A MITEL
PRODUCT
GUIDE

MiVoice Business

MiVoice Business Solution Virtual Instance

Release 2.0

August 2025

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 2.0

Feature	Update	Location	Publish Date
Support of Proxmox VE 8.3 and below	Deploying a VM from OVA on Proxmox VE 8.3	Deploying on Proxmox VE 8.3 on page 71 Deploying on Proxmox VE 8.2 and below on page 74	June 2025

1.3 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 (Chat)
- MiVoice Border Gateway, providing
  - Teleworker Service
  - Secure Recording Connector (for remote Teleworkers only)
  - SIP Trunking Proxy

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

1.3.1 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.

1.3.1.1 MiCollab Client

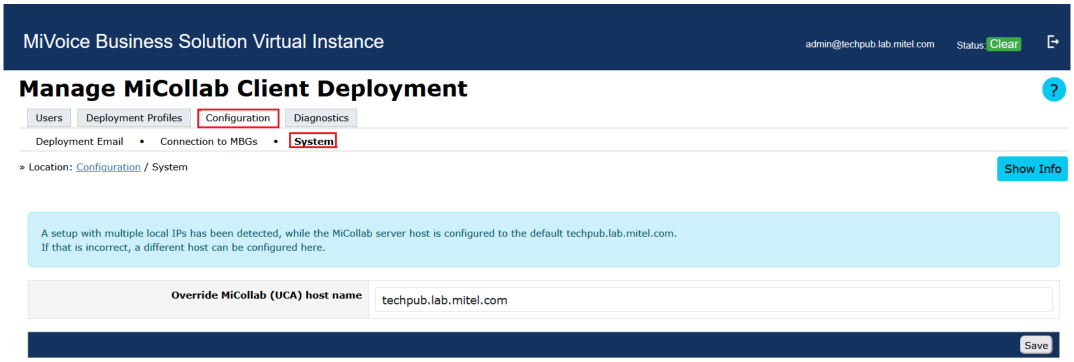
This application provides a single access point for business communication and collaboration needs. It converges the call control capabilities of the MiVoice Business platform with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications. It 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.

1.3.1.2 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**.

  Override MiCollab (UCA) host name - Specify a host name in this field only if your MiCollab client needs a custom name to communicate with the server. Configure this if the host name needs to differ from the default MiCollab server host name (which can be found in the **Enterprise tab** on **MiCollab Client Service Configuration** page).


MiVoice Business Solution Virtual Instance
admin@techpub.lab.mitel.com
Status: Clear
Manage MiCollab Client Deployment
?
Users
Deployment Profiles
Configuration
Diagnostics
Deployment Email
Connection to MBGs
System
» Location: Configuration / System
Show Info
Save

A setup with multiple local IPs has been detected, while the MiCollab server host is configured to the default techpub.lab.mitel.com.
If that is incorrect, a different host can be configured here.

Override MiCollab (UCA) host name: techpub.lab.mitel.com

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

Refer to the MiCollab Client Deployment help.

1.3.2 MiVoice Business

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, 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.

Note:

- Clustering with a 2nd SVI server is supported for resiliency.

1.3.3 CloudLink Gateway

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

For more information on CloudLink Gateway, refer CloudLink Gateway.

1.3.4 Mitel Performance Analytics

Mitel Performance Analytics (MPA) is an optional blade that integrates with the Mitel Performance Analytics Cloud Service, offering real-time alerts, detailed reporting, and secure remote access.

For more information on MPA, refer Mitel Performance Analytics.

1.3.5 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)

1.4 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 (Primary interface), 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 Deployment Model section.
- Override the MiCollab (UCA) host name (FQDN) in Client Deployment as described in Configure MiCollab Client Deployment on page 107.
- 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.
- When in **Server/Gateway or Server-Only mode** do not add the MiCollab server FQDN to the Remote Proxy Domain List.
- 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 bastion on page 109.
- Programming remote proxy / reverse proxy, refer MiVoice Border Gateway Installation and Maintenance Guide.
- Web server certificates. Refer Configure MSL Server on page 96.
- MPA probe monitors all the configured interfaces.
- Clustering with a 2nd MiVoice Business Solution Virtual Instance server is supported for resiliency.

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*
- *MiCollab*
  - *Users and Services*
  - *MiCollab Client*
  - *MiCollab Client Deployment*
- *MiVoice Border Gateway*
- (Optional) *CloudLink Gateway*
- (Optional) *Mitel Performance Analytics (MPA)*

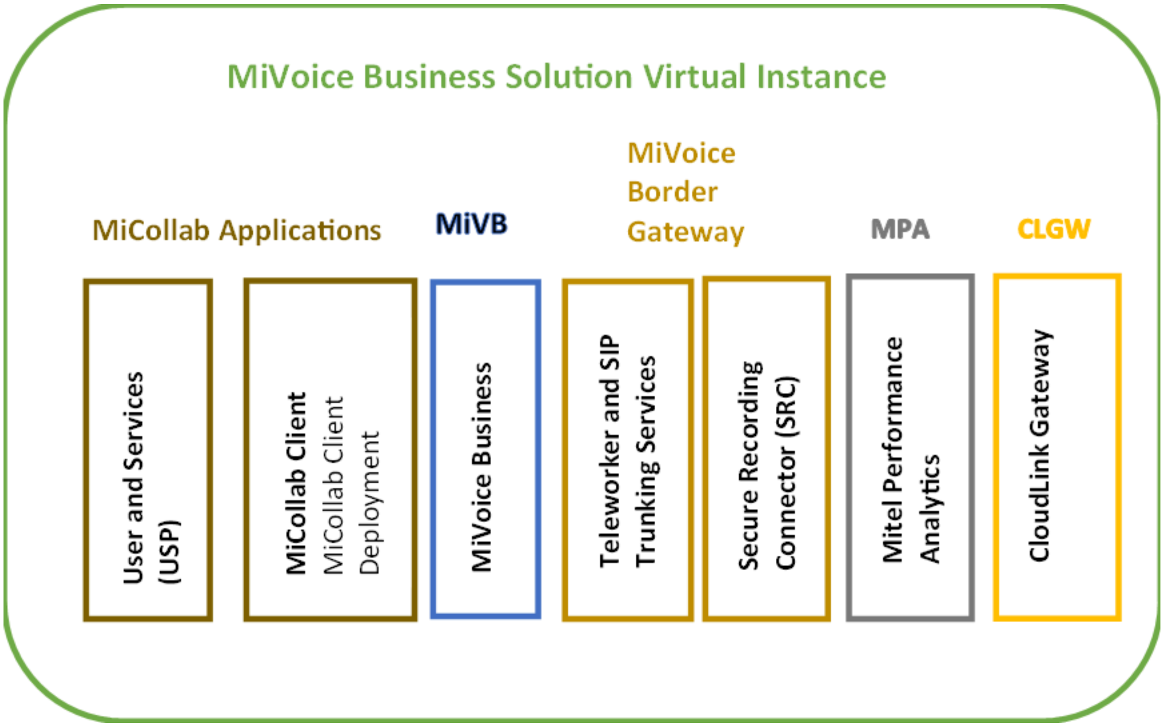

MiVoice Business Solution Virtual Instance
MiCollab Applications
MiVB
MiVoice Border Gateway
MPA
CLGW
User and Services (USP)
MiCollab Client MiCollab Client Deployment
MiVoice Business
Teleworker and SIP Trunking Services
Secure Recording Connector (SRC)
Mitel Performance Analytics
CloudLink Gateway

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.

> **Note**:
> SSH should only be enabled when necessary and under the guidance of technical support.

- 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.
- LDAPS– 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

Document Title	Description	Location
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
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

Document Title	Description	Location
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.

.

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

Each product includes a Security Guidelines document that provides a comprehensive overview of all security controls and features, offers security recommendations to the administrator, and refers to relevant sections of the product documentation for further details designed to be used alongside the full documentation suite to ensure secure deployment and ongoing maintenance of the product.

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 document outlines the types of personal data that are collected, processed, or transferred, provides guidance to administrators on securing this data, and is intended to be used alongside the product documentation suite to support compliance with data protection regulations. 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.

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.

2.5 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, all the software applications are installed when you deploy the MiVoice Business Solution Virtual Instance OVA file.
- Provides flow through 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 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
- 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

2.6 Deployment Models

The solution is well adapted to the following deployments:

- **Server Gateway Deployment model**: In this deployment configuration, MiVoice Business Solution Virtual Instance resides behind the customer's firewall and manages the Mitel connections to the customer firewall by routing Internet data packets to and from the voice network.
- **Server Only with Bastion Host MBG**: In this configuration, MiVoice Business Solution Virtual Instance is deployed on the LAN and connects to a separate MBG that resides in the customer's DMZ. The LAN mode configuration is typically used for the MIVBSVI.

  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.
- **Server Only Deployed behind the customer firewall**: In this configuration, the server is installed behind the customer’s existing firewall. It is a server-only mode and is protected from Internet exposure by the existing firewall.
- **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.

The MiVoice Business Solution Virtual Instance can be hosted either in IaaS or customer on premises.

Hosting Option

- **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.

Note:

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.

This product 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.

2.6.1 Server Gateway Deployment

Prerequisites:

- Firewall is required in front of the MBG WAN interface.
- The WAN IP should be a private IP on the same subnet as the customer's firewall LAN port, depending on the firewall configuration.
  - Custom MBG network profile must be used if private IP is assigned to WAN interface.
    - MBG's ICP-side bind interface is LAN interface, RTP ICP-side override address is LAN 1 IP 1.
    - The teleworker set-side bind interface is WAN interface, RTP Set-side override address is the WAN port.
- Teleworker sets and MiCollab client soft phones must be configured to connect to the FQDN of the MBG server.
- 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 SRC function.

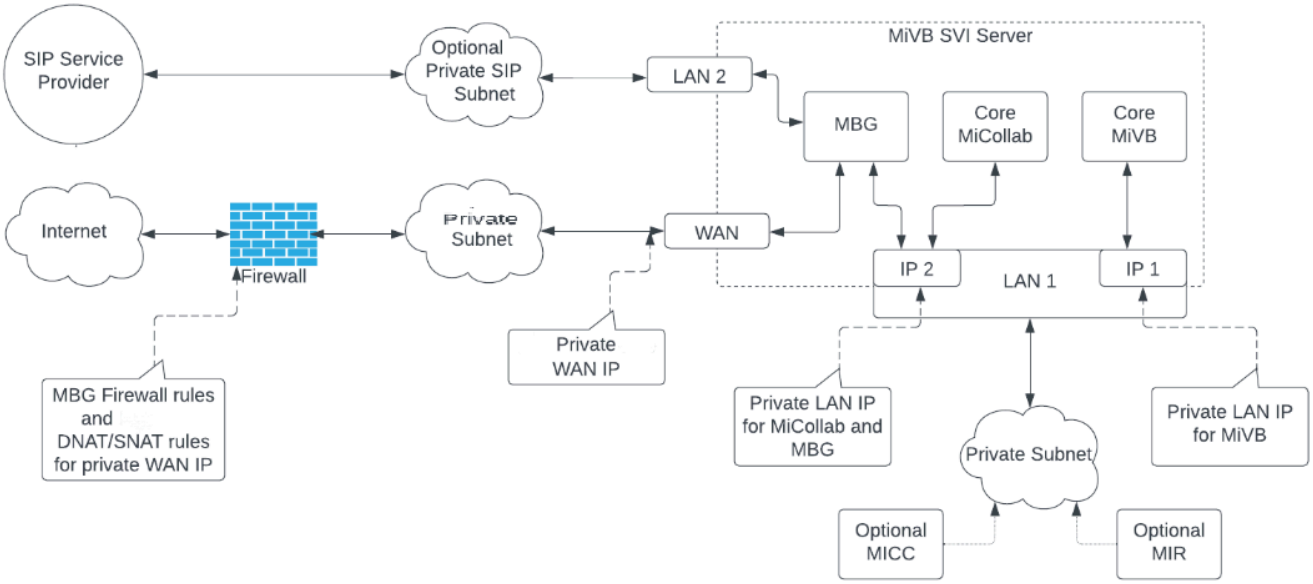


Figure 2: Server Gateway Deployment

Table 3: Public and Private FQDNs

FQDN	Public Resolution	Internal Resolution	Purpose
mivbsvi1.example.com	1.2.3.4	LAN 1 IP 1	Main MiVoice Business Solution Virtual Instance server FQDN for Teleworker phone, SIP, and MiCollab profile.
mivbsvi2-.example.com	1.2.3.4	LAN IP 1	Main public FQDN for access to MiVoice Business Embedded System Management (ESM)
mivb-mgmt.example.com	1.2.3.4	LAN IP 1	MiVoice Business public FQDN for Embedded Voicemail MiVoice Business private FQDN for MiVoice Business Embedded System Management (ESM)
mivb.example.com	1.2.3.4	LAN IP 1	MiVoice Business private FQDN for Embedded Voice Email, SIP devices, and Other.
micollab.example.com	1.2.3.4	LAN IP 2	MiCollab private FQDN
mbg-int.example.com	1.2.3.4	LAN IP 2	MBG's internal private FQDN for MIR, SIP Trunking Proxy
micc.example.com	1.2.3.4	Other LAN IP	Optional MICC private FQDN
mir.example.com	1.2.3.4	Other LAN IP	Optional MIR public FQDN

Steps for Server- Gateway Deployment

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

Step 1: Prepare Site

Step 2: Download MiVB SVI OVA from Mitel Online.

Step 3: Obtain EID/Serial from SLS.

Step 4: Deploy MiVB SVI OVA

Step 5: Setup 2nd IP on using console utility.

Step 6: Configure the internal FQDNs

Step 7: Configure MBG, select network profile

Step 8: Apply EID/Serial

Step 9: Configure MiVB, perform network elements sync

Step 10: Configure MiCollab

Step 11: Run MiCollab Reconcile wizard

Step 12: Provision Users

ℹ **Note**:
The customer must configure split DNS entries for the solution, so that the same FQDN resolves differently depending on whether the user is on the LAN or the Internet.

2.6.2 Server Only with Bastion Host MBG

Prerequisites

- Firewall is recommended in front of WAN interface of the bastion MBG.

- 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 instance when a bastion MBG is deployed.
  - 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 IP 1.
    - Set-side bind interface is WAN interface, RTP Set-side override address is WAN interface 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.

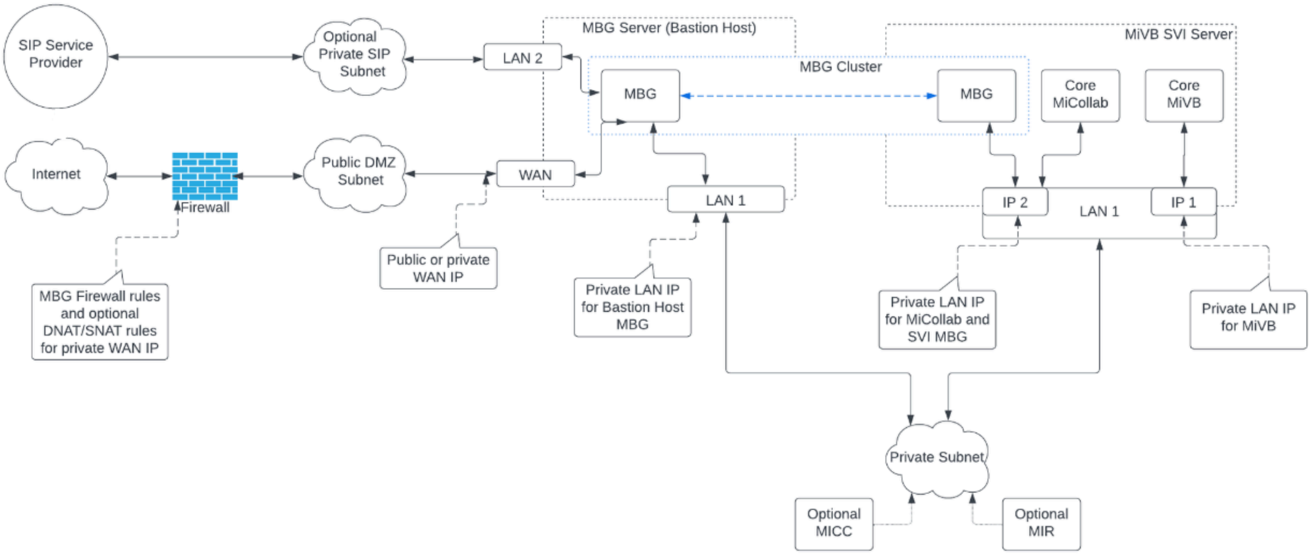


Figure 3: Server Only with Bastion Host MBG

Table 4: 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 5: 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

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
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
mbg-ext.example.com			10.0.50.6		Bastion host MBG's internal private FQDN for MIR, SIP Trunking Proxy

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
micc.example.com				10.0.50.7	Optional MICC private FQDN
mir.example.com				10.0.50.8	Optional MIR private FQDN

Steps for Server Only with Bastion Host MBG deployment

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

Step 1: Prepare Site for DMZ MBG.

Step 2: Download MBG OVA from Mitel Online.

Step 3: Obtain EID/Serial from SLS.

Step 4: Deploy MBG OVA.

Step 5: Configure MBG, select the network profile.

Step 6: Apply EID/Serial.

Step 7: Prepare Site for SVI.

Step 8: Download MiVB SVI OVA from Mitel Online.

Step 9: Obtain EID/Serial from SLS.

Step 10: Deploy MiVB SVI OVA.

Step 11: Setup 2nd IP on using console utility.

Step 12: Configure the internal FQDNs

Step 13: Configure MBG, select network.

Step 14: Apply EID/Serial.

2.6.3 Server Only Deployed behind the customer firewall

Prerequisites

- Firewall is required 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 1.
    - 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.

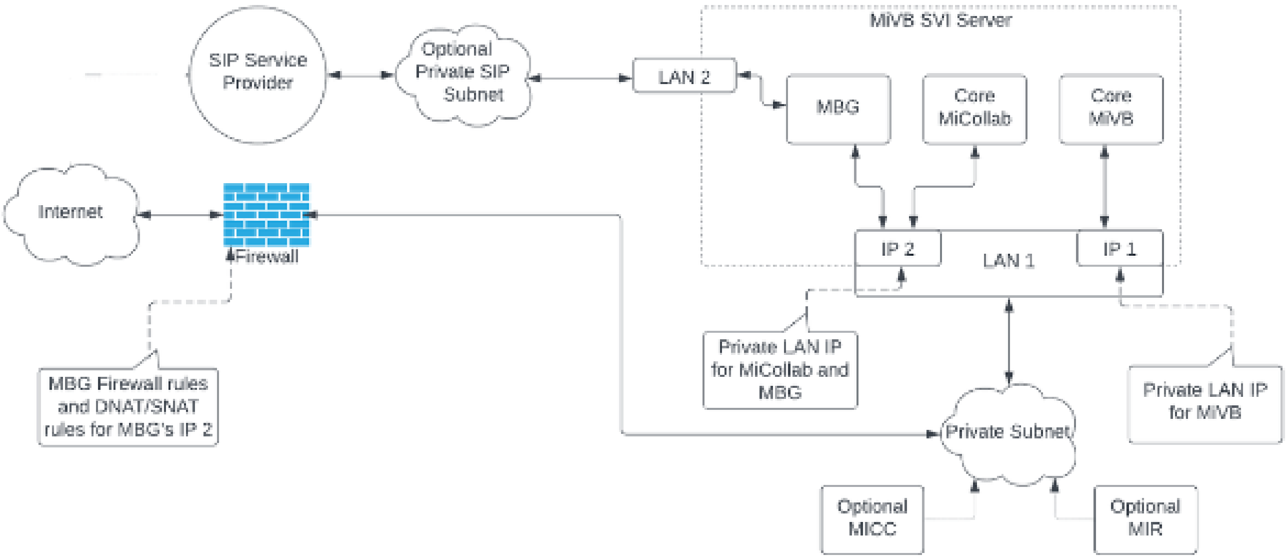


Figure 4: Server Only Deployed Behind the Customer Firewall

Table 6: 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.

FQDN	Public WAN IP	Purpose
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 7: 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.

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
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

Steps for Server Only Deployed behind the customer firewall

The following steps represents the work flow of Server Only Deployed behind the customer firewall:

Step 1: Prepare Site for DMZ MBG

Step 2: Download MiVB SVI OVA from Mitel Online

Step 3: Obtain EID/Serial from SLS.

Step 4: Deploy MiVB SVI OVA and apply EID/Serial.

Step 5: Setup 2nd IP on using console utility.

Step 6: Configure the internal FQDNs

Step 7: Configure MBG, select network profile

Step 9: Configure MiVB, perform network elements sync!

Step 10: Configure MiCollab

Step 11: Run MiCollab Reconcile Wizard

Step 12: Provision Users

2.6.4 Server Gateway with Resiliency

Prerequisites

Note:

- Clustering with a 2nd SVI server is supported for resiliency.

- Firewall is required in front of WAN interfaces.
- The WAN IPs can be public IPs or private IPs on the same subnets as the customer's firewall LAN port, 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.
    - MBG's ICP-side bind interface is LAN interface, RTP ICP-side override address is LAN 1 IP 1.
    - MBG's 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.
- 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 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.

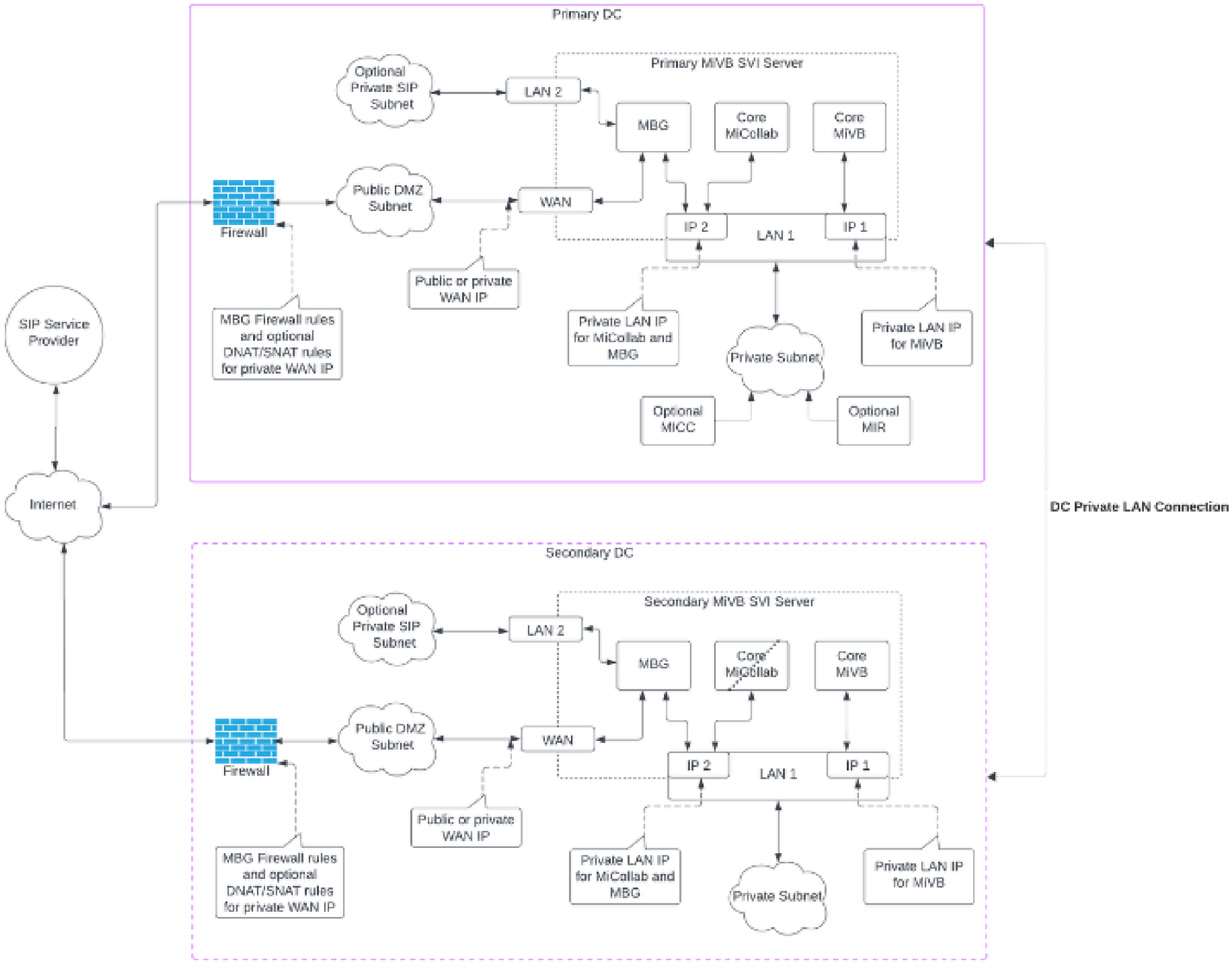


Figure 5: Server Gateway with Resiliency

Table 8: 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 9: 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
	2	mivbsvi2.example.com

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

The following examples assume a /24 subnet mask.

Table 10: 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.
micollab.example.com		10.0.50.5		MiCollab private FQDN

FQDN	LAN 1 IP 1	LAN 1 IP 2	Other IP	Purpose
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 11: 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)
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
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

Steps for Server Gateway with Resiliency Deployment

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

Step 1: Prepare Site for Primary SVI

Step 2: Download MiVB SVI OVA from Mitel Online

Step 3: Obtain EID/Serial from SLS.(refer section Create EID/Serial and Assign Licenses in SLS on page 51)

Step 4: Deploy MiVB SVI OVA and apply EID/Serial. (refer section Deploy Virtual Machine on page 60)

Step 5: Setup 2nd IP on using console utility (refer section Configure the server on page 86

Step 6: Configure the internal FQDNs

Step 7: Configure MBG, select network profile (refer section Configure MBG on page 98)

Step 8: Configure MiVB, perform network elements sync (refer section Configure MBG on page 98)

Step 9: Configure MiCollab (refer section Configure MiCollab on page 105)

Step 10: Run MiCollab Reconcile wizard

Step 11: Repeat Step 1 to Step 9 for secondary SVI (**Resilient config only**)

Step 12: Add secondary MiVB in network element (**Resilient config only**)

Step 13: Start sharing with secondary MiVB (**Resilient config only**)

Step 14: Cluster element provisioning (**Resilient config only**)

Step 15: MBG clustering (**Resilient config only**)

Step 16: ARS resilient routing (**Resilient config only**)

Step 17: Emergency routing to Public Network or SIP Trunk Provisioning

Step 18: Enable secondary element for user services configuration (**Resilient config only**)

Step 19: Valid certificates

Step 20: Ensure the verification of public FQDNs

2.6.5 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:
  - Private network (SD-WAN/MPLS /VPN) 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 (or similar) 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).

2.6.6 CPE Deployment

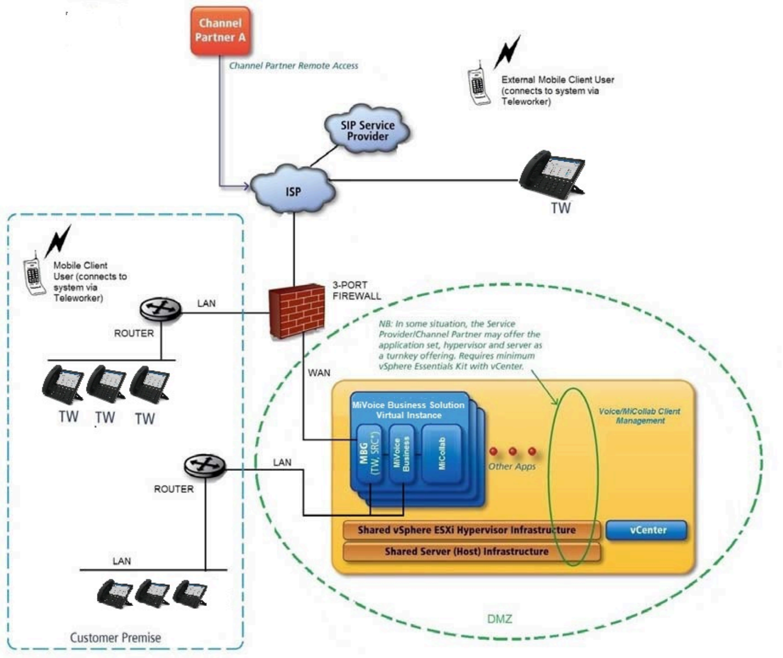
The figure *Customer Premise Equipment Deployment* shows the MiVoice Business Solution Virtual Instance and VMware components in a typical Customer Premise Equipment (CPE) deployment. In this deployment model:

- 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 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.


Channel Partner A
Channel Partner Remote Access
External Mobile Client User (connects to system via Teleworker)
SIP Service Provider
ISP
TW
Mobile Client User (connects to system via Teleworker)
LAN
ROUTER
TW
TW
TW
3-PORT FIREWALL
WAN
MiVoice Business Solution Virtual Instance
MBG (TW, SRC*)
MiVoice Business
MiCollab
Other Apps
Voice/MiCollab Client Management
Shared vSphere ESXi Hypervisor Infrastructure
vCenter
Shared Server (Host) Infrastructure
LAN
ROUTER
LAN
DMZ
Customer Premise

NB: In some situation, the Service Provider/Channel Partner may offer the application set, hypervisor and server as a turnkey offering. Requires minimum vSphere Essentials Kit with vCenter.

Figure 6: Customer Premise Equipment Deployment

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 able to connect outbound to the internet in order to license the product. Internet connectivity must be maintained to support the system licensing.

- UCC 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.

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 EID/Serial on the SLS.
- 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 SLS 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) if configured. 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).

- You can choose to license the MiVoice Business Solution Virtual Instance software bundle and user licenses on a subscription basis from Mitel.

3.1.2 Licensing Detection and Violation Mode

MiVoice Business Solution Virtual Instance appliances must maintain online connectivity to the SLS at all times. Loss of SLS connectivity for a short period of time is tolerated by the system. However, SLS connectivity must be re-established without delay in order to maintain access to all system functions and features. If SLS connectivity is lost for an extended period of time, an automatic alert is generated and sent to the Channel Partner SLS account administrator email address that is programmed in the SLS for the account. If SLS 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 SLS from each virtual appliance deployed at a customer’s site. For this reason, Mitel supports the ability to proxy online SLS connectivity from each virtual appliance through a single named proxy within the customer data center environment. This enables SLS 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	Details
MiVoice Business Solution Virtual Instance Software Base Packages for traditional customer premise or IaaS licensing	
Perpetual license	
MiVoice Business Solution Virtual Instance bundle	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	
MiVoice Business License - Enterprise User	
UCCv4.0 Entry User x1	UCC licenses must be added to ULM EID
UCCv4.0 Standard User x1	UCC licenses must be added to ULM EID
UCCv4.0 Basic to v4.0 Entry	UCC licenses must be added to ULM EID
UCCv4.0 Entry to v4.0 Standard	UCC licenses must be added to ULM EID
UCCv4.0 Basic to v4.0 Standard	UCC licenses must be added to ULM EID
54012626 SWA MiVBus UC Advantage 1y	Advantage SWA for New Systems, 1 year
54012627 SWA MiVBus UC Advantage 2y	Advantage SWA for New Systems, 2 years
54012628 SWA MiVBus UC Advantage 3y	Advantage SWA for New Systems, 3 years
54012629 SWA MiVBus UC Advantage 4y	Advantage SWA for New Systems, 4 years
540126 S30WA MiVBus UC Advantage 5y	Advantage SWA for New Systems, 5 years

Licenses	Details
54012631 SWA MiVBus UC Premium 1y	Premium SWA for New Systems, 1 year
54012632 SWA MiVBus UC Premium 2y	Premium SWA for New Systems, 2 years
54012633 SWA MiVBus UC Premium 3y	Premium SWA for New Systems, 3 years
54012634 SWA MiVBus UC Premium 4y	Premium SWA for New Systems, 4 years
54012635 SWA MiVBus UC Premium 5y	Premium SWA for New Systems, 5 years
54012636 SWA MiVBus UC Premium MPAPlus 1y	Premium SWA with MPA Plus for New Systems, 1 year
54012637 SWA MiVBus UC Premium MPAPlus 2y	Premium SWA with MPA Plus for New Systems, 2 years
54012638 SWA MiVBus UC Premium MPAPlus 3y	Premium SWA with MPA Plus for New Systems, 3 years
54012639 SWA MiVBus UC Premium MPAPlus 4y	Premium SWA with MPA Plus for New Systems, 4 years
54012640 SWA MiVBus UC Premium MPAPlus 5y	Premium SWA with MPA Plus for New Systems, 5 years
54012641 SWA MiVBus UC Advantage	Advantage SWA for Add-ons & Renewals
54012642 SWA MiVBus UC Premium	Premium SWA for Add-ons & Renewals
54012643 SWA MiVBus UC Premium MPAPlus	Premium SWA with MPA Plus for Add-ons & Renewals
54012644 SWA MiVBus UC Uplift Adv-Prem	Uplift from Advantage SWA to Premium SWA

Licenses	Details
54012645 SWA MiVBus UC Uplift Prem-MPAPlus	Uplift from Premium SWA to Premium SWA with MPA Plus
54014057 SWA MiVBus UC Uplift Adv-MPAPlus	Uplift from Advantage SWA to Premium SWA with MPA Plus
54012625 SWA MiVBus UC Reenlist Fee	SWA Reenlistment Fees

Note:

1. MiVoice Business Solution Virtual Instance also supports "à la carte" licensing.
2. The system does not restrict you from applying an EID/Serial ID 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 12: MiVoice Business Solution Virtual Instance system size

Virtual Appliance	Release	System Capacity	Configuration		Resource Reservation	
			vCPU	Disk	CPU	Memory
MiVoice Business Solution Virtual Instance	2.0	250	4	100	4 GHz	10 GB
		500	6	180	6 GHz	12 GB

Virtual Appliance	Release	System Capacity	Configuration		Resource Reservation	
			vCPU	Disk	CPU	Memory
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 13: Required Configuration Parameters

Configuration Items	Field Description	Site Configuration Data
Administration		
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".

Configuration Items	Field Description	Site Configuration Data
Application		
Initial Administrator Password	Record the initial administrator password for the MiCollab server manager interface. This password must be at least 15 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".	
License Key (Optional)	Identify the License Key (MiVoice Business Solution Virtual Instance Business Base EID/Serial) for this system. The EID/Serial is used by the SLS to distribute the system licenses. See Create EID/Serial and Assign Licenses in SLS for instructions. This key can be provisioned later also once the system is deployed.	

Configuration Items	Field Description	Site Configuration Data
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. ℹ **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		
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.	ℹ **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)	

Configuration Items	Field Description	Site Configuration Data
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.	**Note**: You must enter a LAN IP address before you deploy the MiVoice Business Solution Virtual Instance; otherwise, the system will not boot up.
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	ℹ **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.	ℹ **Note**: This is a warning to the user to configure the 2nd LAN IP address.

Table 14: Collect Advanced Deployment Properties

Configuration Items	Field Description	Site Configuration Data
Mitel Software License Server (SLS)	Record IP address or proxy address for the SLS.	
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 15: 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 7 digit extension numbering)	
Incoming Calls		

Configuration Items	Field Description	Site Configuration Data
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. ℹ **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. ℹ **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 EID/Serial and Assign Licenses in SLS

Create EID/Serial for MiVoice Business Solution Virtual Instance installation in your SLS license account and assign the required licenses to them. When you deploy the MiVoice Business Solution Virtual Instance, you will use the software base SLS Serial ID (EID) 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 SLS interaction for Service Providers.

4.2.1 About Licenses and Services

MiVoice Business Solution Virtual Instance supports licensing through the Licenses & Services Application (License Server). The Mitel Licenses & Services Application manages the software licensing and entitlement of the Software Assurance Program. After you obtain a ServiceLink ID or EID/Serial from the License Server, the License Server uses your EID/Serial ID to provide you with access to licenses, software releases, and upgrades.

When you place a new product order, the order information is entered into the Mitel Licenses & Services Application, which can be accessed through the MiAccess Portal. The Licensing & Services system deposits the purchased licenses into your licensing account for use in creating an application record.

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

4.2.1.1 Requesting a New Licenses and Services Account

To request an SLS account, send an e-mail containing the following information to license.support@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 update 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).

> ℹ **Note**:
> Please allow two business days for your Licenses and Services account to be created.

4.2.1.2 Accessing your SLS Account

To access your account for the first time:

1. Go to the Mitel website (https://www.mitel.com) and log in to your Mitel MiAccess account.
2. From the left menu, click **Licenses & Services**.
3. In the Home Page, the license vouchers can be accessed under the License Bank.

4.2.1.3 Creating a new system

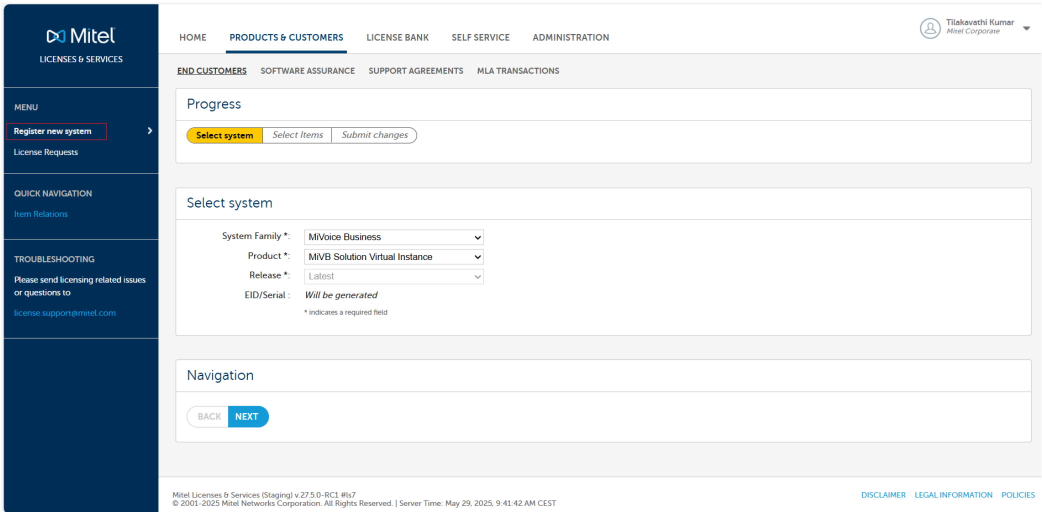
This topic provides systematic instruction on how to create a new system for MiVoice Business Solution Virtual Instance and provision the MSL in ServiceLink.

To create a new system, perform the following steps:

1. Navigate to the **Licenses & Services** home page.
2. In the **Licenses & Services** Home page, under the **Administration** tab, click **License MiVoice Business**.

3. Click **Register new system**.

   The **Select system** tab displays under **Progress** heading.



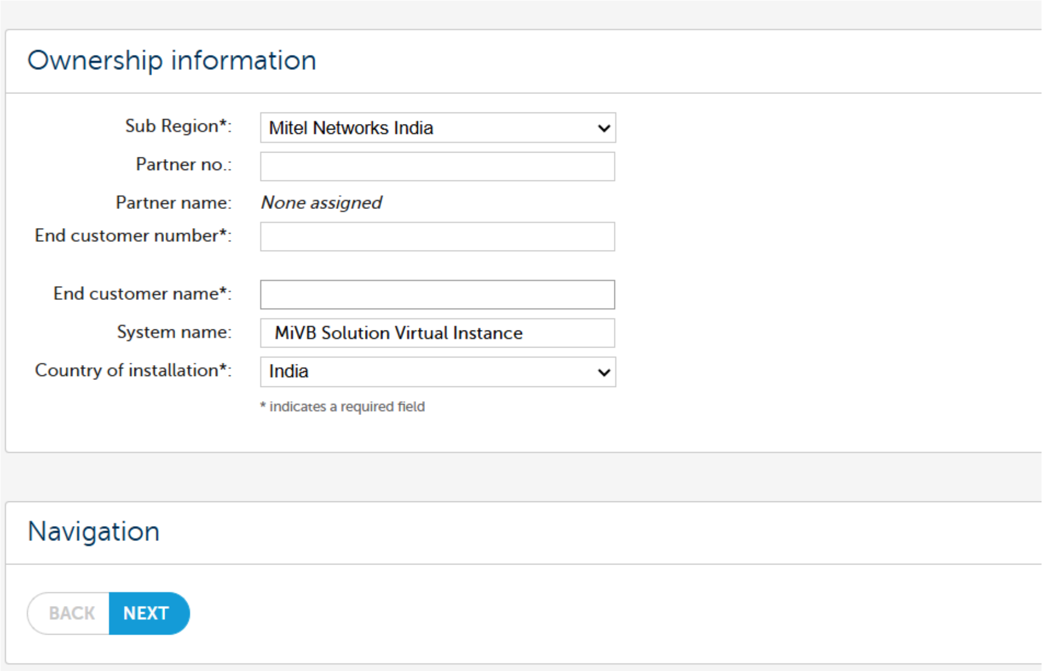
System Family *: MiVoice Business
Product *: MiVB Solution Virtual Instance
Release *: Latest
EID/Serial : *Will be generated*
* indicates a required field

Mitel Licenses & Services (Staging) v.27.5.0-RC1 #ls7
© 2001-2025 Mitel Networks Corporation. All Rights Reserved. | Server Time: May 29, 2025, 9:41:42 AM CEST

4. In the **Select system** section, select the system family, product type, and release number in the respective fields.

   For the MiVoice Business Solution Virtual Instance, the default release number will be set to the **latest** version.
5. Click **Next**.

   The Ownership information section displays.

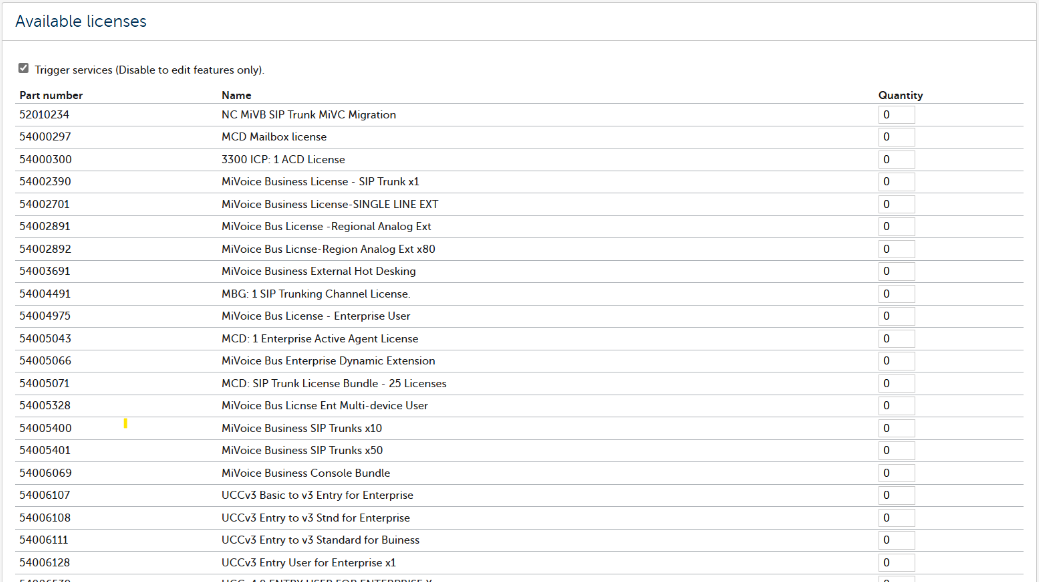


Sub Region*: Mitel Networks India
Partner no.:
Partner name: *None assigned*
End customer number*:
End customer name*:
System name: MiVB Solution Virtual Instance
Country of installation*: India
* indicates a required field

6. In the **Ownership information** section, select the sub-region, end customer number and name, and country in the respective fields.

7. Click **Next**.

   The **Available licenses** section displays under **Select** items tab.



Available licenses

☑ Trigger services (Disable to edit features only).

Part number	Name	Quantity
52010234	NC MiVB SIP Trunk MiVC Migration	0
54000297	MCD Mailbox license	0
54000300	3300 ICP: 1 ACD License	0
54002390	MiVoice Business License - SIP Trunk x1	0
54002701	MiVoice Business License-SINGLE LINE EXT	0
54002891	MiVoice Bus License -Regional Analog Ext	0
54002892	MiVoice Bus Licnse-Region Analog Ext x80	0
54003691	MiVoice Business External Hot Desking	0
54004491	MBG: 1 SIP Trunking Channel License.	0
54004975	MiVoice Bus License - Enterprise User	0
54005043	MCD: 1 Enterprise Active Agent License	0
54005066	MiVoice Bus Enterprise Dynamic Extension	0
54005071	MCD: SIP Trunk License Bundle - 25 Licenses	0
54005328	MiVoice Bus Licnse Ent Multi-device User	0
54005400	MiVoice Business SIP Trunks x10	0
54005401	MiVoice Business SIP Trunks x50	0
54006069	MiVoice Business Console Bundle	0
54006107	UCCv3 Basic to v3 Entry for Enterprise	0
54006108	UCCv3 Entry to v3 Stnd for Enterprise	0
54006111	UCCv3 Entry to v3 Standard for Buiness	0
54006128	UCCv3 Entry User for Enterprise x1	0

8. In the **Available licenses**, enter the required quantity for the corresponding license parts.
9. Click **Next.**
10. Review the following details in the **Submit changes** tab.

    - Product information
    - Selected licenses
    - Future feature status
    - Future service status

11. Click **Generate License**.

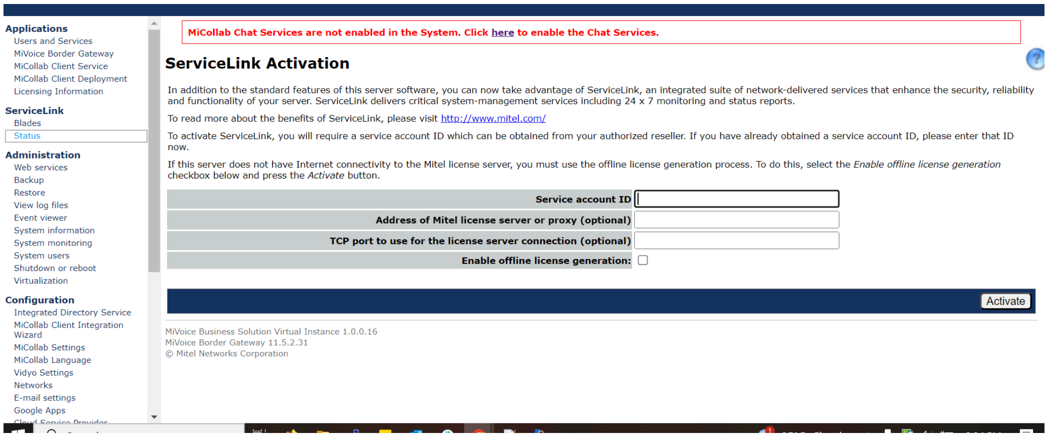
    New **EID/Serial number** is generated and sent to your e-mail address.

    To provision the MSL in ServiceLink, perform the following steps:

12. Navigate to the **Server Manager** application.

13. Under **ServiceLink**, click **Status**.

    The **ServiceLink Activation** screen displays.



MiCollab Chat Services are not enabled in the System. Click here to enable the Chat Services.

ServiceLink Activation

In addition to the standard features of this server software, you can now take advantage of ServiceLink, an integrated suite of network-delivered services that enhance the security, reliability and functionality of your server. ServiceLink delivers critical system-management services including 24 x 7 monitoring and status reports.

To read more about the benefits of ServiceLink, please visit http://www.mitel.com/

To activate ServiceLink, you will require a service account ID which can be obtained from your authorized reseller. If you have already obtained a service account ID, please enter that ID now.

If this server does not have Internet connectivity to the Mitel license server, you must use the offline license generation process. To do this, select the *Enable offline license generation* checkbox below and press the *Activate* button.

Service account ID

Address of Mitel license server or proxy (optional)

TCP port to use for the license server connection (optional)

Enable offline license generation: □

MiVoice Business Solution Virtual Instance 1.0.0.16
MiVoice Border Gateway 11.5.2.31
© Mitel Networks Corporation

14. In the **ServiceLink Activation** screen, enter the following details:

    a. Enter the generated serial number in the Service account ID field.
    b. Enter the address of Mitel License Server or proxy and TCP Port as applicable.
15. Click **Activate**.

4.2.1.4 Offline Sync

This topic provides systematic instruction on how to synchronize the license request offline.

To download the license request file, perform the following steps:

1. Navigate to the **Server Manager** application.
2. On the left page, under **ServiceLink**, click **Status**.

   The **ServiceLink Activation** screen displays.
3. In the **ServiceLink Activation** screen, enter the following details:

   a. Enter the generated serial number in the **Service account ID** field.
   b. Enter the address of Mitel License Server or proxy and TCP Port as applicable.
   c. Select the checkbox next to the **Enable offline license generation**.
4. Click **Activate**.
5. Scroll down and click **Download license request file**.

   The license request file gets downloaded in zip format.

   To upload the license request, perform the following steps:
6. Navigate to **Licenses & Services** home page.
7. Under **Search product/end customer** section, enter the serial number and end customer company details.

8. Click **Start Search**.
9. Click the **View Licenses** icon next to the product release.

   The **Product information** displays with the license information.
10. On the left pane, click **Upload Request**.
11. In the **Upload offline license request**, search and select the license request zip from the local folder.
12. Click **Upload Request**.
13. In the **License** section, click **Download Latest License**.

    The **Latest License** file gets downloaded in zip format.

    To upload the license file, perform the following steps:
14. Navigate to the Server Manager application.
15. On the left pane, under **ServiceLink**, click **Status**.
16. Scroll down and click on the **Upload license file** field to search and select the license zip from the local folder.
17. Once the zip file is selected, click **Upload license file**.

The License is synced to the server manager offline.

4.3 UCC Licensing Procedure

The License Server 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 EID/Serial for the MiVoice Business Solution Virtual Instance deployment.

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 SLS.
- Authorized Partner creates an SLS Serial ID (EID) 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 EID/Serial.
- Authorized Partner creates an associated ULM EID for the MiVoice Business Solution Virtual Instance base EID.
- Authorized Partner assigns MiVoice Business SIP trunk licenses, MBG SIP trunk licenses, UCC User and SWAS licenses to the ULM EID/Serial.
- 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 EID/Serial. The Authorized Partner then selects it and adds the vMBG Serial 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 SLS to the system.

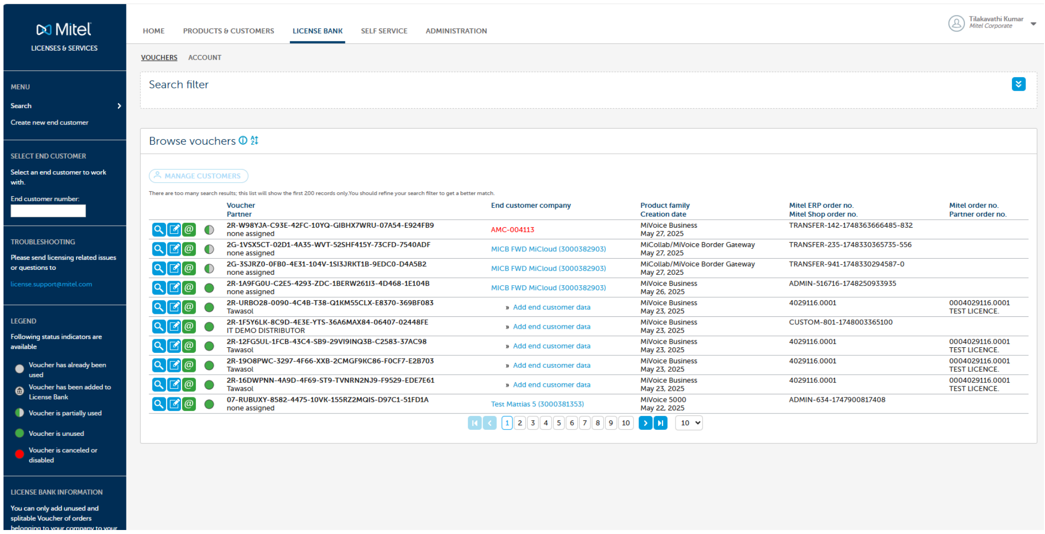
4.3.2 Deploying UCC Licenses

A detailed procedure for deploying UCC licenses follows:

1. Log into the MiAccess portal and then to Licenses & Services Application, for which the following access are needed:
   - MiAccess user account.
   - MiAccess privilege to access Licenses & Services.
2. In the **Licenses & Services** home page, click on the **License Bank** tab. Under the License Bank tab, the list of vouchers are displayed.

> ℹ **Note**:
> In License Server, the end customer is known by the Voucher. The Voucher is the container of licenses that were purchased by the Partner.

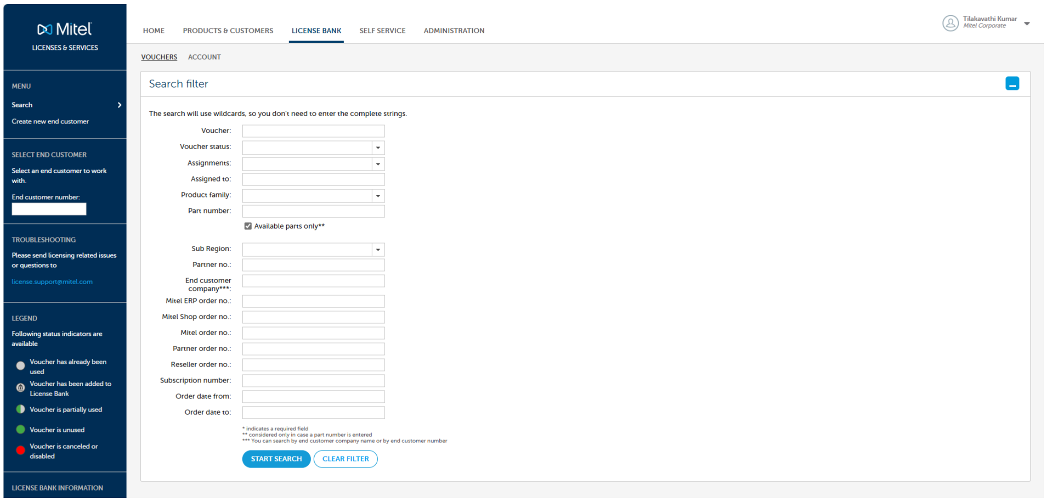
3. Open the voucher window which displays the list of ordered parts.


Mitel
LICENSES & SERVICES
HOME
PRODUCTS & CUSTOMERS
LICENSE BANK
SELF SERVICE
ADMINISTRATION
Tilakavathi Kumar
Mitel Corporate
VOUCHERS
ACCOUNT
MENU
Search
Create new end customer
SELECT END CUSTOMER
Select an end customer to work with.
End customer number:
TROUBLESHOOTING
Please send licensing related issues or questions to
license.support@mitel.com
LEGEND
Following status indicators are available
Voucher has already been used
Voucher has been added to License Bank
Voucher is partially used
Voucher is unused
Voucher is canceled or disabled
LICENSE BANK INFORMATION
You can only add unused and splitable Voucher of orders belonging to your company to your
Search filter
Browse vouchers
MANAGE CUSTOMERS
1 2 3 4 5 6 7 8 9 10
10

There are too many search results; this list will show the first 200 records only.You should refine your search filter to get a better match.

	Voucher Partner	End customer company	Product family Creation date	Mitel ERP order no. Mitel Shop order no.	Mitel order no. Partner order no.
◐	2R-W98YJA-C93E-42FC-10YQ-GIBHX7WRU-07A54-E924FB9 none assigned	AMC-004113	MiVoice Business May 27, 2025	TRANSFER-142-1748363666485-832	
◐	2G-1VSX5CT-02D1-4A35-WVT-52SHF415Y-73CFD-7540ADF none assigned	MICB FWD MiCloud (3000382903)	MiCollab/MiVoice Border Gateway May 27, 2025	TRANSFER-235-1748330365735-556	
◐	2G-3SJRZ0-0FB0-4E31-104V-1SI3JRKT1B-9EDC0-D4A5B2 none assigned	MICB FWD MiCloud (3000382903)	MiCollab/MiVoice Border Gateway May 27, 2025	TRANSFER-941-1748330294587-0	
●	2R-1A9FG0U-C2E5-4293-ZDC-1BERW261I3-4D468-1E104B none assigned	MICB FWD MiCloud (3000382903)	MiVoice Business May 26, 2025	ADMIN-516716-1748250933935	
●	2R-URBO28-0090-4C4B-T38-Q1KM55CLX-E8370-369BF083 Tawasol	» Add end customer data	MiVoice Business May 23, 2025	4029116.0001	0004029116.0001 TEST LICENCE.
●	2R-1F5Y6LK-8C9D-4E3E-YTS-36A6MAX84-06407-02448FE IT DEMO DISTRIBUTOR	» Add end customer data	MiVoice Business May 23, 2025	CUSTOM-801-1748003365100	
●	2R-12FG5UL-1FCB-43C4-SB9-29VI9INQ3B-C2583-37AC98 Tawasol	» Add end customer data	MiVoice Business May 23, 2025	4029116.0001	0004029116.0001 TEST LICENCE.
●	2R-19O8PWC-3297-4F66-XXB-2CMGF9KC86-F0CF7-E2B703 Tawasol	» Add end customer data	MiVoice Business May 23, 2025	4029116.0001	0004029116.0001 TEST LICENCE.
●	2R-16DWPNN-4A9D-4F69-ST9-TVNRN2NJ9-F9529-EDE7E61 Tawasol	» Add end customer data	MiVoice Business May 23, 2025	4029116.0001	0004029116.0001 TEST LICENCE.
●	07-RUBUXY-8582-4475-10VK-155RZ2MQIS-D97C1-51FD1A none assigned	Test Mattias 5 (3000381353)	MiVoice 5000 May 22, 2025	ADMIN-634-1747900817408	

Figure 7: Voucher list



The search will use wildcards, so you don't need to enter the complete strings.

Voucher:
Voucher status:
Assignments:
Assigned to:
Product family:
Part number:
☑ Available parts only**

Sub Region:
Partner no.:
End customer company***:
Mitel ERP order no.:
Mitel Shop order no.:
Mitel order no.:
Partner order no.:
Reseller order no.:
Subscription number:
Order date from:
Order date to:

* indicates a required field
** considered only in case a part number is entered
*** You can search by end customer company name or by end customer number

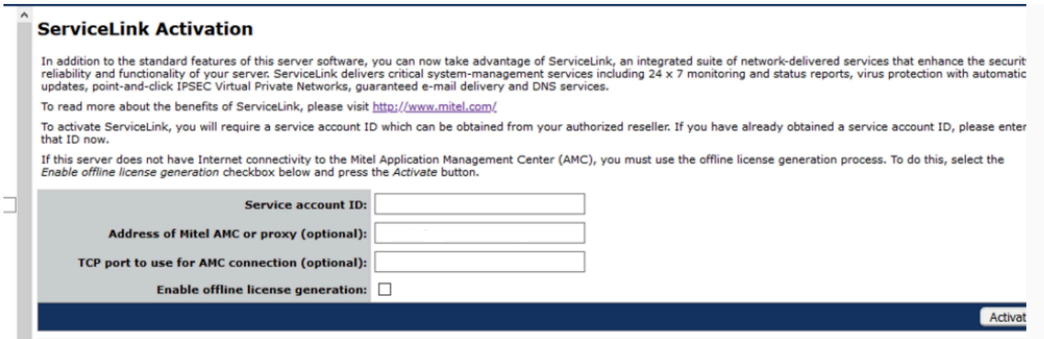
Figure 8: Voucher Search

> **Note**:
>
> You can use the Search function to locate specific part numbers or license descriptions from the voucher list.

4. Register the voucher and click **Next.**
5. Under **Select System**, enter the Release number.

   If it is a new registration, select the **Register new system** from left panel, enter the required details. Click **Next** .
6. Then **Select Items** and **Submit Changes** click and Generate **License**.
7. A confirmation or processing message is displayed and the **Serial ID** or the **ServiceLink ID** is generated.

8. In the MiVoice Business Solution Virtual Instance ServiceLink Activation page, enter the generated ServiceLink ID and License Server proxy address as **sync.sls.mitel.com** and click **Activate**.



ServiceLink Activation

In addition to the standard features of this server software, you can now take advantage of ServiceLink, an integrated suite of network-delivered services that enhance the securit reliability and functionality of your server. ServiceLink delivers critical system-management services including 24 x 7 monitoring and status reports, virus protection with automatic updates, point-and-click IPSEC Virtual Private Networks, guaranteed e-mail delivery and DNS services.

To read more about the benefits of ServiceLink, please visit http://www.mitel.com/

To activate ServiceLink, you will require a service account ID which can be obtained from your authorized reseller. If you have already obtained a service account ID, please enter that ID now.

If this server does not have Internet connectivity to the Mitel Application Management Center (AMC), you must use the offline license generation process. To do this, select the *Enable offline license generation* checkbox below and press the *Activate* button.

Service account ID:

Address of Mitel AMC or proxy (optional):

TCP port to use for AMC connection (optional):

Enable offline license generation: □

9. Once the License is activated, the **ServiceLink Status Information** page shows the status report. The activated licenses can be viewed in the **Licensing Information** page.

4.4 Mitel Software Assurance

Software Assurance is Mitel's support program for lifecycle management of Mitel Software solutions. It enables organizations to maintain operational excellence of their Mitel software by keeping these assets current, delivers and maintains operation of cloud applications, and enables entitlement to Mitel Technical Support resources to address incidents or technical issues not resolvable by themselves or their authorized Mitel Partner. It also provides access to Mitel Performance Analytics (MPA) for fault reporting and performance analytics.

For more information on Software Assurance: Please refer to the most recent Software Assurance Program Guide for the latest information.: https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/f0db86d7-50c6-4923-81d0-0292a20aa11b?source=

The quantities of Software Assurance part numbers are calculated using the "SWA points" pricing model. For more information on this model, Refer to the latest **Points-based Software Assurance Pricing Explained** document, https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/dc3014b4-07bb-43e2-b2a8-40dc47ab3147?source=SAMLSSO

For more information on how to quote and purchase Software Assurance for license add-ons, please refer to the latest **Ordering Information for Aligned Software Assurance with License Add-ons** document: https://nuxeo.unify.com/nuxeo/site/proxy/nxdoc/view/raw/7bc12426-aabf-499d-9819-ba950ed9aa90?source=SAMLSSO "

Deploy Virtual Machine 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 Deploying on VMware

Users can deploy SVI on VMware:

- directly onto the ESXi host
- onto the ESXi host via vCenter Manager, or
- onto the 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.

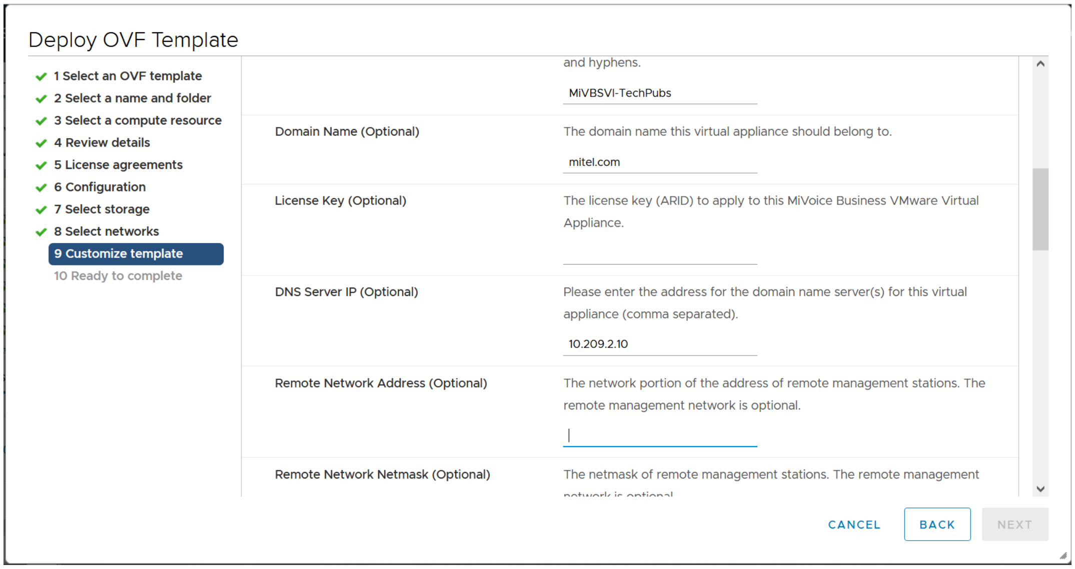
       .

    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** , **Second LAN IP Address** and **Default Gateway Address**.

> **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. Click **NEXT**.



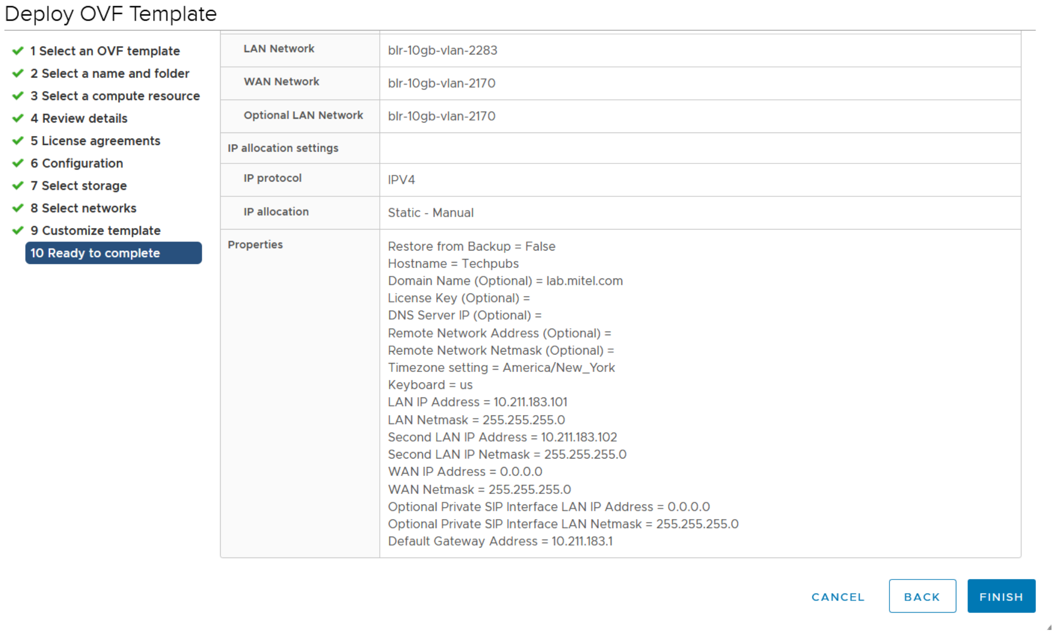
Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- 9 Customize template
- 10 Ready to complete

	and hyphens. MiVBSVI-TechPubs
Domain Name (Optional)	The domain name this virtual appliance should belong to. mitel.com
License Key (Optional)	The license key (ARID) to apply to this MiVoice Business VMware Virtual Appliance.
DNS Server IP (Optional)	Please enter the address for the domain name server(s) for this virtual appliance (comma separated). 10.209.2.10
Remote Network Address (Optional)	The network portion of the address of remote management stations. The remote management network is optional.
Remote Network Netmask (Optional)	The netmask of remote management stations. The remote management network is optional.

Figure 9: Customize template

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



Deploy OVF Template

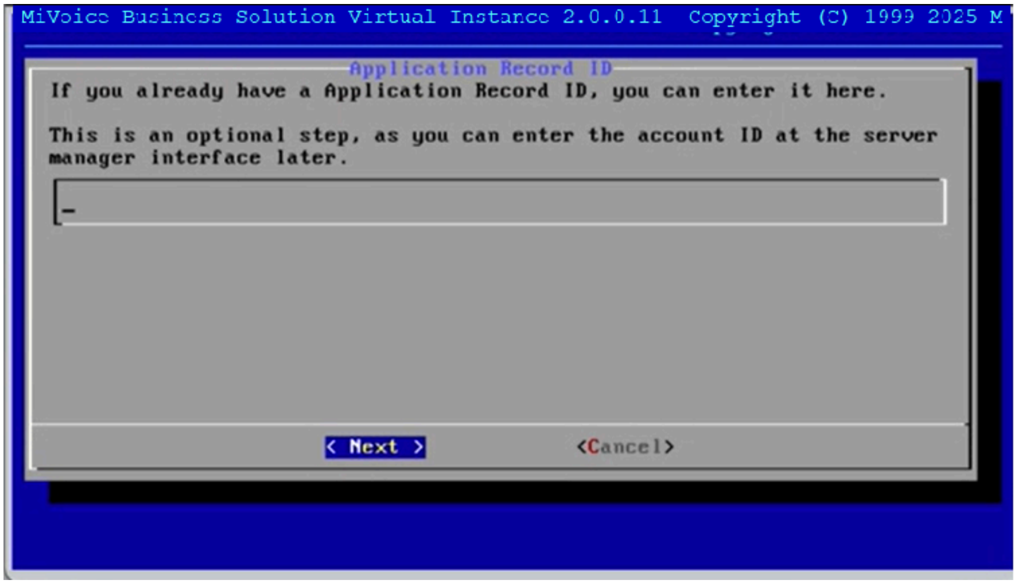
- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- ✓ 9 Customize template
- 10 Ready to complete

LAN Network	blr-10gb-vlan-2283
WAN Network	blr-10gb-vlan-2170
Optional LAN Network	blr-10gb-vlan-2170
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual
Properties	Restore from Backup = False Hostname = Techpubs Domain Name (Optional) = lab.mitel.com License Key (Optional) = DNS Server IP (Optional) = Remote Network Address (Optional) = Remote Network Netmask (Optional) = Timezone setting = America/New_York Keyboard = us LAN IP Address = 10.211.183.101 LAN Netmask = 255.255.255.0 Second LAN IP Address = 10.211.183.102 Second LAN IP Netmask = 255.255.255.0 WAN IP Address = 0.0.0.0 WAN Netmask = 255.255.255.0 Optional Private SIP Interface LAN IP Address = 0.0.0.0 Optional Private SIP Interface LAN Netmask = 255.255.255.0 Default Gateway Address = 10.211.183.1

Figure 10: 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 **SLS Serial ID** page is displayed, click **Next**.



```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999 2025 M

Application Record ID
If you already have a Application Record ID, you can enter it here.

This is an optional step, as you can enter the account ID at the server
manager interface later.

_

< Next >                <Cancel>
```

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 Deploying 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

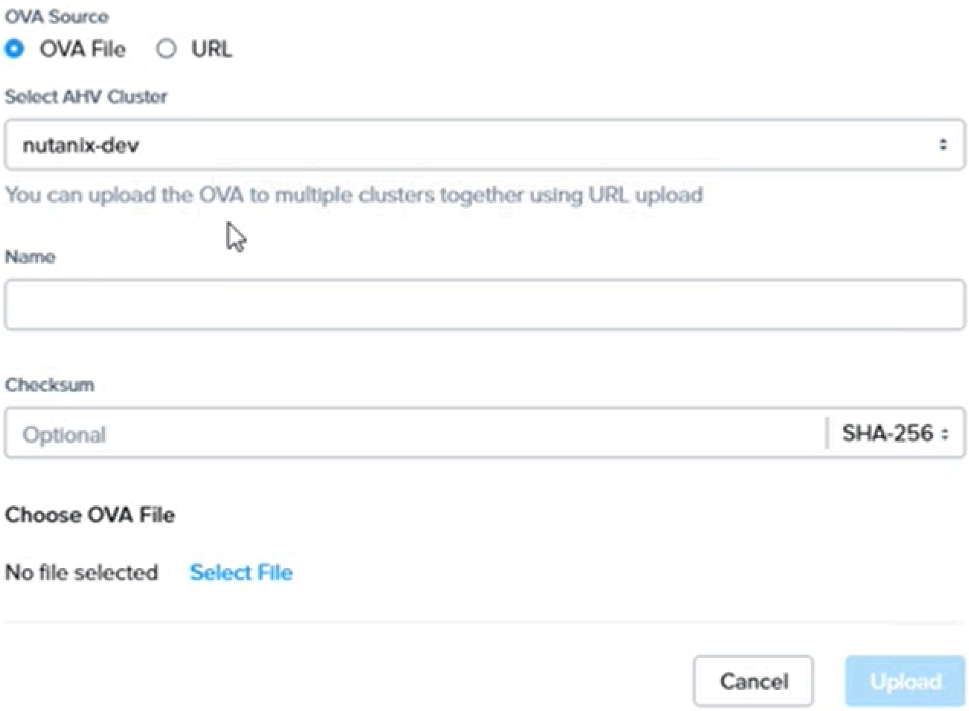
Upload OVA on Nutanix Prism

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.



OVA Source

● OVA File ○ URL

Select AHV Cluster: nutanix-dev

You can upload the OVA to multiple clusters together using URL upload

Name:

Checksum: Optional | SHA-256

Choose OVA File

No file selected

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

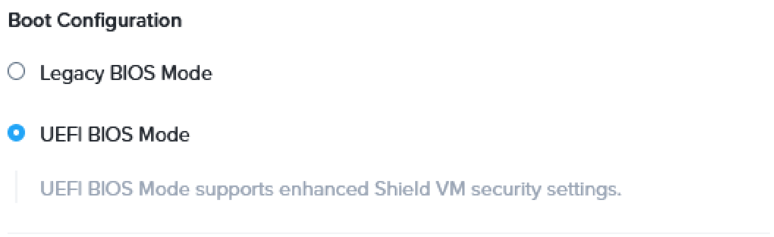
Deploy a VM using the uploaded MiVoice Business Solution Virtual Instance OVA.

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 **UEFI BIOS Mode**.



Boot Configuration

○ Legacy BIOS Mode

● UEFI BIOS Mode

UEFI BIOS Mode supports enhanced Shield VM security settings.

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**.

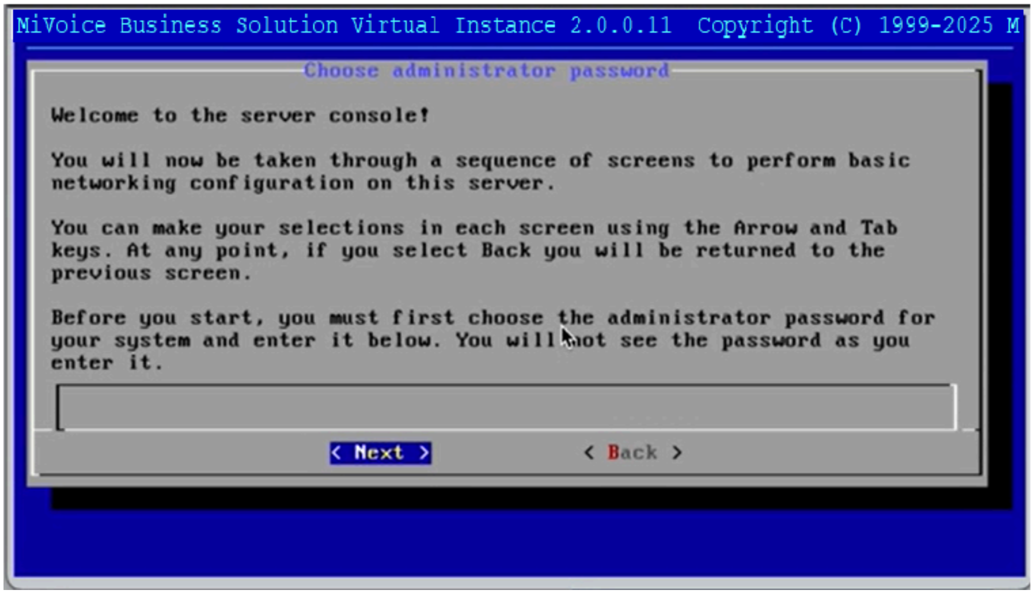
    You can check if the VM is created by by navigating to **Dashboard** > **Computer & Storage** > **VMs** panel.
12. Navigate navigate to **Computer & Storage** > **VMs**.
13. Select the newly created VM.

    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.

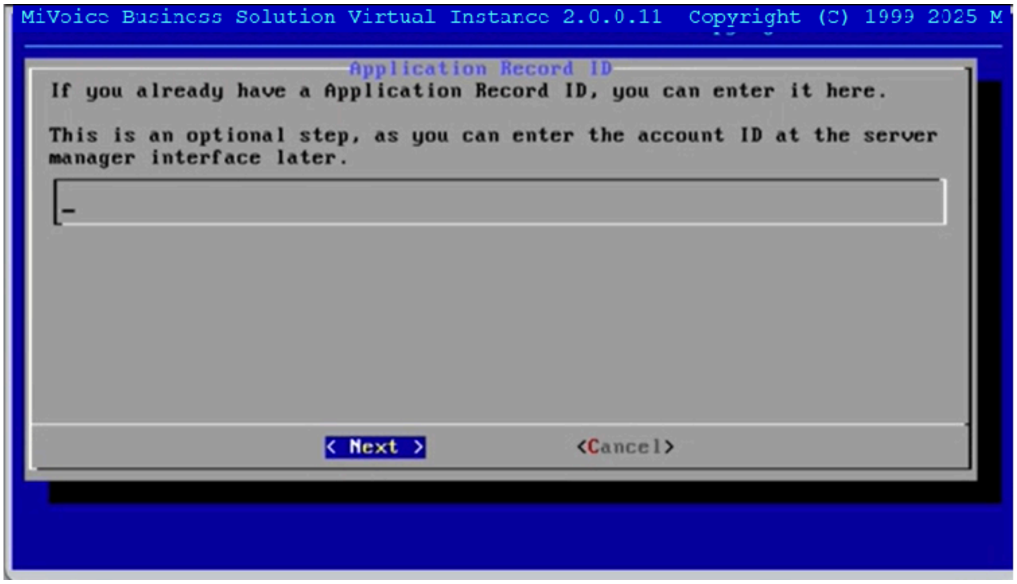
    a. In the **Select Keyboard Language window**, select the language and click **Next**.
    b. In the **Restore From Backup** window, click **No**.
    c. In the **Choose administrator password** window, enter the password and click **Next**.



```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M

Choose administrator password

Welcome to the server console!

You will now be taken through a sequence of screens to perform basic
networking configuration on this server.

You can make your selections in each screen using the Arrow and Tab
keys. At any point, if you select Back you will be returned to the
previous screen.

Before you start, you must first choose the administrator password for
your system and enter it below. You will not see the password as you
enter it.
```

    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 **SLS Serial ID** (optional), enter the account ID and click **Next**.

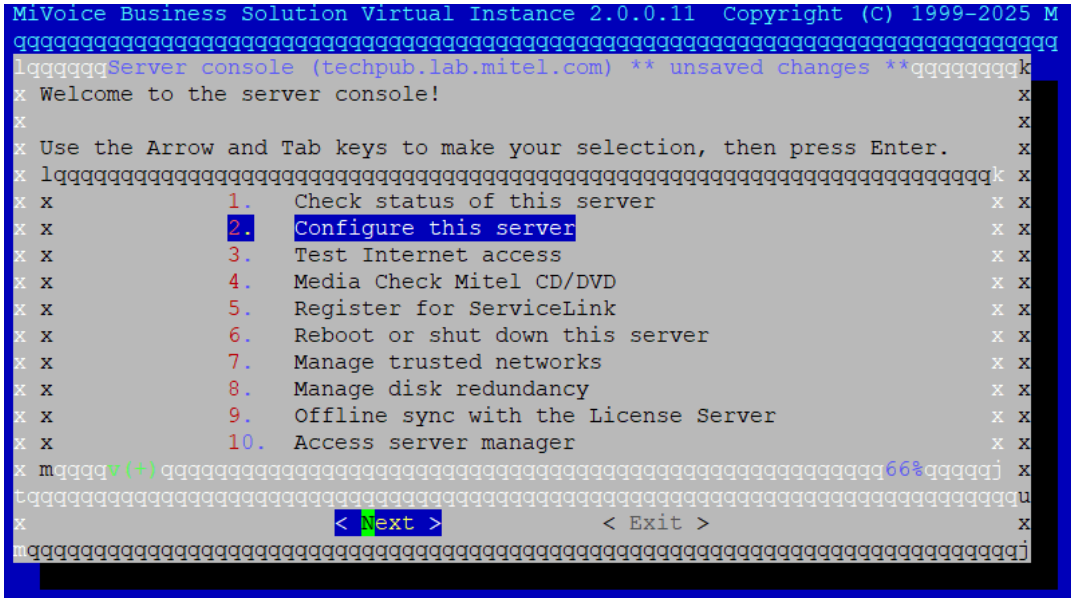


```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999 2025 M

Application Record ID
If you already have a Application Record ID, you can enter it here.

This is an optional step, as you can enter the account ID at the server
manager interface later.
```

    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**.



```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqServer console (techpub.lab.mitel.com) ** unsaved changes **qqqqqqqqk
x Welcome to the server console!                                          x
x                                                                         x
x Use the Arrow and Tab keys to make your selection, then press Enter.    x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk  x
x x              1.    Check status of this server                    x  x
x x              2.    Configure this server                          x  x
x x              3.    Test Internet access                           x  x
x x              4.    Media Check Mitel CD/DVD                       x  x
x x              5.    Register for ServiceLink                       x  x
x x              6.    Reboot or shut down this server                x  x
x x              7.    Manage trusted networks                        x  x
x x              8.    Manage disk redundancy                         x  x
x x              9.    Offline sync with the License Server           x  x
x x              10.   Access server manager                          x  x
x mqqqqv(+)qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq66%qqqqqj  x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                        < Next >            < Exit >                     x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

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 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 **SLS Serial ID (EID)** (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**,

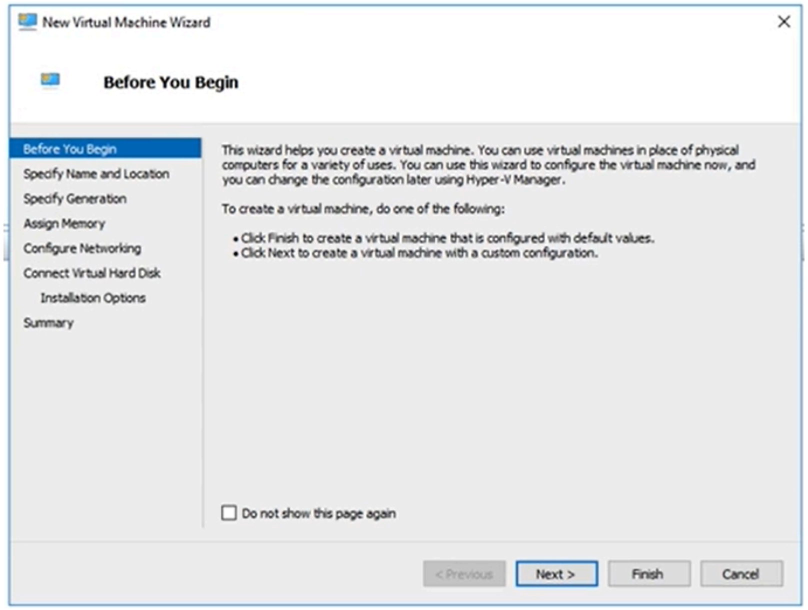
    a. from **Secure shell access** drop-down list, select **Allow public access (entire Internet)**.
    b. from **Allow administrative command line access over secure shell**, drop-down, select **Yes**.
    c. from **Allow secure shell access using standard password** drop-down, select **Yes**.
21. Click **Save**.
22. Proceed with next section.

5.3 Deploying 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.



This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

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 2** and click **Next**.
6. In the **Assign Memory** window, enter the **Startup memory** and click **Next**.

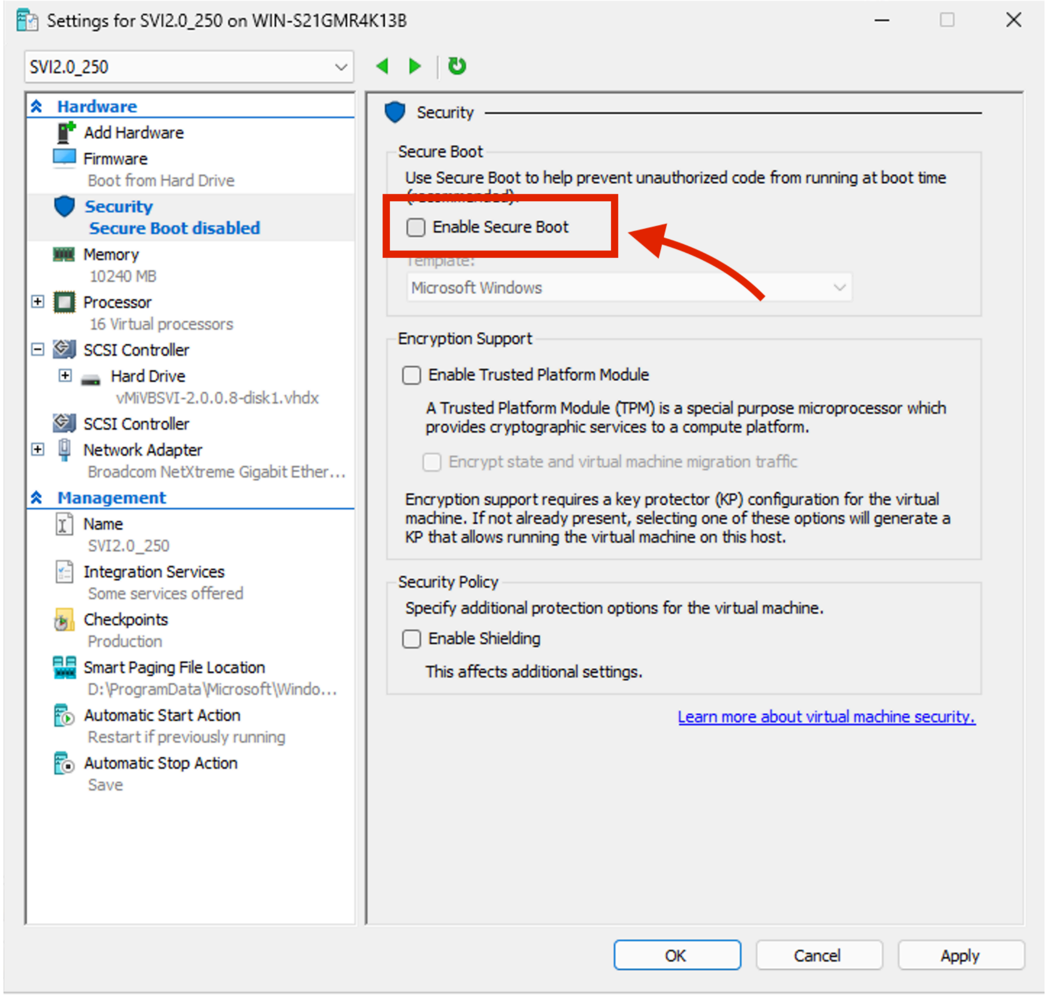
   The memory value depends on the planned system user capacity. Refer to the table MiVoice Business Solution Virtual Instance system size for the details. For example, 250 user system capacity deployment would configure 4 vCPU, 1 Core per CPU and 10 GB memory.

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**.

- Under **Security**, make sure **Enable Secure Boot** is **disabled**.



Settings for SVI2.0_250 on WIN-S21GMR4K13B

SVI2.0_250

Hardware
Add Hardware
Firmware
Boot from Hard Drive
Security
Secure Boot disabled
Memory
10240 MB
Processor
16 Virtual processors
SCSI Controller
Hard Drive
vMiVBSVI-2.0.0.8-disk1.vhdx
SCSI Controller
Network Adapter
Broadcom NetXtreme Gigabit Ether...
Management
Name
SVI2.0_250
Integration Services
Some services offered
Checkpoints
Production
Smart Paging File Location
D:\ProgramData\Microsoft\Windo...
Automatic Start Action
Restart if previously running
Automatic Stop Action
Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

□ Enable Secure Boot

Template:
Microsoft Windows

Encryption Support

□ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

□ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

Specify additional protection options for the virtual machine.

□ Enable Shielding

This affects additional settings.

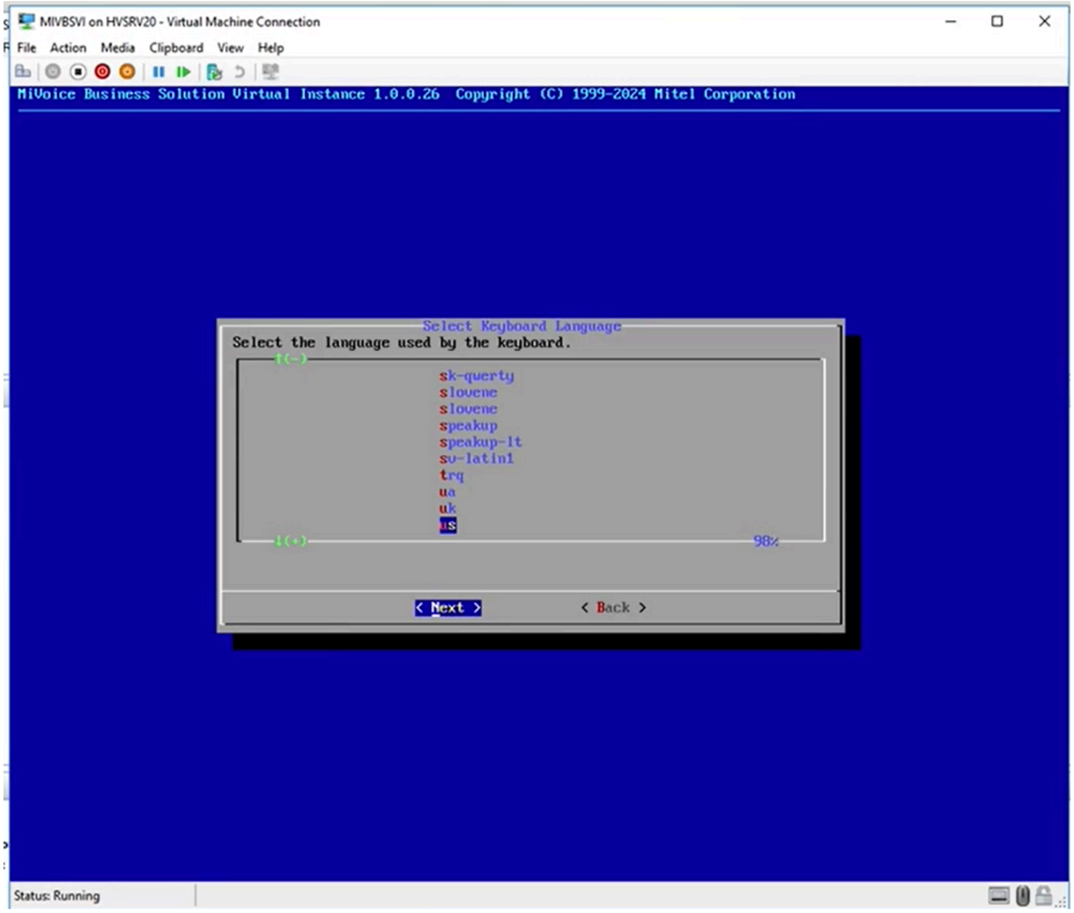
Learn more about virtual machine security.

- 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.



```
MiVoice Business Solution Virtual Instance 1.0.0.26  Copyright (C) 1999-2024 Mitel Corporation

                    Select Keyboard Language
Select the language used by the keyboard.
     ↑(-)
                       sk-qwerty
                       slovene
                       slovene
                       speakup
                       speakup-lt
                       sv-latin1
                       trq
                       ua
                       uk
                       us
     ↓(+)                                        98%

                  < Next >         < Back >
```

13. Follow the procedure from Step 16 > step b to step j in Deploying 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 Deploying on Nutanix Prism on page 63.

5.4 Deploying on Proxmox VE 8.3

Proxmox VE 8.3 simplifies importing and deploying OVA files by eliminating the manual steps that were required in older versions. In Proxmox VE version 8.3 and higher, one can import OVA files directly from the portal UI.

Deploying a VM from OVA on Proxmox VE 8.3 involves these stages:

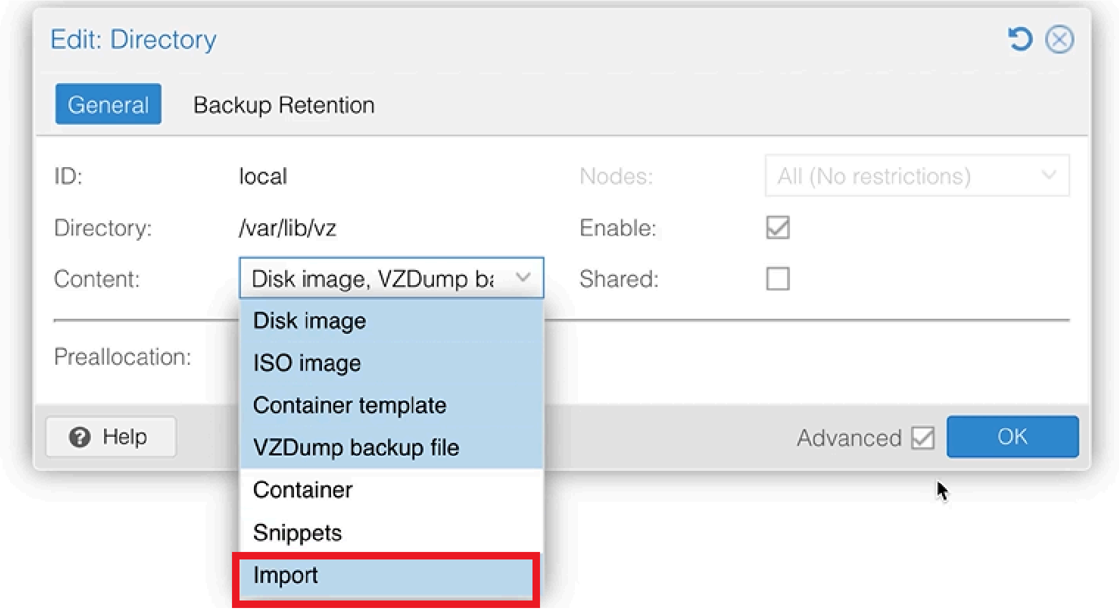
1. Configure Proxmox VE to import OVA files

2. Upload or import MiVB SVI OVA
3. Deploy MiVB SVI VM from OVA

Configure Proxmox VE to import OVA files

1. Log into the **Proxmox VE 8.3** or later version.

   Proxmox VE supports importing of various image formats including ISO files, raw disk images and container templates. However, importing of OVA image format is not enabled by default. Hence a one-time configuration is required to allow the import of the OVA files, as suggested in the following steps.
2. From the dashboard, click on **Datacenter** > **Storage**. There are two storage types available by default **local** and **local-lvm**. There could be additional storage types available on the server depending on configuration such as **NFS** and **CephFS**. One can only import OVA files to **Directory** based storage.
3. Select a storage of type **Directory** and click on **Edit** to enable the import from the drop-down list and then click **OK**.



Edit: Directory

ID: local

Directory: /var/lib/vz

Content: Disk image, VZDump bɛ

Nodes: All (No restrictions)

Enable: ☑

Shared: □

Preallocation:

Advanced ☑

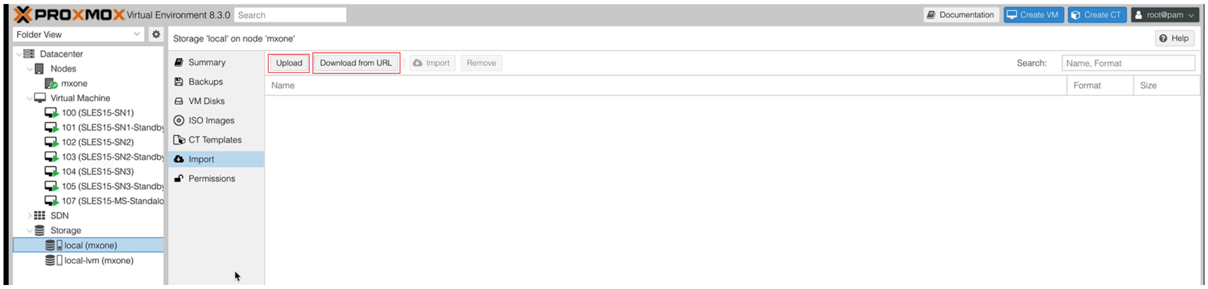
Upload or Import MiVB SVI OVA

To Import a MiVB SVI OVA file, perform the following:

1. Login to **Proxmox VE 8.3** or later version.
2. From the dashboard, select the **Folder View** on the left top panel, as shown in the screenshot below. Click on **Datacenter** > **Storage**, navigate to the specific storage location where we enabled the import feature, and then select Import.

   There are two ways to import the OVA files:

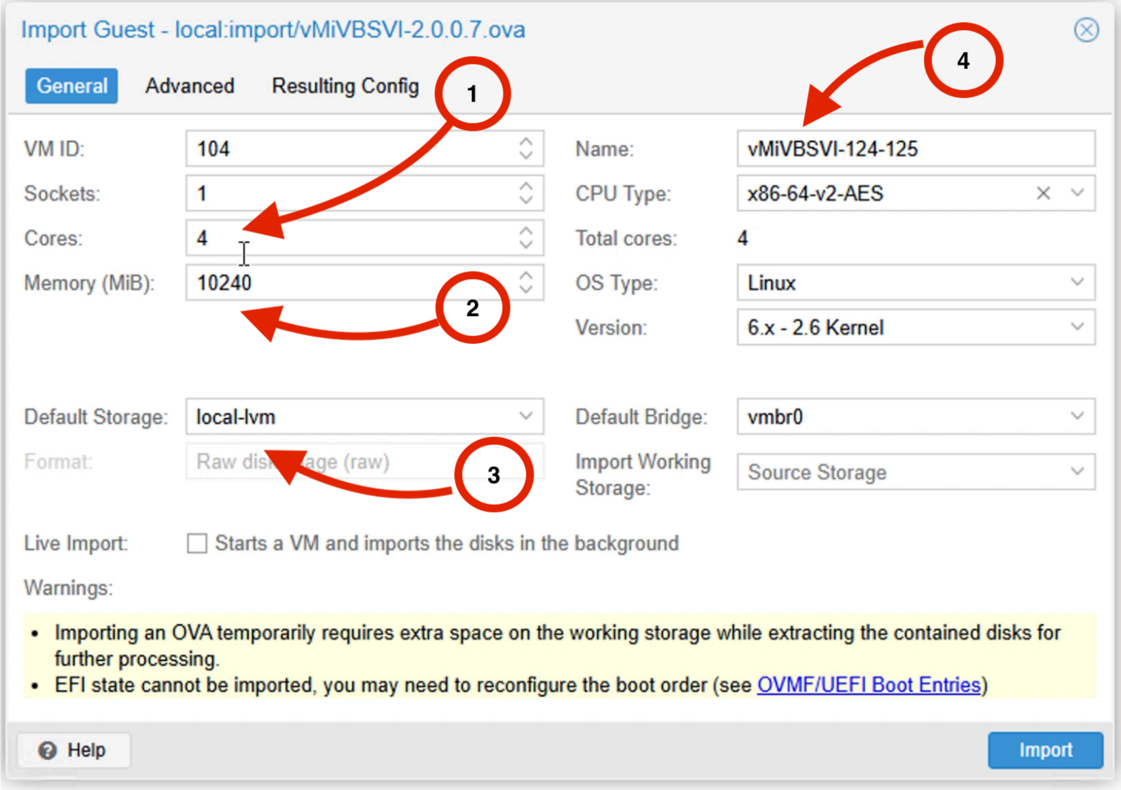
   a. By clicking the Download from URL button.
   b. By Uploading from your Local folder.



Deploying MiVB SVI VM from OVA

Deploy new MiVB SVI virtual machines using the provided OVA file. The allocated hardware resources during deployment depend on the selected model, refer to table MiVoice Business Solution Virtual Instance system size for more information.

The created VM is configured to use the **VirtIO KVM** modules for the **SCSI controller** and **Ethernet interface**, as these drivers provide the best performance on Proxmox.



Import Guest - local:import/vMiVBSVI-2.0.0.7.ova

VM ID: 104

Sockets: 1

Cores: 4

Memory (MiB): 10240

Name: vMiVBSVI-124-125

CPU Type: x86-64-v2-AES

Total cores: 4

OS Type: Linux

Version: 6.x - 2.6 Kernel

Default Storage: local-lvm

Format: Raw disk image (raw)

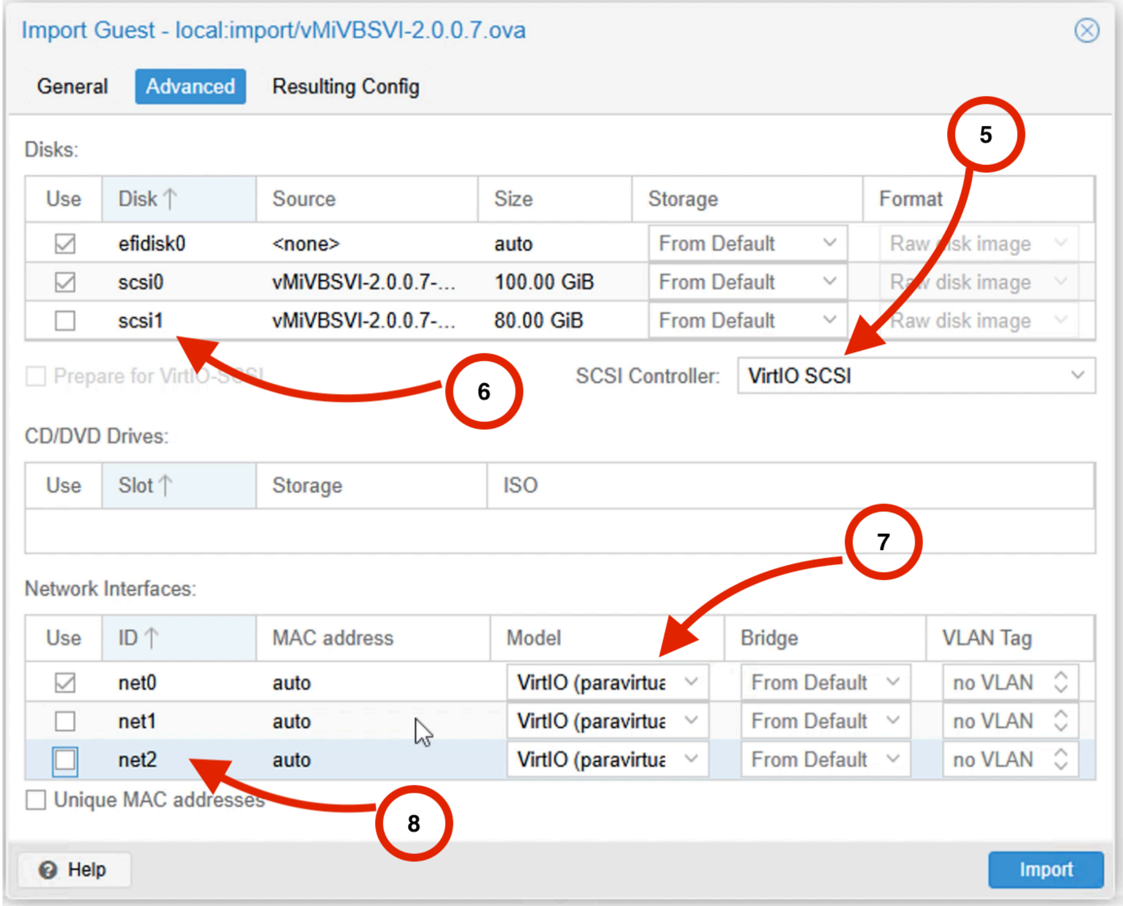
Default Bridge: vmbr0

Import Working Storage: Source Storage

Live Import: □ Starts a VM and imports the disks in the background

Warnings:

- Importing an OVA temporarily requires extra space on the working storage while extracting the contained disks for further processing.
- EFI state cannot be imported, you may need to reconfigure the boot order (see OVMF/UEFI Boot Entries)



Import Guest - local:import/vMiVBSVI-2.0.0.7.ova

General | Advanced | Resulting Config

Disks:

Use	Disk ↑	Source	Size	Storage	Format
☑	efidisk0	<none>	auto	From Default	Raw disk image
☑	scsi0	vMiVBSVI-2.0.0.7-...	100.00 GiB	From Default	Raw disk image
□	scsi1	vMiVBSVI-2.0.0.7-...	80.00 GiB	From Default	Raw disk image

□ Prepare for VirtIO-SCSI

SCSI Controller: VirtIO SCSI

CD/DVD Drives:

Use	Slot ↑	Storage	ISO

Network Interfaces:

Use	ID ↑	MAC address	Model	Bridge	VLAN Tag
☑	net0	auto	VirtIO (paravirtua	From Default	no VLAN
□	net1	auto	VirtIO (paravirtua	From Default	no VLAN
□	net2	auto	VirtIO (paravirtua	From Default	no VLAN

□ Unique MAC addresses

After starting the SVI VM, the first step is configuring the **2 LAN IP addresses** on the default LAN. If deploying in server gateway mode, **WAN** and **Optional LAN IP addresses** can also be configured. To configure the IP addresses and other networking parameters, run the admin console from the terminal.

5.4.1 Deploying on Proxmox VE 8.2 and below

Deploying a VM from OVA on Proxmox VE involves these stages:

1. Copy OVA file to Proxmox VE host system.
2. Extract the OVA file.
3. Create SVI VM by importing the OVF file.
4. Modify the hardware properties of the new VM.
5. Boot up the SVI VM and Configure.
6. Power up the VM and perform any modifications.

5.4.1.1 Copy the OVA file to the Proxmox VE host system

Copy the OVA file to the Proxmox VE host using scp, ftp, or other methods. The OVA file can also be downloaded directly from the terminal via HTTP after logging into Proxmox VE.

1. Log into the Proxmox VE.

    a. Enter your login User ID.
    b. Enter your Password.
2. Navigate to **Dashboard** > **Nodes** > **host** and select any one of the hostnames.
3. From the **Host**, select the **shell**.
4. Create a folder to download the OVA file.
5. Use a utility tool such as SCP or FTP to download the OVA file to the created folder.

5.4.1.2 Extract the OVA file

To extract the OVA file copy the `tar xvf vMiVBSVI-2.x.x.x.ova .`

After extracting the OVA file (using tar), one typically finds the vmdk (disk image), ovf, and mf files.

5.4.1.3 Create an SVI VM by importing the OVF file

A VM on Proxmox can be created by importing the OVF file using the `qm` utility.

To import an OVF file and create an SVI VM in Proxmox:

1. Log in to Proxmox.
2. Go to **Datacenter** -> **Nodes** -> **mxo** -> **Shell** and execute the command:

```
# qm importovf "Unused VM ID" OVF_File storage
```

Note:
Unused **VM ID** with an free unused VM ID. On Proxmox, typically VM IDs start from 100 onwards and are incremented for newly created VMs. The list of existing VM can be observed under PVE portal on the left panel under **Virtual Machine** when **Folder View** is chosen. Pick an ID that is free and unused.

Example: `qm importovf 108 ./vMiVBSVI.ovf local-lvm`

# 108 is the unused VM ID # vMiVBSVI.ovf is the extracted SVI OVF file

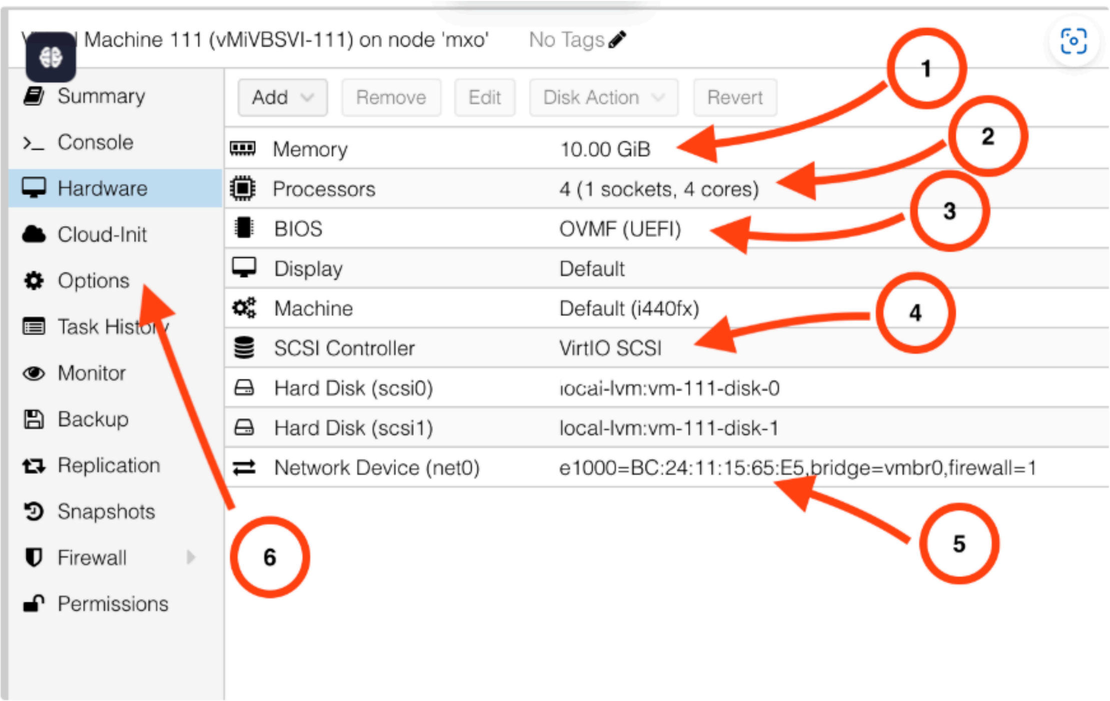
# "local-lvm" is the storage disk where the VM will be stored. "local-lvm" storage option will always be present, but this could be SAN, SSD or any other storage attached to Proxmox.

3. Press **Enter** to start the import process.

5.4.1.4 Modify the hardware properties of the new VM

Even though it is expected that the newly created VM would inherit all the hardware properties from the OVF file, it may not be accurate. Hence the VM hardware properties need to be verified and corrected if necessary. Also one or more network adapter(s) need to be added based on the deployment mode - **Server Gateway** mode or **Server Only** mode.

In Proxmox VM page select the newly created VM and click on **Hardware**.



Memory	10.00 GiB
Processors	4 (1 sockets, 4 cores)
BIOS	OVMF (UEFI)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
Hard Disk (scsi0)	ıocai-lvm:vm-111-disk-0
Hard Disk (scsi1)	local-lvm:vm-111-disk-1
Network Device (net0)	e1000=BC:24:11:15:65:E5,bridge=vmbr0,firewall=1

Note:

If you are installing CloudLink Gateway as a blade on MiVoice Border Gateway, then you must allocate an additional 1 GB RAM.

Table 16: MiVoice Business Solution Virtual Instance system size

Virtual Appliance	Release	System Capacity	Configuration		Resource Reservation	
			vCPU	Disk	CPU	Memory
MiVoice Business Solution Virtual Instance	2.0	250	4	100	4 GHz	10 GB
		500	6	180	6 GHz	12 GB

Required Modifications for Hardware Properties:

1. Set the memory to 10 GB if using **small business** deployment, else 12 GB for **Enterprise**.
2. Set the CPU processor to 4 for both **small business** and **Enterprise** deployments
3. Set the appropriate BIOS mode
   a. For SVI 2.x, set the mode to OVMF (UEFI). SVI 2 switched over to UEFI from legacy BIOS mode.
   b. If you are deploying SVI 1.0 FP1 release (1.0.0.31), then keep the **BIOS** mode to **Default (SeaBIOS)**.
4. Set the SCSI Controller to **VirtIO SCSI**.
5. Then add one or more network devices as per the deployment configuration. A **Server Only** deployment with require only one LAN network interface while **Server Gateway** will need more for WAN and the Option LAN network interface. For network devices, set the Model as **VirtIO (paravirtualized**).
6. Change the name of the VM if required, under the Options panel of the VM.

5.4.1.5 Boot up the SVI VM and Configure

Once the deployment steps are completed, the VM can be started up:

- After the VM boots, the initial task is to configure primary and secondary IP addresses on the default LAN, as only network devices were added before. In Server Gateway mode, WAN and Optional LAN interfaces should also be configured.
- After network configuration, once the VM boots up, the rest of the SVI configuration steps can be followed as shown in the Perform Configuration chapter.

5.4.1.6 Power up the VM and perform any modifications

Power up the VM and perform any modifications to the network parameters if desired.

Application Installation and Upgrade 6

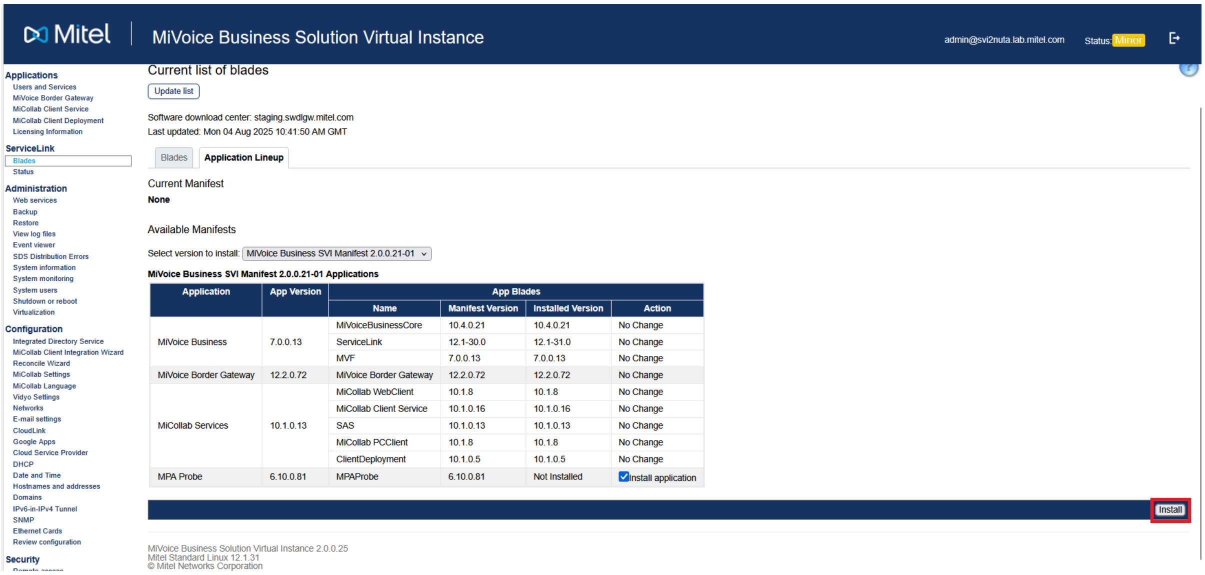
You can install the application software by downloading and installing the application software from the Software Download Center (SWDLC).

1. Log in to the MiVoice Business Solution Virtual Instance Server Manager.
2. In the left pane, click **ServiceLink** and then click **Blades** > **Application Lineup** tab.
3. In the *Available Manifests* section, select the version you want to install from the dropdown list.
4. Review the applications listed under the selected manifest. The **MiVoice Business SVI Manifest 2.0.0.21-01 Applications** table displays the following information for each application: Application name, App Version, Manifest Version, Installed Version, and Action required.
5. For each application you want to install:

    - Locate the application in the list.
    - In the **Action** column, click the **Install application** checkbox.

> **Note**:
> Certain applications are mandatory and do not display a checkbox in the Install Applications list; they are installed automatically.

6. Click the **Install** button to install the required application.



Current list of blades

Software download center: staging.swdlgw.mitel.com
Last updated: Mon 04 Aug 2025 10:41:50 AM GMT

Current Manifest
None

Available Manifests

Select version to install: MiVoice Business SVI Manifest 2.0.0.21-01

MiVoice Business SVI Manifest 2.0.0.21-01 Applications

Application	App Version	App Blades			
		Name	Manifest Version	Installed Version	Action
MiVoice Business	7.0.0.13	MiVoiceBusinessCore	10.4.0.21	10.4.0.21	No Change
		ServiceLink	12.1-30.0	12.1-31.0	No Change
		MVF	7.0.0.13	7.0.0.13	No Change
MiVoice Border Gateway	12.2.0.72	MiVoice Border Gateway	12.2.0.72	12.2.0.72	No Change
MiCollab Services	10.1.0.13	MiCollab WebClient	10.1.8	10.1.8	No Change
		MiCollab Client Service	10.1.0.16	10.1.0.16	No Change
		SAS	10.1.0.13	10.1.0.13	No Change
		MiCollab PCClient	10.1.8	10.1.8	No Change
		ClientDeployment	10.1.0.5	10.1.0.5	No Change
MPA Probe	6.10.0.81	MPAProbe	6.10.0.81	Not Installed	☑ Install application

MiVoice Business Solution Virtual Instance 2.0.0.25
Mitel Standard Linux 12.1.31
© Mitel Networks Corporation

Migration 7

This chapter contains the following sections:

- Prerequisites
- Migration of VMware to Proxmox
- Upgrading from existing SVI 1.0 to SVI 2.0

7.1 Prerequisites

- An SVI VM running on SVI 1.0 FP1 release or higher on the VMWare platform.
- Destination Proxmox VE system must be running 8.0 or higher

7.2 Migration of VMware to Proxmox

Migrating VMs from VMware to Proxmox involves moving virtual machines from vSphere/ESXi to Proxmox Virtual Environment, an open-source alternative based on KVM and LXC

The migration from VMware to Proxmox involves four steps:

1. Adding ESXi storage on Proxmox
2. Shutdown the existing VMWare VM for migration
3. Importing the VM
4. Configuring the migrated VM (Optional)

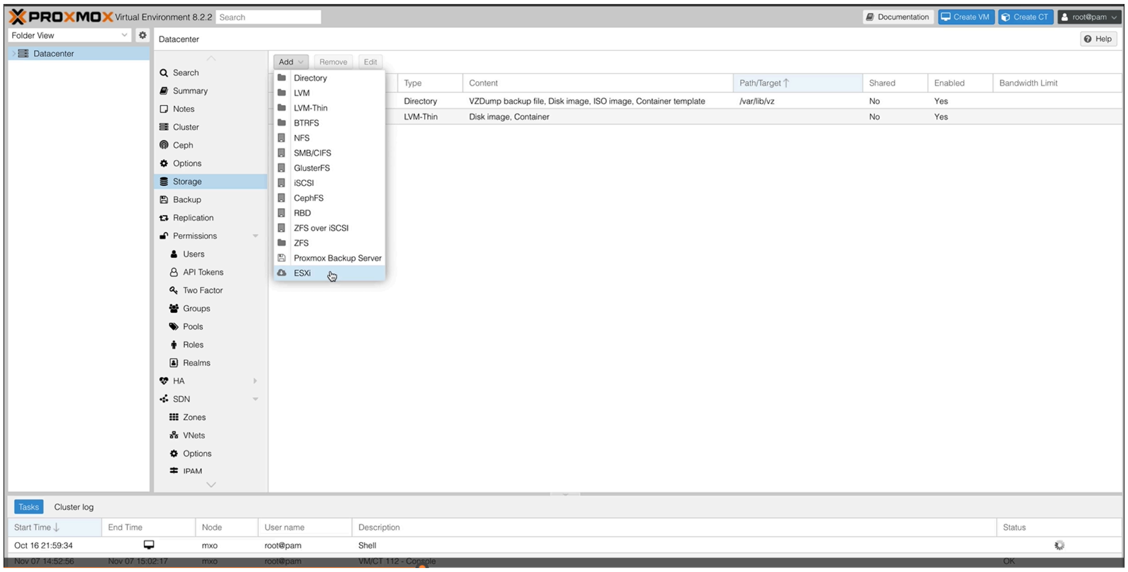
7.2.1 Adding ESXi storage on Proxmox

The existing VMWare ESXi storage can be mounted on the Proxmox VE as an additional storage medium. Once mounted, one has access to all the VMs running on the ESXi. This serves as the first step in the migration process.

To add the ESXi host to Proxmox as storage, perform the following:

1. Login to Proxmox VE.

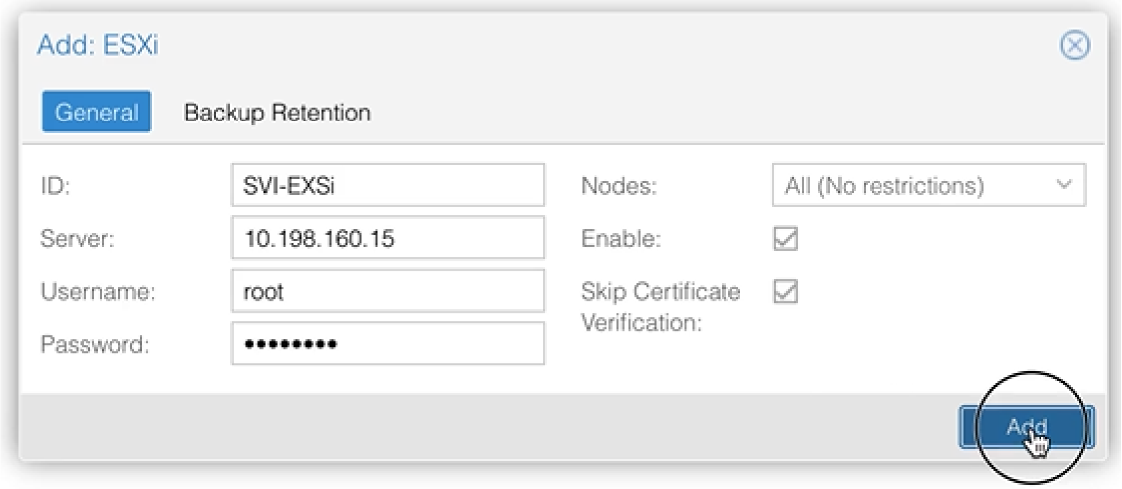
   From the dashboard, click on **Datacenter** > **Storage** > **Add** > **ESXi**.



Type	Content	Path/Target ↑	Shared	Enabled	Bandwidth Limit
Directory	VZDump backup file, Disk image, ISO image, Container template	/var/lib/vz	No	Yes	
LVM-Thin	Disk image, Container		No	Yes	

Start Time ↓	End Time	Node	User name	Description	Status
Oct 16 21:59:34		mxo	root@pam	Shell	
Nov 07 14:52:56	Nov 07 15:02:17	mxo	root@pam	VM/CT 112 - Console	OK

2. Enter the credentials of the VMWare system on which the SVI VM is running. Then, click on **Add**. With the given VMWare credentials, the import utility will be able to access the VMWare system and import the SVI VM.



ID: SVI-EXSi

Server: 10.198.160.15

Username: root

Password: ••••••••

Nodes: All (No restrictions)

Enable: ☑

Skip Certificate Verification: ☑

   The connection name, the FQDN name (IP address) of the ESXi host, and the account to access it (usually *root*). Enable the **Skip Certificate Verification** as it is not a Trusted Root Certificate.

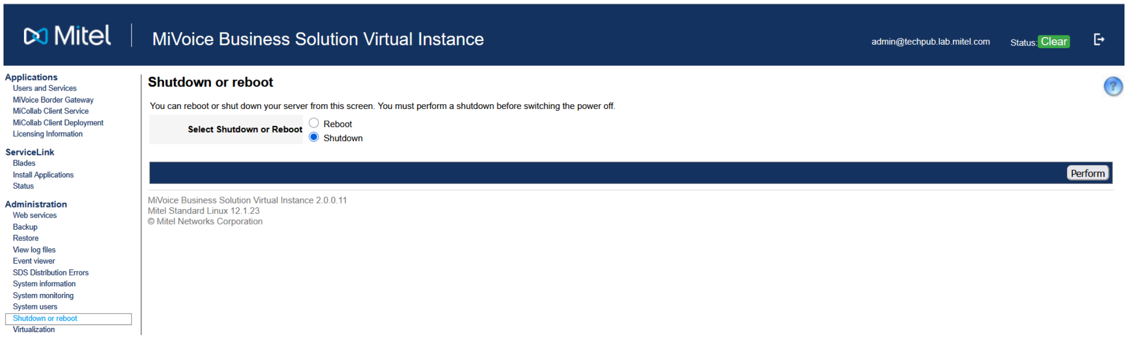
   The ESXi will added as an additional storage medium.

7.2.2 Shutdown the existing VMWare VM for migration

While live migration of the VM is possible, it is recommended to shut down the source VM on the ESXi blade to ensure data integrity and preserve its state. In this step, we ensure that the SVI VM running on ESXi is gracefully shut down.

To shutdown the existing VM on the ESXi blade, perform the following:

1. Login to **MiVoice Business Solution Virtual Instance**.
2. Under **Administration** click **Shutdown or reboot**.
3. Under the **Shutdown or reboot** field, select the **Shutdown** radio button.
4. Click **Perform**.



Shutdown or reboot

You can reboot or shut down your server from this screen. You must perform a shutdown before switching the power off.

Select Shutdown or Reboot ○ Reboot ● Shutdown

MiVoice Business Solution Virtual Instance 2.0.0.11
Mitel Standard Linux 12.1.23
© Mitel Networks Corporation

5. Click **YES** in the confirmation box.
6. Wait for the SVI VM to completely shutdown.

7.2.3 Importing the VM

To import the VM, we use the Proxmox Import Wizard, which simplifies the migration process. The import duration primarily depends on:

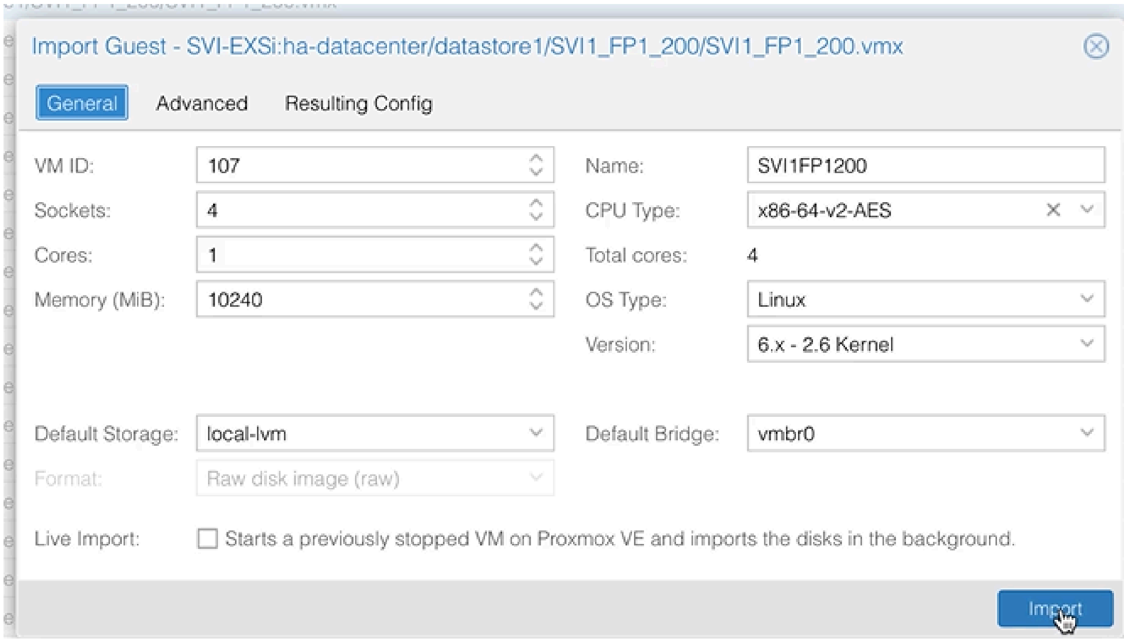
- Network throughout between the source ESXi host and the target Proxmox VE blades.
- Disk image size of the VM being migrated

Note:

Since SVI has a disk image of 100 GB or more based on the deployment model, even for a small business deployment, the import process may take time based on bandwidth and network throughput.

To Import the VM, perform the following:

1. Select the **VM** on the **ESXi** host that you want to migrate.
2. Click **Import** in the Proxmox Import Wizard. By default, the wizard copies the **VM ID**, **Sockets**, **vCPU**, **RAM**, and **VM** name settings from the source machine.
3. Choose the Proxmox storage where the VM will be saved and select the virtual disk format.
4. Click **Import** to start copying the virtual machine files.



Import Guest - SVI-EXSi:ha-datacenter/datastore1/SVI1_FP1_200/SVI1_FP1_200.vmx

VM ID:	107	Name:	SVI1FP1200
Sockets:	4	CPU Type:	x86-64-v2-AES
Cores:	1	Total cores:	4
Memory (MiB):	10240	OS Type:	Linux
		Version:	6.x - 2.6 Kernel
Default Storage:	local-lvm	Default Bridge:	vmbr0
Format:	Raw disk image (raw)		

Live Import: □ Starts a previously stopped VM on Proxmox VE and imports the disks in the background.

7.2.4 Configuring the migrated VM (Optional)

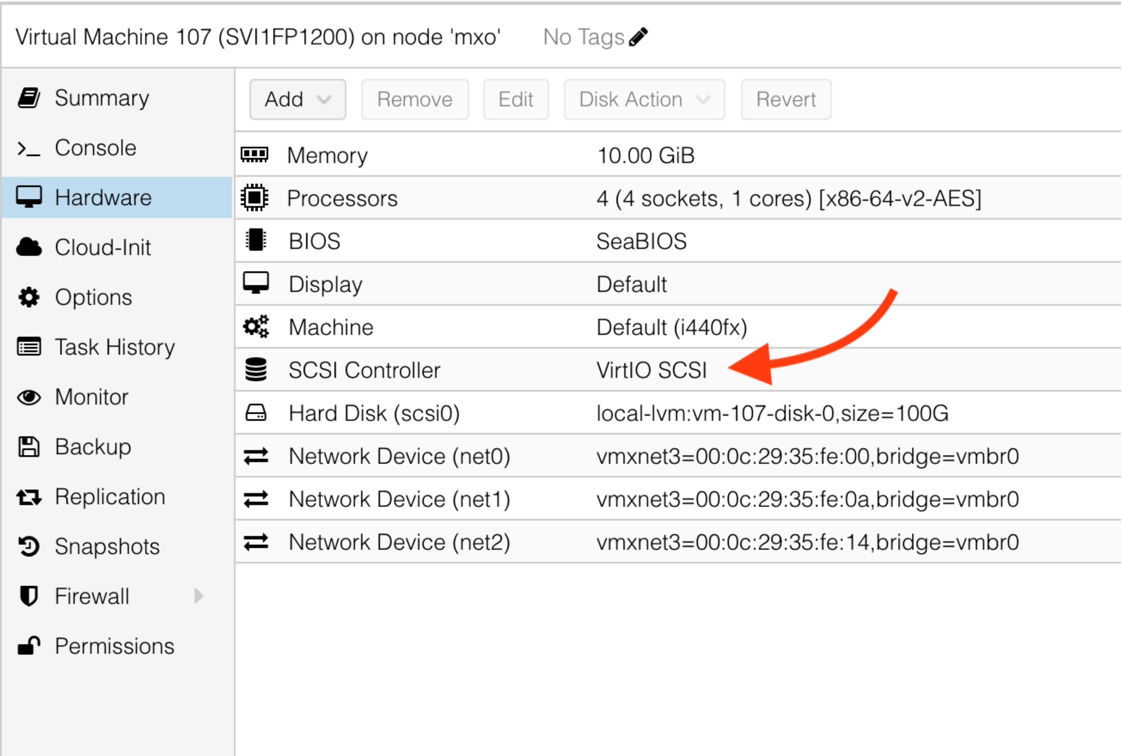
Before powering on the VM in Proxmox, following changes must be made as shown in the image below.

- SCSI controller must be changed to **Virtio SCSI**.
- Network Device must be changed to **Virtio (para-virtualized)**.

After starting the VM, you may need to reconfigure network parameters if required.

Once the migration and validation are complete.

- The original VM instance on VMware ESXi can be deleted.
- The mounted ESXi storage medium on Proxmox can be removed.



Memory	10.00 GiB
Processors	4 (4 sockets, 1 cores) [x86-64-v2-AES]
BIOS	SeaBIOS
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI
Hard Disk (scsi0)	local-lvm:vm-107-disk-0,size=100G
Network Device (net0)	vmxnet3=00:0c:29:35:fe:00,bridge=vmbr0
Network Device (net1)	vmxnet3=00:0c:29:35:fe:0a,bridge=vmbr0
Network Device (net2)	vmxnet3=00:0c:29:35:fe:14,bridge=vmbr0

7.3 Upgrading from existing SVI 1.0 to SVI 2.0

MiVB SVI does not support direct software upgrades from SVI 1.0 to SVI 2.0. Users must deploy SVI 2.0 and restore data from a backup using one of the following methods:

1. Restore from an existing backup (network based).
2. Restore from a running server.

Restore from an existing backup(network-based)

To restore from an existing backup, perform the following steps to:

1. In the server console of the server that you are restoring, select **Restore from backup**.

   A warning message is displayed and then the server reboots.
2. When the restore options are displayed, select **Restore from network share**.
3. Select the network interface to use for the restore (that is, the network interface that has a connection {direct or indirect} to the network file share server).
4. Enter the IP address of the MSL server and the subnet mask to apply.
5. Enter the IP address of the network share server that contains the backup file.
6. If the file server is on a different network than the MSL server, MSL prompts you to enter the gateway IP address to use to access the backup server.
7. Enter the Windows login domain or workgroup of the backup server. (Leave this blank when restoring SFTP backups.)

8. Enter the shared folder name where the backup file is stored. If multiple backup files are stored, you must select the one you want to restore (leave this blank when restoring SFTP backups).
9. Optionally, you can enter a subdirectory or path to store the backup file. (For SFTP backups, if you have created a folder on the backup server (For example:"/backups"), then enter the path to that folder here.) Or press Next to skip this step.

> **Note**:
> If you do not enter a sub-directory here for SFTP backups, the file is stored in the "/" folder by default.

10. Enter the username and password required to log in to the backup server
11. If the backup file has been encrypted (identifiable with a .aes256 extension), you will be prompted to enter the **Encryption password**. Click **Next** and then **Yes**.
12. Click **Next**. A confirmation message is displayed.
13. Click **Yes** to restore the database. The system reboots and restores the database upon restart.

> **Note**:
> After a successful restore, you must manually restart the server to complete the process.

Restore from a running server

If you are replacing an existing MSL 11.x server (physical or virtual), you can pull configuration and application data from it while it's still running and restore the data to a new MSL 12.x or later server.

The restore process automatically shuts down the old server.

> **Note**:
>
> 1. This procedure enables users to easily replace an existing virtual machine with a new one. If any problems arise, the original implementation can be restored with minimal downtime.
> 2. This procedure is not supported for systems with flex dimensions.
> 3. This procedure is not a supported method to migrate between hypervisors.

Conditions

- Installing the same EID/Serial on new physical hardware will require a Hardware ID reset.
- If the two servers are on:
  - connected networks (i.e. they have the same IP address range and there is no router between them), both servers must have the same subnet mask applied.
  - different networks:
    - MSL will request a gateway/router IP address to use for access.
    - When the restore is complete, the new server must be reconfigured for its own network because it will have inherited the network configuration of the original running server.

⚠ **Warning**:
Booting up the original server again after the restore procedure will result in IP address conflicts.

ℹ **Note**:
After a successful restore, you must manually restart the server to complete the process.

Perform Configuration 8

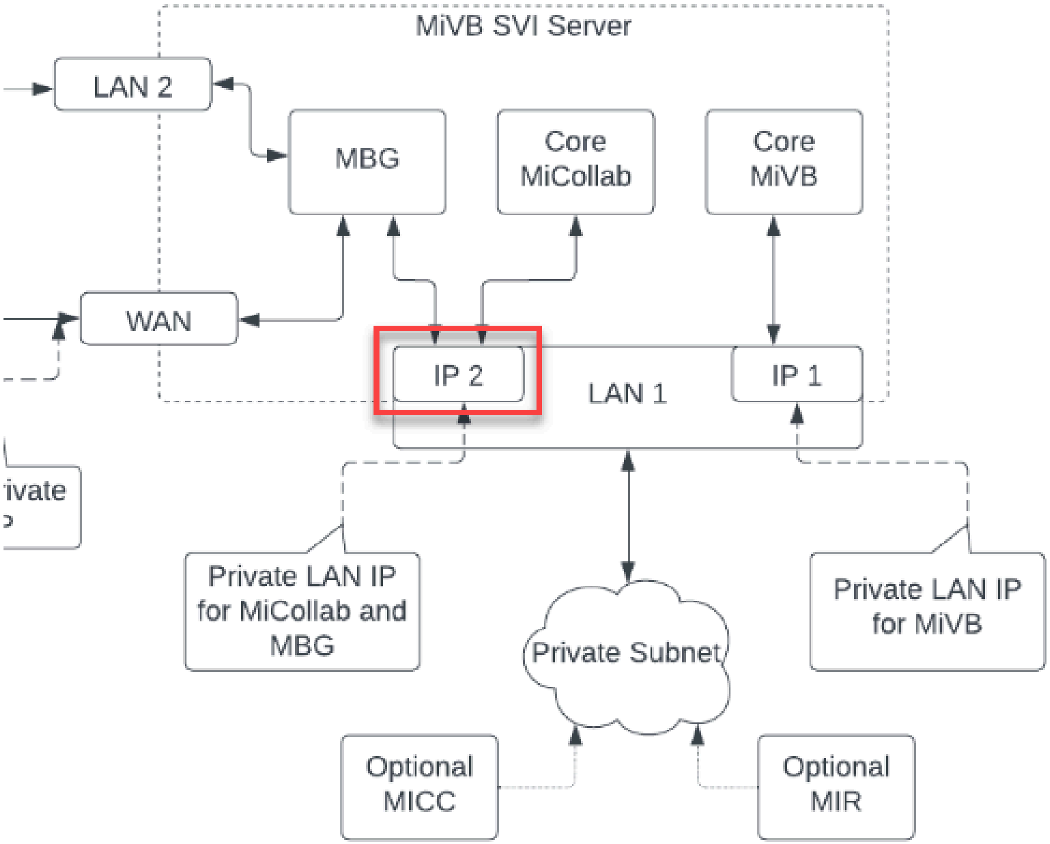
This chapter contains the following sections:

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.

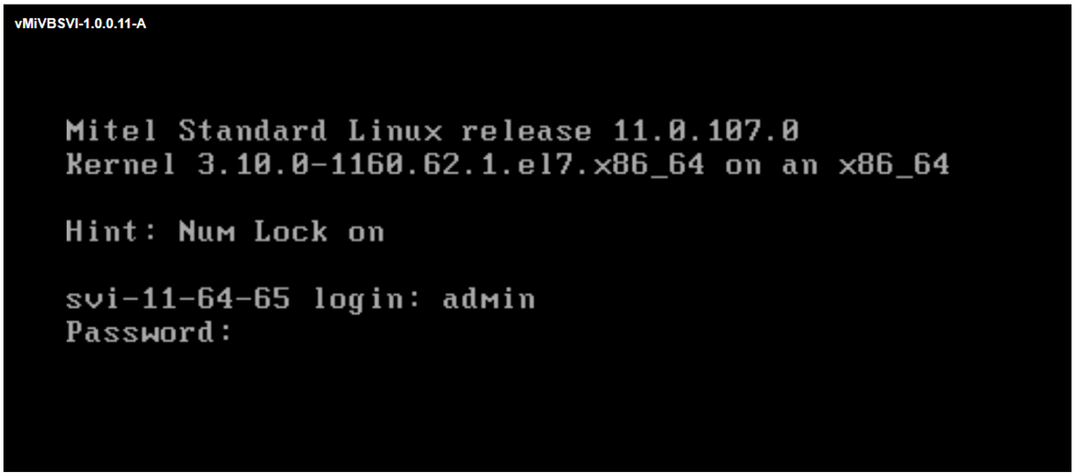
8.1 Configure the server

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

Perform the following steps:

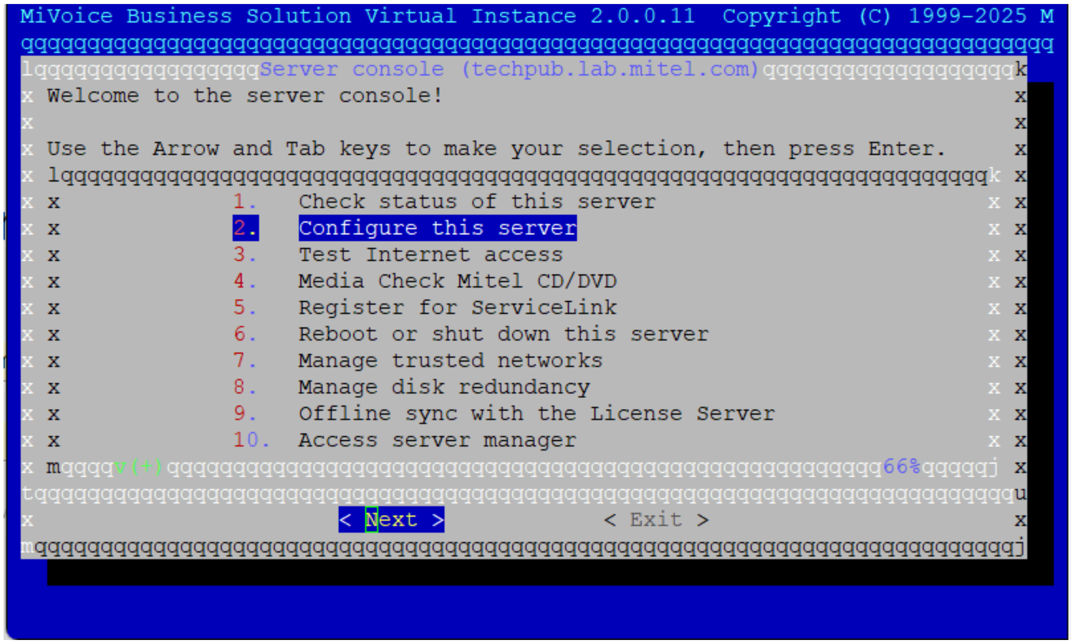


1. Launch the Web Console from vSphere, Nutanix, Hyper-V, or ESXi.
2. Login as **admin** and enter administrator password that was provided during OVA deployment. Type `console` as shown in the picture below:



```
vMiVBSVI-1.0.0.11-A

Mitel Standard Linux release 11.0.107.0
Kernel 3.10.0-1160.62.1.el7.x86_64 on an x86_64

Hint: Num Lock on

svi-11-64-65 login: admin
Password:
```

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



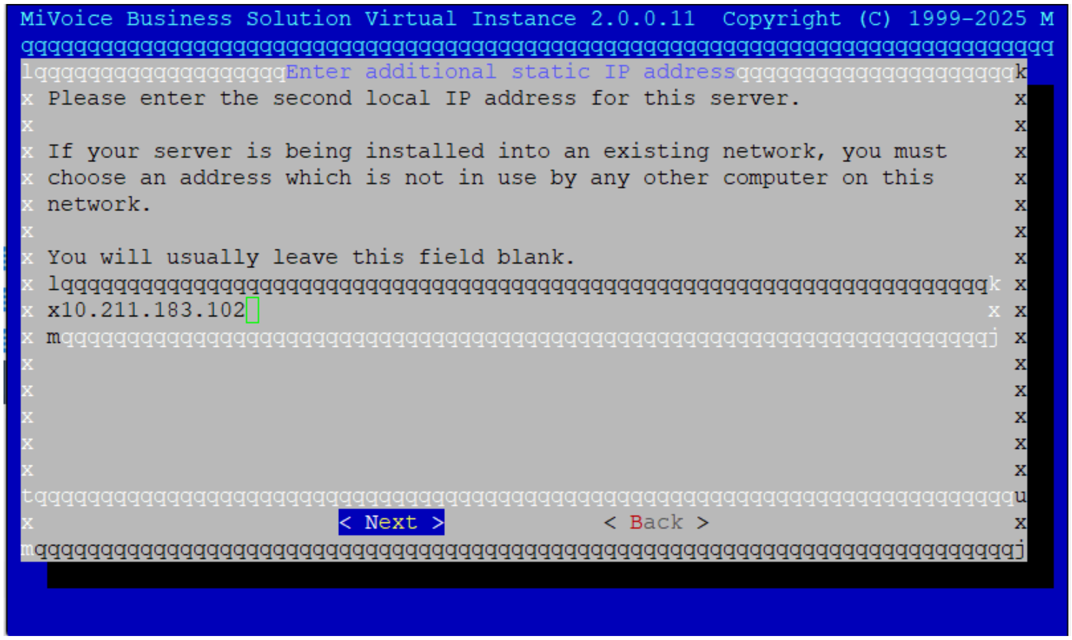
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqServer console (techpub.lab.mitel.com)qqqqqqqqqqqqqqqqqqqqk
x Welcome to the server console!                                             x
x                                                                            x
x Use the Arrow and Tab keys to make your selection, then press Enter.       x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x             1.   Check status of this server                          x x
x x             2.   Configure this server                                x x
x x             3.   Test Internet access                                 x x
x x             4.   Media Check Mitel CD/DVD                             x x
x x             5.   Register for ServiceLink                             x x
x x             6.   Reboot or shut down this server                      x x
x x             7.   Manage trusted networks                              x x
x x             8.   Manage disk redundancy                               x x
x x             9.   Offline sync with the License Server                 x x
x x             10.  Access server manager                                x x
x mqqqqv(+)qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq66%qqqqqj x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                       < Next >                 < Exit >                    x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

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.

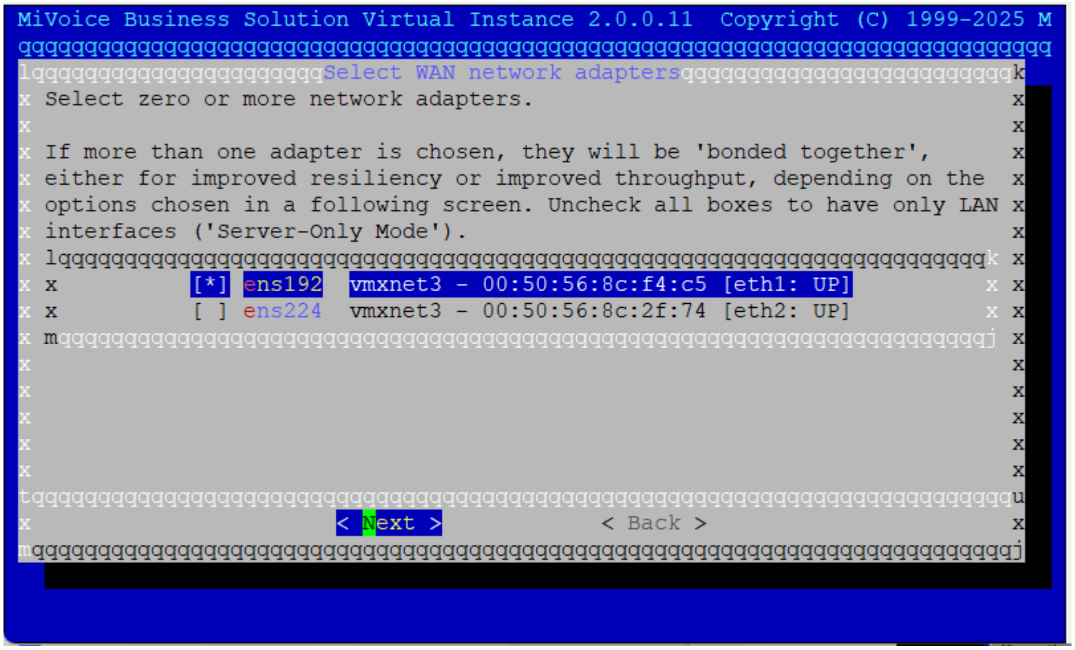


```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M

Enter additional static IP address
 Please enter the second local IP address for this server.

 If your server is being installed into an existing network, you must
 choose an address which is not in use by any other computer on this
 network.

 You will usually leave this field blank.
 x10.211.183.102

                       < Next >                    < Back >
```

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

Note:
This field is dependent on the deployment model.

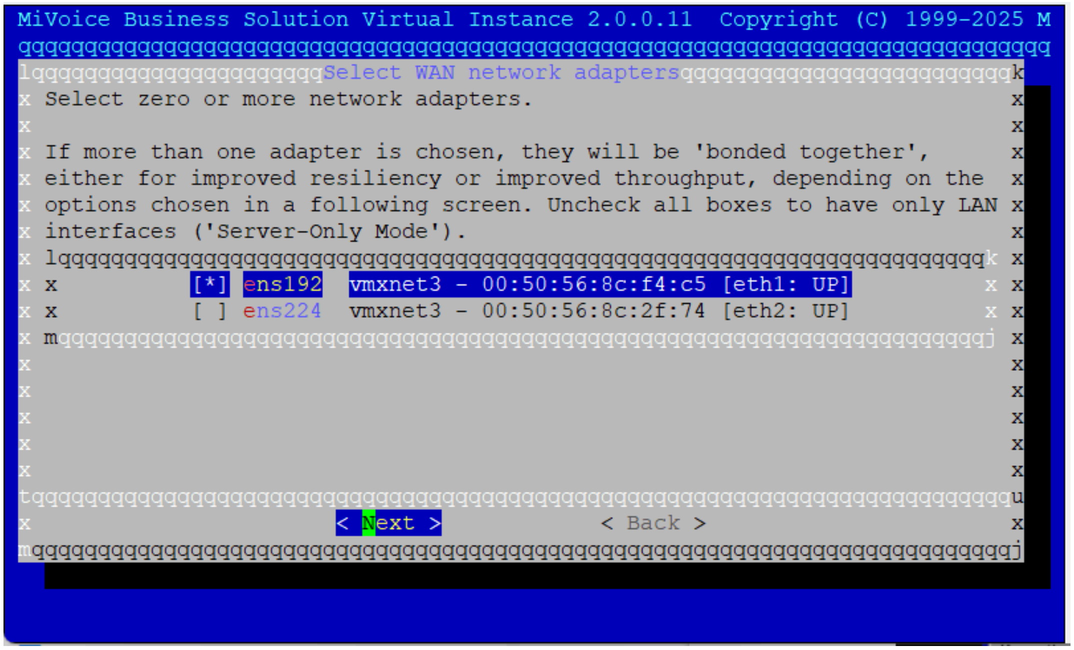
.



```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M

Select WAN network adapters
 Select zero or more network adapters.

 If more than one adapter is chosen, they will be 'bonded together',
 either for improved resiliency or improved throughput, depending on the
 options chosen in a following screen. Uncheck all boxes to have only LAN
 interfaces ('Server-Only Mode').
 x           [*] ens192  vmxnet3 - 00:50:56:8c:f4:c5 [eth1: UP]
 x           [ ] ens224  vmxnet3 - 00:50:56:8c:2f:74 [eth2: UP]

                       < Next >                    < Back >
```

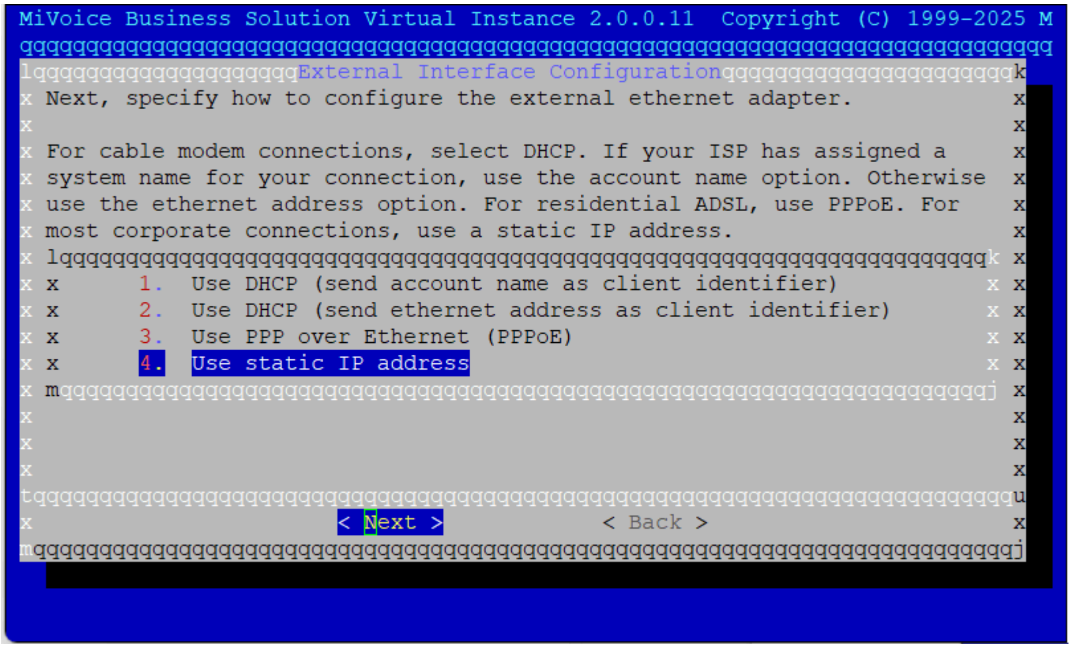
11. Perform Step 21 only if the network is down, otherwise perform Step 12.

12. Click **Next**.



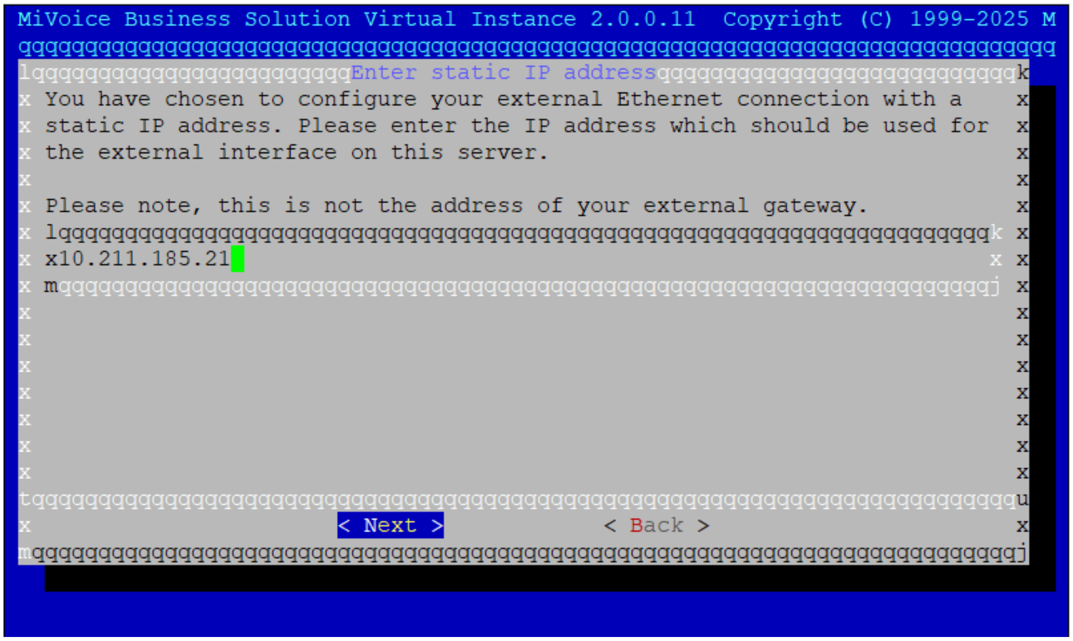
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqqSelect WAN network adaptersqqqqqqqqqqqqqqqqqqqqqqqqqk
x Select zero or more network adapters.                                    x
x                                                                          x
x If more than one adapter is chosen, they will be 'bonded together',      x
x either for improved resiliency or improved throughput, depending on the  x
x options chosen in a following screen. Uncheck all boxes to have only LAN x
x interfaces ('Server-Only Mode').                                          x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x          [*] ens192  vmxnet3 - 00:50:56:8c:f4:c5 [eth1: UP]         x x
x x          [ ] ens224  vmxnet3 - 00:50:56:8c:2f:74 [eth2: UP]         x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                       < Next >             < Back >                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

13. Click **Next**.



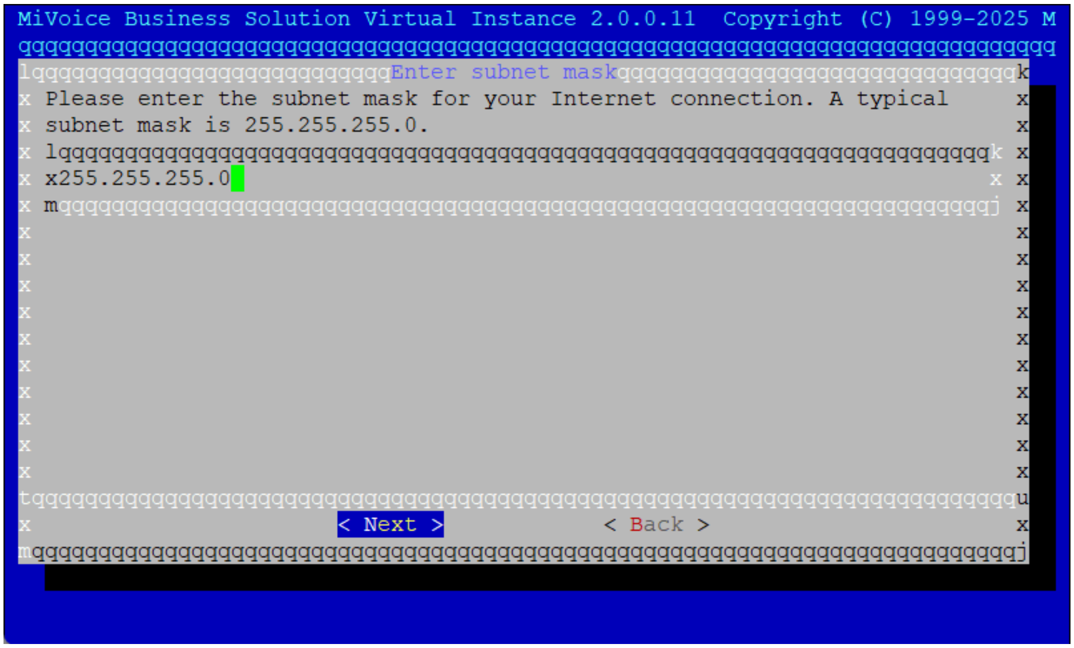
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqExternal Interface Configurationqqqqqqqqqqqqqqqqqqqqqqk
x Next, specify how to configure the external ethernet adapter.            x
x                                                                          x
x For cable modem connections, select DHCP. If your ISP has assigned a     x
x system name for your connection, use the account name option. Otherwise x
x use the ethernet address option. For residential ADSL, use PPPoE. For    x
x most corporate connections, use a static IP address.                     x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x      1.  Use DHCP (send account name as client identifier)          x x
x x      2.  Use DHCP (send ethernet address as client identifier)       x x
x x      3.  Use PPP over Ethernet (PPPoE)                               x x
x x      4.  Use static IP address                                       x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                          x
x                                                                          x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                       < Next >             < Back >                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

14. Click **Next**.



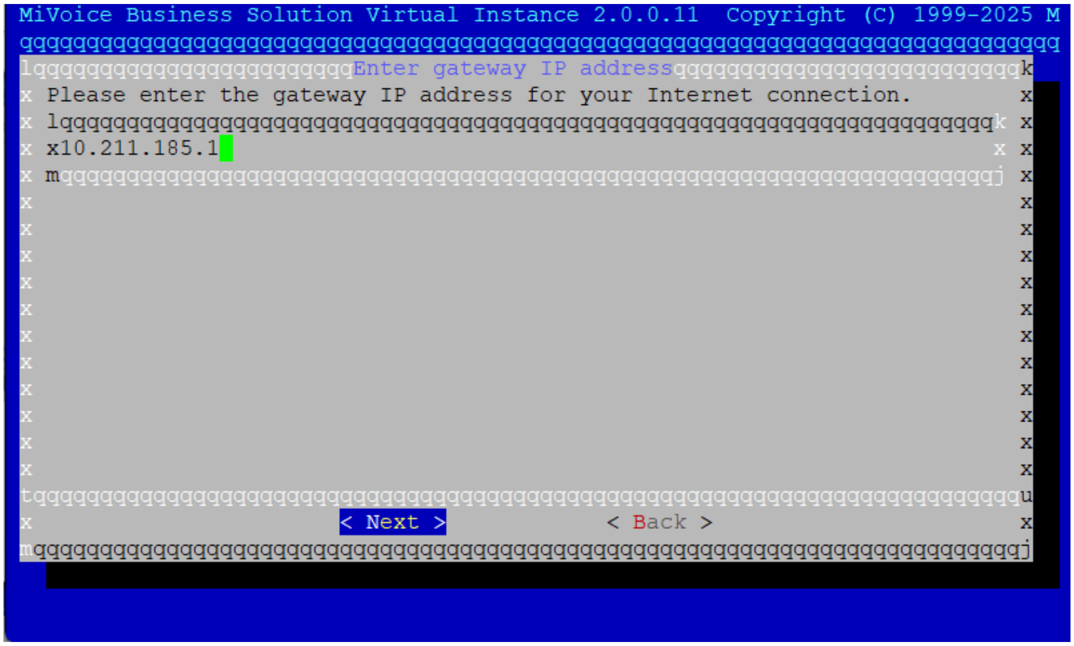
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqqqqEnter static IP addressqqqqqqqqqqqqqqqqqqqqqqqqqqk
x You have chosen to configure your external Ethernet connection with a   x
x static IP address. Please enter the IP address which should be used for x
x the external interface on this server.                                  x
x                                                                         x
x Please note, this is not the address of your external gateway.          x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x10.211.185.21                                                       x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                      < Next >             < Back >                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

15. Click **Next**.



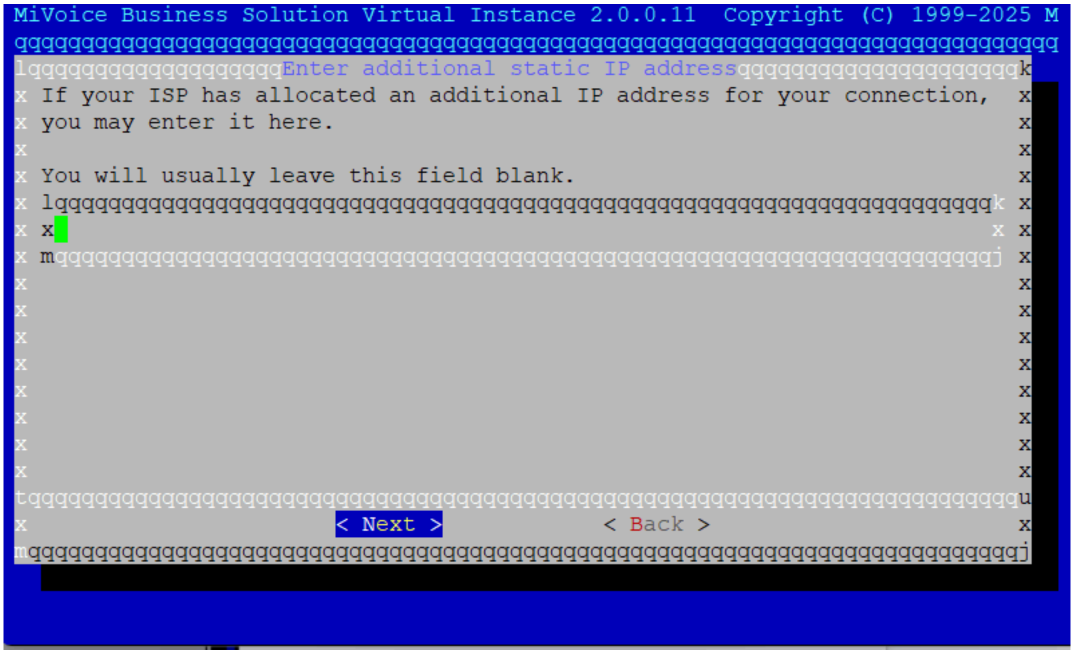
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqEnter subnet maskqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Please enter the subnet mask for your Internet connection. A typical    x
x subnet mask is 255.255.255.0.                                           x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x255.255.255.0                                                       x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
x                                                                         x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                      < Next >             < Back >                      x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

16. Click **Next**.



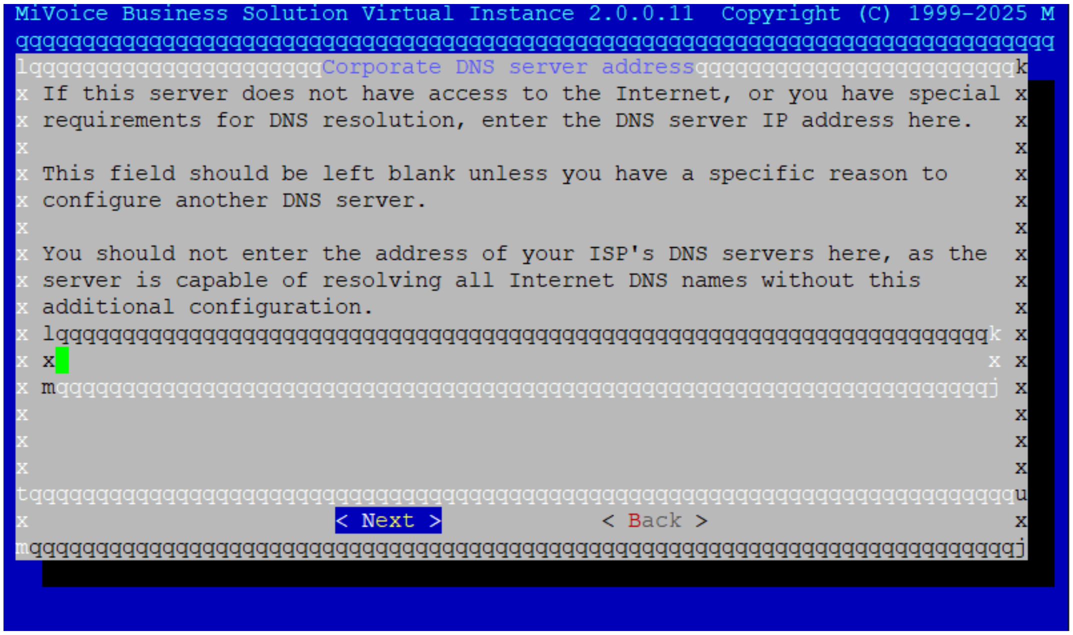
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
Enter gateway IP address
Please enter the gateway IP address for your Internet connection.
10.211.185.1
< Next >              < Back >
```

17. Click **Next**.



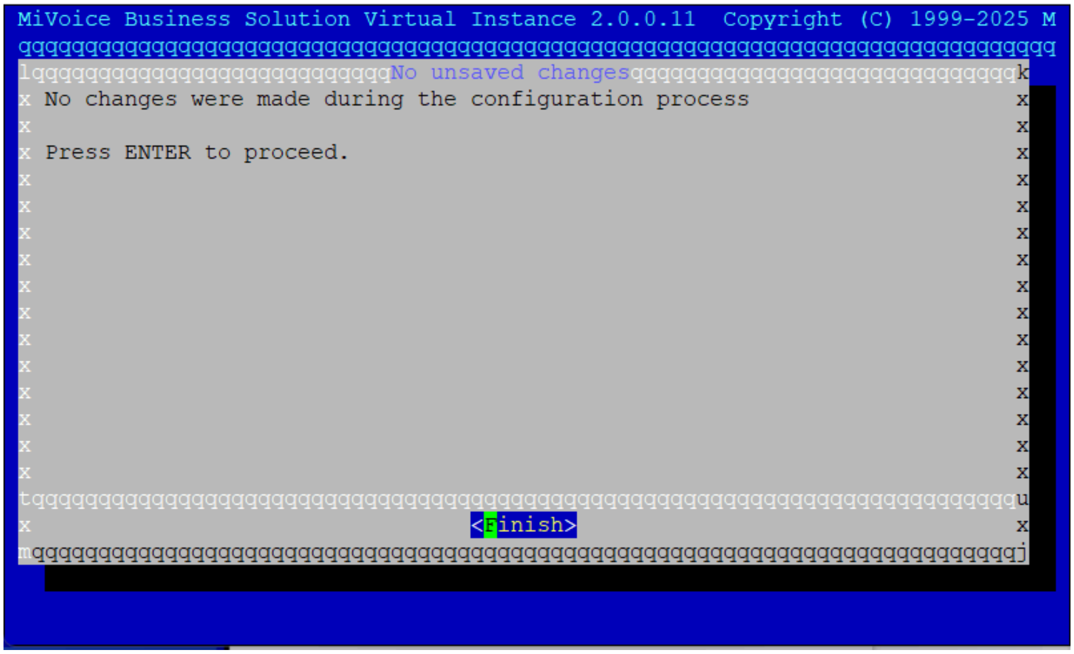
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
Enter additional static IP address
If your ISP has allocated an additional IP address for your connection,
you may enter it here.

You will usually leave this field blank.

< Next >              < Back >
```

18. Click **Next**.



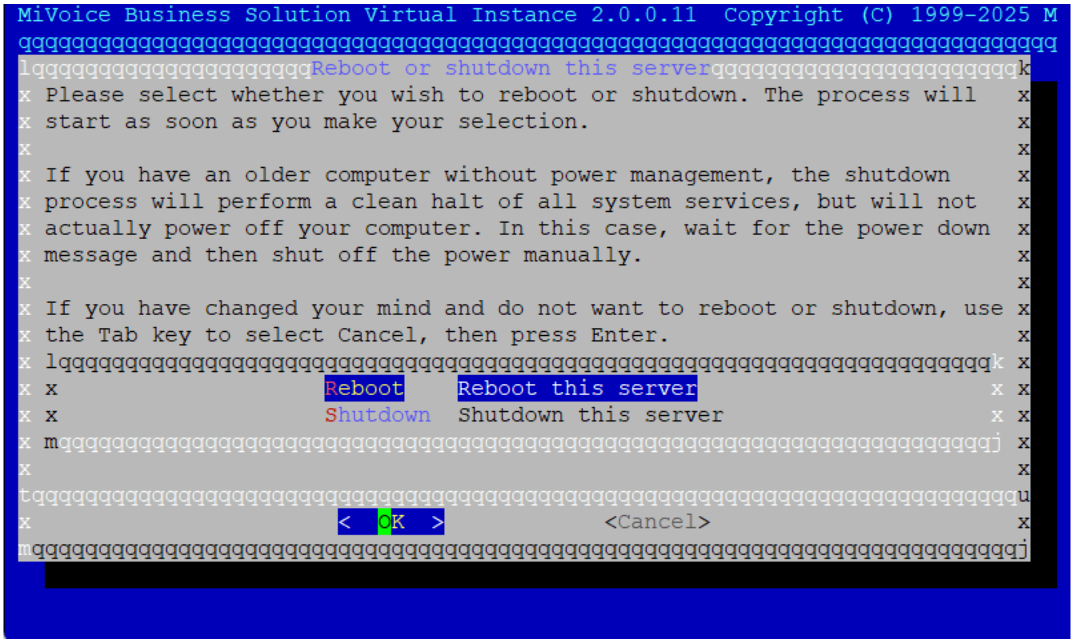
```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqqCorporate DNS server addressqqqqqqqqqqqqqqqqqqqqqqqqk
x If this server does not have access to the Internet, or you have special x
x requirements for DNS resolution, enter the DNS server IP address here.   x
x                                                                          x
x This field should be left blank unless you have a specific reason to     x
x configure another DNS server.                                            x
x                                                                          x
x You should not enter the address of your ISP's DNS servers here, as the  x
x server is capable of resolving all Internet DNS names without this       x
x additional configuration.                                                x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x                                                                      x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                          x
x                                                                          x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                       < Next >            < Back >                       x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

19. Click **Finish**.



```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqNo unsaved changesqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x No changes were made during the configuration process                     x
x                                                                           x
x Press ENTER to proceed.                                                   x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
x                                                                           x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                                 <Finish>                                  x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

20. In **Reboot or Shutdown this server** window, click **Reboot** > **OK**.

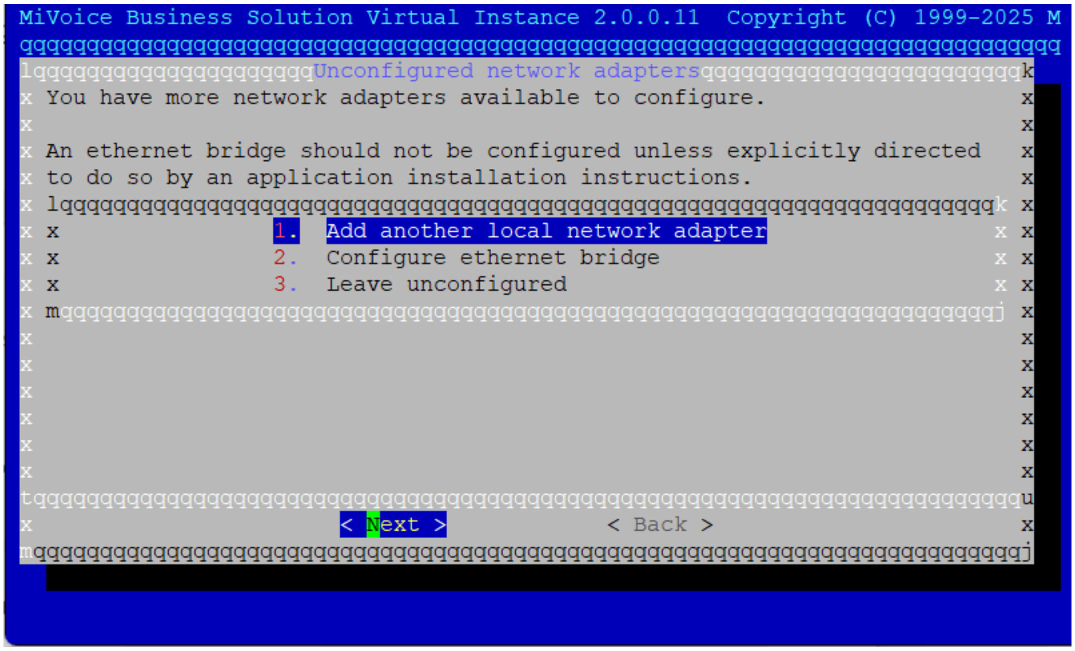


```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqReboot or shutdown this serverqqqqqqqqqqqqqqqqqqqqqqk
x Please select whether you wish to reboot or shutdown. The process will   x
x start as soon as you make your selection.                                x
x                                                                          x
x If you have an older computer without power management, the shutdown     x
x process will perform a clean halt of all system services, but will not   x
x actually power off your computer. In this case, wait for the power down  x
x message and then shut off the power manually.                            x
x                                                                          x
x If you have changed your mind and do not want to reboot or shutdown, use x
x the Tab key to select Cancel, then press Enter.                          x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x                    Reboot    Reboot this server                     x x
x x                    Shutdown  Shutdown this server                   x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                       <  OK  >           <Cancel>                        x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

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**.



```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqUnconfigured network adaptersqqqqqqqqqqqqqqqqqqqqqqqqk
x You have more network adapters available to configure.                   x
x                                                                          x
x An ethernet bridge should not be configured unless explicitly directed   x
x to do so by an application installation instructions.                    x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x                 1.  Add another local network adapter              x x
x x                 2.  Configure ethernet bridge                      x x
x x                 3.  Leave unconfigured                             x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                        < Next >             < Back >                     x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

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**.

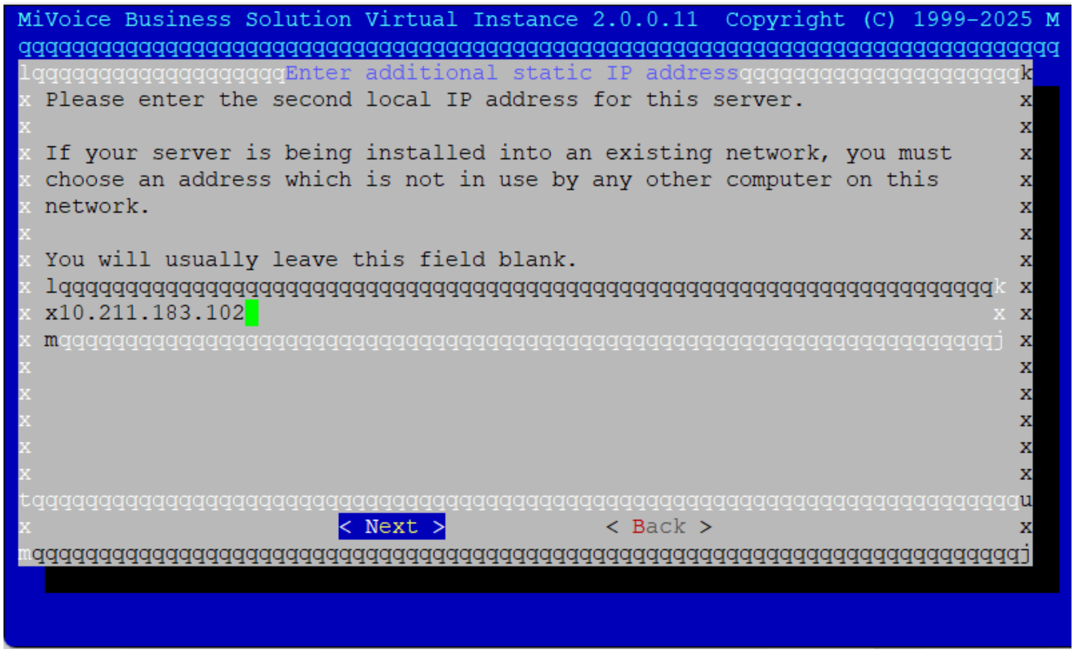
d. In **Enter gateway IP address** window, enter gateway IP address.

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.



```
MiVoice Business Solution Virtual Instance 2.0.0.11  Copyright (C) 1999-2025 M
qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqEnter additional static IP addressqqqqqqqqqqqqqqqqqqqqqqk
x Please enter the second local IP address for this server.                x
x                                                                          x
x If your server is being installed into an existing network, you must     x
x choose an address which is not in use by any other computer on this      x
x network.                                                                 x
x                                                                          x
x You will usually leave this field blank.                                 x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x x10.211.183.102                                                        x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
x                                                                          x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
x                      < Next >               < Back >                     x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

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**.

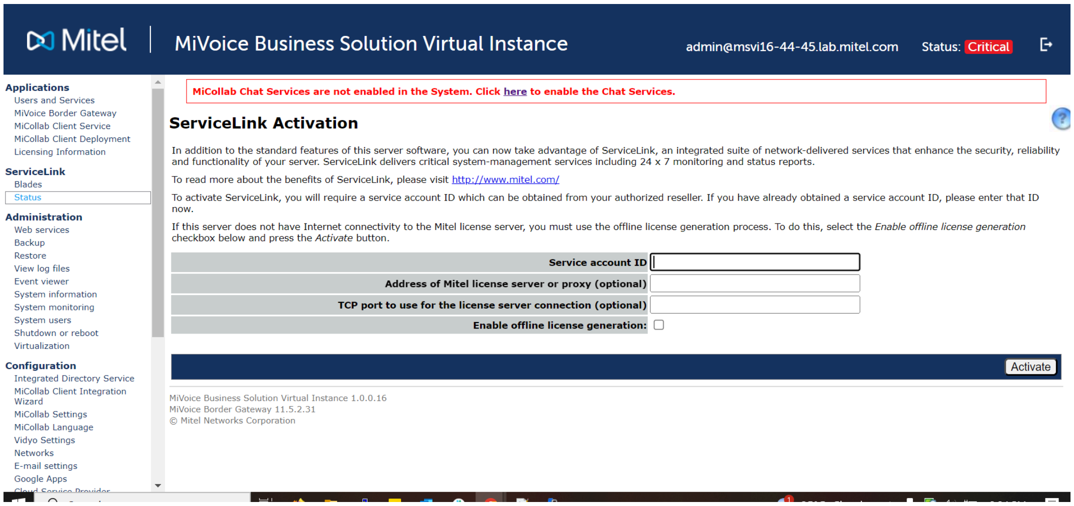
j. In **Resolve primary domain** window, click **Next**.

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

8.2 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 EID/Serial ID that you have received from Mitel, if you have not done it already. Enter the details, click **Activate** to register with Mitel.



MiCollab Chat Services are not enabled in the System. Click here to enable the Chat Services.

ServiceLink Activation

In addition to the standard features of this server software, you can now take advantage of ServiceLink, an integrated suite of network-delivered services that enhance the security, reliability and functionality of your server. ServiceLink delivers critical system-management services including 24 x 7 monitoring and status reports.

To read more about the benefits of ServiceLink, please visit http://www.mitel.com/

To activate ServiceLink, you will require a service account ID which can be obtained from your authorized reseller. If you have already obtained a service account ID, please enter that ID now.

If this server does not have Internet connectivity to the Mitel license server, you must use the offline license generation process. To do this, select the *Enable offline license generation* checkbox below and press the *Activate* button.

Service account ID	
Address of Mitel license server or proxy (optional)	
TCP port to use for the license server connection (optional)	
Enable offline license generation:	☐

MiVoice Business Solution Virtual Instance 1.0.0.16
MiVoice Border Gateway 11.5.2.31
© Mitel Networks Corporation

> **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.

8.3 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.

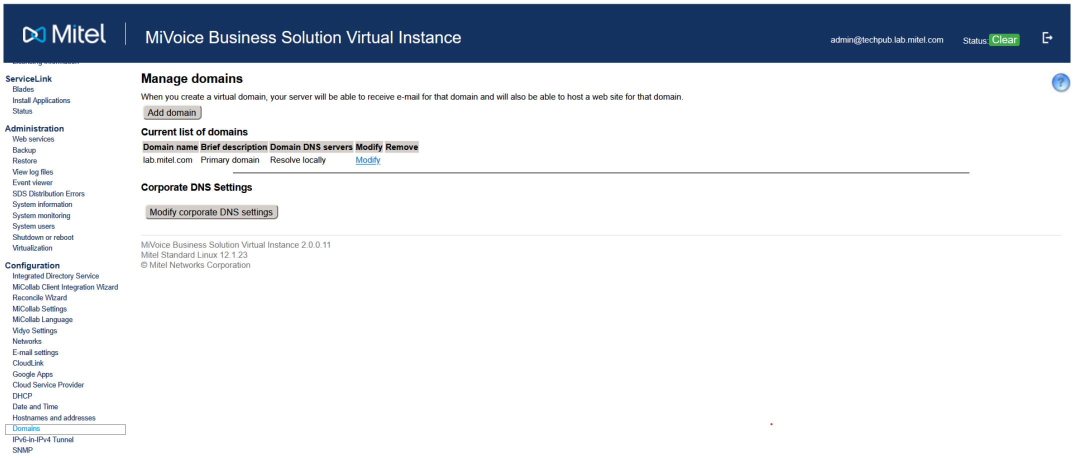
It is mandatory to provision an alias for the MiCollab application against the 2nd IP address of default LAN.

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.



Manage domains

When you create a virtual domain, your server will be able to receive e-mail for that domain and will also be able to host a web site for that domain.

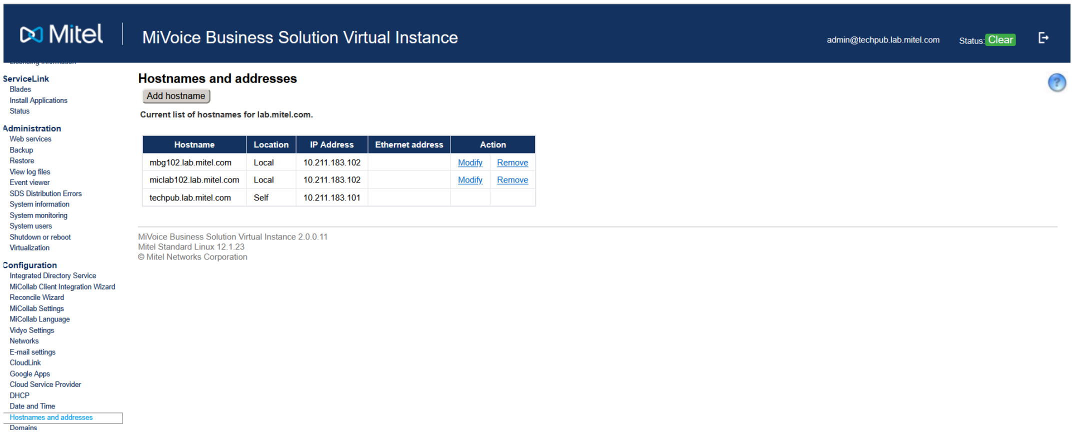
Current list of domains

Domain name	Brief description	Domain DNS servers	Modify	Remove
lab.mitel.com	Primary domain	Resolve locally	Modify	

Corporate DNS Settings

MiVoice Business Solution Virtual Instance 2.0.0.11
Mitel Standard Linux 12.1.23
© Mitel Networks Corporation

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 2^{nd} 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.



Hostnames and addresses

Current list of hostnames for lab.mitel.com.

Hostname	Location	IP Address	Ethernet address	Action	
mbg102.lab.mitel.com	Local	10.211.183.102		Modify	Remove
miclab102.lab.mitel.com	Local	10.211.183.102		Modify	Remove
techpub.lab.mitel.com	Self	10.211.183.101			

MiVoice Business Solution Virtual Instance 2.0.0.11
Mitel Standard Linux 12.1.23
© Mitel Networks Corporation

8.4 Configure MBG

MBG services don't start automatically, it must be started after applying the license.

To configure MBG

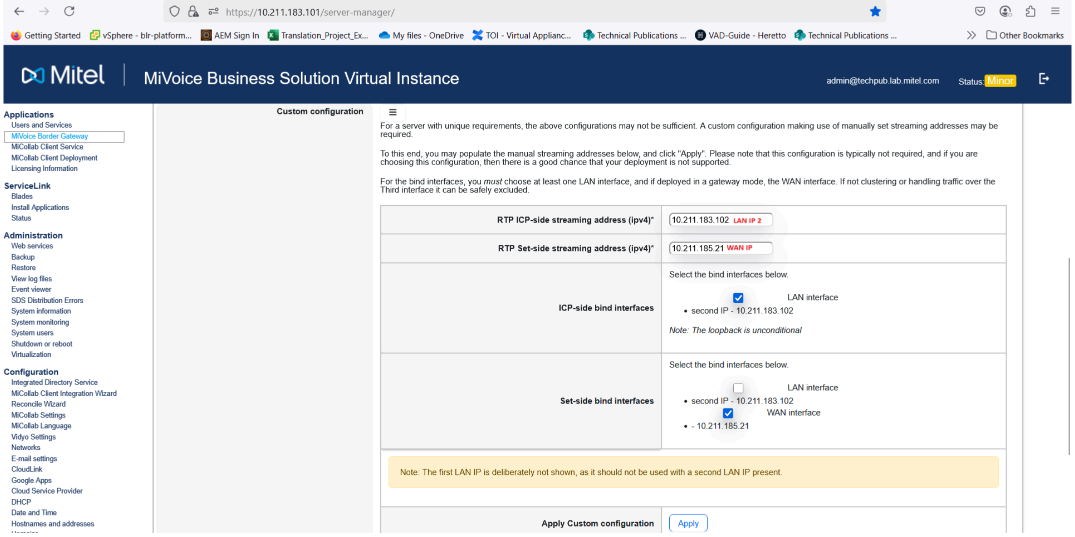
1. Navigate to **MiVoice Border Gateway**.
2. Click on **MBG Status** and from the popup screen click on **start**.

   Please ensure you have set the appropriate **Network Profile** before starting MBG services.

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:



Custom configuration

For a server with unique requirements, the above configurations may not be sufficient. A custom configuration making use of manually set streaming addresses may be required.

To this end, you may populate the manual streaming addresses below, and click "Apply". Please note that this configuration is typically not required, and if you are choosing this configuration, then there is a good chance that your deployment is not supported.

For the bind interfaces, you *must* choose at least one LAN interface, and if deployed in a gateway mode, the WAN interface. If not clustering or handling traffic over the Third interface it can be safely excluded.

RTP ICP-side streaming address (ipv4)*	10.211.183.102 LAN IP 2
RTP Set-side streaming address (ipv4)*	10.211.185.21 WAN IP
ICP-side bind interfaces	Select the bind interfaces below. ☑ LAN interface • second IP - 10.211.183.102 *Note: The loopback is unconditional*
Set-side bind interfaces	Select the bind interfaces below. □ LAN interface • second IP - 10.211.183.102 ☑ WAN interface • - 10.211.185.21

Note: The first LAN IP is deliberately not shown, as it should not be used with a second LAN IP present.

Apply Custom configuration	Apply

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 Bastion 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.

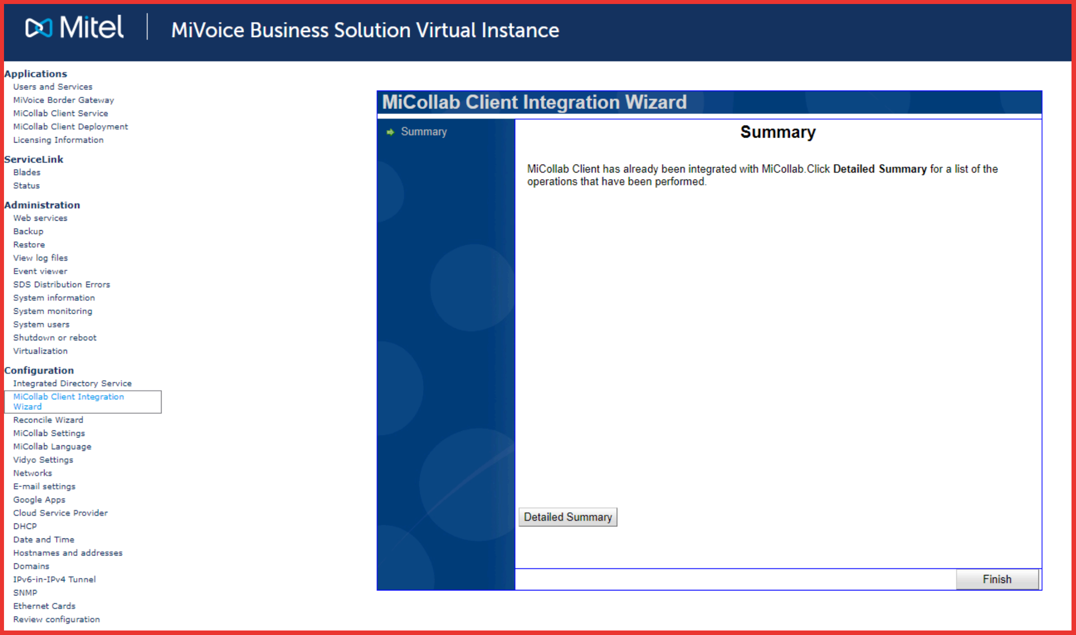
To change node's IP address, follow the procedure below:

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.

8.5 Configure MiVoice Business

Warning:

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



MiCollab Client has already been integrated with MiCollab.Click **Detailed Summary** for a list of the operations that have been performed.

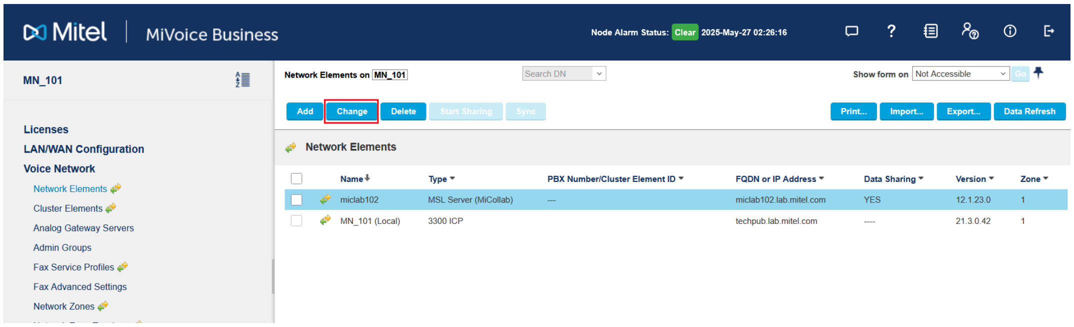
The following options are available to configure MiVoice Business:

- 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**.

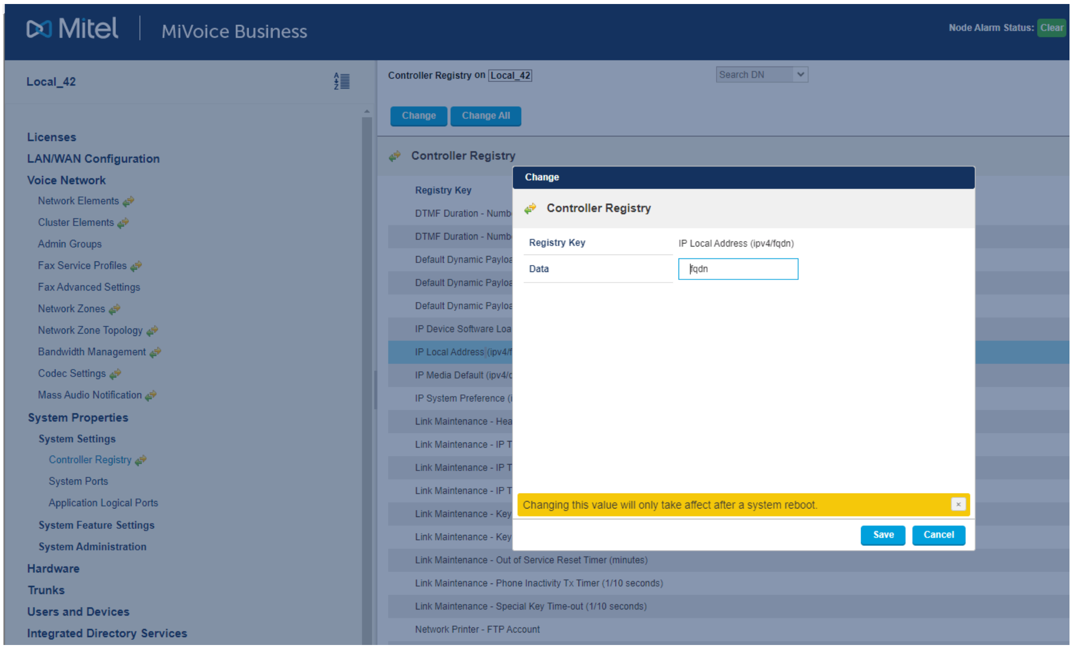


Network Elements on MN_101

Network Elements

Name	Type	PBX Number/Cluster Element ID	FQDN or IP Address	Data Sharing	Version	Zone
miclab102	MSL Server (MiCollab)	---	miclab102.lab.mitel.com	YES	12.1.23.0	1
MN_101 (Local)	3300 ICP		techpub.lab.mitel.com	----	21.3.0.42	1

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



Controller Registry on Local_42

Controller Registry

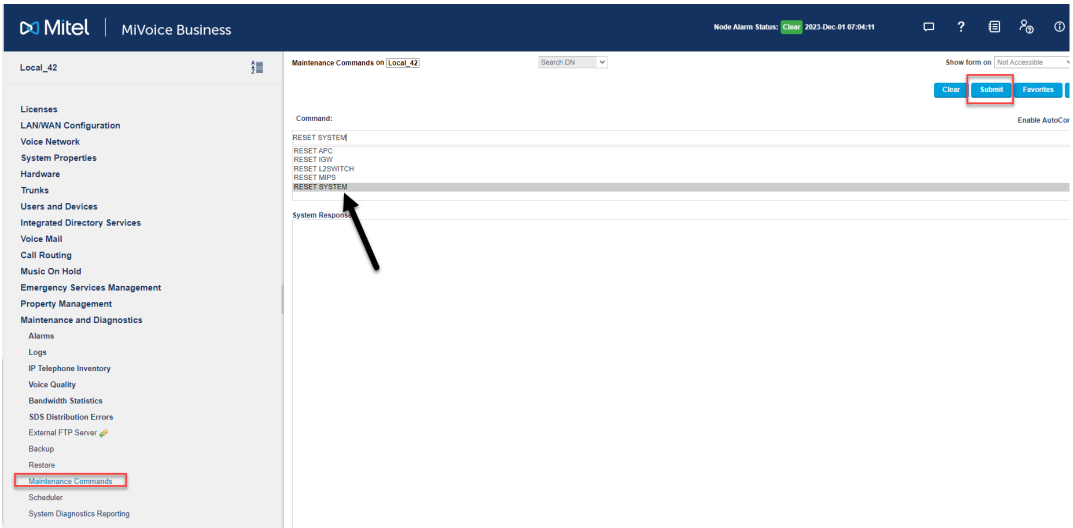
Change

Controller Registry

Registry Key	IP Local Address (ipv4/fqdn)
Data	fqdn

Changing this value will only take affect after a system reboot.

8. Reboot MiVoice Business to apply the FQDN change.



Command: RESET SYSTEM

9. Configure MiCollab Network Element:

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

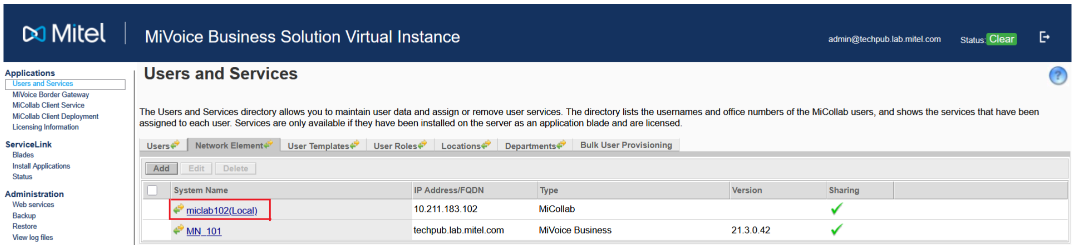
a. To find MiCollab system name[1], login to MiCollab server.

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

[1] 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 Configure the server on page 86 and the server must be licensed Configure MSL Server on page 96 prior to running the wizard.



Users and Services

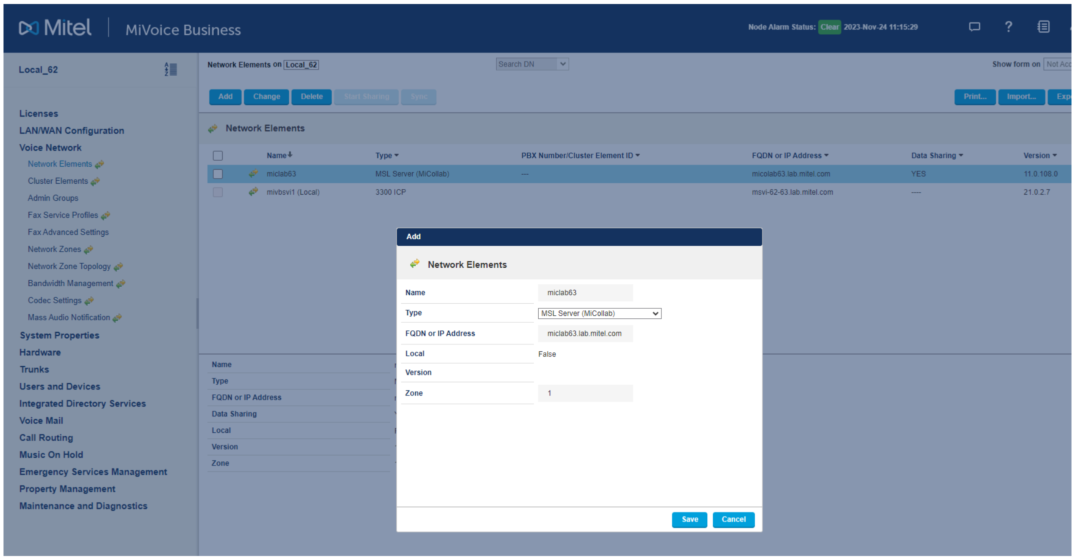
The Users and Services directory allows you to maintain user data and assign or remove user services. The directory lists the usernames and office numbers of the MiCollab users, and shows the services that have been assigned to each user. Services are only available if they have been installed on the server as an application blade and are licensed.

System Name	IP Address/FQDN	Type	Version	Sharing
miclab102(Local)	10.211.183.102	MiCollab		✓
MN_101	techpub.lab.mitel.com	MiVoice Business	21.3.0.42	✓

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.



Network Elements

Name	Type	PBX Number/Cluster Element ID	FQDN or IP Address	Data Sharing	Version
miclab63	MSL Server (MiCollab)	---	micolab63.lab.mitel.com	YES	11.0.108.0
mivbsvi1 (Local)	3300 ICP		msvi-62-63.lab.mitel.com	----	21.0.2.7

Add

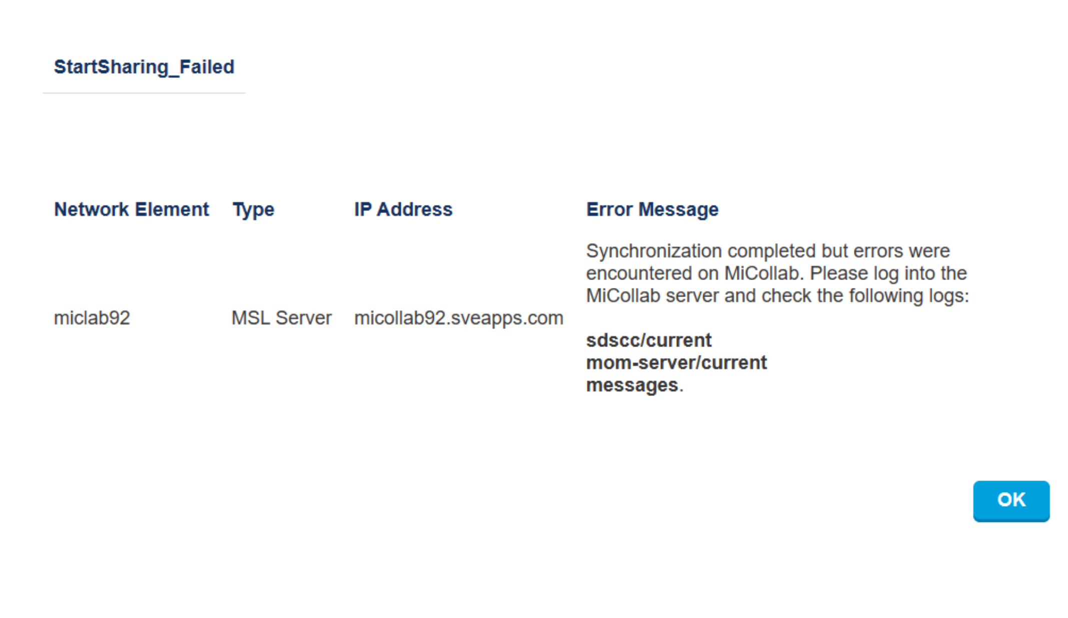
Network Elements

Name	miclab63
Type	MSL Server (MiCollab)
FQDN or IP Address	miclab63.lab.mitel.com
Local	False
Version	
Zone	1

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.



StartSharing_Failed

Network Element	Type	IP Address	Error Message
miclab92	MSL Server	micollab92.sveapps.com	Synchronization completed but errors were encountered on MiCollab. Please log into the MiCollab server and check the following logs: **sdscc/current** **mom-server/current** **messages**.

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

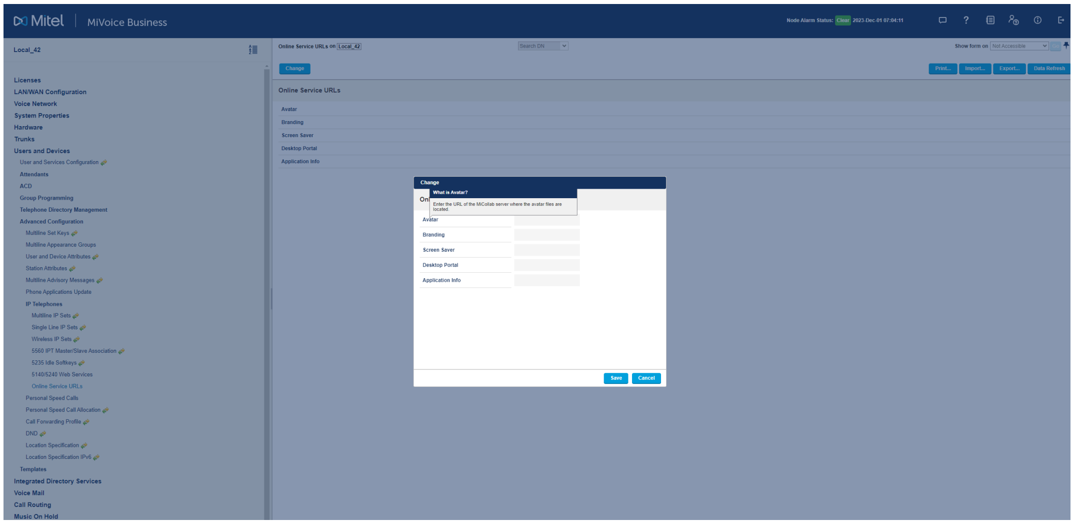
Once the manual configuration is completed, refresh the server manager, and proceed to Configure MiCollab to begin the process of reconciliation.

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.



Node Alarm Status: Clear 2023-Dec-01 07:04:11

Local_42

Online Service URLs on Local_42

Show form on Not Accessible

What is Avatar?

Enter the URL of the MiCollab server where the avatar files are located.

5. Click **Save**.

For more information, refer MiVoice Business.

8.6 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.

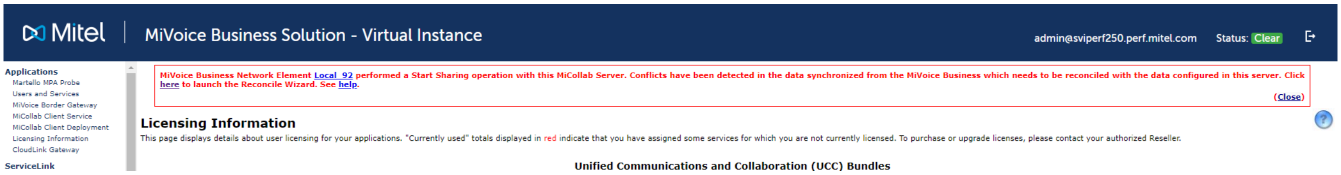
> **Note**:
> IP or FQDN/server-manager redirects to MiVoice Business Solution Virtual Instance server manager page.

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.



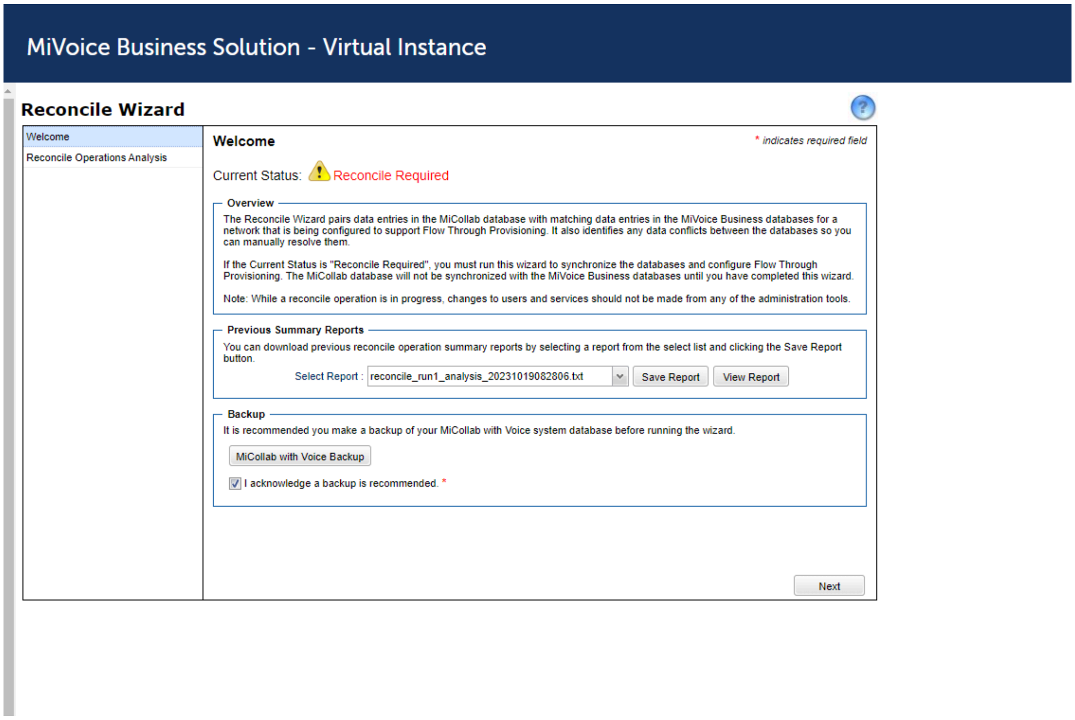
MiVoice Business Network Element Local_92 performed a Start Sharing operation with this MiCollab Server. Conflicts have been detected in the data synchronized from the MiVoice Business which needs to be reconciled with the data configured in this server. Click here to launch the Reconcile Wizard. See help.

(Close)

Licensing Information

This page displays details about user licensing for your applications. "Currently used" totals displayed in red indicate that you have assigned some services for which you are not currently licensed. To purchase or upgrade licenses, please contact your authorized Reseller.

Unified Communications and Collaboration (UCC) Bundles


MiVoice Business Solution - Virtual Instance
Welcome
Reconcile Operations Analysis
Save Report
View Report
MiCollab with Voice Backup
Next

Reconcile Wizard

Welcome

* indicates required field

Current Status: ⚠ Reconcile Required

Overview

The Reconcile Wizard pairs data entries in the MiCollab database with matching data entries in the MiVoice Business databases for a network that is being configured to support Flow Through Provisioning. It also identifies any data conflicts between the databases so you can manually resolve them.

If the Current Status is "Reconcile Required", you must run this wizard to synchronize the databases and configure Flow Through Provisioning. The MiCollab database will not be synchronized with the MiVoice Business databases until you have completed this wizard.

Note: While a reconcile operation is in progress, changes to users and services should not be made from any of the administration tools.

Previous Summary Reports

You can download previous reconcile operation summary reports by selecting a report from the select list and clicking the Save Report button.

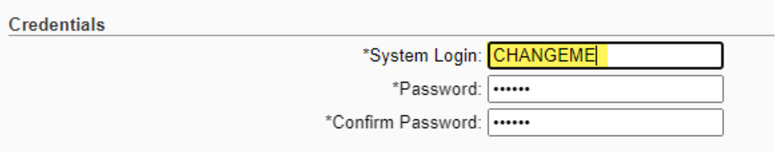
Select Report : reconcile_run1_analysis_20231019082806.txt

Backup

It is recommended you make a backup of your MiCollab with Voice system database before running the wizard.

☑ I acknowledge a backup is recommended. *

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.



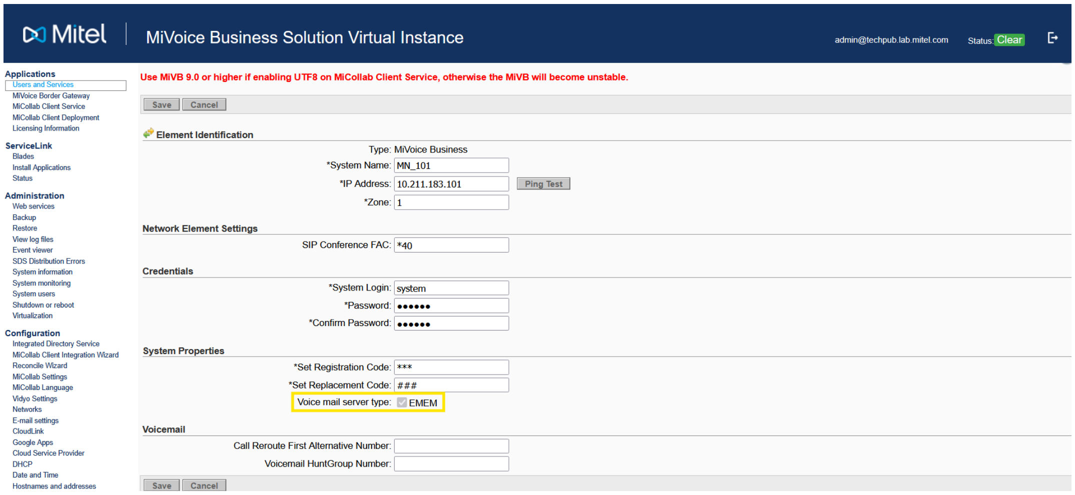
Credentials

*System Login: CHANGEME

*Password: ••••••

*Confirm Password: ••••••

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



Use MiVB 9.0 or higher if enabling UTF8 on MiCollab Client Service, otherwise the MiVB will become unstable.

Element Identification

Type: MiVoice Business
*System Name: MN_101
*IP Address: 10.211.183.101
*Zone: 1

Network Element Settings

SIP Conference FAC: *40

Credentials

*System Login: system
*Password: ••••••
*Confirm Password: ••••••

System Properties

*Set Registration Code: ***
*Set Replacement Code: ###
Voice mail server type: ☑ EMEM

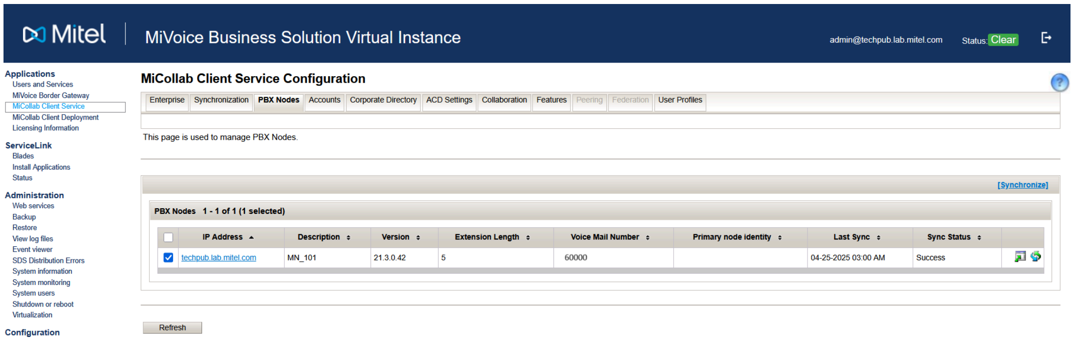
Voicemail

Call Reroute First Alternative Number:
Voicemail HuntGroup Number:

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]**.



MiCollab Client Service Configuration

This page is used to manage PBX Nodes.

PBX Nodes 1 - 1 of 1 (1 selected)

□	IP Address	Description	Version	Extension Length	Voice Mail Number	Primary node identity	Last Sync	Sync Status
☑	techpub.lab.mitel.com	MN_101	21.3.0.42	5	60000		04-25-2025 03:00 AM	Success

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

Configure MiCollab Client Deployment

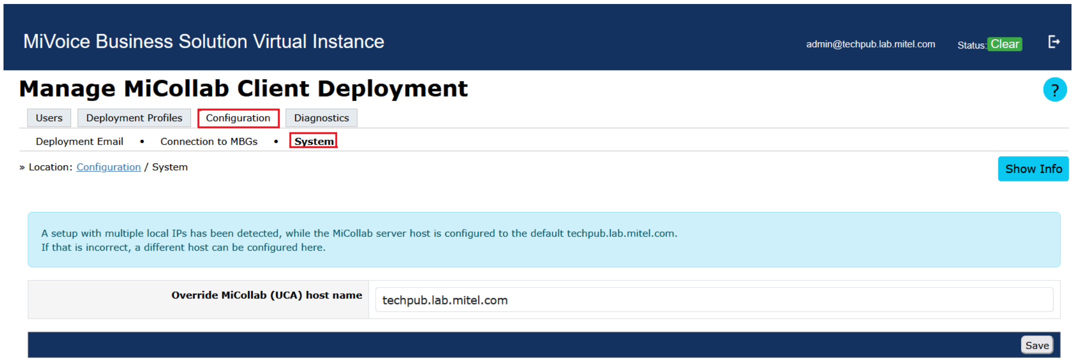
For MiCollab (UCA) host name configuration, refer MiCollab Client Deployment.

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**.



Manage MiCollab Client Deployment

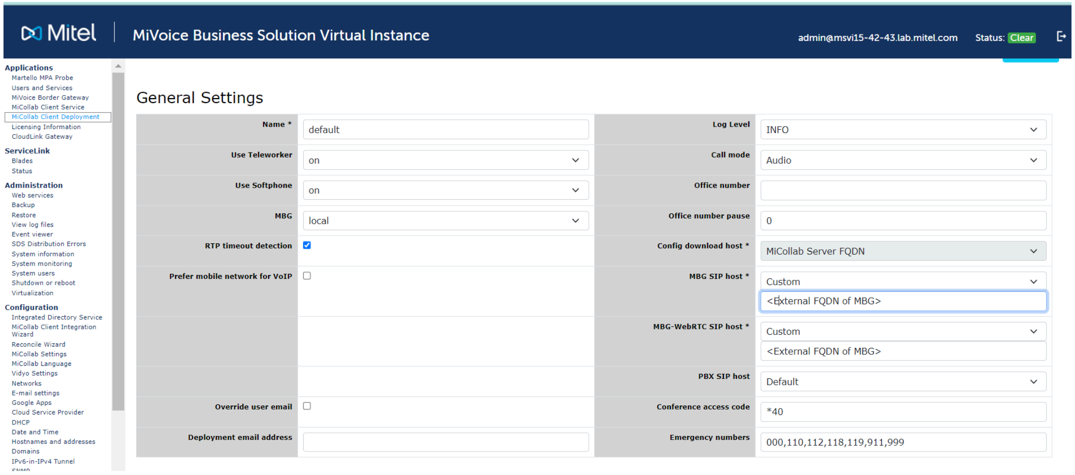
» Location: Configuration / System

A setup with multiple local IPs has been detected, while the MiCollab server host is configured to the default techpub.lab.mitel.com.
If that is incorrect, a different host can be configured here.

Override MiCollab (UCA) host name	techpub.lab.mitel.com

- 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).



General Settings

Name *	default	Log Level	INFO
Use Teleworker	on	Call mode	Audio
Use Softphone	on	Office number	
MBG	local	Office number pause	0
RTP timeout detection	☑	Config download host *	MiCollab Server FQDN
Prefer mobile network for VoIP	☐	MBG SIP host *	Custom <External FQDN of MBG>
		MBG-WebRTC SIP host *	Custom <External FQDN of MBG>
		PBX SIP host	Default
Override user email	☐	Conference access code	*40
Deployment email address		Emergency numbers	000,110,112,118,119,911,999

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.

8.7 Configure Optional Standalone bastion

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.

8.7.1 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.

8.7.1.1 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:

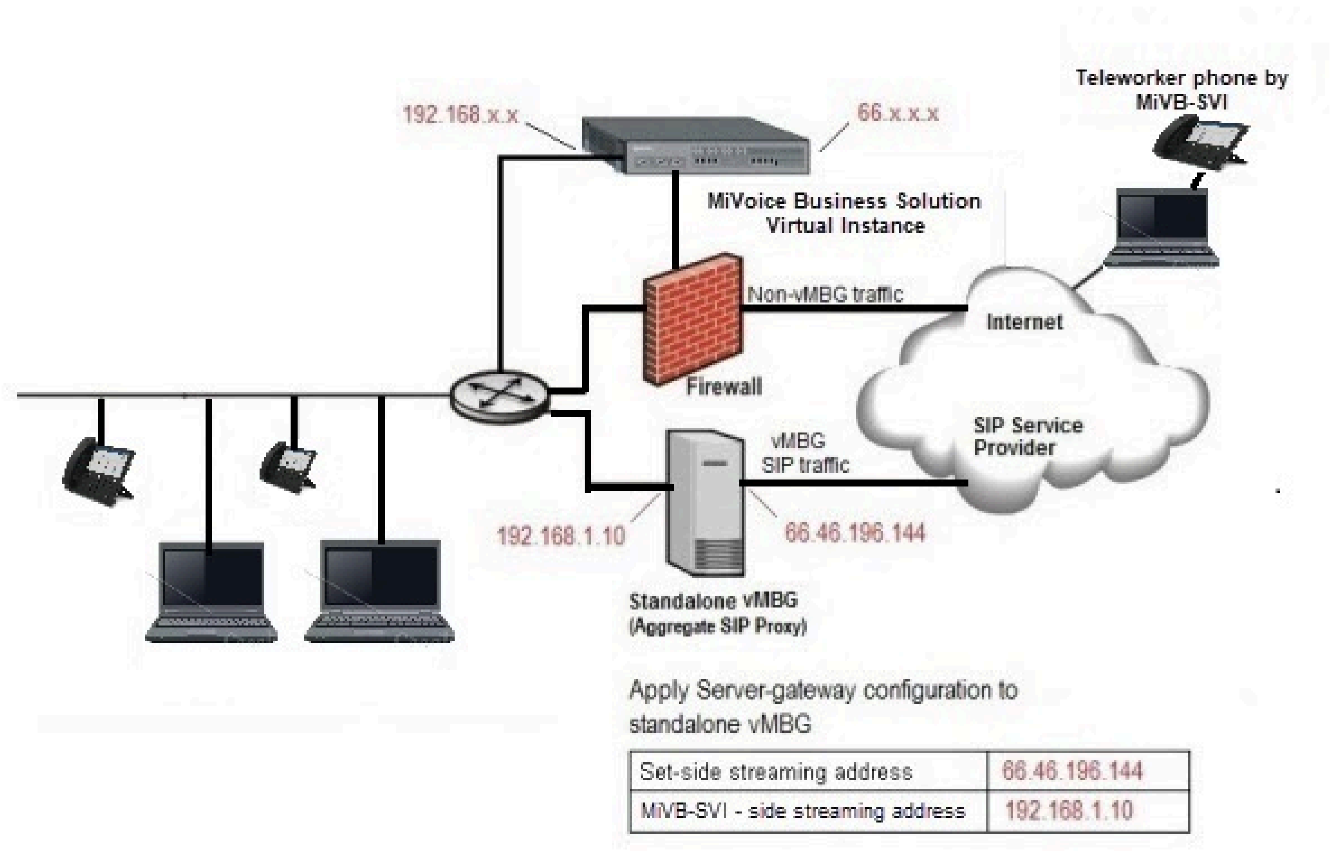
    - dedicated to the MBG Solution
    - routable
    - reachable from the Internet and the internal network.
5. Access the vMBG server manager.
6. On the **Configuration** tab, click **Network Profiles**.
7. Select **Server-gateway configuration** on the network edge.
8. Select **Apply Server-Gateway configuration**.

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.



Apply Server-gateway configuration to standalone vMBG

Set-side streaming address	66.46.196.144
MiVB-SVI - side streaming address	192.168.1.10

Figure 11: Standalone vMBG for SIP Trunk Aggregation

8.7.1.2 Configure Secure Recording Connector

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

8.7.2 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 Server-gateway mode. In this configuration mode, the server functions a firewall/Internet gateway with two Ethernet interfaces. One interface is connected to the customer firewall LAN side, while the other is connected to the customer's 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.

8.7.2.1 Deploy vMBG in Server-Gateway Mode

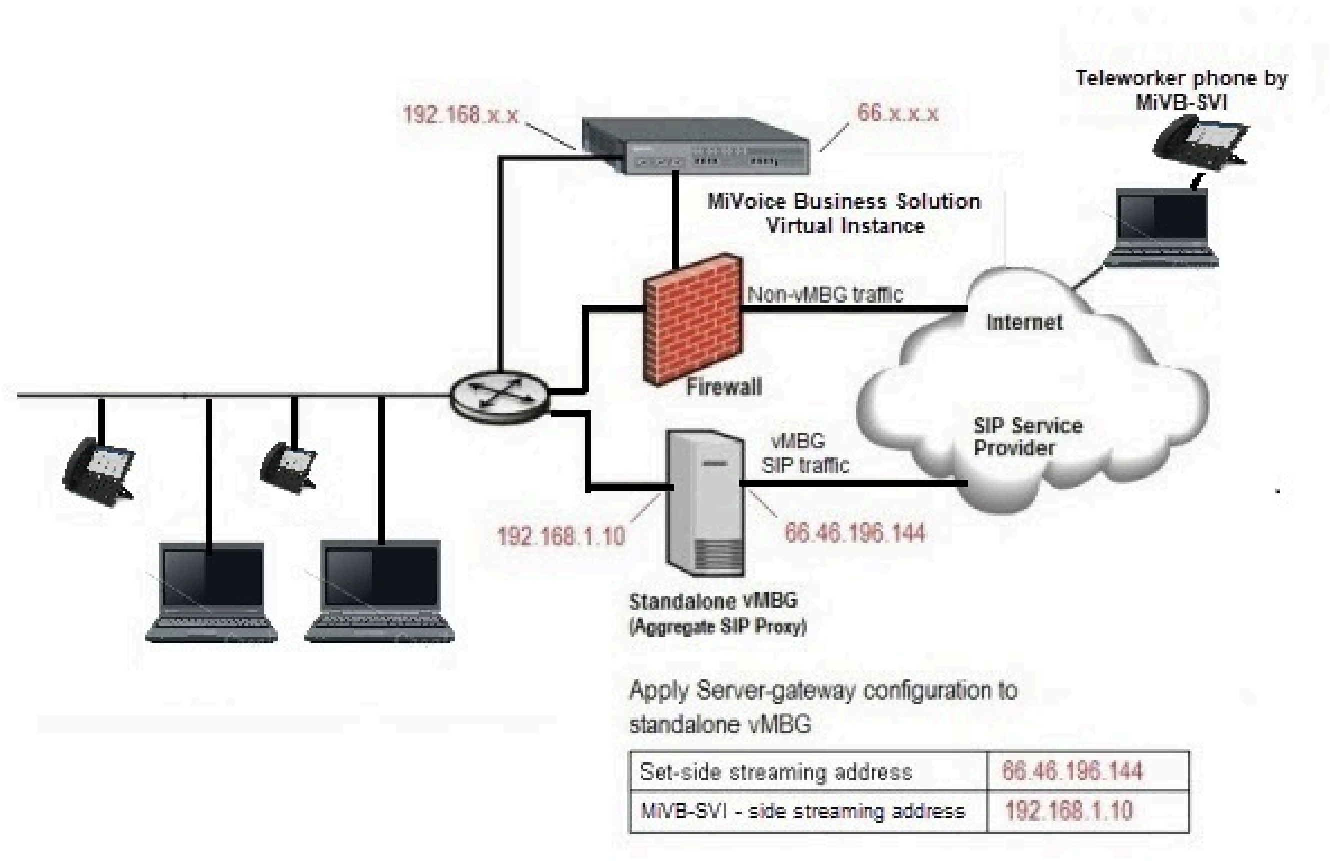
1. Access the MSL Server Console and select Configure this server.
2. In Local Networking Parameters, enter the server's internal (LAN) IP address server or select the default.
3. In WAN Network Adapters, select the server's external (WAN) adapter.
4. The external (WAN) address MUST be:
    - dedicated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



Apply Server-gateway configuration to standalone vMBG

Set-side streaming address	66.46.196.144
MiVB-SVI - side streaming address	192.168.1.10

Figure 12: Standalone vMBG for SIP Trunk Aggregation

8.8 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.

8.9 Configure Mitel Performance Analytics (optional)

For more information on configuring, refer section **Probe MSL Blade Installation** in Mitel Performance Analytics Probe Installation and Configuration Guide.

8.10 Provision Users

Depending on your site configuration, use one of the following methods to provision users on the MiVoice Business Solution Virtual Instance. MiCollab serves as the SVI user configuration hub.

- **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.
- **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.

8.10.1 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.

8.10.1.1 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.

8.10.1.2 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.

8.11 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) Refer to the section Performing Backups for more details.
- Backup the optional vMBG. Refer to the vMBG server manager online help for instructions.

Reconfiguration and Maintenance 9

This chapter contains the following sections:

- Change of resource profile
- Increase the number of devices
- Adding UCC Licenses
- Performing Backups
- Backups using VMware Applications
- Common System Administration Tasks
- Installing a Web Certificate
- Allow Trusted Network Access
- Upgrading of blades

Regular maintenance tasks include:

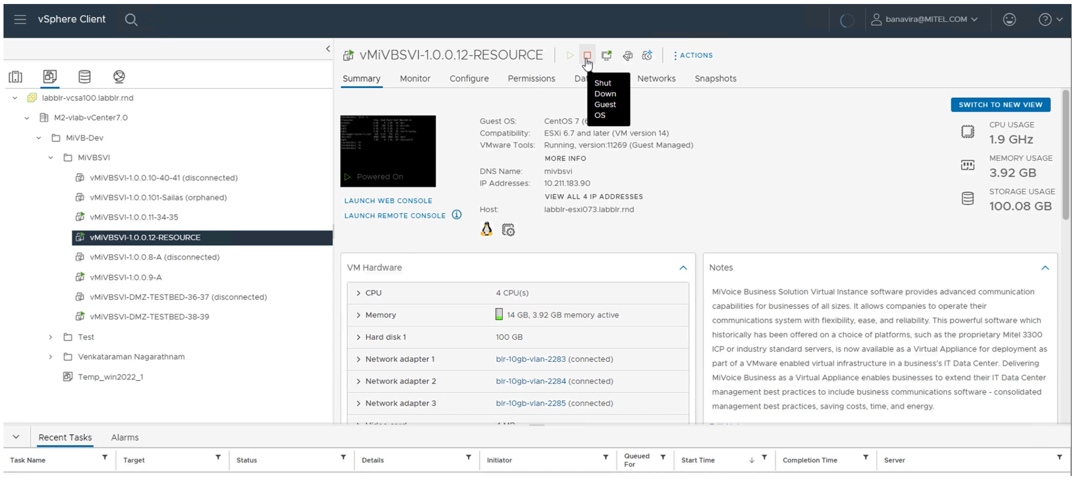
- Performing Backups

9.1 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.
    - In vSphere Client, click Shut Down.



Guest OS: CentOS 7 (
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: mivbsvi
IP Addresses: 10.211.183.90
Host: labblr-esxi073.labblr.rnd

CPU USAGE 1.9 GHz
MEMORY USAGE 3.92 GB
STORAGE USAGE 100.08 GB

VM Hardware

CPU	4 CPU(s)
Memory	14 GB, 3.92 GB memory active
Hard disk 1	100 GB
Network adapter 1	blr-10gb-vlan-2283 (connected)
Network adapter 2	blr-10gb-vlan-2284 (connected)
Network adapter 3	blr-10gb-vlan-2285 (connected)

Notes

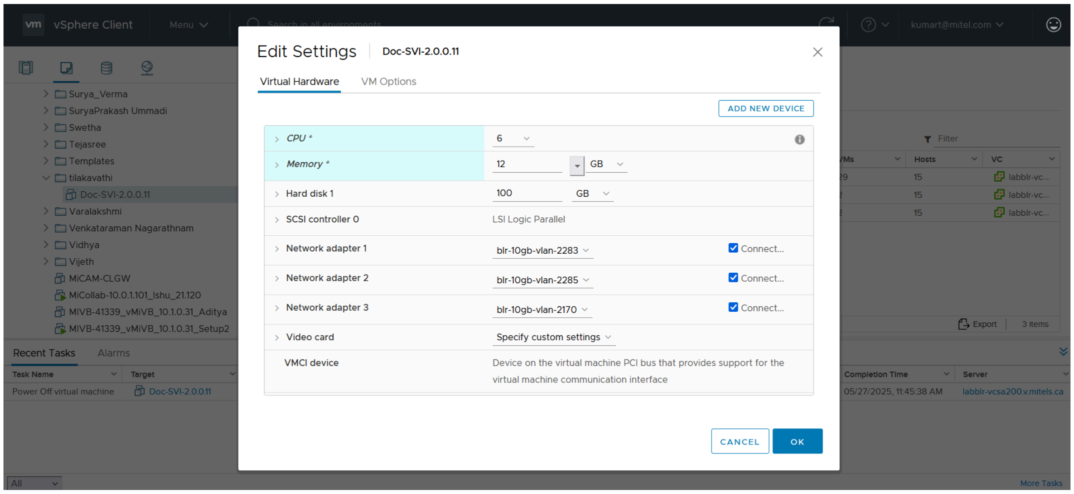
MiVoice Business Solution Virtual Instance software provides advanced communication capabilities for businesses of all sizes. It allows companies to operate their communications system with flexibility, ease, and reliability. This powerful software which historically has been offered on a choice of platforms, such as the proprietary Mitel 3300 ICP or industry standard servers, is now available as a Virtual Appliance for deployment as part of a VMware enabled virtual infrastructure in a business's IT Data Center. Delivering MiVoice Business as a Virtual Appliance enables businesses to extend their IT Data Center management best practices to include business communications software - consolidated management best practices, saving costs, time, and energy.

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server

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

    The VM is powered off.

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



Edit Settings | Doc-SVI-2.0.0.11

Virtual Hardware | VM Options

ADD NEW DEVICE

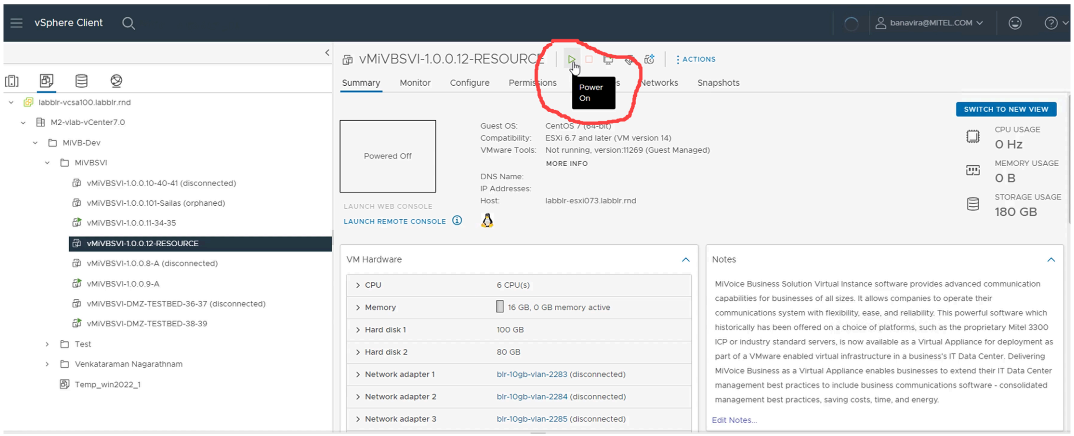
CPU *	6
Memory *	12 GB
Hard disk 1	100 GB
SCSI controller 0	LSI Logic Parallel
Network adapter 1	blr-10gb-vlan-2283 ☑ Connect...
Network adapter 2	blr-10gb-vlan-2285 ☑ Connect...
Network adapter 3	blr-10gb-vlan-2170 ☑ Connect...
Video card	Specify custom settings
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

CANCEL OK

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.



vMiVBSVI-1.0.0.12-RESOURCE

Guest OS: CentOS 7 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Not running, version:11269 (Guest Managed)
DNS Name:
IP Addresses:
Host: labblr-esxi073.labblr.rnd

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 180 GB

VM Hardware

CPU	6 CPU(s)
Memory	16 GB, 0 GB memory active
Hard disk 1	100 GB
Hard disk 2	80 GB
Network adapter 1	blr-10gb-vlan-2283 (disconnected)
Network adapter 2	blr-10gb-vlan-2284 (disconnected)
Network adapter 3	blr-10gb-vlan-2285 (disconnected)

Notes

MiVoice Business Solution Virtual Instance software provides advanced communication capabilities for businesses of all sizes. It allows companies to operate their communications system with flexibility, ease, and reliability. This powerful software which historically has been offered on a choice of platforms, such as the proprietary Mitel 3300 ICP or industry standard servers, is now available as a Virtual Appliance for deployment as part of a VMware enabled virtual infrastructure in a business's IT Data Center. Delivering MiVoice Business as a Virtual Appliance enables businesses to extend their IT Data Center management best practices to include business communications software - consolidated management best practices, saving costs, time, and energy.

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

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

6.

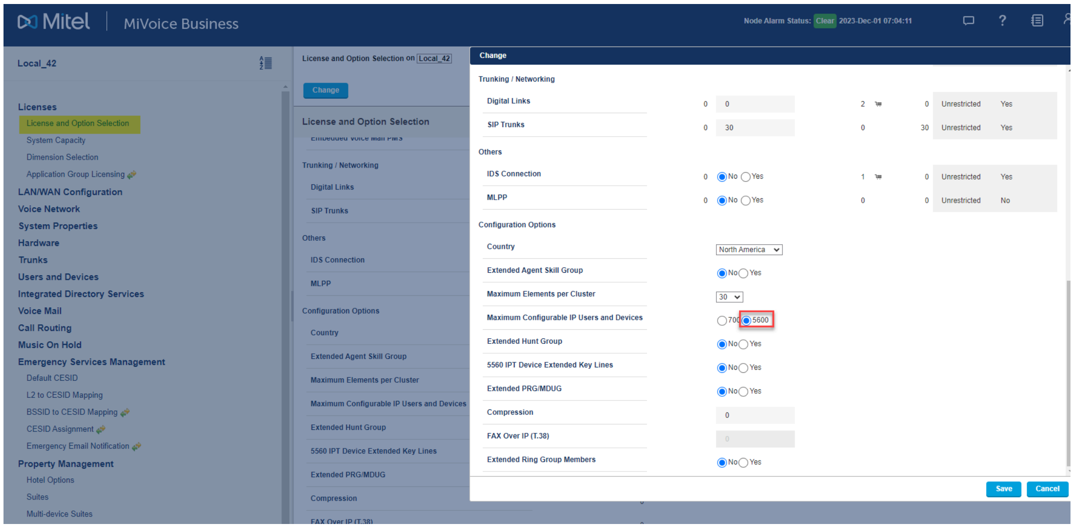
MiVoice Business Solution Virtual Instance system makes use of LVM framework for volume management, which facilitates with seamlessly expanding the existing file system with this additional disk drive.

9.2 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**.

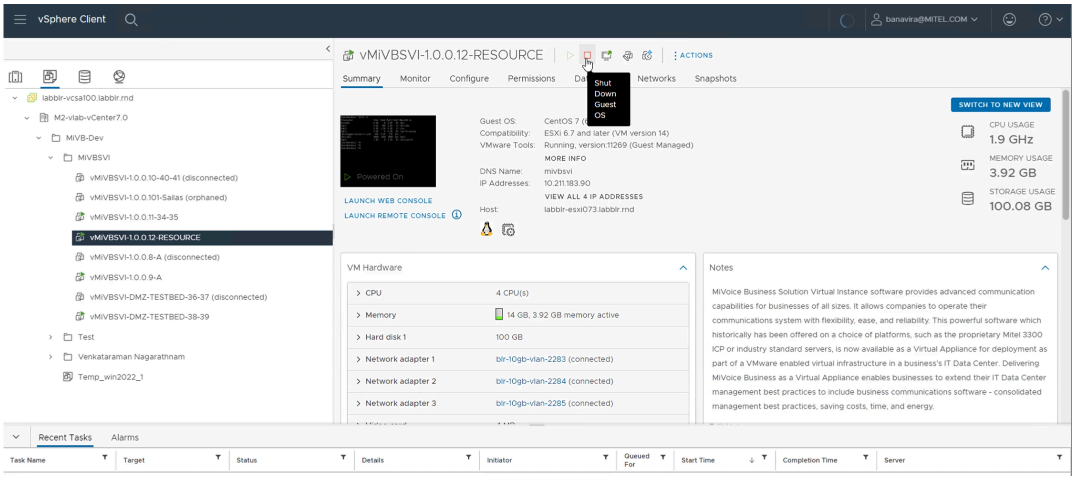


Change

Trunking / Networking						
Digital Links	0	0	2	0	Unrestricted	Yes
SIP Trunks	0	30	0	30	Unrestricted	Yes
Others						
IDS Connection	0	● No ○ Yes	1	0	Unrestricted	Yes
MLPP	0	● No ○ Yes	0	0	Unrestricted	No
Configuration Options						
Country		North America				
Extended Agent Skill Group		● No ○ Yes				
Maximum Elements per Cluster		30				
Maximum Configurable IP Users and Devices		○ 700 ● 5600				
Extended Hunt Group		● No ○ Yes				
5560 IPT Device Extended Key Lines		● No ○ Yes				
Extended PRG/MDUG		● No ○ Yes				
Compression		0				
FAX Over IP (T.38)		0				
Extended Ring Group Members		● No ○ Yes				

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.



Guest OS: CentOS 7 (6
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:11269 (Guest Managed)
DNS Name: mivbsvi
IP Addresses: 10.211.183.90
Host: labblr-esxi073.labblr.rnd

CPU USAGE 1.9 GHz
MEMORY USAGE 3.92 GB
STORAGE USAGE 100.08 GB

VM Hardware

CPU	4 CPU(s)
Memory	14 GB, 3.92 GB memory active
Hard disk 1	100 GB
Network adapter 1	blr-10gb-vlan-2283 (connected)
Network adapter 2	blr-10gb-vlan-2284 (connected)
Network adapter 3	blr-10gb-vlan-2285 (connected)

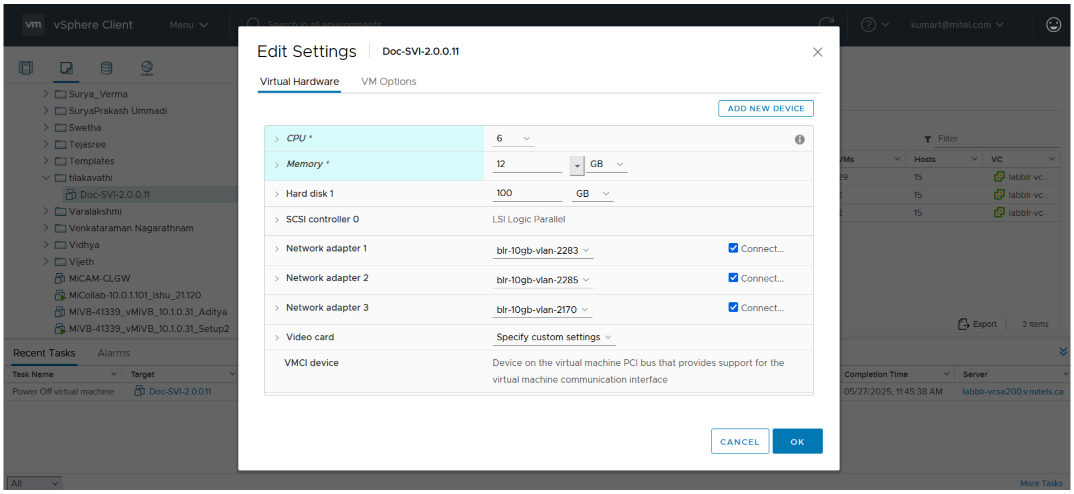
Notes

MiVoice Business Solution Virtual Instance software provides advanced communication capabilities for businesses of all sizes. It allows companies to operate their communications system with flexibility, ease, and reliability. This powerful software which historically has been offered on a choice of platforms, such as the proprietary Mitel 3300 ICP or industry standard servers, is now available as a Virtual Appliance for deployment as part of a VMware enabled virtual infrastructure in a business's IT Data Center. Delivering MiVoice Business as a Virtual Appliance enables businesses to extend their IT Data Center management best practices to include business communications software - consolidated management best practices, saving costs, time, and energy.

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

The VM is powered off.

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



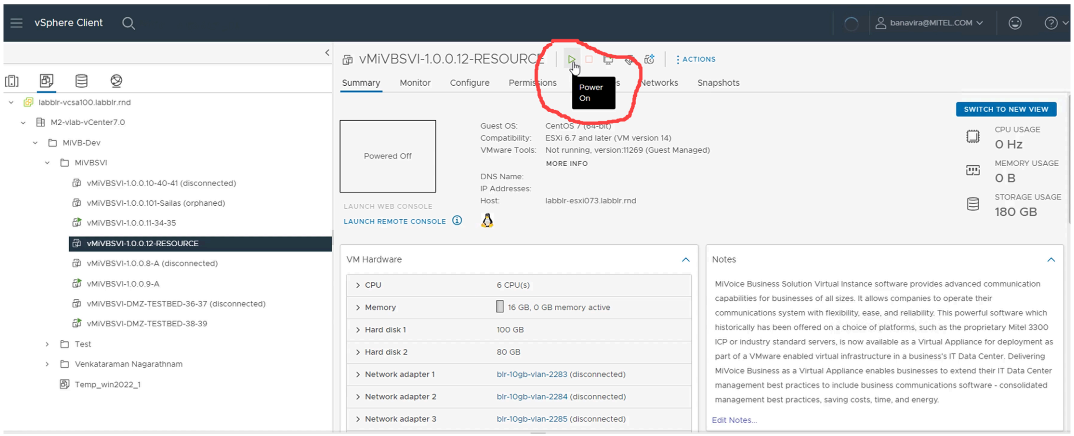
Edit Settings | Doc-SVI-2.0.0.11

CPU *	6
Memory *	12 GB
Hard disk 1	100 GB
SCSI controller 0	LSI Logic Parallel
Network adapter 1	blr-10gb-vlan-2283 ☑ Connect...
Network adapter 2	blr-10gb-vlan-2285 ☑ Connect...
Network adapter 3	blr-10gb-vlan-2170 ☑ Connect...
Video card	Specify custom settings
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

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.



Guest OS: CentOS 7 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Not running, version:11269 (Guest Managed)
DNS Name:
IP Addresses:
Host: labblr-esxi073.labblr.rnd

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 180 GB

CPU	6 CPU(s)
Memory	16 GB, 0 GB memory active
Hard disk 1	100 GB
Hard disk 2	80 GB
Network adapter 1	blr-10gb-vlan-2283 (disconnected)
Network adapter 2	blr-10gb-vlan-2284 (disconnected)
Network adapter 3	blr-10gb-vlan-2285 (disconnected)

MiVoice Business Solution Virtual Instance software provides advanced communication capabilities for businesses of all sizes. It allows companies to operate their communications system with flexibility, ease, and reliability. This powerful software which historically has been offered on a choice of platforms, such as the proprietary Mitel 3300 ICP or industry standard servers, is now available as a Virtual Appliance for deployment as part of a VMware enabled virtual infrastructure in a business's IT Data Center. Delivering MiVoice Business as a Virtual Appliance enables businesses to extend their IT Data Center management best practices to include business communications software - consolidated management best practices, saving costs, time, and energy.

9.3 Adding UCC Licenses

To purchase UCC licenses:

1. Contact Mitel Customer Services (or your Service Provider) and place your order.
2. Obtain your SLS Serial ID (EID) from Mitel Customer Services.
3. In your SLS account, access the appropriate SLS Serial and assign the upgrade products from your license account to the SLS Serial. The SLS 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 SLS license upgrades. UCC licenses are applied automatically during the synchronization.

9.4 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.

9.4.1 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.

9.4.2 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**.

9.5 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.

9.6 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 subnet or device to the 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.

9.7 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.

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.

9.8 Allow Trusted Network Access

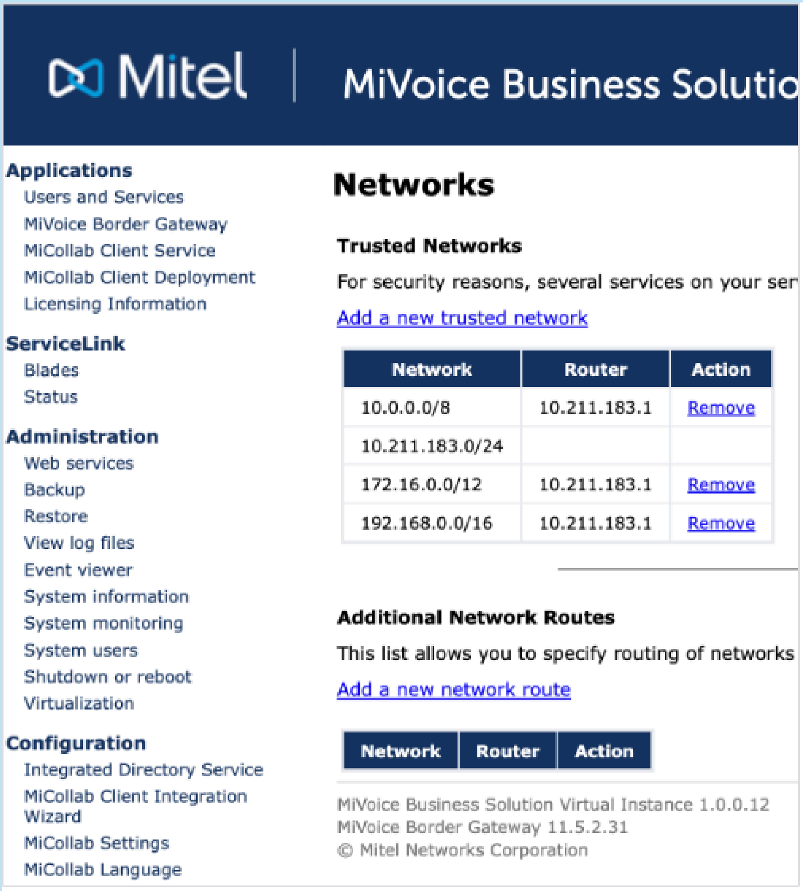
If the users are deployed on a different subnet than the MiVoice Business Solution Virtual Instance, it is necessary to grant them access. First, you must configure them as a trusted local network and then grant them express permission.

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, 10.0.0/8, 172.16.0.0/12, 192.168.0/16).

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`



Networks

Trusted Networks

For security reasons, several services on your ser

Add a new trusted network

Network	Router	Action
10.0.0.0/8	10.211.183.1	Remove
10.211.183.0/24		
172.16.0.0/12	10.211.183.1	Remove
192.168.0.0/16	10.211.183.1	Remove

Additional Network Routes

This list allows you to specify routing of networks

Add a new network route

Network	Router	Action

MiVoice Business Solution Virtual Instance 1.0.0.12
MiVoice Border Gateway 11.5.2.31
© Mitel Networks Corporation

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 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**.

9.9 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 10

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.

10.1 Database Restore or Recovery

This section provides procedures for

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

10.2 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.

10.3 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**.

10.4 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
If CloudLink Gateway Portal Access is failing.	CloudLink Gateway is running on the MBG IP, but the MBG IP is not included in the MiVB trusted subnets.	SSH into each MiVB system manually (if more than one) and, from the `mcdDebug` shell, run `DSCtrlrSetTrustedSubnets "second IP (MBG & MiCollab)"` to ensure the MiVB trusts the MBG where the CloudLink Gateway is running.

Symptom	Possible Cause	Corrective Action

All Network Elements appear grayed out and cannot be selected
Generic error log **60000009**:
`<LMSG><LEN=72>CUDM_GPMSClient:: startupGPMSClient - GPMSGetConfigPolicy failed 60000009</LMSG>`
`<LMSG><LEN=81>CUDM_ ControlEntity:: turnUDMOnImpl - startupGPMSClient failed 60000009(GE_NOTIMPL)</LMSG>`
`<LMSG><LEN=78>CUDM_ ControlEntity ::turnUDMOnImpl - Failed (origUDMOnFlag 0) - result 60000009</LMSG>`
`<LMSG><LEN=57>CUDM_Control::turn UDMOn - turnUDMOnImpl failed : 60000009</LMSG>`
	• The VMware Authorization Service failed to start, often after a VMware Workstation upgrade.
	• The virtual machine did not start properly due to issues such as a corrupted installation, software conflicts, or system errors.
	• A failed or incomplete software installation, update, or configuration may have caused the issue.
		• **Repair VMware Workstation**: Reinstall or repair the software to fix any corrupted files and ensure all services start correctly.
		• **Restart the system**: A reboot can often resolve temporary service startup problems.

When browsing to the MiCollab server webUI on an SVI system the browser freezes.	This problem is caused by the MiCollab server Remote Proxy service trying to proxy web traffic to itself and essentially causing a loop.	The solution is to remove the MiCollab server entry from the Remote Proxy form A restart is not needed to apply this change. **Note**: The MiCollab server FQDN should be programmed in the Remote Proxy list where SVI is deployed in Server-Only mode in DMZ.
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%.

Symptom	Possible Cause	Corrective Action
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.	
	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.	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.
	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.	

Symptom	Possible Cause	Corrective Action
Voice quality issues with audio streams that pass through the SVI application	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.
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.

Symptom	Possible Cause	Corrective Action
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.
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.

Symptom	Possible Cause	Corrective Action
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 Software License Server (SLS). The SLS Serial ID (EID) is not registered with the SLS.	1. Log into the MiVoice Business Solution Virtual Instance server manager. 2. Access the Status page and **Sync** the MiCollab EID/ Serial with the SLS. 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.
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 (Multi Object Manager) server runs after the cleared alarms.

Appendix A

This chapter contains the following sections:

- UCC Default Roles and Templates

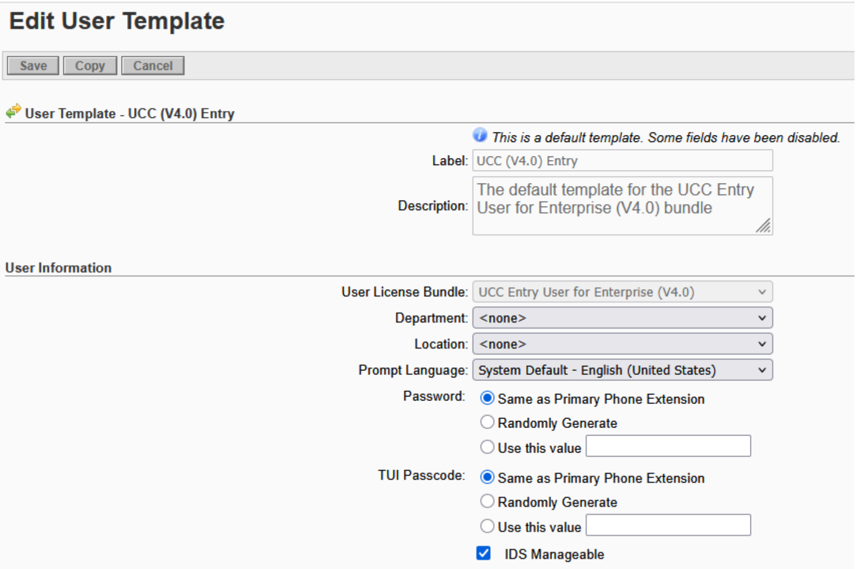
11.1 UCC Default Roles and Templates

Default Roles

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

- Default UCC Entry
- Default UCC Standard

11.1.1 Entry User for Business Template



Edit User Template

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 Enterprise (V4.0) bundle

User Information

User License Bundle: UCC Entry User for Enterprise (V4.0)

Department: <none>

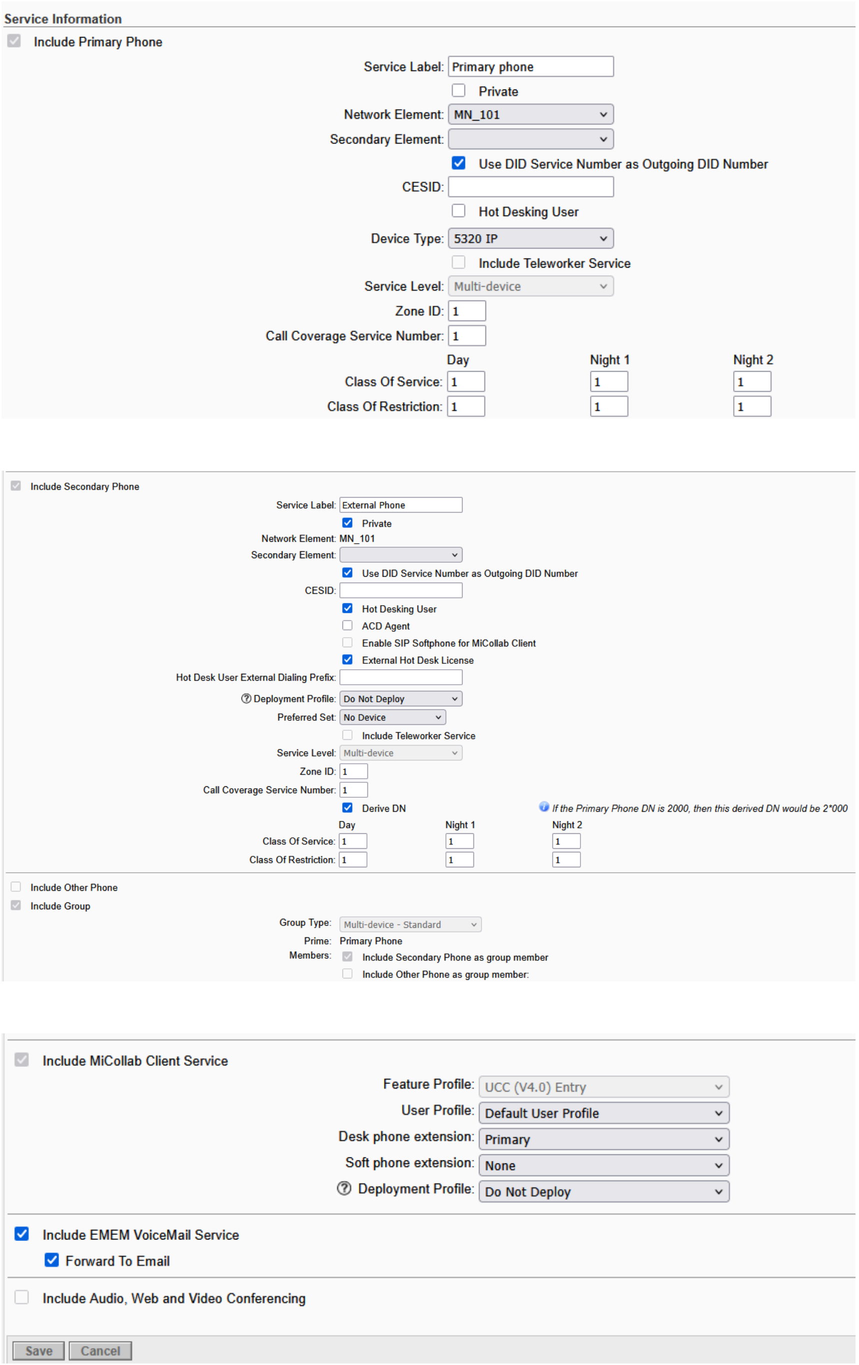
Location: <none>

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: MN_101

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

Network Element: MN_101

Secondary Element:

☑ Use DID Service Number as Outgoing DID Number

CESID:

☑ Hot Desking User

□ ACD Agent

□ Enable SIP Softphone for MiCollab Client

☑ External Hot Desk License

Hot Desk User External Dialing Prefix:

Deployment Profile: Do Not Deploy

Preferred Set: No Device

□ Include Teleworker Service

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 MiCollab Client Service

Feature Profile: UCC (V4.0) Entry

User Profile: Default User Profile

Desk phone extension: Primary

Soft phone extension: None

Deployment Profile: Do Not Deploy

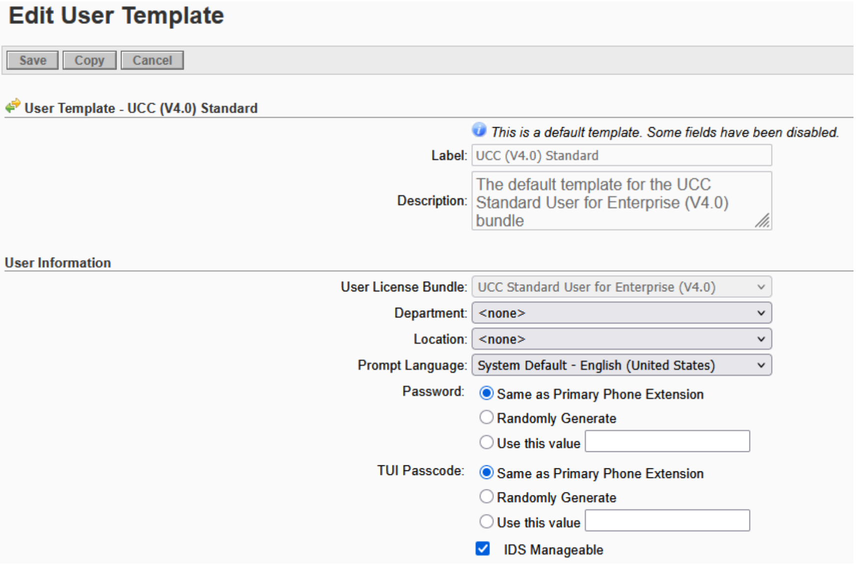
☑ Include EMEM VoiceMail Service

☑ Forward To Email

□ Include Audio, Web and Video Conferencing

Figure 13: Entry User Template (Page 1 of 2)

11.1.2 Standard User For Business Template



Edit User Template

User Template - UCC (V4.0) Standard

This is a default template. Some fields have been disabled.

Label: UCC (V4.0) Standard

Description: The default template for the UCC Standard User for Enterprise (V4.0) bundle

User Information

User License Bundle: UCC Standard User for Enterprise (V4.0)

Department: <none>

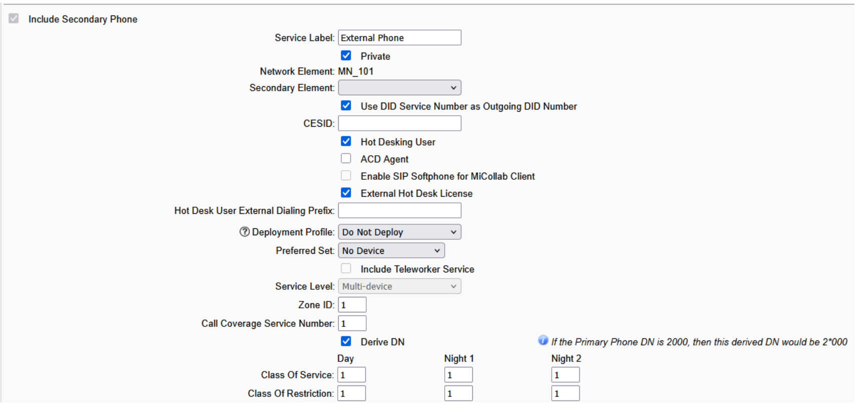
Location: <none>

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



☑ Include Secondary Phone

Service Label: External Phone

☑ Private

Network Element: MN_101

Secondary Element:

☑ Use DID Service Number as Outgoing DID Number

CESID:

☑ Hot Desking User

□ ACD Agent

□ Enable SIP Softphone for MiCollab Client

☑ External Hot Desk License

Hot Desk User External Dialing Prefix:

Deployment Profile: Do Not Deploy

Preferred Set: No Device

□ Include Teleworker Service

Service Level: Multi-device

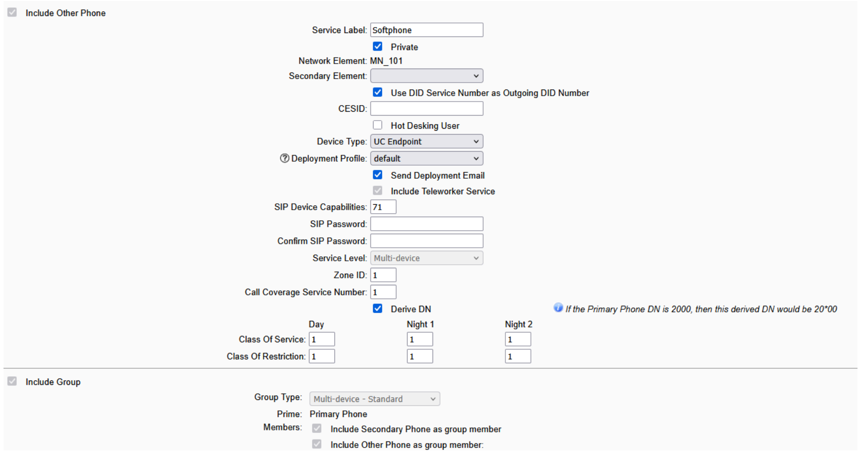
Zone ID: 1

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

Service Label: Softphone

☑ Private

Network Element: MN_101

Secondary Element:

☑ Use DID Service Number as Outgoing DID Number

CESID:

□ Hot Desking User

Device Type: UC Endpoint

Deployment Profile: default

☑ Send Deployment Email

☑ Include Teleworker Service

SIP Device Capabilities: 71

SIP Password:

Confirm SIP Password:

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 20*00*

	Day	Night 1	Night 2
Class Of Service:	1	1	1
Class Of Restriction:	1	1	1

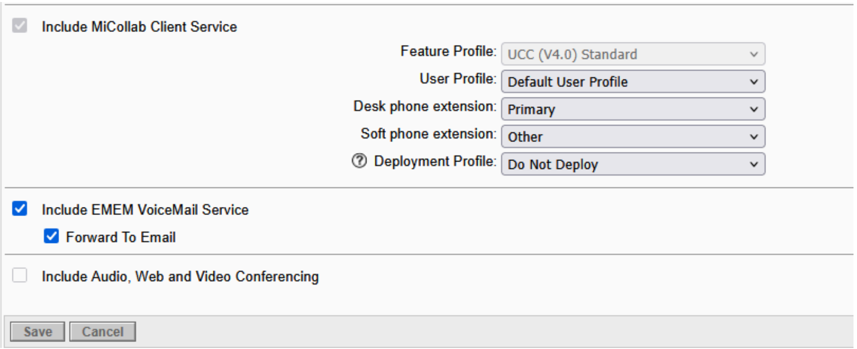
☑ Include Group

Group Type: Multi-device - Standard

Prime: Primary Phone

Members: ☑ Include Secondary Phone as group member

☑ Include Other Phone as group member:



☑ Include MiCollab Client Service

Feature Profile: UCC (V4.0) Standard

User Profile: Default User Profile

Desk phone extension: Primary

Soft phone extension: Other

Deployment Profile: Do Not Deploy

☑ Include EMEM VoiceMail Service

☑ Forward To Email

□ Include Audio, Web and Video Conferencing

Figure 14: Standard User for Business Template

Appendix B 12

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.

12.1 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

12.2 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 EID/Serial ID 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 Serial ID. After you complete this network configuration, you launch the Initial Configuration Wizard to complete initial configuration.

12.3 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.

12.4 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).

12.5 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.

Mitel
Powering connections

mitel.com