# MiVoice Business Multi-Instance

## INSTALLATION AND ADMINISTRATION GUIDE

Release 2.0 SP1

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®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.



### Trademarks



MiVoice Business Multi-Instance Installation and Administration Guide
Release 2.0 SP1 - March 2021

## Chapter 1: Introduction



## Chapter 2: Installation

# Chapter 1

## Introduction

# About this Guide

The MiVoice Business Multi-Instance Installation and Administration Guide is intended for Distributors and Resellers who are installing and configuring MiVoice Business Multi-Instance as a solution for hosted and non-hosted enterprise applications.

This guide describes the installation, administration, maintenance, and troubleshooting of the MiVoice Business Multi-Instance software solution.

# What's New in Release 2.0 SP1?

The following features and functionality have been introduced in this release:

- Support for Mitel Standard Linux (MSL) 10.3.
- Golden database (*.tar*) file and Configuration Wizard (*.zip*) file must be manually backed up during the MSL upgrade and restored using the upload file capability on the **Bulk** tab after a successful upgrade.

# What's New in Release 2.0?

The following features and functionality have been introduced in this release:

- Golden Database
  - MiVoice Business Multi-instance supports the use of a "golden database", an initially created database that can subsequently be distributed across all instances of the MiVoice Business software.
- Bulk ARID Import
  - When creating multiple Instances and selecting the option for entering their license ARIDs, it is now possible to enter a list of ARIDs that can be used for the Instances, as opposed to entering them one-by-one.
- More than 250 Instances
  - More than 250 instances of MiVoice Business can now be added in a MiVoice Business Multi-instance implementation.

# What's new in Release 1.2 SP2?

The following new features and functionality have been introduced in this release:

- Product Re-branding
  - The Multi Instance Communications Director (MICD) product name has been changed to MiVoice Business Multi-instance.
  - The Mitel Communications Director (MCD) product name has been changed to MiVoice Business.
  - These changes are reflected throughout this help system. The instances will be referred to as Instance, or where additional clarity is needed, MiVoice Business Instance.
- Mitel Standard Linux (MSL) Support

  - 64-bit variant of MSL 10.0 only, is supported with this release.
- Remote Fresh Install
  - Remote Fresh Install (RFI) blade will enable upgrades of MSL 9.3 and 9.4 based systems to MSL 10 without requiring a hard disk format. See the MiVoice Business Multi-instance Installation and Administration Guide and the Mitel Standard Linux Installation and Administration Guide for more details.

# What's new in Release 1.2?

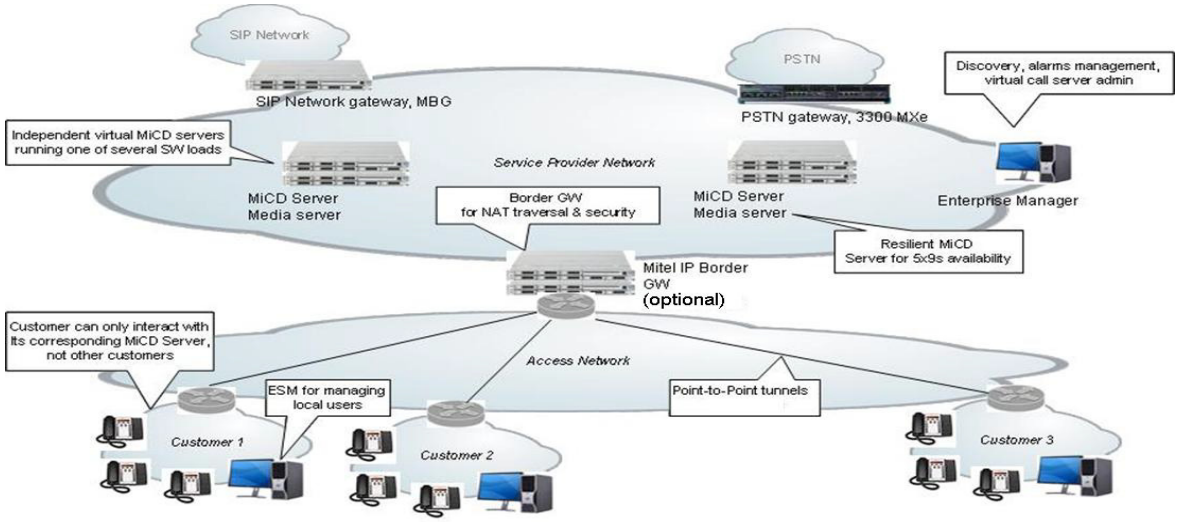
The following new features and functionality have been introduced in this release:

- Support for Virtual LANs (VLANs). In prior releases all MCD Instances were in a single subnet and a single trust domain. A Mitel Border Gateway (MBG) was needed to provide segregation between non-related MCD Instances. This release of MICD provides the option to enable full MCD network isolation with every instance on a Virtual LAN (VLAN).
- Support for software release MCD 5.0 SP1.
- Support for hex-core processors.

Chapter 3 provides additional details about configuring MICD for VLANs, and Appendix C for information regarding network access constraints and restrictions.

# About MiVoice Business Multi-Instance

MiVoice Business Multi-Instance is a Mitel Networks 3300 derivative product intended for either service provider or enterprise deployments. It works in combination with other Mitel portfolio elements to offer hosted unified communications functionality to tenanted end users, across a flexible range of network deployment topologies. The MiVoice Business Multi-Instance solution leverages the Mitel business communications portfolio by supporting the same lines of IP sets, and many applications that the Mitel Networks 3300 communications platform product line supports.



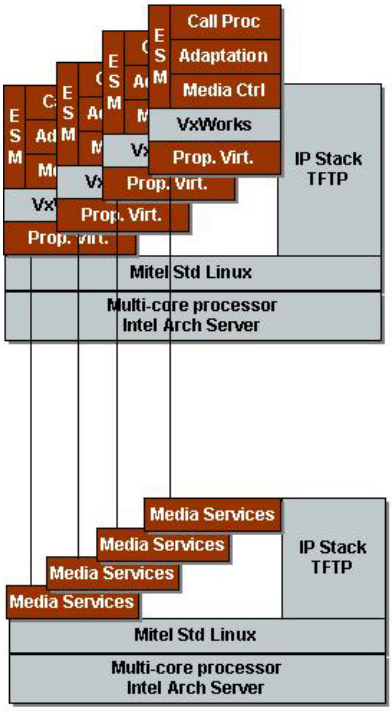

MiVoice Business Multi-Instance contains the following components:

- Mitel Standard Linux (MSL), the base operating system on which all other applications reside.
- MiVoice Business Multi-Instance Server, which contains the MiVoice Business instances.
- MiVoice Business Instances, the multiple instances of the PBX functionality containing the 3300 software. Each of the Customers shown in the diagram above has one MiVoice Business Instance.
- MICD Manager, the administrative interface for managing the MiVoice Business Instances.
- Media Server, which provides the media services for the MiVoice Business Instances. One media server is required for each MiVoice Business Instance.
- Media Server Manager, the administrative interface for managing the media servers for the MiVoice Business Instances.
- Mitel Border Gateway (MBG), an optional item if NAT traversal and security is required.

The MiVoice Business Multi-Instance solution comprises the following features:

- *Call Server at the core*
  The virtual call server functionality derived from the Mitel Networks 3300 call server in its appliance platform form factors (CX, CXi, MXe, MXe Server, AX), provides all call processing features for the full line of currently supported IP sets, Unified Communications applications and CTI interfaces, and SDK toolkits.

- *MiVoice Business Instances through virtualized call centers*
  MiVoice Business Instances, or the multiple virtual instances of the PBX functionality containing the 3300 software, is achieved using an application virtualization technique. This approach allows, for example, the centralization of a high touch application such as call control into a data centre environment, and Enterprise hosting of small and regional branch offices in conjunction with scaling that supports large headquarter sites.




- *Multiple release versions of software*
  The different virtualized call servers have the ability to run different release versions of the 3300 software. A software upgrade can be applied to only the tenant (instance) that requires the functionality lift or support issue, rather than upgrade the entire call server at large and exposing the entire customer population.
- *Optimized for data centre deployments*
  MiVoice Business Multi-Instance has been optimized for data centre deployments, by running virtually all elements of the solution on industry standard x86 servers running MSL. This includes call processing and media processing which has classically operated only on custom hardware. Servers are required for the:
  - MiVoice Business Multi-Instance
  - associated media server which is part of MiVoice Business Multi-Instance
  - Mitel Border Gateway (MBG), for the network topologies that require it
- *Flexible network deployments*
  MiVoice Business Multi-Instance has been designed in conjunction with other portfolio elements and standardized capabilities in IP routers to operate across a range of network deployments. This includes both managed networks with a homogeneous IP addressing plan, as well un-managed heterogeneous networks with tenant locations having overlapped IP addressing.

The MBG is the essential element for supporting heterogeneous network deployments, and is effectively a stateful firewall optimized for protocols used by Mitel products. It supports both near-end and far-end Network Address Translation (NAT) traversal for protocols used by Mitel products, and also performs media stream termination for heightened security, media adaptation, and voice quality.

- *Scaling*
  The MiVoice Business Multi-Instance call server application scales with the industry trend towards higher core counts in processor technology.
- *Management*
  Several management capabilities are featured in the MiVoice Business Multi-Instance solution, over and above embedded management capabilities in the 3300 appliance solution.
  - A customer self-management option is supported at the customer premises to permit simple configuration changes such as user moves/adds/changes. This is done by providing a restricted 3300 ESM interface at the customer premises, both in managed and un-managed IP network configurations.
  - Enterprise Manager is supported for virtual call server SNMP discovery and inventory, fault management, system management reach-through, moves/adds/changes, and voice quality reporting. In addition, a north-bound interface that supports these management capabilities is provided for integration to a Network Management System (NMS).
  - A separate network interface is provided for support of a secure administration plane, where particularly sensitive management capabilities are isolated. Provisioning, licensing, and management of virtual call servers is done through a software blade administration interface accessible only on the separate management plane.
- *High Availability*
  MiVoice Business Multi-Instance can be configured using resiliency to achieve 5x9s availability. IP sets are configured with a primary virtual call server on one physical server, and a secondary virtual call server on a different physical server, and fails over between them in the event of faults.
- *Security*
  MiVoice Business Multi-Instance supports security levels including 128 bit encryption for signaling and voice streaming interfaces, protection against Denial of Service attacks, minimization of open ports, and use of secure versions of protocols such as Secure RTP, Secure HTTP and Secure Shell.

  Using the MBG at the edge of the carrier network provides further protection for equipment on the carrier network behind a hardened stateful firewall. Using topology hiding through customer premise NAT, while providing NAT traversal techniques for required protocols, further enhances security of the carrier and customer premises network.

  The MBG has a separate network interface for connection to an administration plane, to ensure that particularly sensitive administration and management operations are unavailable on other operational interfaces.

  In addition, several measures are taken to ensure high security and isolation between tenants:
  - Each virtualized call server operates under a different "user account" within the Linux operating system, creating security and isolation at the base software level. One virtual call server can neither access the database, program store nor file system of another virtual call server through operating system protection mechanisms.

- A very high degree of separation and isolation can be achieved between Instances using Mitel's suggested deployment topology. Instances are unable to "see" other Instances on the network, with packets unroutable between Instance networks; there is network access only to the service provider's edge firewall for that Instance’s IP border gateway.

- *PSTN Connectivity*
  MiVoice Business Multi-Instance supports several PSTN connectivity options:
  - Can use a 3300 MXe appliance deployed as a PSTN gateway. It has advantages over 3rd party gateways in that it can be managed under the same management capabilities operating across the Mitel portfolio, and supports sophisticated ACD queuing capabilities not supported by 3rd party gateways.
  - Can use AudioCodes Mediant SIP to PSTN Gateways
  - Can also use Direct SIP trunking

# About the Documentation Set

To access the documentation pages at Mitel OnLine, go to **http://edocs.mitel.com**. You require a Mitel Online username and password to access the documents on this web site.

*Mitel MiVoice Business Multi-Instance*

- *MiVoice Business Multi-Instance Installation and Administration Guide* (this guide) provides installation, administration, maintenance, and troubleshooting instructions for the MICD Manager and Media Server Manager software blades.
- *MiVoice Business Multi-Instance Administrator Online Help* provides administration and programming procedures for the MICD Manager and Media Server Manager software blades.
- *MiVoice Business Multi-Instance Engineering Guidelines* provides guidelines for deploying the Multi-Instance Platform solution, including system requirements, capacities and performance, and supported configurations.

### Access Product Documentation

1. Go to **http://edocs.mitel.com**.
2. Select a documentation suite from one of the following drop-down menus:
   - Communications Platforms
   - Applications
   - Solution Guides & Blueprints
   - Software Development
   - MiCloud
   - End User Documents
3. Log in if asked to do so.

   **Note:** For Technical Bulletins (TB) and Release Notes (RN), click Knowledge Base in the Other Resources window in the left-side navigation bar.

### View or Download a Document

To view a document:

- Click the document title.

To download a document:

- Right-click on the document title, and then click Save Target As.
  OR
  When viewing a PDF document, click the disk icon.

## Contacting Mitel

### Sending Us Feedback

If you have suggestions about how to improve this documentation, please contact us at **techpubs@mitel.com**.

## Order Desk

- Mitel NA Order Desk: 1-800-796-4835.
- Mitel UK Order Desk: +44 870 160 0471.
- Mitel EMEA Order Desk: +44 1291 426071.page 55

## Repair Department

You must get a Return of Merchandise Authorization (RMA) form from the Repairs Department before sending equipment back to Mitel.

- Mitel NA Repairs Department: 1-888-222-6483.
- Mitel EMEA Repairs Department: +44 1291 437666.

## Technical Support

Please contact Mitel Technical Support if you require technical assistance.

If you cannot resolve the problem with the Troubleshooting chapter (page 55), please collect the required information listed in the applicable section(s) of the Troubleshooting chapter before calling Mitel Technical Support.

- Mitel NA Technical Support: 1-800-561-0860 or 1-613-592-2122. (Please have your Technical Support ID ready when calling).
- Mitel EMEA Customer Management Center: +44 1291 436888. (Please have your Channel Support Agreement/Contract Number and password ready when calling.)
- Mitel Asia-Pacific Technical Support: ap_productsupport@mitel.com. (Please include your Technical Support ID Code).

# Applications Management Center (AMC) Licensing

The Mitel Applications Management Center (AMC) is an online service accessed through the web that provides licensing, monitoring, management, and a variety of other services for installations of software applications.

## About AMC Licensing

The AMC allows licensing keys to be automatically created at all times (24 hours a day, 7 days a week) through remote license keys generation.

The AMC is also the procurement and provisioning interface for AMC-delivered products and services. As a reseller of Mitel products, you receive a unique licensing account on the AMC. By logging in to the AMC with the username and password you are given when you obtain your account, you can view a list of your AMC-enabled products, check their status, and add services to any of them.

When you place a new order for products with the Mitel Customer Care Center, the order information is entered into the AMC system. The AMC places the purchased licenses into your licensing account. Before you can install the MiVoice Business Multi-Instance software, there are three steps to follow:

1. Take note of the Application Record ID that was assigned by the AMC.
   > **Note:** One Application Record represents one physical hardware device.
2. Assign all purchased application and bundled licenses to the appropriate Application Records.
3. Install the software blades and register with the AMC (activate the license).

## Requesting a New AMC Account

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

- Name of your certified Technician
- Full company name
- Company mailing address
- Phone 1/Phone2
- Fax number
- Admin e-mail (address of the person who should receive notification of service expiry dates)
- Tech e-mail (address of the person who should receive notification of update releases and other technical notices)
- Company URL (if any)
- Your Mitel SAP account number
- Specify if you would like your user ID and password delivered to you by fax, phone, or both (for security reasons user IDs and passwords are not sent by e-mail).

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

## Accessing your Account

To access your account for the first time:

1. Go to the Mitel web site (http://www.mitel.com) and log in to your Mitel OnLine account.
2. In the grey menu bar, point to Online Tools and then click AMC.
3. Sign in with your unique AMC ID and password to establish your "single sign on". On subsequent visits, you access your AMC account directly after signing in to Mitel OnLine.

For information about using the AMC, click the online Help link in your AMC account.

# Chapter 2

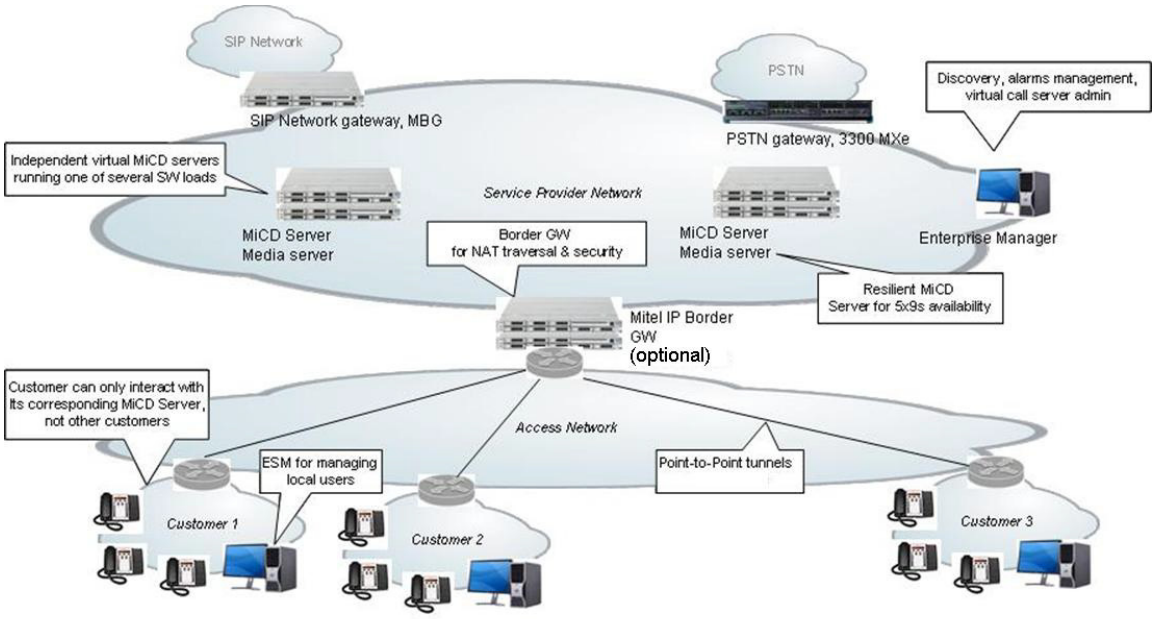
## Installation

# Overview

The MiVoice Business Multi-Instance solution can be deployed in VLAN Mode, where each MiVoice Business Instance is isolated in the network on a virtual LAN (VLAN), or in non-VLAN Mode where there is no network isolation for the Instance. This chapter describes the non-VLAN Mode deployment. See Chapter 3 for deploying the MiVoice Business Multi-Instance solution in VLAN Mode.

The MiVoice Business Multi-Instance solution installation is based on the following reference networks:

- Customer network, that contains all of the phones/consoles.
- Access network, subnets with two nodes: a customer premises router at one end and a service provider router at the other. This can be a third-party leased MPLS WAN.
- Service Provider network that hosts the Multi-Instance Platform servers, MBG servers, and gateways to PSTN/SIP networks. If using a WAN, the service provider typically leases and manages the IP addresses for each customer-service provider subnet and for each service provider-MBG subnet (not required to be globally unique).




For the example above, an MBG Server is deployed for the following roles:

- Access Network Gateway
  - Network Address Translation (NAT) traversal and security for devices on MiVoice Business instance networks.
  - NAT traversal and security for 3300 SIP trunks to the MiVoice Business instance networks.
- SIP Network Gateway
  - NAT traversal and security for 3300 SIP trunks to the SIP network.
- Internet Gateway
  - NAT traversal and security for devices on home networks.

# Installing MiVoice Business Multi-Instance

The following tasks are required to complete the installation of the MiVoice Business Multi-Instance solution:

1. Identify all the solution-specific components (hardware and software).
2. Allocate IP Addresses.
3. Obtain software licenses.
4. Install hardware.
5. Download software.
6. Install 64-bit MSL 10.3.
7. Install the software blades (MiVoice Business Multi-Instance, Media Server Manager) on separate servers. the Media Server cannot be on the same server as MiVoice Business Multi-Instance.
8. Add the MiVoice Business Multi-Instance software (the PBX functionality containing the Mitel 3300 software) to the MiVoice Business Multi-Instance inventory.
9. Create the MiVoice Business Instance(s). This would be each of the Customers shown in the diagram above.
10. Configure MSL for remote management.
11. License the software. This is done automatically If using the embedded Software Installer (SI) Tool and Mitel Configuration Wizard (MiCW) to create and add MiVoice Business Instances.

Details for each of these tasks are described in the sections that follow.

## Solution Components

Depending on the solution being implemented, ensure that all of the hardware and software components are available. Duplicates of each are required for resiliency and to meet high availability specifications. The core hardware components required are:

- MiVoice Business Multi-Instance sever, which contains the MiVoice Business Instance (the instances of the PBX functionality containing the Mitel 3300 component software, known as the MiVoice Business software)
- Media Server
- Mitel Border Gateway (MBG) Server (Optional)

The core software components required are:

- Mitel Standard Linux (MSL) 10.3, 64-bit variant
- MiVoice Business software
- MiVoice Business Multi-Instance software blade
- Media Server Manager

Other hardware and software components, as follows, will be required depending on the enterprise/hosted solution configuration:

- PSTN Gateway
- SIP Trunking Gateway
- Service provider router to the access network
- "Maintenance" PC for Embedded System Management (ESM), Enterprise Manager, and software installations.

## Allocate IP Addresses

Every MiVoice Business Instance operates inside a Mitel proprietary virtualization process hosted by an MSL server. **Each Instance requires four IP addresses in a Classless Inter-Domain Routing (CIDR) /30 block** that must fit within the MSL Server's IP subnet.

See Appendix A for an example of how to allocate IP addresses in a /30 subnet.

Upon completing the IP address allocation, it is recommended to create a network diagram of the solution.

## Obtain software licenses

To order the necessary components (including core and other components) for the solution:

1. Log on to the AMC.
2. Create an Application Record ID (ARID) for each of the following:
   - MiVoice Business Multi-Instance
   - Media Server Manager
   - MBG (for all MBG servers including those for SIP gateways and teleworker devices)
   - PTSN gateways
   - Enterprise Manager (optional)
   - Each MiVoice Business Instance (a different ARID is required for each Instance)
3. Record the ARID for each of the components for later use during activation.

## Install hardware

Install the hardware (including core and other components) for the solution.

1. Ensure that your new computer hardware is running the latest manufacturer’s firmware for that computer model. Do this prior to any Mitel AMC synchronization steps.
2. Configure any out-of-band management system interfaces on each of the following servers with their allocated IP addresses:
   - MiVoice Business Multi-Instance (include each resilient server)
   - Media Server (include each resilient server)

- MBG (if installed, include each resilient server)

  **Note:** Do not configure any G.729/G.711 transcoding on the MBG. Voice quality may degrade and the load on the server's CPU will increase which may reduce the number of simultaneous calls the server can handle. See the *Mitel Border Gateway Installation and Maintenance Guide* for details.

## Download software

Mitel and non-Mitel supported software downloads are required.

1. Download the following CD images from Mitel Online (MOL); login with proper credentials is required:
   - MSL
   - MiVoice Business Multi-Instance (or download using the MSL Server Manager after performing the ARID synchronization)
   - Media Server Manager (or download using the MSL Server Manager after performing the ARID synchronization)
   - MiVoice Business software (the PBX functionality containing the Mitel 3300 software)
2. Burn a CD for each of the downloaded images.
3. Optionally, download the following 3rd party Windows tools (not supported by Mitel):
   - PuTTy
     Windows SSH client. Used to log into a Linux shell on the MSL server.
     (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)
   - WinSCP
     MSL does not have an FTP server. Used to transfer files between the windows computer and MSL.
     (http://sourceforge.net/projects/winscp/)
   - Microsoft IIS
     Use as an FTP server for uploading MiVoice Business Instance software images using the interface on the Advanced page of the MiVoice Business Multi-Instance MCD Manager.

## Install Windows tools

Install the Windows tools (PuTTy, WinSCP, and Microsoft IIS) according to their respective instructions.

**Note:** These Windows tools *are not* supported by Mitel.

## Install MSL

Install and configure MSL according to the solution network design for each of the MiVoice Business Multi-Instance/Media Server/MBG servers, following the instructions in the *Mitel Standard Linux Installation and Administration Guide*. Install MSL in server-only mode (bonded ethernet network interface cards (NICs) are acceptable) for both non-VLAN Mode and VLAN Mode deployments. Multiple ethernet interfaces can not be on different subnets.

## Install the Software Blades: MiVoice Business Multi-Instance and Media Server Manager)

Use the following procedure to install each of the MiVoice Business Multi-Instance/Media Server Manager/MBG Manager software blades on their corresponding servers:

1. *Optional:* Place the CD into the optical drive.
2. Login into the MSL Server Manager using Internet Explorer with the user name '*admin*' and root password '*password*' used when configuring the MSL server.
   The Server Manager is accessed by entering the following URL:
   **http://<*hostname*> OR <*IP address of the MSL Server*>/server-manager**
3. Click on **Blades**, located in the left-side panel under the **ServiceLink** heading.
4. Click **Update List** to ensure an up-to-date listing of software blades.
5. Click the **Install** link, located beside the appropriate software blade name.
6. Click **Accept** for any end user license agreements that appear.

   It may take a few minutes for the software to install. The software blade appears in the left-side panel under the **Applications** heading.
7. When the installation is complete, click **Clear this report**.
8. Repeat steps 1-7 for the Media Server Manager and MBG.

## Installing Media Server Manager

The Media Server Manager is installed as a software blade using the above procedure. The Media Server Manager must be installed and run on a separate computer, with no other software co-located.

Media Server Manager does not require a Mitel license or ARID when installed from a CD using the MSL Server Manager.

When creating Media Server instances, specify the IP addresses of the MiVoice Business instances to which they will connect.

Create and start the Media Server instances prior to creating the MiVoice Business instances (see the *Media Server Manager Administrator Online Help*). MiVoice Business database programming of embedded voice mail will require that a Media Server Instance is connected.

A MiVoice Business Instance can have only one Media Server Instance. A Media Server Instance can connect to only one MiVoice Business Instance. A Media Server Manager computer will contain many Media Server instances. Media Server instances on a single Media Server Manager computer may connect to MiVoice Business instances located on different MiVoice Business Multi-Instance computers.

When installing Media Server Manager with MiVoice Business Multi-Instance in VLAN Mode, the Ethernet connection between the server and network must be configured as follows:

- All customer VLANs must be tagged with VLAN IDs.
- The management network must be untagged (referred to as the Native VLAN in other contexts). See *Trunk Ports and the native VLAN* in http://en.wikipedia.org/wiki/IEEE_802.1Q.

- The MSL IP address is in the Management Network. The MSL gateway is the gateway to additional management subnets and the Internet.
- MSL has a concept of *Local networks* where only computers on the local network may access the MSL IP addresses. This local network is the Management Network. The MSL local networks configuration panel may be used to grant access to additional networks. These additional networks would be part of the Management Network.

## Install the MiVoice Business Instance Software

Install the MiVoice Business Instance software (the PBX functionality containing the MiVoice Business software) by unpacking the software onto a local PC by double-clicking the software exe file, and using an FTP server to distribute the tar files to the MiVoice Business Multi-Instance server(s). These tar files are known as the MiVoice Business software loads. The MiVoice Business software loads are first loaded into the software inventory, then made available for use by the various MiVoice Business Instances.

Use the following procedure for each resilient MiVoice Business Multi-Instance server:

1. Insert the MiVoice Business Product CD into the drive of the network maintenance PC.
2. Double click on the MiVoice Business Product executable file to unpack the tar files.
3. Go to the FTP server (that was set up using Microsoft IIS) and point to where the MiVoice Business software loads are.
4. Add the MiVoice Business software loads to the software inventory (for detailed information see the *MiVoice Business Multi-Instance Manager Administrator Online Help*):
   a. Login to the MSL Server Manager and click **MiVoice Business Multi-Instance** under **Applications** in the left-side navigation pane.
   b. Go to the **Advanced Tab**.
   c. In the **Instance Software Inventory Tag** field, enter a meaningful descriptive name for the MiVoice Business software load being added to the inventory.

   **Note:** Do not add any spaces in this field. This name will appear in the Instance Software Inventory Tag drop-down list on the Advanced Tab.

   d. In the **FTP Server IP Address** field, enter the IP address of the FTP server on which the MiVoice Business software loads reside.

   **Note:** The FTP server is the PC onto which the MiVoice Business Product CD image was downloaded from Mitel Online (see Step 3 above).

   e. In the **FTP User Name** field, enter the user name that will be used to access the server that contains the MiVoice Business software loads.
   f. In the **FTP Password** field, enter the password for the User of the sever that contains the MiVoice Business software loads.
   g. Click **Add Revision** to add the MiVoice Business software load to the inventory. This MiVoice Business software load will appear in the **Instance Software Inventory Tag**

drop-down list, and on the **MiVoice Business Instance Details** page on the **Dashboard Tab**.

**Time:** It can take a few minutes for each version of MiVoice Business software load to download into Inventory.

## Using the Stand-alone Software Installer Tool

The stand-alone Software Installer (SI) Tool offers an alternate way to upgrade MiVoice Business software on a MiVoice Business Multi-Instance server after a MiVoice Business Instance is up and running, using the online upgrade feature. The following pre-requisites must be enabled on the MiVoice Business Multi-Instance Server:

1. Set up the PC from which the SI Tool is running as part of the MSL Local Networks (required for ftp, ssh and others). By default only the subnet on which the MSL server resides is part of Local Networks:
   a. Login into the Server Manager using Internet Explorer with the user name *admin* and the root password used when configuring the MSL server.
   The Server Manager is accessed by entering the following URL:
   **http://<*hostname*> OR <*IP address of the MSL Server*>/server-manager**
   b. Click on **Networks** located in the left-side panel under **Configuration**.
   c. Click **Add a new trusted network**.
   d. Add the management network containing the PC from which the SI Tool is running, to the MSL Networks list.
2. Configure Secure Shell to be accessible from the Local Network:
   a. While still logged in to the Server Manager, click on **Remote Access** located in the left-side panel under **Security**.
   b. In the **Secure Shell Settings** area:
      - In the **Secure shell access** drop-down list, select **Allow access only from local networks**.
      - In the **Allow administrative command line access over secure shell** drop-down list, select **Yes**.
      - In the **Allow secure shell access using standard passwords** drop-down list, select **Yes**.

Whenever using the SI Tool to place a new MiVoice Business software version on a MiVoice Business Multi-Instance Server, also add that software load into the Inventory, as described in “Install the MiVoice Business Instance Software” on page 19 beginning with Step 4. Doing this prevents the inventory from becoming out of sync with the MiVoice Business software loads installed for the MiVoice Business instances. If the MiVoice Business software load is not in the MiVoice Business Multi-Instance inventory, then the embedded SI operations for backup/restore/upgrade will not work.

For more information about installing the MiVoice Business Product software, refer to the *MiVoice Business Multi-Instance Manager Administrator Online Help*.

## Configure MSL for Remote Management

The MSL Firewall is used to restrict access to all applications on the computer. This includes the MiVoice Business instances. The only computers/phones/gateways able to access the Instance are those residing on networks listed in the Networks section of the MSL Server Manager.

Use the following procedure to identify all the networks that contain devices that need to connect to the MiVoice Business instance:

1. Login into the Server Manager using Internet Explorer with the user name and password used when configuring the MSL server.
   The Server Manager is accessed by entering the following URL:
   **http://<*hostname*> OR <*IP address of the MSL Server*>/server-manager**
2. Click on **Networks** located in the left-side panel under **Configuration**.
3. Click **Add Network**.
4. Enter the appropriate information in each of the **Network address**, **Subnet mask**, and **Router** fields for those devices that need connection to the MiVoice Business instance.
   The Router field would contain the IP address of the next hop router that this MSL server will use to reach that subnet. Typically this is the default gateway of that MSL server.
   For phones that are behind MBG, specify just the network containing the MBG Local interface.
   Add the management network containing the Maintenance PC to the MSL Networks list.
5. Repeat for each resilient MiVoice Business Multi-Instance/Media Server/MBG Server.

## License the Software

The MiVoice Business Multi-Instance/Media Server Manager/MBG Manager software for each resilient server will need to be licensed before use.

> **Note:** Media Server Manager does not require a Mitel license or ARID when installed from a CD. A license and ARID are required when installing Media Server Manager from the AMC.

Licensing the software can be done with or without an Internet connection. An Internet connection is required for any configuration steps that involve the embedded SI Tool or Mitel Configuration Wizard (MiCW).

A MiVoice Business Multi-Instance license is needed to start the MiVoice Business instances. A MiVoice Business Software ARID is also needed, on a per-Instance basis, which is entered into the *MiVoice Business System Administration Tool* License-Options-Selection (LOS) form. The MiVoice Business Software licenses are used to program the Instances.

When creating or upgrading Instances using the embedded SI Tool and MiCW, licensing is automatically performed; the embedded tools will connect and synch with the AMC and open the forms in the *MiVoice Business System Administration Tool*.

### Internet connected

To license the software using an internet connection:

1. Login into the Server Manager using Internet Explorer with the user name and password used when configuring the MSL server.

The Server Manager is accessed by entering the following URL:
**http://<*hostname*> OR <*IP address of the MSL Server*>/server-manager**

2. Click on **Status**, located in the left-side panel under the **ServiceLink** heading.
3. Enter the MiVoice Business Multi-Instance ARID.
4. Click **Activate**.
5. Once the confirmation has appeared, the software is ready to use.
6. Repeat steps 1-5 for the software for each resilient server.

### Non-internet connected

To license the software without using an internet connection:

1. Obtain and label one USB flash drive for each resilient server upon which the software will need to be licensed.
2. Insert the flash drive into a USB port on the appropriate server.
3. Login to the MSL Server Console, with the user name *'admin'* and the password of the MSL root user account.
   > **Note:** Use PuTTY or other Windows SSH clients.
4. Navigate to **Offline Sync with AMC**. Click **Next**.
5. Select **Prepare removable storage device for use with offline sync**. Click **OK**.
   MSL writes a batch file that can be run on a Windows PC (as well as on an MSL server) that contains information used for generating license keys.
6. Remove the USB flash drive from the USB port.
7. Repeat for the software for each resilient server.
8. Go to a Windows PC *with Internet access*.
9. Insert the USB flash drive into a USB port on the PC.
10. Navigate to where the batch file is located and double-click on it.
    The PC gets license key information from the AMC and stores it on the USB flash drive.
11. Remove the USB flash drive from the USB port.
12. Repeat for the software for each resilient server.
13. Insert the USB flash drive into a USB port on the appropriate server.
14. Navigate to **Offline Sync with AMC**. Click **Next**.
15. Select **Read back sync data from removable storage device**. Click **OK**.
    MSL reads the data in and writes it to the file system. All of the appropriate server software is now licensed and ready to use.

## Add MiVoice Business Instances

> **Note:** More details for the following steps are available in the MiVoice Business Multi-Instance Web Administration On-line Help. Click the blue question mark in the top right-hand corner of any MiVoice Business Multi-Instance web page and select the section *Adding a MiVoice Business Instance* for greater detail.

There are three different ways to add or create a MiVoice Business Instance:

1. Create the Instance with no MiVoice Business license and no database configuration. This will take approximately 20 seconds per Instance)
2. Create the Instance and license it through the AMC in one step, but no database is provided. This will take approximately 7 minutes per Instance.
3. Create and license the Instance through the AMC, and use embedded Mitel Configuration Wizard (MiCW) to configure and program a supplied default database. This will take approximately 20 minutes per Instance.

The procedures below describe creating the Instance(s) in any of these three ways.

ARIDs can be provided on a per-instance basis, or in bulk, regardless if more than one instance uses the same MiVoice Business s/w version.

The MiVoice Business Multi-Instance software blade also needs a license from the AMC.

A MiVoice Business Multi-Instance solution can become confusing with multiple Instances and multiple other products. To help manage this complexity, choose a consistent naming convention across the whole solution. If the solution includes more than one MiVoice Business Multi-Instance server, it is recommended to use the server name as part of the Instance name, for example MICD1Customer1 and MICD2Customer2.

Use the MiVoice Business Multi-Instance software blade administration interface to add the Instance(s) and corresponding MiVoice Business software load(s) to the MiVoice Business Multi-Instance inventory (for detailed information see the *MiVoice Business Multi-Instance Manager Administrator Online Help*).

Adding Instances involves setting up the Instance name(s) and increment value(s) (using range programming), selecting the MiVoice Business software from the inventory, and optionally selecting a Configuration Wizard file to automatically configure the Instance(s).

> **Note:** MiVoice Business Instance licenses are a pre-requisite, and the MiVoice Business software will need to be in the MiVoice Business Multi-Instance inventory. The number of Instances is restricted by the physical amount of RAM on the server.

To add MiVoice Business Instances:

1. Go to the Bulk Tab.
2. Click **Add** in the **Range Programming** section.
3. Enter the number of instances being added in the **Enter the number of MiVoice Business Instances to create** field.

4. To create the Instance(s) with *no MiVoice Business license(s)* and *no database*, select **No** from the **Do you want to enter the MiVoice Business license ARID for each MiVoice Business instance** drop-down list. This is the default selection.

   **Time:** This approach will take approximately 20 seconds per Instance.

   (Optional) To create the Instance(s) using the embedded Mitel Software Installer (SI) tool to *synchronize and license the Instance with the AMC* in a single step, but *with no database provided*, select **Yes** from the **Do you want to enter the MiVoice Business license ARID for each MiVoice Business instance drop-down** list.

   **Time:** This approach will take approximately 5 - 7 minutes per Instance.

   **Notes:**

   1. A unique ARID will be required for each instance created.
   2. A connection to the AMC is required.

5. (Optional) In the Config Wizard xml file drop-down list, select the configuration file to use for creating the Instance(s). The **Do you want to enter the MiVoice Business license ARID for each MiVoice Business instance** drop-down list field in Step 4 above will need to be set to **Yes** in order to use a Configuration Wizard file.

   **Note:** If the MICW configuration file includes embedded voice mail options, configure the corresponding Media Server before continuing. It will need to be programmed to connect to the corresponding Instance, as described in the *Media Server Manager Administrator Online Help*.

   MiVoice Business Multi-Instance will then:

   - Create the Instance.
   - Start the Instance.
   - Invoke the embedded SI tool with ARID synchronization (to license the MiVoice Business software).
   - Invoke the embedded MiCW with the requested Configuration Wizard file to configure and program a supplied default database.

   **Time:** This approach will take approximately 20 minutes per Instance.

   **Notes:**

   1. The **Config Wizard xml file** drop-down list contains those configuration files that were uploaded using the Upload Config Wizard file capability on the Bulk Tab.
   2. If there is an AMC failure, then the process will skip creating the Instance.
   3. If there is a Configuration Wizard file error, then the Instance will be removed and the process will continue with creating the next Instance.

6. (Optional) In the **Golden db Template** drop-down list, select the golden database template file to use for creating the Instance(s). Golden database template files will be listed only if they have been uploaded through the Bulk Tab.

   MiVoice Business Multi-instance will then:

   - Create the Instance.
   - Start the Instance.
   - Invoke the embedded SI tool with ARID synchronization.
   - Invoke the embedded database restore option to restore the chosen database.
   - Re-boot the system.

    **Time:** This approach will take approximately 15 minutes per instance.

7. Enter the name of the Instance in the **Instance Name** field.

   **Notes:**

   1. When creating the Instance(s) with the MiCW, the Instance name will be "pushed" to the MiVoice Business System Administration Tool. Therefore it is necessary that the Instance name follow the rules as governed by the MiVoice Business System Administration Tool:
      - 9 characters maximum
      - no spaces
      - alpha-numeric only
      - 1st letter capitalized
   2. The entry in this field is for your information only. Since there is no automatic synchronization with the Instance configuration database, it is recommended to adopt a standardized naming convention, and to use that same instance name when completing the Network Element Assignment form in the System Administration Tool for this Instance.
   3. Enter a name that will not be confusing. When creating a number of instances for an entity (e.g. Customer), the MiVoice Business Multi-Instance database will increment the last letter or number by the amount specified in the **Increment by** field. For example, if the first Instance Name is Customer1, and the increment value is 1, the next Instance Name will be Customer2, then next after will be Customer3, etc. until Customer9. If creating 10 or more Instances with this type of naming convention, then the count will loop and begin again with the 10th Instance named Customer1. Using a naming convention where the first Instance Name is Customer01, the counter will increment until Customer99, and begin to loop again at the 100th Instance Name.

8. Enter the value by which each instance name will be incremented in the **Increment by** field opposite **Instance Name**.

9. Enter the IP address of the MiVoice Business Multi-Instance server in the **System IP Address** field. See Appendix A for an example of how to allocate IP addresses in a simple network.

10. Enter 4 in the **Increment by** field opposite **System IP Address**, since each Instance uses four IP Addresses.

    **Note:** This applies to non-VLAN mode configurations only.

11. In the **Enable SNMP Traps and MSL Alarms** drop-down list, select **Yes** to allow alarm and SNMP trap information to be sent to the MSL Alarm subsystem and displayed in the MSL Event

Viewer. Select **No** to disable alarm and SNMP trap information being sent to the MSL Alarm subsystem and from being displayed in the MSL Event Viewer.

**a.** To access the MSL Event Viewer and view the alarms:

- Click **Event viewer** in the left-side navigation pane under **Administration**.
- Select the appropriate time interval from the **Show how far back in age?** drop-down menu.
- Click **Refresh**. See the *Mitel Standard Linux Installation and Administration Guide* for details.

**b.** To allow the alarms to be sent as SNMP traps to an external network management application, configure the MSL server upon which MiVoice Business Multi-Instance is installed as follows:

- Click **SNMP** in the left-side navigation pane under **Configuration** in the MSL Server Manager. The Configure SNMP support page displays.
- Select **Enabled** in the **Service status** drop-down menu.
- Complete the remainder of the fields and menu selections as appropriate. See the *Mitel Standard Linux Installation and Administration Guide* for details.

**12.** In the **Enable Alarms for Media Server connection state changes** drop-down list select **Yes** for this Instance to be configured to display alarms for connection state changes of the associated Media Server. Select **No** if the Media Server alarm is not needed.

The values entered in the next two fields will provide an indication of the overall health of the system, with respect to the number of phones that are connected, as indicated on the Dashboard Tab. It is acceptable that a small number of phones are disconnected, such as those that are unplugged, or undergoing maintenance. However, a large number of disconnected phones would indicated a serious underlying network problem.

Set the value to zero in each field for no alarms to be generated. These fields do not apply to SIP devices.

**13.** In the **Major Alarm if connected MiNet phone count below** field, enter the minimum number of MiNet phones that can be connected before a Major alarm is generated.

**14.** In the **Minor Alarm if connected MiNet phone count below** field, enter the minimum number of MiNet phones that can be connected before a Minor alarm is generated.

**15.** In the **Reset MiVoice Business on Media Server Disconnect** drop-down list, select **Yes** so that the Instance will reboot when it disconnects from its corresponding Media Server. This is the default value.

> **Note:** When the Media Server is disconnected from its corresponding MiVoice Business Instance, Voice Mail, Music on Hold, and Conferencing capabilities are lost, but basic telephony continues. Music on Hold and Conferencing will resume upon re-connection between the Media Server and its corresponding Instance. Embedded Voice Mail will not come back when the Media Server reconnects to the MiVoice Business. A MiVoice Business reboot is required to re-establish Embedded Voice Mail services.

Select **No** to not reboot the Instance when its corresponding Media Server disconnects. This is useful if Embedded Voice Mail services have not been implemented.

16. In the **MiVoice Business S/W Version** drop-down list, select the MiVoice Business software version. This is a list of the MiVoice Business software versions that have been uploaded to the MiVoice Business Multi-Instance inventory.
17. In the **Atlas S/W Version** drop-down list, select the version of the Atlas Vxworks virtual machine configured for the Instance. Unless otherwise directed, leave this at the default selection.
18. In the **On startup, upgrade to latest Atlas Rev** drop-down list, the default selection is **Yes**, indicating that when the Instance starts, it will look for a new version of Atlas, and if a new Atlas exists (and there is a license), it will upgrade to the new version. Select **No** if an older version of Atlas is required, which will prevent the auto upgrade. The only situation under which an older version would be required is if directed by Mitel to do so.
19. In the **Enable MiVoice Business instance Backup, Restore, Upgrade via MiVoice Business Multi-Instance's SI Tool** drop-down list, select **Yes** to allow the MiVoice Business Multi-Instance's embedded Software Installer (SI) Tool to backup, restore, and upgrade the instance(s). If **No** is selected, then the automated bulk operations will be skipped for this instance. This is instance-specific and overrides the bulk operations such as backup, restore, and upgrades. See “Backup and Restore the MiVoice Business Instance software load” on page 48 for details and more information.
20. In the **MICD SI Tool Backup: Include Voice Mail messages** drop-down list, select **Yes** to allow the MiVoice Business Multi-Instance's embedded Software Installer (SI) Tool to include voice mail messages as part of the backup process. The default is **No**.

    **Note:** Selecting **Yes** will cause the backup files to become very large and will increase the time it takes to perform an Instance backup and restore.
21. In the **MICD SI Tool Backup: Include Call History records** drop-down list, select **Yes** to allow the MiVoice Business Multi-Instance's embedded Software Installer (SI) Tool to include call history records as part of the backup process. The default is **No**.

    **Note:** Selecting **Yes** will cause the backup files to become very large and will increase the time it takes to perform an Instance backup and restore.
22. In the **Max simultaneous Voice Mail Ports** drop-down list, select the number of voice mail ports that will be monitored based on the maximum number of users and ACD Agents on the system.
23. Click **Next**.
    Before creating the Instance(s), a basic sanity check is performed to test for conditions that would cause the Instance to fail. When creating a number of Instances, should there be any errors present (as a result of the sanity check) or other failures, that Instance is not created and the next Instance will be created.

Complete the next three steps only if the default MiVoice Business Instance setup was selected in Step 4 above (without using the embedded SI Tool or the embedded MiCW).

24. Start the Instances.
25. License the Instances:
    a. Go to the Dashboard Tab.
    b. Click on the ESM link for the Instance.
    c. Log into the MiVoice Business System Administration Tool:

- Go to the **License-Options-Selection (LOS)** form.
- Enter the **Application Record Identifier** (ARID) in either the **Bulk ARID Input** text box, or individually in **ARID Input Table**. There is now the option to enter ARIDs in bulk. From a comma-, space-, or paragraph-delimited list, copy and paste the ARIDs into the Bulk ARID Input text box.

  > **Note:** ARIDs can only be entered in either the **Bulk ARID Input** text box, or individually in **ARID Input Table**, but not both.

- Click **Retrieve Licenses**. Purchased licenses from AMC displays on the form.

**26.** Configure the Instances:

**a.** Go to the Dashboard Tab.

**b.** Click on the ESM link for the Instance.

> **Note:** The ESM link is active only in non-VLAN mode, or when **ESM Access from** (see the *MiVoice Business Instance Detail* topic of the *MiVoice Business Multi-Instance Manager Administrator Online Help)* is set to **Management Network** in VLAN mode.

**c.** Log into the MiVoice Business System Administration Tool:

- Go to the **Network Element** form, and change the system name so that it is the same for each of the names assigned in Step 4.
- Go to **Maintenance Commands** and execute **DBMS SAVE**.
- Go to **System Date and Time**, and select the Time Zone.
- Go to the **SNMP Trap Forwarding** form, and enable SNMP traps.
- Program phones, voicemail, etc. corresponding to the MiVoice Business software license purchased for the MiVoice Business Instance.

> **Notes:**
>
> 1. Refer to the MiVoice Business System Administration Tool Online Help for details about enabling SNMP traps and programming phones, voicemail, etc.
> 2. If a Mitel Border Gateway (MBG) is incorporated into the network, it is recommended that its Local Streaming feature be enabled to allow for optimal bandwidth management, and then the Network Topology Assignment form in ESM will not need to be programmed for Media Path Anchor Zones. If the MBG Local Streaming Feature is not enabled, then the Network Topology Assignment form in ESM will need to be programmed for Media Path Anchor Zones to optimize bandwidth management.

**27.** If the MiCW configuration file did not include embedded voice mail options (see Step 5 above), configure the corresponding Media Server. It will need to be programmed to connect to the corresponding MiVoice Business Instance, as described in the *Media Server Manager Administrator Online Help*.

## Configuring MiVoice Business Instances

To configure an Instance, refer to the *MiVoice Business Multi-Instance Manager Administrator's Online Help, MiVoice Business Instance Detail* topic. This topic describes all of the parameters that can be configured for the Instances.

# Chapter 3

## Configuring VLAN Mode

# Configuring MiVoice Business Multi-Instance in VLAN Mode

In prior releases all MiVoice Business Instances were in a single subnet and a single trust domain. A Mitel Border Gateway (MBG) was needed to provide segregation between non-related Instances. This release of MiVoice Business Multi-Instance provides the option of enabling full MiVoice Business network isolation with every Instance on a Virtual LAN (VLAN).

It is important to understand the following new terms and concepts brought into play when configuring VLAN mode:

- **Customer Network**: When MiVoice Business Multi-Instance is in VLAN mode, each Instance is on a VLAN. The Customer Network consists of all networks reachable from the MiVoice Business VLAN (routing domain).
  This VLAN Customer Network is a single routing domain consisting of computing devices under the control of a single corporate network. If a customer owns several Instances, they may share a single VLAN or exist on multiple VLANS in the same routing domain.
  A Customer Network is defined with a VLAN ID, subnet mask, and default router. The VLANS can be isolated to restrict communications to one or more selected Instances. The IP phones reside on the Customer Network.
- **Management Network**: The Management Network is owned by server administration when MiVoice Business Multi-Instance is in VLAN mode. Computers on Management Network can connect to every Instance via the MiVoice Business Management IP Address. This network is attached to the MSL server's local interface and is typically located in the Service Provider's data center. Computers on the Customer Network would not have access to the Management Network.
- **Network Domain**: All computers within a data network domain may be interconnected. All have unique IP addresses. Computers in separate domains may not be interconnected (except via a NAT gateway).

When configuring the network in VLAN mode, it is important to note that each and every Instance requires two IP addresses:

- one on the Customer Network
- one on the Management Network

## Deployment Scenarios

There are two basic deployment options, depending on the interconnect configuration:

1. Service Provider, where VLANs are connected to different network domains.
2. Enterprise, where VLANs are connected to a single network domain.

### Service Provider Deployment

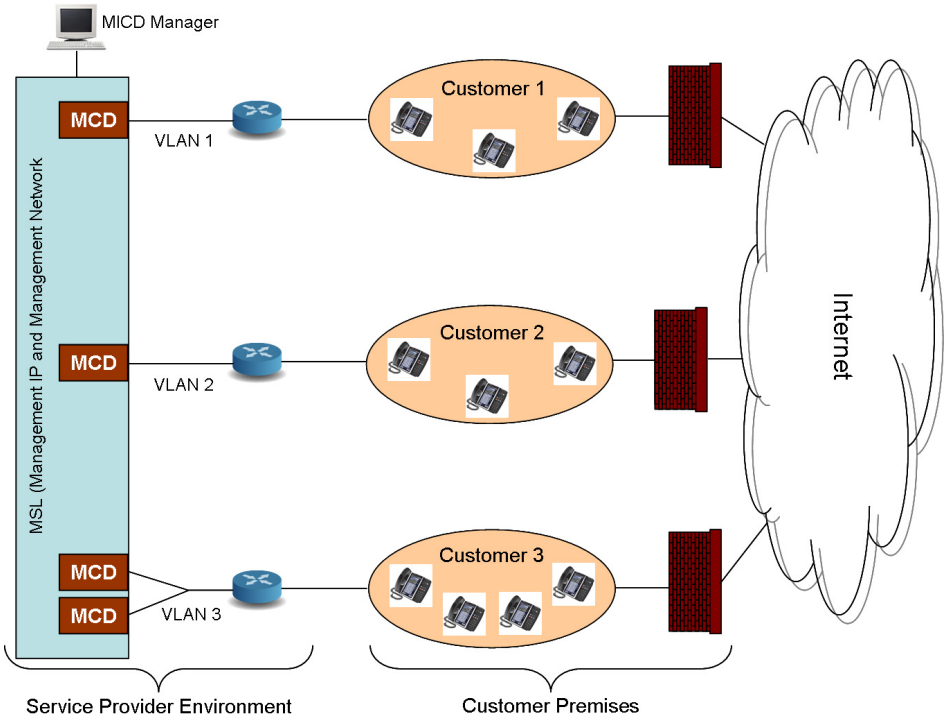
In the Service Provider deployment scenario, the network is configured to isolate the network domains. There is no routing between the different Customer Network domains, and each customer is separate from one another. Each has its own Customer Network domain.

A VLAN joins the Customer Network domain to a MiVoice Business Instance. In situations where more than one Instance is connected in the VLAN, they all share the same Customer Network domain.

A Customer Network may have more than one VLAN in the same network domain.

Network address numbering plans may overlap across different network domains. This is acceptable as long as the computers within a network domain have unique IP addresses.

The diagram below shows a simple example of a Service Provider deployment.

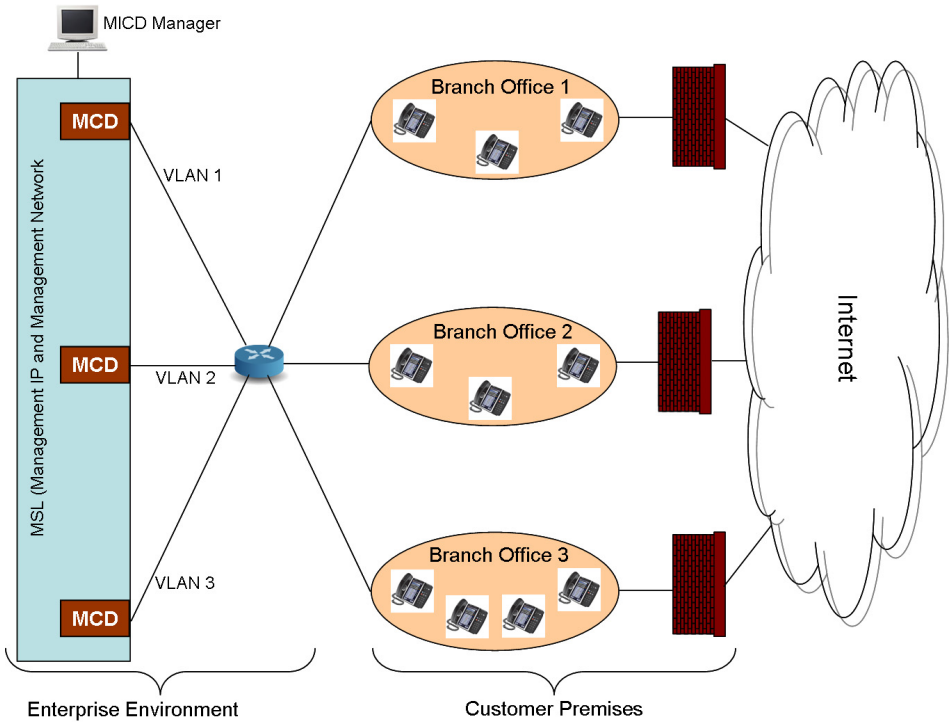



## Enterprise Deployment

In the Enterprise deployment scenario, the network configuration does not isolate the network domains. All VLANs are connected to a single network domain.

Network address numbering plans cannot overlap across the network domain. All computers must have unique IP addresses.

The diagram below shows a simple example of an Enterprise deployment.




## Configuring MSL Networking

MSL needs to be configured in **server-only** mode, and all customer VLANs must be tagged with VLAN IDs. When MSL networking and VLAN tagging are complete, VLAN mode must be enabled in MiVoice Business Multi-Instance using the MiVoice Business Multi-Instance Web Administration interface.

1. Install MSL in server-only mode. If your server has more than one Ethernet interface, then bond the additional interfaces to first interface, or disable them. You may not have multiple Ethernet interfaces on different subnets.
2. The Ethernet connection between the server and network must be configured as follows:
   a. All customer VLANs must be tagged with VLAN IDs.
   b. The Management Network must be untagged (also known as the Native VLAN). See "Trunk Ports and the native VLAN" in http://en.wikipedia.org/wiki/IEEE_802.1Q.
   c. Do not place a firewall on the VLAN trunk, between the MSL computer and the first hop router. Firewalls may be confused by overlapped IP addresses and dropped packets.
3. Ensure the MSL IP address is in the Management Network. The MSL gateway is the gateway to additional management subnets and the Internet (for AMC license access).
4. MSL has a concept of *Local Networks* where only computers on the local network may access the MSL IP addresses. This local network is the Management Network.
   Use the MSL local networks configuration panel to grant access to additional management subnets. These addition subnets would be part of the Management Network. In a service provider configuration, the Customer Network(s) would be configured to not have access to the Management Network.

## Enabling VLAN Mode on MiVoice Business Multi-Instance

Every MiVoice Business Instance is assigned:

- A VLAN id. This is on the Customer Network. A VLAN may contain more than one Instance.
- A MiVoice Business system IP address in the Customer Network. The phones and media server will connect to the MiVoice Business system IP address. Customer applications and telephones need to target the MiVoice Business system IP address on the Customer Network. Hosts need to be in the Customer Network to access the MiVoice Business system IP address. Access to MiVoice Business system IP address is not controlled by MSL local networks settings. All computers on Customer Network have access to this IP address, only if they are configured on the whitelist (see “Whitelist Configuration” on page 38).
- A default gateway to the Customer Network.
- A netmask. All computers attached to the same VLAN must have the same netmask.
- A Management IP address. This is a proxy IP address used by computers in the Management Network to access MiVoice Business. This address will be in the MSL server's local subnet.

*To enable VLAN mode:*

1. Disable all Instances.
2. Login to the MSL Server Manager and click **MiVoice Business Multi-Instance** under **Applications** in the left-side navigation pane.
3. Go to the **Advanced** tab.
4. Click **Enable** opposite **VLAN Mode is Disabled**.
5. Modify any previously existing Instances to add the VLAN attributes. For detailed information see the *MiVoice Business Multi-Instance Manager Administrator Online Help*.

### Access Restrictions

Computers on the same Management Network will have access to the following (but those on the Customer Network, by default, will not have access):

- the MiVoice Business ESM web interface
- other MiVoice Business administrative TCP ports
- MSL server-manager

Computers on the Management Network will have access to MiVoice Business Instances via a management proxy IP address. The management IP address is displayed on the MiVoice Business Multi-Instance Review tab in the MiVoice Business Multi-Instance Manager web administrative interface. All MSL server-manager activities must be performed from the Management Network.

Access to the MiVoice Business System Administration Tool (ESM) is available from either the Management or Customer Network. By default, ESM is available from Customer Network. For detail information see the *MiVoice Business Multi-Instance Manager Administrator Online Help*.

## Setting up the Media Server

Both MSL and network configuration is the same as on MiVoice Business Multi-Instance. Prior to configuring the Media Server Manager, ensure that MSL networking has been configured (see “Configuring MSL Networking” on page 32).

*To configure the Media Server:*

1. Assign an IP address in the Management Network to MSL.
2. Enable VLAN mode (see below).
3. Assign an IP address in the Customer Network to each media server instance.
4. Each media server instance will initiate a signaling connection to an MiVoice Business system IP address via the Customer Network.
5. The phones must be able to connect to the media server instance IP address.

*To enable VLAN mode:*

1. Disable all Media Server Instances.
2. Login to the MSL Server Manager and click **Media Server Manager** under **Applications** in the left-side navigation pane.
3. Go to the **Advanced** tab.
4. Click **Enable** opposite **VLAN Mode is Disabled**.
5. Modify any previously existing Media Server Instances to add the VLAN attributes (Netmask, VLAN ID, IP addresses of the associated Instances, and the default gateway on the Customer Network). For detailed information see the *MiVoice Business Multi-Instance Media Server Manager Administrator Online Help*.

# VLAN Mode Restrictions

There are a number of configuration, IP proxy, ESM access, port and MiVoice Business routing restrictions when MiVoice Business Multi-Instance is configured in VLAN mode. The following sections describe these in detail.

## VLAN Mode and MiVoice Business Configuration Considerations

When a MiVoice Business Instance is added to a VLAN, it will only be able to communicate with other computers that are accessible through that VLAN. In a typical Service Provider configuration, the Management Network is not accessible through the Customer's VLAN.

With this scenario, it is important to be aware of the following:

1. *Programming MiVoice Business (either through ESM or MiCW).*
   All IP addresses programmed into MiVoice Business must be accessible via the Customer's VLAN. Do not enter any IP addresses from the Management Network into the MiVoice Business programming pages. This will affect the following:
   - SNMP traps may only be sent to IP addresses on the Customer Network or Internet (via Customer network).
   - The email server (in *ESM->System Properties->System Feature Settings->System Options* form) is an IP address on the Customer Network or Internet (via the Customer Network).
2. *DNS Server configuration in* MiVoice Business.
   The MiVoice Business configuration may require a DNS server IP address that is reachable through the Customer Network (in *ESM->LAN/WAN Configuration->System IP Properties*). The default DNS server is the MSL IP address. When in VLAN Mode in a Service Provider deployment scenario, the MSL IP address will not be accessible to the MiVoice Business Instance (the MSL IP address is on the Management Network). A DNS server is needed if MiVoice Business licensing is updated via the ESM Licensing & Options form. A DNS server may also be needed if MiVoice Business is to send email and for certain SIP trunking configurations where domain names are entered instead of dotted quad IP addresses into ESM forms. If the Instance needs a DNS server, a DNS server must be programmed that is on the Customer Network (or Internet via the Customer Network).
3. *ESM Access configuration (when creating/modifying Instances using MiVoice Business Multi-Instance Manager web administration).*
   - **Customer Network:** default setting that allows customers to manage their own network. During normal operation, this setting provides access to the ESM from both the Management Network and the Customer Network. However, if there is a device on the Customer Network with the same IP address as that of a device on the Management Network (conflict scenario), this setting provides access to the ESM from the Customer Network only, but not from the Management Network.
   - **Management Network:** use this option if you want to prevent Customer Network devices from accessing the management application ports. With this setting, ESM can be accessed only from the Management Network.
     Note that this setting disables certain MiVoice Business features; these include, but are not limited to, the following:
     - ESM reach-through

- IDS Synchronization to the external Active Directory server
- FTP to external servers.

See “Configuring VLAN Network Access” on page 68 for more detail.

## Configuration Restrictions

- Use the 64-bit variant of MSL 10.3.
- MSL must be installed in server-only mode (see the *Mitel Standard Linux Installation and Administration Guide*).
- MSL Ethernet interface bonding is supported.
- All Customer Networks configured with VLAN tags. The Management Network is untagged. There is no option to provide a VLAN specifically for management. Therefore it is acceptable at the Layer 2 switch (or network backplane) to convert this untagged VLAN to the system network management VLAN, and vice versa (off the server hardware, in the network).
- MiVoice Business Management IP address must be on same subnet as MSL.
- MiVoice Business Management IP address cannot overlap with *any* MiVoice Business System IP address.
- MiVoice Business Management IP address access is restricted to computers on the MSL "Local Networks". By default, MSL "Local Networks" is set to the MSL local subnet (see *Mitel Standard Linux Installation and Administration Guide*).
- MSL "Local Networks" settings are not applicable to computers on Customer Networks. All Customer Network devices can access the MiVoice Business/Media-Server (see “Whitelist Configuration” on page 38 for some exceptions).

> **Note:** Any network configured in Local or Trusted Networks sends all traffic untagged and routes out the Management Network (do not added customer network IP addresses to Local or Trusted Networks. You must add these IP addresses to the allowed list so the traffic is tagged appropriately).

MiVoice Business Multi-Instance uses RFC 3927 link-local IP addresses. Therefore:

- MiVoice Business default gateway, MSL, Management, or MiVoice Business System IP address cannot be in 169.254.77.0/24.
- Any devices on Customer Network communicating with MiVoice Business cannot be in 169.254.77.0/24.

## Management IP Proxy Restrictions

The Management IP address is a proxy to the MiVoice Business System IP address. Computers on the Management Network may access any MiVoice Business port via the MiVoice Business specific IP address. To access ESM web forms from the Management network, switch the **ESM Access from:** setting to **Management Network**. When finished ESM browsing, place the ESM Access setting back to **Customer Network**. While ESM is in Management-mode, the ESM reach-through feature will not work. There may be other issues when ESM is on the Management Network; see Appendix C for further details.

- Do not connect phones to the management IP address. One way or no audio situations will develop depending on the locations of the endpoints. For Service Providers wishing to have customer phones in the management location, connect those phones to the customer VLAN.
- Do not connect any MiVoice Business Instances to a management IP address (i.e. when configuring MiVoice Business via ESM, do not enter any management IP address's for trunk endpoints, cluster nodes, etc).
- The Management IP address is not in the same network domain as the Instance. The management IP address cannot be programmed into any ESM form. When adding MiVoice Business IP addresses to ESM configuration forms, always use the MiVoice Business System IP address.

## ESM Access Restrictions

Access ESM from either the Management Network or the Customer Network. This is configured on a per-instance basis.

### ESM Access Configured from the Management Network

- Applications on the Customer Network may access MiXML (a HTTP protocol) if the source IP address is included in the whitelist (see “Whitelist Configuration” on page 38).
- Whitelisted customer-side computers will be able to access a limited form of ESM. This ESM usage is not recommended.
- All network traffic that can traverse NAT is supported from the Management Network to the Customer Network, including responses back to the Management Network. (Mitel Data Services API can *not* traverse NAT).
- The ESM reach-through feature is *not* supported when ESM is accessed from the Management Network. Reach-through is supported when all reach-through targets are on the Customer Network.

### ESM Access Configured from the Customer Network

Full ESM access is available to computers in the Customer Network that are on the whitelist.

## Port Restrictions and Whitelist

By default, computers on a Customer Network are blocked from accessing MiVoice Business management TCP ports. Specific customer computers and subnets may be granted access to these blocked ports with a whitelist configuration. All applications requiring MiVoice Business access must be added to the whitelist. IP or network addresses are added to the whitelist on the MiVoice Business Instance details page. See “Whitelist Configuration” on page 38 to configure the whitelist.

> **Note:** All computers residing on the Customer Network that are also listed in the Networks form in the MSL Server Manager (i.e. those computers sharing the same address space) will have full access to restricted MiVoice Business ports. If the computers do not share the same address space, then they should be added to the whitelist. The MiVoice Business Multi-Instance Customer Network restricted ports are ordinarily blocked to all but whitelisted hosts. (The Networks form is found on the MSL Server Manager page in **Configuration->Networks**.)

- The MiVoice Business Console connects to MiVoice Business via TCP port 443, and therefore needs to be added to the whitelist.
- All packets on the Management Network directed to a Management IP address are allowed.
- All packets on the Customer Network directed to the MiVoice Business IP address are allowed, except for the following management ports, which are blocked by default:

  TCP ports 22,23,80,443,8080,8443,1750-1754,2000-2002,15373, which correspond to these protocols:

  - SSH
  - Telnet-call control maintenance1
  - HTTP
  - HTTPS
  - Software logs
  - Maintenance logs
  - SMDR
  - Hospitality logs
  - lpr1
  - Telnet-call control maintenance2
  - Telnet-call control debug
  - Telnet-vxworks
  - ACD logs

These ports can be unblocked for packets sent from an IP address or range of IP addresses listed on a whitelist, which is configurable from the MSL command line.

### Whitelist Configuration

The whitelist is configured on a per-Instance basis, when adding or modifying an Instance. See the *MiVoice Business Multi-Instance Manager Administrator Online Help*. By default, there is no whitelist; if there is no whitelist then all ports are blocked. Use the whitelist to remove Port blocking for a netblock, or an IP address.

## MiVoice Business Routing Restrictions

- The MiVoice Business Instances' default gateway are the Gateway IP addresses specified when configuring MiVoice Business VLAN parameters in the MiVoice Business Multi-Instance Manager Administrator Web interface. This gateway/router provides access to the Customer Network
- The MiVoice Business routing table and ARP cache do not have any IP addresses from the Management Network so it cannot send any unsolicited messages to the Management Network (this is why management IP addresses should not be programmed into MiVoice Business ESM forms). The MiVoice Business is able to respond to clients on the Management Network because these incoming packets are translated at the source using Network Address Translation (NAT).

- Any servers to which the MiVoice Business will initiate connections must be in the Customer Network (or on the Internet, reachable through the Customer Network's gateway). This includes: SNMP traps, email, FTP, Active Directory, IMAP, DNS, SIP Trunk, AMC.

# Chapter 4

## Maintenance and Troubleshooting

# Maintenance

Maintenance involves the following activities:

- Backup MSL to include MiVoice Business Instances
- Upgrade MSL
- Upgrade the MiVoice Business Multi-Instance and Media Server Manager software blades
- Upgrade the MiVoice Business Instances' software load (the MiVoice Business software)
- Backup and restore MiVoice Business Instances
- Upgrade the MSL operating system
- Disaster recovery

## Upgrade the MiVoice Business Multi-Instance Manager and Media Server Manager Blade Software

MiVoice Business Multi-Instance Release 1.2 SP2 renamed the MICD Manager blade to MiVoice Business Multi-Instance blade.

The MiVoice Business Multi-Instance and Media Server Manager blades' upgrade process is straight-forward from the MSL Server Manager. Database information such as the System (Call Server) IP, ARID, etc. is retained in the MSL database during the upgrade process.

A 64-bit version of the MSL Operating System is required for MiVoice Business Multi-Instance. To upgrade from MiVoice Business Multi-Instance on a 32-bit MSL to MiVoice Business Multi-Instance on a 64-bit MSL, refer to Appendix B for the detailed upgrade procedure.

### Upgrade the MiVoice Business Multi-Instance blade

1. Backup the MSL Server upon which the blades reside using the MSL backup facility. See the *Mitel Standard Linux Installation and Administration Guide* for details.
2. Log in to the MSL Server Manager using a browser with the user name and password when initially configuring the MSL server (see "Install the Software Blades: MiVoice Business Multi-Instance and Media Server Manager)" on page 18).
3. Click on **Blades**, located in the left-side panel under the **ServiceLink** heading.

   **Notes:**

   1. There may be two entries when upgrading the MiVoice Business Multi-Instance blade. One will be **MiVoice Business Multi-Instance** with a **Remove** link. The other will be **MiVoice Business Multi-Instance** with an **Upgrade** link. Use the **Upgrade** link for the **MiVoice Business Multi-Instance** blade.
   2. There may be a summary of the status of the currently installed blades. If so, click **Clear Report**.

   Click on the **Upgrade** link associated with the MiVoice Business Multi-Instance blade. The license agreement appears.

**CAUTION:** Do not install or upgrade the MiVoice Multi-instance blade while MiVoice Business instances are starting up. This will cause a disruption in the operation of the MiVoice Business instances. The MiVoice Business instances will then need to be rebooted once the blade installation is completed.

**Note:** The MiVoice Business Multi-Instance blade can be upgraded independently of the MiVoice Business Instances or Media Server instances. The blade upgrade will not affect the instances' operation.

Click **Read text** to read the license terms for the application. If you agree with the license terms, click **Accept all licenses**, or click **Cancel** to exit the blade installation. After accepting all licenses, a progress indicator appears.

4. It may take a few minutes for the software to install.
5. When the blade upgrade is complete an overview of installed components appears.
6. Under **ServiceLink**, click **Status**.
7. Scroll down and click **Sync** to synchronize with the AMC and deliver the ordered licenses.

**Time:** The licensing process may take up to 1-2 minutes.

8. Refresh the browser. The **MiVoice Business Multi-Instance** blade appears under **Applications** in the left-side navigation panel.
9. Click MiVoice Business Multi-Instance to begin configuring the MiVoice Business Instances.

## Upgrade the Media Server Manager blade

1. Backup the MSL Server upon which the blades reside using the MSL backup facility. See the *Mitel Standard Linux Installation and Administration Guide* for details.
2. Log in to the MSL Server Manager using a browser with the user name and password when initially configuring the MSL server (see "Install the Software Blades: MiVoice Business Multi-Instance and Media Server Manager)" on page 18).
3. Stop all Media Server Instances:
   a. Click **Media Server Manager** under **Applications** in the left-side navigation panel.
   b. Go to the Advanced Tab.
   c. Click **Stop** in the **Range Programming** section. A form to stop the Media Server Instances displays.
   d. Enter the total number of Media Server Instances in the **Enter the number of instances to stop** field.
   e. Enter the first Media Server Instance's ID in the **ID of first instance to stop** field.
   f. Click **Next**.

4. If there are more than 25 Media Server Instances and their configured number of audio channels is 64 or higher, change the number of audio channels to 32:

   > **Note:** The number of audio channels can be changed back to their original value after the upgrade. If the upgrade proceeds without changing the number of audio channels to 32, then newly created Media Server Instances may end up sharing audio channels with existing Media Server Instances. To correct this, stop all Media Server Instances as described in Step 3, follow the procedures beginning in Step 4 a below to Modify all Media Server Instances audio channels to 32, then change them back to their original values.

   a. Go to the Dashboard Tab and note the instances that have 64 or more audio channels configured (in the **Audio Channels - Max Permitted** column).

   b. Go to the Advanced Tab.

   c. Click **Modify** in the **Range Programming** section. A form to modify the Media Server Instances displays.

   d. Enter the total number of Media Server Instances in the **Enter the number of instances to modify** field.

   e. Enter the first Media Server Instance's ID in the **ID of first instance to modify** field.

   f. Click **Next**.

   g. Select **100 (32 audio channels)** in the **Maximum Users** drop-down list.

   h. Click **Save**.

   i. For those Media Server Instances that cannot be changed using Range Programming:

      - Go to the Dashboard Tab.
      - Click on the **ID** of the Media Server Instance. The Media Server Instance details page displays.
      - Click **Modify**.
      - Select **100 (32 audio channels)** in the **Maximum Users** drop-down list.
      - Click **Save**.

5. When all Media Server Instances have stopped (check the status on the Dashboard Tab), Click on **Blades**, located in the left-side panel under the **ServiceLink** heading.

6. Click on the **Install** link associated with the Media Server Manager blade. The license agreement appears.

7. Click **Read text** to read the license terms for the application. If you agree with the license terms, click **Accept all licenses**, or click **Cancel** to exit the blade installation. After accepting all licenses, a progress indicator appears.

8. It may take a few minutes for the software to install.

9. When the blade upgrade is complete an overview of installed components appears.

10. Under **ServiceLink**, click **Status**.

11. Scroll down and click **Sync** to synchronize with the AMC and deliver the ordered licenses.

**Time:** The licensing process may take up to 1-2 minutes.

12. Refresh the browser. The **Media Server Manager** blade appears under **Applications** in the left-side navigation panel.
13. Click **Media Server Manager** to begin configuring the Media Server Instances.

## MiVoice Business Instance and Media Server Instance Startup Priority

On an MSL server reboot, all MiVoice Business Instances that were in a running state prior to the server reboot will be started. The default instance startup order is by Instance ID, those with lower ID numbers starting first.

To view the startup order, type the following CLI command in the Linux shell (when logged-in as root):

For the MiVoice Business Multi-Instance, type:
mcdshowstartuporder

For the Media Server Manager, type:
msmshowstartuporder

The resulting output is two columns. The first column is the Instance ID (or Media Server Instance ID), and the second column is the Start Up Priority (startUpPriority).

When the server reboots, the instances associated with the lower startUpPriority values will start first. Instances that have the same startUpPriority value will start in order of Instance ID, with the lower Instance ID starting first.

To change the startup priority, type the following command in the Linux shell (when logged-in as root):

For the MiVoice Business Multi-Instance, type:
mcddb setprop tenant22 startUpPriority 50
where 22 is the ID of the MiVoice Business Instance to modify (see Dashboard ID column in the MiVoice Business Multi-Instance Manager web administration interface).

For the Media Server Manager, type:
msmdb setprop ms22 startUpPriority 50
where 22 is the ID of the Media Server Instance to modify (see the Dashboard ID column in the Media Server Manager web administration interface).

## Upgrade the MiVoice Business Instance software load

When MiVoice Business Instances require upgraded MiVoice Business software loads, it is necessary to obtain the new software load from Mitel Online (MOL), add it to the inventory, and associate it with the appropriate Instance.

> **Note:** Upgrading the MiVoice Business software loads is independent of the MiVoice Business Multi-Instance and Media Server Manager blades.

Bulk MiVoice Business Instance software upgrades can be performed using the embedded Software Installer (SI) Tool. Bulk SI is supported with MCD versions 4.2 SP1 and higher. You may use the bulk tools to upgrade MCD instances to MCD 4.2 SP1.

## Offline Licensing

Upgrading MiVoice Business Instances requires an Internet connection to the AMC for license validation. In situations where the MiVoice Business Multi-Instance server has no Internet connection to the AMC, use the stand alone SI Tool instead to perform the upgrade.

Running the stand alone SI Tool on a laptop to begin the upgrade will cause it to fail and prompt for offline licensing.

For more information on how to complete this task, go to the Mitel Software Installer Tool Online Help (available in product and technical documentation on Mitel Online, http://edocs.mitel.com), and navigate to the Offline Licensing section in the Configuring Licensing Options Selection topic in the Performing The Tasks book. Alternatively, search for "offline" in the online help file.

## Upgrade the MiVoice Business Instance software using the embedded SI Tool

The embedded Mitel Software Installer tool (SI Tool) performs upgrades across a range of MiVoice Business Instances, or for a single Instance.

The target version of the upgraded MiVoice Business software must be in the MiVoice Business Software Inventory.

**CAUTION:** If VLAN Mode is enabled, bulk operations can only be performed if the MiVoice Business Instances are running a minimum software version of MCD 5.0 SP1.

1. Go to the Bulk Tab.
2. Click **Upgrade** in **Range Programming** section.
3. In the **Range of MiVoice Business IDs to do a MiVoice Business Software Upgrade on** area, enter the ID number of the first Instance to upgrade in the **ID** field.
4. In the **Range of MiVoice Business IDs to do a MiVoice Business Software Upgrade on** area, enter the ID number of the last Instance to upgrade in the **through to ID** field.
5. Click **Next**. A page listing the Instances and their status details displays.
6. The **Enter the number of MiVoice Business Instances to do a MiVoice Business Software Upgrade on** and **ID of first MiVoice Business Instance to do a MiVoice Business Software Upgrade on** fields shows the values entered from the previous page.
7. In the **MiVoice Business S/W Version** drop-down list, select a version of MiVoice Business software from the local MiVoice Business software inventory. All Instances listed in the table on this page will be upgraded to the selected version. A MiVoice Business database backup and restore also occurs.
8. If desired, defer the upgrade by selecting the delay time from the **Number of hours to delay the start of this activity** drop-down list.
9. Click **Cancel** to cancel the upgrade.

If any issues are encountered during the upgrade or it fails for any given Instance, the process will continue with the next Instance in the list.

Once the upgrades are complete, check the **Pending Maintenance Activities** list in the Bulk Tab. The upgraded software version numbers will be listed under the **MiVoice Business Version** column.

Cancel any pending bulk operations by clicking **Cancel Pending Activities** in the Bulk Tab.

## Upgrade the MiVoice Business Instance software without the embedded SI Tool

If upgrading from a system not configured with a 64-bit MSL operating system, refer to Appendix B for details.

**CAUTION:** The following upgrade procedure is required only if it is necessary to rebuild/restore an Instance from scratch and will result in a fresh install of the selected software load. The previous contents of the MiVoice Business software load (MiVoice Business file system) will be deleted. Backup the MiVoice Business software load database and voicemail prior to taking this action. Otherwise, it is recommended that the stand-alone (embedded) Mitel SI Tool be used to upgrade the MiVoice Business software load, which will preserving all existing data.

1. Download the upgraded CD image from MOL.
2. Burn a CD for the downloaded image.
3. Backup the MiVoice Business software load (see “Backup and Restore the MiVoice Business Instance software load” on page 48).
4. Add the MiVoice Business software load to the inventory following the procedures described in “Install the MiVoice Business Instance Software” on page 19.
5. Associate the upgraded software load with the appropriate Instance:
   a. Go to the MiVoice Business Multi-Instance blade administration interface.
   b. Go to the Dashboard Tab.
   c. Click on the **ID** or **Name** of the Instance being modified. The MiVoice Business Instance Detail page displays.
   d. Click **Modify** opposite the **Configure this instance** item (near the bottom of the item list).
   e. Select a new version of the software from the **Active MiVoice Business Version** drop-down menu.
   f. Click **Save**.

## Using the Stand-alone Software Installer Tool with MiVoice Business Multi-Instance in VLAN Mode

In VLAN mode, when upgrading the MiVoice Business Instance software using the stand-alone SI Tool on a PC in the Management Network, MiVoice Business instances are unable to initiate network connections to computers on the Management Network.

*To upgrade the MiVoice Business Instance software with MiVoice Business Multi-Instance in VLAN mode:*

1. Launch the SI Tool.
2. In the first screen, under Step 1. Choose the option you would like to perform, select Perform Upgrade.

3. Under the Upgrade Configuration section, select 3300 FTP Server. This allows the software load to be pushed to the MiVoice Business Instance using the Instance's FTP server.

   **CAUTION:** Ensure that this option is selected. Otherwise the software will not upload to the MiVoice Business Instance.

4. Enter the location of the software upgrade in the 3300 Software location field, or Browse to its location. This is the path to a location on the PC that contains the software image for the MiVoice Business Instance being upgraded.

## Upgrade MSL

Upgrading the MSL system involves backing up and restoring the MSL databases (see the *Mitel Standard Linux Installation and Administration Guide* for details).

A 64-bit version of the MSL Operating System is required for MiVoice Business Multi-Instance. To upgrade from MiVoice Business Multi-Instance on a 32-bit MSL to MiVoice Business Multi-Instance Manager on a 64-bit MSL, refer to Appendix B for a detailed upgrade procedure.

**CAUTION:** Upgrading the MSL system will trigger a computer re-boot.

During the upgrade process, you will be prompted to select either *Upgrade existing software* or *Erase all disks and perform a fresh install*. Select *Upgrade existing software* to preserve all applications and data.

**ATTENTION:** For MSL 10.0 to MSL 10.3 upgrades, the CD/DVD method is NOT supported. The only supported methods are: a full install and restore or the Remote Fresh Install (RFI).

Implement a backup plan where a scheduled MSL backup will contain the MiVoice Business Instance backup. MSL has a backup facility that will perform regular backups of the MSL databases and any completed MiVoice Business Instance backups. MSL backups will include the most recent previously created MiVoice Business Instance backup.

**Note:** To prevent a scheduled MSL backup from failing, make sure that it is not scheduled to run at the same time as a scheduled MiVoice Business Instance backup.

Before upgrading MSL on the MiVoice Business Multi-Instance server:

1. Backup the MiVoice Business Instances' software databases (see "Back up the MiVoice Business Software Database" on page 49).
2. Go to the MiVoice Business Multi-Instance Manager Bulk Tab and click **Power Down**. Apply this across the full ranges of MiVoice Business instances on the MiVoice Business Multi-Instance server.
3. Backup the MSL server (see the *Mitel Standard Linux Installation and Administration Guide* for details).
4. Perform a manual backup of the golden database (*.tar*) file and the Configuration Wizard (*.zip*) file.

**Note:** The golden database (*.tar*) file is located in the directory */var/mcdmanager/goldendb*. The Configuration Wizard (*.zip*) file is located in the directory */var/mcdmanager/mn3300configwizard*.

5. When all backup procedures are complete, upgrade MSL and restart all MiVoice Business Instances.
6. Upload the backed up golden database (*.tar*) file using the **Upload Golden DB file** capability on the **Bulk** tab.
7. Upload the backed up Configuration Wizard (*.zip*) file using the **Upload Config Wizard file** capability on the **Bulk** tab.

## Upgrade MSL using Remote Fresh Install (RFI)

On MSL 64-bit systems, a new blade allows the upgrade to MSL Release 10.3 without requiring a hard disk format. MiVoice Business databases and hardware identifiers are preserved when using the RFI 64 blade. Therefore it will not be necessary to clear the MiVoice Business hardware IDs on the AMC. Refer to the *Mitel Standard Linux Installation and Administration Guide* for details.

### *To upgrade MSL using RFI:*

The following procedure is valid for MSL release 9.3.21 and higher, and MiVoice Business Multi-Instance release 1.2 and higher.

Use this procedure when upgrading MSL on the Media Server Manager server also. The only difference would be in backing up the Media Server Instances instead, and installing the Media Server Manager software blade.

1. Backup the MiVoice Business Instances' software databases (see "Back up the MiVoice Business Software Database" on page 49).

   **Time:** Depending on the number of Instances being backed up, this could take a long time.

2. Verify that all of the backups are completed as listed in the Maintenance Activities table in the Bulk tab.
3. *For Media Server instances:*

   Go to the Media Server Manager **Advanced** tab and click **Stop**.

   *For MiVoice Business instances:*

   Go to the MiVoice Business Multi-Instance Manager **Bulk** tab and click **Power Down**. Apply this across the full ranges of MiVoice Business instances on the MiVoice Business Multi-Instance server.

   **ATTENTION:** It is important to ensure that all of the Instances are stopped. Failure to do so will result in, upon completing the upgrade, the Instances initially being Up but transitioning to Down. It would then be necessary to stop and then restart all Instances. When stopping the Instances this way, their status will show "Shutdown pending", without the status ever changing to "Disabled". It is at this point that the Instances can be restarted.

4. Click **Save**.
5. Backup the MSL server (see the *Mitel Standard Linux Installation and Administration Guide* for details).

6. Perform a manual backup of the golden database (*.tar*) file and the Configuration Wizard (*.zip*) file.

> **Note:** The golden database (*.tar*) file is located in the directory */var/mcdmanager/goldendb*. The Configuration Wizard (*.zip*) file is located in the directory */var/mcdmanager/mn3300configwizard*.

7. Install the RFI 64 blade (see the *Mitel Standard Linux Installation and Administration Guide* for details).
8. When the RFI 64 blade installation is complete, reboot the MiVoice Business Multi-Instance server. Two reboots will be observed on the server console.
9. Install the Media Server Manager blade.
10. Start the Media Server instances. See the *Media Server Manager Administrator Online Help*, "Starting a Media Server Instance" topic.
11. Install the new version of the MiVoice Business Multi-instance blade. See “Install the Software Blades: MiVoice Business Multi-Instance and Media Server Manager)” on page 18.
    The MiVoice Business Instances and inventory will be as they were prior to the upgrade.
12. Start the MiVoice Business instances. See the *MiVoice Business Multi-instance Administrator Online Help*, "Starting MiVoice Business Instances" topic.
13. Back up the MiVoice Business Instances. See “Back up the MiVoice Business Software Database” on page 49.
14. Upload the backed up golden database (*.tar*) file using the **Upload Golden DB file** capability on the **Bulk** tab.
15. Upload the backed up Configuration Wizard (*.zip*) file using the **Upload Config Wizard file** capability on the **Bulk** tab.
16. Perform a complete MSL backup for the Media Server Manager and the MiVoice Business Multi-instance Manager (see the *Mitel Standard Linux Installation and Administration Guide* for details).

## Backup and Restore the MiVoice Business Instance software load

A backup and recovery plan will mitigate any potential major outages. One aspect of this plan should include regularly scheduled backups of the MiVoice Business Instance software loads.

The embedded SI Tool is used to perform backups and restores for MiVoice Business Instances.

### Schedule MiVoice Business Instance backups

The backups can be scheduled to occur weekly or monthly. The backup schedule applies to all MiVoice Business Instances. Individual instances can be configured to not have a scheduled backup. All Instances planned and scheduled for backup/restore must be up and running.

> **CAUTION:** If VLAN Mode is enabled, bulk operations can only be performed if the MCD instances are running a minimum software version of MCD 5.0 SP1.

> **Note:** To prevent a scheduled MSL backup from failing, make sure that it is not scheduled to run at the same time as a scheduled MiVoice Business Instance backup.

1. Go to the Bulk Tab.
2. In the **Schedule a recurring backup of the MiVoice Business databases** section select the backup schedule frequency, time, and day.
3. Click **Update**.

## Back up the MiVoice Business Software Database

**Tip:** It is very important to maintain current database backups; backups should be done on a regular basis.

**Note:** The MiVoice Business Software Database was traditionally known as the Mitel 3300 ICP database.

The MiVoice Business Instance database files will be backed up and stored in a local default directory on the MSL server. All Instances planned and scheduled for backup/restore must be up and running. More than one Instance can be backed up at the same time.

**CAUTION:** During a backup, no other users can access any of the MiVoice Business web- based tools (Desktop Tool, Group Administration Tool, or System Administration Tool), or save changes. To avoid blocking other users, we recommended that you perform system backups outside of business hours.

*To backup a single MiVoice Business Instance:*

1. Go to the Dashboard Tab.
2. Click the **ID** or **Name** of the Instance. Ensure that the instance is up and running. The MiVoice Business Instance details page displays.
3. Scroll to near the bottom of the page and click **Backup** opposite **Perform MiVoice Business db Backup**.
4. The correct directory location for the backup files is shown in the **SI Tool db Backup/Restore directory** field.
5. Click **Save**.

MiVoice Business Multi-Instance Manager places the backup files into the specified directory with the following filename format example:

*backup_20100507135848_tenant24_rev_10.1.0.67.tar*, which indicates that the backup was created on 7-May-2010 13:58:48, on MiVoice Business Instance tenant24, that was running MiVoice Business software version 10.1.0.67.

The number of backup files retained for each Instance can be configured. The default is 3.

*To backup more than one MiVoice Business Instance:*

1. Go to the Bulk Tab.
2. The correct directory location for the backup files is shown in the **SI Tool db Backup/Restore directory** field.
3. Click **Backup** in the **Range Programming** section.

4. In the **Range of MiVoice Business IDs to SI Tool Backup** area, enter the ID number of the first Instance to backup in the **ID** field.
5. In the **Range of MiVoice Business IDs to SI Tool Backup** area, enter the ID number of the last Instance to backup in the **through to ID** field.
6. Click **Next**. A page displays listing the MiVoice Business Instances selected for backup.
7. Click **Save**.

## Restore the MiVoice Business Instance Software Database

**CAUTION:** Do not use the MiVoice Business Multi-Instance Restore feature to restore MiVoice Business databases that have modified Dimensions. This affects customers who have modified ESM->Licenses->Dimension to optimize the memory usage of their MiVoice Business. MiVoice Business databases that contain modified Dimensions must be restored via ESM (ESM->Maintenance->Backup/Restore->Restore with "From archived file" selected).

A restore cannot happen unless the MiVoice Business Instance is licensed.

All MiVoice Business Instances planned and scheduled for backup/restore must be up and running.

All corresponding Media Server Instances must be up and running.

The MiVoice Business Instance database files will be restored from the local default directory on the MSL server. More than one Instance can be restored from backup at the same time.

Restoring the MiVoice Business Instance database will result in an automatic reboot of the instance.

**CAUTION:** Service will be LOST during the automatic reboot.

**CAUTION:** During a database restore, no other users can access any of the MiVoice Business web-based tools (5140/5240 IP Appliance Online Services, Desktop Tool, Group Administration Tool, or System Administration Tool), or save changes. To avoid blocking other users, we recommended that you perform system restores outside of business hours.

Progress is reported in the event log.

### *To restore a single MiVoice Business Instance:*

1. Go to the Dashboard Tab.
2. Click the **ID** or **Name** of the MiVoice Business Instance. Ensure that the instance is up and running. The MiVoice Business Instance details page displays.
3. Scroll to near the bottom of the page and click **Restore** opposite **Perform MiVoice Business db Restore**.
4. The correct directory location for the backup files is shown in the **SI Tool db Backup/Restore directory** field.
5. Select the backup file to be restored from the **Previous MiVoice Business db Backup files** drop-down list. The default file is that which was the last backup for the instance.
6. Click **Save**.

7. If the Instance being restored is part of Application Group Licensing, and the Instance is the Designated License Manager (DLM), do the following:
   a. Log into the Instance's MiVoice Business System Administration Tool.
   b. Go to the Application Group Licensing form.
   c. Set the DLM to Yes, by entering the GARID (Group Application Record ID).
   d. Click Save.
   e. Navigate to the Network Element Assignment Form.
   f. Do an SDS Sync among all group members.

*To restore more than one MiVoice Business Instance:*

MiVoice Business Multi-Instance Manager chooses the last backup file for each MiVoice Business Instance from the configured backup directory location.

1. Go to the Bulk Tab.
2. The correct directory location for the backup files is shown in the **SI Tool db Backup/Restore directory** field.
3. Click **Restore** in the **Range Programming** section.
4. In the **Range of MiVoice Business IDs to SI Tool Restore** area, enter the ID number of the first Instance to restore in the **ID** field.
5. In the **Range of MiVoice Business IDs to SI Tool Restore** area, enter the ID number of the last Instance to restore in the **through to ID** field.
6. Click **Next**. A page displays listing the Instances selected for restoring.
7. Click **Save**.
8. If the Instances being restored are part of Application Group Licensing:
   a. Log in to the MiVoice Business System Administration Tool of the Instance that is the Designated License Manager.
   b. Go to the Application Group Licensing form.
   c. Set the DLM to Yes, by entering the GARID (Group Application Record ID).
   d. Click Save.
   e. Navigate to the Network Element Assignment Form.
   f. Do an SDS Sync among all group members.

## Removing a Media Server Blade

Sometimes it is necessary to remove the Media Server Manager blade from a server in order to re-purpose that server. To remove the Media Server Manager software blade:

1. Login to the MSL Server Manager and click **Media Server Manager** under **Applications** in the left-side navigation pane.
2. Stop all media server instances:

a. Go to the Advanced Tab.

b. Click **Stop** in the **Range Programming** section.

c. Enter the total number of media server instances that reside on the server, in the **Enter the number of instances to stop** field. (Click the Dashboard Tab to see the complete list of instances.)

d. Enter the first media server instance ID in the **ID of first instance to stop** field (click the Dashboard Tab to see the instances' ID).

e. Click **Next**.

3. Delete all media server instances:

a. Go to the Advanced Tab.

b. Click **Delete** in the **Range Programming** section.

c. Enter the total number of media server instances that reside on the server, in the **Enter the number of instances to delete** field. (Click the Dashboard Tab to see the complete list of instances.)

d. Enter the first media server instance ID in the **ID of first instance to delete** field (click the Dashboard Tab to see the instances' ID).

e. Click **Next**.

4. Click **Blades**, located in the left-side navigation panel under the **Service Link** heading.

5. Click the **Remove** link in the row listing the **MiVoice Business MediaSvrMgr** blade.

## Disaster Recovery

Disaster recovery scenarios include:

- Computer migration.
- Hard disk replacement.
- Hard disk re-formatting.

Have a backup and recovery plan in place to mitigate any potential major outages.

Implement a backup plan where a scheduled MSL backup will contain the MiVoice Business Instance backup. MSL has a backup facility that will perform regular backups of the MSL databases and any completed MiVoice Business Instance backups. MSL backups will include the most recent previously created MiVoice Business Instance backup.

Go to the Bulk Tab to ensure that the selection from the **Add MiVoice Business instance db backup files to MSL backup** drop-down list is **Yes**. All future Instance backups will be included in the MSL backup archive.

When the MSL backup is complete (which includes the MiVoice Business Instance backup files), copy all of the files to a USB device, or a network location.

> **Note:** MSL supports backup and recovery to and from a file located on a USB device or on a Network Share location.

**CAUTION:** The following procedure supports those MiVoice Business Instances that run in GDM mode. Any Instances running in Classic mode will not be recovered. Instances in Classic mode will need to be restored using the standalone SI Tool, and then subsequently migrate the databases to GDM Mode. See the MiVoice Business System Administration Tool for details. MCD Release 4.0 provided the choice between running in Classic and GDM mode. MCD Release 4.1 and up run only in GDM mode.

**CAUTION:** Do not use the MiVoice Business Multi-Instance Restore feature to restore MiVoice Business databases that have modified Dimensions. This affects customers who have modified ESM->Licenses->Dimension to optimize the memory usage of their MiVoice Business. MiVoice Business databases that contain modified Dimensions must be restored via ESM (ESM->Maintenance->Backup/Restore->Restore with the "From archived file" option selected).

To perform a full system recovery where (at a minimum) the hard disk has been replaced and/or reformatted:

**Note:** The backed-up files can be located on a USB device or on a Network Share location.

1. Ensure all corresponding Media Server Instances are up and running.
2. Attach the USB device containing the MSL (and MiVoice Business Instance) backup files (or retrieve them from the network location) to the server upon which the system is being recovered.
3. Ensure an Internet connection is available and be able to reach mitel.com on port TCP 22.
4. Install MSL (see the *Mitel Standard Linux Installation and Administration Guide*), and indicate that an MSL backup file is available from the USB device (or network location). The MSL server configuration and the MiVoice Business Multi-Instance Manager database will be restored. The MiVoice Business Instance database backup tar files will be restored to their previous location.
5. Install MiVoice Business Multi-Instance Manager (see “Install the Software Blades: MiVoice Business Multi-Instance and Media Server Manager)” on page 18).

   **Note:** When installing MiVoice Business Multi-Instance, select a Blade with the same or higher version as was used to create the MSL backup file. If the MiVoice Business Multi-Instance Blade being installed is from a MiVoice Business Multi-Instance Version older than the MiVoice Business Multi-Instance used when the MSL backup was created, then there may be failures.

   MiVoice Business Multi-Instance will detect that a restore is required (because it has databases describing MiVoice Business Instances but a sanity check revealed that those instances are empty).
   On the MiVoice Business Multi-Instance Dashboard Tab a large warning box displays that indicates a file system restore is required. The MSL Restore populates the MiVoice Business Multi-Instance's database, but does not re-create the MiVoice Business Instance's file system. The warning box will list the steps required to restore the Instances' file system.
6. Add a compatible MiVoice Business software image (see “Install the MiVoice Business Instance Software” on page 19) to MiVoice Business Multi-Instance software inventory.
7. Connect to the AMC, and clear all MiVoice Business hardware IDs.
8. Go to the Bulk Tab.

9. Click **Recover File System** and enter a range of MiVoice Business Instances.

   > **Note:** All existing Instance settings are shown on the Review Tab, particularly those including an ARID. **Recover File System** appears after installation if no MiVoice Business file system exists.

10. Enter the ID of the first and last Instance being restored in the **Range of MiVoice Business IDs to SI Tool Restore** field.
11. In the **MiVoice Business S/W Version** drop-down list, select the version of MiVoice Business software to which all instances will be upgraded. The MiVoice Business database backup file will not be different than that supplied by the MSL restore.
12. Click **Save**.
    The process will then create and license (automatically through the AMC) the MiVoice Business Instances and then restore the respective databases.
    **Recover File System** will disappear from the Bulk Tab after all Instances have been restored.
13. If the Instances being restored are part of Application Group Licensing:
    a. Log in to the MiVoice Business System Administration Tool of the Instance that is the Designated License Manager.
    b. Go to the Application Group Licensing form.
    c. Set the DLM to Yes, by entering the GARID (Group Application Record ID).
    d. Click Save.
    e. Navigate to the Network Element Assignment Form.
    f. Do an SDS Sync among all group members.

## Disaster Recovery for the Media Server

Similar to that of recovering from a disaster of MiVoice Business Multi-instance, ensure that a backup and recovery plan is in place to mitigate any potential major outages.

Implement a backup plan where a scheduled MSL backup will contain the Media Server Instance backup. MSL has a backup facility that will perform regular backups of the MSL databases and any completed Media Server Instance backups. MSL backups will include the most recent previously created Media Server Instance backup.

To recover the Media Server:

1. Install MSL.
2. Reboot the server. A prompt displays at the end of the MSL installation process.
3. Accept the End User License Agreement.
4. Connect to the AMC, and clear all MiVoice Business hardware IDs.
5. Restore the Media Server instances from where they were backed up.
6. Install the Media Server Manager software blade (“Install the Software Blades: MiVoice Business Multi-Instance and Media Server Manager)” on page 18).

# Troubleshooting

## Administration

**Table 1: Administration Troubleshooting**

| Symptom | Possible Cause | Corrective Action |
|---|---|---|
| Some computers, phones, and other gateways cannot access the MiVoice Business Instance. | The MSL firewall restricts access to all applications on the given computer.<br>Not all computers, phones, and other gateways have been configured in MSL to access the MiVoice Business Instance. | 1. Log in to the MSL Server Manager.<br>2. In the left-side navigation pane, click **Networks** under **Configuration**.<br>3. Click **Add Network** to add a network that contains devices that need to access the MiVoice Business Instance.<br>**Note:** For phones behind an MBG (Teleworker), add only the network containing the Teleworker local interface (see step 4 in "Configure MSL for Remote Management" on page 21). |
| System Errors are generated regarding voicemail and greetings. | A Media Server has not been integrated within the MiVoice Business Multi-Instance solution.<br>The MiVoice Business Instance's corresponding Media Server instance has not started and is not providing media services. | Configure the Media Server with it's appropriate MiVoice Business Instance. A delay is expected until the Media Server's connection status is **UP**.<br>Ensure the MiVoice Business ESM voicemail/greeting-related forms properly completed and programmed. |
| Cannot access the MiVoice Business Multi-Instance Manager or MiVoice Business Instance using the standalone Software Installer tool. | The MSL firewall restricts access to all applications on the given computer.<br>Not all computers and other gateways have been configured in MSL to access the MiVoice Business Instance. | 1. Log in to the MSL Server Manager.<br>2. In the left-side navigation pane, click **Networks** under **Configuration**.<br>3. Click **Add Network** add a network that contains devices that need to access the MCD Instance. |
| | Secure Shell (SSH) access has been disabled. | 1. Log in to the MSL Server Manager.<br>2. In the left-side navigation pane, click **Remote Access** under **Security**.<br>3. In the **Secure Shell Settings** area, select the appropriate settings from the drop-down menus to allow access to the computer hosting MiVoice Business Multi-Instance Manager and the MCD Instance. |
| MiVoice Business Instance was not backed up during the MSL backup. | The MiVoice Business Instance was not backed up prior to the MSL backup. | Ensure that the MiVoice Business Instances are backed up in a timely manner to coincide with an MSL backup.<br>Configure the MSL backup to occur after all of the MiVoice Business Instances' backups are completed. It can take several hours for the full set of MiVoice Business Instance backups to complete. |

**Table 1: Administration Troubleshooting**

| Symptom | Possible Cause | Corrective Action |
|---|---|---|
| Media Server Instance is able to get its executable image from MiVoice Business, but is unable to connect to MiVoice Business Instance. | There is another Media Server Instance already connected to this MiVoice Business. This could be the case if there are multiple media server computers and an instance from another media server computer is already connected to that MiVoice Business. Verify this by looking for a media server IP address on the MiVoice Business Instance on the MiVoice Business Multi-Instance Manager. | Decide which Media Server Instance to keep. Only one Media Server Instance can be connected to an MiVoice Business Instance. |
| Voice mail forms do not appear on the corresponding MiVoice Business Instance System Administration Tool. | The corresponding Media Server Instance is not available when the MiVoice Business Instance started up. | Ensure there is a Media Server Instance connected to the associated MiVoice Business Instance.<br>If there is a Media Server Instance connected, then re-start the MiVoice Business Instance. |
| An instance background job (backup, restore, upgrade) is taking a long time. | It may be in a long queue of other jobs. (Check the Maintenance table under the Bulk tab.)<br>Possibly too many instances are installed or need additional RAM. (Verify if this is an issue from tenant's log. Tenant log can be viewed from the tenant's detail info page. Look for a log with "Not enough free memory to launch background job thread".) | If background jobs recover on their own, then there may be no changes required. Intermittent background job memory logs are not a problem.<br>If the memory issue does not clear up on its own, then you can try the following:<br>• If you have more tenants than recommended (see under Advanced tab for max tenant number), then stop some tenants. Background jobs should resume when available memory increases.<br>• If you have upgraded MiVB-MI software and background jobs worked fine before, then you can try lowering the background job free memory threshold. Background jobs should resume, but they may fail. If background jobs fail after lowering the threshold, then you will need to lower the number of tenants or add RAM. You should consult with Mitel Support.<br>Lower the default threshold RAM size required by setting the freeRamThreadThreshold_kB from the server's console as follows:.<br>To change the required free memory threshold to start job to 1000000 kilobytes:<br>config setprop mcddb freeRamThreadThreshold_kB 1000000<br>To return to default free memory threshold, do the following:<br>config delprop mcddb freeRamThreadThreshold_kB |

## VLAN Mode

**Table 2: VLAN Mode Troubleshooting**

| Symptom | Possible Cause | Corrective Action |
|---|---|---|
| Standalone SI Tool fails to complete MiVoice Business s/w Upgrade | The SI Tool is on the Management Network. The MiVoice Business is trying to connect to the stand-alone SI Tool computer to retrieve the upgraded software load. There is network isolation between the Customer and Management Network. MiVoice Business only has access to the Customer Network and cannot reach the server to retrieve the new software load. | Use the MiVoice Business Multi-Instance Bulk MiVoice Business Upgrade features to perform this activity instead of the Standalone SI Tool. |
| Unable to perform 'Retrieve Licenses' function in ESM 'License and Options' form. | MiVoice Business is unable to contact the AMC server on the Internet at sync.mitel-amc.com. Either, there is no Customer Network DNS server configured in ESM, or there is no access to the Internet via the Customer Network. | 1. Verify AMC reachability from ESM as follows: ESM->Maintenance and Diagnostics->Maintenance Commands->command=PING sync.mitel-amc.com.<br>2. Ensure MiVoice Business has Internet connectivity via Customer Network.<br>3. Ensure DNS server programmed in ESM is on Customer Network.<br>4. Go to the MiVoice Business Multi-Instance and Media Server Administrator on-line help, and follow the instructions in the *VLAN Mode and MiVoice Business Configuration Considerations* sub-section in the *Maintenance and Troubleshooting* book.<br>5. Follow the instructions in “Configuration Restrictions” on page 36, and “Management IP Proxy Restrictions” on page 36. |
| MiVoice Business unable to email, SNMP, FTP, SIP trunk. | ESM is not configured on the Customer Network.<br>The destination IP address is not reachable via the Customer Network. | Verify that ESM is configured on the Customer Network.<br>Verify the IP address reachability from ESM as follows:<br>ESM->Maintenance and Diagnostics->Maintenance Commands->command=PING <target IP>. If a domain name (FQDN) is used, verify that MiVoice Business has programmed a DNS server on the Customer Network. |
| Stand-alone SI Tool fails to upgrade MiVoice Business Instance software when in VLAN Mode. | SI Tool not configured properly to push the software to the MiVoice Business Instance. | Ensure 3300 FTP Server is selected in the Upgrade Configuration section in Step 1of the SI Tool. See “Using the Stand-alone Software Installer Tool with MiVoice Business Multi-Instance in VLAN Mode” on page 45 for details. |

**Table 2: VLAN Mode Troubleshooting**

| Symptom | Possible Cause | Corrective Action |
|---|---|---|
| MiVoice Business Instance was not backed up during the MSL backup. | The MiVoice Business Instance was not backed up prior to the MSL backup. | Ensure that the MiVoice Business Instances are backed up in a timely manner to coincide with an MSL backup.<br><br>Configure the MSL backup to occur after all of the MiVoice Business Instances' backups are completed. It can take several hours for the full set of MiVoice Business Instance backups to complete. |
| Computers on the Customer Network that are not on the whitelist have access to MiVoice Business Instance System Administration Tool and other restricted ports. | The computers may be listed in the Networks form on the MSL Server Manager->Configuration page. | Go to the MSL Server Manager page, and navigate to **Configuration->Networks**.<br>Ensure that the computers listed should indeed have access to the MiVoice Business Instance System<br>Administration Tool and restricted ports. |
| Unable to access MiVoice Business Instance System Administration Tool from the Customer Network<br>(including when the whitelist is configured properly). | The MiVoice Business Customer Network gateway/router has been replaced (new MAC address), and MiVoice Business Multi-Instance is in VLAN Mode. Or, the instance was started when there was no gateway router in place. | Restart the MiVoice Business Instance through the Dashboard tab in MiVoice Business Multi-Instance Manager. |

# Appendix A

## IP Address Allocation

# IP Address Allocation

The following is an example of how MiVoice Business Instances' IP addresses can be allocated within the MSL subnet.

> **Note:** The IP address allocation example that follows only applies to MiVoice Business Multi-Instance in non-VLAN Mode.

For Example, if the host MSL server has the following network configuration:

- IP: 10.38.193.2/24
- Gateway: 10.38.193.1,

then the available remaining addresses on this subnet are 10.38.193.3 - 10.38.193.254. A /30 subnet has four IP address, two of which are reserved as the network and broadcast addresses (all 0's and all 1's). There are 62 potential Classless Inter-Domain Routing (CIDR) /30 networks that overlay within the MSL server's IP network. The table below illustrates the addresses available for this example.

| IP Address | Description |
|---|---|
| 10.38.193.0 | Broadcast address |
| 10.38.193.1 | Router |
| 10.38.193.2 | MSL |
| 10.38.193.3 | Spare. This can be used for the Media Server, if decided so by the network administrator. |
| 10.38.193.4 | Network address |
| 10.38.193.5 | Instance MiVoice Business 0 |
| 10.38.193.6 | Reserved |
| 10.38.193.7 | Broadcast address |
| 10.38.193.8 | Network address |
| 10.38.193.9 | Instance MiVoice Business 1 |
| 10.38.193.10 | Reserved |
| 10.38.193.11 | Broadcast address |
| 10.38.193.12 | Network address |
| 10.38.193.13 | Instance MiVoice Business 2 |
| 10.38.193.14 | Reserved |
| 10.38.193.15 | Broadcast address |
| . . . | |
| 10.38.193.252 | Reserved. Can be used for the optional MBG. |
| 10.38.193.253 | |
| 10.38.193.254 | |
| 10.38.193.255 | Broadcast address |

The first /30 subnetwork in the table above is not suitable for MiVoice Business instances because 10.38.193.2 is already used by the MSL host. The last /30 network is not suitable because 10.39.193.255 is the broadcast address of the MSL subnet. The remaining 61 CIDR /30 networks are available for the MCD instances.

> **Note:** If more than 62 MiVoice Business instances are needed, then use a /23 or /22 network. Do not straddle two /24 networks.

In the table above, there is one spare address (10.38.193.3) that can be used for the Media Server, if decided so by the network administrator.

The first available (*not subnet nor broadcast*) IP address in the /30 block should be selected for the MiVoice Business instance System IP address. The MiVoice Business instance System IP address is the address used for ESM web management and the one to which IP Phones connect for signaling. To calculate the System IP of the next MiVoice Business instance, add 4 to the previous MiVoice Business instance's System IP.

> **Note:** When employing resiliency, the redundant MiVoice Business Multi-Instance servers should be on separate subnets to improve availability.

# Appendix B

## MiVoice Business Multi-Instance Blade

## Upgrade to 64-bit MSL

# Upgrading the MiVoice Business Multi-Instance Blade to 64-bit MSL

This section describes the procedure for upgrading the MiVoice Business Multi-Instance Blade to a 64-bit MSL operating system.

This also assumes the following operational parameters:

- MSL v9.1 or v9.2 (32-bit)
- MCD Manager v3.0 or v3.1
- MCD v10.1.1.12

A configuration with more than 32 GB RAM requires the 64-bit MSL version, otherwise the 32-bit MSL version will suffice.

**CAUTION:** The system may become unstable if there is an excess of 32GB RAM on a 32-bit MSL version.

## Scenario 1: Upgrade and remain with 32-bit MSL

1. Stop all MCD instances.
2. Upgrade to MSL 9.2.27.0 32-bit ( "_64" is *not included* in the iso/image name). During the upgrade process, you will be prompted to select either *Upgrade existing software* or *Erase all disks and perform a fresh install*. Select *Upgrade existing software* to preserve all applications and data. See the *Mitel Standard Linux Installation and Administration Guide* for details.
3. Reboot the server.
4. Upgrade to MICD Manager 3.2. See “Upgrade the MiVoice Business Multi-Instance blade” on page 40.
5. Start all MCD instances; indicate that the upgrade is now complete.

## Scenario 2: To upgrade to 64-bit MSL

**Note:** The 64-bit MSL version can be installed on any system, regardless of the amount of RAM installed.

1. Stop all MiVoice Business instances.
   a. Refer to “Disaster Recovery” on page 52, and also in the MiVoice Business Multi-Instance Manager Administrator on-line help (in the *Maintenance and Troubleshooting* section). A pdf formatted copy of the on-line help is available from *PDF Downloads* section of on-line help.
   b. The Mitel AMC must be reachable from this server.
2. Upgrade to MSL 9.2.27.0 32-bit ("_64" is *not included* in the iso/image name). During the upgrade process, you will be prompted to select either *Upgrade existing software* or *Erase all disks and perform a fresh install*. Select *Upgrade existing software* to preserve all applications and data. See the *Mitel Standard Linux Installation and Administration Guide* for details.

3. Reboot the server.
4. Upgrade the MiVoice Business Multi-Instance. See “Upgrade the MiVoice Business Multi-Instance blade” on page 40.
5. Start all MiVoice Business instances; indicate that the upgrade is now complete.
6. Upgrade all Instances to MCD 5.0SP1 (also referenced as release 11.0.1.20).

   **Notes:**

   1. Use the stand-alone SI Tool to do this if upgrading from a version lower than 10.2.1.x. This will take approximately 36 minutes per instance.
   2. For upgrades from MCD 4.1SP1 (10.1.1.12) you can use the new MiVoice Business Multi-Instance Bulk upgrade feature, *only* if MiVoice Business is using the default system/password account.
   3. For upgrades from MCD 4.2 (10.2.0.26) and above you can use the new MiVoice Business Multi-Instance Bulk upgrade feature regardless of the MiVoice Business logon credentials.
   4. Monitor the progress of background bulk jobs in **Maintenance Activities** table at bottom of Bulk Tab in the MiVoice Business Multi-Instance Manager Web Administration tool.
   5. If you are using the new Bulk features then MCD 5.0SP1 must have been added to MiVoice Business Multi-Instance Inventory with MICD Manager 3.3. Otherwise you will get *Unable to find SI Tool* errors. If this is the case, delete and then add MCD 5.0SP1 to MiVoice Business Multi-Instance Inventory.

*The following steps require MCD 5.0SP1.*

7. Go to the Bulk Tab to ensure that the selection from the **Add MiVoice Business instance db backup files to MSL backup** drop-down list is **Yes**.
8. Backup all MiVoice Business instances using the new MiVoice Business Multi-Instance Bulk feature. See “To backup more than one MiVoice Business Instance:” on page 49.
   Wait for backups to complete.
9. Go to the Review Tab to ensure that all MiVoice Business instances have an ARID displayed. If not, perform an AMC Sync by clicking on **ServiceLink** in the left-side navigation panel, then click **Status** in the right-side main page, then scroll down and click **Sync**.
   *Do not proceed to the next step until all MiVoice Business instances are displaying their ARID!*
10. Perform an MSL backup; *this is an important step*. See the *Mitel Standard Linux Installation and Administration Guide*.
    The backup will include MiVoice Business Multi-Instance and all MiVoice Business databases.
11. Verify on the MiVoice Business Multi-Instance Manager Dashboard Tab that the **MiVoice Business Status Table** column **MiVoice Business db in MSL Backup** contains a date for all MiVoice Business instances. This date indicates the MiVoice Business database backup datestamp of MiVoice Business database files included in the MSL backup. If no date is present, then there is no database backup for that instance included in the MSL backup file.
12. Verify the MSL backup. On a Windows computer, expand the backup zip file. Look for the MiVoice Business instance backups in this zip directory `mslserver\home\e-smith\files\mn3300dbbackups` (one file per MiVoice Business instance, for example: `backup_20110412105557_tenant4_rev_10.2.1.13.tar`).
13. Print the MiVoice Business Multi-Instance Server Review panel and note the MSL Service account ID number (ARID) from **MSL ServiceLink–>Blade panel**.

14. Install the MSL 64-bit operating system (see the *Mitel Standard Linux Installation and Administration Guide* for details):

    a. At the AMC, clear hardware id's that are associated with each MiVoice Business and MiVoice Business Multi-Instance Manager ARID.

    b. Perform a fresh install of MSL 64-bit OS. ( _64 *is* included in the iso/image name). Select the option **Erase all disks and perform a fresh install** when presented. *Do not select* **Upgrade existing software**.

    c. After the installation is complete and the system rebooted, you will be asked to restore from backup. Select the option **Yes** to restore MSL from Backup.

    d. Install MiVoice Business Multi-Instance (see “Install the Software Blades: MiVoice Business Multi-Instance and Media Server Manager)” on page 18).
    After installation is complete, you will be told that a file system restore is required.

    > **Note:** It is important that you are using a version of MiVoice Business Multi-Instance that is the same, or newer, than the MiVoice Business Multi-Instance that was used when the MSL Backup file was created. Failure to do so this will result in database incompatibility failures.

    e. Add MCD 5.0SP1 to MiVoice Business Multi-Instance inventory (see “Install the MiVoice Business Instance Software” on page 19).

    f. Go to the Bulk Tab, click **Recover File System** to rebuild the MiVoice Business filesystems. When the system detects that file systems are missing, then **Recover File System** will appear to the right of the Bulk page range programming buttons.

    > **Note:** Progress of background jobs is monitored in the **Maintenance Activities** table near the bottom of the Bulk Tab.

# Appendix C

## VLAN Configuration: Network Access

# Configuring VLAN Network Access

Appendix C is intended for Service Providers who have isolated Customer Networks and a Management Network. Some applications that Service Providers use will require access to MiVoice Business. The level of access available to applications will depend on:

- where the application is placed in the network
- the **ESM Access from Management/Customer Network** MiVoice Business Multi-Instance configuration setting (see “ESM Access Restrictions” on page 37)
- the whitelist (see “Port Restrictions and Whitelist” on page 37)

When MiVoice Business Multi-Instance is configured in VLAN mode, there are certain network access constraints and restrictions. Consider the following general access guidelines:

- Computers on the Customer Network must be on the MiVoice Business whitelist to enable access to MiVoice Business ports.
- Computers on the Customer Network will not have access to MSL or the MiVoice Business Multi-Instance Manager Web Administrative interface.
- Computers on the Management Network will always have full access to MiVoice Business ports through the Management IP NAT. Applications using protocols that are not NAT compatible will not work. The following Mitel protocols are not NAT compatible:
  - MiNet
  - Data Services
  - SDS

The table below shows the network access restrictions for each management interface and each application that is used in a MiVoice Business Multi-Instance VLAN mode deployment.

Use the following legend for the various network access restrictions:

- **EonM / Mgmt**: Management Network access when configuration is ESM access from Management Network.
- **EonC / Mgmt**: Management Network access when configuration is ESM access from Customer Network.
- **EonM / Cust**: Customer Network access when configuration is ESM access from Management Network.
- **EonC / Cust**: Customer Network access when configuration is ESM access from Customer Network.
- **Yes***: A "Yes" indication qualified with an "*" means that access is only available if the client originating the access is configured on the whitelist. For example, the table indicates Yes* for UCA on the Customer Network because MiXML is blocked by default but will have access if the UCA IP address or network is added to the whitelist. On the other hand, the Software Installer (SI)I Tool can never have access from the Customer Network because it needs to communicate with both MiVoice Business and MSL, and it can't reach MSL from the Customer Network.

| Management Interfaces / Applications | EonM Mgmt | EonC Mgmt | EonM Cust | EonC Cust |
|---|---|---|---|---|
| *For this group, note that computers on the Customer Network cannot reach ILOM or MSL/MiVoice Business Multi-Instance web interfaces on the Management Network.* | | | | |
| ISS iLOM Port | Yes | Yes | No | No |
| MSL Secure Shell | Yes | Yes | No | No |
| MSL Secure Copy | Yes | Yes | No | No |
| MSL SNMP Agent | Yes | Yes | No | No |
| MSL SNMP Traps | Yes | Yes | No | No |
| MSL Server-Manager | Yes | Yes | No | No |
| MiVoice Business Multi-Instance Download Logs | Yes | Yes | No | No |
| MiVoice Business Multi-Instance FTP Client - Add Inventory | Yes | Yes | No | No |
| MiVoice Business Multi-Instance Upload MiCW Files | Yes | Yes | No | No |
| *For this group, note that computers on the Customer Network cannot reach ILOM or MSL/MiVoice Business Multi-Instance/Media Server web interfaces on the Management Network. Also, MiVoice Business unsolicited messages (e.g. SNMP traps) cannot reach the Management Network, and Data Services does not work through NAT (e.g. MSPLogs Viewer).* | | | | |
| MiVoice Business ESM Desktop tool/Group Administration Tool | Yes | No | No | Yes |
| MiVoice Business ESM Javalayer System Administration Tool - SDS Reach-Through | No | No | No | Yes |
| MiVoice Business Database Backup | Yes | No | No | Yes |
| MiVoice Business Database Restore | Yes | No | No | Yes |
| MiVoice Business Audio Files Updates | Yes | No | No | Yes |
| MiVoice Business System Diagnostic Report | Yes | No | No | Yes |
| MiVoice Business ESM Import Forms | Yes | No | No | Yes |
| MiVoice Business ESM Export Forms | Yes | No | No | Yes |
| MiVoice Business Audit Trail Logs | Yes | No | No | Yes |
| MiVoice Business Updates to ER-Adviser (unsolicited MiVoice Business messages) | No | No | Yes | Yes |
| MiVoice Business SNMP Agent (client connects to MiVoice Business SNMP port) | Yes | Yes | Yes | Yes |
| MiVoice Business SNMP Traps (unsolicited MiVoice Business messages) | No | No | Yes | Yes |
| MiVoice Business MSPLogs Viewer Application | No | No | Yes | Yes |
| MiVoice Business Maintenance Console port 23 | Yes | Yes | Yes* | Yes |
| MiVoice Business SMDR Logs port 1752 | Yes | Yes | Yes* | Yes |

| Management Interfaces / Applications | EonM Mgmt | EonC Mgmt | EonM Cust | EonC Cust |
|---|---|---|---|---|
| MiVoice Business Software Logs port 1750 | Yes | Yes | Yes* | Yes |
| MiVoice Business Maintenance Logs port 1751 | Yes | Yes | Yes* | Yes |
| MiVoice Business Hospitality Hotel Logs port 1753 | Yes | Yes | Yes* | Yes |
| MiVoice Business LPR1 Output port 1754 | Yes | Yes | Yes* | Yes |
| MiVoice Business ACD Logs port 15373 | Yes | Yes | Yes* | Yes |
| MiVoice Business via standalone SI Tool Application (needs MSL+ESM) | Yes | Yes | No | No |
| MiVoice Business via standalone MiCW Application | Yes | Yes | Yes* | Yes* |
| *For this group, Data Services does not work through NAT (e.g. SDS), and MiVoice Business unsolicited messages (e.g. connect to LDAP server) cannot reach the Management Network.* | | | | |
| MiVoice Business - Exchange SDS Synchronization - Data Services | No | No | Yes | Yes |
| MiVoice Business - IDS LDAP Server Pushes Configs into MiVoice Business | No | No | N0 | Yes |
| MiVoice Business - Designated License Manager ICP Pushes Keys to MiVoice Business Cluster (SDS/Data Services, customer side only) | No | No | Yes | Yes |
| MiVoice Business access by Phones MiNet (customer only due to NAT) | No | No | Yes | Yes |
| MiVoice Business access by MiVoice Business Console Application | No | No | Yes* | Yes* |
| **The following list of Server-Applications reside on a Customer Network.** | | | | |
| *For this group, note that the EonM Mgmt and EonC Mgmt columns are not affected and all marked No, because this group is about MiVoice Business Instances on the Customer Network communicating with application servers also on the Customer Network.* | | | | |
| MiVoice Business access to Domain Controller for IDS Synchronization | No | No | Yes | Yes |
| MiVoice Business access to FTP Server | No | No | Yes | Yes |
| MiVoice Business access to DNS Server | No | No | Yes | Yes |
| MiVoice Business access to SMTP/IMAP Server | No | No | Yes | Yes |
| MiVoice Business access by UCA Server | No | No | Yes* | Yes |
| MiVoice Business access by UCA Clients | No | No | Yes | Yes |
| MiVoice Business access by UCX Clients (PC to phone to MiVoice Business over SAC) | No | No | Yes | Yes |
| MiVoice Business access by MAS UC Mobile | No | No | Yes* | Yes |
| MiVoice Business access by MAS NuPoint | No | No | Yes | Yes |
| MiVoice Business access by MAS Teleworker | No | No | Yes | Yes |
| MiVoice Business access by MAS AWC | No | No | Yes | Yes |

| Management Interfaces / Applications | EonM Mgmt | EonC Mgmt | EonM Cust | EonC Cust |
|---|---|---|---|---|
| MiVoice Business access by MAS Secure Recording Connector | No | No | Yes | Yes |
| MiVoice Business access by MAS CSM | No | No | Yes* | Yes |
| MiVoice Business access by MAS Business Dashboard | No | No | Yes* | Yes |
| MiVoice Business access by MAS End-User-Portal | No | No | Yes* | Yes |
| MiVoice Business ESM access by MAS GUI "Connect to ESM" button | No | No | No | Yes |
| MiVoice Business access by NuPoint Server (MiNet) | No | No | Yes | Yes |
| MiVoice Business access by UIC Sun Ray Server (MiTai) | No | No | Yes | Yes |
| MiVoice Business access by PrairieFyre CCS | No | No | Yes* | Yes |
| MiVoice Business access by MBG for Teleworkers | No | No | Yes | Yes |
| MiVoice Business access by MBG SIP Outbound Proxy | No | No | Yes | Yes |
| MiVoice Business access by MBG Web Proxy Services | No | No | No | Yes |
| MiVoice Business access by MBG GUI "ICP-Test" Button | No | No | Yes | Yes |
| **The Cambrai Server-Application resides on the Management Network (equivalent to ESM access).** | | | | |
| MiVoice Business via Cambrai Oria Portal for Service Provider | Yes | Yes | Yes | Yes |
| MiVoice Business via Cambrai Oria Portal for Company Admin | Yes | Yes | Yes | Yes |
| MiVoice Business via Cambrai Oria Portal for Company Phone Users | Yes | Yes | Yes | Yes |
| *Note that customers could reach Cambrai Portal via their Internet access, which then forwards into the Management Network via the Data Center.* | | | | |