be added via the *Local Networks* panel of the server manager. This access can be limited to individual hosts, or large network blocks can be used. In all cases, the *Router* property should be set to the address of the router on the subnet attached to the MSL server's internal interface.

For example, to allow access from the single subnet 192.168.12.0/24, you would enter a network of 192.168.12.0 and a mask of 255.255.255.0 in the *Local Networks* panel, plus the address of the router on the local subnet through which this network can be reached.

If the customer’s network has multiple subnets with a common prefix, access can be allowed from the prefix. For example, if the customer uses various subnets within the 192.168.0.0/16 network, enter a network of 192.168.0.0 and mask of 255.255.0.0 in the *Local Networks* panel, and allow the local router to determine the routing to the individual subnets.

Note:

Warning: It is worth noting that unless these networks are added via the Local networks panel, the MBG server may be unable to route traffic to those networks. The local networks configuration serves as both application access control and as static routing configuration.

Note:

Local Networks is a feature of MSL. Refer to the MSL documentation for a full description of its capabilities.

4.6.8 Firewall Configuration

In Network Edge (Server-Gateway) mode, MiCollab automatically sets the firewall configuration. This configuration is automatic in the Network Edge deployment. Hence, the information in this section is for reference only.

Table 8: AWV Firewall Settings (MiCollab in Network Edge Mode)

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 22 (SSH)	MiCollab Server → Internet	**AMC Communication**. Allow outbound packets (and replies) on TCP port 22 between the MiCollab Server and the Internet to enable AMC communications (i.e., enable server registration, software and license key downloads, alerts and reporting).
TCP80 (HTTP)	MiCollab Server ← Internet	**Web Browser Access**. Allow inbound packets (and replies) on TCP port 80. Used for communication between MiCollab server and Web browser.
TCP 443 (default - port value is configurable in the Web Conference Settings page of AWV). (HTTPS)	Server ← Internet Server → Internet Server ← LAN	**Web Browser Access**: Allow inbound packets (and replies) for AWV web pages when set for SSL mode. If AWV is not set to SSL mode, this port should be closed or limited to specific hosts. **MiTeam Classic Integration**: Used to connect with Mitel's Cloud-based MiTeam Classic solution located on the Internet.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 4443 (default – port value is configurable in the Web Conference Settings page of AWV)	Server ← LAN	Allow outbound packets and replies from internal users and port 4443. Used between internal users for Web conferencing
	Server ← Internet	Allow outbound packets and replies from external users on port 443 (default is 443, for single IP allow outbound packets on TCP port 4443 or configured port) and redirects them to port 4443 on the server. Used between external users for Web conferencing.
UDP 5060 UDP 6060	SIP phone ← # → #MiVoice Business SIP phone ← # → #SIP Gateway in MiCollab Server to MiVoice Office 250	By default for UDP connections, the MiVoice Business ICP listens on port 5060. The MiVoice Office 250 listens to a SIP gateway running on the MiCollab box using port 6060. AWV SIP phones are configured to use the same port. Refer to the communication platform documentation for configuring these ports.
UDP 12000 - 12600 (RTP)	SIP Phone ←→ ICP	MiVoice Business ICP SIP phone default port range.

Table 9: Teleworker Firewall Settings (MiCollab in Network Edge Mode)

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 22 (SSH)	MiCollab Server → Internet	**AMC communications.** Allow outbound packets (and replies) on TCP port 22 between the MiCollab Server and the Internet to enable server registration, software and license key downloads, alerts and reporting.
UDP 53 (DNS)	MiCollab Server → Internet	**Domain Name System.** The server requires DNS to look up the IP address of the Mitel AMC. 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)	MiCollab Server → Internet	**Remote Server Management**. *(Optional)* Allow inbound and outbound packets on TCP port 443 between the MiCollab Server and the Internet to allow remote management of the server, if required.HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 443 (HTTPS)	MiCollab Server ← LAN	**Local Server Management**. Allow inbound and outbound packets on TCP port 443 between the MiCollab Server and the LAN to allow for management of the server.HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface. **The firewall should be configured to limit HTTPS access to desired management hosts.**
TCP 6800, 6801 and 6802 TCP 6801 and 6802	MiCollab Server → LAN MiCollab Server → ICP(s) MiCollab Server ← Internet	**MiNET Call Control.** Allow incoming and outgoing packets for TCP ports 6801 (MiNET-SSL) and 6802 (MiNET-Secure V1) between the MiCollab server and the Internet. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNET), 6801 and 6802 between the server and the LAN and the server and the ICP(s). The LAN rule can be omitted if there are no IP sets on the LAN, but ensure that the ICP(s) can communicate with the server's **public** address.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 3998 and 6881	MiCollab Server ← Internet	**SAC Connection Support.** Allow incoming TCP on ports 3998 and 6881 to support the applications and the web browsing, respectively, on the 5235, 5330, 5340, 5360 type sets, from the Internet to the MiCollab server. There is an additional LAN rule below that follows this rule to complete the support.
TCP 3998, 3999 and 6881	MiCollab Server → ICP(s)	**SAC Connection Support.** Allow bi-directional TCP traffic on port 3999 to the ICP(s). This is to support the applications on the 5235, 5330, 5340, 5360 type sets. **Note**: 3998 and 6881 are dependent on an additional, internal MBG server that the Internet-facing MiCollab server is daisy-chained to.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 80	MiCollab Server → LANMiCollab Server → Internet	**SAC Connection Support (Optional).** Allow TCP port 80 from the server to the internet, and to the LAN, to support web browsing on the 5235, 5330, 5340, 5360 type sets. Also required to the Internet to allow browsing of the Internet from the set.
TCP 6881	Internet → MiCollab Server	**MiNET MiVoice 69xx Avatar support.** Allow incoming TCP from the Internet to the MiCollab server on port 6881 to support avatars on MiVoice 6920, 6930, 6940 phones
TCP 80	MiCollab Server ← MBG Server	**MiNET MiVoice 69xx Avatar support.** Allow MBG to connect to the MiCollab server to retrieve avatars for MiVoice 6920, 6930, 6940 Phones. (Optional).
UDP 20,000 to configured upper bound* (SRTP)	MiCollab Server ← Internet MiCollab Server ← LAN	**Voice Communications.** Allow incoming SRTP on UDP ports 20000 – configured upper bound* from all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
UDP 1024 to 65,535 (RTP)	MiCollab Server → LAN MiCollab Server → Internet	**Voice Communications.** Allow outgoing SRTP on UDP ports greater than, or equal to, 1024 from the server to all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.
TCP MiVoice Business (VFA)	MiCollab Server ← Internet MiCollab Server ←→ LAN	**Optional VoiceFirst Communications.** Allow bi-directional traffic on TCP port MiVoice Business if you have a VoiceFirst Solution installed.
TCP 2114	MiCollab Server ←→ LAN MiCollab Server ← Internet	**MiCollab Client Support.** To permit the client to connect to the logon server on the LAN side, this port must be permitted. Failure to do so will result in the client being unable to logon via their client.
TCP 2116	MiCollab Server ←→ LAN MiCollab Server ← Internet	**MiCollab Client Support.** To permit the client to connect to the telephony server on the LAN side, this port must be permitted. Failure to do so will result in the client being unable to control their set via the Mitel ICP.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 35000	MiCollab Server ←→ LAN MiCollab Server ← Internet	**MiCollab Client Support.** To permit the client to connect to the presence server on the LAN side, this port must be permitted. Failure to do so will result in the presence features in MiCollab Client failing to function.
TCP 37000	MiCollab Server ←→ LAN MiCollab Server ← Internet	**MiCollab Client Support.** To permit the client to connect to the collaboration server on the LAN side, this port must be permitted. Failure to do so will result in the collaboration features in MiCollab Client failing to function.
UDP 5060	MiCollab Server ←→ LAN MiCollab Server ←→ Internet	**SIP Support.** If the SIP connector is enabled, then this port is required for SIP signaling between Teleworker and the set, and Teleworker and the ICP.
TCP 5060	MiCollab Server ←→ Internet Server ←→ ICPs	**SIP TCP Support**. Open this port for SIP signaling over TCP between the server and remote SIP devices that use TCP on port 5060. This port may also be opened between the server and the ICPs.

PORT RANGE	DIRECTION	PURPOSE AND DETAILS
TCP 5061	MiCollab Server ←→ Internet MiCollab Server ←→ ICPs	**SIP TCP/TLS Support**. This port is required for SIP signaling between the server and remote SIP devices that have been configured to use TCP/TLS on port 5061 (the default client configuration). This port may also be opened between the server and the ICPs.
TCP 6806	Internet → MiCollab Server	**IP Console Support**. Open TCP port 6806 to support presence status updates.
TCP 6807	Internet → MiCollab Server	**IP Console and MiVoice Business Console Support**. Open TCP port 6807 to support presence status updates.

* Configured upper bound for SRTP on UDP ports is controlled by a setting in the Teleworker Solution Advanced panel. You must reserve four ports per set that you wish to support. Thus, to support 1000 sets, 4000 ports are required, from 20000 to 24000, and those ports must be open in the firewall configuration of any firewall that the Teleworker server is installed behind.

Table 10: NP-UM Firewall Settings (MiCollab in Network Edge Mode)

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 22 (SSH)	Server → Internet	**AMC communications.** Allow outbound packets (and replies) on TCP port 22 between the MiCollab Server and the Internet to enable server registration, software and license key downloads, alerts and reporting.
UDP 53 (DNS)	Server → Internet	**Domain Name System.** The server requires DNS to look up the IP address of the Mitel AMC. Alternatively, the MiCollab 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)	Server ← Internet	Remote Server Management. *(Optional)* Allow inbound and outbound packets on TCP port 443 between the MiCollab Server and the Internet to allow remote management of the server, if required. HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface.

PORT RANGE	DIRECTION	PURPOSE & DETAILS
TCP 443 (HTTPS)	Server ← LAN	**Local Server Management**. Allow inbound and outbound packets on TCP port 443 between the MiCollab Server and the LAN to allow for management of the server.HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface. **The firewall should be configured to limit HTTPS access to desired management hosts.**
TCP 6800, 6801 and 6802	Server → LAN Server → ICP(s)	**MiNET Call Control.** Allow incoming and outgoing packets for TCP ports 6801 (MiNET-SSL) and 6802 (MiNET-Secure V1) between the server and the Internet. Allow incoming and outgoing packets for TCP ports 6800 (unencrypted MiNET), 6801 and 6802 between the server and the LAN and the server and the ICP(s). The LAN rule can be omitted if there are no IP sets on the LAN, but ensure that the ICP(s) can communicate with the server's **public** address.

PORT RANGE	DIRECTION	PURPOSE & DETAILS
UDP 20,000 to configured upper bound* (SRTP)	Server ← Internet Server ← LAN	**Voice Communications.** Allow incoming SRTP on UDP ports 20000 – configured upper bound* from all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.
UDP 1024 to 65,535 (RTP)	Server → LAN	**Voice Communications.** Allow outgoing SRTP on UDP ports greater than, or equal to, 1024 from the server to all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.
TCP 8001	Server → LAN Server → ICP(s)	**MiTAI.** API used by applications to monitor phone activities and invoke 3rd party call control.

Table 11: MiCollab Client Firewall Settings (MiCollab in Network Edge Mode)

Port Range	Direction	Purpose & Details
MiCollab Server		

Port Range	Direction	Purpose & Details
TCP 22 (SSH)	Server → Internet	**AMC communications.** Allow outbound packets (and replies) on TCP port 22 between MiCollab and the Internet to enable server registration, software and license key downloads, alerts and reporting.
TCP 8000 and 8001	Server → LAN	MiTAI
TCP 80 (HTTP) and 443 (HTTPS)	Server ← LAN	Web Services Interface

Port Range	Direction	Purpose & Details
TCP 443 (HTTPS)	Server → Internet Server → Internet	**Mobile Client Deployment**. Used to send deployment tokens and the configuration download URLs to the Mitel redirect deployment servers. **MiTeam Classic Integration**: Used to connect with Mitel's Cloud-based MiTeam Classic solution located on the Internet. The MiCollab server requires bi-directional access to the MiTeam Classic solution on the Internet at the following top-level MiTeam Classic FQDNs: miteam.micloudoffice.com and api.micloudoffice.com. Because Internet access is required, MiTeam Classic is not available to Dark Data Centers. Note that in a private cloud these FQDNs will be different**.**
TCP 5060	Server ←→ Internet Server ←→ ICPs	**SIP TCP Support**. Open this port for SIP signaling over TCP between the server and remote SIP devices that use TCP on port 5060. This port may also be opened between the server and the ICPs.

Port Range	Direction	Purpose & Details
TCP 5061	Server ←→ Internet Server ←→ ICPs	**SIP TCP/TLS Support**. This port is required for SIP signaling between the server and remote SIP devices that have been configured to use TCP/TLS on port 5061 (the default client configuration). This port may also be opened between the server and the ICPs.
TCP 6800, 6801, and 6802	ICP(s) ← Internet	MiNET
UDP 50000 to 50511	ICP(s) ← Internet ICP(s) → Internet	Voice
UDP 50098 to 50508	ICP(s) ← LAN ICP(s) → LAN	Voice (MiCollab Client)
TCP 389	Server → LAN	LDAP
TCP 636	Server → LAN	LDAPs
TCP 36008 (SSL)	Server ← Internet	Websocket proxy. This connection is used by the Collaboration Mobile clients for real-time notifications.

System Requirements 5

This chapter contains the following sections:

5.1 Supported Communications Platforms

MiCollab is supported for the following Mitel communications platforms:

- MiVoice Business
- MiVoice Business for Industry Standard Servers
- MiVoice Business VMware Virtual Appliance
- MiVoice Office 250
- MiVoice Office 400
- MiVoice 5000
- MiVoice MX-ONE

The following table identifies the maximum number of communication platforms or users supported by a MiCollab system.

Table 12: Maximum Number of Supported Platforms

COMMUNICATIONS PLATFORM	CONFIGURATION	MAXIMUM NUMBER OF PLATFORMS SUPPORTED
MiVoice Business	With NP-UM application	NP-UM application is limited to four IP-connected MiVoice Business platforms.

	With applications not including NP-UM	Limited only by the number of users supported by the MiCollab system.
MiVoice Office 250	Any supported configuration	Maximum of 99 networked MiVoice Office 250 platforms (see **Note**).
MiVoice Office 400	The only supported configuration is a single MiVoice Office 400 or Advanced Integrated Network (AIN) with a single MiCollab server in the same network.	Single MiCollab with single MiVoice Office 400 platform.
MiVoice 5000	Any supported configuration **Note**: Each connection to the CSTA Proxy Service allows up to 2048 devices to be monitored. In order to exceed this number, additional PBX links are required. For example, to reach 5,000 devices, three links are required.	One MiCollab supports site configurations with one or more MiVoice 5000 systems up to the MiCollab platform user capacity. Note that a mix of different types of communications platforms (for example MiVoice 5000 and MiVoice Business) is not supported.

MiVoice MX-ONE	Any supported configuration up to 5000 users and 10,000 devices.	One MiCollab supports site configurations with one or more MiVoice MX-ONE systems up to the MiCollab platform user capacity. Note that a mix of different types of communications is not supported.

Note:

The MiVoice Office 250 supports up to 250 IP phone users (endpoints). To support a greater number of IP users, you can network up to 99 MiVoice Office 250s. You can connect the MiCollab system directly to a single MiVoice Office 250. However, to support a network of MiVoice Office 250s, you must connect the MiCollab system to the network through a MiVoice Office 250 Gateway.

5.2 Hardware

MiCollab is supported on the following platforms:

- MiCollab Server (third-party manufacturer server platform)
- MiCollab Server Appliance (turnkey hardware platform shipped from Mitel Networks)
- MiCollab Virtual Appliance (deployed as virtual machine)

5.2.1 MiCollab Server Platform

MiCollab runs on the Mitel Standard Linux (MSL) operating system.

Note the following conditions:

- MiCollab Release 7.2 and later is only supported on 64-bit server architecture. To upgrade MiCollab Release 6.0 and earlier systems to MiCollab Release 7.2 software or later, you must re-install the system software on a 64-bit server platform and restore a database backup.
- The MiCollab Server Appliance requires 6 GB of RAM to run all supported applications. The MiCollab Server Appliance is shipped with 8 GB of RAM.
- 2500-user systems require 8 GB of RAM and six cores.
- 5000-user systems require 16 GB of RAM and eight cores.

- Applications that require serial ports (such as NP-UM PMS and ESMDI) are not supported.
- Your server model may require modifications to the BIOS settings.
- For hardware platforms with two hard drives, do not change BIOS settings from the default RAID1 setting. (RAID 0 (striping) is not supported.)
- NuPoint Unified Messaging is supported on mid-range servers if you deploy it as part of MiCollab.

5.2.2 MiCollab Server Appliance

Refer to the *MiCollab Installation and Maintenance Guide* for the MiCollab Server Appliance specifications.

5.2.3 MiCollab Virtual Appliance Platform

MiCollab Virtual Appliance consists of hardware-independent MSL operating software and application software running within a virtual machine that encapsulates both MSL and MiCollab. You can deploy the MiCollab Virtual Appliance in a supported virtual environment. Refer to the Virtual Appliance Deployment Guide for the virtual environment requirements.

5.3 Supported USB Memory Sticks

You can install MiCollab application software from a USB memory stick. The memory stick must have at least 8 GB of memory to support the installation of all applications. You can also perform MiCollab database backups to USB memory stick. The USB memory stick connects directly to a USB port on the MiCollab server. If manual verification of the MiCollab database backup file fails, we suggest that you try a different brand of USB stick. Our testing has determined that some USB memory sticks do not function consistently with the MiCollab backup option. (For example, the Verbatim, GXT, and brands consistently work well, but the Lexar brand does not.) For more information about backup verification, see the *Maintenance chapter of the MiCollab Installation and Maintenance Guide.*

5.4 Software

Table 13: Minimum MiCollab Rel 8.1 Server Platform Software Requirements

Item	Minimum Requirement
Web Browser	Microsoft Edge 20, Internet Explorer Release 10 or 11, Google Chrome version 46 or higher, or Mozilla Firefox 41 or higher
Mitel Standard Linux	Release 10.5 (64-bit only)
Communications platform	MiVoice Business Release 6.0 SP3 or higher (with Single Point Provisioning)MiVoice Business Release 7.2 or higher (with Flow Through Provisioning)MiVoice Office 250 Release 6.2 SP2 or higherMiVoice Office 400 Release 4.1 or higherMiVoice 5000 Release 6.3 or higherMiVoice MX-ONE Release 6.3 SP1 or higher
MiCW	MiCW 6.0.2.x supports MiCollab 8.0 with MiVoice Business 8.0 SP2 or higher

Table 14: Minimum MiCollab Virtual Appliance Rel 8.1 Platform Software Requirements

Item	Requirement
Server O/S	Refer to the Virtual Appliance Deployment Guide.
vCenter Manager (optional)	
vCloud Director (optional)	
Web Browser	Microsoft Edge 20, Internet Explorer Release 10 or 11, Google Chrome version 46 or higher, or Mozilla Firefox 41 or higher

Item	Requirement
Communications platform	MiVoice Business Release 6.0 SP3 or higher (with Single Point Provisioning)MiVoice Business Release 7.2 or higher (with Flow Through Provisioning)MiVoice Office 250 Release 6.2 SP2 or higherMiVoice Office 400 Release 4.1 or higherMiVoice 5000 Release 6.3 or higherMiVoice MX-ONE Release 6.3 SP1 or higher
MiCW	MiCW 6.0.2.x supports MiCollab 8.0 with MiVoice Business 8.0 SP2 or higher

Table 15: Minimum Application Software Versions for MiCollab Rel 8.1

Item	Minimum Requirement
Suite Applications Services	Release 8.1
MiVoice Border Gateway	Release 10.1
NuPoint Unified Messaging and Speech Auto Attendant	Release 19.1
MiCollab Client	Release 8.1
AWV	Release 8.1
Legacy MiVoice for Skype for Business	Release 1.4
MiCollab for Microsoft	Release 8.1

Table 16: MiCollab Application Client Station Requirements

Item	Supported Operating Systems
Requirements for MiCollab Client stations for MiCollab End User portal, MiCollab Server Manager portal, and application clients (such as AWV and MiCollab Client).	Windows 10
	Windows 8 and 8.1 Pro (both 32 and 64-bit versions)
	Windows 7 Professional (both 32 and 64-bit versions)

5.5 Supported Applications

the applications supported by a micollab installation are dependent on the following criteria:

- deployment configuration (refer Deployment configurations).
- micollab hardware platform.
- communications platform.

5.5.1 MiVoice Business Communication Platforms

For the supported MiVoice Business communications platforms, the following MiCollab applications are available:

- NuPoint Unified Messaging
- Speech Auto Attendant
- Speech Navigation
- MiCollab Client
- AWV
- MiVoice Border Gateway (Teleworker, SIP, and SRC services) with Web Proxy Service.

Note:

The Speech Navigation option is only supported if NuPoint Unified Messaging is the only configured (used) application. This restriction applies to both the MiCollab server and virtual MiCollab. Although all apps are installed in the MiCollab Virtual Appliance OVA, if you only apply NuPoint licenses (à la carte) then it is considered a single application installation.

5.5.2 MiVoice 5000 Platforms

For these platforms, the following MiCollab applications are supported:

- NuPoint Unified Messaging
- AWV
- MiCollab Client
- MiVoice Border Gateway (Refer to the *MiVoice Border Gateway Installation and Maintenance Guide* for a table of the supported features)

Note:

The Speech Auto Attendant and Speech Navigation applications are not supported on the MiVoice 5000 platform.

5.5.3 MiVoice MX-ONE Platforms

For these platforms, the following MiCollab applications are supported:

- NuPoint Unified Messaging or MiCollab Advanced Messaging (AVST)
- AWV
- MiCollab Client
- MiVoice Border Gateway (Refer to the *MiVoice Border Gateway Installation and Maintenance Guide* for a table of the supported features)

Note:

The Speech Auto Attendant and Speech Navigation applications are not supported on the MiVoice MX-ONE platform.

5.5.4 MiVoice Office 400

This platform supports the following MiCollab applications:

- Audio, Web and Video
- MiCollab Client
- MiVoice Border Gateway (Refer to the *MiVoice Border Gateway Installation and Maintenance Guide* for a table of the supported features).

Note:

The MBG Secure Recording Connector service, NuPoint Unified Messenger, Speech Auto Attendant, and Speech Navigation applications are not supported for the MiVoice Office 400 platform.

5.5.5 MiVoice Office 250 Platform

This platform supports the following MiCollab applications:

- NuPoint Unified Messaging
- Speech Auto Attendant
- Speech Navigation
- AWV
- MiVoice Border Gateway (Refer to the *MiVoice Border Gateway Installation and Maintenance Guide* for a table of the supported features).

Note:

The Speech Navigation option is only supported if NuPoint Unified Messaging is the only configured (used) application. This restriction applies to both the MiCollab server and virtual MiCollab. Although all apps are installed in the MiCollab Virtual Appliance OVA, if you only apply NuPoint licenses (à la carte) then it is considered a single application installation.

5.6 Compression

Compression is supported only for single-app software for AWV, and TW. If multiple applications are being used in your MiCollab deployment, using compression can have adverse effects on the co-resident applications because compression can be very CPU intensive.

5.7 Firewall

A MiCollab deployment requires a suitable firewall that can provide the necessary port mapping for the packaged applications. Required Firewall features are as follows:

- Stateful Inspection or Dynamic Packet Filtering
- DMZ support
- SIP Aware
- VPN Support

The MiCollab server firewall is enabled by default in server-only mode. Therefore, the server firewall rules must be configured to allow all local networks (or "trusted networks") to have access to the MSL server. See the MSL Installation and Administration Guide for more details on how to configure local networks on MSL.

Note:

It is very important that you restrict access to the MiCollab server as much as possible to ensure the highest level of security.

5.7.1 Significant Firewall Characteristics

The firewall must have at least three physical interfaces:

- Internal network
- External network/Internet
- DMZ

The MBG is provided by an MSL server installed in the customer's existing DMZ. In this configuration, the MSL must be installed in "server-only" mode. The corporate firewall provides static network address translation between an externally visible address and the DMZ address of the MSL server.

The MSL server used in the DMZ must have a static IP address. This IP address should be a separate address from the external IP address of the firewall, although some firewalls that support port forwarding may allow sharing the address. It is vital that this address actually be static as any change of the address will cause remote sets to lose connectivity.

The TCP and UDP port numbers used on the external address of the firewall must be preserved when the packets are passed to the MSL server in the DMZ.

Details of the protocols that must be configured in the firewall are provided in Firewall Configuration. Particular attention should be paid to the requirement that all UDP ports >= 1024 on the LAN be permitted to reach the public IP of the MBG server.

Failure to configure the firewall properly will result in audio problems (typically one-way audio).

5.7.2 Known Issues

5.7.2.1 Checkpoint Firewalls

We have seen issues in the past with Checkpoint NG firewalls and their use of the "Smart Connection Re-use" feature. It is apparently enabled by default, and has caused issues with sets behind it attempting to reconnect to an MBG server. The firewall has no knowledge of the current state of the connection endpoints, but attempts to determine that state by mangling the connection attempt of the set through the firewall. "Smart Connection Re-use" feature should be disabled with older sets.

With newer sets this should not be a problem, as the set should randomize the client port used with the new connection, resulting in the firewall treating the new connection properly.

5.7.2.2 Port-forwarding Firewalls

Firewalls (and other types of devices) with only two ports are not supported. While these firewalls may be able to simulate a DMZ for a simple service such as a web server, they are unable to provide the true DMZ environment required for the Multi-Protocol Border Gateway. The Multi- Protocol Border Gateway requires the coordination of multiple simultaneous connections, which cannot be achieved with simple port-forwarding.

Some two-port firewalls (for example, the SonicWall SOHO2) will allow the firewall to have multiple external IP addresses, but perform port forwarding to simulate a DMZ. These firewalls are not supported.

MiCollab System Capacities, Performance, and Constraints

6

This chapter contains the following sections:

This section provides the MiCollab system capacities, performance, and constraints.

- Multi-application deployments support both UCC Licensing and à la carte licensing.
- Single application deployments support à la carte licensing only.

Use the following tables to locate the capacity and performance details:

Table 17: Multi-Application Capacities (UCC licensing supported)

PLATFORM	DEPLOYMENT	USER CAPACITY	SEE TABLE
MiCollab Server Appliance	Server Appliance platform	**150**	On MiCollab 9.2 and older systems, for a large Enterprise configuration, it is required to execute the below
Industry Standard Servers Table 20 to page 31	Entry-level server	**500**	Entry-Level Server with Multiple Applications
	Mid-range server	**1500**	Mid-Range Server with Multiple Applications

	Mid-range system server with 8 GB RAM	**2500**	Mid-Range System Server (with 8 GB RAM) with Multiple Applications
	Mid-range system server with 16 GB RAM	**5000**(Note 1)	Mid-Range System Server (with 16 GB RAM) with Multiple Applications
vMiCollab (Note 2)	Small Business	**250**	Virtual Appliance Small Business with Multiple Applications
	Mid-Market	**1500**	Virtual Appliance Mid-Market with Multiple Applications
	Enterprise	**2500** (Note 1)	Table 27: Virtual Appliance Enterprise with Multiple Applications (2500-User) on page 89
	Large Enterprise	**5000** (Note 1,3)	Virtual Appliance Large Enterprise with Multiple Applications (5000-User)

Note:
1

MiVoice Business systems support up to 5600 Multi-device User Group (MdUG) devices. On average, the UCC default licensing roles and templates assign 2.75 devices per user. To minimize the possibility of exceeding the MiVoice Business device limits, do not assign users with unnecessary phones. During initial bulk provisioning, create and apply custom roles and templates that assign the actual phone requirements to the users.

Note:
2

vMiCollab Virtual Appliance support VMware and Hyper-V deployments.

Table 18: Single-Application Capacities (à la carte licensing only)

PLATFORM	DEPLOYMENT	USER CAPACITY	SEE TABLE
Industry Standard Servers	Entry-level server	**1500**	Entry-Level Server Capacity with Single Application
	Mid-range server	**2500**	Mid-Range Server Capacity with Single Application
MiCollab Virtual Appliance	Enterprise (Note 1)	**5000**	Virtual Appliance Enterprise Capacity with Single Application

Note:
1

To support a large single-application configuration (5000-user capacity) you must manually increase the VMware resources for the MiCollab virtual machine. Refer to the Virtual Appliance Deployment Guide for instructions.

Table 19: Advanced UM users Capacities

E-MAIL VERSIONS	IMAP INTEGRATION	MAPI INTEGRATION
Exchange 2007, 2010 SP3, and 2013	**500**	**2500**
Exchange 2016	**1500**	**Not supported**
Google	**2500**	**Not supported**
Office 365*	**1500**	**Not supported**

***For Office 365**, minimum upload speed of 5 Mbps from Internet Service Provider (ISP) is recommended.

The user capacities listed in the following tables are based on a UCC license mix of 25% Entry, 50% Standard, and 25% Premium.

6.1 Multi-Application Capacities (UCC Licensing Supported)

Table 20: Server Appliance Small Business with Multiple Applications

APPLICAT	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUI CALL SECONI (CCS)	AVG HOLD TIME (SEC)	COMPRESSI
Total Users: 150 **Total MiVoice Business Devices: 413** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 300**					
NuPoint Unified Messaging	165 NP-UM mailboxes 150 Standard UM User 150 Advanced UM Users 20 WebView Sessions Maximum 4 TTS and 3 SoftFAX ports	60	10 CCS	100 sec	G.711 or G.729
		4 TTS	10 CCS	100 sec	
		3 SoftFax			
MiVoice Border Gateway	150 Teleworkers or SRC connections (See Note 6)	150	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
	30 Teleworkers or TAP streams (or any combination up to 30)	30			
Speech Auto Attendant	165 SAA Directory Entries	4	10 CCS	100 sec	G.711 only

APPLICAT	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUI CALL SECONI (CCS)	AVG HOLD TIME (SEC)	COMPRESSI
AWV	50 Audio ports (G.711)	50			G.711
	50 Audio ports (G.722)	50			G.722
	50 Audio ports (G.729, G.722.1)	50			G.729, G.722.1
	50 Web & Collaboration Sessions (See Note 7)	50			
	25 concurrent video streams with conferencing (See Note 11	25			
MiCollab Client	Maximum Devices per User	8			
	Total Corporate Contacts	40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			
	Maximum concurrent MiCollab Client connections (Deskphones, Softphones, Web Clients or Mobile Clients)	225			G.711 and G.722 See Note 8

APPLICAT	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUI CALL SECONI (CCS)	AVG HOLD TIME (SEC)	COMPRESSI
WebRTC	Maximum # of Concurrent Calls	250			

Table 21: Entry-Level Server with Multiple Applications

APPLICAT	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTU CALL SECON (CCS)	AVG HOLD TIME (SEC)	COMPRESS
Total Users: 500 **Total MiVoice Business Devices: 1375** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 1000**					
NuPoint Unified Messaging	550 NP-UM mailboxes 500 Standard UM User	60	10 CCS	100 sec	G.711 or G.729
	500 Advanced UM Users	4 TTS	10 CCS	100 sec	
	50 WebView Sessions(See Note 4)	3 SoftFax			
	Maximum 4 TTS and 3 SoftFAX ports (See Note 5)				
MiVoice Border Gateway	150 Teleworkers or SRC connections (See Note 6	150	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
	30 Teleworkers or TAP streams (or any combination up to 30)	30			

APPLICAT	NUMBER OF USERS	SIMULTAN PLATFORM CONNECT	CENTU CALL SECON (CCS)	AVG HOLD TIME (SEC)	COMPRESS
Speech Auto Attendant	550 SAA Directory Entries	12	10 CCS	100 sec	G.711 only
AWV	50 Audio ports (G.711)	50			G.711
	50 Audio ports (G.722)	50			G.722
	50 Audio ports (G.729, G.722.1)	50			G.729, G.722.1
	50 Web & Collaboration Sessions (See Note 7)	50			
	25 concurrent video streams with conferencing (See Note 11	25			
MiCollab Client	Maximum Devices per User	8			
	Total Corporate Contacts	40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			

APPLICAT	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTU CALL SECOI (CCS)	AVG HOLD TIME (SEC)	COMPRESS
	Maximum concurrent MiCollab Client connections(Deskphones, Softphones, Web Clients or Mobile Clients)	560			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

Note:

To support more than 500 advanced UM users (Exchange 2007, 2010 SP3, and 2013), the system requires a MAPI or vMAPI gateway. Refer to the NuPoint Unified Messaging Engineering Guidelines for MAPI and vMAPI gateway capacities. The vMAPI gateway is an alternative deployment option to the MAPI gateway. vMAPI gateway is not supported with Exchange 2016.

Table 22: Mid-Range Server with Multiple Applications

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
Total Users: 1500 **Total MiVoice Business Devices: 4125** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 3000**					

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
NuPoint Unified Messaging	1650 NP-UM mailboxes 1500 Standard UM Users 1500 Standard UM User (See Note 3) 50 WebView Sessions (see Note 4 Maximum 8TTS and 6SoftFAX ports	120	10 CCS	100 sec	G.711 or G.729
		8 TTS	10 CCS	100 sec	
		6 SoftFax			
MiVoice Border Gateway	375 Teleworkers or SRC connections (See Note 6) 38 Teleworker or TAP streams (or any combination up to 38)	375	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
		38			
Speech Auto Attendant	1650 SAA Directory Entries for mid-range server	24	10 CCS	100 sec	G.711 only
Micollab AWV	150 Audio ports (G.711) (See Note 6)	150			G.711
	150 Audio ports (G.722)	150			G.722

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	100 Audio ports (G.729, G.722.1)	100			G.729, G.722.1 (Up to 100 G.729 or G.722.1 sessions are supported at any one time in all conferences)
	150 Web & Collaboration Sessions (See Note 7)	150 Sessions			
	75 concurrent video streams with conferencing (See Note 11)	75			
MiCollab Client	Maximum Devices per User	8			
	Total Corporate Contacts	40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	Maximum concurrent MiCollab Client connections(Deskphones, Softphones, Web Clients or Mobile Clients)	2250			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

Table 23: Mid-Range System Server (with 8 GB RAM) with Multiple Applications

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
Total Users: 2500 **Total MiVoice Business Devices: 6875** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 5000**					

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
NuPoint Unified Messaging	2750 NP-UM mailboxes 2500 Standard UM Users 2500 Advanced UM User (See Note 3) 50 WebView Sessions (see Note 4 Maximum 12TTS and 6SoftFAX ports (See Note 5)	120	10 CCS	100 sec	G.711 or G.729
		8 TTS	10 CCS	100 sec	
		6 SoftFax			
MiVoice Border Gateway	1000 Teleworkers or SRC connections (See Note 6)	1000	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
	250 Teleworker or TAP streams (or any combination up to 38)	250			
Speech Auto Attendant	2750 SAA Directory Entries for mid-range server	30 multi-app	10 CCS	100 sec	G.711 only
AWV	500 Audio ports (G.711) (See Note 6)	500			G.711
	500 Audio ports (G.722)	500			G.722

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	100 Audio ports (G.729, G.722.1)	100			G.729, G.722.1 (Up to 100 G.729 or G.722.1 sessions are supported at any one time in all conferences)
	300 Web & Collaboration Sessions (See Note 7)	300 Sessions			
	Maximum # of members in a single conference	200			
	120 concurrent video streams with conferencing (See Note 11)	120			
MiCollab Client	Maximum Devices per User	8			
	Total Corporate Contacts	40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	Maximum concurrent MiCollab Client connections(Deskphones, Softphones, Web Clients or Mobile Clients)	3750			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

Table 24: Mid-Range System Server (with 16 GB RAM) with Multiple Applications

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
Total Users: 5000 **Total MiVoice Business Devices: 13750** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 5000**					

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
NuPoint Unified Messaging	5500 NP-UM mailboxes 5000 Standard UM Users 2500 Standard UM User (See Note 3) 50 WebView Sessions (see Note 4 Maximum 12 TTS and 6SoftFAX ports (See Note 5)	120	27 CCS	100 sec	G.711 or G.729
		24 TTS	10 CCS	100 sec	
		6 SoftFax			
MiVoice Border Gateway	1000 Teleworkers or SRC connections (See Note 6)	1000	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
	250 Teleworker or TAP streams (or any combination up to 38)	250			
	For MiVoice 5000 and MiVoice MX-ONE deployments, the MiCollab MBG application must be clustered with a standalone MBG. The Teleworker traffic is handled by the standalone MBG. Refer to MBG Engineering Guidelines to size the installation.				
Speech Auto Attendant	5000 SAA Directory Entries for mid-range server	30	10 CCS	100 sec	G.711 only
AWV	500 Audio ports (G.711) (See Note 6)	500			G.711

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	500 Audio ports (G.722)	500			G.722
	100 Audio ports (G.729, G.722.1)	100			G.729, G.722.1 (Up to 100 G.729 or G.722.1 sessions are supported at any one time in all conferences)
	500 Web & Collaboration Sessions (See Note 7)	500 Sessions			
	150 concurrent video streams with conferencing (See Note 11)	150			
MiCollab Client	Maximum Devices per User	8			
	Total Corporate Contacts	40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	Maximum concurrent MiCollab Client connections(Deskphones, Softphones, Web Clients or Mobile Clients)	7500			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

Table 25: Virtual Appliance Small Business with Multiple Applications

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
Total Users: 250 **Total MiVoice Business Devices: 688** **Total MiVoice Office 400 Devices: 500** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 500**					

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
NuPoint Unified Messaging	275 NP-UM mailboxes 250 Standard UM Users 250 Advanced UM User 20 WebView Sessions (see Note 4 Maximum 4 TTS and 6SoftFAX ports (See Note 5)	8	10 CCS	100 sec	G.711 or G.729
		4 TTS	10 CCS	100 sec	
		3 SoftFax			
MiVoice Border Gateway	150 Teleworkers or SRC connections	150	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
	50 Teleworker or TAP streams (or any combination up to 50)	50			
Speech Auto Attendant	275 SAA Directory Entries for mid-range server	4	10 CCS	100 sec	G.711 only
AWV	50 Audio ports (G.711)	50			G.711
	500 Audio ports (G.722)	50			G.722
	50 Audio ports (G.729, G.722.1)	50			G.729, G.722.1

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	500 Conferencing Web & Collaboration Sessions (See Note 7)	50			
	16 concurrent video streams with conferencing (See Note 11)	16			
MiCollab Client	Maximum Devices per User	8			
	Total Corporate Contacts	43000 (MiVB) with 11 peered MiCollab servers (See Note 13) 40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			
	Maximum concurrent MiCollab Client connections(Deskphones, Softphones, Web Clients or Mobile Clients)	375			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

Table 26: Virtual Appliance Mid-Market with Multiple Applications

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
Total Users: 1500 **Total MiVoice Business Devices: 4125** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 3000**					
NuPoint Unified Messaging	1650 NP-UM mailboxes 1500 Standard UM Users 1500 Advanced UM User (See Note 3) 50 WebView Sessions (See Note 4 Maximum 8 TTS and 6SoftFAX ports (See Note 5)	60 - 120	10 CCS	100 sec	G.711 or G.729
		8 TTS	10 CCS	100 sec	
		6 SoftFax			
MiVoice Border Gateway	Teleworkers or SRC connections (See Note 6)	375	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
	50 Teleworker or TAP streams (or any combination up to 75)	75			
Speech Auto Attendant	1650 SAA Directory Entries for mid-range server	24	10 CPH	100 sec	G.711 only

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
AWV	150 Audio ports (G.711) (See Note 6)	150			G.711
	150 Audio ports (G.722)	150			G.722
	100 Audio ports (G.729, G.722.1)	100			G.729, G.722.1 (Up to 100 G.729 or G.722.1 sessions are supported at any one time in all conferences.)
	150 Conferencing Web & Collaboration Sessions (See Note 7)	150			
	75 concurrent video streams with conferencing (See Note 11)	75			
MiCollab Client	Maximum Devices per User	8			

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	Total Corporate Contacts	43000 (MiVB) with 11 peered MiCollab servers (See Note 13) 40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			
	Maximum concurrent MiCollab Client connections (Deskphones, Softphones, Web Clients or Mobile Clients)	2250			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

Table 27: Virtual Appliance Enterprise with Multiple Applications (2500-User)

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
Total Users: 2500 **Total MiVoice Business Devices: 6875** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 5000**					

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
NuPoint Unified Messaging	2750 NP-UM mailboxes 2500 Standard UM Users 2500 Advanced UM User (See Note 3) 50 WebView Sessions (see Note 4 Maximum 12 TTS and 6SoftFAX ports (See Note 5)	120	10 CCS	100 sec	G.711 or G.729
		12 TTS	10 CCS	100 sec	
		6 SoftFax			
MiVoice Border Gateway	1000 Teleworkers or SRC connections	1000	6 CCS	100 sec	G.711, G.722, G729 with no transcoding.
	250 Teleworker or TAP streams (or any combination up to 250)	250			
Speech Auto Attendant	2750 SAA Directory Entries for mid-range server	30 multi-app	10 CCS	100 sec	G.711 only
AWV	300 Audio ports (G.711) (See Note 6)	300			G.711
	300 Audio ports (G.722)	300			G.722

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	100 Audio ports (G.729, G.722.1)	100			G.729, G.722.1 (Up to 100 G.729 or G.722.1 sessions are supported at any one time in all conferences.)
	300 Web and Collaboration Sessions (See Note 7)	300 Sessions			
	Maximum # of members in a single conference	200			
	120 concurrent video streams with conferencing (See Note 11)	120			
MiCollab Client	Maximum Devices per User	8			

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	Total Corporate Contacts	43000 (MiVB) with 11 peered MiCollab servers (See Note 13) 40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			
	Maximum concurrent MiCollab Client connections(Deskphones, Softphones, Web Clients or Mobile Clients)	3750			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

Table 28: Virtual Appliance Large Enterprise with Multiple Applications (5000-User)

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
Total Users: 5000 **Total MiVoice Business Devices: 13750** **Total MiVoice 5000 or MiVoice MX-ONE Devices: 5000**					

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
NuPoint Unified Messaging	5500 NP-UM mailboxes 5000 Standard UM Users 2500 Advanced UM User (See Note 3) 50 WebView Sessions (see Note 4 Maximum 12 TTS and 6SoftFAX ports (See Note 5)	120	27 CCS	100 sec	G.711 or G.729
		24 TTS	10 CCS	100 sec	
		6 SoftFax			
MiVoice Border Gateway	Standalone MiVoice Border Gateway required (The MiCollab MBG application must be clustered with a standalone vMBG. The Teleworker traffic is handled by the standalone vMBG. Refer to MBG Engineering Guidelines to size the installation.)				
Speech Auto Attendant	5000 SAA Directory Entries for mid-range server	30 multi-app	10 CCS	100 sec	G.711 only
AWV	500 Audio ports (G.711) (See Note 6)	500			G.711
	500 Audio ports (G.722)	500			G.722

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	100 Audio ports (G.729, G.722.1)	100			G.729, G.722.1 (Up to 100 G.729 or G.722.1 sessions are supported at any one time in all conferences.)
	500 Web & Collaboration Sessions (See Note 7)	500 Sessions			
	150 concurrent video streams with conferencing (See Note 11)	150			
MiCollab Client	Maximum Devices per User	8			
	Total Corporate Contacts	43000 (MiVB) with 11 peered MiCollab servers (See Note 13) 40000 (MiVB or MiVoice MX-ONE) with 8 peered MiCollab servers 20000 (Other platforms) with 4 peered MiCollab servers			

APPLICATI	NUMBER OF USERS	SIMULTAN PLATFORI CONNECT	CENTUM CALL SECOND (CCS)	AVG HOLD TIME (SEC)	COMPRES
	Maximum concurrent MiCollab Client connections (Deskphones, Softphones, Web Clients or Mobile Clients)	7500			G.711 and G.722 See Note 8
WebRTC	Maximum # of Concurrent Calls	250			

6.2 NuPoint Unified Messaging Capacities

The NP-UM Single Application is a product offering that consists of a single instance of the NuPoint application running on a mid-range server. This section provides the capacities and limits for the NP-UM Single Application offering. Note that these limits are based on the criteria that no other applications will be running on this server.

6.2.1 NP-UM Single Application Capacities

Table 29: NP-UM Single Application Capacities

SYSTEM FEATURE	MAXIMUM CAPACITY
This configuration requires a mid-range server.	
Voice Mailboxes	2750
Voice Channels/Ports	120 ports - IP via MiVoice Business system

Prompt Sets	6 concurrent FULL prompt sets **Note**: NP Call Director does not count as a full prompt set. As a rule of thumb, a total of 4 NP Call Director Prompts are the equivalent of 1 Full prompt set.
NP Web View sessions	50

6.2.2 Message Compression and Storage Capacity

It is important to have an understanding of the message storage requirements of your environment. The following factors affect this calculation:

- Maximum number of messages allotted per user
- Maximum message length
- Days to keep read messages
- Days to keep unread messages
- Message File Format used

The message file format determines the message storage capacity for the system because the file format determines the size of the actual messages.

The two supported message formats are G711 and G721. G711 is used for audio format while G721 is used only for VPIM messaging between old and new systems. The following table shows the message compression for G711 and G721.

Table 30: Message Compression for G711 and G721

FILE FORMAT	BYTES / SEC	BYTES / MIN	MB / HOUR
G711	8000	480000	28.8
G721	1000	60000	3.6

6.2.3 MiCollab System Storage Capacity

The minimum MiCollab system storage capacity is 160 GB when the system is using G711 file format.

6.2.4 Web View Session Requirements

Web View users access the NuPoint Unified Messaging server via a Web browser, and thus an adequate number of concurrent sessions must be enabled on the server to support the number of Web View users. Use the following table as a guideline to determine the number of concurrent sessions you require on your system. The table shows the recommended number of sessions for systems with average and heavy use.

Table 31: Web Session Guidelines

AVERAGE USERS		HEAVY USERS	
NUMBER OF WEB VIEW USERS	SESSIONS REQUIRED	NUMBER OF WEB VIEW USERS	SESSIONS REQUIRED
25	2	25	3
50	3	50	5
100	6	100	10
150	9	150	15
200	12	200	20
250	15	250	25
300	18	300	30
350	21	350	35

AVERAGE USERS		HEAVY USERS	
NUMBER OF WEB VIEW USERS	SESSIONS REQUIRED	NUMBER OF WEB VIEW USERS	SESSIONS REQUIRED
400	24	400	40
450	26	450	45
500	29	500	50

If at some point, users begin noticing an increase in the number of times they see a message that instructs them to access the system again later, then more sessions need to be added to the system. A maximum of **50** sessions is supported on the NuPoint Unified Messaging application.

Note:

Call Director call flow licenses are granted on a per-mailbox basis and are absolute licenses (direct license mapping to a mailbox, there is no concept of license session). However, in order to author a Call Director call flow through the Web GUI you must have enough Web GUI sessions available.

6.2.5 Advanced Unified Messaging Support

The NuPoint Unified Messaging Standard Edition system with the Advanced Unified Messaging feature supports both IMAP and MAPI integration with e-mail servers. For details on user capacities, see Table 14: Advanced UM users Capacities.

For NuPoint Advanced UM with MAPI or vMAPI Gateway, the gateway software can be installed on a computer with any of the following operating systems:

- Windows 7 Professional, Enterprise, and Ultimate (32 and 64 bit)
- Windows 8 Professional (64 bit)
- Windows Server 2008 R2 (64 bit)
- Windows Server 2012 R2 (64-bit).

Refer to the *NuPoint Unified Messaging* documentation for details.

Upgrades, Conversions, and Migrations

7

This chapter contains the following sections:

Refer to Product Bulletin 20110051 for full details of the upgrade, conversion, and migration options.

7.1 Upgrade Considerations

- MiCollab 7.2 must be installed on a 64-bit server. MiCollab 7.2 is only supported on MSL 64-bit architecture. You cannot upgrade MSL from 32-bit to 64-bit architecture. If your current system is running on 32-bit architecture, you must perform a backup of your data, a fresh install, followed by a restore.
- If you have active Software Assurance, you can upgrade directly from MiCollab 4.x or later to MiCollab 7.x free of charge without an upgrade part number
- Direct upgrades to MiCollab 7.2 from releases below MiCollab Release 4.0 are not supported.
- To support all the available MiCollab Release 7.2 applications, the MiCollab Server or MiCollab Server Appliance must meet minimum hardware requirements. Refer to the MSL Qualified Hardware List available on Mitel Online for the requirements. You can upgrade a MiCollab 4.0 Server or Server Appliance that has only 4 GB of RAM to MiCollab Release 7.2 providing you do not install the Collaboration Client application. To install the MiCollab Client, you must first upgrade the MiCollab Server or MiCollab Server Appliance to a minimum of 6 GB of RAM.
- Do not attempt to restore a database that has been taken from an individual application (for example, a NP-UM database) within a MiCollab Server to either a MiCollab Server system or a MiCollab Virtual Appliance deployment.
- If an installation or upgrade fails to complete, you must re-install MiCollab.
- For major upgrades (for example from Release 6.0 to 7.2) you must perform a fresh install and restore or deploy a new OVA file.
- For service pack upgrades (for example from Release 7.2 to 7.3) you can install applications from the web-based server manager interface.
- Refer to the Virtual Appliance Deployment Guide for MiCollab Virtual Appliance upgrade considerations.
- Refer to the *MiCollab Installation and Maintenance Guide* on the Mitel Customer Documentation site for software installation, upgrade, and update instructions.

7.2 Conversion and Migration Considerations

- You can migrate a Collaboration Client Server standalone database to a MiCollab 8.1 system. For Collaboration Client data migrations, the backup database that you restore to MiCollab must originate from a Collaboration Client Release 5.0 or higher system. When you migrate a Collaboration Client database to MiCollab 8.1, MiCollab will not prevent you from provisioning too many users. If you over provision the MiCollab system, performance will be degraded. To determine the maximum number of Collaboration Client users that are supported for your deployment configuration refer to .

  MiCollab System Capacities, Performance, and Constraints on page 25
- You can migrate from a Virtual Collaboration Client deployment to MiCollab Virtual Appliance 8.1 with Collaboration Client. However, the virtual machine must have sufficient resources.
- You can migrate from a MiCollab Server Appliance to MiCollab 8.1 deployment with Collaboration Client. However, you must upgrade the server hardware to meet the hardware requirements for MiCollab 8.1.
- If a conversion or migration fails to complete, you must re-install MiCollab.
- Refer to the Virtual Appliance Deployment Guide for MiCollab Virtual Appliance conversion and migration considerations.
- Refer to the *MiCollab Installation and Maintenance Guide* on the Mitel Customer Documentation site for database conversion and migration instructions.

NuPoint Unified Messaging Guidelines 8

This chapter contains the following sections:

8.1 Voice User Interface Port Characteristics

NuPoint Unified Messaging is a voice over IP (VoIP) product whereby each of its Voice User Interface Ports (VUI ports or ports) behaves the same as a VoIP end point.

NP-UM emulates IP sets (virtual extensions) which register with the MiVoice Business. Each “port” of the NP-UM system appears as a 5020 or 5240 IP set to the MiVoice Business. At the same time, MiTAI software directs the call handling and the MWI for the NP-UM system.

The following table provides some key characteristics of the NuPoint ports.

Table 32: Port Characteristics

PROPERTY	VALUE	DESCRIPTION
Encoding rule	G.711	G.711 only for current release

Encryption	NO	Currently, no encryption is supported
Signaling	SIP or Mitai/Minet	One signaling channel per port
Compression	NO	Currently, no compression is supported

8.2 IP Bandwidth Considerations

The rule of thumb in allocating IP bandwidth for a voice channel is 100kbits/s for each uncompressed channel. Add to this a 10% signaling overhead and we have the following guideline:

BW (kbits/s) = 110 x Number of voice channels

Example: A 120-port NuPoint Unified Messaging system will require a peak LAN bandwidth of 13,200 Kb/s or 13.2M b/s. 100 Mb/s full duplex L2 switches would be required to support this bandwidth requirement.

8.3 IP Network Requirements

A successful VoIP implementation is dependent on the IP network complying with strict network parameters. To ensure good voice quality, the network connecting the MiVoice Business servers, MiCollab server, and IP phones should comply with the recommendations provided in the following table.

Table 33: Voice over IP Network Limits

PACKET LOSS	JITTER	END-TO-END DELAY	LEGEND
< 1%	< 30 ms	< 50 ms	Green = Go
< 5%	< 60 ms	< 80 ms	Yellow = Caution
< 5%	< 60 ms	< 80 ms	Red = Stop

Note:

The time derived from a Ping command is twice the end-to-end delay.

Note:

The value that PING reports back to the user is the number of milliseconds for a “round trip.” In other words, the actual latency between two nodes will be half of the figure reported by PING.

When transmitting Faxes over IP networks, the network parameters required are even more stringent than with VoIP. This is described in NP Fax.

8.4 Network Implementation Guideslines

8.4.1 Integrating NuPoint on MiCollab into the Network

The following figure shows how the MiCollab server should be deployed in the LAN. Since the NuPoint application is VLAN unaware, it is important to connect the MiCollab server to the Access L2 switch and to configure the Access L2 switch as shown, so that voice quality is maintained.

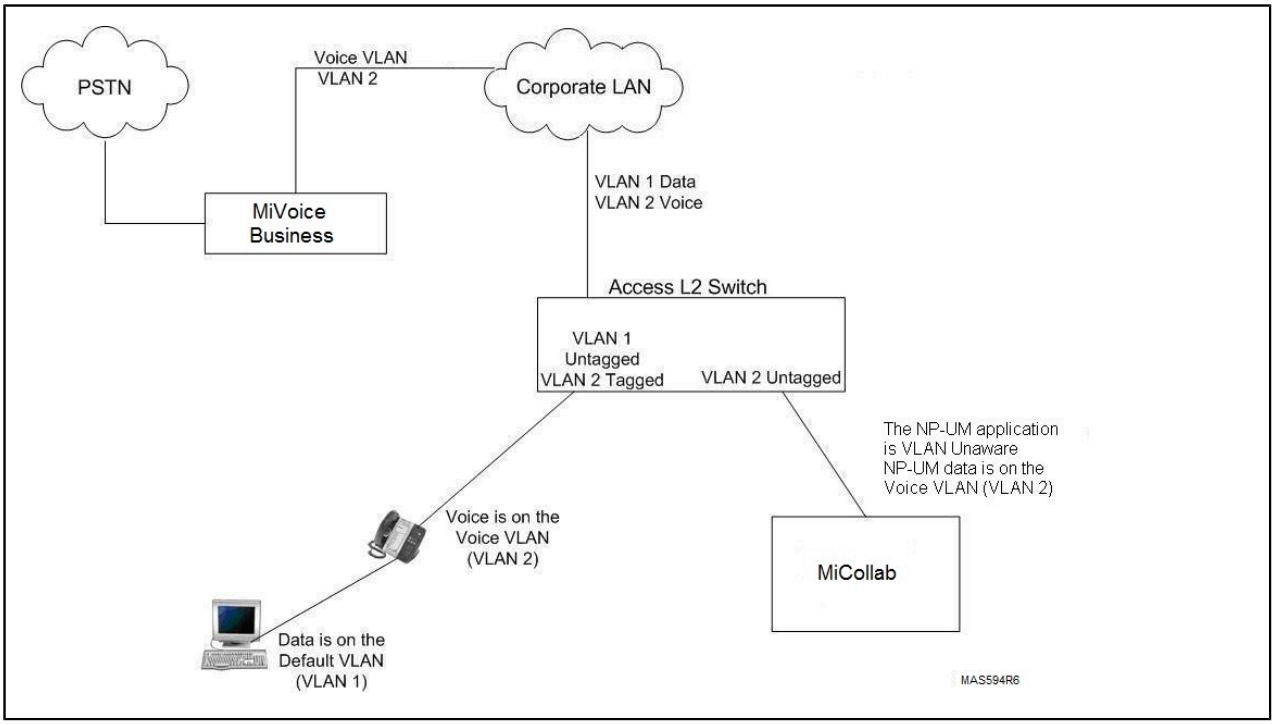


Figure 15: NP-UM LAN Integration

8.4.2 Access L2 Switches

The L2 switches that are selected to serve as the Access L2 switches must be managed switches and must provide LAN interfaces that are capable of 100 Mb/s minimum. If the customer is running, or chooses to run, Spanning Tree Protocol on their LAN, then the Access L2 switch must be configured so the MiCollab server does not participate in the Spanning Tree Protocol. To ensure that the MiCollab server is not part of the Spanning Tree, the Access L2 switch ports that are used to connect to the MiCollab server must have PortFast enabled.

Regardless of what L2 switch technology is used, the basic requirement is that the Access L2 switch port used to connect to the MiCollab server must not forward Bridge Protocol Data Unit (BPDU) packets to the MiCollab server. Enabling PortFast on a Cisco L2 switch port prevents this port from transmitting BPDUs.

Note:

PortFast is a Cisco term. Other L2 switch vendors use different terminology to describe this function, such as or Spanning Tree Edge Port.

8.5 Deployment Scenario: Integration with a Cluster of MiVoice Business Systems

When integrating with a cluster of MiVoice Business systems one requirement overrides all others; that there should be only one voice mail hunt group. This requirement is needed for two important reasons:

1. One hunt group pilot for all users.
2. When a user sees a message waiting light on the phone and hits on the Messages key, it is the voice mail hunt group pilot number that must be called. Therefore, all the MWI must be in this same hunt group.

This requirement means that all voice mail ports must land on one ICP and be grouped in a hunt group on that ICP. The hunt group pilot number can then be made into a network number, reachable from all other ICPs.

If very high voice mail call rates (>4000 calls per hour including MWI calls) are expected, the interfacing ICP must not do much else other than being the interfacing ICP.

While all voice mail ports (including MWI ports) must be in one hunt group, the non-voice mail ports can be in different hunt groups and can even reside on different ICPs. For example, pager ports simply make outgoing calls so they can land on any ICP, and they don’t have to be in any particular hunt group. Record-a-call (RAC) ports should land on as many ICPs as possible (up to four) because only the users on those ICPs can activate the feature. RAC ports have to be contained by a Recorder hunt group on the ICP where they land. Receptionist lines can also land on a different ICP.

8.6 Deployment Scenario: Integration with the MiVoice Office 250

NuPoint Unified Messaging can be integrated with the MiVoice Office 250 on the MiCollab platform.

The requirements stated below must be satisfied before NuPoint Unified Messaging can be integrated with a MiVoice Office 250 SIP Gateway connected to IP Endpoints. Please ensure that each requirement has been satisfied before continuing with the integration.

1. It is assumed that the SIP Gateway is running and correctly configured with IP Endpoints so that each endpoint has a registered extension.
2. Mitel Standard Linux (MSL) and NuPoint Software (NPM) must be installed and running on a computer system connected to the same physical network as the SIP

Gateway. Also full IP connectivity is assumed possible between NPM and the SIP Gateway, meaning that no security hardware or software is active.

3. MSL has been properly licensed using Mitel's server (AMC). In order to be used or tested, NPM features must be enabled in an AMC Application Record. The Application Record ID is requested and the Application Record is "activated" during the MSL installation.
4. The NPM server is mapped from the SIP gateway by a Pilot Number and configured as a SIP Trunk.
5. The security settings on the NPM server must be modified so that it is possible to establish full telephony communication between the SIP Gateway and NuPoint. Security modifications are completed within the MSL Server Console using the following instructions.

   a. Log in to the MSL Server Console by using the "admin" account locally on NPM server, or remotely with SSH if access is possible.
   b. Select "Access Server Manager" and log in with the same "admin" account.
   c. Under the "Security" heading, select "Local Networks".
   d. Click "Add Network".
   e. Define the "Network Address" and "Subnet mask" that defines a range of addresses including the SIP Gateway IP address. Also, enter the "Router" IP address directly reachable from the NPM server. Select "Add".

Note:

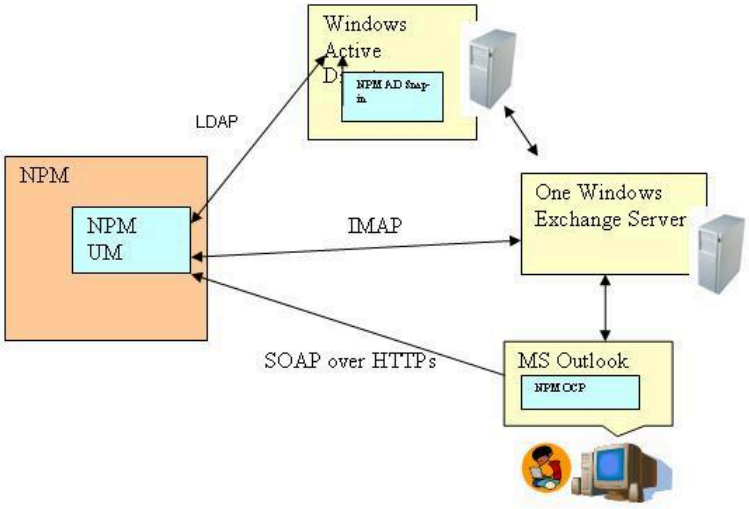
Under some circumstances, modifying the "Local Networks" will not update security settings correctly. Should call connectivity or two-way audio not appear to be initiated correctly, the following command may be issued, as a last resort, to disable the NPM server's firewall through a Linux console session: service masq stop.

8.7 Deployment Scenario: Advanced Unified Messaging

NuPoint Messaging supports the IMAP and MAPI protocols in order to connect to the Exchange Servers for voicemail synchronization and TTS. The IMAP connector, which is deployed by default on, supports Exchange server.

The IMAP connector is targeted for small and medium-sized companies with one Exchange server. The IMAP connector in NuPoint Messaging will support only **one Exchange server** as illustrated in the following figure.

Figure 16: NP-UM Advanced UM with IMAP Integration



8.8 NP FAX

Transmitting Faxes over an IP network can be accomplished in two ways:

- Fax data can be carried in G.711 voice packets, or
- Fax data can be transported using the T.38 protocol.

Transmitting Faxes over IP networks via G.711 voice packets is referred to as 'G.711 pass through'. This method of transmitting Faxes requires that the LAN meet more stringent network parameters than is required for VoIP applications. G.711 Fax pass-through is susceptible to failure if the IP network presents any significant packet loss or jitter. To ensure high-quality Fax reception with G.711 pass through, the network between MiVoice Business servers, and the MiCollab server should comply with the recommendations shown in Table 32.

Table 34: Fax over G.711 (Pass-Through): Network Limits

PACKET LOSS	JITTER	END-TO-END DELAY	LEGEND
< 0.1 %	< 20 ms	< 300 ms	Green = Go
< 0.2 %	< 40 ms	< 500 ms	Yellow = Caution

> 0.2 %	> 40 ms	> 500 ms	Red = Stop

Note:

The time derived from a Ping command is twice the end-to-end delay.

Note:

The value that PING reports back to the user is the number of milliseconds for a “round trip.” In other words, the actual latency between two nodes will be half of the figure reported by PING.

If it is necessary to transmit Faxes on an IP network that cannot meet the G.711 pass through IP network requirements then T.38 Fax support should be considered as a solution.

NuPoint on MiCollab does not natively support the T.38 protocol; however, the MiCollab provides T.38 support as a licensable option and it can be used to ensure Fax transmission integrity over a major portion of the customer's network.

For details on T.38 and how to deploy it in conjunction with NuPoint refer to the *NuPoint Engineering Guidelines* and the *MiVoice Business Engineering Guidelines.*

8.9 Record-a-Call

Record-A-Call (RAC) is an optional feature that allows mailbox users to record both ends of a two-party external trunk call in progress on their phone. Recorded conversations are delivered to the user's voice mailbox. Unlike regular voice mail messages, RAC messages are stored immediately as saved messages, so they do not trigger Message Waiting Indicators on the user's telephone.

The MiVoice Business system must have the Advanced Voice Mail option enabled. For MiVoice Business system users to use RAC, the RAC feature must be configured in the MiVoice Business system administration tool for their phones. Refer to the MiVoice Business online help for RAC configuration details.

If RAC is enabled on the NuPoint Unified Messaging system, all voice mail ports will register on the MiVoice Business system as 5240 devices and ports that are used for MWI will register as 5020 devices.

- Tones are not given to either party to indicate that the call is being recorded. Recording is done silently.
- It is the customer's responsibility to ensure that the RAC feature and use of the feature does not contravene any laws of the jurisdiction where the call is placed from, and/or of the place being called. No indication is given to either party to indicate that the call is being recorded. Mitel is not liable for use of this feature in a manner that does not conform to the applicable laws of the calling or called location.
- RAC is supported on MiVoice Business systems only. In a MiVoice Business cluster environment, RAC can only be activated on phones registered to an ICP that is connected to the NuPoint Unified Messaging server. Up to four ICPs can be connected to one NuPoint Unified Messaging server.
- At least one EMEM mailbox license (minimum) is required on the MiVoice Business system to use RAC.
- A maximum of 12 RAC conversations can run concurrently on an ICP. For information on the current limitations of the MiVoice Business system, please contact Mitel Support.

8.10 Softkeys

Mitel IP Phone softkeys allow users to control voice mail functions through context-sensitive "softkeys" on the telephone. This feature is included with the base software, but can only be used on NuPoint Unified Messaging systems that are integrated with MiVoice Business platforms, using IP integration.

Softkeys are supported when you integrate NP-UM with the MiVoice Office 250.

8.11 Call Director Licensing

Ensure that you have enough Call Director licenses for your organization. One Call Director license is required for each Call Director user. The System Administrator must assign licenses carefully. The licensing logic grants licenses to mailboxes in a sequential and incremental manner. If you assign the Call Director FCOS bit to a group of users in which the number of users exceeds the number of purchased licenses, the users in the upper range of mailbox numbers will not be licensed to use Call Director call flows and will be unable to use the feature. The Call Director license database is updated nightly or upon system reboot. Use the Call Director reports to know which mailboxes have been granted with Call Director licenses.

8.12 Multiple Numbers Associated to Single Mailbox

NuPoint Unified Messaging allows you to assign multiple numbers to a single mailbox. You can associate a total of 5 phone numbers to a mailbox. The first extension is the primary extension and the 4 new ones are the alternate extensions.

8.13 Speech Auto Attendant (SAA)

The Speech Auto Attendant (SAA) is the first speech-enabled application that leverages the VXML and MRCP technology and infrastructure on the NuPoint platform. The Speech Auto Attendant directs calls to the intended party by recognizing the spoken names from the callers. Callers could be internal users or external users to the system. SAA recognizes a spoken name, department name, spoken digits and DTMF digits via a single Voice User Interface (VUI).

SAA supports 1000 directory names (500 names licensing increments), and 15 department names. The NuPoint Unified Messaging of the SAA speech engine supports English for North America and .

Number of the SAA ports is limited to 24.

8.13.1 Line Group for SAA

In order to configure lines to use speech recognition applications, the administrator needs to create line groups in a way similar to creating other line groups on the system. The “Speech Recognition” line group application will not be available if the system has not previously been licensed to perform speech recognition and if the Speech Auto Attendant is not installed on the system. Similarly, the web interface will not allow the administrator to create more lines than have been licensed.

8.13.2 Standalone SAA without NuPoint Unified Messaging

The Speech Auto Attendant can be installed along with NuPoint Unified Messaging or as a standalone application, without any of the voicemail features included in NuPoint.

Existing NuPoint properties displayed in the NuPoint tab (NuPoint User, Mailbox number, Extension number, Pin, FCOS, LCOS, Message Waiting Types and UM e-mail addresses) will be disabled when the Speech Auto Attendant is installed as a standalone application.

8.13.3 Dialing Plan

In order to prevent users from using the Speech Auto Attendant feature as a long distance call proxy, dialing policies allow the administrator to program rules and determine which numbers can be dialed from the Speech Auto Attendant. The dialing policy also allows numbers to be rewritten before the system places the call. Refer to the MiVoice Business System Administration Help on Mitel Document Center for more information on how to set up the dialing policy.

Setting up proper dialing policies can be difficult and it is recommended that the administrator test the policies first before making them effective. In order to do this, you can type a phone number in the field labeled “Enter a phone number to test” and click the “Simulate” button. The result (the call type and the resulting number that would be dialed) will be displayed next to the “Simulate” button.

8.13.4 SAA Backup & Restore

The Speech Auto Attendant user data source configuration, departments, dialing policies, misc. parameters and line group configuration will be picked-up automatically by the current NuPoint backup and restore procedure.

On standalone Speech Auto Attendant systems, the administrator will perform backup and restore using the same text-console menus. Options to backup/restore messages and fax cover pages will not be presented to the administrator on standalone Speech Auto Attendant systems. The same backup/restore strategies (USB, LAN FTP, LAN MS and Hard Drive) will be offered to the administrator.

When the Speech Auto Attendant is configured to use Active Directory or MiCollab as its user data source, the backup and restore will not backup (or restore) any information stored in the Active Directory. **Failure to properly backup Active Directory could result in data being lost.**

8.13.5 Speech Tuning and SAA Customization

The basic speech recognition parameters are used system-wide and will be shared by every speech recognition application hosted on the NuPoint system.

Customers can customize the SAA internal/external announcement prompts, dialing plan, and operator transfer destination. The end user can select the device destination for call transfer (in cases where a user has multiple phone devices).

SAA handles speech ambiguity for more than one person with the same first/last name in the data source by transferring the caller (internal/external) to the operator.

The following speech-related parameters are exposed via the web console interface to allow system tuning to fit into a specific customer’s environment. By default, these

parameters are already fine-tuned with optimal values as part of SAA installation. However, if the administrator needs to further adjust these values, it is recommended to consult with Mitel speech experts first.

8.13.5.1 *Low Recognition Confidence Level*

This value specifies the relative confidence level below which speech recognition results are rejected. The minimum value is 0 and the maximum value is 1, with a two-digit precision. The default value is 0.5.

8.13.5.2 *High Recognition Confidence Level*

This value specifies the relative confidence level above which speech recognition results are implicitly confirmed. The minimum value is 0 and the maximum value is 1, with a two-digit precision. The default value is 0.8.

8.13.6 No Speech Timeout

This value specifies the length of silence that will trigger help prompts to be played to the user. The minimum value is 0 and the maximum value is 60,000 milliseconds. The default value is 10,000 milliseconds. This value can be tuned to 20,000 milliseconds if the customer site runs into issues with external callers experiencing a high rate of misrecognition.

8.13.7 Post-Speech Silence

This value specifies the length of silence that must follow an utterance before the speech recognition engine begins to process it as a complete sentence. The bigger this value is, the longer the pauses are allowed from the users. The minimum value is 0 and the maximum value is 60,000 milliseconds. The default value is 1000 milliseconds.

8.13.8 Output Volume

This value specifies the linear volume that is applied to the output signal before prompts are played back to the users. The administrator can use this parameter to adjust the volume when the signal played to the users is too weak or too loud. The minimum value is 0.0 and the maximum value is 100.0. The default value is 100.0.

8.13.9 Speech versus Accuracy

This value specifies the relative priority of speech vs. accuracy. Using high accuracy algorithms requires more CPU resources and thus limits the number of concurrent speech recognition sessions. The minimum value is 0.0 and the maximum value is 1.0.

Entering “0.0” places the emphasis on speed, while entering “1.0” places the emphasis on accuracy. The default value is 0.5.

8.13.10 Sensitivity

This value allows you to configure the level between background noise and speech, and thus it controls the sensitivity of the speech detector. The minimum value is 0.00 and the maximum value is 1.00. Values approaching 1.00 improve the detection of speech but also increase the detection of background noise and thus utterances need to be spoken with a strong voice so as not to be mistaken with background noise. The default value is 0.5.

8.13.11 Barge-in

This field allows you to enable or disable barge-in for the entire speech recognition engine (that is, the Speech Auto Attendant and every other installed speech recognition application). Barge-in is enabled by default.

8.14 Presence-Enabled Speech Auto Attendant

The Presence feature supports the Office Communications server 2007, IBM Lotus Sametime 8.0, Live Comm Server, and the Mitel Unified Comms Server.

As part of the Speech Auto Attendant application, prior to routing a call to its destination, the Speech Auto Attendant announces the presence status of the called party. This presence information helps the caller determine whether to accept the call transfer or prematurely terminate the call before it reaches voicemail (if the called party’s status is OFFLINE, for example).

If the presence information is not available for a certain user, the speech application will not announce the status. This means that if the presence service (i.e., Proxy) is not available, then the NuPoint speech application still functions as normal.

The Presence Proxy is a NuPoint application that can be enabled on MiCollab. It is packaged as a NuPoint software blade that is installed by default. The Presence Proxy remains dormant until the “NuPoint Messaging: Enable Presence (SAA)” license is purchased and activated. A few minutes after the license is activated, the Presence Proxy will automatically start up and be fully functional.

The Presence Proxy is the broker between an application and a presence server. Because the presence servers require an Active Directory infrastructure, the Presence Proxy can only work where Active Directory is installed and configured. For the presence-enabled NuPoint application (SAA), this means presence is available only when SAA is configured with Active Directory as its user repository. The Presence Proxy supports the connection to just one presence server.

The Presence Proxy communicates with an application over an HTTP transport and with MS presence servers using the Microsoft SIP/SIMPLE interface.

The Presence Proxy provides applications with the current presence state of users. It does not, however, support changing that presence state back on the presence server. It is the responsibility of the presence server and its associated clients to manage the setting of a user's presence state.

The states returned by the Presence Proxy are listed in the following table:

Table 35: Presence States

STATE	MICROSOFT OFFICE COMMUNICATOR EQUIVALENT
Unknown[1]	
Online	Online
Busy	Busy
Be Right Back	Be Right Back
Do Not Disturb	Do Not Disturb
Away	Away
Offline	Offline
[2]	On The Phone[3]
[2]	In a Conference[3,4]

[1] Unknown is returned by the Presence Proxy when an invalid SIP URI is passed as an argument or some other problem prevents it from determining the presence state. In NPM Release 12, SAA will not say a presence state to the caller when it receives Unknown back from the Presence Proxy.

[2] The Presence Proxy will return the underlying state, typically Online, Busy, Away, or Offline.

[3] Available when LCS is integrated with the enterprise phone system (e.g., using the Mitel Live Business Gateway).

2	Presenting[4]
2	Tentative[5]
2	In a Meeting[5]
2	Out of Office[5]

The Presence Proxy is not meant to be deployed in the DMZ, outside of the firewall.

In a NuPoint cluster environment, each NuPoint in the cluster has its own Presence Proxy, and all are connected to a common presence server.

8.15 Trusted Service Support

The MiCollab NuPoint Unified Messaging application is supported as a Trusted Service (application) on MiVoice Business Release 5.0 SP1 and later platforms. Refer to the *MiCollab Installation and Maintenance Guide* for more information on Trusted Service support.

[4] Available when in a Communicator conference.
[5] Available when user has configured Communicator to use Outlook as their Personal Information Manager.

MiVoice Border Gateway Guidelines 9

This chapter contains the following sections:

9.1 Supported Services

MBG provides the following services:

- **Remote MiNET IP Phones**: Formerly known as the Teleworker Solution, this service is the most common use of MBG. It permits remote MiNET phones to securely access the corporate phone network over the Internet.
- **Remote SIP IP Phones**: Permits Teleworker functionality for SIP hard or soft phones over the Internet.
- **SIP Trunking**: Allows a corporate phone switch to connect SIP trunks to a SIP trunk provider, protecting the switch from malformed messages, unauthorized use, and various attacks. It also provides an anchor point for media streams.
- **Call Recording**: Formerly the Secure Recording Connector, this service allows secure recording of phone calls by a third-party application.

MiVoice Border Gateway can be deployed in several ways depending on the services required.

9.2 Embedded MBG Service in MiCollab Deployments

The MBG service that is embedded in the MiCollab server is supported on the LAN only. Deployment of the MBG services on the network edge (Gateway mode) or in the DMZ is not supported.

The safest way to deploy MBG is to leave MiCollab and its applications on the LAN, and deploy a second standalone MBG server in the DMZ. Remote access to the MiCollab server on the LAN is provided via Web Proxy on the Internet-facing MBG server. If centralized management is desired, the two MBG applications can be clustered, with

the LAN server having a weight of zero to prevent sets being directed to it by the load balancer. All changes made on LAN MiCollab server will be reflected on the network edge MBG server.

9.3 Teleworkers and Remote Offices

This is the original design intent of the Teleworker solution. Once a MiVoice Border Gateway is installed, extensions from the office PBX can be extended across the Internet to permit MiNET phones to work from homes, remote offices, hotels, and so forth.

To support Teleworkers on MiCollab, deploy a second server running MBG (either standalone or single-app MiCollab) in the DMZ

Note:

For deployment as an Internet gateway, the external address must be dedicated to the MiVoice Border Gateway, publicly routable, and reachable from both the Internet and the internal network.

Failure to follow these guidelines will result in one-way or no-way audio.

9.4 Secure Recording Environment

When MBG is provisioned with call recording licenses, it can provide a secure man-in-the-middle for call recording. This mode is supported only in a LAN environment.

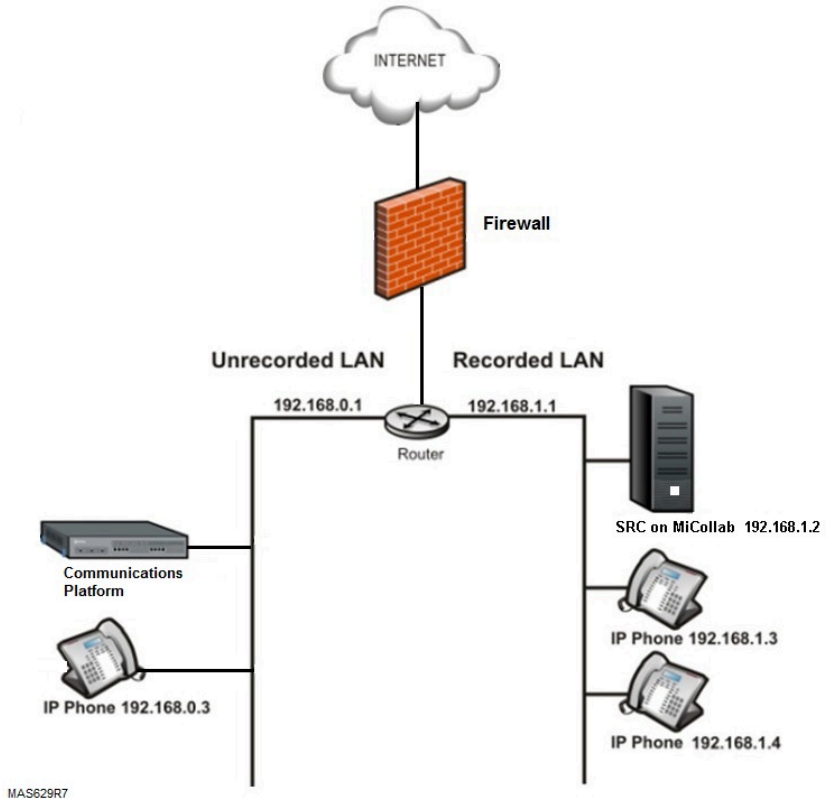
It is advisable to disable MiNET restrictions on the MBG server providing call recording service, as having all LAN sets authenticate through MBG is likely not required.

Teleworker sets connected through an MBG at the network edge can be recorded as well, by configuring the edge MBG such that the desired sets point to the LAN MBG as if it was an ICP.

9.4.1 MBG Deployed on the LAN for Call Recording

When possible, Mitel recommends deploying the MBG call recording server on the same LAN segment as the ICP(s) with which it will be working. However, it is often practical to use a separate segment if not all devices should be recordable.

Figure 17: Sample Call Recording Deployment

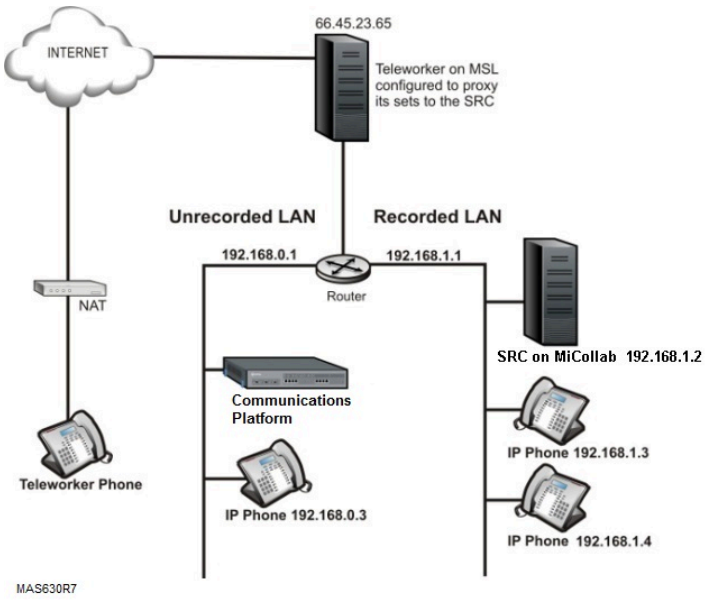


The above figure shows one sample configuration that could be used. The IP phones that are to be recorded are located on the same LAN segment as the server. DHCP is enabled in MSL, and MBG provides DHCP configuration such that the sets use the server as their TFTP server and as their ICP. Then, the MBG proxies the set registrations to the real ICP on the other segment. Sets located on a different LAN segment use the ICP DHCP server to connect directly to the ICP and are therefore not recordable.

As an alternative to changing the network topology, each set that should be recordable could be individually programmed to connect to the MBG.

The following figure below shows an example of a teleworker set connecting through the edge MBG to an MiCollab server for call recording (and finally to the MiVoice Business), so that it can be recorded along with the sets on the Recorded LAN. To configure this scenario, an “ICP” entry is added to the edge MBG containing the IP address of the LAN MBG used for recording. All remote sets that should be recordable must be configured with that “ICP”. The recording MBG will then proxy the remote sets to their real ICP.

Figure 18: Recording Teleworker Sets



Note:

CIS softphone ( ) can function properly in this configuration. However, only the signaling and voice should be proxied through the MBG secure call recording application. Additional applications protocols should be proxied directly from the edge MBG to the CIS server.

Warning:

TO HAVE BOTH TELEWORKER SETS AND CALL RECORDING, YOU MUST USE THE DEPLOYMENT CONFIGURATION SHOWN IN FIGURE 13. COMBINING TELEWORKER SERVICE AND CALL RECORDING OF LAN SETS ON A SINGLE SERVER IS NOT SUPPORTED.

9.5 SIP Trunking

The SIP trunk is established from the communications platform to the SIP trunk provider, using MBG as a SIP-aware firewall and proxy. MBG's SIP trunk service provides:

- NAT traversal of media and signaling
- Media anchoring for the remote provider, regardless of the internal device
- SIP adaptation and normalization to improve interoperability

- Protection from malformed & malicious requests, various types of attack, and request flooding

Some of the key benefits of using SIP trunks are:

- consolidation of capacity; all trunks come to one location, calls routed to branch offices over MPLS or VPN links already in place
- increased simplicity for bandwidth management
- local phone numbers from anywhere in the world to permit customers to reach the company in question easily
- cheaper toll-free service in most cases
- cost savings over PRI/T1/POTS lines
- increased resiliency with the potential for disaster recovery configuration.

9.6 Partial Service Configurations

All MBG services are not available in all supported configurations. This section identifies for each MBG service configurations where the service is not supported at the time of writing. In some cases the service may be technically possible but not currently supported pending further testing or to reduce complexity.

MBG provides the following services:

Remote MiNET IP Phones

- Connecting to MBG in MiCollab on the LAN is not supported for Internet phones.

Remote SIP IP Phones

- Connecting to MBG in MiCollab on the LAN is not supported for Internet phones.

SIP Trunking

- Connecting to a SIP trunk *service provider from MBG in MiCollab on the LAN is not supported.*

Call Recording

- Recording calls with MBG in MiCollab on the network edge is not supported for LAN phones.
- Recording calls with standalone MBG on the network edge is not supported for LAN phones.
- Call recording with MBG is only available for MiVoice Business communication platforms.

9.7 Remote Phone Access

A major function of the MBG application is to allow remote MiNET IP and/or SIP phones to connect to the office PBX over an insecure wide-area network such as the Internet, as if they were physically in the office. Most current (and many older) models of IP sets are supported by MBG. However, please refer to the *Remote IP Phones Configuration Guide* for guidance on specific models. Most SIP devices, including all Mitel-branded SIP devices, can also be configured to work with MBG.

This section provides general guidelines for the Teleworker service. Please refer to page 66 to determine detailed requirements and performance limits.

Remote Phone Access 10

This chapter contains the following sections:

A major function of the MBG application is to allow remote MiNET IP and/or SIP phones to connect to the office PBX over an insecure wide-area network such as the Internet, as if they were physically in the office. Most current (and many older) models of IP sets are supported by MBG. However, please refer to the *Remote IP Phones Configuration Guide* for guidance on specific models. Most SIP devices, including all Mitel-branded SIP devices, can also be configured to work with MBG.

This section provides general guidelines for the Teleworker service. Please refer to page 66 to determine detailed requirements and performance limits.

10.1 Remote Site Requirements

A set in a remote site (such as a home or branch office) is assumed to be part of a wired or wireless LAN behind a simple NAT router that provides access to the Internet, typically through a DSL or cable modem. Mitel IP and SIP phones generally require a 10/100/1000 Mbps Ethernet connection, although some

Mitel IP and SIP phones generally require a 10/100/1000 Mbps Ethernet connection, although some models can be configured for WiFi. (Refer to the device's documentation for configuration details.) All devices expect a TCP/IP network regardless of the link-layer technology.

The remote site router must provide, at minimum:

- 10/100/1000 Mbps Ethernet with RJ45 connectors, for Mitel sets and connection to cable/DSL modem
- NAT from the internal network to the external network

- pass-through of UDP and TCP protocols, including TFTP

The router should provide DHCP service, offering at least an IP address and default gateway. However, devices can be programmed with static IP addresses and settings in the absence of DHCP.

The router may need to support PPPoE/PPPoA when used with a DSL modem, and must be configured with the user name and password provided by the ISP.

The router may need to support Authenticated DHCP (client) when used with a cable modem, and must be configured with the user name and password provided by the ISP.

If WiFi sets are to be used, the router or a separate WiFi access point must also provide 802.11 b/g/n.

The router must control the Internet connection in order for multiple devices to share the connection. When using desktop phones, the use of USB PPPoE/PPPoA modems, USB 3G/4G modems, etc are not supported as they do not provide a port to plug in the phone. However, such devices can be used with softphones running on the PC if no other devices need to share the internet connection of the PC. A similar caveat applies to any service that requires software to be loaded on the PC, such as AOL Broadband. It cannot be used with a desktop device, but can possibly be used with a softphone application such as MiCollab Client.

Note:

The remote site may have a dynamic IP address. However, if the address changes during a call, the call will drop and all devices at the site must re-register with MBG to restore service.

10.1.1 VPN Connectivity

Connecting a PC to the second Ethernet port on the back of a Mitel IP phone does not provide the PC with a VPN connection to the office network. That connection must still be made by use of the organization's supported VPN client software. This ensures that security of the corporate network is maintained when using MiVoice Border Gateway.

A gateway-to-gateway VPN can be constructed between branch offices (or homes) and the main office, if desired, such that all the PCs in the remote office have full access to the corporate LAN. However, Mitel advises that only non-voice traffic should be routed across the VPN; voice traffic between sets and the MBG should traverse the Internet whenever possible. Routing real-time voice protocols across a VPN can result in degraded service.

Mitel Standard Linux, upon which the MBG application runs, does provide a PPTP VPN service. If desired, the MiCollab server can be used as a VPN concentrator for access to the corporate network. However, a VPN is not required to use the features of MBG itself. For more details, see the *Mitel Standard Linux Installation & Administration Guide* (available from Mitel Document Center).

10.1.2 Using an Existing VPN

Using the MiVoice Border Gateway does not affect any existing VPN client software (e.g. IPSEC road warrior connection) installed on the remote PC. The PC should be connected to either the second Ethernet port of the IP phone or directly to the router and the existing software should be used as before.

Note:

VPN (e.g.IPSEC) pass-through must be supported by the router at the remote site.

10.1.3 Corporate Firewall & Network Configuration for VPN Access

The corporate office firewall may need to be reconfigured to allow other traffic from the MSL server to the internal network if the MSL server is used as a VPN server. The ports and protocols required will depend on the applications used by the client PCs and this configuration is outside the scope of this document.

10.1.4 Bandwidth Requirements for the Remote Site

This section analyzes bandwidth requirements of the remote site using the MiVoice Border Gateway. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, e-commerce) must be provisioned as well. Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service provided by the MiVoice Border Gateway.

The table below shows examples of bandwidth required for various types of remote media streams.

Table 36: Bandwidth Requirements of a Single IP Phone

VOICE	IF COMPRESSION (G.729A) ENABLED: 24 KBPS (BI-DIRECTIONAL) IF COMPRESSION NOT ENABLED (): 80 KBPS (BI-DIRECTIONAL)
Collaboration	**192** Kbps (bi-directional)
Collaboration Client Video	**256** Kbps – **1600** Kbps (bi-directional)
MiVoice Video Unit	**512** Kbps – **1500** Kbps (bi-directional)

This table does not consider bandwidth requirements for PCs or other devices, which must be provisioned in addition to the IP Phone. If there is insufficient bandwidth, symptoms experienced by the IP phone user may include degraded voice quality, slow response, service interruption or loss of service. It also does not consider bandwidth requirements for additional applications. See for more information.

Note:

A video call requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings.

A remote MiVoice Video Unit connecting to MBG over the Internet should be configured to disable the H.264 High Profile codec and to disable the Dynamic Bandwidth Allocation option. A video conference should not be initiated from a MiVoice Video Unit on the Internet because it would serve as a bridge and dramatically increase bandwidth requirements for the call.

Video calls between MiCollab Client 6.0 and MiVoice Video Unit 2.0 are supported through MBG but they do not negotiate bandwidth at the time of writing. For example, a MiCollab Client on the Internet will receive video at the rate configured on a MiVoice Video Unit on the LAN even if the MiCollab Client is configured to use low bandwidth. This will be rectified in a future release of MiCollab Client and/or MiVoice Video Unit.

For details and current values, please see the engineering guidelines for the devices/ applications referenced as examples here (available from Mitel Document Center).

10.1.5 Bandwidth Usage and ISP Quotas

Many Internet Service Providers set quotas on the amount of IP bandwidth per month. As an aid in predicting whether a specific quota will be exceeded, this section provides the necessary data and a sample calculation.

Assumptions:

- Signaling channel requires 1 KByte per minute (average), based on 6 calls per hour, business usage, 15 minutes per hour
- Options keepalive and Gap registration enabled for SIP, at 20s and 300s respectively

Table 37: Bandwidth Usage versus Time for an IP or SIP Phone

	BANDWIDTH REQUIRED	HOURLY USAGE (100%)	MONTHLY USAGE (100%)
Signaling (MiNET)	1 KB/minute	60 KB	43.2 MB
Signaling (SIP)	1.75 KB/minute	105 KB	75.6 MB
G.711 voice stream (IP), 20ms	80 kbps	36 MB	25.92 GB
G.729a voice stream (IP), 20ms	24 kbps	10.8 MB	7.78 GB

Note:

20 ms is the default RTP frame size, but the value is configurable in the MiVoice Border Gateway administration panel.

The data in the above table can be used to:

- estimate the available call time given a quota.
- estimate the monthly bandwidth requirement for a given call volume.

Example 1: Estimating Available Call Time

Given an ISP quota of 2 GB/month and continuous use:

- Call hours of G.729a = (2000 MB - 43.2 MB) / 10.8 MB per hour = 181 hours
- Call hours of G.711 = (2000 MB - 43.2 MB) / 36 MB per hour = 54 hours

Given the same 2 GB/month quota, and usage of 15 min/hr, 12 hours per day, 7 days per week:

- Call hours of G.729a = (1448 hours or more than 1 month)
- Call hours of G.711 = (432 hours or roughly 18 days)

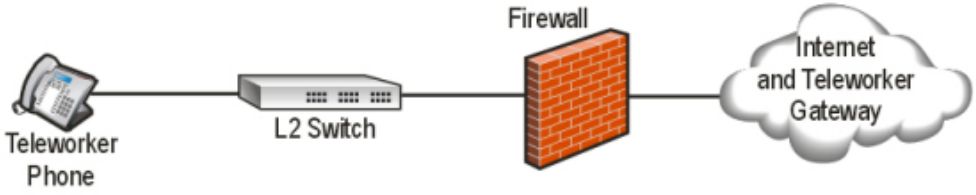
Example 2: Estimating Monthly Bandwidth Requirements

Given a user that averages 4 hours of phone calls per day, for 22 workdays in a month:

- Bandwidth Usage for G.729a = 43.2 MB + (10.8 MB x 4 hr per day x 22 days) = 994 MB
- Bandwidth Usage for G.711 = 43.2 MB + (36 MB x 4 hr per day x 22 days) = 3200 MB or 3.2 GB

10.1.6 Configuring the Remote Site Firewall

Figure 19: Remote Site Firewall



If the remote office has a firewall, it must be configured to allow the IP or SIP phone to connect through it to the MiVoice Border Gateway. The simplest approach is to permit all connections to or from the MBG's IP address. A second very simple approach is to permit all outgoing connections and any responses to them. By default, most small office and home NAT routers allow outgoing connections and responses to those outgoing connections.

Sites with more restrictive security policies may wish to use the following rules:

- Allow a bi-directional TCP connection to destination ports 6801 and 6802 on MiVoice Border Gateway IP address.
- Allow bi-directional TCP connections to destination ports 3998 and 6881 on the MiVoice Border Gateway IP address (for 5235, 5330, 5340 and Navigator set features).

- Allow bi-directional TCP connections to destination port 6881 on the MiVoice Border Gateway IP Address (for MiVoice 69xx Phone avatar support).
- Allow incoming UDP from source ports 20000 to 31000 on MiVoice Border Gateway IP address.
- Allow outgoing UDP to destination ports 20000 to 31000 on MiVoice Border Gateway IP address.
- Allow bi-directional TCP connections to destination ports 36005, 36006, 36007, 36008 and 37000 on the MiVoice Border Gateway IP address, if using Collaboration Client.
- Allow incoming and outgoing UDP to port 5060 on the MiVoice Border Gateway IP address, if SIP support is desired.

10.2 TFTP Behavior

Mitel IP phones require a TFTP server that holds their set firmware and HTML applications. For remote phones, this TFTP service is provided by MBG.

Previous versions of MBG bundled a version of the HTML Applications and served them directly. This approach made it difficult to keep versions in sync, especially with multiple ICPs. MBG does a proxy request to the appropriate ICP instead.

When an IP phone connects to its ICP, the ICP (MiVoice Business) may issue a File Download directive over the SAC protocol connection. MBG intercepts these directives and downloads the file on behalf of the remote set. It then sends a modified directive to the set instructing it to download the cached file from MBG. This ensures that the set receives the same file that it would if it were directly connected to MiVoice Business. MBG checks periodically for updated HTML application files at the ICP. The frequency of checks depends on the feature set supported by the ICP. It could be as often as 10 minutes, and as infrequent as 24 hours.

Note:

MBG's file downloader does not know about any ICPs until sets connect to MBG and thus get connected to an ICP. This step occurs after a set has already retrieved its firmware load via TFTP. Therefore, set firmware loads are still bundled with MBG and are not fetched from the ICPs.

10.3 Configuring MBG for Remote SIP Devices

10.3.1 Remote SIP Device Limitations

MBG cannot yet load-balance SIP devices. In general, resiliency for a SIP device can be achieved through external DNS by configuring multiple “A” records for the FQDN of the MBG, or by configuring SRV records. Refer to the documentation of the remote SIP devices for guidance on configuring resiliency.

10.3.2 Tuning Global Parameters

The default values for all parameters assume a Teleworking installation, with SIP devices being used over the Internet. In a LAN context, these parameters will work correctly but may be slightly aggressive.

By default, MBG sends a SIP “Options” request to every connected device at an interval of 20s (“Options keepalives”). The responses from these requests reset the idle timer for each connection. Each connection has a 300s (5 minutes) idle timeout, so the most important thing to remember is that the MBG server must see valid SIP traffic from each device within the 300s interval. A device that times out due to inactivity is disconnected and becomes out of service.

On a “quiet” network it is sufficient to disable gapped registration and raise the options interval to its maximum value (180s at this time). If all remote SIP devices send their own keepalives or re-register at an interval less than 300s, MBG's Options Keepalives can be turned off.

10.3.3 DNS Support

While SIP clients can address MBG by its IP address, Mitel recommends the use of a fully-qualified domain name (FQDN) in the public Domain Name System (DNS) that resolves to the public IP of the MBG server.

Advantages:

- The IP address of the MBG server can be changed, and the clients will not need to be reconfigured.
- DNS can provide a certain level of resiliency in case an MBG server experiences any kind of service outage. Simply configure the FQDN to resolve to multiple MBG servers. Please note that MBG cannot control how a SIP device behaves when it receives multiple IP addresses in a DNS response.

Note:

A remote SIP message will be recognized as being addressed to MBG if the IP in the URI is one that MBG owns, or the FQDN in the URI either resolves to an IP that MBG owns, or is one of the configured “Allowed URIs” in the “SIP options” section of the Configuration tab.

Warning:

A SIP SERVER REQUIRES FUNCTIONAL DNS EVEN IF ALL DEVICES ARE CONFIGURED TO USE IP ADDRESSES INSTEAD OF FQDNS. MBG IS NO EXCEPTION. FAILURE TO PROVIDE MBG WITH A WORKING DNS RESOLVER OR PREVENTING MBG FROM REACHING THE INTERNET DNS ROOT SERVERS CAN CAUSE DELAYS OR FAILURES IN CALL SETUP.

10.4 SIP Trunking

A “SIP trunk” in the context of MBG is simply a pair of endpoints, defined by their IP addresses and signaling ports. One of the endpoints is usually your ICP and the other is your SIP provider’s firewall or SBC.

A trunk can have any number of “channels,” each of which corresponds to an active media stream. A channel license is required for each active channel, so you will need enough channel licenses to cover the maximum number of active calls. As an analogy, an ISDN PRI link contains 23 B channels for audio and one D channel for signaling, and can carry a maximum of 23 simultaneous calls. This would be equivalent to a SIP trunk with 23 channel licenses.

Note:

On the MiVoice Business the MBG is configured as an outbound proxy in the Network Element form.

Warning:
IN THE 5.X RELEASE AND HIGHER, THE CONNECTOR LISTENED ON 5064 BY DEFAULT. AS OF MBG 6.0 THE SIP CONNECTOR CAN HANDLE DEVICE ENDPOINTS, SO 5060 IS USED FOR BOTH DEVICES. THE LEGACY CONNECTOR CAN NO LONGER BE RE-ENABLED AS OF MBG 8.0 OR HIGHER. IF UDP PORT 5064 IS IN USE THEN YOU WILL NEED TO CONTACT YOUR SIP TRUNK PROVIDER TO HAVE THEIR EQUIPMENT CHANGED TO USE MBG'S 5060 BEFORE UPGRADING MBG.

Warning:
A SIP SERVER REQUIRES FUNCTIONAL EVEN IF ALL DEVICES ARE CONFIGURED TO USE IP ADDRESSES INSTEAD OF FQDNS. MBG IS NO EXCEPTION. FAILURE TO PROVIDE MBG WITH A WORKING RESOLVER OR PREVENTING MBG FROM REACHING THE INTERNET ROOT SERVERS CAN CAUSE DELAYS OR FAILURES IN CALL SETUP.

10.4.1 Bandwidth Requirements

See Sizing Your Installation.

10.4.2 Resilient Trunk Configuration

This section describes a sample resilient SIP trunk configuration using two ICPs and two MBGs.

First, configure resiliency between the ICPs.

On ICP “A”:

- Create a Network Element Assignment for MBG “A” (as type Outbound Proxy) and another for the SIP provider’s SBC (as type Other). Create a SIP Peer Profile for the SBC using MBG “A” as the Outbound Proxy.
- Add a Network Element Assignment for MBG “B” (as type Outbound Proxy) and create another SIP Peer Profile for the SBC using MBG “B” as the Outbound Proxy.
- Program a Route List in ARS with SIP peer “A” and SIP peer “B”. Then program ARS Digits Dialed such that outgoing calls use the new route list.

Repeat the above configuration on ICP “B”, except reverse the order of trunks in the route list so that “B” comes before “A”.

Configure MBG clustering. On the master MBG, go to the “ICPs” tab and add both ICP “A” and ICP “B”. On the “SIP Trunking” tab, configure a trunk profile for the remote SBC.

Add a single routing rule of “*” with ICP “A” and ICP “B” as the targets of the rule. This configuration will propagate to the secondary MBG.

Incoming calls from the SBC will arrive at either MBG A or MBG B. From there, the MBG will route them to ICP A if it is up, or to ICP B if ICP A is down. Outgoing calls from either ICP can be routed through either MBG.

10.5 DNS Support

While the ICP can address MBG by its IP address, Mitel recommends the use of a fully-qualified domain name (FQDN) in the public Domain Name System () that resolves to the public IP of the MBG server.

Advantage:

- The IP address of the MBG server can be changed, and the ICPs will not need to be reconfigured.

Note:

An ICP SIP message will be recognized as being addressed to MBG if the IP in the URI is one that MBG owns, or the FQDN in the URI either resolves to an IP that MBG owns, or is one of the configured “Allowed URIs” in the “SIP options” section of the Configuration tab. Typically, the hostnames you add to the “Allowed URIs” list will be for the SIP service provider's session border controller or service domain.

Warning:
A SIP SERVER REQUIRES FUNCTIONAL EVEN IF ICPS ARE CONFIGURED TO USE IP ADDRESSES INSTEAD OF FQDNS. MBG IS NO EXCEPTION. FAILURE TO PROVIDE MBG WITH A WORKING RESOLVER OR PREVENTING MBG FROM REACHING THE INTERNET ROOT SERVERS CAN CAUSE DELAYS OR FAILURES IN CALL SETUP.

10.6 Call Recording

MBG includes the ability to act as a secure man-in-the-middle for SRTP voice streams, enabling a third-party call recording solution to tap calls by using MBG’s SRC interface.

See Sizing Your Installation on page 66 to determine performance limits and resource requirements.

10.6.1 Call Recording versus Local Streaming

MiVoice Border Gateway supports both Local Streaming and Call Recording, both of which can be enabled or disabled for individual users. These options are not compatible.

Local Streaming is a generally desirable feature that reduces bandwidth needed for voice/video calls by allowing the RTP stream(s) to bypass the MBG when two devices are able to communicate directly. However, this means such calls cannot be recorded. If both *Local Streaming and Call Recording are enabled on a device, Call Recording wins*. All streams to and from that device will go through MBG so they can be recorded.

10.6.2 Indirect Call Recording

Indirect Call Recording (ICR) is a feature supported by MiVoice 53XX series IP sets and MiVoice Business software release 5.0 SP1 and higher. It also has only limited support from CRE vendors.

With ICR in place, SRC can support recording of any supported sets that are connected to any supported MiVoice Business without having to reconfigure the sets to connect through SRC, as is the case with “direct” call recording. SRC can be configured with a mix of both ICR and "direct" call recording. This would be required if non-supported sets or MCDs are deployed.

Using ICR allows for some cost reductions and more network flexibility in certain call recording deployments. It is especially applicable for network deployments where centralized call recording is desired in a network situation where remote, WAN-connected sets are connected to remote office MiVoice Business systems.

10.7 Additional Application Requirements

MBG allows the use of several supported applications from remote sites, just as it allows use of IP phones. When MBG is deployed in the DMZ of a third-party firewall, that firewall must be configured to allow connections from these applications.

10.7.1 MiCollab Client 3.0+

Warning:
MBG 7.1 REQUIRED A PORT-FORWARDING RULE FOR PORT 36008 THAT DIRECTED TRAFFIC TO THE COLLABORATION CLIENT SERVER. AFTER UPGRADING TO MBG 7.1 OR HIGHER, THIS RULE MUST BE REMOVED FROM THE MSL PORT FORWARDING PANEL.

The following additional rules are required, excluding the Collaboration Client softphones:

From the Internet to the MBG server:

- allow protocol TCP, destination ports 36005 – 36008 (inclusive)

From the MBG server to the LAN:

- allow protocol TCP, destination ports 80, 443, 5060, 36008

Note:

When Collaboration Client server is behind MBG, remote clients require access via Web Proxy for Collaboration Client 5.1 and above.

Collaboration clients also include MiNET and SIP softphones.

MBG 8.0 includes two additional connectors to help with specific kinds of Collaboration Client SIP softphone connectivity issues that may be experienced in some deployments due to improper handling of SIP UDP by some NAT firewalls. These MBG connectors allow the configuration on selected Collaboration Client SIP softphones to be changed from SIP UDP signaling to use SIP TCP or SIP TLS signaling (TLS preferred). When the selected Collaboration Client SIP softphone connects to MBG on TCP or TLS from the Internet, the MBG bridges it internally to the SIP UDP connector used by default for the unmodified Collaboration Client SIP softphones.

The following additional rules are required for Collaboration Client SIP softphone signaling over TCP or TLS:

From the Internet to the MBG server:

allow protocol TCP, destination ports 5060, 5061

10.7.2 Mitel Contact Center

The following additional rules are required:

From the Internet to the MBG server:

- allow protocol TCP, destination ports 35001 – 35008 (inclusive), 36000 – 36004 (inclusive)

From the MBG server to the LAN:

- allow protocol TCP, destination ports 80, 443, 1443, 5024 – 5026 (inclusive), 5030, 7001, 7003, 8083, 8084, 8188, 42440

The following additional rules are required, at minimum:

From the Internet to the MBG server:

- allow protocol TCP, destination port 443

From the MBG server to the LAN:

- allow protocol TCP, destination port 443

10.7.3 Special consideration for MiCollab AWV through Web Proxy

In addition to https traffic, AWV requires pass-through of its ConnectionPoint connection. It will arrive at the firewall on TCP port 443, on a dedicated IP address for AWV (see the MiCollab documentation for full details), and the firewall must forward the traffic to the server (MBG) at whatever listen port is configured in Web Proxy.

From there, the traffic will be forwarded to the AWV server on the LAN on TCP port 4443. The required rules are:

From the Internet to the Firewall:

- allow protocol TCP, destination port 443 on the AWV IP address

From the Firewall to the (MBG):

- allow protocol TCP, destination port A, where A is the listen port for AWV configured by the administrator

From the (MBG) to the AWV server on the LAN:

- allow protocol TCP, destination port 4443

10.8 Advanced Options

10.8.1 Streaming Addresses

The MBG server will automatically determine the correct IP addresses to which endpoints must send their (S)RTP, if the server has been put into a standard, supported configuration and the correct network profile for that configuration has been chosen.

However, sometimes it is necessary to override the default streaming addresses, typically due to a non-standard configuration. When the administrator views the Network profiles (under the Configuration tab), the current network profile is shown with an interface to apply the supported network profiles.

Arbitrary addresses can be entered by selecting the Custom profile, if the “canned” configurations are not suitable. These addresses are used during signaling to inform the endpoints where to send RTP. If they are incorrect, there will be audio problems (typically one-way audio or no audio).

10.8.2 Gateway Deployment Profile

A standard example of the gateway deployment is shown in Figure 29 on page 101. In this configuration, the WAN interface on the server is routable on the “public” network. This is referred to as the “set-side” streaming address, to which teleworker devices and service provider trunk equipment sends RTP. The “public” network is typically the Internet, but may instead be a managed service-provider network, MPLS LAN extension, corporate network, and so forth.

The LAN interface is attached to the private network. This is referred to as the “ICP-side” streaming address, to which LAN devices (phones), conference bridges, ICPs, voicemails, etc send RTP. The private and public addresses must be on different IP networks.

The defaults are usually acceptable. However, if not, they can be changed by using the Custom profile.

10.9 RTP Frame Size

By default, the RTP frame size is auto-negotiated between the endpoints. A size of 20ms is common in North America, with 40 ms becoming common in Europe. If needed, the administrator can force use of a particular frame size. For example, some SIP trunk service providers insist on a particular RTP frame size.

The Configuration tab holds the global master setting. This setting is used as the default, and should be left on “Automatic” unless there is a pressing need to change it. Overrides can be placed on specific devices and trunks as required. For example, certain wireless networks handle RTP streams using larger (for example, 40ms) packets better than streams using smaller ones.

Note:

The frame size override only affects the streams to and from devices. The ICP-side streaming is always auto-negotiated. On SIP trunks, both WAN and ICP sides can be specified separately.

10.9.1 TFTP Block Size

MiNET devices use the TFTP protocol to fetch their firmware from the MBG server. The Mitel TFTP server is slightly non-standard – it uses symmetric UDP to traverse NAT devices, and a “sliding window” to improve performance – but is otherwise RFC-compliant.

The default block size in the TFTP protocol is 512 bytes, and with large firmware loads in a lock-step protocol like TFTP[6] this can take a prohibitively long amount of time to download. MBG employs the TFTP “blksize” option to attempt to transfer 4096 byte blocks, if possible. Depending on one’s network this may or may not be possible: the large packets will require fragmentation on a standard Ethernet network with a 1500 byte MTU, and some ISPs do not permit this.

Set the global TFTP block size to the largest value that works. Only the options in the pulldown (512, 1024, 2048 or 4096) are permitted.

10.9.2 Set-side Codec

MBG allows transcoding from G.711 to G.729 or from G.729 to G.711, if Compression licenses have been purchased. The usual use of this is to force a lower-bandwidth codec for remote devices. However, it can also be used to force G.711 for devices that do not support G.729 (e.g. voicemail systems) and that register to MiVoice Business as a MiNET IP device.

The global default setting is found under Configuration; Settings; MiNET Options, but the codec can also be set for each individual device.

[6] Receipt of each block must be acknowledged before the next block is sent.

10.9.3 SRTP Port Range

Each active call on the MBG requires two UDP ports for the RTP stream. Some SIP calls (video, T.38) may require four or more ports. (Two ports per SDP media line are required.) Ports are only used while calls are actually active, and are released upon the end of the call, or, for MiNET, end of the stream (which may be a hold or transfer, not actually the end of the “call”).

The default SRTP port range of 20000-31000 provides enough ports for over 5000 simultaneous voice calls or 2500 video calls. For smaller sites, this range can be reduced if desired. However, be sure any third-party firewalls have the matching range programmed. Mismatches between a DMZ firewall and the MBG will result in some calls having no audio (or one-way audio). This problem appears after many successful calls and is cleared by a reset of the MBG.

10.10 Sizing your Installation

MBG installations come in many sizes, from a handful of remote workers, to large call centers with recording requirements, to service providers with hundreds of SIP trunks routed to customer MiVoice Business systems. This section provides guidelines for selecting appropriate hardware and network capacity for any size of installation.

For site with fewer than 500 users and 100 simultaneous streams, skip to on Determine Call Equivalents.

Note:

The calculations in this section assume that no other applications besides MBG will be running on the MSL server.

10.10.1 Determining Line Size for Large Sites

10.10.1.1 *Step One: Determine Call Rate*

The first step is to estimate how busy the site will be. Ideally, this figure will come from observations of actual usage, but it can be estimated. The services provided by the MBG server affect how much load it needs to handle.

Consider a typical teleworker scenario: 20 users working in a remote office. Assume that these users are on the phone about 10 minutes of each hour, or 6 CCS. If the users make two calls per hour, each call is 300s (5 minutes) long.

Multiply the average CPH rate by the total number of users to get the Erlang-B lambda value:

λ = 2 CPH x 20 users = 40 CPH

A call center might have usage of 20 CCS per agent. Assume an average call time of 600s (10 minutes). If the agent is busy 2000 call-seconds (20 CCS) and each call is 600s, the agent is handling 3⅓ calls per hour. For a busy call center with 1000 agents, lambda is:

λ = 3.3333 CPH x 1000 users = 3333.3 CPH

10.10.1.2 *Step Two: Determine Service Rate*

The service rate, represented by μ, is the mean number of calls the MBG can handle successfully per unit of time, without blocking. If it takes 20 minutes to service one call, then three calls can be serviced per hour, and the service rate is 3 CPH.

In the teleworker example above, the call duration is 300s, so MBG is processing 12 calls per hour:

μ = 12

In the call center example, the call duration is 600s, so the MBG is processing 6 calls per hour:

μ = 6

10.10.1.3 *Step Three: Determine Grade of Service*

The *grade of service*, represented by *P(b)*, is the percentage of calls that are turned away (blocked) because of insufficient capacity. The nominal and recommended P(b) is 1%, or 0.01.

10.10.1.4 *Step Four: Erlang-B Calculator*

An Erlang-B calculator can now be used with the values above to find the number of lines required to handle the load. (Free Erlang-B calculators are widely available online.) Following the teleworker example above, the Erlang-B calculation is:

λ = 40, μ = 12, P(b) = 0.01

c = 9

The site will need 9 lines to handle the load. In MBG terms, this is 9 simultaneous calls. The number of simultaneous calls is the key value in determining MBG resource requirements.

For the call center example:

λ = 3333.3, μ = 6, P(b) = 0.01

c = 583

The call center would require 583 lines (and agents) to handle the call volume. Again, this is 583 simultaneous calls going through the MBG.

10.10.2 Determine Call Equivalents

The next step is to determine the impact of transcoding, taps, and codec choices on CPU load and network bandwidth. The baseline is a single non-transcoded call with one RTP stream. The procedure in this step applies a load factor to convert more complex calls into an equivalent number of simple calls.

Table 38: Call Equivalents

USAGE	CALL EQUIVALENT (CPU)
Basic (non-transcoded) call	1
Transcoded call	3
SIP trunk call	1
Tapped call	1.2

Example:

4 MiNET sets all in calls with other parties, plus 2 SIP trunk calls, and two of the calls being tapped, all using G.711, would constitute:

CPU use = (4 MiNET calls – 2 tapped) + 2 SIP trunk + 2 tapped

= 2 untapped + 2 trunk + 2 tapped

= 2 + 2 + 2#x#1.2

= 6.4 calls

10.10.3 Determine Bandwidth Requirements

VoIP devices, including phones and SIP trunks, use RTP/SRTP for voice communication. The bandwidth required for the RTP stream depends on the codec selected by the device. MiVoice Border Gateway supports the use of G.711, G.729, and G.722.1. Typically, there will be other requirements for Internet access, and these requirements (such as e-mail, web browsing, and e-commerce) must be considered as well.

Failure to provide sufficient bandwidth for all Internet activities may compromise the quality of service of the MiVoice Border Gateway.

The bandwidth figures for a single device are provided in *Bandwidth Requirements for the Remote* Site on page 57. For multiple devices, follow the procedure below.

Assumptions:

- Internet Service Providers specify bandwidth available to the user (that is, PPPoE overhead does not need to be included in the provisioning of DSL bandwidth, but IP overhead does need to be included).
- RTP Bandwidth Requirements are as follows:
  - G.711 = 80 Kbps
  - G.729 = 24 Kbps
  - G.722.1 = 48 Kbps
- At 6 calls per hour Control stream bandwidth requirement is 20 Kbps peak for each 12 remote devices, and 1 Kbps idle for each remote device.
- The calculation below does not include bandwidth required for features such as paging. If group paging is enabled for teleworkers, an additional RTP stream should be provisioned for each remote member of the paging group.
- Whenever possible, transcoding should be performed by the ICP rather than the MiVoice Border Gateway, as this typically provides improved voice quality.

If the mix of codecs in use cannot be reliably estimated, it is safest to assume G.711 for all calls.

Note:

The actual bandwidth available will likely be less than the amount of bandwidth the ISP advertises. Also, the amount of available bandwidth may fluctuate throughout the day based on usage patterns of other subscribers.

The best way to determine the amount of available bandwidth is to use a speed test tool, preferably one provided by a third party rather than the ISP themselves – buyer beware.

10.10.3.1 *G.711 Calculation*

Bandwidth = number of users x idle control stream requirement

+ number of calls x RTP requirement

+ number of users / 12 x peak control stream bandwidth

For the teleworker example of 20 remote users:

20 x 1 Kbps + 9 x 80 Kbps + 20/12 x 20 Kbps = 773 Kbps

For the call center example of 1000 remote agents:

1000 x 1 Kbps + 583 x 80 Kbps + 1000/12 x 20 Kbps = 49307 Kbps or 48.15 Mbps

10.10.3.2 *G.729a Calculation*

Bandwidth = number of users x idle control stream requirement

+ number of calls x RTP requirement

+ number of users / 12 x peak control stream bandwidth

For the teleworker example:

20 x 1 Kbps + 9 x 24 Kbps + 20/12 x 20 Kbps = 270 Kbps

For the call center example:

1000 x 1 Kbps + 583 x 24 Kbps + 1000/12 x 20 Kbps = 16659 Kbps or 16.27 Mbps

10.10.3.3 *Video Calculation*

Some VoIP devices support video as well as voice, and extra bandwidth must be provisioned if video calls will be made. Although the exact bandwidth required depends on the content of the image, number of frames per second (fps), the codec and compression selected, and the video resolution, the list below gives approximations for some typical video streams.

Table 39: Video Bandwidth Requirements

CODEC	RESOLUTION	FPS	BANDWIDTH
H.263 or H.264	QCIF (176x144)	15	~ 128 kbps

		30	~ 256 kbps
	CIF (352x288) or QVGA (320x240)	15	~ 384 kbps
		30	~ 768 kbps
MPEG-4	CIF (352x288) or 320x240	15 – 30	~ 128 – 360 kbps

The following table shows the bandwidth required for video streams from some Mitel devices contrasted with bandwidth required for other types of media streams.

Table 40: COMPARISON OF BANDWIDTH REQUIREMENTS

Voice	**If compression (G.729a) enabled: 24 Kbps (bi-directional)** **If compression not enabled (): 80 Kbps (bi-directional)**
Collaboration	**192** Kbps (bi-directional)
Collaboration Client Video	**256** Kbps – **1600** Kbps (bi-directional)
MiVoice Video Unit	**512** Kbps – **1500** Kbps (bi-directional)

Note:

A video call requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings.

The Internet bandwidth provisioned at the MBG server must take into account the maximum number of simultaneous video calls from the remote devices and applications.

When a MiVoice Video Unit initiates a video conference it will also serve as the video bridge for the conference. For example, a MiVoice Video Unit that is acting as a video

bridge for a 4 party conference will require three times the video bandwidth and three times the audio bandwidth required by a MiVoice Video Unit that is only a participant in the conference.

Video calls between MiCollab Client 6.0 and MiVoice Video Unit 2.0 are supported through MBG but they do not negotiate bandwidth at the time of writing. For example, a MiCollab Client on the Internet will receive video at the rate configured on a MiVoice Video Unit on the LAN even if the MiCollab Client is configured to use low bandwidth. This will be rectified in a future release of MiCollab Client and/or MiVoice Video Unit.

MiCollab voice and video conferencing between clients via the conferencing server is also supported through MBG. The bandwidth usage per video stream is configurable on the conferencing client. An additional consideration is that a conferencing client can receive multiple video streams, one for each video participant in the conference. That number can be reduced at the conferencing client by minimizing or closing video windows.

For details and current values, see the engineering guidelines for the devices/ applications referenced as examples here (available from Mitel Document Center).

10.10.3.4 *Fax Calculation*

A fax call made over a SIP trunk or to a SIP device supporting fax will be either a G.711 voice stream or a T.38 fax session. For the purposes of bandwidth calculations, consider both cases to be an 80 kbps G.711 stream.

10.10.3.5 *Call Recording Calculation*

When using MBG's Secure Call Recording service, a third-party Call Recording Equipment (CRE) device registers to MBG and requests “taps” of calls in progress. The control connection is an SSL-encrypted TCP stream authenticated by an X.509 client certificate provided by the CRE. (Refer to the *MBG Installation and Maintenance Guide* for information on the process used to obtain and install the CRE certificate.)

A small amount of bandwidth is used for the CRE control connection. However, it is usually insignificant when compared to the volume of voice traffic, and can be safely ignored. A small amount of CPU load is also incurred for the control connection. Again, it is usually insignificant compared to the load of processing voice signaling and RTP.

MBG makes a copy of the RTP streams for each call that is being recorded, and forwards them to the CRE. Therefore, each tapped call requires 50% more bandwidth than an untapped call. Only audio is recorded; any video or T.38 streams should be ignored when calculating call recording bandwidth requirements. Simply estimate the number of calls that will be recorded simultaneously and multiply by the codec in use. When in doubt, it is safest to assume G.711 for all calls.

For example, assume that 10 calls will be recorded at a time. All calls are G.711.

Bandwidth = 10 calls x 80 kbps

= 800 kbps

The site requires 800 kbps on top of the bandwidth used by the calls themselves.

Note:

When transcoding, the bandwidth requirements are different on the two “sides” of the MBG.

10.10.3.6 *Example Bandwidth Calculation*

A site has 48 SIP trunks shared by remote and in-office users. Most users are in the office, but 100 work in various remote branch offices with Teleworker phones hosted on a MiVoice Business at the main office. Remote phones are configured for G.729 to save bandwidth, and all SIP trunk calls are G.711. (MiVoice Business handles any transcoding.) In addition, the site records up to 10 remote office calls at any given time.

At peak, the site uses 40 trunk channels and 75 of the remote users are in a call. Ten percent of the remote users are in Collaboration Client video calls configured to match the lowest bandwidth setting of a MiVoice Video Unit device.

The system is deployed in gateway mode, in parallel with the company firewall.

Step one: G.711 trunk calls

WAN BW = 40 channels x 80 kbps

= 3200 kbps

LAN BW = 40 channels x 80 kbps

= 3200 kbps

Step two: Remote office calls; voice

WAN BW = 75 x 24 kbps

= 1800 kbps

LAN BW = 75 x 24 kbps

= 1800 kbps

Step three: Remote office calls; video

10% of 75 users = 7.5

WAN BW = 7.5 x 512 kbps

= 3840 kbps

LAN BW = 7.5 x 512 kbps

= 3480 kbps

Step four: Recorded calls

LAN BW = 10 tapped calls x 24 kbps= 240 kbps

Step five: Totals

Adding up the results from the four steps, the WAN bandwidth requirement is 3200 + 1800 + 3840 kbps for a total of 8840 kbps. The site will require at least a 9 megabit connection just for voice and video capacity. The LAN bandwidth, which includes tapped calls, is 3200 + 1800 + 3840 + 240, or 9080 kbps.

Note:

For a server in LAN mode or in a DMZ (with a single NIC), calculate the bandwidth required for the WAN “side” (no tap streams) and LAN “side” (including tap streams) and add them together, since one NIC handles all of the traffic. In the example above, the network would have to handle 8840 + 9080 = 17920 kbps, or 17.9 Mbps. However, the WAN pipe still only has to handle 9 Mbps.

Also see the following sections:

- Web Proxy Requirements on page71
- MiCollab Client and Conferencing Requirements on page 71
- Mitel Contact Center Softphone Requirements on page 72.

10.10.4 Web Proxy Requirements

The bandwidth requirements for any and all applications proxied by Web Proxy are documented in their respective Engineering Guidelines, and are beyond the scope of this document.

10.10.5 MiCollab Client and Conferencing Requirements

MiCollab Client with Softphone module counts as a remote IP set, with additional bandwidth required for its login and presence. The login and presence connections use negligible bandwidth and do not require real-time priority. The MiCollab Client SIP Softphone supports video calls, which requires 10 to 20 times more bandwidth than a compressed audio call even when configured with the lowest bandwidth settings (see section 12.3 for examples).

MiCollab AWV with video between clients via the server is also supported through MBG, which requires significantly more bandwidth than audio calls (see section 12.3 for examples).

A MiCollab AWV collaboration connection can also require considerable bandwidth, based on the features used, the number of presenters, and the number of participants. The table below provides a typical use-case by number of presenters and participants, with the estimated bandwidth required. For more details, refer to the MiCollab Engineering Guidelines.

Note:

The table assumes the following settings

PowerPoint sharing: enabled

Desktop/App Sharing: disabled

Audio Setting: good

Video Setting: low

The collaboration bandwidth is in addition to that required for voice communications.

Table 41: Bandwidth Requirements for MiCollab Client Collaboration

PRESENTERS	PARTICIPANTS	BANDWIDTH REQUIRED
1	1	192 Kbps
1	2	256 Kbps

1	5	448 Kbps
2	2	460 Kbps
2	5	736 Kbps
1	10	768 Kbps
2	10	1.2 Mbps
2	50	4.9 Mbps
5	100	18.7 Mbps

10.10.6 Mitel Contact Center Softphone Requirements

MBG supports the Mitel Contact Center Softphone. The softphone has multiple components. Bandwidth requirements of the voice component are identical to any other Mitel set using G.711 or G.729 (compression). In addition to voice, Mitel Contact Center Softphone supports the following connections through the MBG server:

Table 42: Softphone Requirements

USED	DEFAULT DESTINATION PORT	DESCRIPTION
TCP 36000	TCP 80	HTTP authentication and user profile access
TCP 36001	TCP 443	HTTPS authentication and user profile access
TCP 36002	TCP 5024	Real-time client
TCP 36003	TCP 5025	Auditor connection

TCP 36004	TCP 5026	Telephony proxy

The “MBG Server Port Used” column indicates the port on which MBG listens, on its Internet-facing side, for the incoming connection. The “Default Destination Port” is the port on the server to which MBG routes the connection. Additional Mitel contact center connections were added over multiple releases and as of MBG 8.0 also include MBG Server TCP ports 35001 to 35008 inclusive. Refer to Mitel Contact Center on page 64 for firewall configuration instructions.

Bandwidth requirements will vary depending on the type of activity being performed. During installation of the client, software is downloaded and installed. The client periodically checks for updates and may download and install them. The bandwidth required by these tasks is not included in the tables below; it is assumed to be part of the bandwidth used by the user's PC.

When a user first launches the client and selects devices to view, there is a database transfer. The size of the database depends on the objects selected, as follows:

1 Queue (Q) = 65 KB1

Agent (A) = 39 KB

1 Employee = 20 KB

1 Extension = 17 KB

1 Network Monitor (NM) (1 x MiVoice Business) = 56 KB

Refer to the following table to determine the size and download time for the database at various line speeds.

Table 43: Download Times

# OF DEVICES	CONFIG	DATA SIZE	512 KBPS	1024 KBPS	1.54 MBPS	2.048 MBPS	10 MBPS
5	1Q, 1A 1Ex, 1Em, 1NM	157.6 KB	00:00:02	00:00:01	00:00:01	00:00:00	00:00:00
50	15Q, 11A, 11Ex, 12Em, 2NM	303.2 KB	00:00:04	00:00:02	00:00:01	00:00:01	00:00:00

100	25Q, 25A, 22Ex, 25Em, 3NM	348.8 KB	00:00:06	00:00:03	00:00:02	00:00:01	00:00:00
500	200Q, 100A, 92Ex, 100Em, 8NM	1.304 MB	00:00:20	00:00:10	00:00:06	00:00:05	00:00:01
1500	500Q, 300A, 385Ex 300Em 15NM	3.528 MB	00:00:55	00:00:27	00:00:18	00:00:13	00:00:02
5000	2086Q, 2379A, 247Ex, 322Em, 16NM	14.24 MB	00:03:42	00:01:51	00:01:13	00:00:55	00:00:11
8100	3036Q, 4379A, 247Ex, 322Em, 16NM	22.72 MB	00:05:55	00:02:57	00:01:57	00:01:28	00:00:18

Note:

The use of traffic shaping (to prioritize RTP ahead of other packets) at the remote site is recommended, to prevent data transfers, such as the initial DB transfer above, from affecting calls in progress.

The table below provides bandwidth requirements for a typical contact center configuration at various call rates, in addition to the bandwidth required for voice communications.

Table 44: Bandwidth Requirements

CALLS PER HOUR (CPH)	BANDWIDTH PER ICP	BANDWIDTH PER REAL-TIME CLIENT
100	0.48 kbps	0.48 kbps
1000	4.88 kbps	4.72 kbps
2000	9.76 kbps	9.44 kbps

3000	14.72 kbps	14.16 kbps
4000	19.6 kbps	18.88 kbps
5000	24.48 kbps	23.6 kbps
6000	29.36 kbps	28.32 kbps

Note:

This is a guideline only. Actual results may vary with each contact center configuration.

MiCollab AWV Guidelines 11

This chapter contains the following sections:

11.1 Specifications and Requirements

Hardware, software, network, and communication platform specifications and requirements for MiCollab AWV are defined in accordance with MiCollab server specifications. To use MiCollab AWV and the Collaboration Client application, the user's computer must meet the requirements detailed in the *MiCollab Audio, Web and Video Conferencing User Help*.

Note:

Web client users must allow popups when joining a conference by turning off their popup blocker or allowing the popup when prompted.

11.2 Capacity

The capacity and performance information for MiCollab Audio, Web and Video Conferencing provided in this section is based on single-application MiCollab server deployment. If you are running multiple applications on the MiCollab server, the capacity and performance of MiCollab Audio, Web and Video Conferencing are affected, depending on the loading of server resources with the other applications running. In addition, capacities are also affected if MiCollab is run in a virtualized environment.

AWV DEPLOYED AS SINGLE-APPLICATION MICOLLAB SERVER			
	Audio	Web	Video
Maximum ports per system	500	500	300
Maximum ports per conference	300	300	100

Note:

Five hundred audio ports are supported on a single MiCollab Audio, Web and Video Conferencing application on MiCollab. The system supports up to 500 audio ports at the same time, with up to 300 per single conference.

Note:

The system can support up to 70 users joining an audio conference concurrently. When a higher number of users attempt to join the conference concurrently, some of the users might be denied access to the conference. These users might be able to join the conference if they call again after 30 seconds.

Note:

The MiVoice MX-ONE Hunt Group supports up to 160 members. In order to exceed this number in the support of 500 AWV ports, the hunt groups can be cascaded and daisy chained. Refer to the MiVoice MX-ONE documentation "Internal Group Hunting" - 35_15431 for instructions on how to daisy chain hunt groups to support more than 160 ports.

Note:

In addition to telephone devices calling into a conference, the Browser audio feature (1-way audio streaming) also uses one audio port/license on the system. The Windows audio feature (2-way audio streaming) uses one audio port/license on the system. The first client connecting with web client audio uses two ports.

The system will negotiate G.729, G.722, G.722.1 or G.711 calls based on the incoming call settings. Once the system reaches the G.729 port setting (combined in all conferences), the system will offer G.711 for all additional calls into the bridge up to the maximum per conference limit.

Note:

The G.729 port setting is found under system options. It has a range of 0-100 (where 0 indicates G.729 ports are disabled).

11.2.1 Audio-Only Conference

The following capacities are supported for audio conferencing:

- Total number of concurrent audio conference users: 500
- Maximum number of users per audio conference: 300

A maximum of 100 concurrent users with G.729 encoding can connect to all audio conference calls in progress. Once the maximum number of G.729 ports has been reached, additional users with G.711 encoding can connect and join an audio conference up to the supported limits.

Note:

MiCollab Audio, Web and Video Conferencing supports a maximum of 100 G.729 ports is a single application configuration and a maximum of 50 ports on MiCollab running multiple applications.

11.2.2 Web-Only Conference

Note:

Terminal server environments, such as Citrix® and Remote Desktop, do not support video.

Higher bandwidth requirements are necessary to support Web conferencing collaboration features. The MiCollab Audio, Web and Video Conferencing server does not prevent more than the supported limits, it only tracks what is licensed. The following capacities are supported for Web conferencing:

- Total number of concurrent Web conference users: 500
- Maximum number of users per Web conference: 300

11.3 Determining Bandwidth

Note:

Bandwidth is a significant factor for performance during a Web conference or a Video call and MiCollab Audio, Web and Video Conferencing server resources (CPU and memory) usage is minimal.

The following is a scenario to help determine approximate usage type and measure the amount of bandwidth required. Video quality and frames per second (fps) are features that are configurable by the individual user according to their preference. Combine the collaboration bandwidth (Table 43) and video bandwidth (Table 44) for the number of users to estimate the total bandwidth required.

Running multiple Web conferences simultaneously with high quality video (30 fps) and Desktop Sharing on a network with high traffic could degrade overall performance. Mitel recommends that you set up a test conference based on the intended use to determine actual performance and monitor the attendee settings. This is the most accurate way to approximate the actual bandwidth required, which provides an estimate of required throughput needed by the host and participants.

Note:

The recommended setting for video quality is 8 fps (default) or 15 fps. Settings above the recommended values will significantly increase the bandwidth required.

Typical meeting description running Microsoft® PowerPoint® presentation at a Viewpoint resolution of 1280x1024 (16-bit color resolution) with medium graphics changing slides every 6 seconds.

Bandwidth consumption varies widely based on the features in use, the settings chosen for each feature, and the content of the Viewer (Desktop Sharing). Settings that impact bandwidth include:

- *Video*: Video size, frame rate, video quality, raw image size, number of participants, and full or standard screen size.
- *Web conference*: Size, scan rate, content, and color resolution.
- *File Sharing*: File size and the number of participants that a file is being shared with.

11.4 Banwidth Requirements

There are bandwidth limitations to consider when running the features of MiCollab AWV. Web Collaboration Bandwidth Requirements shows the estimated bandwidth requirements for a typical Web collaboration meeting.

Note:

Web client users must allow popups when joining a conference by turning off their popup blocker or allowing the popup when prompted.

11.5 Determining Bandwidth

The following table, shows what the bandwidth capacity is estimated to be for the total number of concurrent users. For example, one Web conference with a host and 24 participants is the same as three Web conferences with a host for each and five, eight, and nine participants.

Table 45: Web Collaboration Bandwidth Requirements

USERS	BANDWIDTH (KBPS)	
	VIEWER (1024X768)	VIEWER (1280X1024)[7]
2	75	100
5	188	250
10	375	500
25	938	1250

The following table shows a sampling of the estimated bandwidth capacity for a single video stream. One two-party video involves four streams; from each participant to the server and from the server to each participant. A 200-party conference with only the host broadcasting video involves 200 streams; one from the host to the server and 199 from the server to each participant's computer.

Table 46: Video Bandwidth Guide (single stream)

RAW IMAGE SIZE	IMAGE QUALITY SETTING	MAXIMUM BANDWIDTH (KBPS)	PEAK BANDWIDTH(KBPS)
352 x 288	Good	96	768
	Better	128	
	Best	256	
640 x 360	Good	128	10000

[7] Typical meeting description running Microsoft PowerPoint presentation at a Viewpoint resolution of 1280x1024 (16-bit color resolution) with medium graphics changing slides every 6 seconds.

	Better	256	
	Best	384	
640 x 480	Good	128	10000
	Better	256	
	Best	384	
800 x 450	Good	488	14000
	Better	896	
	Best	1792	
800 x 600	Good	512	14000
	Better	1024	
	Best	2048	
1280 x 720	Good	1024	14000
	Better	2048	
	Best	4096	
1280 x 1024	Good	1536	20000
	Better	3072	
	Best	6144	

Audio and Web conference bandwidth requirements are based on that of an audio-only and Web-only conference. That is, bandwidth is a significant factor for performance during a Web conference, and MiCollab AWV server resources (CPU and memory) used are minimal. Whereas, an audio conference requires more MiCollab AWV server resources and has minimal impact to bandwidth, the capacities of an audio and web conference are the same as that defined previously in this section for the conference type.

11.6 Firewall and DNS Server Configuration

MiCollab AWV can operate either behind a firewall in LAN mode (server-only) as shown in

The following figure, or in Network Edge mode (server-gateway) where the MiCollab server provides the firewall as shown in AWV (Network Edge). Refer to the MiCollab Installation and Maintenance Guide for instructions on how to configure these deployments. The firewall or MiCollab Network Edge configuration must provide Network Address Translation (NAT) for external connections to AWV and for external clients and Web browsers to connect.

In addition, NAT connections (originated by the MiCollab server) to an external Domain Name System (DNS) server must be provided. Audio, Web and Video Ports provides firewall port setting information when configuring AWV on MiCollab.

Consider the following when configuring AWV with two external IPs.

- AWV must be behind a firewall or router that allows port mapping.
- You must have two external IP addresses available for AWV.
- Have two domain names (or subdomains) available when using address translation.
    - Route external IP address 1, port 443 to Internal IP address 1 port 443.
    - Route external IP address 2, port 443 (default) to Internal IP address 1 port 4443 (default).

Consider the following when configuring AWV with single external IP.

- AWV must be behind a firewall or router that allows port mapping.
- You must have one external IP address available for AWV.
- Have one domain name (or subdomain) available when using address translation.
    - Route external IP address, port 443 to Internal IP address 1 port 443.
    - Route external IP address, port 4443 to Internal IP address 1 port 4443 (default).

Note:

Ports 443 and 4443 are the default values in AWV. These ports values are what you enter when configuring Web conference settings. For single external IP, set the value 4443 in external and internal port when configuring Web conference settings.

Port 4443 is the preferred port. Ensure the port number for external and internal is same in case of single IP. Port 443 cannot be used for internal port.

In the following example with two external IPs, the firewall does not rewrite the source address. The DNS is split. Everyone uses the external name. Inside the firewall, it resolves to the internal address. Outside the firewall, it resolves to the external address. To configure this, set the Web server name to the external name. The customer can upload a certificate/key pair to the User Provisioning Gateway (UPG).

Figure 20: AWV (LAN Mode)

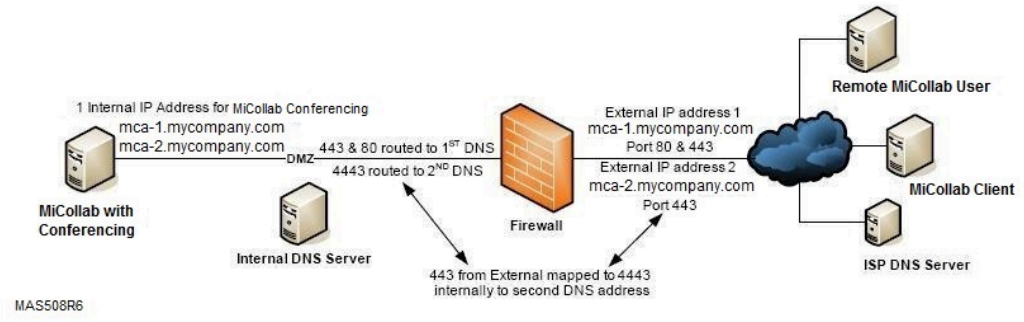
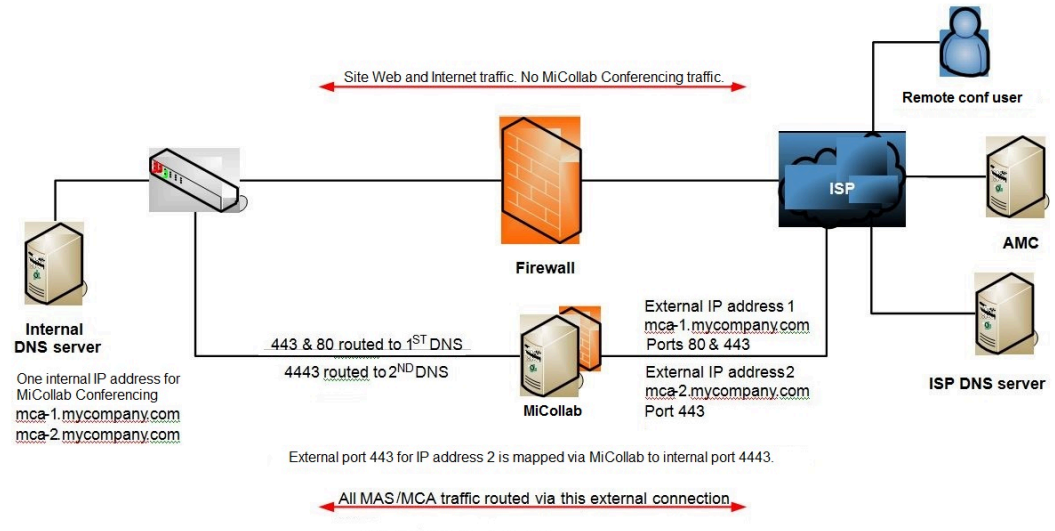


Figure 21: AWV (Network Edge)



11.6.1 Real-Time Transport Protocol (RTP) Port Range

Each audio call on AWV allocates two UDP ports (even ports are used for RTP, odd ports are reserved for RTCP). Audio calls can originate from either IP sources (IP phones or trunks) or Desktop/Web Clients. Hence, to support the maximum of 500 calls from either source, AWV uses the port range of 12000-13999. To support the maximum of 300 video calls, AWV uses the port range of 14000-14611.

11.7 Connection Point Health Statistics

To obtain Connection Point Health statistics for Java Remote Method Invocation (RMI) calls that invoke Java Management Extension (JMX) MBeans managed objects:

1. Navigate to the following Linux directory:

   /var/service/cpctl/run
2. Add the following commands to the JAVA_OPTIONS file:

   - Dcom.sun.management.jmxremote
   - Dcom.sun.management.jmxremote.port=50000
   - Dcom.sun.management.jmxremote.local.only=false
   - Dcom.sun.management.jmxremote.authenticate=true
   - Dcom.sun.management.jmxremote.ssl=false
   - Dcom.sun.management.jmxremote.password.file=$CP_PATH/CNPRemoteConnection.config
3. Restart all AWV services from the MiCollab server manager administration interface.

You can use the following credentials to access a remote connection:

User name: monitorRole

Password: cnpremotepwd.

To change the password required to update the password, file edit the following file:

/usr/awc/connpoint/cp/CNPRemoteConnection.config.

MiCollab Client Guidelines 12

This chapter contains the following sections:

Refer to the latest MiCollab Client Engineering Guidelines available on the Mitel Customer Documentation web site. Note the following condition exists for MiCollab Mobile Client users:

- If a MiCollab for Mobile Client (Android and iPhone) softphone user receives an incoming PSTN call while on a PBX call, the PBX call is put on hold without warning.

The following additional guidelines apply to MiCollab Client on MiCollab:

- The MiCollab for Mobile Client Softphone is designed for use on mobile phones. Although it can be installed on tablet devices, the user interface is currently not designed for use on tablets.
- A user's MiCollab mobile client can register with a MiVoice Office 400 communications platform if the user is configured with a terminal type “MiCollab Softphone”. However, in order for a user's PC client to register with a MiVoice Office 400 communications platform, the user must be configured with a terminal type “MiCollab Softphone” and a MiVoice Office 400 SIP terminal type.
- The default URL https://FQDN/ for MiCollab redirects the user to the End-User Portal. The URL https://FQDN/ for standalone MiCollab Client redirects the user to Server Manager.
- MiCollab does not prevent you from selecting UC Advanced supported languages from the UC Administration interface even if these languages are not supported by MiCollab.
- MiCollab Client utilizes TCP port 36008 for web socket connections from the Android Clients. The same port is used by the MiVoice Border Gateway application so that the Android client uses port TCP/36008 regardless of whether the connection to MiCollab Client is local or via MBG.
- The MiCollab Client desktop client uses non-SIP packets as Keep-Alive on port 5060. So any kind of SIP inspection must be turned off in the firewalls.
- MiCollab Release 7.2 is only supported on 64-bit architecture. To migrate a MiCollab Client stand-alone system to MiCollab Release 7.2, you must upgrade the server hardware to 64-bit.
- When you migrate a MiCollab Client stand-alone system to MiCollab Release 7.2, there is no protection from over-provisioning. See page 42 to determine the maximum number of MiCollab Client users supported for your deployment configuration.
- Standard ACD is not supported in MiCollab Release 7.2 for the MiCollab Client application. MiCollab only supports provisioning for ACD hotdesk agents, but MiCollab Client does not support ACD hotdesk agents.

- Although standalone Client Server (without MiCollab) supports deployment in the DMZ, MiCollab does not.
- For capacities, see the tables in MiCollab System Capacities, Performance, and Constraints. The capacities listed in the MiCollab Client Engineering Guidelines apply only to standalone Collaboration Client-server systems.
- On MiCollab, prior to R9.2, the MiCollab Client application is supported either in integrated mode or co-located mode. From R9.2 onwards, MiCollab only supports Integrated mode.

    - **Integrated Mode**: In this mode, the MiCollab system keeps the Users and Services database and MiCollab Client database synchronized so that they function as a single database on the MiCollab server. It allows you to provision MiCollab Client services from the MiCollab Users and Services application and supports Flow Through Provisioning of the MiCollab Client services to the MiVoice Business platform(s). This is the recommended mode for sites that meet the integration requirements. For, MiVoice 5000, MiVoice MX-ONE, and MiVoice Office 400 platforms, MiCollab Client must be in integrated mode. Flow Through Provisioning is not supported for MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 400 platforms.

- Standalone MiCollab Client Server languages that are not supported by MiCollab. The following MiCollab Client Server languages are not supported by MiCollab:

    - Chinese (Simplified)
    - Chinese (Traditional)
    - Italian
    - Portuguese (Brazil)

12.1 Conferencing

Refer to the *MiCollab Client Engineering Guidelines* for MiCollab Client device conferencing support.

12.2 MiTeam Configuration Limits and Considerations

MiTeam is a workstream communications and collaboration tool that provides a highly collaborative, persistent workspace for team-based meetings, conversations, content collaboration, and project management. MiTeam is available with MiCollab Web Client, MiCollab MAC Client, and MiCollab Mobile Client for Android and iOS devices.

In a Stream, you can store files, hold chats, add to-do lists, and set up online meeting sessions.

The following tables summarize the system and equipment considerations that a user of the MiTeam feature might need to consider:

Table 47: User Capabilities

MITEAM MEET USER CAPABILITIES	GUEST USER (MEET ONLY)	GUEST USER (STREAM PARTICIPANT)	MITEAM USER (MEET AND STREAM)
Account lifetime	Meet duration	Account is cleared after 14 days if not accessed after initial invite.Account is cleared after 60 days of inactivity.	Until deleted
Attends Meets	Yes	Yes	Yes
Chat and History	Only within Meet	Yes	Yes
Chat History duration	No	Unlimited	Unlimited
Invites participants	No	No	Yes
Launches Meets	No	No	Yes
Maximum file download	Unlimited	Unlimited	Unlimited
Maximum file upload	5 MB (Only within Meet)	5 MB	300 MB
Maximum meeting duration	24 hours	24 hours	24 hours
Meet recording controls	No	No	Yes
Tasks	No	Yes	Yes

Session is recordable	Yes	Yes	Yes

Table 48: User and MiTeam Stream Limits

FEATURE	**LIMIT**
Maximum Users in a MiTeam Stream (including guests)	100
Maximum users in a Collaboration Meeting	50
MiTeam Stream storage capacity	Unlimited

MiCW Specific Guidelines 13

Check the compatibility table below to determine the version of Mitel Integrated Configuration Wizard (MiCW) that you should use with your MiVoice Business platform.

Table 49: MiCW Compatibility Table

CONFIGURATION WIZARD RELEASE	MIVOICE BUSINESS RELEASE	MICOLLAB RELEASE
4.1.x.x	6.0 SP1	5.0
4.2.x.x	6.0 SP2	5.0 SP1
5.0.x.x	7.1	6.0
5.1.x.x	7.1 SP1	6.0 SP1
5.2.x.x	7.1	6.0 SP1
5.3.x.x	7.2	7.0
5.3.x.x	7.2 SP1	7.1
5.3.x.x	7.2 SP1	7.2
6.0.1.x	8.0	7.3
6.0.2.x	8.0 SP2	8.0

For more information about MiCW refer to the MiCollab Installation and Maintenance Guide in the Mitel Documentation Center.

Appendix A: Port Usage 14

This chapter contains the following sections:

14.1 MiCollab Port Usage

TCP/IP ports 10255, 10256, 10257, 10258, 10259, and 10260 are open on the MSL IP address. They are external ports on the MiCollab server that provide external Application Programming Interfaces (APIs) with access to the MiCollab system. APIs can be used to support management applications.

Note:

MiCW Release 5.3.0.4 and later requires the following ports to be open in MiCollab: 80, 443, 10255, 10256, 10258, 10259, and 10260. If these ports are not open, then MiCW fails to "Connect to server" at the start of the wizard. These ports are open by default.

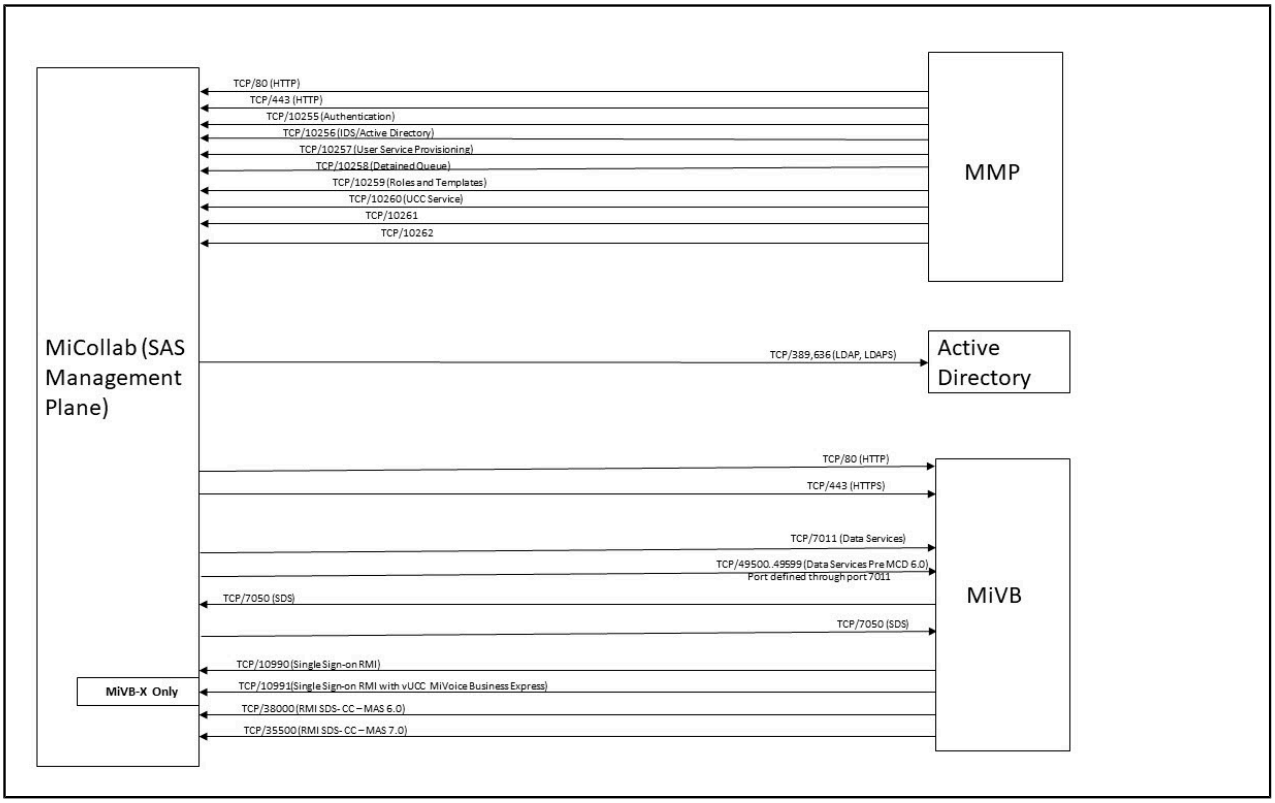


Figure 22: Usage

14.2 NuPoint Unified Messaging Ports

If MiCollab Server or MiCollab Virtual Appliance is connected to a MiVoice Office 250, you must configure port 5058 on the MiVoice Office 250 to support SIP communication from the NuPoint application.

Figure 23: NuPoint Unified Messaging Ports (Diagram 1)

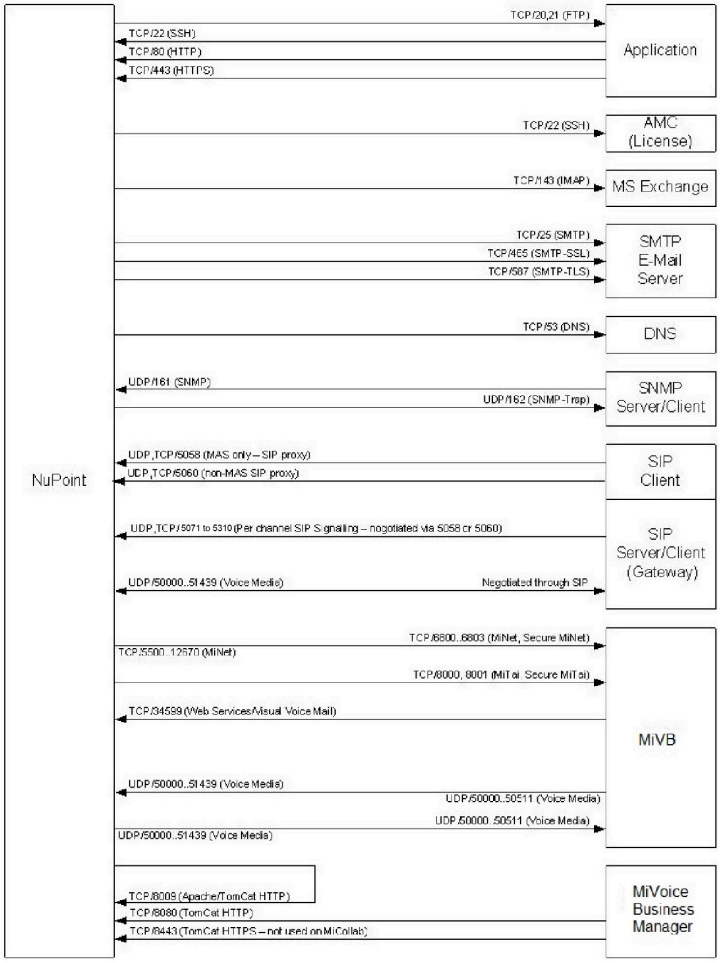
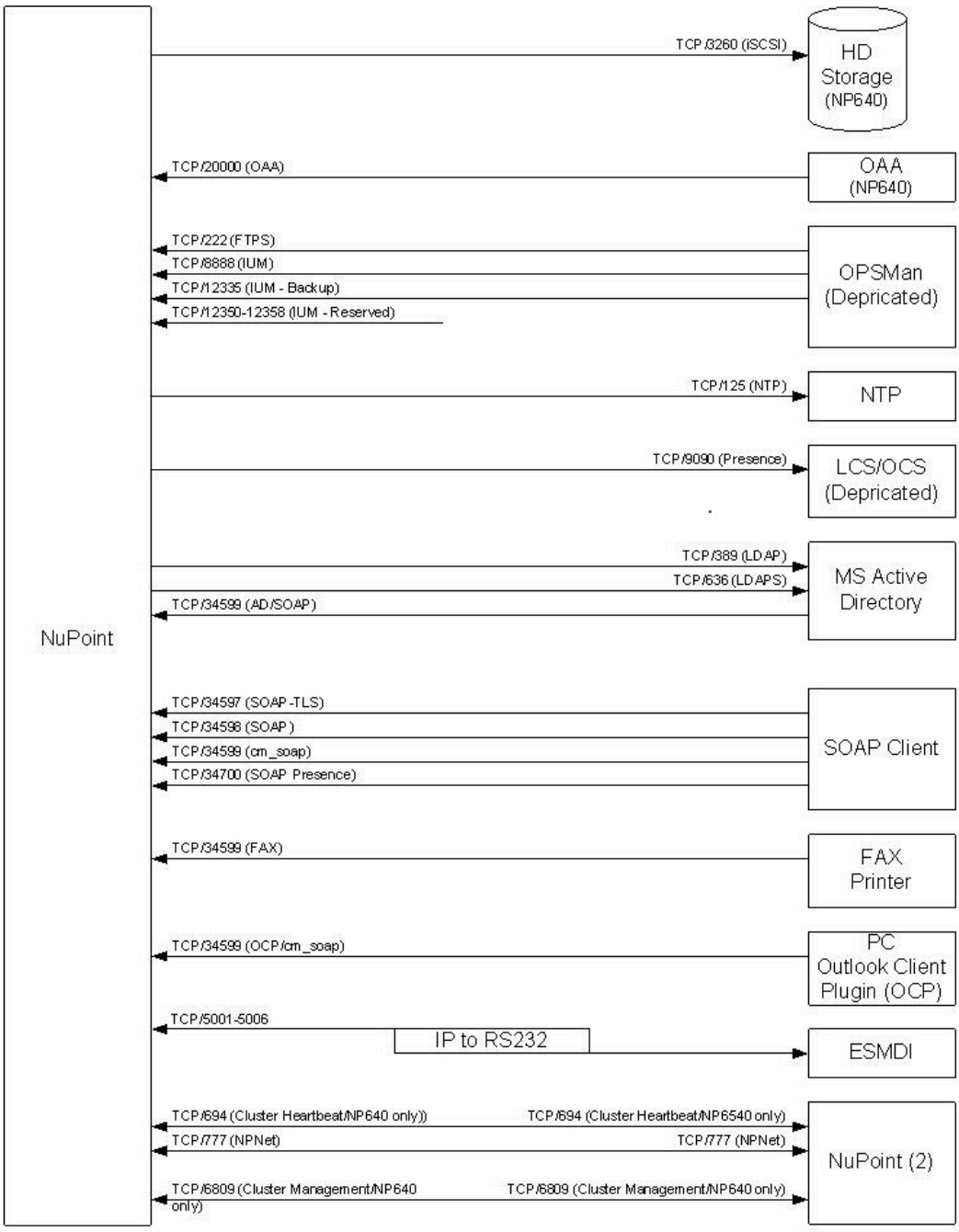


Figure 24: NuPoint Unified Messaging Ports (Diagram 2)



14.3 MiVoice Business Gateway Port Usage

Figure 25: MiVoice Business Gateway Port Usage (Diagram 1)

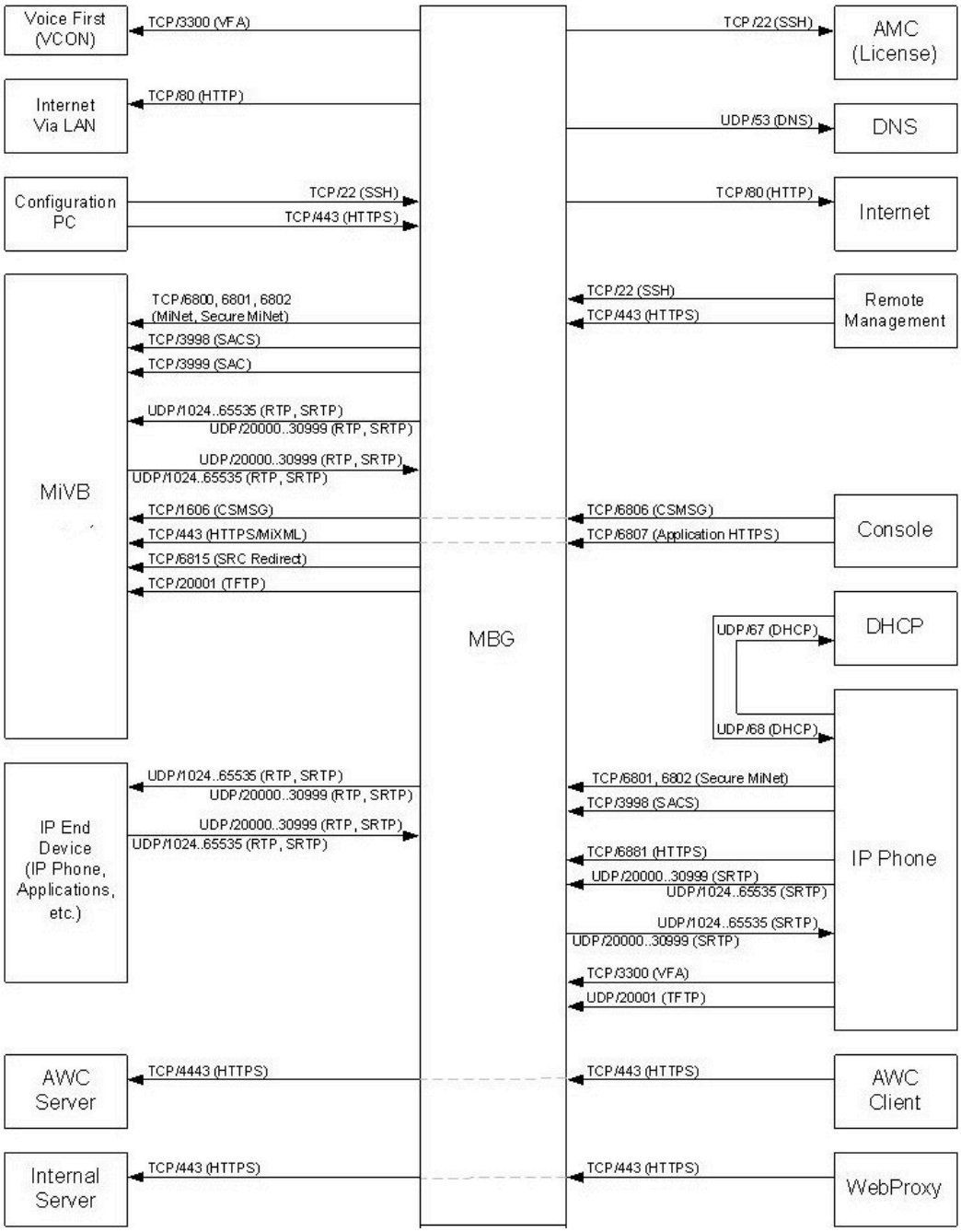


Figure 26: MiVoice Business Gateway (Diagram 2)

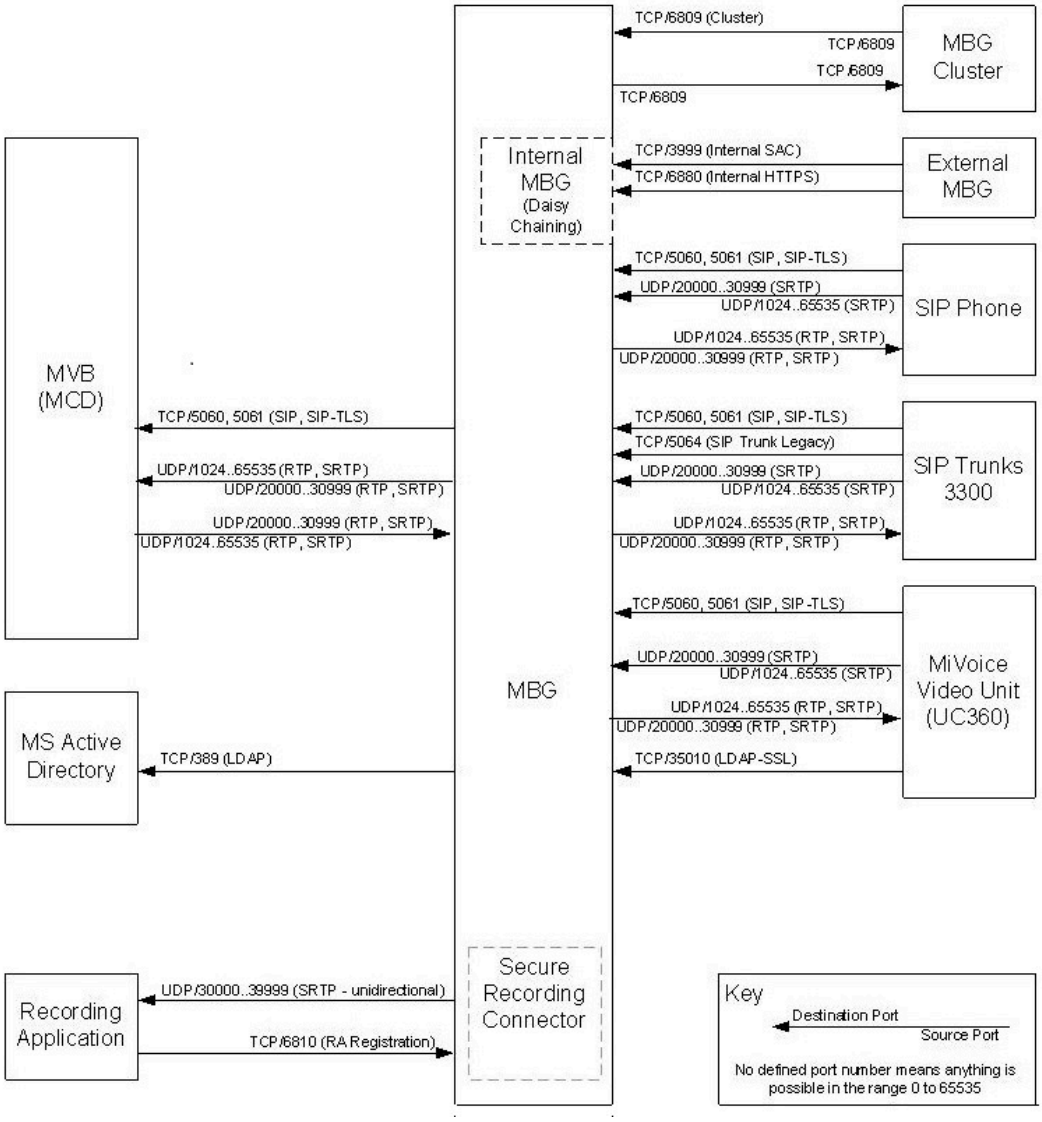
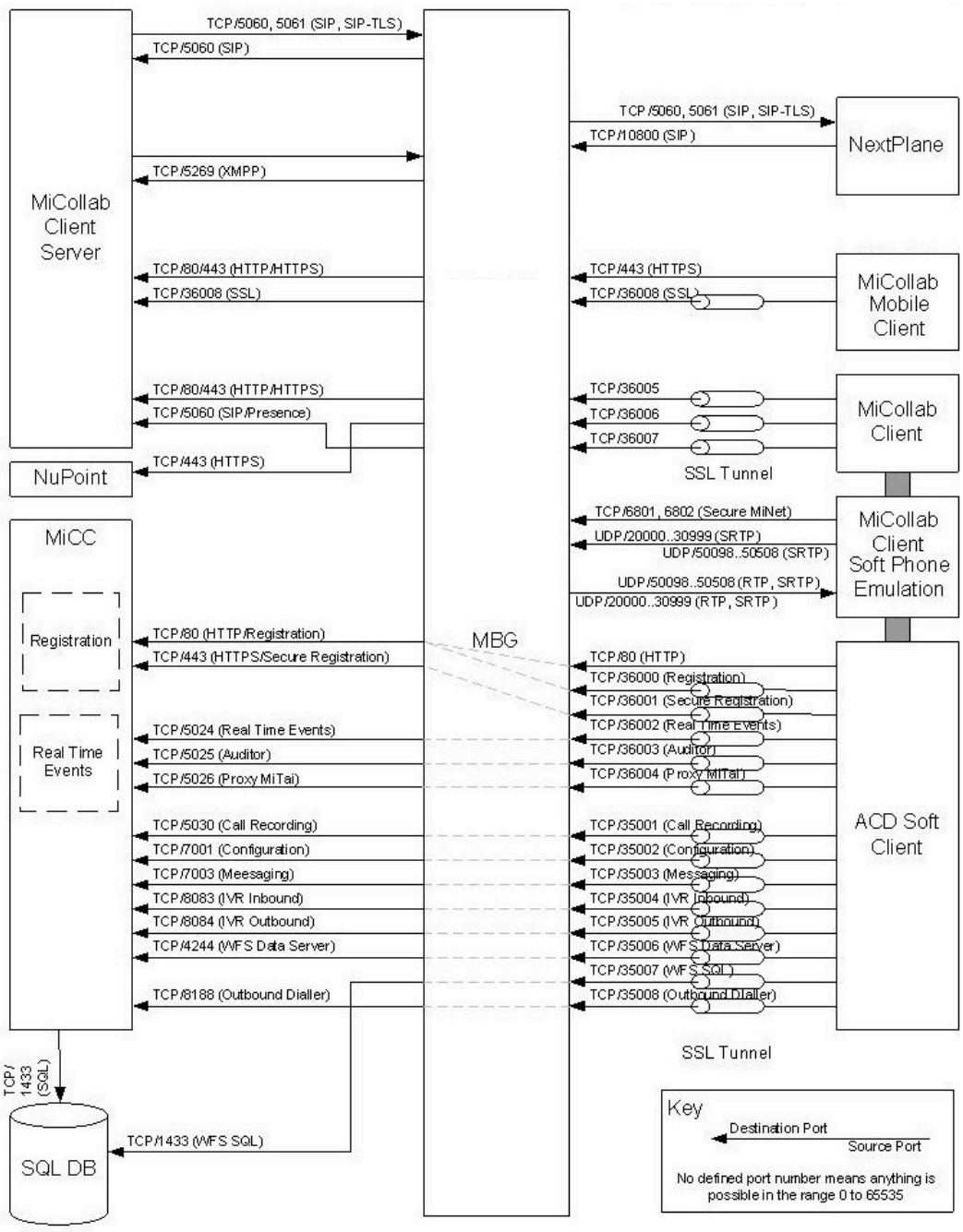
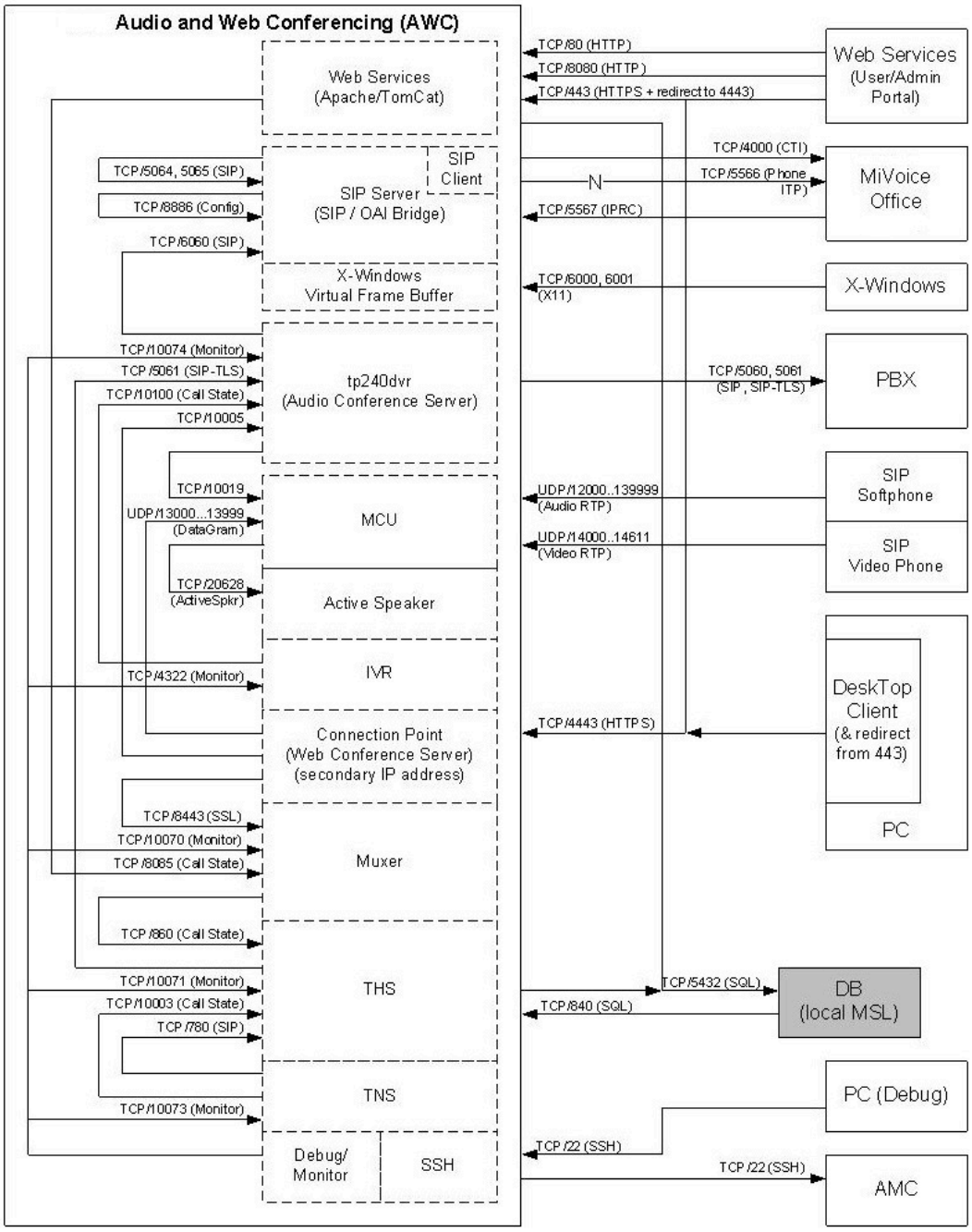


Figure 27: MiVoice Border Gateway Ports (Diagram 3)



14.4 MiCollab AWV Port Usage

Figure 28: Audio, Web and Video Ports



14.5 MiCollab Client Port Usage

Figure 29: MiCollab Client Ports (Network Edge Mode)

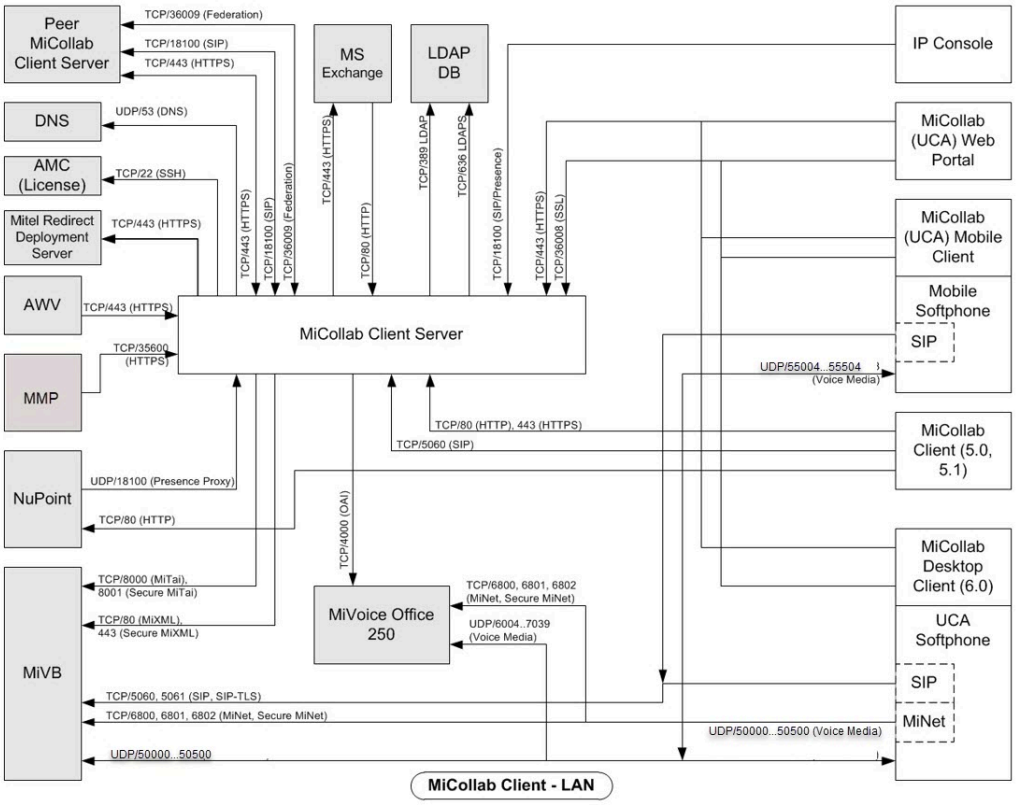
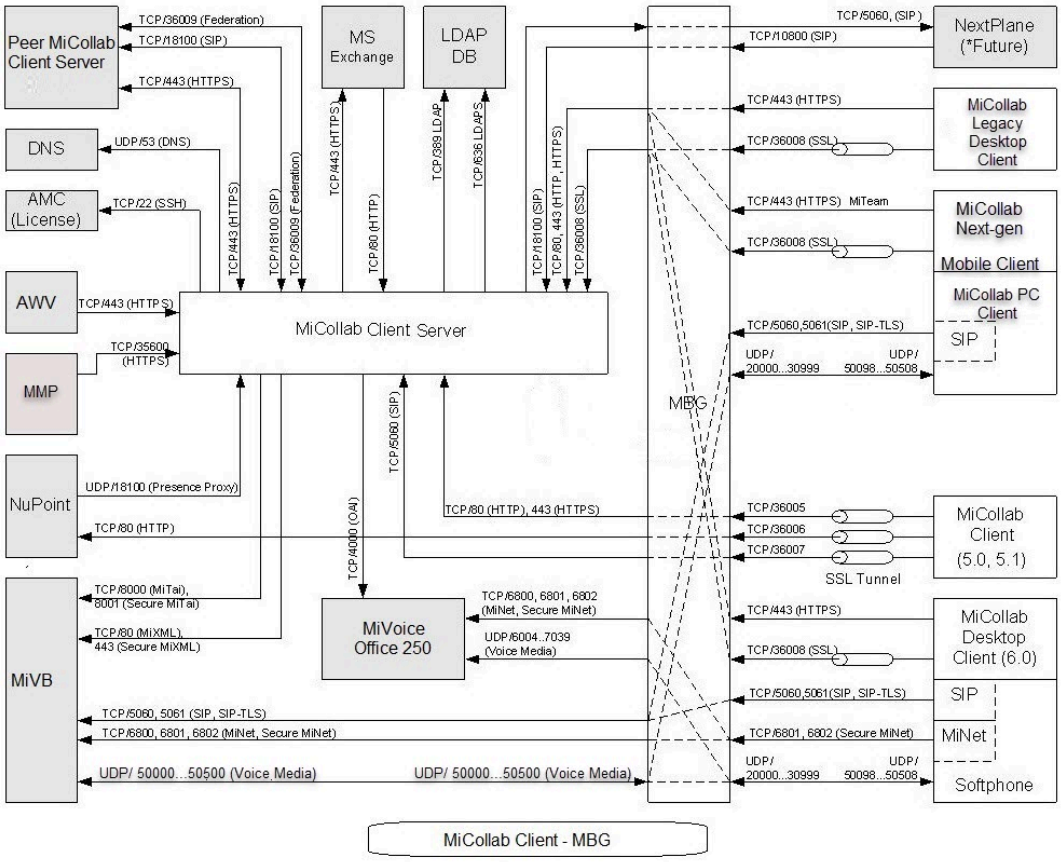


Figure 30: MiCollab Client Ports (LAN Mode)



14.6 MiVoice MX-ONE Port Information

Table 50: Port Access via MiCollab Server in LAN

PORT	DIRECTION	PURPOSE & DETAILS
TCP 22 (SSH)	Web Proxy Server → Internet MiCollab Server → Internet	**AMC Communications**. Allow outbound packets (and replies) on TCP port 22 between the Web Proxy and MiCollab Server and the Internet to enable AMC communications (i.e., enable server registration, software and license key downloads, alerts and reporting).
UDP 53 (DNS)	MiCollab Server → Internet Web Proxy Server→ Internet	**Domain Name System**. The server requires DNS to look up the IP address of the Mitel AMC. Alternatively, the server can be configured to forward all DNS requests to another DNS server.

PORT	DIRECTION	PURPOSE & DETAILS
TCP 80 (HTTP)	Web Proxy Server ← Internet	**Web Browser Access**. Allow inbound packets and replies on TCP port 80 between the Web Proxy server and the Internet. Used for remote web browser pages; will be redirected to TCP port 443 (HTTPS).
TCP 443 (HTTPS)	Web Proxy Server ← Internet Web Proxy Server→ LAN	**Web Browser Access**. Allow inbound and outbound packets on TCP port 443 between the Web Proxy server and the Internet for web pages (SSL mode). Allow inbound and outbound packets on TCP port 443 between the Web Proxy server and the LAN for web pages.
	MiCollab Server → Internet	**Mobile Client Deployment**. Used to send deployment tokens and the configuration download URLs to the Mitel redirect deployment servers.
	MiCollab Server → Internet	**MiTeam Integration**. Used to connect with Mitel's Cloud-based MiTeam solution located on the Internet.
	MiCollab Server ← Internet	**Remote Server Management**. *(Optional)* Allow inbound and outbound packets on TCP port 443 between the MiCollab Server and the Internet to allow remote management of the server, if required. HTTPS access to the manager on the external interface must also be explicitly enabled from the server manager interface.
TCP 4443 (default – can be configured in web proxy)	Web Proxy Server ← Internet Web Proxy Server →LAN	**MiCollab AWV Collaboration Client**. Allow inbound packets on TCP port 443 and forward them to configured port (default 4443) on the Web Proxy server as well as return traffic. Allow inbound packets on TCP port 4443 between the Web Proxy server and the LAN. Used for Connection Point traffic related to MiCollab AWV Web Collaboration.

PORT	DIRECTION	PURPOSE & DETAILS
TCP/5060 TCP/5061	MiCollab Server ← Internet	SIP proxy and TCP/80 (HTTP) are used by internal MiCollab Client PC clients (on the LAN) to connect to the MiCollab Server TLS (default port used by the MiCollab Mobile Client)
TCP 8882	CSTA link ←→MX-ONE	**MiCollab Client CSTA Proxy** application supports the call control messaging between MiCollab and the MiVoice MX-ONE platform to support MiCollab Client features such as "Click-to-Call".
UDP 1024 to 65,535 (RTP)	MiCollab Server → LAN	**Voice Communications**. Allow outgoing RTP on UDP ports greater than, or equal to, 1024 from the server to all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.
UDP 20,000 to configured upper bound* (SRTP)	MiCollab Server ← LAN	**Voice Communications**. Allow incoming SRTP on UDP ports 20000 – configured upper bound* from all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.

*Configured upper bound for RTP/SRTP on UDP ports is controlled by a setting in the Teleworker Solution Advanced panel. You must reserve four ports per set that you wish to support. Thus, to support 1000 sets, 4000 ports are required, from 20000 to 24000, and those ports must be open in the firewall configuration of any firewall that the Teleworker server is installed behind.

Table 51: Port Access via Standalone MBG Server in DMZ

PORT	DIRECTION	PURPOSE & DETAILS
TCP 22 (SSH)	MBG Server →.Internet	**AMC communications**. Allow outbound packets (and replies) on TCP port 22 between the MBG Server and the Internet to enable server registration, software and license key downloads, alerts and reporting
UDP 53 (DNS)	MBG Server→.Internet	**Domain Name System**: The server requires DNS to look up the IP address of the Mitel AMC. 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)	Web Proxy Server ← Internet Web Proxy Server → LAN	**Web Browser Access**: Allow inbound and outbound packets on TCP port 443 between the Web Proxy server and the Internet for web pages (SSL mode). Allow inbound and outbound packets on TCP port 443 between the Web Proxy server and the LAN for web pages.
	MiCollab Server → Internet	**Mobile Client Deployment**: Used to send deployment tokens and the configuration download URLs to the Mitel redirect deployment servers.
	MBG Server ← Internet	**Remote Server Management**: *(Optional)* Allow inbound and outbound packets on TCP port 443 between the MBG Server and the Internet to allow remote management of the MBG server, if required. HTTPS access to allow remote management of the MBG server must be also be explicitly enabled from the server manager interface.

PORT	DIRECTION	PURPOSE & DETAILS
TCP 4443 (default – can be configured in web proxy)	Web Proxy Server ← Internet Web Proxy Server → LAN	**MiCollab AWV Collaboration Client**: Allow inbound packets on TCP port 443 and forward them to configured port (default 4443) on the Web Proxy server as well as return traffic. Allow inbound packets on TCP port 4443 between the Web Proxy server and the LAN. Used for Connection Point traffic related to MiCollab AWV Web Collaboration.
TCP/5060	MBG Server ← Internet	SIP proxy and TCP/80 (HTTP) are used by internal MiCollab Client PC clients (on the LAN) to connect to the MiCollab Server.
TCP/5061	MBG Server ← Internet	TLS (default port used by the MiCollab Mobile Client).
TCP/5063	MBG Server ← Internet	SIP over TLS for Webclient access.
TCP/36008	MBG Server ← Internet	Web socket proxy required for MiCollab for Mobile.
UDP 20,000 to configured upper bound# (SRTP)	MiCollab Server ← Internet MiCollab Server ← LAN MBG Server → LAN MBG Server → Internet	**Voice Communications**: Allow incoming SRTP on UDP ports 20000 – configured upper bound* from all streaming devices on the LAN and the Internet. Configuration errors here are a common cause of one-way audio problems.

PORT	DIRECTION	PURPOSE & DETAILS
Ports 32000 to 32500 (public) Ports 33000 to 33500 (private)	LAN → MBG Server MBG Server ← Internet	**WebRTC Port Ranges**: 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.

*Configured upper bound for RTP/SRTP on UDP ports is controlled by a setting in the Teleworker Solution Advanced panel. You must reserve four ports per set that you wish to support. Thus, to support 1000 sets, 4000 ports are required, from 20000 to 24000, and those ports must be open in the firewall configuration of any firewall that the Teleworker server is installed behind.

14.7 MiVoice 5000 Port Information

14.7.1 Ports required by MiCollab Client Server on the LAN

- MiCollab > MiVoice 5000 : TCP/3211 (CSTA).
- UCA Softphone > MiVoice 5000 : TCP/5060, 5061 (SIP, SIP-TLS) UDP 5060 (SIP)
- UCA Softphone < > MiVoice 5000 : UDP/40000..40064 UDP/50098..50508 (Voice Media)
- MiCollab > MiVoice 5000 : TCP/389 (LDAP)
- MiVoice 5000 > MiCollab : TCP/10245..10252 (Provisioning)

14.7.2 Ports required by MiCollab Client Server on a LAN where Clients connect via MBG:

- MiCollab > MiVoice 5000: TCP/3211 (CSTA)
- UCA Softphone > MiVoice 5000: TCP/5060, 5061 (SIP, SIP-TLS) UDP 5060 (SIP)
- MiVoice 5000 <> MBG: UDP/40000..40064 UDP/20000..30999 (Voice Media)
- MiCollab > MiVoice 5000: TCP/389 (LDAP)
- MiVoice 5000 > MiCollab: TCP/10245..10252 (Provisioning)
- MiVoice 5000 > MBG: TCP/443 (HTTPS)
- MBG > MiVoice 5000: TCP/4445 (HTTPS)
- MiCollab WebRTC Client > MBG: TCP/443 (HTTPS)
- MiCollab WebRTC Client > MBG: TCP/5063 (WSS)

- MBG > MiCollab WebRTC Client: UDP/33000.33500 (Voice Media)
- MBG > MiVoice 5000: TCP/389 (LDAP)
- MBG > MiVoice 5000: TCP/5060, 5061 (SIP, SIP-TLS) UDP 5060 (SIP)
- MBG > MiVoice 5000: TCP/443 (HTTPS)
- MiVoice 5000 > MBG: TCP/443 (HTTPS)
- MiVoice 5000 < > MBG: UDP/40000..40064 UDP/32000..32500 (Voice Media)

14.8 MiVoice Office 400 Port Information

14.8.1 Softphone:

- UDP/TCP/5060 (SIP), TCP/5061 (SIP-TLS)
- Virtual Appliance Media Server (vApp): UDP/40000 … 40499 (Voice Media) > Default ports, configurable
- Standard Media Switch (StMS): UDP/5004 … 5051 (Voice Media) > Default ports, configurable
- Media Gateway Module (EIP): UDP/5004 … 5131 (Voice Media) > Default ports, configurable

14.8.2 MiCollab Client Server

- TCP/7001 (CSTA) > Default port, configurable
- MiVoice Office 400 <> MBG: UDP/40000..40064 UDP/20000..30999 (Voice Media)
- MiCollab > MiVoice Office 400: TCP/389 (LDAP)
- MiVoice Office 400 > MiCollab: TCP/10245..10252 (Provisioning)
- MiVoice Office 400 > MBG: TCP/443 (HTTPS)
- MBG > MiVoice Office 400: TCP/4445 (HTTPS)
- MiCollab WebRTC Client > MBG: TCP/443 (HTTPS)
- MiCollab WebRTC Client > MBG: TCP/5063 (WSS)
- MBG > MiCollab WebRTC Client: UDP/33000.33500 (Voice Media)
- MBG > MiVoice Office 400: TCP/389 (LDAP)
- MBG > MiVoice Office 400: TCP/5060, 5061 (SIP, SIP-TLS) UDP 5060 (SIP)
- MBG > MiVoice Office 400: TCP/443 (HTTPS)
- MiVoice Office 400 > MBG: TCP/443 (HTTPS)
- MiVoice Office 400 < > MBG: UDP/40000..40064 UDP/32000..32500 (Voice Media)

Appendix B: Migration to Single WAN IP Solution for MiCollab Audio, Web and Video Conferencing 15

This chapter contains the following sections:

This Appendix section describes the procedure to migrate to a single WAN IP solution for the existing deployments.

Note:

The default upgrade path is to retain the two WAN IPs for the existing deployments.

The existing MiCollab systems have different deployments with MBG and MiCollab collocated or MBG on the edge on a different host. The following deployment scenarios and configurational changes are needed to move to single WAN IP solution.

Note:

The configuration method using two external IP addresses is helpful in preventing connectivity issues that may arise when AWV Clients are behind a corporate firewall with rules for outgoing traffic, where those rules may only allow web-based ports to be reached at a remote location.

For example, a remote user is more likely to be able to make a connection to a server outside of their network using port 443, than port 4443.

Note:

The single IP address configuration will avoid the additional usage of a dedicated IP address (useful when IP addresses are costly or simply not possible), however it should be noted that some external users sitting behind a firewall with restricting outgoing traffic rules at ports other than 80 and 443 may experience connectivity issues.

15.1 Requirements

- The FQDN for web conferencing is updated and the second FQDN is not required by the AWV application. The Clients fetch the updated configuration at AWV from the web requests during the connection automatically.
- The external and internal port at AWV Web Conferencing must be set to the same port (if not 4443).
- Update the firewall rules for Internet to MBG (if applicable). If corporate firewall is present in front of the system, then create the rules for allowing access to port 4443 for WAN IP1.
- Log in as user administrator. Under **Configure this server** remove the second IP address by removing **additional static IP address** value. This requires a reboot of MiCollab Server (network edge mode) or MBG (as applicable).

15.2 Deployment Scenarios

Note:

If FQDN for web conferencing is updated, the second FQDN is no longer needed by AWV application. The Clients connect to the updated configuration at AWV automatically.

Note:

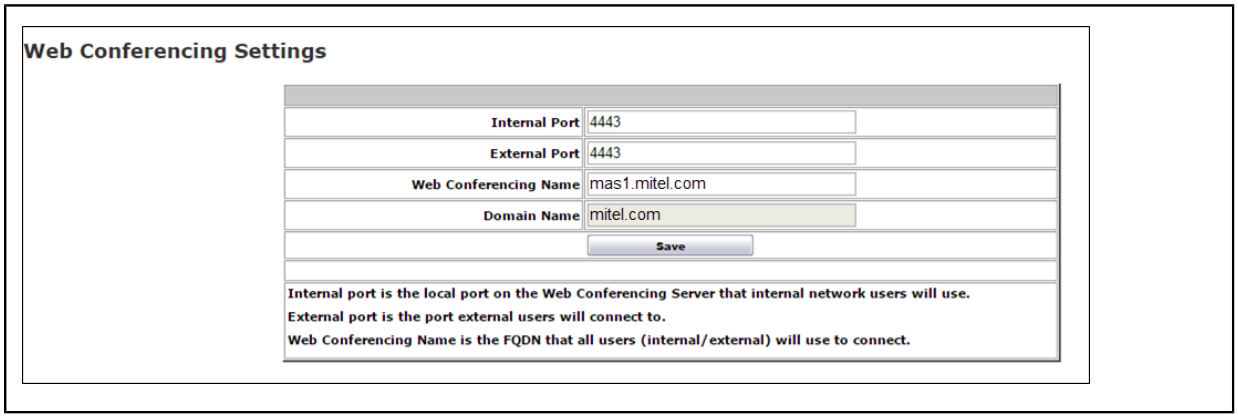
Port 4443 is recommended, because of the existing setups and default configurations at AWV. Selecting a different port number, then the port needs to be opened at firewall if firewall is configured.

15.2.1 MiCollab in Network Edge mode (Server-Gateway)

In this configuration, the AWV and MSL configurations are updated. The MBG remote-proxy application is not involved. There are no configuration changes needed at MBG.

To configure, follow the procedure below:

1. Go to MiCollab Server Manager.
2. Under Applications, click Audio, Web and Video Conferencing.
3. Under Configuration, click Web Conferencing Settings.



4. Change the port numbers of **Internal Port** and **External Port** to **4443** for web conferencing.
5. Update the domain name for MiCollab host at **Web Conferencing Name**.
6. Update MSL configuration to remove the second IP.
7. Click **Save**.
8. Click **OK** in the pop-window to restart the Web Conferencing Server.

15.2.2 MiCollab in the LAN with MBG on the Network Edge

In this configuration, the AWV, MSL, and MBG remote-proxy must be updated. The MBG remote proxy will set up the access to the AWV application.

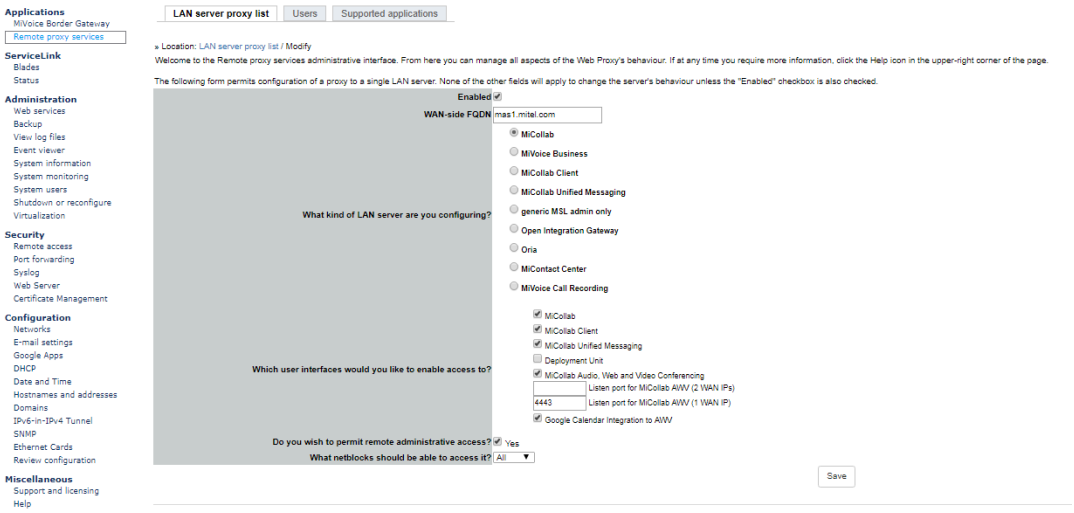
Note:

The DMZ firewall must be reconfigured to allow external access to MBG on TCP port 4443.

To configure, follow the procedure below:

1. Go to MSL Server Manager.
2. Under Applications, click Remote proxy services.
3. Select **LAN** server proxy list and modify the **WAN-side FQDN** entry associated with the MiCollab server.

Figure 31: Remote proxy services

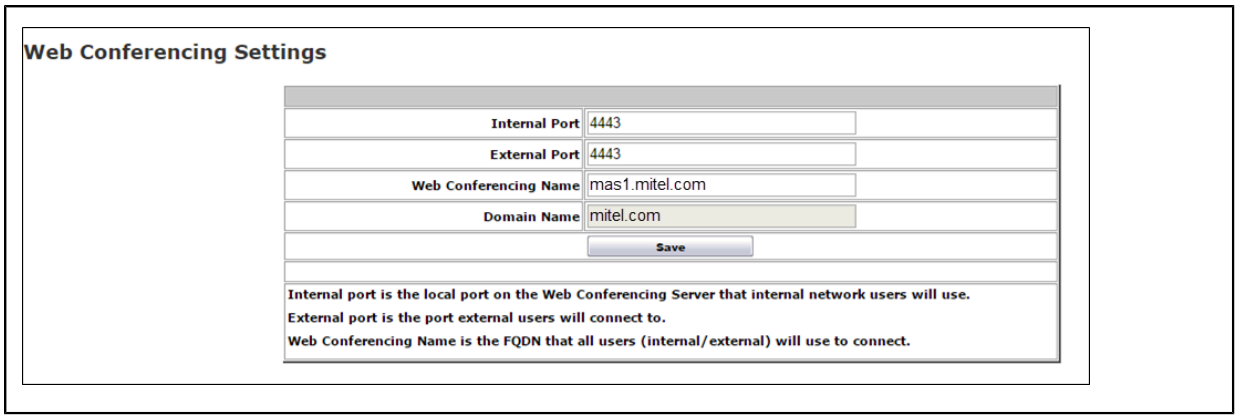


4. Update Listen port for MiCollab AWV (1 WAN IP) to 4443.

Note:

Port number 4443 is same as the port number in **AWV admin portal > Web Conferencing Settings** for external and internal ports.

5. In AWV admin portal, update the **Web Conferencing Name** with the domain name for MiCollab host.



6. **Save** the configuration settings.
7. Click **Ok** in the pop-window to restart the Web Conferencing Server.

Note:

Make sure that the external conferences are successfully established.

8. If MBG is deployed in server-gateway, update MSL configuration to remove the second IP.
9. Click **Ok** in the pop-window to restart the MSL Server.

Appendix C: Client Requirements 16

The following tables identify the operating systems, web browsers, and e-mail applications that are supported for the MiCollab application clients.

Table 52: Client Operating Systems

MICOLLAB FUNCTIONALITY	WIN 7.1	WIN 8.0 WIN 8.1	WIN 10	ANDROID	IPAD	IPHONE	APPLEMAC
MiCollab End User Portal	Yes	Yes	Yes	No	No	No	No
MiCollab AWV Desktop Client	Yes	Yes	Yes	No	No	No	No
MiCollab AWV Web Client	Yes	Yes	Yes	Yes	Yes	No	Yes
MiCollab AWV Web sharing	Yes	Yes	Yes	Yes	Yes	No	Yes
MiCollab Desktop Client	Yes	Yes	Yes	No	No	No	Yes
MiCollab Web Client	Yes	Yes	Yes	No	No	No	Yes
MiCollab Web RTC client	Yes	Yes	Yes	No	No	No	Yes
MiCollab Mobile Clients	No	Yes (8.1)	Yes	Yes (5.0 and 6.0)	No	Yes (8.0+)	No

MiCollab Server Manager	Yes	Yes	Yes	No	No	No	No
MiCollab Microsoft Outlook Plugin	Yes	Yes	Yes	No	No	No	No
NP-UM Outlook Client Plugin	Yes	Yes	Yes	No	No	No	No
NP-UM Fax Plugin	Yes	Yes	Yes	No	No	No	No
NP-UM Active Directory Snap-in	Yes	Yes	Yes	No	No	No	No
MAPI Gateway	Yes	No	No	No	No	No	No
MiCW	Yes	Yes	Yes	No	No	No	No
MiTeam	Yes	Yes	Yes	Yes (4.4+)	No	Yes(IOS 9+)	Yes

Note:

No = Not supported or not applicable

Table 53: Client Web Browsers

MICOLLAB FUNCTIONALITY	WEB BROWSERS					
	GOOGLE CHROME	INTERNET EXPLORER	MICROSOFT EDGE	FIREFOX	SAFARI	ANDROID STOCK BROWSER
My Unified Communications Portal	Yes (46+)	Yes (10 & 11)	Yes	Yes (41+)	No	N/A
MiCollab Audio, Web and Video Conferencing Web Client[8]	Yes (46+)	Yes (10 & 11)	Yes	Yes (41+)	Yes (9.0)	Yes
MiCollab AWV Web Sharing	Yes (46+)	No	No	No	No	No
MiCollab Web Client	Yes (46+)	Yes (10 & 11)	Yes	Yes (41+)	Yes(9.0)	N/A
MiCollab Web RTC Client	Yes (50+)	No	No	Yes (46+)	No	N/A
MiCollab Server Manager	Yes (46+)	Yes (10 & 11)	Yes	Yes (41+)	N/A	N/A
NP-UM Admin Web Console	Yes (46+)	Yes (10 & 11)	Yes	Yes (41+)	N/A	N/A
NP-UM Personal Web GUI	Yes (46+)	Yes (10 & 11)	Yes	Yes	No	N/A

[8] MiCollab AWV web client is also supported on Apple iPad iOS 8.x and Android 5.0

NP-UM Web Console	Yes (46+)	Yes (10 & 11)	Yes	Yes	No	N/A
Mitel Integrated Configuration Wizard	No	Yes (10 & 11)	Yes	No	No	N/A
MiCollab for Voice Initial Configuration Wizard	No	Yes (10 & 11)	Yes	No	No	N/A
MiTeam	Yes (46+)	Yes (10 & 11)	Yes	No	Yes (9.0+)	Yes

Note:

If using IE9 you must install the Google Chrome Frame plug-in to support real-time data and have chat, presence, and call control functionality.

Note:

MiCollab Audio, Web and Video Conferencing web sharing is not supported on Virtual Desktop environment.

Table 54: Client Personal Information Managers (PIM)

MICOLLAB FUNCTIONALITY	PIM APPLICATION			
	EXCHANGE	LOTUS	GOOGLE	OUTLOOK

MiCollab Desktop Client	2007, 2007 SP1, 2010, 2010 SP1 & SP2, 2013, 2013 & SP1, 2016 (server)	7.1, 8.0, 8.5, 8.5.1, 8.5.2, 9.0	Yes	2007, 2010, 2013, 2016
MiCollab Mobile Client for iOS	2007, 2007 SP1, 2010, 2010 SP1 & SP2, 2013, 2013 & SP1, 2016 (server)	No	Yes	No
MiCollab Mobile Client for Android	2007, 2007 SP1, 2010, 2010 SP1 & SP2, 2013, 2013 & SP1, 2016 (server)	No	Yes	No
MiCollab Microsoft Outlook Plugin	N/A	No	N/A	2010, 2013 2016
NP-UM Adv UM	2007, 2007 SP1, 2010, 2010 SP1 & SP2, 2013, 2013 & SP1, 2016 (server)	No	Yes	2007, 2010, 2013 2016
NP-UM Outlook Client Plugin	N/A	No	N/A	2007, 2010, 2013 2016
MiCollab AWV User Portal	2007, 2007 SP1, 2010, 2010 SP1 & SP2, 2013, 2013 & SP1 (server)	7.1, 8.0, 8.5, 8.5.1, 8.5.2	Yes	2007, 2010, 2013, 2016

Appendix D: Azure Guidelines 17

This chapter contains the following sections:

17.1 High Availability Configurations on Azure

The Azure platform offers three levels of deployment and availability:

- Hosted machines within a single data center: 99.95% availability
- Hosted machines within a region, and backup between zones: 99.99% availability
- Hosted machined in multiple regions: >99.999% availability

Further information can be found at the following link: https://docs.microsoft.com/en-us/azure/architecture/example-scenario/infrastructure/iaas-high-availability-disaster-recoveryMitel products have a latency dependency between applications and storage, and so these two must be co-located within the same data center or same zone. This means that deployments must be within the same Availability Sets within the same physical data center. Although a region may offer multiple zones (data centers) and offer an Availability Zone between zones within a region, this is not the recommended deployment, i.e. ensure that the applications and services are accessible within the same single Mitel applications that need to be resilient will deploy the primary function in one zone within one region, and the secondary functions within one zone in a different region. Availability of the solution in this configuration is still capable of achieving >99.999% availability.

17.2 Azure Virtual Machine Resource Allocation

Performance testing on Azure suggests that server resource profiles closely match those of VMware. However. The definition of those resources in Azure are different, and may require some additional consideration at deployment, as adjustments after the application are installed may be difficult to achieve, for example, storage may be increased, but not decreased. Three server types are defined:

- Ds v4 series (enterprise-grade applications)
- Eas v4 series (high in-memory processing, large RAM)
- F series (excellent choice for workloads that demand faster CPUs, such as analytics, web servers, and batch processing)

There are other virtual machine series, but these are either not suitable for a real-time voice streaming application or are not cost-effective given the poor matching of available resources to requirements. In some cases, there are v5 versions, which recently became available. However, these units are not yet globally available, until then the Ds and Es series will continue with v4. Some comments around supported series can be found at these websites:

- Ddv4 and Ddsv4-series: https://docs.microsoft.com/en-us/azure/virtual-machines/ddv4-ddsv4-series
- Eav4-series and Easv4-series: https://docs.microsoft.com/en-us/azure/virtual-machines/eav4-easv4-series
- F-series: https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-previous-gen

An overview of the different Azure machines can also be found here: https://docs.microsoft.com/en-us/azure/virtual-machines/sizesOther server types have been reviewed but are less suitable for continuous real-time streaming applications. As server types and capabilities change, these will be reviewed and considered for inclusion. In addition to the server machine types, there are also different storage types available. The following are recommended in the deployment:

- Managed Disks (S-Type): Standard HDD for the applications and operating system. In most cases, data for the applications can also be stored along with the application. This is considered the ‘OS Disk’.
- Managed Disks (E-Type): Standard SSD: for data storage on data-intensive applications and also where access speed may need to be considered. Typically, the database and SQL servers would use this in preference to Standard HDD. This is considered the ‘Data Disk’ and may be further segmented into different data partitions.
- Cool Storage: This is a longer-term storage with a minimum storage period and limited read access. This is used for specific applications such as call recording, where data is stored for a period of time, but infrequently accessed
- File Share: This may also utilize Cool Storage but is typically used for local backups and log storage from the applications.

Deployment considerations for servers and storage are identified in the section below. Note that by default most virtual machines are created with an allocation of S-Type storage which may need to be adjusted. Storage allocation is included in the Server Resource Definitions, below.

17.2.1 Azure Virtual Machine Location Availability

These systems have been found to be readily available in most geographic regions, including:

- West Europe
- France Central

- France South
- UK South
- UK West
- Canada Central
- Canada East
- Australia East
- Australia Central
- East US
- West US

17.2.2 Azure Virtual Machine Deployment Considerations

At deployment time Azure also allocates a certain amount of Hard Drive storage to a drive called the “OS Drive”. This is where the applications and operating system reside. At installation time, the size of this drive may need to be increased or changed. The default sizes for this drive, at installation time, appear to be:

- Mitel Standard Linux (MSL): 16GBytes
- Windows OS: 128GBytes

If a Windows server does not require the full 128GBytes, some cost savings can be obtained by reducing this drive to 64GBytes. However, the cost reduction is minimal, and reducing this drive below 64GBytes is not recommended for this operating system the SQL server is used, additional drives will be required for the data, and this will be defined as a Premium SSD drive. Most of the Mitel applications are not intensive users of SQL, and may not need the performance, with associated costs, of this storage. Selections and adjustments are possible to change this to Standard SSD, at a more reasonable cost. Additional information on the process is included the *Azure Deployment Guidelines*.Some applications use PostgreSQL, an alternative to SQL. It is recommended that the data for these databases is also deployed on a separate partition, and the recommendation is to allocate this to a separate SSD drive, especially for larger installations. However, the use of HDD drives has also been shown to work well, especially at the more cost-sensitive smaller installations. Additional information on the process is included the *Azure Deployment Guidelines*.Refer to the application requirements in terms of how this storage is defined, especially when there is a requirement to provide multiple partitions within this space. Azure provides the infrastructure; it is not application-aware nor aware of the requirements of any associated storage. The Call and Screen Recording (MIR) applications require connection to a ‘Cool Storage’ file share, which also needs to be configured on the appropriate servers. The size of this file share is dynamic, and Azure charges according to the space used and how often the data is retrieved. It is strongly recommended to include data retention controls to these files within the application and in the storage, in order to prevent storage over-use and costs exceeding expected limits. The amount of expected storage can be calculated in advance along with the expected costs for this. The Call and Screen Recording require a database. This is based on PostgreSQL, and not subject to the

same limits and license costs of SQL. The size of this database is dependent on the quantity of the recordings required, the traffic rate, and the retention period, i.e. it is very customer dependent. Select an appropriate E-Type SSD storage partition to meet the customer requirements. Again, the size of this database can be defined in advance, given sufficient inputs. The storage can be increased at a later date, if necessary - remember Azure allows the storage to grow, but NOT decrease. Understanding the storage quantity requirements and storage retention policy in advance of deployment will help minimize this situation occurring.

17.2.3 Server Resource Definitions (Azure)

		Azure Definition				Azure Resources				
Description	Product	CPU	OS HDD	Data SSD	Cool Storage	vCPU	RAM	OS HDD	Data HDD/ SSD	Application Cool Storage
MiCollab 250	MiCollab	**D2s v4**	**S6**			2	8	64		
MiCollab 500	MiCollab	**D4s v4**	**S6**			4	16	128		
MiCollab 2500	MiCollab	**D8s v4**	**S6**			8	32	128		
MiCollab 5000	MiCollab	**D8s v4**	**S6**			8	32	128		

*Note 1: The database needs to be provided on a separate partition and the size of the partition is determined by customer requirements, such as number of calls, number of users and database retention period. Calculators are available to determine the size of the database in advance. Since this is a database with high level of access, the use of SSD rather than HDD is recommended for the Medium and Large server configurations.

*Note 2: Call and Screen Recording files are stored in Azure Cool Storage. This storage is expandable, depending on use and customer usage. Calculators are available to determine the size of the storage requirements in advance. This can

be mapped directly for smaller systems. Access to the Cool Storage can be via the core server. However, where this storage exceeds 700G, it is recommended to use the Archive server as the front end to the Cool Storage, especially in a multi-server deployment.

Appendix E: Glossary 18

TERM	NAME	DESCRIPTION
3300 ICP	3300 IP Communications Platform	Mitel IP communications platform supporting 30 to 60,000 users. The 3300 ICP is the hardware platform that runs the MiVoice Business (MiVoice Business) software.
AMC	Application Management Center	A web-based service that handles licensing of Mitel products
ARID	Application Record ID	An identification number obtained from the Mitel Application Management Center (AMC). Used to license software on a specific Mitel product.
BUP	Bulk User Provisioning	A software tool within the USP application that allows you to bulk import user data from a .csv or LDIF file; use Quick Add to provision a single user; program a range of fields using Auto-Fill; apply roles to multiple users; and resolve detained and failed IDS updates.
CLID	Calling Line Identification	CLID enables the telephone number of the calling party to be displayed on the display screen of the receiver's telephone. There are now a number of contact-management applications that have made it possible to use CLID to automatically bring up client information from a database and display it on the screen of a personal computer (PC) before the call is answered.
Cluster		Refers to a grouping of elements (for example, a network of MiVoice Business systems) that share common dialing plans, or common directory information, such as Remote Directory Numbers with Telephone Directory.

TERM	NAME	DESCRIPTION
CO	Central Office	A switch, installed in a telephone system serving the general public, that has the necessary equipment and operating arrangements for terminating and interconnecting lines and trunks.
CODEC	Encoder/Decoder	Software or hardware that compresses and decompresses audio and video data streams.
CPN	Calling Party Number	CPN (Calling Party Number) substitution is typically used to show the customer's corporate name and number for all outgoing calls to the public network.
Directory Server		A directory server is not simply a form of database, but a specialized server for directories. A directory can be distinguished from a general-purpose database by the usage pattern. A directory contains information that is often searched but rarely modified. Host names or user names, for example, are assigned once and then looked up thousands of times. Directory servers are tuned for this type of usage, whereas relational databases are much more geared toward maintaining data that's constantly changing. Another difference is that relational databases store information in rows of tables, whereas in directory server they use object-oriented hierarchies of entries.
DMZ	Demilitarized Zone	In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network like the Internet. One or more computers also run outside the firewall, in the DMZ.

TERM	NAME	DESCRIPTION
DHCP	Dynamic Host Configuration Protocol	This is a TCP/IP protocol that automates the assignment of IP addresses of devices on a network from a central server. The DHCP server is run on the host computer and the DHCP Client is the workstation. Information given to a client includes the subnet mask, gateway address, and DNS (Domain Name Server) address.
DSL	Digital Subscriber Line	A Digital Subscriber Line provides high-bandwidth information over conventional copper wiring. The four most commonly used types of DSL are: ADSL, HDSL, SDSL, and VDSL
DTMF	Dual Tone Multi-Frequency	Tones generated typically by touch tone phones.
E2T	Ethernet to TDM	Ethernet to TDM – a system component that provides a gateway function for voice samples, between the packet domain (Ethernet) and Time Division Multiplexing (TDM) domain.
G.711	ITU-T codec audio standard	This standard specifies an audio signal that uses a 3.4 KHz bandwidth (ordinary analog voice signal) over an A-law and μ-law digitized, linear PCM at 64Kbps. In G.711, encoded voice is already in the correct format for digital voice delivery in the PSTN or through PBXs.
G.729	ITU-T standard	This standard describes CELP compression where voice is coded into 8-kbps streams. The two variations of this standard (G.729A and G.729A Annex A) differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM.
ICP	IP Communications Platform	MiVoice Business IP Communications Platform

TERM	NAME	DESCRIPTION
IDS	Integrated Directory Services	Synchronizes user and service data between a corporate directory server and the MiCollab-IDS using the Lightweight Directory Access Protocol (LDAP).
IPSect	Internet Protocol Security	A set of protocols for encryption of IP traffic over the Internet through virtual private networks (VPNs).
ISP	Internet Service Provider	An organization that provides users with an Internet connection.
IVR	Integrated Voice Response	Interactive Voice Response is an automated call handling system in which the caller interacts with a computer device which can interpret and react to voice or touch tone commands. The interaction can be through the use of a touch tone telephone or through speech recognition. This telephone-based application prompts the inbound caller for information using a recorded or synthesized human voice. Most IVR systems do not allow the caller to respond by voice, but require user input through touch-tone response
LAN Mode	Local Area Network Mode	A deployment model for the MiCollab (or Mitel Standard Linux) server. When MiCollab is deployed in server-only mode, it provides the network with services, but not the routing and security functions associated with the role of "gateway". The LAN mode configuration is typically used for networks that are already behind a separate firewall. In other words, a separate firewall fulfills the role of gateway, providing routing and network security. (Also known as Server-only mode).

TERM	NAME	DESCRIPTION
LDAP	Lightweight Directory Protocol	Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.
MBG	MiVoice Border Gateway	Previously known as the Multi-Protocol Gateway. The MiVoice Border Gateway (MBG) is a multi-service software application with a Web proxy that provides a secure method for Teleworker Web clients to connect to the LAN.
MiCollab	Formerly Mitel Applications Suite	Mitel product that unifies communication applications for small and medium sized businesses into an easy -to-use, cost effective solution. MiCollab supports multiple Mitel applications on a single industry standard server.
MiCollab Client	Formerly Unified Communicator Advanced	Application that provides users with a single access point for all their business communication and collaboration needs. It converges the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications.

TERM	NAME	DESCRIPTION
MiCollab Client Integration Wizard		A software application (wizard) that integrates MiCollab Client user and phone data with the MiCollab USP data (see MiCollab Client Integrated Mode). If you are installing a new MiCollab system into an existing site that consists of one or more MiVoice Business platforms, you can use this wizard to update the MiCollab database with the user and phone data from the MiVoice Business.
MiCollab AWV		Mitel software solution that provides conferencing and collaboration services using a Web-based browser. In previous MiCollab releases, the product name for this application was Mitel Conferencing Advanced.
MiCollab Server		MiCollab software installed in conjunction with the MSL operating system on a server platform.
MiCollab Virtual Appliance	Formerly Mitel Applications Suite Virtual Appliance	MiCollab running as a virtual application (vApp) within the VMware VSphere environment.
MiCW	Mitel Integrated Configuration Wizard	A standalone software application that performs initial system setup of the MiCollab server and the MiVoice Business software.
MiVoice Business	Formerly Mitel Communications Director (MCD)	MiVoice Business is the brand name of the call-processing software that runs on hardware platforms, such as 3300 ICP controllers.
MiVoice Business-ISS	Formerly Mitel Communications Director (MCD) for Industry Standard Servers	This communications platform consists of MiVoice Business call processing software running on an industry standard platform. MiCollab is supported for the MiVoice Business-ISS platform.

TERM	NAME	DESCRIPTION
MiCollab for Microsoft		An application that integrates with Microsoft Skype Client and allows Microsoft Skype users to use Mitel telephony functionality through its feature rich MiCollab Client infrastructure.
MiVoice Office 250	Formerly Mitel 5000 Communications Platform	Mitel IP communications platform supporting up to 250 users.
MOL	Mitel Online	Mitel's web portal for authorized dealers and technicians.
MiNET	Mitel Network Layer Protocol	A layer 2 protocol used to transport messages between the PBX and all Mitel DNIC phones
MSL	Mitel Standard Linux	The operating system that supports MiCollab software; along with Mitel SDK components, it comprises a base for all MiCollab software.
My Unified Communications Portal		MiCollab application that provides a common interface for users to update/enter user-configurable information for all applications.
NAT	Network Address Translation	For a computer to communicate with other computers and Web servers on the Internet, it must have an IP address. An IP address is a unique 32-bit number that identifies the location of your computer on a network. An IP address is similar to a street address in that it is means to find out exactly where you are and deliver information to you. Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers

TERM	NAME	DESCRIPTION
Network Edge Mode		A type of deployment for the MiCollab (or Mitel Standard Linux) server. In this deployment configuration, MiCollab manages the connection to the Internet by routing Internet data packets to and from the network (which allows all the computers on the network to share a single Internet connection) and by providing security for the network, minimizing the risk of intrusions. When one of the computers on the local network contacts the Internet, MiCollab not only routes that connection, but seamlessly interposes itself into the communication. This prevents a direct connection from being established between an external computer on the Internet and a computer on the local network, which significantly reduces the risk of intrusion. (Also known as Server-gateway mode).
NP-UM	NP-UM Messaging	Server-based voice processing system that provides call processing along with voice messaging and paging support.
Oria	A system management and customer self-service application. It allows a service provider to manage and deploy hosted voice services to their customers. Oria also allows a service provider to offer each of their customers an administration and self-service portal to make site specific moves, adds, changes, and deletes.	
Outgoing Line	Mobile Extension software phone emulator which calls user mobile phone when a call is received at the User's desktop.	
OVA	Open virtual appliance or application	A packaging format for virtual machines that allows virtual machine templates to be distributed, customized, and instantiated on any OVA supporting VMM/hypervisor.

TERM	NAME	DESCRIPTION
PPPoA	Point-to-Point Protocol over Asynchronous Transfer Mode (ATM)	A protocol that encapsulates PPP frames in ATM Adaptation Layer 5 (AAL5). PPPoA is used primarily in cable modems, wireless devices, and ADSL broadband local loops for Internet access.
PPPoE	Point-to-Point Protocol over Ethernet	An access control method that allows remote hosts to log on and off using a simulated dial-up connection. PPPoE is typically offered by cable and DSL Internet service providers.
PPTP	Point to Point Tunneling Protocol	A protocol that encapsulates data sent over the Internet within a virtual private network (VPN).
QoS	Quality of Service	Quality of Service. The performance of a communications channel or system is usually expressed in terms of QoS. The QoS will relate to the type of system. SNR (Signal to Noise Ratio), BER (Bit Error Ratio), maximum and mean throughput rate, reliably, priority and other factors specific to each service.
Role		A role defines the task, position, or responsibilities for a type of user within the organization. Roles are associated with user templates that define the common phone and application service settings for the roles.
RTP	Real Time Protocol (FRD 1889)	A transport protocol to deliver live media to viewers simultaneously.
SAA	Speech Auto Attendant	Speech-enabled software application that allows users to place calls quickly and efficiently by speaking a person’s name, a department name, or telephone number.

TERM	NAME	DESCRIPTION
SAS	Suite Application Services	This application provides single-point user services provisioning and centralized management of shared system resources for all the MiCollab applications. This application also provides the My Unified Communications web portal.
Server Console		A text-based control panel built into the Mitel Standard Linux operating system that technicians use to perform maintenance tasks such as • install the MAS software • configure network parameters • perform upgrades and software updates • upgrade application suite licensing • perform backups.
Server-gateway mode		See Network Edge mode.
Server manager		A web-based control panel, also called the "server manager", that administrators use to configure and administer the MAS applications • perform server administration tasks, such as view logs, display system information, assign system users, and perform backups • configure network and server security settings • set system-wide parameters, such as system language and password strength.
Server-only mode		See LAN mode.

TERM	NAME	DESCRIPTION
SIP	Session Internet Protocol	SIP is an ASCII-character-based signaling protocol designed for real-time transmission using Voice over IP (VoIP). The appeal of SIP is the promise of interoperability of telephones from propriety PBXs. SIP extends the foundation of open-standards from the Internet to messaging, enabling disparate computers, phones, televisions and software to communicate. SIP is a streamlined protocol, developed specifically for IP telephony. It is smaller and more efficient than H.323. SIP takes advantage of existing protocols to handle certain parts of the process. For example, Media Gateway Control Protocol (MGCP) is used by SIP to establish a gateway to connect to the PSTN system. SIP operates independently of the underlying network transport protocol and is indifferent to media. Instead, it defines how one or more participant's end devices can create, modify and terminate a connection whether the content is voice, video, data or Web-based. Using SIP, programmers can add new fragments of information to messages without compromising connections.
SRC	Secure Recording Connector	Formerly a standalone call recording product, SRC is now incorporated in the MBG software.
STT	Speech to Text	An optional, licensed feature of NuPoint UM that converts voice mail messages to text, allowing users to discreetly access voice messages in a text format.
SRTP	Secure Real Time Protocol (IETF Standard: http://www.ietf.org/rfc/rfc3711.txt – Apr 04)	Defines a profile that can be used to provide encryption, message authentication and integrity, and protection from replay attacks to the RTP data for audio and video streams.

TERM	NAME	DESCRIPTION
SSL	Secure Socket Layer	A technology that works at the transport layer that does authentication and encryption between a Web server and a Web browser.
Stateful Inspection		Stateful inspection is an advanced firewall architecture that was invented by Check Point Software Technologies in the early 1990s. Also known as dynamic packet filtering, it has replaced static packet filtering as the industry standard firewall solution for networks.
TCP	Transmission Control Protocol (RFC 1122 Section 4.1)	A transport layer protocol with sequencing error detection and flow control. Transmission Control Protocol is a method used along with the IP to send data in the form of message units between computers over a network. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data that a message is divided into for efficient routing through the Internet.
TFTP	Trivial File Transfer Protocol (RFC 783)	A simple file transfer protocol (no password protection or user directory services) that uses UDP to transfer files across a network.
Transcode	Changing audio digital format from one format to another (G.711 to G.729)	
TUI	Telephone User Interface	Prompts played by a system application over the telephone that instruct users on how to use application features, such as voice mail features, from the telephone.
TW	Teleworker	Software that connects a remote office to the corporate voice network to provide full access to voice mail, conferencing and all the other features of the office phone system.

TERM	NAME	DESCRIPTION
UCC Licensing	Unified Communications and Collaboration Licensing	Mitel's licensing model. The platform and application user licenses are bundled together to meet the needs of different user levels (for example, Entry, Standard, and Premium). Instead of ordering an MiVoice Business user license and multiple individual applications licenses for each MiCollab user, you order a single UCC license per user.
UC Portal	My Unified Communications portal	A MiCollab application that provides a common portal for users to update/enter user-configurable information for all applications.
UDP	User Datagram Protocol (RFC 1122 Section 4.1)	UDP is an alternative to the TCP and, together with IP, is sometimes referred to as UDP/IP. Like TCP, UDP uses IP to actually get a datagram from one computer to another. UDP does not provide the service of dividing a message into packets and reassembling it at the other end. UDP doesn't provide sequencing of the packets that the data arrives in. Network applications that want to save processing time because they have very small data units or don't require the above services may prefer UDP to TCP e.g. TFTP uses UDP instead of TCP.
USP	User and Service Provisioning	MiCollab tool used to provision users

TERM	NAME	DESCRIPTION
VoIP	Voice over Internet Protocol	VoIP technology, also known as IP Telephony, is the technology used to deliver telephony over a data network instead of using the standard public switched telephone network Rather it uses the Internet Protocol. VoIP means that voice is converted from an analogue signal, encoded digitally, then is converted into packets. It then uses a data network to move those packets along the most efficient path to their destination, where they are reassembled and delivered and converted back into a voice transmission.
VPN	Virtual Private Network	VPN support by the firewall is one of the core features that enable flexibility in a variety of environments. The VPN supports both site-to-site and remote-access VPNs encryption. This dual support provides the ability to connect two branch offices together using only firewalls on each side (site-to-site), or to connect remote users to the office via a VPN across the Internet (remote-access). IPSec, PPTP, and L2TP are the main VPN technologies supported.