MiVoice Business Express Deployment Guide

RELEASE 8.0

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

MiVoice Business Express Deployment Guide
Release 8.0
September 2017

CHAPTER 1: INTRODUCTION

CHAPTER 2: DESCRIPTION

CHAPTER 7: PERFORM CONFIGURATION

Chapter 1

INTRODUCTION

PURPOSE OF THIS GUIDE

This guide provides instructions on how to deploy the Mitel® MiVoice Business Express (MiVB-X) software in a virtualized environment. It covers the following topics:

- Product Description
- Plan Customer Site
- Deploy or Install MiVoice Business Express
- Configure System
- Maintenance and
- Troubleshooting.

INTENDED AUDIENCE

This guide is intended primarily for

- Service providers who host MiVoice Business Express in a data center and provide it as a software solution to customers
- Data center providers who host the virtual infrastructure on which the MiVoice Business Express resides
- Dealers who deploy, configure, provision, and maintain the MiVoice Business Express solution
- Customers who choose to deploy the virtual infrastructure and then allow a dealer to deploy, configure, provision, and maintain the solution.

Service providers, dealers, and customers who use this document must have successfully completed the required Mitel MiVoice Business Express Deployment Training.

In addition, service providers must have the ability to

- Configure and manage a data center infrastructure
- Deploy and support VMware and/or Microsoft Hyper-V virtualization products.

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

ROLES AND TASKS

The tasks that you perform during a MiVoice Business Express deployment depend on your role (solution provider, data center provider, dealer or customer administrator) and the deployment model (Software as a Service, Infrastructure as a Service, or Customer Premise Equipment). Use the following table as a general guideline to help you identify your responsibilities.

Table 1: MiVoice Business Express Roles and Tasks

TASK/DEPLOYMENT	SOFTWARE AS A SERVICE (SAAS)	INFRASTRUCTURE AS A SERVICE (IAAS)	CUSTOMER PREMISE EQUIPMENT (CPE)
Set up virtualization environment (page 46)	Service provider	Data center provider	VMware dealer, Microsoft Hyper-V consultant, or customer
Plan site (page 31)	Service provider	Dealer	Dealer
Deploy virtual appliance (page 63) or Install on Hyper-V (page 67)	Service provider	Dealer or Service provider	Customer
Run configuration wizard (page 78)	Service provider	Dealer or Service provider	Dealer
Perform advanced configuration (page 98)	Service provider	Dealer	Dealer
Configure optional standalone vMBGs (page 108)	Service provider	Dealer	Dealer
Perform user provisioning (page 112)	Service provider	Dealer	Dealer
Perform backups (page 121)	Service provider	Dealer	Dealer or customer administrator
Install phones and train users	Service provider	Dealer	Dealer
Perform user administration (add, edit, and delete) from the MiCollab Users and Services application	Service provider or customer administrator	Dealer or customer administrator	Dealer or customer administrator
Perform maintenance (page 115)	Service provider	Dealer	Dealer

ABOUT THE DOCUMENTATION SET

MIVOICE BUSINESS EXPRESS

- *MiVoice Business Express Deployment Guide* (this guide) provides installation instructions for the system software and supported applications.
- *MiVoice Business Express Engineering Guidelines* provides deployment models, limitations and constraints, and performance capacities for the MiVoice Business Express solution.
- *MiCollab Engineering Guidelines* provides guidelines for the supported applications.
- *Virtual Appliance Deployment Guide* provides guidelines for deploying Mitel Virtual Appliances and applications in a virtual infrastructure.

MITEL MIVOICE BUSINESS COMMUNICATIONS PLATFORM

- *MiVoice Business System Administration Tool Online Help* provides instructions on how to configure and program the MiVoice Business communications platform.

MICOLLAB

Administrator

- *Server Manager help* provides configuration, administration, and maintenance procedures for the system server.
- *Users and Services help* provides instructions on how to manage user data (add, edit, and delete users) and assign or remove user services, such as MiVoice Border Gateway or Teleworker.
- *NuPoint Unified Messaging help* provides system administrators with instructions on how to configure and maintain NuPoint Unified Messaging functionality through the web console interface.
- *MiCollab AWV help* provides instructions on how to provision the MiCollab AWV application.

End User

- *MiCollab End User Portal Online Help* provides users with instructions on how to configure their portal settings and use the communication applications.
- *MiCollab AWV Quick Reference Guide* provides procedures on how to set up and use the conferencing features.

NUPOINT UNIFIED MESSAGING

- *NuPoint Unified Messaging User Guide* describes how to use the voice mail system.
- *Nupoint Unified Messaging Mitel TUI Quick Reference Guide* provides a summary of basic user options and procedures for the Mitel TUI.

MIVOICE BORDER GATEWAY (TELEWORKER)

- *Engineering Guidelines:* provides firewall configuration information.
- *Installation and Maintenance Guide with Web Proxy* describes the installation requirements and provides installation instructions for the MBG server.

MICOLLAB CLIENT

- *Administrator Guide* provides instructions on how to configure MiCollab Client on MiVoice Business Platforms.
- *Administrator Portal Online Help* provides information and instructions for the UC Server administrator interface.
- *MiCollab Client Deployment Online Help* provides instructions on how to deploy MiCollab Client for Mobile clients.
- *MiTeam Reference Guide:* provides user information for Mitel's Cloud-based collaboration tool.
- *MiCollab Client Quick Reference Guide*

MITEL STANDARD LINUX

- *Mitel Standard Linux Installation and Administration Guide* provides installation and administration information for the MSL operating system.

USER DOCUMENTATION

- Download end-user documentation for Mitel phones, softphone clients, and applications from the **End-User** screen on the Mitel Customer documentation site.

PHONE INSTALLATION GUIDES

- Download phone installation guides from the Mitel Customer documentation site.

ACCESSING DOCUMENTATION

MITEL PRODUCT DOCUMENTATION

To access MiCollab product documentation:

1. Log on to **Mitel Connect.**
2. Click **Mitel Online**.
3. Under **Support**, click **Product Documentation**.
4. Click **Communications Platforms** and then click **MiVoice Business Express**.

MITEL KNOWLEDGE BASE ARTICLES

To access Mitel Knowledge Base articles:

1. Log on to **Mitel Connect**.
2. Click **Mitel Online**.
3. Click **Support**, under **Technical Support**, click **Mitel Knowledge Base**. The Knowledge Base search engine opens.

PRODUCT BULLETINS

To access Mitel Product Bulletins:

1. Log on to **Mitel Connect**.
2. Click **Mitel Online**.
3. Under **Support**, click **Bulletins**.
4. Click the link to access a list of recent product bulletins.

GLOSSARY

TERM	NAME	DESCRIPTION
3300 ICP	3300 Integrated Communications Platform	Mitel IP communications platform supporting 30 to 60,000 users. The 3300 ICP is the hardware platform that runs the MiVoice Business (MiVoice Business) software.
AMC	Application Management Center	A web-based service that handles licensing of Mitel products
ARID	Application Record ID	An identification number obtained from the Mitel Application Management Center (AMC). Each ARID is used to license software on a specific Mitel product.
Authorized Partner		Dealers, resellers, and solutions providers who are authorized by Mitel to sell and service Mitel products and solutions.
BUP	Bulk User Provisioning	A software tool within the USP application that allows you to bulk import user data from a CSV or LDIF file; use Quick Add to provision a single user; program a range of fields using Auto-Fill; apply roles to multiple users; and resolve detained and failed IDS updates.
CA	Certificate Authority	To securely authenticate connections, applications may request a security certificate signed by the MSL server using a Mitel Certificate Authority (CA). You can manage Certificate Signing Requests (CSRs) and issued certificates using the **Certificate Management** panel in the MiCollab Server manager.
CESID	Caller Emergency Service Identification.	A number that uniquely identifies the device that dialed an emergency call (for example 911). The CESID is fed into the automatic location identification (ALI) database at the Public Safety Answering Point (PSAP) so that emergency services can be dispatched to the correct location

TERM	NAME	DESCRIPTION
Cluster (MiVoice Business)		Refers to a grouping of elements (for example, a network of MiVoice Business systems) that share common dialing plans, or common directory information, such as Remote Directory Numbers with Telephone Directory.
COR	Class of Restriction	A programming feature of the MiVoice Business that gathers Class of Restriction numbers into groups. The COR Groups define which Classes of Restriction cannot access an outgoing trunk route. COR group numbers are assigned to users to restrict their outgoing call privileges.
COS	Class of Service	A programming feature of the MiVoice Business that specifies the optional features associated with that COS. Classes of Service, identified by Class of Service numbers, are assigned to MiVoice extensions and trunks.
Detained Queue		The *Detained Queue* in the *Bulk User Provisioning* tool lists the detained and failed Integrated Directory Services operations: • Detained IDS operations are operations that have been performed on the directory server that have not been applied to the USP database yet. • Failed IDS operations are directory server updates that the MiCollab system could not apply to the USP database. From the Detained Queue, you can add, update, or delete IDS operations that have been detained.
DID	Direct Inward Dial	Also known as DDI (Direct Dialing Inwards). This MiVoice Business feature allows an external caller to dial an internal extension without having to go through an attendant or operator.
Directory Server		A directory server is not simply a database, but a specialized server for directories. A directory can be distinguished from a general-purpose database by the usage pattern. A directory contains information that is often searched but rarely modified. Host names or user names, for example, are assigned once and then looked up thousands of times. Directory servers are suited for this type of usage; whereas, relational databases are best suited for maintaining data that is constantly changing. Another difference is that relational databases store information in rows of tables; whereas a directory server uses object-oriented hierarchies of entries.
DMZ	Demilitarized Zone	A computer host or small network inserted as a “neutral zone” between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.
ESX Hypervisor		Main Hypervisor from VMware. Phased out in favour of ESXi in Release 4.1.
ESXi Hypervisor		The latest variant of Hypervisor It has a smaller footprint because it does not require or include the ESX Service Console.

TERM	NAME	DESCRIPTION
Hot Desk		Hot Desking allows a number of users to share one or more hot desk sets. Anyone with a Hot Desk DN and User PIN can log to log into an available hot desk-enabled telephone. Once logged in, the user can • Receive incoming calls at the set • Place outgoing calls • Retrieve voice messages • Program and use feature keys 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.
Hunt Groups		A hunt group is a group of phones to which incoming calls are directed by dialing a master number. Two types of hunting are provided by the system, circular and terminal: • Circular hunting starts at the extension after the last extension in the hunt group to which a call was placed (the extension rung), and hunts overall extensions in the hunt group in the sequence programmed. Hunting stops at the first idle extension. • Terminal hunting starts at the first extension in the hunt group and ends at the first idle extension found. Hunting takes place in the order in which the extensions were programmed into the hunt group.
Hyper-V (Microsoft)		Microsoft virtualization product that allows you to create and run virtual machines.
Hypervisor	A platform that allows multiple operating systems to run on a host computer at the same time.	
ICP	Integrated Communications Platform	
ICW	Initial Configuration Wizard	A wizard that guides you through the initial configuration of the MiVoice Business Express system. Do not confuse the ICW with the Mitel Integrated Configuration Wizard (MiCW) that technicians use to perform the initial programming of MiCollab and MiVoice Business platforms
IDS	Integrated Directory Services	Synchronizes user and service data between a corporate directory server and the MiCollab-IDS using the Lightweight Directory Access Protocol (LDAP).
LAN Mode	Local Area Network Mode	A deployment model for the MiCollab (or Mitel Standard Linux) server. When MiCollab is deployed in server-only mode, it provides the network with services, but not the routing and security functions associated with the role of "gateway". The LAN mode configuration is typically used for networks that are already behind a separate firewall. In other words, a separate firewall fulfills the role of gateway, providing routing and network security. (Also known as Server-only mode).

TERM	NAME	DESCRIPTION
LDAP	Lightweight Directory Protocol	Lightweight Directory Access Protocol is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.
MBG	MiVoice Border Gateway	Formerly know as the Multi-Protocol Border Gateway. MBG software supports teleworking and call recording services. The MBG server supports the Teleworker service in the DMZ.
MCS	Mitel Communications Suite	This communications platform consists of MiVoice Business call processing software running on an SUN Microsystems server. MiCollab supports the MCS platform.
MiCollab		Mitel software solution that enables Mitel applications to be co-resident on one server.
MiCollab Client		Software solution that provides clients (MiCollab Client deskphone users or MiCollab Client softphone users) with a single access point for communication and collaboration needs. It converges the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications
MiCollab Client Deployment		This MiCollab software application supports the simplified deployment of MiCollab for Mobile clients. This functionality is supported in integrated and co-located MiCollab Client deployments. The administrator uses this application to • deploy large groups of users • leverage user profiles • download multiple files to the clients • update clients.
MiCollab Client Integration Wizard		A software application (wizard) that integrates MiCollab Client user and phone data with the MiCollab USP data (see MiCollab Client Integrated Mode). If you are installing a new MiCollab system into an existing site that consists of one or more MiVoice Business platforms, you can use this wizard to update the MiCollab database with the user and phone data from the MiVoice Business.
MiCollab Client Integrated Mode		In this mode, the MiCollab system keeps the Users and Services database and MiCollab Client database synchronized so they function like a single database on the MiCollab server. This mode is only supported with MiVoice Business systems. It allows you to provision MiCollab Client services from the MiCollab Users and Services application and supports Single Point of User Provisioning of the MiCollab Client services on the MiVoice Business platform(s). This is the recommended mode for sites that meet the integration requirements.
MiCollab Client Co-located Mode		In this mode, the Users and Services data and MiCollab Client data are contained in separate, independent databases on the MiCollab server. This mode is supported for sites with either MiVoice Business or MiVoice Office platforms. With this mode, you must provision MiCollab Client services separately from the MiCollab Client Service Application interface.

TERM	NAME	DESCRIPTION
MiCollab Client Integration Wizard		Migrates the MiCollab Client database in a MiCollab system from co-located mode to integrated mode.
MiCollab Audio, Web, and Video (AWV) Conferencing		Mitel software solution that provides conferencing and collaboration services using a Web-based browser. In previous MiCollab releases, the product name for this application was Mitel Conferencing Advanced.
MiCollab End User portal		A MiCollab web interface that provides a common portal for users to update/enter user-configurable information for all applications.
MiCollab Server		MiCollab software installed in conjunction with the MSL operating system on a server platform.
MiCollab Virtual Appliance		MiCollab system deployed as a virtual appliance (vApp) running in a virtualization environment.
MiVoice Business Express	Formerly Unified Communications and Collaboration Virtual Appliance (vUCC)	Mitel communications solution for small to medium business that runs as a virtual appliance.
MICW	Mitel Integrated Configuration Wizard	A standalone software application that performs initial system setup of a MiCollab server and MiVoice Business platforms. The MiCW is a separate wizard from the Initial Configuration Wizard (ICW). The MiCW is not used to configure the MiVoice Business Express.
MiTeam		
MiVoice for Lync		An application that integrates with Microsoft Lync Client and allows Microsoft Lync users to use Mitel telephony functionality through its feature-rich MiCollab Client infrastructure.
MiVoice Business	MiVoice Business	MiVoice Business (MiVoice Business) is the brand name of the call-processing software that runs on hardware platforms, such as 3300 ICP controllers.
MiVoice Business-ISS	MiVoice Business for Industry Standard Servers	This communications platform consists of MiVoice Business call processing software running on an industry standard platform. MiCollab is supported for the MiVoice Business-ISS platform.
MiVoice Office	MiVoice Office Communications Platform	Mitel IP communications platform (formerly Inter-Tel 5000 Network Communications Solutions) supporting up to 250 users.
MOL	Mitel Online	Mitel's web portal for authorized dealers and technicians.
MSL	Mitel Standard Linux	The operating system that supports MiCollab software that comprises a base for all MiCollab software.
MWI	Message Waiting Indication	Line keys on multi-line phones can be programmed as message waiting indicators which are associated with the mailboxes of other phones. The indicator flashes when a message is waiting in the associated mailbox.

TERM	NAME	DESCRIPTION
Network Edge Mode		A type of deployment for the MiCollab (or Mitel Standard Linux) server. In this deployment configuration, MiCollab manages the connection to the Internet by routing Internet data packets to and from the network (which allows all the computers on the network to share a single Internet connection) and by providing security for the network, minimizing the risk of intrusions. When one of the computers on the local network contacts the Internet, MiCollab not only routes that connection, but seamlessly interposes itself into the communication. This prevents a direct connection from being established between an external computer on the Internet and a computer on the local network, which significantly reduces the risk of intrusion. Network Edge mode is also known as Server-gateway mode.
NP-UM	NuPoint Unified Messaging	Server-based voice processing system that provides call processing along with voice messaging and paging support.
Oria		A system management and customer self-service application. It allows a service provider to manage and deploy hosted voice services to their customers. Oria also allows a service provider to offer each of their customers an administration and self-service portal to make site specific moves, adds, changes, and deletes.
OVA	Open virtual appliance or application	A packaging format for virtual machines that allows virtual machine templates to be distributed, customized, and instantiated on any OVA supporting VMM/hypervisor.
OVF	Open Virtualization Format	A distribution format for virtual appliances that uses existing packaging tools to combine one or more virtual machines with a standards-based XML wrapper. OVF gives the virtualization platform a portable package containing all required installation and configuration parameters for virtual machines. This format allows any virtualization platform that implements the standard to correctly install and run virtual machines.
Role		A role defines the task, position, or responsibilities for a type of user within the organization. Roles are associated with user templates that define the common phone and application service settings for the roles.
Server Console		A text-based control panel built into the Mitel Standard Linux operating system that technicians use to perform maintenance tasks such as • install the MiCollab software • configure network parameters • perform upgrades and software updates • upgrade application suite licensing • perform backups.
Server-gateway mode		See Network Edge mode.

TERM	NAME	DESCRIPTION
Server Manager		A web-based control panel, also called the "server manager", that administrators use to • configure and administer the MiCollab applications • perform server administration tasks, such as view logs, display system information, assign system users, and perform backups • configure network and server security settings • set system-wide parameters, such as system language and password strength.
Server-only mode		See LAN mode.
SIP	Session Internet Protocol	SIP is an ASCII-character-based signaling protocol designed for real-time transmission using Voice over IP (VoIP). The appeal of SIP is the promise of interoperability of telephones from propriety PBXs. SIP extends the foundation of open-standards from the Internet to messaging, enabling disparate computers, phones, televisions and software to communicate. SIP is a streamlined protocol, developed specifically for IP telephony. It is smaller and more efficient than H.323. SIP takes advantage of existing protocols to handle certain parts of the process. For example, Media Gateway Control Protocol (MGCP) is used by SIP to establish a gateway to connect to the PSTN system. SIP operates independently of the underlying network transport protocol and is indifferent to media. Instead, it defines how one or more participant's end devices can create, modify and terminate a connection whether the content is voice, video, data or Web-based. Using SIP, programmers can add new fragments of information to messages without compromising connections.
SMDR	Station Message Detail Recording	Records and prints out the details of incoming and outgoing trunk calls. Such details include the numbers of all parties involved in the call, the time and duration of each call, account codes and other pertinent details.
SPP	Single Point Provisioning	A MiCollab feature that allows an administrator to perform user and service provisioning for a MiVoice Business platform from a single interface, the MiCollab Users and Services application. SPP uses MiMXL to apply updates to the MiVoice Platform. Updates made on the MiVoice Business are not distributed back to the MiCollab.
SRC	Secure Recording Connector	Formerly a standalone call recording product, SRC is now incorporated in the MBG software.
SWAS	Software Assurance	A Mitel subscription-based service that provides customers with access to new software releases, software upgrades, and product support services for all users (ports) on a given Application Record ID (ARID).
Template		A User and Services template defines the user information, phone services, and applications for a type of user. You can use templates to provision users quickly. User and Services templates are comprised of sub-sections that define each service.
TW	Teleworker	Software that connects a remote office to the corporate voice network. Teleworker provides users who are located off-site with full access to the office phone system features including conferencing and voice mail.

TERM	NAME	DESCRIPTION
UCC Licensing	Unified Communications and Collaboration Licensing	Mitel's licensing model. The platform and application user licenses are bundled together to meet the needs of different user levels (for example, Basic, Entry, Standard, and Premium). Instead of ordering an MiVoice Business user license and multiple individual applications licenses for each user, you order a single UCC license per user.
USB	Universal Serial Bus	A connection standard used by computers and other devices like smartphones, flash drives, cameras, and such.
USP	Users and Services	Refers to the interface used to provision users and services on MiCollab.
VA	Virtual Appliance	Defined by VMware as: "a pre-built software solution, comprised of one or more virtual machines that is packaged, maintained, updated, and managed as a unit."
vCenter	vSphere vCenter Server	VMware management server that provides a centralized platform for managing virtual infrastructure.
vCloud Director		A cloud computing initiative from VMware that allows customers to migrate work on demand from their "internal cloud" of cooperating VMware hypervisors to a remote cloud of VMware hypervisors. The goal of the initiative is to provide the power of cloud computing with the flexibility allowed by virtualization.
VM	Virtual Machine	Virtual machines allow the sharing of the underlying physical machine resources between different virtual machines, each running its own operating system. The software layer providing the virtualization is called a hypervisor. A hypervisor can run on bare hardware (Type 1 or native VM) or on top of an operating system (Type 2 or hosted VM).
vSphere	VMware's Cloud Operating System	Cloud computing is Internet-based computing. VMWare's Cloud Operating system provides software resources and information to computers and other devices on-demand over the Internet.
vSphere Standalone		VMware vSphere deployed as a standalone ESX/ESXi host.
vSphere Managed		VMware vSphere deployed as a vCenter Server "managed" environment with ESX/ESXi hosts.

Chapter 2

DESCRIPTION

ABOUT THE MIVOICE BUSINESS EXPRESS VIRTUAL APPLIANCE

The Mitel® MiVoice Business Express provides a complete communications solution for small to mid-range businesses. MiVoice Business Express runs as virtual appliance.

COMPONENTS

The MiVoice Business Express consists of the following components:

- *MiVoice Business*: provides Voice over IP (VoIP) telephony support for Mitel IP phones, SIP trunking, and a wide range of phone features.
- *MiCollab*: provides the Server Manager interface for system administration and the following applications:
  - *Users and Services*: for provisioning users and their services.
  - *NuPoint Unified Messaging*: provides voice messaging and unified messaging
  - *MiCollab Client*: combines the call control capabilities of Mitel communications platforms with contact management, Dynamic Status, and collaboration applications, to simplify and enhance real-time communications
  - *MiCollab Client Deployment*: supports the simplified deployment of MiCollab for Mobile clients.
  - *MiCollab AWV:* allows users to collaborate in real time, give presentations, and conduct interactive online meetings
- *MiVoice Border Gateway*: provides teleworker service and secure recording connector for the remote Teleworker sets only.
- *Initial Configuration Wizard (ICW)*: guides you through the initial configuration of the MiVoice Business Express system.

Figure 1 is a block diagram of the main components:

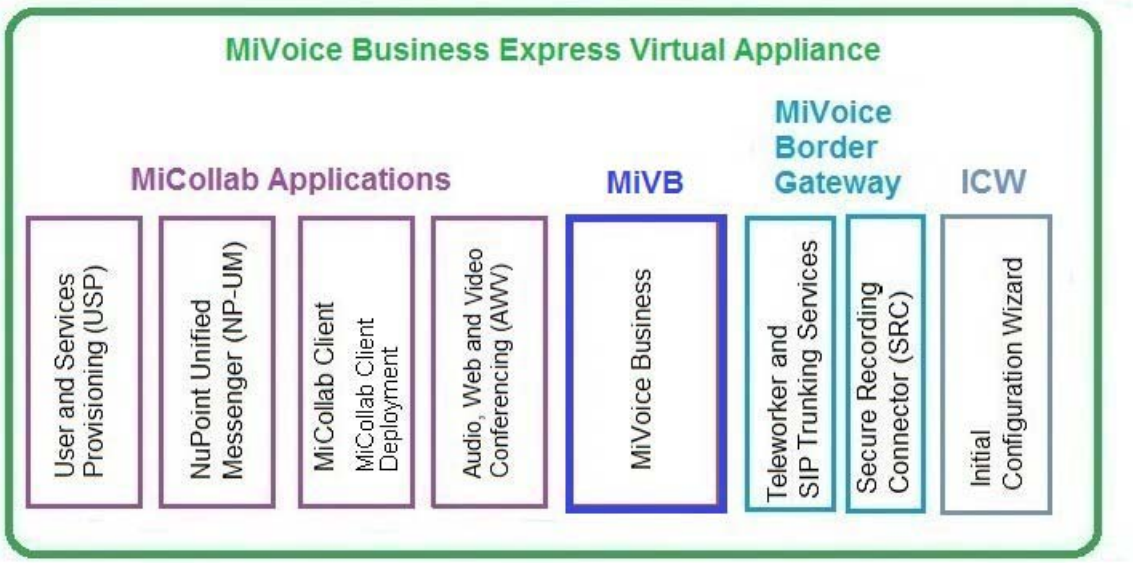

Figure 1: MiVoice Business Express Components

CHARACTERISTICS

MiVoice Business Express has the following characteristics:

- Supports the following user resource capacities. Refer to the MiVoice Business Express Engineering Guidelines for details.
  - 1500 user resource capacity for small business
  - 2500 user resource capacity for mid-market business.
- For installations on VMware all software applications are installed when you deploy the MiVoice Business Express OVA file. For installations on Microsoft Hyper-V, you install the software applications separately.
- Employs an initial configuration wizard and system default settings to simplify installation and minimize initial system configuration.
- Can be deployed in Network Edge (Server-gateway) or LAN only (server-only) mode.
- Provides single point of provisioning to the MiVoice Business and applications from MiCollab.
- Minimizes user provisioning through bulk data import and the application of roles and templates
- Integrates with Active Directory (supports the addition and deletion of users from Active Directory)
- Supported in VMware and Microsoft Hyper-V virtualized environments. See the *Virtual Appliance Deployment Guide* guide for details.
- Supports a subset of VMware vSphere, vCenter, and vCloud Director management tools. See the *Virtual Appliance Deployment Guide* guide for details.
- Supports Flow Through Provisioning: This feature synchronizes updates made to the following data between the User and Services Provisioning database and the MiVoice Business database using System Data Synchronization (SDS):
  - User and services data
  - Programmable Ring Groups (PRGs)
  - Multi-Device User Groups
  - Roles, and
  - Templates
- Supports Reach-Through: This feature allows you to access MiVoice Business System Administration System Administration tool forms from links or drop-down menus within specific User and Services administration pages. Because you have logged into the MiCollab server manager, you are allowed direct access and do not have to log in separately to the MiVoice Business. This functionality reduces the amount of time it takes to perform programming tasks that require configuration on the MiVoice Business, such as modifying a user's MiVoice Business phone and group settings. MiVoice Business systems also support Reach Through to MiCollab. Administrators can link directly to certain MiCollab USP pages from specific MiVoice Business system administration tool forms.

DEPLOYMENT MODELS

This solution is well adapted to the following deployments:

- **Unified Communications as a Service (UCaaS)**: Service Providers host the MiVoice Business Express solution as a software application within a virtualized server infrastructure and offer it to customers as a service.
- **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 Express solution on their virtualized server infrastructure.
- **Customer Premise Deployment**: Mitel certified dealers install and configure MiVoice Business Express in the virtual environment on the customer's premise.

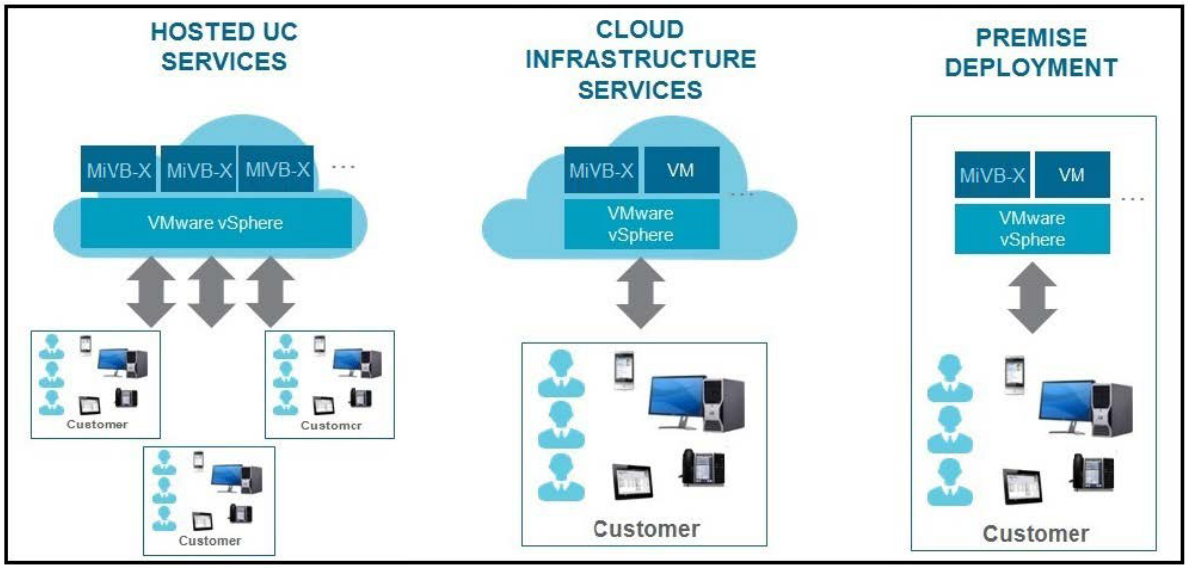

Figure 2: MiVoice Business Express Deployment Models

Depending on the deployment model and site requirements, you deploy MiVoice Business Express in server gateway mode

- by itself with the integrated MBG used to support Teleworker and SIP trunking
- with a standalone vMBG that provides SIP trunk proxy
- with a third-party SBC/gateway for SIP trunk interconnect to the service provider.

Note: To support Secure Recording Connector for phones on the LAN, you must deploy a separate vMBG on the LAN (preferably on the same LAN segment as MiVoice Business Express). The SRC component within MiVoice Business Express can only be used to record calls on remote Teleworker sets.

UCAAS DEPLOYMENT

Figure 3 shows the MiVoice Business Express and VMware components in a typical UCaaS deployment. In this deployment model:

- MiVoice Business Express is deployed as a single virtual appliance that provides MiCollab, MiVoice Business, and MBG functionality. The MBG component of MiVoice Business Express provides the firewall, router, AWV Web Proxy, and Secure Recording Connector of remote Teleworker sets. It also acts as the main hub for the remote Teleworker sets.
- The hosted UCaaS service provider deploys and maintains the MiVoice Business Express solution. If the service provider deploys a management solution with a customer self-serve portal, then the end customer's IT administrator can manage their users directly.
- For UCaaS deployments, the MiVoice Business Express software bundle and user licenses can be licensed on a subscription basis from Mitel or purchased as a capital expense (CAPEX).
- Two distinct network connectivity models are supported from the end customer premise to the hosted UCaaS infrastructure:
  - **MPLS Connected End Customer(s)**: MiVoice Business Express connected to a remote office using an MPLS router.
  - **Public Internet Connected End Customer(s)**: standalone MiVoice Business Express servicing Telworker phones in one or multiple remote offices.
- UCaaS deployments typically use the on-board MBG to provide the SIP trunking proxy. However, a separate external standalone vMGB can be added to provide SIP trunking resources. Adding an external standalone vMBG has the following advantages:
  - consolidates trunking capacity for multiple customers; all trunks come to one location and the incoming calls are routed to the appropriate customer's MiVoice Business Express
  - increased simplicity for bandwidth management
  - cost savings when SIP services are purchased in bulk
  - the ability to configure trunk resiliency for disaster recovery.
- For UcaaS deployments where end customers are connected via a MLPS router, MiCollab mobile clients can be used in the remote office because they route to the Internet via a separate router (not the MPLS router).

Note: Optionally, you can deploy a standalone vMBG to aggregate the SIP trunk proxy functionality among several customers.

Note: This deployment model is available from Mitel as part of the Mitel Authorized Partner Service Provider Addendum. It can be commercially licensed under Subscription or CAPEX pricing from Mitel.

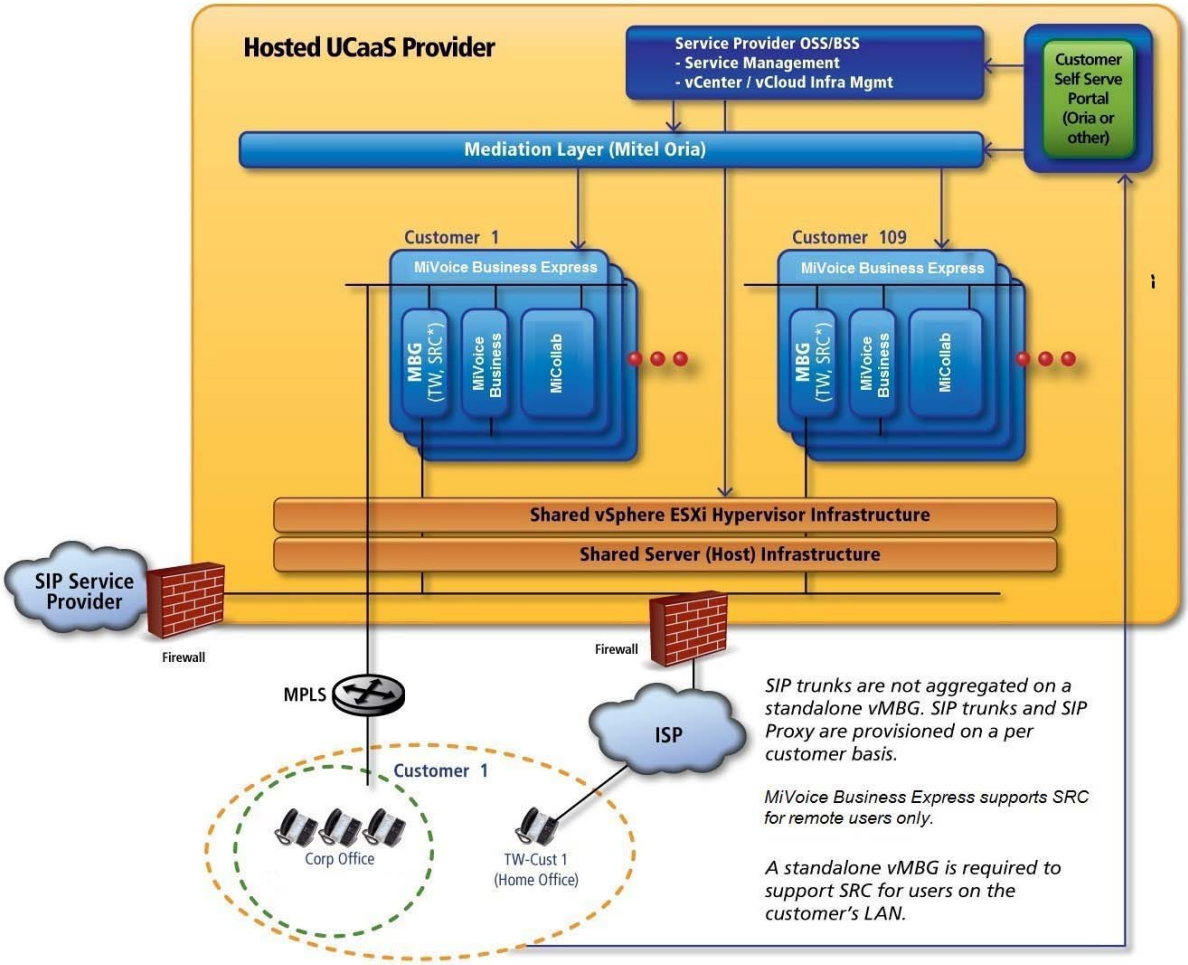

Figure 3: UCaaS Infrastructure: MPLS Connected End Customer(s)

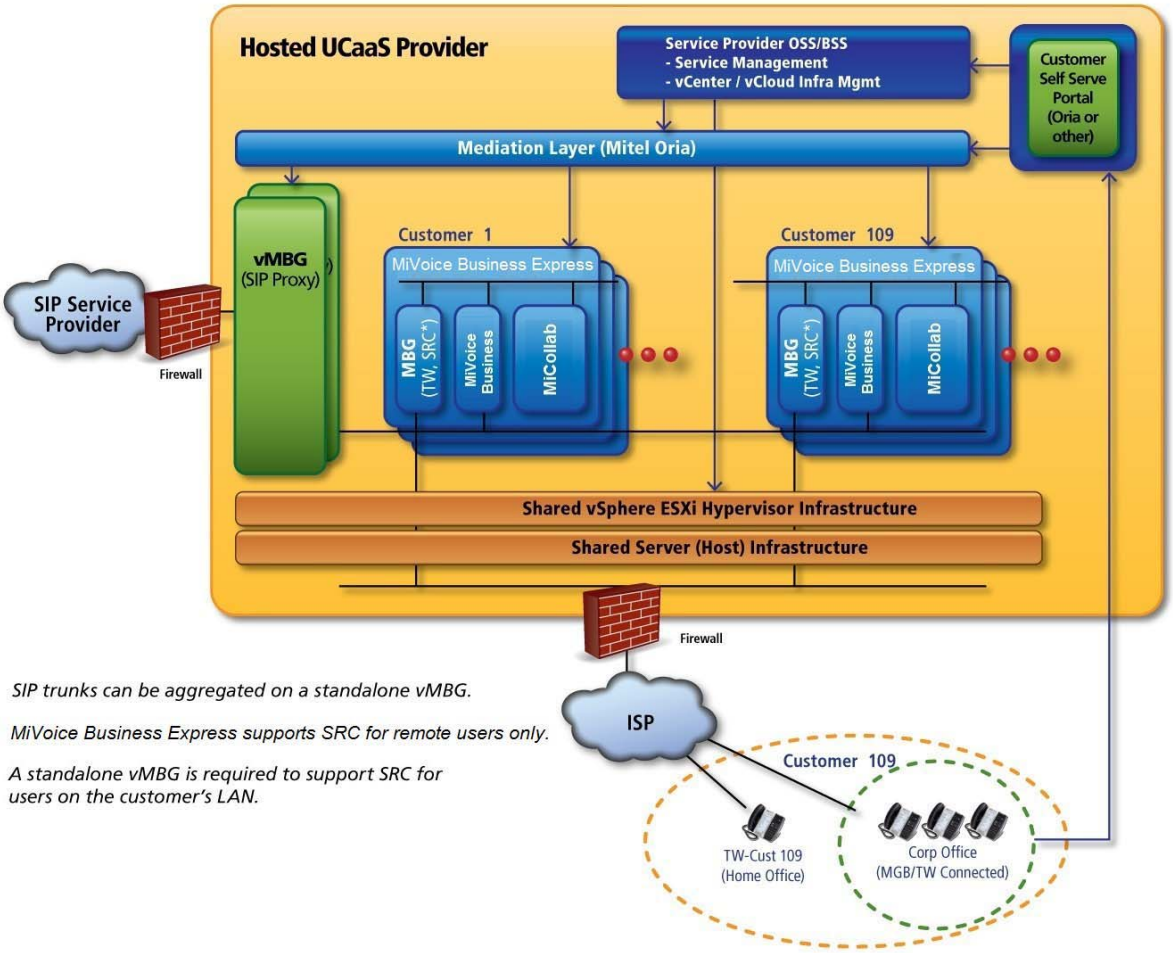

Figure 4: UCaaS Infrastructure: Public Internet Connected End Customer(s)

IAAS DEPLOYMENT

Figure 5 shows the MiVoice Business Express and VMware components in a typical IaaS deployment. In this deployment model:

- MiVoice Business Express is deployed as a single virtual appliance that provides MiVoice Business, MiCollab, and MBG functionality. The MBG component of each MiVoice Business Express 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 Express solution. The channel partner may, or may not, have access to the hosted infrastructure.
- Two distinct network connectivity models are supported from the end-customer premise to the hosted UCaaS infrastructure:
  - **MPLS Connected End Customer(s)**: MiVoice Business Express connected to a remote office using an MPLS router.
  - **Public Internet Connected End Customer(s)**: standalone MiVoice Business Express servicing Telworker phones in one or multiple remote offices.
- For IaaS deployments where end customers are connected via a MLPS router, MiCollab mobile clients can be used in the remote office because they route to the Internet via a separate router (not the MPLS router).

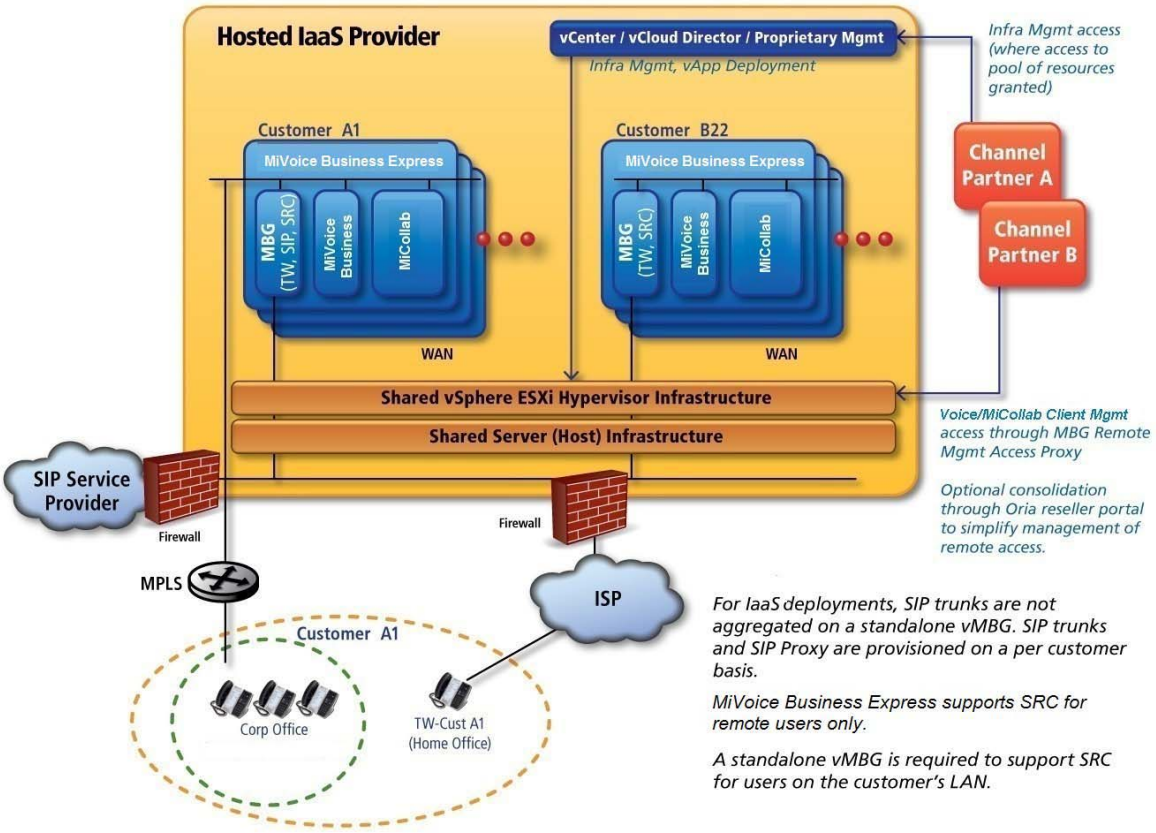

Figure 5: Example IaaS MPLS Connected End Customers

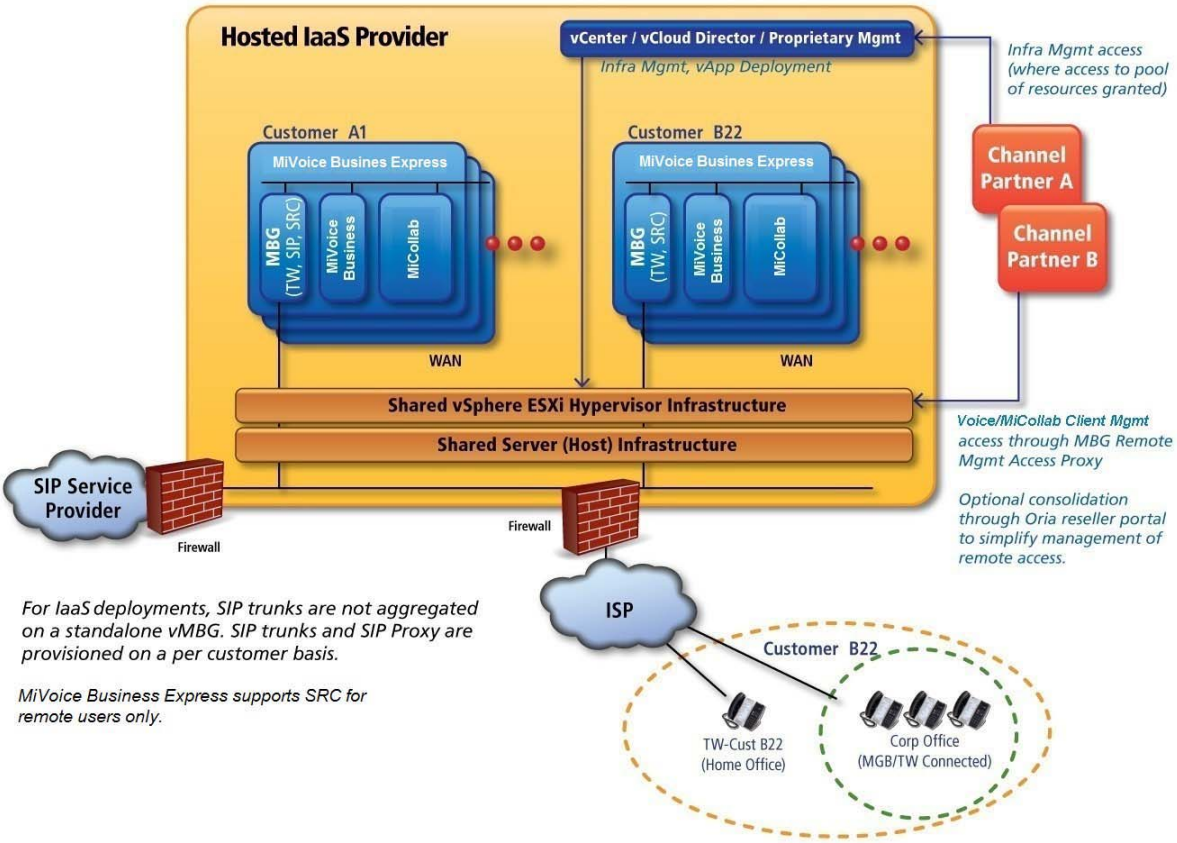

Figure 6: IaaS Infrastructure: Public Internet Connected End Customer(s)

CPE DEPLOYMENT

Figure 7 shows the MiVoice Business Express and VMware components in a typical Customer Premise Equipment (CPE) deployment. In this deployment model:

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

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

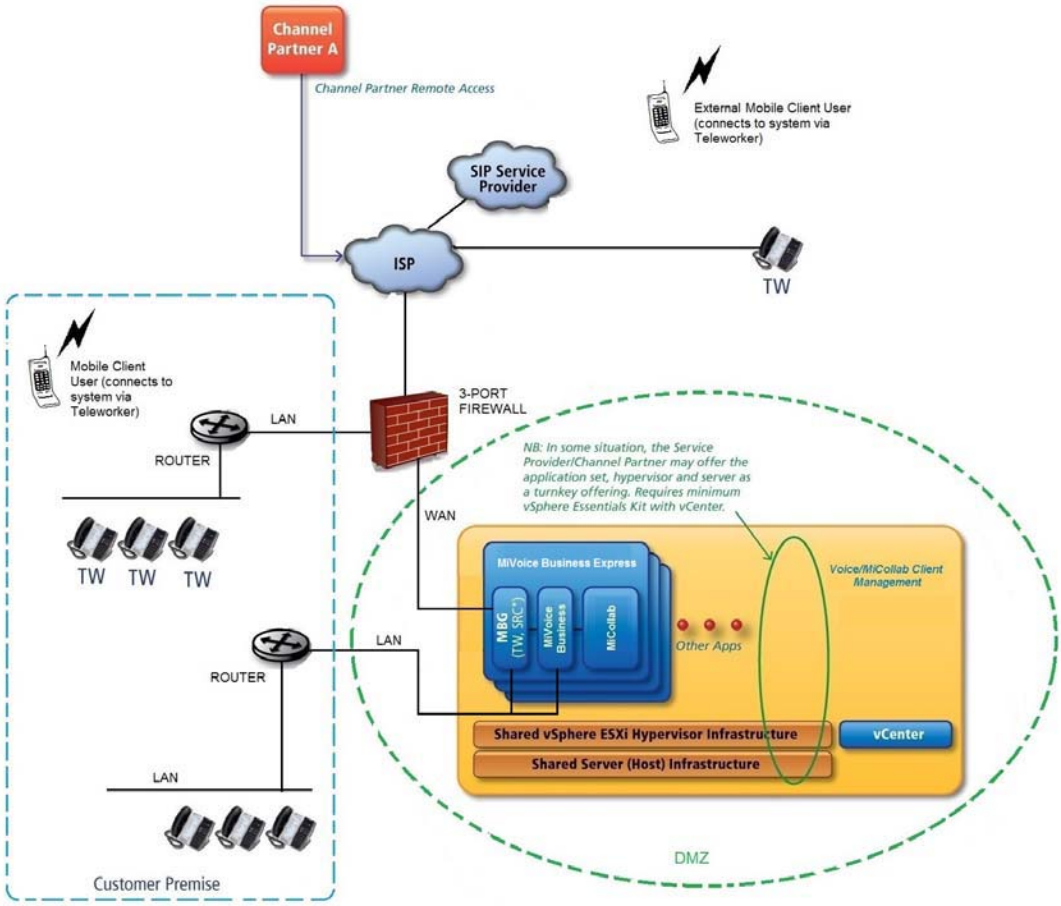

Figure 7: Customer Premise Equipment Deployment

SUPPORTED FUNCTIONALITY

OVERVIEW

MiVoice Business Express 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
- NuPoint Unified Messenger voicemail application
  - Voicemail
  - Standard UM and Advanced UM
  - Auto Attendant, Inbound and Outbound FAX, Record-A-Call, Call Director, Miscellaneous Options (NP Page, Forms, On Demand, and Rapid Dial)
- MiCollab Client
  - Desktop client with optional softphone
  - MiCollab Client for Mobile deployment
  - Web and mobile client support for audio, video, and instant messaging collaboration
  - Collaboration features
  - ACD agent
  - Console
- MiCollab AWV
  - Audio, web and video collaboration
  - Desktop/application collaboration
- MiVoice Border Gateway, providing
  - Teleworker Service
  - Secure Recording Connector (for remote Teleworkers only)
  - SIP Trunking Proxy

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

- Vidyo
- Initial Configuration Wizard

Note: Speech applications are not supported (MiVoice Business embedded voicemail, Speech Auto Attendant, Text to Speech, Speech to Text, Speech Navigation, or Network Voicemail).

APPLICATIONS SUITE MANAGEMENT

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.

The MiCollab End User portal is a web-based interface that gives end users a single point of access to all their applications. The portal allows users to

- set personal settings, such as passwords and phone numbers
- configure and maintain their communication application settings.

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, multimedia collaboration, and unified messaging. It provides seamless IP networking and SIP trunking.

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

NUPOINT UNIFIED MESSENGER

NuPoint Unified Messaging is a powerful, voice processing application that provides voice messaging and paging support. Users can access their voice mails remotely and can be notified by telephone or pager when a voice message is left for them. Users can also use NuPoint's Unified Messaging capabilities to listen to their voice mail messages through their Lotus Notes, Novell GroupWise, or Microsoft Outlook clients with Message Waiting Indicator (MWI) on playback via a URL. In addition, they can play their emails through the Telephony User Interface. Messages between these clients and the NuPoint TUI are synchronized for message playback. NuPoint Unified Messaging also offers desktop access to voice messages from an email client or web browser.

Features include:

- Multiple language support
- Integration to MiVoice Business communications platform
- Automated attendant
- Unified Messaging

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.

MICOLLAB TEAM (MITEAM)

MiTeam is a cloud-based mobile first collaboration tool that allows teams to work together in real time no matter where they are. It is integrated into the iOS and Android native mobile clients and launched from the MiCollab Client for Mobile left tab.

MiTeam includes the following user features:

- Create collaboration channels (streams)
- Hold chat sessions with associated annotation features, pages, to-do lists
- Participate in real-time meetings hosted through AWV technology
- Invite participants to streams as guests.

MICOLLAB CLIENT DEPLOYMENT

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

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

Refer to the *MiCollab Client Deployment* help.

MICOLLAB AWV

The MiCollab AWV application allows users to schedule and create audio or web conferences. A web-based interface is used to schedule conferences, and to view conference calls. Configuration is performed in the MiCollab administrator portal. All interfaces are directly accessed through the secure HTTPS protocol. Authorization and authentication allows only valid users to access the services. Secure Sockets Layer (SSL) encryption for secured messages and server-side digital certificates are used to meet the highest security requirements.

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 and MiCollab AWV 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.

VIDYO

Vidyo is a video conferencing solution that provides users with high definition, low-latency video to mobile phones, desktops, and meeting rooms. Refer to the Vidyo Product Documentation and the Mitel Vidyo Quick Reference Administrator Guide for details.

INITIAL CONFIGURATION WIZARD

The MiVoice Business Express Initial Configuration Wizard guides you through the initial system set up. It allows you to configure the system with the basic settings required to get the system up and running. It guides you through the following configuration steps:

- Select configuration options (restore from backup or create new database)
- Review initial configuration parameters
- Configure administration email and servers
- Configure languages
- Configure numbering plan
- Configure incoming call configuration
- Configure SIP provider
- Configure SIP trunk proxy
- Configure optional services: Hot Desking, AWV, Music on Hold, and Remote Access
- Change the administrator password for both the MiCollab Server Manager and the MiVoice Business system administration tool.

You only run this wizard once during the initial configuration of the system. After you deploy or install the MiVoice Business Express software in the virtualization environment, you run this wizard in an internet browser and enter the site specific settings in the screens. The wizard then configures the system with your settings.

After you run the wizard, you must

- Configure advanced features through the application programming interfaces
- Provision users through the Users and Services application.

Note: Do not confuse the MiVoice Business Express Initial Configuration Wizard (ICW) with the Mitel Integrated Configuration (MiCW) that configures standalone MiCollab and MiVoice Business systems. They are separate tools.

Chapter 3

PLAN CUSTOMER SITE

PLANNING OVERVIEW

To prepare for MiVoice Business Express deployment, complete the following:

- ☐ Collect service provider and customer details
- ☐ Collect customer site requirements
- ☐ Record licensing requirements
- ☐ Review engineering guidelines
- ☐ Collect site configuration data
- ☐ Review installation and provisioning workflow

COLLECT SERVICE PROVIDER AND CUSTOMER DETAILS

Table 2: Collect Service Provider and Customer Details

STEP	DETAILS
1. List site information	
Company Name	
Address	
State/Province/Country	
ZIP/Postal Code	
Time zone	
2. List contact information	
Contact Name	
Telephone Number	
Cell Phone	
Email Address	
3. List Authorized Partner Information	
VAR/Partner Name	
Address	
City	
State/Province	
Country	
Time Zone	
4. Complete pre-installation VoIP Site Survey	

Table 2: Collect Service Provider and Customer Details

STEP	DETAILS
5. Complete data network assessment	
6. Obtain customer site floor plan	
Site plan should identify	Site locations Trunk Requirements Numbering Plans Building Layout Existing PBXs Existing cable runs Equipment rooms LAN information
7. Obtain information on site power distribution, backup power, and the physical distribution	
8. Obtain IP addresses for MiVoice Business Express and IP Phones	
9. Obtain and review Layer 2 switch settings with customer.	

COLLECT CUSTOMER SITE REQUIREMENTS

Table 3: Identify Deployment Configuration Requirements

STEP	DETAILS	
1. Identify Deployment Model	Unified Communications as a Service (UCaaS)	❑
	Infrastructure as a Service (IaaS)	❑
	Customer Premise Equipment	❑
2. Identify Deployment Configuration	Network Edge (Server Gateway) mode	❑
	LAN Mode (Server-only)	❑
3. Identify Connectivity Model	MiVoice Business Express hosting remote office via MPLS router	❑
	MiVoice Business Express hosting remote office Teleworker sets (internet connected)	❑

Table 3: Identify Deployment Configuration Requirements

STEP	DETAILS	
3. Identify Firewall Configuration Requirements (refer to MiVoice Border Gateway Engineering Guidelines at http://edocs.mitel.com for details)	Checkpoint "Network Gateway" Firewall	❑
	Port forwarding Firewall	❑
	SIP-Aware Firewall	❑
	UDP Flood Protection	❑
	Remote Site Firewall	❑
	Firewall Configuration for SIP Trunking	❑
	Firewall for Remote SIP Devices	❑
4. System User Capacity	**Small Business**	
	1500 user resource capacity. Refer to MiVoice Business Engineering Guidelines.	❑
	Mid-Market	
	2500 user resource capacity. Refer to MiVoice Business Engineering Guidelines.	❑
5. Optional vMBGs Required?	Do you require SIP trunk aggregation for multiple MiVB-X deployments?	❑
	Do you require Secure Recording Connector for phones on the LAN?	❑

Table 4: Identify Telephony Requirements

STEP	DETAILS	NUMBER REQUIRED
1. Record Number	IP Phone users	
	SIP Phone users	
	Hot Desk Users	
	External Hot Desk Users	
	Teleworkers	
	ACD Agents (Hot Desk)	
	SIP Trunks	
2. Identify DID/DDI Requirements?	Direct Inward Dial (DID)/Direct Dialing Inwards (DDI) required on SIP trunks?	❑

Table 5: Identify Device Requirements

DEVICE TYPE	NAME	NUMBER REQUIRED
Phones	5005 IP	
	5010 IP	
	5020 IP	
	5140 IP	
	5205 IP	
	5207 IP	
	5212 dual mode	
	5215 dual mode	
	5215 IP	
	5220 dual mode	
	5220 IP	
	5224 dual mode	
	5230 IP	
	5235 IP	
	5240 IP	
	5302 IP	
	5304 IP	
	5312 IP	
	5320 IP	
	5320e IP	
	5324 IP	
	5330 IP	
	5330e IP	
	5340e IP	
	5360 IP	
	5560 IP	
	6920 IP	
	6930 IP	
	6940 IP	
Wireless DECT	56xx DECT Wireless Phones	
Conference Units	UC 360	
Softphones	MiCollab Client Softphones	
Generic SIP Phones (hard/softphone)	5304 SIP phone	
	5330e SIP Phone	

Table 5: Identify Device Requirements

DEVICE TYPE	NAME	NUMBER REQUIRED
	5340e SIP Phone	
	5360 SIP Phone	
	5603 SIP	
	5604 SIP	
	5607 SIP	
	5610 SIP	
	5624 SIP	
	MiCollab Client SIP Softphones	
	Other (specify)	

Table 6: Identifying User Types (UCC Version 4)

UCC USER LICENSE	FUNCTIONALITY	NUMBER REQUIRED
Basic IPT	See the table under "Record Licensing Requirements for a definition of the licenses	
Standard IPT (Note that this license is only offered for Service Provider market).		
Entry		
Standard		
Premium		

Table 7: Identifying Database Management Requirements

REQUIREMENT	DETAILS	
Integrated Directory Service Synchronization with Active Directory Database	❑ Yes ❑ No If Yes, field attribute mapping: ❑ Default, or ❑ Custom?	Refer to Manage IDS Attribute Mappings in the USP application online help for details.
User Provisioning Method (See "Perform Advanced Configuration" on page 98 for information)	Sync Active Directory database with MiVoice Business Express	❑
	Import user data from CSV file	❑

Table 7: Identifying Database Management Requirements

<table>
<tr><th>REQUIREMENT</th><th colspan="2">DETAILS</th></tr>
<tr><td rowspan="9">USP Roles and Templates
(See “Perform Advanced Configuration” on page 98 for information)</td><td colspan="2">❑ Use Default roles and templates?
❑ Create roles and templates?</td></tr>
<tr><td>Role Name:</td><td>Associated Template Name</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td>:</td><td></td></tr>
<tr><td rowspan="2">MiCollab Client Deployment (Refer to the online help associated with this application for instructions)</td><td>MiVoice Business Express is deployed on the network edge using the on-board MBG</td><td>❑ MiCollab Server with MBG on the Network Edge (Server Gateway Mode)</td></tr>
<tr><td>Purchase a Third-Party SSL Certificate and install it on the MiVB-X server. See Add Web Server Certificate in the MiCollab server manager help for more information.</td><td>❑ Third-Party SSL Certificate</td></tr>
<tr><td colspan="3"></td></tr>
</table>

RECORD LICENSING REQUIREMENTS

ABOUT LICENSING

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

Unified Communications and Collaboration (UCC) licensing simplifies the selling and ordering process because it bundles the platform and application user licenses together. Instead of ordering a MiCollab license, MiVoice Business user license, and multiple individual applications licenses for each user, you just order a single UCC license per user. Although you can order licenses individually (à la carte) we recommend that you use UCC licensing because it offers the following benefits:

- Simplifies the licensing of a MiVoice Business Express user by bundling the required MiCollab 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 Basic IPT**: provides the Basic MiCollab Client.
  - **UCC Standard IPT**: provides the Basic MiCollab Client plus voicemail.
  - **UCC Entry**: provides the Entry MiCollab Client, voicemail, unified messaging, and the required call manager platform licenses.
  - **UCC Standard**: adds the UCC desk with Softphone, Mobile with softphone (one of the softphones and teleworker access can be provisioned per user) and web client and full audio and web collaboration, as well as additional device support depending on call manager to the Entry license.
  - **UCC Premium**: adds full mobile and softphone UCC functionality with two additional teleworker accesses to the Standard license.
- Software assurance: The Mitel Software Assurance (SWAS) Program is a subscription-based service that provides customers with access to new software releases, software upgrades, and product support services for all users (ports) on a given application record. Under the SWAS program, software upgrades are provided at no additional cost without any of the new features or functionality that are available in the base upgrade package.

LICENSING RULES

The following rules apply to UCC Licensing:

- UCC v4.0 licensing is supported with MiVoice Business Express Release 7.0 and later.
- You require a UCC License Manager (ULM) to create a UCC Group ARID on the AMC.
- You cannot split the UCC license bundle and deploy the application licenses across different users within a system.
- If you downgrade the UCC license bundle of an existing user (for example, from Entry to Basic, from Standard to Entry, or from Premium to Standard) MiCollab will not delete any

of the services. Instead, MiCollab attempts to apply any available "à la carte" licenses to support the extra services. If "à la carte" licenses are not available, then a license violation is generated.

- If you have different types of upgrade licenses (for example, "Basic to Entry", "Entry to Standard", and "Standard to Premium") available on the system, apply the highest upgrade licenses first. For example, upgrade the Standard users to Premium licenses first, before you upgrade the Entry users to Standard licenses.
- If new UCC licensing bundles are available, the AMC automatically converts the existing bundles to the latest version and passes the new bundles down to the server. The new bundles replace the existing bundles on the system. For example in Release 7.0, UCC V4.0 license bundles replaced UCC V3.0 license bundles. 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 Express 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 or Premium 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. Both phones ring simultaneously for an incoming call.
  - In addition to the teleworker license provided in the Standard or Premium UCC User license, each user requires a second teleworker license.Two teleworker user licenses are required to allow both of the user's phones to be registered with teleworker service (so that they both ring simultaneously on an incoming call).

Additionally, for UCaaS deployments:

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

LICENSING DETECTION AND VIOLATION MODE

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

Mitel recognizes that in some deployment situations, it is not practical to implement online connectivity to the AMC from each virtual appliance deployed at a customer's site. For this reason, Mitel supports the ability to proxy online AMC connectivity from each virtual appliance

through a single named proxy within the customer data center environment. This enables AMC online connections to be managed and controlled from one central point within the data center rather than from each individual product.

NUPOINT VOICEMAIL PORT ALLOCATION

NuPoint ports are licensed on the MiVoice Business Express system based on the number of UCC user licenses purchased. However the Initial Configuration Wizard (ICW) configures fewer than the actual number of licensed NuPoint ports. The ICW does not configure all the ports in order to reserve some ports for Recording Announce Devices (RADs). You can manually configure these reserved ports up to the specified engineering limits.

Note: A basic user is created for each MiCollab AWV port and these users are taken into consideration in the NuPoint voice port allocation algorithm.

Table 34 identifies the number of ports that are configured by the ICW based on the number of licensed users and ports.

Table 8: NuPoint VoiceMail Port Allocation

LICENSED USERS	LICENSED PORTS	PORTS CONFIGURED BY ICW	PORTS RESERVED FOR RADS
0	6	6	0
20	7	6	1
40	8	7	1
60	9	8	1
80	10	8	2
100	11	9	2
120	12	10	2
140	13	10	3
160	14	11	3
180	15	11	4
200	16	12	4
220	17	12	5
240	18	13	5
260	19	13	6
280	20	14	6
300	21	14	7
320	22	15	7
340	23	15	8
360	24	16	8
380	25	16	9

Table 8: NuPoint VoiceMail Port Allocation

LICENSED USERS	LICENSED PORTS	PORTS CONFIGURED BY ICW	PORTS RESERVED FOR RADS
400	26	17	9
420	27	17	10
440	28	18	10
460	29	18	11
480	30	19	11
500	31	19	12

LICENSING CONDITIONS FOR MICOLLAB AWV

The following UCC Licensing conditions apply to the MiCollab AWV application:

- MiCollab AWV is licensed by port. Each port enables one simultaneous audio and web connection in the system. For example, a 10-party conference would require 10 ports.
- The system includes nine ports plus an additional port for every 10 Standard UCC User licenses. If the system has no Standard or Premium UCC User licenses, then no ports are included with the system. Typical configurations use one audio port for every 10 MiCollab AWV users.
- The AMC uses a set of pre-defined rules to deliver audio and web collaboration entitlement. The number of ports is based on the number of UCC Standard or Premium licenses that are assigned to users.

  The following licenses are provisioned for every 10 Standard UCC Users:

  1 x Communications Platform Connection User

  1 x MiCollab AWV Web Port, 1 x Audio Port, 1 x HDCodec Port

  The following licenses are provisioned for every 5 Premium UCC Users:

  1 x Communications Platform Connection User

  1 x MiCollab AWV Web Port, 1 x Audio Port, 1 x HDCodec Port

  For example: 11 UCC Standard licenses earns 11 audio and web collaboration ports at no additional charge
- A total of 21 UCC Standard licenses earns 12 audio and web collaboration ports at no additional charge.
- A conferencing port is comprised of 1 audio port, 1 web port, and 1 H.264 video port.
- If required, you can purchase additional ports separately to achieve the customer's required quantity, depending on the end-customers particular business requirements for simultaneous audio conferencing.

- UCC Standard and Premium licenses include collaboration licenses. UCC Basic and Entry licenses do not include collaboration licenses, so they do not include any MiCollab AWV ports.

Note: System capacities are identified in the MiVoice Business Express Engineering Guidelines. Licensing rules may grant you more port licenses than are allowed to be configured from an engineering standpoint. Adhere to the engineering rules.

RECORD LICENSING REQUIREMENTS

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

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

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

LICENSES	PART NUMBER	NUMBER REQUIRED
MiVoice Business Express Software Base Packages for traditional customer premise or IaaS licensing		
MiVoiceBusExpress Standalone Virt (see **Note 3**) (without user licenses or SIP trunk licenses) Contains the following base system packages • Virtual MiVoice Business - with Standard User licensing • Virtual MiCollab – with access to all advanced Unified Communications features and functions • Virtual MBG – Mitel's Border Gateway for secure Voice and MiCollab Client interaction with Service Providers and the Internet	54005919	
MiVoiceBusExpress Standalone Bundle Virt (see **Note 3**) Contains the following base system packages: • Virtual MiVoice Business - with Standard User licensing • Virtual MiCollab – with access to all advanced Unified Communications features and functions • Virtual MBG – Mitel's Border Gateway for secure Voice and MiCollab Client interaction with Service Providers and the Internet Includes: • 16 x UCC Entry User License for Business • 4 x MiVoice Business SIP Trunk licenses • 4 x MBG SIP Trunk Proxy licenses	54005892	
MiVoice Business Express Bundle Virtual (see **Note 4**)	54006089	
MiVoice Business Express Virtual (see **Note 4**)	54006091	
MiVoice Business Express Software for UCaaS and CAPEX Deployments		
SP Subscript Base-MiVoiceBus Express Virt includes the following licenses: • 275 x MiVoice Business SIP Trunk licenses • 5 x G.729 (8-pack) licenses	54005931	
SP CAPEX Base - MiVoiceBus Express Virt (CAPEX licensing is used with UCaaS deployment models where user licenses are purchased as a capital expense and not on a subscription basis) includes the following licenses: • 275 x MiVoice Business SIP trunk licenses • 5 x G.729 (8-pack) licenses • MBG SP client license (MBG SIP Proxy client license is not included.)	54005920	

LICENSES	PART NUMBER	NUMBER REQUIRED
User		
UCCv4.0 Entry User x1	54006539	
UCCv4.0 Standard User x1	54006542	
UCCV4.0 Premium User x1	54006545	
UCCv4.0 Entry User x100	54006541	
UCCv4.0 Standard User x100	54006544	
UCCv4.0 Premium User x100	54006547	
User Licenses - Service Provider Subscription Fulfilment		
SP Subscript Licnse-UCC Entry Users x50	54006122	
SP Subscript Licnse-UCC Stnd Users x50	54006117	
SP Subscript Licnse-UCC Prem Users x50	54006118	
SP Subscript Licnse-UCC Std IPT Userx1	54006610	
SP Subscript Licnse-UCC Std IPT Userx50	54006611	
User Licenses - Service Provider CAPEX		
SP Capex Licnse - UCC Entry User x1	54006119	
SP Capex Licnse - UCC Stnd User x1	54006120	
SP Capex Licnse - UCC PremUser x1	54006121	
SP Capex License-UCC Standard IPT Userx1	54006615	
SP Capex Licnse -Standard IPT User X1000	52002993	
SP Capex Licnse -Standard IPT User X2500	52002994	
SP Capex Licnse - Std IPT SB User X1000	52002995	
SP Capex Licnse - Std IPT SB User X2500	52002996	
Uplift		
UCCv4.0 Basic to v4.0 Entry	54006553	
UCCv4.0 Entry to v4.0 Standard	54006548	
UCCv4.0 Basic to v4.0 Standard	54006704	
UCCv4.0 Basic to v4.0 Premium	54006705	
UCCv4.0 Standard to v4.0 Premium	54006549	
Software Assurance Support (SWAS)		
Standard SWAS UCC(V4.0) Entry	54006135	
Standard SWAS UCC(V4.0) Standard	54006136	
Standard SWAS UCC(V4.0) Premium	54006137	
Premium SWAS UCC(V4.0) Entry	54006138	
Premium SWAS UCC(V4.0) Standard	54006139	
Premium SWAS UCC(V4.0) Premium	54006140	

LICENSES	PART NUMBER	NUMBER REQUIRED
Standard SWAS:UCC Virtual Appliance Base	54005936	
Premium SWAS:UCC Virtual Appliance Base	54005937	
Standard SWAS:UCC Virtual Appliance Base for SP CAPEX	54005938	
Premium SWAS:UCC Virtual Appliance Base for SP CAPEX	54005939	

Notes:

1.Premium SWAS must be applied as an upgrade to Standard SWAS.

2.MiVoice Business Express also supports "à la carte" licensing.

3.The system does not restrict you from applying an ARID with a MiVoiceBusExpress Standalone Virt (PN 54005919) or a MiVoiceBusExpress Standalone Bundle Virt (54005892) to a system that has been deployed as a mid-market business configuration. However, these parts numbers are for small business configurations and only support the small business user capacity.

4.The system does not restrict you from applying an ARID with a MiVoice Business Express Bundle Virtual (PN 54006089) or a MiVoice Business Express Virtual (PN54006091) 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.

REVIEW ENGINEERING GUIDELINES

Review the MiVoice Business Express site requirements detailed in the *MiVoice Business Express Engineering Guidelines*. Also review the *Virtual Appliance Deployment Guide*. It provides guidelines for deploying Mitel Virtual Appliances and applications in a virtual infrastructure.

COLLECT SITE CONFIGURATION DATA

Before you begin deployment, collect and record the data specified in Table 9. You will need this information in order to successfully deploy MiVoice Business Express and perform initial configuration using the wizard.

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 Express.

Table 9: Collect Custom OVA Template Information

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".
Localization		
Time zone setting	Identify the MSL operating system time zone setting. The default is America/New York. The Time zone setting also determines your system telecom regional settings.	**Note**: If you select a Time zone that is not within one of Countries supported by the system, the Country value is set to "Other" and the Telecom Region is defaulted to North America.
Keyboard Type	Identify the preferred keyboard type (default is **us**)	
Application		
Initial Administrator Password	Record the initial administrator password for the MiCollab server manager interface. This password must be at least six characters long. After you access the MiCollab server manager, you will be prompted to change this initial password. **Note**: You must enter a password before you deploy the MiVoice Business Express; otherwise, the system will not boot up.	Initial MiCollab Server manager Administrator Password: _____ Final MiCollab server manager Administrator Password: _____ **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 Express.	

Table 9: Collect Custom OVA Template Information

CONFIGURATION ITEMS	FIELD DESCRIPTION	SITE CONFIGURATION DATA
Domain Name (Optional)	Specify the domain name for the hostname above. The default domain name is "mycompany.local".	
License Key (Optional) (MiVoice Business Express Business Base ARID)	Identify the License Key (MiVoice Business Express Business Base ARID) for this system. The ARID is used by the AMC to distribute the system licenses. See “Create ARIDs and Assign Licenses in AMC” on page 56 for instructions.	
DNS Server IP (Optional)	Record the DNS Server IP Address	
Remote Network Addresses for MiCollab Server administration (Optional)	List the Network IP address that is allowed to access the MiCollab server and perform remote administration. **Note**: You can only configure one IP address or subnet as the Remote Network Address during OVA deployment. Any additional Remote Network addresses must be configured from the Remote Access panel in the server manager.	_____ _____ _____ _____
Remote Network Netmask (Optional)	Enter the Netmask associated with the remote network address.	
Network Settings		
LAN IP Address (IP Address of the MiVoice Business Express) **Note**: Identified as LAN IP Address # 1 in Initial Configuration page of Initial Configuration Wizard.	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 also can set this IP address from vSphere Client. Right-click on the MiVoice Business Express and click **Edit Settings**. Click the **Options** tab, click **Properties** and enter the LAN IP Address.	---------- **Note**: You must enter a LAN IP address before you deploy the MiVoice Business Express; otherwise, the system will not boot up.
LAN Netmask	Record the Netmask of the LAN	

Table 9: Collect Custom OVA Template Information

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 vSphere Client. Right click on the MiVoice Business Express 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.	
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	
Default Gateway IP Address	Record the Gateway IP address. For Server-gateway deployments this gateway typically points to an Internet router. For Server-only deployments, this gateway typically points to an Internet router.	**Note**: You must enter a Default Gateway IP address before you deploy the MiVoice Business Express; otherwise, the system will not boot up.

Table 10: Collect Advanced Deployment Properties

CONFIGURATION ITEMS	FIELD DESCRIPTION	SITE CONFIGURATION DATA
Mitel Application Management Center (AMC)	Record IP address or proxy address for the AMC	
MiVoice Business IP address **Note**: Identified as LAN IP Address # 2 in Initial Configuration page of the ICW	With vCenter deployments, this address defaults to the MiVoice Business Express LAN IP address +1. If you want to override the default MiVoice Business IP address that is applied during initial configuration, record the desired IP address.	

Table 11: Collect MiVoice Business Express Initial Provisioning Wizard 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 Express database file.	
Initial Configuration		
Time Zone	Same as Custom Template settings. This page allows you to change these settings if necessary.	
Country		
Telecom Region		
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).	
Languages		
System Language	Identify the MiCollab default language. The selected language is applied to the MiCollab End User portals and the Telephone User Interfaces (TUIs) for the MiCollab application end-users.	
Voice Mail Language	Identify the other languages for the NuPoint UM prompts. When users call into the NuPoint UM system through the voice mail auto attendant, they are asked to select the language of the NuPoint UM prompts for the duration of their call. Users can select either the primary prompt language or one of the other languages. The primary (first) language is determined by the System Language setting above; the other languages are determined by the settings in these fields. For example, the primary system language could be English (United Kingdom); the second language; French (Canada), the third language Swedish (Sweden), and so on.	_____ _____ _____ _____ _____

Table 11: Collect MiVoice Business Express Initial Provisioning Wizard Data

CONFIGURATION ITEMS	FIELD DESCRIPTION	SITE CONFIGURATION DATA
Select the languages that users can have on their phone displays. Select a primary (default), auxiliary 1, and auxiliary 2 language.	Primary Phone Display Language	The following languages are supported: Dutch, English, French, German, Italian, Portuguese (Brazil), Portuguese (Portugal), Spanish (Europe), Spanish (Latin America), Polish, Romanian, Russian, Simplified Chinese, or Swedish.
	Auxiliary 1 Phone Display Language	
	Auxiliary 2 Phone Display Language	
Numbering Plan		
Extension Length	Specify the required extension length (3 to 5 digit extension numbering)	
Voice Mail Hunt Group Ext	Default is 7000	
Voice Mail Starting Port Ext	Default is 7001 (up to 7007)	
Voice Mail HCI Hunt Group Extension	Default is 7400	
Voice Mail Record A Call Hunt Group Extension	Default is 7500	
MiCollab AWV Hunt Group Extension	Default is 7850	
MiCollab AWV Starting Point Extension	Default is 7851 (up to 7854)	
Incoming Calls		
Main Business Number	Enter the phone number of the site. External callers dial this number to place incoming calls on the SIP trunks.	
OR		
Incoming Call Handling Extension	Specify the answerpoint extension number.	
Auto Receptionist Hunt Group Extension	Specify the extension number.	
Advanced Incoming Call Configuration		
Number of Digits to Absorb		
Digits to Insert		

Table 11: Collect MiVoice Business Express Initial Provisioning Wizard Data

CONFIGURATION ITEMS	FIELD DESCRIPTION	SITE CONFIGURATION DATA
SIP Provider		
SIP Provider	Identify your SIP Service Provider. **Note**: The wizard lists the most common Service Providers for your region for selection. A "Generic" SIP peer profile is also available. If required, you can specify a "Custom Profile" and import a CSV file saved from the SIP Peer Profile form in the MiVoice Business System Administration Tool (see “Obtain a Custom SIP Peer Profile (optional)” on page 54 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. The ICW provisions the number of trunks licensed in the ARID up to the maximum capacity. See the Engineering Guidelines for capacities. **Note:** You need to configure the MiVoice Business Express ULM with at least two MiVoice Business SIP Trunk Licenses in order to successfully complete the Initial Configuration Wizard.	
Number of MBG SIP Trunk Channel Licenses	Record the number of licenses required. **Note:** If using internal SIP trunking, you need to configure the MiVoice Business Express ULM with at least two MBG SIP Trunk Channel licenses in order to successfully complete the Initial Configuration Wizard.	
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		

Table 11: Collect MiVoice Business Express Initial Provisioning Wizard Data

CONFIGURATION ITEMS	FIELD DESCRIPTION	SITE CONFIGURATION DATA
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		
MiVoice Border Gateway SIP Trunk Proxy	Select **Internal** if the SIP trunk proxy is supported on the MiVoice Business Express system. Select **External** if the SIP trunk proxy is supported on a separate optional MiVoice Border Gateway (MBG). Refer to the *MiVoice Business Express 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 ❒ MiCollab AWV ❒ Music on Hold ❒ Remote Access
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)	

Table 11: Collect MiVoice Business Express Initial Provisioning Wizard Data

CONFIGURATION ITEMS	FIELD DESCRIPTION	SITE CONFIGURATION DATA
MiCollab AWV: allows users to set up audio and web conferences for online meetings, training sessions, and presentations. Users can share their desktops or individual applications during the conferences. Video recordings of the web sessions can be made for playback.		
Conferencing FQDN	Record the Fully Qualified Domain Name (FQDN) of the MiCollab AWV server.	
Conference WAN IP Address:	MiCollab AWV public IP address on the WAN.	
AWV Main Dial-In Number	Record the main dial-in number that you want to present to users in the conference email invite.	
Direct Inward Dialing Number	Obtain a telephone number from your SIP service provider that will be used to access the AWV conference application. This number is mapped to the AWV conference hunt group in MiVoice Business.	
AWV Toll Free Dial-In Number	Record the toll free dial-in number that you want to present to users in the conference email invite.	
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.		
Music on Hold File	Identify the filename and location of the music source file. Refer to the *MiVoice Business Express 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.		
Configure remote access to MiCollab Server Manager interface	Network Address	
	Network Prefix	
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 (resolved locally or via a LAN DNS server?)	
MiCollab		
Active Directory Integration (optional)	Record the Active Directory Server IP address.	

Table 11: Collect MiVoice Business Express Initial Provisioning Wizard Data

CONFIGURATION ITEMS	FIELD DESCRIPTION	SITE CONFIGURATION DATA
Administrator Password		
Replaces the password that you used to access the wizard. It allows you to log into the server manager administration interface.	A strong password is recommended. A strong password would contain all the following: upper case letter, lower case letter, number, non-alphanumeric character and be at least seven characters long. **Note**: If you deploy MiVoice Business Express in an environment without vCenter, (where it is deployed using vSphere connected directly to an ESXi server) then this Administrator Password is not applicable. Instead, you must use the administrator password that you configure through the server console during initial configuration.	

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 Express system from the Initial Configuration Wizard.

1. Log into the MiVoice Business System Administration tool. See “Logging into the MiVoice Business Tools” on page 125.
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 Express system.

REVIEW WORKFLOW

Figure 8 summarizes the installation and provisioning workflow when deploying MiVoice Business Express in a VMware environment.

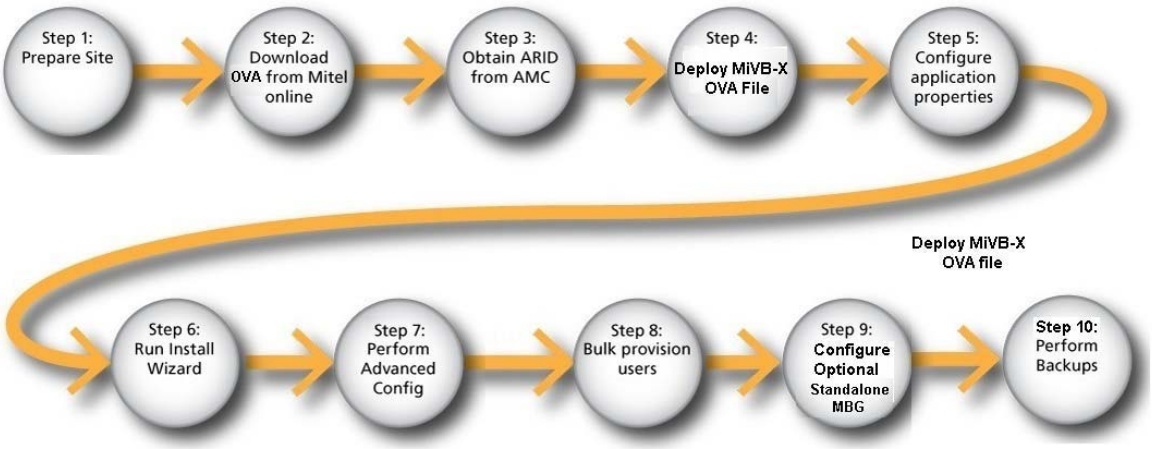

Figure 8: MiVoice Business Express Deployment on New Site

Figure 9 summarizes the installation and provisioning workflow when deploying MiVoice Business Express in a environment.

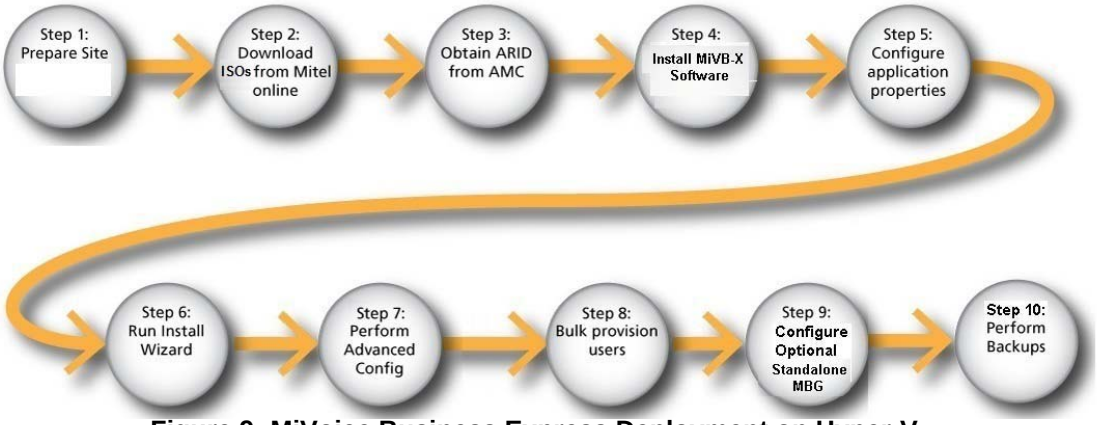

Figure 9: MiVoice Business Express Deployment on Hyper-V

Chapter 4

PREPARE SITE

SITE REQUIREMENTS

- The MiVoice Business Express requires access to the internet in order to obtain its licenses from the Applications Management Center (AMC). Internet connectivity is required to license the product and must be maintained to support the system licensing.
- The available virtual appliance resources for the MiVoice Business Express virtual machine must meet or exceed the minimum requirements listed in the *Virtual Appliance Deployment Solutions Guide*.

SET UP ACTIVE DIRECTORY SERVER (OPTIONAL)

If required, set up the Active Directory server prior to deploying the MiVoice Business Express. Ensure that you have recorded the Active Directory Server IP address in Table 9 on page 46.

DEPLOY AND CONFIGURE OPTIONAL EXTERNAL VMBG SIP PROXY

For UCaaS deployments, configure and deploy the optional external vMBG SIP Proxy server before you deploy and provision the MiVoice Business Express. The Initial Configuration Wizard prompts you for the standalone vMBG IP address during the wizard.

Refer to the *MiVoice Border Gateway Installation and Maintenance Guide with Web Proxy* on the Mitel Customer documentation site at http://edocs.mitel.com for deployment and configuration instructions.

CREATE ARIDS AND ASSIGN LICENSES IN AMC

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

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

ABOUT THE MITEL APPLICATION MANAGEMENT CENTER (AMC)

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

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

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

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

REQUESTING A NEW AMC ACCOUNT

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

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

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

ACCESSING YOUR AMC ACCOUNT

To access your account for the first time:

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

UCC LICENSING PROCEDURE

The Application Management Center distributes the platform and application user licenses that are contained within a UCC license bundle to the members of a Unified Licensing Manager

(ULM) group. During the licensing process, you create a ULM group ARID for the MiVoice Business Express deployment.

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

OVERVIEW

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

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

DEPLOYING UCC LICENSES

A detailed procedure for deploying UCC licenses follows:

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

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

2. Create a Customer Account for each MiVoice Business Express customer. Do not put multiple customers in a single customer account.
   - Under **Systems**, click **Customers**.
   - Click the **Create Customer** button.
   - Enter the end-customer information. Record the Customer Name and Customer ID.
   - Enter the email address of the account manager responsible for this customer.
   - Enter the email address of the technician responsible for supporting this customer.

- Click **Submit**.
- Click **Confirm**.

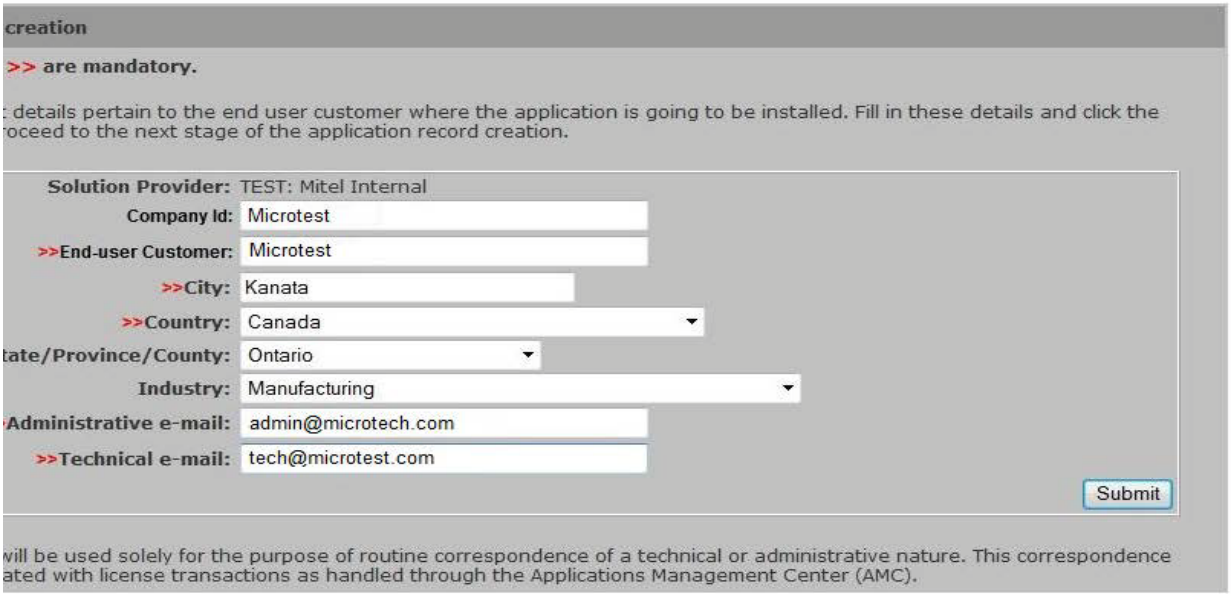

Figure 10: Creating a Customer

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

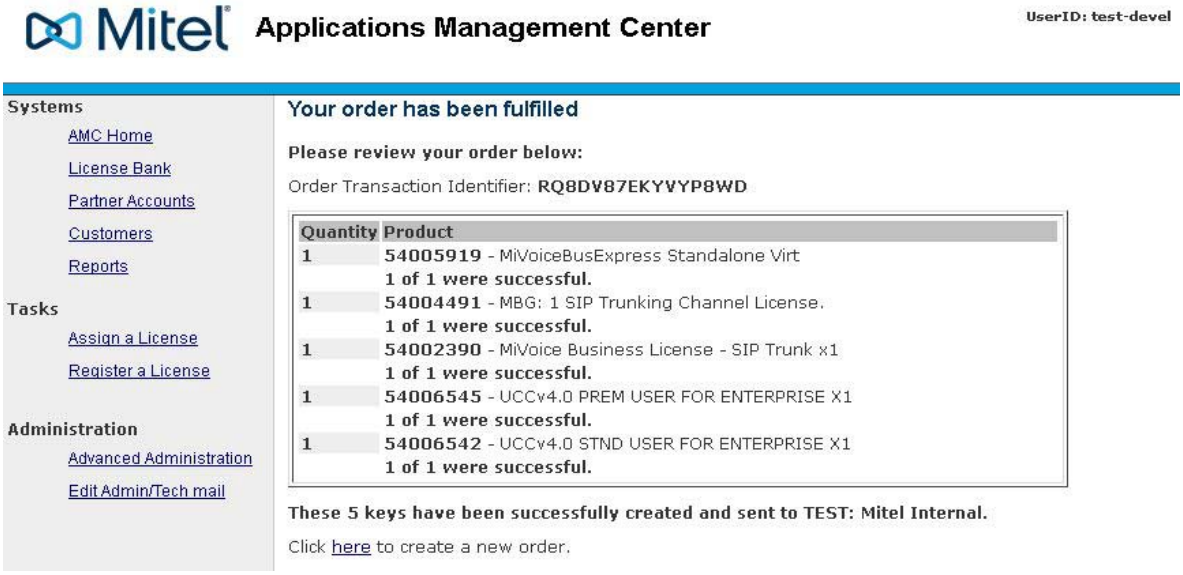

Figure 11: Order Confirmation

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

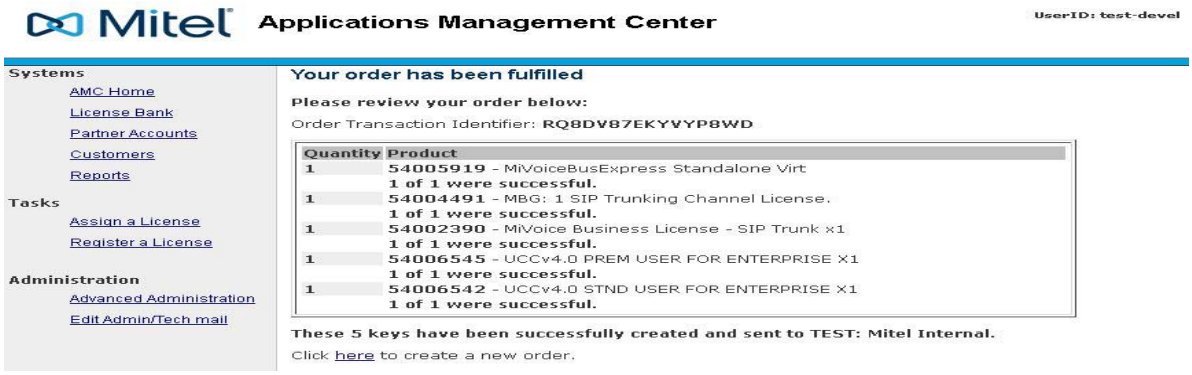

Figure 12: MiVoice Business Express Base ARID Created

5. Assign the MiVoice Business Express base software license to the MiVoice Business Express Base ARID:
   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.

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

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

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

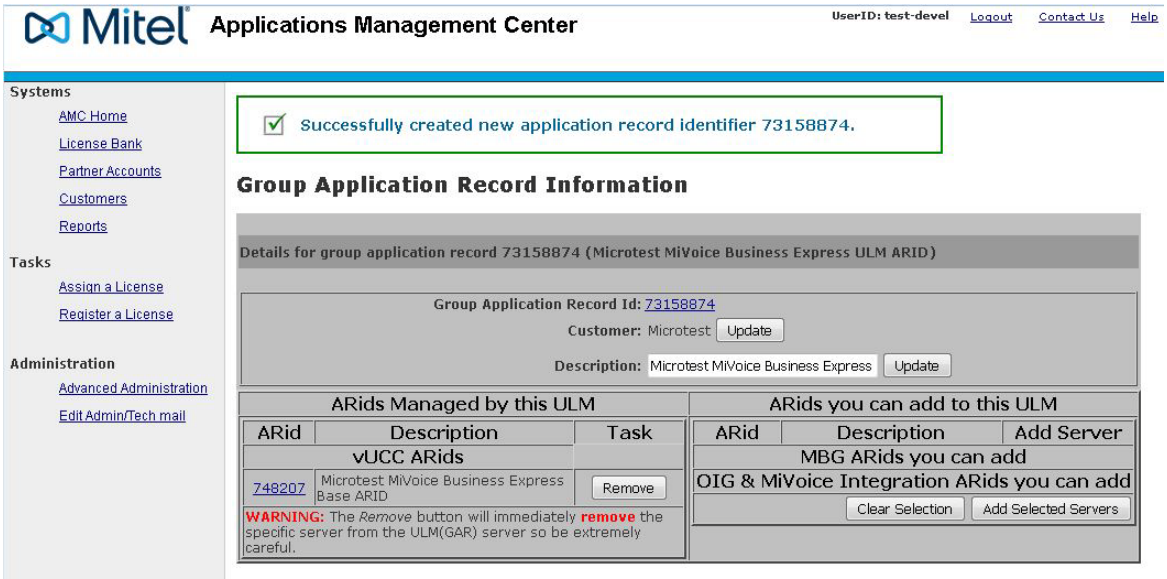

Figure 13: Create the Group ULM ARID

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

EFFECT OF UPGRADING ON UCC LICENSING

When you upgrade to MiVoice Business Express 7.0, UCC v3 Entry, Standard, and Premium licenses are upgraded to UCC v4 licenses. However, the number of external hot desk licenses that were provided by the UCC v3 Entry licenses remains the same.

Chapter 5

DEPLOY ON VMWARE

BEFORE YOU BEGIN

This chapter describes the deployment of the MiVoice Business Express virtual appliance in a VMware environment. It does not describe the setup and operation of the virtualization environment. Note the following deployments are supported:

MiVoice Business Express can be deployed using the vSphere Client:

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

See the *Virtual Appliance Deployment Guide* guide for the virtualized environment requirements.

DOWNLOAD OVA FILE

Download the MiVoice Business Express OVA file from Mitel Online:

1. Launch your browser.
2. Log into Mitel Online at https://www.ebiz.mitel.com.
3. Click **Technical Support** and then click **Software Downloads**.
4. Click **Mitel Applications Suite** (MiVoice Business Express).
5. Click **MiVoice Business Express Release 8.0. and Previous**.
6. Click the appropriate MiVoice Business Express Software Download version.
7. Review the Release Notes.
8. Verify that the versions of the software and applications are correct.
9. Download the required OVA file by clicking the link in the table. When you click a link, you are presented with a software **Disclaimer**.
10. Click "I Agree [Download using Software Download Manager (Recommended)]".
11. If you don't already have the Download Manager installed on your local PC, you are prompted to install it. The Download Manager is an Active X application that optimizes the software download speed. After you install the Download Manager, it is available for subsequent software downloads.
12. Save the OVA file to a network drive or to a folder on your PC.
13. Proceed to "Deploy Virtual Appliance" on page 65.

DEPLOY VIRTUAL APPLIANCE

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

See the *Virtual Appliance Deployment Guide* guide for deployment instructions

MODIFYING ADVANCED DEPLOYMENT PROPERTIES

The addresses of the following deployment properties are not configurable from the Custom Template screen during initial deployment:

- **Mitel AMC Server IP**: Defaults to the IP address of the Mitel AMC Licensing server.
- **MiVoice Business**: Defaults to the MiVoice Business Express LAN IP address +1. For example, if the MiVoice Business Express LAN IP address is 10.45.102.88, the MiVoice Business address defaults to 10.45.102.89.

If necessary, you can modify the deployment properties of the virtual appliance from the vSphere Client. Modify the properties before you power on the virtual appliance for the first time after deploying the OVA. If you power-up the virtual appliance and then shut it down first, you may not be able to modify the properties.

1. Deploy the MiVoice Business Express OVA file.
2. In the vSphere Client screen, select the MiVoice Business Express virtual appliance.
3. Do not power up the virtual appliance yet. You cannot edit advanced properties while the virtual appliance is running.
4. For vSphere 5.5
   - Right-click and select **Edit Settings**.
   - Click **vApp Options**.
   - Check the **Enable vApp options** box.
   - Under **Authoring**, click **Properties**. The Advanced Property Configuration screen opens (see Figure 14).
5. Select the required key, click **Edit**, enter the required value in the Default Value field and click **OK** to apply:
   - **mitel_amc_server_ip**: If want to proxy the Mitel AMC server, enter the IP address of the proxy server.
   - **telephony_server_ip**: Enter the IP address of the MiVoice Business system.

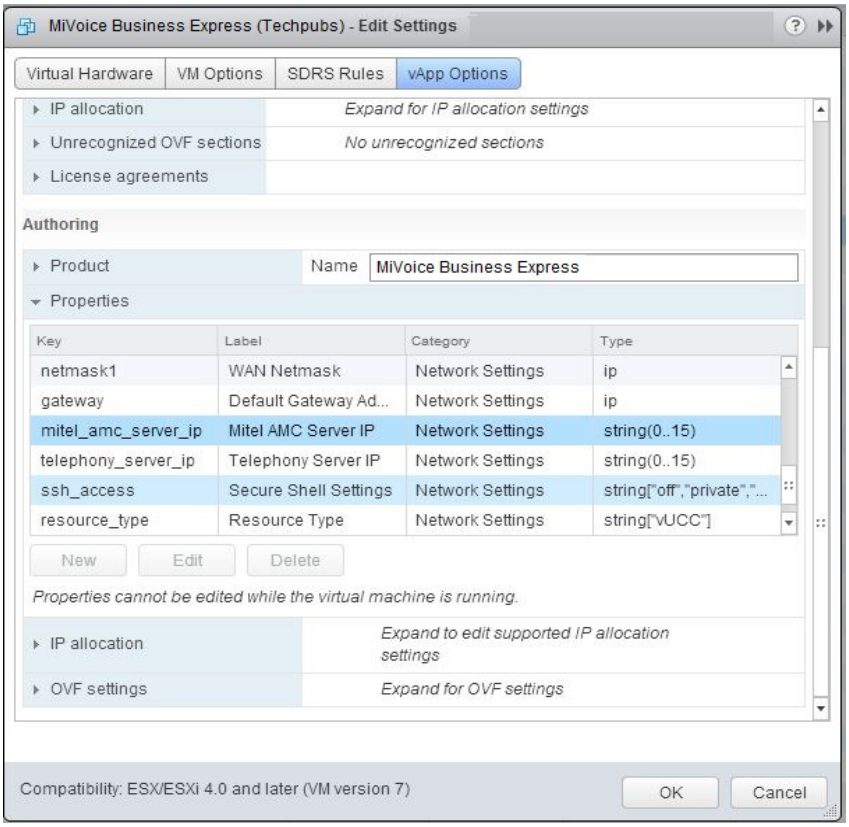

Figure 14: Advanced Property Configuration Screens (vSphere 5.5)

POWER ON MIVOICE BUSINESS EXPRESS

1. Right-click on the newly created MiVoice Business Express (for example: MiVoice Business Express --8.0 build) and select **Power On**.

2. Click **Console** (vSphere 5.0 or 5.5 desktop client) or right click on the MiVoice Business Express virtual machine and select **Open Console** (vSphere 5.5 web client). The system boot up progress messages are displayed in the Console screen. When the system is finished booting up, the **mitel-vm login:** _ prompt is displayed. The "prompt" changes to the system name that you chose during deployment (default is mivb-x). Do not log in at this prompt. Instead, you will log into the MiCollab server manager via your web browser and run the Initial Configuration Wizard.

3. If your MiVoice Business Express does not have access to the WAN, proceed to “Configure LAN Access to AMC Server (Optional)” on page 75. Otherwise, proceed to “Run the Wizard” on page 78.

Chapter 6

INSTALL ON MICROSOFT HYPER-V

INTRODUCTION

This chapter describes the installation of the MiVoice Business Express software on a Microsoft Hyper-V virtual machine.

REQUIREMENTS

Before you can install the MiVoice Business Express software on Microsoft Hyper-V, you must first complete the following tasks:

- Create the Hyper-V virtual machine, and
- Configure the network adaptors

See the *Virtual Appliance Deployment Guide* guide for the virtualized environment requirements.

DOWNLOAD SOFTWARE ISO FILES

Download the MSL ISO software file and application software ISO files and save them to a network share or copy them to portable CD/DVDs.

Note: Installation of application software is not supported from the MSL server console. You must install the application software from the server manager **Install Applications** panel.

To download the software ISO files from Mitel OnLine:

1. Log on to **Mitel Connect**.
2. Click **Mitel OnLine**.
3. Click **Support**.
4. Under **Technical Support** click **Software Downloads**.
5. Click **Mitel Applications Suite** (for MiVoice Business Express).
6. Click the appropriate MiVoice Business Express Software Download version.
7. Review the Release Notes.

8. Download the ISO files for your deployment by clicking the file links in the table. When you click a link, you are presented with a software **Disclaimer**. Note that you only need to download NPM DVD ISO #1 file. You can install the other applications from the Applications Management Center (AMC).
9. Click the "I Agree [Download using Software Download Manager (Recommended)]".
10. If you don't already have the Download Manager installed on your local PC, you are prompted to install it. The Download Manager is an Active X application that optimizes the software download speed. After you install the Download Manager, it is available for subsequent software downloads.
11. Save the downloaded software ISO images to a folder on the network.

After you download the MiVB-X and application software, burn the ISO files to CD/DVDs.

You will require up to eight, blank, formatted CDs or DVDs for all the ISO files. Note that the MiVB-X and NP-UM ISO files must be burned to separate DVDs. They are too large for CDs. Each CD/DVD must be labeled with the ISO file name. The installation script uses the ISO file name to request the software.

1. Insert a CD/DVD into CD/DVD ROM drive of the maintenance PC.
2. Navigate to a stored ISO image and use a CD/DVD burner application to create a CD/DVD. Label the CD/DVDs as follows:

LABEL	CD/DVD CONTENT	FILE NAME DOWNLOADED
CD/DVD1	MSL 10.5 for MiCollab Servers	msl-10.5.xx.0.x86_64.iso
CD/DVD2	MiCollab Application Services	SAS_8.0.x.xx-01.iso
DVD3	MiCollab NuPoint Unified Messaging (Main)	NPM_Blades-DVD_1_19.x.x.xx-01.iso
DVD4	MiCollab NuPoint Unified Messaging (includes Speech to Text option)	NPM_Blades-DVD_2_19.x.x.xx-01.iso
CD/DVD5	MiCollab Audio, Web and Video Conferencing	Blade_AWC-8.0.x.xx-1.x86_64.iso
CD/DVD6	MiVoice Border Gateway	mbg_10.0.x.xx-01-bladecd.iso
CD/DVD7	MiCollab Client Service	MITEL_UC_SERVER-8.x.x.xx-01.iso
CD/DVD8	MiVoice Business	mivb_core_blade_8.x.x.xx-01.iso
DVD9	MiCollab Client Deployment	ClientDeployment_8.x.x.x-01.iso
DVD10	Initial Configuration Wizard	Blade-InitialConfigWizard_4.x.x.x-01.iso

INSTALL MSL OPERATING SYSTEM SOFTWARE

During the install, if you accidentally exit from the server console, you can use Secure Shell (SSH) to access the server console again (see "Logging into the Server Manager (Administrator Portal)" on page 124 for details).

It takes approximately 15 minutes to install the MSL operating system software.

1. Mount the MSL_10.5.xx.0.iso file on the CD/DVD drive or network drive.

2. Power up the virtual machine or physical server. After the physical server or virtual machine powers up, the server console launches, and you are presented with the installation choices.

3. Select the following software load:
   - **MSL 10.5.xx.x SL** for MiVoice Business Express
4. Depending on your model of CD/DVD drive, you may be prompted to select the installation language. Use the Space bar on the keyboard to select the desired language and select **Ok**.
5. Choose your preferred keyboard from the list (default is **us**).
6. You are prompted to test the CD/DVD media. Select **Test** to test the CD/DVD for validity and readability. The software installer runs.
7. At the **Install** option, select **Yes**.
8. Select your Time Zone from the list. Select **Ok**.
9. You are reminded to review the log file of the install. During the installation, logs are generated. After the installation is complete, the log file is saved to the root directory of the server: /root/install.log. Select **Next**.
10. Finishing the installation is automatic and takes only a few minutes. At the end of the process, you are prompted to remove any media and reboot the system.
11. Remove the CD/DVD media.
12. Press **Enter** to reboot. The server reboots.

CONFIGURE THE MSL OPERATING SYSTEM

Next, you must configure the MSL operating system. Refer to your Site Information sheet (Table 9 on page 46) while completing the entries in the following sections.

Note: To ensure that your entered information is not lost when you use the MSL server console, always press the **Alt** keyboard key to recover from power saving mode or screen saver mode. Do **not** press the Space bar or **Return** keyboard key when the terminal screen has gone blank.

ACCEPT END USER LICENSE

Select **Accept** to proceed with the installation. At the "Restore from backup?" prompt, select **No** since this is your initial installation of the software.

SET KEYBOARD TYPE AND ADMINISTRATOR PASSWORD

Set the keyboard type.

Enter the Administrator password and then re-enter it for confirmation.

The Administrator password (or System password) is used to access the administrator portal or the server console. 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.

SELECT SYSTEM TIMEZONE

Select the system timezone by typing the first letter of the timezone and then use the up and down arrow keyboard keys to select the desired timezone.

CONFIGURE DOMAIN NAME

Enter the primary domain name that will be associated with the MSL server (Field defaults to "mycompany.local"). This domain will become the default for the web-based administrator 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.

Note: Do not change the primary domain name after you have configured it. If the domain is modified, the server and all clients will require a reboot and a manual modification of all references (such as bookmarks) that point to the server.

CONFIGURE SYSTEM NAME

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, MiVB-x1).

ENTER LOCAL NETWORK ADAPTER

MSL allows you to configure your system's network adapters and displays them so you can configure:

- a "Local" adapter (for LAN mode) or
- a "Local" adapter AND a "WAN" adapter (for Network Edge mode)
- an "Optional" adapter that can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.

Note that although MSL offers the choice to bond two Network Interface Cards, this option is not supported for MiVB-X.

Regardless of the server mode, you must always configure a Local (internal) adapter. Use the space bar to select the adapter to configure as Local.

- Use the space bar and up/down arrow keys to select the adapter you want to configure as local.

Note: If you are installing the Teleworker application, you will need to configure one adapter as a WAN (external) adapter in a later step.

ENTER LOCAL NETWORKING PARAMETERS

- Enter the local IP address for this server. This is the *LAN IP Address* for the MiVoice Business Express.
- Enter the subnet mask for the local network, or accept the default.

These settings provide information about the internal network so that the server can communicate with other machines on the local network. If you enter the wrong IP address, you will not be able to activate the software.

Enter the local IP address for this server or select from the default parameters provided. If the server is being installed into an existing network, choose an address that is not in use by any other computer on the network.

Note: If you are installing servers at multiple sites within the organization, use different network addresses for each site. This simplifies later troubleshooting and VPN setups.

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.

ENABLE IPV6 PROTOCOL AND ADDRESS

Select **No** to limit the server to IPv4 addresses. IPv6 addressing is not supported.

Continue with the next configuration step “Select WAN Adapters”.

SELECT WAN ADAPTERS

MSL prompts you to configure WAN adapters:

- If you are deploying in Network Edge mode, (that is, with Internet access), you must configure a WAN (external) adapter. MSL offers the choice to bond two Network Interface Cards - bonding is not supported.
- If you are deploying in Network Edge mode with MiCollab AWV, you must configure two external IP addresses on the WAN adapters for MiCollab AWV web collaboration support. In Network Edge mode, the MSL firewall is located in the MiCollab server that resides on the network edge. Obtain two external IP addresses from your Internet Service Provider (ISP) for the web server interface and the conference functions. The MSL firewall on the MiVoice Business Express system is pre-configured to port forward from the second external alias IP address to the MiCollab AWV service on MiVoice Business Express.
  - Configure WAN interface
  - Select STATIC from (static/dhcp/ppoe)
  - Enter WAN IP address of the MiCollab AWV web server interface
  - Enter WAN IP netmask
  - Enter WAN alias IP address of the MiCollab AWV conference functions
  - Enter WAN alias IP netmask. If you leave the WAN alias IP address blank, this screen is not presented.
- If your MiVoice Business Express system will be operating in LAN mode, do not configure a WAN adapter. Press the space bar to clear the selection.

Note: If you still have unconfigured adapters at this time, MSL will prompt you to configure them. Select **Yes** to configure the remaining adapter(s) as Local or select **No** to leave them unconfigured.

SELECT GATEWAY IP ADDRESS

If you did not configure a WAN adapter, you are prompted to enter a gateway IP address. If you want this server to access the Internet, then enter your gateway (router) IP address..

Note: If you have configured a WAN adapter, this prompt does not appear.

CONFIGURE EXTERNAL INTERFACE

Specify how the WAN adapter will be configured. Use a static IP for the WAN adapter.

- Select Option 4.
- Enter the IP address that this system should use to access the Internet.
- Enter the subnet mask.

CONFIGURE DNS

- If there are specific routes out to the Internet and you want the server to do DNS lookups to other servers in the network, enter the Corporate DNS server address, click **Next** and then specify how name resolution is performed for the local domain (the domain configured on the MSL server):
  - **localhost** – the localhosts file is used resolve names for the local domain while the corporate DNS server handles name resolutions for all other domains.
  - **corporate** – The corporate DNS server is used to resolve names for all domains.
- Click **Next**. The MSL operating system is now configured.

LOG INTO THE MICOLLAB SERVER MANAGER

1. Open a browser. See page 124 for a list of the supported browsers. Note that on Microsoft Windows 8 with Internet Explorer 10, the Integrated Configuration Wizard is only supported in compatibility mode.
2. On a PC on the same subnet as the MiVoice Business Express virtual machine, open your browser and enter the following in the address bar:
   https://*<LAN IP Address of the MiVoice Business Express>/server-manager*
3. Enter the administrator username and password.

ENTER SERVICE ID (ARID)

1. In the server manager, under **ServiceLink**, click **Status**.
2. Enter your Application Record ID (also called Service account ID).
3. If the Internet is accessed via a proxy, enter:
   - Address of proxy
   - TCP port used to connect to proxy. The proxy server must be configured to forward TCP packets on the incoming port to the AMC address (sync.mitel-amc.com) on port 22.
4. Click **Activate**.

INSTALL APPLICATIONS SOFTWARE

Installation of application software is not supported from the MSL server console. Install the application software from the server manager **Install Applications** panel.

1. In the server manager, under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab.
3. Set the **PBX Type** to "MiVoice Business" and then click **Next**. The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.
4. Select the software version.
5. Check the **Download from AMC** box of **each application** in the list. You must select all the listed applications.
6. Click **Install**. The applications are installed.

Note: The NuPoint ISO files are not available from the AMC for download. You must install them from a network share or from DVDs. Refer to the **Install Applications** panel online help for instructions.

7. Reboot the MiVoice Business Express server.
8. Proceed to “Run the Wizard” on page 78.

Chapter 7

PERFORM CONFIGURATION

CONFIGURE LAN ACCESS TO AMC SERVER (OPTIONAL)

By default, MiVoice Business Express must have access to the WAN in order to obtain its licensing from the Mitel AMC server. Typically, the trusted local network of the MiVoice Business Express system will have access to the WAN through a firewall as shown in Figure 15.

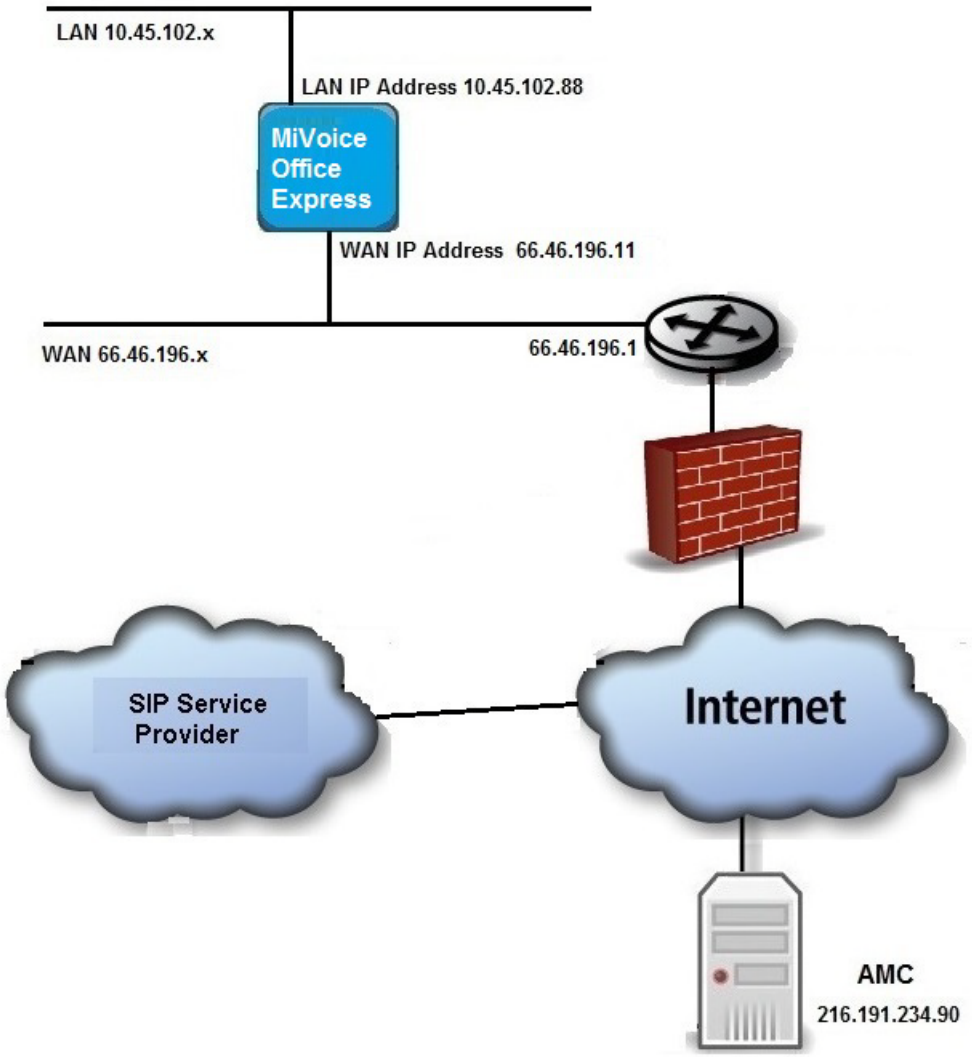

Figure 15: Typical LAN Access to AMC Server (Example)

If the trusted local network does not have access to the WAN, you can add a host local network that redirects the AMC public address to the LAN router as shown in Figure 16.

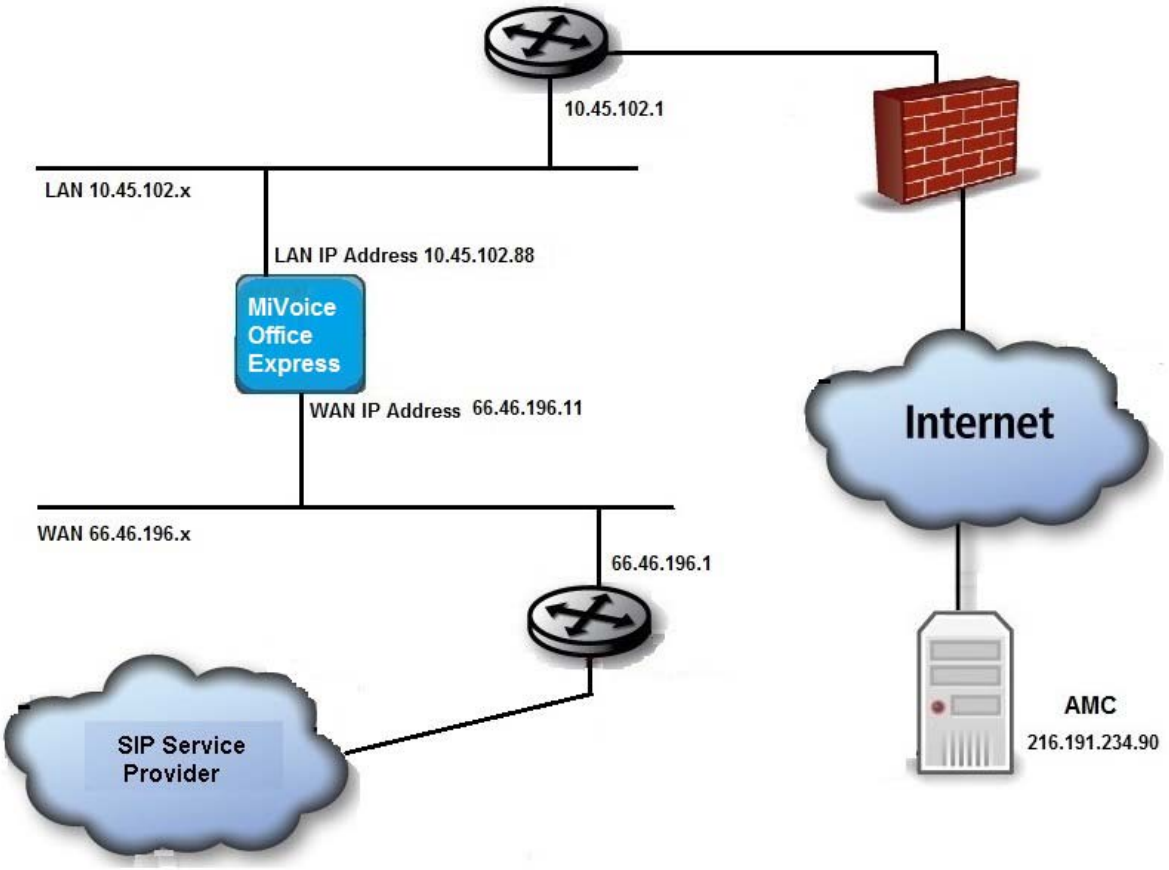

Figure 16: Configuring LAN Access to AMC Server (Example)

To configure LAN Access to AMC Server

1. Deploy the MiVoice Business Express software without specifying the license key.
2. Log into the MiCollab server manager:
   - Open a browser. See page 124 for a list of the supported browsers. Note that on Microsoft Windows 8 with Internet Explorer 10, the Integrated Configuration Wizard is only supported in compatibility mode.
   - On a PC on the same subnet as the MiVoice Business Express open your browser and enter the following in the address bar:
     https://*<LAN IP Address of the MiVoice Business Express>/server-manager*
   - Enter your username and password.
3. Under **Configuration**, click **Networks**.
4. Click **Add a new trusted network** and add a single host local network that redirects the AMC public address to the LAN router. Refer to the example shown in Figure 17.

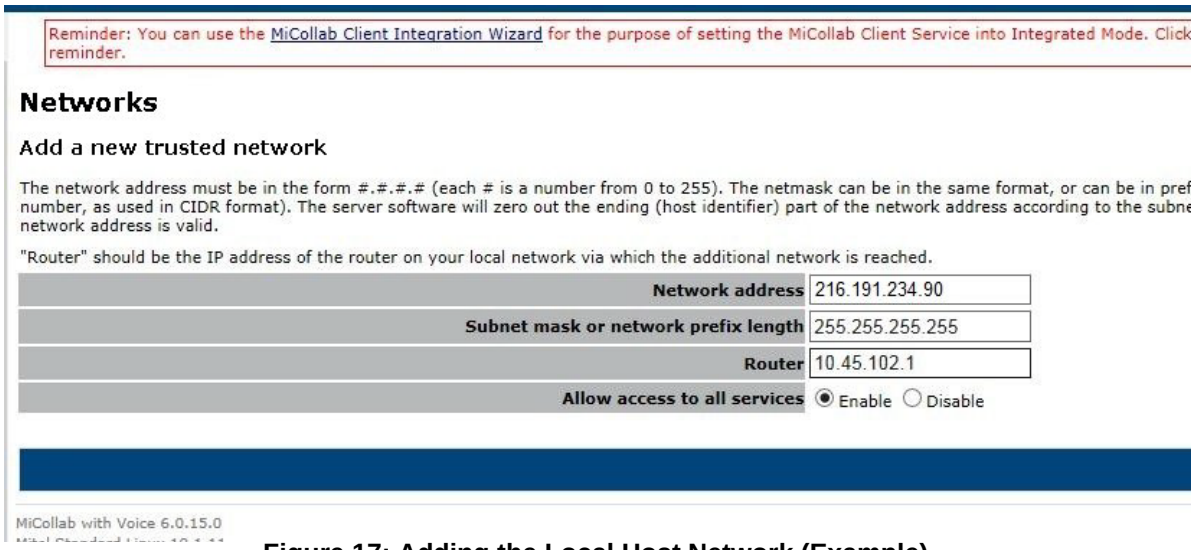

Figure 17: Adding the Local Host Network (Example)

5. To verify that the AMC server licensing is redirected to the router:
   - Log into your account on the AMC server.
   - Display the Application Record for the MiVoice Business Express ARID.
   - Click **Update**.
   - Scroll down to the "Sync IP" field. The Sync IP field should display the MiVoice Business Express LAN IP address.

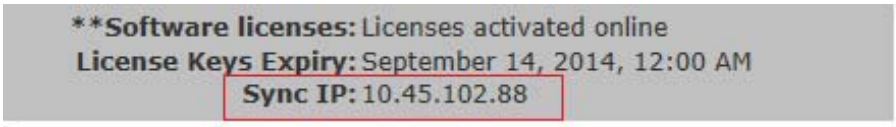

Figure 18: Sync IP Field (Example)

6. Proceed to “Run the Wizard” on page 78.

RUN THE WIZARD

The Initial Configuration Wizard fully supports the configuration of the MiVoice Business Express system in the following telecom regions: North America, United Kingdom, Australia, France, Netherlands, Belgium, Germany, and New Zealand.

- For telecom regions that are fully supported, the wizard presents all the configuration screens detailed in the following procedure.
- However, 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. The wizard will present a subset of the configuration screens. After you run the wizard, to complete the configuration you must import MiVoice Business form data or program the region specific settings manually from the MiVoice Business System Administration tool.

CAUTION: You must complete the Initial Configuration Wizard before you log into an MiVoice Business Administration session. The first time that you log into the MiVoice Business System Administration Tool, it prompts you to change your password. After you change the MiVoice Business System Administration Tool password, you will be unable to run the wizard.

Note that the values shown in the following screens are examples only.

1. Before you begin, ensure that you have assigned the following minimum number of licenses to the MiVoice Business Express base ARID:
   - two MiVoice Business SIP Trunking Licenses, and
   - if using internal SIP trunking, two MBG SIP Trunking Channel Licenses.

   The Initial Configuration Wizard requires these licenses in order to complete configuration of the system.
2. On a PC on the same subnet as the MiVoice Business Express open your browser and enter the following in the address bar:
   https://<*LAN IP Address of the MiVoice Business Express*>/icw

Note: See Table 9, “Collect Custom OVA Template Information,” on page 46 for the LAN IP Address of the MiVoice Business Express.

Note: See page 124 for a list of the supported browsers. Note that on Microsoft Windows 8 with Internet Explorer 10, the Integrated Configuration Wizard is supported only in compatibility mode.

3. Enter your username and password in the login screen.
4. The Initial Configuration Wizard Welcome screen opens.The wizard applies defaults to a majority of the MiVoice Business Express configuration settings. See “System Defaults” on page 141 for details.During the wizard, use the information that you collected in the *MiVoice Business Express Site Specific Provisioning* section of Table 9 on page 46 to complete the fields that are not defaulted.

Note: If the server console menu is displayed instead of the Initial Configuration Wizard, you may have entered invalid IP addressing in the Custom Template page. Use the server console menu to check your LAN, WAN and Gateway IP addresses. The WAN IP address and LAN IP address must be on different subnets and the Gateway IP address must be on a subnet of one of the IP addresses.

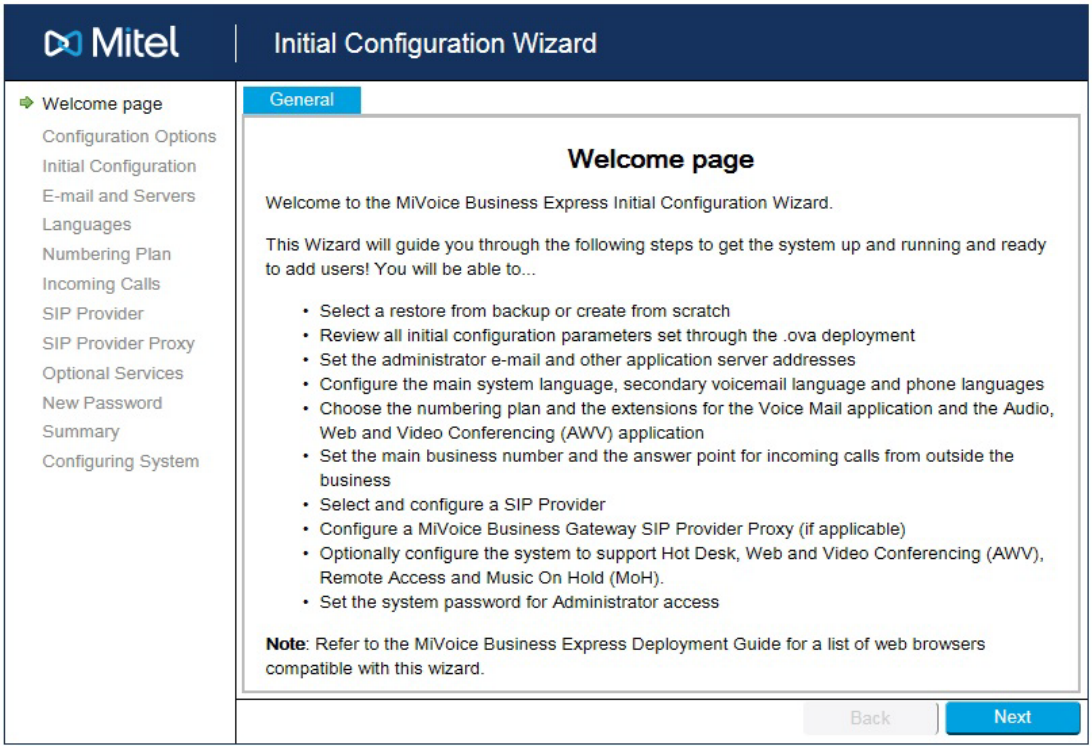

Figure 19: Initial Configuration Wizard - Welcome

5. Click **Next**. The Configuration Options screen is displayed. Since you are deploying a new MiVoice Business Express site, click **Create a new configuration**.

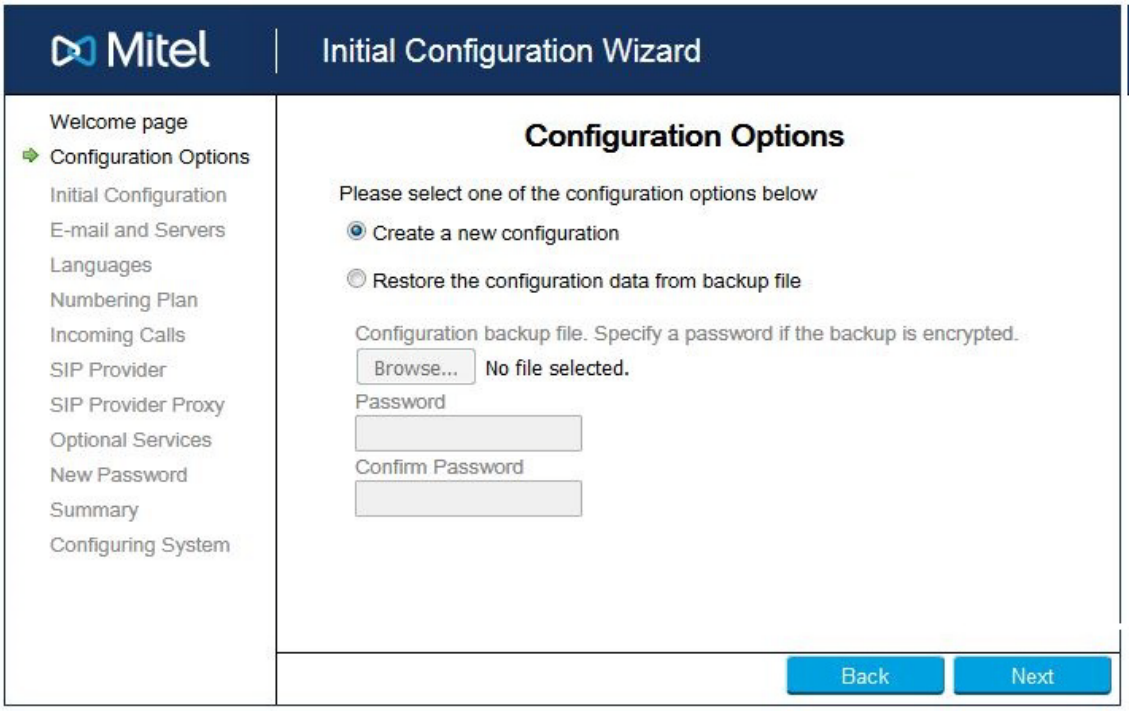

Figure 20: Configuration Options

6. Click **Next**. The Review Initial Configuration screen is displayed. Review the IP network addresses that you configured during the deployment of the OVA. If necessary, you can select a different *Time Zone*, *Country*, and *Telecom Region*. If you select *Other* for the Country setting, the wizard will only partially configure the system and you will need to manually configure the MiVoice Business trunking, Direct Inward Dialing, and Automatic Route Selection after initial deployment. See “Manual Configuration for "Other" Country Setting” on page 98 for details.

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.

Note: If you are deploying the OVA on a Hyper-V server or on a vSphere Client directly connected to an ESXi server, you must enter the LAN IP Address #2 (MiVoice Business IP address) and the Licensing Key in this page.

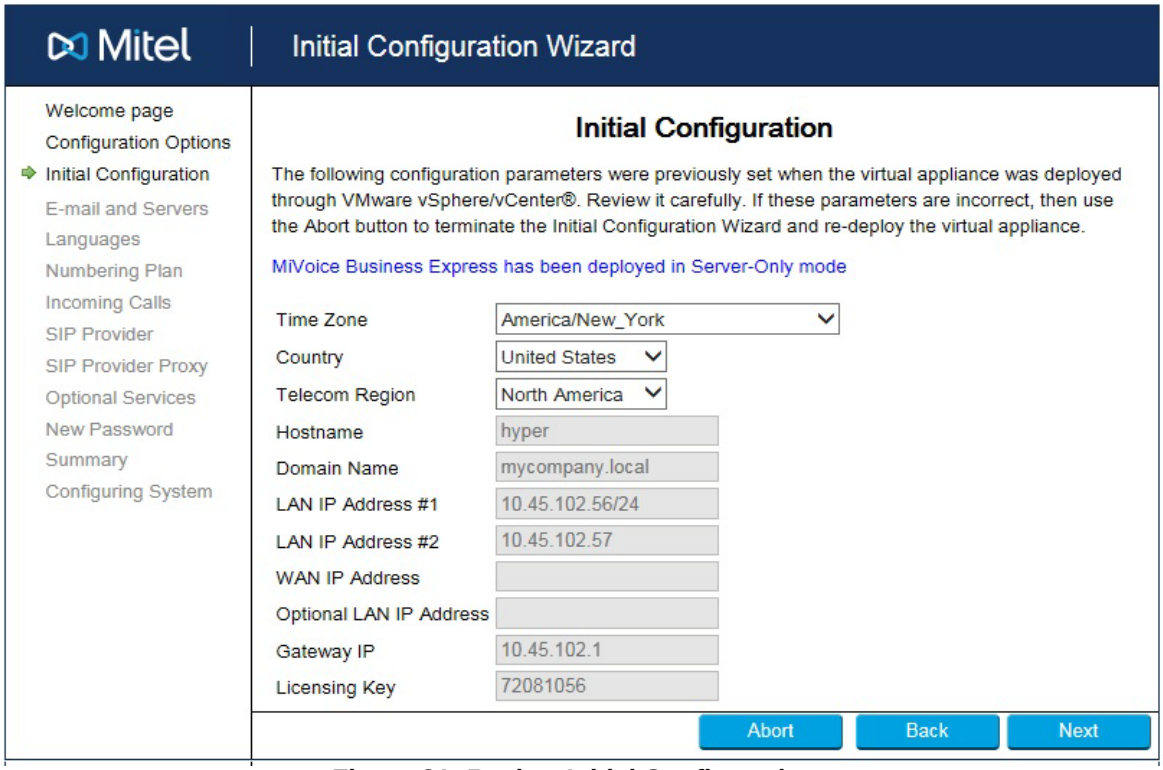

Figure 21: Review Initial Configuration

7. Click **Next**. After the system validates the LAN IP Address # 2 and Licensing key, the E-mail and Servers screen is displayed. Complete the following:
   - *Administrative E-mail Address*:
   - *Corporate DNS IP Address:*
   - *Secondary DNS IP Address*:
   - *SMTP mail server*:
   - *Network Time Server*:

Note: If a licensing error message appears on the Initial Configuration screen, you cannot proceed with configuration. To remedy:

1. Abort the ICW configuration wizard.
2. Delete the partially configured MiVoice Business Express virtual machine.
3. Update the ARID with the required licenses in the AMC.
4. Deploy the OVA again using the updated ARID.

You cannot simply apply the licenses to the ARID and then continue with the current deployment because the license updates will not be recognized by the MiVoice Business.

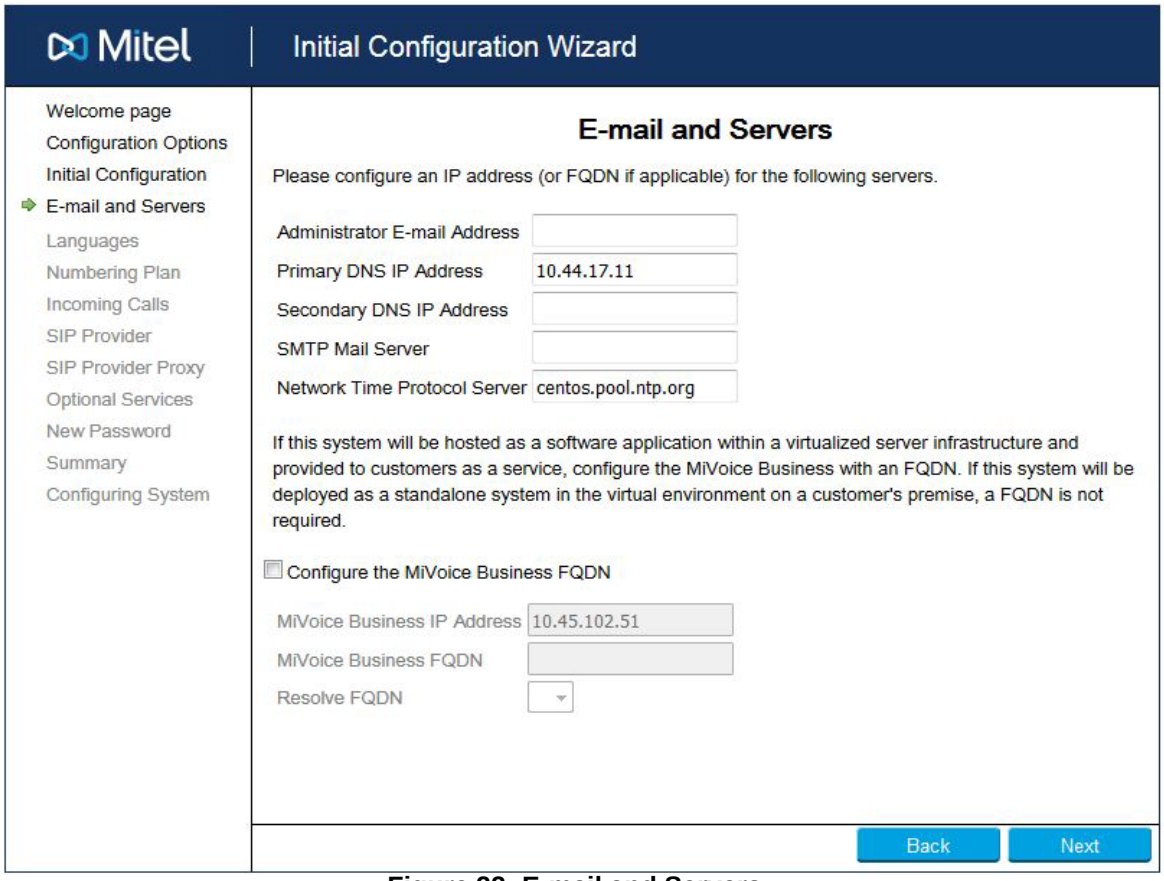

Figure 22: E-mail and Servers

5. If Reach-Through (single sign-on) is required from the Internet to the MiVoice Business, configure the MiVoice Business with an FQDN. Note that the MiVoice Business IP Address must resolve to the FQDN.

6. Click **Next**. The Languages screen is displayed. Set the following
   - *System Language*: Identify the MiCollab default language. The selected language is applied to the MiCollab End User portals and the Telephone User Interfaces (TUIs) for the MiCollab application end-users.
   - Select the other languages for the voice mail prompts. When users call into the voice mail system through the Message Center auto attendant or Receptionist application, they are asked to select the language of the prompts for the duration of their call. Users can select either the primary prompt language or one the other languages. The primary (first) language is determined by the System Language setting above; the other languages are determined by the settings in these fields.
   - Select the languages that users can have on their phone displays. The Primary language appears by default on the phones.

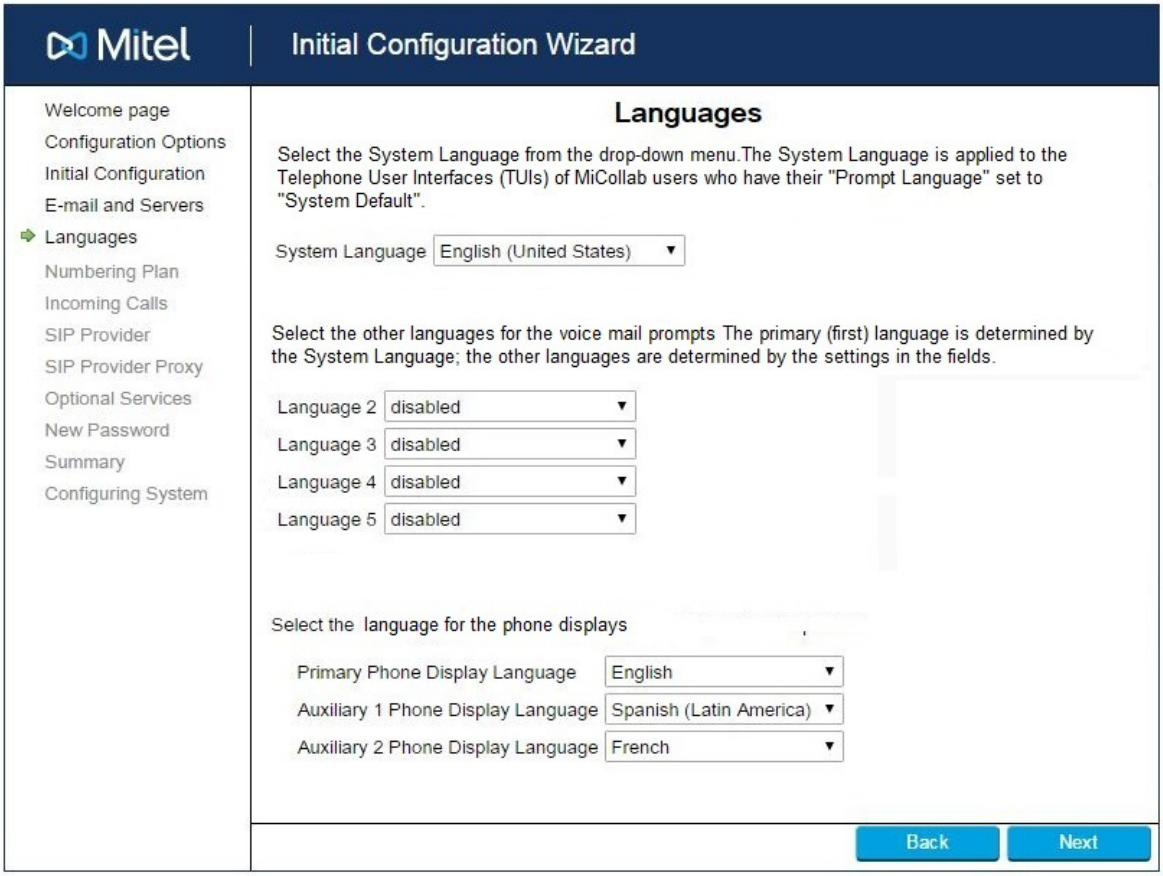

Figure 23: Languages

7. Click **Next**. The Numbering Plan screen is displayed.

   Extension Length: Set the length from (3 to 5 digits) of the system extension numbers.

   Hunt groups are used to route incoming calls to a group of designated extensions or application ports. A hunt group consists of a hunt group extension number (pilot number) and a group of member extension numbers or ports. Calls to the hunt group extension ring the first idle member in the group. Enter the hunt group extension numbers and starting port extensions for the hunt groups or use the default settings provided.

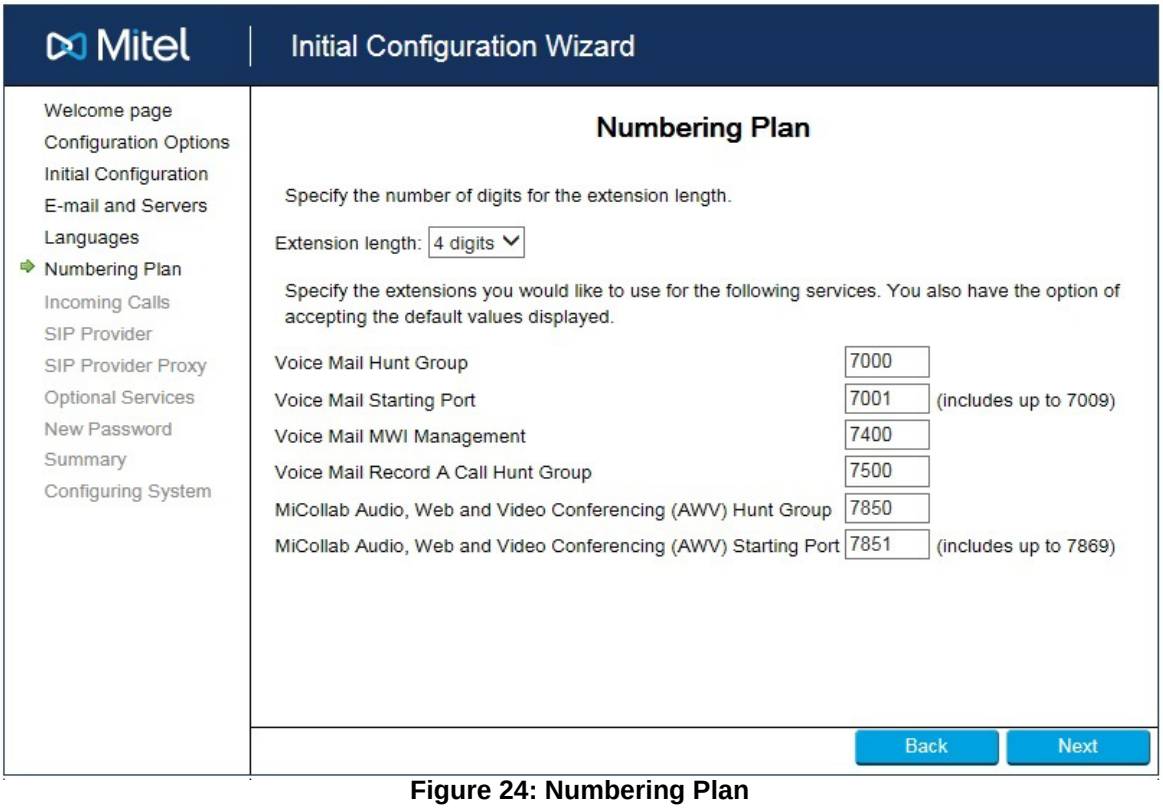

Figure 24: Numbering Plan

8. Click **Next**. The Incoming Calls screen is displayed. Incoming calls on the SIP trunks can ring a Main Business Number or an attendant extension.
   - *Main Business Number*: Enter the phone number of the site. External callers dial this number to place incoming calls on these SIP trunks.
     OR
   - Check the **Configure Incoming Call Handling** box.
   - Select **Auto Attendant** and enter the Hunt Group Extension number to be used for the voice mail system's auto attendant. Note that two voice mail extensions are used to support this service.

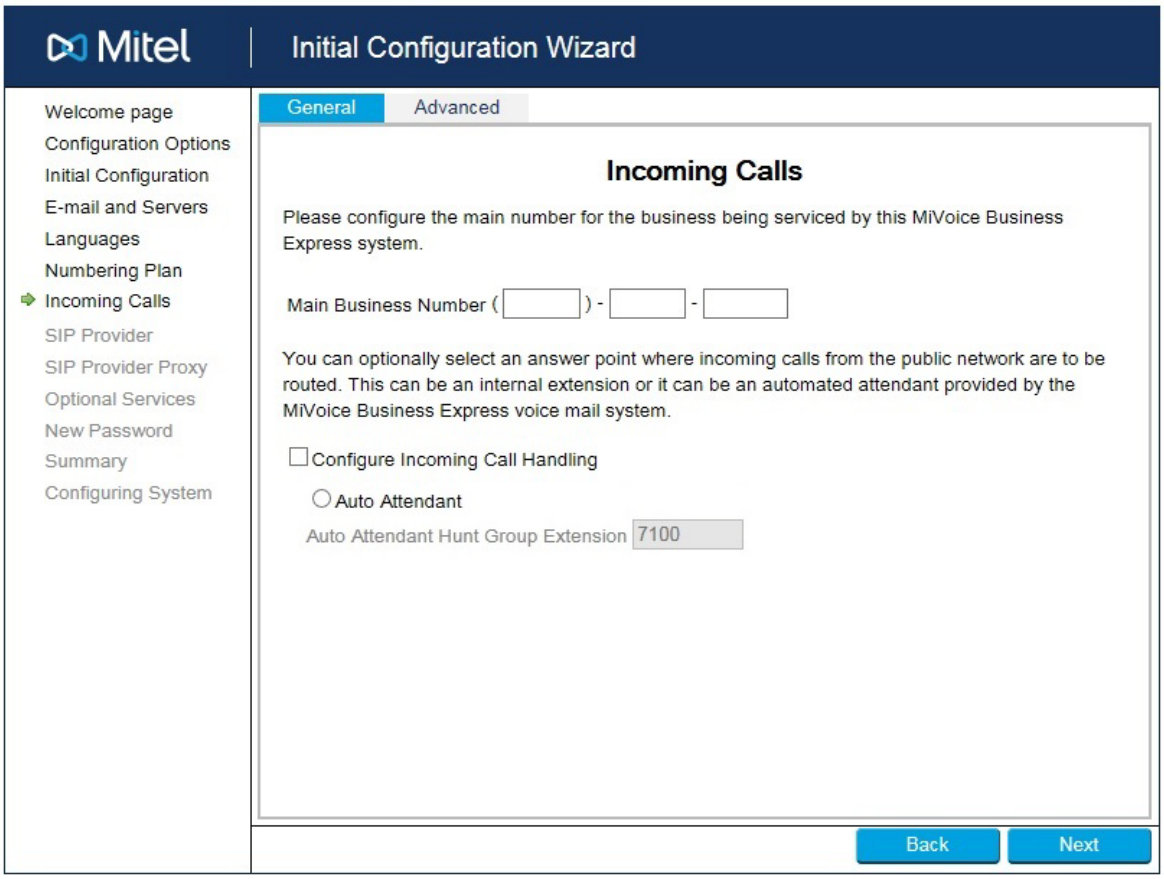

Figure 25: Incoming Calls

9. Click the **Advanced** tab**.** The Advanced Incoming Call Configuration Screen opens. To program Direct Inward Dialing (DID)/Direct Dialing Inwards to a range of directory numbers:
   - In the "Number of digits to absorb" field, enter the number of leading digits to remove from the incoming DID number. For example, to remove the entire DID number 613 592 5661, enter 10. Note that Dial-in trunks used as incoming trunks must always have an entry in the Absorb column. (You must enter "0" if no digits are to be absorbed. If you leave this field as Blank, calls will fail).
   - In the "Digits to insert" field, enter the actual digits to insert as leading digits to form a directory number (for example, 3333). For MiVoice Business Express systems, the maximum number of digits is 4. Both the Answer Point and Digit Modification columns are left blank if the trunk is outgoing only. If a Dial-In trunk does not require digit modification, enter "0" in the Absorb field and leave the Insert field blank. Note that the Extension field and the DID Digit Modification fields are mutually exclusive. If one option is completed, the other must be left blank.

Note: During user provisioning, you assign DID numbers to users in the Phone tab of the User and Services application.

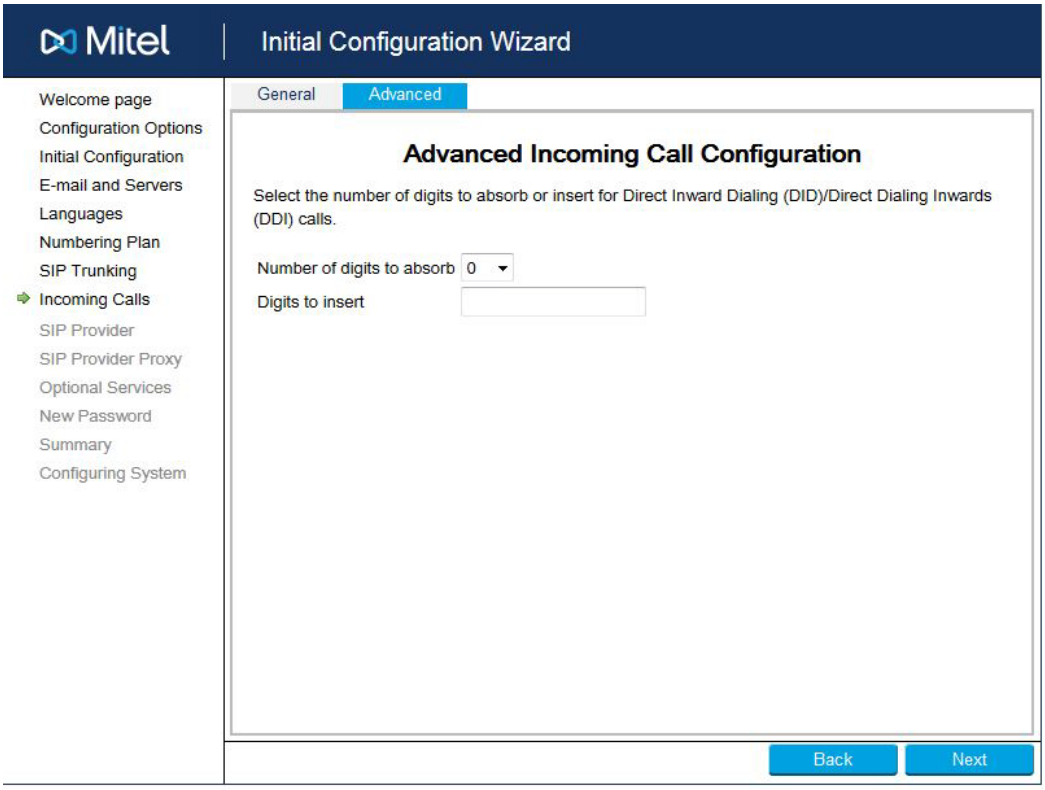

Figure 26: Advanced Incoming Call Configuration

10. Click **Next**. The SIP Provider screen is displayed. Complete the following:
    - *SIP Service Provider*: Select your Service Provider. The most common Service Providers for your region are listed in drop down menu for selection. A "Generic" SIP peer profile is available.You can also select "Custom Profile" and import a CSV file saved from the SIP Peer Profile form of the MiVoice Business System Administration Tool:

-Save a CSV file of a SIP Peer Profile. See “Obtain a Custom SIP Peer Profile (optional)” on page 54 for instructions.

-Select **Custom Profile** from the drop-down menu.

-Click **Browse** and navigate to the CSV file.

- *External Session Border Controller IP address or FQDN*: Enter the IP address or Fully Qualified Domain Name of the External Session Border Controller (proxy server) that is provided by your SIP Service Provider. Refer to the *MiVoice Business Express Engineering Guidelines* for a configuration diagram with an External Session Border Controller. Do not enter the IP address of the MiVoice Border Gateway in this field.
- *Number of SIP channels*: Displays the number of SIP channels licensed for the system.
- *Phone number(s) from Service Provider*: This field is optional. In cases where the FQDN/IP of an incoming call does not match the FQDN/IP address of the Service Provider specified above, the MiVoice Business system will not accept the call unless the number is included in this list. Enter one or more telephone numbers. The maximum number of digits per telephone number is 26. You can enter a mix of single numbers and number ranges (for example, 6135554500, 6135554000-6135554400). The entire field is limited to 60 characters.
- *Enable SIP Authentication*: If your SIP Provider requires authentication with a user-name and password, check this box to authenticate the Telephone Numbers that you entered in the field above. Enter the SIP Authentication username and password that you received from your SIP Provider.

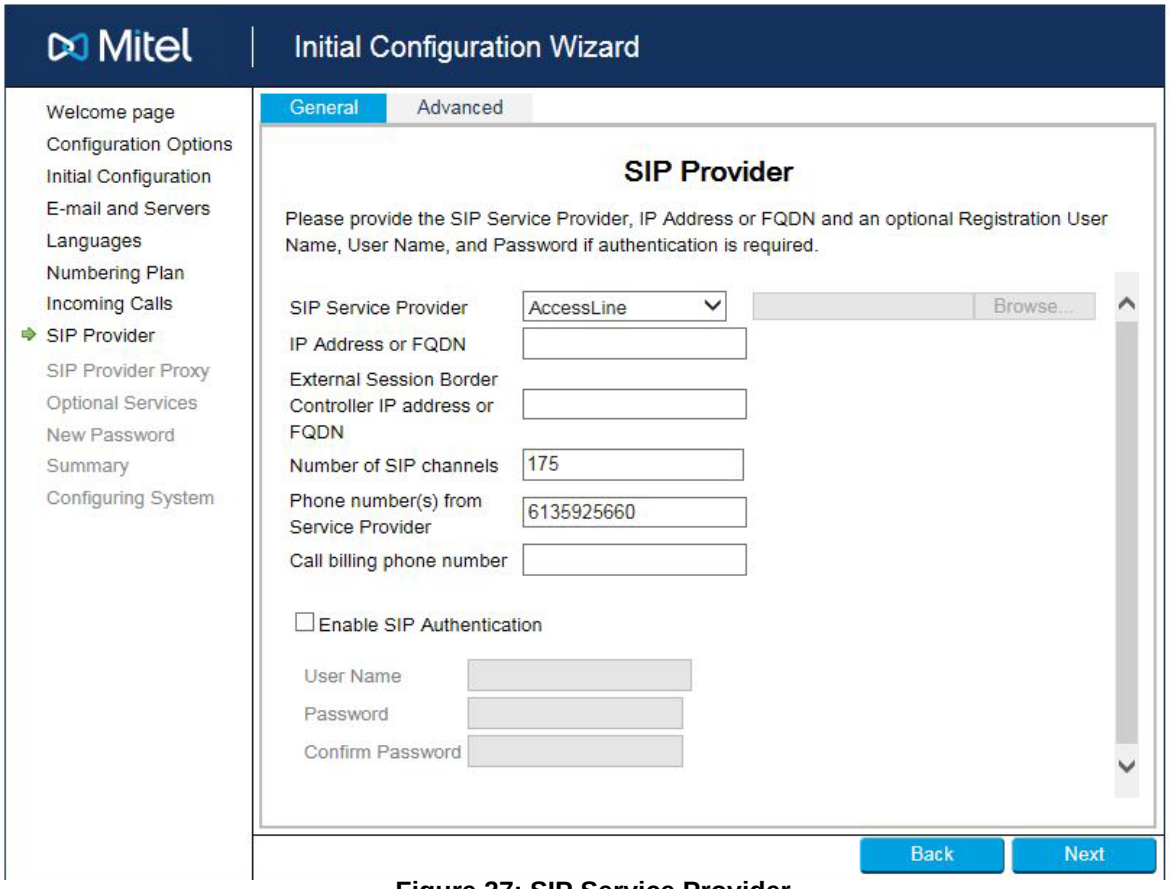

Figure 27: SIP Service Provider

11. Click the **Advanced** tab. Enter the following:
    - *Subscription User Name*
    - *Subscription Password*
    - *Subscription Password Confirmation*

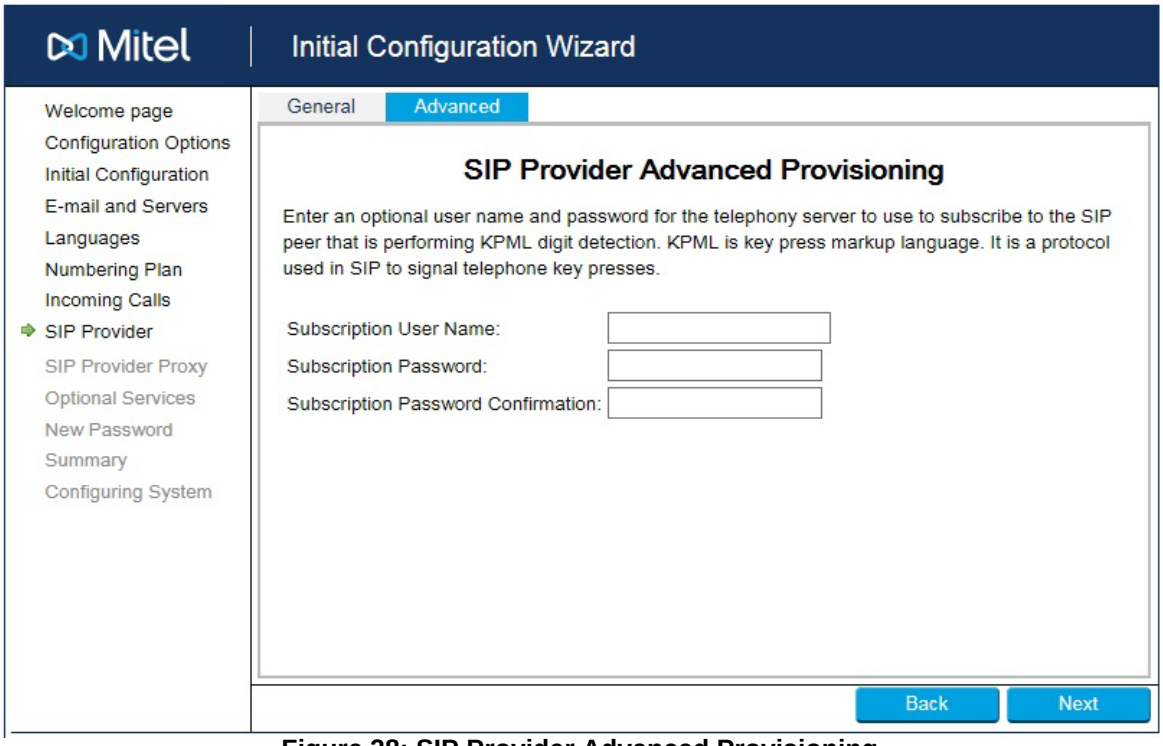

Figure 28: SIP Provider Advanced Provisioning

12. Click **Next**. The SIP Provider Proxy screen opens.
    - Refer to the *MiVoice Business Express Engineering Guidelines* for configuration diagrams of the supported SIP Trunk Proxy options.
    - Select a SIP Trunk Proxy option:

      -*Internal SIP Trunk Proxy*: Select this option if the SIP trunk proxy is supported internally on the MiVoice Business Express system.

      -*External SIP Trunk Proxy*: Select this option if the SIP trunk proxy is supported on a separate optional MiVoice Border Gateway (MBG). For this option, you must enter the addresses required to specify a route to the MBG.

      -*No SIP Trunk Proxy:* Select this option if a SIP trunk proxy is not required on the system.
    - Select the "SIP Service Provider or Proxy is on a different local network" option if either are located on a different local network. Enter the local network address, netmask, and network router address for the local network.

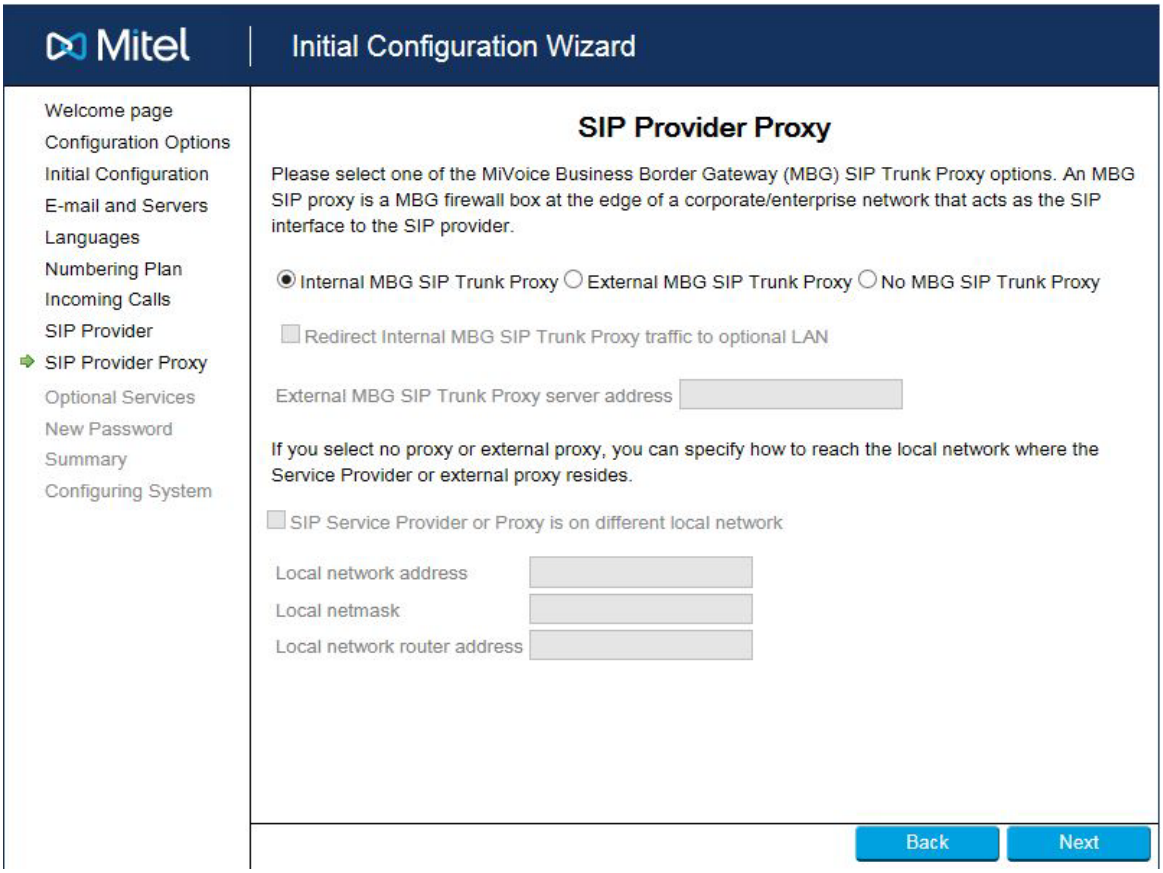

Figure 29: SIP Provider Proxy

13. Click **Next**. The Optional Services screen opens.

14. Select the desired optional services on the **Optional Services** tab and then click **Next**.

Note: Remote Access service is only available for Server Gateway mode.

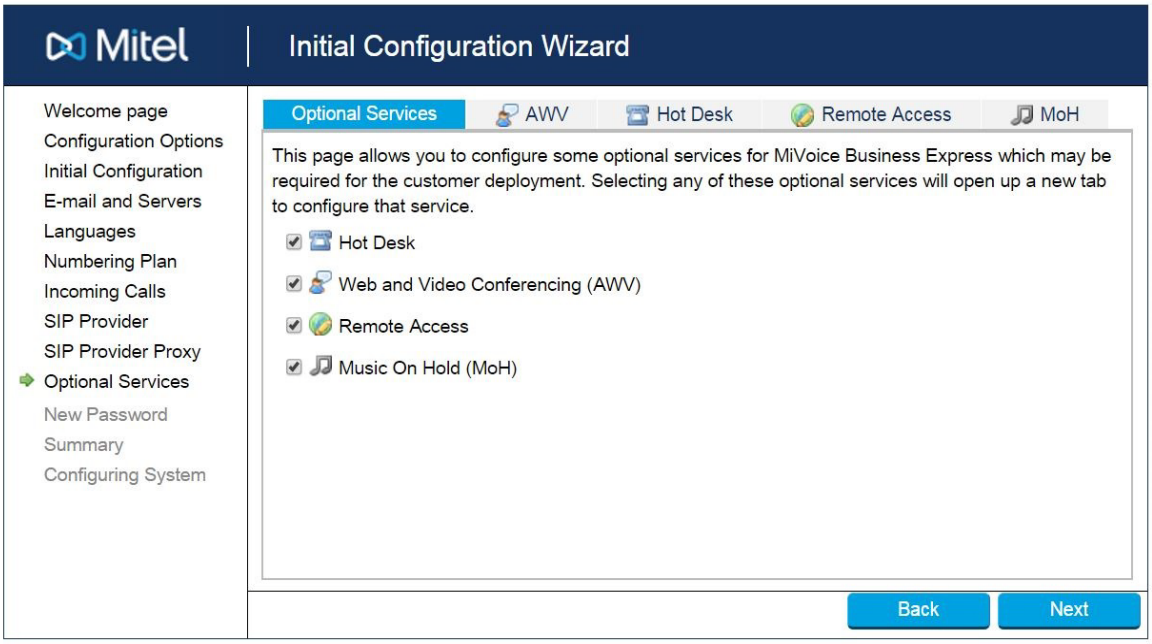

Figure 30: Configure Optional Services

15. For the hot desking feature, configure the hot desk enabled phones for the site. A hot desk user can log into any hot desk enabled phone and the system applies the user's profile to the phone:

- *Starting Extension*: Enter the starting extension number (default 2000) of the range of numbers that the system will assign to the hot desk enabled phones. The hot desk extensions must be different from the extension numbers that you entered in the Numbering Plan screen (that is, the numbers must not overlap).
- *Number of Devices*: Enter the number of phones that you want to support hot desking.
- *Extension Range*: This field displays the range of extension numbers that the wizard assigns to the hot desk devices.The extension numbers are assigned consecutively.

Note: Ensure that the selected extension range does not conflict with the system's dialing plan.

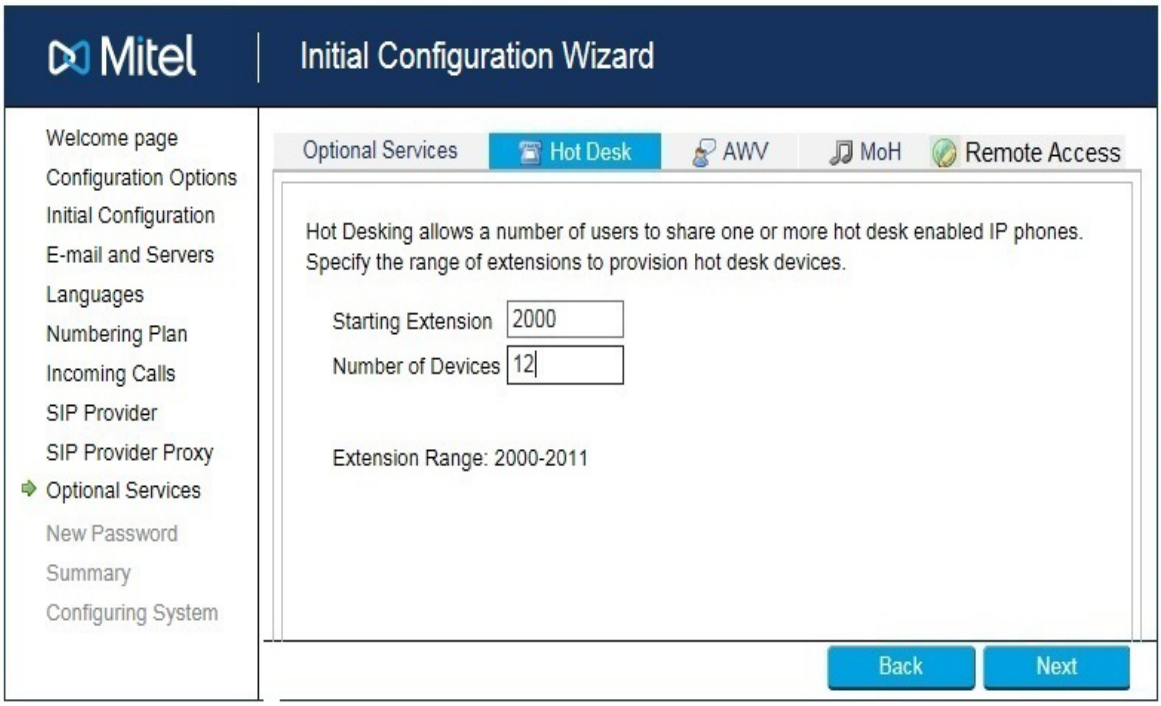

Figure 31: Hot Desking

16. Click **Next**. On the MiCollab AWV tab specify the following:

- *Conference Name (FQDN)*: Enter the Fully Qualified Domain Name (FQDN) of the MiCollab AWV server. To allow users to access AWV via the WAN, the FQDN must resolve to a public IP address that is externally accessible.The External MiCollab Web Conference FQDN Name cannot begin with a number. If the FQDN begins with a number, the Initial Configuration Wizard will fail to deploy the MiVoice Business Express appliance as MiCollab AWV will consider the FQDN invalid.
- *Conference WAN IP Address*: Enter the IP address that users will use to access the Web page of the MiCollab AWV interface. The address must be accessible to everyone who will be invited to attend a web conference, both inside and outside of your local network.
- *AWV Main Dial-In Number*: Enter the main dial-in number that you want to present to users in the conference email invite.
- *Direct Inward Dialing Number*: Enter the phone number that you obtain from your SIP service provider for accessing the AWV conference application. This number is mapped to the AWV conference hunt group in MiVoice Business.
- *AWV Toll Free Dial-In Number*: Enter the toll free dial-in number that you want to present to users in the conference email invite.

Note: The Initial Configuration automatically generates a SIP Password for the AWV SIP server. However, in order to provision additional AWV ports on the MiVoice Business, you must first clear the SIP Password from the following server manager page: Applications > Audio, Web and Video > Configuration > Configure SIP Server.

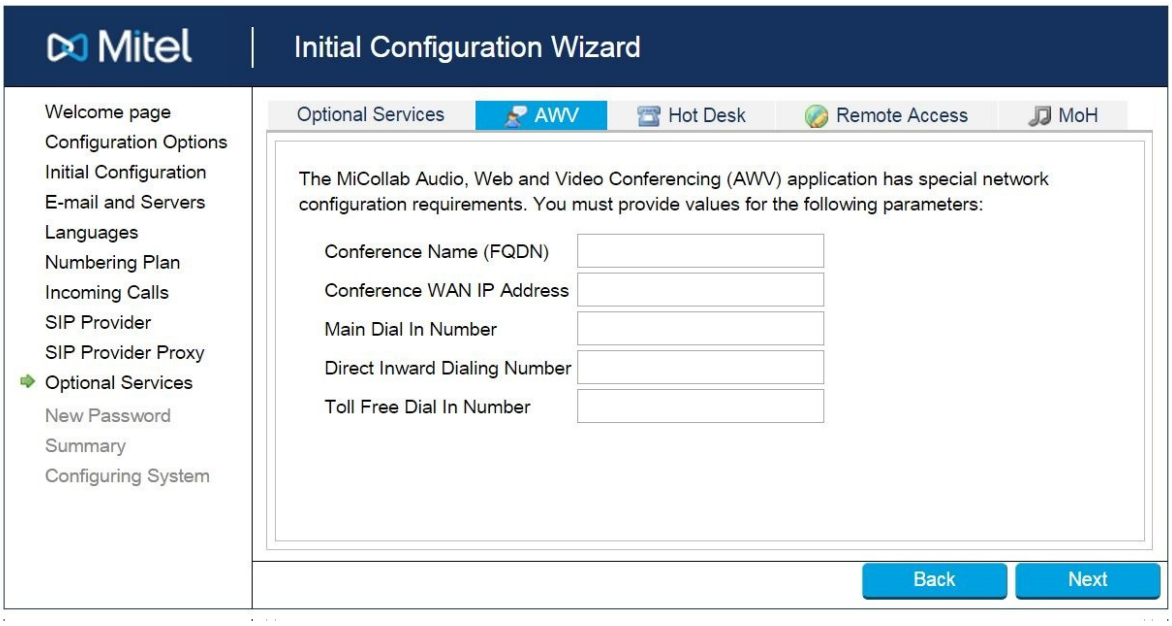

Figure 32: MiCollab AWV External Access

17. Click **Next**. The Configure Music on Hold tab is displayed. Browse to the file.

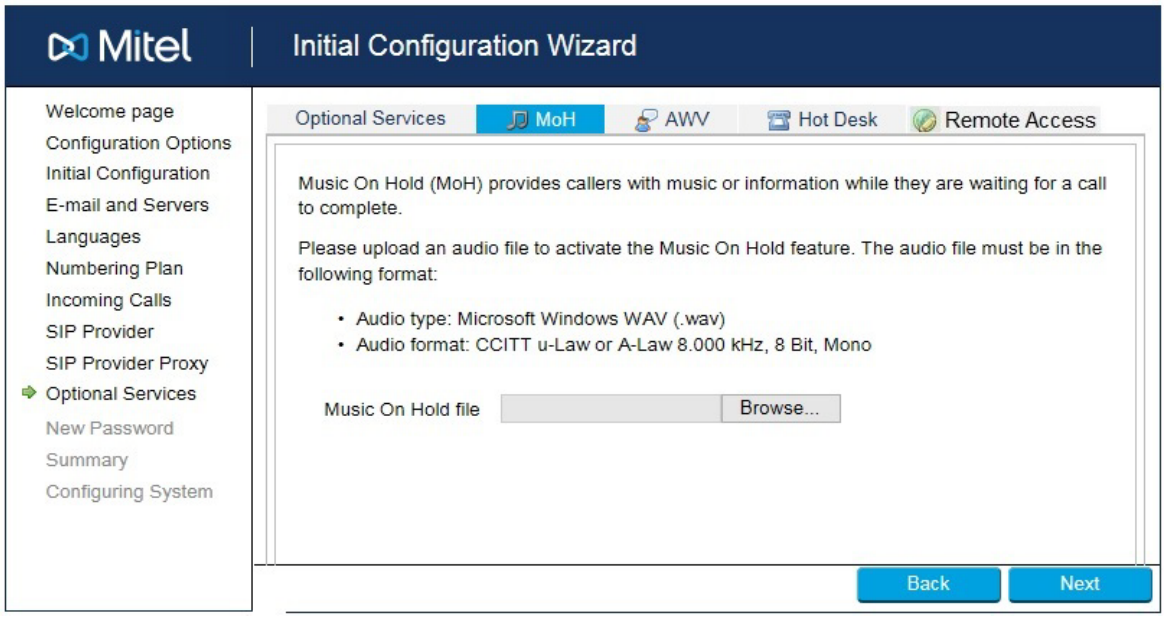

Figure 33: Configure Music on Hold

18. Click **Next**. The Remote Access tab is displayed.

- To allow remote access to the MiCollab server manager interface, check the **Configure Remote Access to MiCollab Server** box.
- Enter the network address and select the proper network bit mask. If you need to grant additional administrators with remote access, you can do so through the MiCollab server manager Remote Access panel.

- To allow remote access to telephony server (MiVoice Business) administration tools, check the **Configure Remote Access to Telephone Server** box.
- Click **Add User**, enter the required information and click **OK**. It is strongly recommended that you assign strong passwords. You can add up to five users.
- Enter the Telephony Server Management Web Interface FQDN.
- Resolve Telephony Server Management Web Interface FQDN either locally or via a LAN DNS server.

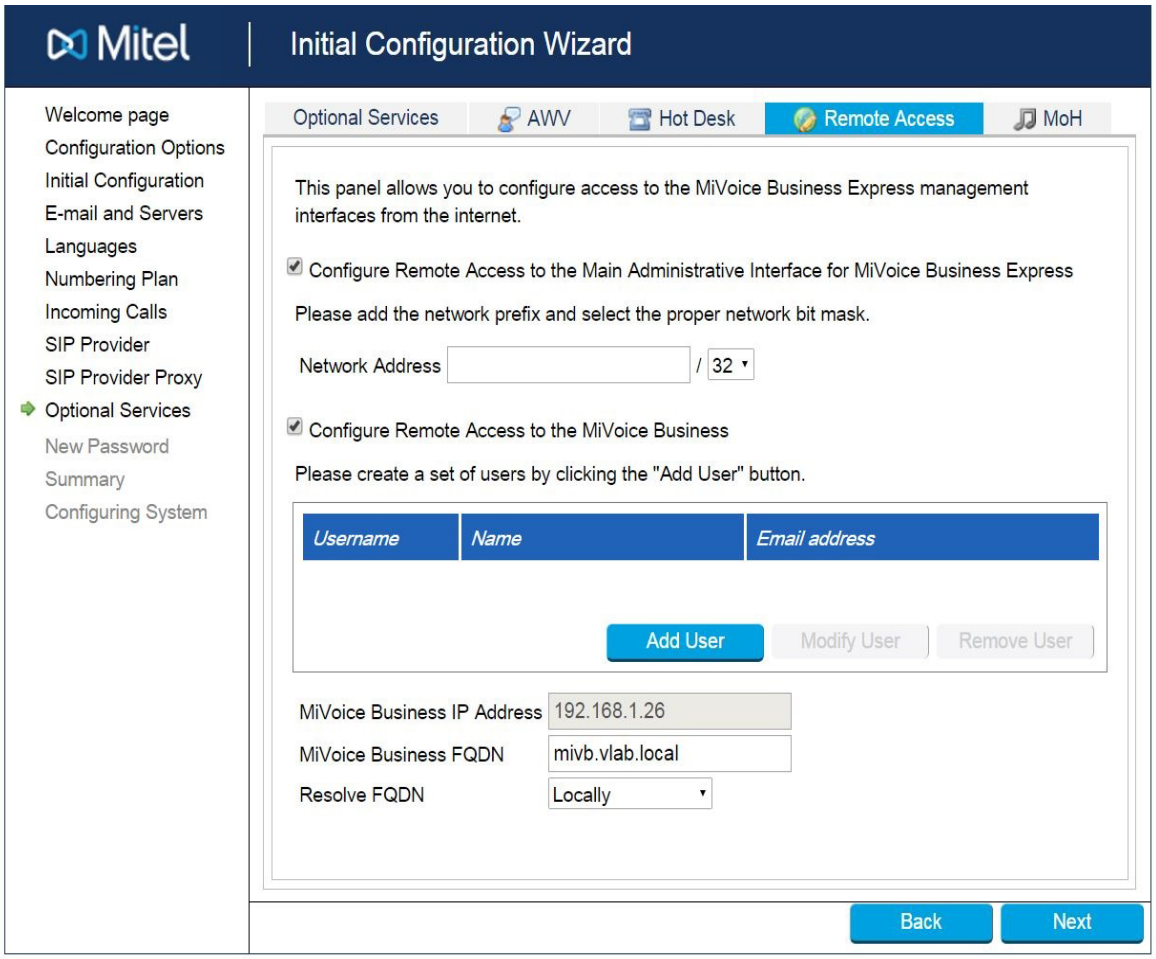

Figure 34: Configure Remote Access to Administration Tools

19. Click **Next**. Enter a new administrator password. This new password replaces the one that was used to access the wizard. It allows you to log into the MiCollab server manager interface and the MiVoice Business administration tools.

Note: This New Password is applied to the MiCollab server manager, MiCollab server console, and MiVoice Business administration tools. However, if you later change the password from a MiCollab administration interface, the change is not applied to the MiVoice Business administration tools. Likewise, if you change the password from the MiVoice Business System Administration tool, the change is not applied to the MiCollab administrator interfaces. This is because the MiCollab and MiVoice Business admin accounts are separate and independent.

Note: If you are deploying the OVA using vSphere directly on an ESXi host or if you are installing on a Hyper-V virtual machine, you will be prompted to provide an old password. Enter the administrator password that you created during initial deployment.

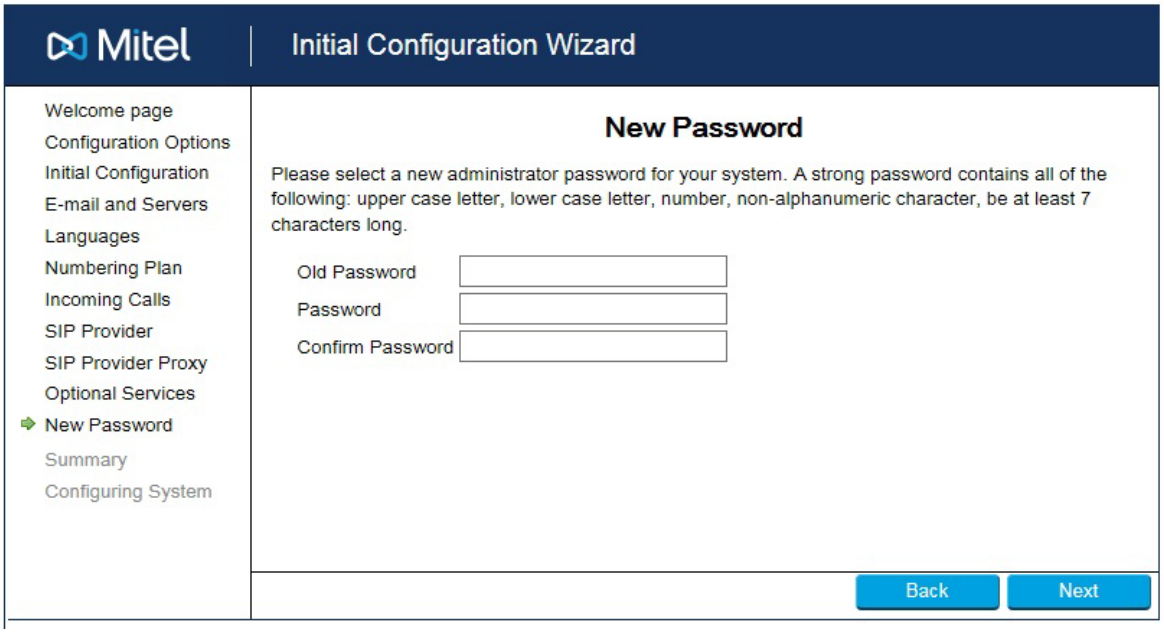

Figure 35: New Password

20. Click **Next**. Review the settings summary and click **Print** to obtain a copy. Ensure that you have entered your settings correctly before proceeding.

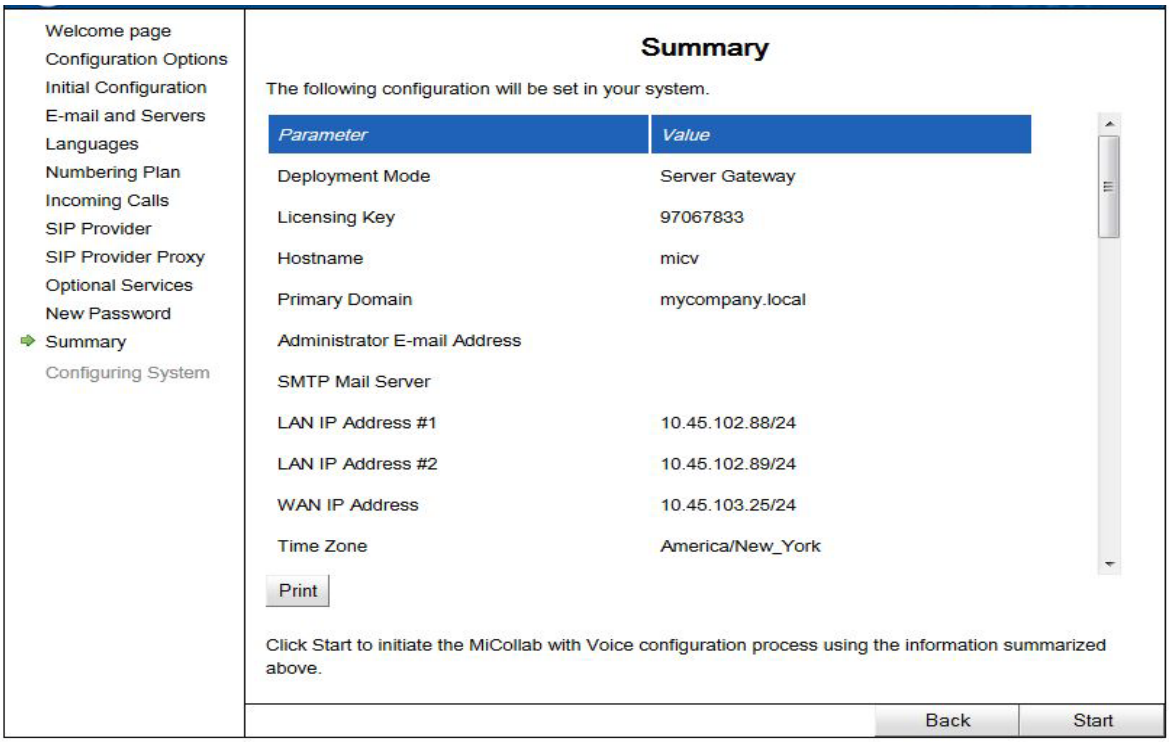

Figure 36: Summary screen

21. Click **Start**. The final screen displays the configuration progress.

WARNING:IT CAN TAKE UP TO 20 MINUTES FOR THE CONFIGURATION TO COMPLETE. WHILE CONFIGURATION IS IN PROGRESS, DO NOT EXIT YOUR BROWSER WINDOW.

22. Upon successful completion, a green check appears in the Status column for each of the listed operations. If the wizard fails to configure the system, check the logs to determine the issue. You must restart the wizard and re-enter your data correctly.

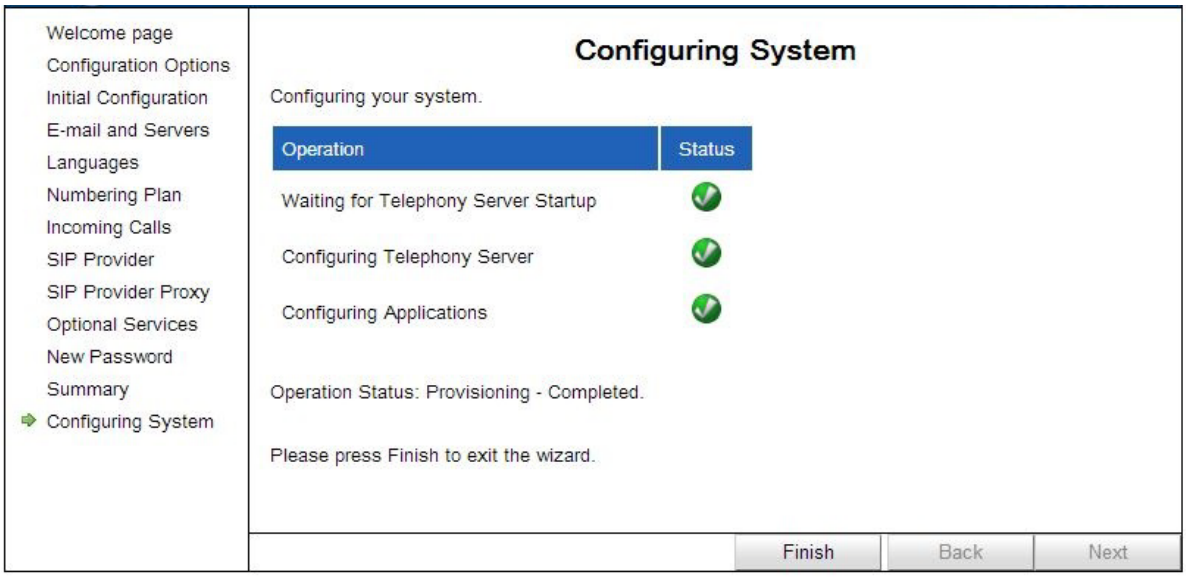

Figure 37: Configuring System

23. Click **Finish** and the MiCollab server manager interface is displayed.
24. Log into the MiCollab server manager and provision the MiCollab Network Element page with the MiVoice Business FQDN.
    - In MiCollab server manager, under **Applications**, click **Users and Services**
    - Click the **Network Elements** tab.
    - Select the MiVoice Business Network Element and click **Edit**.
    - Enter the MiVoice Business FQDN.
25. Synchronize the MiCollab Client server with MiCollab AWV software versions (required to support video):
    - In MiCollab server manager, under **Applications**, click **MiCollab Client Service**
    - Click **Configure MiCollab Client Service**.
    - Click the **Collaboration** tab.
    - Click the Local AWV Server link.
    - Click **Sync Now**. The MiCollab AWV Server and Client software versions are updated.
26. Configure the **MiCollab Client** dialing settings:
    - In the server manager, under **Applications**, click **MiCollab Client Service**
    - Click **Configure MiCollab Client Service**.
    - Click **Enterprise**.
    - Under **Settings**, click **Plus Dialing Settings**.
    - Enter the Country code, International access code, and Long distance access code, for your region.
    - Click **Apply**.
    - Click the **PBX Nodes** tab.
    - Under PBX Nodes, click the IP address or system name of the node.
    - Click **Default Dynamic Phone Status**.
    - Set both the "When I am on the phone:" field and "If I do not answer:" field to Voice Mail.
    - Click **Apply**.
27. Set the MiCollab AWV dialing code and prefix settings:
    - In the server manager, under **Applications**, click **Audio, Web and Video**.
    - Under **Configuration**, click **System Options**.
    - Click the **Collaboration** tab.
    - Enter the International Dialing Prefix, National Dialing Prefix, and Country Code for your region.
    - Click **Save**.
28. For countries other than North America, you must set the AWV Country Variant for the Country Tone Plan:
    - In the server manager, under **Applications**, click **Audio, Web and Video**.
    - Under **Configuration**, click **Country Tone Plan**.
    - Select the appropriate Country Variant. You can also upload custom tones. Refer to

the online help for instructions.

29. If your region was not fully supported by the wizard (you selected "Other" as your Country type) region-specific settings, such as Class of Restriction, Route Assignment, ARS, ARS Leading Digits, and so forth have not been configured. You must now configure these settings manually through the MiVoice Business System Administration tool, or export them from an existing MiVoice Business system and then import them into the MiVoice Business Express system. See “Import a Custom MiVoice Business Database” on page 99 for instructions.
30. Proceed to “Perform Advanced Configuration” on page 98.

ABOUT FLOW THROUGH PROVISIONING

Flow Through Provisioning keeps the following data synchronized between the MiVoice Business Express USP application database and the MiVoice Business system database:

- user and services data
- Programmable Ring Groups (PRGs)
- Multi-Device User Groups
- roles, and
- templates.

Any changes that you make to phone or application services in the USP application are distributed to the MiVoice Business system tool database and any changes made in the MiVoice Business system tool database are distributed to the USP application. Although data changes are distributed in both directions, the recommended practice is to perform all user and service provisioning from the MiCollab USP application.

Reach Through allows you to link (browse) directly from User and Services application pages to specific MiVoice Business programming forms. For example, you can reach-through from the User and Services Network Element tab to the Class of Service form to modify the MiVoice Business COS parameters. However. in a Cloud deployment, you cannot use the reach through functionality within the MiVoice Business Express MiVB application to access other MiVoice Business systems within a cluster and vice versa. This limitation exists because internal IP addresses are used in the URLs of the MiVoice Business systems instead of FQDNs.

To configure Flow Through Provisioning to an external MiVoice Business platform to support IP trunking or device resiliency, you must add the external MiVoice Business platform as an network element on the MiVoice Business Express. Then, start sharing from the MiVoice Business platform. See in the MiCollab server manager help for instructions.

Note: You must manually provision the MiVoice Business FQDN into the User and Services Network Element tab form after the initial provisioning or following a database restore.

PERFORM ADVANCED CONFIGURATION

The following functionality requires additional configuration in the application programming interfaces:

- Integrated Directory Services
- Direct Inward Dialing
- Customer Emergency Services IDs (CESID)
- Zones
- Advanced Unified Messaging
- Configure MSL DHCP Server.
- Deploy MiCollab for Mobile Clients

CAUTION: You must complete the Initial Configuration Wizard before you log into an MiVoice Business Administration session. The first time that you log into the MiVoice Business System Administration Tool, it prompts you to change your password. After you change the MiVoice Business System Administration Tool password, you will be unable to run the wizard.

Note: The Mitel Customer Documentation web site provides additional documentation for advanced configuration that is not covered in this section. See “About the Documentation Set” on page 4 for a list of the available documentation.

MANUAL CONFIGURATION FOR "OTHER" COUNTRY SETTING

You can modify a standard deployment to support country specific settings where the country is not natively supported by the MiVoice Business Express product.

1. Log into the MiVoice Business system administration tool.
2. Modify the necessary system and voice network configuration settings of the MiVoice Business to reflect the desired country settings: Automatic Route Selection table, COR, SIP Service Provider settings, and so forth, or import database files from an existing system that has the desired country specific settings (see “Import a Custom MiVoice Business Database” on page 99).
3. Back up the MiVoice Business database. Note that the MiVoice Business database MUST be backed up BEFORE you change the MiVoice Business country setting. Otherwise, you will lose your database changes.
4. Change the MiVoice Business Country Setting to the target country.
   - Access the **License and Options** form.
   - Under **Configuration Options**, change the **Country Setting** to the target country.
5. Restore the MiVoice Business database.
6. Log into the MiCollab server manager and change the MiCollab settings to the target country
   - Under **Configuration** click **MiCollab Language**.
   - Change the language to the target country. This will update the language for all the MiCollab applications.

- Under **Configuration**, click **Date and Time**.
- Set the System Timezone.

7. Log back into the MiVoice Business system administration interface and update the MiVoice Business timezone:
   - Click **System Properties**, click **System Settings**, click **Date and Time**.
   - Change the date and time settings to match the target country.
8. Complete any other required Advanced Configuration procedures.
9. Proceed to “Provision Users” on page 112

IMPORT A CUSTOM MIVOICE BUSINESS DATABASE

To import a customized MiVoice Business database into the MiVoice Business Express.

1. Log into the System Administration Tool of the MiVoice Business system that has the desired database.
2. Export the forms listed in Table 12 to CSV files. Refer to the System Administration Tool online help for export instructions.
3. Make the modifications indicated in Table 12 to the CSV files.
4. Log into the MiVoice Business System Administration Tool of the MiVoice Business Express system and import the CSV files. Import the files in the indicated order.

Table 12: Export and Customize MiVoice Business CSV Files

IMPORT ORDER	MIVOICE BUSINESS PROGRAMMING FORM/ CSV FILE	REQUIRED CHANGES PRIOR TO IMPORT. .
1	Class of Service	MiVoice Business Express uses COS 80 to 86 for the NuPoint Unified Messenger and MiCollab AWV hunt groups. If COS 80 to 86 are in use in the CSV import file, you must free up these COSs by assigning different, unused COS numbers to the groups or devices. See for “COS for Application Ports” on page 157 for default settings.
2	Feature Access Codes_blank.csv	You must blank out the current Feature Access Code values from the MiVoice Business database of the MiVoice Business Express before you can import the Feature Access Codes CSV file. Import the Feature Access Codes_blank.csv to blank out the codes.
3	Feature Access Codes	No changes required
4	System Options Assignment	
5	Class of Restriction Groups	
6	ARS Digit Modification Plans	
7	Route Assignment	Change the SIP Peer Profile name to "Sipsp" and delete Routes 7 to 9 prior to importing this form

Table 12: Export and Customize MiVoice Business CSV Files

IMPORT ORDER	MIVOICE BUSINESS PROGRAMMING FORM/ CSV FILE	REQUIRED CHANGES PRIOR TO IMPORT. .
8	Route List	No changes required
9	ARS Maximum Dialed Digits	
10	ARS Digits Dialed	
11	Multiline Advisory Messages	
12	SIP Device Capabilities	
13	SMDR Options	
14	SNMP Configuration	
15	User Authorization	

5. Set the desired default Class of Services (COS) in the MiCollab application:
   - Log into the Server Manager and launch the Users and Services application.
   - Click the **Network Element** tab.
   - Select the **System Name** of the MiVoice Business and click **Edit**.
   - Under System Properties, modify the COS settings and click **Save**.
6. Provision users on the system. See “Provision Users” on page 112.
7. Assign the Class of Restriction (COR) for each user to the required setting (by default, MiCollab applies COR 2). See “Configure MSL DHCP Server” on page 107 for instructions.

CONFIGURE INTEGRATED DIRECTORY SERVICES

You can integrate the user database of a corporate directory service with the MiVoice Business Express database to minimize data entry and administration. The user data on the corporate directory server is synchronized with the MiVoice Business Express database using Lightweight Directory Access Protocol (LDAP). If single point provisioning is enabled, then the user data is also distributed to the MiVoice Business. Synchronization occurs in one direction only—from the directory server to MiVoice Business Express.

1. Log into the server.
2. Under **Configuration** click **Integrated Directory Services**.
3. Follow the instructions in the Integrated Directory Services (IDS) online help.

Note: For information on performing LDAP Search Queries, go to the following URL: http://technet.microsoft.com/en-us/library/aa996205(v=exchg.65).aspx

PROVISION CESIDS

A Customer Emergency Services ID (CESID) is used to provide location information for a phone extension on a private network, when a caller makes an emergency call. The information can

help direct emergency crews to a caller's location. CESID programming and maintenance is a required component of Emergency Services.

CESIDs are public network Listed Directory Numbers (LDNs) that you obtain from your local carrier or SIP Service Provider. When an emergency call is made, the system sends the CESID of the extension out to the PSTN. The CESID is used by the service provider to route the call to the local Public Safety Answering Point (PSAP) and then by the PSAP to call up information such as the address, building, floor, area, and call-back number.

- CESIDs can be manually or automatically updated to maintain current CESID information in the system.
- CESIDs and their assigned location information are stored in an Automatic Location Information (ALI) database.
- CESIDs are not dialable numbers and the data contained in them is only used for out-bound Emergency calls. CESID numbers are never displayed to a third party during a routine call.

For MiVoice Business Express, the default CESID is the main business number for the system.

Note: Different state or provincial regulations may govern the CESID requirements at your location. Some require a unique CESID for every telephone, and others allow the sharing of CESIDs if the telephone users are within sight of one another. One dialable call-back number is required for each CESID.

COORDINATING CESIDS WITH THE ALI DATABASE

The CESID sent to the PSAP to identify the location of the emergency caller must be the same number that resides in the Automatic Location Information (ALI) database for that location. The ALI database is independent of the MiVoice Business and may reside at the local PSAP, at the telephone company Central Office, or at an independent location. It is essential that CESID numbers and the ALI database remain synchronized when moves, adds, and changes take place. Any changes made to a user's location or data associated with a CESID must be communicated to the ALI database administrator. Ensure that local changes affecting ALI information are kept from going into service until the ALI database has been updated. The System Administrator must ensure that CESID related changes are communicated to the ALI database. A minimum of one L2 connectivity detection protocol (STP, or CDP) must be uniformly and consistently configured on all the L2 switches that the devices are connected to. The administrator must define the same protocol of choice for every MiVoice Business in the network.

CESID CONDITIONS

- CESIDs are not associated with location independent entities such as ACD agents and regular Hot Desk users. If an ACD agent or regular Hot Desk user makes an emergency services call, the CESID associated with the originating set is sent.
- For EHDUs logged on to private trunks (such as a Suite EHDU), the CESID associated with the user’s mobile DN is sent. For EHDUs logged on to public trunks (such as cell phones), the external party’s public number is sent as the CESID. For EHDUs logged in over public trunks that provide no calling line identification, the EHDU configured external number is sent as the CESID.

Note: An EHDU external number configured with *, # or P characters cannot be used for the CESID. For EHDUs logged in internally (such as a Minet device), the CESID associated with the originating set is sent.

- Class of Restriction and Interconnect Restrictions remain in effect for emergency services calls. Specific users may be restricted from accessing the designated Emergency Services number.
- SMDR output is changed in the event of an emergency services call; the prime directory number of the originating station is output.

AUTOMATIC CESID UPDATING

The following conditions apply to automatic CESID updating:

- Automatic CESID updating is not supported on hubs where multiple devices report connectivity to the same L2 port, or on L2 switches that do not have STP or CDP enabled. The system detects and logs this condition upon device registration.
- The MiVoice Business portion of the Mitel Emergency Services solution does not support handling of "special circumstance" DNs. Some DN users have special needs: for example, a DN may be associated with a wheelchair user or with an area where dangerous chemicals are stored. The PSAP may have a record associating a user or DN with this type of special circumstance. If such a device is moved, the MiVoice Business treats it like any other device move and attempts to automatically update the CESID Assignment form. This causes the PSAP database to be out of sync with the MiVoice Business. To avoid this situation, the administrator should ensure that such DNs are not moved.
- Automatic CESID updating does not function during a database backup or restore.
- A log is generated if the system detects a conflict between STP and CDP data.

Automatic CESID updating should not be enabled for

- Devices in Teleworker mode or devices that are connected outside of the corporate firewall. 911 calls placed from such devices may report an incorrect CESID, or may be outside of the PSAP's coverage area. Devices are not compatible with the Mitel Emergency Services solution when they are operating outside the corporate network serviced by the MiVoice Business. The reasons are as follows:
  - A Teleworker device operating outside the corporate network may or may not trigger a device move;
  - The system will not be able to accurately assign a CESID to such a device outside the network;
  - The MiVoice Business will not be able to route the 911 correctly. Note that the system will not block Teleworker devices from making 911 calls. However, it is not recommended that users make 911 calls from devices operating in Teleworker mode outside the corporate firewall. It is best if the administrator changes the CESID Updating state manually for Teleworker enabled devices.
- Generic SIP phones
- MiCollab Client softphones. MiCollab Client softphones cannot detect L2 connectivity data.

CESID PROGRAMMING GUIDELINES

Defining default zone CESIDs - You can define a default CESID for each zone in the network. This will allow the system to identify the location of the caller, when an emergency call is routed to a different zone and no CESID is available for the calling DN.

911 and CESID - For a 911 call to be compliant with FCC guidelines, the call must report a CESID to the PSAP. At a minimum, you must define a CESID for each DN in the MiVoice Business CESID Assignment form. In order to ensure that CESIDs are updated when a device is moved and can be correctly reported to the PSAP, you must promptly investigate and address all CESID-related alarms. You may have to return a phone to its original location if the move was not authorized or update the CESID Assignment and/or L2 to CESID Mapping forms. Alternatively, you can update the "L2 to CESID Mapping" form in advance of a device move.

Defining the primary protocol - Carefully consider the difference between the protocols (STP and CDP), and designate one as your primary protocol. Remember that the L2 STP Port Identifier may not correspond to the physical port number on the L2 switch (with VLANs, the L2 port number may be virtual). You designate a primary protocol for Detecting IP Device Moves in the CESID Assignment form.

Switching between CDP and STP in the network - The system may detect a false device move if the primary protocol is changed while a device is connected to an L2 switch.

Enabling Layer 2 (L2) protocol - Ensure that all L2 switches in the network have the primary protocol enabled. If there is an L2 switch that does not have the protocol enabled, devices may move from one port to another on that switch and the system will be unable to detect the device move because no L2 data will be reported.

New installations - In a new MiVoice Business Express installation scenario it is recommended that you allow the system to auto-discover the L2 Port MAC and L2 Port, as devices are registered, rather than manually entering the information. Auto-discovery ensures that the values are correct (particularly for VLANs), while manual entry can be prone to error. After the information has been auto-discovered, you can go into the CESID Assignment form or the L2 to CESID Mapping form and enter the CESID for each entry. You may also want to go to other network drops where a phone might be moved to and allow the device to register there as well so that the ports can be auto-discovered. Note that any network drops that do not have a Mitel IP device connected to them will remain undiscovered by the MiVoice Business. You can either wait for a CESID alarm to be generated when a device connects to an unknown L2 port, or you can pro actively auto-discover L2 data by plugging devices into L2 ports.

Upgrades - When you restore a database that contains accurate and complete CESID assignments, the L2 to CESID mapping for known devices will be fully and automatically discovered upon device registration. For this to happen, the CESID Assignment data must be accurate prior to the backup and upgrade.

Backup and restore - Device move detection, automatic CESID updating, and alarming do not function during a database backup or restore. This is because all database files needed to detect device moves and update CESIDs are locked during a backup and restore. For this reason, you should perform backups and restores during times when devices are least likely to be moved. To ensure that no devices are moved, it may be helpful to notify users of backups and restores and instruct them not to move devices, if possible, during these times.

Maintaining CESID Logs - The CESID Logs form overwrites data, from the oldest to newest entries, after 5000 CESID logs have been posted. If you wish to have traceability of the logs, perform regular database backups, or print or export this information.

Replacing L2 switches - If an L2 switch is replaced in the network (for example, a non-functional switch is replaced with a new one), the MiVoice Business recognizes the event as a device move after the sets re-register through the new L2 switch (because the sets are reporting a new L2 connectivity point). Assuming that no new L2 to CESID mappings were manually created for the new switch, the system clears the CESID values in the CESID Assignment form (only for the devices registered to the new L2 switch) and raises a CESID alarm.

Therefore, when a switch is replaced (old with new), you must reprogram the CESID assignments for the sets that were connected to the replacement switch. Also, you must delete the old L2 to CESID mappings for the replaced switch, because they are no longer relevant. Alternately, you may wish to set the DNs connected to the retiring L2 switch to Manual CESID updating (as opposed to Automatic - see CESID Assignment form), to prevent the CESIDs from being deleted.

Another replacement scenario is when two L2 switches are swapped in the network. Again, the MiVoice Business and IP devices register this swap as device moves, even though it was the switches that were moved and not the devices. In this case, the system automatically updates the CESID Assignment for each moved device (assuming that CESID Assignment was complete prior to the swap). The problem here is that the automatic CESID updating will likely be inaccurate because the L2 swapping will cause the L2 to CESID mapping to become incorrect. For this reason, it is recommended that you delete the CESID assignments before swapping the L2 switches, update the L2 to CESID mapping, and then allow the correct CESID assignments to be auto-discovered.

Retiring an L2 switch - When an L2 switch is retired, delete the relevant entries from the L2 to CESID mapping form, since these are no longer being used.

Physically moving a network drop - For automatic CESID updating, the system will not be able to detect when a network drop is physically moved from one location to another (assuming the L2 port connection point remains the same). You should be wary of any physical port location changes (for example, those done during a re-wiring project). It may happen that if a network drop is physically moved, it will move into a location serviced by a different CESID. It is the system administrator's responsibility to ensure that network drops aren't moved without permission, and to update CESIDs when they are.

Connecting IP devices to a hub - It is recommended that devices be connected directly to an L2 switch. Avoid connecting IP devices to a hub that is, in turn, connected to an L2 switch. Apart from Quality of Service reasons, IP devices connected directly to a hub will all report the same L2 Port MAC/Port, and the system will not be able to automatically update the CESID for any devices registering to that hub.

Swapping Ethernet cables on an L2 switch - It is recommended that you do not swap Ethernet cables on L2 switches (for example, when troubleshooting a malfunctioning port). The system will see this switch as a device move. The device will report a new L2 connectivity point, even though it was not physically moved. Depending on the configuration, this could result in an automatic CESID update (likely with the wrong CESID), a CESID alarm, or the deletion of the device's CESID. If you must swap Ethernet cables on an L2 switch, be aware of the effect this will have on device detection and CESID assignment.

Addressing CESID alarms and logs - If a device is moved, and the system is unable to assign a CESID to the device at its new location, the system will raise an alarm, and log the problem. The user should monitor the system alarms for such an event, and when it occurs, use the logs, the CESID Assignment form, the L2 to CESID Mapping, and/or the Device Connectivity forms to determine the nature of the problem. Once the problem is understood, you should update the CESID Assignment or L2 to CESID Mapping form. This will ensure that the device has the correct CESID and will clear the alarm once all CESIDs have been assigned (for DNs in Automatic CESID Handling mode.)

Teleworkers - Mitel IP devices that are running in Teleworker mode and are connected outside the corporate network through the Mitel Standard Linux (MSL) gateway will not be blocked from making 911 calls, however an incorrect CESID may be reported.

ASSIGNING CESIDS

You can assign CESIDs to each directory number (DN) on your network, using the MiVoice Business CESID Assignment form:

1. Log into the MiVoice Business System Administration tool. See “Logging into the MiVoice Business Tools” on page 125.
2. Choose to view forms alphabetically.
3. In the left forms menu, select **CESID Assignment**.
4. Assign a CESID number to each primary extension number. The MAC address of the Layer 2 switch port and the Layer 2 switch port identifier are detected by the system when an IP phone registers.
   - *CESID*: Enter the CESID to be sent to the PSAP in the event of an emergency call. Up to 12 digits can be programmed.
   - *CESID Comments*: Enter location information for the person at this extension.
   - *CESID Updating*: Leave setting to "Automatic".
   - *Route Emergency Calls*: Leave setting at "Through System Only".

Note: Automatic CESID updating should not be enabled for devices in Teleworker mode or devices that are connected outside of the corporate firewall. Emergency calls placed from such devices may report an incorrect CESID, or may be outside of the PSAP's coverage area. Devices are not compatible with the Mitel Emergency Services solution when they are operating outside the corporate network serviced by the MiVoice Business.

CESID ALARMS AND LOGS

For information on CESID alarms and logs:

1. Log into the MiVoice Business System Administration tool. See “Logging into the MiVoice Business Tools” on page 125.
2. Click the  help button in the top right of the System Administration Tool interface. The System Administration Tool help opens.
3. In the table of contents, click **System Applications**, click **General Business Solutions**, click **Emergency Services**, click **CESID Support** and then click **CESID logs**.

CONFIGURE NETWORK ZONES

Network zones are used for bandwidth management, compression, location based routing, and emergency services. Zone 2 is reserved for SIP Trunking.

- For specific MiVoice Business Express zone configuration information, refer to the MiVoice Business Engineering Guidelines.
- For general instructions on how to configure network zones:
  - Log into the System Administration tool. See “Logging into the MiVoice Business Tools” on page 125.
  - Choose to view forms alphabetically.
  - In the left forms menu, select **Network Zones**.

CONFIGURE UNIFIED MESSAGING (UM)

Unified Messaging (UM) allows you to integrate your NuPoint Unified Messaging voice mail system with your e-mail client for increased access to messages. When you assign an Entry, Standard, or Premium UCC license to a user, both Standard and Advanced UM are supported.

INTEGRATE NUPOINT APPLICATION WITH MAIL SERVER

You must integrate the MiVoice Business Express NuPoint Unified Messaging application with the external mail server (Exchange, Lotus Domino, or Google Apps).

1. Log into the MiCollab Server manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 124).
2. Under **Applications**, click **NuPoint Web Console**.
3. Click the  help button in the top right of the user interface. The NP-UM Web help opens.
4. In the table of contents, click **Optional Features**, click **Unified Messaging**.
5. Follow the instructions to configure Standard and Unified Messaging.

ASSIGN USERS WITH UNIFIED MESSAGING

All users who are assigned with UCC Entry, Standard, or Premium licenses support Standard and Advanced Unified Messaging by default:

1. Log into the MiCollab server manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 124).
2. Under **Applications**, click **Users and Services**.
3. In the directory list, select the user and click **Edit**.
4. Click **NuPoint Unified Messaging**.
5. Assign a mailbox to the user. The default Feature COS 14 enables Standard and Advanced Unified Messaging. The Standard and Advanced Unified Messaging check boxes are selected by default.
6. Click **Save**.

7. Unified Messaging users can configure the encoding format for their audio files on the Settings tab of their Web View interface.

CONFIGURE MSL DHCP SERVER

To configure the internal MSL DHCP server to support devices on the LAN:

1. Log into the MiCollab server manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 124).
2. Under **Configuration**, click **DHCP**.
3. Click the **DHCP Service** tab.
4. Click **Edit**.
   - Check the **Enable DHCP Service** and **Allow BootP boxes**.
   - Click **Update**.
5. Click the **Subnets** tab.
   - Click Add Subnet.
   - Enter the Name, Subnet IP address, and Subnet Mask of the subnet.
   - Click **Save**.
   - Click Add Range.
   - In the Range start field, enter the IP address at the start of the range.
   - In the Range end field, enter the IP address at which to end the range.
   - In the Lease time field, enter the number of seconds to hold DHCP leases or accept the default setting.
   - Click **Save**.
6. Click the **Options** tab.
   - Click Add Option.
   - Set Scope to "Subnet".
   - Click **Standard Option**. Set the option field to "3 routers".
   - Click **Next**.
   - In the Value field, enter the local gateway IP address.
   - Click **Save**.

DEPLOY MICOLLAB FOR MOBILE CLIENTS

MiCollab Client 8.0 introduces a new blade (MiCollab Client Deployment) which allows for the simplified deployment of the MiCollab for Mobile application. This solution is supported in integrated and co-located MiCollab Client deployments.

1. Log into the MiCollab server manager
2. Under **Applications**, click **MiCollab Client Deployment**.
3. Refer to“MiCollab Client Deployment” on page 171 and the associated online help for deployment instructions.

CONFIGURE OPTIONAL STANDALONE VMBGS

You can deploy and configure separate optional standalone vMBGs to

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

See the *MiVoice Border Gateway Installation and Maintenance Guide* on the Mitel Customer Documentation web site at http://edocs.mitel.com for installation instructions.

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.

DEPLOY VMBG IN SERVER-ONLY MODE

1. Log into 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. This address SHOULD be:
   - dedicated to the MBG solution
   - private
   - reachable only from the internal network.
3. Log into the vMBG server manager.
4. Under **Applications**, click **MiVoice Border Gateway**.
5. On the **Configuration** tab, click **Network Profiles**.
6. Select **Server-only configuration** on the network LAN.
7. Select **Apply LAN configuration**.

When configuration is complete, the system will use the LAN address of the server for both the set-side and ICP-side streaming addresses of the MBG. The following diagram provides an example of a "Server-only configuration on the network LAN":

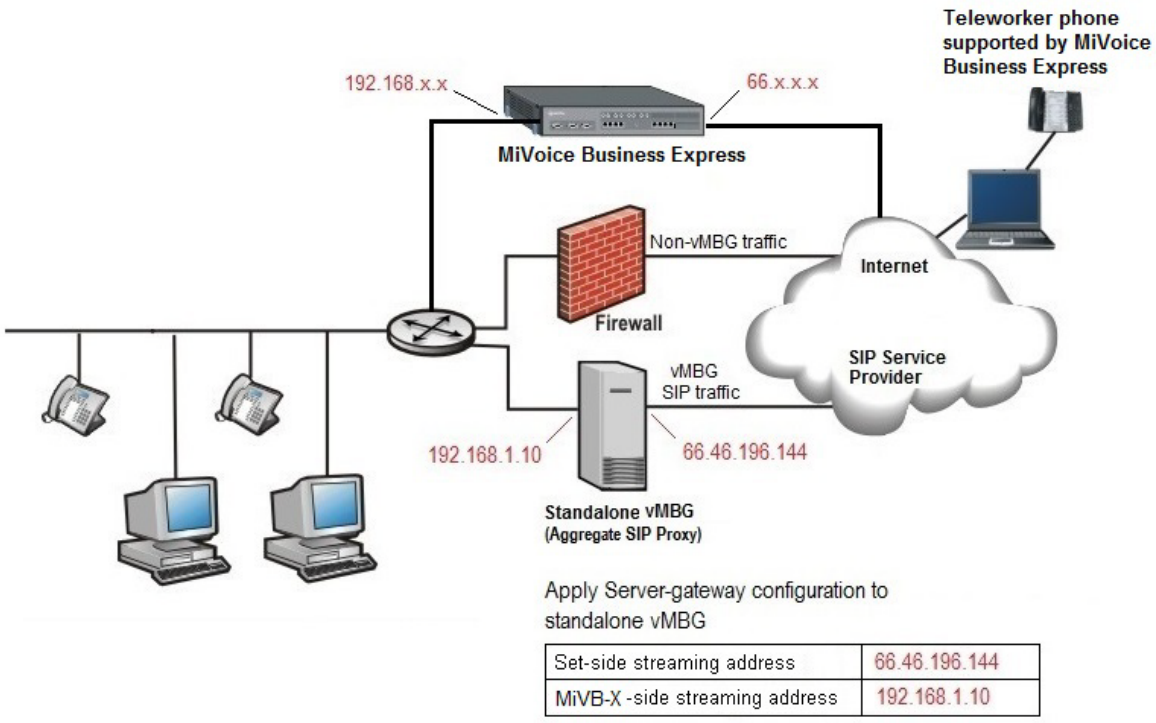

Figure 38: Standalone vMBG for Secure Call Recording

CONFIGURE SECURE RECORDING CONNECTOR

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

SIP TRUNK AGGREGATION

If your hosted infrastructure has multiple MiVoice Business Express 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 Express systems via the vMBG SIP Trunking web proxy services.

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

DEPLOY VMBG IN SERVER-GATEWAY MODE

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

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

5. Access the vMBG server manager.
6. On the **Configuration** tab, click **Network Profiles**.
7. Select **Server-gateway configuration on the network edge**.
8. Select **Apply Server-Gateway configuration**.

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

- ICP-side (MiVoice Business Express-side) streaming address = LAN interface address
- Set-side streaming address = WAN interface address

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

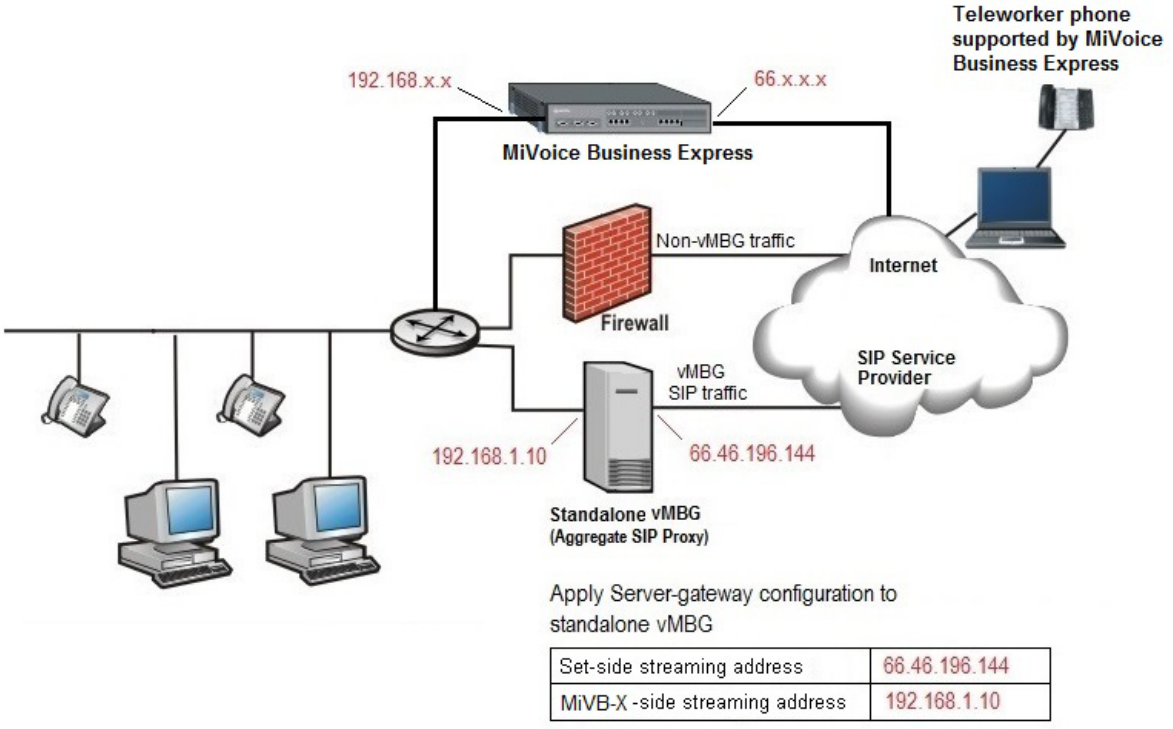

Figure 39: Standalone vMBG for SIP Trunk Aggregation

CONFIGURE SIP TRUNKS

For Hosted UCaaS Provider deployments, a separate external standalone vMGB can be added to provide SIP trunking resources. The SIP trunking is consolidated on the standalone vMBG

and provides the trunking capacity for multiple customers; all trunks come to one location and the incoming calls are routed to the appropriate MiVoice Business in each customer's MiVoice Business Express virtual appliance.

The IP addresses shown in are used as examples to illustrate the required configuration on the vMBG. In the following example, a SIP trunk is programmed for each customer.

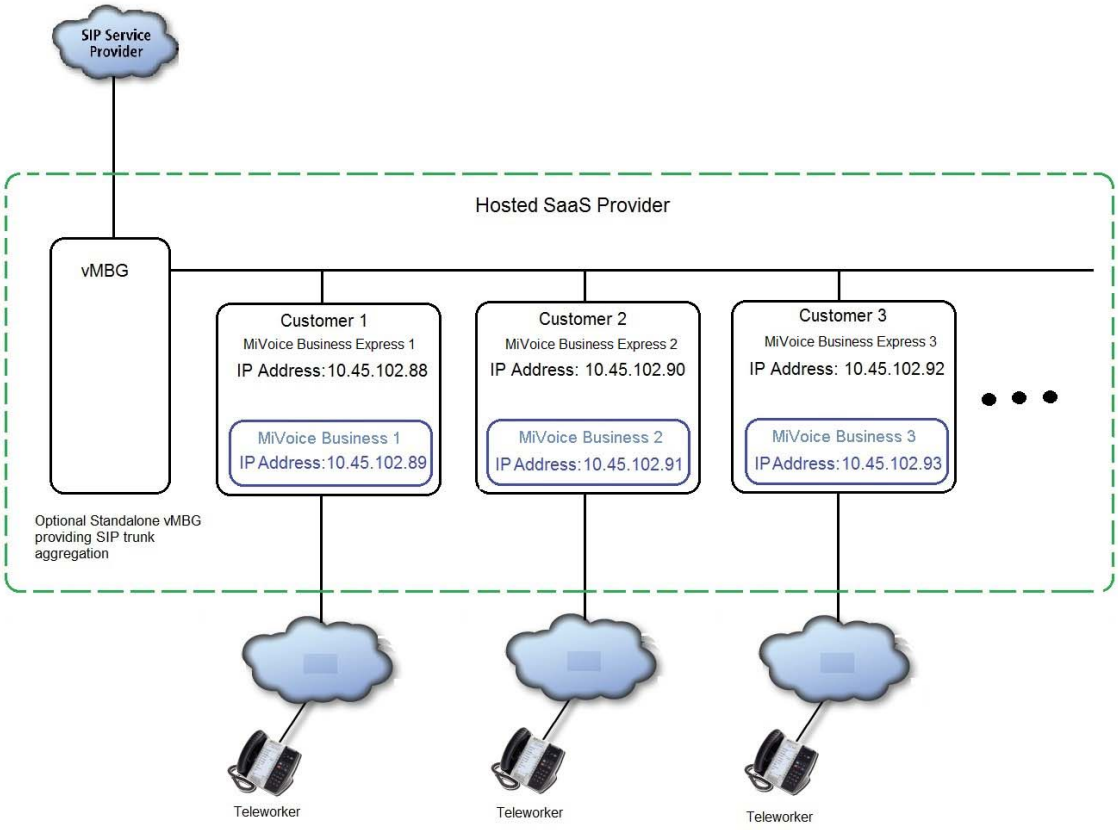

Figure 40: SIP Aggregate Trunking - Example IP Addresses

To configure SIP trunk aggregation:

1. Log into the standalone vMBG server manager.
2. Under **Applications**, click **MiVoice Border Gateway**.
3. Program the vMiVoice Business for each customer into the ICPs screen:
   - Click the **Configuration** tab.
   - Click the **ICPs** tab.
   - Click the Add ICP link to add the vMiVoice Business into the screen. Refer to the online help for field descriptions and additional information. Figure 41 shows an example of the ICP Configuration screen.
   - Click **Save**.

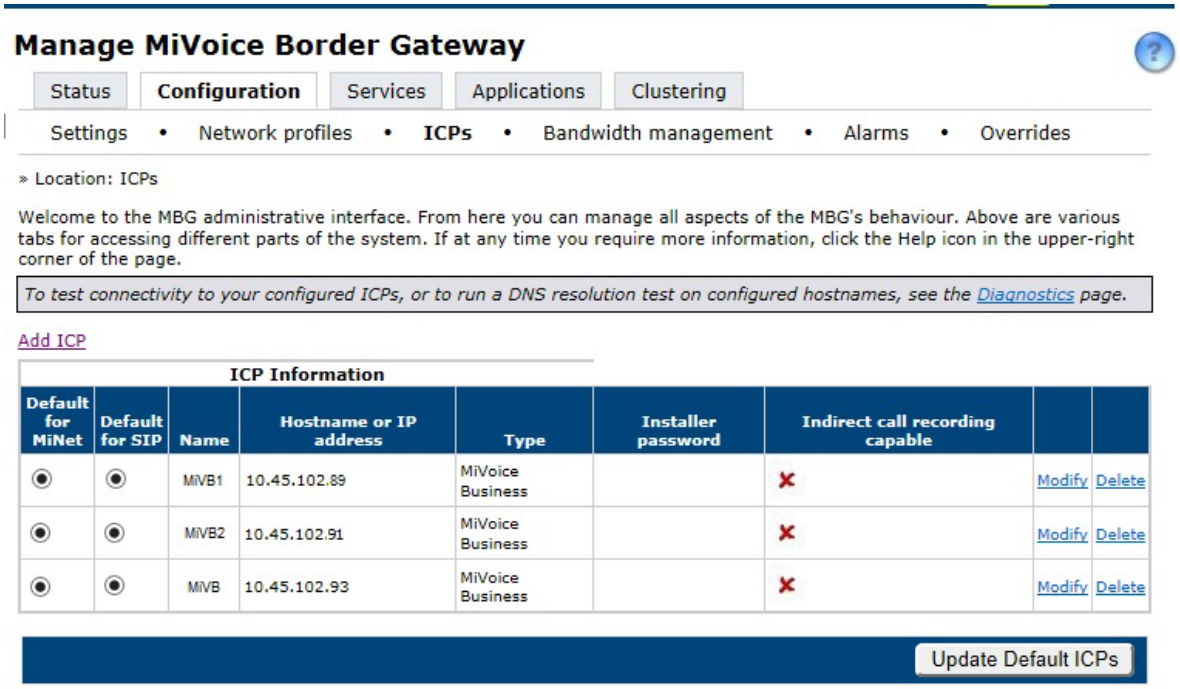

Figure 41: ICP Configuration (Example)

4. Program SIP trunks to connect to the MiVoice Business of the MiVoice Business Express:
   - Click the **Configuration** tab.
   - Click the **Services** tab.
   - Click the Add a SIP trunk link to add a connection. Refer to the online help for field descriptions and additional information. Note that you must enter the MiVoice Business IP address (not the MiVoice Business Express IP address) in the "Remote trunk endpoint address" field.
   - Click **Save**.

PROVISION USERS

Depending on your site configuration, use one of the following methods to provision users on the MiVoice Business Express system.

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

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.

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. See “Logging into the Server Manager (Administrator Portal)” on page 124)
3. Under **Applications**, click **Users and Services**.
4. From the Users and Services application, define roles and user templates. See the Manage Roles and Templates book in the USP application online help for instructions. You have the option of using the default roles and templates provided by the system.

Note: The Message Waiting Indicator (MWI) is not automatically setup if a default UCC Template is used to provision a user. It is recommended that you create custom UCC templates based on the default UCC templates and modify them to use the Message Waiting method required by the customer site. Selectable Message Waiting methods for Message Waiting #1 and #2 include:

- DTMF to PBX
- Pager
- Program RS232
- Centrex RS232
- HIS PMS
- Unified Integration
- Hitachi PMS
- MiTAI Messaging

MiTAI Messaging is recommended as the messaging option as other methods will consume additional Voicemail ports.

5. Import users using the Bulk User Provisioning Tool in the User and Services application.
6. Assign the UCC licenses to users through the Users and Services application. See Managing UCC licenses in the USP online help for instructions.

SYNC USER DATABASE WITH ACTIVE DIRECTORY SERVICE

To sync the user database with an Active Directory server:

1. Log into the MiCollab server manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 124)
2. Under **Applications**, click **Users and Services**.

3. From the Users and Services application, define roles and templates. See the Manage Roles and Templates book in the USP application online help for instructions. You have the option of using the default roles and templates provided by the system.
4. Sync the databases by performing an initial synchronization.
5. Resolve any detained or failed updates.

PROVISION USERS MANUALLY

To provision users manually:

1. Log into the MiCollab server manager portal. See “Logging into the Server Manager (Administrator Portal)” on page 124)
2. Under **Applications**, click **Users and Services**.
3. From the Users and Services application, create the users and assign services. See the Manual Provisioning topic in the USP application online help for instructions.

PROVISIONING DID FOR USERS (OVERVIEW)

This section provides an explanation of how DIDs are provision for MiVoice Business Express 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.

PERFORM BACKUPS

After you complete MiVoice Business Express advanced configuration, perform the following backups:

- Backup the MiVoice Business Express database (see “Server Manager Backup” on page 121)
- For deployments in a VMware environment, backup the MiVoice Business Express virtual appliance using VMware Applications (see page 123)
- Backup the optional vMBG. Refer to the vMBG server manager online help for instructions.

Chapter 8

MAINTAIN

MAINTENANCE OVERVIEW

Regular maintenance tasks include:

- ☐ “Performing Upgrades” on page 115
- ☐ “Performing Backups” on page 121
- ☐ “Converting From Business to Enterprise” on page 124

PERFORMING UPGRADES

An upgrade is when you move a MiVoice Business Express system software up to a new release:

- A major upgrade installs a new release of software, for example:
  - from Release 7.0.x to Release 8.0 x, or
  - from Release 7.3.x to Release 8.0.x
- For deployments on VMware, you must deploy a new OVA file to perform a major upgrade (for example, from Release 7.0 to 8.0). You cannot upgrade VMware deployments from the MiCollab server manager **Install Applications** panel.
- A service pack upgrade installs new version of software within the same release (for example, from Release 7.0 SP1 to Release 7.0 SP2)

Note: There are no upgrade paths from existing Mitel products (for example MiCollab, MiCollab Virtual Appliance, MiVoice Business, or vMiVoice Business) to MiVoice Business Express.

PREREQUISITES

For major upgrades:

- ❒ The system must be able to connect to the AMC over the internet.
- ❒ The new MiVoice Business Express must be deployed on the same network as the current MiVoice Business Express. You must configure the new MiVoice Business Express with a temporary IP address to allow the backup to be restored from the current MiVoice Business Express system.
- ❒ All administrative applications on MiVoice Business Express are closed.

- ❒ Perform major upgrades outside of business hours. Ensure that the system is NOT processing calls during a major upgrade.
- ❒ Ensure that the virtual appliance has the required resources.

For service pack upgrades:

- ❒ The system must be able to connect to the AMC over the internet.

MAJOR UPGRADES

The upgrade procedure is very similar to the install procedure. You simply deploy the new OVA file (VMware) or install the system software (Hyper-V) and then run the Initial Configuration Wizard. From the wizard, restore the system database from a backup file on a network share. The system will be taken out of service during the restore process.

1. Convert your UCC User licenses. See “When you upgrade to MiVoice Business Express 7.0, UCC v3 Entry, Standard, and Premium licenses are upgraded to UCC v4 licenses. However, the number of external hot desk licenses that were provided by the UCC v3 Entry licenses remains the same.” on page 62.
2. Log into the MiCollab server manager. Under **Administration**, click **Backup**. Back up the MiVoice Business Express database to a network drive.
3. Shut down the current Release 5.0.x or Release 6.0.x MiVoice Business Express.

Note: If you are deploying/installing with new IP Addresses, you don't need to shut down the current MiVoice Business Express until just before you start the restore.

4. Install the system software:

   For VMware virtualized environments:

   - Download the new MiVoice Business Express vApp (OVA file) and deploy it on the host system.
   - In the Custom Template screen, set the Country and Telecom Region fields. You can leave the Timezone blank. It will be restored from your database backup.
   - Leave the Hostname, Domain Name, and ARID fields blank. This information will also be restored from your database backup.
   - If you are restoring the database from a Network Share, you must enter the LAN IP Address and Netmask, a WAN IP Address and Netmask, and a Gateway IP Address**. You must assign the LAN and WAN IP addresses to different networks**.
     OR
     If you are restoring from the current MiVoice Business Express, enter a new, temporary IP address in the LAN IP Address field. This address must available on the local LAN and be different than the one used by the current virtual appliance. The temporary IP address will be replaced by the original address during the restore.
   - Click **Next** to proceed with vApp deployment.
   - Right-click on the newly created MiVoice Business Express (for example: MiVoice Business Express 8.0.0.40 build) and select **Open Console**. The MiVoice Business Express console opens within the vSphere Client.
   - Power on the MiVoice Business Express vApp by clicking the green button in the toolbar.

   For Hyper-V virtualized environments:

   - Create a new virtual machine.
   - Restore your database backup to apply your existing ARID.
   - Download and install the new MiVoice Business Express application software (ISOs) on the virtual machine. See “Install on Microsoft Hyper-V” on page 67.

- Power on the MiVoice Business Express system.

5. On a PC on the same subnet as the MiVoice Business Express open your browser and enter the following in the address bar to launch the Initial Configuration Wizard:
   https://*<LAN IP Address of the MiVoice Business Express>*

Note: If you are using a temporary IP address, ensure that the current MiVoice Business Express virtual appliance is shut down before you proceed with the restore.

6. In the Initial Configuration Wizard:
   - Click **Next** to display the **Configurations Options** page.
   - Click **Restore the configuration data from backup file**.
   - Navigate to the backup file.
   - If the backup file is encrypted, you must enter and confirm the Encryption Password to proceed. The filename for an encrypted backup ends with ".aes256".
   - Click **Next**.
7. During the restore process, do not access the Users and Services application until the restore completes.

Note: Flow Through Provisioning is enabled automatically during the upgrade.

8. Log into the MiCollab server manager and provision the MiCollab Network Element page with the MiVoice Business FQDN:
   - In MiCollab server manager, under **Applications**, click **Users and Services**
   - Click the **Network Elements** tab.
   - Select the MiVoice Business Network Element and click **Edit**.
   - Enter the MiVoice Business FQDN.
   - Enter 2 for the Call Reroute First Alternative number.
9. Access the MiVoice Business platform System Administration Tool and program CRFA index number 2 with the NuPoint voicemail hunt group number.
   - Reach Through to the MiVoice Business System Administration Tool.
     or
     Log into the MiVoice Business platform and then click **System Administration Tool**.
   - In the top left corner of the System Administration screen, select **View Alphabetically**.
   - Select **Call Rerouting First Alternatives** from the list of forms. This form allows you to set the call routing when the called DID number is busy or has set Do Not Disturb. The "Normal" setting routes the call to busy or reorder tone; the "This" setting routes the call to the directory number entered in the last column; the "Last" setting routes the call to the corresponding index entry in the Call Rerouting Second Alternatives form.
   - Select First Alternative Number 2.

Figure 42: Call Rerouting First Alternatives Form

- Click **Change** and set the call rerouting options and NuPoint voicemail hunt group extension number (Default 7000) as shown below.

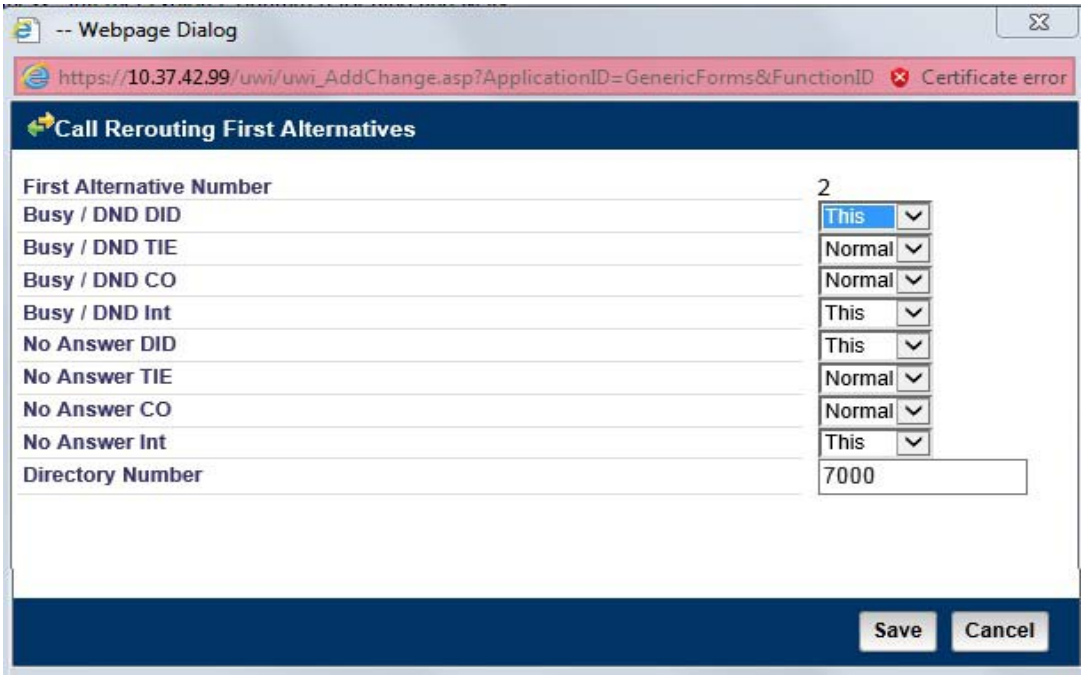

Figure 43: Set Call Rerouting Options

- Click **Save**.

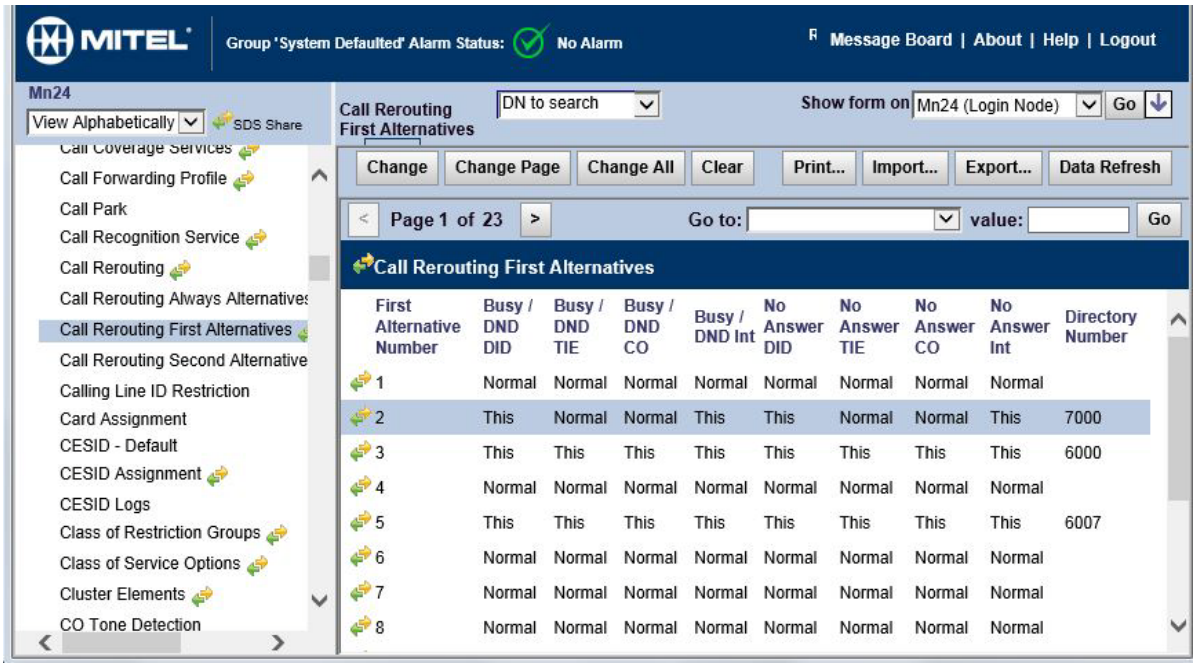

Figure 44: Call Rerouting First Alternatives

10. Synchronize the MiCollab Client server with MiCollab AWV software versions (required to support video):
    - In MiCollab server manager, under **Applications**, click **MiCollab Client Service**.
    - Click **Configure MiCollab Client Service**.
    - Click the **Collaboration** tab.
    - Click the Local AWV Server link.
    - Click **Sync Now**. The MiCollab AWV Server and Client software versions are updated.

SERVICE PACK UPGRADES

You can perform service pack upgrades from the MiCollab server manager **Install and Upgrade Software** panel. Perform a backup from the server-manager prior to doing the upgrade. Refer to the Online Help for instructions.

UPGRADING APPLICATIONS SUITE LICENSES

To purchase and activate additional UCC licenses:

1. Contact Mitel Customer Services (or your Service Provider) and place your order.
2. Obtain your Application Record ID from Mitel Customer Services.
3. In your AMC account, access the appropriate Application Record and assign the upgrade products from your license account to the Application Record. Assign any MiVoice Business User and Device licenses to the MiVoice Business ICP Application Record. The AMC upgrades your licenses on its hourly synchronization.

4. Access the server manager. See “Logging into the Server Manager (Administrator Portal)” on page 124.
5. Under **ServiceLink**, click **Status**.
6. Click the **Sync** button to download your AMC license upgrades. UCC licenses are applied automatically during the synchronization.

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 Express 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 Express OVA file.

Notes:

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 Express 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 Express database and the vMBG database at the same time.
3. Installations on Hyper-V only support the MSL Server Manager Backup method.

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 page 124 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.

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 7:

1. Right-click on the desktop and select **New** and then select **Folder**.
2. Name the folder, for example: "MiVoice Business Express Backups".
3. Right-click on the folder and select **Properties**.
4. Click the **Sharing** tab.
5. Click **Share**.
6. Select "Everyone" 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 Express 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 Express/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**.

BACKUPS USING VMWARE APPLICATIONS

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

CONVERTING FROM BUSINESS TO ENTERPRISE

To convert a MiVB Express Release 7.0 or later system from Business to Enterprise.

1. Log into the Application Management Center.
2. Click **Register a License**.
3. Enter a Reference number (Purchase Order number).
4. Click **+** to expand the MiVoice Business Express Products.
5. Select 1 Part Number 54006840 "Convert MiV Bus Express to Enterprise".
6. Click **Next**.
7. Click **Confirm**.
8. Under **Tasks**, click **Assign a License**.
9. Enter the Customer Name in the Name field and then click **Retrieve**.
10. Click **+** beside the customer's ID.
11. Select the option button next to the MiVB Express ULM ARID and then click **Assign**.
12. Enter the Purchase order number in the Search Criteria and click **Retrieve**.
13. Click **+** to expand the Purchase Order.
14. Assign Part Number 54006840 to the MiVB ULM ARID.
15. Click **Assign**.
16. Click **Confirm** to assign the license.
17. Click **Done**.
18. Log into the server manager, access the **Status** page and click **Sync** to sync the MiCollab Business Express server with the AMC.
19. Under **Applications**, click **MiVoice Business**. Check the MIVB status to determine when the system has been updated with the new license.
20. Under **Administration**, click **Shutdown or Reconfigure**. Reboot the system.

COMMON SYSTEM ADMINISTRATION TASKS

LOGGING INTO THE SERVER MANAGER (ADMINISTRATOR PORTAL)

The MiVoice Business Express 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 - allow you to configure and administer the installed applications (for example NuPoint Unified Messenger).

Web browser access to MiVoice Business Express administration and end-user interfaces is provided through

- Internet Explorer 9, 10, or 11
- 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 Express server, open a browser and enter the following URL in the address bar:
   https://*<IP Address of the MiVoice Business Express>*/server-manager

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

2. Enter User Name (default is "admin") and the system Password that you created during installation, and then click **Login**. The administrator portal opens.
3. Do one of the following:
   - In the left-hand menu, under **Applications**, click an application name to open the interface of that application.
   - Click the **Help** link in the administrator portal for detailed server administration instructions.
4. By default, MiCollab is configured to send a Welcome E-mail to new users. The e-mail contains:
   - a link to the MiCollab End User portal, and
   - the user's login ID, password, and passcode

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

   If you choose to disable the Service Information E-mail functionality, you will need to advise users of the URL for the MiCollab End User portal:
   https://*<IP Address of the MiVoice Business Express>*/portal
5. Proceed to "Installing a Web Certificate" on page 127.

LOGGING INTO THE MIVOICE BUSINESS TOOLS

The MiVoice Business includes a number of Embedded System Management (ESM) programming tools:

- **System Administration Tool** that provides a Web-based interface that trained technicians use to program the system.

- **Group Administration Tool** that provides a Web-based interface to enable administrators to make changes to user information.
- **Desktop Tool** that provides a Web-based interface to enable display IP telephone users to program feature keys on their phone.

Note: You can reach through directly from the User and Services application interface to the MiVoice Business System Administration tool without having to log in to the MiVoice Business system.

OBTAIN MIVOICE BUSINESS SYSTEM IP ADDRESS

1. Log into the Server Manager (see page 124).
2. Under **Applications**, click **MiVoice Business**.
3. Record the MiVoice Business System IP Address.

LOGGING INTO THE TOOLS

To log into one of the ESM tools:

1. Launch a browser and enter the URL of the MiVoice Business system: https://<System IP Address>. The login screen opens.

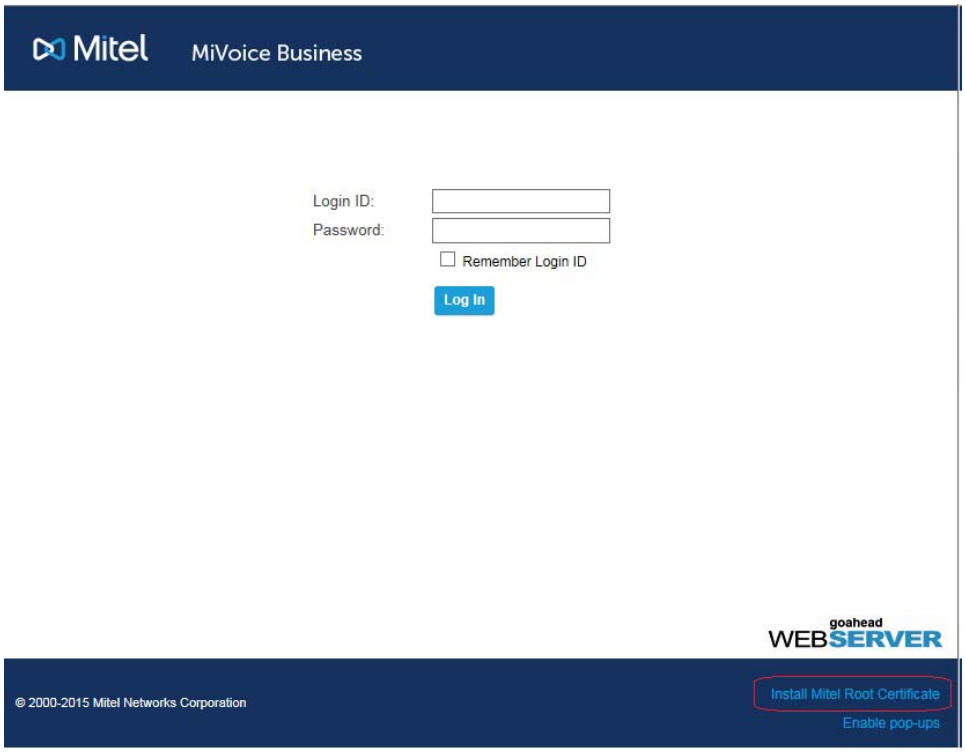

Figure 45: MiVoice Business Login Screen

2. To log into the ESM tools screen:
   - In the **Login ID** field enter "admin".
   - In the Password field, enter the MiVoice Business Express Administrator password that you configured during the Initial Configuration Wizard.

- Select **Remember Login ID** if you want to save the Login ID on your computer.
- Click **Log In**.

Note: The Administration password that you configured in the Initial Configuration Wizard is applied to the MiCollab server manager, MiCollab server console, and MiVoice Business Embedded System Management tools. However, if you later change the password from a MiCollab administration interface, the change is not applied to the MiVoice Business administration tools. Likewise, if you change the password from the MiVoice Business system administration tool, the change is not applied to the MiCollab administrator interfaces. This is because the MiCollab and MiVoice Business admin accounts are separate and independent.

Note: When logging into the MiVoice Business administration tools on the MiVoice Business Express, you must enter "admin" as the username (not "system" which is the default username for standalone MiVoice Business systems).

3. Click the desired Tool (Desktop, Group Administration, or System Administration).
4. You might be prompted to install some XML Components when you log into the System Administration Tool for the first time. At the following prompt, “Do you wish to install or upgrade the required XML components?”, click “Install Now”. The install takes less than 30 seconds and you do not need to restart your computer.

Note: The system will allow up to five concurrent System Administration Tool or Group Administration Tool sessions (or any combination of the two) provided that the initial login browser is closed plus ten concurrent Desktop Tool sessions.

Note: The System Administration Tool will temporarily lock you out for 15 minutes after three consecutive attempts to log in have failed.

INSTALLING A WEB CERTIFICATE

When users connect to their MiCollab End User portal for the first time, they may get a warning message stating that there is a problem with the website’s security certificate or that your browser has blocked the content. This message appears because the application web server is not recognized as a trusted site. Users can safely select the option to continue to the application web server site.

To prevent these security warnings from appearing

- install the Mitel Root CA certificate locally on each user’s client PC, or
- purchase and install a Secure Sockets Layer (SSL) certificate from a third-party Certificate Authority (CA).

For instructions on how to install the Mitel Root CA certificate (security certificate), see the *Install Mitel Root Certificate* topic in the MiCollab End User portal Online Help.

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 Express virtual appliance and then import it onto the MiVoice Business Express 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.

ALLOW TRUSTED NETWORK ACCESS

If the users are deployed on a different subnet than the MiVoice Business Express virtual appliance, 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 MiCollab server manager (see page 124).
2. Navigate to **Networks** in the **Configuration** section 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).
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 address**. (IP address of the router on your trusted local network).
6. Click **Save**.
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 MiCollab server manager (see page 124).
2. Navigate to **Remote Access** under the **Security** section.
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**.

ALLOWING REMOTE ACCESS TO MIVOICE BUSINESS SYSTEM ADMIN INTERFACE

You can enable Internet-based dealers or administrators with remote access to the MiVoice Business System Administration Tool during the Initial Configuration Wizard via the *Telephony Server Management* screen. Access should be configured in the following cases:

- When MiVoice Business Express is deployed in a cloud environment and the dealer or administrator cannot connect or access the LAN.
- When MiVoice Business Express is deployed behind an MPLS network and a dealer or administrator requires Internet access to manage the system (assuming that VPN connectivity is not available to manage MiVoice Business Express from the data center).

If you do not enable access from the Initial Configuration Wizard during initial configuration, you can enable it later from the Remote Proxy Services panel in the MiVoice Business Express server manager using the following procedure:

1. If you haven't done so already, open remote access to the MiVoice Business Express server manager (see "Power on MiVoice Business Express" on page 66).
2. Log into the server manager.
3. Remove the Corporate DNS reference, if programmed:
   - Under **Configuration**, click **Domains**.
   - Click **Modify corporate DNS settings**.
   - Delete any Corporate DNS references.
   - Click **Save**.
4. Configure the hostname and IP address for the MiVoice Business application in the MiVoice Business Express. The MBG Web Proxy requires that the MiVoice Business WAN FQDN be resolved to the MiVoice Business internal IP address:
   - Under **Configuration** click **Hostnames and addresses**.
   - Click **Add Hostname**.
   - Enter the MiVoice Business WAN FQDN in the Hostname field.
   - Set the Location field to "Remote".
   - Click **Next**.
   - Enter the IP Address of the remote host and then click **Add**.

5. Configure Remote Proxy Services:
   - Under **Applications** click **Remote proxy services**.
   - Click the **LAN server proxy list** tab
   - Click Add new LAN server proxy.
   - Check the **Enabled** box.
   - Enter the MiVoice Business WAN FQDN that was provisioned on the external DNS servers.
   - Select **MiVoice Business**.
6. Configure the MiVoice Business administrator's login credentials:
   - Click the **Users** tab.
   - Click Add new user.
   - Check the **Active** box.
   - In the Username field, enter the username used for authentication.
   - In the Password field, enter the user's password used for authentication.
   - In the Confirm Password field, re-type the user's password.
   - In the First Name field, type the user's first name.
   - In the Last Name field, type the user's last name.
   - In the Email address field, type the user's email address.
   - Set the "Add permission" field to **MiVoice Business- Admin interfaces** and click **Add**.
   - Click **Save**.
7. Test access to the MiVoice Business System Administration interface:
   - Open a supported internet browser.
   - Enter the MiVoice Business FQDN (for example, mcd.mycompany.com) that was provisioned on the external DNS server. The MiVoice Business login screen is displayed.
   - Enter the username and password that was configured above.

Note: The Remote Proxy Services should only be used for remote MiVoice Business administration. Configuration for other applications is not supported.

CHANGING THE SYSTEM LANGUAGE

During the initial deployment of a new system, you set the system language. End-users can also set the language of their MiCollab End User portal interface from their login screen and set the prompt language from their Settings screen.

To change the system's end-user language to one of the other supported languages (such as North American English, British English, Canadian French, European French, Dutch, Latin American Spanish, or German):

1. Log into the MiCollab server manager (see page 124).
2. Under **Configuration**, click **MiCollab Language**.
3. Select the desired language from the Language drop-down box.

4. Click **Save**.

Note: For details regarding language support, see Configure MiCollab Language Settings in the Server Manager Online Help.

Chapter 9

TROUBLESHOOT

VIEWING OR COLLECTING LOG FILES

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 5 seconds with any new logs.

DATABASE RESTORE OR RECOVERY

This section provides procedures for

- MiVoice Business Express database restore
- MiVoice Business Express system disaster recovery.

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 Express deployment.
- All application data programmed in the MiVoice Business Express 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 Express OVA file from a newer vSphere platform to a platform with an older version of vSphere. For example, you cannot restore a MiVoice Business Express OVA file that was exported from a vSphere 5.5 platform to a vSphere 5.1 platform.

RESTORING A DATABASE BACKUP

You can restore a database from the server manager or server console.

Note: To restore a database backup (for example, a "Golden" database) during initial deployment, specify a LAN and Default Gateway IP address of 0.0.0.0 during the OVA deployment. This causes the MiVoice Business Express virtual machine to start up in restore mode. You can then restore a database backup from the server console interface.

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. The same restriction applies against restoring a Server-Gateway backup into a Server-only deployment.

To restore a database from the server manager:

1. Log into the server manager interface using the administrator password that you entered in the Custom Template screen. See “Logging into the Server Manager (Administrator Portal)” on page 124 for instructions.
2. Launch the Mitel Integration Wizard.
   - Select **Upgrade**.
   - Navigate to the backup file.
   - Click **Restore**.
3. Wait until the MiVoice Business restore completes, then reboot the MiVoice Business Express server. The MiVoice Business Express system software upgrade procedure is complete.
4. Log into the MiCollab server manager and provision the MiCollab Network Element page with the MiVoice Business FQDN.
   - In MiCollab server manager, under **Applications**, click **Users and Services**
   - Click the **Network Elements** tab.
   - Select the MiVoice Business Network Element and click **Edit**.

- Enter the MiVoice Business FQDN.

5. If Teleworker is running remotely on a vMBG server in the DMZ, you must also restore the vMBG server with the current database; otherwise, the databases will be out of sync.

SYSTEM DISASTER RECOVERY

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

Note: VMware SRM cannot be used for MiVoice Business Express disaster recovery.

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.

1. Download the MiVoice Business Express OVA file from Mitel Online to a network drive or vSphere Client PC (see page 64 for instructions).
2. Shut down the current MiVoice Business Express.
3. Deploy the new MiVoice Business Express (OVA file) on the host system (see page 65 for instructions).
4. Right-click on the newly created MiVoice Business Express (for example: MiVoice Business Express 8.0.0.40 build) and select **Open Console**. The MiVoice Business Express console opens within the vSphere Client.
5. Power on the MiVoice Business Express by clicking the green button in the tool bar.
6. After you power on the MiVoice Business Express VM, the Custom Template screen is displayed.
   - Complete the fields in the Custom Template screen with the information for the existing MiVoice Business Express VM. Note that if you enter different IP addresses, they will be overwritten buy 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. See “Logging into the Server Manager (Administrator Portal)” on page 124 for instructions.
8. Launch the Initial Configuration Wizard.
   - Select **Upgrade**.
   - Navigate to the backup file.
9. Click **Restore**.

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. This guide is available at http://edocs.mitel.com/TechDocs/Solutions-Guides/vQuickRef.pdf

SYMPTOM	POSSIBLE CAUSE	CORRECTIVE ACTION
In the VMware deployment wizard, the IP Address fields in the Properties screen are truncated.	If your PC screen resolution is set above 100%, for example 125%, some IP Address fields in the wizard may be truncated.	Ensure that your PC display resolution is set to 100%.
Unable to access MiCollab server manager interface after deployment.	An invalid LAN IP address was entered in the MiVoice Business Express Properties screen during OVF deployment.	Enter a valid LAN IP or WAN IP address through the MiCollab server console interface: 1. Right-click on the newly created MiVoice Business Express (for example: MiVoice Business Express 8.0.0.40 build) and select **Open Console**. The MiCollab virtual appliance console opens within the vSphere 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 Express 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)
	An valid LAN IP address was entered in the MiVoice Business Express Properties screen during OVF deployment, but this IP address is not on the same subnet as the MiVoice Business Express.	
After a restore, you attempt to log into the server manager interface, but the Initial Configuration Wizard page is displayed instead.	If you log from the system IP address only, the system may redirect you to the Initial Configuration Wizard page.	Log from the following URL: **https://**<*IP Address of the MiVoice Business Express*>/server-manager
During the Initial Configuration Wizard, you receive an insufficient license error on the Initial Configuration screen.	The licensing key is missing the minimum required number of licenses to support deployment.	In the AMC, add the specified licenses to the MiVoice Business Express Base ARID, ULM ARID, or both as indicated in the warning message
Cannot power up MiVoice Business Express.	You have cloned a MiVoice Business Express and are attempting to power it up.	Cloning of an MiVoice Business Express is not supported. You can only clone MiVoice Business Express templates.

SYMPTOM	POSSIBLE CAUSE	CORRECTIVE ACTION
After you deploy the and complete the Initial Configuration Wizard, the MiCollab clients cannot connect to MiVoice Business Express via the WAN IP.	The MiCollab Client Connector is not configured with the MiVoice Business Express LAN IP Address.	1. Log into the MiCollab server manager. 2. Under **Applications**, click **MiVoice Border Gateway**. 3. Click **Applications**. 4. Click **MiCollab Client**. 5. Click **Edit**. 6. Check the **MiCollab Client connector enabled** box. 7. Enter the MiVoice Business Express LAN IP Address in the following three fields: •MiCollab Clienthostname or server IP address •Nupoint Voicemail hostname or server IP address •Collaboration server hostname or server IP address.
MiVoice Business Express system performance is slow.	VMware resources are inadequate.	1. Log into the MiCollab 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 Express. System performance is degraded if snapshots are present on the platform	Delete all MiVoice Business Express snapshots from system.
Voice quality issues	VMware resources are inadequate.	1. Log into the MiCollab server manager. 2. Under **Administration**, click M**itel 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.
	MiVoice Business Express is installed in the vSphere environment using **Thin** provisioning. Thin provisioning can cause voice quality issues due to disk sharing.	Reinstall MiVoice Business Express and select Thick provisioning during the install wizard.

SYMPTOM	POSSIBLE CAUSE	CORRECTIVE ACTION
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 or upgrade MiVoice Business Express to Release 7.0 or later, Flow Through Provisioning and Reach Through to the MiVoice Business application are not functioning. After you restore a MiVoice Business Express database, Flow Through Provisioning and Reach Through to the MiVoice Business application are not functioning	MiCollab and the MiVoice Business applications failed to start sharing data.	1. Log into the MiVoice Business system administration tool. 2. Choose to view the forms alphabetically and select the **Network Elements** form. 3. Locate the MiCollab network element, select it, click **Start Sharing** and then **OK.** 4. Verify the sharing and synchronization completes successfully. If you receive a banner warning, log into the MiCollab server, and run the **Reconcile Wizard** to align the data.
After a database restore the following error message appears in the server manager banner: "Failed to start the data synchronization between MiCollab and MiVoice Business. Reason: The MiVoice Business application has not started".	The MiVoice Business application failed to start so the automatic database synchronization could not proceed.	1. Log into the MiCollab 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 Application Management Center (AMC). The Application Record ID is not registered with the AMC.	1. Log into the MiCollab server manager. 2. Access the Status page and **Sync** the MiCollab ARID with the AMC. 3. Log into the MiVoice Business system administration tool. 4. Choose to view the forms alphabetically and select the **Network Elements** form. 5. Locate the MiCollab network element, select it, click **Start Sharing** and then **OK.** 6. Verify the sharing and synchronization completes successfully. If you receive a banner warning, log into the MiCollab server, and run the **Reconcile Wizard** to align the data.

Appendix A

SYSTEM DEFAULTS

INTRODUCTION

This appendix identifies the following system defaults:

- Defaults applied from the Custom Template page to the OVF property configuration file during initial configuration
- Default settings applied to the vMiVoice Business, vMiCollab, and vMBG applications by the Initial Configuration Wizard
- Default SIP Service Provider settings
- Default Class of Service (COS) settings applied to new users who are created using single-point of provisioning from Active Directory or MiCollab
- Default Class of Service settings applied to application ports
- Default UCC Roles and Templates that you can use to assign UCC licenses to users.

CUSTOM TEMPLATE CONFIGURATION PAGE DEFAULTS

The settings that you enter in the Custom Template screen define the MiVoice Business Express OVA properties that are applied to the OVA.

Table 13: Custom Template Configuration Page Defaults

CONFIGURATION ITEM	DESCRIPTION	DEFAULT
Time zone Setting	Time zone setting for the MiVoice Business Express.	America_New York
Keyboard	MiCollab server keyboard language	us
Initial Administrator Password	Initial administrator password for the MiCollab server manager after the VA is deployed. The initial configuration wizard requires you to change the administrator password. If you leave the password field blank, MSL will not boot.	No default
Hostname	Host name used by the MiVoice Business Express. This field can be left blank for VMware template creation.	MiVB-X

Table 13: Custom Template Configuration Page Defaults

CONFIGURATION ITEM	DESCRIPTION	DEFAULT
Domain Name	Domain name for this host. This field can be left blank for VMware template creation.	mycompany.local.
License Key	Record ID for licensing the system. This field can be left blank for VMware template creation.	Blank
DNS Server IP	DNS Server IP Address(es)	No default
Remote Network Address	Network address for the remote hosts	No default
Remote Network Netmask	Netmask for the remote hosts	No default
LAN IP Address	IP address for the local (LAN) interface. The selected IP address must belong to the local (LAN) interface. This address can be left blank for template creation, but must be set in the VM "Edit Settings" > Option > vApp Options > Properties dialog box before you power on the VM.	No default
LAN Netmask	Netmask of the LAN	255.255.255.0
WAN IP Address	IP address for the external (WAN) interface. The IP address selected must belong to the external (WAN) interface. This IP address can be left blank for VMware template creation, but must be set in the VM "Edit Settings" > Option > vApp Options >Properties dialog box before you power on the VM.	0.0.0.0
WAN Netmask	Netmask of the WAN	255.255.255.0
Optional LAN IP Address	IP Address for an 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.	0.0.0.0
Optional LAN Netmask	Netmask of the optional LAN	255.255.255.0
Default Gateway Address	WAN Gateway IP Address	No default

INITIAL CONFIGURATION WIZARD DEFAULTS

To simplify initial configuration, the wizard applies default settings to the MiVoice Business Express system. Default settings are applied to the vMiCollab, vMiVoice Business, and vMBG applications.

STANDARD DEFAULT SETTINGS

Refer to the MiVoice Business system administrator online help for the standard default settings that are applied to the vMiVoice Business platform and vMiCollab applications:

MIVOICE BUSINESS EXPRESS-SPECIFIC DEFAULT SETTINGS

Table 14 summarizes the default settings that are applied specifically to MiVoice Business Express deployments.

Table 14: MiVoice Business Express Application-Specific Defaults

APPLICATION	CONFIGURATION ITEM	DEFAULT
MiVoice Business	System Administration Tool Login and Password	Defaults to MiCollab server manager Username and Password.
MiVoice Business	Administrator email address and SMTP email	Defaults to settings in MiCollab server manager under Configuration > E-mail settings.
MiVoice Business	Licenses and Options	Refer MiVoice Business defaults (go to link above) with the following additional defaults: • No Extended Agent Skill Groups • Maximum Elements per Cluster = 30 • Maximum Configurable IP Users and Devices = 700 • No Extended Hunt Groups.
MiVoice Business	Class of Service (COS), Feature Access Codes (FAC), Speed Calls, Station Message Detail Recording (SMDR) Options	Refer to the MiVoice Business system administration help for the Standard Defaults
MiCollab Network Element page and MiVoice Business	Class of Restriction (COR)	When you create a user from the MiCollab USP application, the user is created with COR 2.
	Call Reroute First Alternative (CRFA)	When you create a user from the MiCollab USP application, the user is assigned CRFA 2 by default. CRFA 2 reroutes calls to the voice mail hunt group extension 7000.
MiVoice Business	Domain Name, Primary and Secondary DNS servers	Defaults to the settings in MiCollab server manager under Configuration > Domain
MiVoice Business	Date and time zone	Defaults to the settings in the MiCollab server manager under Configuration > Date and Time.
MiVoice Business	SIP Trunks	SIP peer profile defaults are provided for common SIP Service Provider on a per-country basis. The SIP Network Element name defaults to the SIP Service Provider Name. The number of SIP trunk defaults to 1. For North America, you are prompted for a local number (main business number) and the number of digits dialed for that local number (7 or 10). This local number is typically registered with the Service Provider. You are also prompted for username and password to access the SIP Service Provider.

Table 14: MiVoice Business Express Application-Specific Defaults

APPLICATION	CONFIGURATION ITEM	DEFAULT
MiVoice Business	SIP Trunk Proxy	Defaulted if MBG SIP Proxy is onboard the MiVoice Business Express system, configurable if MBG SIP proxy is on an external MBG. SIP Network Element name is defaulted. You are prompted for external MBG SIP proxy FQDN or IP address.
MiVoice Business	Automatic Route Selection	Refer to the MiVoice Business system administration help for the Standard Defaults.
MiVoice Business	Voicemail Hunt Group	Defaults to hunt group pilot number 7000 with ports starting at 7001. The number of ports is dependent on licensing. Message waiting indicator set to HCI reroute. HCI hunt group defaulted to 7400.
MiVoice Business	Call Services Emergency ID (CESID)	Defaults to main business number.
MiVoice Business	MiCollab AWV Hunt Groups	Defaults to hunt group pilot number 7850 with 3 ports starting at 7851.
MiCollab	MiCollab Language setting	System language is based on country selection.
MiCollab	IP Phone display languages	Dependent on country and telecom region settings.
MiCollab - NPM	Voice mail message storage per user	200 voice mail messages per user (LCOS 1).
MiCollab - NPM	Limits COS and Feature COS settings	Refer to NuPoint Messaging documentation for the LCOS and FCOS default settings.
MiCollab-NM	NuPoint Administrator Mailbox	By default, only generic non-customer-specific greetings are supported.
MiCollab AWV	MiVoice Business COS options for MiCollab AWV ports	Refer to the MiVoice Business system administration help for the Standard Defaults.
MiCollab AWV	Administrator email settings	Defaults to settings in MiCollab server manager under Configuration > E-mail settings.
MiCollab Client	Database management mode	The "first-run" wizard puts the MiCollab Client server in integrated mode using the default MSL domain name and time zone. The language defaults to the MiCollab application suite language
MBG	SIP Connector	SIP Connector is provisioned if internal SIP proxy is used.

COMPRESSION AND BANDWIDTH MANAGEMENT

By default, compression is applied between SIP trunks and non-SIP endpoints while bandwidth management is not applied.

TIME ZONE

Time-zone does not allow for out-of-zone set location.

MAIN BUSINESS NUMBER

By default, the Main Business is provisioned as a DID number that points to the auto receptionist (7100 default).

SIP TRUNK ATTRIBUTE

The SIP trunk attribute is configured as a DID trunk.

COUNTRY SPECIFIC DEFAULTS

The following sections list defaults specific to each country.

NORTH AMERICA

Table 15: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Local	1	1	4, 5, 8	1-3, 6, 9-75	1	0
Long Distance	2	2	1, 4, 5, 7, 8, 10-75	2-3, 6, 9	1	0
Overseas	3	3	1, 2, 4-8, 10-75	3, 9	1	0
Emergency	4	4		1, 2-75	0	0
Mobile Calls	6	6	1, 2, 4, 5, 7, 8, 10-75	3, 6, 9	0	0
Emergency	7	4		1, 2-75	1	0
Toll Free	8	8	4, 5	1-3, 6-75	1	0
Premium	9	9	1-8, 10-75	9	1	0

Note: By default, users are assigned COR group 2, which allows them to make Local and Long Distance calls, but restricts them from making Overseas calls.

Table 16: Local Attributes for North America

PARAMETER	DESCRIPTION	COUNTRY SETTING
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	Format consists of an area code, followed by a city code and a local number. For example: 613 592 2122

Table 16: Local Attributes for North America

PARAMETER	DESCRIPTION	COUNTRY SETTING
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	9
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	1
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	011
Emergency Calls	The digits that a user dials to place an emergency call	911

	Type of Calls	Digits Dialed	Digits to Follow
1	Overseas	9011	Unknown
2	Long Distance	91	10
3	Local	9	10
4	Toll Free	91800	7
5	Toll Free	91856	7
6	Toll Free	91866	7
7	Toll Free	91877	7
8	Toll Free	91888	7
9	Barred Calls	91900	7
10	Barred Calls	91976	7
11	Barred Calls	91809	7
12	Emergency	9911	0
13	Emergency	911	0

Figure 46: ARS Rules for North America

UNITED KINGDOM

Table 17: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Local	1	1	4, 5, 8	1-3, 6, 9-75	1	0
Long Distance	2	2	1, 4, 5, 7, 8, 10-75	2-3, 6, 9	1	0
Overseas	3	3	1, 2, 4-8, 10-75	3, 9	1	0
Emergency	4	4		1, 2-75	0	0
Mobile Calls	6	6	1, 2, 4, 5, 7, 8, 10-75	3, 6, 9	0	0
Emergency	7	4		1, 2-75	1	0

Table 17: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Toll Free	8	8	4, 5	1-3, 6-75	1	0
Premium	9	9	1-8, 10-75	9	1	0

Note: By default, users are assigned COR group 2, which allows them to make Local and Long Distance calls, but restricts them from making Overseas calls.

Table 18: Local Attributes for United Kingdom

PARAMETER	DESCRIPTION	COUNTRY SETTING
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	Regional or mobile code followed by the number: 01xxx yyyyyy 02xxx yyyyyy 07xxx yyyyyy (mobile) For example: 01291 430000
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	9
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	9 followed by the national code. For example: 901xxx yyyyyy 902xxx yyyyyy
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	9 followed by the country code For example: 9001xxx yyyyyy
Emergency Calls	Digits user dials to place an emergency call	9999, 9112, 9101, 9111

	Type of Calls	Digits Dialed	Digits to Follow
1	Emergency	101	0
2	Emergency	111	0
3	Emergency	112	0
4	Toll Free	116	3
5	Overseas	900	Unknown
6	Long Distance	901	9
7	Long Distance	901XXXXXXXX	0
8	Long Distance	902	9
9	Long Distance	903	9
10	Long Distance	905	9
11	Toll Free	90500	6
12	Long Distance	907	9
13	Premium	9070	8
14	Long Distance	908	Unknown
15	Toll Free	90800	Unknown
16	Toll Free	90808	Unknown
17	Long Distance	90845	Unknown
18	Long Distance	9087	8
19	Barred Calls	909	Unknown
20	Barred Calls	9100	0
21	Emergency	9101	0
22	Emergency	9111	0
23	Emergency	9112	0
24	Premium	9118	3
25	Barred Calls	9155	0
26	Emergency	999	0
27	Emergency	9999	0

Figure 47: ARS Rules for United Kingdom

AUSTRALIA

Table 19: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Local	10	10	1, 5	10,15,20,25,30	1	0
Long Distance	20	20	1, 5,10,15	20,25,30	1	0
Overseas	25	25	1, 5, 10, 15, 20	25, 30	1	0
Emergency	1	1			1	0
Mobile Calls	15	15	1, 5, 10	15, 20, 25, 30	1	0
Toll Free	5	5	1	5,10,15,20,25,30	1	0

Note: By default, users are assigned COR group 2, which allows them to make Local and Long Distance calls, but restricts them from making Overseas calls.

Table 20: Local Attributes for Australia

PARAMETER	DESCRIPTION	COUNTRY SETTING
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	End-user numbers are 10 digits long, conventionally written in the form **(0x) xxxx xxxx** for geographic and **04xx xxx xxx** for mobile numbers. If the number is written where it may be viewed by an international audience (for example, on an email signature or website) then the number is often written as **+61 x xxxx xxxx** or **+61 4xx xxx xxx** respectively (the initial **0** is not used for calls from overseas).
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	0
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	0
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	0011
Emergency Numbers	The digits that a user dials to place an emergency call	000, 106

	Type of Calls	Digits Dialed	Digits to Follow
1	Emergency	0000	0
2	Overseas	00011	Unknown
3	Overseas	00019	Unknown
4	Overseas	0012	3
5	Long Distance	002	8
6	Long Distance	003	8
7	Mobile Calls	004	8
8	Long Distance	005	8
9	Long Distance	006	8
10	Long Distance	007	8
11	Long Distance	008	8
12	Long Distance	009	8
13	Long Distance	01223	0
14	Long Distance	01300	6
15	Long Distance	013	4

Figure 48: ARS Rules for Australia

FRANCE

Table 21: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Local	1	1	4, 5, 8	1-3, 6, 9-75	1	0
Long Distance	2	2	1, 4, 5, 7, 8, 10-75	2-3, 6, 9	1	0
Overseas	3	3	1, 2, 4-8, 10-75	3, 9	1	0
Emergency	4	4		1, 2-75	0	0
Mobile Calls	6	6	1, 2, 4, 5, 7, 8, 10-75	3, 6, 9	0	0
Emergency	7	4		1, 2-75	1	0
Toll Free	8	8	4, 5	1-3, 6-75	1	0
Premium	9	9	1-8, 10-75	9	1	0

Note: By default, users are assigned COR group 2, which allows them to make Local and Long Distance calls, but restricts them from making Overseas calls.

Table 22: Local Attributes for France

PARAMETER	DESCRIPTION	COUNTRY SETTING
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	01 xx xx xx xx The numbering plan uses a ten-digit closed numbering scheme, where the first two digits denote the area: 01 Ile-de-france 02 Northwest France 03 Northeast France 04 Southeast France 05 Southwest France 06 and 07 Mobile phone services 08 Freephone 09 Non-geographic number
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	None
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	None
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	00
Emergency Numbers	The digits that a user dials to place an emergency call.	15, 17, 18, 112, 115, 119

	Type of Calls	Digits Dialed	Digits to Follow
1	Long Distance	01	8
2	Long Distance	02	8
3	Long Distance	03	8
4	Long Distance	04	8
5	Long Distance	05	8
6	Mobile Calls	06	8
7	Mobile Calls	07	8
8	Mobile Calls	087	7
9	Toll Free	0800	6
10	Toll Free	0805	6
11	Toll Free	08088	5
12	Toll Free	0809	6
13	Barred Calls	081	7
14	Barred Calls	0820	6
15	Barred Calls	0821	6
16	Barred Calls	0825	6
17	Barred Calls	0826	6
18	Barred Calls	0884	6
19	Barred Calls	0890	6
20	Barred Calls	0891	6
21	Barred Calls	0892	6
22	Barred Calls	0893	6
23	Barred Calls	0897	6
24	Barred Calls	0898	6
25	Barred Calls	0899	6
26	Long Distance	08	8
27	Local	09	8
28	Toll Free	30	2
29	Toll Free	31	2
30	Barred Calls	3	3
31	Barred Calls	32	2
32	Barred Calls	36	2
33	Barred Calls	39	2
34	Local	118	3
35	Local	10	2
36	Barred Calls	0033	Unknown
37	Overseas	00	Unknown
38	Emergency	15	0
39	Emergency	17	0
40	Emergency	18	0
41	Emergency	112	0
42	Emergency	115	0
43	Emergency	119	0

Figure 49: ARS Rules for France

NETHERLANDS

Table 23: Call Type to Route, COR Group, Disallowed and Allowed CORs

Type of Calls	Route	COR Group	Disallowed CORs	Allowed CORs	Digits to Absorb	Digits to Insert
Local	1	1	4, 5, 8	1-3, 6, 9-75	1	0
Long Distance	2	2	1, 4, 5, 7, 8, 10-75	2-3, 6, 9	1	0
Overseas	3	3	1, 2, 4-8, 10-75	3, 9	1	0
Emergency	4	4		1, 2-75	0	0
Mobile Calls	6	6	1, 2, 4, 5, 7, 8, 10-75	3, 6, 9	0	0
Emergency	7	4		1, 2-75	1	0
Toll Free	8	8	4, 5	1-3, 6-75	1	0
Premium	9	9	1-8, 10-75	9	1	0

Note: By default, users are assigned COR group 2, which allows them to make Local and Long Distance calls, but restricts them from making Overseas calls.

Table 24: Local Attributes for Netherlands

PARAMETER	DESCRIPTION	COUNTRY SETTING
Phone Number Format	This attribute specifies the format of the Main Business Number that you enter in the Incoming Call page of the Initial Configuration Wizard.	Geographical telephone numbers are sequences of 9 digits (0-9) and consist of an area code of two or three digits and a subscriber number of seven or six digits, respectively. When dialed within the country, the number must be prefixed with the trunk access code 0, identifying a destination telephone line in the Dutch telephone network. Non-geographical numbers have no fixed length, but also required the dialing of a trunk access code (0). They are used for mobile telephone networks and other designated service types, such as toll-free dialing, Internet access, voice over IP, restricted audiences, and information resources.
Outgoing Prefix	The digit that a user dials to obtain an outgoing line.	0
National Prefix	The digits that a user dials in front of the telephone number when placing a national call.	0
International Prefix	The digits that a user dials in front of the telephone number when placing an international call.	000 (followed by country code)
Emergency Numbers	The digits that a user dials to place an emergency call	112 is emergency Police emergency is 09008844

	Type of Calls	Digits Dialed	Digits to Follow
1	Local	01	6
2	Local	02	6
3	Local	03	6
4	Local	04	6
5	Local	05	6
6	Local	06	6
7	Local	07	6
8	Local	08	6
9	Local	09	6
10	Long Distance	001	8
11	Long Distance	002	8
12	Long Distance	003	8
13	Long Distance	004	8
14	Long Distance	005	8
15	Long Distance	006	8
16	Long Distance	007	8
17	Long Distance	00031	9
18	Long Distance	008	8
19	Overseas	00044	10
20	Overseas	00032	8
21	Overseas	0003247	7
22	Overseas	0003248	7
23	Overseas	0003249	7
24	Overseas	00033	9
25	Overseas	00034	9
26	Overseas	00039	9
27	Overseas	0003	Unknown
28	Overseas	0004	Unknown
29	Overseas	0001	10
30	Overseas	000	Unknown
31	Emergency	0112	0
32	Emergency	009008844	0
33	Premium	00900	Unknown
34	Barred Calls	00906	Unknown
35	Barred Calls	00909	Unknown

Figure 50: ARS Rules for Netherlands

DEFAULT SIP SERVICE PROVIDERS

The following table lists the SIP Service Providers that are supported for each region/country in the drop down list of the Initial Configuration Wizard. It identifies whether or not the Initial Configuration Wizard automatically codes the Direct Inward Dialing rules for the listed Service Providers.

In cases where the Initial Configuration Wizard codes the Direct Inward Dialing rules, it applies the settings defined in the associated configuration guide. To locate a guide in the knowledge base set the Product to "3300 Integrated Communications Platform (ICP)" and enter the guide number in the Keyword Search field. For additional information, see the "SIP CoE SIP Interop Reference" also available in the Mitel Knowledge Base.

Note that you can also select the Generic setting and then modify the recommended SIP CoE defaults in the SIP Peer Profile form of the MiVoice Business system Administration Tool.

Table 25: SIP Service Provider

COUNTRY	SIP SERVICE PROVIDER	INWARD DIALLING RULES CODED?	CONFIGURATION GUIDE:
USA	Mitel NetSolutions		
	Windstream	N	10-4940-00102_3
	Stream-NuVox	N	09-4940-00085_2
	Paetec-BroadSoft	N	08-4940-00035
	Paetec-Genband	N	08-4940-00038
	Paetec-Lucent (McLeod)	N	08-4940-00009
	AccessLine	N	08-4940-00036_5
	CenturyLink	?	13-4940-00241
	TW Telecom	?	
	AT&T	?	08-4940-00014_5
	Generic	No	See **Note 1**
Canada	MTS Allstream	?	08-4940-00015
	Shaw	?	13-4940-00260
	ThinkTel	?	12-4940-00197_2
	Bell	?	11-5159-00071_3
	Generic		See **Note 1**
France	Hub One (HUB Telecom)	Y	11-5159-00078
	Open IP	Y	11-4940-00186
	Acropolis	Y	11-5159-00069
	Generic	N	See **Note 1**

Table 25: SIP Service Provider

COUNTRY	SIP SERVICE PROVIDER	INWARD DIALLING RULES CODED?	CONFIGURATION GUIDE:
UK	Gamma Telecom	N	11-4940-00156_2
	Cable & Wireless (Vodafone)	N	10-4940-00151
	BT	N	09-4940-00097
	Generic	N	See **Note 1**
Netherlands	Vodafone	Y	13-4940-00263
	OneXS	Y	13-4940-00264
	UPC Telecom	N	10-4940-00110_2
	Generic	N	See **Note 1**
Australia	Telstrat	N	13-4940-00281
	AAPT	N	13-4940-00255
	IINet	N	08-4940-00044
	Generic	N	See **Note 1**
New Zealand	SNAP AKL	N	
	SNAP CHC	N	
	SNAP WGN	N	
	WorldExchange	N	
	2Talk (Opal)	N	10-4940-00147
	Generic	N	See **Note 1**
Belgium	Destiny	Y	13-4940-00262
	Belgacom	Y	13-4940-00238
	Telenet	Y	13-4940-00276
	Generic	N	See **Note 1**
Germany	QSC	Y	13-4940-00240
	Vodafone	N	14-4940-00290
	Colt	Y	13-4940-00277_2
	Generic	N	See **Note 1**

Note 1: The Initial Configuration Wizard applies the recommended Generic SIP CoE default settings that you can modify through the MiVoice Business System Administration Tool. The Generic SIP CoE default settings are defined in Configuration Guide 12-4940-00215 in the Mitel Knowledge Base.

COS SETTINGS FOR MICOLLAB USERS

The following tables list the COS settings that the Initial Configuration Wizard applies to the MiVoice Business system and the MiCollab application services (where applicable).

If you manually configure the MiVoice Business system and MiCollab applications, then you must program these Class of Service Option settings into the MiVoice Business system through the System Administration Tool. The corresponding COS option number must also be programmed into the Network Elements screen of the Users and Services application. If you choose to manually program these COSs, it is recommended that you use the default COS numbers.

For simplicity, only the settings that have been changed from their default Class of Service settings are listed. Therefore, to manually create a required COS, select the COS number and then apply the settings specified below. On an existing MiVoice Business system, if a COS number (for example COS 11) is already in use, you will need to modify your COS programming to free up the required COS. Note that you can use the **Copy** button in the Class of Service Assignment form to copy existing settings to a different COS number. You can also use the Copy button to copy the default settings from a blank COS to one of the required COS numbers if the COS has been modified.

The wizard creates COS 11 and 13 with the required settings for Hot Desk users.

Table 26: Default Hot Desk User COSs

	HOT DESK USER COSS (DEFAULT)	
OPTION	USER (COS 11)	VM USER WITH RAC (COS 13)
ACD Silent Monitor Accept	Yes	Yes
ACD Silent Monitor Allowed	Yes	Yes
ACD Silent Monitor Notification	Yes	Yes
Group Presence Control	No	No
Group Presence Third-Party Control	No	No
Hot Desk External User Answer Confirmation	No	Yes
Hot Desk External User Permanent Login	Yes	Yes
Hot Desk Login Accept	Yes	Yes
Hot Desk Remote Logout Enabled	Yes	Yes
SMDR External and Internal	Yes	Yes
Work Timer	20 s	20 s

COS FOR APPLICATION PORTS

The wizard creates COS 82, 84, and 85 for the NuPoint Unified Messaging application with the required settings for the ports:

Table 27: Default NuPoint Unified Messaging Ports COSs

OPTION	NP PORTS COS (DEFAULT) (COS 82)	NP MWI PORTS COS (DEFAULT) (COS 84)	SPEECH AA PORTS COS (DEFAULT) (COS 85)
Calling Party Name Substitution	No	No	Yes
COV/ONS/E&M Voice Mail Port	Yes	Yes	No
Dialled Night Service	No	No	Yes
Display Dialed Digits during Outgoing Calls	No	No	Yes
Do Not Disturb Permanent	No	Yes	No
HCI/CTI/TAPI Call Control Allowed	Yes	Yes	Yes
HCI/CTI/TAPI Monitor Allowed	Yes	Yes	Yes
Public Network Access via DPNSS	Yes	No	Yes

The wizard creates COS 86 with the required settings for the MiCollab AWV ports:

Table 28: Default MiCollab AWV Ports COS

OPTION	MICOLLAB AWV PORTS COS (DEFAULT) (COS 86)
Suppress Simulated CCM after ISDN Progress	Yes

UCC DEFAULT ROLES AND TEMPLATES

DEFAULT ROLES

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

- Default UCC Entry
- Default UCC Standard
- Default UCC Premium

ENTRY USER FOR BUSINESS TEMPLATE

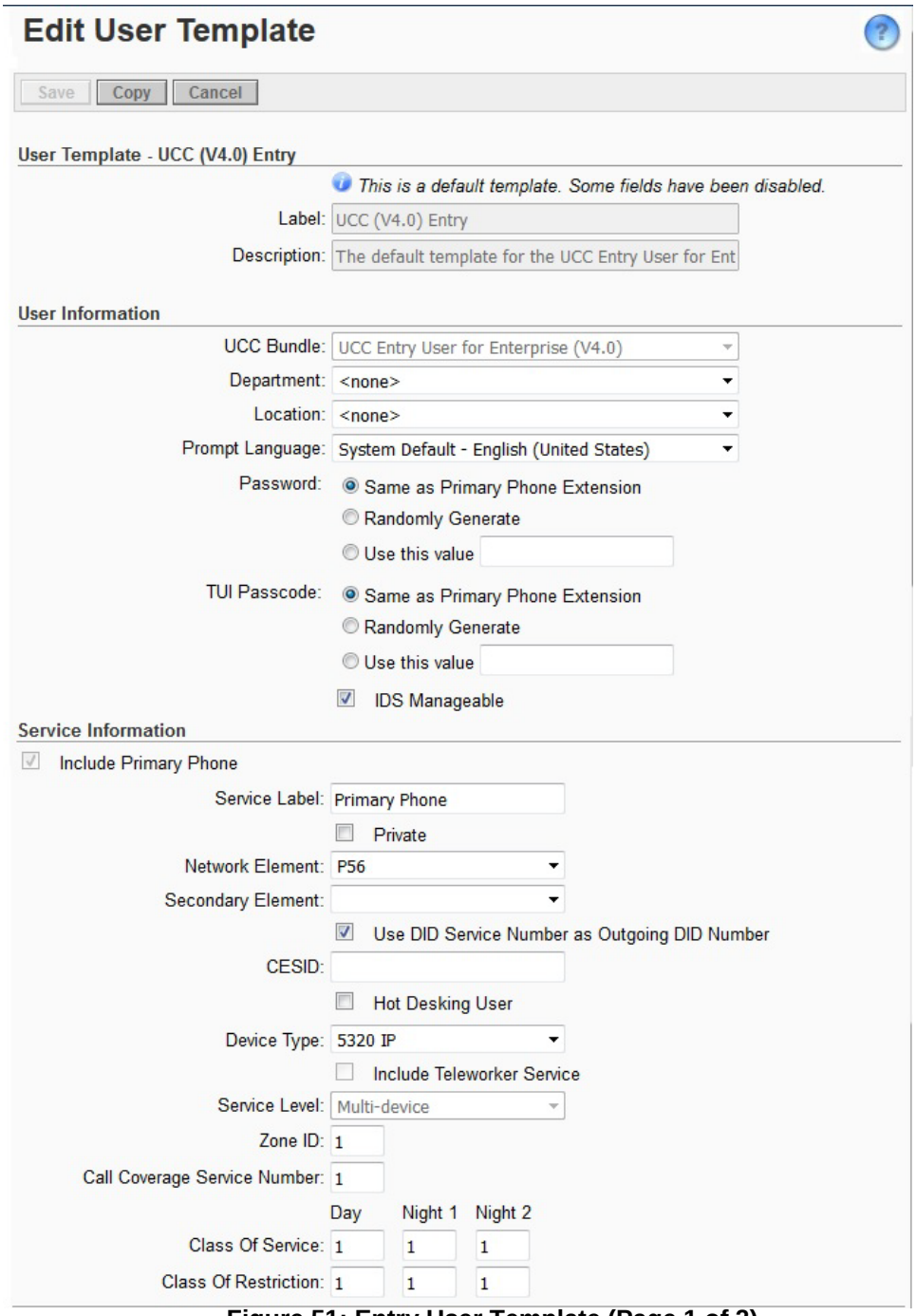

Figure 51: Entry User Template (Page 1 of 2)

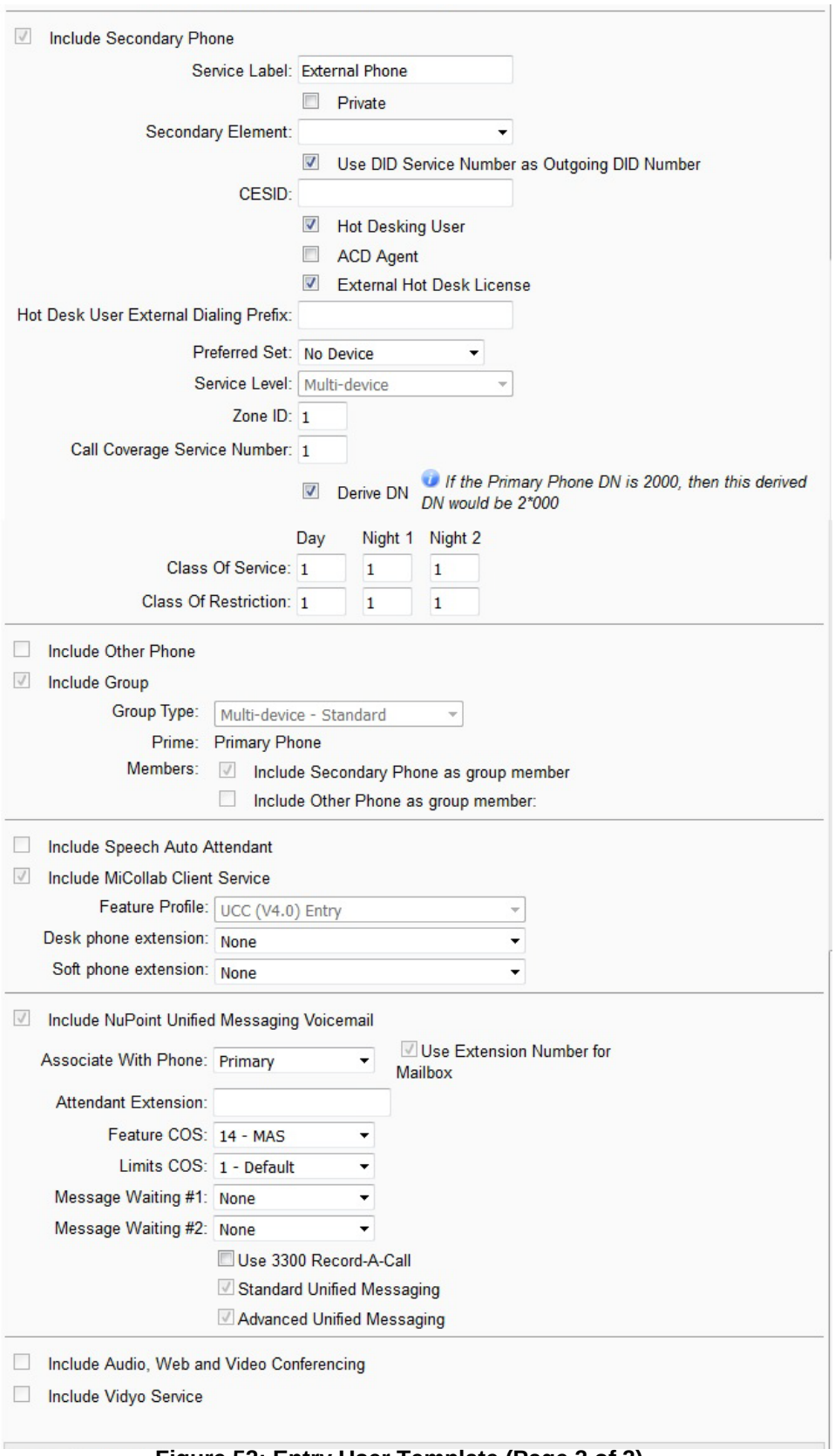

Figure 52: Entry User Template (Page 2 of 2)

STANDARD USER FOR BUSINESS TEMPLATE

Figure 53: Standard User for Business Template (Page 1 of 3)

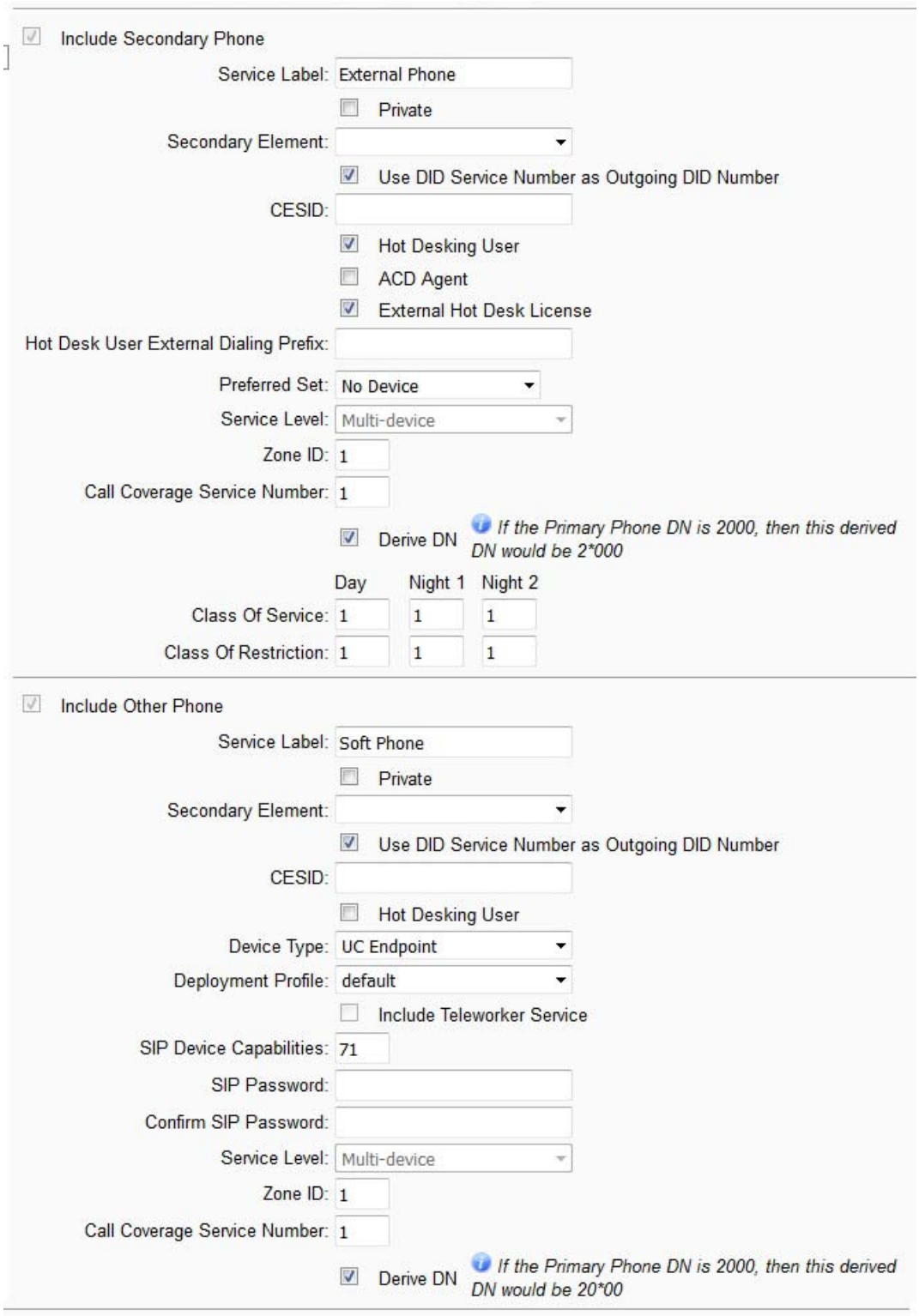

Figure 54: Standard User for Business Template (Page 2 of 3)

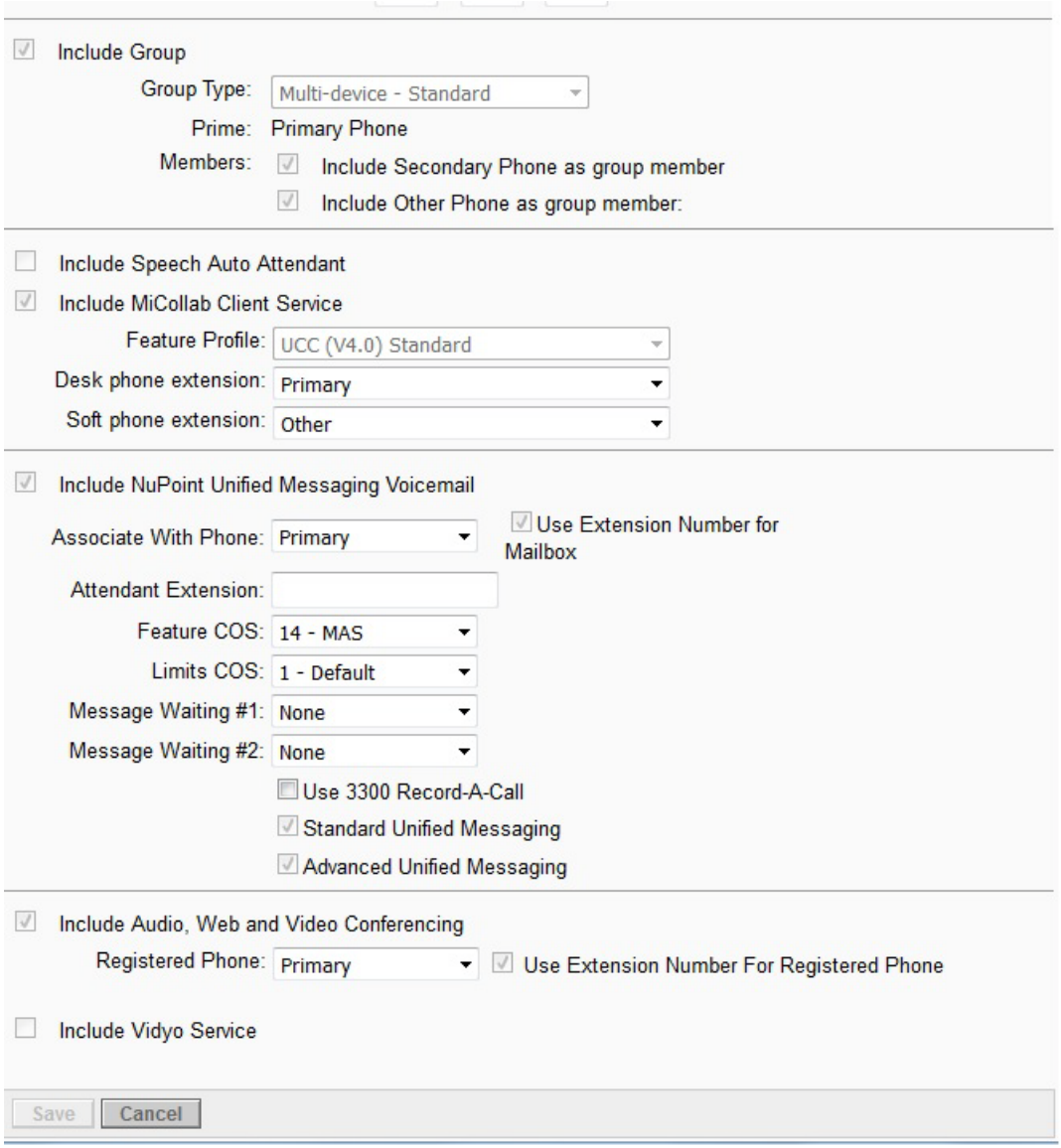

Figure 55: Standard User Template (Page 3 of 3)

PREMIUM USER FOR BUSINESS TEMPLATE

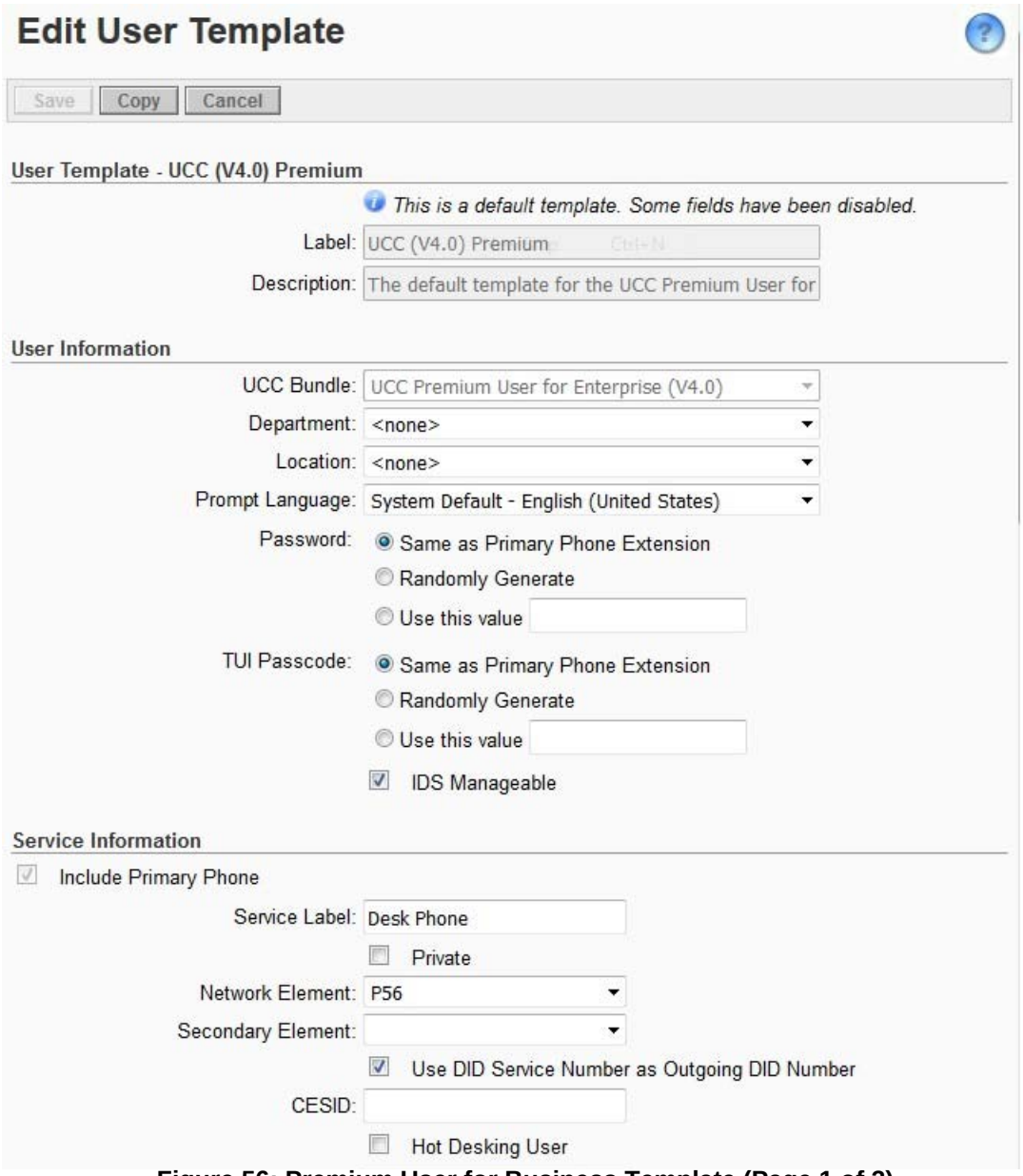

Figure 56: Premium User for Business Template (Page 1 of 3)

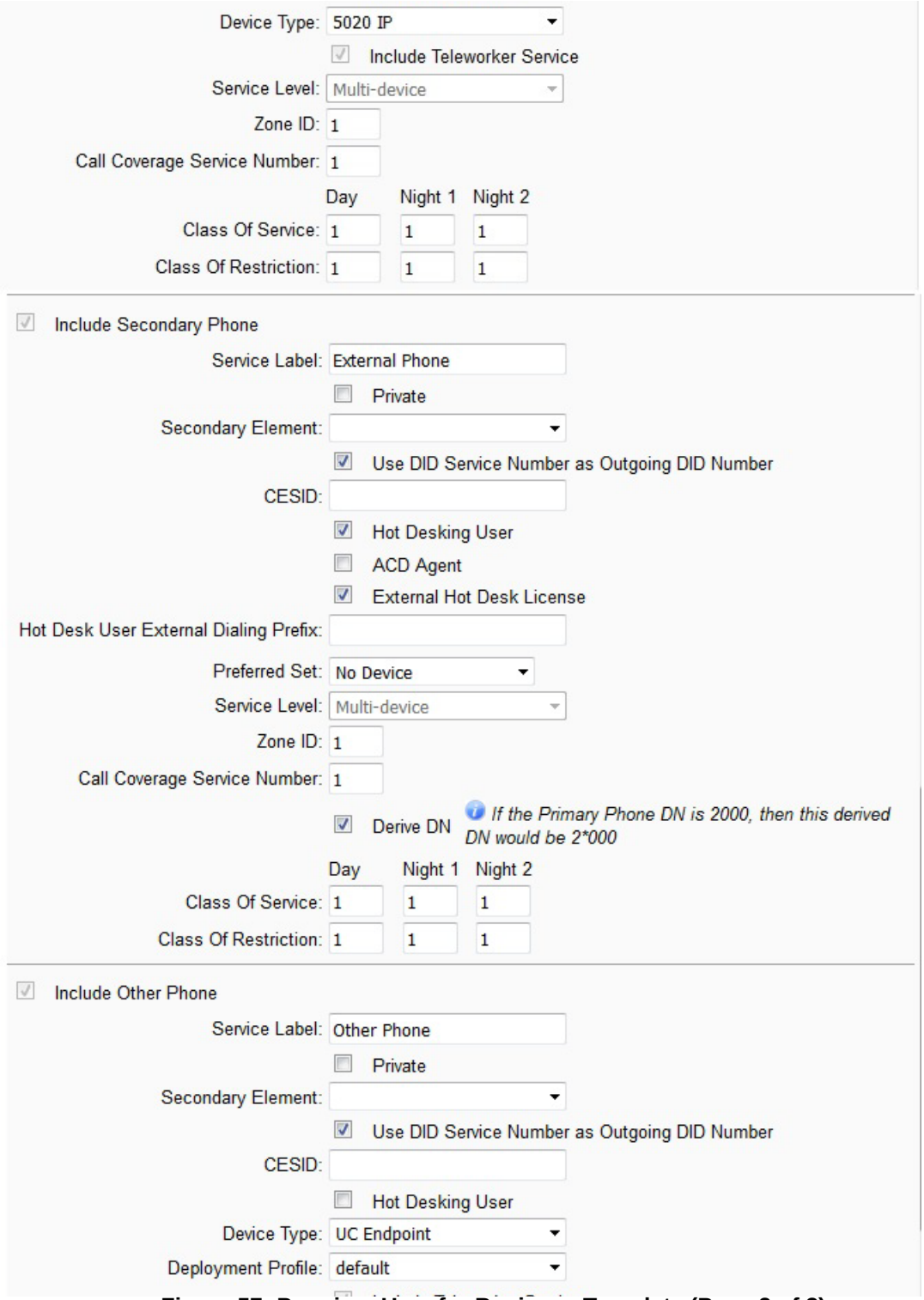

Figure 57: Premium User for Business Template (Page 2 of 3)

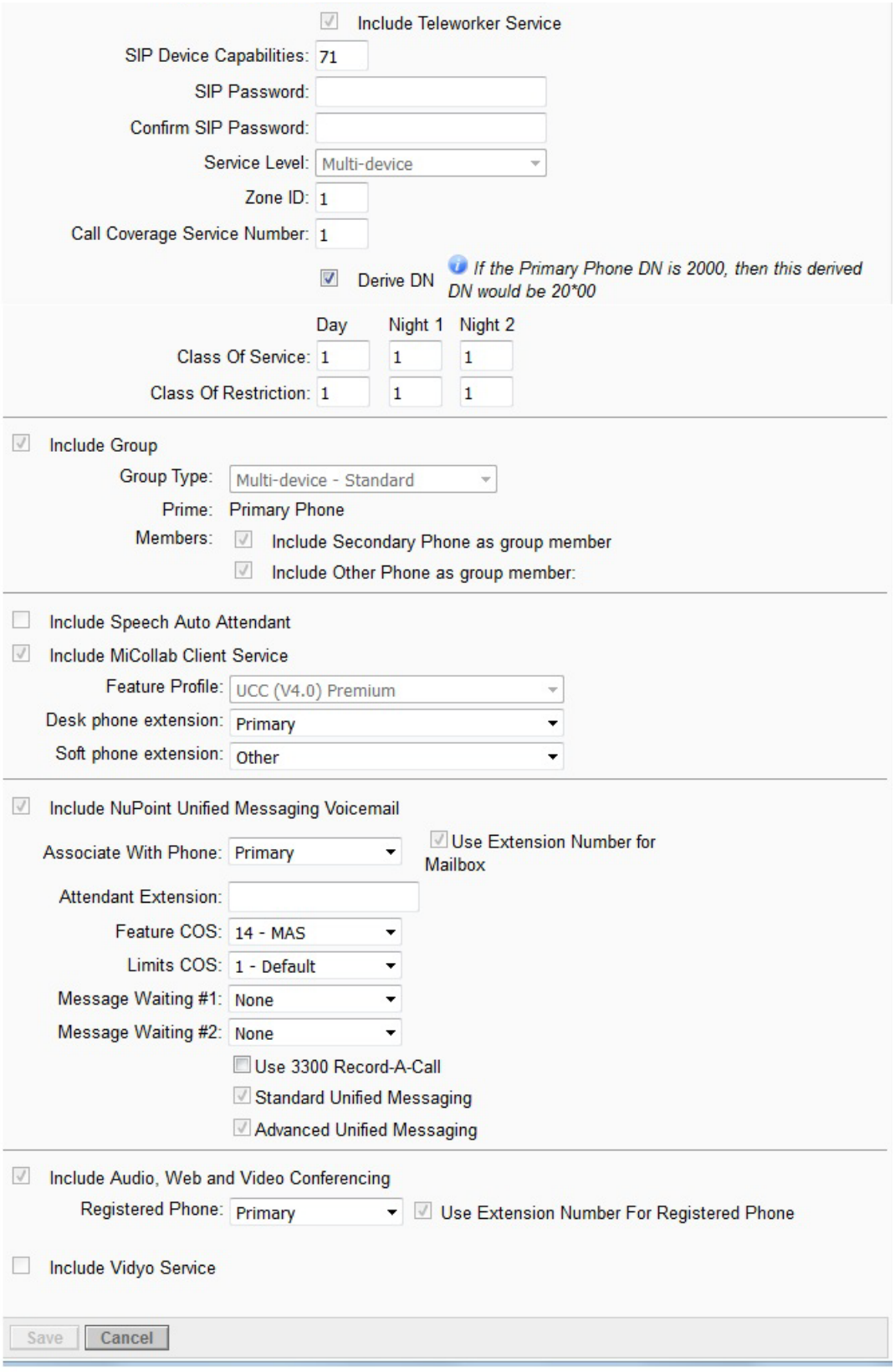

Figure 58: Premium User Template (Page 3 of 3)

Appendix B

DEPLOYING DIRECTLY TO AN EXSI HOST

INTRODUCTION

This appendix provides instructions on how to deploy the MiVoice Business Express OVA using vSphere 5.0, 5.1, or 5.5 when connected directly to an ESXi host.

DEPLOYING DIRECTLY TO AN ESXI HOST

OVERVIEW

- 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
- Run Initial Configuration Wizard.

CONDITIONS AND LIMITATIONS

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

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

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

In an environment without vCenter, where MiVoice Business Express is deployed using vSphere connected directly to an ESXi server, the Application Configuration Properties screen is not available. Therefore, you must access the MiCollab server console and configure the system with its network addresses, admin password, and ARID. After you complete this network configuration, you launch the Initial Configuration Wizard to complete initial configuration.

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 MiCollab server console.

PERFORM NETWORK CONFIGURATION THROUGH MICOLLAB SERVER CONSOLE

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

1. Right-click on the newly created MiVoice Business Express (for example: MiVoice Business Express 6.2.3.0 build) and select **Open Console**. The MiVoice Business Express virtual appliance console opens within the vSphere Client.
2. Power on the MiVoice Business Express VM by clicking the green button in the toolbar.
3. Click **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 MiCollab Server Console interface:

   - 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. 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 Express 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 MiVB-X 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**.
- 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 MiVB-Xserver 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.
- In the "Enter additional static IP address", you can optionally enter the WAN IP address that is to be used by the internet based MiCollab AWV clients.
- 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)” on page 169.

ADD TRUSTED NETWORK (OPTIONAL)

You will need to launch a web session to the MiVoice Business Express to run the Initial Configuration Wizard. In order to launch a web session from a computer that is located on a

different network than the MiVoice Business Express, you must first add that network as a trusted local network.

Note: If the computer is on the same network as the MiVoice Business Express, then you do not need to add a trusted network.

1. After the MiCollab server boots up, log into the MiVoice Business Express 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 you will launch the web session.
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.
8. Proceed to “Run Initial Configuration Wizard” on page 170.

RUN INITIAL CONFIGURATION WIZARD

Run the Initial Configuration Wizard. See “Run the Wizard” on page 78 for instructions. The steps are the same as those when you deploy using vSphere on a ESXi host via vCenter with the following exceptions:

- You must enter the LAN IP Address #2 (MiVoice Business IP address) in the Initial Configuration screen.
- You are prompted to provide an old password in the New Password screen. Enter the administrator password that you created during network configuration from the MiCollab Server Console.

Appendix C

MICOLLAB CLIENT DEPLOYMENT

ABOUT MICOLLAB CLIENT DEPLOYMENT

This appendix provides instructions on how to deploy MiCollab Clients for MiVoice Business Express. The MiCollab Client Deployment blade in the MiCollab server manager supports the simplified deployment of MiCollab for Mobile.

End users are no longer required to enter configuration settings such as server and SIP credentials. Administrators configure these settings and MiCollab for Mobile clients are deployed Over the Air (OTA). The administrator portal enables administrators to:

- deploy large groups
- leverage profiles
- download multiple files to the clients
- update clients

DEPLOY MICOLLAB FOR MOBILE CLIENTS

To deploy MiCollab for Mobile clients with MiVoice Business Express:

1. Log into the MiCollab Server manager,
2. Under **Applications**, click **MiCollab Client Deployment**. Refer to the MiCollab Client Deployment online help for instructions on how to complete the following steps:
   - Define the deployment configuration and configure MiCollab Client Deployment.
   - Add connections to MBGs.
   - Add profiles.
   - Customize deployment email.
3. Program a SIP device on the MiVoice Border Gateway:

   For MiVoice Business platforms, you must first provision a SIP device in the MiVoice Border Gateway for the MiCollab for Mobile Client. This allows the Set Side Username/Password to be synchronized with the MiCollab Client Deployment application when you add the user or phone to the MiCollab Client Deployment through the MiCollab Users and Services (USP) application. The ICP SIP password and Directory Number that you use to provision the SIP device on the MiVoice Border Gateway must match the SIP password and Directory Number that you use to add the user's UC Endpoint in the Users and Services application.

   - Log into the MiCollab or standalone MiVoice Border Gateway server manager.
   - Click **MiVoice Border Gateway**, click **Service configuration**, and then click **SIP devices**.
   - Select **+** (add).
   - Check the **Enabled** box.
   - In the **Set-side username** field, enter the user's name. You will need to enter the same user name in the MiCollab Users and Services application.

- In the **Icp-side username**, field, enter the SIP softphone extension. You will need to enter the same extension number for the SIP softphone in the MiCollab Users and Services application.
- In the **Configured ICP** field, select the name of the MiVoice Business Express.
- Enter the **Set-side password** and **Confirm set-side** password. The Set-side password is the SIP password that you need to provision and communicate to the end-user. They use this password to log into their End-User portal or UCA desktop client portal.
- Enter the **Icp-side password** and Confirm icp-side password. The Icp-side password is the SIP password that you will enter in the USP Quick Add template. The system configures this password on the MiVoice Business. If the Icp-side password does not match with the password on the MiVoice Business, the SIP client will be unable to register.
- In the **Description** field, enter the Softphone extension.
- Click **Save**.

4. 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 fromthe 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 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.