MiCloud Flex Deployment Guide (Google Cloud)

May 2021

Mitel®

Notice

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

Trademarks

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

Contents

Revision History

Document Version	Document Release Date	Description
1.0	15 May, 2020	Initial release
2.0	14 Aug, 2020	Updated: • *Supported Applications* section • Sample welcome email under *Prerequisites* section • *Configuring Resiliency* section • *Addendum Endpoints* section to add information about RCS (Redirection and Configuration Service)
3.0	29 Oct, 2020	Made the following changes for bundle 1.2: • Added *Onsite Gateway* section • Added *Support for 5300 Phones* section • Added *Clearing Hardware IDs using AMC* section • Added *Emergency Services – MPA Notification Programming* section • Added *Configuring Voice Mail Resiliency for Onsite Gateway* section • Updated sample welcome email under *Prerequisites* section which contains details of the onsite gateway • Updated *Setting up Mitel Interaction Recording* section • Updated *Addendum MiVB* section to mention that the Nupoint Messaging feature is not available in MiVoice Business for the MiCloud Flex solution • Updated *Configuring DHCP Option 125 or 43* section • Updated *Troubleshooting MiCloud Flex Issues* section
4.0	20 Jan, 2021	Added step 2 in the section *Setting up MiCollab post ICW* for MiCollab Client resiliency.
5.0	25 May, 2021	Added a note regarding restoring a database in the section *Restoring MiCloud Flex Solution*.

Introduction

This chapter contains the following sections:

Purpose

This guide is designed to give you an overview of Mitel's MiCloud Flex solution, architecture, management components, and topology.

This guide is designed to give you a deployment overview of Mitel's MiCloud Flex solution.

Audience

This guide is for the Mitel partners, solution architects and network administrators who use the MiCloud Flex solution.

About MiCloud Flex Documentation

The documentation set consists of guides in PDF format and online help systems that are integrated with the various management applications. The following documents are the main source of information for the MiCloud Flex solution:

- MiCloud Flex General Information Guide
- MiCloud Flex Solution and Engineering Guidelines
- MiCloud Flex Deployment Guide
- Solution Manager Online Help
- Initial Configuration Wizard (ICW) Online Help

Additional guides and help systems are available that provide instructions on how to configure and use the individual Mitel applications that are supported on MiCloud Flex. The complete documentation set is listed in the *Appendix*.

To access the MiCloud Flex product documentation set:

1. Access Mitel Document Center (URL: http://www.mitel.com/document-center).
2. From Document Center you can either:
   - Navigate to the respective document.
   - Use the search functionality to search for the document that you want to access.

     NOTE: Ensure that you select Document Center as the search repository before clicking the search icon.

Overview

This chapter contains the following sections:

Overview of MiCloud Flex

MiCloud Flex is a Mitel unified communications (UC) and collaboration solution built on Google Cloud and encompasses a full suite of Unified Communications and Contact Center solutions. Unified communications (UC) is a term that implies real-time integration of voice, data, and video communication. Without UC, a user's voice mail, email, video conferencing, voice conferencing, chat, and desktop-sharing applications are independent and require separate interaction.

A rich UC solution delivers a user experience that integrates all communication tools into a unified experience. With a UC solution, a user can seamlessly choose the medium they want to use without affecting the medium that other participants are using. For example, users may attend a meeting from different locations using a combination of text, voice, or video technologies without affecting other attendees. Combined with real-time presence, each participant knows what options are available for communicating with another participant. UC provides a user with a consistent unified experience across multiple devices and media types. For a complete list of applications available on MiCloud Flex, see *Applications Supported on MiCloud Flex*.

NOTE: This general information guide provides a high-level overview of the solution. For MiCloud Flex deployment, see *MiCloud Flex Deployment Guide*.

Onsite Gateway

Customers who connect to MiCloud Flex through private networking (MPLS or SD-WAN) via Point-of-Presence (PoP) may choose to deploy an onsite gateway. This gateway can support local analog extensions as well as local functions such as paging adapter support or music on hold. It can also support local PSTN connections via PRI E1, PRI T1, or analog trunks. IP phones located at this site, registered to MiCloud Flex, can optionally fail over to this gateway instead of to a controller in a secondary data center. This would enable local voice extension calling at the gateway site should the primary controller become unavailable.

Resilient voicemail service can also be provided by the onsite gateway using the embedded voicemail capabilities of the gateway. Configuration of resiliency is on a per-set and per user basis. Some IP phones and users at the site can be administratively programmed to failover to the onsite gateway while others can be configured to fail over to the secondary data center.

The onsite gateway is a Mitel MiVoice Business controller running Release 9.1 or higher. This minimum release is required in order to support Fully Qualified Domain Name (FQDN) addresses. The onsite gateway can be monitored from the MiCloud Flex MPA.

MiCloud Flex users at this site are registered to the MBGs or controller in the MiCloud Flex deployment. They receive their primary voice services from MiCloud Flex. In a failover scenario, if the MiCloud Flex

users are programmed to fail back to the onsite gateway, they can then receive their PSTN services from the onsite gateway. Analog users connected to the onsite gateway, as well as IP set users who are not MiCloud Flex users, may receive their PSTN services from the onsite gateway or via the centralized trunk services in the cloud depending upon configuration and licensing.

Requirements for Onsite Gateway

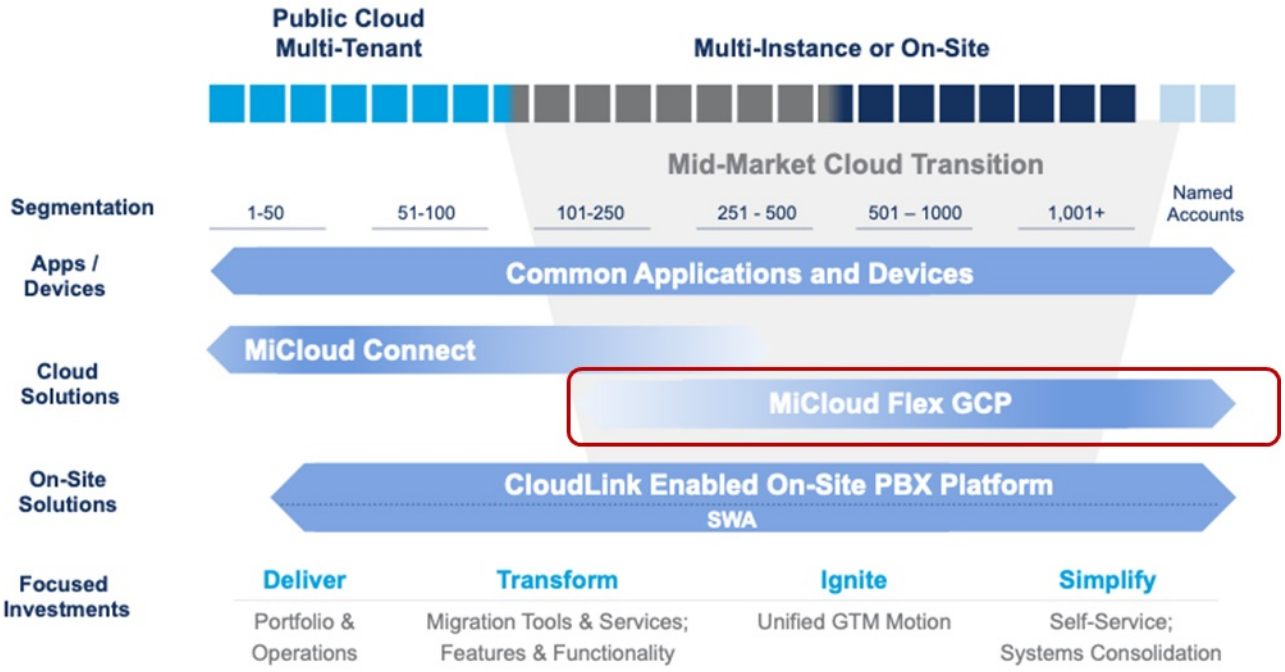
- **Controller Hardware** - New customers will purchase or lease an EX or AX to be the onsite gateway. Existing customers with controllers that can be upgraded to MiVoice Business 9.1 and above may use them as MiCloud Flex Onsite Survivable Gateways. For a list of supported controllers, see the MiVoice Business Migration Guidelines document.
- **IP Set Hardware** - The introduction of onsite gateway does not alter the list of supported IP phones that can register to MiCloud Flex. The onsite gateway will still support the same phones as an on-premise MiVoice Business of the same release.
- **Software** - The onsite gateway software must be running release 9.1 or newer because FQDN support is required for this solution. It is recommended to upgrade the onsite gateway software to the same MiVoice Business release as what is in the MiCloud Flex offering.
- **PSTN Connectivity** - The onsite gateway supports PSTN connectivity via local analog and E1/T1 links. It does not support PSTN connectivity via SIP.
- **Connection to MiCloud Flex** - The connection between the onsite gateway and MiCloud Flex is via Mitel proprietary IP trunks. These trunks need to be enabled at firewalls to allow calls on the local gateway to be routed to other phones that will be registered with MiCloud Flex. This connection must support FQDNs.
- **Embedded Voice Mail (EMEM)** - There are different capacities and functionality between what is supported by EMEM in MiCloud Flex and what is supported by EMEM in an onsite gateway. For further information on capacities, see to the MiVoice Business Engineering Guidelines.
  - Mitel 3300 ICP platforms support 20 or less Voice Mail ports, versus up to 120 in MiCloud Flex and other x86 platforms.
  - Mitel 3300 ICP platforms support 750 or less Voice Mail boxes, versus up to 5000 in MiCloud Flex and other x86 platforms.
  - Call Flows are only supported in MiCloud Flex currently. The feature is under consideration for adding support in a future release on the x86 platforms including EX (not 3300s)
  - EMEM Auto Attendant programming on the gateway is a manual process. The Hunt Group pilot number will most likely be different than the one initially setup using the Initial Configuration Wizard on the resilient MiCloud Flex pair. If the hunt group pilot number must be the same on all the systems in the cluster, you must mark the hunt group pilot number on all systems as Local Only.
- **MiVoice Border Gateway (MBG)** - Local MBGs providing SIP connectivity, teleworker or SRC are not supported at the local gateway.
- **MiCollab** - You must setup onsite DNS server and MiCollab Client Deployment profile for each resilient pair where onsite gateway is involved. This is required only for MiCollab Clients registering directly to MiVB over MPLS network. For more information on how to add or modify MiCollab Client Deployment Profile, see MiCollab Client Deployment Web Help > Deployment Profiles > Add or Modify a Profile page available on Document Center. For information on DNS, see the MiCloud Flex Solution Engineering Guidelines document available on Document Center.
- **Mitel Business Analytics (Tollring)** - If an update is made to the user profile in the Mitel Business Analytics portal, you must restart the tollring probe from the Solution Manager GUI so that the updated user profile can be downloaded and then connect to configured PBXs.

Market Segments

The market for MiCloud Flex are customers who:

- are of 150+ users in general; but need a solution that can scale beyond this as well
- need complete control over upgrades and maintenance schedules
- want to customize their deployments with integrations to their business workflows
- require optional capabilities including contact/call centres, and call/screen recording
- are highly mobile and may use multiple devices
- want the deployment over dedicated network connections, such as MPLS
- want the deployment in a secure dedicated customer instance

The following illustration shows the market segmentation for MiCloud Flex.



MiCloud Flex Benefits

The MiCloud Flex solution offers various benefits including the following:

- **Dedicated Instance Solution** - MiCloud Flex is deployed in a dedicated and secure environment that cannot be accessed by other organizations. The solution also allows more secure access to customers who are sensitive about using the public internet for accessing data. MiCloud Flex solution offers private and secure network links for such customers. The customer has full and complete administrative rights to the system. Google Cloud meets rigorous privacy and compliance standards that test for data safety, privacy, and security.
- **Customization and integration** - MiCloud Flex offers easy and extensive integration with popular back-office cloud solutions, such as CRM, ERP and other apps, and turns a cloud communications system into a hub that enhances productivity and collaboration.

- **Maintenance and Updates** - With MiCloud Flex you can perform your upgrades and other maintenance activities during a specified time frame of your choice. This helps reduce the overall impact of system downtime and outages.
- **Purpose-built communications solution** - MiCloud Flex uses the same communication, collaboration, and contact center applications as on-site platforms. Users have access to the same easy-to-use features and functionality whether they are in the main office, working from a remote location, or on the road. With MiCloud Flex, Mitel offers full PBX, applications, and contact center features thereby providing customers with more reliability and flexibility.
- **Integrated Omnichannel Contact Center** - MiCloud Flex Contact Center is an optional all-in-one contact center platform designed to enable exceptional customer experiences anywhere, anytime and is integrated with our communication platform. It leverages Google Artificial Intelligence (AI) capability, drastically reduces the complexity associated with integrating multiple tools and generates deep insights into data and performance.
- **Devices, Endpoints, and Applications** - A robust suite of Mitel desktop endpoints that enhances the communication experience for businesses at all levels. Mitel owns and develops the hardware and software, and offers tight integration with collaboration tools in a harmonized ecosystem, which results in improved employee productivity.
- **Emergency Services** - Emergency call routing and notification is as per standard MiVoice Business practices. The existing resiliency guidelines also apply to the onsite gateway

Partner Prerequisites and Requirements

At Mitel, our partners form the cornerstone of our success. We value the investment our partners make to effectively position and deliver our solutions.

The Mitel MiCloud Flex program strategy aims to:

- Offer their customers a path to move to the cloud while maintaining full control of their existing customer relationships and experience
- Align and provide a uniform Mitel partner experience
- Provide an opportunity to build a new business model with an innovative OPEX solution to build and increase MRR
- Provide Mitel partners an opportunity to leverage attained competencies
- Provide process improvements in the areas of:
  - Activations
  - Offering additional Services
  - Support
- Improve customer experience by creating loyal customers

Following are the prerequisites that each Mitel partner must meet:

- Complete all the requisite Mitel training and certifications
- Expertise with the various network monitoring tools to identify and triage problems in the MiCloud Flex Applications that are deployed for customers

In the Mitel MiCloud Flex program, the partners are responsible for:

- Sales and provisioning
- Site surveys, discovery sheets, user provisioning, and on-site deployment

- Customer onboarding
- Level 1 and Level 2 customer support

MiCloud Flex Management Components

This chapter contains the following sections:

The key management components of MiCloud Flex are:

- **Solution Manager**- Solution Manager provides navigation to other applications such as MiVoice Business, MiCollab, MiVoice Border Gateway, Initial Configuration Wizard. It is also used to configure functions that are common for all the applications.
- **Initial Configuration Wizard (ICW)** - ICW allows you to configure the system with the basic settings required to get the solution up and running.
- **Mitel Performance Analytics (MPA)** - Mitel Performance Analytics is a fault and performance management system designed to provide users with fast actionable problem resolution so that optimal service quality levels are maintained for end-customers. Mitel Performance Analytics provides real-time alerts, detailed reporting, and ubiquitous accessibility with secure remote access.

Solution Manager

Solution Manager supports a suite of managed services and applications delivered from the MiCloud Flex solution.

Solution Manager is a GUI that provides:

- Navigation to other applications such as MiVoice Business, MiCollab, MiVoice Border Gateway, and Initial Configuration Wizard
- System User Administration
- Time Zone Configuration
- AMC Synchronization
- Backup and Restore
- SNMP Configuration
- Mitel Performance Analytics (MPA) Probe
- Mitel Business Analytics
- Solution Information
- Log files

Initial Configuration Wizard

The Initial Configuration Wizard (ICW) is launched from the Solution Manger GUI. You only run ICW once on the primary deployment during the initial configuration of the system. ICW allows you to configure the system with the basic settings required to get the solution up and running. After completing the wizard, the wizard configures the system with your settings. ICW guides you through the following configuration steps:

- Review initial configuration parameters
- Configure resiliency
- Configure administration email and servers
- Configure languages
- Configure numbering plan
- Configure SIP Trunking (optional)
- Configure incoming call configuration
- Select and configure SIP provider
- Configure MPA Probe
- Configure optional services: AWV, Hot Desking, and Music on Hold
- Change the administrator password for MiVoice Business
- View a summary of the configuration
- Download Logs

NOTE: For more information about ICW, see the online help that is part the ICW application.

IMPORTANT: ICW does not configure MiContact Center Business, Wordkforce Optimization, and MiTeam Meetings.

Mitel Performance Analytics

Mitel Performance Analytics (MPA) provides fault, inventory, and performance management for Mitel Networks Unified Communications systems, multiple enterprise VoIP systems, and associated network infrastructure, both LAN and WAN. MPA supports monitoring and remote access both for private networks, such as enterprise LANs and MPLS, and for public networks or Internet-reachable devices, such as access routers. MPA has two major components: the Mitel Performance Analytics server and the Probe.

MPA can be used in Small Medium Businesses, Medium Large Businessess, and Scalable architectures.

The MPA portal is used to monitor the health of your system. Before you can view the health of your system you must establish a connection between the MPA portal and your solution. The MPA Probe enables secure communication between Mitel Performance Analytics and the customer's MiCloud Flex instance. It also acts as a data collector between Mitel Performance Analytics and the monitored devices. The monitored devices send their data to MPA probe, which securely relays the data to Mitel Performance Analytics. The MPA probe activation URL is configured initially through the ICW.

NOTE: You also use the MPA portal to perform scheduled backups and upgrade procedures.

Mitel Performance Analytics (MPA) is available with Mitel's Premium Software Assurance subscription. MiCloud Flex on Google Cloud is available with Mitel Performance Analytics Plus licensing. The MPA Plus license is deployed in the cloud for the MiCloud Flex on Google Cloud solution. MPA provides:

- VoIP Quality monitoring and visualization for MiVoice Business, Mitel SIP sets, and MBG (Teleworker and SIP trunk)
- Real-time and historical fault and performance monitoring
- Alarm management tools (dashboards, alerting, and views) and alarms analytics tool that customizes the alarm management environment according to the behavior of the user and others. Alarms that are deemed to be the most important to the user are shown first. Contains advanced tools for determining related alarms.

- Display of dynamic health status icons over user-supplied network diagram, with devices and containers arranged according to user preferences
- Flexible container architecture allowing users to configure data reporting to match their size and organization (for example, data reporting according to geographical locations, functional or organizational groupings, or customer groupings)
- IP SLA monitoring
- Supports multiple internationalized character sets for content entry into Mitel Performance Analytics
- Branded dashboard can be created for service providers, resellers, and customers
- Resellers can choose any URL they own for their Mitel Performance Analytics login page
- Emergency Response (ER) alarm monitoring and alerts from MiVoice Business
- Support for SNMP based third-party devices and applications
- Advanced user, set, and service inventory reporting for MiVoice Business and MiVoice Border Gateway
- Device and extension inventory for MiVoice Business and MiVoice Border Gateway
- Agent-based network testing to assess, monitor and troubleshoot the availability, capacity, and performance of the network
- Solution-wide backups, stored in the cloud
- Trunk capacity reporting for MiVoice Business
- Audio, web, and video port usage reporting for MiCollab
- Upgrade and backup support

Applications Supported on MiCloud Flex

This chapter contains the following sections:

Supported Applications

The MiCloud Flex solution provides a rich feature set encompassing core voice capabilities with an extensive telephony feature set, and a customizable UC feature set including mobility capabilities. The solution architectures rely on several common product and application portfolio elements to deliver this functionality.

The following table lists the applications that are supported with this release of MiCloud Flex solution. Based on the requirements, Mitel can recommend a package, a combination of one or more of these applications, that is best suited for your customer.

Application name	Release Number	Classification	Link to Documentation
MiVoice Business	9.1	Call Manager/PBX	https://www.mitel.com/document-center/business-phone-systems/mivoice-business/mivoice-business
MiCollab	9.1.3	Collaboration Application	https://www.mitel.com/document-center/applications/collaboration/micollab
MiVoice Border Gateway	11.1	Session Border Controller	https://www.mitel.com/document-center/applications/mivoice-border-gateway

Application name	Release Number	Classification	Link to Documentation
MiContact Center Business	9.2 SP2	Contact Center Application	https://www.mitel.com/document-center/applications/contact-center/micontact-center-business/micontact-center-business-for-mivb
Mitel Interaction Recording (ASC Call Recorder)	6.x	Call Recording Application	https://www.mitel.com/document-center/applications/contact-center/call-recording/mitel-interaction-recording-powered-by-asc
Mitel Workforce Management (WFM)	11.5	Workforce Engagement Management Suite	https://www.mitel.com/document-center/applications/contact-center/workforce-management
Mitel Business Analytics	3.7	Business Analytics Application	Accessible from the application user interface
Mitel Performance Analytics	3.1	Performance Analytics Application	https://www.mitel.com/document-center/applications/analytics/mitel-performance-analytics

MiVoice Business

MiVoice Business includes an extensive number of applications and system features that enable effective and efficient communications. These applications enhance communication, productivity, accessibility, and mobility, and support the specialized site requirements of businesses and institutions such as hotels, hospitals, schools, military sites, and contact centers.

Call control

The MiVoice Business call control engine provides sophisticated call management, applications, and desktop solutions to businesses. MiVoice Business is a proven, highly scalable, resilient, and robust call control engine.

The MiVoice Business architecture uses the IP network to connect IP telephony devices together.

If support for TDM telephony is required, then the same can be deployed.

Embedded voice mail

MiVoice Business includes an integrated feature-rich voice mail system. The number of ports are auto configured based on the number of mailboxes at time of order.

MiCollab

MiCollab unifies Mitel applications into an easy to use, cost effective communications solution. The MiCollab applications include:

- MiCollab Client (including Visual Voicemail integration with MiVB EMEM) – provides contact management, dynamic status, instant messaging, and audio conferencing
- MiCollab Audio, Web, and Video Conferencing – provides web conferencing, supporting audio, video, chat (text) and presentations
- MiCollab Suite Application Services – provides user services provisioning, centralized management of shared system resources and license management. It also offers the administrator and My Unified Communications portals.
- MiTeam Meetings – provides MiCollab users with the ability to initiate Mitel Meetings from their MiCollab Client
- Persistent Chat – provides comprehensive Instant Messaging features from any devices (Web, desktop applications, mobile applications)

MiCollab Audio, Web, and Video Conferencing

MiCollab Audio, Web, and Video Conferencing allows users to schedule and hold audio and web conferences. MiCollab Audio, Web, and Video Conferencing supports three types of conferences: Audio and Web, Audio-only, and Web-only.

Audio conferences allow users to:
• upload documents to present to callers during a conference call • mute, drop, or add participants and place individual participants on hold while the call is in progress.
Web conferences allow users to:
• upload documents, transfer files, record the conference, chat on-line, and broadcast videos • share applications or desktop and use white board features.
Users access and manage their conferences using:
• MiCollab Audio, Web, and Video Conferencing Desktop client. Allows users to schedule and join audio and web conferences. The desktop client supports two-way audio participation. • MiCollab Audio, Web, and Video Conferencing Web portal. Allows users to schedule and view conferences with listen-only audio support. The web-based interface is integrated into MiCollab End-User Portal.

Conferences can be initiated immediately or scheduled in advance. MiCollab Audio, Web, and Video Conferencing may be integrated with corporate directories and personal address books from Microsoft

Outlook and Lotus Notes. Optionally, conference accessibility requires personal identification for added security. MiCollab Audio, Web, and Video Conferencing supports recording conference calls and collaborative sessions for later playback. Call Detail Records (CDRs) provide a log of all calls with dates, times, and call durations for audit and billing purposes.

MiCollab Audio, Web, and Video Conferencing has additional IP network configuration requirements. For detailed networking information, see the MiCloud Engineering Guidelines.

MiTeam Meetings

MiTeam Meetings application is Mitel's Cloud-based collaboration tool (based on CloudLink infrastructure) that provides MiCollab users with the ability to initiate Mitel Meetings from their MiCollab Client. With MiTeam Meetings you can:

- Manage collaboration meetings
- Hold chat sessions and receive chat notifications
- Store and share files
- Perform audio, video, and web sharing

MiTeam Meetings is supported with the following MiCollab Clients:

- MiCollab for PC Client
- MiCollab for Mac Client
- MiCollab Web Client
- MiCollab for Mobile Client (iOS/Android only)

For information about MiTeam Meetings end-user features, see MiCollab Client End-User Online Help.

CloudLink Chat

CloudLink Chat is a chat engine for MiCollab that is powered by Mitel's CloudLink infrastructure/platform. CloudLink Chat functionality is used by MiCollab and optionally MiContact Center Business is hosted in Amazon Web Services (AWS) cloud. The key capabilities of CloudLink chat engine are:

- Persistent chat messages are synchronized across all their MiCollab clients – so no longer is the chat history only presented on the client/device where the chat was originated or responded from. Now users can stop the conversation on one device and seamlessly pick it up on another.
- All chat messages collected and made available to the user when they access the client – including those during the period that their MiCollab client was turned off
- The ability to always be available to send chats even when access/connectivity to the MiCollab server is not possible
- The ability to share files
- The ability to share their location details
- The ability to share audio instead of text
- A robust Emoji picker
- To reply to a select post within the chat through text or select emojis
- To provide @Mentions

MiVoice Border Gateway

MiVoice Border Gateway (MBG) is a platform for the secure deployment of multiple services in a variety of network configurations. MBG provides the following services:

- **Teleworking**- remote MiNET and SIP access (Teleworker) for IP phones connecting to the MiCloud Flex solution over the Internet
- **SIP Trunking**- SIP trunking provided to the MiCloud Flex solution
- **Secure Call Recording**- call recording solution that allows third-party recording equipment to record Mitel encrypted voice streams
- **WebRTC**- gateway to support browser-based voice and video calling

MiContact Center Business

NOTE: MiContact Center Business is an optional application that is provided with the MiCloud Flex solution.

MiContact Center Business provides a modular suite of applications for streamlining contact center management, and enabling voice and multimedia contact center functionality. The applications included in MiContact Center Business are:

- **Contact Center Management (CCM)** - This is the core application. It provides historical and real-time reporting and forecasting for all agents and queues. CCM supports customizable notifications and replay of real-time data, and is also used to configure, manage, and maintain the contact center configuration and database.
  - **MiVoice Business Reporter** - Allows reporting and monitoring of general business extensions and ring groups, including traffic analysis reports.
  - **MiVoice Call Accounting** - Supports call costing to track the cost of incoming and outgoing calls and adjust costs based on carrier reports. Provides services to track subscribers' use of services, and to adjust prices based on fixed rates.
- **Interactive Contact Center** - Allows supervisory control over agent availability and queue states and agent control over their own availability. It includes an interactive visual queue that enables identifying contacts, along with the capability to manually control the position in queue, and view abandoned calls with call back option.
- **Messaging and Routing** - Routes calls to the most appropriate group based on caller and call center statistics, such as type of service, agent skills, agent availability, idle time, and queue conditions. MiContact Center Business supports either Messaging and Routing ports or IVR ports, but not both in the same Enterprise server.
- **Contact Center IVR** - Provides intelligent routing of voice calls based on call meta-data, caller menu choices, and call center statistics. It can be configured to collect and verify information with external data sources, enable callers to request call backs, enable caller self-service capabilities, and run outbound dialing campaigns. Contact Center IVR includes the Visual Workflow Manager tool to facilitate configuration.
- **Multimedia Contact Center** - Provides queuing, inbound and outbound routing, and real-time and historical reporting functionality for email, real-time chats, SMS messages, and social media interactions. Multimedia Contact Center also includes graphical tools to facilitate maintaining workflows. These workflows may include self-servicing and intelligent routing for all media types.

- **Flexible Reporting** - When used with Contact Center Management, allows for the creation and customization of reports based on the contact center data. Reports use a spreadsheet look and feel, allowing a quick learning curve.

Mitel Interaction Recording

Mitel Interaction Recording (also known as ASC Call Recorder) suite captures, saves and archives multiple communication channels including mobile voice, video, and chat for financial institutions, contact centers and public safety organizations. The recording suite provides you with communications recording and quality management as a service whereby capacities and features can be added as needed to react quickly and grow in the long-term. The solution offers the following capabilities:

- State-of-the-art recording and analysis for complex infrastructures
- Systematic capture and assessment of customer communications
- Solutions for financial institutions, contact centers and public safety organizations
- Compliance with the highest security requirements and regulations such as MiFID II

Mitel Workforce Management (WFM)

Mitel Workforce management (WFM) is a top Workforce Management solution that encompasses everything needed to plan and successfully manage a contact center, back office, branch or store. Mitel WFM provides a feature-rich solution that includes tools to manage staff, accurately forecast demand, and automatically schedule, report, and improve a company's operations. Several package options exist to further tailor the WFM to your needs. These include the WFM Advanced and Premium offerings – including multi-skill, multi-site, multichannel support, agent self-service, gamification, full intraday capabilities and real-time adherence functionalities.

The Connector, included with any purchase of Mitel WFM offering, fully supports voice and multimedia agent data (including all supported media types and open media). This enables the WFM solution to perform forecasting, scheduling, and reporting of MiContact Center Business multimedia agents.

NOTE: WFM is hosted in Microsoft Azure cloud.

Mitel Business Analytics

Mitel Business Analytics is a fully integrated multi-tenant call analytics and call recording service which allows you to monitor business-critical call metrics by accessing real-time reports, configurable dashboards, and visual wallboards. Mitel Business Analytics has two call analytics modules, namely Insight and Report. Insight provides powerful data visualization via an intuitive dashboard and essential wallboard. And the Report module delivers enhanced level reporting and call accounting. If enabled in your solution, you access Mitel Business Analytics by creating a DCID (Delivery Controller ID) and providing the Reseller URL of that region in the Solution Manager GUI.

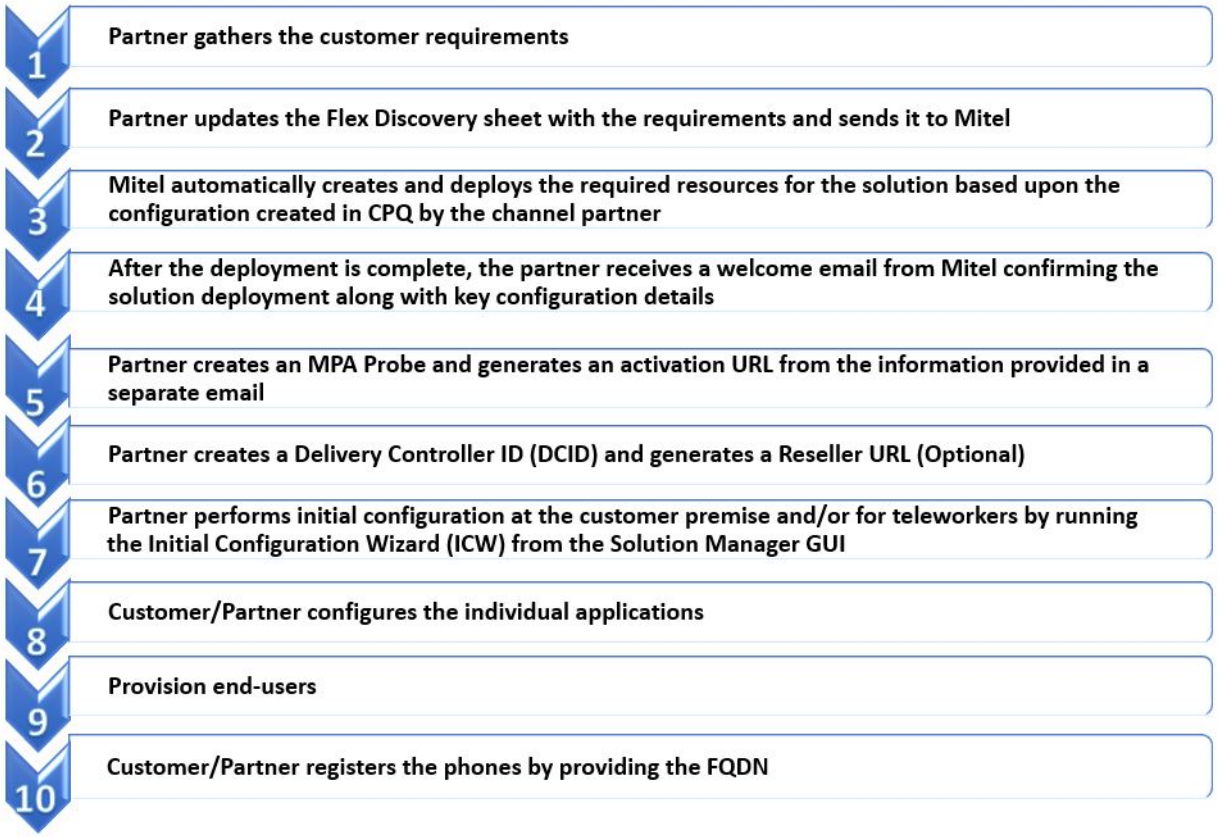
NOTE: Contact your deployment engineer to get the DCID and Reseller URL. Mitel Business Analytics is hosted in Microsoft Azure cloud.

MiCloud Flex Deployment

This chapter contains the following sections:

MiCloud Flex Deployment Workflow

The following illustration depicts the end-to-end workflow that needs to be followed to deploy MiCloud Flex.



Deployment Steps

To deploy MiCloud Flex, you need to complete a series of tasks arranged in a set sequence. The table below lists these tasks (and the sequence) that need to be completed.

	Task	Owner	Description
1.	Collects the information from the customer	Channel Partner	The partner collects the following information. • Customer Sites • User Profiles • Agent Profiles • Endpoints • Accessories
2.	Partner sends the completed discovery sheet to Mitel	Channel Partner	For more information about the GCP resources and capabilities, see MiCloud Flex Engineering Guidelines.
3.	Create and deploy the required resources for the solution based upon the configuration created in CPQ by the channel partner	Mitel	
4.	A welcome email is sent	Mitel	Welcome email contains the deployment details such as the public FQDN (which the partner provided) and IP addresses of the applications with user names and passwords. For more information about getting started with MiCloud Flex, see *Getting Started with MiCloud Flex*.
5.	Create MPA Probe Activation URL	Channel Partner	For more information about MPA integration, see *MPA Integration with MiCloud Flex*.

	Task	Owner	Description
6.	Create Mitel Business Analytics DCID and Reseller URL	Channel Partner	For more information about Mitel Business Analytics integration, see *Mitel Business Analytics Integration with MiCloud Flex*.
7.	Perform initial configuration	Channel Partner	1. Configure EMEM Resiliency. See *Configuring Resiliency*. 2. Run the Initial Configuration Wizard (ICW) from the Solution Manger GUI.
8.	Configure the applications after running ICW	Channel Partner or Customer (System Administrator)	For more information about configuring the applications, see the corresponding product documentation *Appendix*.
9.	Provision end-users	Channel Partner or Customer (System Administrator)	For more information on end-user provisioning, see the corresponding product documentation *Appendix*.
10.	Connect devices and installing client applications	Channel Partner or Customer (System Administrator)	For more information about connecting the devices and managing client applications, see the corresponding product documentation *Appendix*.

Before you Begin

This chapter contains the following sections:

Creating MPA URL in MPA portal

1. Log into the MPA portal.
2. Click **System Administration** > **New Container**.
3. In the **New Container** page, provide the following information:
   a. Under **General**, enter the name of the solution.
   b. Under **Voice Quality**, select the **Display VQ** check box.
   c. Under **Container Type**, select the type of container. Container types are used for data queries or reports.
   d. Under **Contact Information**, select the **Show on Dashboard** check-box and enter information for the following:
   - Account #
   - Contact Name
   - Phone #
   - Contact Email:
4. Click **Create**.
5. In the Dashboard on the left, click the Container just created.
6. Click **System Administration** > **Flex Creation**.

   The **Flex Deployment Wizard** opens.
7. Click **Start**.
8. In the **New Probe** page, do the following:
   a. Under **General**, enter the name of the probe.
   b. Under **Probe Diagnostics**, select the **Collect JVM Stat** and **Collect Probe Status** check-box.
   c. Under **Remote Access**:
      i. Select **To Monitored Devices Only** from the **Allow Port Forwards** drop-down.
      ii. Select the **I accept** check box to allow permissive port forwarding.
9. Click **Next**.
10. In **New MiVoice Border Gateway (K8s)** page, under **General** enter the name of application, for example MBG.
11. Click **Next**.

12. In the **New MiVoice Business (K8s)** page, do the following:
    a. Under **General**, enter the name of application, for example MiVB.
    b. Under **MiXML Credentials**, enter the MiVB system user name and password that is required to log in to the MiVB application.

       IMPORTANT: The credentials entered here must be the exact same as the credentials provided for MiVoice Business when Integrated Configuration Wizard (ICW) is run. If different credentials are used in the ICW, they must be updated here.
13. Click **Next**.
14. In the **New MiCollab (K8s)** page, under **General**, enter the name of application, for example MiCollab.
15. Click **Next**.
16. In the **New MiContact Center Business (K8s)** page, under **General**, enter the name of application, for example MiCC.

    NOTE: This step is optional. Enter the details only if MiContact Center Business is part of the deployment.
17. Click **Next**.
18. In the **New Workforce Optimization (K8s)** page, under **General**, enter the name of application, for example WFO.

    NOTE: This step is optional. Enter the details only if Workforce Optimization is part of the deployment.
19. Click **Next**.
20. In **New K8s Cluster** page, under **General** enter the name of cluster.
21. Click **Complete**.
22. The **Setup Complete** page opens which contains the Probe URL.
23. Click **Copy URL** to copy the probe URL and save the URL in a text file. This is the URL that needs to be provided in the ICW wizard to establish a connection between the MPA portal and your applications.

    NOTE: Do not generate a new Probe URL unless absolutely necessary. Doing so renders the existing URL invalid and the newly generated URL must be implemented in order for the Probe to function properly again.
24. Click **Return to Dashboard**.
25. On the left hand side you will see all the applications that have been added.

Creating Mitel Business Analytics DCID and Reseller URL

Mitel Business Analytics is a fully integrated multi-tenant call analytics and call recording service which allows you to monitor business-critical call metrics by accessing real-time reports, configurable dashboards and visual wallboards. If enabled in your solution, you access Mitel Business Analytics by creating a DCID (Delivery Controller ID) and providing the Reseller URL of that region in the Solution Manager GUI.

NOTE: Contact your deployment engineer to get the DCID and Reseller URL.

Clearing Hardware IDs using AMC

If you want to use the existing hardware IDs for new ARIDs on an existing gateway, you must first clear the hardware IDs for that controller in the Mitel Application Management Center (AMC). Click here to see how to clear or reset your hardware ID. Also, If the system is part of an existing customer DLM, that controller must also be removed from the DLM. To remove the controller, contact Mitel support.

After the clearing the hardware IDs, you must sync that controller to the new ARID that was provided in the welcome email. To sync the hardware ID use the **Solution Manager > AMC Sync Status** page.

NOTE: For the MiVoice Business system, the Hardware ID is the SYS ID and can be viewed in the MiVoice Business System Administration Tool, under **System Configuration > System Capacity > License and Option Selection**.

Getting Started with MiCloud Flex

This chapter contains the following sections:

Prerequisites

To start using your solution you must have the:

1. Welcome email which contains deployment details such as the public FQDN and IP addresses of the applications with user names and passwords. A sample welcome email is shown below for reference.

Mitel

Dear mivbbgl,

Great news! The MiCloud Flex Service Order for **SVE-BGL** has been completed. This email contains important information about the services that have been created.

Service Notes

The infrastructure on Google Cloud has been deployed, Network Interconnect has been enabled, and Software Licenses have been assigned for this customer based on the original MiCloud Flex Service Order Estimate submitted with the corresponding Activation Report and, if applicable, any Supplemental Contract(s).

From here, log into your Mitel Performance Analytics (MPA) portal, set up this customer in MPA, and log into the UCS Manager (noted below) to begin configuring the system. Refer to the MiCloud Flex Deployment Guide for more details about how to configure the system.

Also, please review the licensing assigned to the product instances created, as listed below, to ensure the system, user and options licensing made available supports the Service Order Estimate and Activation Report submitted by you to Mitel.

If Mitel Business Analytics or Workforce Optimization Interaction Recording have been ordered, then additional emails regarding those services will be sent.

Please refer to the MiCloud Flex Deployment Guide for configuration of your system.

Use of any and all parts of this Service is governed by your Authorized Partner Agreement, the Terms and Conditions noted on the MiCloud Flex Service Order Estimate and the MiCloud Flex Terms of Service.

Primary

Details

The following services were deployed in the Google Compute Region **'us-central1'** using POP location **Dallas**.

Application	Version
MiContact Center	9.3.0.0
UCCS	1.2.6
Initial Configuration Wizard	5.0.2.3
MBG	11.1.0.217
MiCollab	9.2.0.28
MiVoice Business	9.1.1.29
UCS Manager	1.0.1.4

Address Allocation

The following services were assigned the following addresses and set with the following usernames/passwords.

Application	VM Name	FQDN	Username	Password	ARID	GARID/DLM
MiContact Center Web Portal	-	micc.sve-bgl.ve.ucs.mitel.io/CCMWeb	_admin	_password		
MiContact Center Enterprise server	-	micc.sve-bgl.ve.ucs.mitel.io	MiCCAdmin	Mitel@123	13861828	
MiContact Center SQL Server	Micc-SQL	-	MiCCAdmin	Mitel@123		
MiContact Center Remote Server	micc-remote-0 - 10.223.133.121	-	MiCCAdmin	Mitel@123		
Application Static IP	-	134.199.56.88	-	-		
UCS Manager	-	ucs.sve-bgl.ve.ucs.mitel.io	admin	Mitel@123		
MBG	-	mbg.sve-bgl.ve.ucs.mitel.io	-	-		
MiCollab AWV	-	aww.sve-bgl.ve.ucs.mitel.io	-	-		
MiCollab AWV Static IP	-	134.199.56.89	-	-		
MiCollab	-	-	-	-	64200582	
MiVoice Business	-	-	system	password	25634612	62534498
On-site Gateway 01	-	-	-	-	35363652	

On-site Gateway 02	-	-	-	-	85830538
On-site Gateway 03	-	-	-	-	48402044
On-site Gateway 04	-	-	-	-	28303113
On-site Gateway 05	-	-	-	-	76625339
On-site Gateway 06	-	-	-	-	39419225
On-site Gateway 07	-	-	-	-	60012875
On-site Gateway 08	-	-	-	-	32257196
On-site Gateway 09	-	-	-	-	68267496
On-site Gateway 10	-	-	-	-	83914781
On-site Gateway 11	-	-	-	-	93685327
On-site Gateway 12	-	-	-	-	87975335
On-site Gateway 13	-	-	-	-	10321798
On-site Gateway 14	-	-	-	-	90856385
On-site Gateway 15	-	-	-	-	2865828

Private Cloud Connectivity/IP Scheme

This is an OTT MPLS via POP deployment.

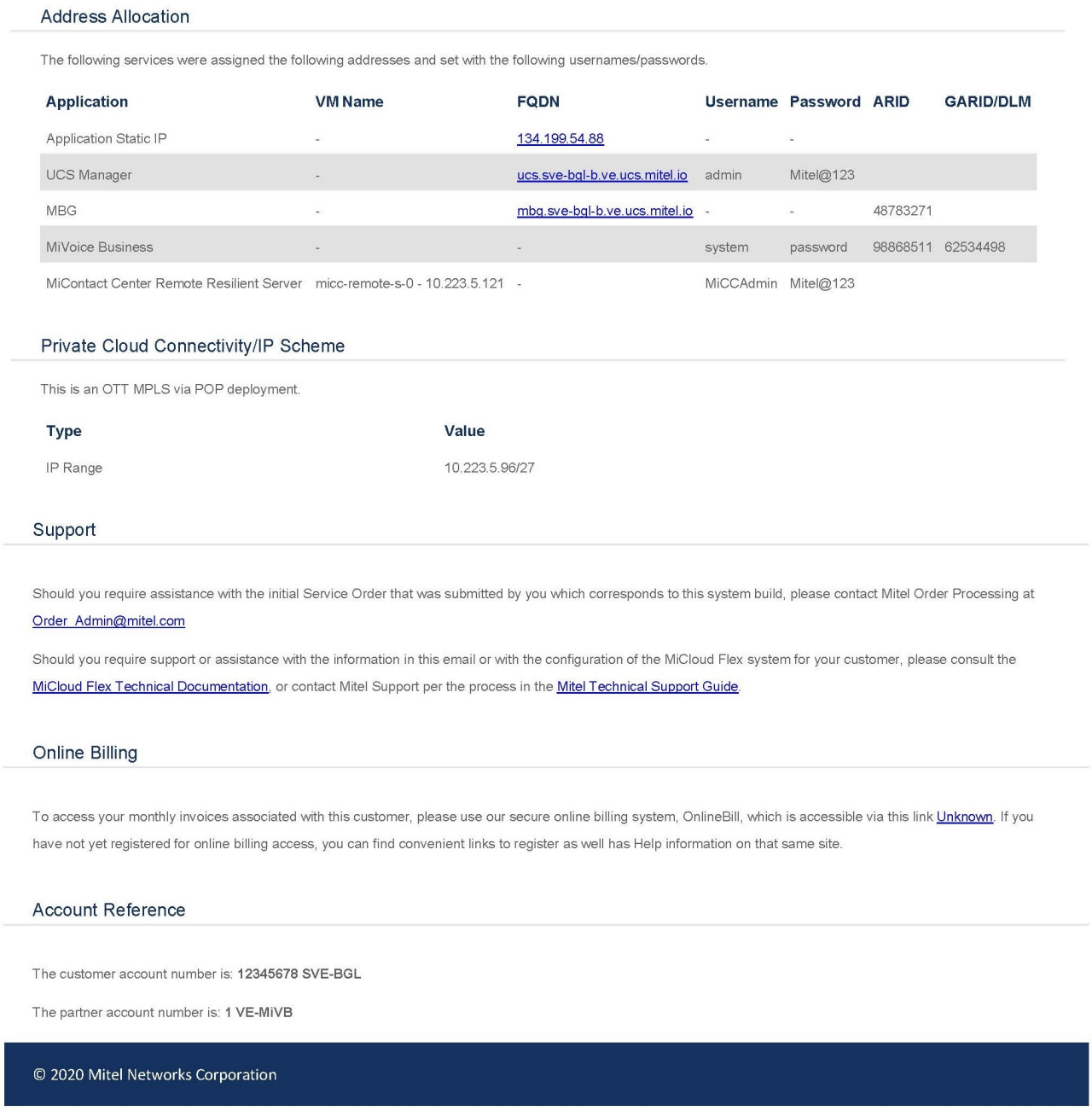
Type	Value
IP Range	10.223.133.96/27

Secondary

Details

The following services were deployed in the Google Compute Region **'us-east1'** using POP location **Reston**.

Application	Version
MiContact Center	9.3.0.0
UCCS-EXT	1.2.6
MBG	11.1.0.217
MiVoice Business	9.1.1.29
UCS Manager	1.0.1.4



Address Allocation

The following services were assigned the following addresses and set with the following usernames/passwords.

Application	VM Name	FQDN	Username	Password	ARID	GARID/DLM
Application Static IP	-	134.199.54.88	-	-		
UCS Manager	-	ucs.sve-bgl-b.ve.ucs.mitel.io	admin	Mitel@123		
MBG	-	mbg.sve-bgl-b.ve.ucs.mitel.io	-	-	48783271	
MiVoice Business	-	-	system	password	98868511	62534498
MiContact Center Remote Resilient Server	micc-remote-s-0 - 10.223.5.121	-	MiCCAdmin	Mitel@123		

Private Cloud Connectivity/IP Scheme

This is an OTT MPLS via POP deployment.

Type	Value
IP Range	10.223.5.96/27

Support

Should you require assistance with the initial Service Order that was submitted by you which corresponds to this system build, please contact Mitel Order Processing at Order_Admin@mitel.com

Should you require support or assistance with the information in this email or with the configuration of the MiCloud Flex system for your customer, please consult the MiCloud Flex Technical Documentation, or contact Mitel Support per the process in the Mitel Technical Support Guide.

Online Billing

To access your monthly invoices associated with this customer, please use our secure online billing system, OnlineBill, which is accessible via this link Unknown. If you have not yet registered for online billing access, you can find convenient links to register as well has Help information on that same site.

Account Reference

The customer account number is: **12345678 SVE-BGL**

The partner account number is: **1 VE-MiVB**

2. MPA Probe Activation URL.
3. Delivery Controller ID (DCID) and Reseller URL.

Logging in to Solution Manager

After you have received the welcome email, click on the Solution Manager (UCS Manager) link and log in to the Solution Manager GUI with the provided user name and password.

NOTE: When you log in to Solution Manager for the first time, you must change your password. The new password must be different from the old password. The password must consist of a minimum of 8 characters using at least one character from each of the four valid character sets:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special characters (~ ! @ # $ % & ^ * +)

To protect against a lost password locking out access to the solution, it is recommended to create more than one administrator for Solution Manager as administrators can reset passwords for each other.

After logging in, you can:

- *Create Users*
- *Configure the Time Zone*
- *AMC Sync Status*
- *Configure SNMP Support*
- *Configure SNMPv3 Users*

Create Users

You can add system users using the **Solution Manager** GUI. To add system users:

1. In the **Solution Manager** GUI, click **System Users**.
2. In the **System Users** page, click **Add**.
3. In the **Add User** page, enter information for the following fields:
   - First Name
   - Last Name
   - Userid
   - Password
   - Confirm password
4. Click **Save changes**.
5. To edit the user privileges, click the **Pen** icon for the user to be edited.
6. To delete the user, click the **Delete** icon for the user to be deleted.

Configure the Time Zone

The **Solution Manager** GUI allows the admin to change the time zone. When the time zone is changed, the Solution Manager updates the timezone-data config map and all applications that are monitoring the timezone data config map file will get the updated time zone change.

To set your time zone:

1. In the **Solution Manager** GUI, click **Time Zone**.
2. Under **Set Time Zone**, from the **Time Zone** drop-down list select your time zone.
3. Click **Apply**.

AMC Sync Status

Although the system automatically synchronizes with the Applications Management Center (AMC) on a periodic basis (every 24 hours by default), you can force an immediate synchronization at any time. This is useful to check the network connection between other applications provisioned via the **Solution Manager** and the AMC or to obtain up-to-date configuration information from the AMC.

To manually synchronize with the AMC:

1. In the **Solution Manager** GUI, click **AMC Sync Status**.
2. In the **AMC Sync Status** page, click **Sync**.
3. The **Sync Status** column displays the overall progress.

Configure SNMP Support

SNMP, or Simple Network Management Protocol, provides a set of operations and a protocol to permit remote management and remote monitoring of a network device and/or its services. This server currently offers support for remote monitoring via get requests and traps using both IPv4 and IPv6 protocols.

NOTE: SNMP service is disabled by default.

To configure SNMP support:

1. In the **Solution Manager** GUI, click **SNMP**.
2. Complete the following fields as required and then click **Save**.

Field	Description
SNMPv2c community string for read-only access	Enter the community string that SNMPv2c clients use to monitor this server via get requests and traps. The community string defaults to “public”.
SNMPv2c community string for read-write access	Enter the community string that SNMPv2c clients use to monitor this server via get requests and traps. The community string defaults to “public”.
SNMPv3 Settings	To facilitate SNMPv3 communication, you must add a user account to the MSL server that matches an account on the SNMP manager. This “User-based Security Model” (USM) enables unique authentication and encryption settings to be configured for each account. For instructions, see *Configure SNMPv3 Users*.
System contact address	Specify the email address to which all system notifications should go. • If Email service is enabled, and this field is left blank, the address defaults to the Admin forwarding address. • If Email service is not set, the address defaults to the local-admin account.

Field	Description
System location	Enter a string that identifies the location of the system. (for example, Server room 2, rack 1)
Trap host or address	If you wish to send trap messages to a remote host or hosts, whenever the server boots, the snmpd daemon starts and for authentication failures with the snmpd daemon, enter the hostname or IP address of the host designated to receive these trap messages. If this is left blank, traps will not be sent. To send traps to more than one host, enter the hostnames and/or IP addresses separated by commas.
SNMPv2c Trap community string	Enter the trap community string to use when sending trap messages. If you do not enter a trap community string, the community string for read-only access will be used.
SNMPv3 Trap username	Enter the SNMPv3 trap user name to use when sending trap messages. If you leave this field blank, SNMP traps will be sent using SNMP v2c.

Configure SNMPv3 Users

If you implement support for SNMPv3, you must add at least one user account that matches an account on the SNMP manager. As part of this configuration, you can enable authentication and encryption.

To add an SNMP v3 user:

1. In the **Solution Manager** GUI, click **SNMP**.
2. Locate and click **Configure SNMP v3 Users**.
3. Click **Add** and complete the following fields as required.

Field	Description
User name	Type a user name (also known as securityname) for the SNMPv3 user.
Authentication Type	Select the Authentication Type that matches SNMP manager/agent configuration: – MD5 – SHA1 – None (no authentication)
Authentication Password	If you selected an Authentication Type (MD5 or SHA1), you must enter an authentication password (also known as “authentication passphrase”) that contains at least eight characters long.

Field	Description
Privacy Protocol	Select the Privacy Protocol that matches SNMP manager/agent configuration: – DES – None (no encryption)
Privacy Password	If you selected a Privacy Protocol (DES), you must enter a privacy password.
Engine ID (Optional)	If the SNMP manager requires a hard-coded Engine ID, enter it here. Otherwise, leave this field blank and the SNMP manager will discover the Engine ID automatically.

4. Click **Add**.

MPA Integration with MiCloud Flex

To integrate MPA with the MiCloud Flex solution, you must:

1. Create an MPA Probe Activation URL in the MPA portal. See *Creating MPA URL in MPA portal* to create the MPA Probe Activation URL.
2. Add the created MPA Probe Activation URL in the Solution Manager GUI or ICW.
3. Verify the connection between the MPA portal and Solution Manager GUI.

Adding the MPA Probe Activation URL

To add **MPA Probe Activation URL**:

1. In the **Solution Manager** GUI, click **MPA Probe**.
2. In the **MPA Probe Configuration** page, enter the **Activation URL** and click **Apply**.

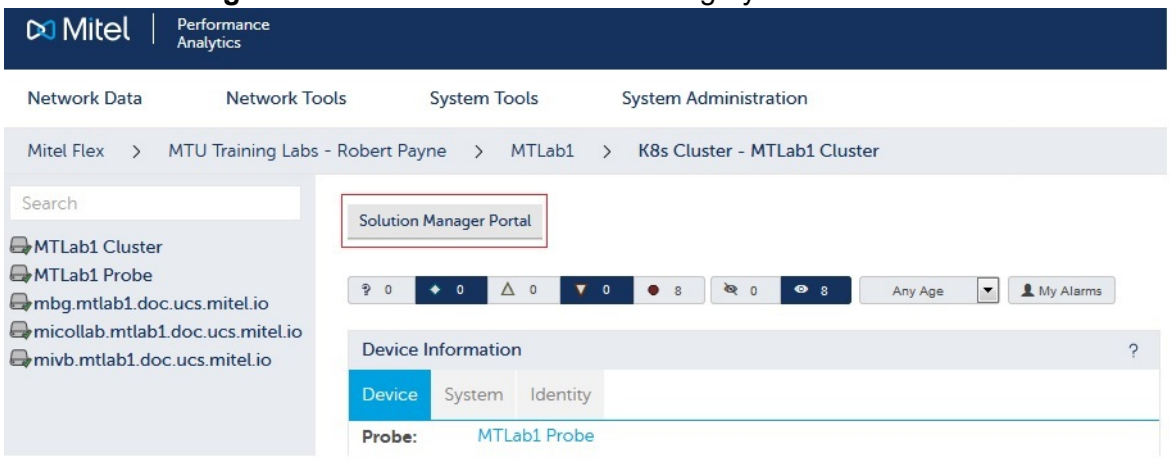
NOTE: See *Creating MPA URL in MPA portal* to create the MPA Probe Activation URL.

Verifying MPA Connection

After you have generated the MPA Probe Activation URL and added the same in the **Solution Manager** GUI, you must test if the connection between **Solution Manager** GUI and MPA portal is established. To test the connection:

1. Log in to the MPA portal.
2. Select the K8's cluster device.

3. The **Solution Manager Portal** link will be active and not grayed out if the connection is established.



4. Click the **Solution Manager Portal** link to test the connection to the customer **Solution Manager** GUI.
5. The **Solution Manager** GUI should open in a new tab from with the browser.

Mitel Business Analytics Integration with MiCloud Flex

Mitel Business Analytics is integrated with the MiVoice Business solution to capture the SMDR Logs and provide necessary analytics. The Delivery Controller ID (DCID) field, is available within the Solution Manager GUI to view and to change the current value, if required.

Configuring Resiliency

This sections contains the following topics:

IMPORTANT: Resiliency must be configured before running ICW. Also, while making any change to csv files before importing the files into MiVB, you must make the change using Windows Notepad and not Microsoft Excel® or WordPad, as Microsoft Excel or WordPad can modify the file and may cause errors when the file is imported in to MiVB.

Configuring IP Trunking and Voice Mail Resiliency for MiVB

Use the following procedures to configure resiliency, IP Trunking, Voice Mail resiliency, and SIP Trunk resiliency by logging in to both the primary and secondary MiVB System Administration Tool.

To configure IP Trunking and Voice Mail resiliency for MiVB:

1. Log in to the primary Solution Manager GUI.

   NOTE: You will be prompted to change your password, the first time you login.
2. Click **MPA Probe**.

3. In the **MPA Probe Configuration** page, enter the Activation URL and click **Apply**. See *Creating MPA URL in MPA portal*.

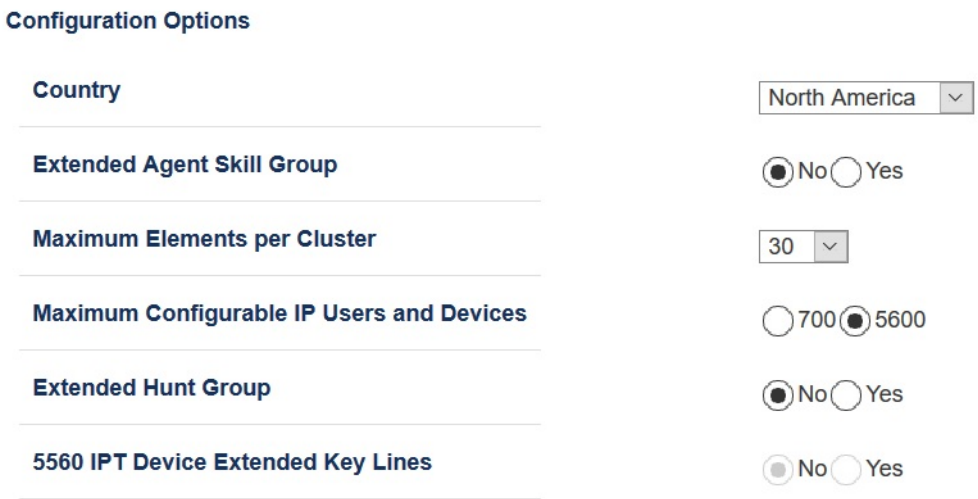
   NOTE: Ensure the primary and secondary MPA probe URLs are different.
4. Click **AMC Sync Status** and ensure that MiVoice Business is successfully synchronized.
5. (Primary MiVB) Click on the **MiVoice Business** URL from the primary Solution Manager GUI.
6. You will be prompted to change your password, the first time you login. Remember this password as you will be prompted to enter this password once you run ICW.

   NOTE: This is a temporary password. After resiliency is configured and ICW is run, you will be prompted to change your password again.
7. Acknowledge any **Restart Required** message, if it appears by clicking the **Acknowledge and remove this warning** check box.
8. From the left menu, click **Maintenance and Diagnostics**.
9. Click **Maintenance Commands**.
10. In the Command field, type `reset system`.
11. Click **Submit** to restart MiVB.

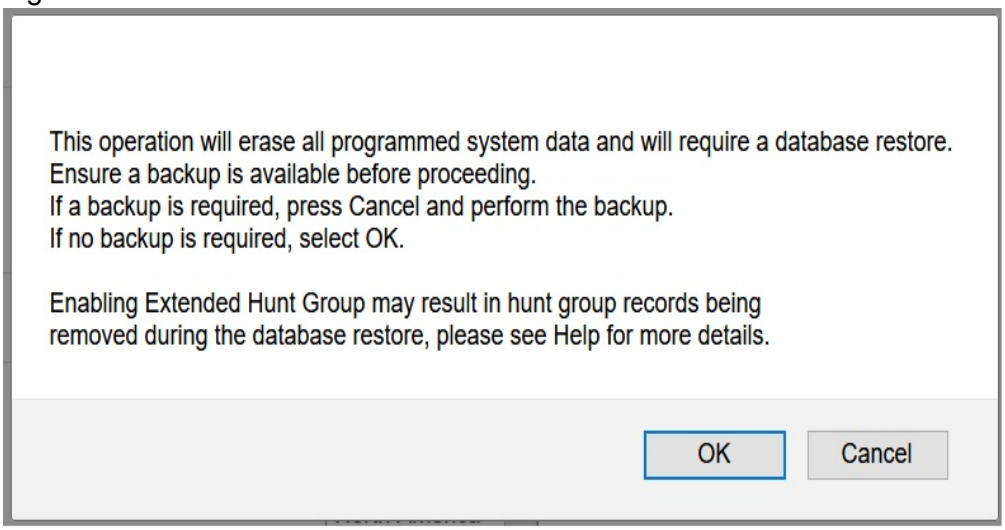
    IMPORTANT: Perform steps 1-5 on the secondary MiVB.
12. (Secondary MiVB) Navigate to **Licenses and Option Selection** to match the dimensions of primary MiVB.

    NOTE: The Primary MiVB license will be configured after the Secondary MiVB.

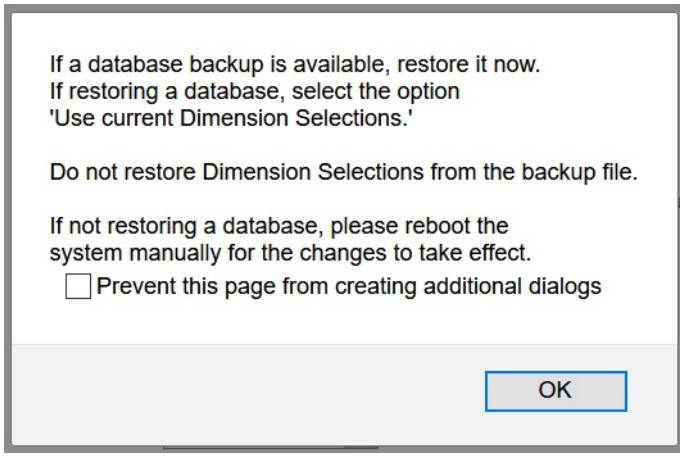
- Click Change
- Scroll down and locate Configuration Options and change the following values:
  - Country - Select the country based on your deployment
  - Maximum Elements per Cluster - Select 30 from the drop down list
  - Maximum Configurable IP Users and Devices - Select the 5600 radio button
  - Extended Hunt Group - Select the Yes radio button, if you want to configure more than 64 voice-mail ports



- Click Save. A warning message appears suggesting that you take a backup of the system before proceeding.



- Click OK



- Click OK

13. (Secondary MiVB) From the left menu, click **Maintenance and Diagnostics**.
14. Click **Maintenance Commands**.
15. In the Command field, type `reset system`.
16. Click **Submit** to restart MiVB.
17. After Secondary MiVB is successfully restarted, perform a backup procedure from the Secondary Solution Manager GUI, by clicking **Backup** from the left navigation menu. This ensures you can fall-back in case of any failures that you may encounter.
18. (Primary MiVB) From the left menu, click **Licenses > Application Group Licensing**.
19. In the Application Group Licensing form do the following:
    - Check Group Application Record ID (GARID) is not applied
    - Click **Change**.
    - Change the **Designated License Manager** field to **Yes**.

- In the **Group Application Record ID (GARID)** field enter the GARID that has been received in the Welcome Email.
- Click **Save**. The purchased licenses are visible under **License Information**.

20. (Primary MiVB) From the left menu, click **Licenses > License and Option Selection**.
21. In the License and Option Selection form, do the following:

    NOTE: License should be visible in the **Available for Allocation** column.

- Click **Change**.
- Scroll down and locate the **Users** section and assign appropriate values to the primary MiVB.
- Scroll down and locate the **Embedded Voice Mail** field. Allocate 50% of mailbox licenses to the primary MiVB.
- Scroll down and locate the **SIP trunks** field. Allocate 50% of SIP trunk licenses to the primary MiVB.

  WARNING: ICW configuration will fail if this step is skipped or appropriate licenses are not allocated
- Click **Save**. You are prompted to reboot the system.
- Click **OK**.

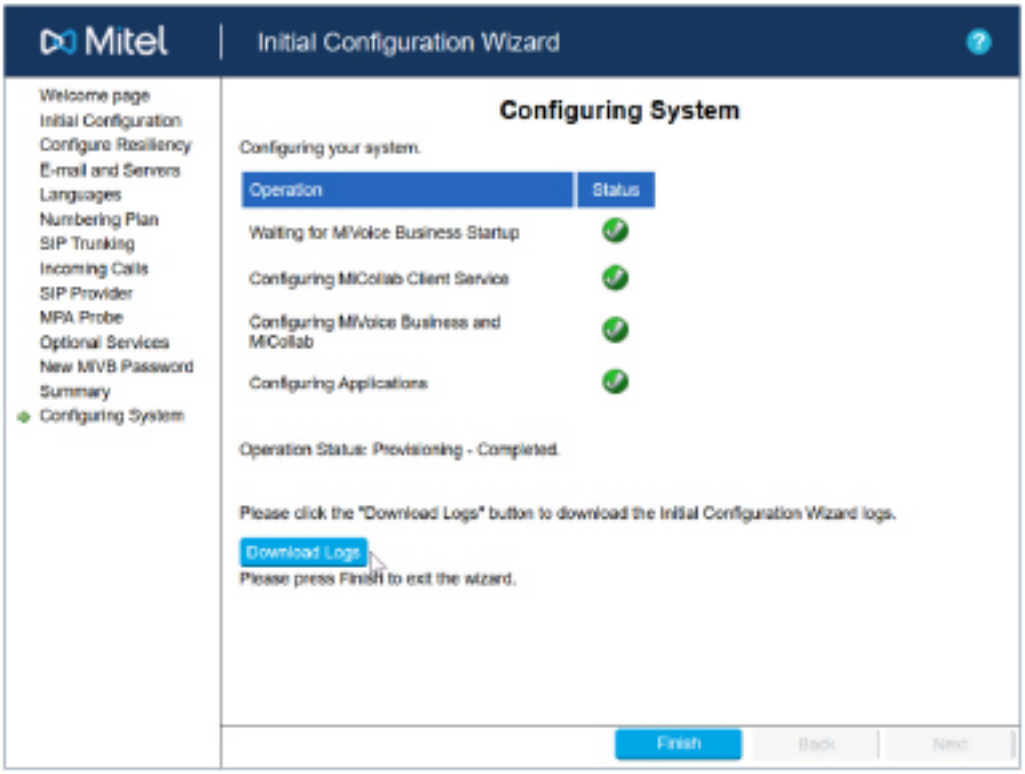
22. (Primary MiVB) From the left menu, click **Maintenance and Diagnostics**.
23. Click **Maintenance Commands**.
24. In the Command field, type `reset system`.
25. Click **Submit** to restart MiVB.

    NOTE: Wait for approximately 5 minutes for MiVB to restart.
26. After MiVB is successfully restarted, perform a backup procedure from the Solution Manager GUI, by clicking **Backup** from the left navigation menu. This ensures you can fallback in case of any failures that you may encounter.
27. From the primary Solution Manager GUI, click the **Initial Configuration** URL. The Welcome page appears.
28. Click **Next**. The Initial Configuration page appears.
29. Select the default values or if necessary, select a different Time Zone, Country, and Telecom Region. 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.
30. Click **Next**. The **Configure Resiliency** page appears.
31. In the **Configure Resiliency** page, enter information for the following fields:

- System Name - Enter a unique name of up to nine characters for the network element. For example, `MiVB1`
- FQDN or IP Address - Defines the Fully Qualified Domain Name (FQDN) or IP Address (IPv4 or IPv6) of the network element specified during deployment. This value is pre-filled.
- PBX Number - The unique identifier assigned to the element. For example, `1`. The PBX Number range is 1-999.
- Zone - The zone specified for the IP voice media stream originating or terminating at the selected MiVoice Business system. For example, `1`.The zone range is 1-999.

- CEID Digits - Enter a CEID (Cluster Element Identifier) digit string. Assign unique CEID digit strings to each cluster element. In a network that is configured for the Voice Clustering (Portable Directory Number) feature, the CEID digit string allows calls to be routed between elements in the network. The CEID digit strings for remote elements must translate to a programmed ARS route, list, or plan for correct call routing. Choose a value of up to 7 digits. For example, `7701`.
- Feature DN - For the local element enter a feature directory number. For a remote element, enter the feature directory number that corresponds to the local feature directory number of the remote element within the cluster. Choose a value of up to 7 digits. For example, `7702`.
- Cluster Name - Enter a unique name of up to 128 characters for the cluster. For example, `Cluster`.
- Master MiVB Address (FQDN) - Specify the master MiVB address of the existing cluster. This field is visible only if you deploy the uccs-ext bundle.
- Master MiVB Password - Enter the master MiVB password. This field is visible only if you deploy the uccs-ext bundle.

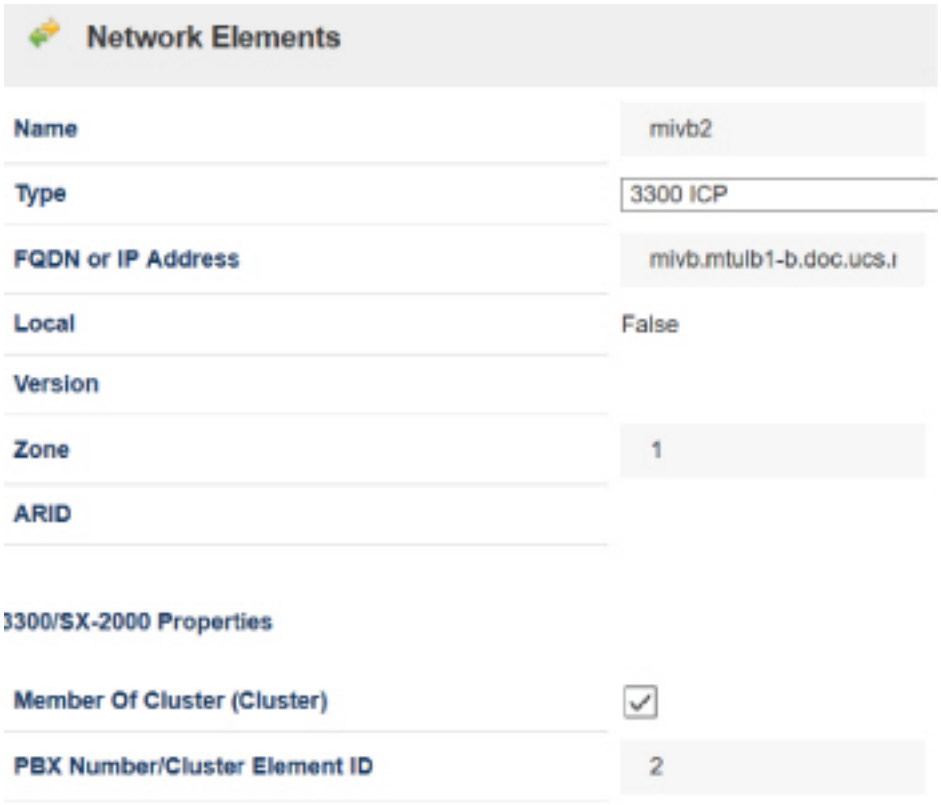
32. Complete the remaining Initial Configuration Wizard successfully. See the online help that is part of the ICW wizard.



33. (Primary MiVB) Navigate to **Voice Network > Network Elements > Add** to add MiVB2 as a network element to begin utilizing file imports and System Data Synchronization (SDS) to complete the programming steps on the secondary MiVB.

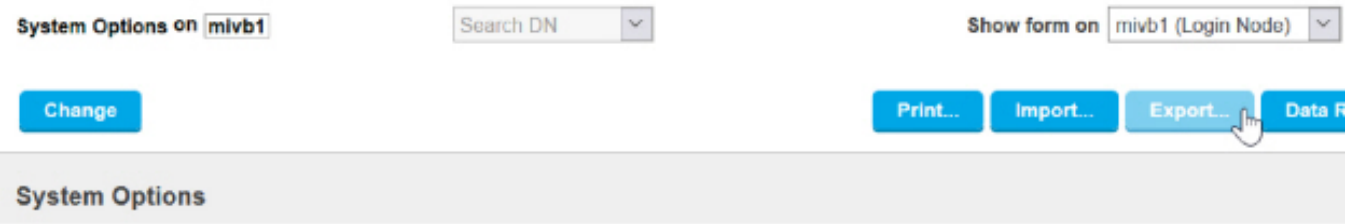
- Name – MiVB2 (the planned system name for secondary MiVB)
- FQDN or IP Address – MiVB.mtulb1-b.doc.us.mitel.io (the current FQDN of the secondary MiVB)
- Zone – 1 (the same zone as MiVB1)
- PBX number – 2 (the planned PBX number to assign)
- Member of Cluster – Check this value

– Click Save



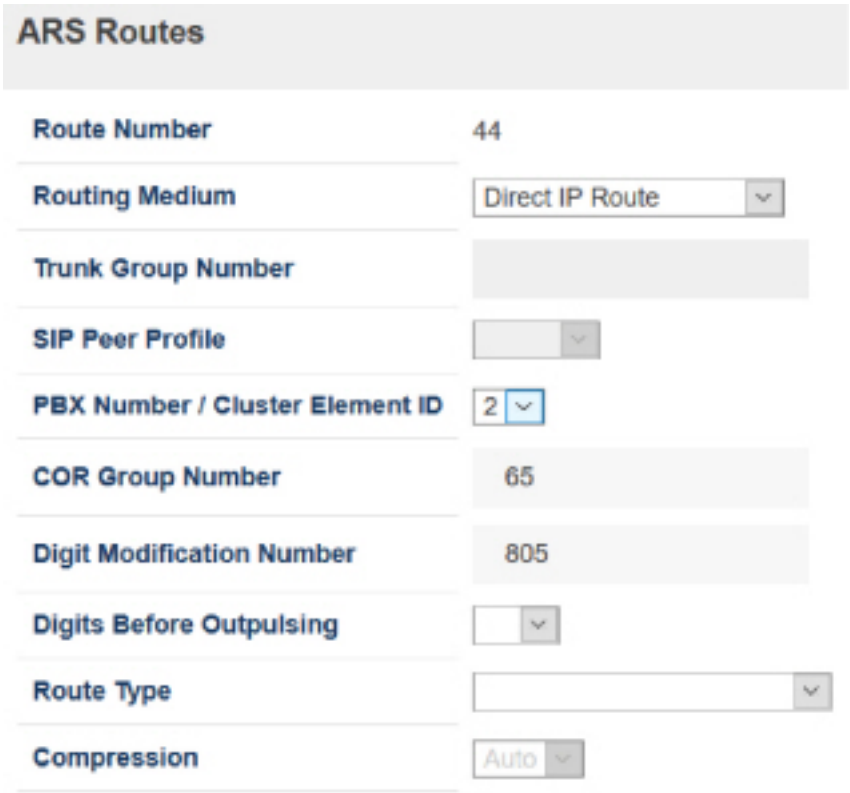
34. (Primary MiVB) Navigate to **System Properties > System Feature Settings > System Options** to export the system options from (Primary MiVB- MiVB1) to (Secondary MiVB-MiVB2) because ICW sets the system options only on (Primary MiVB- MiVB1). This is required because the EMEM services under the MiCollab User templates have the option of Forward to Voicemail set by default. Unless the MiVB System Options are set to include either 0.0.0.0 (disable Voicemail to email forwarding) or a valid email server address, there will be a failure when creating either the primary or resilient mailbox. When we complete the steps for setting up voicemail resiliency, for example, the System Options on the secondary MiVB must either be manually edited or can be Exported from MiVB1 and Imported into MiVB2. In this step, we will Export from MiVB1 and Import into MiVB2 at a later step.

– Select Export
– Keep the default values for the Export Range and File Type
– Select Export
– Identify where the File is saved
– Select OK to complete saving the file



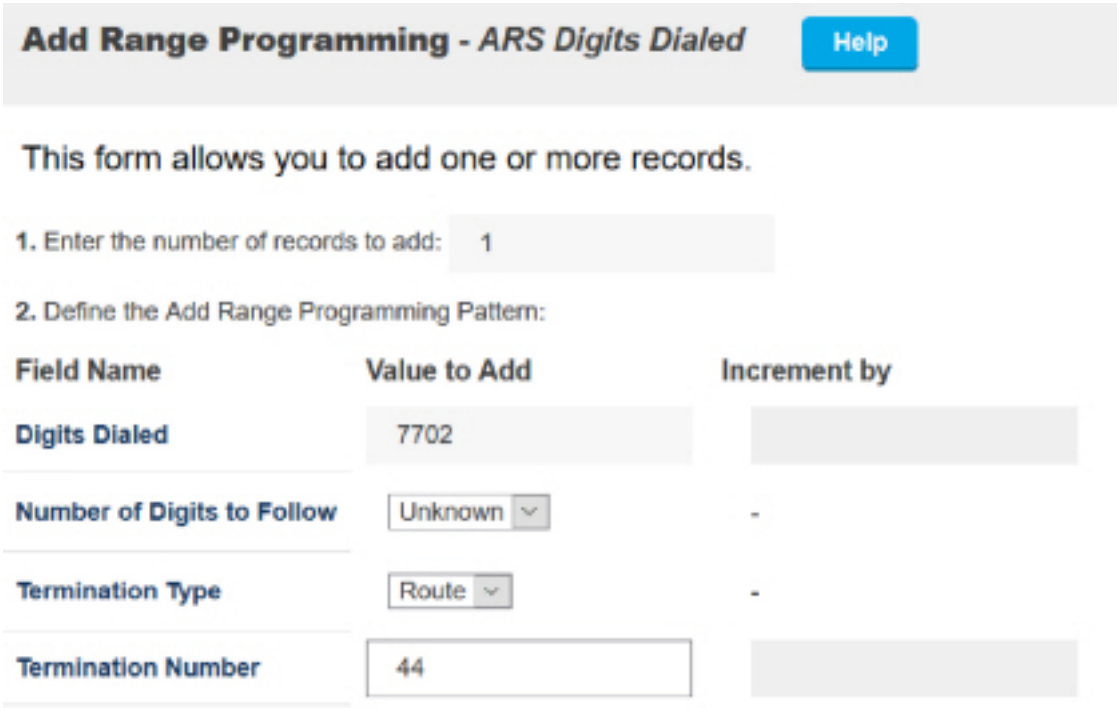
35. (Primary MiVB) Navigate to **System Properties > System Feature Settings > SMDR Options** to export SMDR Options. ICW sets the SMDR Options to include a System Identification value. This value causes an error when synchronizing, but we can export and import this form from MiVB1 to MiVB2 to ensure the values are consistent.
    - Click Export
    - Keep the default values for the Export Range and File Type
    - Click Export
    - Identify where the file is saved
    - Click OK to complete saving the file

36. (Primary MiVB) Navigate to **Call Routing > Automatic Route Selection > ARS Routes** to add Direct IP Route from MiVB1 to MiVB2.
    - Select an unassigned Route (for example, Route 44), Select Change
    - Routing Medium – Direct IP Route
    - PBX # - 2
    - Click Save



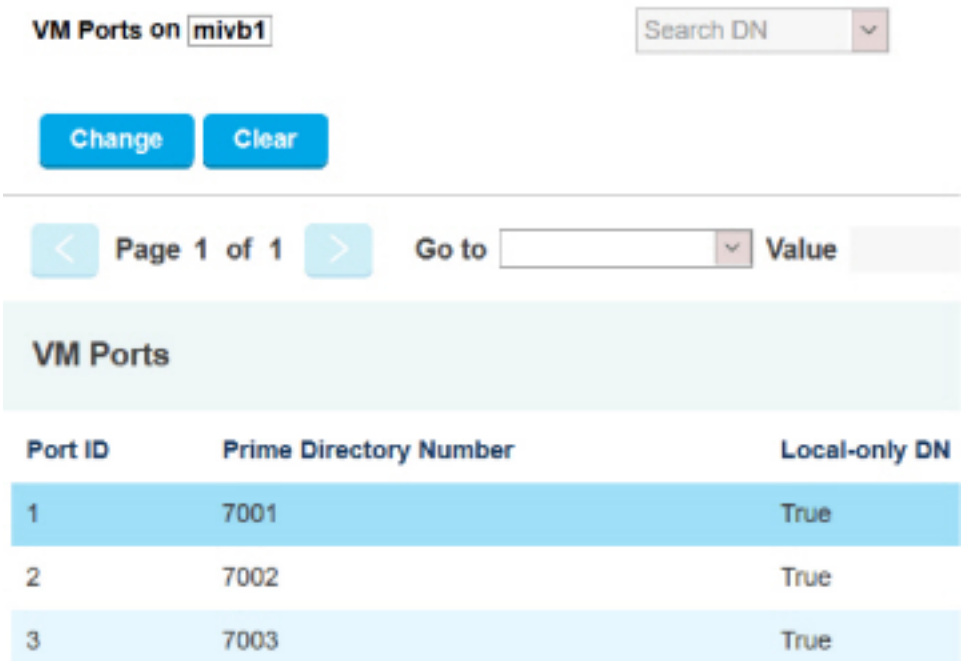
37. (Primary MiVB) Navigate to **Call Routing > ARS > ARS Digits Dialed > Add** and enter information for the below fields to assign ARS Digits dialed that will include the secondary MiVB's Cluster Element ID Digits (CEID). When the MiVB cluster is ready to be synchronized, the CEID Digits must exist within the ARS Digits Dialed.

- Digits Dialed – The planned CEID Digits for MiVB2 (for example, 7702)
- Number of Digits to Follow – UNK (unknown to account for variable digit length)
- Termination Type – Route
- Termination Number – 44 (the route number created in the previous step)
- Click Save



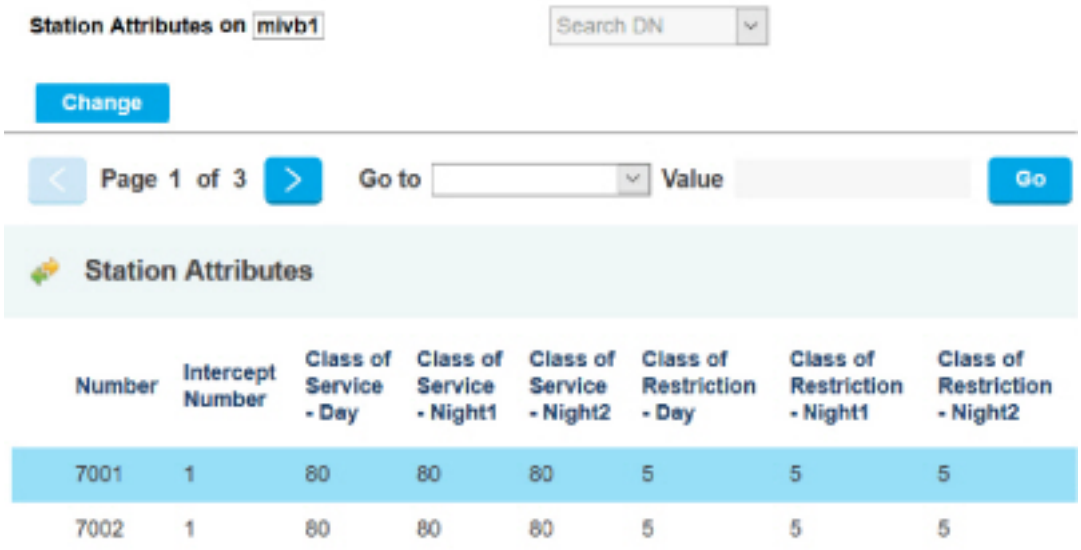
38. (Primary MiVB) Navigate to **Voicemail > System Setting > VM Ports** to support voicemail redundancy. In order to do so, the voicemail ports need to be duplicated using the `Local-only DN= True` attribute to allow the port numbers to be duplicated within an MiVB cluster. If you are unsure of what those ports are:
    - Verify the DN range of the VM ports (for example, 7001 to 7020)

- Verify that the VM ports have been created by the ICW as `Local-only DN = True`. This will allow duplicate directory numbers within an MiVB Cluster. The restriction is that any Local Only Directory Number cannot also have a Telephone Directory Entry



Port ID	Prime Directory Number	Local-only DN
1	7001	True
2	7002	True
3	7003	True

- Navigate to **Users and Devices > Advanced Configuration > Station Attributes**
- Verify that the voicemail ports have been assigned COS 80 and COR 5 (Day /N1/N2)

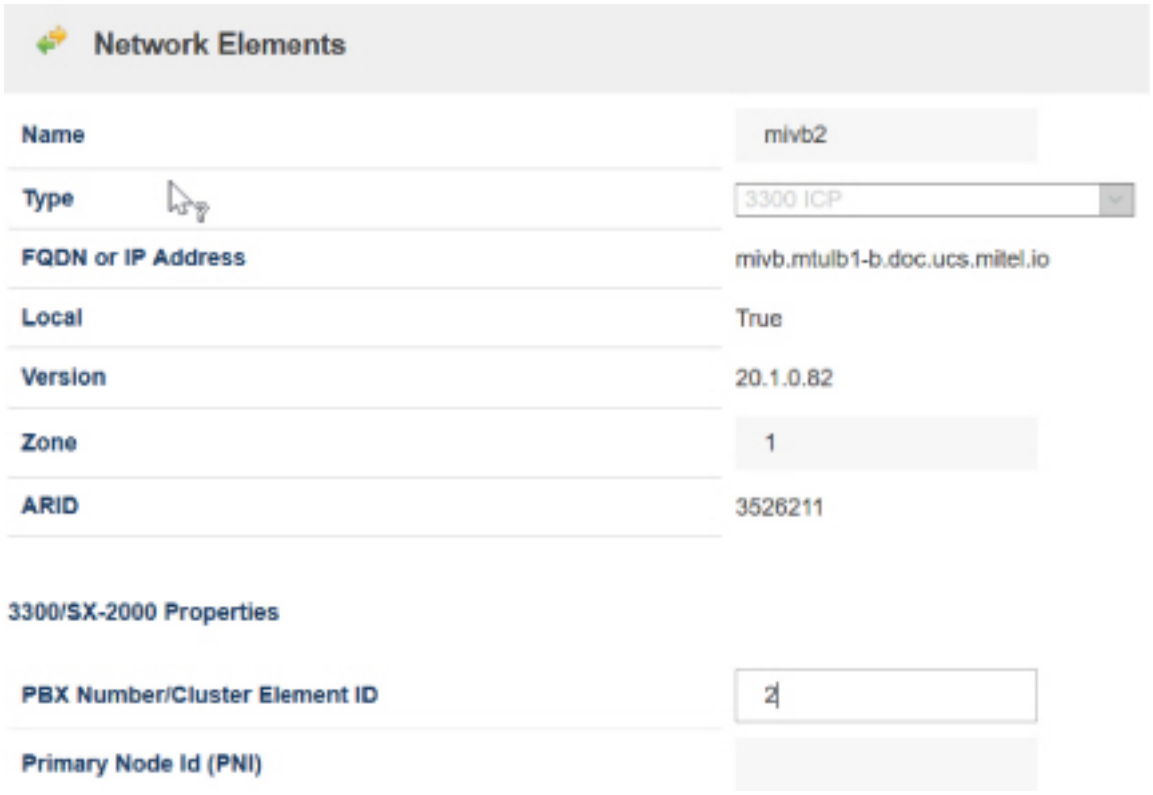


Number	Intercept Number	Class of Service - Day	Class of Service - Night1	Class of Service - Night2	Class of Restriction - Day	Class of Restriction - Night1	Class of Restriction - Night2
7001	1	80	80	80	5	5	5
7002	1	80	80	80	5	5	5

39. (Secondary MiVB) Navigate to **Voice Network > Network Elements** to begin programming the network elements. First, we must modify the existing local network element.

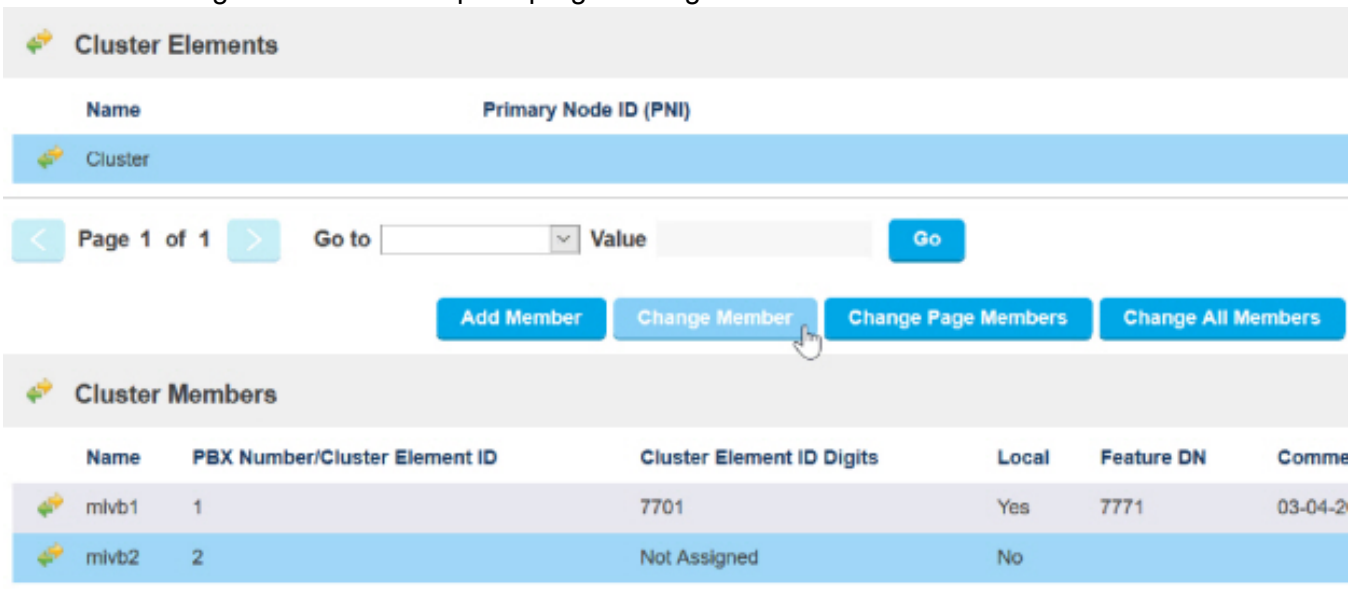
- Select the local MiVB element
- Click Change
- Name – MiVB2 (planned system name for example)
- Zone – 1 (same as MiVB1)
- PBX Number – 2 (the planned PBX / Cluster Element ID number (must match what was added in Primary MiVB))

– Click Save



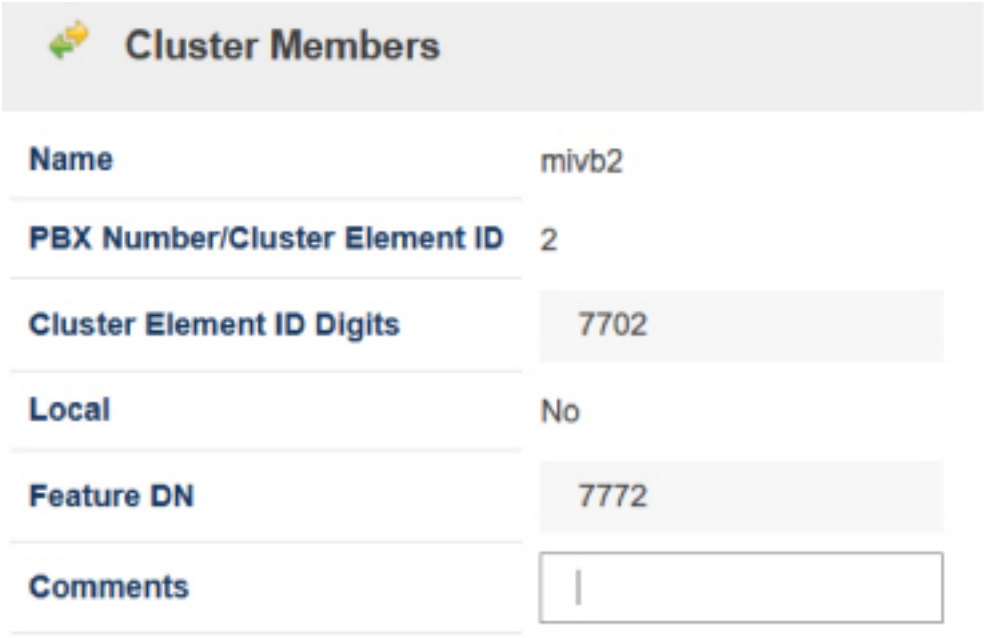
40. (Primary MiVB) Navigate to **Voice Network > Cluster Elements**

– Click MiVB2
– Click Change Member to complete programming the cluster attributes

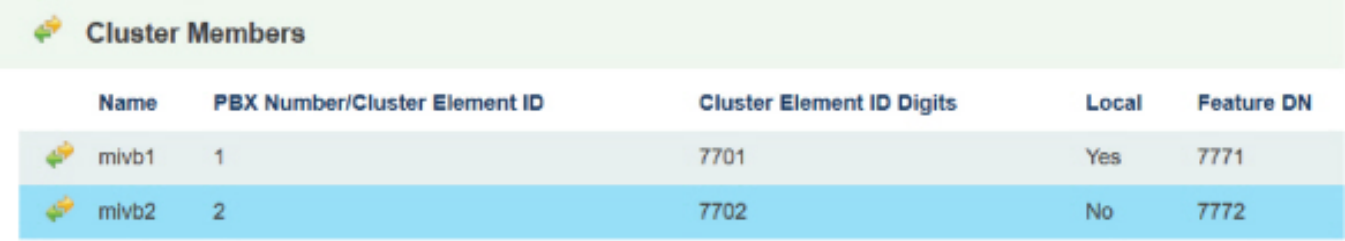


– Cluster Element ID Digits – 7702 (for example based on partner plan)
– Feature DN – 7772 (for example, based on Partner Plan)

– Click Save



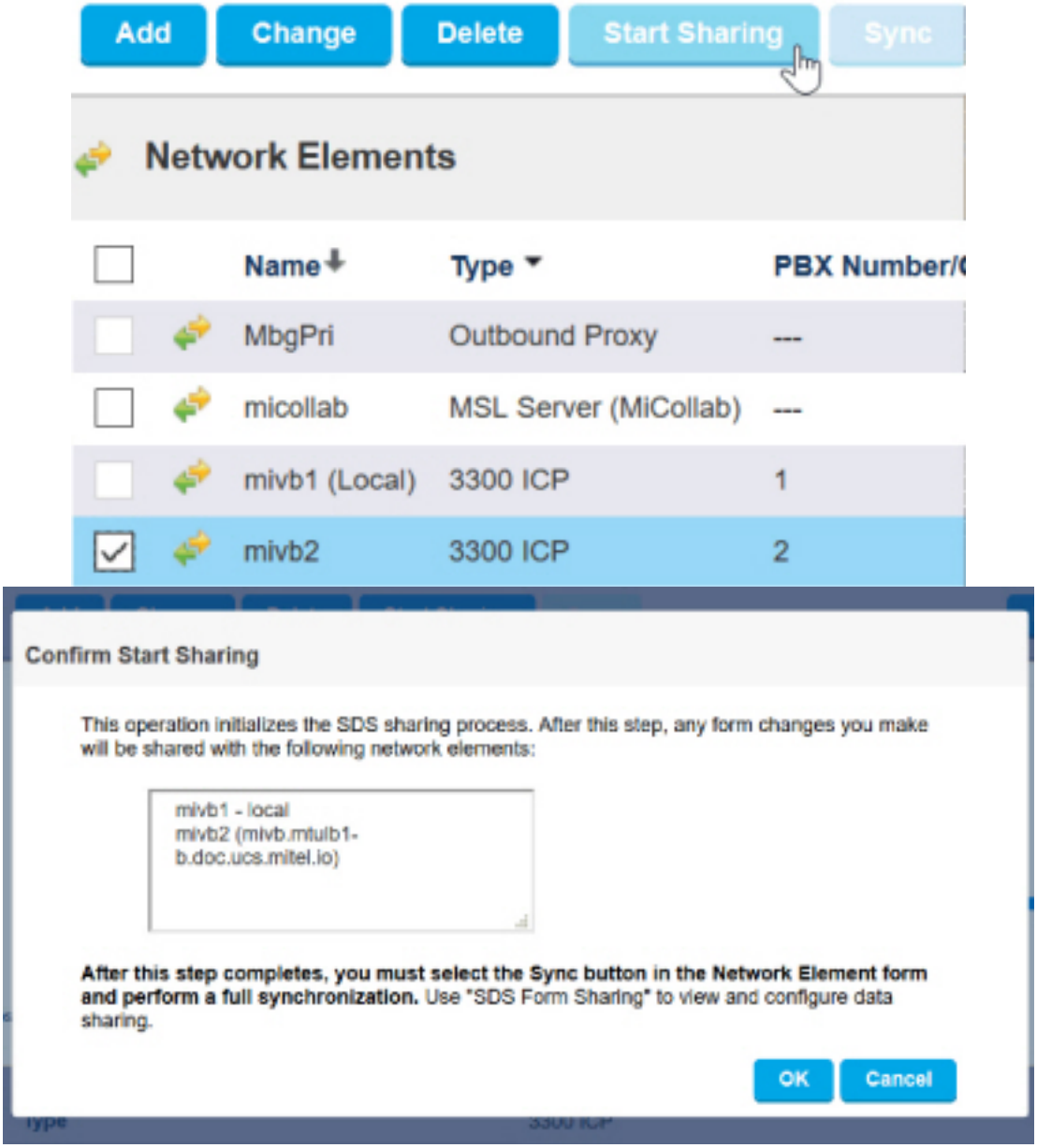
– Both members should show with the CEID Digits and Feature DN's assigned



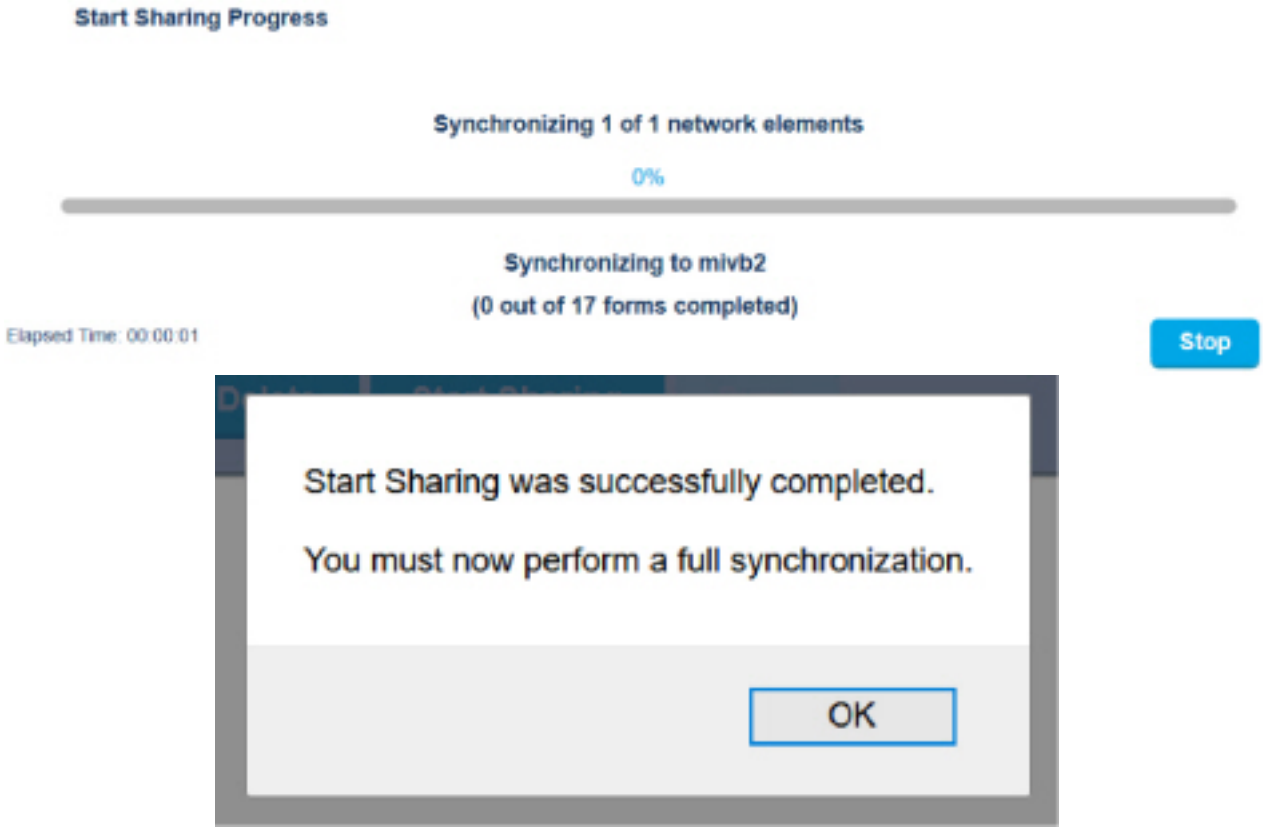
41. (Primary MiVB) Navigate to **Voice Network > Network Elements** to start sharing and sync only the Application Group Licensing so the secondary MiVB can be allocated remaining licensing and we can join the secondary MiVB to the primary cluster.

– Select MiVB2
– Click Start Sharing

– Confirm Start Sharing by clicking OK

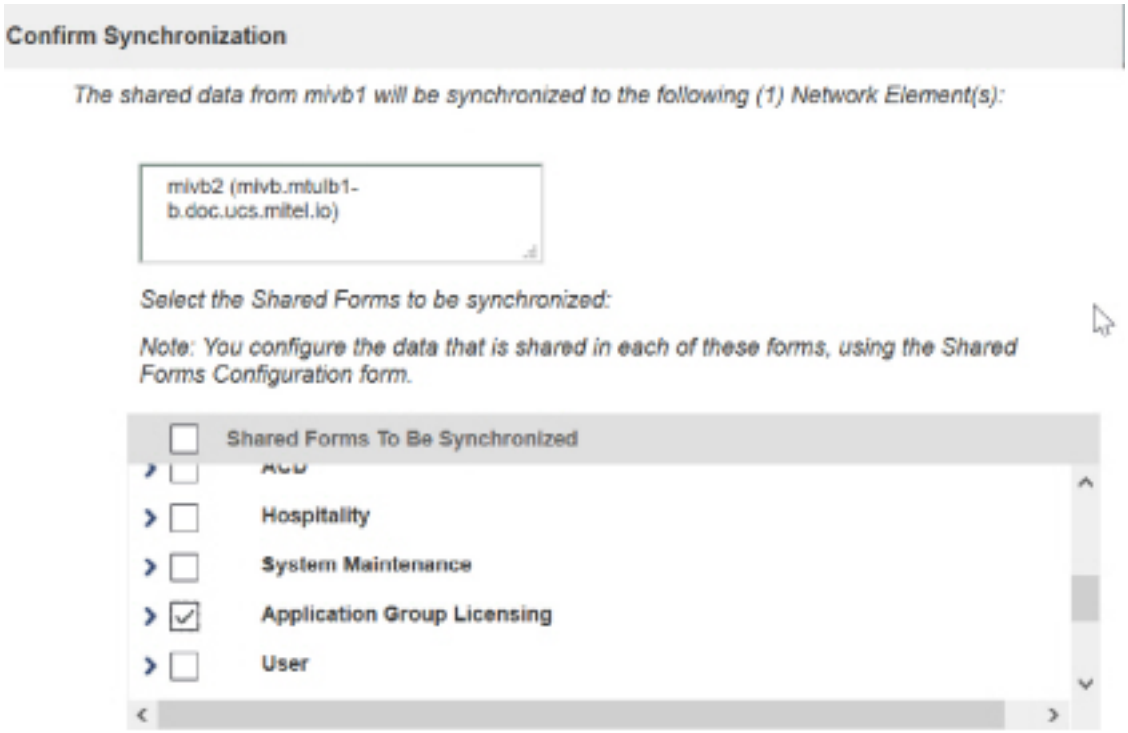


- Allow to finish

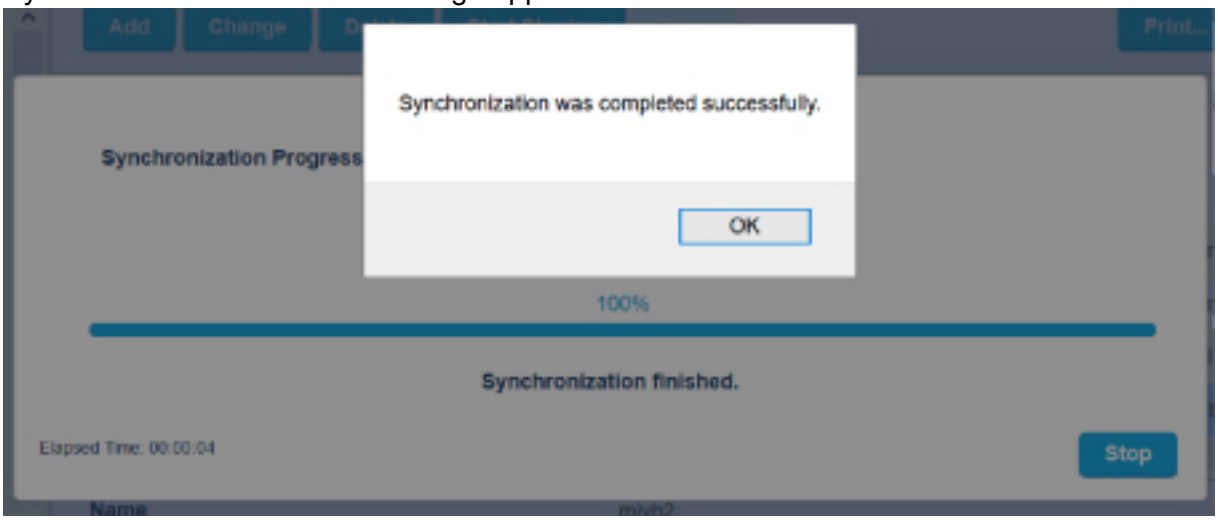


- Confirm Synchronization will now attempt to run automatically
- Clear all values except for Application Group Licensing

– Click OK



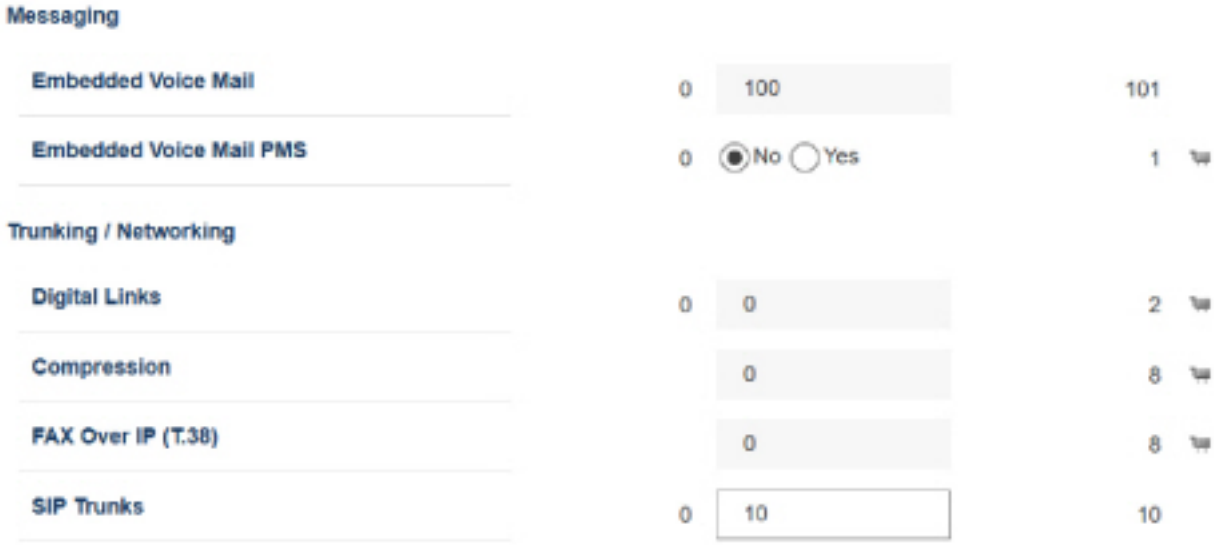
– Synchronization successful message appears



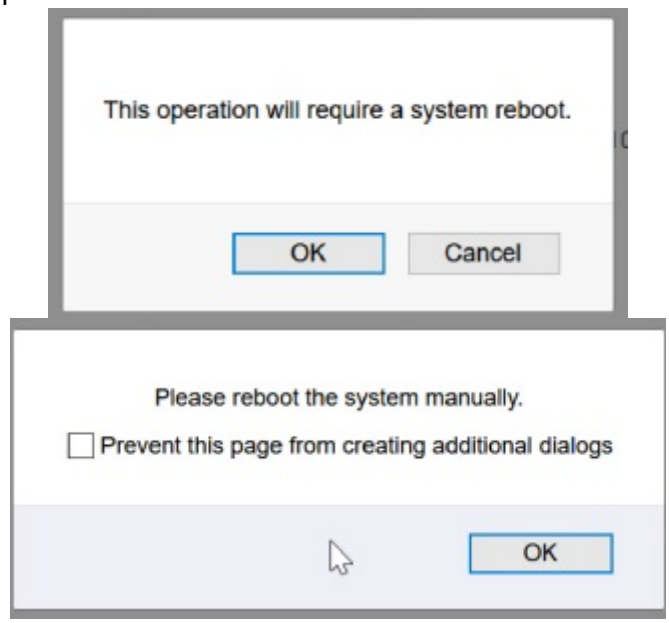
42. (Secondary MiVB) Navigate to **Licenses and Option Selection** to assign the remaining vmailbox and SIP Trunk licenses. Remember that the secondary MiVB's password has not been synchronized with MiVB1 yet, so use the correct password.

– Click Change

– Assign remaining Embedded Voicemail and SIP Trunk licenses



– Click OK. The system will require a reset to update the voicemail forms now that the system has been licensed to support Embedded Voicemail.

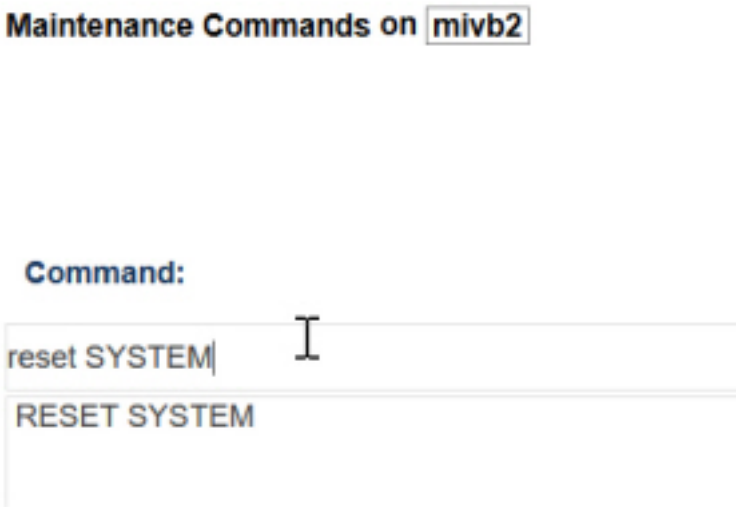


– Click OK

43. (Secondary MiVB) Navigate to **Maintenance and Diagnostics > Maintenance Commands** to reset the secondary MiVB to finish assigning the licenses and update the MiVB forms to display the Voicemail forms.

– Enter Reset System
– Click Submit
– Click Confirm

– Logout of MiVB2



NOTE: Wait for 3-4 minutes for the secondary MiVB to complete the reset.

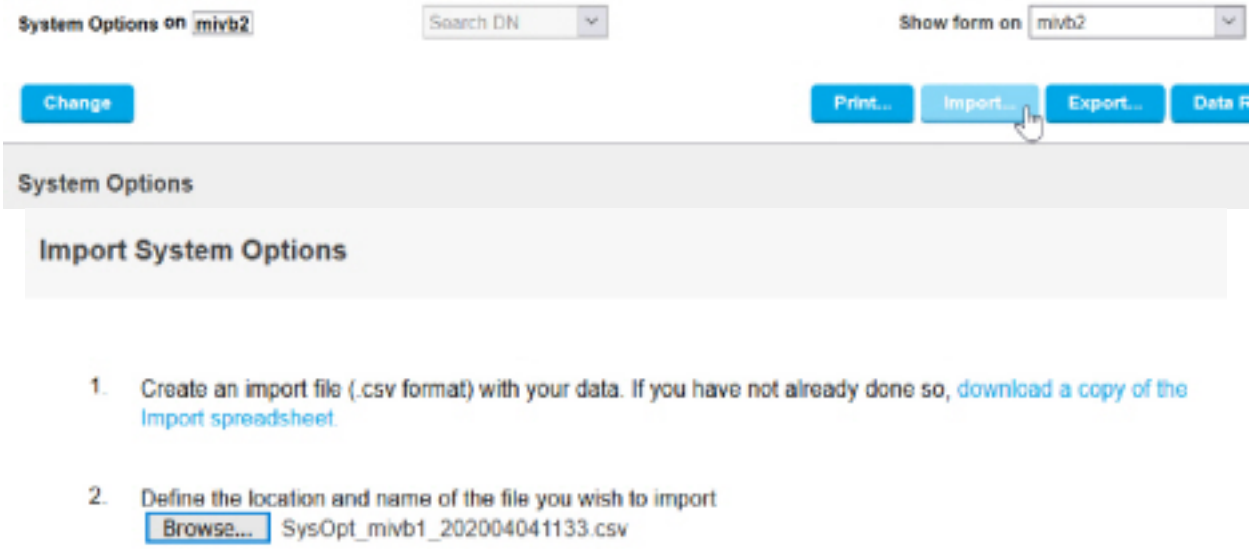
44. (Secondary MiVB) If you have set a value for the **Set Registration Auto DN Selection - Prefix** field under **System Properties > System Feature Settings > Shared System Options** in the Primary MiVB, you must configure the same field with an appropriate value in the Secondary MiVB.

    NOTE: If you do not configure the **Set Registration Auto DN Selection - Prefix** field, you will encounter a *The Set Registration Auto DN Selection - Begin must have a prefix.* error message when you import the system options in the next step.

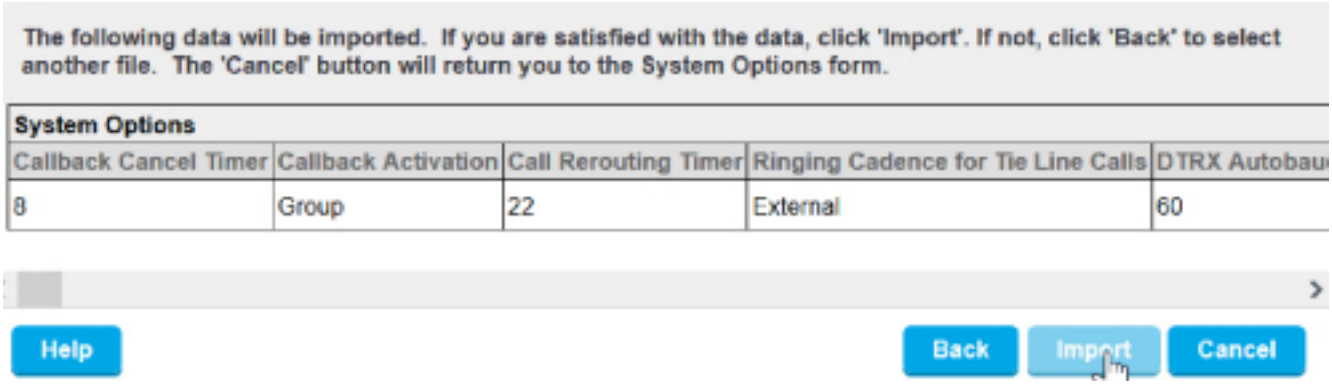
45. (Secondary MiVB) We are yet to sync the User Authorization profiles, as the password of MiVB2 is still not changed. This password will be synchronized to match MiVB1 as we complete the cluster synchronization. We will import the System Options and SMDR options forms.

    a. Navigate to **System Properties > System Feature Settings > System Options**

- Click Import
- Navigate to the file location
- Click Next



- Click Import. File should import without error

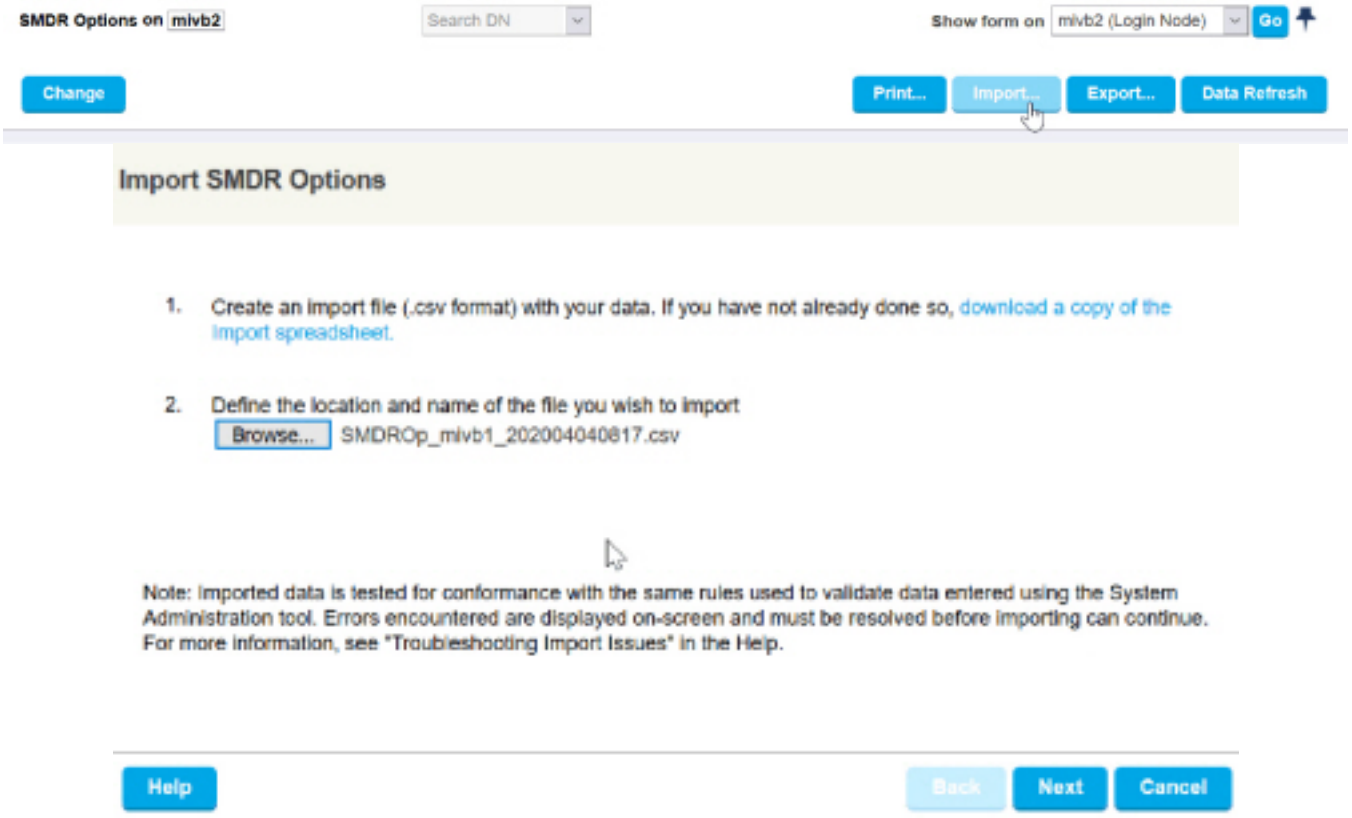


- Click Finish

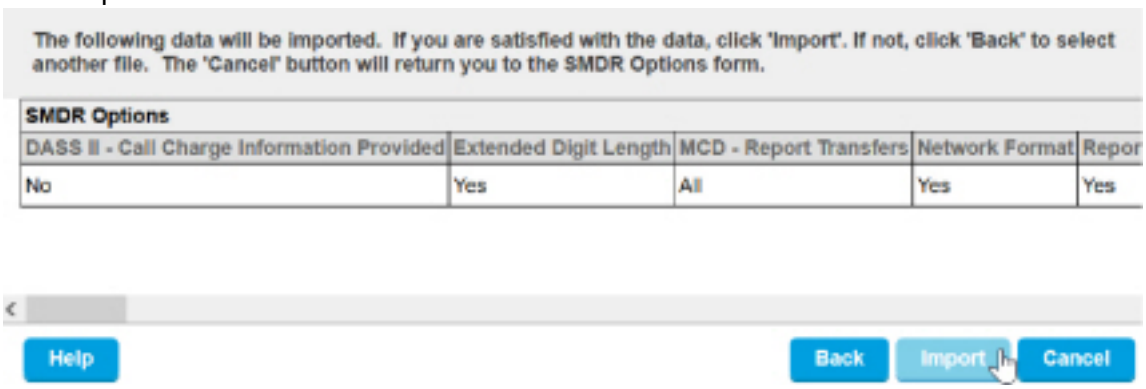
NOTE: After importing all the values of the System Options form will be overwritten.

b. Navigate to **System Properties > System Feature Settings > SMDR Options**

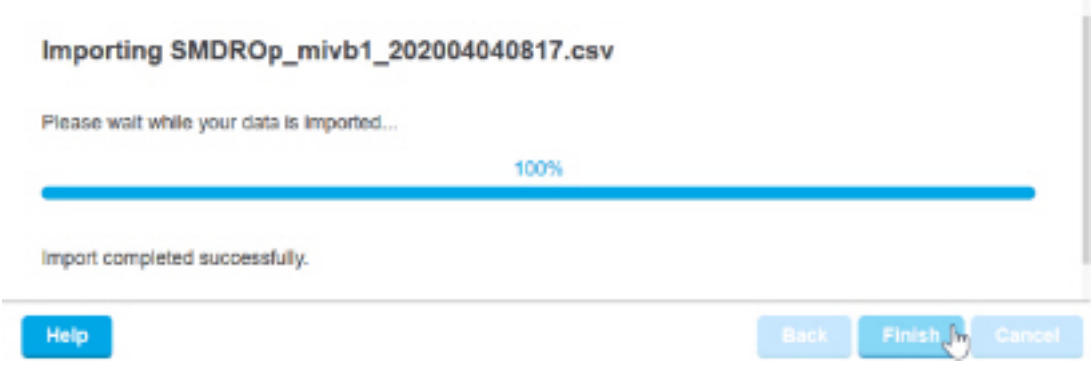
- Click Import
- Navigate to the file location
- Click Next



- Click Import



- File should import without error
- Click Finish



46. (Secondary MiVB) Navigate to **Voicemail > System Settings > VM Options > Change**
    - Scroll down and locate the Mailbox Length field
    - Change the value to match the value provided in the primary MiVB
    - Click Save
47. (Secondary MiVB) Navigate to **Voicemail > System Settings > VM Ports > Change** to create the local only voicemail ports that will be used to support voicemail resiliency. We will use Range Programming to program all 20 ports in one step.
    - Number of Records to Change – 20. **This value should match the value in the primary MiVB**.
    - Prime Directory Number – Increment
    - Value to Change – 7001. **The DNs must match what was programmed on MiVB1**.
    - Increment by – 1
    - Local-only DN – Change all to
    - Select the Check Box

– Click Save

Port ID	Prime Directory Number	Local-only DN	Interconnect Number	Tenant Number
1		False	1	1

1. Enter the number of records to change: 20

2. Define the Change Range Programming Pattern:

Field Name	Change action	Value to change	Increment by
Port ID	-	1	-
Prime Directory Number	Increment	7001	by 1
Local-only DN	Change all to	☑	-
Interconnect Number	Leave all unchanged	1	
Tenant Number	Leave all unchanged	1	

VM Ports on mivb2 Search DN

Change Clear

Page 1 of 6 Go to Value

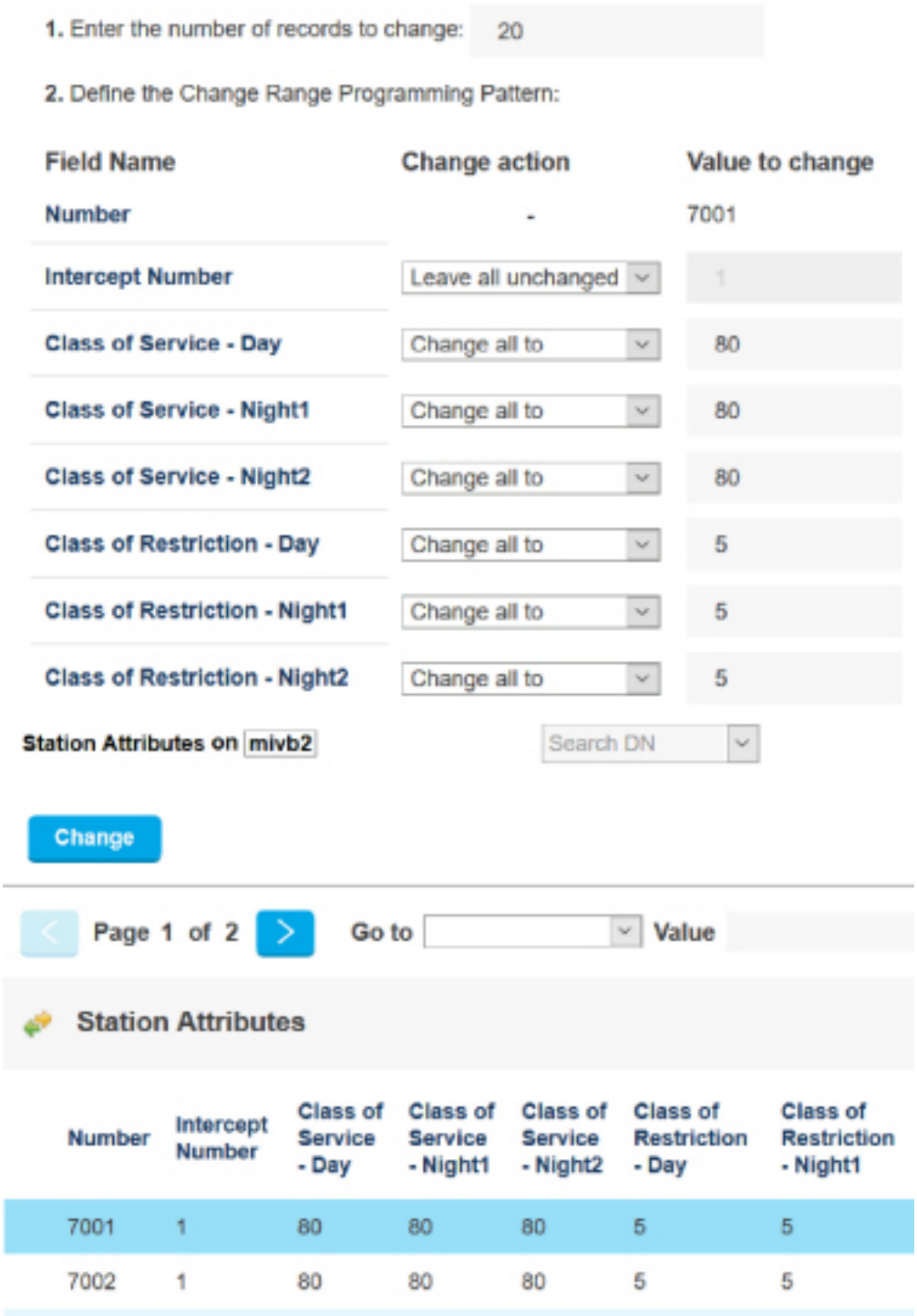
VM Ports

Port ID	Prime Directory Number	Local-only DN
1	7001	True
2	7002	True

48. (Secondary MiVB) Navigate to **Users and Devices > Advanced Configuration > Station Attributes (use Range Programming)** to assign the COS and COR to all 20 ports at once. These values were added by the ICW for MiVB1 that we will synchronize MiVB2 against.

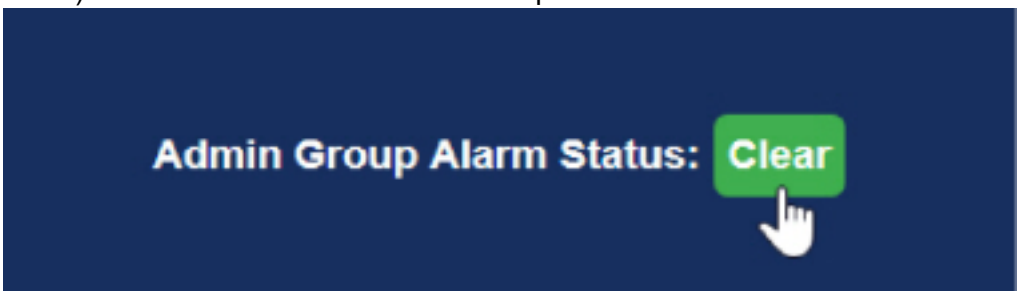
– Ensure the first port in the range is selected (for example, 7001)
– Click Change
– Number of Records to Change – 20. This value should match the value in the primary MiVB.
– Class of Service Day / N1 / N2 – Change All To

- Value to Change – 80 (for all 3)
- Class of Restriction Day / N1 / N2 – Change all to
- Value to Change – 5 (for all 3)
- Click Save



49. (Secondary MiVB) Navigate to **Voicemail > System Settings > VM Port Capacity > Change** and set the Number Of Ports value to the number of ports required. This must match the same value as the primary MiVB.

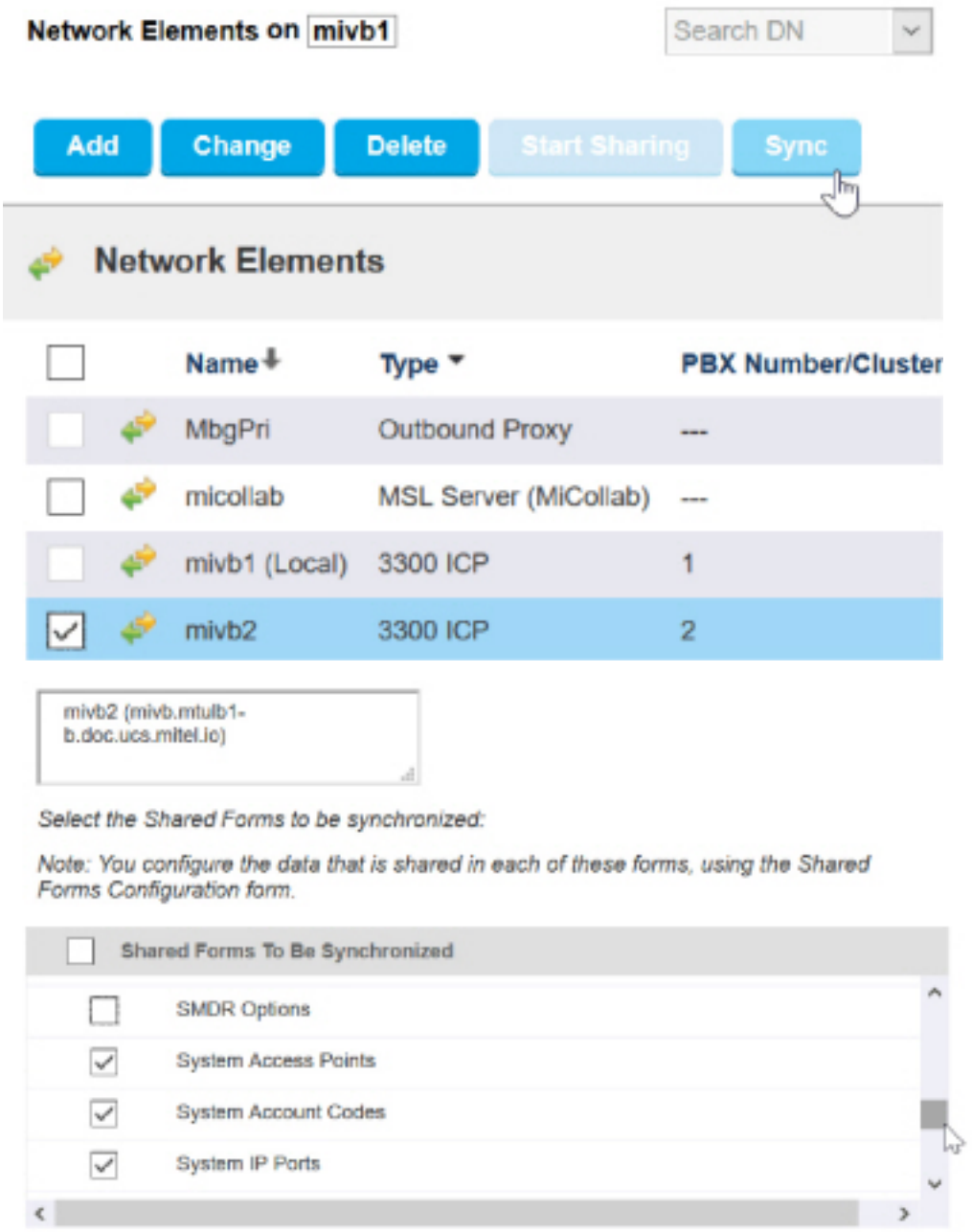
50. (Secondary MiVB) To activate the newly created voicemail ports you must reboot the system. To reboot:
    - From the left menu, click **Maintenance and Diagnostics**.
    - Click **Maintenance Commands**
    - In the Command field, type `reset system`.
    - Click **Submit** to restart MiVB.
51. (Primary MiVB) There should be no alarms at this point



52. (Primary MiVB) Navigate to **System Properties > System Administration > SDS Forms Sharing > Voice Mailboxes (found under Device Level Resiliency Category)** and verify that the VM Mailboxes SDS Form Sharing Form rules is set to Resilient Pair. This ensures the creation of users with Embedded Voicemail to have a redundant mailbox created on the secondary MiVB.

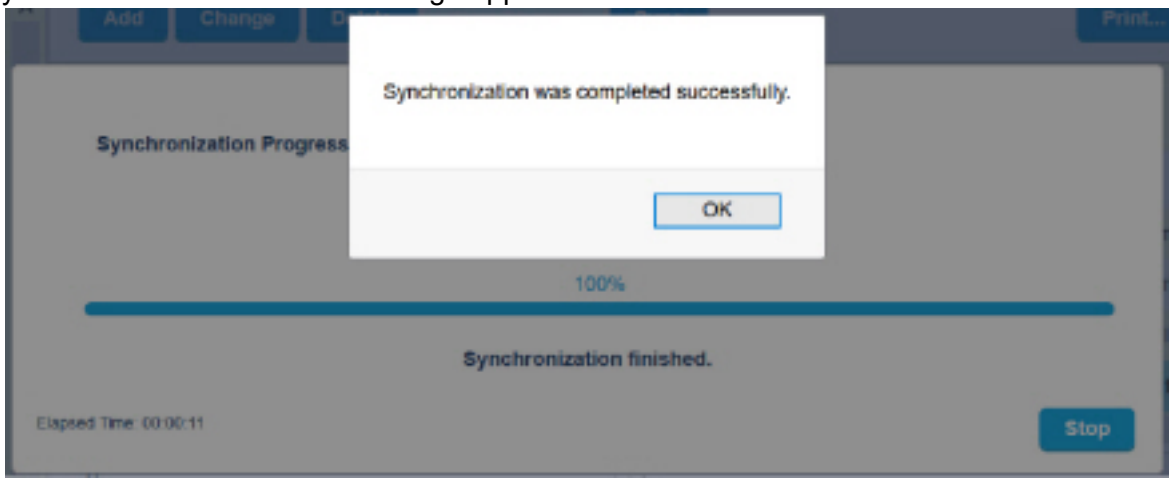
    NOTE: We will now complete a full synchronization of all forms at the Cluster Scope (excluding the SMDR Options form).
53. (Primary MiVB) Navigate to **Voice Network > Network Elements** to complete synchronizing the forms using SDS.
    - Select MiVB2 (the network element to synchronize to)
    - Click Sync
    - Select All Forms next to Shared Forms to be Synchronized
    - Under the General Category of Form, clear SMDR Options
    - Leave all other forms in their default selection

– Click OK.



– Allow the forms to complete synchronizing

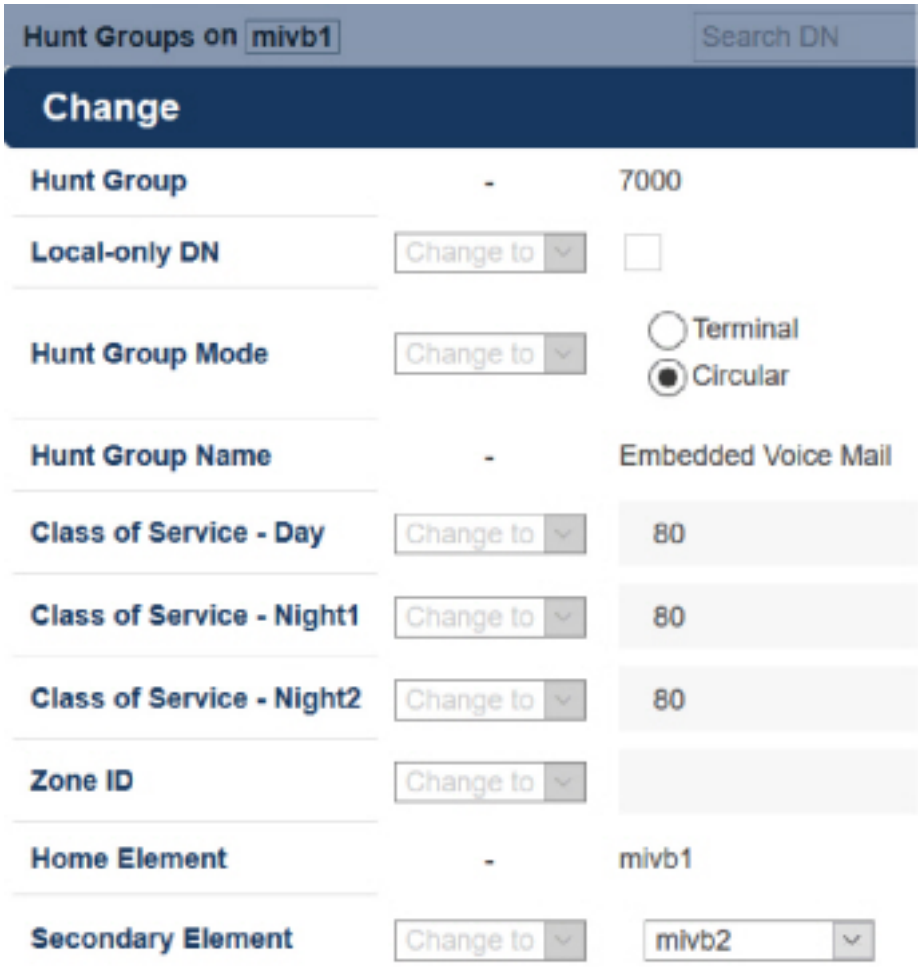
- Synchronization successful message appears



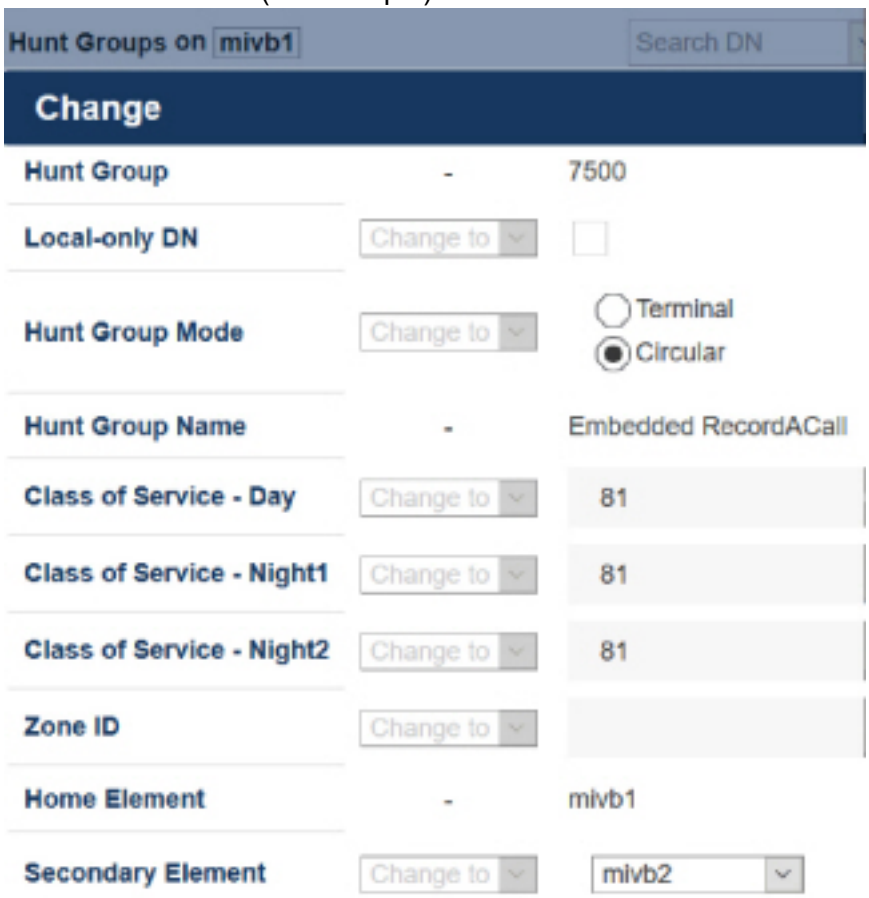
54. (Primary MiVB) Navigate to **Users and Devices > Group Programming > Hunt Groups** to set the Voicemail Hunt group and the Voicemail Record A Call Hunt group to be resilient to the Secondary MiVB.

- Select the VMAIL Hunt Group (for example, HG 7000)
- Click Change
- Set the Secondary Element to MiVB2 (for example)

– Click Save


Hunt Groups on mivb1
Search DN
Change
Hunt Group
-
7000
Local-only DN
Change to
Hunt Group Mode
Change to
Terminal
Circular
Hunt Group Name
-
Embedded Voice Mail
Class of Service - Day
Change to
80
Class of Service - Night1
Change to
80
Class of Service - Night2
Change to
80
Zone ID
Change to
Home Element
-
mivb1
Secondary Element
Change to
mivb2

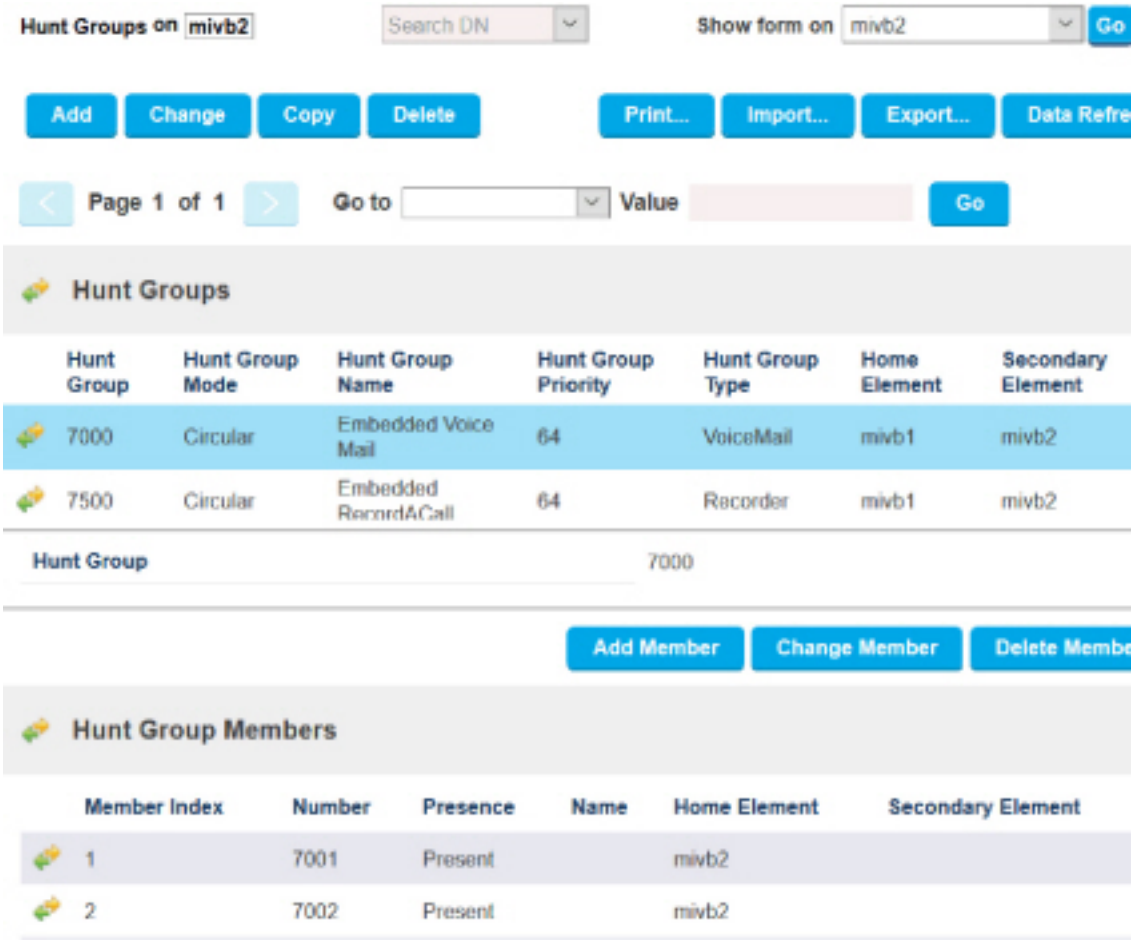
– Repeat the process for HG 7500 (for example)



55. (Secondary MiVB) Navigate to **Users and Devices > Group Programming > Hunt Groups** or use Application Reach Through to verify that both Hunt Groups have been synchronized to MiVB2 and populated with the correct Local Only ports.

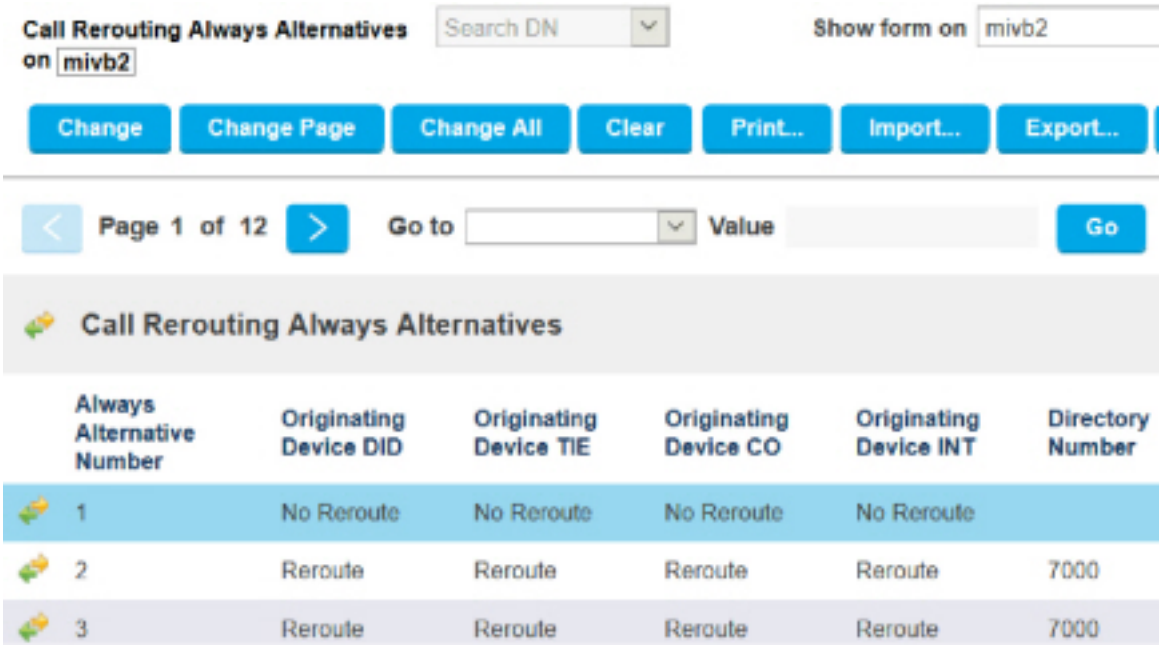
– Verify that HG 7000 and 7500 (for example) show the Home Element and Secondary Element (for example, MiVB1 and MiVB2)

– Verify that HG 7000 and 7500 are populated with the appropriate ports (for example, 7001- 7020 in the Vmail HG)

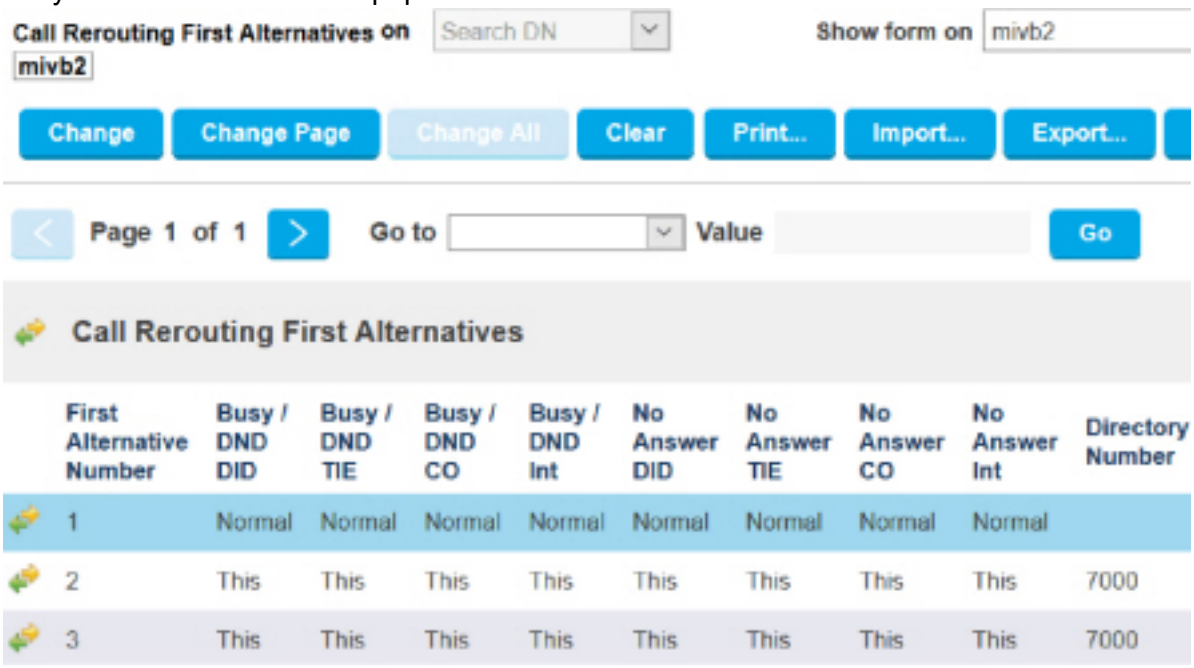


56. (Secondary MiVB) Navigate to **Call Routing > Call Handling > Call Reroute Always Alternative** to synchronize Call Rerouting Always and Call Rerouting First Alternative rules across the MiVB cluster to support resilient embedded voicemail services.

- Verify that Rules 2 and 3 are populated



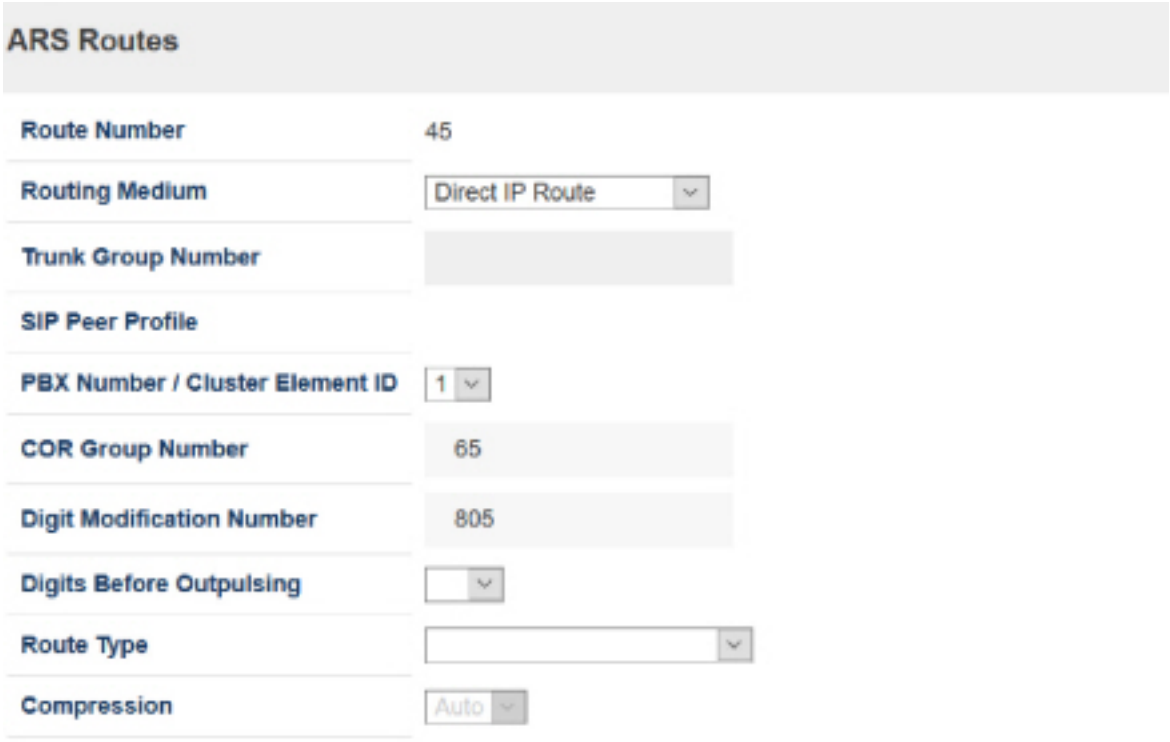
- Navigate to Call Rerouting First Alternative form
- Verify that Rules 2 and 3 are populated



57. (Secondary MiVB) Navigate to **Call Routing > ARS > ARS Routes** to assign a Direct IP Route to route IP calls to MiVB1.

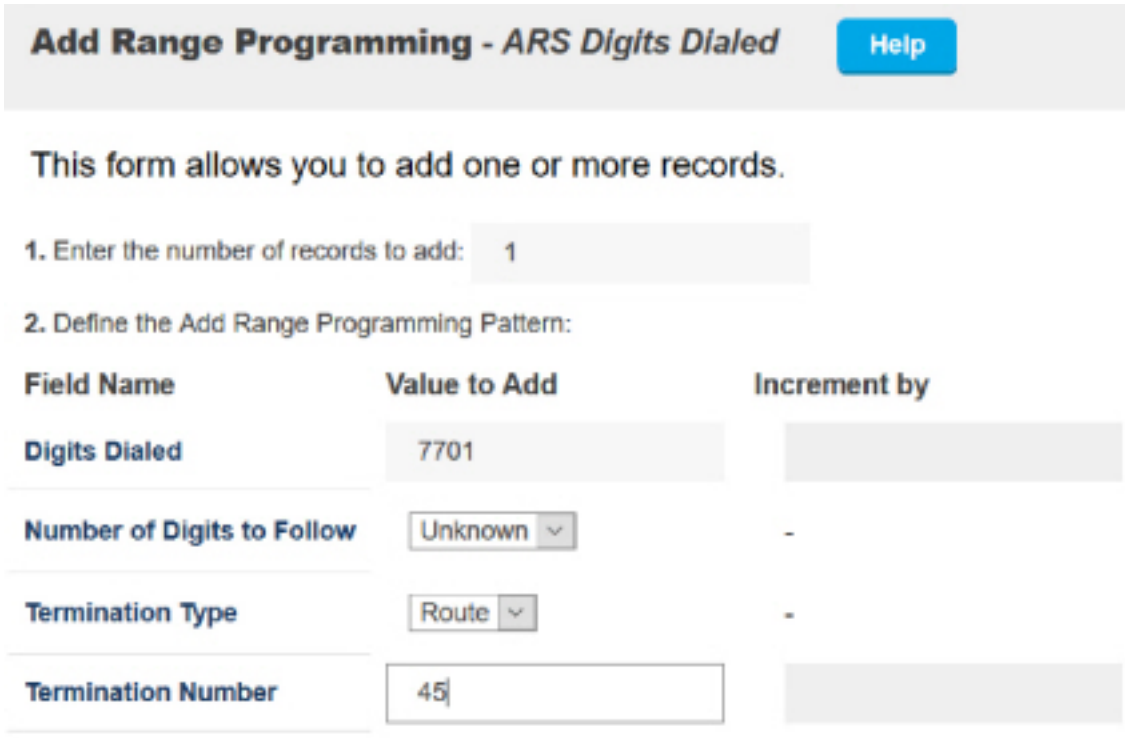
- Select an open route, for example, route 45
- Click Change
- Routing Medium – Direct IP Route
- PBX number – 1 (referencing the primary MiVB)

- Click Save

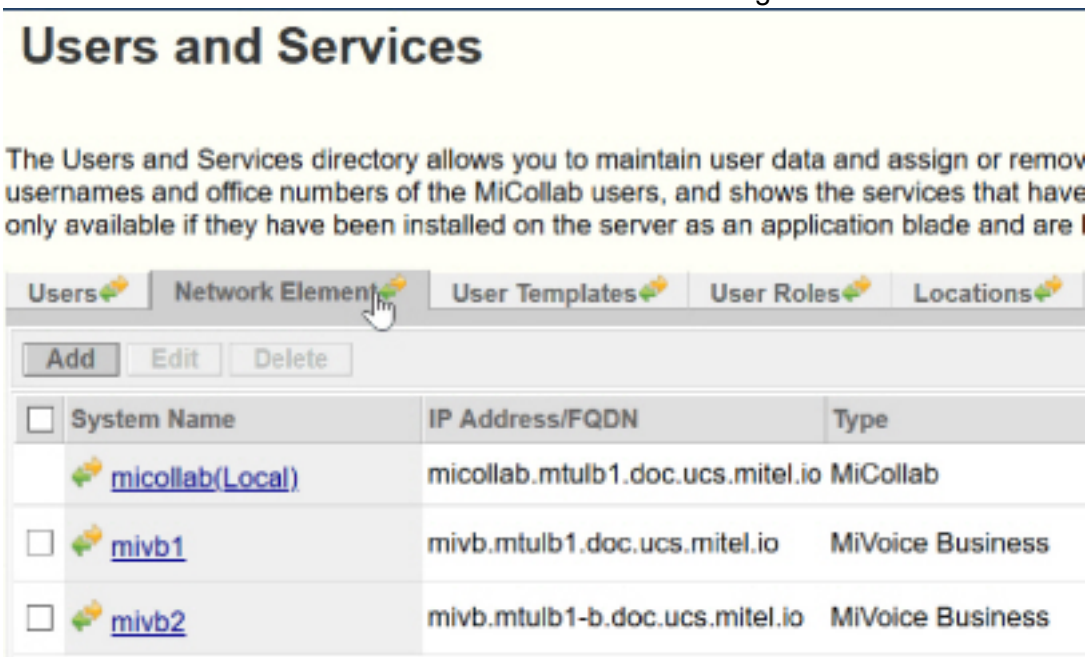


58. (Secondary MiVB) Navigate to **Call Routing > ARS > ARS Digits Dialed > Add** to assign an ARS Digits Dialed using the created route.
    - Digits Dialed – 7701 (the CEID Digits assigned to MiVB1)
    - Number of Digits to Follow – Unknown
    - Termination Type – Route
    - Termination Number – 45 (the route created in the previous state)

– Click Save

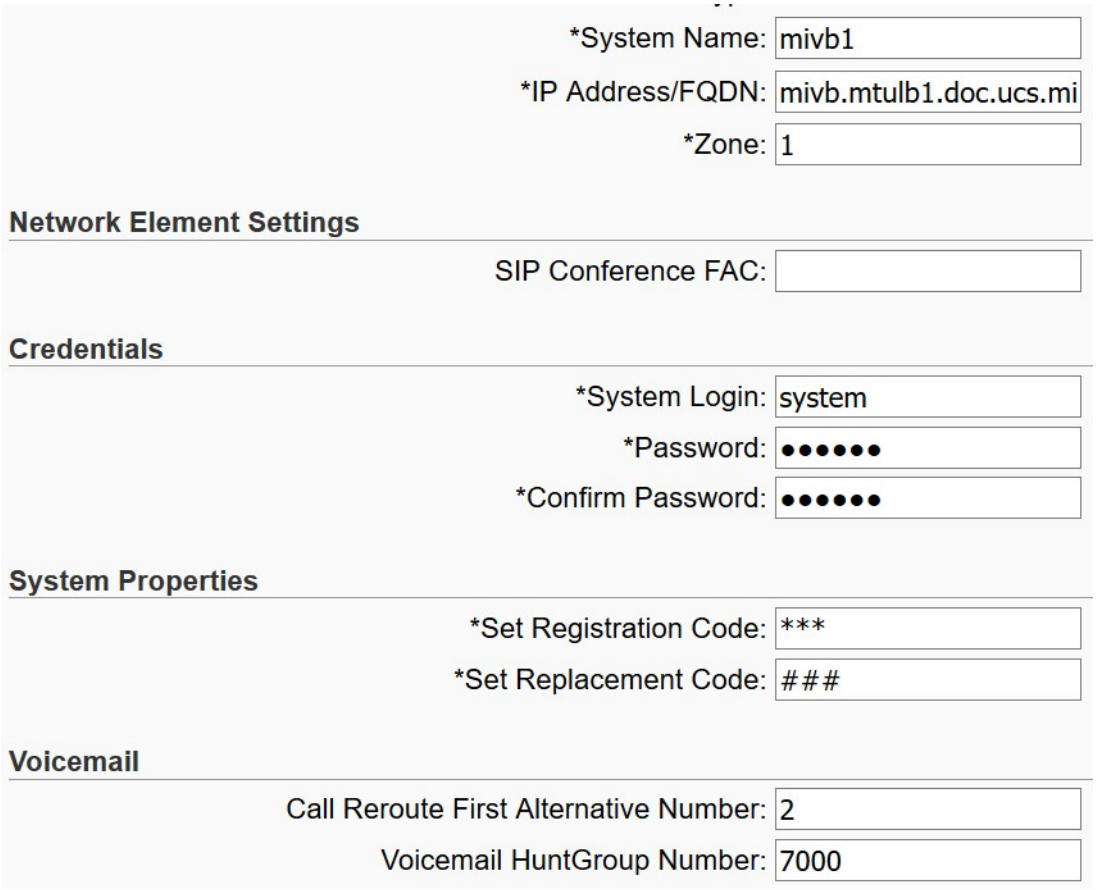


59. (MiCollab) Navigate to **Users and Services > Network Elements** in MiCollab to create a user with resilient voicemail. Access the MiCollab GUI from Solution Manager.

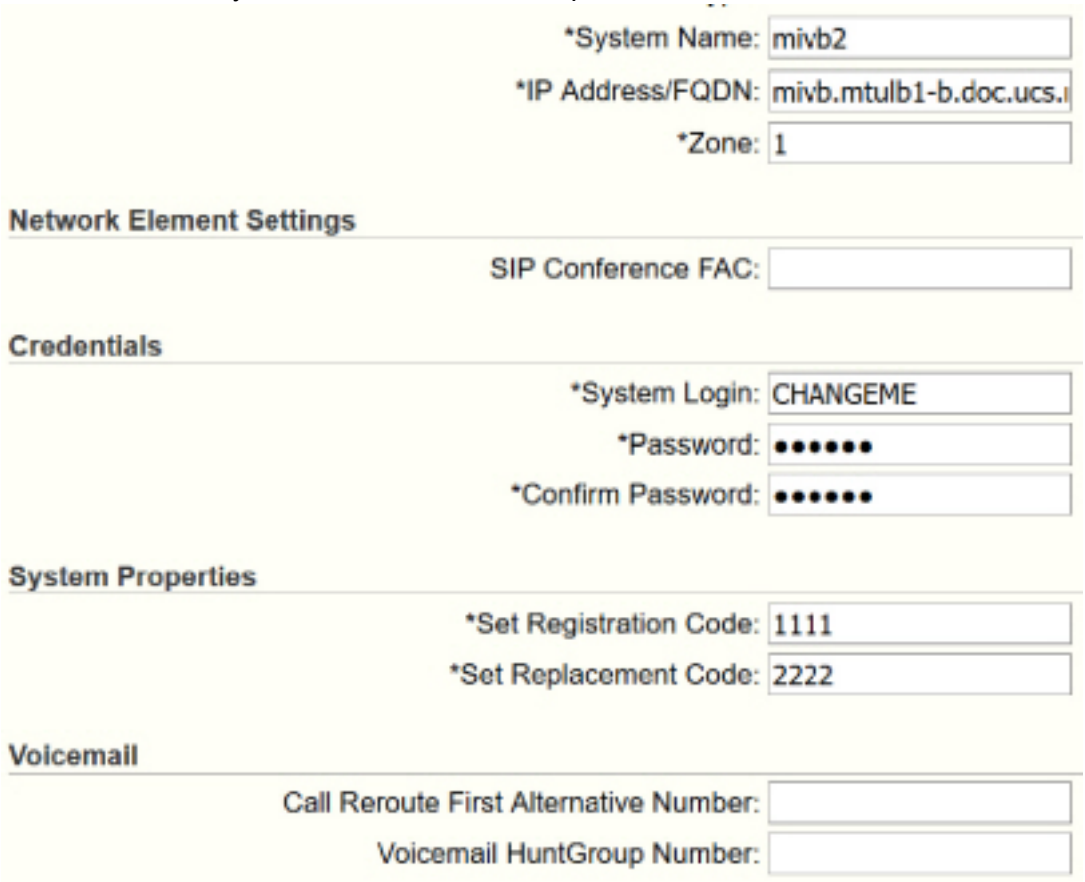


– Select MiVB1 to identify its attributes
– Under the Voicemail category:
  • Change the Call Rerouting First Alternative rule from 1 (the default) to 2 (what was assigned by the ICW)
  • Voicemail Hunt Group – 7000 (for example)

- Click Save
- Click Cancel to return to the Network Elements form

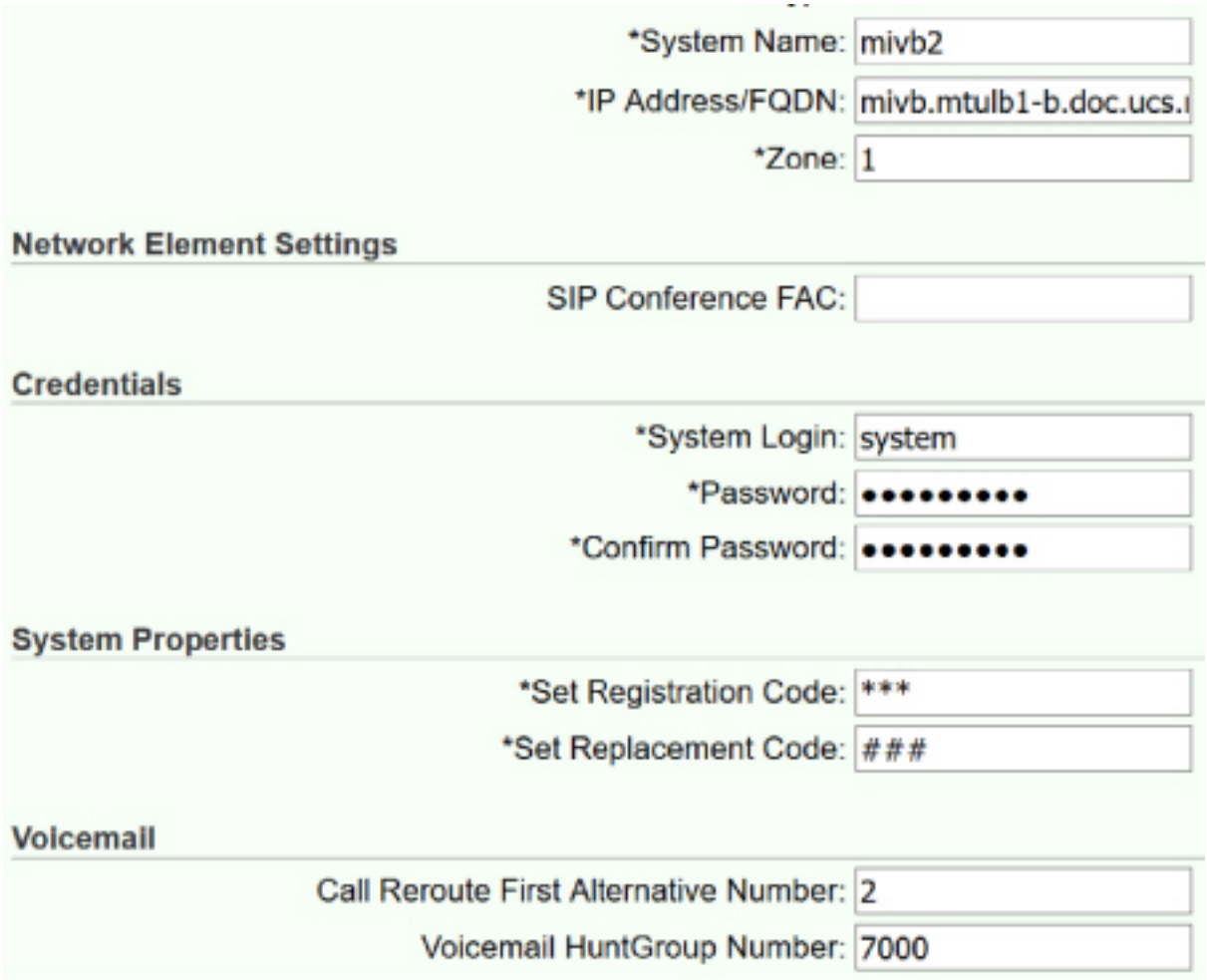


60. (MiCollab) Select the secondary MiVB (MiVB2 for example). The secondary MiVB attributes are incomplete. Since a reference to the secondary MiVB synchronized via SDS and not by the ICW, there are values that are set by default that need to be updated:



- Under Credentials:
  - System Login – system (for example)
  - Password – (the current password – MiCl0ud1! For example)
  - Confirm Password – MiCl0ud1!
- Under System Properties:
  - Set Registration Code - ***
  - Set Replacement Code - ###
- Under Voicemail:
  - Call Reroute First Alternative – 2
  - Voicemail Hunt Group Number – 7000
- Click Save

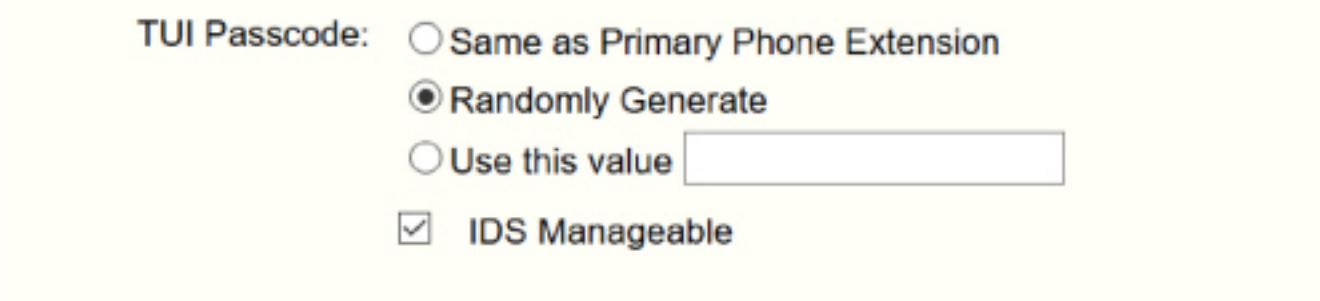
– Click Cancel to return to the MiCollab GUI



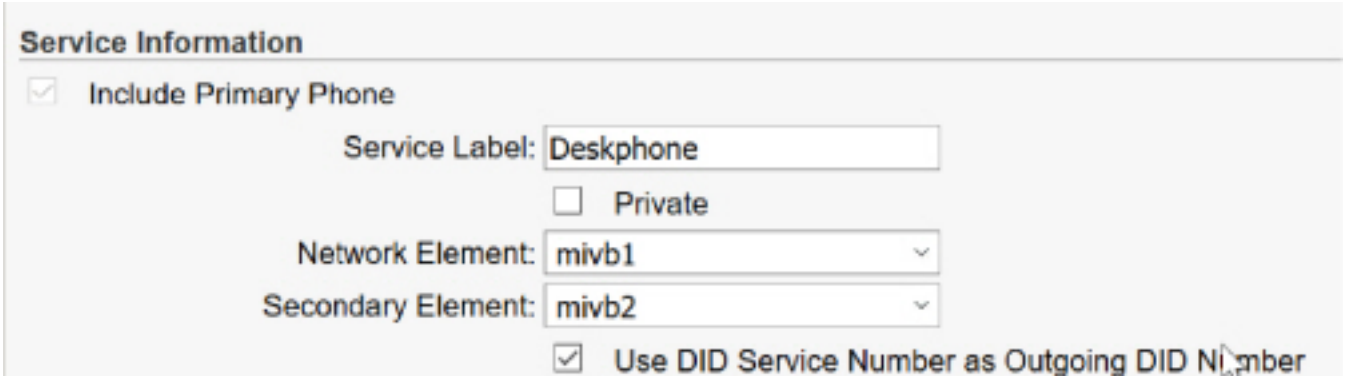
61. (MiCollab) You must select the appropriate User Template. For this example, navigate to **Users and Services > User Template > UCC Entry** to create a sample user template that will include EMEM services. There is no selection under the templates to create voicemail resiliency. It is dependent on whether or not the user profile created has resiliency set that determines whether or not an associated voicemail box is also created on the secondary MiVB. Edit the default UCC Entry template to include resiliency on the primary service with EMEM services selected.

– Review the TUI Passcode. The voicemail options set by default on the MiVB enforces passcode complexity. The validation rules are as follows:
  - The new PIN cannot match the old PIN.
  - The new PIN must have a length of 4 to 10 digits.
  - The new PIN cannot match its respective user's mailbox number.
  - The new PIN cannot be a sequence of consecutive digits (example, 1234 is not allowed).
  - The new PIN cannot be a digit repeated more than thrice in succession (example, 1111 is not allowed)

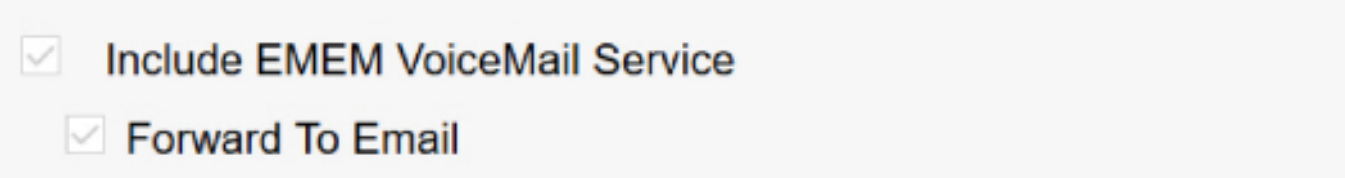
– In the template, the default rule is to randomly generate a passcode. Either keep that selection or use a value that follows the listed rules.



– Set MiVB2 as the secondary element to enable resiliency on the user services

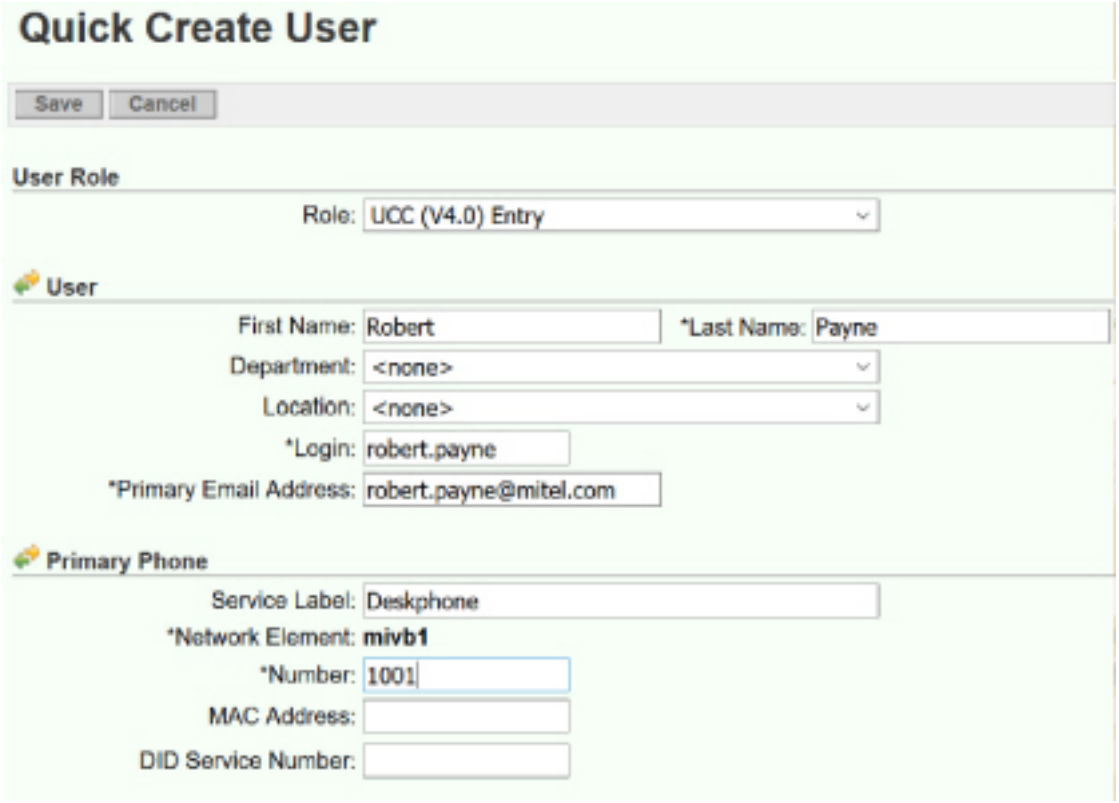


– The EMEM Voicemail Service is enabled on the template by default.

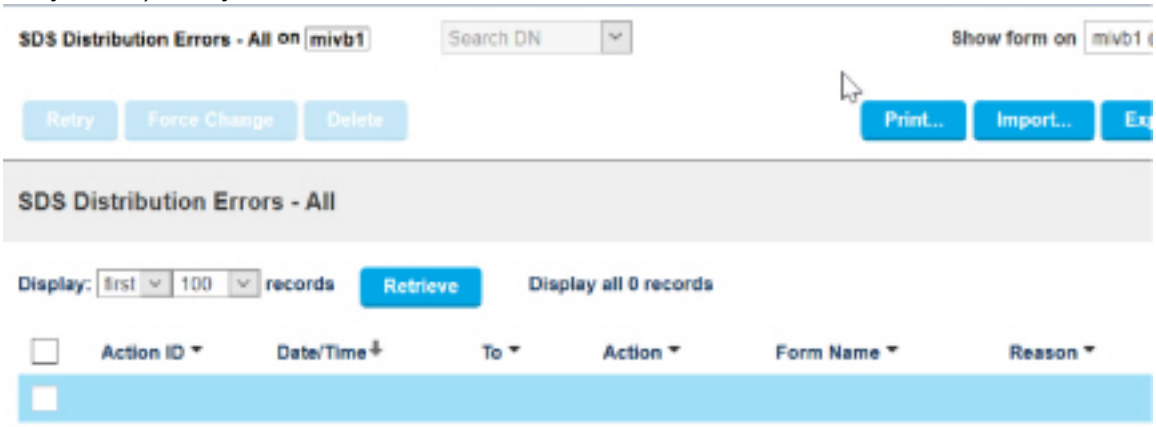


62. Test the resilient voicemail services by creating a test user with voicemail. The voice mailboxes should be created on both the primary and secondary MiVBs. It is important to note that embedded voicemail

boxes are not resilient so much as redundant. Any rules, greetings, names, are not synchronized and must be managed by the user on both MiVBs.

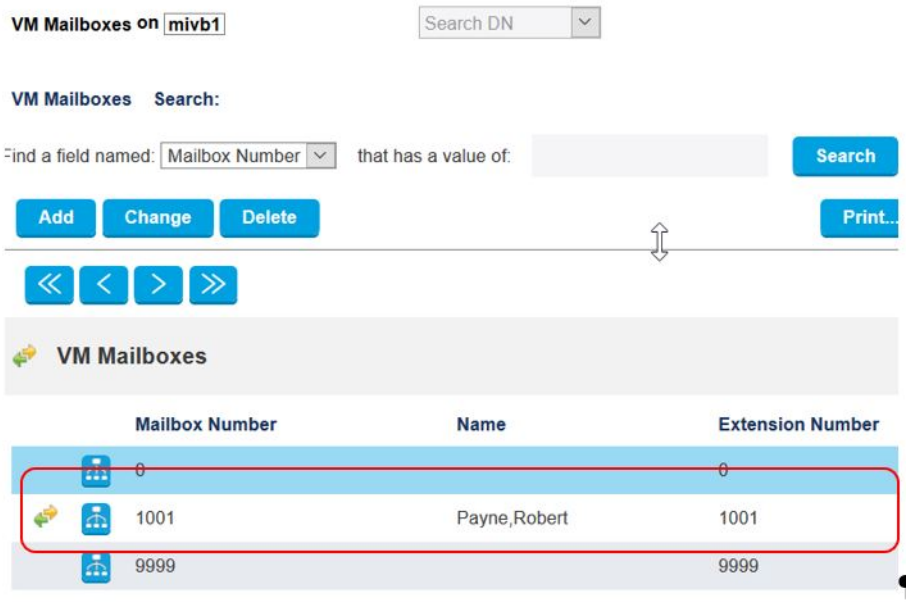


63. (Primary MiVB) Verify there are no SDS Distribution Errors:

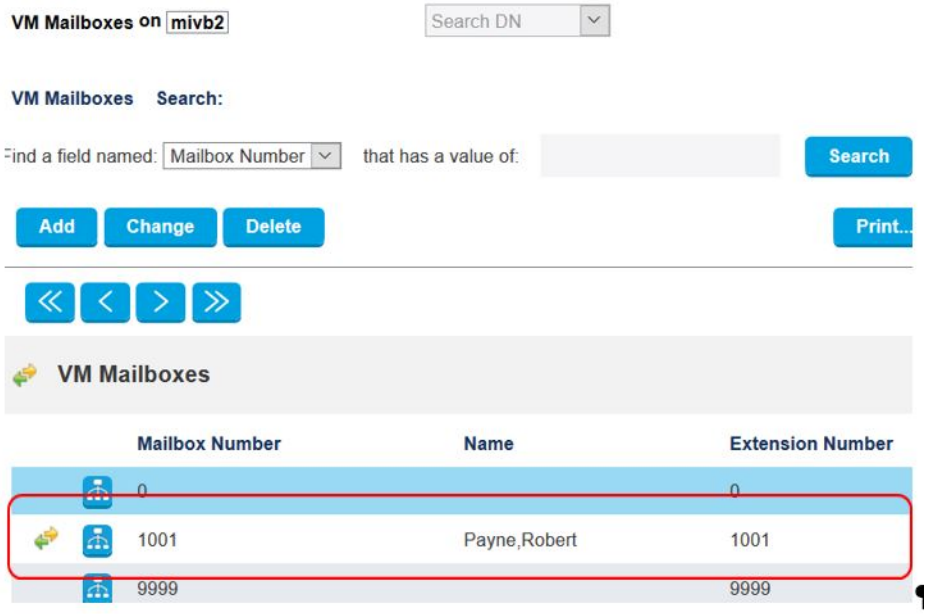


64. Verify the user mailbox has been created on MiVB1 and MiVB2

MiVB1



MiVB2



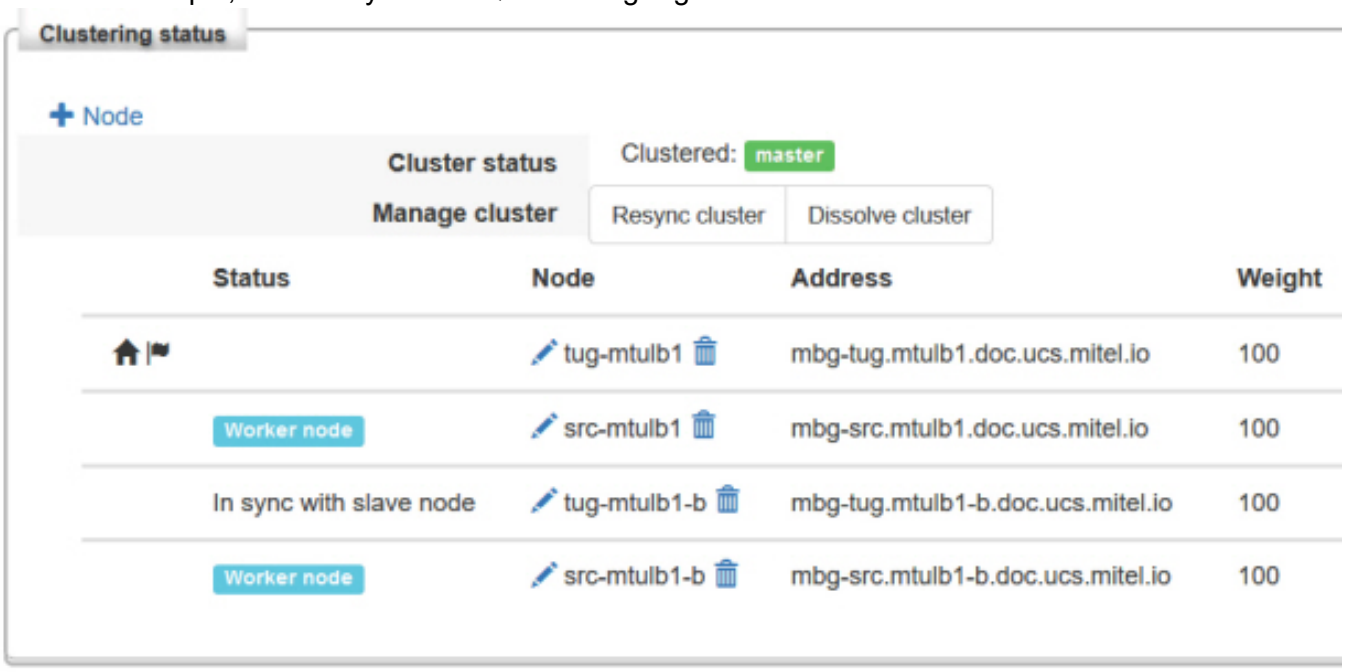
Configuring SIP Trunking Resiliency for MiVB

IMPORTANT: While making any change to csv files before importing the files into MiVB, you must make the change using Windows Notepad and not Microsoft Excel® or WordPad, as Microsoft Excel or WordPad can modify the file and may cause errors when the file is imported in to MiVB.

Before You Begin

Before you begin, ensure the following configuration steps have been completed:

- The Primary and Secondary MBG are deployed within an MBG Cluster. This means that programming that has occurred on the primary MBG by the ICW, for example, SIP Trunking configuration, has already been synchronized to the secondary MBG. Take note of the secondary MBG FQDN as we will require that in a later step.
  - For example, primary MBG FQDN is mbg-tug.mtulb1.doc.ucs.mitel.io
  - For example, secondary MBG FQDN is mbg-tug.mtulb1-b.doc.ucs.mitel.io



- If SIP Trunking is selected in the ICW, the wizard has configured the following steps on the Primary MiVB:
  - Network elements for the Session Border Controller (SipPRI) and Outbound Proxy (MbgPri) are created.

Name	Type	PBX Number/Cluster Element ID	FQDN or IP Address
MbgPri	Outbound Proxy	---	mbg-tug.mtulb1.doc.ucs.mitel.io
micollab	MSL Server (MiCollab)	---	micollab.mtulb1.doc.ucs.mitel.io
mivb1 (Local)	3300 ICP	1	mivb.mtulb1.doc.ucs.mitel.io
mivb2	3300 ICP	2	mivb.mtulb1-b.doc.ucs.mitel.io
SipPri	Other	---	sipco.miteluniversity.us

– A sip peer profile on the Primary MiVB is created. The SIP Peer Profile label typically matches the Network Element name, for example, SipPri, and references the primary MBG as the Outbound Proxy Server, for example, MbgPri.

SIP Peer Profile

Network Element	SIP Peer Profile Label	Outbound Proxy Server
SipPri	SipPri	MbgPri

- On the primary MiVB, Automatic Route Selection (ARS) values are generated using the Sip Peer Profile. This includes a base selection of ARS Digit Modification Plans, ARS Routes and ARS Digits dialed. These are based on the telecommunication region selected within the ICW and can be further modified based on the customer needs.
  – **ARS Digit Modification Plans**

ARS Digit Modification Plans

Digit Modification Number	Number of Digits to Absorb	Digits to be Inserted
1	1	
2	1	
3	1	
4	0	
5	0	
6	0	
7	1	
8	1	
9	1	
10	0	

– **ARS Routes**

ARS Routes

Route Number	Routing Medium	Trunk Group Number	SIP Peer Profile	PBX Number / Cluster Element ID	COR Group Number	Digit Modification Number	Digits Before Outpulsing	Route Type	Compression
1	SIP Trunk		SipPri		1	1			Auto
2	SIP Trunk		SipPri		2	2			Auto
3	SIP Trunk		SipPri		3	3			Auto
4	SIP Trunk		SipPri		4	4		Emergency	Auto
5	SIP Trunk		SipPri		5	5			Auto
6					1	1			Off
7	SIP Trunk		SipPri		4	7		Emergency	Auto
8	SIP Trunk		SipPri		8	8			Auto
9	SIP Trunk		SipPri		9	9			Auto

– **ARS Digits Dialed**

NOTE: The Digits Dialed of 7702 was added in the previous step of setting up the MiVB Cluster by the administrator. Direct IP Trunks are not part of the primary ICW.

ARS Digits Dialed

Digits Dialed	Number of Digits to Follow	Termination Type	Termination Number
7702	Unknown	Route	44
9	10	Route	1
9011	Unknown	Route	3
91	10	Route	2
91800	7	Route	8
91809	7	Route	5
91855	7	Route	8
91866	7	Route	8
91877	7	Route	8
91888	7	Route	8
91900	7	Route	5
91976	7	Route	5
9911	0	Route	7

Programming Steps

The following steps are one example of how to set up a method of SIP Trunking resiliency to support call routing survivability in the event there is an outage of the primary cluster and users are required to failover to a resilient cluster. These steps are assuming that the customer is deployed using 1 (one) SIP Trunking Provider, so the primary and the secondary MBG and MiVBs will be referencing the same provider. Some customer deployments may reference more than one provider dependent on customer needs, but that is not covered within this example.

MBG Configuration

When the Primary and Secondary MBG's are deployed, a cluster is created and the primary MBG set as the master. The ICW has configured the SIP Trunking values within the primary MBG, which has synchronized the values with the secondary MBG.

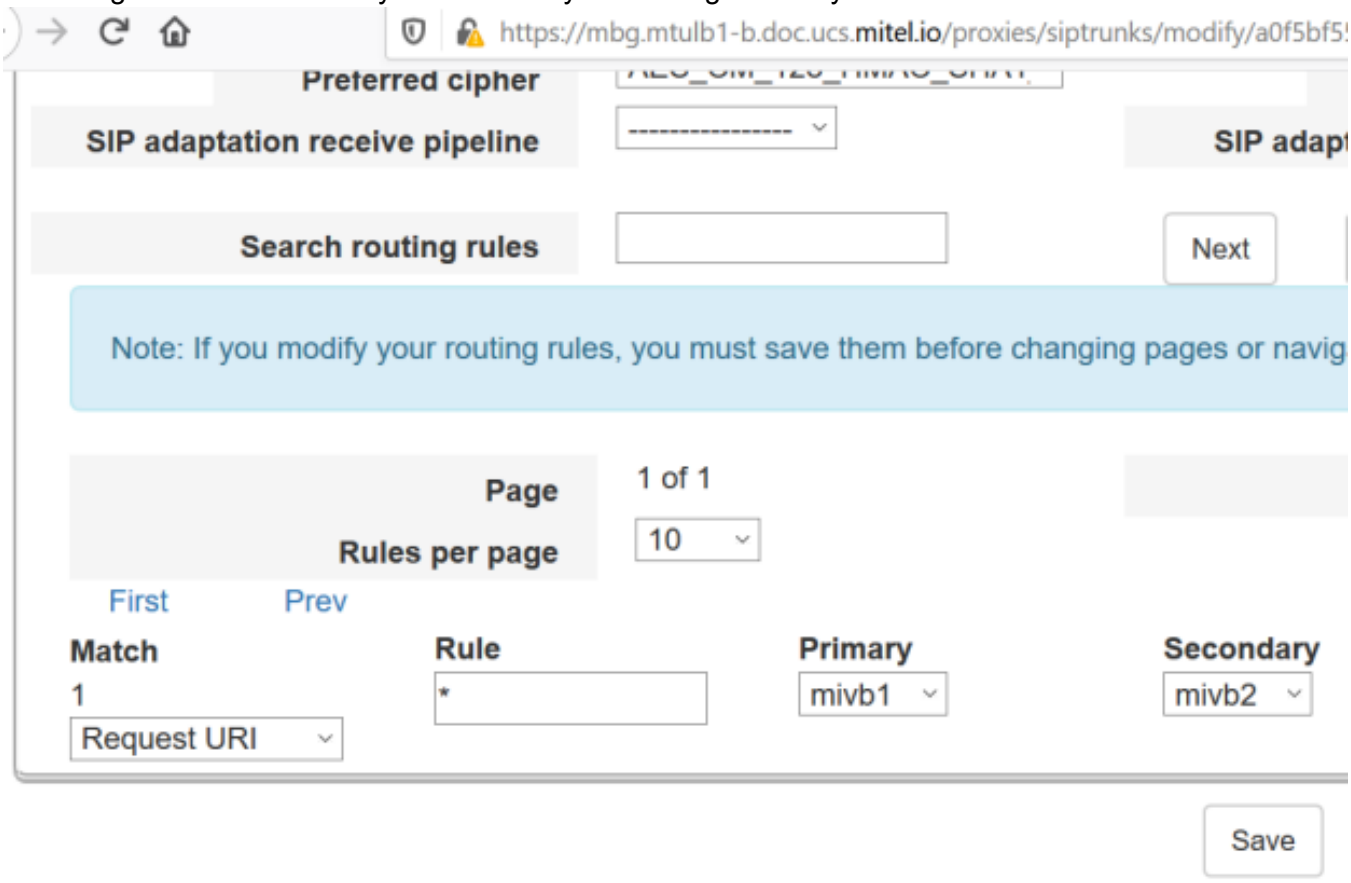
From the primary MBG dashboard:

1. Navigate to **SIP Trunking > Configuration**
2. Select the **Edit** icon to modify the values

3. Set the Secondary MiVB as MiVB2 (for example)
4. Click Save to apply the values

NOTE: MBG routes an incoming SIP trunk call to the secondary MiVB only if the primary MiVB is marked unavailable, unreachable, or down because the primary MiVB failed to respond to three consecutive SIP option keepalives or to a SIP message within 32 seconds.

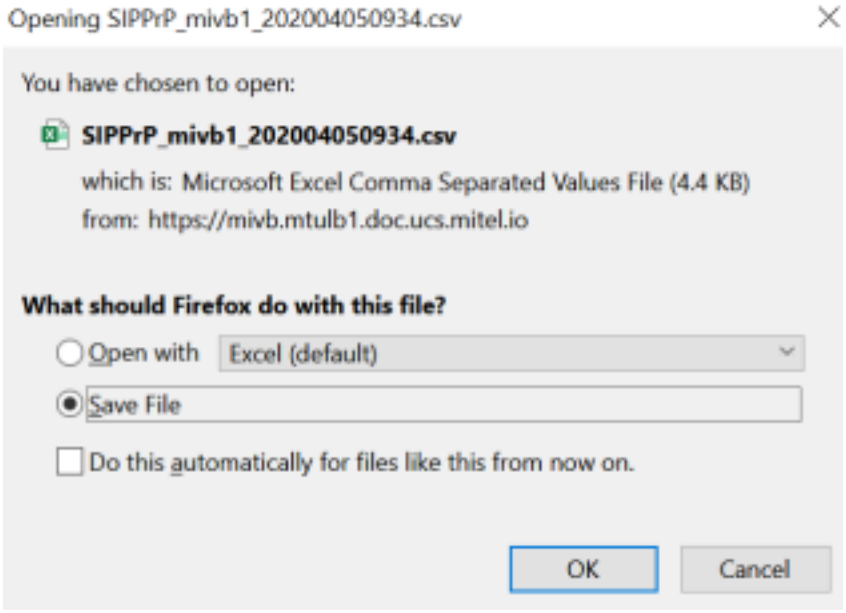
5. Navigate to the secondary MBG to verify the settings were synchronized



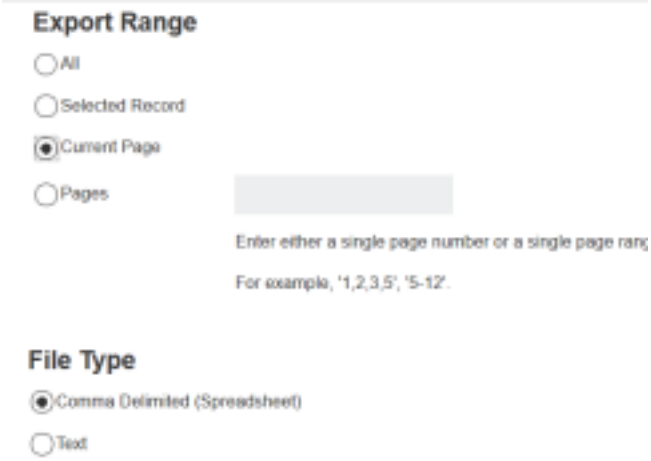
MiVB Configuration

ICW has configured SIP Trunking in the primary MiVB. However, SIP trunking is not automatically added to the secondary MiVB. The following steps demonstrate how to setup SIP Trunking in secondary MiVB by utilizing System Data Synchronization and appropriate form export and imports.

1. (Primary MiVB) Navigate to **Trunks > SIP > SIP Peer Profile** and export several forms from the primary MiVB (MiVB1 for example) that we will later import into the secondary MiVB (MiVB2 for example).
   - Click Export
   - Keep all the default values
   - Click Export and note the location of the saved file
   - Click OK



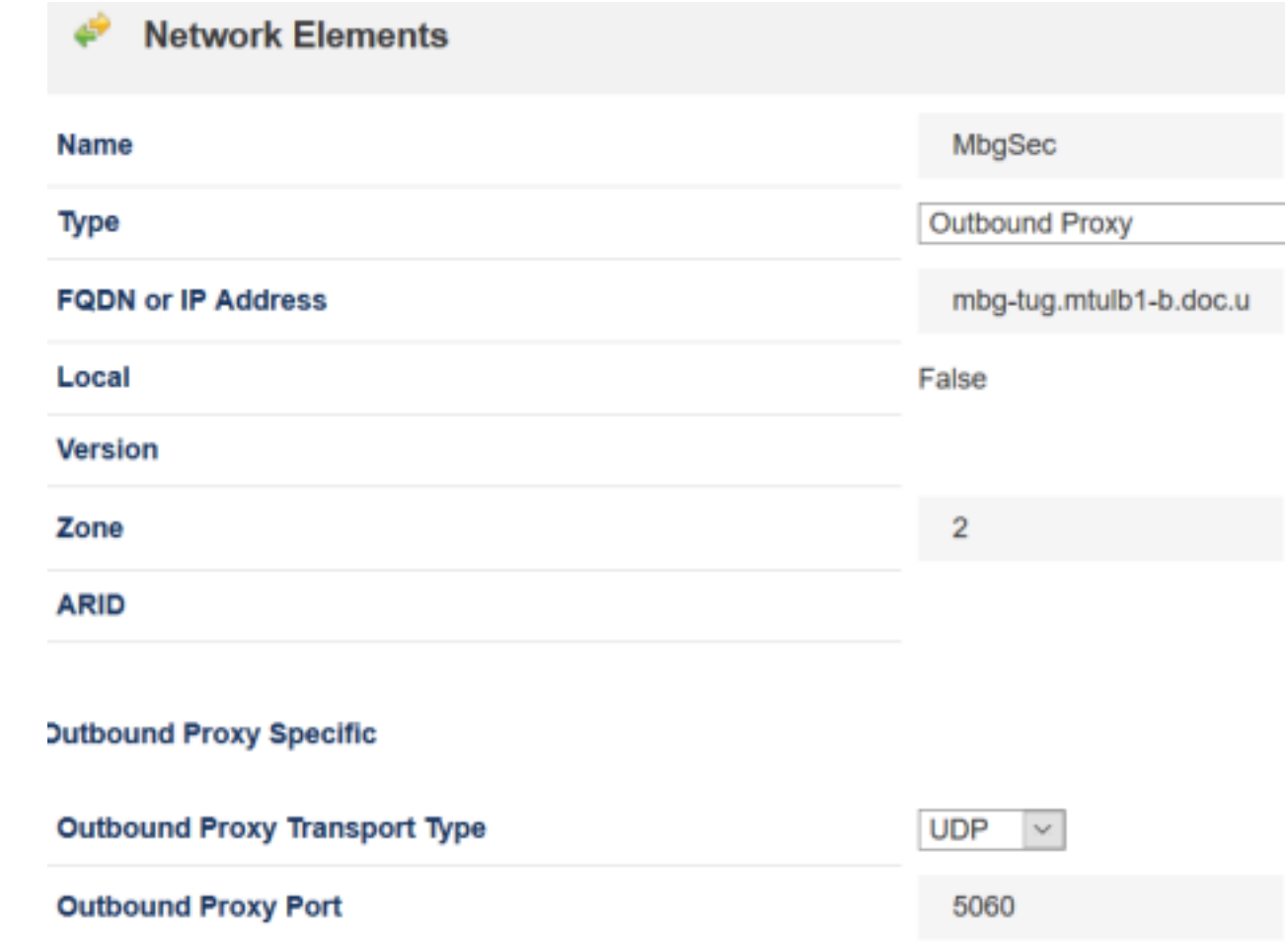
2. (Primary MiVB) Navigate to **Call Routine > ARS > ARS Routes** and export the form.
   - Click Export
   - Select Current Page as the Export Range



   - Click Export and note the location of the saved file

- Click OK

3. Navigate to **Call Routing> ARS > ARS Digits Dialed**
   - Click Export
   - Keep all the default values
   - Click Export and note the location of the saved file
   - Click OK
4. (Secondary MiVB) Navigate to **Voice Network > Network Elements > Add** to set the secondary MBG as a network element on the secondary MiVB.
   - Name – MbgSec (for example)
   - Type – Outbound Proxy
   - Zone – 2 (to match the primary MBG)
   - Outbound Proxy Transport Type – UDP
   - Outbound Proxy Port – 5060
   - Select Save

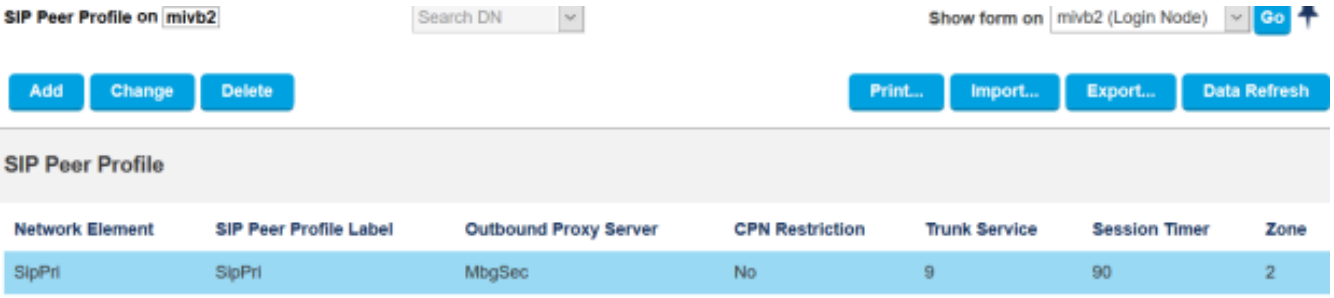


Name	Type	PBX Number/Cluster Element ID	FQDN or IP Address	Data Sharing	Version	Zone
MbgPri	Outbound Proxy	---	mbg-tug.mtulb1.doc.ucs.mitel.io	NO		2
MbgSec	Outbound Proxy	---	mbg-tug.mtulb1-b.doc.ucs.mitel.io	NO		2

5. Locate the SIP Peer Profile csv file, and edit the following values to import the file into the secondary MiVB
   - Network Element – Remove the existing value and replace with the current SIP Network element name, for example, SipPri (the name must match the current network element name)
   - Outbound Proxy Server – Remove the existing value and replace with the current Secondary MBG network element FQDN, for example MbgSec
   - Zone – While the current zone (2) is set correctly, the import of the file if left as 2 is seen as an error. We will temporarily change the zone to 1, then manually change it back to 2 after import. Change the Zone to 1 in the CSV file and import. After importing, change the Zone back to 2 from the Network Elements form
   - Save the file

SIP Peer P	vid0.160	20.1.0.81									
0	1	2	3	8	9	32	4	12	7	11	
SIP Peer P	Network Element	Registration	Address Type	Interco	Maxim	Minim	Outbound Proxy Server	SMDR	Trunk	Zone	U
SipPri	SipPri		FQDN: mivb.n	1	10	10	MbgSec	1	9	1	

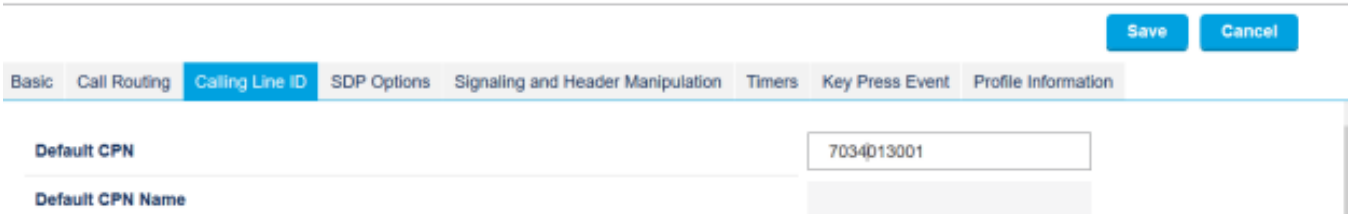
6. (Secondary MiVB) Navigate to **Trunks > SIP > SIP Peer Profile** to import the SIP Peer Profile
   - Click Import
   - Navigate to the edited csv file saved in the previous step
   - Click Next
   - Verify the values displayed
   - Click Import
   - Click Finish



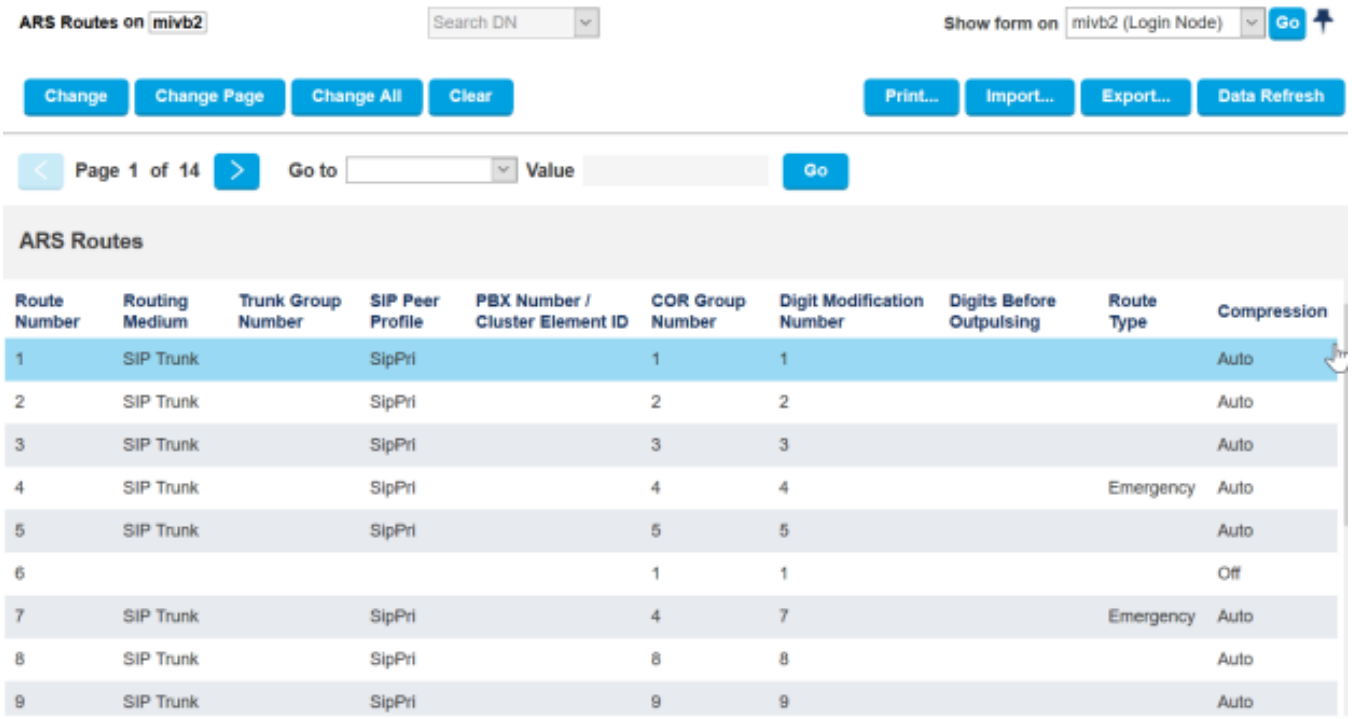
NOTE: The Zone will revert back to the network element value of Zone 2. Also, if you see a **SIP Link Alarm** in the critical state you must clear the alarm by entering the password and confirming the same under **Trunks > SIP > SIP Peer Profile > Basic > Authentication Options**.

- The SIP Peer Profile may require additional setting changes. For example, a provider may have a secondary account for resilient customers that may need to be added (for example, a user authentication such as customer for the primary account and customer-sec for the resilient account). In this example, we will change the primary Default CPN
  - Click Change
  - Change the Default CPN to that of the secondary account. In this example, the Default CPN was changed from 7033013001 to 7034013001

- Click Save. This is just one example of values that may need to be edited to support a resilient account. See your specific provider for further details.



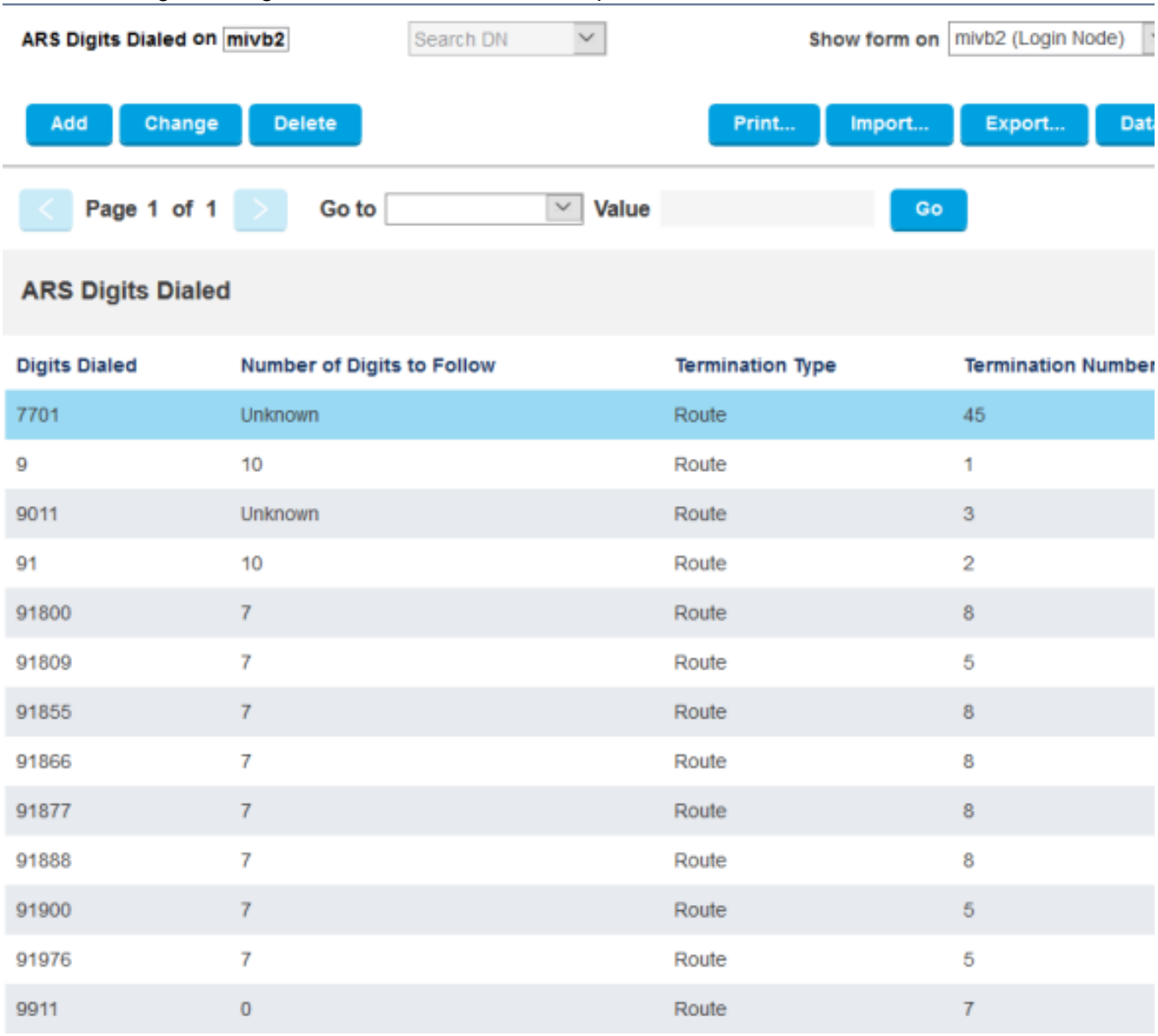
7. (Secondary MiVB) Navigate to **Call Routing > ARS > ARS Routes** to configure the SIP Peer Profile before importing the ARS Routes into the secondary MiVB.
   - Click Import
   - Locate the csv file you had exported earlier
   - Click Next
   - Click Import
   - There are several ARS Routes that were not populated. These display as errors since they are blank. This is normal.
   - Click Done to complete the import



Route Number	Routing Medium	Trunk Group Number	SIP Peer Profile	PBX Number / Cluster Element ID	COR Group Number	Digit Modification Number	Digits Before Outpulsing	Route Type	Compression
1	SIP Trunk		SipPri		1	1			Auto
2	SIP Trunk		SipPri		2	2			Auto
3	SIP Trunk		SipPri		3	3			Auto
4	SIP Trunk		SipPri		4	4		Emergency	Auto
5	SIP Trunk		SipPri		5	5			Auto
6					1	1			Off
7	SIP Trunk		SipPri		4	7		Emergency	Auto
8	SIP Trunk		SipPri		8	8			Auto
9	SIP Trunk		SipPri		9	9			Auto

8. (Secondary MiVB) Navigate to **Call Routing > ARS > ARD Digits Dialed** to import the ARS Digits Dialed form.
   - There will be 1 (one) existing ARS Digits Dialed rule that currently exists which points towards the primary MiVB, in this example, 7701. This rule will not be overwritten when we complete the import
   - Click Import
   - Navigate to the file location where the ARS Digits Dialed csv file was saved

- Click Next
- Click Import to complete the process
- There will be a notification of the secondary ARS Digits Dialed digits already existing (in this example, 7702) The digits already exist. The record is not found. This error is expected.
- Click Done to complete the import
- Verify that the existing ARS Digits Dialed rule, 7701, still exists and was not overwritten, while the remaining ARS Digits Dialed rules have been imported.



9. Ensure to backup the primary and secondary solution from their respective Solution Manager GUIs.

Configuring Voice Mail Resiliency for Onsite Gateway

You can fallback on the onsite gateway in case of a failover instead of falling back on the secondary MiVB. Use the steps listed below to configure voice mail resiliency for onsite gateway:

1. Configure Hunt Group members of the Hunt Group type Voicemail to add members that need to fallback or failover to the secondary MiVB in the MiCloud Flex solution. For information on how to configure Hunt Groups, see the **Forms Reference > Forms H to M > Hunt Groups** topic of the *System Administration Tool Online Help* that is part of the MiVB GUI available in the MiCloud Flex solution.
2. Create an additional Hunt Group of type Voicemail and add appropriate Hunt Group members that need to fallback to the onsite gateway in the **Hunt Groups** form. For information on how to add additional Hunt Groups, see the **Forms Reference > Forms H to M > Hunt Groups** topic of the *System Administration Tool Online Help* that is part of the MiVB GUI available in the MiCloud Flex solution.
3. Configure the **Secondary Element** field in the **Hunt Groups** form for each of the secondary and onsite gateway Hunt Groups to ensure users can fallback or failover to the respective secondary or onsite gateway MiVB. For information on how to configure the **Secondary Element** field, see the **Forms Reference > Forms H to M > Hunt Groups** topic of the *System Administration Tool Online Help* that is part of the MiVB GUI available in the MiCloud Flex solution.
4. Configure Call Rerouting to ensure that the voicemail can fallback or failover to the appropriate hunt group configured for the secondary or onsite gateway MiVB. For information on how to configure call rerouting, see the **Forms Reference > Forms A to C > Call Rerouting** topic of the *System Administration Tool Online Help* that is part of the MiVB GUI available in the MiCloud Flex solution.
5. Configure Class of Service Options (COS) for voicemail as required based on your MiCloud Flex deployed solution. For information on how to configure COS, see the **Forms Reference > Forms A to C > Class of Service Options** topic of the *System Administration Tool Online Help* that is part of the MiVB GUI available in the MiCloud Flex solution.
6. Configure the **Secondary Element** field in the **User and Services Configuration** form to split the users to redirect the users to fallback or failover to secondary MiVB or onsite gateway accordingly. For information on how to split users, see the **Forms Reference > Forms S to Z > User and Services Configuration** topic of the *System Administration Tool Online Help* that is part of the MiVB GUI available in the MiCloud Flex solution.

Using the Initial Configuration Wizard

The Initial Configuration Wizard (ICW) is launched from the **Solution Manager** GUI. You only run ICW once on the primary deployment during the initial configuration of the system.

When the Initial Configuration Wizard (ICW) is launched, the system applies default settings to the following applications based on your deployment:

- MiVoice Business
- MBG
- MiCollab

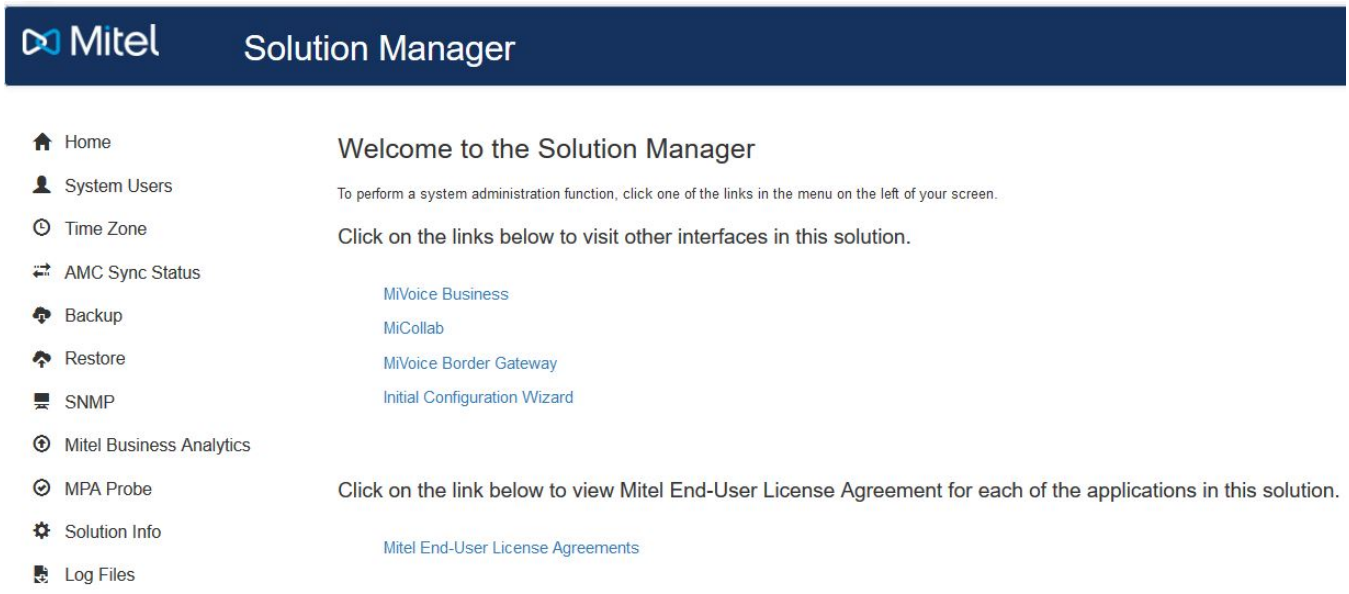
Refer to the respective online help for the standard default settings that are applied to the MiVoice Business platform, MiCollab, and MBG applications.

ICW allows you to configure the system with the basic settings required to get the system up and running. After completing the wizard, the wizard configures the system with your settings. ICW guides you through the following configuration steps:

- Review initial configuration parameters
- Configure Resiliency
- Configure administration email and servers
- Configure languages
- Configure numbering plan
- Configure SIP Trunking (optional)
- Configure incoming call configuration
- Select and configure SIP provider
- Configure MPA Probe
- Configure Mitel Business Analytics
- Configure optional services: AWV, Hot Desking, and Music on Hold
- Change the administrator password for MiVB
- View a summary of the configuration
- Download Logs

To launch ICW, log in to **Solution Manager** GUI and click on **Initial Configuration Wizard**.

IMPORTANT: Ensure that your primary and secondary solution is backed up from their respective Solution Manager GUIs before you launch ICW.



Next Steps – Accessing and Using MiCloud Flex Applications

This chapter contains the following sections:

Accessing MiCollab

You launch MiCollab from the **Solution Manager** GUI. When you click the MiCollab link in Solution Manager, you will be redirected to the MiCollab GUI. MiCollab is enabled with single sign on.

The MiCollab deployment is set to Integrated mode by default. 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. It allows you to provision MiCollab Client services from the MiCollab Users and Services application and supports flow through provisioning of the MiCollab Client services on the MiVoice Business platform(s). This is the recommended mode for sites that meet the integration requirements. Integrated Mode is required to support MiCollab Integrated Directory Services (IDS).

Verifying Licenses

To verify MiCollab licenses:

1. Click the MiCollab link from the **Solution Manager** GUI.
2. The **MiCollab** GUI opens on the **Licensing Information** page.
3. Verify the licenses that have been applied.

   NOTE: If the licensing does not appear to be applied correctly, return to the Solution Manager GUI and attempt to Sync with the AMC again.

Setting up MiCollab post ICW

After running ICW, there are several settings on the MiCollab that you must configure before you can use MiCollab.

1. **Provision network elements**: Configure MiCollab with the MiVoice Business network elements for Flow Through Provisioning. For more information on configuring network elements, see the *MiCollab*

Server Manager Online Help > Applications > Users and Services > System Administrator > Manage Network Elements section.

2. **Setting up MiCollab Client resiliency**: Create DNS Service (SRV) records to provide FQDN-to-host-name mapping and specify priorities, weightings, port configuration, and Time to Live (TTL). You can find the DNS SRV records information in the Welcome e-mail.

   If the MBG or MiVB that connects the softphone to the network fails, the softphone registers with a secondary MBG or MiVB in the cluster depending on the FQDN configured in the SRV record. For more information on how to create DNS SRV records, see **Overview > DNS Service Records** in the *MiCollab Client Resiliency Guide*.

NOTE: If the system is deployed under the domain name **flex.gc.mitel.io**, then the system automatically creates the DNS SRV records during the deployment.

3. **Create templates and roles**: Create MiCollab user templates that reflect the MiCollab service mixes that you want to assign to users. For more information on creating roles and templates, see the *MiCollab Server Manager Online Help > Applications > Users and Services > System Administrator > Manage Roles and Templates* section.

4. **Provision users and services**: There are multiple ways to create users and provision services for the users. Following are the users and services provisioning methods:

   - Manual Provisioning
   - Flow Through Provisioning
   - Bulk User Provisioning
   - Provisioning with IDS

   For more information on users and services provisioning, see the *MiCollab Server Manager Online Help > Applications > Users and Services > System Administrator > Provision Users and Services* section.

5. Configure **Voicemail Hunt Group number** in the **Network Element** tab. For more information on configuring voicemail hunt group number, see the *MiCollab Server Manager Online Help > Applications > Users and Services > System Administrator > Manage Network Elements > MiVoice Business Field Descriptions* section.

6. Configure **Call Reroute First Alternative (CRFA) number** in the Voicemail settings. For more information on configuring Call Reroute First Alternative (CRFA) number, see the *MiCollab Server Manager Online Help > Applications > Users and Services > System Administrator > Manage Network Elements > MiVoice Business Field Descriptions* section.

7. Configure **EMEM Voicemail Service** in the template information. For more information on changing the template information, see the *MiCollab Server Manager Online Help > Applications > Users and Services > System Administrator > Manage Roles and Templates* section.

Accessing MiVoice Business

You launch MiVoice Business (MiVB) from the **Solution Manager** GUI. When you click the MiVoice Business link in Solution Manager, you will be redirected to the MiVoice Business GUI. Enter the user name and password that was provided while running ICW to log into the MiVoice Business GUI.

Verifying Licenses

To verify MiVoice Business licenses:

1. Click the MiVoice Business link from the **Solution Manager** GUI.
2. Log in to the **MiVoice Business** GUI, by entering the user name and password provided in the welcome e-mail
3. In the **MiVoice Business** GUI, click **Licenses**>**License and Option Selection** from the left of the menu.
4. The **License and Option Selection** page opens, displaying the licenses that have been applied.
5. View the page to verify whether the correct licenses have been applied.

NOTE: *Use the **License and Option Selection** page to modify licenses through the Applications Management Center (AMC). On MiVoice Business, licenses are required for options, features, and system capacity. For example, each IP Phone user that you connect to the system requires an IP User license.*

Setting up MiVoice Business post ICW

NOTE: System user access will continue to be used in MPA 3.1 and MiVB 9.1; however, changing the password in MiVB requires that it must also be changed in MPA and vice-versa.

After running ICW, there are several settings on the MiVoice Business that you must configure before you can use MiVoice Business. These are:

1. Use the **Network Zones** form to create zones for compression and bandwidth management, to associate the zones to time zones for the display of local time on IP sets, to configure the zone's Location Based Number (LBN) prefix to be used for Location Based Call Routing (optional), and to define the zone's CESID (optional). For more details, see *MiVoice Business System Administration Tool help.*
2. All MiCollab applications must be able to connect to the MiVoice Business through MiTAI. The user name and password used for this connection must be the same as the MiVoice Business System login credentials. You must enable CTI Application Authentication using the **Shared System Options** page in MiVoice Business System Administration tool.
3. Ensure that the default values set for the various settings in the **System Options** page are accurate for your deployment.
4. Use the **System Access Points** form to assign values to various devices in the system which require no special programming other than one parameter.
5. Use the **Feature Access Codes (FACs)** form to define codes that users can dial to access system features, such as Do Not Disturb.
6. To view additional details about call rerouting and call transfer, use the Station Message Detail Recording (SMDR) form.
7. Use the **Admin Policies** form to add, modify, and delete policies that control access to the forms in the System Administration Tool.
8. Create, modify, and delete user profiles which are required to access the MiVoice Business management interfaces such as System Administration Tool, Group Administration Tool, and Desktop Tool using the **User Authorization Profiles** form.

9. Use the **SIP Peer Profile** form to configure licensing, authentication, and site or peer specific features and requirements for SIP trunks.
10. Use the **Hunt Groups** form to gather directory numbers into terminal or circular groups.
11. Use the **Call Coverage Services** form to provision Group Announcements, Hot Desk PIN Security, Direct Transfer to Voice Mail, Post Call Destination, and Workgroup and Branch Office Music on Hold features.
12. To redirect calls to alternate answering points or devices under specified conditions, use the **Call Rerouting** form.
13. Use the **Direct Inward Dialing Services** form to map DID numbers to their destinations, but the configured data is saved, stored in, and retrieved from the Call Recognition Service (CRS) database. Use the **Call Recognition Service** form to search and view the DID records.
14. Use the **Voice Quality Monitoring** form to enable or disable voice quality monitoring.
15. Use the maintenance commands from the **ESM Maintenance Commands** form to verify the SIP Connection on MiVB.

NOTE: *See the MiVoice Business product documentation for information about configuring these settings.*

Kari's Law Requirements

The United States Congress passed H.R.582 - Kari's Law Act of 2017 into law on February 16, 2018 as Public Law No: 115-127. Kari's Law requires compliance by February 16, 2020 for all United States business utilizing multi-line telephone systems (MTLS) in their enterprise. For more information on Kari's Law, click here.

Karis' Law requires the following:

- Direct access to 9-1-1 without an access code.
- Routing to the 9-1-1 PSAP (public safety answer point) with no interception.
- On-site notification to staff of who dialed 9-1-1.

Direct access to 9-1-1

Kari's law requires that any multi-line telephone system will allow callers to reach emergency services (911) without the need to dial a prefix for an outside number first. Thus, among other things, all enterprises utilizing MLTS will need to update their phone configurations accordingly. To add the digit string of 911 in MiVB:

1. Log in to MiVB
2. From the left menu, click **Call Routing > Automatic Route Selection (ARS) > ARS Digits Dialed > Add** and enter information for the following fields:
   - Digits Dialed – 911
   - Number of Digits to Follow – 0
   - Termination Type – Route
   - Termination Number – 4
3. Click Save

Emergency Services – MPA Notification Programming

To program Emergency Services notification for MPA (Mitel Performance Analytics):

1. Ensure that you have completed CESID Programming. See **System Applications > General Business Solutions > Emergency Services > CESID Support > Programming**in the System Administration Tool Online Help.
2. In the **Shared System Options** form:
    a. Ensure that the **Enable ER TRAPS** field is set to **Yes**.
    b. Enter the following:
        i. ***Trap IP Address/FQDN for ER notification = mpa-probe**
        ii. ***TRAP Community String**
            NOTE: Ensure that you enter the same TRAP community string in the Mitel Performance Analytics (MPA).
3. For Container-based MiVoice Business (cMiVB), in the Solution Manager, do the following:
    a. Navigate to **SNMP**, and set **Status** to **Enable**, enter the following:
        i. ***SNMPv2c community string for read-write access**
    b. Repeat this step for all the cMiVB systems in a cluster.
4. In the Server Manager of the remote gateway MiVoice Business system, navigate to **Configuration > Networks**, and add the MPLS network as a trusted network.
    a. Repeat this step for all of the remote gateway MiVoice Business systems in a cluster
        i. In the **Ring Groups** form, (for provisioning internal answering points as emergency responders), set the **Ring Group Type** to **Emergency Response**.
5. Configure your DNS server to resolve the MPA probe FQDN. To resolve the MPA probe FQDN:
    a. Log into the MiVoice Business which points to the DNS server within Google Cloud
    b. From the left menu, click **Maintenance and Diagnostics**.
    c. Click **Maintenance Commands**.
    d. In the Command field, type `ping mpa-probe` to resolve the MPA probe FQDN.

Accessing MiVoice Border Gateway

You launch MiVoice Border Gateway (MBG) from the **Solution Manager** GUI. Unlike the MiVB application, MBG does not require a separate administrative login. MBG will be deployed with initial settings applied by default.

NOTE: To return to the Solution Manager interface, in the MBG GUI on the right top corner click **Back to Manager**

Verifying Licenses

To verify MBG licenses:

1. Click the MiVoice Border Gateway link from the **Solution Manager** GUI.
2. In the **MiVoice Border Gateway** GUI, scroll down to the **License information** section.

3. Verify that the application displays the number of licenses required for deployment (for example, Tele-worker and SIP Trunk licenses).

Accessing MiContact Center Business

If MiContact Center Business has been deployed as part of your solution, you access the application by creating a RDP port rule in MPA for MICC and use that RDP link to access the virtual windows server. You must also enable Symantec Antivirus Protection before you access MiContact Center Business. To enable Symantec Antivirus Protection:

1. From the **Windows System Tray**, click the **Symantec Endpoint Protection** yellow badge. The **Status - Symantec Endpoint Protection** window appears.

2. Click **Fix All** to enable Symantec Endpoint Protection.

The following window appears

NOTE: *In some instances, a restart message may appear asking for a computer reboot.*

Setting up MiContact Center Business

Since MiContact Center Business is deployed on a Virtual Machine on MiCloud Flex, there are several settings on MiContact Center Business that you must configure before you can use MiContact Center Business. See the *Managing MiCC On MiCloud Flex In GCE* section in the MiContact Center Business - MiVoice Business Installation And Administration Guide.

Accessing Mitel Interaction Recording

If Mitel Interaction Recording has been deployed as part of your solution, you access the application by creating a RDP port rule in MPA for Mitel Interaction Recording and use that RDP link to access the virtual windows server.

NOTE: If you want to upgrade Mitel Interaction Recording, it is recommend to log on to each Mitel Interaction Recording server individually and download Mitel Interaction Recording ISO file using a web browser (HTTP download) directly from the ASC website. Alternatively the ISO can be uploaded to OneDrive or Google Drive and use the drive to download the software to the remote servers. For more information on how to upgrade Mitel Interactive Recording, see the **Software updates – Installation manual for service providers** document on Document Center.

You must also enable Symantec Antivirus Protection before you access Mitel Interaction Recording. To enable Symantec Antivirus Protection:

1. From the **Windows System Tray**, click the **Symantec Endpoint Protection** yellow badge. The **Status - Symantec Endpoint Protection** window appears.

2. Click **Fix All** to enable Symantec Endpoint Protection.

   The following window appears

NOTE: *In some instances, a restart message may appear asking for a computer reboot.*

Setting up Mitel Interaction Recording

IMPORTANT:

- For an OTT POP deployment, the WFO call recording VM needs to be configured with the internal FQDN of the mbg-tug pods for both the primary and secondary.
- For an MPLS deployment, the WFO call recording VM needs to be configured with the internal FQDN of the mbg-src and mbg-tug pods to be able to record IP Phones on the LAN.

The following tables below show an example of the internal FQDNs that are created for the primary domain name **gtsca.gts.ucs.mitel.io** and the secondary domain name **gtscar.gts.ucs.mitel.io** by the external-dns pod within the primary/secondary deployment for the MiCloud Flex solution:

Private DNS Record (Primary)	Purpose
mbg-src.gtsca.gts.ucs.mitel.io	Internal FQDN pointing to the mbg-src pod used for tapping IP Phone conversation on the LAN
mbg-tug.gtsca.gts.ucs.mitel.io	Internal FQDN pointing to the mbg-tug pod used for tapping IP Phone conversation on the Internet

Private DNS Record (Secondary)	Purpose
mbg-src.gtscar.gts.ucs.mitel.io	Internal FQDN pointing to the mbg-src pod used for tapping IP Phone conversation on the LAN
mbg-tug.gtscar.gts.ucs.mitel.io	Internal FQDN pointing to the mbg-tug pod used for tapping IP Phone conversation on the Internet

To set up Mitel Interaction Recording to record calls:

1. Enter the PSK password in the MBG GUI. To enter the PSK password:
   a. Log in to the MBG GUI.
   b. Navigate to **Call recording > Configuration**.
   c. Under **Secure Recording Connector**, select the **Enabled** check box.
   d. From the **Mode** drop down, select **PSK**.
   e. In the **PSK password** field, enter a matching password to the one configured for WFO.
2. In the Mitel Interaction Recording GUI, enter the same PSK password that was given in the MBG GUI. To enter the password:
   a. Log in to the Mitel Interaction Recording GUI.
   b. Navigate to **System Configuration > Setup > Integrations > Configure CTI connection data > Add**.
   c. In the **Configure Connection** dialog box, enter information for the following fields:
   - **Connection data** - Enter the internal FQDNs of MBG that were created as part of the deployment.
   - **PBX port** - Enter the port for MBG, default 6810.
   - **Activate indirect recording** - Select the check box if you would like to use indirect recording.
   - **Use pre-shared key** - Select the check box as MBG is used in the PSK mode.

- **Pre-shared key (PSK)** - Enter the pre-shared key that was given in the MBG GUI.

d. Click **Add**.

3. In the MBG GUI, navigate to **System > Settings**, and from the **Codec support** drop down, select **Restricted to G.729, G.711 (a-law and µ-law)**.

Monitoring and Maintenance

The chapter contains the following sections:

Viewing MiCloud Flex Solution Information

WARNING: Restarting components may affect service depending on component restarted.

The **Solution Information** page allows you to restart different components of the following applications:

- MiCollab
- MiVoice Border Gateway
- MiVoice Business
- Miscellaneous (Mitel Business Analytics, MPA Probe, External DNS)
- Solution Manager

NOTE: The **Solution Information** page displays each application as a heading with a table, which lists the component names, version and status. A **Restart** link for restarting each component is available.

To restart a component:

1. In the **Solution Manager** GUI, click **Solution Info**.
2. In the **Solution Information** page, under the different applications, navigate to the component you want to restart.
3. Click **Restart**.

   NOTE: A component that is running can be restarted. If the component has any other status it cannot be restarted. As a result the **Restart** link will not be displayed.
4. A warning message is shown when the user clicks on **Restart** asking for a confirmation.
5. Click **OK**.
6. The component is restarted. The status of the restart is highlighted either with a blue background (indicating that the component is being started) or with the red background (indicating an error in the restart process). Once the restart is successful the status changes to **Running**.

Backing-up MiCloud Flex Solution

You can perform 2 types of backup procedures:

- On demand. For on demand you use the **Solution Manager** GUI
- Scheduled. For scheduled, you use the MPA portal.

On Demand Backup using Solution Manager

The **Solution Manager** GUI allows the admin to perform a backup procedure.

To perform a backup:

1. In the **Solution Manager** GUI, click **Backup**.
2. To back up the data from this solution, click **Perform Backup**.

NOTE: The backup operation is a disruptive operation and will cause load on the system.

When the solution is deployed for the first time and you want to perform a backup procedure on MiVB using Solution Manager, you must reboot MiVB. To reboot MiVB:

1. Log into **Solution Manager** GUI.
2. Click **AMC Sync Status** from the left-hand menu.
3. In the **AMC Sync Status** page, verify that the MiVoice Business has successfully synced with the AMC. If the MiVoice Business is not synced, clear the hardware ID from the AMC website and click the **Sync** button.
4. Open MiVoice Business from the **Solution Manager** home page.
5. Log in to MiVoice Business.
6. Click **Maintenance and Diagnostics** at the left of the menu.
7. Click **Maintenance Commands**.
8. In the Command field, type `reset system` to restart MiVB.

Scheduled Backup using MPA Portal

It is recommended to use the MPA portal to perform a scheduled backup procedure. The perform a scheduled backup

1. Log in to the MPA portal.
2. Click **System Tools** > **Select Device Operations**.
3. In the **Device Operations** page, click **New Schedule**.

NOTE: The **Device Operations** page also displays any scheduled tasks that have already been scheduled.

4. In the **New Operation Schedule** page, from the **Select Operation Type** drop-down list, select **Backup (Cloud Storage)**.
5. Click **Next**.
6. In the **New Operation Schedule** page, enter the required information
7. Click **Save**.
8. In the **Add/Remove Devices** page, add the devices that must be backed up.

   NOTE: You can also remove devices that need not be backed up.
9. Click **Done**.

NOTE: After you have created the scheduled backup, in the **Device Operations** page, you can edit, add/remove devices or delete the scheduled backup.

Restoring MiCloud Flex Solution

NOTE: Once your solution is deployed and if you are performing a restore procedure and encounter an **Invalid signature for service account** error you must clear the hardware ID in the AMC.

The **Solution Manager** GUI allows the admin to perform a restore procedure. To perform a restore procedure, you must first perform a backup procedure.

To perform a restore:

1. In the **Solution Manager** GUI, click **Restore**.
2. To restore data from a solution export, click **Restore** and follow the prompts.

NOTE:

- The **Restore** operation will cause a small service outage as services are restarted. Also, restoring an older backup may change settings for solution components if configuration changes were made after older backups. For example, if changes were made to MiVB configuration settings, a restore of a backup prior to the changes will revert the settings.
- Do not restore a database from a virtually installed MiVoice Business application (vMiVB) to a Container-based MiVoice Business (cMiVB) application. The cMiVB application requires a base configuration different from that of other installations.
  Mitel recommends using the Initial Configuration Wizard for setting the initial configuration for all components of the MiCloud Flex solution.

Viewing MiCloud Flex Solution Logs

The **Solution Manager** GUI allows you to download log files generated by the services running on the system. You must first collect the log files in an archive before it is available for download. This process may take some time to complete. Once you start to collect logs, you can leave this page and return to it later to download the log archive.

NOTE:

- As log collection is a time consuming process, it is recommended to download the logs during after-hours.
- This page retrieves logs previously stored by the solution. As logs are stored on an hourly basis, the latest logs may not be available immediately.

To collect and download logs:

1. In the **Solution Manager** GUI, click **Log Files**.
2. In the **Log Files** page, under **Date Range**, select the date range. The available options are **Today**, **Yesterday**, **Last 2 Days** and **Custom Range**. For **Custom Range**, select the start and end date. The calendar will not allow the end date to go beyond the current date. The calendar will not allow user to select more than two days.
3. Click **Apply**.
4. Click **Collect Logs**.

   NOTE: After log collection completes, the **Log Files** page displays information on the log archive file that is available for download.
5. Click **Download**.

NOTE: The system keeps only one log archive at a time. If you perform another **Collect Logs** operation, the new log archive will replace the previous one. The log archive stored in boot disk space is lost if the manager pod restarts or if the user restarts the pod via the **Solution Info** page. If the user requires the log archive, the user will need to perform the **Collect Logs** action again to get the logs.

NOTE: For MiCollab, you must collect the logs from the MiCollab GUI. For more information on collecting logs on MiCollab, see the MiCollab Server Manager Online Help > Configuration > MiCollab Settings > Collect Logs section.

Upgrading MiCloud Flex Solution

Guidelines for Upgrading

Use the below recommended guidelines before you perform an upgrade procedure:

1. Ensure that your solution is resilient. The deployment engineer must define resiliency support within the MIVB call control servers. The deployment engineer must also program SIP Trunking resiliency within the MBG servers.
2. From the MPA portal and the K8s Partner device, upgrade or schedule an upgrade of the UCCS-EXT bundle for the selected customer(s).
3. From the MPA portal and the K8s Partner device, upgrade or schedule an upgrade of the UCCS bundle for the selected customer(s).
4. Since MiCC-B and WFO servers are virtual Windows servers they must be manually upgraded.
5. The deployment engineer must upgrade the MiVB console(s) that have been installed within the customer site(s).
6. The deployment engineer must upgrade the remote clients/end points as necessary.

Upgrading MiCloud Flex Solution using MPA Portal

IMPORTANT: To perform an upgrade procedure you need the K8s Partner device. This device will be added and configured in advance by your service provider. Do not remove or make changes to this device without assistance from your service provider.

To upgrade the MiCloud Flex solution using the MPA portal:

1. Log in to the MPA portal.
2. Access the dashboard for the K8s Partner device.
3. Click **MiCloud Flex Upgrade Tool** > **System Tools** > **K8s Upgrade Tool**.

   IMPORTANT: The **K8s Upgrade Tool** is available only if the K8s Partner device is added and configured in advance by your service provider.
4. When all application information is collected from the **K8s Upgrade Tool**, select the application you want to upgrade.

5. From the **Available Upgrades** table select the K8s Cluster(s) to upgrade with the selected application, then select **Upgrade Selected**. All of the applicable devices associated with the selected clusters are upgraded.
6. On the **Upgrade Application** dialog, set the following parameters:
   - Upgrade To - Select the application version to upgrade to.
   - Date and Time - Set the day and time for the upgrade to run.
   - Click **Schedule**.
7. From the K8s Partner Upgrade Tool, **Scheduled**, **Recent**, and **Installed** tabs you can view upgrades that are scheduled to run, the status of upgrades that have recently run, and the installed application versions.

   IMPORTANT: During the upgrade process, the solution will complete a backup, upgrade the deployed solution, and restore the entire solution. This will be a disruptive process as services are upgraded and restored.

Upgrading and Downgrading Plans

MiCloud Flex has different plans (profile) options, so you can subscribe to the features that are right for your business. Mitel gives you the flexibility to mix and match service levels, allowing you to easily adapt to changing or growing business demands. The available MiCloud Flex plans are:

- UCC Entry User for Enterprise (V4.0)
- UCC Premium User for Enterprise (V4.0)
- UCC Standard User for Enterprise (V4.0)

  NOTE: For more information about the features supported with each plan, see the MiCloud Flex General Information Guide.

Upgrading Plans

To upgrade from UCC Entry User for Enterprise (V4.0) to UCC Standard User for Enterprise (V4.0), do the following:

1. Click the **MiCollab** link from the **Solution Manager** GUI.
2. Navigate to **Applications > Users and Services**.
3. In the **Users and Services** page, do the following:
   a. Click the **Users** tab.
      i. Locate an existing user which needs to be upgraded using search.
      ii. Select the user and click **Edit**.
      iii. From the **UCC Bundle** drop-down list, select **UCC Standard User for Enterprise (V4.0)**.
      iv. Click **Save**.
   b. Click the **MiCollab Client** tab.
      i. From the **Feature Profile** drop-down list select **UCC (4.0) Standard**.
      ii. Click **Save**.
   c. Click the **Phones** tab.

i. Click **Add New Phone** to add a phone to the new plan.
ii. In the **Number** field, enter the phone number.
iii. From the **Device Type** drop-down list, select **UC Endpoint**.
iv. Click **Save**.

4. Click the **MiVoice Business** link from the **Solution Manager** GUI.
5. Navigate to **Users and Devices > Group Programming > Multi-device User Groups**.
6. Click **Add**.
7. In the **Value to Add** text box of the **Multi-device User Group** field, enter the phone number created in Step *3 c*.
8. Click **Save**.
9. Click the **MiCollab** link from the **Solution Manager** GUI.
10. Navigate to **MiCollab Client Services > Configure MiCollab Client Services**.
11. Click the **PBX Nodes** tab.
12. Under **PBX nodes**, select the required PBX and click **Synchronize**.
13. Access **Solution Manager** GUI.
14. Click **AMC Sync Status**.
15. In the **AMC Sync Status** page, click **Sync**.

Downgrading Plans

To downgrade from UCC Standard User for Enterprise (V4.0) to UCC Entry User for Enterprise (V4.0), do the following:

1. Access **AMC** and remove UCC Standard User for Enterprise (V4.0) and add UCC Entry User for Enterprise (V4.0).
2. Click the **MiCollab** link from the **Solution Manager** GUI.
3. Navigate to **Applications > Users and Services**.
4. Click the **MiCollab Client** tab.
5. From the **Feature Profile** drop-down list select **Default Feature Profile**.
6. Click **Save**.
7. From the **Solution Manager** GUI, click **AMC Sync Status**.
8. In the **AMC Sync Status** page, click **Sync**.
9. Click the **MiCollab** link from the **Solution Manager** GUI.
10. Navigate to **Applications > Users and Services**.
11. In the **Users and Services** page, do the following:
    a. Click the **Users** tab.
        i. Locate an existing user which needs to be downgraded using search.

ii. Select the user and click **Edit**.
iii. From the **UCC Bundle** drop-down list, select **UCC Entry User for Enterprise (V4.0)**.
iv. Click **Save**.

b. Click the **MiCollab Client** tab.
i. Under the **Feature Profile**, select **UCC (4.0) Entry**.
ii. Click **Save**.

NOTE: By performing a downgrade procedure, AWC, Teleworker and IP user licenses will no longer be available.

Troubleshooting MiCloud Flex Issues

This chapter contains the following sections:

Solution Manager back up failed on MiVB

When the solution is deployed for the first time and you want to perform a backup procedure on MiVB using Solution Manager, you must reboot MiVB.

To reboot MiVB, do the following:

1. Log into **Solution Manager** GUI.
2. From the left menu, click **AMC Sync Status**.
3. In the **AMC Sync Status** page, verify that the MiVoice Business has successfully synced with the AMC.

   If the MiVoice Business is not synced, clear the hardware ID from the AMC website and click the Sync button.
4. From the Solution Manager home page, open **MiVoice Business** application.
5. Log into the MiVoice Business.
6. From the left menu, click **Maintenance and Diagnostics**.
7. Click **Maintenance Commands**.
8. In the Command field, type `reset system` to restart MiVB.

NOTE: The Solution Manager restore does not require a MiVB reboot.

MiCollab PC Client failing to connect to Remote Gateway

If the MiCollab PC Client fails to connect to a remote gateway, you must create MiCollab Client Deployment Profiles for each device's resilient MiVB pair and add DNS SRV records for each pair to the on-premise DNS server. For more information on how to add or modify MiCollab Client Deployment Profile, see MiCollab Client Deployment Web Help > Deployment Profiles > Add or Modify a Profile page available on Document Center. For information on DNS, see the MiCloud Flex Solution Engineering Guidelines document available on Document Center.

Teleworker Issues

The table below lists some of the common teleworker troubleshooting scenarios:

Symptom	Probable Cause	Corrective Action
Teleworker phones cannot connect to the PBX	The teleworker phone is not configured properly.	Fix the issue listed in the probable cause column, and do the following: 1. Power cycle the phone. 2. As it starts up hold down the red button. 3. Confirm the sets display the correct FQDN of the MBG.
One-way or no-way audio on Connected phones	The router at the customer premises is blocking network traffic.	Run the Teleworker Network Analyzer (TNA) tool

Installation / Upgrade Issues

The table below lists some of the common installation or upgrade troubleshooting scenarios:

Symptom	Probable Cause	Corrective Action
Unable to connect to MiCloud Flex Solution Manager from Mitel Performance Analytics (MPA)	MPA probe is not included in MiCloud Flex Solution Manager	For more information on MPA integration, see *MPA Integration with MiCloud Flex*. To create the MPA probe, see *Creating MPA URL in MPA portal*.
MiCloud Flex is unable to get a valid certificate after an upgrade from Mitel Performance Analytics (MPA) in implementations that use custom FQDN. Applications such as Web RTC and MiCollab that require a valid certificate will not work after the upgrade.	The Let's Encrypt CA cannot validate the custom domains because the DNS server is not resolving the FQDN to a correct IP address. Logs from Certs-Manager shows failed authorization procedure.	Ensure that the user adds the correct FQDN and IP address in the public DNS. If this does not resolve the problem: 1. In the left pane of Solution Manager GUI, click **Solution Info**. 2. In the right pane, scroll down to **Solution Manager** section and click **Restart** beside **manager**.

Operational Issues

The table below lists some of the common operational troubleshooting scenarios:

Symptom	Probable Cause	Corrective Action
Mitel Business Analytics (Tollring) stopped reporting on new calls when failed over to remote gateway	A update is made with respect to the user profile in the Tollring portal	Tollring probe needs to be restarted to download the latest updated user profile and connect to configured PBXs. To restart the tollring probe: 1. In the left pane of Solution Manager GUI, click **Solution Info**. 2. In the right pane, scroll down to **Miscellaneous** section and click **Restart** beside **tollring-probe**.

Documentation Addendum

The chapter is designed to be used in conjunction with the MiCloud Flex Documentation application documentation. For a complete list of application documents, see *Appendix*. Everything in those guides applies to the individual applications, except as noted in this addendum.

Each section in the addendum corresponds to a product documentation set. New features are described in topics in the applicable guide. Information that has changed in the product documentation is due to the change in the feature set that is supported on MiCloud Flex.

Note that if a guide has no corresponding section in the addendum, it means that there is no new or changed content, and the documentation available is current.

This chapter contains the following sections:

Addendum MiCollab

The following are the changes for MiCollab in the MiCloud Flex solution:

- The Nupoint Messaging feature is not available in the MiCollab Server.
- Speech Auto Attendant feature is not available in the MiCollab Server.
- The MiVoice Border Gateway application is not available.

Addendum Mitel Border Gateway

The following are the changes for Mitel Border Gateway in the MiCloud Flex solution:

- There are no separate admin logins to access Mitel Border Gateway.
- There are no navigation menus in the Mitel Border Gateway GUI.
- The Remote Proxy Services Configuration tab is not available in the Mitel Border Gateway GUI.
- The following items on the Dashboard of the Mitel Border Gateway GUI are not available:
  - The ability start/stop MBG service. Mitel Border Gateway services cannot be stopped within a MiCloud Flex solution.
  - The ability to view system metrics. Application metrics are still available within Mitel Border Gateway.
- Network Profiles and Port Ranges are pre-set at deployment and cannot be edited.

Addendum MiCCB

The following are the deployment limitations for MiContact Center Business:

- You must download the Client Component Pack to access MiContact Center Business applications. Optionally, you can configure Port Forwarding in Mitel Performance Analytics (MPA) to directly access these applications from the VM.
- Contact Center Messenger works only if the MiCC VM and the Google Cloud are set to the same time-zone.
- Mitel's MiCloud Flex Contact Center Workforce Scheduling application is not supported on MiCloud Flex when MiCloud Flex is deployed on Google Cloud.
- Mitel's Workforce Management (Teleopti) solution is supported for use with MiCloud Flex Contact Center when MiCloud Flex is deployed on Google Cloud; however, real-time data feed is not currently supported. All scheduling and adherence data is sent in 15-minute intervals from the Teleopti Work-force Management Connector. This limitation is restricted to Teleopti's real-time alarming engine. Real-time data feed is expected to become available in a subsequent release of MiCloud Flex.

Addendum MiVB

The following are the changes for MiVoice Business in the MiCloud Flex solution:

- Server Manager and Server Console are not supported.
- Only the Embedded Voice Mail system is supported.
- The Nupoint Messaging feature is not available.

Addendum Endpoints

The following are the changes for Endpoints in the MiCloud Flex solution:

- FQDN is used instead of IP Address for set registration (MBG or Static Call Server).
- You can connect devices in two modes:
  a. Office User – Devices that are connected to the cloud platform from an office. These devices require a DHCP server with specific options configured to be able to connect to the call server and register automatically. Customers must set up the DHCP server on a Windows server and configure the DHCP Option 125 or 43. See *Configuring DHCP Option 125 or 43*.
  b. Home users – Devices that are connected remotely (also known as Teleworker). These devices require the following:
  - MBG configured with FQDN of the call server. FQDN for each MiCloud Flex component is provided in the welcome email.
  - FQDN of the call server manually entered in the set to connect to the call server. FQDN for each MiCloud Flex component is provided in the welcome email.
- You can register customer end-devices through the RCS (Redirection and Configuration Service) so that phones plugged in would re-direct to the correct MBG and register. If RCS service is required, an account request must be sent to rcsadmin@mitel.com. For more information on RCS, see the Redi-rection and Configuration Service (RCS) User Guide.

Support for 5300 Phones

For a 5300 series phone to function in MiCloud Flex, it must use FQDN instead of static IP addresses. This support is available in FW version 6.5.0.28 and newer versions. The endpoints supported are: 5304, 5312, 5324, 5320, 5320e, 5330e, 5340e, 5360.

NOTE: The endpoints not supported are: 5302, 5330 (10/100Mbps) and 5340 (10/100Mbps).

If the 5300 series phone is not already at this supported version, upgrade the phone to FW version 6.5.0.28 or newer using one of the following methods:

1. Obtain the firmware from the hosted MBG in MiCloud Flex. To reach this MBG, manually configure the phone to register with that MBG, using the external IP address of that MBG.
   - If all 5300 series phones at a site are to be registered with MiCloud Flex, place the supported FW version or newer on the tftp site where the phone would currently get its firmware. Reboot the phones.
   - Update RCS to redirect the phone to the hosted MBG. Reset the phone to factory defaults to contact RCS.
2. After the firmware is downloaded, reboot the phone.
3. Update any DHCP options and RCS configurations to use FQDN instead of IP addresses.

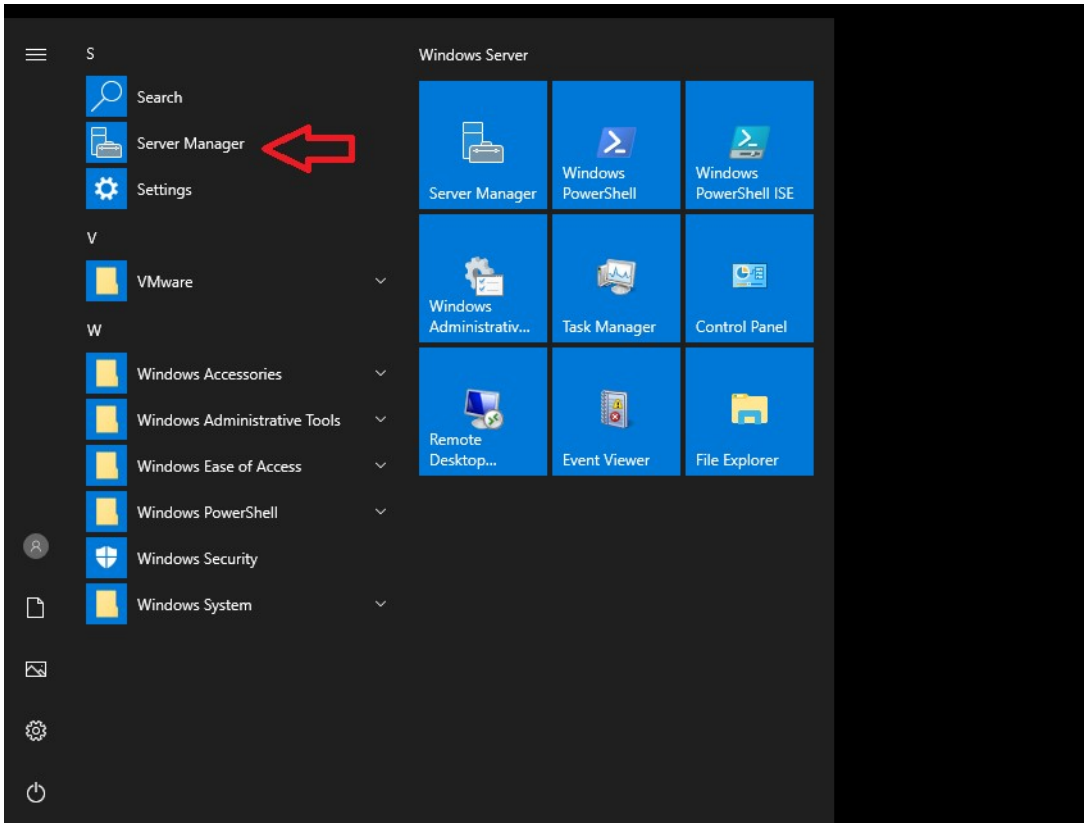
   NOTE: See the **DHCP Option Reclassification** section of the Mitel IP Sets Engineering Guidelines for further information on programming DHCP options.
4. Configure the phone to use FQDN instead of an IP address to connect to the hosted MBG in the MiCloud Flex solution using the following manual method:
   a. Enter Debug Mode (Up/Down arrow, release Down Arrow, enter 234 (cfg)
   b. Select ‘Network Parameters’ (*)
   c. Bypass ‘View Current Values’ (#)
   d. Bypass ‘Static QoS’ (#)
   e. Select ‘Static FQDN’ (*)
   f. Bypass ‘View FQDN Params’ (#)
   g. Select ‘Modify FQDN Params’ (*)
   h. Select ‘Modify Static FQDN’ (use Scroll – Down arrow)
   i. Enter FQDN of MBG using dialpad
   j. Press down-arrow to complete
   k. Select Save and reboot to complete the task. Phone will reboot and startup with FQDN parameters and register to MBG

      NOTE: See the **Fully Qualified Domain Name Support for 5300 and 6900 Series IP Phones** section in the Mitel IP Sets Engineering Guidelines for further information on FQDN support.

Configuring DHCP Option 125 or 43

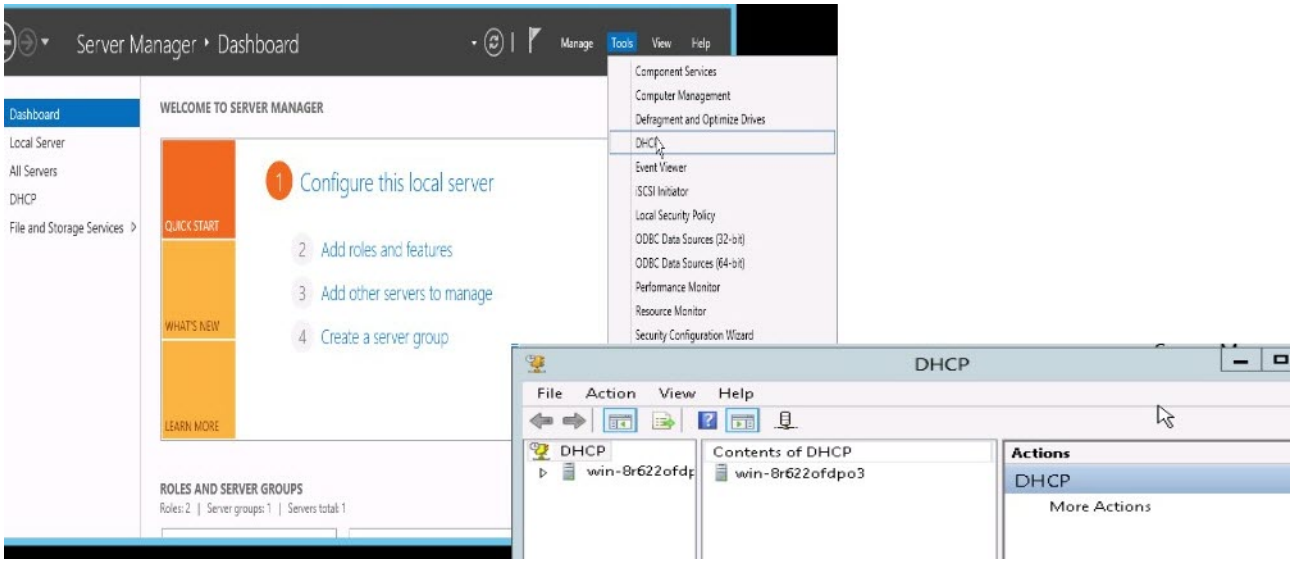
To create Options 125/43 on a Windows 2019 DHCP server:

1. Start **Server Manager**.



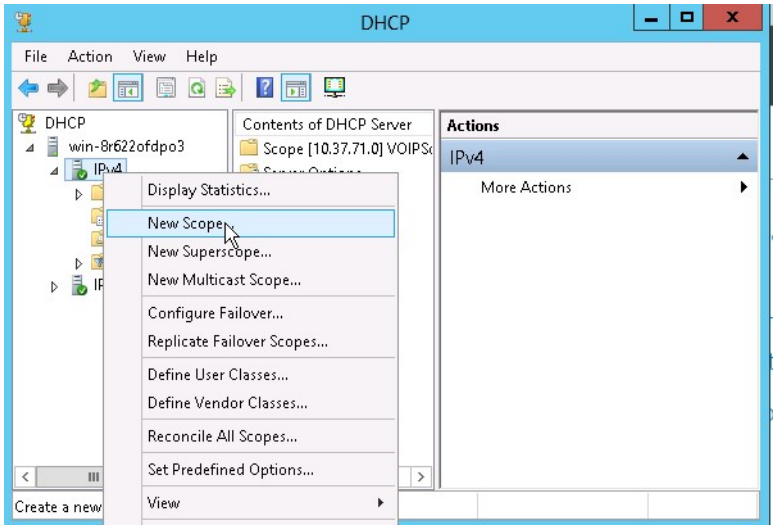
2. On the **Tools** menu, click **DHCP**.

   The DHCP window is displayed.



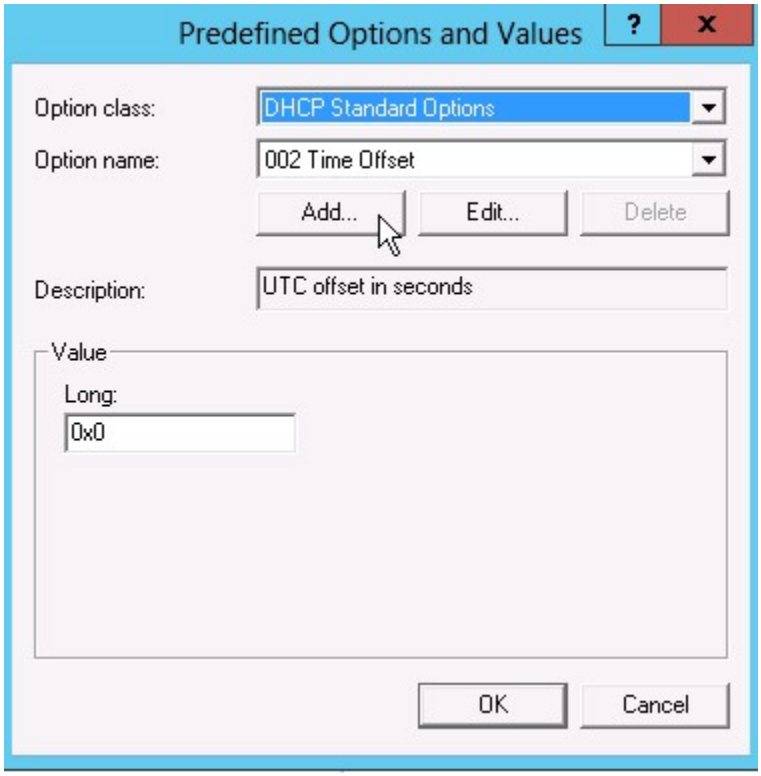
3. In the left pane, navigate to **DHCP > server name> IPv4**.
4. Right-click **IPv4**, and click **New Scope**.

   The New Scope Wizard window is displayed.



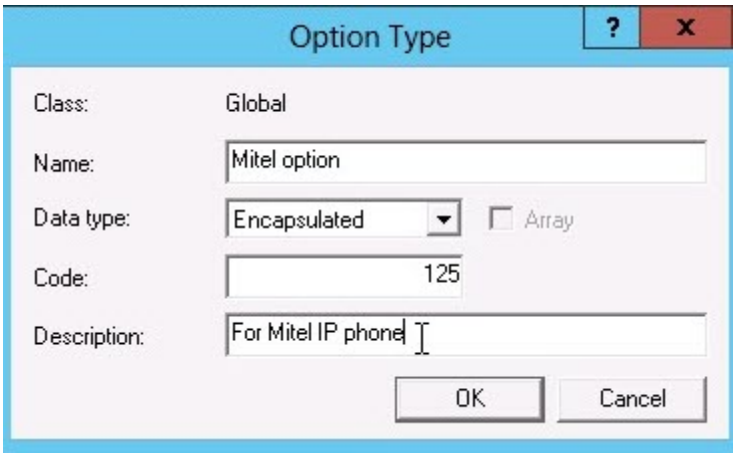
5. Follow the wizard to enter the following details (skip rest of the wizard windows that are not listed below by clicking **Next**):
   a. **Scope Name** (for example, VOIPScope)
   b. **IP Address Range**
   c. **Configure DHCP Options**
   d. Select **Yes, I want to configure these options now**.
   e. **Router (Default Gateway)**
   f. **Domain Name and DNS Servers (if applicable)**
   g. **Activate Scope**
   h. Select **No, I will activate this scope later.**
   i. Click **Finish**.
6. In the left pane, navigate to **DHCP > server name> IPv4**.
7. Right-click **IPv4**, and click **Set Predefined Options**.

   The Predefined Options and Values window is displayed.



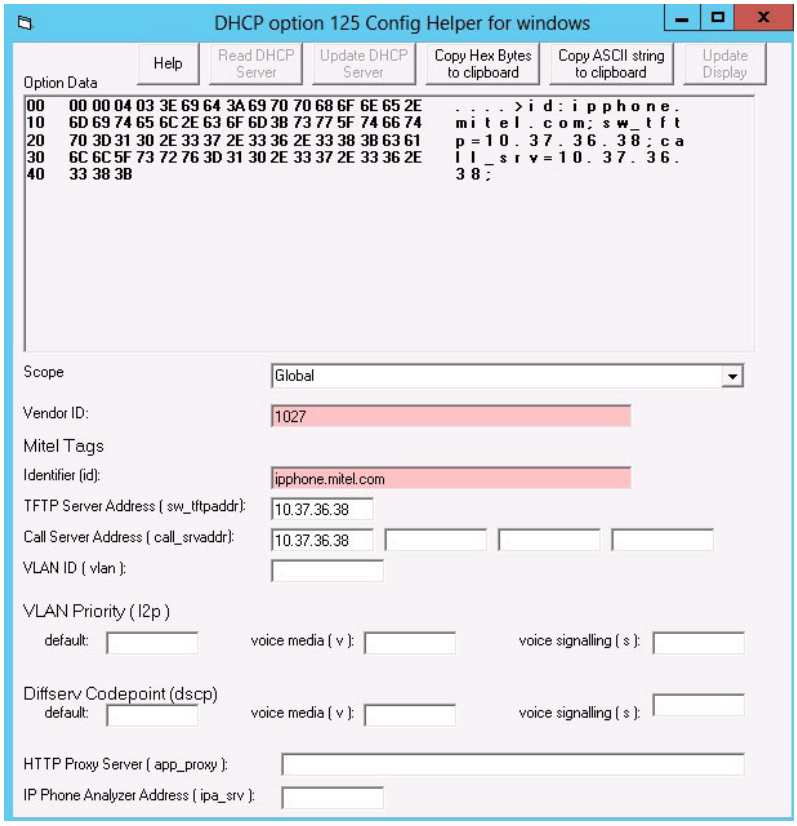
8. Click **Add**.

   The Option Type window is displayed.



9. Enter the following, and click **OK**.
   - **Name** - **Mitel option**
   - **Data type** - **Encapsulated**
   - **Code** - **125 or 43**
   - **Description** - **For Mitel phone**
10. In the Windows 2019 server, start the **DHCP Config Helper** application.

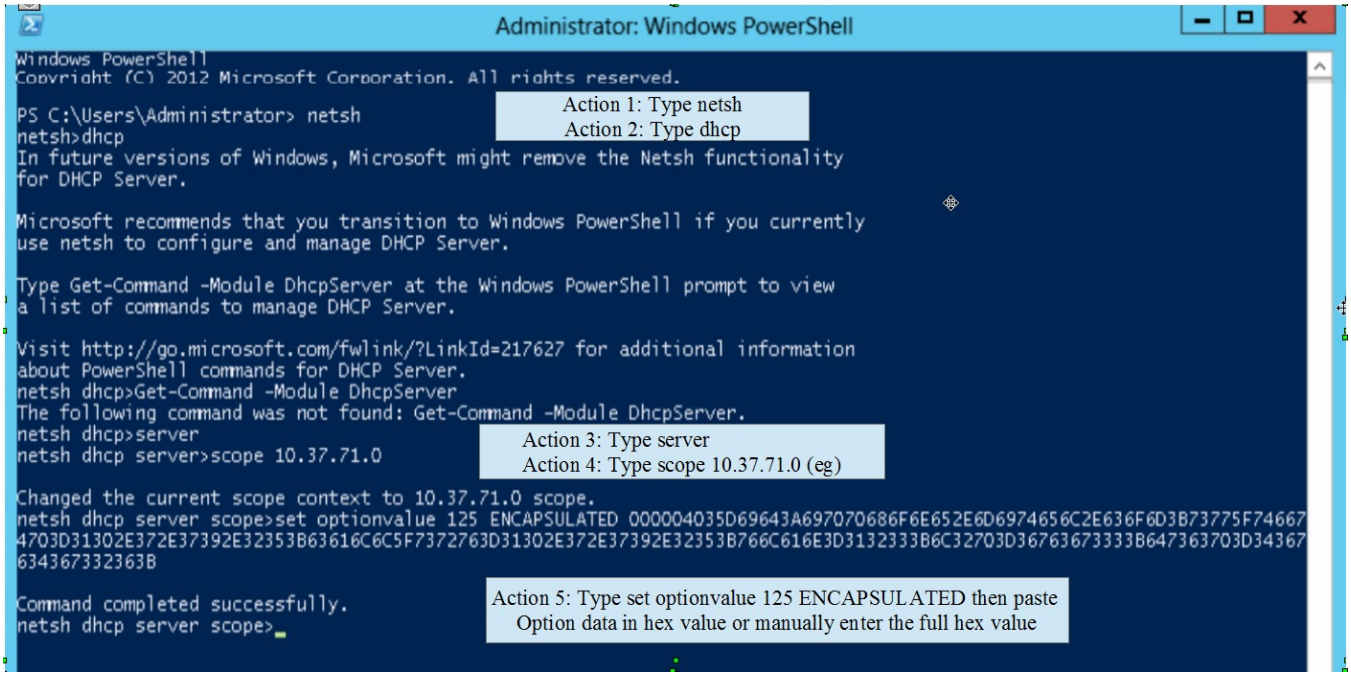
NOTE: You can download the **DHCP Config Helper** application from **Software Download Center** (under the **MiVoice Business** category).



11. Enter the following:
    - **TFTP Server Address (sw_tftpaddr)** - FQDN of the TFTP server provided in the welcome e-mail.
    - **Call Server Address (call_srvaddr)** - FQDN of the call server provided in the welcome e-mail.
    - **VLAN ID (vlan)** (if applicable)
    - **Diffserv Codepoint (dscp)** (if applicable)
12. Click **Update Display**.

NOTE: The **Update Display** button is not available until you specify the mandatory fields.

13. Click **Copy Hex Bytes to clipboard**, and past the Hex Bytes to a txt file using the Notepad application.
14. In the Windows 2019 server, start **Windows PowerShell**.



15. Enter the following command:

    a. `netsh`
    b. `dhcp`
    c. `server`
    d. `scope <fqdn/ip address of the scope>`
    e. `set optionvalue 125 ENCAPSULATED <paste the Hex Bytes from the txt file)`

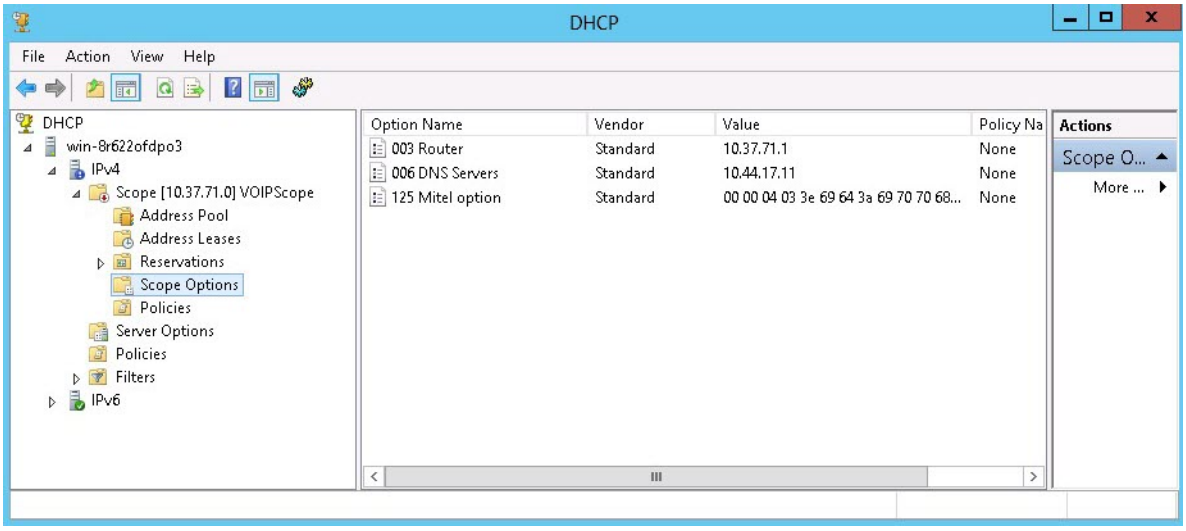
NOTE: To set option 43, enter the command `set optionvalue 43 ENCAPSULATED <paste the Hex Bytes from the txt file)`

16. In the DHCP window, in the left pane, navigate to **DHCP > server name > IPv4 > Scope**.

17. Click **Scope Options**.

    The DHCP Option 125 or 43 is displayed on the right side of the pane.

    NOTE: If the DHCP Option is not displayed, then on the **Action** menu, click **Refresh**.



18. In the DHCP window, in the left pane, navigate to **DHCP > server name > IPv4**.
19. Right-click **Scope** and click **Activate**.

Appendix

This chapter contains the following sections:

MiCollab Documentation

Document Name	Description
MiCollab Client Administrator Online Help	Provides a high-level overview of the provisioning process with links to task-related instructions. The task-related instructions provide detailed descriptions for fields and options.
MiCollab Client Deployment Web Help	Provides MiCollab Client Deployment service that is used to configure the deployment parameters, change the default deployment profile, or to run the diagnostics.
MiCollab Client Administrator Guide	Includes PBX configuration information, Unified Communications specifications and hardware configuration information, and configuration information for integrated applications.
MiCollab Client Engineering Guidelines	Provides system requirements, configuration information, network diagrams, virtualization information, performance recommendations, system capacities.
MiCollab Server Manager Web Help MAC	Provides configuration, administration, and maintenance procedures for the MiCollab server.
MiCollab Users and Services Provisioning USP	Provides instructions on how to manage user data and assign or remove user services, such as MiVoice Border Gateway or Teleworker.
MSL Server Manager MAS	Highlights MiCollab Server-level features on MSL.

Document Name	Description
MiCollab Engineering Guidelines	Highlights specific areas of the product that you must consider before installation. Use them to plan site installations.
MiCollab General Information Guide for MiVB and MiVO 250	Provides a high-level overview of the MiCollab product.
MiCollab ACD SIP Softphone Agents Integration Guide	This document describes how to provision and setup the ACD SIP Softphone in MiCollab, MiVB, and MiCC. It includes procedures on how to setup a new agent on MiCC, MiCollab, MiVB, and MBG for the SIP ACD softphone to function.

MiContact Center Business Documentation

Document Name	Description
MiContact Center Business General Information Guide	Provides detailed information on how MiContact Center Business and the ACD system interact with the MiVoice Business platform
MiContact Center Business Installation and Administration Guide	Provides instructions for deploying and configuring MiContact Center Business, remote site deployments, and all IVR Routing configuration
MiVoice Analytics Installation Guide	Provides instructions for deploying and configuring Call Accounting and MiVoice Analytics.
MiVoice Analytics Reports Guide	Provides descriptions of all the report types available with MiVoice Analytics and how to generate, view, and share reports.
MiVoice Analytics User Guide	Provides information on general business and call costing concepts and describes Business Reporter and Call Accounting features and configuration
MiContact Center Business and MiVoice Analytics System Engineering Guide	Provides information on hardware and software requirements, virtualization, data storage, licensing, and third-party integrations.
MiContact Center Business Reports Guide	Provides descriptions of all the report types available with MiContact Center Business' Contact Center Starter Pack and how to generate, view, and share reports

Document Name	Description
MiContact Center Business-MiVoice Business Deployment Guide	Provides information regarding how to scale up from a simple solution for a deployment that can grow as the contact center grows. High-level requirements, specifications, networking considerations, best practices, and other useful references for planning the deployment of large-scale, complex contact centers are discussed.
MiContact Center Business BluePrint Guide	Provides an overview of MiContact Center use cases, topologies, technical considerations, best practices, on-premises, cloud, and hybrid deployment models.
MiContact Center – Workgroup Reports Guide	Provides descriptions of all the report types available with MiContact Center Business' Workgroup Starter Pack and how to generate, view, and share reports
MiContact Center User Guide	Provides information on the basics of contact center management and descriptions for use of all agent and supervisor desktop/Web applications within the MiContact Center Business solution. This guide focuses specifically on voice media.
Multimedia Contact Center Installation and Deployment Guide	Provides all information on deploying and configuring sites with email, chat, and SMS media, including end-user instructions for supervisor and agents using the multimedia Web applications.

Mitel Performance Analytics

Document Name	Description
Mitel Performance Analytics Engineering Guidelines	Guidelines and requirements to help the customer plan for MPA installations.
Mitel Performance Analytics Installation and Maintenance Guide	Provides information required to install and configure a Mitel Performance Analytics Probe.
Mitel Performance Analytics Probe Installation and Configuration Guide	Guide to assist users with the installation and maintenance of MPA
Mitel Performance Analytics Quick Start Guide - Cloud Users	Guide to get started on MPA deployments where the software is installed on the cloud.

Document Name	Description
Mitel Performance Analytics System Description	Provides information required to administer and use an MPA monitoring system

MiVoice Business Documentation

Document Name	Description
General Information Guide	Provides an overview of the MiVoice Business c all-processing software and its host hardware platforms.
Engineering Guidelines	Highlight specific areas of the product that you must consider before installation. Use them to plan site installations.
Security Guidelines	Provides information for ensuring the secure deployment and secure operation of the MiVoice Business system.
Resiliency Guidelines	A comprehensive overview of the Mitel® Resiliency solution and provides customers the tools to understand, plan, and implement a resilient network.
Troubleshooting Guide	Lists problem symptoms, possible causes, and corrective actions for MiVoice Business installation and configuration issues.
Clustering Design and Implementation Guide	Provides design considerations and configuration guidelines for networking MiVoice Business systems with emphasis on setting up a cluster.
Voice Quality Troubleshooting Guide	Provides information on how to troubleshoot voice quality issues on the Mitel MiVoice Business platform and its supported applications.
System Administration Online Help	The primary source of information on configuring and maintaining the MiVoice Business software.

MiVoice Border Gateway Documentation

Document Name	Description
MBG Customer GDPR Compliance Initiatives	Discusses security processes, security controls and features available on MiVoice Border Gateway (MBG) to comply with GDPR.
MiVoice Border Gateway Online Help	Provides instructions to deploy multiple services in a variety of network configurations securely.
MBG Remote Phone Guide	Provides procedures to configure your Mitel or non-Mitel IP or SIP phone to work remotely using MBG.

Endpoints Documentation

Document Name	Description
6900 IP Phones	https://www.mitel.com/document-center/devices-and-accessories/ip-phones/6900-series/6900-ip-phones
MiVoice 6900 Series IP Phones Administrator Guide	This guide explains how to use the administrator features of the Mitel MiVoice 6900 Series (6920, 6930, and 6940) IP Phones that can be accessed through the IP Phones' advanced Settings menu and Web UI.
Mitel 6900 Series IP Phones Administrator Guide	This guide explains how to use the administrator features of the Mitel 6970 IP Conference Phone that can be accessed through the IP Phones' advanced Settings menu and Web UI.
MiVoice 6905 IP Phone User Guide	This guide explains how to use the basic features of your Mitel MiVoice 6905 IP Phone.
MiVoice 6910 IP Phone User Guide	This guide explains how to use the basic features of your Mitel MiVoice 6910 IP Phone.
MiVoice 6920 IP Phone User Guide	This guide explains how to use the basic features of your Mitel MiVoice 6920 IP Phone.
MiVoice 6930 IP Phone User Guide	This guide explains how to use the basic features of your Mitel MiVoice 6930 IP Phone.
MiVoice 6940 IP Phone User Guide	This guide explains how to use the basic features of your Mitel MiVoice 6940 IP Phone.

Document Name	Description
MiVoice 6905 IP Phone Quick Reference Guide	This guide contains an overview of the User Interface (UI), call handling instructions and information on other important features for Mitel MiVoice 6905 IP Phone.
MiVoice 6910 IP Phone Quick Reference Guide	This guide contains an overview of the User Interface (UI), call handling instructions and information on other important features for Mitel MiVoice 6910 IP Phone.
MiVoice 6920 IP Phone Quick Reference Guide	This guide contains an overview of the User Interface (UI), call handling instructions and information on other important features for Mitel MiVoice 6920 IP Phone.
MiVoice 6930 IP Phone Quick Reference Guide	This guide contains an overview of the User Interface (UI), call handling instructions and information on other important features for Mitel MiVoice 6930 IP Phone.
MiVoice 6940 IP Phone Quick Reference Guide	This guide contains an overview of the User Interface (UI), call handling instructions and information on other important features for Mitel MiVoice 6940 IP Phone.
MiVoice 6905 IP Phone Installation Guide	This guide contains installation and set-up instructions for Mitel MiVoice 6905 IP Phone along with general features and functions.
MiVoice 6910 IP Phone Installation Guide	This guide contains installation and set-up instructions for Mitel MiVoice 6910 IP Phone along with general features and functions.
MiVoice 6920 IP Phone Installation Guide	This guide contains installation and set-up instructions for Mitel MiVoice 6920 IP Phone along with general features and functions.
MiVoice 6930 IP Phone Installation Guide	This guide contains installation and set-up instructions for Mitel MiVoice 6930 IP Phone along with general features and functions.
MiVoice 6940 IP Phone Installation Guide	This guide contains installation and set-up instructions for Mitel MiVoice 6940 IP Phone along with general features and functions.
Mitel 6970 IP Conference Phone Installation Guide	This guide contains installation and set-up instructions for Mitel MiVoice 6970 IP Conference phone along with general features and functions.

Document Name	Description
XML API for Mitel 69xx MiNet Phones Firmware 1.5.0 Development Guide	This document details the XML objects supported by the Mitel 69xx phones using firmware version 1.5.0 and how to implement them.
6900 Accessories	https://www.mitel.com/document-center/devices-and-accessories/ip-phones/6900-series/6900-accessories
Mitel S720 Bluetooth Speakerphone QRG	This guide contains instructions to connect and use the Mitel S720 Bluetooth Speakerphone with your Mitel MiVoice 6930 and 6940 IP Phones.
Cordless Bluetooth Handset Install Guide	This guide contains installation and set-up instructions for pairing the Mitel Cordless Bluetooth Handset to your Mitel MiVoice 6800 Series, 6930 and 6940 IP Phones.
M695 Programmable Key Module Install Guide	This guide contains installation and set-up instructions for connecting the M695 PKM to your Mitel MiVoice 6900 Series IP Phones.
Mitel IP Conference Phone	https://www.mitel.com/document-center/devices-and-accessories/conference-phones/6970-ip-conference-phone
Mitel 6970 IP Conference Phone Quick Reference Guide	This guide contains an overview of the User Interface (UI), call handling instructions and information on other important features for Mitel MiVoice 6970 IP Conference phone.
Mitel 6970 IP Conference Phone User Guide	This guide explains how to use the basic features of your Mitel MiVoice 6970 IP Conference phone.
Networking Equipment	https://www.mitel.com/document-center/devices-and-accessories/networking-equipment/mitel-wireless-lan-adapter
Mitel WLAN Adapter documentation	This documentation explains how to configure, setup and use the Mitel WLAN Adapter in a wireless network.
General IP Phone Documentation	https://www.mitel.com/document-center/devices-and-accessories/ip-phones/general-ip-phone-documentation
Mitel IP Sets Engineering Guidelines	This document covers engineering guidelines for the 5000, 5200, 5300 and 6900 families of IP Phones as well as a number of specialized phones and consoles.

Document Name	Description
Network Engineering for IP Telephony	This document covers networking for the 5000, 5200, 5300 and 6900 families of IP Phones as well as a number of specialized phones and consoles.
Wireless Solutions and Handsets	https://www.mitel.com/document-center/devices-and-accessories/wireless-solutions-and-handsets/sip-dect-multi-cellular-solution/sip-dect
SIP-DECT documentation	This documentation provides information on installation, configuration, administration, and maintenance of the SIP-DECT solution.
112 DECT documentation	This documentation provides information on installation and configuration of 112-DECT phone with RFP 12 Single Cell Base Station.