A MITEL
PRODUCT
GUIDE

MiVoice Business

MiVoice Business Solution Virtual Instance

Release 1.0 FP1

November 2024

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), its affiliates, parents, or 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.

Contents

Introduction 1

This chapter contains the following sections:

MiVoice Business Solution Virtual Instance (MiVB SVI) is a single Virtual Machine that includes Mitel's MiVoice Business, MiCollab Client and Admin services, and MiVoice Border Gateway (MBG). The distribution features a single virtual instance of Mitel Standard Linux (MSL), which runs all the software applications.

MiVoice Business Solution Virtual Instance supports the installation of the CloudLink Gateway blade (optional) in support of Mitel Administration for MiVoice Business and other CloudLink applications. Additionally, the Mitel Performance Analytics (MPA) probe (optional) can be deployed on the same virtual server.

1.1 Intended Audience

This document is intended for certified MiVoice Business, MiCollab, MBG, CloudLink for MiVoice Business, and / or MPA technicians who are installing, on-boarding, maintaining, or troubleshooting the solution and pre-sales engineering.

This guide is intended primarily for

- Installers who install and perform initial configuration on the product
- Service providers who performs ongoing maintenance and upgrades on the product
- Site Engineers who qualify and plan site-specific information for installation of the product
- System Administrators who program and troubleshoot the product
- Data center providers who host the virtual infrastructure on which the MiVoice Business Solution Virtual Instance resides
- Partners who deploy, configure, provision, and maintain the MiVoice Business Solution Virtual Instance.
- Customers who choose to deploy the virtual infrastructure and then allow a partner to deploy, configure, provision, and maintain the solution

Service providers, partners, and customers who use this document must have successfully completed the required MiVoice Business Solution Virtual Instance Training.

Note:
This document does not describe management tools that service providers might use or offer to resellers to manage their infrastructure.

1.2 What's New in this Document

This section describes changes in this document due to new and changed functionality in MiVoice Business Solution Virtual Instance.

Table 1: Document Version 1.0 FP1

Feature	Update	Location	Publish Date
Support of Nutanix and Hyper-V platforms	Added Nutanix, Hyper-V along with vSphere platforms	Deploy on Nutanix Prism on page 63 Deploy VM on Hyper-V on page 68	November 2024

1.3 MiVoice Business Virtual Instance Solution Key Highlights

This section highlights the key differences of MiVoice Business Solution Virtual Instance compared to the other stand-alone products like MiVoice Business, MiCollab, MBG, and SMBC.

Note:
If you are used to configuring and managing Mitel Virtual solutions like vMBG, vMiCollab, it is important to note that MiVoice Business Solution Virtual Instance is different in many aspects and requires different configuration.

The key differences are mentioned below:

- Configure the 2nd IP address on default LAN, as MiCollab and MBG are dependent on the second IP.
- Provision separate FQDNs for MBG, MiCollab, MiVoice Business ESM, and MiVoice Business Embedded Voice Mail as recommended in the the Deployment Model section.
- Override the MiCollab (UCA) host name (FQDN) in Client Deployment as described in Configure MiCollab Client Deployment on page 92.
- MiCollab User Portal is not supported. The users can change their MiCollab settings (like password, external hot desk number) from MiCollab Client.
- AWV and NuPoint are not part of MiVoice Business Solution Virtual Instance.
- The **Reach Through** option is not available for the MiVoice Business Solution Virtual Instance deployment.
- Default enterprise ID [1]/ domain[2] can be configured in the Configure MiVoice Business section.

[1] Enterprise ID is a unique ID and is derived from system name during system deployment. It remains non-editable and cannot be changed by Administrators.

- Provision MiCollab public FQDN as the additional Allowed URI Names (under the SIP Options in MBG).
- Voicemail solution is Embedded Voice Email.
- Embedded Voice Email passcode can be changed using Embedded Voice Mail menu system. Refer Configure MiVoice Business.
- Desktop tool is not supported. The user can change embedded voice mailbox PIN code using TUI menu system by calling into the voicemail system and using the keypad to navigate to the appropriate menu.
- Unique SDS system name is "default".
- To configure MBG network profile, refer Configure Optional Standalone vMBGs on page 94.
- Programming remote proxy / reverse proxy.
- Web server certificates. Refer Configure MSL Server on page 80.
- MPA probe monitors all the configured interfaces.
- Clustering with a 2nd MiVoice Business Solution Virtual Instance server is supported for resiliency.
- Clustering with other MiVoice Business products is not supported.

Description 2

This chapter contains the following sections:

The Mitel® MiVoice Business Solution Virtual Instance provides a complete unified and collaboration communication solution for small to mid-range businesses.

2.1 Components

The MiVoice Business Solution Virtual Instance consists of the following components:

- *MiVoice Business*: provides teleworker service and secure recording connector for the remote Teleworker sets only. It also supports SIP trunks.
- *MiCollab*: provides the Server Manager interface for system administration and the following applications:
  - *Users and Services*: for provisioning users and their services.
  - *MiCollab Client*: combines the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications.
  - *MiCollab Client Deployment*: supports the simplified deployment of MiCollab for Mobile clients.
- *MiVoice Border Gateway*: provides teleworker service and secure recording connector for the remote Teleworker sets only.
- (Optional) *CloudLink Gateway*: provides integration with CloudLink-based (for example, CloudLink API program or Mitel Assistant).
- (Optional) *Mitel Performance Analytics (MPA)*: provides integration with Mitel Performance Analytics Cloud Service.

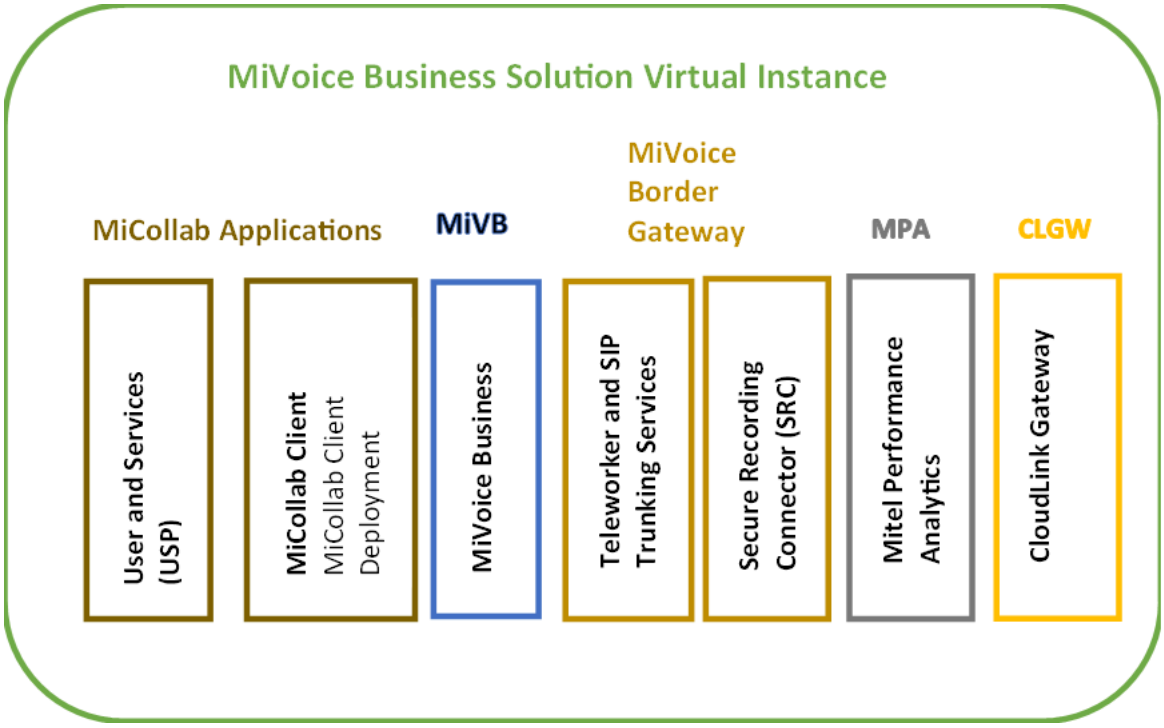


Figure 1: MiVoice Business Solution Virtual Instance components

2.2 MiVoice Business Solution Virtual Instance Security Controls

The security controls provided by the MiVB SVI, and the associated applications are primarily based on the following open standard technologies and management access controls:

- TLS – Transport Layer Security (TLS) provides:
  - Secure signaling between IP phones and MiVoice Business.
  - Secure signaling between remote IP phones and the MiVoice Border Gateway.
  - Secure access to the administration tools for managing the various applications.
  - Secure communications between the CloudLink platform and the Virtual Private Cloud.
- SSH - Secure Shell (SSH) provides secure console-based access to:
  - The MiVoice Business System administration and configuration tools.
  - The MiVoice Border Gateway administration and configuration tools.
  - The MiCollab administration and configuration tools.
- SRTP - Secure Real-time Transport Protocol (SRTP) is used to protect:
  - The voice media streams between IP phones.
  - The voice media streams between IP phones and the MiVoice Business.
  - The voice media streams between remote IP phones and the MiVoice Border Gateway.
- Correct configuration of identity and access management policies to ensure all end user and administrator accounts, roles, permissions and password policies.

- OAuth 2.0 (Open Authorization) is used by voice mail and MiCollab to authenticate with other email applications such as Google Apps and Microsoft Office 365.
- S-LDAP – Secure LDAP is used for connectivity from MiVoice Business to a customer's Active Directory server.

Other mechanisms that can be employed to protect the MiVoice Business Solution Virtual Instance solution are based on the following:

- A securely designed corporate Local Area Network (LAN) infrastructure.
- Correct configuration of internal and external (Internet facing) routers and firewalls

In addition to the security recommendations described in this document and in the applications documentation, there are a number of general security aspects that must be addressed by the system Administrator and/or the Information Technology (IT) security officer.

An important security measure is to establish and maintain physical security. Only authorized personnel should have access to server locations since many data-exposure attacks can be mounted by having physical access to a host. Further, the IT data infrastructure should be designed with security in mind, security controls, and protocols should be enabled, and all components of the whole system should be correctly configured and maintained and updated as necessary.

2.3 About MiVoice Business Solution Virtual Instance

Complete product installation, engineering and administration documentation related to MiVoice Business Solution Virtual Instance, and the associated applications can be found on Mitel's Document Center.

The Mitel Document Center web site can also be accessed by anyone with a miaccess.mitel.com account via the MiAccess Portal.

The following table lists the product documentation that is applicable to the MiVoice Business Solution Virtual Instance solution.

Table 2: Document Version 1.0

Document Title	Description	Location
MiVoice Business Solution Virtual Instance – Solution Guide	Current document	https://www.mitel.com/document-center/business-phone-systems/mivoice-business/mivoice-business
MiVoice Business General Information Guide	Provides an overview of the MiVoice Business system	https://www.mitel.com/document-center/business-phone-systems/mivoice-business/mivoice-business

Document Title	Description	Location
MiVoice Business Troubleshooting Guide	Provides troubleshooting instructions related to MiVoice Business.	https://www.mitel.com/document-center/business-phone-systems/mivoice-business/mivoice-business
MiVoice Business Engineering Guidelines	Provides guidelines for planning an installation of a MiVoice Business Communications Platform.	https://www.mitel.com/document-center/business-phone-systems/mivoice-business/mivoice-business
Mitel IP Sets Engineering Guidelines	Provides guidelines for individuals who are planning for the installation of Mitel IP phones.	https://www.mitel.com/document-center/business-phone-systems/mivoice-business/mivoice-business
Network Engineering for IP Telephony	Provides guidelines that is considered prior to deploying IP phones, such as network design, QoS mechanisms, and related protocols.	https://www.mitel.com/document-center/devices-and-accessories/ip-phones/general-ip-phone-documentation/all-releases/en/network-engineering-for-ip-telephony
MiVoice Border Gateway documentation	Provides information on how to install, maintain, configure, and get performance information for the MiVoice Border Gateway and associated products.	https://www.mitel.com/document-center/applications/mivoice-border-gateway
Mitel Performance Analytics documentation	Provides instructions for installing a new Mitel Performance Analytics (MPA) monitoring system and its operations.	https://www.mitel.com/document-center/applications/analytics/mitel-performance-analytics/
CloudLink documentation	Provides information on how to integrate CloudLink with MiVoice Business	https://www.mitel.com/document-center/technology/cloudlink
MiCollab documentation	Provides information on how to install, maintain and configure the MiCollab application.	https://www.mitel.com/document-center/applications/collaboration/micollab/micollab-client

2.4 Product Security

Security controls and features for specific applications and how to enable them are discussed in various documents within the product documentation suite. The product documentation suite includes product administration, management, deployment, installation guides, and security related documents.

The product's Security Guidelines summarize all of the product's security controls and features in one document and provides the Administrator with security recommendations. The product Security Guidelines also refers the Administrator to the appropriate sections of product documents for further details on specific security controls.

The product's Personal Data Protection and Privacy Controls document identifies the personal data collected, processed or transferred by the product. The Personal Data Protection and Privacy Controls document also provides the Administrator with recommendations on how to secure the personal data and refers the Administrator to the appropriate product documents for further details.

Additional product security information and recommendations may be found in Technical Papers, White Papers, and FAQs, which are located on Mitel's Document Center. The following section provides an overview of the type of information that are found in the Security Guidelines and the Personal Data Protection and Privacy Controls document.

Product Security Guidelines

The product security guidelines are to be used in conjunction with the product's documentation suite to ensure the product is securely deployed and maintained. The product security guidelines provide detailed information and recommendations on the following topics:

- The product's architecture.
- An overview of the product's security controls and features.
- How the administration interfaces are secured.
- Certificate management.
- Access controls and authentication controls.
- Audit trails and logs.
- LAN and WAN communications security.
- VoIP security

Product Personal Data Protection and Privacy Controls documents

The Personal Data Protection and Privacy Controls documents are to be used in conjunction with the product's documentation suite to assist the customer with their data security regulations compliance initiatives. The Personal Data Protection and Privacy Controls documents provide detailed information on the following:

- Identification of personal data that is collected, processed, or transferred.
- How the product security features relate to data security regulations.
- Where the security feature is documented.

2.5 MiVoice Business Solution Virtual Instance Security

To ensure that the MiVoice Business Solution Virtual Instance is securely deployed, operated, and maintained, the Administrator must be familiar with the information and the recommendations provided in the security documents that are listed in this section.

MiVoice Business

- Mitel MiVoice Business – Security Guidelines.
- Mitel MiVoice Business – Personal Data Protection and Privacy Controls.
- MiVoice Business Secure Voice Communications.
- MiVoice Business Security FAQ.

IP Phones and MiVoice Business Console

- Mitel MiVoice 6900 Series IP Phones (MiNET) Personal Data Protection and Privacy Controls.
- Mitel MiNet 6900 Series SIP Phones - Personal Data Protection and Privacy Controls.
- Mitel MiNet 6900 Series SIP Phones Administrator Guide.
- Mitel IP Sets Engineering Guidelines, refer to the section on Security.
- MiVoice Business Console Personal Data Protection and Privacy Controls.
- SIP-DECT Security Guidelines.

MiVoice Border Gateway

- MiVoice Border Gateway Personal Data Protection and Privacy Controls.
- MiVoice Border Gateway Engineering Guidelines.
- Security and the Mitel Teleworker Application Whitepaper.

Mitel Performance Analytics

- Mitel Performance Analytics Security Summary.
- Mitel Performance Analytics Best Practices.

MiCollab

- MiCollab Personal Data Protection and Privacy Controls.
- MiCollab Security Guidelines.

CloudLink Gateway

- CloudLink Security.
- CloudLink Chat Security.
- CloudLink Security FAQ.

Mitel Standard Linux

- Mitel Standard Linux Security Technical Paper.
- MSL Installation and Administration Guide.

MiTeam Meetings

- MiTeam Meetings Security Guidelines.

2.6 Characteristics

MiVoice Business Solution Virtual Instance has the following characteristics:

- Supports the following user resource capacities:
  - 250 user resources capacity for small business. 700 devices is supported for 250 users deployment by default.
  - 500 user resource capacity for enterprise business.

MiVoice Business Solution Virtual Instance Deployment	ACD Agent Limit	SIP Trunk Limit	Embedded Voice Mail Channel Limit
250 users	50 agents	50 trunks	10 channels
500 users	100 agents	100 trunks	20 channels

- For installations on VMware, all the software applications are installed when you deploy the MiVoice Business Solution Virtual Instance OVA file.
- Can be deployed in Network Edge (Server-gateway) or LAN only (server-only) mode.
- Provides single point of provisioning to the MiVoice Business and applications from MiCollab.
- Minimizes user provisioning through bulk data import and the application of roles and templates
- Integrates with Active Directory (supports the addition and deletion of users from Active Directory)
- Supported in virtual environment. See the Virtual Appliance Deployment Guide guide for details.
- Supports Flow Through Provisioning: This feature synchronizes updates made to the following data between the User and Services Provisioning database and the MiVoice Business database using System Data Synchronization (SDS):
  - User and services data
  - Programmable Ring Groups (PRGs)
  - Multi-Device User Groups
  - Roles
  - Templates
- Supports Reach-Through: This feature allows you to access MiVoice Business System Administration System Administration tool forms from links or drop-down menus within specific User and Services administration pages. Because you have logged into the MiCollab server manager, you are allowed direct access and do not have to log in separately to the MiVoice Business. This functionality reduces the amount of time it takes to perform programming tasks that require configuration on the MiVoice

Business, such as modifying a user's MiVoice Business phone and group settings. MiVoice Business systems also support Reach Through to MiCollab. Administrators can link directly to certain MiCollab USP pages from specific MiVoice Business system administration tool forms.

- Support of Mitel Administration for MiVoice Business for user provisioning: The Mitel Administration portal is used to provision users and services in the MiVoice Business Solution. The Mitel Administration for MiVoice Business application is provided via CloudLink. For more information, see Mitel Administration for MiVoice Business Solution Guide

2.7 Deployment Models

The solution is well adapted to the following deployments:

- **Server Gateway Deployment model**: In this deployment configuration, MiVoice Business Solution Virtual Instance 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.
- **Server Only with Bastion Host MBG**: In this configuration, MiVoice Business Solution Virtual Instance 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).
- **Server Only Deployed in DMZ**:
- **Server Gateway with Resiliency**: In this configuration, resiliency for telephony applications is provided by deploying a secondary MiVoice Business Solution Virtual Instance server. Resiliency is supported for the MiVoice Business and MBG applications in this configuration. MiCollab application is not resilient.
- **Infrastructure as a Service (IaaS)**: Infrastructure providers rent out the resources (for example: vCPU, GHz, RAM, HDD, ports and so forth) required to host the MiVoice Business Solution Virtual Instance solution on their virtualized server infrastructure.
- **Customer Premise Deployment**: Mitel certified dealers install and configure MiVoice Business Solution Virtual Instance in the virtual environment on the customer’s premise.

All Mitel internet-facing applications must be deployed behind a properly configured corporate firewall. Mitel recommends following the best practice of deploying stand-alone gateways specifically designed to be internet-facing, such as the Mitel Border Gateway (MBG), as bastion hosts in the corporate DMZ to protect LAN-based applications.

A bastion host is a special purpose system on a network specifically designed and configured to withstand potential attacks. The system generally hosts a single application (in this case it hosts the MBG application) and all other services (UC applications such as MiVoice Business, MiCollab) are not installed to reduce the threat to the system. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of a firewall or inside of a demilitarized zone (DMZ) and usually involves access from untrusted networks or system. MBG is optimized to withstand high-bandwidth attacks through the Internet.

The MiVoice Business Solution Virtual Instance product features an embedded gateway (MBG). It is recommended to employ a separate MBG gateway as a bastion host in the DMZ. In situations where cost or management complexities prohibit this approach, the embedded gateway can be deployed in an internet-facing behind the corporate firewall via its WAN interface, while still connecting to the LAN via a separate network interface.

This product has has undergone security hardening measures to minimize its vulnerability to external attacks from the Internet by isolating LAN and WAN traffic via separate network interfaces with an internal firewall.

Deploying any product intended for internet-facing use must always be coordinated with the corporate IT and conducted in compliance with their established security protocols.

2.7.1 Server Gateway Deployment

The following flowchart represents the work flow of Server Gateway Deployment:

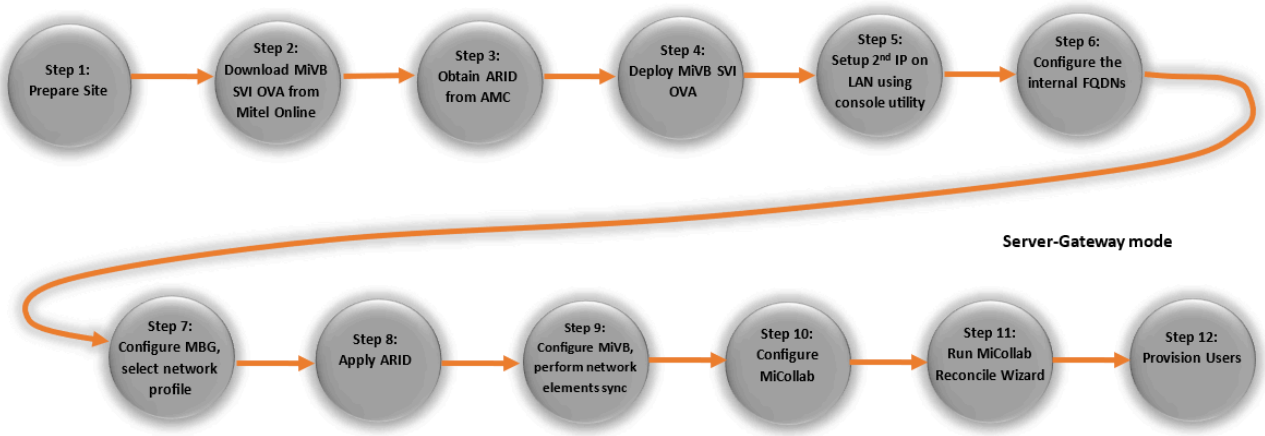


Figure 2: Server-Gateway mode

- Firewall is recommended in front of WAN interface.
- The WAN IP can be a public IP or a private IP in a public DMZ subnet, depending on the firewall configuration.
  - Co-resident MBG network profile can be used if public IP assigned to WAN interface.
  - Custom MBG network profile must be used if private IP is assigned to WAN interface.
    - ICP-side bind interface is LAN interface, RTP ICP-side override address is LAN 1 IP 2.
    - Set-side bind interface is WAN interface, RTP Set-side override address is Public IP.
- Teleworker sets and MiCollab client soft phones must be configured to connect to the main server FQDN.
- MiCollab client must be configured to connect to MiCollab public FQDN.
- MBG internal private FQDN must be programmed as SIP Trunking Proxy in MiVoice Business network element form.
- MBG internal private FQDN must be programmed in MIR for connecting to MBG.

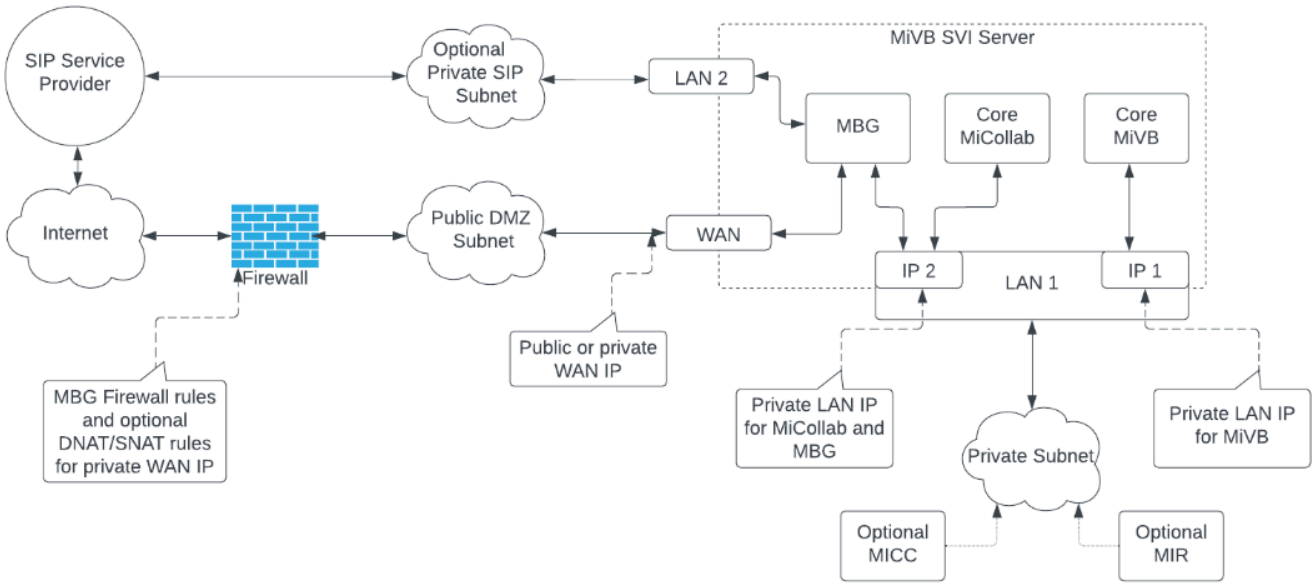


Figure 3: Server Gateway Deployment

Table 3: Public FQDNs

FQDN	Public WAN IP	Purpose
mivbsvi.example.com	1.2.3.4	Main MiVoice Business Solution Virtual Instance server FQDN for Teleworker phone, SIP, and MiCollab profile.
mivb-mgmt.example.com	1.2.3.4	Main public FQDN for access to MiVoice Business Embedded System Management (ESM)
mivb.example.com	1.2.3.4	MiVoice Business public FQDN for Embedded Voicemail
micollab.example.com	1.2.3.4	MiCollab public FQDN for MiCollab Applications
micc.example.com	1.2.3.4	Optional MICC public FQDN
mir.example.com	1.2.3.4	Optional MIR public FQDN

Table 4: Private FQDNs

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
mivbsvi.example.com	10.0.50.4			Main MiVoice Business Solution Virtual Instance server FQDN
mivb-mgmt.example.com	10.0.50.4			MiVoice Business private FQDN for MiVoice Business Embedded System Management (ESM)
mivb.example.com	10.0.50.4			MiVoice Business private FQDN for Embedded Voice Email, SIP devices, and Other.
micollab.example.com		10.0.50.5		MiCollab private FQDN
mbg-int.example.com		10.0.50.5		MBG's internal private FQDN for MIR, SIP Trunking Proxy
micc.example.com			10.0.50.6	Optional MICC private FQDN
mir.example.com			10.0.50.6	Optional MIR private FQDN

2.7.2 Server Only with Bastion Host MBG

The following flowchart represents the work flow of Server Only with Bastion Host MBG deployment:

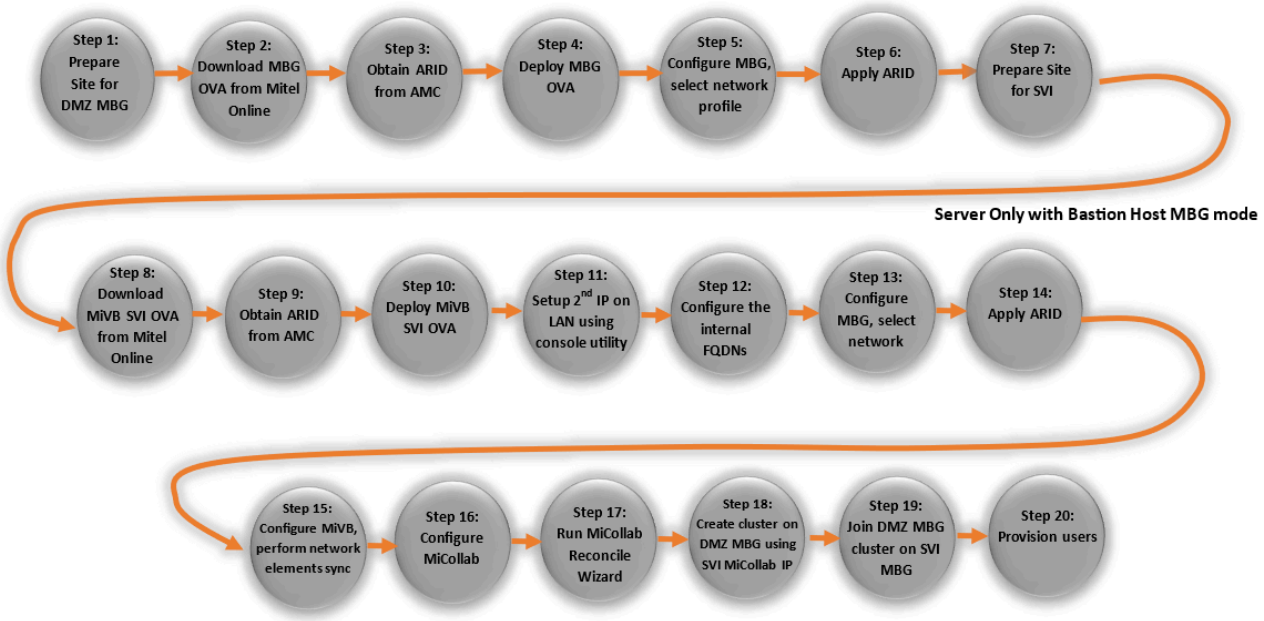


Figure 4: Server Only with Bastion Host MBG mode

- Firewall is recommended in front of WAN interface.
- The WAN IP can be a public IP or a private IP in a public DMZ subnet, depending on firewall configuration.
    - Server-only MBG network profile must be used for the MBG application in the MiVoice Business Solution Virtual Instance server.
    - Server/gateway MBG network profile can be used for the bastion host MBG if public IP assigned to WAN interface.
    - Custom MBG network profile must be used for the bastion host MBG if private IP assigned to WAN interface.
        - ICP-side bind interface is LAN interface, RTP ICP-side override address is LAN 1.
        - Set-side bind interface is WAN interface, RTP Set-side override address is Public IP.
- Teleworker sets and MiCollab client soft phones must be configured to connect to public MBG bastion host FQDN.
- MiCollab client must be configured to connect to MiCollab public FQDN.
- Bastion host MBG internal private FQDN must be programmed as SIP Trunking Proxy in MiVB network element form.
- Bastion host MBG internal private FQDN must be programmed in MIR for connecting to MBG.
- Bastion host MBG must be clustered with MBG in MiVoice Business Solution Virtual Instance server.
    - Private FQDNs must be used for MBG addresses in MBG cluster.
    - Bastion host MBG must be primary node in MBG cluster.
    - MiVoice Business Solution Virtual Instance MBG should have weight of zero in MBG cluster.

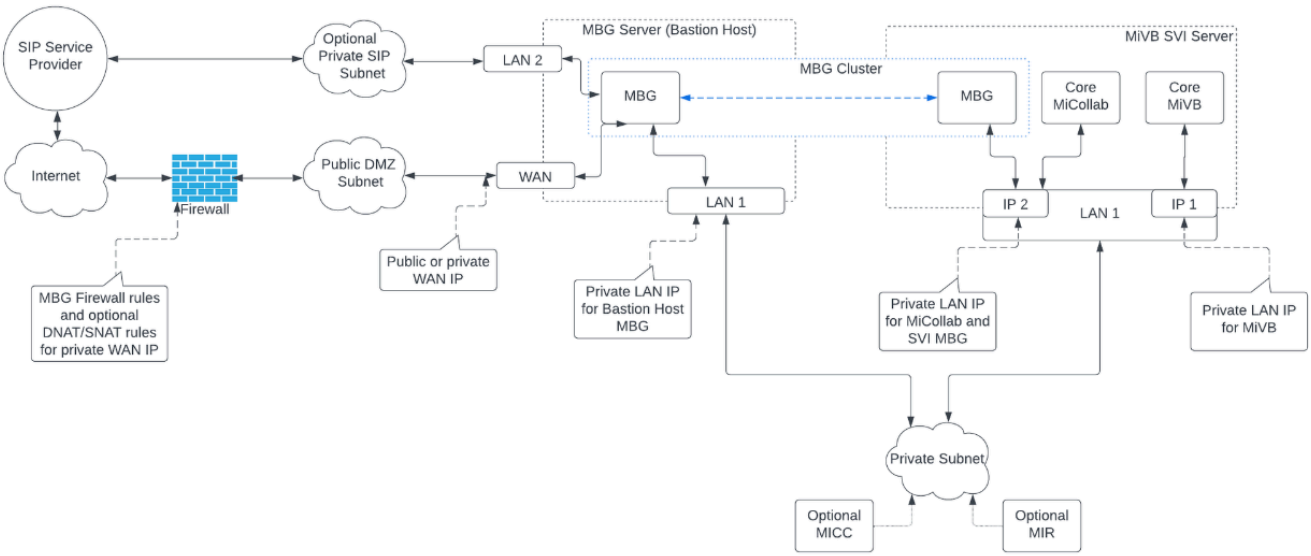


Figure 5: Server Only with Bastion Host MBG

Table 5: Public FQDNs

FQDN	Public WAN IP	Purpose
mbg.example.com	1.2.3.4	MBG bastion host FQDN for Teleworker phone, SIP, and MiCollab profile.
mivb-mgmt.example.com	1.2.3.4	MiVoice Business public FQDN for access to MiVoice Business Embedded System Management (ESM)
mivb.example.com	1.2.3.4	MiVoice Business public FQDN for Embedded Voicemail
micollab.example.com	1.2.3.4	MiCollab public FQDN for MiCollab Applications
micc.example.com	1.2.3.4	Optional MICC public FQDN
mir.example.com	1.2.3.4	Optional MIR public FQDN

Table 6: Private FQDNs

FQDN	MiVoice Business Solution Virtual Instance LAN 1 IP 1	MiVoice Business Solution Virtual Instance LAN 1 IP 2	MBG LAN IP	Other IP	Purpose
mivbsvi.example.com	10.0.50.4				Main MiVoice Business Solution Virtual Instance server FQDN
mivb-mgmt.example.com	10.0.50.4				MiVoice Business private FQDN for MiVoice Business Embedded System Management (ESM)
mivb.example.com	10.0.50.4				MiVoice Business private FQDN for Embedded Voice Email, SIP devices, and Other.
micollab.example.com		10.0.50.5			MiCollab private FQDN
mbg-int.example.com		10.0.50.5			MiVoice Business Solution Virtual Instance MBG's internal private FQDN for cluster configuration

FQDN	MiVoice Business Solution Virtual Instance LAN 1 IP 1	MiVoice Business Solution Virtual Instance LAN 1 IP 2	MBG LAN IP	Other IP	Purpose
mbg-ext.example.com			10.0.50.6		Bastion host MBG's internal private FQDN for MIR, SIP Trunking Proxy
micc.example.com				10.0.50.7	Optional MICC private FQDN
mir.example.com				10.0.50.8	Optional MIR private FQDN

2.7.3 Server Only Deployed in DMZ

The following flowchart represents the work flow of Server Only Deployed in DMZ Deployment:

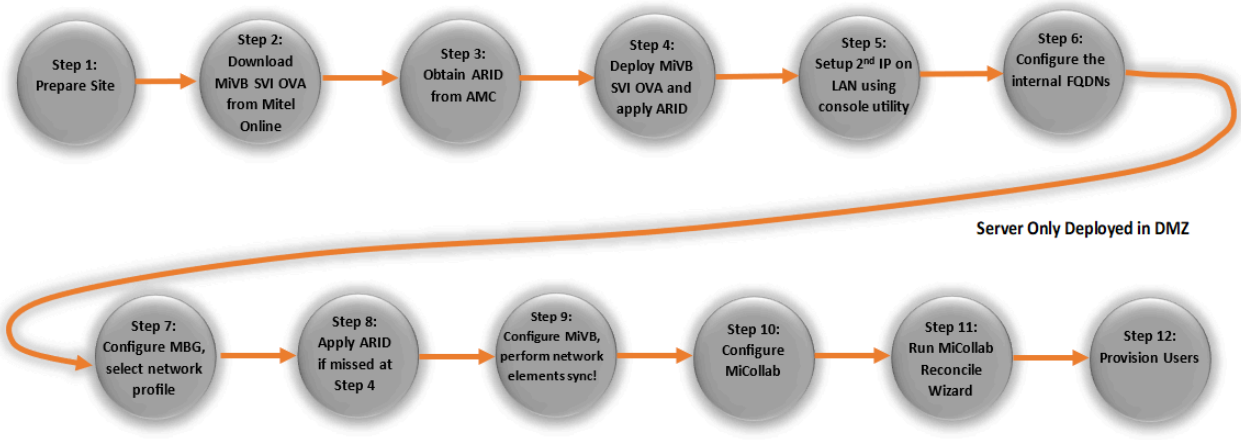


Figure 6: Server Only Deployed in DMZ

- Firewall is recommended between public IP and LAN IP.

- Custom MBG network profile must be used.
  - ICP-side bind interface is LAN interface, RTP ICP-side override address is LAN 1 IP 2.
  - Set-side bind interface is LAN interface, RTP Set-side override address is Public IP.
- Teleworker sets and MiCollab client soft phones must be configured to connect to main server FQDN.
- MiCollab client must be configured to connect to MiCollab public FQDN.
- MBG internal private FQDN must be programmed as SIP Trunking Proxy in MiVB network element form.
- MBG internal private FQDN must be programmed in MIR for connecting to MBG.

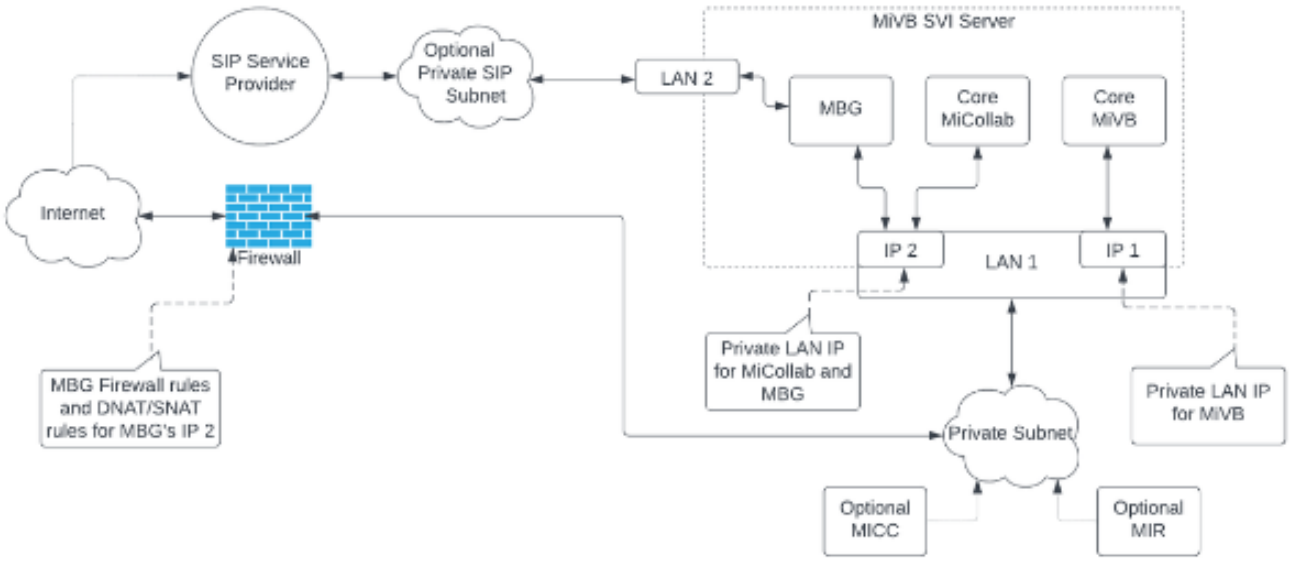


Figure 7: Server Only Deployed in DMZ

Table 7: Public FQDNs

FQDN	Public WAN IP	Purpose
mivbsvi.example.com	1.2.3.4	Main MiVoice Business Solution Virtual Instance server FQDN for Teleworker phone, SIP, and MiCollab profile.
mivb-mgmt.example.com	1.2.3.4	MiVoice Business public FQDN for access to MiVoice Business Embedded System Management (ESM)
mivb.example.com	1.2.3.4	MiVoice Business public FQDN for Embedded Voicemail

FQDN	Public WAN IP	Purpose
micollab.example.com	1.2.3.4	MiCollab public FQDN for MiCollab Applications
micc.example.com	1.2.3.4	Optional MICC public FQDN
mir.example.com	1.2.3.4	Optional MIR public FQDN

Table 8: Private FQDNs

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
mivbsvi.example.com	10.0.50.4			Main MiVoice Business Solution Virtual Instance server FQDN
mivb-mgmt.example.com	10.0.50.4			MiVoice Business private FQDN for MiVoice Business Embedded System Management (ESM)
mivb.example.com	10.0.50.4			MiVoice Business private FQDN for Embedded Voice Email, SIP, and Other.
micollab.example.com		10.0.50.5		MiCollab private FQDN
mbg-int.example.com		10.0.50.5		MBG's internal private FQDN for MIR, SIP Trunking Proxy

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
micc.example.com			10.0.50.6	Optional MICC private FQDN
mir.example.com			10.0.50.6	Optional MIR private FQDN

2.7.4 Server Gateway with Resiliency

The following flowchart represents the work flow of Server Gateway with Resiliency Deployment:

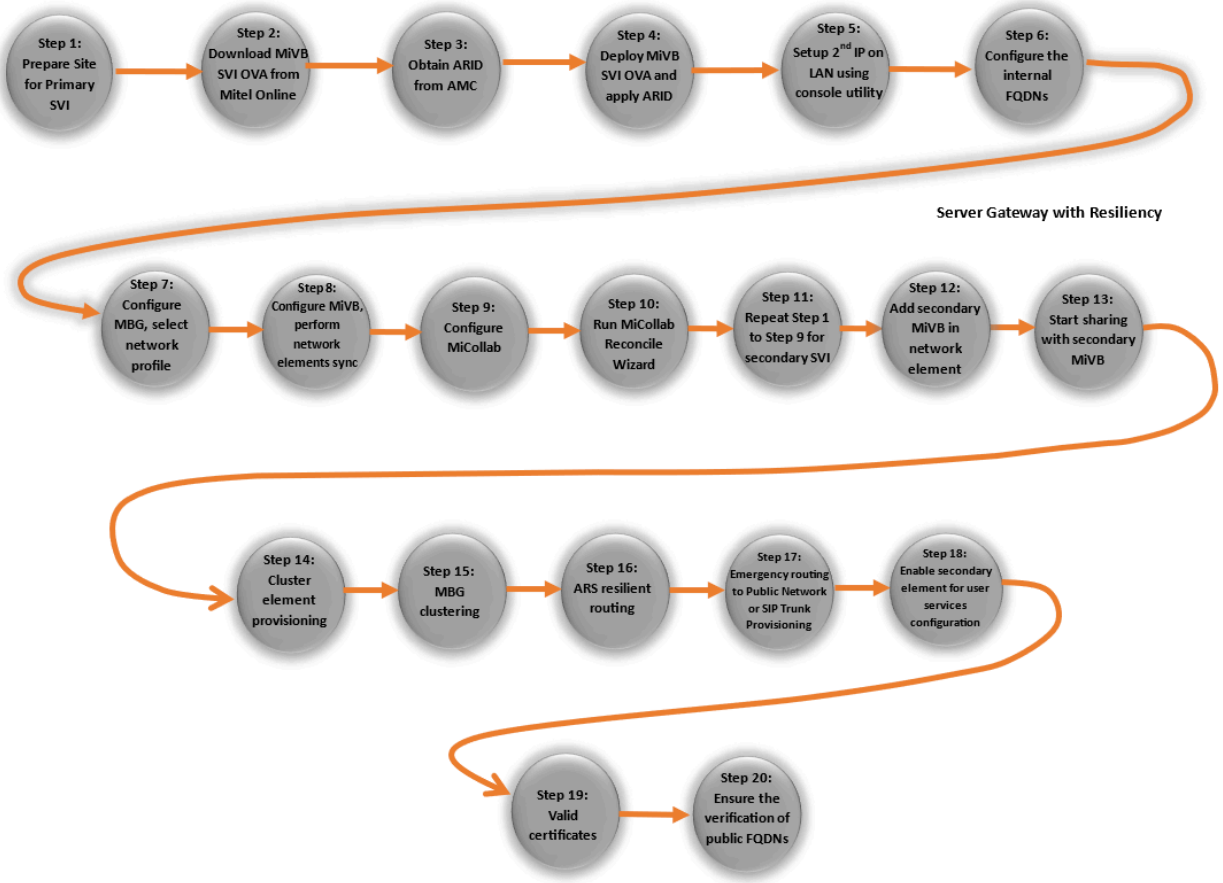


Figure 8: Server Gateway with Resiliency

Note:

- Clustering with a 2nd SVI server is supported for resiliency.
- Clustering with other MiVoice Business products is not supported.

- Firewall is recommended in front of WAN interfaces.
- The WAN IPs can be public IPs or private IPs in public DMZ subnets, depending on firewall configuration.
  - Co-resident MBG network profile can be used if public IPs assigned to WAN interfaces.
  - Custom MBG network profile must be used if private IPs assigned to WAN interfaces.
    - ICP-side bind interface is LAN interface, RTP ICP-side override address is LAN 1 IP 2.
    - Set-side bind interface is WAN interface, RTP Set-side override address is Public IP.
- Deployment shown in the figure below is two separate data centers. Separate subnets in a LAN is also possible.
- Secondary MiVoice Business Solution VIrtual Instance server should be deployed on separate infrastructure and subnet.
- MiCollab is not resilient. The MiCollab in the secondary MiVoice Business Solution Virtual Instance server is not used.
- Teleworker sets and MiCollab client soft phones must be configured to connect to main server FQDN.
  - DNS service records must be provisioned for both primary & secondary main server FQDNs.
- MiCollab client must be configured to connect to MiCollab public FQDN.
- MBG internal private FQDNs must be programmed as SIP Trunking Proxy in MiVoice Business network element forms.
- MBG internal private FQDNs must be programmed in MIR for connecting to MBG.

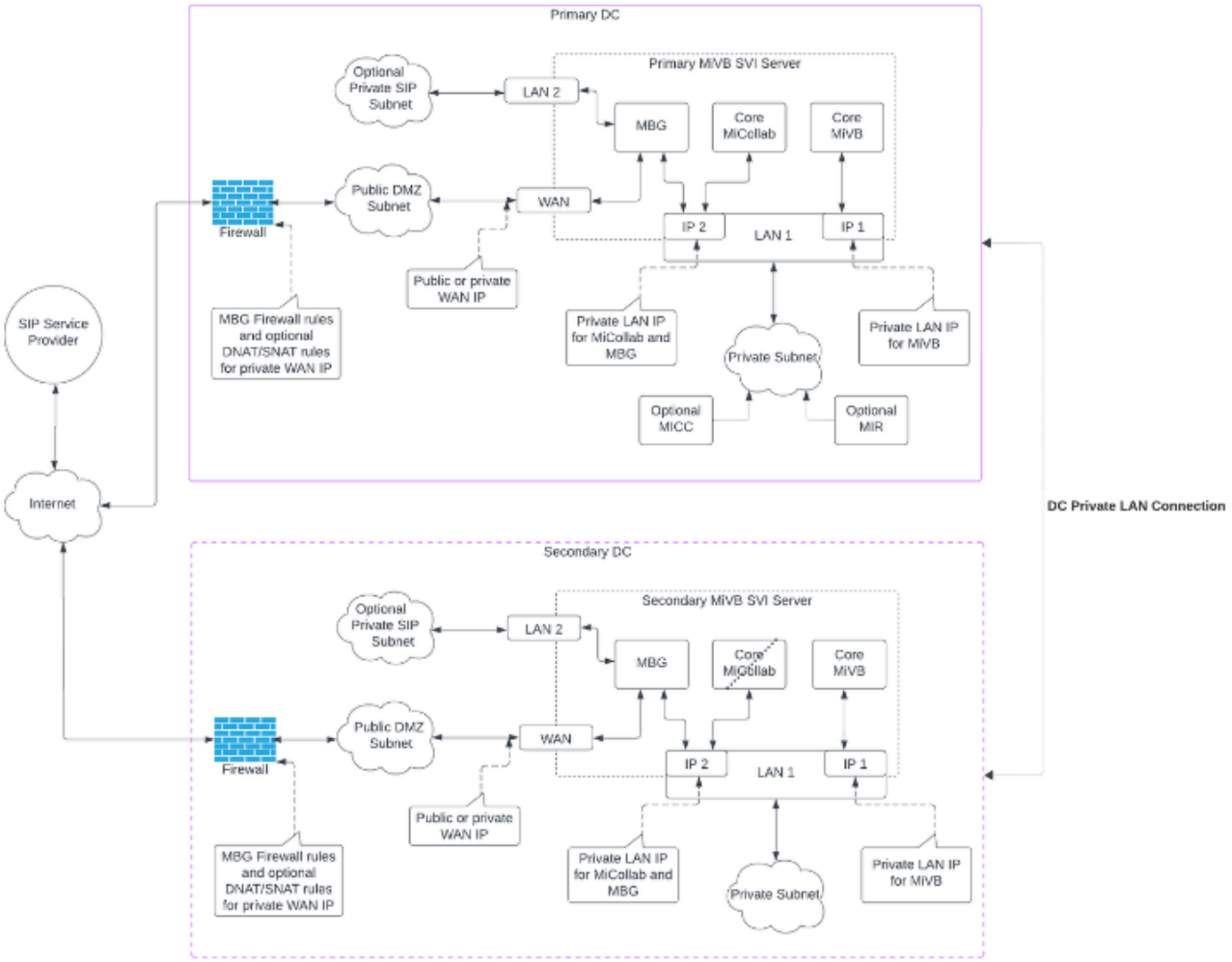


Figure 9:

Table 9: Public FQDNs

FQDN	Public WAN IP	Purpose
mivbsvi1.example.com	1.2.3.4	Primary MiVoice Business Solution Virtual Instance server FQDN for Teleworker phone, SIP, and MiCollab profile
mivb-mgmt1.example.com	1.2.3.4	Primary MiVoice Business Solution Virtual Instance server FQDN for access to MiVoice Business Embedded System Management (ESM)

FQDN	Public WAN IP	Purpose
mivb1.example.com	1.2.3.4	Primary MiVoice Business public FQDN for Embedded Voicemail
micollab.example.com	1.2.3.4	MiCollab public FQDN for MiCollab Applications
micc.example.com	1.2.3.4	Optional MICC public FQDN
mir.example.com	1.2.3.4	Optional MIR public FQDN
mivbsvi2.example.com	5.6.7.8	Secondary MiVoice Business Solution Virtual Instance server FQDN for Teleworker phone, SIP, and MiCollab profile
mivb-mgmt2.example.com	5.6.7.8	Secondary MiVoice Business Solution Virtual Instance server FQDN for access to MiVoice Business Embedded System Management (ESM)
mivb2.example.com	5.6.7.8	Secondary MiVoice Business public FQDN for Embedded Voicemail

Table 10: DNS Service Records

DNS SRV Record	Priority	Associated FQDNs
_sip._tcp.mivbsvi.example.com	1	mivbsvi1.example.com
	2	mivbsvi2.example.com
_sips._tcp.mivbsvi.example.com	1	mivbsvi1.example.com

DNS SRV Record	Priority	Associated FQDNs
	2	mivbsvi2.example.com
_sip._udp.mivbsvi.example.com	1	mivbsvi1.example.com
	2	mivbsvi2.example.com

Table 11: Primary DC Private FQDNs

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
mivbsvi1.example.com	10.0.50.4			Primary MiVoice Business Solution Virtual Instance server FQDN
mivb-mgmt1.example.com	10.0.50.4			Primary MiVoice Business private FQDN for MiVoice Business Embedded System Management (ESM)
mivb1.example.com	10.0.50.4			Primary MiVoice Business private FQDN for Embedded Voice Email, SIP devices, and Other.
mivb2.example.com	10.0.51.4			Secondary MiVoice Business private FQDN for Embedded Voice Email, SIP devices, and Other.

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
micollab.example.com		10.0.50.5		MiCollab private FQDN
mbg-int1.example.com		10.0.50.5		Primary MBG's internal private FQDN for MIR, SIP Trunking Proxy
mbg-int2.example.com		10.0.51.5		Secondary MBG's internal private FQDN for MIR, SIP Trunking Proxy
micc.example.com			10.0.50.6	Optional MICC private FQDN
mir.example.com			10.0.50.7	Optional MIR private FQDN

Table 12: Secondary DC Private FQDNs

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
mivbsvi2.example.com	10.0.51.4			Secondary MiVoice Business Solution Virtual Instance server FQDN
mivb-mgmt2.example.com	10.0.51.4			Secondary MiVoice Business private FQDN for MiVoice Business Embedded System Management (ESM)

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
mivb2.example.com	10.0.51.4			Secondary MiVoice Business private FQDN for Embedded Voice Email, SIP devices, and Other.
mivb1.example.com	10.0.50.4			Primary MiVoice Business private FQDN for Embedded Voice Email, SIP devices, and Other.
mbg-int2.example.com		10.0.51.5		Secondary MBG's internal private FQDN for MIR, SIP Trunking Proxy
mbg-int1.example.com		10.0.50.5		Primary MBG's internal private FQDN for MIR, SIP Trunking Proxy

2.7.5 IAAS Deployment

The figure shows the MiVoice Business Solution Virtual Instance and VMware components in a typical IaaS deployment. In this deployment model:

- MiVoice Business Solution Virtual Instance as a single virtual appliance that provides MiVoice Business, MiCollab, and MBG functionality. The MBG component of each MiVoice Business Solution Virtual Instance provides a SIP proxy to the SIP Service provider.
- The service provider maintains the infrastructure and a channel partner deploys and maintains the MiVoice Business Solution Virtual Instance. The channel partner may, or may not, have access to the hosted infrastructure.
- Two distinct network connectivity models are supported from the end-customer premise to the hosted UCaaS infrastructure:
  - MPLS Connected End Customer(s): MiVoice Business Solution Virtual Instance connected to a remote office using an MPLS router.
  - Public Internet Connected End Customer(s): standalone MiVoice Business Solution Virtual Instance servicing Teleworker phones in one or multiple remote offices.

- For IaaS deployments where end customers are connected via a MLPS router, MiCollab mobile clients can be used in the remote office because they route to the Internet via a separate router (not the MPLS router).

2.7.6 CPE Deployment

The figure *Customer Premise Equipment Deployment* shows the MiVoice Business Solution Virtual Instance and VMware components in a typical Customer Premise Equipment (CPE) deployment. In this deployment model:

- MiVoice Business Solution Virtual Instance is deployed as a single virtual appliance that provides MiVoice Business, MiCollab, and MBG functionality.
- The MiVoice Business Solution Virtual Instance vApp MBG application provides SIP trunking support. A separate, optional external standalone vMGB can be added for SIP trunking.
- Customers use the MiVoice Business Solution Virtual Instance solution and can perform user provisioning through the administration tools (MiCollab server manager and USP application).
- To support mobile clients users on the WAN and on the customer premise, MiVoice Business Solution Virtual Instance must be deployed in the DMZ using a 3-port firewall as shown in the following figure. The mobile client user always connects to the system as a Teleworker.

Note:
Mobile clients are NOT supported on the customer premise if the MiVoice Business Solution Virtual Instance is deployed behind a 2-port firewall. If a call is placed from the MiCollab mobile client on the customer premise and routed through a 2-port firewall, a network loop is detected and packets are dropped.

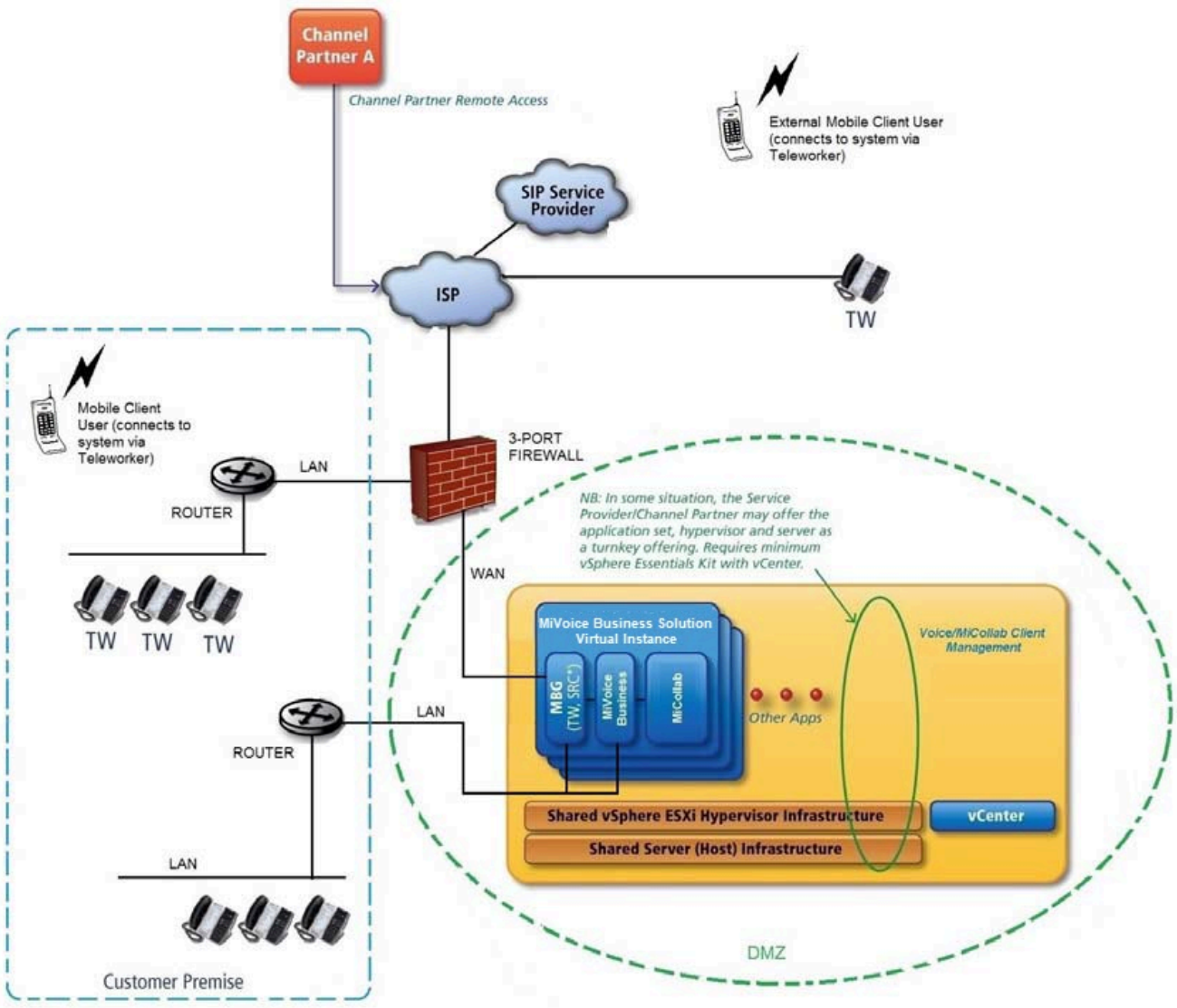


Figure 10: Customer Premise Equipment Deployment

2.8 Supported Functionality

Overview

MiVoice Business Solution Virtual Instance supports the following:

- Applications Suite Management
  - Central point of management for applications
  - User and services provisioning
  - Active Directory integration
  - Remote access

- MiVoice Business Voice over IP telephony platform, including
  - IP Phone features
  - SIP trunking
  - Automatic Call Distribution (ACD) and ACD Express
  - Embedded Voice Email
- MiCollab Client
  - MiCollab Client support (PC, Web, and mobile)
  - Collaboration features
- MiVoice Border Gateway, providing
  - Teleworker Service
  - Secure Recording Connector (for remote Teleworkers only)
  - SIP Trunking Proxy

Note:
Web Real-Time Communication (WebRTC) is an API definition drafted by the World Wide Web Consortium (W3C) that provides browsers and mobile applications with Real-Time Communications (RTC) capabilities. MBG supports WebRTC for browser-based voice and video calling without the need of plug-ins using Google Chrome, Mozilla Firefox and Opera on all platforms except iOS. WebRTC is NOT supported for MiVoice Business Release 7.1

Remove this note and add a reference to MBG Engineering Guidelines

.

Note:
Speech applications are not supported (Text to Speech, Speech to Text, Speech Navigation, or Network Voicemail).

2.8.1 MiCollab

The MiCollab administration interface allows administrators to configure system settings for all the applications. Common data elements are shared among the applications, reducing both the need for duplicate entry and the possibility of an error.

The administrator uses the Users and Services Provisioning application to add, edit, or delete user data and to modify users' application settings. This application significantly reduces administration costs.

2.8.1.1 MiCollab Client

This application provides a single access point for business communication and collaboration needs. It converges the call control capabilities of the MiVoice Business platform with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications. It gives users control over their communications and allows real-time access to everyone in the organization, on or off the premises, with user and phone presence information.

2.8.1.2 MiCollab Client Deployment

This MiCollab software application supports the simplified deployment of MiCollab Client for Mobile clients. This functionality is supported in integrated MiCollab Client deployments. The administrator uses this application to

- Provision MiCollab FQDN in **MiCollab Client Deployment** > **Configuration**. In **Configuration** tab, select **System**. Enter **Override MiCollab (UCA) host name**.

- deploy large groups of users
- leverage user profiles
- download multiple files to the clients
- update clients.

Refer to the MiCollab Client Deployment help.

2.8.2 MiVoice Business

Note:

- Clustering with a 2nd SVI server is supported for resiliency.
- Clustering with other MiVoice Business products is not supported.

MiVoice Business is a feature-rich communications system that provides IP-PBX capability plus a range of embedded applications, such as auto-attendant, hot desking, multimedia collaboration, and unified messaging. It provides seamless IP networking and SIP trunking.

MiVoice Business software has over 500 telephony features – features that are provided to users through easy-to-use phones and web-based user desktop interfaces. It also supports a wide-range of desktop devices, including entry-level IP phones, web-enabled IP devices, wireless handsets (WiFi or IP DECT), and full-duplex IP audio conference units.

2.8.3 CloudLink Gateway

CloudLink Gateway is a technology that connects MiVoice Business Solution Virtual Instance to the CloudLink platform and CloudLink applications.

For more information on CloudLink Gateway, refer CloudLink Gateway.

2.8.4 Mitel Performance Analytics

Provides instructions for installing a new Mitel Performance Analytics (MPA) is an optional blade that provides integration with Mitel Performance Analytics Cloud Service to provide users with realtime alerts, detailed reporting and ubiquitous accessibility with secure remote access.

(Optional) Mitel Performance Analytics (MPA) provides monitoring system as well as its operations.

For more information on MPA, refer Mitel Performance Analytics.

2.8.5 MiVoice Border Gateway

The MiVoice Border Gateway (MBG) is a multi-service software solution that provides the following functionality:

- Teleworker service
- Web proxy blade that provides a secure method for MiCollab Client end-user web clients to connect with their LAN-based applications
- Secure remote SIP access for IP phones on the MiVoice Business and an outbound proxy for SIP trunking from internal MiVoice Businesses to external third-party SIP providers
- Secure Recording Connector service to facilitate the recording of Mitel-encrypted voice streams by third-party call recording equipment
- Supports Web Real-Time Communication (WebRTC)

Plan Customer Site 3

This chapter contains the following sections:

3.1 Record Licensing Requirements

About Licensing

When you deploy MiVoice Business Solution Virtual Instance, the system must be connected to the internet in order to license the product. Internet connectivity must be maintained to support the system licensing.

- Simplifies the licensing of a MiVoice Business Solution Virtual Instance user by bundling the required MiCollab, MBG (for example: SIP, Teleworker, and SRC), and MiVoice Business user licenses with a specific set of application user licenses.
- Offers a significant pricing discount over "à la carte" licenses.
- Provides tiered functionality with progressive discounts. The following UCC user licenses are available:
  - **UCC Entry**: provides the Entry MiCollab Client, voicemail, unified messaging, and the required call manager platform licenses.
  - **UCC Standard**: adds full mobile and softphone UCC functionality with two additional teleworker accesses to the Standard license.
- Software assurance:The Mitel Software Assurance (SWAS) Program is a subscription-based service that provides customers with access to new software releases, software upgrades, and product support services for all users (ports) on a given application record. Under the SWAS program, software upgrades are provided at no additional cost without any of the new features or functionality that are available in the base upgrade package

3.1.1 Licensing Rules

The following rules apply to UCC Licensing:

- UCC v4.0 licensing is supported with MiVoice Business Solution Virtual Instance.
- You require a UCC License Manager (ULM) to create a UCC Group ARID on the AMC.
- You cannot split the UCC license bundle and deploy the application licenses across different users within a system.
- If you downgrade the UCC license bundle of an existing user (for example, from Entry to Basic, from Standard to Entry, or from Premium to Standard) MiCollab will not delete any of the services. Instead, MiCollab attempts to apply any available "à la carte" licenses to support the extra services. If "à la carte" licenses are not available, then a license violation is generated.
- If you have different types of upgrade licenses (for example, "Basic to Entry", "Entry to Standard", and "Standard to Premium") available on the system, apply the highest upgrade licenses first. For

example, upgrade the Entry users to Standard licenses first, before you upgrade the Basic users to Entry licenses.

- If new UCC licensing bundles are available, the AMC automatically converts the existing bundles to the latest version and passes the new bundles down to the server. The server updates the users' license bundles with the new entitlements. Note that you still need to configure the users with any new services that are provided in the updated bundles. The roles and templates associated with the previous UCC license bundle are not deleted from the system, but are changed to non-default and you can delete them if they are not required.
- If you are configuring a **Public Internet Connected End Customer** deployment where the customers are internet connected, the following conditions apply:
  - All users are connected to the MiVoice Business Solution Virtual Instance system through the internet (even desk phones are routed through an MBG).
  - Users hot desk between their home phone and their work phone.
  - Users are all assigned Standard UCC User Licenses and have been created with the corresponding default UCC User Template.
  - Users have their desk phone and a soft phone in a MDUG or PRG (Personal Ring Group). Both phones ring simultaneously for an incoming call.
  - In addition to the teleworker license provided in the Standard UCC User license, each user requires a second teleworker license.Two teleworker user licenses are required to allow both of the user's phones to be registered with teleworker service (so that they both ring simultaneously on an incoming call).

Additionally, for UCaaS deployments:

- You can choose to license the MiVoice Business Solution Virtual Instance software bundle and user licenses on a subscription basis from Mitel.
- MiVoice Business License Manager is not supported for MiVoice Business Solution Virtual Instance.

3.1.2 Licensing Detection and Violation Mode

MiVoice Business Solution Virtual Instance appliances must maintain online connectivity to the AMC at all times. Loss of AMC connectivity for a short period of time is tolerated by the system. However, AMC connectivity must be re-established without delay in order to maintain access to all system functions and features. If AMC connectivity is lost for an extended period of time, an automatic alert is generated and sent to the Channel Partner AMC account administrator email address that is programmed in the AMC for the account. If AMC connectivity is not re-established, then the virtual appliance system goes into license violation mode and certain capabilities are no longer be accessible.

Mitel recognizes that in some deployment situations, it is not practical to implement online connectivity to the AMC from each virtual appliance deployed at a customer’s site. For this reason, Mitel supports the ability to proxy online AMC connectivity from each virtual appliance through a single named proxy within the customer data center environment. This enables AMC online connections to be managed and controlled from one central point within the data center rather than from each individual product.

3.1.3 Record Licensing Requirements

If SIP provisioning is required, then you need two MiVoice Business and two MBG SIP trunk licenses if using internal MBG SIP trunking.

There are several tiers of UCC User licensing. Refer to the MiCollab Ordering Guide for details.

Enter the licensing requirements for the site in the following table:

Licenses	Part Number	Details
MiVoice Business Solution Virtual Instance Software Base Packages for traditional customer premise or IaaS licensing		
Perpetual license		
MiVoice Business Solution Virtual Instance bundle	54012174	Includes base packs for MiVoice Business, MiVoice Border Gateway, and MiCollab, 30 SIP trunks, 30 MBG compression licenses, 30 SRC licenses, and 20 embedded mailboxes.
Single Line License	54002701	
MiVoice Business License - Enterprise User	54004975	
UCCv4.0 Entry User x1	54006539	UCC licenses must be added to ULM ARID
UCCv4.0 Standard User x1	54006542	UCC licenses must be added to ULM ARID
UCCv4.0 Basic to v4.0 Entry	54006553	UCC licenses must be added to ULM ARID
UCCv4.0 Entry to v4.0 Standard	54006548	UCC licenses must be added to ULM ARID
UCCv4.0 Basic to v4.0 Standard	54006704	UCC licenses must be added to ULM ARID
SWA Adv 1y MiVoice Business Solution Virtual Instance Bundle	54012161	

Licenses	Part Number	Details
SWA Adv 2y MiVoice Business Solution Virtual Instance Bundle	54012162	
SWA Adv 3y MiVoice Business Solution Virtual Instance Bundle	54012163	
SWA Adv 4y MiVoice Business Solution Virtual Instance Bundle	54012164	
SWA Adv 5y MiVoice Business Solution Virtual Instance Bundle	54012165	
SWA Prem 1y MiVoice Business Solution Virtual Instance Bundle	54012166	
SWA Prem 2y MiVoice Business Solution Virtual Instance Bundle	54012167	
SWA Prem 3y MiVoice Business Solution Virtual Instance Bundle	54012168	
SWA Prem 4y MiVoice Business Solution Virtual Instance Bundle	54012169	
SWA Prem 5y MiVoice Business Solution Virtual Instance Bundle	54012170	
SWA Reenl MiVoice Business Solution Virtual Instance Bundle	54012173	
SWA Adv-Prem MiVoice Business Solution Virtual Instance Bundle	54012172	
SWA Adv OLD MiVoice Business Solution Virtual Instance Bundle	54012171	

Licenses	Part Number	Details
Subscription activation license		
SP Subs Base-MiVB Solution Virt Instance	54012175	Includes base packs for MiVoice Business, MiVoice Border Gateway, and MiCollab, 275 SIP trunks, 40 MBG compression licenses, 275 SRC licenses, and 20 embedded mailboxes.
User Licenses		
• Single Line extension • Basic IPT Users v2 • Entry UCC Users v2 • Standard UCC Users v2 • Standard Plus UCC Users v2	Refer to CPQ for Billing and Activation Part Numbers	

Note:

1. Premium SWAS must be applied as an upgrade to Standard SWAS.
2. MiVoice Business Solution Virtual Instance also supports "à la carte" licensing.
3. The system does not restrict you from applying an ARID with a MiVoice Business Solution Virtual Instance Bundle (PN 54012174) to a system that has been deployed as a small business configuration. However, these part numbers are meant for mid-market business configurations and your virtual machine will consume the virtual resources required for a mid-market deployment.

3.2 Review Engineering Guidelines

Review the MiVoice Business Solution Virtual Instance site requirements details in the table below. Also review the Virtual Appliance Deployment Guide. It provides guidelines for deploying Mitel Virtual Appliances and applications in a virtual infrastructure.

Table 13: MiVoice Business Solution Virtual Instance system size

Virtual Appliance	Release	System Capacity	Configuration		Resource Reservation	
			vCPU	Disk	CPU	Memory
MiVoice Business Solution Virtual Instance	1.0	250	4	100	4 GHz	10 GB
		500	6	180	6 GHz	12 GB
ESXi	8.0, 7.0, 6.7		1		2 GHz	2.0 GB

3.3 Collect Site Configuration Data

Before you begin deployment, login using credentials, collect and record the data specified in the following table. You need this information in order to successfully deploy MiVoice Business Solution Virtual Instance.

Note:

To create a blank template for cloning, leave the following fields empty: Administrator Password, Hostname, Domain Name, LAN and WAN IP addresses. Before you power up the clone, **Edit Settings** on the VM, complete these fields, and then proceed with deployment. You cannot clone an active (deployed) MiVoice Business Solution Virtual Instance.

Table 14: Collect Custom OVA Template Information

Configuration Items	Field Description	Site Configuration Data
Administration		

Configuration Items	Field Description	Site Configuration Data
Restore from backup	Check this box to restore the VM from an existing backup via the server console. Note that you still need to assign valid values to the fields in the Properties page.	**Note**: If the backup file is encrypted, you will need the password that was assigned to the file to proceed. The filename for an encrypted backup ends with ".aes256".
Application		
Initial Administrator Password	Record the initial administrator password for the MiCollab server manager interface. This password must be at least six characters long. After you access the MiCollab server manager, you will be prompted to change this initial password. **Note**: You must enter a password before you deploy the MiVoice Business Solution Virtual Instances; otherwise, the system will not boot up.	**Note**: It is recommended that you use a strong password that contains all of the following: upper case letter, lower case letter, number, non-alphanumeric character, and be at least seven characters long. Do not use a commonly used word (for example: 'password').
Hostname	Set the hostname of the MiVoice Business Solution Virtual Instance.	
Domain Name (Optional)	Specify the domain name for the hostname above. The default domain name is "mycompany.local".	

Configuration Items	Field Description	Site Configuration Data
License Key (Optional)	Identify the License Key (MiVoice Business Solution Virtual Instance Business Base ARID) for this system. The ARID is used by the AMC to distribute the system licenses. See Create ARIDs and Assign Licenses in AMC for instructions. This key can be provisioned later also once the system is deployed.	
DNS Server IP (Optional)	Existing DNS Server IP Address	
Remote Network Addresses (Optional)	List the Network IP address that is allowed to access the MiCollab server and perform remote administration. **Note**: You can only configure one IP address or subnet as the Remote Network Address during OVA deployment. Any additional Remote Network addresses must be configured from the Remote Access panel in the server manager	
Remote Network Netmask (Optional)	Enter the Netmask associated with the remote network address.	This netmask field corresponds to the Remote Network Address specified in the Remote Network Addresses.
Localization		

Configuration Items	Field Description	Site Configuration Data
Timezone setting	Identify the MSL operating system time zone setting. The default is America/New York. The Time zone setting also determines your system telecom regional settings.	**Note**: If you select a Time zone that is not within one of Countries supported by the system, the Country value is set to "Other" and the Telecom Region is defaulted to North America
Keyboard	Identify the preferred keyboard type (default is US)	
Network Settings		
LAN IP Address	Record the IP address of the local (LAN) interface. This must be a valid IP address on the local LAN. You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance.	You must enter a LAN IP add ress before you deploy the MiVoice Business Solution Virtual Instance; o therwise, the system will not boot u p.
LAN Netmask	Record the Netmask of the LAN	This netmask corresponds to the LAN IP address configured above.

Configuration Items	Field Description	Site Configuration Data
WAN IP Address (Optional)	For Network Edge (Server-gateway) deployments, record the IP address of the external (WAN) interface. This must be a valid IP address on external WAN. For LAN only (Server-only) deployments, use an IP address of 0.0.0.0. **Note**: You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this address from Hyper-V Client. Right click on the MiVoice Business Solution Virtual Instance and click **Edit Settings**. Click the **Options** tab, click **Properties** and enter the WAN IP Address.	**Note**: Ensure that the LAN and WAN IP addresses are assigned to different networks
WAN Netmask (Optional)	Record the Netmask of the WAN.	This netmask corresponds to the WAN IP address configured above
Optional LAN IP Address	Record the IP Address for this additional optional network interface. This interface can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.	
Optional LAN Netmask	Record the Netmask of the optional LAN	

Configuration Items	Field Description	Site Configuration Data
Default Gateway IP Address	Record the Gateway IP address. For Server-gateway mode of deployment, this gateway typically points to an Internet gateway. For Server-only deployments, this gateway typically points to a LAN router	**Note**: You must enter a Default Gateway IP address before you deploy the MiVoice Business Solution Virtual Instance; otherwise, the system will not boot up.
Next Steps		
Provision 2nd IP address on default LAN	Provision 2nd IP address for default LAN using console utility before configuring any other aspects of the system. Checking this option does not affect the system behavior.	**Note**: This is a warning to the user to configure the 2nd LAN IP address.

Table 15: Collect Advanced Deployment Properties

Configuration Items	Field Description	Site Configuration Data
Mitel Application Management Center (AMC)	Record IP address or proxy address for the AMC.	
MiCollab/MBG IP address	Record the IP address of the local (LAN) interface for MiCollab/MBG. This must be a valid IP address on the local LAN interface.	

Table 16: Collect MiVoice Business Solution Virtual Instance Initial Provisioning Data

Configuration Items	Field Description	Site Configuration Data
Configuration Options		
New configuration OR Restore database from an existing configuration (upgrade only)	If upgrade, record the location of the MiVoice Business Solution Virtual Instance database file.	
E-mail and Servers		
Administrator Email Address	Record the email address of the system administrator.	
Primary DNS IP Address	Specify the IP address of the SMTP Server.	
Secondary DNS IP Address	Specify the IP address of the DNS IP Address.	
SMTP Mail Server	Record the host name of the SMTP Mail server	
Network Time Server Source	Identify the Network Time Server Source for the system (for example: centos.pool.ntp.org).	
Numbering Plan		
Extension Length	Specify the required extension length (3 to 5 digit extension numbering)	
Voice Mail Hunt Group Ext	Default is 7000	

Configuration Items	Field Description	Site Configuration Data
Voice Mail Starting Port Ext	Default is 7001 (up to 7007)	
Voice Mail HCI Hunt Group Extension	Default is 7400	
Voice Mail Record A Call Hunt Group Extension	Default is 7500	
Incoming Calls		
Main Business Number	Enter the phone number of the site. External callers dial this number to place incoming calls on the SIP trunks.	
OR		
Incoming Call Handling Extension	Specify the answer point extension number.	
Auto Receptionist Hunt Group Extension	Specify the extension number.	
Advanced Incoming Call Configuration		
Number of Digits to Absorb		
Digits to Insert		
SIP Provider		

Configuration Items	Field Description	Site Configuration Data
SIP Provider	Identify your SIP Service Provider. **Note**: The wizard lists the most common Service Providers for your region for selection. A "Generic" SIP peer profile is also available. If required, you can specify a "Custom Profile" and import a CSV file saved from the SIP Peer Profile form in the MiVoice Business System Administration Tool (see Obtain a Custom SIP Peer Profile (optional) for instructions)	SIP Server Provider Name or Generic profile or Custom profile
Number of MiVoice Business SIP Trunk Licenses	Record the number of required MiVoice Business SIP trunk licenses. See the Engineering Guidelines for capacities.	
Number of MBG SIP Trunk Channel Licenses	Record the number of licenses required. **Note**: If using internal SIP trunking, you need to configure the MiVoice Business Solution Virtual Instance ULM with at least two MBG SIP Trunk Channel licenses in order to successfully complete the Initial Configuration Wizard.	

Configuration Items	Field Description	Site Configuration Data
Numbers to Register/Accept (optional)	Identify the range of SIP telephone numbers that you want to register with the SIP Provider.	You can specify a mix of single numbers and number ranges (for example, 6135554500, 6135554000-6135554400).
External Session Border Controller (optional)	Identify the IP address of the SIP Provider's External Session Controller (This server is non-Mitel equipment -- not to be confused with the MiVoice Border Gateway proxy server).	
Call Billing Phone Number	Record the desired call billing number for system Network Zone 1 (default).	
SIP Authentication	Does your SIP Service Provider require authentication?	
SIP Authentication	Record the username and password for your SIP Service account. Obtain these credentials from your SIP Service Provider.	
User Name		
Password		
SIP Provider Advanced Provisioning		
Subscription User Name	Record the optional user name and password for the telephony server to subscribe to the SIP Peer that is performing KPML digit detection.	
Subscription Password		
SIP Provider Proxy		

Configuration Items	Field Description	Site Configuration Data
MiVoice Border Gateway SIP Trunk Proxy	Select **Internal** if the SIP trunk proxy is supported on the MiVoice Business Solution Virtual Instance system. Select **External** if the SIP trunk proxy is supported on a separate optional MiVoice Border Gateway (MBG). Refer to the *MiVoice Business Solution Virtual Instance* Engineering Guidelines for configuration diagrams of the supported SIP Trunk Proxy options.	Internal External No SIP Trunk Proxy
MiVoice Border Gateway SIP Trunk Proxy Server Address	If you are using an external SIP trunk proxy, record the SIP trunk proxy server address.	
Local Network Details	Will SIP Service Provider be located on a different local network? If Yes, record the IP addresses.	Yes
Local Network Address		
Local Netmask		
Local Network Router Address		
Optional Services		
Optional Services	Identify the required optional services	• Hot Desking • Music on Hold • Remote Access

Configuration Items	Field Description	Site Configuration Data
Hot desking: allows a number of users to share one or more phones. Hot desking is ideal for telecommuters, sales agents, and other employees who spend only part of their time in the office. With hot desking, a company does not have to provide a dedicated phone for each of these employees. Instead, the company can make a pool of shared phones available on a first-come, first-served basis. A hot desk user can log into any available hot desk-enabled phone on the system. After a user logs into a hot desk phone, the system applies the user's profile to the phone and it functions as the user's desk phone.		
Hot desk users	Record the number of phones that you want to support hot desking.	
	Enter the starting extension number of the range of numbers that the system will assign to the hot desk enabled phones. Hot desk enabled phones are typically assigned non-standard extension numbers (for example 1*01)	
Music on Hold: provides callers with music or information while they are waiting for a call to be completed. It's played whenever a call is on Hold, transferred to a busy or ringing station, or camped-on to a station. The customer site must provide the music or information source file.		
Configure remote access to MiCollab Server Manager interface	Network Address Network Prefix	
Music on Hold File	Identify the file name and location of the music source file. Refer to the *MiVoice Business Solution Virtual Instance Engineering Guidelines* for file requirements.	
Remote Access: allows you to configure remote access to the MiCollab server manager interface and the MiVoice Business telephony server administration tools.		

Configuration Items	Field Description	Site Configuration Data
Configure up to five dealers or administrators with remote access from the Internet (WAN) to the MiVoice Business System Administration tool.	Username Password First name Last name Email address	
Telephony Server Management Web Interface FQDN	Record the FQDN	
MiCollab		
Active Directory Integration (optional)	Record the Active Directory Server IP address.	

3.3.1 Obtain a Custom SIP Peer Profile (optional)

If required, you can save a custom SIP Peer Profile CSV file from an existing MiVoice Business system database and import it into the MiVoice Business Solution Virtual Instance system from the Initial Configuration Wizard.

1. Log into the MiVoice Business System Administration tool. See Logging into the MiVoice Business Tools.
2. Choose to view forms alphabetically.
3. In the left forms menu, select **SIP Peer Profile**.
4. Select the label of the desired SIP Peer Profile. The wizard only supports the import of a single SIP Peer Profile.
5. Click **Export**.
6. Select Export Range: All and File Type: Comma Delimited (Spreadsheet).
7. Click **Export** and then click **OK** to download.
8. Save the CSV file to a network drive. During the Initial Configuration Wizard, you can import this custom SIP Peer Profile into the MiVoice Business Solution Virtual Instance.

Prepare Site 4

This chapter contains the following sections:

4.1 Set Up Active Directory Server (Optional)

If required, set up the Active Directory server prior to deploying the MiVoice Business Solution Virtual Instance. Ensure that you have recorded the Active Directory Server IP address.

4.2 Create ARIDs and Assign Licenses in AMC

Create Application Record Identifications (ARIDs) for MiVoice Business Solution Virtual Instance installation in your AMC license account and assign the required licenses to them. When you deploy the MiVoice Business Solution Virtual Instance, you will use the software base Application Record ID to activate the system and user licenses.

For Managed Service Providers: For Service Providers who have subscribed to Mitel's Managed Service Provider program, refer to the "MiCloud for Service Provider Licensing Structures" document available under the Managed Service Provider Program. This document provides additional information regarding licensing and AMC interaction for Service Providers.

For information on AMC, refer to AMC Manager User Manual

4.2.1 About the Mitel Application Management Center (AMC)

Mitel Application Management Center Licensing is supported through the Mitel Application Management Center (AMC). The Mitel AMC manages the software licensing and entitlement of the Software Assurance Program. After you obtain an Application Record ID (ARID) from the AMC, the AMC uses your Application Record ID (ARID) to provide you with access to licenses, software releases, and upgrades.

The Mitel Software Assurance (SWAS) Program is a subscription-based service that provides customers with access to new software releases, software upgrades, and product support services for all users (ports) on a given application record.

When you place a new order for products through the Mitel Online Store, the order information is entered into the AMC system. The AMC places the purchased licenses into your licensing account. You assign the licenses to one or more product application records.

When you install MiVoice Business Solution Virtual Instance, it generates a unique Hardware ID that includes the MAC address of the server. When you connect to the AMC over the internet, the Hardware ID and the Application Record ID are synchronized with the AMC to obtain the licensing information.

4.2.1.1 Requesting a New AMC Account

To request an AMC account, send an e-mail containing the following information to amc_accounts@mitel.com:

- Name of your certified Technician
- Full company name
- Company mailing address
- Phone 1/Phone 2
- Fax number
- Admin e-mail (address of the person who should receive notification of service expiry dates)
- Tech e-mail (address of the person who should receive notification of upgrade releases and other technical notices)
- Company URL (if any)
- Your Mitel SAP account number
- Specify if you would like your user ID and password delivered to you by fax, phone, or both (for security reasons user IDs and passwords are not sent by e-mail).

Note:
Please allow two business days for your AMC account to be created.

4.2.1.2 Accessing your AMC Account

To access your account for the first time:

1. Go to the Mitel web site (https://www.mitel.com) and log in to your Mitel OnLine account.
2. Point to **Purchasing**. Under **Licensing**, click **AMC**.
3. Click **Go** to the **Applications Management Center (AMC)**.
4. Sign in with your unique AMC username and password. On subsequent visits, you access your AMC account directly after signing in to Mitel OnLine.
5. For information about using the AMC, click the online Help link in your AMC account.

4.3 UCC Licensing Procedure

The Application Management Center distributes the platform and application user licenses that are contained within a UCC license bundle to the members of a Unified Licensing Manager (ULM) group. During the licensing process, you create a ULM group ARID for the MiVoice Business Solution Virtual Instance deployment.

Note:
If SIP provisioning is required then you need two MiVoice Business and two MBG SIP trunk licenses if using internal MBG SIP trunking.

4.3.1 Overview

The following is an overview of the main steps required to deploy UCC licenses:

- Authorized Partner creates customer account.
- Authorized Partner registers (purchases) and assigns UCC licenses on AMC.
- Authorized Partner creates an Application Record ID for the MiVoice Business Solution Virtual Instances base software.
- Authorized Partner assigns the MiVoice Business Solution Virtual Instance base software license to the MiVoice Business Solution Virtual Instance Base ARID
- Authorized Partner creates an associated ULM ARID for the MiVoice Business Solution Virtual Instance base ARID.
- Authorized Partner assigns MiVoice Business SIP trunk licenses, MBG SIP trunk licenses, UCC User and SWAS licenses to the ULM ARID.
- If the site requires a standalone vMBG for SIP trunking, the Authorized Partner purchases the vMBG base under the same customer and applies it to the vMBG ARID. The Authorized Partner then selects it and adds the vMBG ARID to the ULM group ("Business" for CPE and IaaS sites; "Enterprise" for UCaaS deployments).
- Installer deploys MiVoice Business Solution Virtual Instance. During deployment, the licenses are automatically downloaded from the AMC to the system.

4.3.2 Deploying UCC Licenses

A detailed procedure for deploying UCC licenses follows:

1. Log into the Applications Management Center:
   - Enter your login User ID.
   - Enter your Password.

Note:

While you are using the AMC interface, if you click the browser back button, you may need to refresh your browser to display the screen again.

2. Create a Customer Account for each MiVoice Business Solution Virtual Instance customer. Do not put multiple customers in a single customer account.

   - Under **Systems**, click **Customers**.
   - Click the **Create Customer** button.
   - Enter the end customer information. Record the Customer Name and Customer ID.
   - Enter the email address of the account manager responsible for this customer.
   - Enter the email address of the technician responsible for supporting this customer.
   - Click **Submit**.
   - Click **Confirm**.

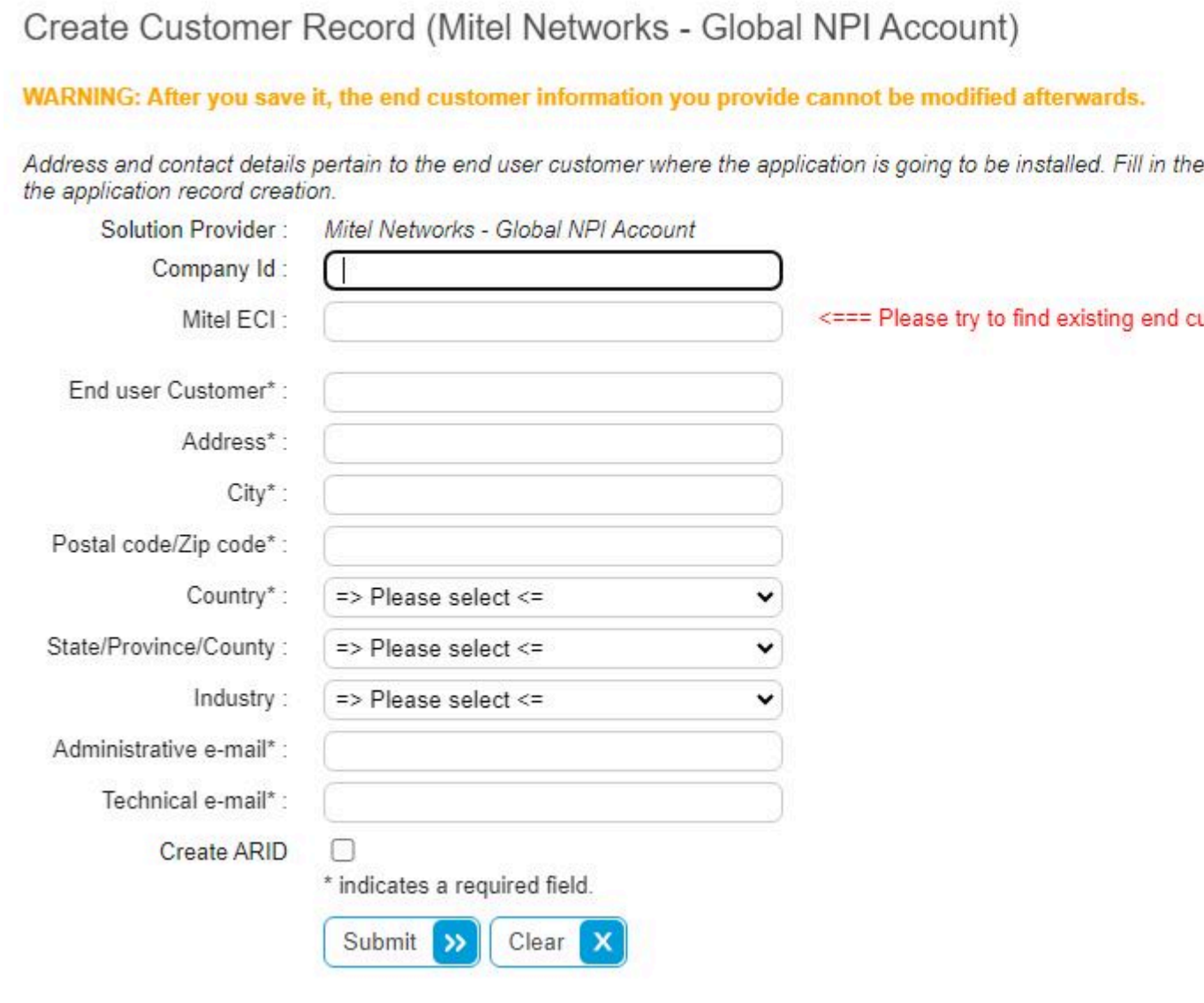


Figure 11: Creating a Customer

3. Register (purchase) products and licenses for the MiVoice Business Solution Virtual Instance deployment. The following is an example for the MiVoice Business Solution Virtual Instance using the clear base:

   - Click **Register a License**.
   - Enter a Purchase Order reference number.
   - Enter your products and licenses, for example:
     - Click **+** beside Mitel MiVoice Business Solution Virtual Instance Products. Enter the desired MiVoice Business Solution Virtual Instance Virtual Appliance base software product. To locate a part number or license description in the displayed list, use the browser Find function.
     - Click **+** beside MiVoice Border Gateway Products. Enter the desired number of "MBG: 1 SIP Trunking Channel Licenses".
     - Click **+** beside MiVoice Business Products. Enter at least two "54002390 MiVoice Business Trunk Licenses".
     - Click **+** beside Mitel Unified Collaboration and Communication Products. Enter the desired number of UCC User Licenses.
     - Click **Next**.
     - Click **Confirm**.

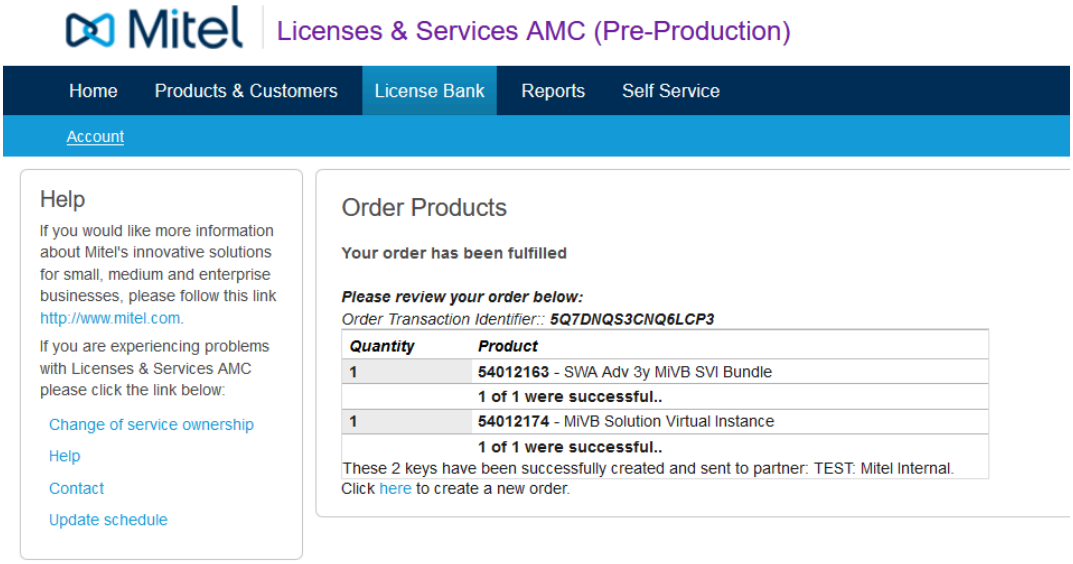
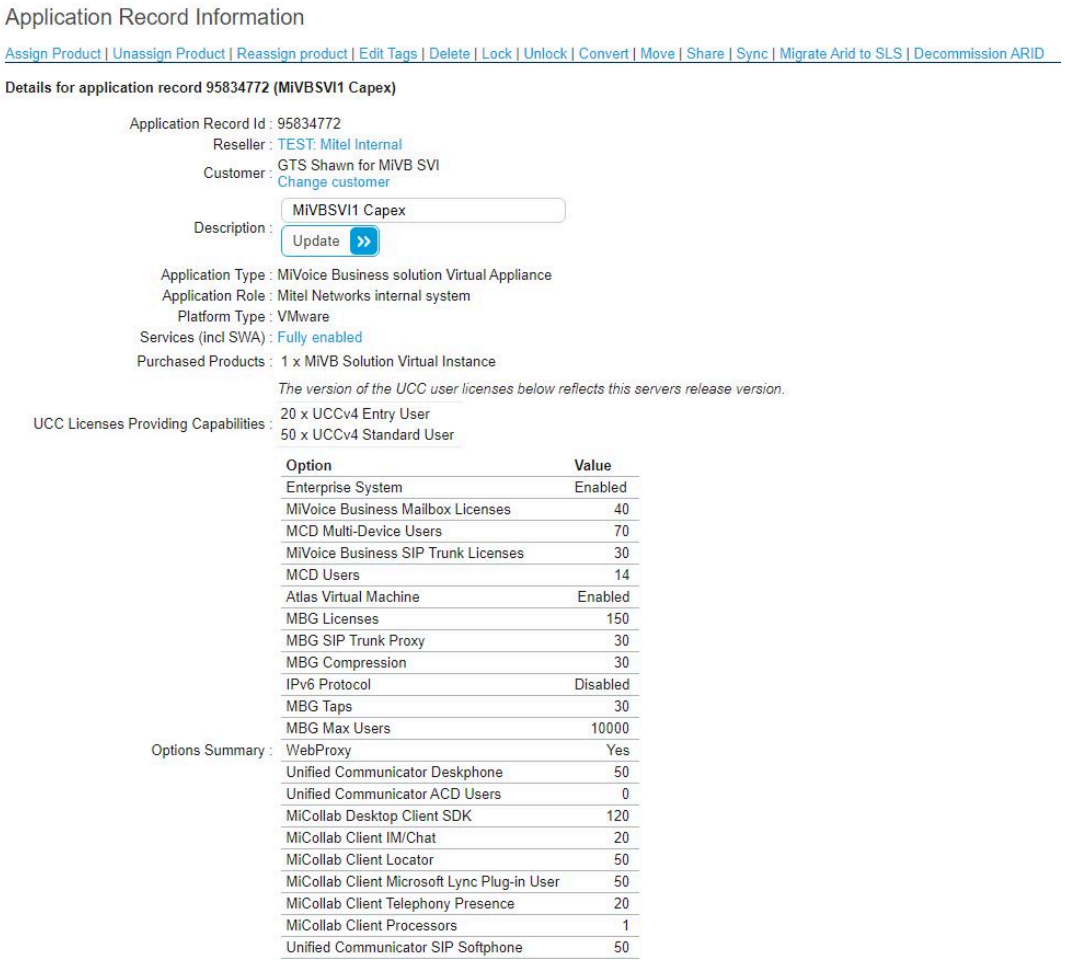


Figure 12: Order Confirmation

4. Create an Application Record ID for the MiVoice Business Solution Virtual Instance base software:

   - Click **Customers**. Enter the customer name and click **Retrieve**.
   - Select the Customer ID.
   - Click **Create App Record**.
   - Enter a description for the MiVoice Business Solution Virtual Instance base software Application Record. For example: "Microtest MiVoice Business Solution Virtual Instance Base ARID".
   - Click **Submit**. Click **Next**. The system displays the newly created ARID at the top of the screen. Record the MiVoice Business Solution Virtual Instance ARID. When you deploy the MiVoice Business Solution Virtual Instance, the Initial Configuration Wizard prompts you to enter this ARID.



Application Record Information

Assign Product | Unassign Product | Reassign product | Edit Tags | Delete | Lock | Unlock | Convert | Move | Share | Sync | Migrate Arid to SLS | Decommission ARID

Details for application record 95834772 (MiVBSVI1 Capex)

Application Record Id : 95834772
Reseller : TEST: Mitel Internal
Customer : GTS Shawn for MiVB SVI
Change customer
Description : MiVBSVI1 Capex
Update
Application Type : MiVoice Business solution Virtual Appliance
Application Role : Mitel Networks internal system
Platform Type : VMware
Services (incl SWA) : Fully enabled
Purchased Products : 1 x MiVB Solution Virtual Instance

The version of the UCC user licenses below reflects this servers release version.

UCC Licenses Providing Capabilities : 20 x UCCv4 Entry User
50 x UCCv4 Standard User

Options Summary :

Option	Value
Enterprise System	Enabled
MiVoice Business Mailbox Licenses	40
MCD Multi-Device Users	70
MiVoice Business SIP Trunk Licenses	30
MCD Users	14
Atlas Virtual Machine	Enabled
MBG Licenses	150
MBG SIP Trunk Proxy	30
MBG Compression	30
IPv6 Protocol	Disabled
MBG Taps	30
MBG Max Users	10000
WebProxy	Yes
Unified Communicator Deskphone	50
Unified Communicator ACD Users	0
MiCollab Desktop Client SDK	120
MiCollab Client IM/Chat	20
MiCollab Client Locator	50
MiCollab Client Microsoft Lync Plug-in User	50
MiCollab Client Telephony Presence	20
MiCollab Client Processors	1
Unified Communicator SIP Softphone	50

Figure 13: MiVoice Business Solution Virtual Instance Base ARID Created

5. Assign the MiVoice Business Solution Virtual Instance base software license to the MiVoice Business Solution Virtual Instance Base ARID:

   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
     - Click **+** beside the customer's ID.
     - Select the option button next to the MiVoice Business Solution Virtual Instance Base ARID and then click **Assign**.
     - Enter the Purchase order number in the Search Criteria and click **Retrieve**.
     - Click **+** to expand the Purchase order.
     - Assign the Business MiVoice Business Solution Virtual Instance base software license to the base ARID.
     - Click **Assign**.
     - Click **Confirm** to assign the licenses.
     - Review the licenses and record the ARID.
     - Click **Done** or click **Email**. Click **E-Mail Report** to notify to the administrator. You can send the notification to your technician or customer by including their email addresses.

6. In the Customer profile, select the MiVoice Business Solution Virtual Instance base ARID and create an associated ULM ARID:

   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
   - Click **+** beside the customer's ID.
   - Select the option button next to the MiVoice Business Solution Virtual Instance Base ARID.
   - Click the **Create ULM Record** button.
   - Enter a description for the MiVoice Business Solution Virtual Instance ULM Application Record. For example: "Microtest MiVoice Business Solution Virtual Instance ULM ARID".
   - Click **Submit**.
   - Click **Next**. The system displays the newly created ARID at the top of the screen. Record the MiVoice Business Solution Virtual Instance ULM ARID.
   - Click Return to License Manager page.

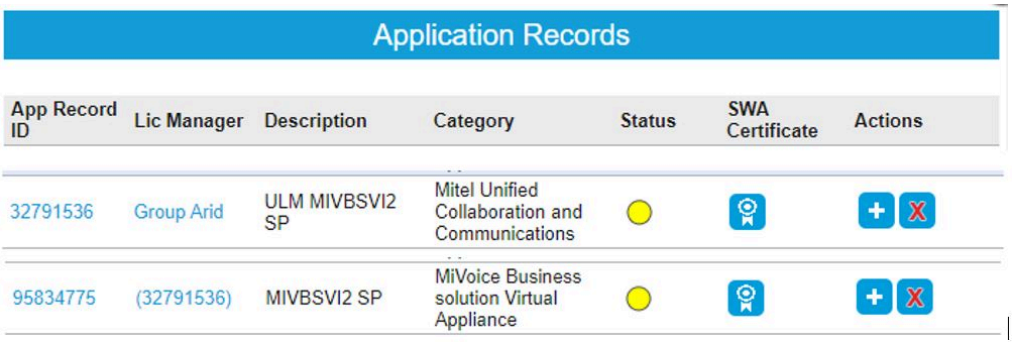


Figure 14: Create the Group ULM ARID

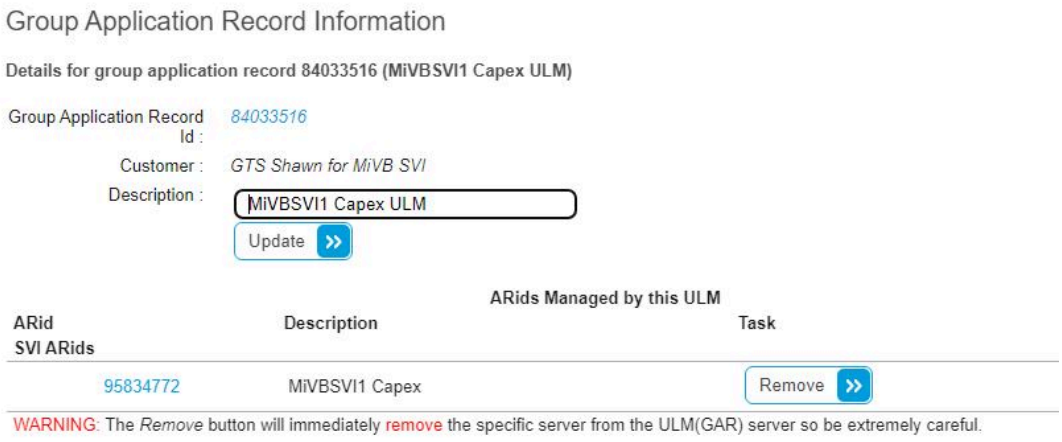


Figure 15: Group ARID

7. Assign the MiVoice Business SIP trunk licenses, MBG SIP trunk licenses, UCC User and SWAS licenses to the MiVoice Business Solution Virtual Instance ULM ARID:

   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
   - Click **+** beside the customer's ID.
   - Select the option button next to the MiVoice Business Solution Virtual Instance ULM ARID and then click **Assign**.
   - Enter the Purchase order number in the Search Criteria and click **Retrieve**.
   - Click **+** to expand the Purchase order.
   - Assign the licenses to the ULM ARID.
   - Click **Assign**.
   - Click **Allocate** to assign the licenses.
   - Review the licenses and record the ARID.
   - Click **Confirm**.
   - Click **Done** or click **Email**. Click **E-Mail Report** to notify to the administrator. You can send the notification to your technician or customer by including their email addresses.

Deploy VM 5

This chapter contains the following sections:

This chapter describes the steps involved in deploying a MiVoice Business Solution Virtual Instance on various supported virtualization platforms. Subsequent sections provide information on setting up and operating the SVI instance.

5.1 Deploy on VMware

Users can deploy SVI on VMware:

- directly onto the ESX/ESXi host
- onto the ESX/ESXi host via vCenter Manager, or
- onto the ESX/ESXi host via vCloud Director

You deploy the MiVoice Business Solution Virtual Instance as an image in OVF package format (file ending in OVA). The MiVoice Business Solution Virtual Instance OVA file contains the VMware tools, MSL operating system, MiCollab, MiVoice Business, and MBG software as a pre-installed image.

Deploy OVF Template

1. Login to vSphere or ESXi.
2. In **Select an OVF template** window, enter URL by copying the URL of OVA download or click **Browse** to upload the .ova file. Click **NEXT**.
3. In **Select a name and folder** window, select a name and target location. Click **NEXT**.
4. In **Select a computer resource** window, click **NEXT**.
5. In **Review details** window, click **NEXT**.
6. In **License agreement** window, enable **I accept all license agreements** checkbox and click **NEXT**.
7. In **Configuration** window, select any one option based on deployment size and click **NEXT**.
8. In **Select storage** window, **Select virtual disk format** from the drop-down list. click **NEXT**.
9. In **Select networks** window, select **Source Network** and **Destination Network** from the drop-down list of the corresponding source network. **LAN Network** is mandatory and the other two networks are optional. Click **NEXT**.

10. In **Customize template** window, perform the following steps:

    a. Under **Administration**, enable **Restore from Backup** checkbox only if you are upgrading. For a new installation, skip this step.

    Only MiVoice Business Solution Virtual Instance to MiVoice Business Solution Virtual Instance backup and restore is supported.

    b. Under **Applications**, set **Initial Administration Password**. This field is mandatory. Applications like vCloud Director and ESXi may not enforce to set the value.

    c. Enter a unique **Hostname**.

    d. Enter **Domain Name (Optional)**.

    e. Enter **License Key (Optional)**. License key is required to license the applications and enable user / service provisioning. If not provided during OVA deployment, it must be configured using server manager before attempting user provisioning.

    f. Enter **Remote Network Address (Optional)**. Remote Network Address is required to be able to connect a browser to MSL server manager.

    g. Enter **Remote Network Netmask (Optional)**. Remote Network Netmask refers to the netmask associated with the IP address of the remote network.

> **Note**:
> If an optional value for Domain Name, License Key, Remote Network Address, or Remote Network Netmask is not provided during OVA deployment, it must be added later using server console / server manager.

.

    h. Under **Localization**, select **Timezone setting** and select a **Keyboard** from the drop-down list.

    i. Under **Network Settings**, enter the values in the required fields. Mandatory fields are **LAN IP Address** and **Default Gateway Address**.

    - A WAN IP must be provisioned if MBG is connected to the internet, otherwise enter 0.0.0.0.
    - Optional LAN IP must be provisioned if MBG is connected to a private SIP service provider, otherwise enter 0.0.0.0.

Note:
If a WAN IP is entered, then the default gateway address must be within the WAN subnet. Otherwise, it must be within the LAN subnet.

j. Under **Next Steps**, please read the mandatory steps post deployment regarding **Provision 2nd IP address on default LAN**. This step is an acknowledgment statement.

k. Click **NEXT**.

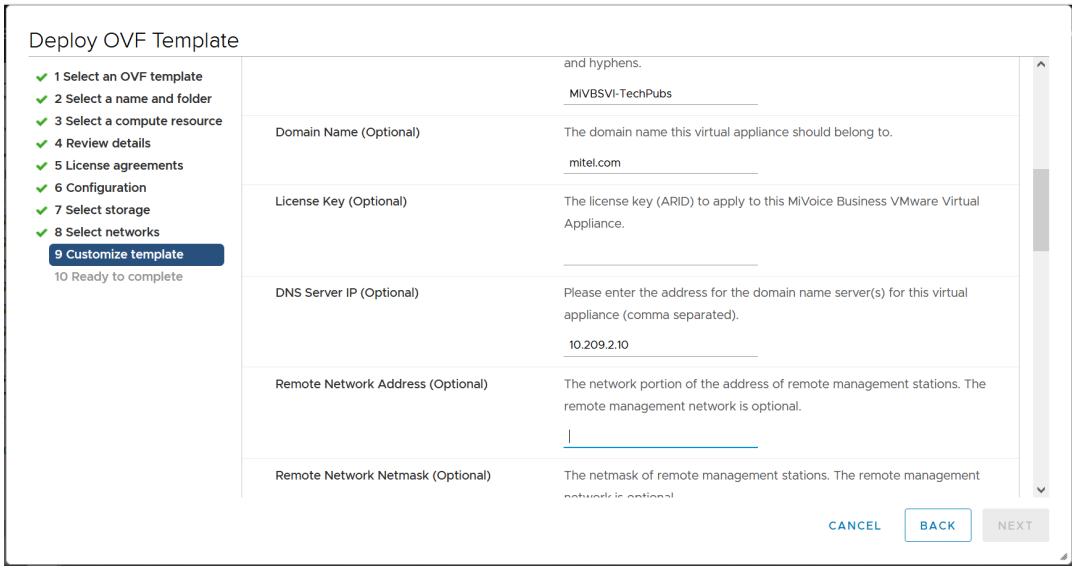


Figure 16: Customize template

11. In **Ready to complete**, you can view all the details entered to deploy OVF. click **FINISH**.

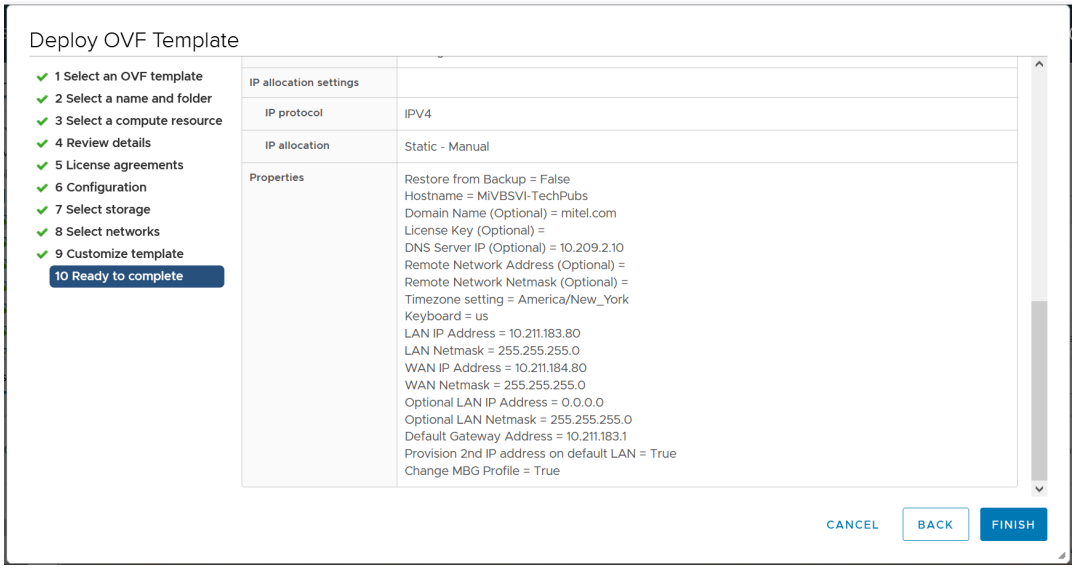
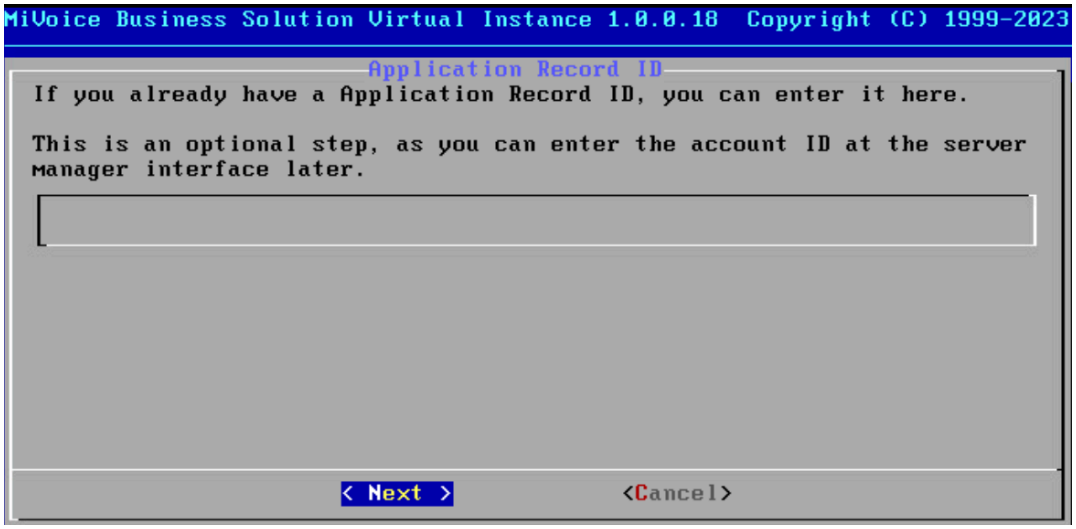


Figure 17: Ready to complete

5.1.1 Power on MiVoice Business Solution Virtual Instance

1. Select the newly created MiVoice Business Solution Virtual Instance and select **Power On** or click the Play button.
2. Launch the Console. The system boot up progress messages are displayed in the Console screen.
3. When the system is finished booting up, if **Application Record ID** page is displayed, click **Next**.



4. The mitel-vm login: prompt is displayed. The "prompt" changes to the system name that you chose during deployment.

> **Note**:
> It may take up to 10 minutes before the prompt appears.

5.2 Deploy on Nutanix Prism

SVI VM can be deployed on Nutanix AHV using the Prism management interface by using the OVA file. Deploying SVI OVA in Nutanix Prism involves two steps:

1. Upload SVI OVA on Nutanix Prism
2. Deploy SVI OVA on Nutanix

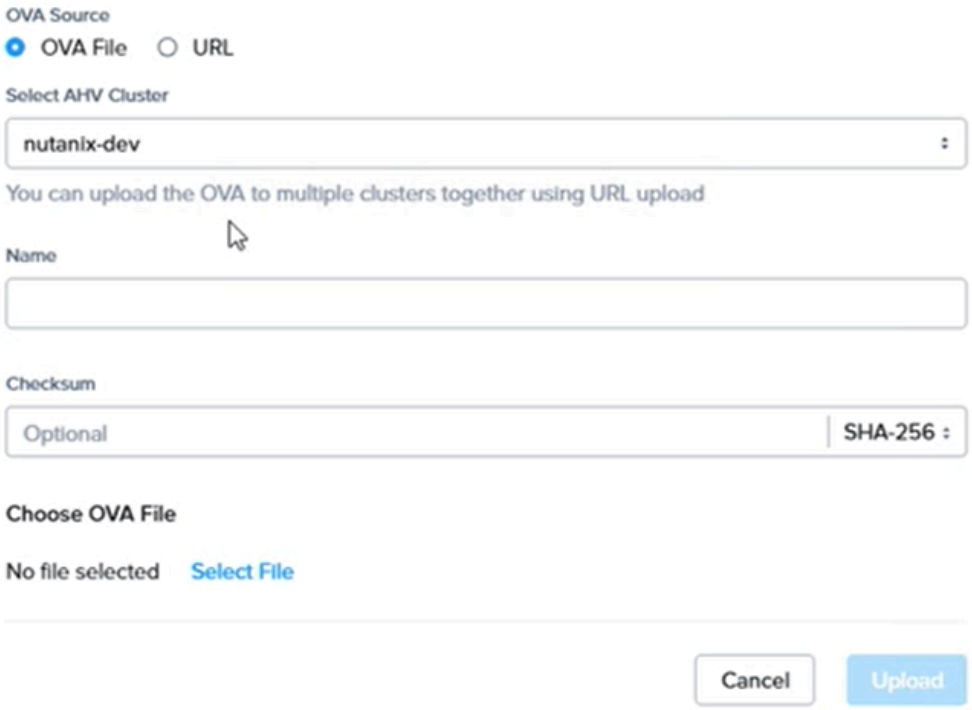
Upload OVA on Nutanix Prism

The OVA image can be uploaded either from the local system or through a network URL.

Follow the procedure below to upload OVA image from local system:

1. Log in to Nutanix Prism.
2. Click the menu icon on the left hand side of the Dashboard.
3. In the left panel, navigate to **Computer & Storage** > **OVAs**.
4. Click **Upload OVA**.

   Upload OVA window is displayed.



5. Select **OVA File** and enter the **Name**.
6. Click **Select file**.
7. Navigate to the folder where the .ova file is stored.

   Upload progress is displayed
8. Click **Upload**.

   Uploading of the OVA file happens asynchronously in the background. The uploading can be monitored from **Dashboard** > **Computer & Storage** > **OVAs** page. The upload can be restarted from the same page in case it gets terminated.

Deploy OVA on Nutanix

Deploy a VM using the uploaded MiVoice Business Solution Virtual Instance OVA.

1. In the Prism, navigate to **Computer & Storage** > **OVAs**.
2. Select the uploaded OVA checkbox.

3. From **Actions** drop-down list, select **Deploy as VM**.

   Deploy as VM window is displayed.
4. Enter the required fields.
5. Under **VM Properties**, select the value for **CPU** , **Cores per CPU**, and **Memory** as per the planned system capacity.

   Refer to the table MiVoice Business Solution Virtual Instance system size for details. For example, 250 user system capacity deployment would configure 4 vCPU, 1 Core per CPU and 10 GB memory.
6. Click **Next**.
7. Under **Networks**, delete existing networks if any. Click **Attach to Subnet** and add the LAN and WAN networks as per the chosen deployment mode. For a server-only mode of deployment, at least a single LAN network must be configured.
8. Under **Boot Configuration**, select **Legacy BIOS Mode**.

9. Click **Next**.
10. Under **Guest Customization**, from **Script Type** drop-down list, select **No Customization** and click **Next**.

    The window displays all the configuration values to review.
11. Click **Create VM**.

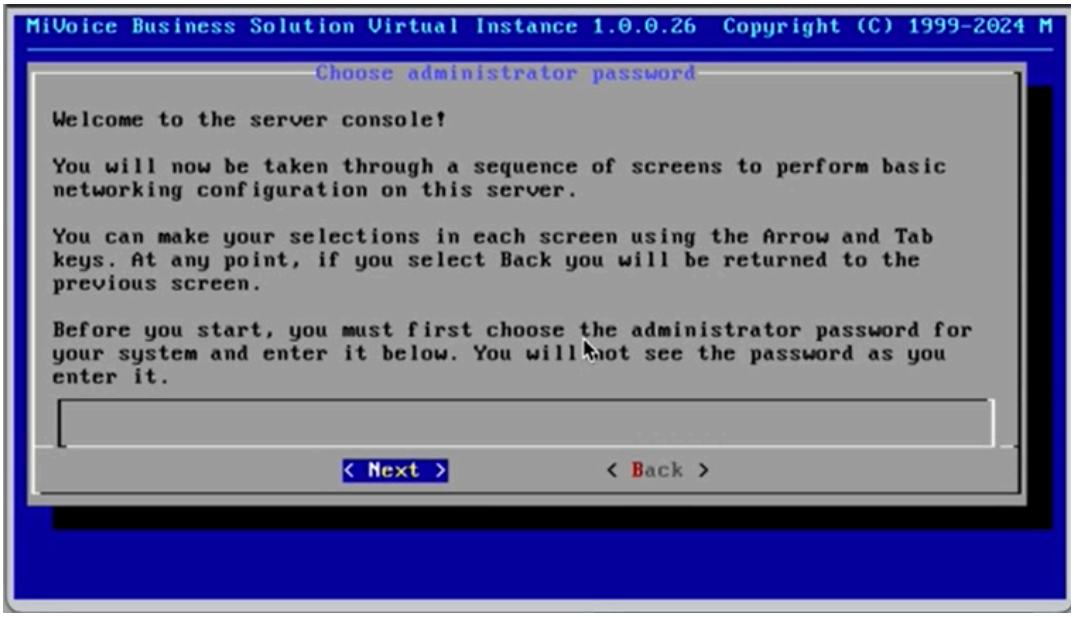
    You can check if the VM is created by by navigating to **Dashboard** > **Computer & Storage** > **VMs** panel.
12. Navigate navigate to **Computer & Storage** > **VMs**.
13. Select the newly created VM.

    You can see that the Power State if Off.
14. In the **Actions** drop-down list, select **Power On**.
15. Select the newly created VM.

16. In the **Actions** drop-down list, select **Launch console**.

    The console is launched in a new window.

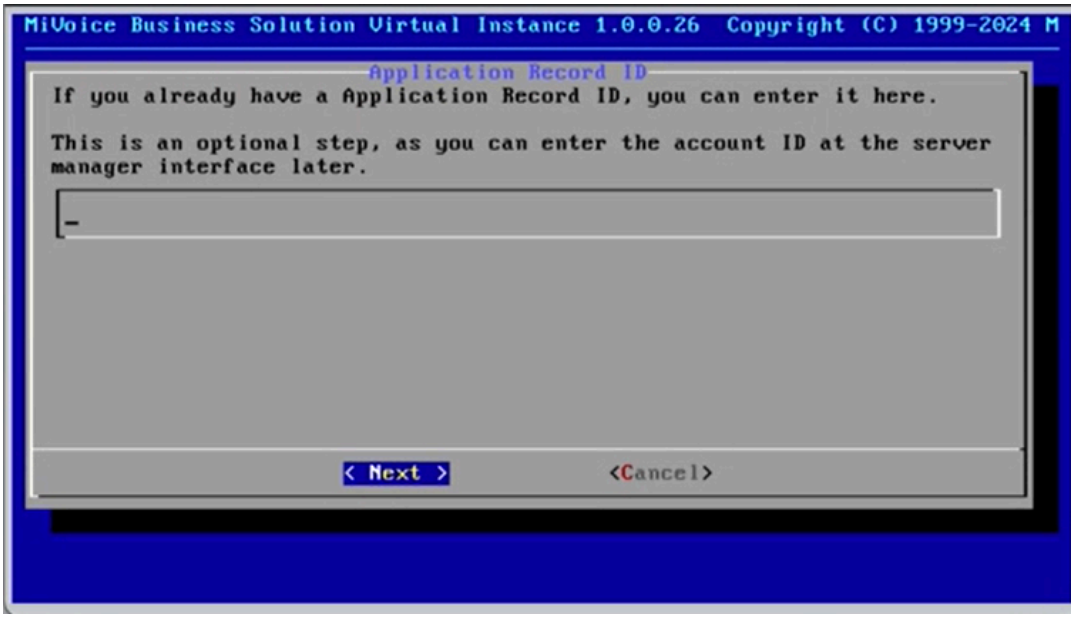
    a. In the **Select Keyboard Language window**, select the language and click **Next**.
    b. In the **Restore From Backup** window, click **No**.
    c. In the **Choose administrator password** window, enter the password and click **Next**.



    d. In the **Choose administrator password** window, enter the password again and click **Next**.

    In the **Activating configuration settings** page, status of configuration is being displayed. The activation process might take a few seconds to a few minutes.

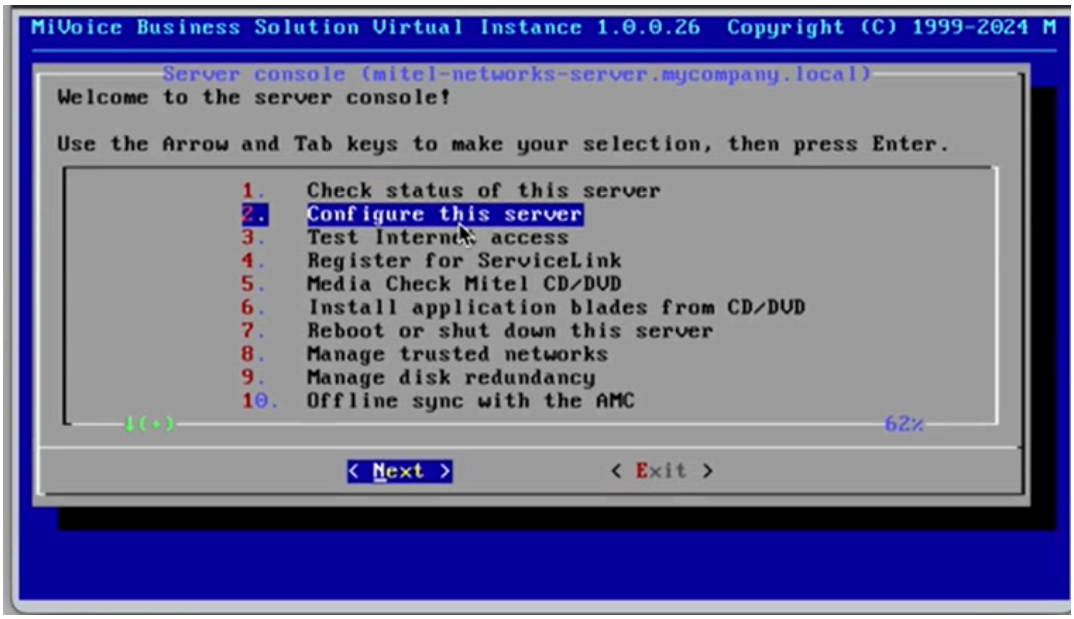
    e. In the **Application Record ID** (optional), enter the account ID and click **Next**.



f. In the command line prompt window, enter mitel-networks-server login as *admin* and use the password set during step 16c.

The **Server console** window is displayed.

g. In the **Server console (mitel-networks-server.mycompany.local)** window, select **Configure this server** and click **Next**.



h. In the **Primary domain name**, enter the domain name for your server and click **Next**.

i. In the **Enter system name** window, enter the system name and click **Next**.

j. In the **Select local network adapters** window, select *eth0* and click **Next**.

k. In the **Local networking parameters** window, enter local IP address and click **Next**.

l. In the **Enter local subnet mask** window, enter the local subnet mask and click **Next**.

m. In the **Enable IPv6 protocol** window, click **Next.**

n. In the **Enter additional static IP address** window, enter the IP address and click **Next**.

o. In the **Enter gateway IP address** window, enter the gateway IP address and click **Next**.

p. **Select WAN network adapters** window: If the the WAN adapter is selected, follow the steps below. If not, skip to step q.

- In the **External Interface Configuration** window, select **Use static IP address** and click **Next**.
- In the **Enter static IP address** window, enter the static IP address and click **Next**.
- In the **Enter subnet mask** window, enter the subnet mask and click **Next**.
- In the **Enter gateway IP address** window, enter the gateway IP address and click **Next**.
- In the **Enter additional static IP address** window, enter the static IP address and click **Next**.
- In the **Unconfigured network adapters** window, select the value and click **Next**.

q. In the **Corporate DNS server address**, enter the DNS server IP address and click **Next**.

r. In the **System Reboot Required** window, click **Reboot Now**.

Reboot process might take a few seconds to a few minutes.

In the **Activating configuration settings** page, status of configuration is being displayed and in the **Starting system services** window, the progress is shown the progress bar. The activation process might take a few seconds to a few minutes.

s. In the **Application Record ID** (optional), enter the account ID and click **Next**.

t. In the command line prompt window, enter login and password to check the status.

17. Login to MiVoice Business Solution Virtual Instance.
18. Change account password and log in again.
19. Navigate to **Security** > **Remote access**.
20. Under **Secure Shell Settings**,

    a. from **Secure shell access** drop-down list, select **Allow public access (entire Internet)**.

    b. from **Allow administrative command line access over secure shell**, drop-down, select **Yes**.

    c. from **Allow secure shell access using standard password** drop-down, select **Yes**.

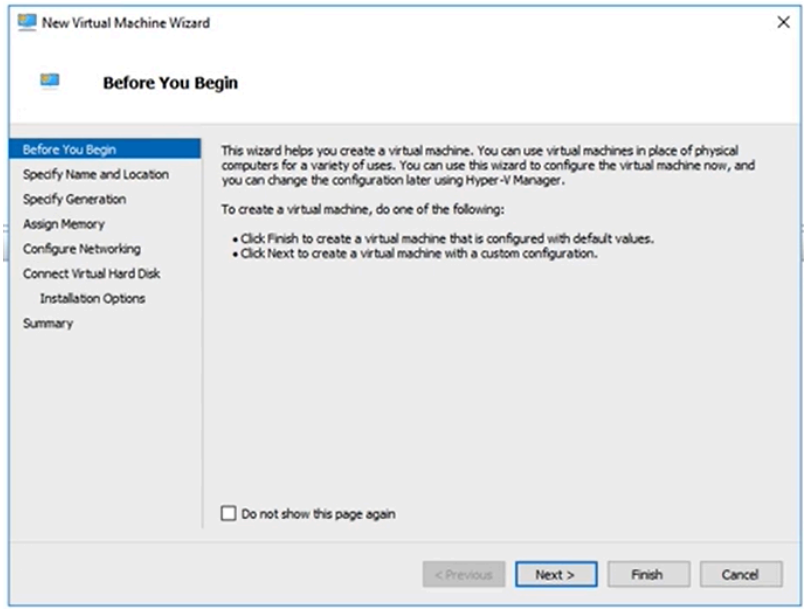
21. Click **Save**.
22. Proceed with next section.

5.3 Deploy VM on Hyper-V

SVI VM is deployed on Hyper-V using VHDX files.

1. Login to Hyper-V Manager.
2. Under Hyper-V Manager, right click on the VM and select **New** > **Virtual Machine**.

   The **New Virtual Machine Wizard** window is displayed.



3. In the **Before You Begin** tab, click **Next**.
4. In the **Specify Name and Location** window, enter the **Name** and click **Next**.

5. In the **Specify Generation** window, select **Generation 1** and click **Next**.
6. In the **Assign Memory** window, enter the **Startup memory** and click **Next**.

   The memory value depends on the planned system user capacity. Refer to the table MiVoice Business Solution Virtual Instance system size for the details. For example, 250 user system capacity deployment would configure 4 vCPU, 1 Core per CPU and 10 GB memory.
7. In the **Configuration Networking** window, select desired network connection from the **Connection** drop-down list.
8. In the **Connect Virtual Hard Disk** window, select **Use an existing virtual hard disk**. Click **Browse** and navigate to the folder where the file is saved. Select the disk1 VHDX file (designed for deployments with up to 250 users) and click **Next**.
9. In the **Summary** window, check the values and click **Finish**.

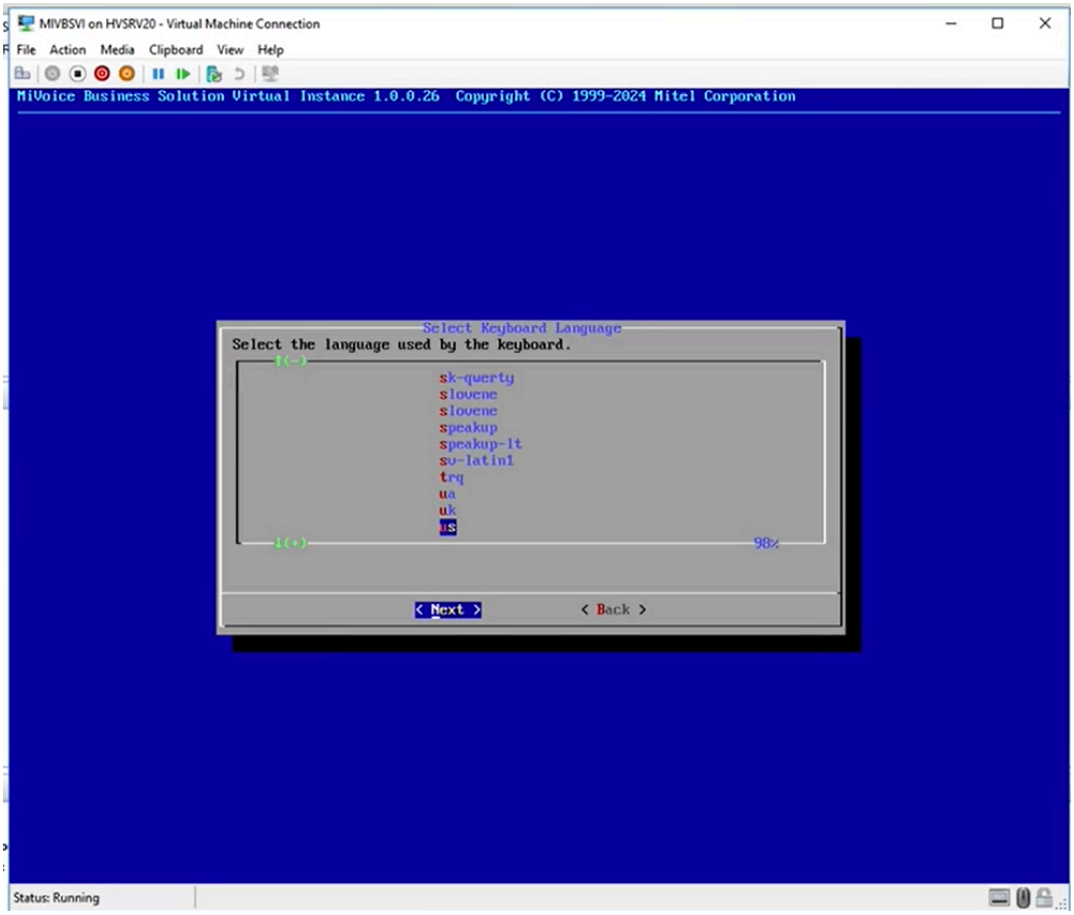
   The VM is displayed under **Virtual Machines** in the Hyper-V Manager window.
10. Right click on the newly created window and select **Settings**.
11. Settings page:

    - Select **Processor**. From the **Number of virtual processors** drop-down list, select a value as per the planned system user capacity. Refer to the table MiVoice Business Solution Virtual Instance system size for the details. For example, 250 user system capacity deployment would configure 4 vCPU where as a 500 system user deployment would need 6 vCPU. Click **Apply**.
    - Select **Add Hardware**. Select **SCSI Controller** and click **Add**.

      The SCSI Controller tab is selected.
    - Select **Hard Drive** and click **Add**.
    - Under **Hard Drive**, in **Virtual har drive** option, click **Browse** and navigate to the folder and select disk2 VHDX (80 GB additional capacity for deployments exceeding 250 users).
    - Click **Apply** and click **OK**.

12. Under Virtual Machines, right click on the newly created VM and select **Start**.

    The Virtual Machine connection is established and a new Virtual Machine connection window is displayed.



13. Follow the procedure from Step 16 > step b to step j in Deploy on Nutanix Prism on page 63section.
14. In the **Enter local subnet mask**, enter the subnet mask and click **Next**.
15. In the **Enter additional static IP address**, enter the second local IP address.
16. In the **Enter gateway IP address**, enter the gateway IP address.
17. Again follow the procedure from step m to step p and step 17 to step 21. in Deploy on Nutanix Prism on page 63.

Perform Configuration 6

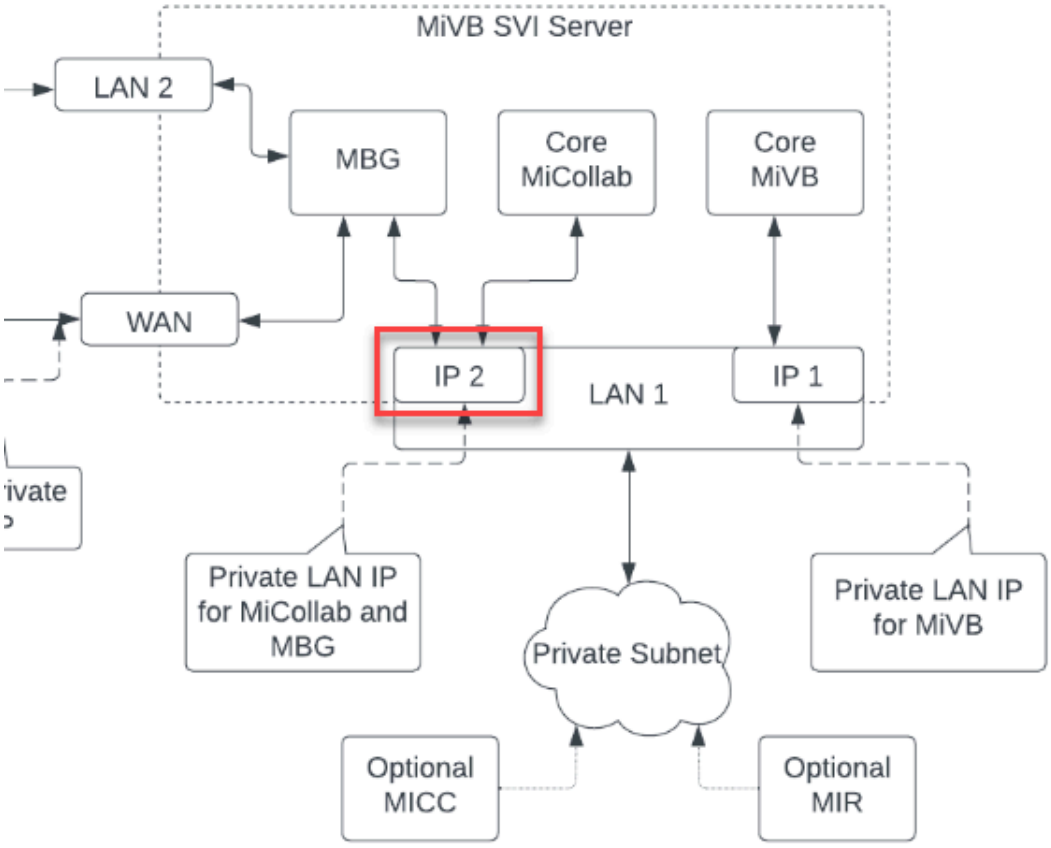
This chapter contains the following sections:

Note:
Configure the MSL server through MSL console application if it is not already done during OVA deployment. This configuration includes setting the system name, domain name, gateway, and configuring LAN, WAN, and DNS Server settings.

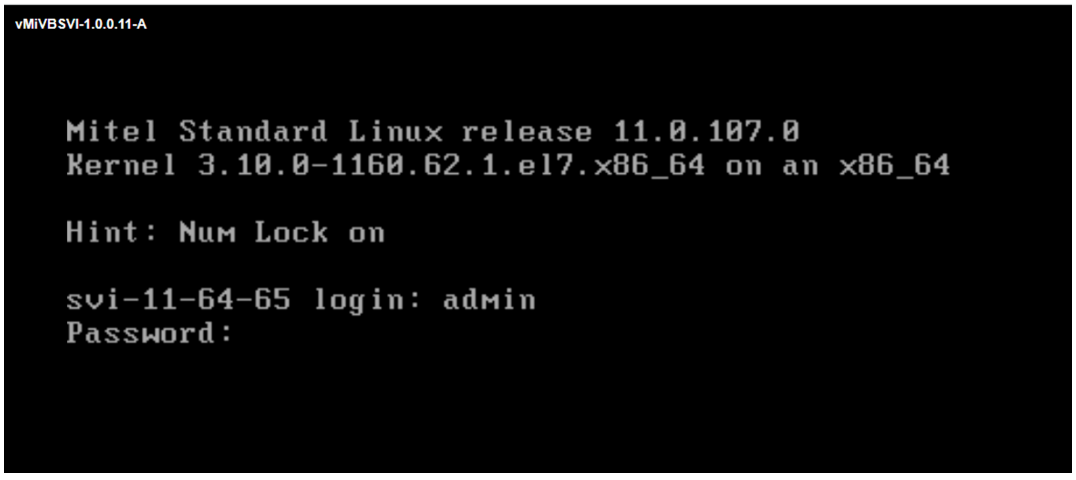
6.1 Add 2nd IP address to default LAN interface

It is mandatory to add 2nd IP address to default LAN interface.

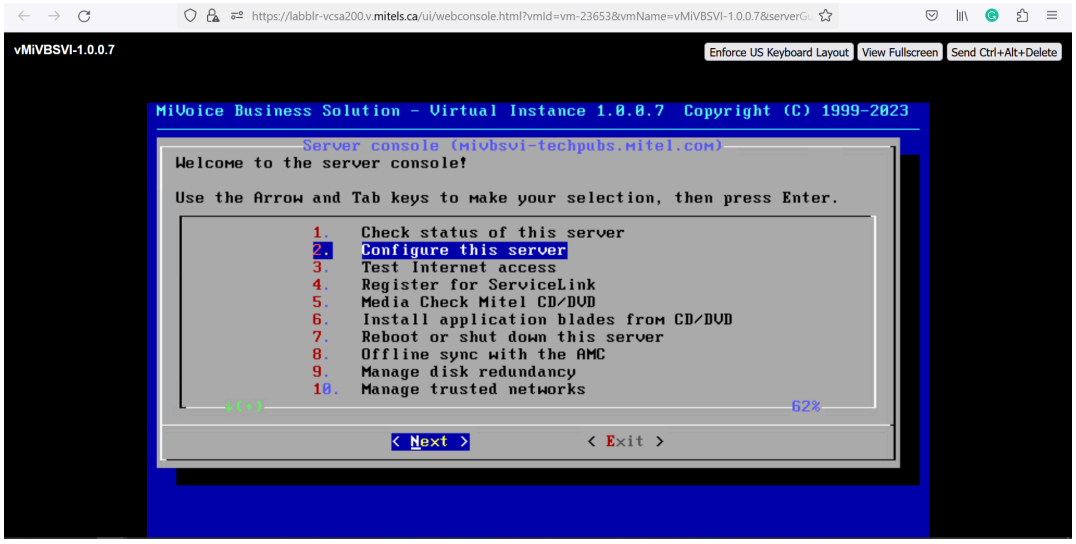
To configure the 2nd IP address, perform the following steps:



1. Launch the Web Console from vSphere, Nutanix, Hyper-V, or ESXi.
2. Login as **admin** and enter administrator password that was provided during OVA deployment. Type `console` as shown in the picture below:



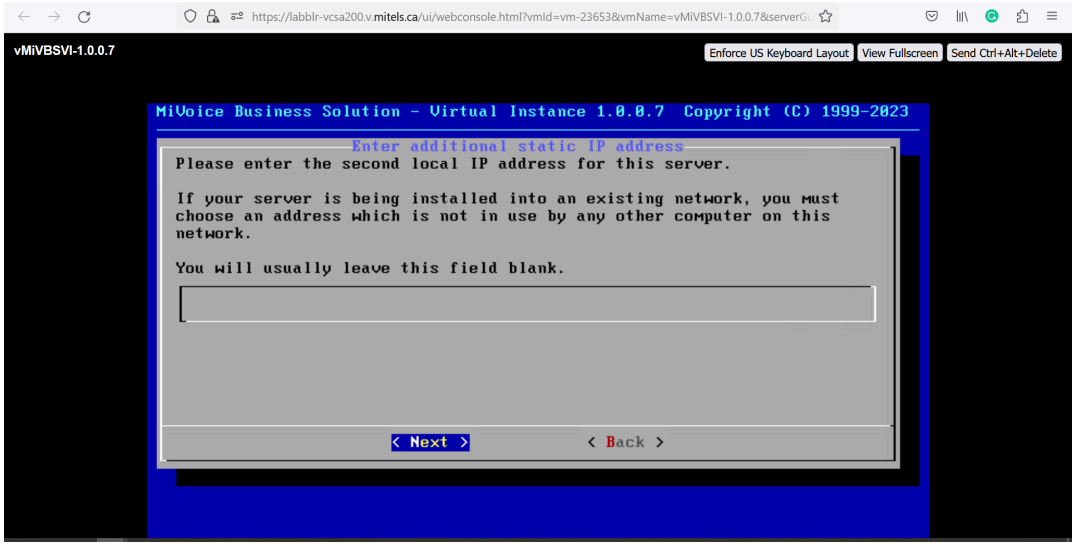
3. In the **Server console** window, select **Configure this server** and click **Next**.



4. In **Primary domain name** window, continue with the existing value or enter/modify the domain name. Click **Next**.

> **Note**:
> The domain name must be provided, otherwise the procedure fails.

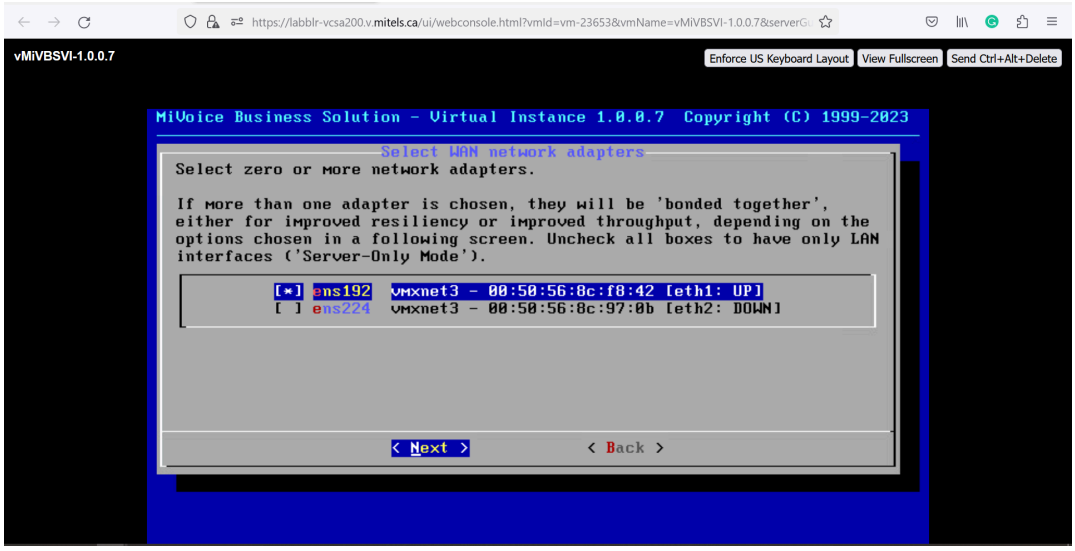
5. In **Enter system name** window, continue with the existing value or enter/modify the system name. Click **Next**.
6. In **Select local network adapters** window, select eth0 adapter by pressing space bar. Click **Next**.
7. In **Local networking parameter**, continue with the existing value or enter/modify the default LAN IP address and click **Next**.
8. In **Enable IPv6 protocol** window, select **no**.
9. In **Enter additional static IP address** window, enter the 2nd LAN IP address. Click **Next**. Note that this is a mandatory field.



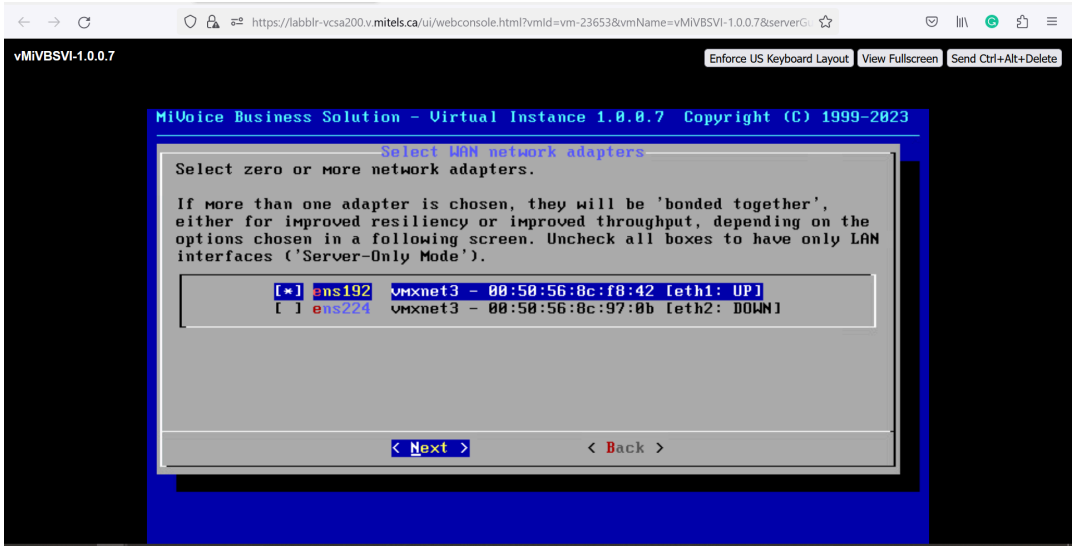
10. In **Select WAN network adapters** window, select network adapter. Click **Next**

Note:
This field is dependent on the deployment model.

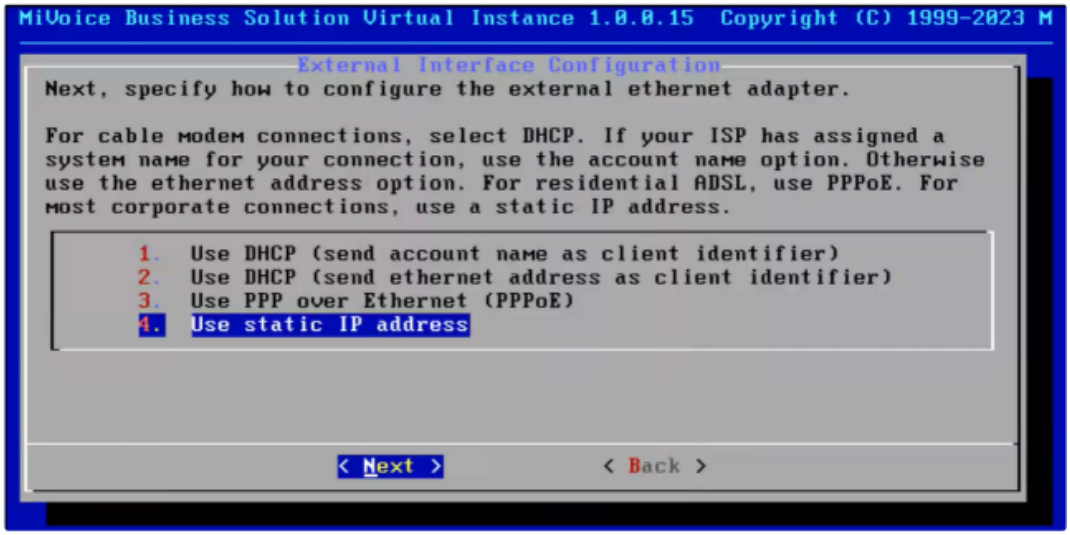
.



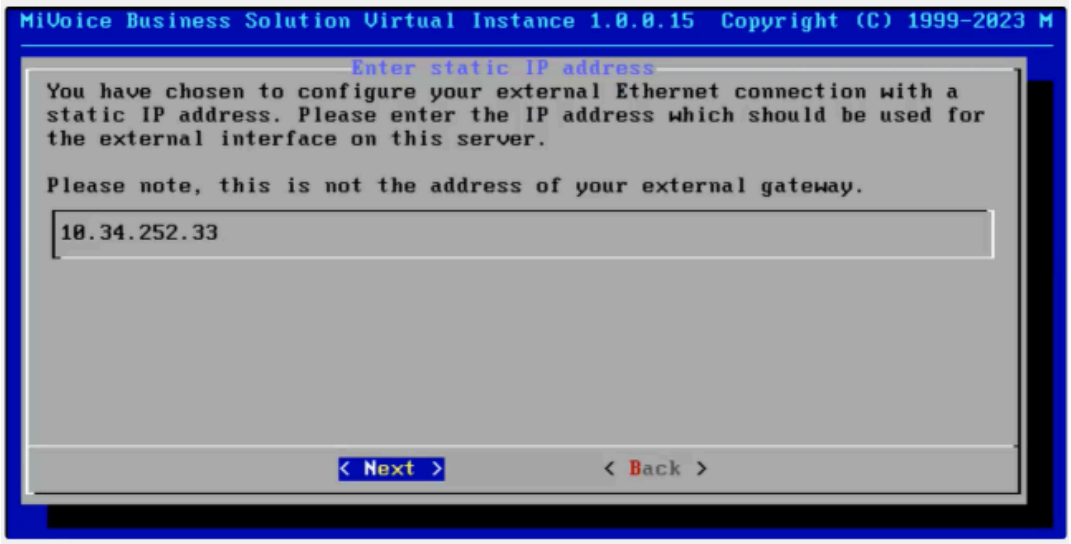
11. Perform Step 21 only if the network is down, otherwise perform Step 12.
12. Click **Next**.



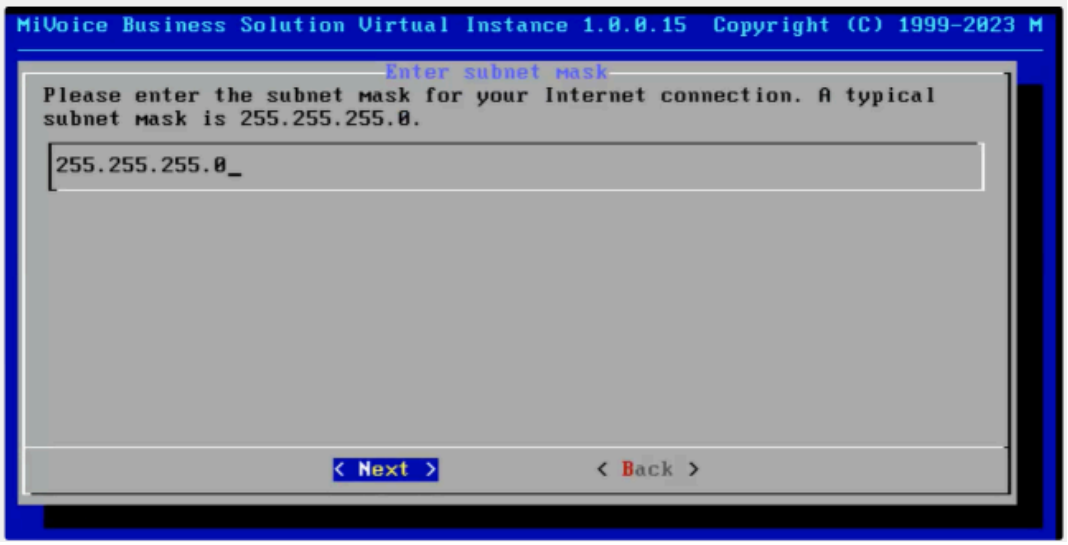
13. Click **Next**.



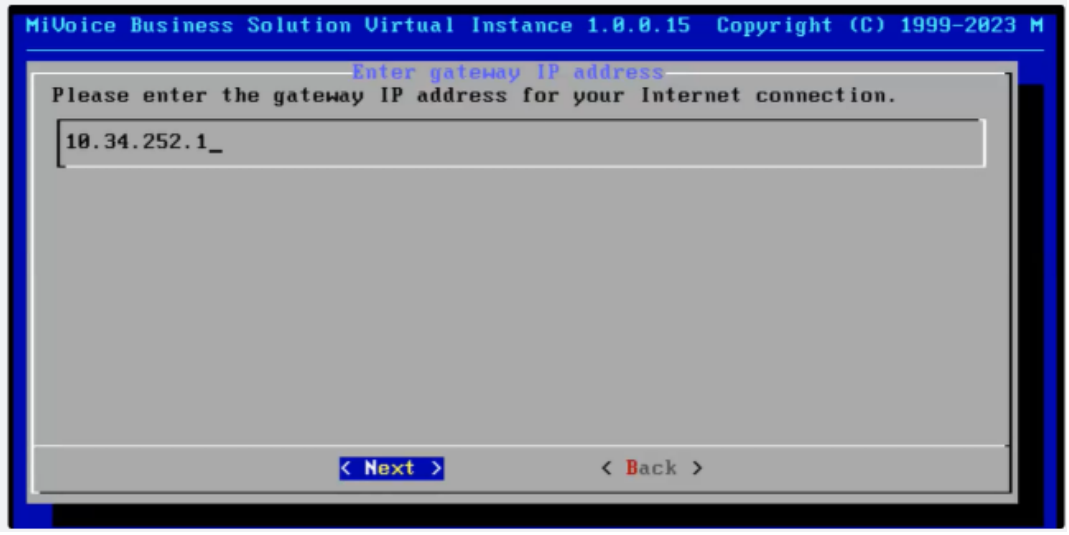
14. Click **Next**.



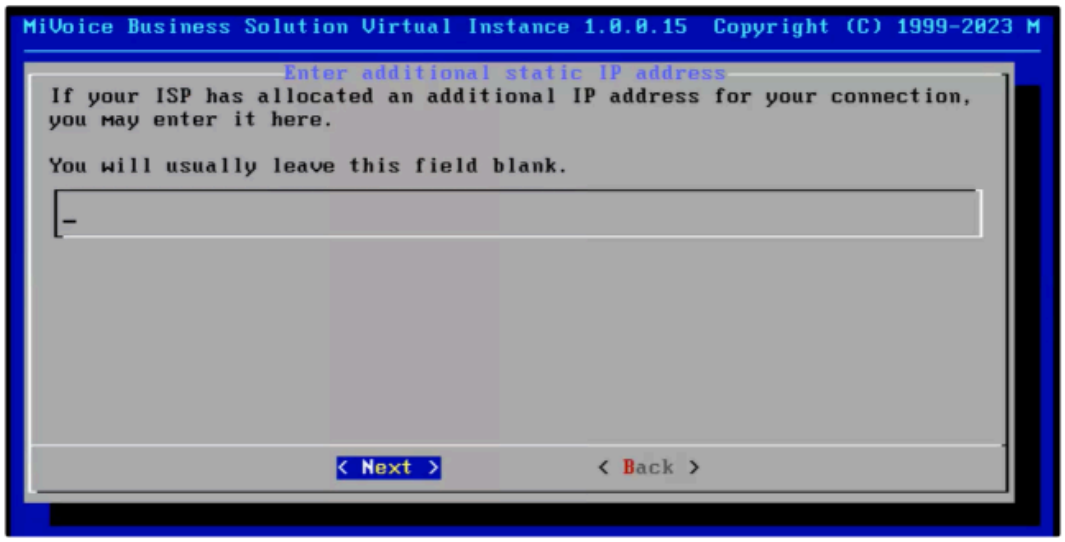
15. Click **Next**.



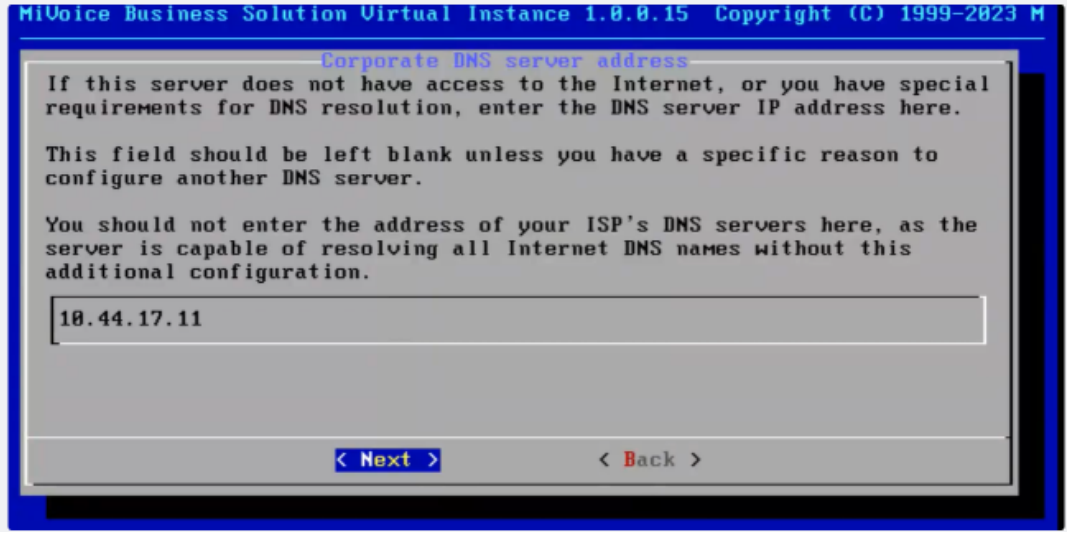
16. Click **Next**.



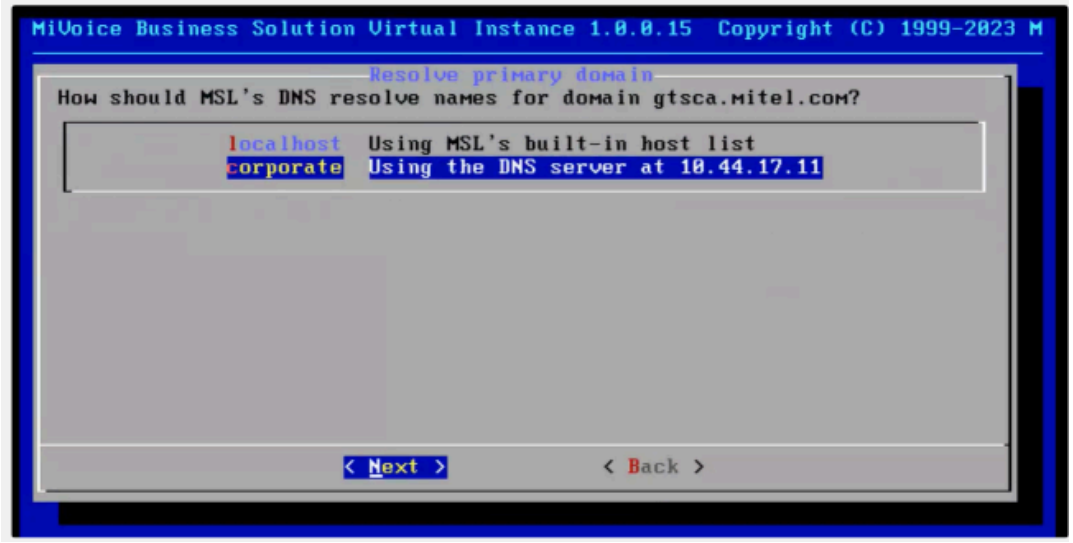
17. Click **Next**.



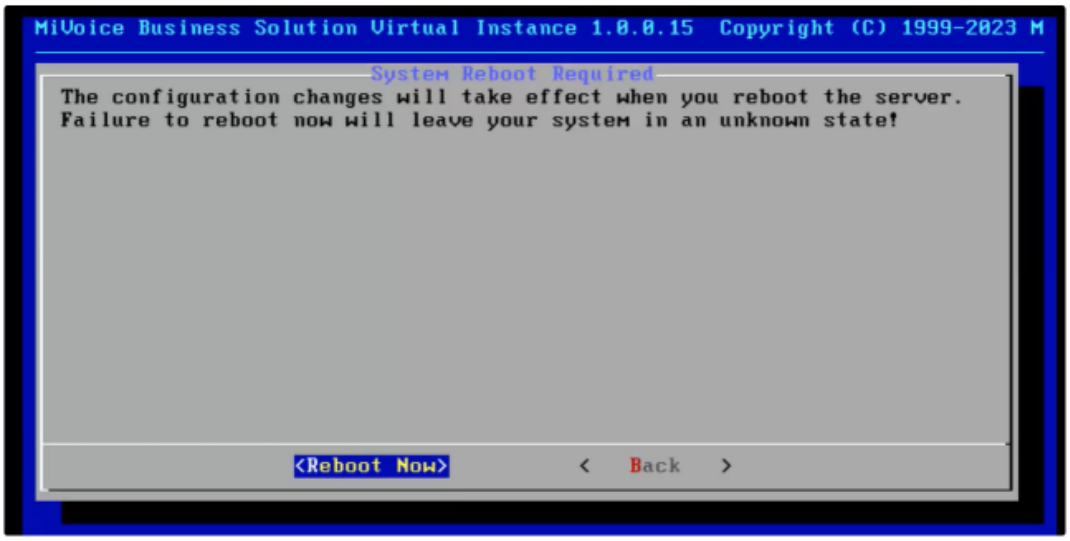
18. Click **Next**.



19. Click **Next**.



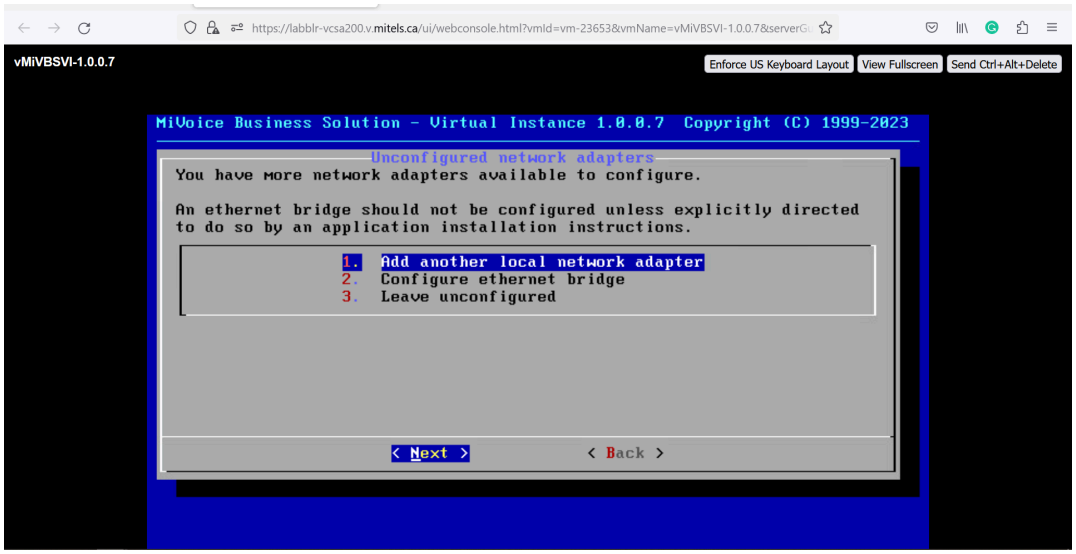
20. In **System Reboot Required** window, click **Reboot Now**.



21. (Optional) If the network is down, perform the following steps:

Note:
If the deployment uses private SIP-Trunking functionality, the following procedure is mandatory.

a. In **Unconfigured network adapters** window, select **Add another local network adapter** and click **Next**.



b. In **External Interface Configuration** window, select **Use static IP address** and click **Next**.

c. In **Enter Static IP address** window, enter WAN IP address and click **Next**.

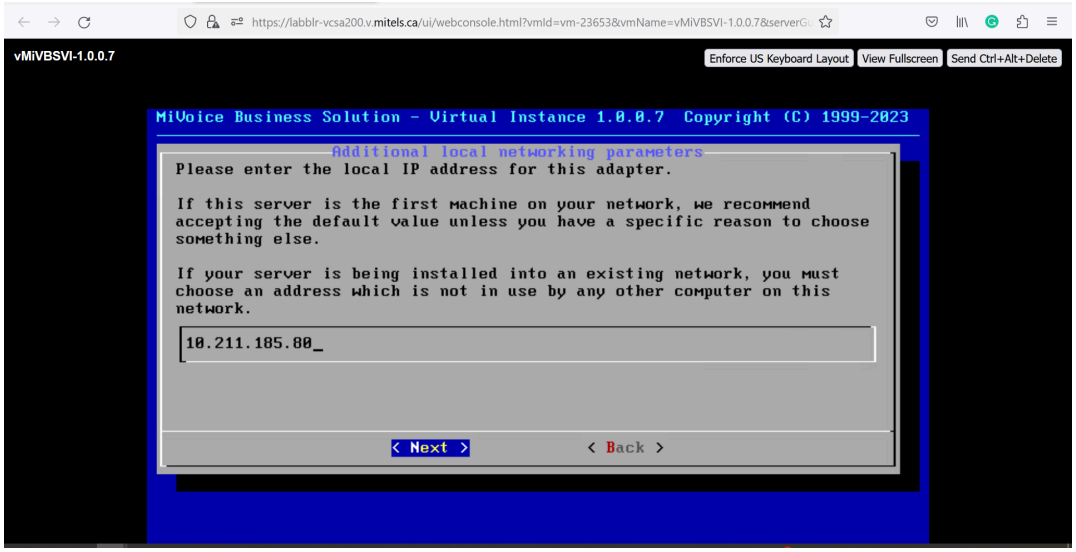
d. In **Enter gateway IP address** window, enter gateway IP address.

e. In **Enter additional static IP address** window, leave it blank.

f. In **Unconfigured network adapters** window, select **Add another local network adapter** and click **Next**.

g. In **Select additional LAN network adapters**, select the network by pressing space bar. Click **Next**.

h. In **Additional local networking parameters** window, enter local IP address.



i. In **Corporate DNS server address** window, enter DNS server IP address of the corporate DNS server only if it is available, else, leave it blank and click **Next**.

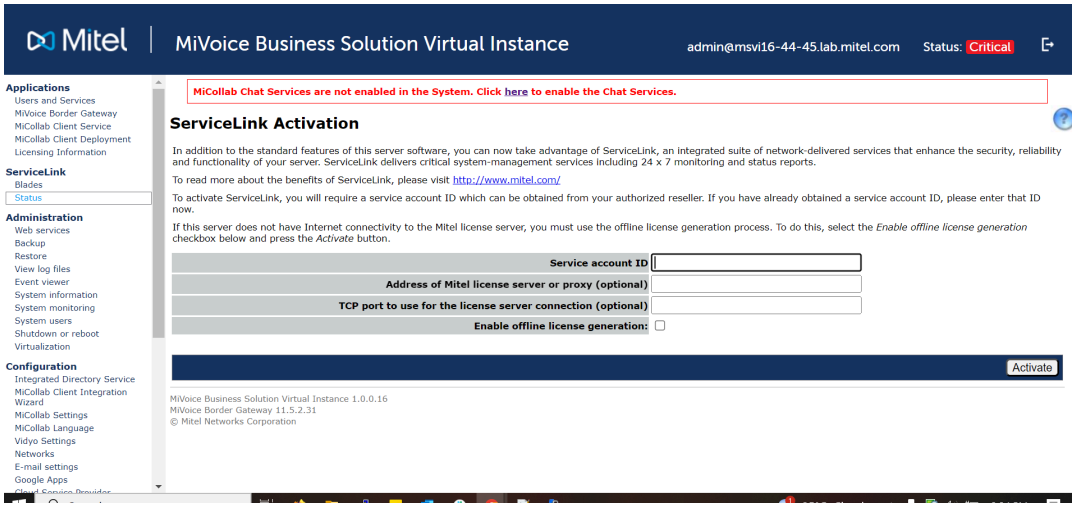
j. In **Resolve primary domain** window, click **Next**.

k. In **System Reboot Required** window, click **Reboot Now**.

6.2 Configure MSL Server

To configure the MSL server, follow the guidelines below:

1. Login to server manager. You will be prompted to select a new password.
2. Assign ARID that you have received from Mitel, if you have not done it already. Enter the details, click **Activate** to register with Mitel.



Note:
When the license is applied, MiCollab Client Integration Wizard runs automatically and creates enterprise details.

3. To add trusted networks, navigate to **Configuration** > **Networks** > **Trusted Networks**.

   Trusted Networks must be added if phones are deployed on a different network other than the local network.
4. To manage Web Server Certificates – Let's Encrypt or wildcard certificate, navigate to **Security** > **Web Server**.
5. Log out and log in again to continue further with configuration.

For more information, refer MSL Installation and Administration Guide.

6.3 Add FQDN(s) for 2nd IP address on default LAN

FQDN is required for Embedded Voicemail functionality. You can provision FQDNs in the following ways:

- Populate private FQDNs in MSL by navigating to **Configuration** > **Hostnames and addresses**.
- Configure a corporate DNS server and add FQDN on the corporate DNS server.

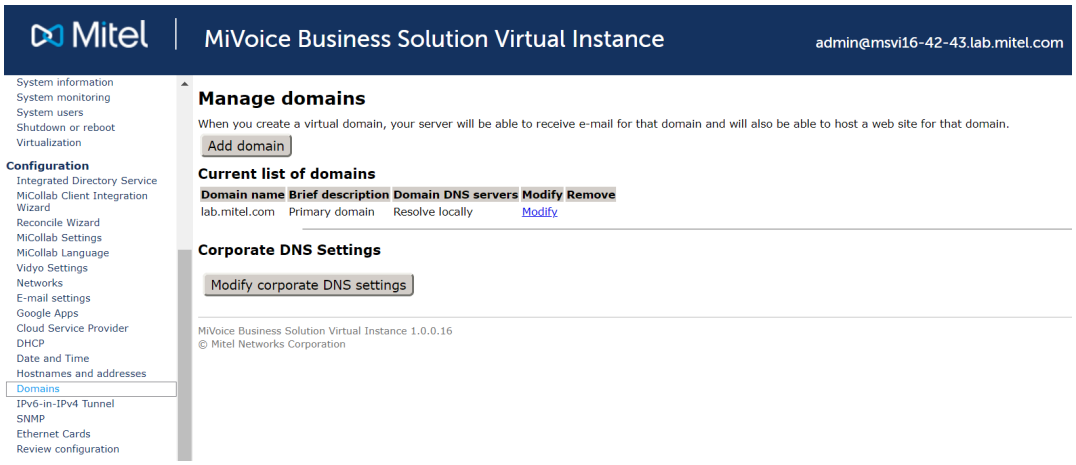
If a corporate DNS service is configured, the FQDNs must be provisioned in the corporate DNS. The user would have made the decision of using corporate or local DNS server in the step 18 of Add 2nd IP address to default LAN interface.

It is mandatory to provision an alias for the MiCollab application against the 2nd IP address of default LAN.

It is recommended to provision an alias for the MBG application against the 2nd IP address of default LAN.

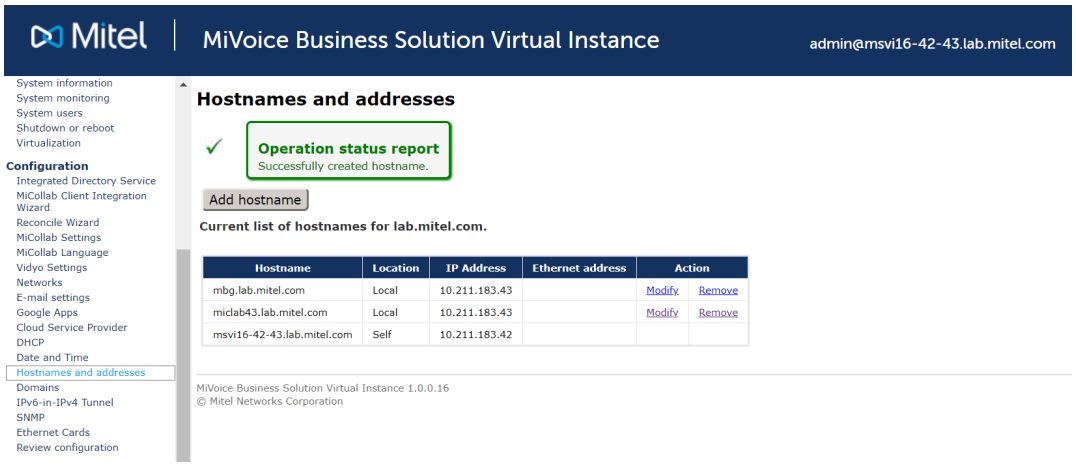
To provision FQDN in the MSL server's (local) DNS, follow the instructions below:

1. Login to MiVoice Business Solution Virtual Instance server manager.
2. To check if the Corporate DNS is set, navigate to **Configuration** > **Domains**. If set, remove it and proceed to next step.



3. Navigate to **Configuration** > **Hostnames and addresses**.
4. Click **Add hostname**.
5. Enter **Hostname**. Hostname must be a unique.
6. Select **Domain** from the drop-down list.
7. Select **Local** from **Location** drop-down list.
8. Click **Next**.
9. Enter 2nd IP address on default LAN in the **Local IP** field.
10. Click **Next**.
11. Click **Add**.

12. To add one more FQDN, perform Step 1 to Step 10.

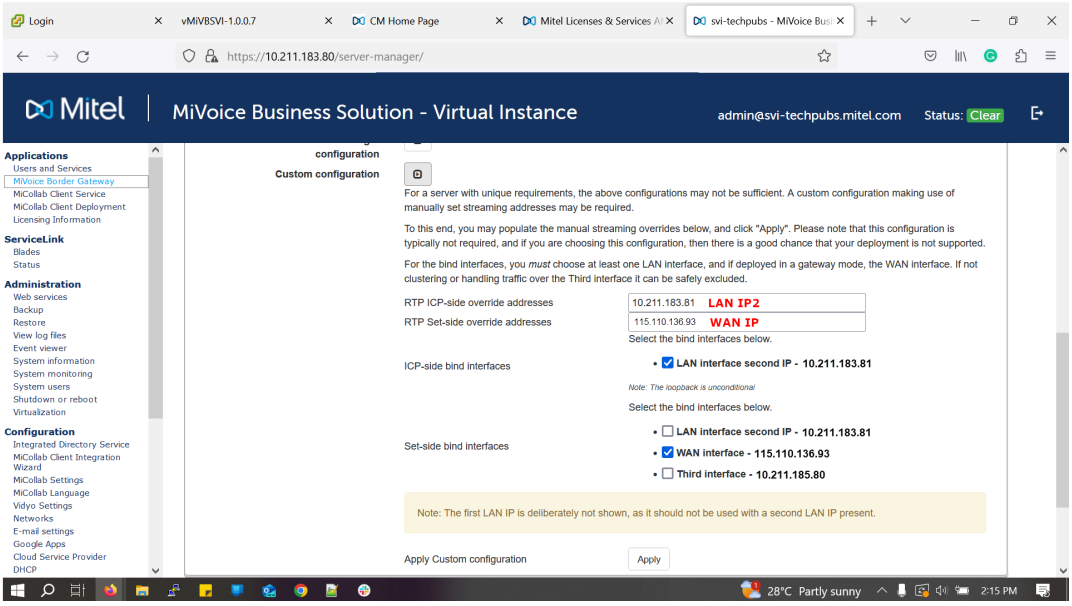


6.4 Configure MBG

Server-gateway mode

Set MBG profile to custom configuration by navigating to **Applications** > **MiVoice Border Gateway**. Then click **Network** > **Profiles**.

The following image shows **custom configuration** for **server-gateway mode** deployment:



Server-only mode

- **RTP Set-side override addresses** is set to the IP address associated with **LAN interface second IP - <IP address>** (LAN 1 and IP 2).
- In **Set-side bind interface**, select **LAN interface second IP - <IP address>** (2nd IP on default LAN interface) checkbox.

External MBG

Following configuration is applicable only if an external MBG is being (or has been) deployed (that is, admin is using the bastion host deployment).

- Create an MBG cluster that includes both the MiVoice Business Solution Virtual Instance MBG and external MBG.
- The MBG within MiVoice Business Solution Virtual Instance must have a Cluster weight of 0 and the external MBG must have a Cluster weight of 100 set.

Changing Cluster Node's IP Address

MBG clustering uses IP addresses to identify each node and to initiate cluster communications connections.

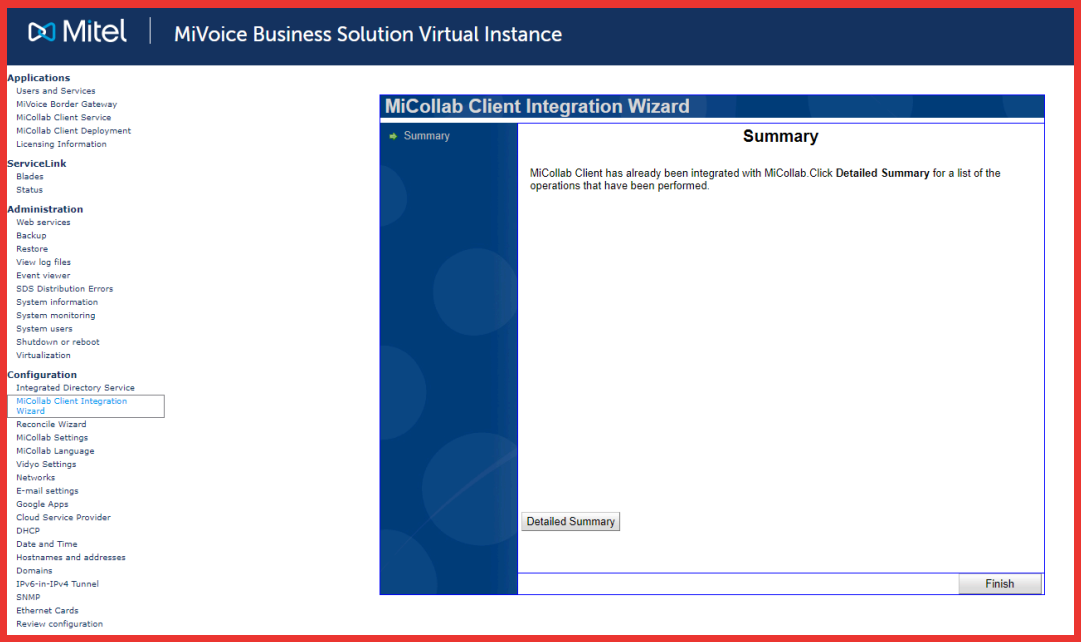
To change node's IP address, follow the procedure below:

1. Navigate to **Applications** > **MiVoice Border Gateway**.
2. Under **Clustering status**, make sure that the node to be changed is not the master node. Take ownership from another node if required.
3. From the slave node to be changed, select **Clustering** tab and click **Leave cluster**.
4. In MSL console, pre-configure the address and follow the prompts to reboot.
5. Add the node on the master, and join the server to the cluster.

6.5 Configure MiVoice Business

Mitel® MiVoice Business is the brand name of the call-processing software that runs on several hardware platforms including industry-standard servers, virtual machines, and MiVoice Business Applications purpose-built hardware.

Warning:
Do not proceed with configurations until MiCollab Client Integration Wizard (MCIW) has run successfully.



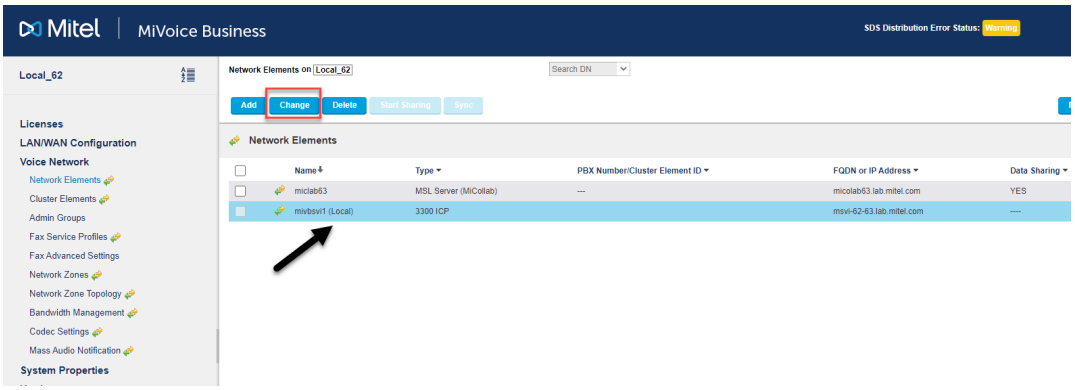
The following options are available to configure MiVoice Business:

- Restore a templated database via ESM.
- Export/Import database forms from another system.
- Manual configuration.

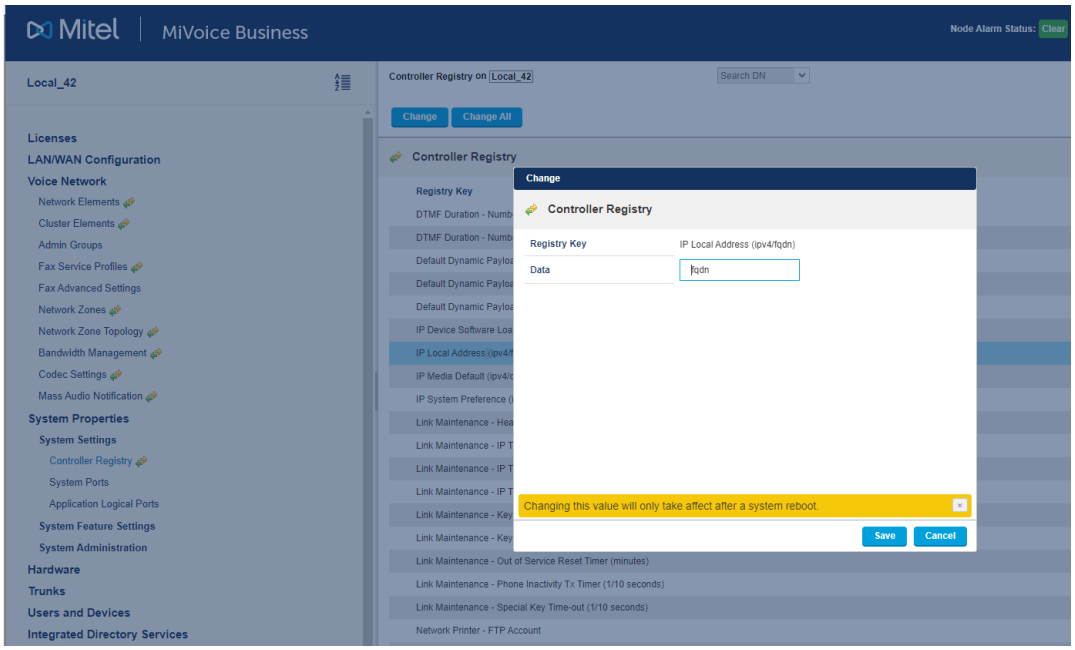
Manual configuration

1. Log into the ESM after changing the default password.
2. Navigate to **System Properties**> **System Feature Settings** > **System Options**.
3. Click **Change**. Enter **Email - sender's Address** and **Email Server**. Click **Save**.
4. Navigate to **Voice mail** and configure Embedded Voice Email.

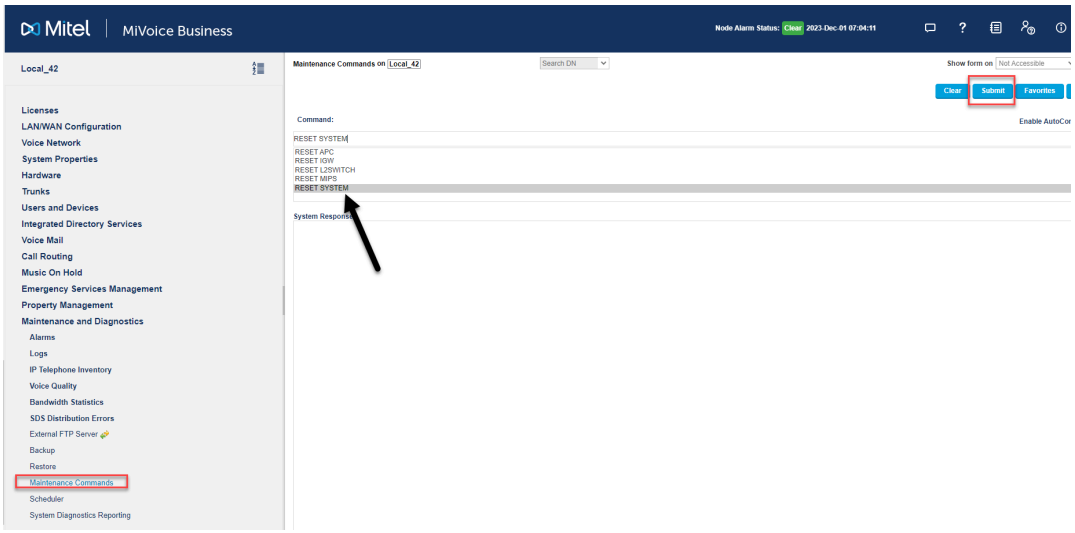
5. (Optional) Modify existing MiVoice Business network element **Name** to a more meaningful text by selecting the network element and clicking **Change**.



6. Navigate to **System Properties** > **System Settings** > **Controller Registry**.
7. Select **IP Local Address (ipv4/fqdn)** and change the entry from ipv4 to fqdn.



8. Reboot MiVoice Business to apply the FQDN change.



9. Configure MiCollab Network Element:

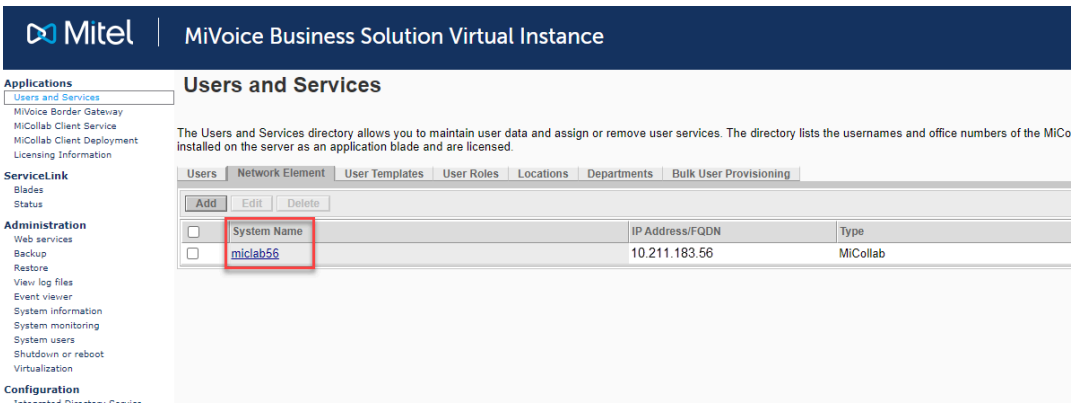
> **Note**:
> It is important to have MiCollab's network element name same as MiCollab system name

a. To find MiCollab system name[3], login to MiCollab server.

b. Navigate to **Applications** > **Users and Services**. Select **Network Element** tab.

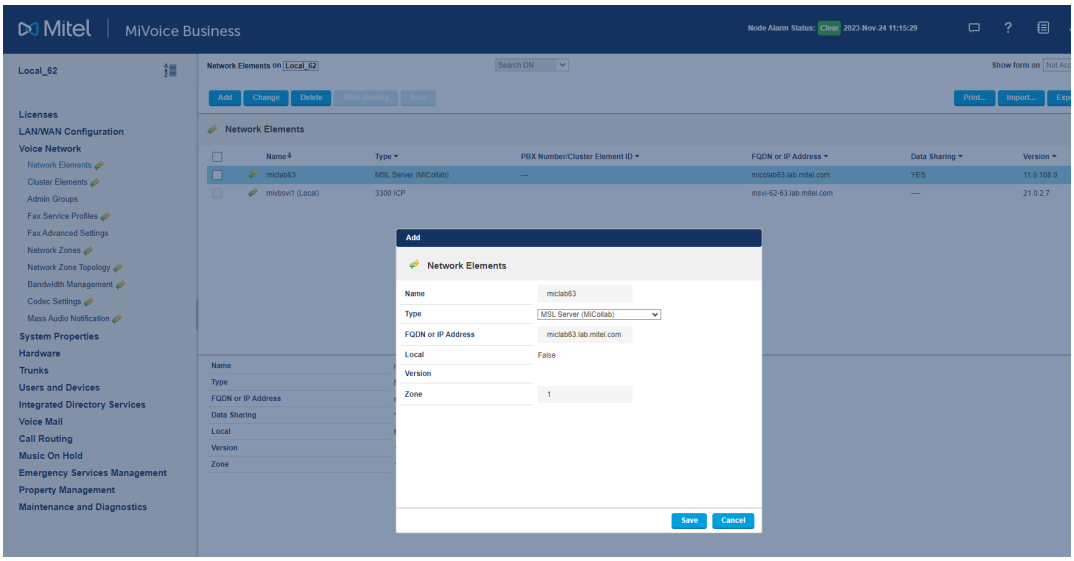
[3] System name is derived from hostname part of MiCollab FQDN (after doing DNS reverse lookup on the MiCollab IP (2nd LAN IP). If system name is not derivable due to DNS failures (non-configured, DNS reverse lookup issues, network errors etc), it is derived as miclab<lastIPOctet> where lastIPOctet is the last octet of the MiCollab IP (2nd LAN IP address). For example: If MiCollab IP address is 10.112.85.34, the system name is derived as miclab34. It can be changed by the administrators from the *MiCollab Network Element* form and from the MiVoice Business Network Element form (when servers are sharing data with each other). This system name is used in data sharing between MiCollab and MiVoice Business through system data synchronization, changing this will not change any other settings on MiCollab.

Note:
Navigate to **Configuration** > **MiCollab Client Integration Wizard** to confirm if MCIW has run successfully. **If it has not run, then it should be run manually**. Note that the 2nd LAN IP address must be configured Add 2nd IP address to default LAN interface on page 71 and the server must be licensed Configure MSL Server on page 80 prior to running the wizard.



c. After ESM reboot from Step 8, login again to ESM and navigate to **Voice Network** > **Network Elements**. Click **Add** to add a network element for MiCollab. Enter the details. For example: Enter **Name** as derived from previous step and select **Type** as **MSL Server (MiCollab)**, and enter MiCollab FQDN in the **FQDN or IP Address** field.

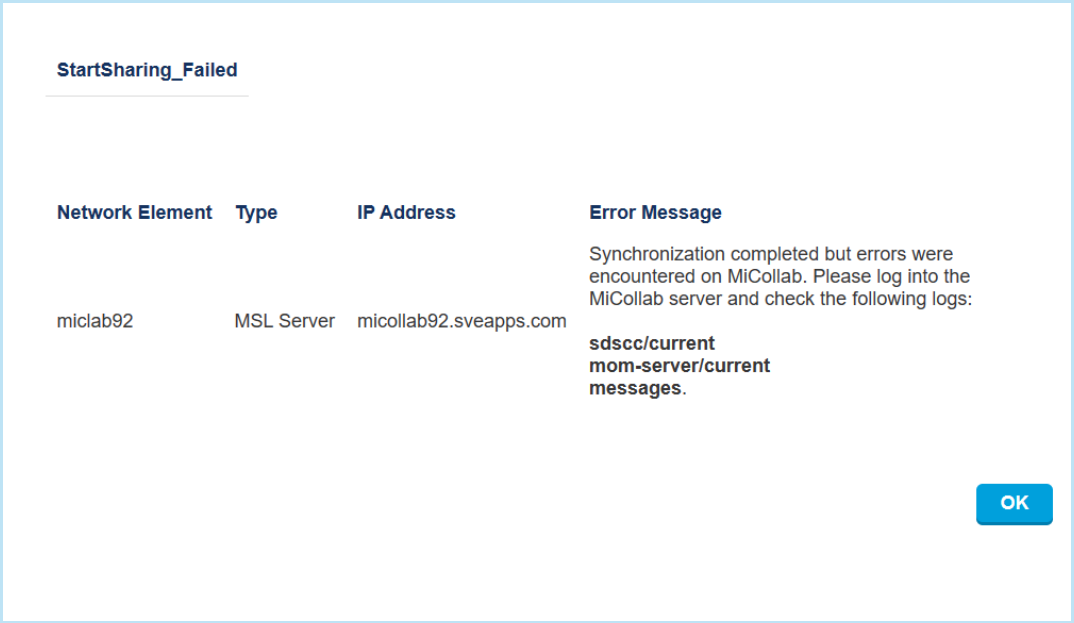
Note:
Using FQDN is recommended for this solution.



d. Click **Save**.

10. Select the newly created network element. Click **Start Sharing** and follow the instructions.

Note:
If sharing fails in mid-execution, click **OK** and perform Sync operation as mentioned in Step 11.



11. Perform **Sync** of MiCollab network element, if not already done.

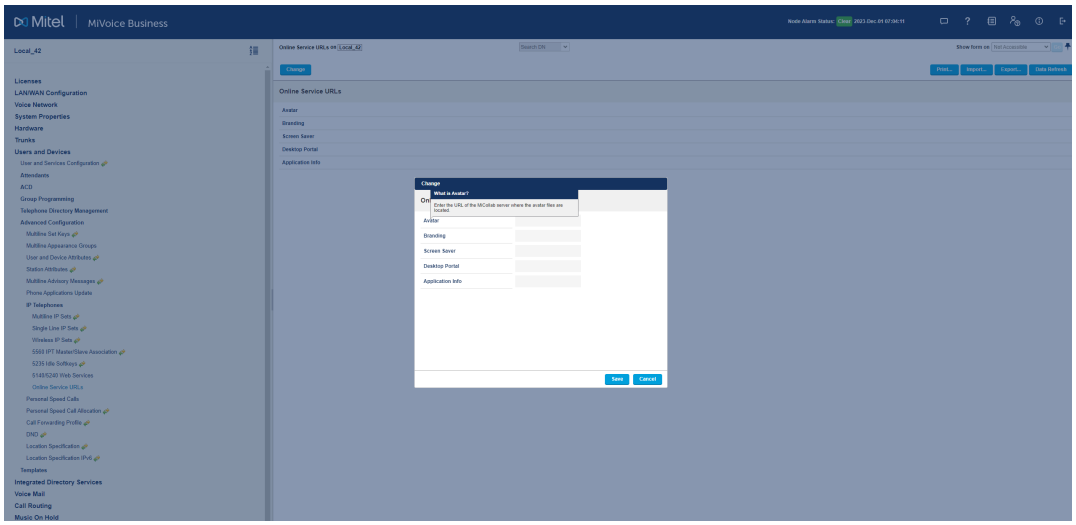
Once the manual configuration is completed, refresh the server manager, and proceed to Configure MiCollab to begin the process of reconciliation.

To enable Avatars

To enable Avatars, configure the Avatar URL by following the procedure below:

1. Login to MiVoice Business ESM.
2. Navigate to **Users and Devices** > **Advanced Configuration** > **IP Telephones** > **Online Service URLs**.
3. Click **Change**.

4. In the **Avatar** filed, enter the URL of the MiCollab server or MiVoice Business server where the avatar files are located.



5. Click **Save**.

For more information, refer MiVoice Business.

6.6 Configure MiCollab

To configure MiCollab, follow the guidelines below:

Note:
"MiCollab Client Integration Wizard" is run automatically. It may take at least five minutes since both the 2nd LAN IP was configured in Add 2nd IP address to default LAN interface and the server has been licensed in Configure MSL Server.

- If prompted to run the reconcile wizard in step 10 and step 11 in Configure MiVoice Business section, the reconcile wizard can be run.
- SMTP Server Configuration for MiCollab Client Welcome email.
- Web Server Certificates – Let's Encrypt or wildcard certificate.
- The MiCollab should not be configured on a resilient MiVoice Business Solution Virtual Instance.

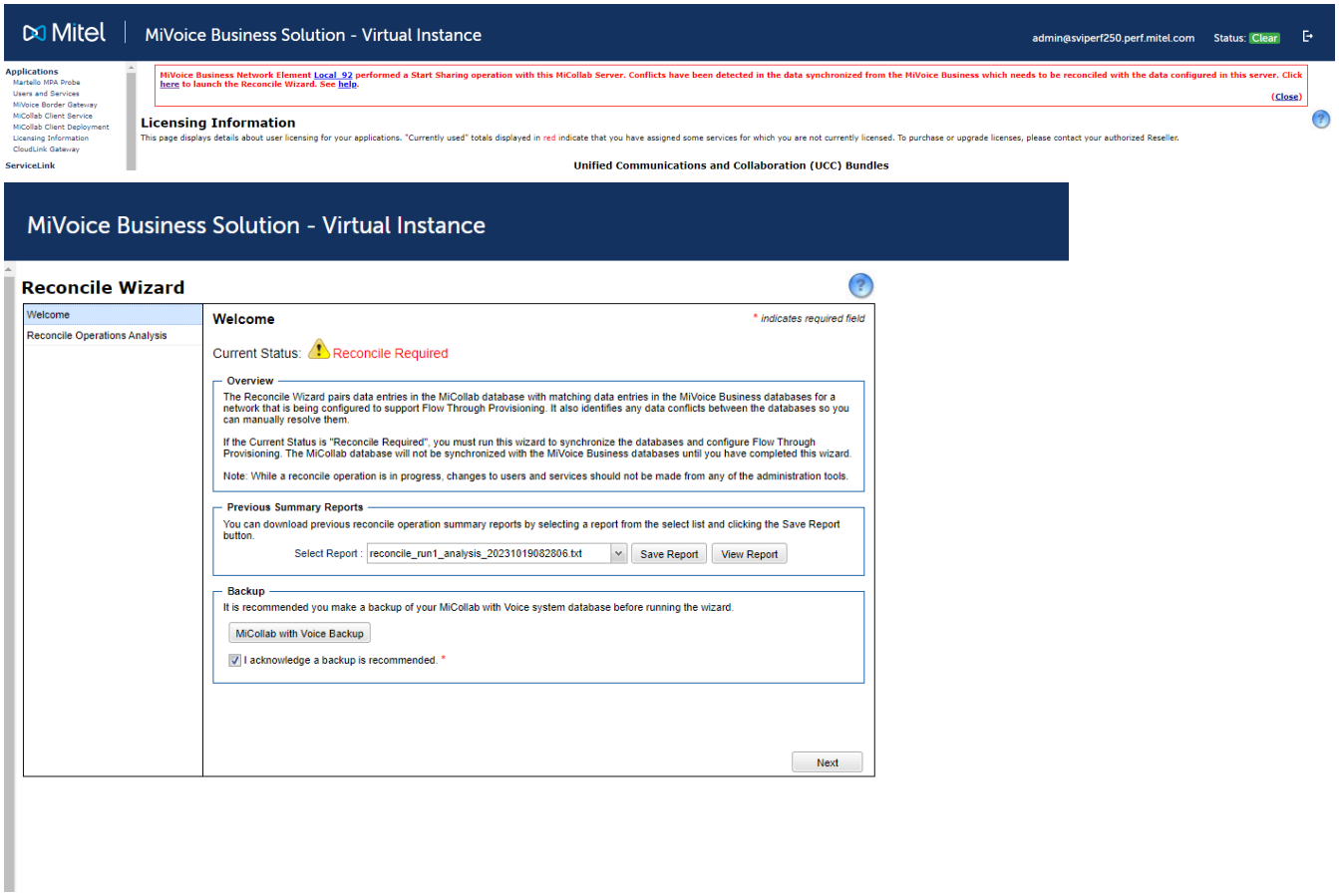
  For more information, refer Server Gateway with Resiliency section.

Note:
IP or FQDN/server-manager redirects to MiVoice Business Solution Virtual Instance server manager page.

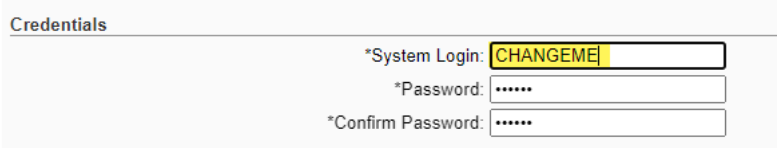
Note:
IP or FQDN without server-manager link redirects to MiVoice Business ESM login page (for example: mivbsvi.example.com/server-manager to be used)

Manual Configuration

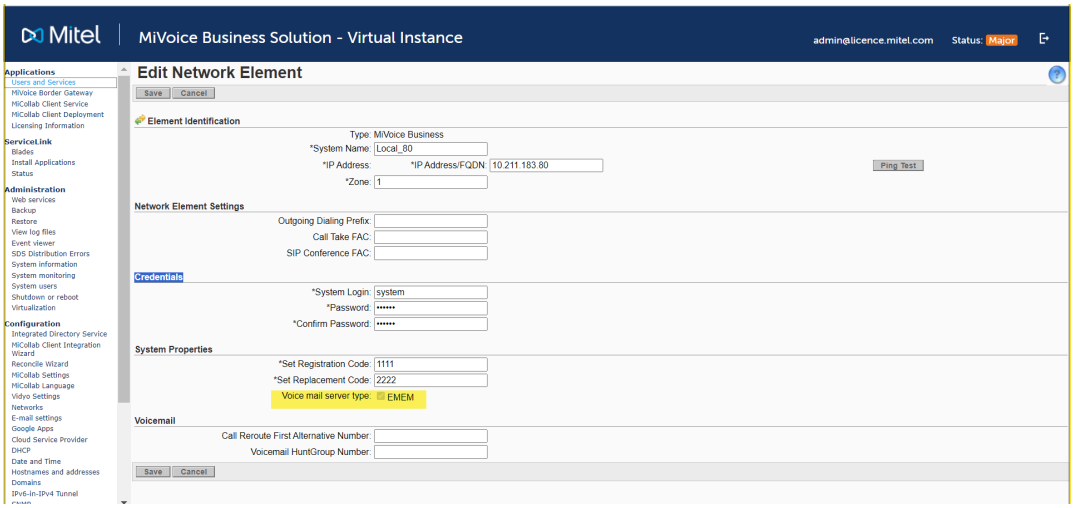
1. Log into the MiCollab server manager.



2. Navigate to **Configuration** > **Reconcile Wizard** and follow the instructions.
3. Navigate to **Applications** > **Users and Services**.
4. Select **Network Element** tab. Click entry for MiVoice Business.
5. Under **Credentials**, change the **System Login** and the **Password** as configured in MiVoice Business ESM portal.



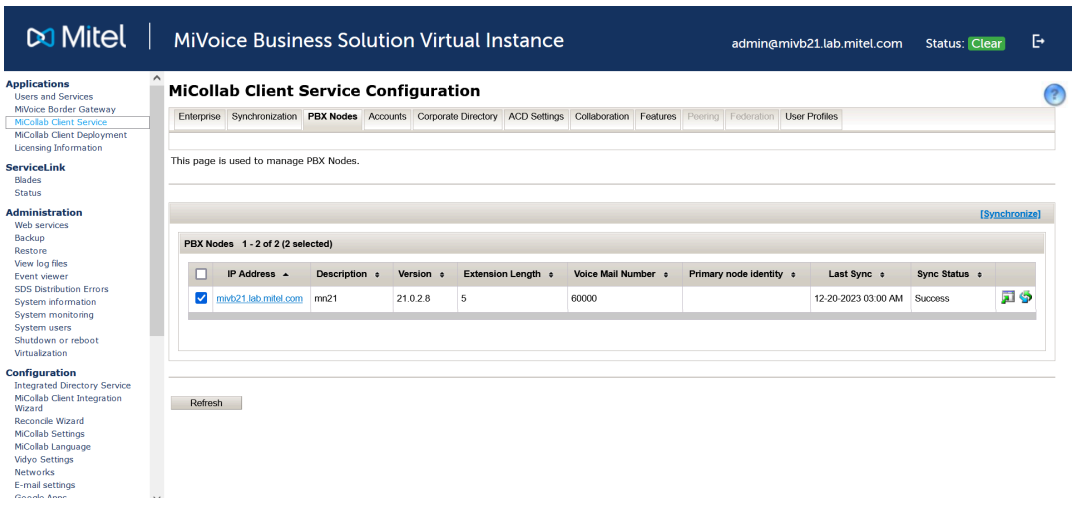
6. Under **System Properties**, in **Voice mail server type**, enable **EMEM** checkbox for voicemail and click **Save**.



7. Navigate to **Applications** > **MiCollab Client Service**.
8. Under **Configuration**, click **Configure MiCollab Client Service**.

> **Note**:
> The **Reach Through** option is not available for the MiVoice Business Solution Virtual Instance deployment.

9. Select **PBX Nodes** tab. Select the required checkbox(s) and click **[Synchronize]**.



10. Click **Refresh** to check the current synchronization status if it is "In Progress", "Failed", or "Success".

Configure MiCollab Client Deployment

For MiCollab (UCA) host name configuration, refer MiCollab Client Deployment.

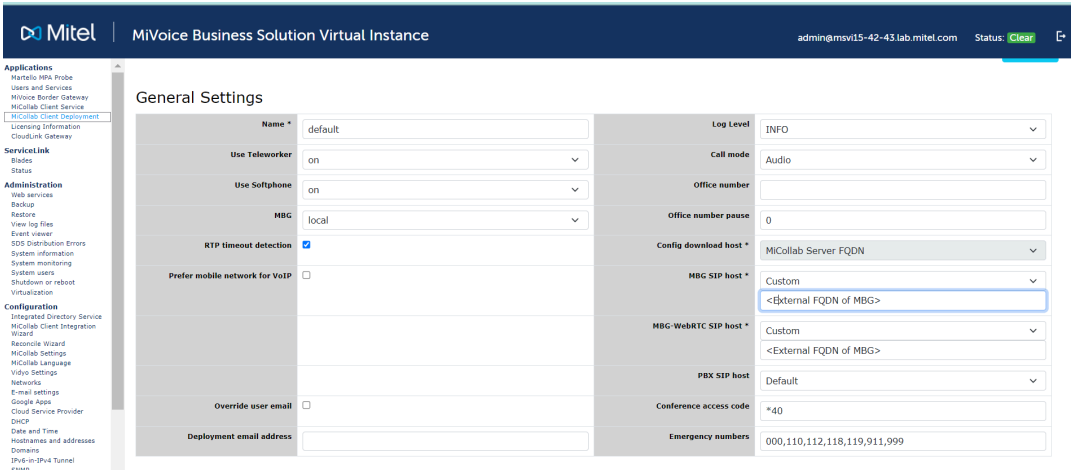
To configure MiCollab client deployment with MiVoice Business Solution Virtual Instance:

1. Log into the MiCollab server manager.
2. Under **Applications**, click **MiCollab Client Deployment**.

- Select **Configuration** tab and click **System**. Enter MiCollab FQDN in the **Override MiCollab (UCA) host name** field and click **Save**.

- Configure the Deployment Profile by selecting the deployment from **MBG SIP host** and **MBG-WebRTC SIP host** drop-down list. If the deployment is Server Gateway or Server Only DMZ, select MBG FQDN from the drop-down list. If the deployment is Server Only with Bastion Host MBG, select Custom from the drop-down list.

Note:
MBG FQDN must be the external FQDN of MBG, which is associated with the 2nd IP address on LAN and the WAN interface for public DNS resolution (that is split DNS).



3. Add the MiCollab Client for Mobile softphone user through the Users and Services application:

   - Log into the MiCollab server manager.
   - Under **Applications**, click **Users and Services**.
   - Click **Quick Add**.
   - Select the default UCC (Vx.0) Premium role or create a custom role and template from the Premium template. The template must have a Teleworker license and the MiCollab Client Feature Profile must be licensed for Mobile SIP Softphone.

   Note:
   The user will be deployed with the default deployment profile. If you want to use a custom default profile, create a custom template from the Premium template and select the desired profile in the template

   - Enter the user's first and last name (Enter the same user name that you programmed for the user's SIP device in the MiVoice Border Gateway).
   - Enter the user's primary email address.
   - Under **Other Phone**, enter the same extension number that you entered for the user in the MiVoice Business Gateway.
   - In the **SIP Password** and the **Confirm SIP Password** fields, enter the Icp-side password that you configured on the MiVoice Business Gateway.
   - Click **Save**.

     The user downloads the client from the store and scans the code in the deployment e-mail with their cell phone to initiate activation. The MiCollab for Mobile Client deployment configuration is downloaded to the user's cell phone.

6.7 Configure Optional Standalone vMBGs

You can deploy and configure separate optional standalone vMBGs to

- support Secure Recording Connector for phones on the LAN, or
- aggregate (collect) SIP trunks from a SIP service provider for distribution among multiple MiVoice Business Solution Virtual Instance systems.

See the MiVoice Border Gateway Installation and Maintenance Guide on the Documentation Center for installation instructions.

6.7.1 Secure Recording Connector Support

MBG provides a secure recording connector (SRC) service that allows third-party Call Recording Equipment (CRE) to record Mitel-encrypted voice streams. The SRC service is supported only in LAN only (Server-only) mode.

To support Secure Recording Connector for phones on the LAN, install the optional standalone vMBG in server-only mode on the LAN with no exposure to the Internet.

6.7.1.1 Deploy vMBG in Server-Gateway Mode

1. Access the MSL Server Console and select Configure this server.
2. In Local Networking Parameters, enter the server's internal (LAN) IP address server or select the default.
3. In WAN Network Adapters, select the server's external (WAN) adapter.
4. The external (WAN) address MUST be:

   - dedicated to the MBG Solution
   - publicly routable
   - reachable from the Internet and the internal network (that is, the server should not reside behind a NAT device).
5. Access the vMBG server manager.
6. On the **Configuration** tab, click **Network Profiles**.
7. Select **Server-gateway configuration** on the network edge.
8. Select **Apply Server-Gateway configuration**.

When configuration is complete, the system programs the Real Time Protocol (RTP) streaming addresses as follows:

- ICP-side (MiVoice Business Solution Virtual Instance-side) streaming address = LAN interface address
- Set-side streaming address = WAN interface address

Note:

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

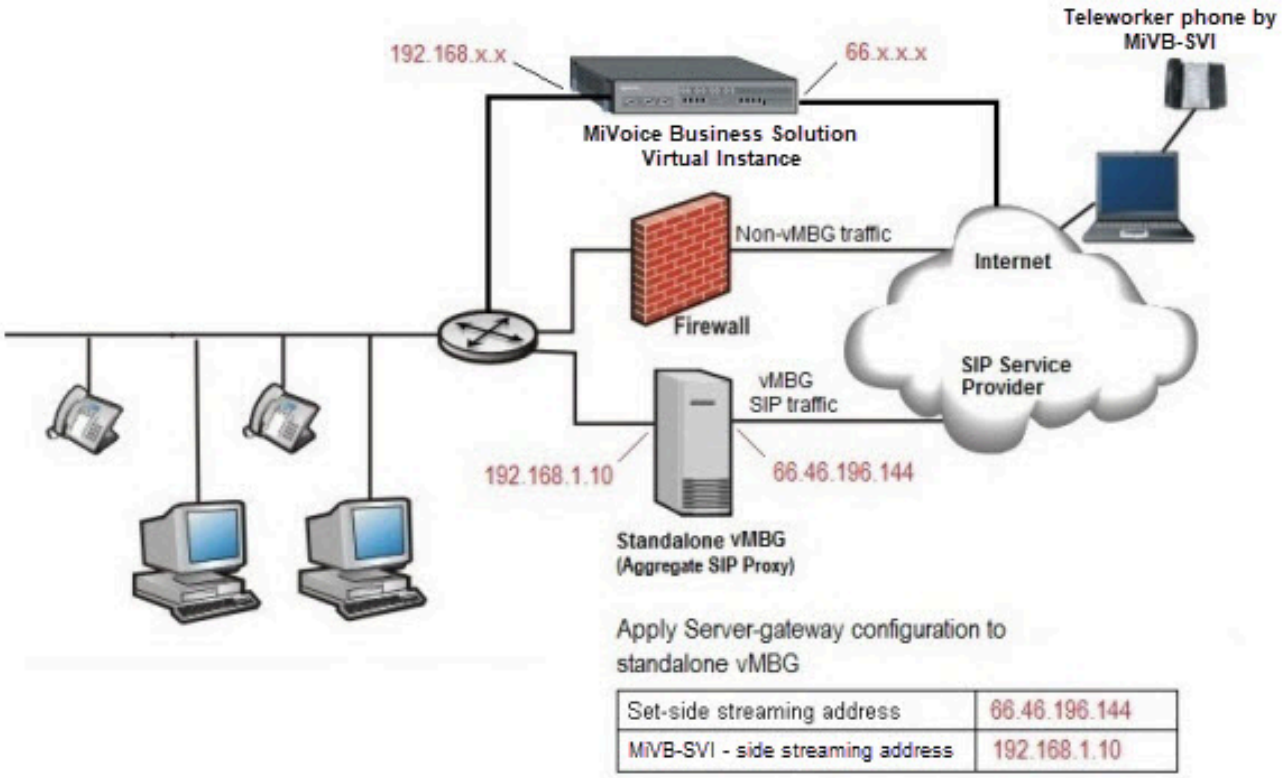


Figure 18: Standalone vMBG for SIP Trunk Aggregation

6.7.1.2 Configure Secure Recording Connector

Refer to the MBG online help for instructions on how to configure SRC.

6.7.2 SIP Trunk Aggregation

If your hosted infrastructure has multiple MiVoice Business Solution Virtual Instance systems, it is possible to reduce SIP trunking costs by purchasing the trunks in bulk and then aggregating (consolidating) the trunks on a separate standalone vMBG. The SIP trunks can then be distributed among the MiVoice Business Solution Virtual Instance systems via the vMBG SIP Trunking web proxy services.

To support SIP trunk aggregation, the vMBG is deployed in Network Edge (Server-gateway) mode. In this configuration mode, the server functions a firewall/Internet gateway with two Ethernet interfaces. One interface is connected to the external network (Internet) while the other is connected to the internal network. The firewall provided by the standalone vMBG server is not configurable. All default data traffic initiated inside the network is allowed while data traffic initiated outside the network is denied.

6.7.2.1 Deploy vMBG in Server-Gateway Mode

1. Access the MSL Server Console and select Configure this server.

2. In Local Networking Parameters, enter the server's internal (LAN) IP address server or select the default.
3. In WAN Network Adapters, select the server's external (WAN) adapter.
4. The external (WAN) address MUST be:

   - dedicated to the MBG Solution
   - publicly routable
   - reachable from the Internet and the internal network (that is, the server should not reside behind a NAT device).
5. Access the vMBG server manager.
6. On the **Configuration** tab, click **Network Profiles**.
7. Select **Server-gateway configuration** on the network edge.
8. Select **Apply Server-Gateway configuration**.

When configuration is complete, the system programs the Real Time Protocol (RTP) streaming addresses as follows:

- ICP-side (MiVoice Business Solution Virtual Instance-side) streaming address = LAN interface address
- Set-side streaming address = WAN interface address

Note:

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

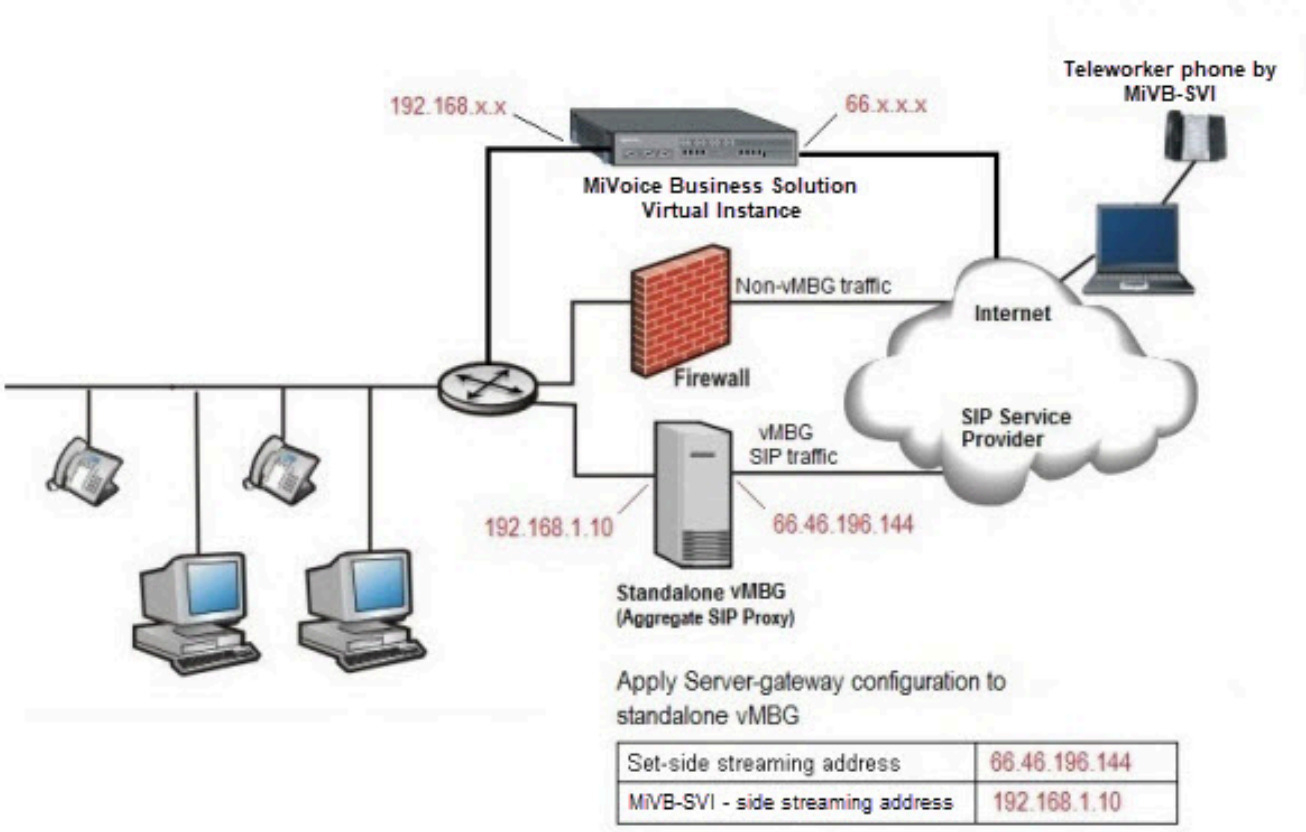


Figure 19: Standalone vMBG for SIP Trunk Aggregation

6.8 Configure CloudLink Gateway (optional)

CloudLink Gateway is a technology that connects premise-based PBXs to the CloudLink platform and CloudLink applications. For more information on how to configure, refer the CloudLink Gateway document.

6.9 Configure Mitel Performance Analytics (optional)

Provides instructions for installing a new Mitel Performance Analytics (MPA) monitoring system as well as its operations. For more information on configuring, refer section *PROBE MSL BLADE INSTALLATION* in Mitel Performance Analytics Probe Installation and Configuration Guide.

Note:
Ping Gadget appears empty when all values are less than 0.1 ms.

6.10 Provision Users

Depending on your site configuration, use one of the following methods to provision users on the MiVoice Business Solution Virtual Instance.

- **Import user data from a CSV file**: If a MiVoice Business Solution Virtual Instance is replacing an existing PBX system, export a CSV file of the user data and then import the CSV file using the Bulk Provisioning Tool. During the import, you can apply roles and templates to provision the users with phone services and applications.
- **Sync user database with directory service**: If the site uses Active Directory and if the directory server contains an accurate, up-to-date list of users, synchronize the MiVoice Business Solution Virtual Instance database with the Active Directory database.
- **Manually provision users**: If this is a new site without an existing user database, you can provision users manually from the Users and Services application.
- **User provisioning from Mitel Administration**: You can create new users or modify the role of an existing user from Mitel Administration.

Note:

You can reduce the time spent provisioning by applying roles and templates. Roles and templates allow you to add phone services and applications to the users. Default roles and templates are available.

6.10.1 Import User Data From a CSV File

To import user data from a CSV file:

1. Export a CSV file of user data from the existing PBX system.
2. Log into the MiCollab server manager portal.
3. Under **Applications**, click **Users and Services**.
4. Roles and templates during user provisioning Templates during user provisioning From the Users and Services application, define roles and user templates. Refer the topic *Manage Roles and Templates* in the MiCollab Users and Services Provisioning USP document for instructions.
5. Import users. Refer the topic *Bulk Import from Files* in the MiCollab Users and Services Provisioning USP document for instructions.
6. Assign the UCC licenses to users through the Users and Services application. Refer the topic *Manage UCC Licensing Bundles* in the MiCollab Users and Services Provisioning USP document for instructions.

6.10.1.1 Sync User Database with Active Directory Service

To sync the user database with an Active Directory server:

1. Log into the MiCollab server manager portal.
2. Under **Applications**, click **Users and Services**.
3. From the Users and Services application, define roles and templates. See the Manage Roles and Templates book in the USP application online help for instructions. You have the option of using the default roles and templates provided by the system.
4. Sync the databases by performing an initial synchronization.
5. Resolve any detained or failed updates.

6.10.1.2 Provision Users Manually

To provision users manually:

1. Log into the MiCollab server manager portal.
2. Navigate to **Applications** > **Users and Services**.
3. From the Users and Services application, create the users and assign services. Refer the topic *Manage Roles and Templates* in the MiCollab Users and Services Provisioning USP document for instructions.
4. Sync the databases. Refer the topic *Perform an Initial IDS Synchronization* in the MiCollab Users and Services Provisioning USP document for instructions.
5. Resolve any detained or failed updates. Refer the topic *Managing Detained and Failed IDS Operations* in the MiCollab Users and Services Provisioning USP document for instructions.

6.10.1.3 Provisioning DID for Users (Overview)

This section provides an explanation of how DIDs are provisioned for MiVoice Business Solution Virtual Instance users:

1. The system administrator uses the MiCollab Flow Through Provisioning to configure users. The Bulk User Interface can also be used to import users from a CSV file.
2. The system administrator is allowed to configure a specific DID per user and whether or not this DID number should be published to the public network for all outgoing calls. This DID number has an association with the Primary DN.
3. MiCollab Flow Through Provisioning provisions the user's primary DN and DID Service Number into the User and Services Configuration form of the MiVoice Business.
4. The system propagates the DID configuration data from the User and Services Configuration form to the appropriate MiVoice Business sub-forms: Associated Directory Number and Direct Inward Dialing Service.

6.11 Perform Backups

After you complete MiVoice Business Solution Virtual Instance advanced configuration, perform the following backups:

- Backup the MiVoice Business Solution Virtual Instance database (see Server Manager Backup)
- For deployments in a VMware environment, backup the MiVoice Business Solution Virtual Instance using VMware Applications.

- Backup the optional vMBG. Refer to the vMBG server manager online help for instructions.

Maintenance 7

This chapter contains the following sections:

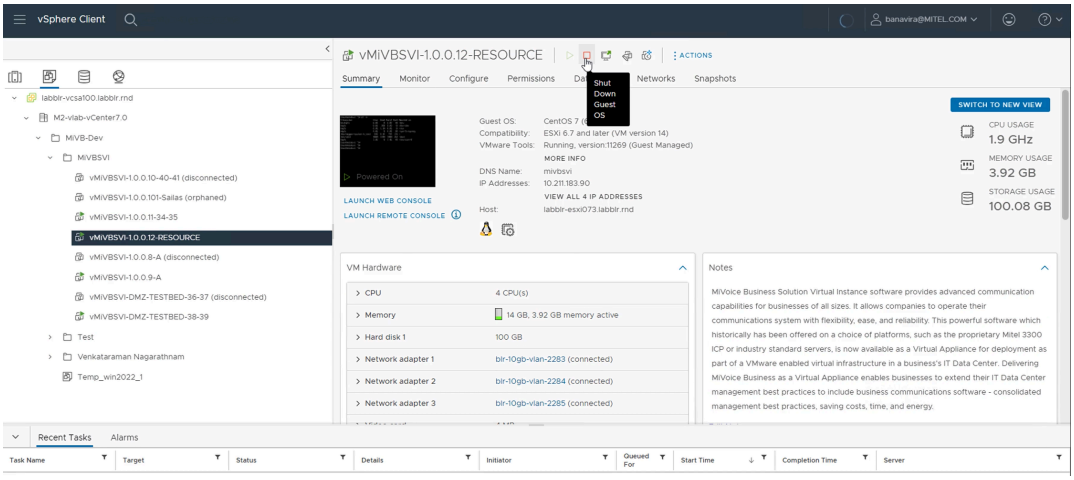
Regular maintenance tasks include:

7.1 Change of resource profile

To manually update the resource profile from 250 users to 500 users allocated to the VM to support, follow the procedure below:

1. Power-down the MiVoice Business Solution Virtual Instance VM:

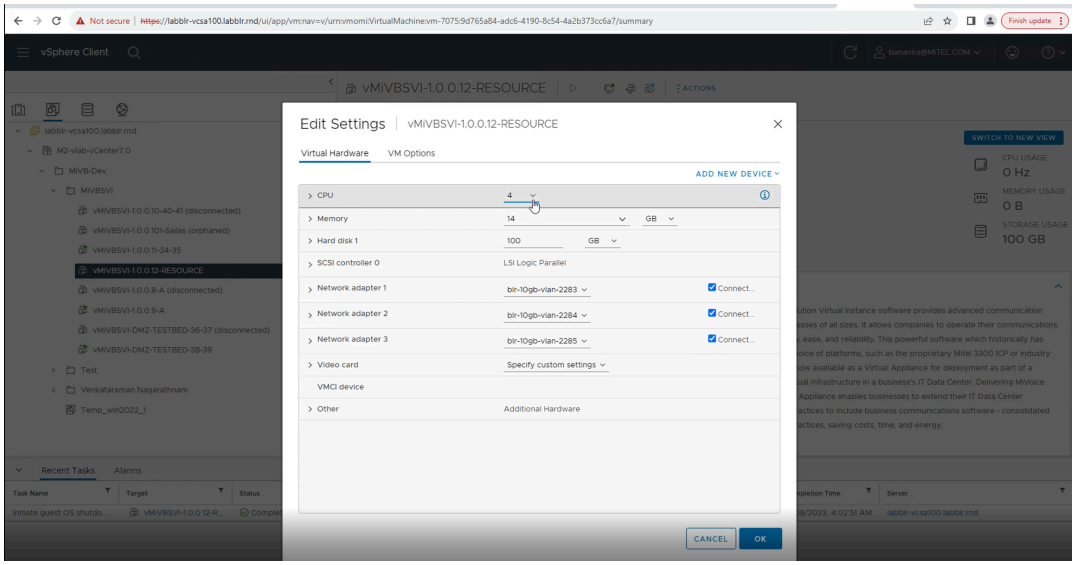
   - In vSphere, navigate to the resource.
   - Click **Launch Console**. Select **Web Console** and click **OK**.
   - In the Web Console, enter Mivbsvi credentials.
   - Run the command `df -h` and press enter.
   - In vSphere Client, click Shut Down.



   - Click **YES** in the confirmation box.

     The VM is powered off.

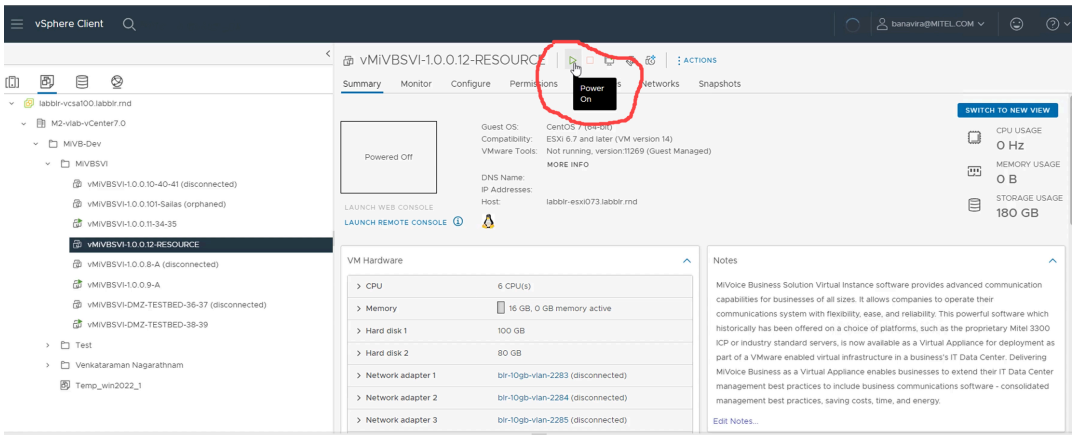
2. In **ACTIONS** drop-down list, select **Edit Settings**.



3. In **Edit Settings** page,

   - to increase vCPU count and the reservation value, expand **CPU**. Change the values of **CPU** from 4 to 6 and **Reservation** to 6000.
   - to increase memory and reservation value of memory, expand Memory, change the values of Memory to 12 GB and Reservation value to12288 MB.
   - Add a separate hard disk of size 80 GB (in addition to existing primary hard disk of size 100 GB). To add a secondary hard disk, click **ADD NEW DEVICE** and select **Hard Disk**.
   - Enter **New Hard disk** value as 80 GB and click **OK**.

4. Click Power On.



5. Once powered up, launch **Web Console**.

   - In **Application Record ID** window, press Enter.
   - Enter Mivbsvi credentials and run the command `df -h`.

6. MiVoice Business Solution Virtual Instance system makes use of LVM framework for volume management, which facilitates with seamlessly expanding the existing file system with this additional disk drive.

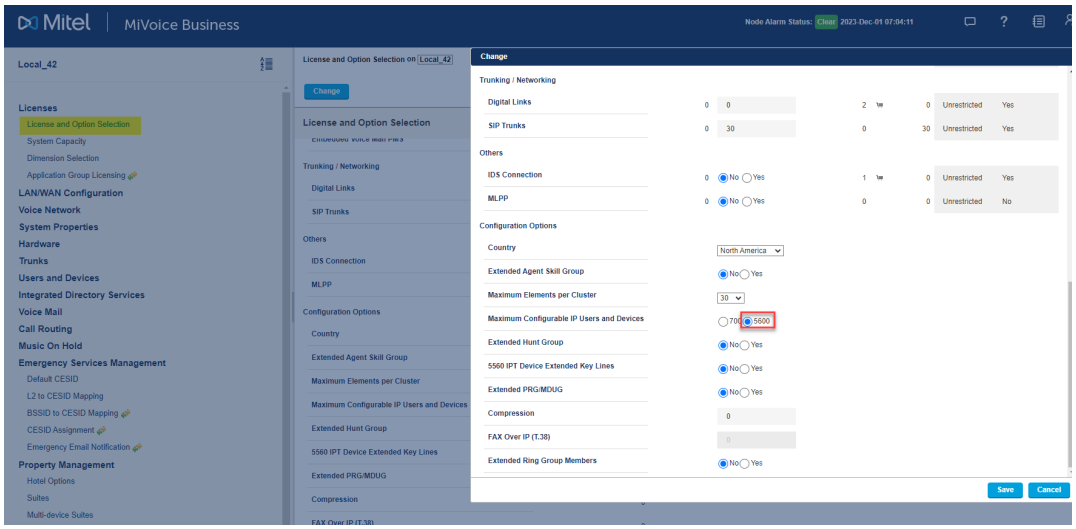
7.2 Increase the number of devices

For 250 users deployment, a maximum of 700 devices is supported by default.

To increase the number of supported devices, follow the procedure below:

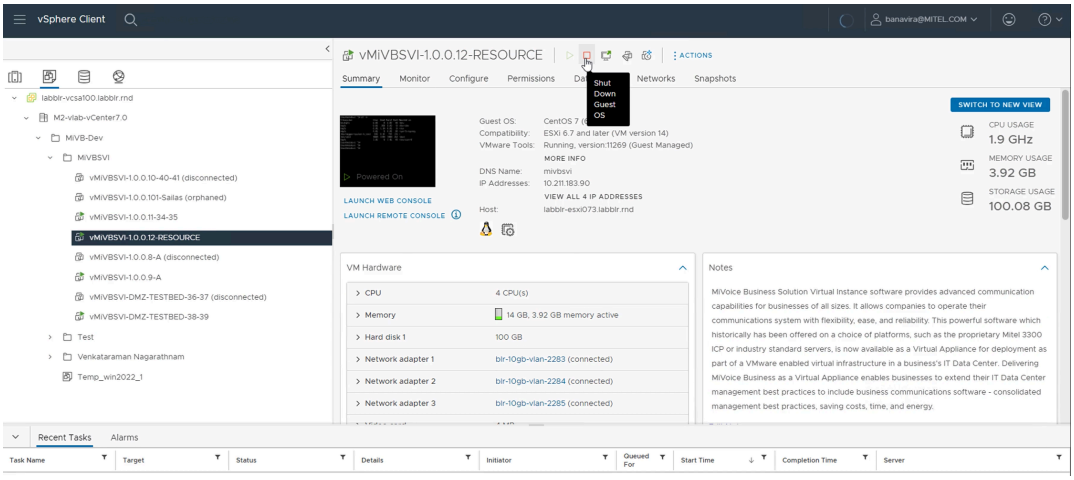
1. In MiVoice Business ESM portal, update the **Maximum Configurable IP Users and Devices** by navigating to **Licenses** > **License and Option Selection**.

2. Click **Change**. Select **5600** and click **Save**.



3. Power-down the MiVoice Business Solution Virtual Instance VM:

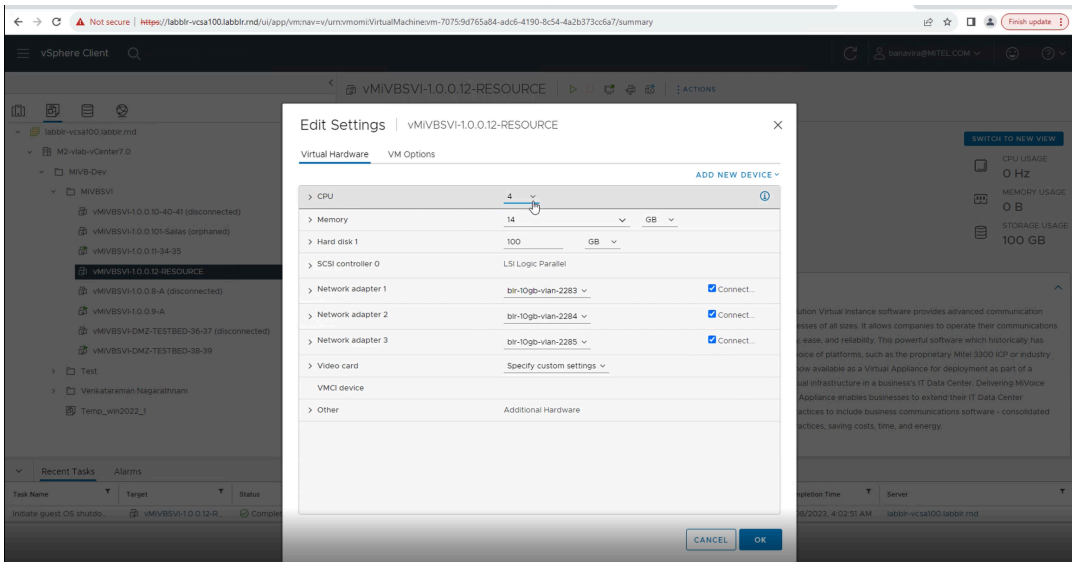
- In vSphere, navigate to the resource.
- Click **Launch Console**. Select **Web Console** and click **OK**.
- In the Web Console, enter Mivbsvi credentials.
- In vSphere Client, click Shut Down.



- Click **YES** in the confirmation box.

  The VM is powered off.

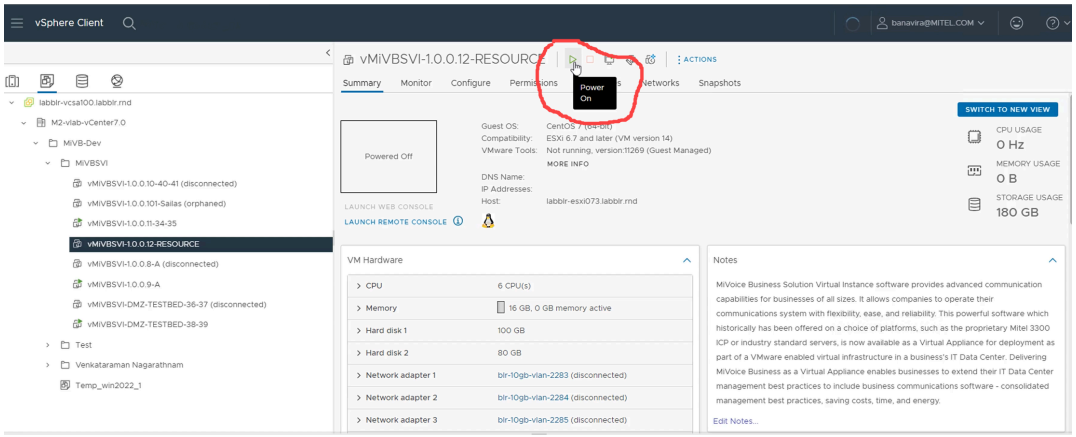
4. In **ACTIONS** drop-down list, select **Edit Settings**.



5. In **Edit Settings** page,

   - To increase memory and reservation value by 2GB, expand **Memory**, change the value of **Memory** to 12 GB and **Reservation** value to12288 MB.

6. Click Power On.



7.3 Adding UCC Licenses

To purchase UCC licenses:

1. Contact Mitel Customer Services (or your Service Provider) and place your order.
2. Obtain your Application Record ID from Mitel Customer Services.
3. In your AMC account, access the appropriate Application Record and assign the upgrade products from your license account to the Application Record. The AMC upgrades your licenses on its hourly synchronization.
4. Access the server manager.

5. Under **ServiceLink**, click **Status**.
6. Click the **Sync** button to download your AMC license upgrades. UCC licenses are applied automatically during the synchronization.

7.4 Performing Backups

There are two methods that you can use to back up system data (including all server configuration data, application configuration data, user settings, messages, and greetings):

- **Server Manager "Backup"**: allows you to perform backups of the MiVoice Business Solution Virtual Instance database (includes the application databases and the MiVoice Business system database) to a local desktop computer or schedule backups to a network file server.
- **VMware Applications**: allow you to back up the MiVoice Business Solution Virtual Instance OVA file.

Note:

1. You can use different filenames for server manager database backup files, but the filename must not contain spaces and the file extension must be TGZ. For example: "backup_file_Jan23.tgz"
2. If MiVoice Business Solution Virtual Instance is deployed in LAN only (server-only) mode with Teleworker running remotely on an vMBG in the DMZ, you should back up both the MiVoice Business Solution Virtual Instance database and the vMBG database at the same time.

7.4.1 Server Manager Backup

Backup to Desktop

Use this procedure to save your system backup to a file or device on your desktop computer or maintenance PC.

A **Backup to desktop** operation saves all of the data to a single, large compressed file and is therefore limited by the maximum file size of the client operating system. For example, if you are backing up data to a Windows client that uses the FAT file system (the default for many versions of Windows), you are limited to a maximum file size of 2 GB. Other file systems may have a larger limit. If the backup file exceeds the maximum file size of the client operating system, it cannot be properly restored.

1. Log into the Administrator portal (server manager). See Common_System_Administration_Tasks topic for instructions.
2. Under **Administration**, click **Backup**.
3. Select the **Backup** to desktop option.
4. Click **Perform**. MSL prepares the system for backup. The "Backup to desktop - Operation status report" screen is displayed with the estimated backup size.

5. To create an encrypted backup that is password protected, enter and confirm a password. Record the password. You cannot restore an encrypted backup without the password.
6. Ensure that your browser and target file system support downloads of this size, and click **Download Backup File**.
7. When prompted to Open or Save, click **Save**.
8. In the file download screen that appears:

   - Name the file and then select the location where the file will be saved. Note that the filename of the backup must not contain any spaces; otherwise, you will receive an error when you attempt to restore it.
   - Click **Save**.
   - In the **Download Complete Window**, click **Close**.
   - After saving, you can copy the backup file to a CD/DVD or USB storage device, if required.

7.4.2 Schedule Backups to Network File Server

Use this option to

- perform immediate system backups to a Network File Server
- schedule daily, weekly, or monthly system backups to a Network File Server.

Note:

You can only have one backup scheduled on the server. To cancel an existing backup schedule, select **Disabled** and then click **Update**.

Before you can perform network backups, you must create a shared folder on the Network File Server that allows network users to write to the folder. For example, to create a shared folder on a PC running Windows 11:

1. Right-click on the desktop and select **New** and then select **Folder**.
2. Name the folder, for example: "MiVoice Business Solution Virtual Instance Backups".
3. Right-click on the folder and select **Properties**.
4. Click the **Sharing** tab.
5. Click **Share**.
6. Select "Everyone" from the drop-down and click **Add**.
7. Set the **Permission level** to **Read/Write**.
8. Click **Share**.
9. Click **Done**.

Next, specify the Network File Server and shared folder in the MiCollab server manager interface:

1. Log into the MiCollab server manager.

2. Under **Administration**, click **Backup**.
3. From the **Select an action list**, click **Configure network backup**.
4. Click **Perform**.
5. Identify the server where the backup file will be stored.

   - Enter the **IP address** of the file server where the backup will be stored.
   - Enter the **Sharename** of the shared folder where the backup file will be stored. (For example, "MiVoice Business Solution Virtual Instance Backups".) You must set the permissions of the shared folder to allow network users to write files to the folder.
   - Enter an **Optional Sub Directory** for the backup file, if desired. The specified directory must exist in the share folder. The field accepts multi-level directories; for example "MiVoice Business Solution Virtual Instance/Sept/backups". If you leave this field blank, the system stores the file in the root directory of the specified network share.
   - Enter the **Username** to use when connecting to the backup server.
   - Enter the **Domain or Workgroup Name** of the server. (For example, mitel.com.)
   - Enter the **Password** to use when connecting to the backup server.
   - (Optional) Select the **Maximum number of backup files to keep**(1-999) on the server. When the number of stored files reaches this maximum count, the oldest version is deleted.
   - Click **Update**.

To perform an immediate backup

1. Click **Backup Now**.

To schedule backups to a network file server:

1. Under **Administration**, click **Backup**.
2. From the **Select an action** list, click **Configure network backup**.
3. Click **Perform**.
4. Select the frequency with which you want to perform backups. Backup file names will include timestamps, for example: mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz).

   - To disable regularly scheduled backups, click **Disabled**.
   - For Daily backups, select a time of day (hour, minute, AM/PM).
   - For Weekly backups, select a time of day, and day of the week.
   - For Monthly backups, select a time of day, and day of month.
5. Click **Save**.

7.5 Backups using VMware Applications

You can use VMware applications to create MiVoice Business Solution Virtual Instance backups to recover the system from database corruption or disaster situations. See the Virtual Appliance Deployment Guide for instructions.

7.6 Common System Administration Tasks

Logging into the server manager (Administrator Portal)

The MiVoice Business Solution Virtual Instance server manager is a web-based administrator portal that provides a central location for configuring the virtual appliance and system settings. This administrator portal web interface provides access to the

- Server Manager - allows you to configure and maintain the virtual appliance
- Application web pages Application Web Pages - allow you to configure and administer the installed applications.

Web browser access to MiVoice Business Solution Virtual Instance administration and end-user interfaces is provided through

- Chrome or Microsoft Edge
- Mozilla® FireFox® 41 or higher

Note:
On Microsoft Windows 8 with Internet Explorer 10, the Integrated Configuration Wizard is supported in compatibility mode only.

To log into server manager:

1. On a PC on the same subnet as the MiVoice Business Solution Virtual Instance server, open a browser and enter the following URL in the address bar:

   https://<IP Address of MiVoice Business Solution Virtual Instance>/server-manager.

   Note:

   If your client PC is on a different subnet than the MiVoice Business Solution Virtual Instance, you must add your trusted local network in Networks page of the Server Manager.

2. Enter User Name (default is "admin") and the system Password that you created during installation, and then click **Login**. The administrator portal opens.

3. Do one of the following:

   - In the left-hand menu, under **Applications**, click an application name to open the interface of that application.
   - Click the **Help** link in the administrator portal for detailed server administration instructions.

4. By default, MiCollab is configured to send a Welcome E-mail to new users. The e-mail contains:

   - the user's login ID, password
   - passcode

   See Configure Service Information Email in the MiCollab Administrator Online Help for the Service Information (Welcome) E-mail configuration options.

5. Proceed to Installing a Web Certificate.

7.7 Installing a Web Certificate

When users connect to their MiCollab Web Client (https://<Micollab FQDN/ucs/micollab) for the first time, they may get a warning message stating that there is a problem with the website's security certificate or that your browser has blocked the content. This message appears because the application web server is not recognized as a trusted site. Users can safely select the option to continue to the application web server site.

To prevent these security warnings from appearing

- Certificate root certificate installation Root CA certificate Mitel Root CA certificate install the Mitel Root CA certificate locally on each user's client PC, or
- Certificate authority Secure Sockets Layer purchase and install a Secure Sockets Layer (SSL) certificate from a third-party Let's Encrypt.

For instructions on how to install a third-party SSL certificate, refer to the Manage Web Server Certificate topic in the Server Manager Online Help for details.

- To prevent the Security Alert warning from appearing on client stations on the local network, purchase a Secure Sockets Layer (SSL) certificate for the MiVoice Business Solution Virtual Instance virtual appliance and then import it onto the MiVoice Business Solution Virtual Instance virtual appliance.
- To prevent the Security Alert warning from appearing on remote client stations, purchase a Secure Sockets Layer (SSL) certificate for the MBG Web Proxy server and then import it onto the MBG Web Proxy server.

7.8 Allow Trusted Network Access

If the users are deployed on a different subnet than the MiVoice Business Solution Virtual Instance, it is necessary to grant them access. First, you must configure them as a trusted local network and then grant them express permission.

To configure trusted networks:

1. Log into the MiVoice Business Solution Virtual Instance server manager.
2. Navigate to **Configuration** > **Networks** and then click **Add a new trusted network**.
3. Enter the **Network address** of the network to which you are granting access. (For example, 168.195.52.0).

Note:
When MiVoice Business Solution Virtual Instance is deployed in server-only mode, the following list of private address ranges are automatically added to the trusted networks.

- `10.0.0/8`
- `172.16.0.0/12`
- `192.168.0/16`

4. In the **Subnet mask or network prefix length** field, enter the dot-decimal subnet mask or CIDR network prefix to apply to the Network address. If this field is left blank, the system assigns a network prefix length of /24 for IPv4 networks or /64 for IPv6 networks. (For example, if your network IP address is 168.195.52.0 and you want to allow access to all network IP addresses in the range from 1 to 255, enter 255.255.255.0. This allows IP addresses 168.195.52.1 through 168.195.52.255 to access your server).
5. Enter the **Router**. (IP address of the router on your trusted local network).
6. Click **Add**.
7. Repeat steps 1 through 5 to configure additional trusted networks.

To grant secure shell access to the trusted network you have created:

1. Log into the the MiVoice Business Solution Virtual Instance server manager.
2. Navigate to **Security** > **Remote Access**.
3. In the **Secure Shell Access** field, select one of the following:
   - **No Access**: Select this option to restrict access to your own local network.
   - **Allow access only from trusted and remote management networks**: Select this option to allow access to selected trusted local networks (required if using Mitel Integrated Configuration Wizard) and remote management networks. This is the recommended setting.
   - **Allow Public access (entire Internet)**: Select this option to allow access to the entire Internet. This setting is selectable only if you have configured a strong SSH (admin) password. Its use is NOT recommended.
4. In the **Allow administrative command line access over secure shell** field, do one of the following:
   - Select **Yes** to allow users to connect to the virtual appliance and log in as root.
   - Select **No** to restrict users from logging in as root.
5. In the **Allow secure shell access using standard passwords** field, do one of the following:
   - Select **Yes** to allow users to connect to your virtual appliance using a standard password.
   - Select **No** to restrict virtual appliance access to users with RSA Authentication.
6. Click **Save**.

7.9 Upgrading of blades

- Blades can be upgraded from the blades panel.

Note:
It is recommended to take a backup before the blade upgrade

General recommended sequence for upgrading the blades is as follows:

1. ServiceLink (reboot of MiVoice Business Solution Virtual Instance is required after upgrading this blade)
2. Blade-MVF (Mitel Virtualization Framework)

3. MiVoice Business
4. Blade-SAS
5. Blade-MiCollab_Client_Service (UCA)
6. Client Deployment (CDU)
7. MiCollab PC-Client
8. MiCollab Web-Client
9. MiVoice Border Gateway(MBG)
10. MPA Probe (MarWatch Probe Blade)
11. Mitel CloudLink Gateway

Troubleshooting 8

This chapter contains the following sections:

To assist in troubleshooting, you can either view or download the log files generated by the services running on MiCollab.

To view/download the log files:

1. Under **Administration**, click **View log files**.
2. Under **View Log Files**, choose a log view. Most system services write their logs to the messages file.
3. Enter a **Filter Pattern** to view online the lines of the log that contain that text. This option applies only to viewed files. Check the **Regular expression** box if you want to apply the text filter in the format of a regular expression.

   A regular expression (abbreviated as regexp, regex, or regxp) is a string that describes or matches a set of strings, such as particular characters, words, or patterns of characters, according to certain syntax rules. A regular expression is written in a formal language that can be interpreted by a regular expression processor, a program that either serves as a parser generator or examines text and identifies parts that match the provided specification.
4. Specify a **Highlight Pattern** to mark in bold the specified text in any logs that the text appears. This option applies only to viewed files. Check the Regular expression box if you want to apply the text filter in the format of a regular expression.
5. From **Operation**, select **View log file** or **Download**.
6. Click **Next**. If you selected **View log file**, the log files are displayed.

Note:

The system automatically updates the list every five seconds with any new logs.

8.1 Database Restore or Recovery

This section provides procedures for

- MiVoice Business Solution Virtual Instance database restore
- MiVoice Business Solution Virtual Instance disaster recovery.

8.2 Conditions and Constraints

The following conditions and constraints apply to database restores:

- Do not attempt to restore a database that has been taken from an individual application (for example, a NP-UM database) within MiCollab to a MiVoice Business Solution Virtual Instance deployment.
- All application data programmed in the MiVoice Business Solution Virtual Instance database is overwritten by the backup data during the restore operation. The data in the backup is not merged with the existing database.
- You cannot restore a MiVoice Business Solution Virtual Instance from a newer vSphere, Nutanix, or Hyper-V platform to a platform with an older version of vSphere, Nutanix, or Hyper-V. For example, you cannot restore a MiVoice Business Solution Virtual Instance that was exported from a vSphere 5.5 platform to a vSphere 5.1 platform.

8.3 System Disaster Recovery

You can recover a MiVoice Business Solution Virtual Instance system on the same virtual appliance by deploying the latest MiVoice Business Solution Virtual Instance OVF file and then restoring your database backup.

Note:

You cannot restore a database backup that was performed on a Server-only configuration into a server that was deployed in Server-gateway mode is not allowed. The same restriction applies against restoring a Server-Gateway backup into a Server-only deployment.

Note:

VMware SRM cannot be used for MiVoice Business Solution Virtual Instance disaster recovery.

1. Download the MiVoice Business Solution Virtual Instance OVA/vhdx file from Mitel Online to a network drive or vSphere, Nutanix, or Hyper-V Client PC.
2. Shut down the current MiVoice Business Solution Virtual Instance.
3. Deploy the new MiVoice Business Solution Virtual Instance on the host system for instructions.
4. Select the newly created MiVoice Business Solution Virtual Instance (for example: MiVoice Business Solution Virtual Instance 8.0.2.101 build) and launch Console. The MiVoice Business Solution Virtual Instance console opens within the vSphere, Nutanix, or Hyper-V Client.
5. Power on the MiVoice Business Solution Virtual Instances (only for VMware).

6. After you power on the MiVoice Business Solution Virtual Instance VM, the Custom Template screen is displayed.
   - Complete the fields in the Custom Template screen with the information for the existing MiVoice Business Solution Virtual Instance VM. Note that if you enter different IP addresses, they will be overwritten by the addresses from the backup file when you perform the restore.
   - Click **Next**.
7. Log into the server manager interface using the administrator password that you entered in the Custom Template screen.
8. Click **Restore**.

8.4 Troubleshooting Chart

Note:

Refer to the Virtual Appliance Quick Reference Guide for a list of the top five problems encountered while deploying Mitel virtual appliances, as reported by Support.

Symptom	Possible Cause	Corrective Action
In the VMware deployment wizard, the IP Address fields in the Properties screen are truncated.	If your PC screen resolution is set above 100%, for example 125%, some IP Address fields in the wizard may be truncated.	Ensure that your PC display resolution is set to 100%.
Unable to access MiCollab server manager interface after deployment.	An invalid LAN IP address was entered in the MiVoice Business Solution Virtual Instance Properties screen during OVF deployment.	

Symptom	Possible Cause	Corrective Action
	An valid LAN IP address was entered in the MiVoice Business Solution Virtual Instance Properties screen during OVF deployment, but this IP address is not on the same subnet as the MiVoice Business Solution Virtual Instance.	Enter a valid LAN IP or WAN IP address through the MiCollab server console interface: 1. Select the newly created MiVoice Business Solution Virtual Instance (for example: MiVoice Business Solution Virtual Instance 1.0 build) and launch Console. The MiCollab virtual appliance console opens within the vSphere, Nutanix, or Hyper-V Client. 2. Power on the VM by clicking the green button in the toolbar. 3. Click the **Console** tab. The MSL Server Console boots up and the server console login prompt appears. 4. Place the cursor in the console screen and enter the MiVoice Business Solution Virtual Instance administration login and password. If at any time you need the cursor available for other desktop activities, press the CTRL + ALT keys. 5. Use the Server Console menu to correct the IP address(es)
Cannot power up MiVoice Business Solution Virtual Instance.	You have cloned a MiVoice Business Solution Virtual Instance and are attempting to power it up.	Cloning of an MiVoice Business Solution Virtual Instance is not supported. You can only clone MiVoice Business Solution Virtual Instance templates.

Symptom	Possible Cause	Corrective Action
After you deploy the and complete the Initial Configuration Wizard, the MiCollab clients cannot connect to MiVoice Business Solution Virtual Instance via the WAN IP.	The MiCollab Client Connector is not configured with the **MiVoice Business Solution Virtual Instance** LAN IP Address.	1. Log into the MiVoice Business Solution Virtual Instance. 2. Under **Applications**, click **MiVoice Border Gateway**. 3. Under **Teleworking** drop-down, select **Application integration**. 4. Under **MiCollab Client**, enable the **MiCollab Client connector enabled** checkbox. 5. Enter **MiCollab Client hostname or server IP address**. 6. Click **Save**.
MiVoice Business Solution Virtual Instance system performance is slow.	VMware resources are inadequate. You have taken snapshots of MiVoice Business Solution Virtual Instance. System performance is degraded if snapshots are present on the platform Delete all MiVoice Business Solution Virtual Instance snapshots from system.	1. Log into the MiVoice Business Solution Virtual Instance server manager. 2. Under **Administration**, click **Mitel Virtualization**. 3. Run the Mitel Virtualization Diagnostics Tool. 4. See the Virtual Appliance Deployment Guide. This guide lists the resource requirements for all Mitel virtual solutions.

Symptom	Possible Cause	Corrective Action
Voice quality issues	VMware resources are inadequate. MiVoice Business Solution Virtual Instance is installed in the vSphere environment using **Thin** provisioning. Thin provisioning can cause voice quality issues due to disk sharing.	1. Log into the MiVoice Business Solution Virtual Instance server manager. 2. Under **Administration**, click Mitel Virtualization. 3. Run the Mitel Virtualization Diagnostics Tool. 4. See the Virtual Appliance Deployment Guide. This guide lists the resource requirements for all Mitel virtual solutions. Reinstall MiVoice Business Solution Virtual Instance and select Thick provisioning during the install wizard.
The Table of Contents or help topics in an application online help system are not present or not functioning correctly in Internet Explorer 10 or 11.	Help compatibility issues with Internet Explorer 10 and 11.	Put the browser in compatibility mode. For Internet Explorer 10, click the Compatibility View icon located in the browser address bar on the right side. For Internet Explorer 11, press the F12 keyboard key to open Emulation Mode. Set Documentation Mode to 10.

Symptom	Possible Cause	Corrective Action
After you install MiVoice Business Solution Virtual Instance, Flow Through Provisioning and Reach Through to the MiVoice Business application are not functioning. After you restore a MiVoice Business Solution Virtual Instance database, Flow Through Provisioning and Reach Through to the MiVoice Business application are not functioning	MiCollab and the MiVoice Business applications failed to start sharing data.	1. Log into the MiVoice Business system administration tool. 2. Choose to view the forms alphabetically and select the **Network Elements** form. 3. Locate the MiCollab network element, select it, click **Start Sharing** and then **OK**. 4. Verify the sharing and synchronization completes successfully. If you receive a banner warning, log into the MiCollab server, and run the **Reconcile Wizard** to align the data.
After a database restore the following error message appears in the server manager banner: "Failed to start the data synchronization between MiCollab and MiVoice Business. Reason: The MiVoice Business application has not started".	The MiVoice Business application failed to start so the automatic database synchronization could not proceed.	1. Log into the MiVoice Business Solution Virtual Instance server manager. 2. Click **Applications** and then click **MiVoice Business**. 3. Check the panel for a MiVoice Business error message. 4. Troubleshoot based on the error message.

Symptom	Possible Cause	Corrective Action
After a database restore one of the following error messages appears in the server manager banner: "Failed to start the data synchronization between MiCollab and MiVoice Business. Reason: The MiVoice Business database restore process failed". Reason: Could not add the MiCollab Network Element to MiVoice Business or the START SHARING maintenance command failed. Reason: The MiColllab sync did not start or complete after 20 minutes.	The MiVoice Business automatic "start sharing" operation failed.	Start sharing between MiCollab and MiVoice Business manually: 1. Log into the MiVoice Business system administration tool. 2. Choose to view the forms alphabetically and select the **Network Elements** form. 3. Locate the MiCollab network element, select it, click **Start Sharing** and then **OK**. 4. Verify the sharing and synchronization completes successfully. If you receive a banner warning, log into the MiCollab server, and run the **Reconcile Wizard** to align the data.
After a database restore one of the following error messages appears in the server manager banner: "The automatic reconcile between MiCollab and MiVoice Business failed. You can use the Reconcile Wizard to consult the analysis report."	The automatic reconcile between MiCollab and MiVoice Business failed to start because the Reconcile Wizard is not properly licensed with the Application Management Center (AMC). The Application Record ID is not registered with the AMC.	1. Log into the MiVoice Business Solution Virtual Instance server manager. 2. Access the Status page and **Sync** the MiCollab ARID with the AMC. 3. Log into the MiVoice Business system administration tool. 4. Choose to view the forms alphabetically and select the **Network Elements** form. 5. Locate the MiCollab network element, select it, click **Start Sharing** and then **OK**. 6. Verify the sharing and synchronization completes successfully. If you receive a banner warning, log into the MiCollab server, and run the **Reconcile Wizard** to align the data.

Symptom	Possible Cause	Corrective Action
MPA Remote access to ESM & Server Manager fails	**Use Subdomains for Remote Access:** checkbox is enabled in **System Configuration** under **Remote access** of MPA.	Disable **Use Subdomains for Remote Access:** checkbox in **System Configuration** under **Remote access** of MPA.
Internal Server Error on License Information page or any MiCollab admin pages on the server manager.	2nd IP on default LAN interface is not set.	Login to console application and set the 2nd LAN IP. Refer Add 2nd IP to default LAN interface.
MOM server crash alarms observed after deployment of MiVoice Business Solution Virtual Instance.	This is observed during startup when the system is not fully configured.	This is normal and MOM server runs after the cleared alarms.

Appendix A 9

This chapter contains the following sections:

9.1 UCC Default Roles and Templates

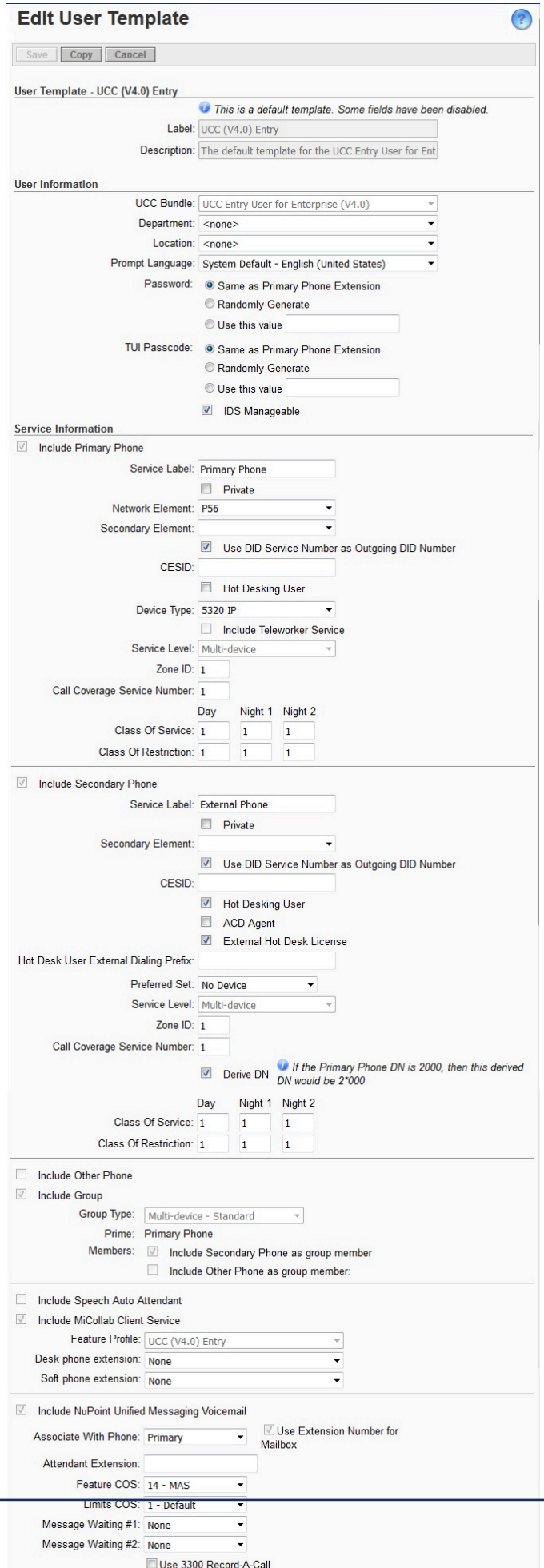
Default Roles

There are three primary default UCC roles. Each of these roles is associated with a default template:

- Default UCC Entry
- Default UCC Standard

9.1.1 Entry User for Business Template

Template for entry level Template for entry level user Entry user template Entry User for Business Template


Edit User Template
Save
Copy
Cancel
User Template - UCC (V4.0) Entry
This is a default template. Some fields have been disabled.
Label: UCC (V4.0) Entry
Description: The default template for the UCC Entry User for Ent
User Information
UCC Bundle: UCC Entry User for Enterprise (V4.0)
Department: <none>
Location: <none>
Prompt Language: System Default - English (United States)
Password: Same as Primary Phone Extension
Randomly Generate
Use this value
TUI Passcode: Same as Primary Phone Extension
Randomly Generate
Use this value
IDS Manageable
Service Information
Include Primary Phone
Service Label: Primary Phone
Private
Network Element: P56
Secondary Element:
Use DID Service Number as Outgoing DID Number
CESID:
Hot Desking User
Device Type: 5320 IP
Include Teleworker Service
Service Level: Multi-device
Zone ID: 1
Call Coverage Service Number: 1
Day Night 1 Night 2
Class Of Service: 1 1 1
Class Of Restriction: 1 1 1
Include Secondary Phone
Service Label: External Phone
Private
Secondary Element:
Use DID Service Number as Outgoing DID Number
CESID:
Hot Desking User
ACD Agent
External Hot Desk License
Hot Desk User External Dialing Prefix:
Preferred Set: No Device
Service Level: Multi-device
Zone ID: 1
Call Coverage Service Number: 1
Derive DN
If the Primary Phone DN is 2000, then this derived DN would be 2*000
Day Night 1 Night 2
Class Of Service: 1 1 1
Class Of Restriction: 1 1 1
Include Other Phone
Include Group
Group Type: Multi-device - Standard
Prime: Primary Phone
Members: Include Secondary Phone as group member
Include Other Phone as group member:
Include Speech Auto Attendant
Include MiCollab Client Service
Feature Profile: UCC (V4.0) Entry
Desk phone extension: None
Soft phone extension: None
Include NuPoint Unified Messaging Voicemail
Associate With Phone: Primary
Use Extension Number for Mailbox
Attendant Extension:
Feature COS: 14 - MAS
Limits COS: 1 - Default
Message Waiting #1: None
Message Waiting #2: None
Use 3300 Record-A-Call

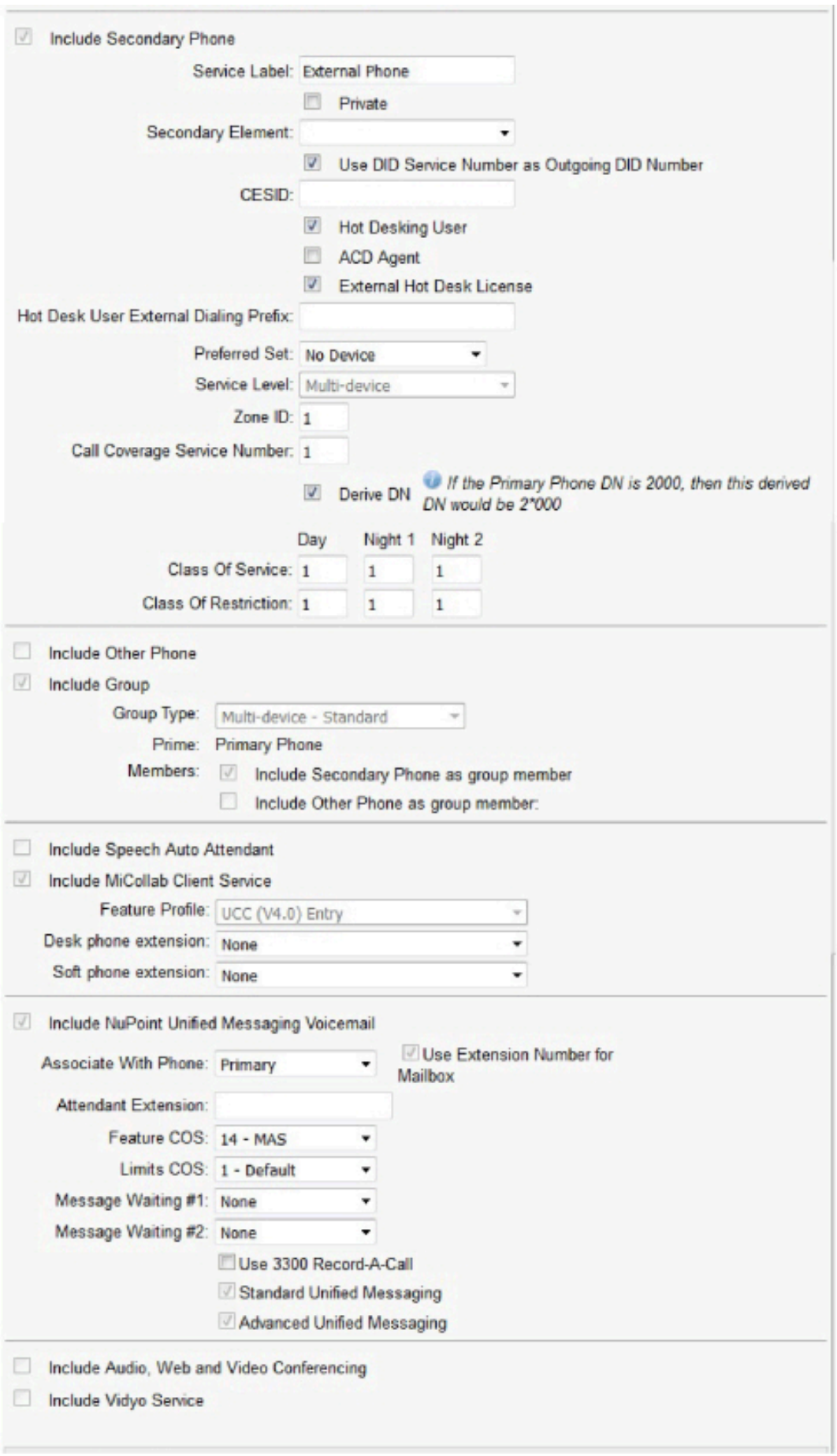
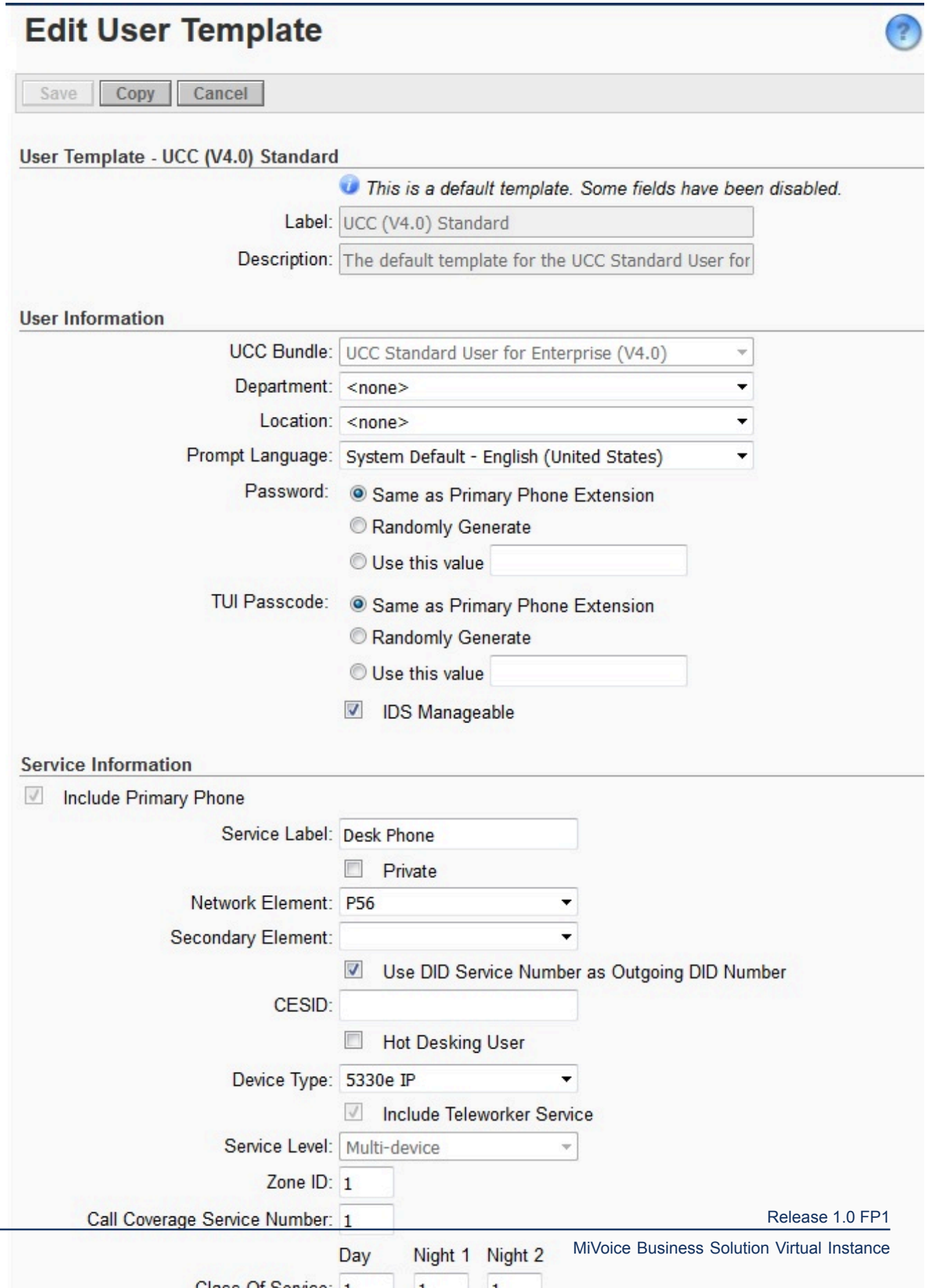


Figure 21: Entry User Template (Page 2 of 2)

9.1.2 Standard User For Business Template



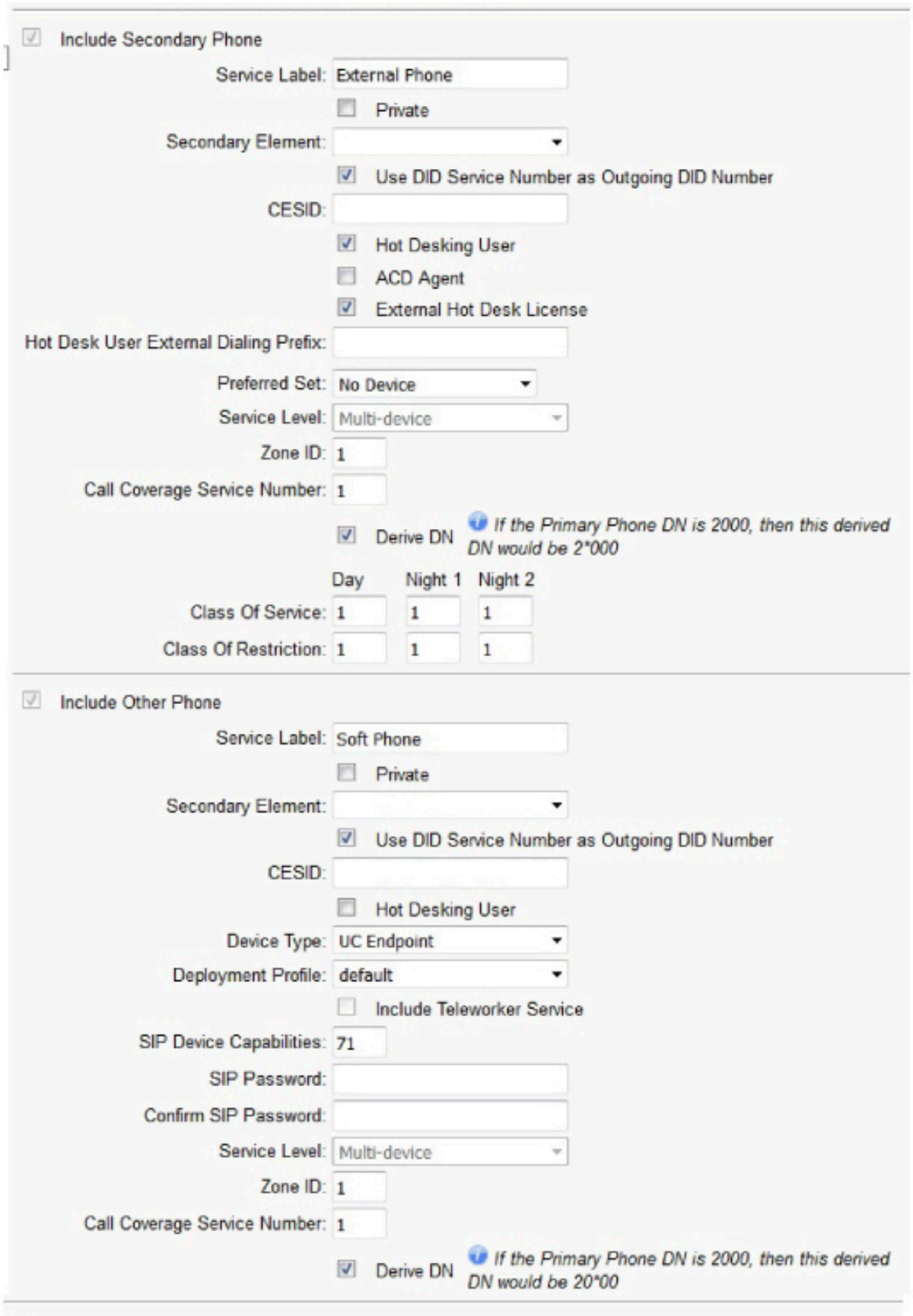


Figure 23: Standard User for Business Template (Page 2 of 3)

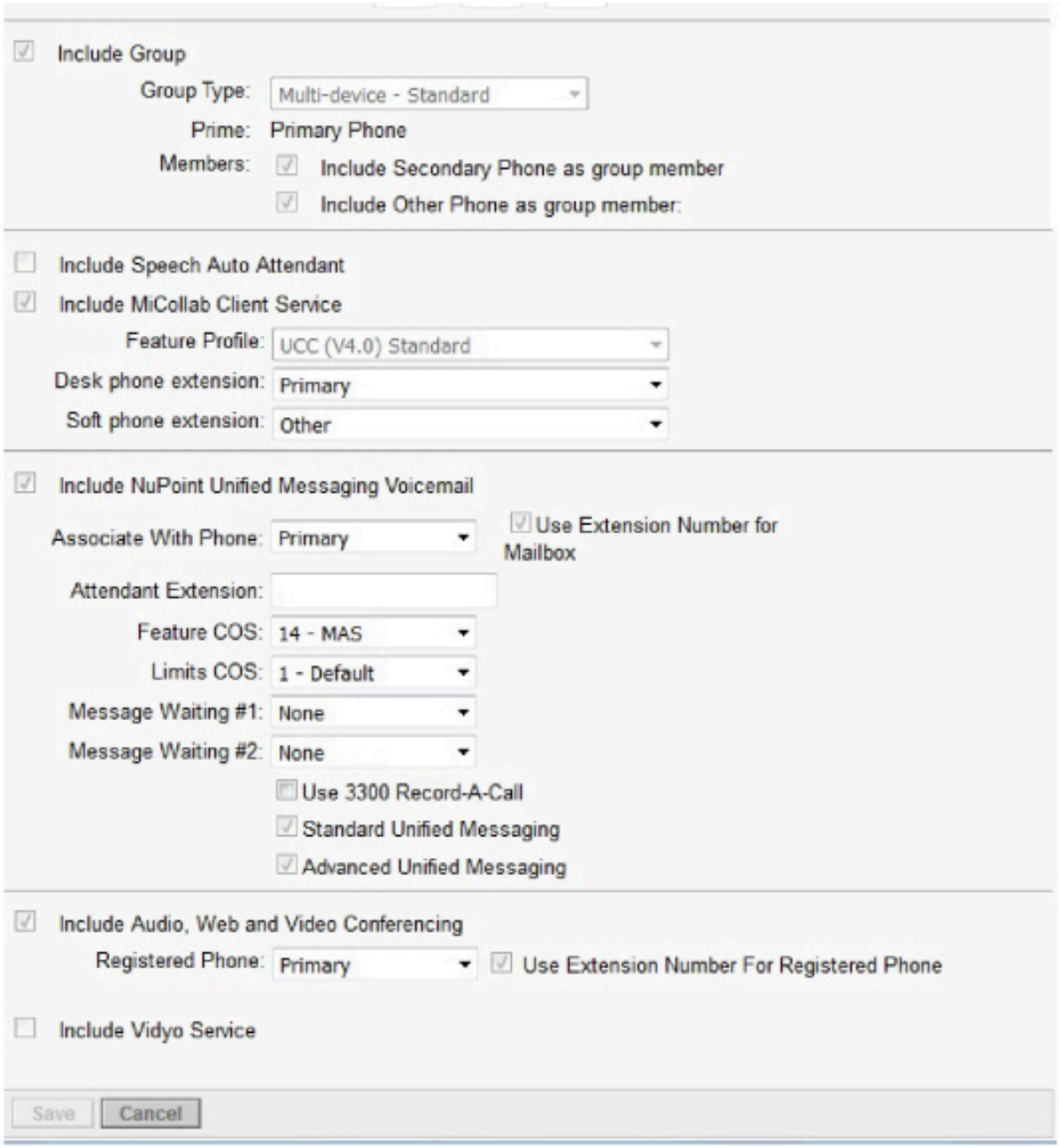


Figure 24: Standard User Template (Page 3 of 3)

Appendix B 10

This chapter contains the following sections:

This appendix provides instructions on how to deploy the MiVoice Business Solution Virtual Instance OVA using vSphere when connected directly to an ESXi host.

10.1 Deploying Directly to an ESXi Host

- Deploy OVA using VMware vSphere Client directly connected to the ESXi server
- Set up network configuration through MiCollab server console
- Optionally, log into console as administrator and add trusted network

10.2 Conditions and Limitations

In a vCenter environment, MiVoice Business Solution Virtual Instance uses the OVF properties to provide information and settings to MiCollab server manager on initial boot. The OVF properties include

- initial configuration information, such as IP address, netmask, gateway, DNS, and
- application-level settings, such as the Application Record ID (ARID) required for licensing, administration login credentials, and so forth.

This configuration information is stored in the vCenter database at deployment time.

In an environment without vCenter, where MiVoice Business Solution Virtual Instance is deployed using Nutanix, or Hyper-V, the Application Configuration Properties screen is not available. Therefore, you must access the MiVoice Business Solution Virtual Instance server console and configure the system with its network addresses, admin password, and ARID. After you complete this network configuration, you launch the Initial Configuration Wizard to complete initial configuration.

10.3 Deploy OVA

The OVA deployment is almost identical to the steps required to deploying the OVA through vCenter. The only difference is that the Application Configuration Properties screen at the end of the deployment wizard is not available.

During the deployment wizard, ensure that you record which vLAN networks are connected to the LAN and WAN. You will need to enter this information through the MiVoice Business Solution Virtual Instance server.

10.4 Perform Network Configuration through MiCollab Server Console

After you have deployed the OVA, follow the procedure below to perform the network configuration:

1. Select the newly created MiVoice Business Solution Virtual Instance (for example: MiVoice Business Solution Virtual Instance 1.0 build) and launch Console.
2. Power on the MiVoice Business Solution Virtual Instance VM.
3. Launch **Console**. The system boot up progress messages are displayed in the Console screen. When the system is finished booting up, the "Select Keyboard Language" page is displayed. Select the desired keyboard language and select **Next**.

   To use the MiVoice Business Solution Virtual Instance server:

   - Press the Space bar on your computer keyboard to select the items in a list.
   - Use the left and right arrow keys to highlight a command (for example **Next**).
   - Press the keyboard Enter key to select a command.
4.

   Note:
   Step 4 and beyond do not apply to Nutanix and Hyper-V.

   At the "Restore from backup?" prompt, select **No**.
5. In the "Choose Administrator password" screen, enter an Administrator password and then re-enter it for confirmation. This password allows you to access the MiCollab Server Console and MiCollab Server Manager.

   Choose a password that contains numbers, mixed upper- and lower-case letters, and punctuation characters.After you have entered and confirmed the password, the system examines the password for strength. If it is found to be weak, you are offered the chance to change it or continue.
6. In the "Select Timezone" screen, select the desired timezone.
7. In the "Primary domain name" screen, enter the primary domain name that will be associated with the MiVoice Business Solution Virtual Instance server. This domain will become the default for the server manager portal. The name must start with a letter and can contain letters, numbers, and hyphens (for example, mitel.com). DO NOT use the default setting "mycompany.local".
8. In the "Enter system name" screen, enter a unique system name or host name for the server. The name must start with a letter and can contain letters, numbers, and hyphens (for example, Server1).

9. Assign the network interfaces to support either LAN Only Mode or Network Edge Mode:

   For LAN Only (Server-only) Mode:

   - In the "Select local network adapter" screen, select the **eth0** adapter only.
   - In the "Local networking parameters" screen, enter the MiVoice Business Solution Virtual Instance server LAN IP address.It must be a valid IP address on the same network to which you connected the LAN interface during OVA deployment.
   - In the "Enter local subnet mask screen", enter the subnet mask for the local network. If you are adding the server to an existing network, use the subnet mask used by the local network. Otherwise, accept the default setting.
   - In the "Enable 1Pv6 protocol" screen, select **No**.
   - To configure the second IP, select **Yes**.
   - In the "Select WAN network adapters" screen, select Next. (Do not select any adapters).
   - Proceed to Step 10.

   For Network Edge (Server Gateway) Deployments:

   - In the "Select local network adapter" screen, select the **eth0** adapter only.
   - In the "Local networking parameters" screen, enter the MiVoice Business Solution Virtual Instance server LAN IP address.It must be a valid IP address on the same network to which you connected the LAN interface during OVA deployment.
   - In the "Enter local subnet mask screen", enter the subnet mask for the local network. If you are adding the server to an existing network, use the subnet mask used by the local network. Otherwise, accept the default setting.
   - In the "Select WAN network adapters" screen, select the **eth1** adapter.
   - In the "External Interface Configuration" screen, select **Use static IP address**.
   - In the "Enter static IP address" screen, enter the IP address of the WAN interface. It must be a valid IP address on the same network to which you connected the WAN interface during OVA deployment.
   - In the "Enter subnet mask" screen, enter the netmask for the WAN IP address.
   - In the "Enter gateway IP address" screen, enter the gateway IP address for the WAN.
   - Proceed to Step 10.

10. In the "Unconfigured network adaptors" screen, select **Leave unconfigured**. This optional network interface can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.
11. In the "Corporate DNS server address" screen, enter the IP address of the DNS server.
12. In the "Resolve primary domain name" screen, select the **Corporate address**.
13. Select **Next** and select **Finish**. The MiCollab server reboots with your initial configuration settings.
14. Proceed to Add Trusted Network (Optional).

10.5 Add Trusted Network (Optional)

To launch a web session from a computer that is located on a different network than the MiVoice Business Solution Virtual Instance, add that network as a trusted local network.

Note:

If the computer is on the same network as the MiVoice Business Solution Virtual Instance,then you do not need to add a trusted network.

1. After the MiVoice Business Solution Virtual Instance server boots up, log into the MiVoice Business Solution Virtual Instance server console using the administrator password that you created in the previous procedure.
2. In the "Welcome" page, select **Manage trusted networks**.
3. In the "Trusted Networks Operations" page, select **Add IPv4 trusted network** or **Add IPv6 trusted network**.
4. In the "Trusted Network IP" page, enter the IP address of the trusted local network for the computer from which web session is launched.
5. In the "Trusted Network Mask", specify the network mask of this network.
6. In the "Trusted Network Router Address", enter the router address of the trusted network that is used used to reach the additional network.
7. Click **Next** to complete the configuration.