

MiVoice Business

EX Controller Installation and Administration Guide

RELEASE 9.0 and later

October 2021



Notice

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

Trademarks

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

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2021, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	About this Guide	1
	What's new	1
	Related Documents	1
	Contacting Mitel Technical Support	2
 Chapter: 2	 About EX Controller	 4
	Overview	4
	EX Controller Architecture	4
	User Interfaces	6
	Deployment Tool	6
	Server Manager	7
	MiVoice Business System Administration Tool	7
	Mitel Integrated Configuration Wizard	8
	EX Controller Web GUI	9
	Supported Hardware Configuration	10
	Sample Configuration	10
	Optional Accessory	11
	Models and Part Numbers	11
	Specifications	11
	Operating Environment	11
	Storage Temperature	12
	Dimensions and Weight	12
	Connection Interfaces and LEDs	12
 Chapter: 3	 Hardware Installation	 15
	Overview	15
	Package Checklist	15
	Requirements	15
	Location	15
	Wiring	16
	Tools and Equipment	16
	Installation Checklist	16

Cleaning Instructions17
Installing the EX Controller17
Installing Telephony Cards18
Cabling18

Chapter: 4

Software Installation	20
Overview20
PC Requirements20
Prerequisites20
Accessing the EX Controller Deployment Tool21
Updating the EX Controller Deployment Tool22
Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine23
Post-Installation Tasks31
Default Passwords31
Log into Server Manager31
Licensing the MiVoice Business system32
Log into the MiVoice Business System Administration Tool32
Log in to the EX Controller Web GUI34
Program the MiVoice Business System35
Trunk Configuration36

Chapter: 5

Maintenance	38
Software Upgrade38
Prerequisite39
Procedure39
Mount Software Blade on Server Manager Manually39
Backup and Restore40
Backup and Restore Using Server Manager40
Backup and Restore Using MiVoice Business System Administration Tool40

40

Field Replaceable Units41
SSD41
Telephony Cards41
Change IP Address of the EX Controller Web GUI42
Configure the Server Using Server Console43
Accessing Server Console44
Server Console46
Configure this Server47
Manage trusted networks48
Perform backup48
Verifying a Backup File49

Chapter: 6

Troubleshooting	50
System Software50

Reset/Default Button54
Partial Reset54
Factory Reset56
Reset the System Administration Tool Password60
Overview60
Procedure60

Chapter: 7 Appendix A: Assigning a Static IP Address to the EX Controller Deployment Tool
61

Assigning a static IP address manually61
Prerequisites61
Procedure61
Assigning a static IP address by using a USB flash drive68
Prerequisites68
Procedure69

Chapter: 8 Appendix B: Programming an R2 Trunk 70

Programming an R2 trunk70
Customize default settings72

Chapter: 9 Appendix C: Enabling USB Ports for the Deployment Tool 74

Procedure74
---------------------	-----

Chapter: 10 Appendix D - Programming Enterprise Gateway Trunks and Analogue FXS Ports
77

Programming Enterprise Gateway Trunks77
Conditions77
Programming PRI77
Programming FXO78
Programming Analogue FXS Ports79
Programming79

About this Guide

The EX Controller Installation and Administration Guide is intended for certified MiVoice Business technicians who are installing, upgrading, maintaining, and troubleshooting the Mitel® MiVoice Business software deployed on an EX Controller.

What's new

Table 1.1: Issue 0.01

Feature/Enhancement	Document Updates	Location
MIVB-26762/EX I&M needs better section on changing the IP address.	Updated the document with the procedure to change the IP address of the host Mitel EX Platform and the Virtual MiVB running on the Mitel EX .	EX-solution have two different platforms
MIVB-25880/Mitel EX documentation needs to state that VLAN's are not supported.	Added a note to state that VLAN's are not supported.	EX Controller Architecture

Related Documents

Document Title	Description	Location
General Information Guide	Provides an overview of the MiVoice Business system.	Document Center
Troubleshooting Guide	Provides troubleshooting instructions related to MiVoice Business.	Document Center
MiVoice Business Migration Guidelines	Provides guidelines for preparing and migrating your MiVoice Business system to MiVoice Business Release 9.0 or later, or to another platform.	Document Center
EX Controller and GX Gateway Safety Instructions	Provides basic installation information, necessary for the proper and safe functioning of this equipment.	Document Center

Document Title	Description	Location
MiVoice Business Engineering Guidelines	Provides guidelines for planning an installation of a MiVoice Business Communications Platform.	Document Center
MiVoice Business Security Guidelines	Provides guidelines for secure deployment and secure operation of the MiVoice Business (MiVoice Business) system.	Document Center
Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines	Provides information about network cabling and guidelines for twisted pair cabling installation.	Document Center
Mitel IP Sets Engineering Guidelines	Provides guidelines for individuals who are planning for the installation of Mitel IP phones.	Document Center
Network Engineering for IP Telephony	Provides guidelines that should be considered prior to deploying IP phones, such as network design, QoS mechanisms and related protocols.	Document Center

Contacting Mitel Technical Support

Keep the following information handy when you contact the Mitel Technical Support:

- MiVoice Business software version installed or trying to install
- DGW firmware version
- EX Controller Deployment Tool version number or the exdeploy zip file (exdeploy-x.x.x.x.zip) version number
- Product serial number
- Nature of the problem
- What you were doing with the application when the problem occurred
- Troubleshooting results

For information about contacting Mitel Technical Support:

1. Go to [Mitel MiAccess](#), and in the left navigation pane, click **InfoChannel**.
2. In the **Select Infochannel** drop-down, click **Mitel - Worldwide**.
3. In the left navigation pane, click **Services and Support > Support Services**.
4. Under **Support Services**, click **Technical Support**.

5. Under **Technical Support**, click **Contacting Mitel Technical Support**.

The Contacting Mitel Technical Support page is displayed that describes various ways to contact Mitel Technical Support.

About EX Controller

Overview

The EX Controller is a hardware platform that supports the MiVoice Business call processing software. The EX Controller supports up to 1400 IP users and provides analog capabilities of up to 28 Foreign Exchange Subscriber (FXS) or Foreign Exchange office (FXO) ports or 8 T1/E1 ports.

IMPORTANT: The architecture and deployment of the EX Controller is different from MiVoice Business 3300 Integrated Communication Platform (ICP) controllers. Strictly follow the deployment procedures provided in this document to avoid issues with deployment.

EX-solution have two different platforms:

1. **The EX host hardware-** to change the IP address of the host Mitel EX Platform:
 - Log in to the MiVB ESM forms
 - Under **Voice Network** click **Enterprise Gateway**
 - Click Current IP address to get the host Mitel EX platform
 - Click **Change**
 - Enter the new IP scheme in the three advanced fields - **Update IPv4 Address, Update IPv4 Subnet Mask, and Update IPv4 Gateway Address**
 - Click **Save**
2. **The MiVB Virtual Machine** - to change the virtual MiVB running on the Mitel EX:
 - Connect with putty to the current MiVB IP In SSH mode to port 22
 - Login as: admin
 - Password: your MSL server manager password
 - Choose option 2 **configure this server**
 - Make the required changes to the IP config.

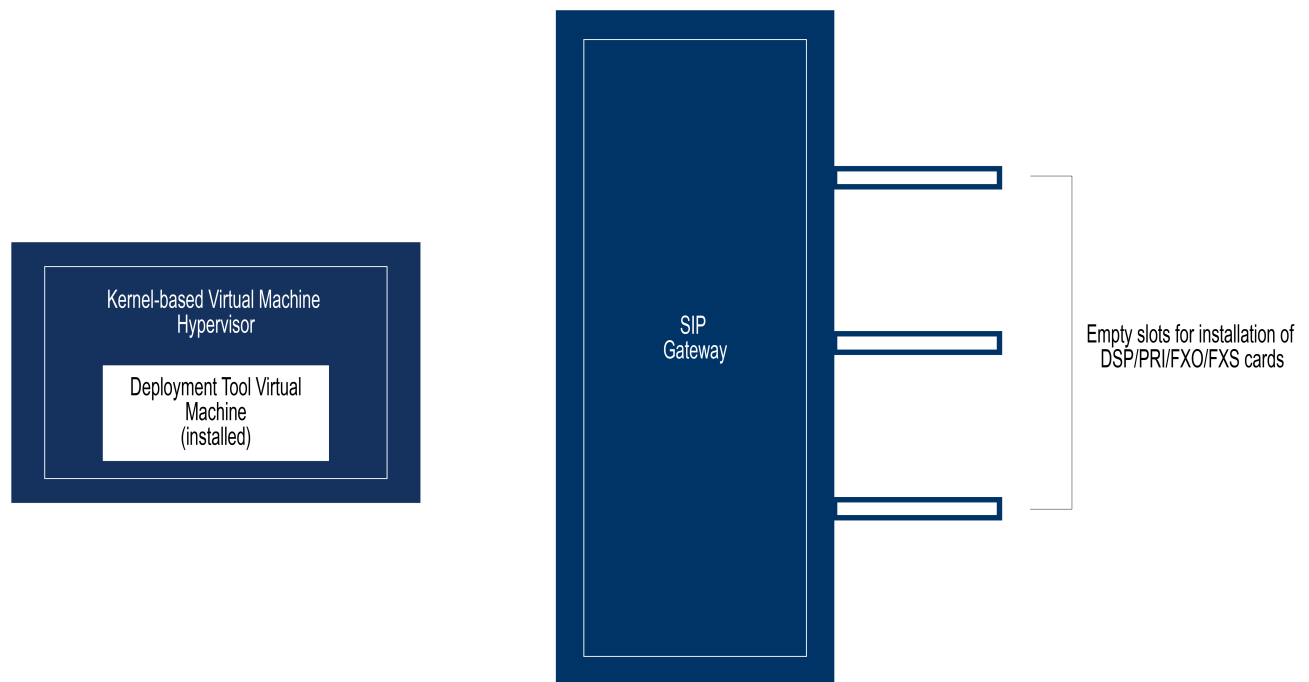
NOTE: Mitel does not recommend making any changes or modifications in the Mitel EX interface unless specifically directed.

EX Controller Architecture

The EX Controller is shipped from the factory with the Deployment Tool installed as a virtual machine on a Kernel-based Virtual Machine (KVM) hypervisor.

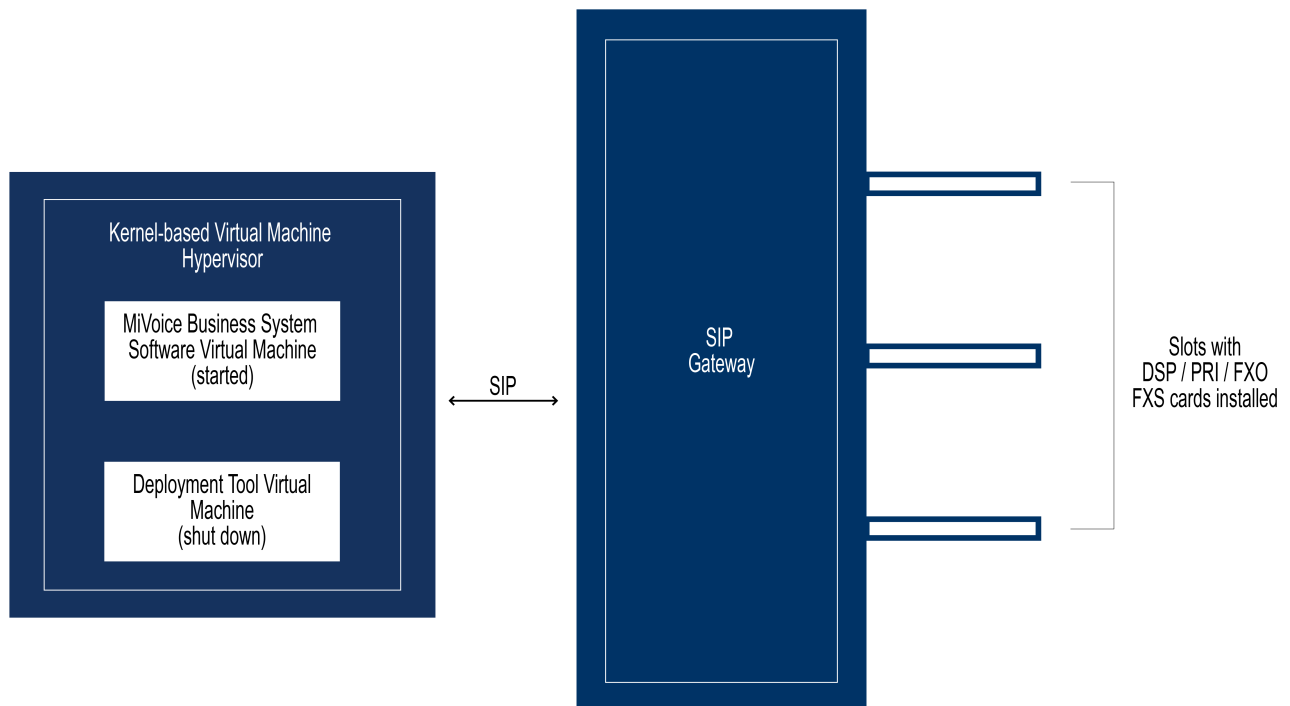
NOTE: As the EX controller does not support 802.1Q VLAN Trunks, the EX controller does not set an 802.1p Ethernet priority. The EX controller will use DSCP information to provide priority information in packets sent at layer 3. However, Ethernet Priority information and VLAN assignment must be configured at the first access port of the Ethernet switch because data will be assigned to an untagged VLAN, which is usually VLAN 1. Voice can be prioritized using the DSCP value, which can also be used to identify the Ethernet priority value set in the DSCP to Priority map in the Ethernet switch. This is also known as QoS to CoS mapping. For more details, contact your LAN switch vendor. For more examples, refer to the [MiVoice Business Engineering Guidelines](#).

The following is a graphical representation of the EX Controller (factory) architecture.



The Deployment Tool is a web-based application that is used for deploying the MiVoice Business virtual machine on the EX Controller.

The following is a graphical representation of the EX Controller architecture after deploying the MiVoice Business system software.



After the deployment, the controller shuts down the Deployment Tool virtual machine and starts the MiVoice Business virtual machine. The MiVoice Business virtual machine provides access to the MiVoice Business system software through a browser-based interface called the MiVoice Business System Administration Tool. The System Administration Tool is used for programming the MiVoice Business system. The SIP Gateway facilitates the communication between PRI/FXO/FXS cards and the MiVoice Business system (call server). For more information about the MiVoice Business system, see the *General Information Guide*.

User Interfaces

The EX Controller has the following user interfaces:

- Deployment Tool
- Server Manager
- MiVoice Business System Administration Tool
- Mitel Configuration Wizard (MiCW)
- EX Controller Web GUI

Deployment Tool

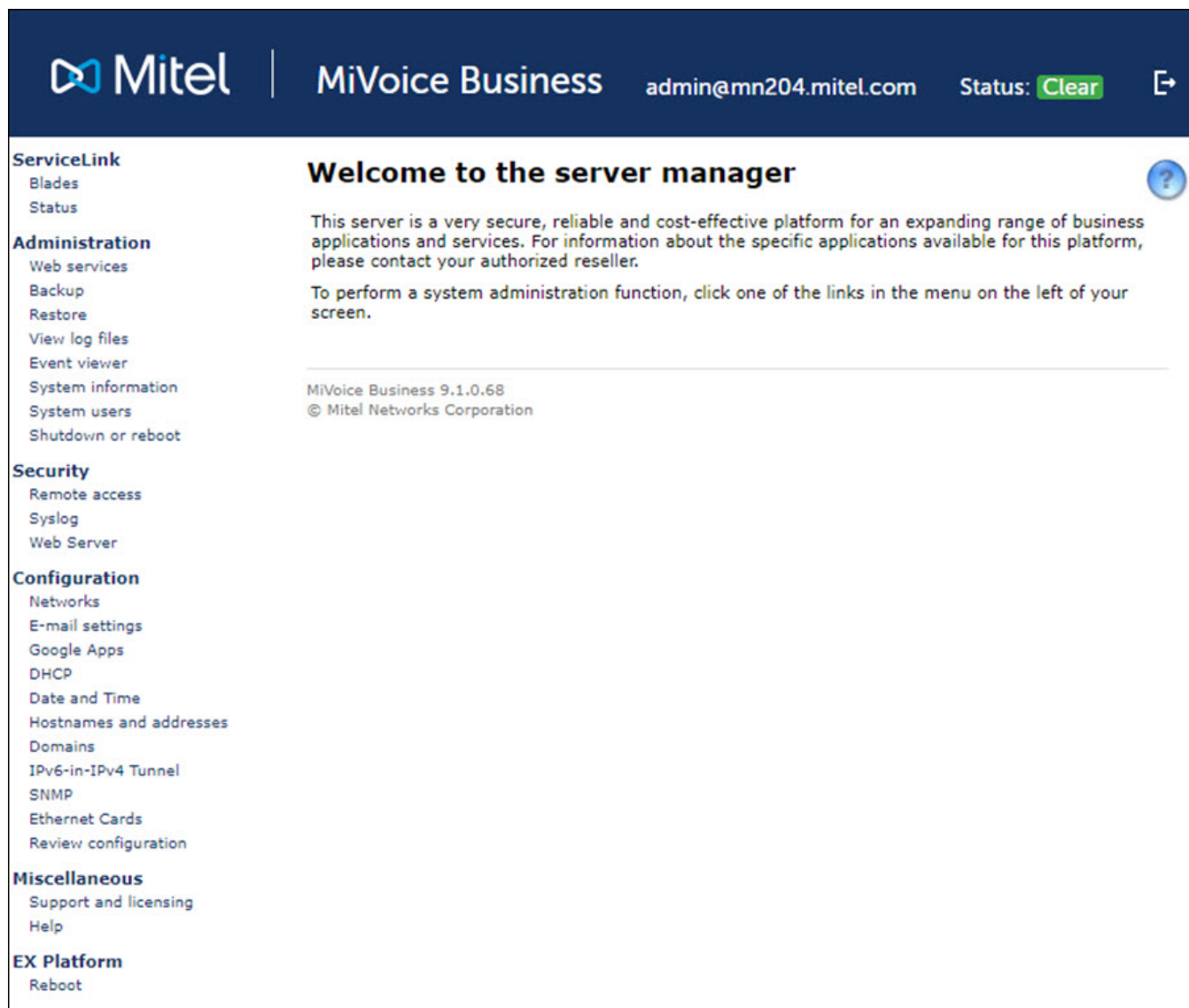
The Deployment Tool is a web-based application that is used for deploying the MiVoice Business system software on the EX Controller. The Deployment Tool is available during the deployment.

The screenshot displays the 'EX Controller Deployment - Deploying' web interface. At the top, there is a header with the Mitel logo, the title 'EX Controller Deployment - Deploying', and links for 'Help', 'Update', and 'Reboot'. Below the header, there are three tabs: 'Recall', 'Progress', and 'Options'. The main content area is divided into two sections: 'Platform variant' and 'General Settings'. In the 'Platform variant' section, there is a dropdown for 'Call Manager type' set to 'MIVB', a 'Call Manager image' field with a 'Choose File' button and 'No file chosen' text, and a 'USB' dropdown. The 'General Settings' section contains several text input fields: 'ARID' (42226716), 'Call Manager FQDN' (ex41.vlab.local), 'Distinguished name' (cn=ex41, ou=R&D, o=Mitel, h=Kanata, st=Ontario, c=CA), 'IPv4 DNS servers' (10.44.17.11, 10.44.17.31), and 'IPv4 trusted network address' (10.0.0.0/8). At the bottom, there are two checkboxes: 'Restore via console' and 'Enable secure EX Controller access', both of which are currently unchecked.

NOTE: Systems running on Deployment Tool older than 1.1.13, must upgrade to the version 1.1.13 or higher and [enable the USB ports manually](#).

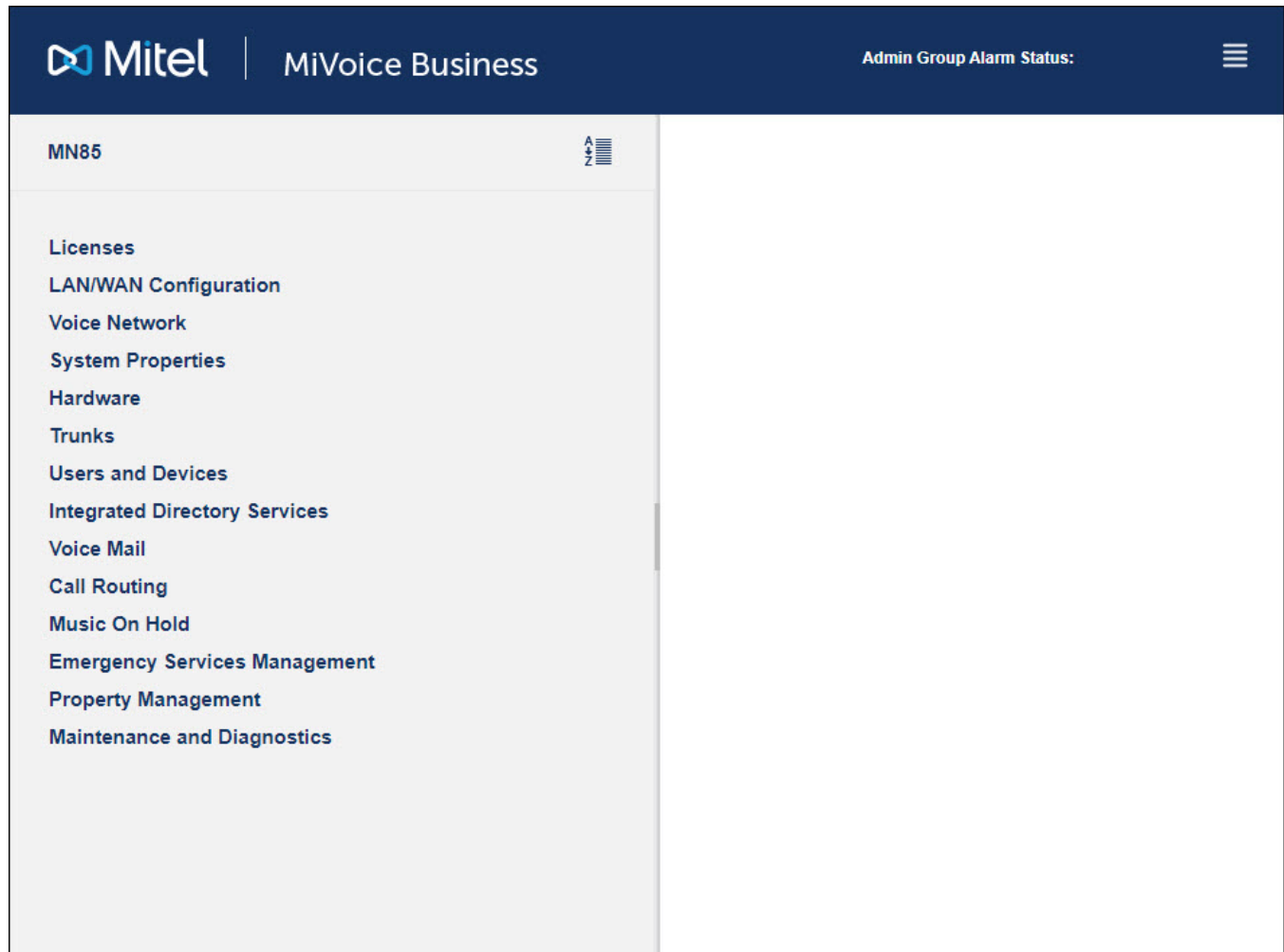
Server Manager

Server Manager is a web-based application that allows you to perform administrative tasks on the MiVoice Business system. Server Manager is available after the deployment.



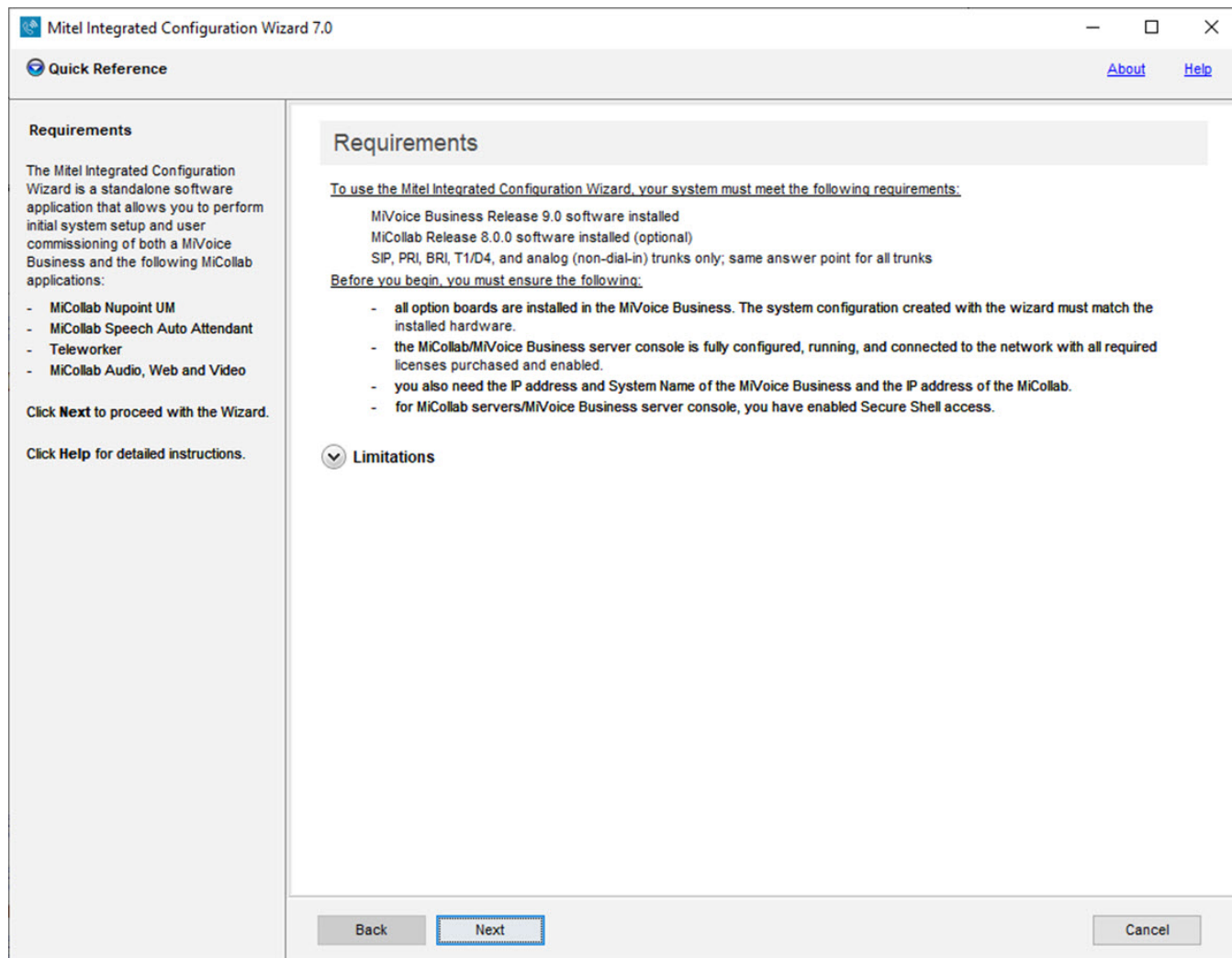
MiVoice Business System Administration Tool

The MiVoice Business System Administration Tool is a web-based application that is used for programming the MiVoice Business system (call programming). The MiVoice Business System Administration Tool is available after the deployment.



Mitel Integrated Configuration Wizard

The Mitel Integrated Configuration Wizard (MiCW) allows you to perform initial system setup and user commissioning of a MiVoice Business platform. The MiCW is available after the deployment.



EX Controller Web GUI

The EX Controller Web GUI is a web-based application that is typically used only for troubleshooting purposes. The EX Controller Web GUI is available after the deployment.

IMPORTANT: Do **NOT** use this interface for programming trunks or the MiVoice Business system.

The screenshot shows the Mitel EX Controller web interface. The top navigation bar includes 'System', 'Network', 'SBC', 'Management', and 'Reboot'. Below this, a secondary navigation bar highlights 'Information' and includes links for 'Services', 'Hardware', 'Event Log', 'Local Log', 'Packet Capture', 'Diagnostic', and 'VM'. The main content area is titled 'Information' and contains three sections: 'Current Status', 'Licences', and 'Activate Licence'.

Current Status	
Device Identification:	EX Controller
Firmware:	Dgw 44.3.1746
Profile:	STNL-MT-D2000-155
MAC Address:	0090f80bdc88
Serial Number:	000400001M318170017
Number of DSPs:	0
Storage Memory (in use/total):	18.3 GB / 60 GB
Volatile Memory (in use/total):	2.3 GB / 8 GB
System Uptime (D:HH:MM:SS):	12:19:04:19
System Time (DD/MM/YYYY HH:MM:SS):	28/11/2019 02:34:15

Licences	
CWMP/TR-069	
SBC Licence for 3 concurrent sessions	
Virtual Machine Licence	

Activate Licence	
Licence Key:	<input type="text"/>

[Apply](#)

Supported Hardware Configuration

The EX Controller has eight slots for accommodating the following cards:

- 1 port PRI (T1/E1) card
- 1 DSP card (required one per chassis when using an FXS or FXO card)
- 4 port FXS card
- 4 port FXO card

Sample Configuration

A sample EX Controller configuration has:

- 2 PRI cards
- 1 DSP card
- 4 FXS cards (providing 16 FXS ports)
- 1 FXO card (providing 4 FXO trunks)

Optional Accessory

A Linux-compatible USB audio is required to support an external Music on Hold source. Mitel recommends using [Pluggable USB Audio Adapter](#). The USB audio can be plugged into, USB1 or USB2 port of the EX Controller.

Models and Part Numbers

The following table describes the supported EX Controller models and their part numbers.

Part Number	Model
50008229	EX Controller with 4 GB RAM and 60 GB storage
50008230	EX Controller with 8 GB RAM, 120 GB storage, and Dual PSU

The following table describes the supported telephony cards for an EX Controller.

Part Number	Telephony Card
50008234	DSP card
50008233	one Port PRI card
50008231	Four Port FXS card, loop limit of 450 m
50008232	Four Port FXO card
51309241	Four Port FXS-LP for EX Controller
50008353	FXO card for Australia

NOTE: The following requirements apply only to Australia:

- FXS wiring cannot be bundled with any network cabling. FXS port wiring must be routed in separate cables away from any network cables.
- The FXO interface is voice only, and does not support FAX or modem.
- The FXS and the FXS-LP (available in Q1 2021) interfaces are installed on-premise only.

Specifications

Operating Environment

- Operating temperature range 0 °C (0 ° F) to +40 °C (104 ° F)
- Humidity maximum 85% and non-condensing

Storage Temperature

-20 °C (-4 °F) to +70 °C (158 °F)

Dimensions and Weight

PARAMETER	DESCRIPTION
Dimensions	Height: 4.4 cm (1.75 in.) Width: 48.3 cm (19 in.) Depth: 36.5 cm (14.4 in.)
Weight	Weight 4.8 kg (10.6 lb.)

Connection Interfaces and LEDs



Table 2.1: LEDs (Sheet 1 of 3)

#	LED	LED State	Description
1	Unit with Power 1 connector only	Green blinking 1 cycle per second, 50% duty	Unit is being restarted.
		Green steady on	Unit is restarted.
		off	No current or failing power supply.
1 and 2	Unit with power 1 and power 2 connectors	Green blinking 1 cycle per second, 50% duty	Unit is being restarted.
		Green steady on	Unit is restarted.
		one LED Red, steady on	No current or failing power supply on the power connector.
		Both LEDs off	No current or failing power supply on both power connectors.

Table 2.1: LEDs (Continued) (Sheet 2 of 3)

#	LED	LED State	Description
3	Ready	Green steady on	All lines are enabled (operational state).
		Green steady off	All lines are disabled (operational state).
		Green blinking 1 cycle per 4 seconds, 75% duty	At least one line is enabled and at least one line is disabled (operational state).
5	In-Use	Off	Lines are idled and unlocked.
		Yellow steady on	Lines are in use and unlocked.
		Yellow blinking 1 cycle per second, 50% duty	Locked
10	Link	Green steady on	Indicates that the PRI port is connected, and the link is up.
		Off	Indicates that the PRI port is not connected, and the link is down.
10	In-Use	Amber steady ON	Indicates that the PRI port is connected.
		Off	Indicates that the PRI port is not connected.
10	Error/Trouble	Red, steady ON	Indicates that the PRI port is not working properly.
		Off	Indicates that the PRI port is working properly.
11	Ready	Amber steady ON	Indicates that the DSP card is ready to send and receive calls.
		Off	Indicates that the DSP card is not connected.
13	ETH1 - Right LED (activity)	Green blinking, variable rate	Connected with active network traffic.
		Green steady on	Connected with no network traffic.
		Off	Not connected

Table 2.1: LEDs (Continued) (Sheet 3 of 3)

#	LED	LED State	Description
13	ETH1 -Left LED (speed)	Off	10 Mbps
		Green	100 Mbps
		Yellow	1000 Mbps
14	ETH2/3/4/5/ext -Right LED (activity)	Green blinking, variable rate	Connected with active network traffic.
		Green, steady on	Connected with no active network traffic.
		Off	Not connected
14	ETH2/3/4/5/ext -Left LED (speed)	Off	10 Mbps
		Green	100 Mbps
		Yellow	1000 Mbps

Table 2.2: Switch

#	SWITCH	DESCRIPTION		
4	Reset/Default	Pressing Duration	Result	LED Pattern
		2 to 6 seconds	entry> PoRestarts the EX Controller unit.	

Hardware Installation

Overview

This chapter describes the following procedures that must be performed sequentially to complete the hardware installation:

1. [Installing the EX Controller](#)
2. [Installing Telephony Cards](#)
3. [Cabling](#)

Package Checklist

Item	Condition
EX Controller (Qty 1)	
Power cord with the proper model for the country (Qty 1) * Qty 2 for EX Controller with dual power supply unit.	
Chassis rack mounting bracket (Qty 2)	
Chassis rack mounting bracket screws (Qty 2)	
Ethernet patch cable, CAT-5E, 7 feet (Qty 1)	
Polyurethane self-adhesive black cylindrical bumper (Qty 1)	
EX Controller and GX Gateway Safety Instructions document (Qty1)	

Requirements

Location

- Install the controller:
 - In a standard 48.26 cm (19 in.) equipment rack
 - On a flat surface (such as a desk or a table)
- Do not install the controller in a location exposed to direct sunlight or near stoves or radiators. Excessive heat could damage the internal components.
- The controller should be positioned to be accessible for future upgrade, maintenance, and troubleshooting and where cables can be easily connected.
- Maintain a minimum of 25 mm (1 in.) clearance in the front, back, on top, under, and on sides of the controller.

- Keep airflow around and through the vents of the controller clear of any obstruction.

Wiring

These guidelines apply Ethernet cables, supplied or not, used with an EX Controller.

- Category 5 cables can be used for 10/100 Base T-Connections.
- Category 5e or 6 cables are recommended for Gigabyte Ethernet.
- Always use straight-through cables.
- Cables must not pull or create a lateral stress on the connectors; that is, they must be long enough.
- Cables must be installed in such a way the personnel working in the vicinity of the equipment do not trip on them.
- Keep cables away from:
 - Sources of electrical noise such as radios, transmitters, and broadband amplifiers
 - Power lines
 - Fluorescent lighting fixtures
 - Liquids or moisture
 - Heat sources

For more information, see *Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines*.

Tools and Equipment

- Screwdriver as required for attaching brackets to rack
- ESD wrist strap
- Earth ground cable
 - WARNING:** The earth ground cable should be the same size (18 AWG minimum) as the earth cable of the provided power cord. Otherwise, make sure the earth ground cable meets the standards and requirements of your local electrical code. The type of the cable is likely to have VW-1 or RT1 markings on the cable.
- RJ45 cables for LAN connections
- RJ48 cables for PRI connections
- RJ11 cables for FXS and FXO connections

Installation Checklist

Task	Verified by	Date
Network information available and recorded in site log.		
Location requirements verified.		
Site power Voltage		
Installation site pre-power check completed.		

Task	Verified by	Date
Mounting tools and equipment available.		
Additional equipment available.		
EX Controller received.		
Regulatory compliance and safety information received.		
Warranty card received.		
Software version verified (download the latest Deployment Tool)		
Rack, desktop mounting of chassis completed.		
Initial electrical connections established.		
Cable length limits verified.		
Initial configuration performed.		
Initial operation verified.		

Cleaning Instructions

To clean an EX Controller, wipe with a soft dry cloth.

CAUTION: Do not use volatile liquids such as benzene or thinner as they can damage the unit's casing.

For resistant markings, wet a cloth with a mild detergent, wring well and then wipe off. Use a dry cloth to dry the surface.

Installing the EX Controller

IMPORTANT: Before installing, ensure that you have read the **EX Controller and GX Gateway Safety Instructions** document supplied with the controller.

To install an EX Controller on a flat surface or in a rack:

1. Make a note or take a picture of your unit's serial number before you begin the installation. The serial number is located underneath the EX Controller casing.
2. Unpack the controller and go through the [Package Checklist](#).
3. Apply the polyurethane self-adhesive black cylindrical bumper protective products to the bottom of the controller. This will improve the airflow under the controller.

NOTE: Skip this step if you are installing the controller in a rack.

4. Install the controller on a flat surface or in a rack, making sure that the unit is at 20 cm (8 in.) from your monitor, computer casing, or other peripheral, including speakers.

Installing Telephony Cards

To install telephony cards:

1. Ensure that adequate earth ground connection has been made between the grounding screw on the back of the controller and an appropriate grounding point in your site.
WARNING: Adequate earth ground connection of the controller is mandatory to avoid any damage or injuries.
2. Wear an ESD wrist strap, ensuring that it makes good contact with bare skin.
3. Attach the ESD wrist strap end to an earth ground (grounding screw on the back of the controller or unpainted bare metal spot of a grounded equipment rack).
4. Turn off the power switch of the controller.
NOTE: Redundant power supply units do not have a power switch.
WARNING: The controller unit must be turned off before adding, removing, or swapping the system cards.
5. Turn off the power sources used to power the controller at the circuit breaker.
6. Disconnect all cables (except the earth ground connection) from the controller.
CAUTION: Power source cables must be disconnected last.
7. Unscrew the two thumb screws of the slot where you want to install or replace a card.
NOTE: Before installing a new card, refer to .
8. Gently remove the blank plate or the existing card.
9. Gently slide the new card into the internal plastic rails of the slot.
NOTE: Insert a blank plate in each unused slot.
NOTE: While sliding in the card, take care not to damage the electronic parts on the card. The card, when properly inserted, slides in easily.
10. Tighten the thumb screws back into place. Do not over-tighten.

Cabling

To connect cables:

1. Wear an ESD wrist strap, ensuring it makes good contact with your bare skin.
2. Attach the ESD wrist strap end to an earth ground (unpainted bare metal spot of a grounded equipment rack).
3. Turn off the power switch of the controller.
NOTE: Redundant Power Supply units do not have a power switch.
4. Make sure the circuit breakers of AC power sources used to power the EX Controller are off.
5. Make sure the provided power cable is connected to the EX Controller and in an appropriate AC electrical outlet.
6. Connect faxes, phones or a PBX to the FXS card.
7. Connect a PBX or ISDN line to the PRI card.

8. Connect a PSTN or a PBX to the FXO card.

Software Installation

Overview

This chapter describes the following procedures that must be performed sequentially to complete the software installation:

1. [Accessing the EX Controller Deployment Tool](#)
2. [Updating the EX Controller Deployment Tool](#)
3. [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#)
4. [Post-Installation Tasks](#)

NOTE: As the EX controller does not support 802.1Q VLAN Trunks, the EX controller does not set an 802.1p Ethernet priority. The EX controller will use DSCP information to provide priority information in packets sent at layer 3. However, Ethernet Priority information and VLAN assignment must be configured at the first access port of the Ethernet switch because data will be assigned to an untagged VLAN, which is usually VLAN 1. Voice can be prioritized using the DSCP value, which can also be used to identify the Ethernet priority value set in the DSCP to Priority map in the Ethernet switch. This is also known as QoS to CoS mapping. For more details, contact your LAN switch vendor. For more examples, refer to the [MiVoice Business Engineering Guidelines](#).

PC Requirements

The following lists the PC requirements for the deployment:

- Linux or Windows operating system
 - Windows 10, Windows Vista (Business or Ultimate), Windows 8 or 8.1
 - Minimum 4 GB RAM for Windows 10; Minimum 2 GB RAM for Windows Vista (Business or Ultimate), Windows 8 or 8.1
- Minimum 4 GB free disk space
- JRE (Java Run-time Environment) 1.6.0_1 or later installed
- Google Chrome or Mozilla Firefox installed.
- Latest version of UltraVNC Viewer application installed.
- WinZip compression software installed (required during debugging)

Prerequisites

- Download the latest **exdeploy-x.x.x.x.zip** file from **Mitel MiAccess > Software Download Center** to your deployment PC.
- Download the EX MiVoice Business software image zip file (**MiVB-9.x.x.x-yy.img.zip**) from **Mitel MiAccess > Software Download Center** to your deployment PC.
- Download the latest Mitel Configuration Wizard (MiCW) executable file (**MICW_7_x_x_x_x_x_-Setup.exe**) from **Mitel MiAccess > Software Download Center** to your deployment PC.

Accessing the EX Controller Deployment Tool

When you connect the EX Controller to a network, the Deployment Tool broadcasts its FQDN `http://exdeploy` to its local subnet through NetBIOS and acquires an IP address from the DHCP server. When the Deployment Tool successfully acquires an IP address, you can access the Deployment Tool using its FQDN `http://exdeploy`.

If there is no DHCP server available on the network, then you must manually assign a static IP address to the Deployment Tool. For more information, see [Appendix A: Assigning a Static IP Address to the EX Controller Deployment Tool](#).

WARNING: Make sure that you turn on and connect only one EX Controller to the network. If you connect more than one EX Controller to the network, then you might not know which controller you are connected to.

To access the Deployment Tool:

1. Enable NetBIOS over TCP/IPv4 on your deployment PC.
2. Ensure that the PC and the EX Controller are connected to the same subnet.
3. Connect an RJ45 Ethernet cable from any one of the **ETH2 - ETH5** ports of the EX Controller to the Layer2 switch on the network.
4. Turn on the EX Controller.

The Power LED will be flashing when the unit performs a DHCP server query. It will become solid once it successfully gets an IP address from the DHCP server. At this point, you can use the domain name (`exdeploy.local` or `exdeploy`) to access the Deployment Tool.

5. Enter **`http://exdeploy`** in the address bar of your web browser (recommended Mozilla Firefox and Google Chrome) to access the Deployment Tool.

The EX Controller Deployment Tool home page is displayed.

The screenshot shows the web interface of the EX Controller Deployment Tool. At the top, there is a dark blue header with the Mitel logo on the left, the title "EX Controller Deployment - Deploying" in the center, and links for "Help", "Update", and "Reboot" on the right. Below the header, a status bar indicates "Idle - No existing deployment session" and version "v1.1.13-0". A navigation bar contains three buttons: "Recall", "Progress", and "Options". The main content area is divided into two sections. The "Platform variant" section includes a "Call Manager type" dropdown menu set to "MIVB", a "Call Manager image" section with a "Choose File" button and the text "No file chosen", and a "USB" dropdown menu. The "General Settings" section includes an "ARID" text field with the value "42226718" and a "Call Manager FQDN" text field with the value "ex41.vlab.local".

NOTE: The **USB** list is available with Deployment Tool versions 1.1.13 and later. To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#).

- Continue with [Updating the EX Controller Deployment Tool](#).

Updating the EX Controller Deployment Tool

After you access the Deployment Tool, you must update the Deployment Tool.

To update the Deployment Tool:

- In the Deployment Tool home page, click **Update**.

NOTE: Updating the Deployment Tool upgrades the DGW firmware also.

Platform variant

Call Manager type: MIVB

Call Manager image: No file chosen

USB:

General Settings

ARID: 42226718

Call Manager FQDN: ex41.vlab.local

Distinguished name: cn=ex41, ou=R&D, o=Mitel, l=Kanata, st=Ontario, c=CA

IPv4 DNS servers: 10.44.17.11, 10.44.17.31

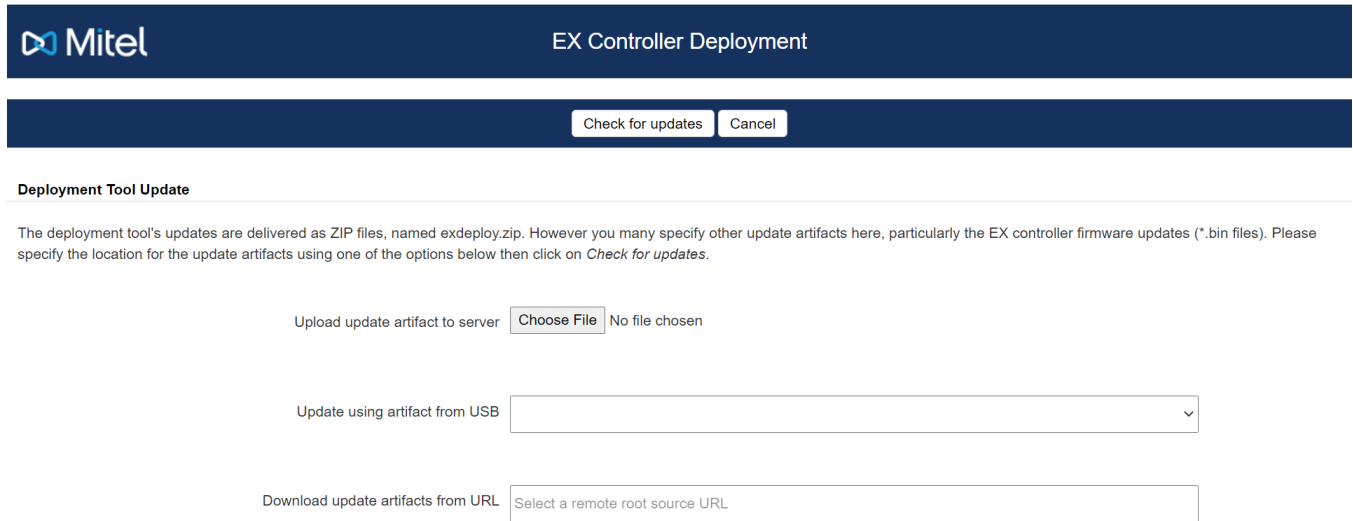
IPv4 trusted network address: 10.0.0.0/8

Restore via console: ☐

Enable secure EX Controller access: ☐

NOTE: The **USB** list is available with Deployment Tool versions 1.1.13 and later. To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#).

- Do either of the following:



The screenshot shows the 'EX Controller Deployment' window. At the top is the Mitel logo. Below it is a dark blue bar with the title 'EX Controller Deployment'. Underneath is a light blue bar containing two buttons: 'Check for updates' and 'Cancel'. The main content area is titled 'Deployment Tool Update'. It contains a paragraph explaining that updates are delivered as ZIP files and that users can specify other update artifacts. Below this are three options for updating: 'Upload update artifact to server' with a 'Choose File' button and 'No file chosen' text; 'Update using artifact from USB' with a dropdown menu; and 'Download update artifacts from URL' with a text field for a remote root source URL.

- Click **Choose File**, and select the **exdeploy-x.x.x.x.zip** file.
- In the **Update using artifact from USB** list, select the **exdeploy-x.x.x.x.zip** file.

NOTE: The **Update using artifact from USB** list is available with Deployment the Tool versions 1.1.13 and later. To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#).

3. Click **Check for updates**.

If an update is available, the system updates the Deployment Tool. The **Progress** window displays the progress of the update. Verify the update by checking the version number displayed on the top-right corner of the Deployment Tool home page.

Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine

After you update the Deployment Tool, use the Deployment Tool to install the MiVoice Business system software as a virtual machine on the EX Controller.

NOTE: If the deployment fails due to interruptions, such as a power or network outage, you must restart the deployment procedure.

The Deployment Tool supports two modes of deployment to complete the installation, **Full** and **Partial + Finish**.

Full deploy

The *full deployment mode* allows you to deploy the MiVoice Business system software in a single procedure. After a full deployment, the controller starts the MiVoice Business virtual machine and shuts down the Deployment Tool virtual machine.

Partial + Full deploy

The *partial + finish deployment mode* allows you to complete the deployment in two phases.

In the first phase, the EX Controller is partially deployed. That is, after a partial deployment, the Deployment Tool virtual machine continues to run, and the MiVoice Business virtual machine is shut down. Partial deployment allows you to review and modify certain configuration parameters before you finish the deployment later.

In the second phase, you can review and modify certain configuration parameters, and then finish the deployment.

After you finish the deployment, the controller starts the MiVoice Business virtual machine and shuts down the Deployment Tool virtual machine.


To run the EX Controller Deployment Tool to install the MiVoice Business virtual machine:

NOTE: Only the fields on the EX Controller Deployment home page are required for typical installations. It is recommended that you do **NOT** modify the fields displayed under the **Options** button.

EX deployment options

Call Manager source URL	<input type="text" value="Enter the URL from which the Call Manager image"/>
Deployment private address	<input type="text" value="169.254.10.1"/>
Local address	<input type="text" value="169.254.10.2"/>
VNC display	<input type="text" value="1"/>
Number of cores	<input type="text" value="3"/>
Storage capacity	<input type="text" value="32"/>

1. Under **Platform Variant**, in the **Call manager** list, select **MiVB**.


EX Controller Deployment - Deploying
Help | Update | Reboot
v1.1.13-0

Recall
Progress
Options

Platform variant

Call Manager type
MIVB

Call Manager image
Choose File
No file chosen

USB

General Settings

ARID
42226718

Call Manager FQDN
ex41.vlab.local

Distinguished name
cn=ex41, ou=R&D, o=Mitel, l=Kanata, st=Ontario, c=CA

IPv4 DNS servers
10.44.17.11, 10.44.17.31

IPv4 trusted network address
10.0.0.0/8

Restore via console
☐

Enable secure EX Controller access
☐

2. Do either of the following:

- If you have the **MiVB-9.x.x.x-yy.img.zip** file on your local PC, click **Choose File**, and select the **MiVB-9.x.x.x-yy.img.zip** file.
- In the **USB** list, select the **MiVB-9.x.x.x-yy.img.zip** file.

NOTE: The **USB** list is available with the Deployment Tool version 1.1.13 or later. The EX Controllers procured in MiVoice Business Release 9.2 or later have the Deployment Tool version 1.1.13 pre-installed. For more information on how to use the **USB** list, see [Assigning a static IP address by using a USB flash drive](#). To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#).

3. Under **General Settings**, enter the following details:

- **ARID** — The Application Record ID (ARID) for the MiVoice Business system to acquire and register licenses with the Mitel Application Management Center (AMC). Optionally, you can license the system after the deployment through Server Manager.
- **Call Manager FQDN** — The FQDN of the MiVoice Business virtual machine. For example, `coyote.acme.com`, where **coyote** is the hostname and **acme.com** is the domain name (resolvable by the **IPv4 DNS** server listed below)

- **Distinguished name** —The Distinguished Name (DN) of the MiVoice Business virtual instance that is used to create a host certificate for the controller. For example, cn= coyote, ou= Research and Development, o= Acme Company, l= Bangor, st= Maine, c= US. Leave the field as is.

NOTE: The hostname of the MiVoice Business system specified in the **Call Manager FQDN** field must match the cn of the **Distinguished Name** field for the certificate generated during the deployment.

- **IPv4 DNS servers** — The IPv4 address of one or more DNS servers of the network where the EX Controller is installed; comma-separated in case of multiple DNS servers.
- **IPv4 trusted network address** — The IPv4 address of the management networks or trusted networks from which you want to allow access to the MiVoice Business System Administration Tool and the Server Manager by generating a certificate for HTTPS use.

4. (Optional) Select the **Restore via console** check box, if you want to enable restore via server console option after the deployment. The Server Manager prompts the user to restore the system configuration upon startup.

NOTE: The controller does not support the **Restore from another running server** option.

5. Select **Enable secure EX controller access** to disable the SNMP v2 protocol on the EX Controller. This blocks unsecure access to the controller.

It is recommended to leave the check box cleared to configure the MiVoice Business system using the Mitel Configuration Wizard (MiCW) post deployment.

6. Leave the following **WAN Settings** blank unless you are setting up a WAN configuration for the EX Controller:

The screenshot shows a configuration interface with two main sections: **WAN Settings** and **LAN Settings**. Each section contains three input fields for IPv4 addresses. The WAN section has placeholder text 'Enter an IPv4 address/CIDR' for the EX Controller, 'Enter an IPv4 address' for the Call Manager, and 'Enter an IPv4 address' for the default gateway. The LAN section has pre-filled values: '10.37.27.80/24' for the EX Controller, '10.37.27.81' for the Call Manager, and '10.37.27.1' for the default gateway. At the bottom, there are three buttons: 'Full deploy', 'Partial deploy', and 'Finish deploy'.

Section	Field	Value
WAN Settings	IPv4 EX Controller WAN address	Enter an IPv4 address/CIDR
	IPv4 Call Manager WAN address	Enter an IPv4 address
	IPv4 default WAN gateway	Enter an IPv4 address
LAN Settings	IPv4 EX Controller LAN address	10.37.27.80/24
	IPv4 Call Manager LAN address	10.37.27.81
	IPv4 default LAN gateway	10.37.27.1

Buttons: Full deploy, Partial deploy, Finish deploy

- a. **IPv4 EX Controller WAN address**
 - b. **IPv4 Call Manager WAN address**
 - c. **IPv4 default WAN gateway**
7. Under **LAN Settings**, specify the IPv4 LAN settings:
 - a. **IPv4 EX Controller LAN address** — IPv4 address with CIDR for the EX Controller Web GUI that will overwrite the default IP address of the EX Controller Web GUI, 192.168.0.10. For example, 10.211.13.42/12.
 - b. **IPv4 Call Manager LAN address** — IPv4 address for the MiVoice Business system virtual machine. (No CIDR is required)
 - c. **IPv4 default LAN gateway** — IPv4 default LAN gateway address
8. If you want to perform a **partial + finish** deploy, skip this step and proceed to step 10. If you want to deploy and enable the MiVoice Business virtual machine immediately, click **Full deploy**.

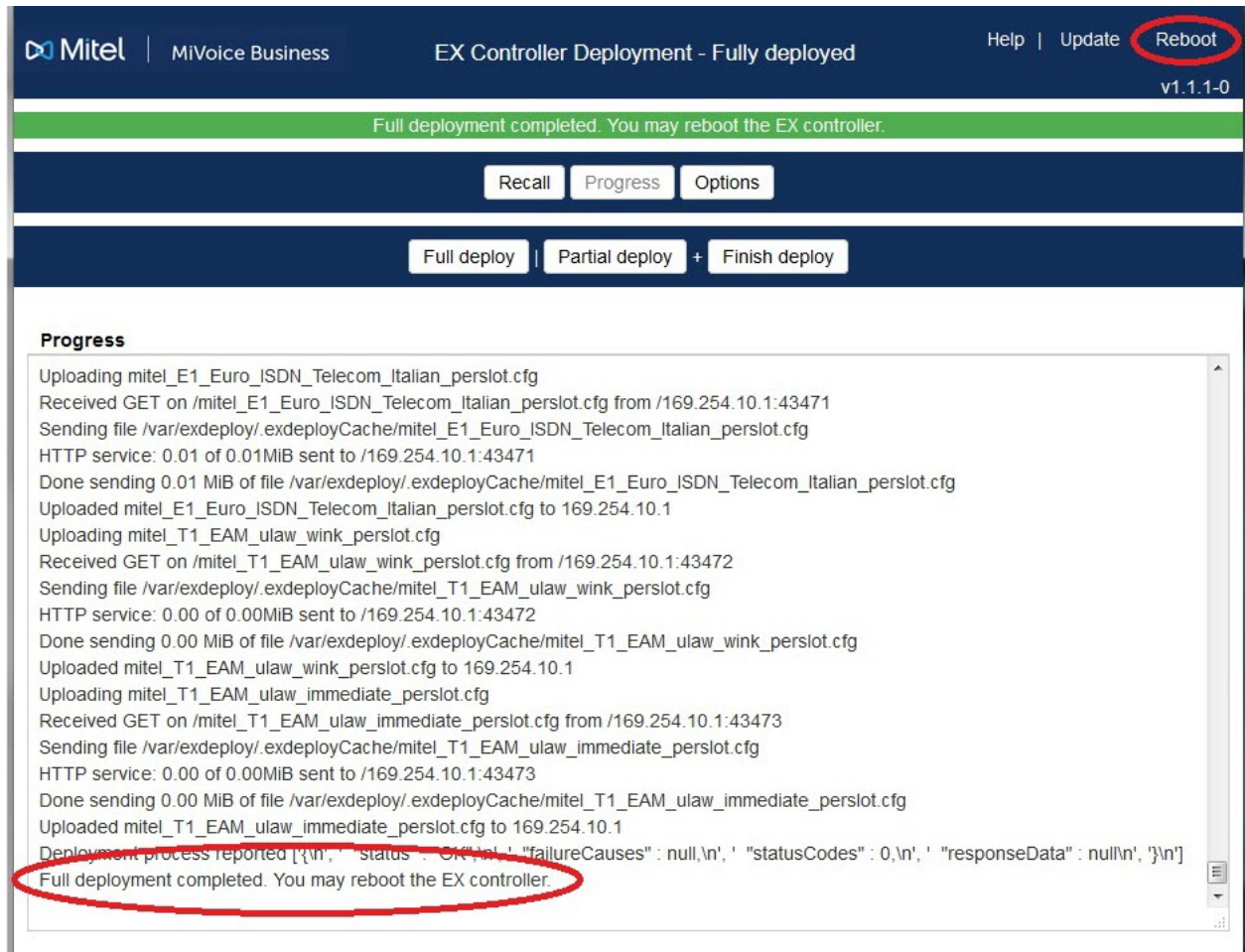
A confirmation message is displayed.

- a. Click **OK** to confirm the deployment.

NOTE: Ignore the warning message about FQDN. For example, “FQDN coyote.acme.com is not resolvable”.

The system starts the full deployment process. It takes approximately 25 minutes to complete the deployment. When the deployment is complete, the following message is displayed.

“Full deployment completed. You may reboot the EX controller.”



b. Continue with [step 11](#).

9. If you want to deploy now but configure and enable the MiVoice Business virtual machine later, click **Partial deploy**.

A confirmation message is displayed.

- a. Click **OK** to confirm the deployment.

NOTE: Ignore the warning message about FQDN. For example, “FQDN coyote.acme.com is not resolvable”.

The system starts the partial deployment process. It takes approximately 25 minutes to complete the deployment.

- b. After the partial deployment, if required, power off the EX Controller, and finish the deployment later.
- c. When you want to enable the MiVoice Business virtual machine, [access the Deployment Tool](#). If you have already accessed the Deployment Tool, continue with the next step.
- d. If required, click **Recall** to go back to the Deployment Tool home page to review and modify **General Settings**, **WAN Settings**, and **LAN Settings**.

NOTE: You can modify only **General Settings**, **WAN Settings**, and **LAN Settings**. Other configuration parameters are blocked for modification.

- e. Click **Finish deploy**.

A confirmation message is displayed.

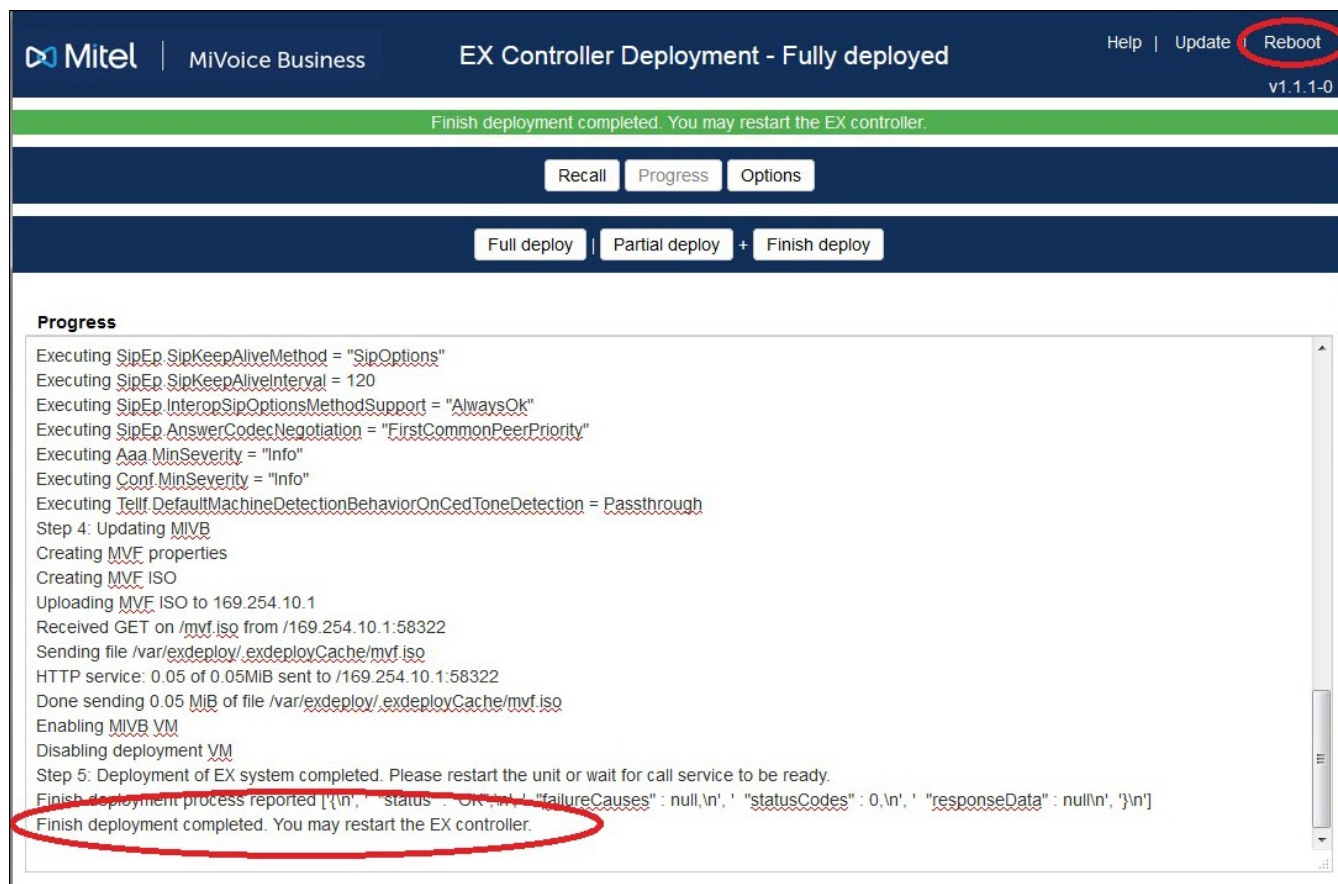
- f. Click **OK** to confirm the deployment.

NOTE: Ignore the warning message “FQDN coyote.acme.com is not resolvable”.

The system starts to finish the deployment. It takes approximately 2 minutes to finish the deployment.

- g. When the deployment is complete, the following message is displayed.

“Finish Deployment Completed. You may restart the EX controller.”



- h. Continue with [step 11](#).

10. Click **Reboot** to restart the EX Controller.

It takes approximately 20 minutes for the EX Controller to boot the first time. Subsequent reboots are faster.

After the reboot, the Deployment Tool virtual machine shuts down and MiVoice Business virtual machine starts automatically.

11. Ensure that you have the system on the correct network for the new IP addresses as configured during the deployment process.
12. If you have inserted the USB flash drive, remove the USB flash drive from the EX Controller.

Post-Installation Tasks

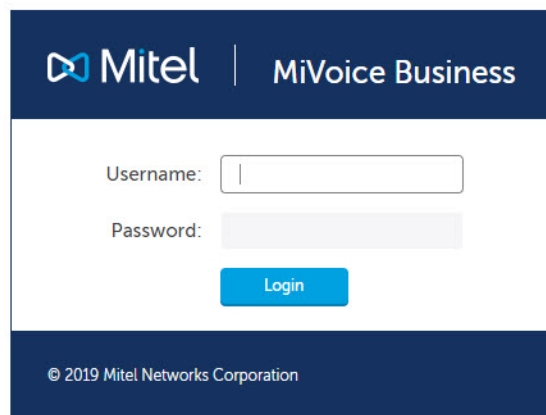
Default Passwords

The default user names and passwords to be used after the deployment are as follows:

- The default user name for the Server Manager user accounts is **admin** and **root** and the default password is **default1**.
- The default user name for the System Administration Tool user account is **system** and the default password is **password**.
- The default user name for the EX Controller Web GUI user account is **public**. There is no default password.

Log into Server Manager

1. Log into Server Manager by entering **<IPv4 Call Manager LAN address>/server-manager** in the address bar of your web browser.
The Server Manager login page is displayed.



2. Type the default **Username** (admin) and **Password** (default1).

You are prompted to change the password. The new password must have at least eight characters consisting of:

- an upper case letter
- a lower case letter
- a number
- a non-alphanumeric character

For more information on password quality requirements, refer to the Help page associated with the Password Requirements tab in the Administration > System users page on Server Manager.

NOTE: The modified password is also applied as the SNMP v3 privacy password, the EX Controller Web GUI password, and the System Administration Tool mimx account password. However, if the new password does not conform with the minimum eight-character rule, it does not get synchronized. For information about troubleshooting the password synchronization issue, see [Unable to log into the EX Controller Web GUI as mimx user after a password reset using Server Manager](#).

Licensing the MiVoice Business system

If you did not specify the ARID during the deployment, license the MiVoice Business system using Server Manager (**ServiceLink > Status**).

1. [Log into Server Manager](#).
2. Navigate to **ServiceLink > Status**.
3. In the **Service account ID** field, enter the Application Record ID (also called Service account ID).
4. If the Internet is accessed via a proxy, enter:
 - Address of proxy
 - TCP port used to connect to proxy. The proxy server must be configured to forward TCP packets on the incoming port to the AMC address (sync.mitel-amc.com) on port 22.
5. Click **Activate** to synchronize with AMC and activate ServiceLink.

Following successful activation, Server Manager periodically reconnects to the AMC (every 24 hours by default) via a secure, encrypted connection to synchronize ServiceLink status information. New configuration instructions, such as services you have added or deleted to your AMC account, are updated at this time.

Log into the MiVoice Business System Administration Tool

1. Log into the MiVoice Business System Administration Tool by entering **<IPv4 Call Manager LAN address>** in the address bar of your web browser.
The System Administration Tool login page is displayed.



 A login form with two input fields: "Login ID" and "Password". Below the "Password" field is a checkbox labeled "Remember Login ID". A blue "Log In" button is positioned to the right of the checkbox. Below the button, there are two links: "Install MiVoice Business Certificate" and "Enable pop-ups".

2. The first time you connect, you must install the MiVoice Business certificate.

Chrome and Edge

To install the MiVoice Business certificate:

- a. On the login page, click **Install MiVoice Business Certificate** and follow the instructions provided to install the certificate.

Firefox

To install the MiVoice Business certificate:

- a. Start a System Administration Tool session by connecting to the MiVoice Business system.
- b. Click **I Understand the Risks** followed by **Add Exception...**
- c. Clear the **Permanently store this exception** check box, and then click **Confirm Security Exception**.
- d. Once you confirm the exception, the System Administration Tool Login page will be displayed.

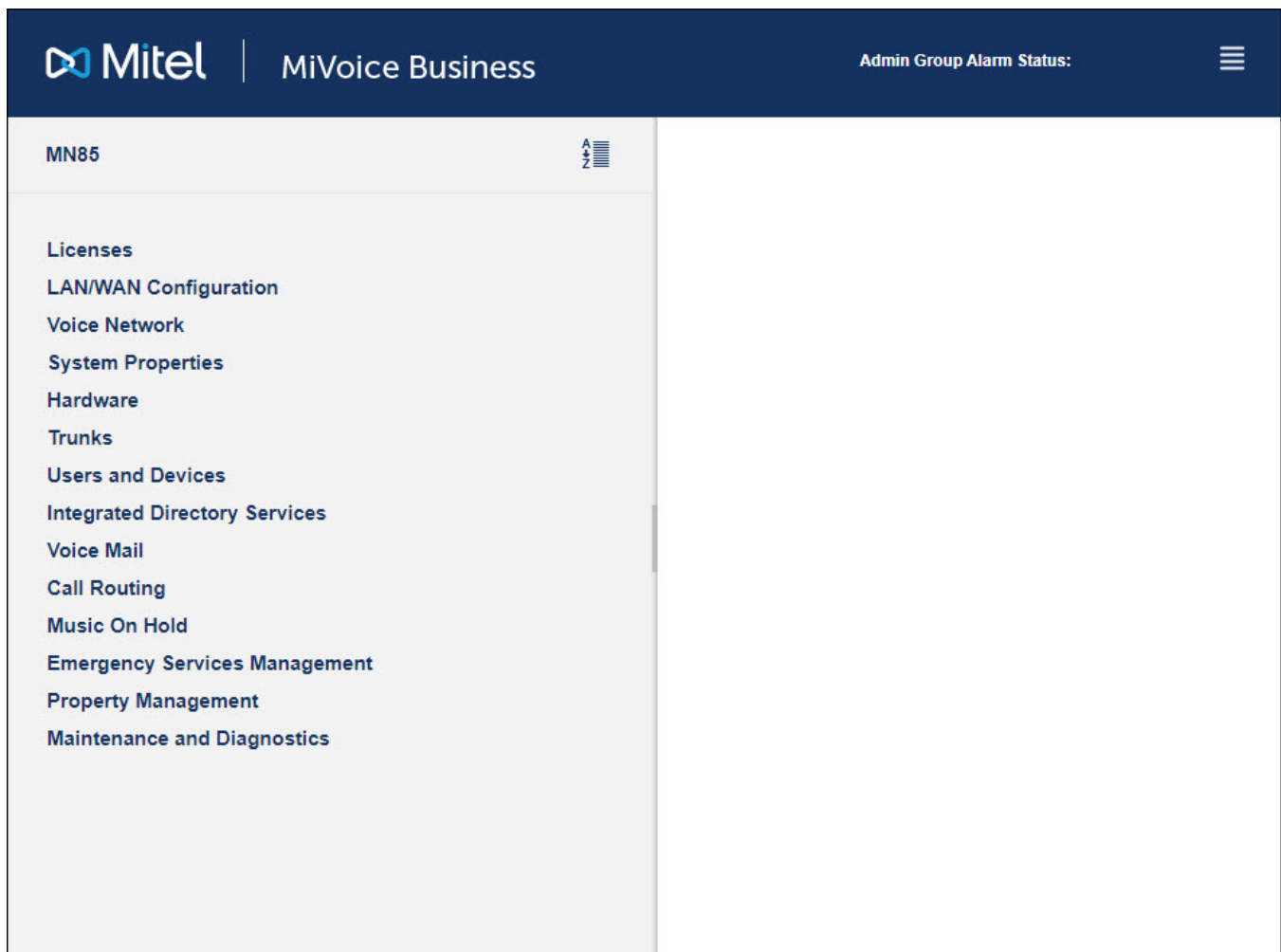
Click **Install MiVoice Business Certificate** and follow instructions provided to install the certificate. After the certificate is installed, exit the browser, and then restart it. You can now log in to MiVoice Business and not receive the security certificate warnings.

3. Type the default **Login ID** (system) and **Password** (password).
4. Select **Remember Login ID** if you want to save the Login ID on your computer.
5. Click **Log In**.

To prevent unauthorized use, you will be prompted to change the password the first time you log in.

6. Click **System Administration Tool**.

The System Administration Tool home page is displayed.



7. You will be prompted to install XML Components when you log into the System Administration Tool for the first time. At the prompt, “Do you wish to install or upgrade the required XML components?”, click **Install Now**. The installation takes less than 30 seconds and you do not need to restart your computer.

TIP: The system allows up to 5 concurrent System Administration Tool or Group Administration Tool sessions (or any combination of the two) provided that the initial login browser is closed and 10 concurrent Desktop Tool sessions.

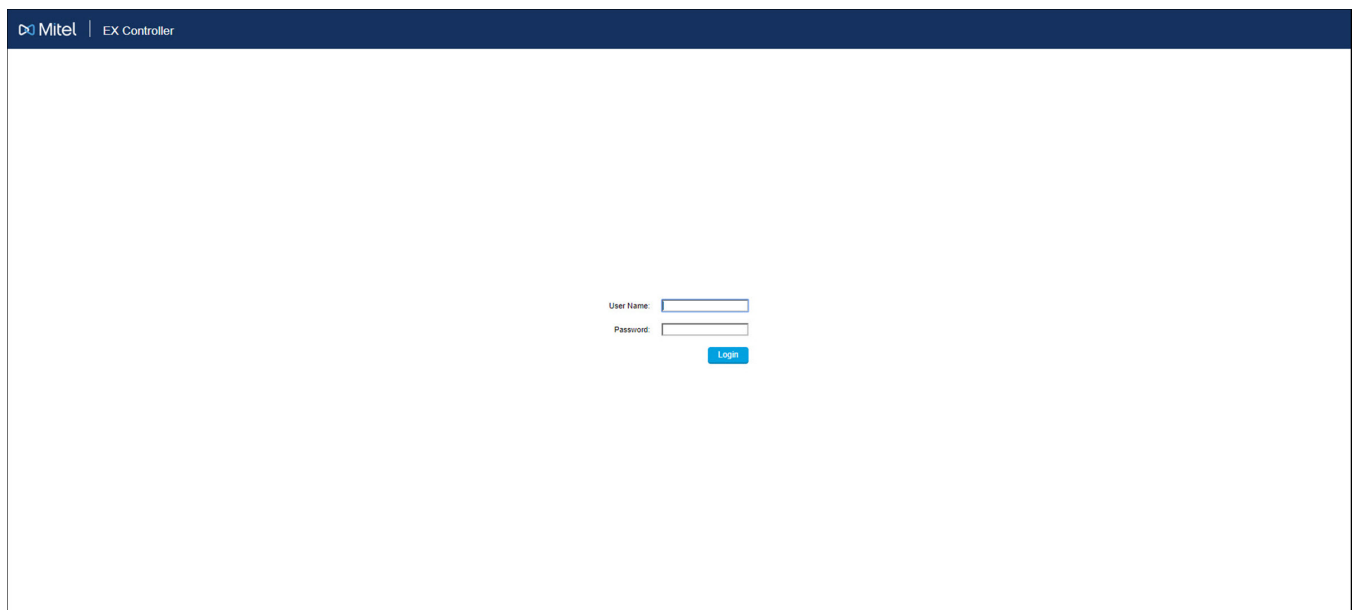
NOTE: The System Administration Tool will temporarily lock you out for 15 minutes after three consecutive attempts to log in have failed.

8. Navigate to the **Hardware > Hardware Modules** form and verify that all the telephony cards are listed.
9. Reboot the system from Server Manager (**Administration > Shutdown or reboot**).

Log in to the EX Controller Web GUI

1. Enter the **IPv4 EX Controller LAN address** specified during the deployment in the address bar of your web browser.

The EX Controller Web GUI login page is displayed.



The screenshot shows the login page of the EX Controller Web GUI. At the top, there is a dark blue header bar containing the Mitel logo and the text 'EX Controller'. The main body of the page is white. In the center, there is a login form consisting of two text input fields. The first field is labeled 'User Name' and the second is labeled 'Password'. Below the 'Password' field, there is a blue button with the word 'Login' in white text.

2. In the **User Name** field, type **Public**.
3. In the **Password** field, type the password of the Server Manager's **admin** user.
4. Click **Login**.

The EX Controller Web GUI home page is displayed.

Mitel | EX Controller

System Network SBC Management Reboot

Information Services Hardware Event Log Local Log Packet Capture Diagnostic VM

• Information

Current Status	
Device Identification:	EX Controller
Firmware:	Dgw 44.3.1746
Profile:	STNL-MT-D2000-155
MAC Address:	0090f80bdc8
Serial Number:	000400001M318170017
Number of DSPs:	0
Storage Memory (in use/total):	18.3 GB / 60 GB
Volatile Memory (in use/total):	2.3 GB / 8 GB
System Uptime (D:HH:MM:SS):	12:19:04:19
System Time (DD/MM/YYYY HH:MM:SS):	28/11/2019 02:34:15

Licences	
CWMP/TR-069	
SBC Licence for 3 concurrent sessions	
Virtual Machine Licence	

Activate Licence	
Licence Key:	<input type="text"/>

Apply

If the login fails, see [Unable to log into the EX Controller Web GUI as mimx user after a password reset using Server Manager](#).

IMPORTANT: The EX Controller Web GUI is used for troubleshooting purposes only. Do **NOT** use this GUI for programming trunks or the MiVoice Business system. Use the MiVoice Business System Administration Tool for programming trunks (**Trunks > Enterprise Gateways**) and the MiVoice Business system.

Program the MiVoice Business System

- Program the MiVoice Business system using one of the following options:
 - Mitel Integrated Configuration Wizard (only if you have cleared the **Enable secure EX controller access** check box (step 6) in the [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#))
 - Manually, by logging into the MiVoice Business System Administration Tool
- (Optional) If you are migrating from an unsupported 3300 ICP controller, continue with step 6 of the **Migration Guidelines for an Unsupported 3300 ICP Controller** procedure (**Chapter 4 Migration**) in the *MiVoice Business Migration Guidelines* document.

Trunk Configuration

After you perform the basic programming of the MiVoice Business System Administration Tool, you can configure trunks automatically by executing configuration scripts in the **Gateway Configuration Scripts** form (**Trunks > Enterprise Gateways**) of the MiVoice Business System Administration Tool.

NOTE: On the EX platform, individual trunk access is not supported as ISDN, T1, and FXO trunks are not assigned trunk numbers when programmed.

NOTE: If you hover over the default configuration file, a Tooltip is displayed that provides information about the default configuration file.

Trunk	Configuration Details
T1/D4 E&M trunks	<p>Execute the following configuration scripts:</p> <ul style="list-style-type: none"> To configure Immediate Start, execute: <code>mitel_T1_EAM_ulaw_immediate_perslot.cfg</code> To configure Wink Start, execute: <code>mitel_T1_EAM_ulaw_wink_perslot.cfg</code>
PRI trunks	<p>Execute one of the following configuration scripts depending on the protocol provided by the PSTN:</p> <p>To configure DMS-100 protocol per specific PRI slot, execute:</p> <pre>mitel_E1_Euro_ISDN_Euro_Cayman_perslot.cfg mitel_E1_Euro_ISDN_Euro_Numeris_perslot.cfg mitel_E1_Euro_ISDN_Euro_Standard_perslot.cfg mitel_E1_Euro_ISDN_Euro_Telecom_Italian_perslot.cfg mitel_T1_DMS100_perslot.cfg mitel_T1_DMS250_perslot.cfg</pre>
FXO trunk	<p>Execute the following configuration scripts:</p> <ul style="list-style-type: none"> To configure FXO trunks that use loaded coils, execute: <code>mitel_fxo_north_america.cfg</code> To configure FXO trunks that use non-loaded coils, execute: <code>mitel_fxo_default.cfg</code> To disable the Dial Tone Detection Mode, execute: <code>mitel_Disable_Dialtone_Detection.cfg</code>

Trunk	Configuration Details
R2 trunk	<p>To configure R2 trunks, execute the configuration file applicable to your country:</p> <ul style="list-style-type: none">• To configure R2 trunks execute: mitel_R2_Argentina_perslot.cfg mitel_R2_Brazil_perslot.cfg mitel_R2_ITU_perslot.cfg NOTE: mitel_R2_ITU_perslot.cfg is applicable for generic ITU configuration. mitel_R2_Mexico_perslot.cfg mitel_R2_Philippines_perslot.cfg mitel_R2_SaudiArabia_perslot.cfg mitel_R2_Venezuela_perslot.cfg• You can also manually program the R2 trunk using the EX Controller Web GUI. For more information about Programming R2 Trunk and Customizing default settings, see Appendix B: Programming an R2 Trunk

Maintenance

Software Upgrade

You can upgrade the MiVoice Business system software using the blades utility in Server Manager (**ServiceLink > Blades**).

Mitel

MiVoice Business

admin@ex207.mitel.com

Status: Clear

ServiceLink
Blades
Status
Administration
Web services
Backup
Restore
View log files
Event viewer
System information
System users
Shutdown or reboot
Security
Remote access
Syslog
Web Server
Configuration
Networks
E-mail settings
Google Apps
DHCP
Date and Time
Hostnames and addresses
Domains
IPv6-in-IPv4 Tunnel
SNMP
Ethernet Cards
Review configuration
Miscellaneous
Support and licensing
Help
EX Platform
Reboot

Current list of blades

Update list

Software download center: staging.swdlgw.mitel.com
Last updated: Thu 16 Jan 2020 05:41:06 AM EST

Blade	Description	Status	Installation	Documentation
EX	EX Platform Specific Software	installed	installed (V2.1.0.18) <div>Upgrade Cache (V2.1.0.19)</div>	
Blade-MVF	Mitel Virtualization Framework	installed	installed (V5.0.22.0)	
MiVB Debug Tools	x86 Only!! An add-in Blade with useful stuff for debugging the MiVB native Linux Blade.		<div>Install Cache (V9.0.0.184)</div>	View
			<div>Install Cache (V9.0.0.185)</div>	View
			<div>Install Cache (V9.0.0.193)</div>	View
			<div>Install Cache (V9.1.0.48)</div>	View
			<div>Install Cache (V9.1.0.49)</div>	View
			<div>Install Cache (V9.1.0.50)</div>	View
			<div>Install Cache (V9.1.0.51)</div>	View
			<div>Install Cache (V9.1.0.52)</div>	View
			<div>Install Cache (V9.1.0.53)</div>	View
			<div>Install Cache (V9.1.0.54)</div>	View
			<div>Install Cache (V9.1.0.55)</div>	View
			<div>Install Cache (V9.1.0.56)</div>	View
			<div>Install Cache (V9.1.0.57)</div>	View
			<div>Install Cache (V9.1.0.58)</div>	View
			<div>Install Cache (V9.1.0.59)</div>	View
			<div>Install Cache (V9.1.0.60)</div>	View
			<div>Install Cache (V9.1.0.61)</div>	View
			<div>Install Cache (V9.1.0.63)</div>	View
			<div>Install Cache (V9.1.0.64)</div>	View
			<div>Install Cache (V9.1.0.68)</div>	View
			<div>Install Cache (V9.1.0.71)</div>	View
			<div>Install Cache (V9.1.0.73)</div>	View
MiVoice Business	MiVoice Business software for installation on MiVB vApp and ISS platforms.	installed	<div>Remove (V9.1.0.73)</div> <div>Upgrade Cache (V9.1.0.74)</div> <div>Upgrade Cache (V10.0.0.90)</div>	View View View
ServiceLink	ServiceLink for Mitel Standard Linux	installed	installed (V11.0.63.0)	

MiVoice Business 9.1.0.73
© Mitel Networks Corporation

Prerequisite

Ensure that the network backup is configured properly in Server Manager (**Administration > Backup**).

Procedure

To upgrade the software

CAUTION: The upgrade process causes service interruption.

1. [Log into Server Manager](#).
2. Click on **Blades**, located in the left-side panel under **ServiceLink**.
3. Click **Update List** to view the new versions available from the AMC in the blade list.
4. Install the blades in the following order:
 - a. ServiceLink
 - b. EX
 - c. MiVoice Business
5. Read the End User License Agreement, and at the bottom of the page click **Accept all Licenses**. A page showing the upgrade progress appears.
6. When the installation is complete, click **Clear this report**.

NOTE: The installation time is dependent on the size of the database being backed up. The system takes approximately 30 to 90 minutes to back up an average-sized database (50 - 100 MB).

Mount Software Blade on Server Manager Manually

If a software blade is not available on AMC or Server Manager for an upgrade, you can manually mount the software blade on Server Manager and then perform the software upgrade.

To manually mount the software blade on Server Manager and upgrade the software:

1. Using a file transfer application (for example, FileZilla), copy the downloaded software blade ISO file to the **tmp** folder under the *root* directory in the MiVoice Business system.
2. Using a terminal emulator application (for example, PuTTY), connect to the MiVoice Business system remotely as *root* user using the SSH protocol.
3. Run the following commands:
 - a. `cd /tmp`
 - b. `mkdir -p /mnt/cdrom`
 - c. `mount Blade-MiVoiceBusiness-9.1.0.88-01.iso /mnt/cdrom`
mount: /dev/loop0 is write-protected, mounting read-only
 - d. `cd /mnt/cdrom/Software/`
4. [Log into Server Manager](#) and verify that the mounted software blade is displayed in the **ServiceLink > Blades** page.
5. [Perform the software upgrade](#).

6. If the remote connection with the MiVoice Business system established in step 2 is lost, perform step 2, and then run the following commands:
 - a. `cd`
 - b. `umount /mnt/cdrom`
 - c. `rm Blade-MiVoiceBusiness-9.1.0.88-01.iso`
 - d. At the following prompt, type **y**.
`rm: remove regular file 'Blade-MiVoiceBusiness-9.1.0.88-01.iso'?`

Backup and Restore

You can perform database backup and restore either from Server Manager or the MiVoice Business System Administration Tool.

Backup and Restore Using Server Manager

The database backup using Server Manager includes the server database, the EX Controller (host) database, and the MiVoice Business system database.

To perform a backup, log into the Server Manager, and navigate to **Administration > Backup**. For more information, refer to the associate Help page.

To perform a restore, log into the Server Manager, and navigate to **Administration > Restore**. For more information, refer to the associate Help page.

Backup and Restore Using MiVoice Business System Administration Tool

The database backup using the MiVoice Business System Administration Tool includes the MiVoice Business system database.

NOTE: The database backup generated from the System Administration Tool does not include the EX Controller (host) database.

To perform a backup, log into the MiVoice Business System Administration Tool, and navigate to **Maintenance and Diagnostics > Backup**. For more information, refer to the associate Help page.

To perform a restore, log into the MiVoice Business System Administration Tool, and navigate to **Maintenance and Diagnostics > Restore**. For more information, refer to the associate Help page.

WARNING: Do NOT restore the MiVoice Business system database on a blank EX Controller (that is, an EX Controller (host) with no database). Otherwise, there will be data inconsistency.

Field Replaceable Units

SSD

In case of a Solid-State Drive (SSD) failure of an EX controller, you must replace the EX Controller unit:

1. Make a note of the slot number and telephony card (PRI, DSP, FXO, or FXS) installed into the slot. For example, slot 1 has PRI card installed, slot 2 has DSP card installed, and so on.
2. Ensure that you have the latest backup file from Server Manager.
3. Remove the telephony cards from the EX Controller. See [Telephony Cards](#).
4. Procure a new EX Controller. For part numbers, see [Models and Part Numbers](#).
5. Install the EX Controller. See [Hardware Installation](#).

NOTE: Ensure that you install the cards in the slots as noted in step 1.

6. Deploy the system software. See [Software Installation](#).

Ensure to select the **Restore via console** option in the EX Controller Deployment Tool.

7. Restore the database from the Server Manager (**Administration > Restore**).

Telephony Cards

If you are replacing a card, it is recommended to replace a card with the same type of card in a slot. For example, replace an FXO card with a new FXO card. If you replace a card with a different type of card or move a card to a different slot, then the configuration data is lost. You must deprogram the old card and reprogram the new card.

If you are installing a new card, refer to the guidelines in the following table for installing a new slot to the current slot configuration:

Current slot configuration	If the new card you want to install is	Recommended action
Slot 1 - PRI Slot 2 - DSP Slot 3 - FXO Slot 4 - FXS	PRI	<ol style="list-style-type: none"> 1. Replace the DSP card in slot 2 with the PRI card. 2. Install the DSP card in slot 5 (next available slot).
	DSP	Install the DSP card in slot 5 (next available slot).
	FXO or FXS	Install the FXS or FXO card in slot 5 (next available slot).
Slot 1- DSP Slot 2- FXO Slot 3- FXS	PRI	<ol style="list-style-type: none"> 1. Replace the DSP card in slot 1 with the PRI card. 2. Install the DSP card in slot 4 (next available slot).
	DSP	Install the DSP card in slot 4 (next available slot).
	FXO or FXS	Install the FXS or FXO card in slot 4 (next available slot).

To add or replace a card:

1. Make sure an adequate earth ground connection has been made between the grounding screw on the back of the controller and an appropriate grounding point in your site.
WARNING: Adequate earth ground connection of the controller is mandatory to avoid any damage or injuries.
2. Wear an ESD wrist strap, ensuring that it makes good contact with bare skin.
3. Attach the ESD wrist strap end to an earth ground (grounding screw on the back of the controller or unpainted bare metal spot of a grounded equipment rack).
4. Turn off the power switch of the controller.
NOTE: Redundant Power Supply units do not have a power switch.
WARNING: The controller unit must be turned off before adding, removing or swapping cards.
5. Disconnect all cables (except the earth ground connection) from the controller.
CAUTION: Power source cables must be disconnected last.
6. Unscrew the two thumb screws of the slot where you wish to install or replace a card.
7. Gently remove the blank plate or the existing card.
8. Gently slide the new card into the internal plastic rails of the slot.
NOTE: The slot must not be left empty. If do not want to install a new card after removing a telephony card, insert the blank plate in the slot.
NOTE: While sliding in the card, take care not to damage the electronic parts on the card. The card, when properly inserted, slides in easily.
9. Set the thumb screws back into place. Do not over-tighten.
10. Apply the label indicating the ISED and ACTA registration numbers on the exterior surface of the casing.

Change IP Address of the EX Controller Web GUI

To change IP address of the EX Controller Web GUI (EX Controller):

NOTE: Do not change the IP address from the EX Controller Web GUI.

1. [Log in the System Administration Tool](#), and navigate to the **Voice Networks > Enterprise Gateways** form.
2. Select the IP address, and click **Change**, and specify the following:
 - a. **Update IPv4 Address**
 - b. **Update IPv4 Subnet Mask**
 - c. **Update IPv4 Gateway Address**

The screenshot shows the 'Enterprise Gateways' section in the Server Console. A 'Change' dialog is open for the gateway with IP/FQDN 10.211.26.205. The dialog has a dark blue header with the title 'Change'. Below the header, the title 'Enterprise Gateways' is repeated. The form contains the following fields:

- IP/FQDN: 10.211.26.205
- Authentication: (empty)
- Privacy Password: (password field with dots)
- User: mimx
- Password: (password field with dots)
- Advanced section with three sub-fields:
 - Update IPv4 Address: (empty)
 - Update IPv4 Subnet Mask: (empty)
 - Update IPv4 Gateway Address: (empty)

At the bottom right of the dialog are 'Save' and 'Cancel' buttons.

Ensure that the EX Controller and the MiVoice Business system are on the same subnet. If the EX Controller is on a different subnet, then [Change the IP address of the MiVoice Business system](#) to the same subnet as that of the EX Controller.

Configure the Server Using Server Console

The server console provides basic, direct access to the server. Most server console operations are also available from the server manager. You can also perform basic MSL configuration using the Server Console.

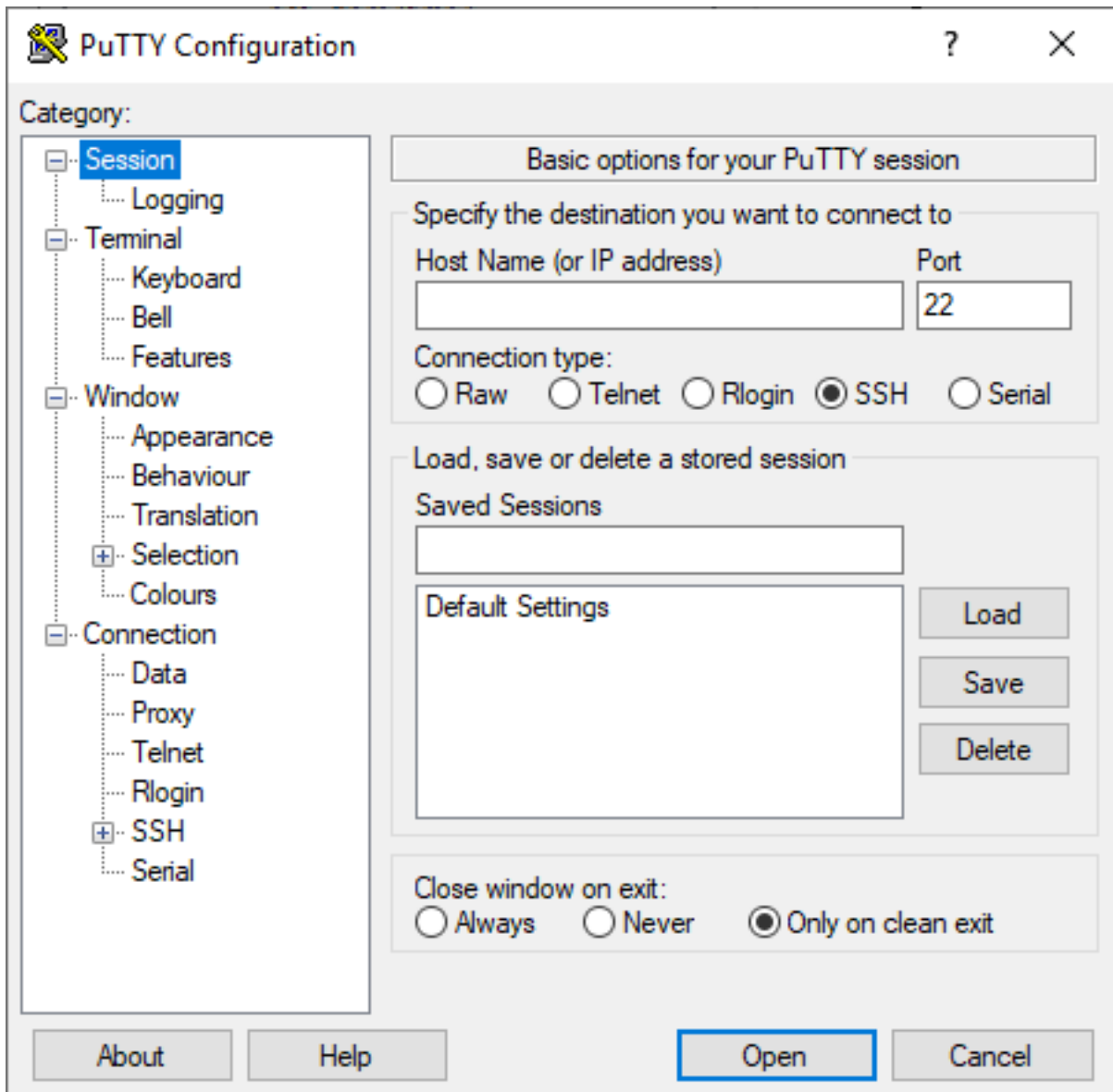
Accessing Server Console

To access the Server Console remotely:

1. Connect to the MiVoice Business system using a terminal emulator application (for example, PuTTY).

NOTE: Before you begin, ensure that you have enabled SSH access through the Server Manager (**Security > Remote Access**).

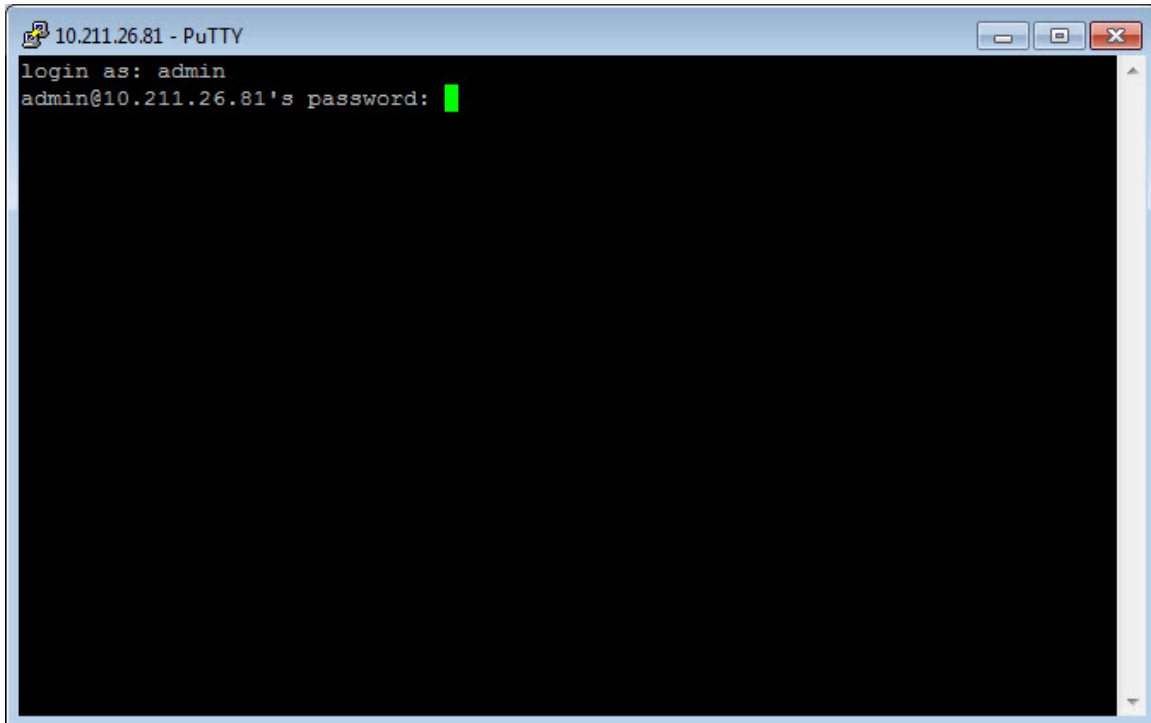
- a. Launch a terminal emulator application.



- b. In the **Host Name (or IP address)** field, type the IP address of the MiVoice Business system.
- c. Select **SSH** under **Connection type**, and then click **Open**.

The login prompt is displayed.

- d. At the login prompt (**login as:**), type **admin** (user *admin*) and press the Enter key.



NOTE: You can also log in as the *root* user and type **su admin** to switch to the *admin* user.

- e. At the password prompt, type the administrator password, and press the ENTER key.

[illegible]

Server Console

From the Server Console, you can view the following information and perform the following tasks.

Option:	Use this option to:
Check status of this server	View uptime information about the server.
<i>Configure this Server</i>	View and modify the configuration information entered during installation (Ethernet cards, IPv4 and IPv6 address information, DHCP, DNS, domain names, etc.).
Test Internet access	Test your connection by contacting Mitel Corporation via Internet
Media Check Mitel CD/DVD	Test a Mitel application CD/DVD (supported only for applications that have embedded checksum values.)
Register for Service Link	Activate ServiceLink on the AMC via text mode browser; (normally you would use the web-based server manager)
Install application blades from CD/DVD	Install application software blades from CD/DVD. Your application documentation specifies when to use this option.
Reboot or shut down the server	Reboot or shut down the server. Configuration settings in effect at the time of reboot are re-applied.
Offline Sync with the AMC	Use for AMC activation at sites where the MSL server does not have direct Internet access. (Note: You will need Internet access from another PC/workstation.)
Manage disk redundancy	Manage configuration of redundant (RAID1) disks.
Access server manager Note: select [+] to access the second page of options.	Access the server manager using a text-based browser. This is the same interface to which you can connect remotely using a web browser; this option allows you to perform server manager functions directly from the server console. Use the keyboard arrow keys to navigate the pages. Type 'q' (for quit) to exit the text-based browser. Note: most applications cannot be managed using the text-mode browser. The server uses a text-based browser called "ELinks" to access the web-based server manager. ELinks information is available at http://elinks.or.cz/about.html . Note that for security reasons some ELinks features are disabled when you are browsing from the server console (such as the ability to specify an external URL).
<i>Manage trusted networks</i>	Show, add, or delete trusted networks access privileges to additional IPv4 and IPv6 networks. Note: For security, we recommend that you be as precise as possible when granting access (for example, enter the IP address of a specific PC or subnet).

Option:	Use this option to:
View support and licensing information	Display the licensing terms.
Perform backup	Back up configuration information to a USB device or a network file server. For more information see Performing Backups . It is recommended to perform backup using Server Manager (Administration > Backup).
Verify a backup file	Verify previous backup files. For more information, see Verify Backup .
Restore from backup	Restore backup files is not supported remotely. User Server Manager (Administration > Restore) to restore backup file.
Exit from the server console	Exit from the Server Console.

Configure this Server

To configure this server:

1. In the Server Console main menu, click **2. Configure this server**, and then click **Next**.
2. In the configuration screens, enter the settings listed in the following table:

Screen	Action
Primary domain name	Enter the domain name (for example, mitel.com).
Enter system name	Enter a system name (for example, your company name)
Select local network adapters.	<p>Select one or more network adapters.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • This screen is displayed only for an EX controller. • If you have restored a database from the MiVoice Business Virtual system in an EX controller, then after the restore, select eth1 virtio_net - <IP address of the adapter> [eth1: UP].
Local networking parameters	Enter an available IP address (without leading zeros) that is used to access both the Server Manager and the MiVoice Business system.
Enter local subnet mask	Enter the IP address of the subnet mask.
Enable IPv6 protocol	Specify whether you want to enable IPv6 addresses.
Select WAN network adapters	Select a network adapter. Skip if you have only LAN interfaces.
Enter gateway IP address	Enter the gateway IP address.
Corporate DNS server addresses	Enter one or more corporate DNS server IP addresses, separated by a comma.

Screen	Action
Resolve primary domain	Specify how MSL's DNS should resolve names for the domain.

3. Do one of the following:

- If you have modified only **DNS server addresses** configuration setting, click **Finish** to save the configuration changes.
The configuration settings are applied without rebooting the system.
- If you have modified any other configuration setting, click **Reboot**.
The configuration settings are applied upon system reboot.

Manage trusted networks

To manage trusted networks:

1. In the Server Console main menu, click **9. Manage trusted networks**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Trusted Networks Operations	<ul style="list-style-type: none"> • Click 1. Show trusted networks, and then click Next. The system displays the trusted IPv4 networks. • To add IPv4 trusted networks, click 2. Add IPv4 trusted network, and then click Next. <ul style="list-style-type: none"> a. Enter the IP address, and then click Next. b. Enter the subnet mask, and then click Next. c. Enter the gateway IP address, and then click Next. • To delete the trusted IPv4 networks added, click 3. Delete IPv4 trusted network, and then click Next. <ul style="list-style-type: none"> – Click to select the network you want to delete, and then click Next.

Perform backup

To back up the database:

- Samba (SMB)/Common Internet File System (CIFS)
- Secure File Transfer Protocol (SFTP) To back up the database:

NOTE: It is recommended to perform backup using Server Manager (**Administration > Backup**).

1. In the Server Console main menu, click **6. Perform backup**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Backup server IP address	Enter the IP address of the network file share server where you want to store the database backup file.
Backup server domain or workgroup name	Enter the Domain or workgroup name. Applies only to SMB/CIFS. Leave the field blank for SFTP. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then the server's local Security Account Manager (SAM) is used for authentication, instead of the domain SAM. This field is required only for the SMB/CIFS protocol.
Backup share name	Enter the file-share name. Applies only to SMB/CIFS. Leave the field blank for SFTP. The restore utility will try to connect to the server/shared folder as an SMB/CIFS resource. The shared folder must have permissions set to Full Control .
Optional Directory Path	Enter the name of the sub-folder where you have stored the database backup file. For SMB/CIFS, the sub-directory is relative to the share. For SFTP, the sub-directory is relative to the root of the file system accessed through the SFTP protocol.
Backup username	Enter the user name to use when connecting to the network file share server.
Backup password	Enter the password to use when connecting to the network file share server.
Proceed with Backup to network	Click Proceed .

The system creates a database backup file in the specified directory on the file server.

Verifying a Backup File

To verify previous backup files:

1. In the Server Console main menu, click **14. Verify a backup file**, and then click **Next**.
2. At the prompt, insert your storage medium. (Note: if your USB device was left mounted after your last backup, you must remove it and re-mount it first.)
3. If more than one storage device is connected to your system, select the device that contains the backup file.
4. If more than one backup file is contained on the storage device, select the file you want to verify.
5. Click **OK**. Verification of the file is confirmed. If you receive an error message, you cannot use this backup file for the restore. Check your storage media and try the backup procedure again.

Troubleshooting

This chapter provides troubleshooting information for the EX Controller, intended for use by Mitel certified technicians.

For troubleshooting other general issues, see *MiVoice Business Troubleshooting Guide*.

System Software

The following logs provide information for troubleshooting EX Controller issues:

- Software logs from the System Administration Tool (**Maintenance and Diagnostics > Logs > All Maintenance and Software Logs**)
- Log files from the Server Manager (**Administration > View Log Files**)
- EX Controller local logs from the EX Controller Web GUI (**System > Local Log**)

NOTE: In the event of a system failure that requires assistance, collect log files and diagnostic data (SOS report) from the Server Manager before contacting Product Support.

Table 6.1: System Software Troubleshooting (Sheet 1 of 4)

Symptom	Possible Cause	Corrective Action
<ul style="list-style-type: none"> • Telephony cards are not listed in the Hardware Modules form in the MiVoice Business System Administration Tool. • Unable to perform backup from Server Manager. • Telephony cards are not functioning properly. 	Unable to log into the EX Controller Web GUI as <i>mimx</i> user after a password reset using Server Manager	<ol style="list-style-type: none"> 1. Reset the <i>admin</i> user password from Server Manager to the same password. For example, if the old password is <i>Company@123</i>, reset the new password to <i>Company@123</i>. The system takes about 30 seconds to update the passwords of the user accounts on EX Controller. 2. If you are still unable to log into the EX Controller Web GUI as <i>mimx</i> user, then log into the EX Controller Web GUI as <i>public</i> user and navigate to Management > Access Control, and enter the Server Manager <i>admin</i> user password for the <i>mimx</i> user. 3. Repeat step 1 and monitor <i>/var/log/ex/ex.log</i> for <i>mimx</i> communication errors. If so, this could be due to network setup issues. Resolve the network setup issues.

Table 6.1: System Software Troubleshooting (Continued) (Sheet 2 of 4)

Symptom	Possible Cause	Corrective Action
The EX Controller Web GUI fails to initialize or stops responding.	Incorrect configuration	<ul style="list-style-type: none"> Check whether the System Administration Tool is up and running and is accessible. Investigate whether the IP address of the EX Controller Web GUI has been modified. Check for network issues. <p>If the above corrective actions does not resolve the issue, perform a partial reset. See Partial Reset. If partial reset does not resolve the issue, perform a factory reset. See Factory Reset.</p>
Unable to access System Administration Tool.	The MiVoice Business software deployed on the EX Controller is corrupted.	<ul style="list-style-type: none"> Check whether the MiVoice Business virtual machine deployed on the EX Controller is up and running. Check whether you can access Server Manager. Check whether you can generate the SOS logs from Server Manager (Administration > View log files) and collect SOS logs. Check whether there is CPU hogging. Check for network issues. Access the MiVoice Business virtual machine through VNC Viewer and monitor the shell activity for issues. <p>If you need help with any of the above corrective actions, contact Mitel Technical Support with SOS logs.</p>
The EX Controller Deployment Tool virtual machine cannot be located on the EX Controller Web GUI.	The EX Controller Deployment Tool virtual machine is deleted from the EX Controller Web GUI.	Contact Mitel Technical Support.

Table 6.1: System Software Troubleshooting (Continued) (Sheet 3 of 4)

Symptom	Possible Cause	Corrective Action
Cannot log into the System Administration Tool.	Forgot the login credentials	See Reset the System Administration Tool Password .
	<ul style="list-style-type: none"> IP addresses (static IP address or the IP address provided by DHCP service) modified by someone The network is misconfigured or is in an invalid state 	<ul style="list-style-type: none"> Check whether you can access the EX Controller Web GUI. If the EX Controller Web GUI is accessible, then log in to the EX Controller using the VNC application by entering <IP address of the EX Controller Web GUI>:1, in the VNC Server field. Run the ifconfig command and verify whether eth1 has the correct MiVoice Business IP address. If not, modify the IP address of the MiVoice Business. To modify the MiVoice Business IP address, see Configure this Server. Collect SOS logs from Server Manager (Administration > View log files). <p>If you need help with any of the above corrective actions, contact Mitel Technical Support with SOS logs.</p>
Unable to log in to the EX Controller Web GUI	User account locked after multiple failed log in attempts	<p>Check the <i>syslog</i> file generated from the EX Controller Web GUI to confirm whether the user account is locked. The account is automatically unlocked after a certain configurable duration (default is 300 seconds).</p> <p>NOTE: Lock protection locks the user account after multiple (default is 5) failed log in attempts. Lock protection is enabled by default for a user. You can disable lock protection from Management > Access Control in the EX Controller Web GUI.</p> <p>Also, see the corrective actions described for Unable to log into the EX Controller Web GUI as mimx user after a password reset using Server Manager.</p>

Table 6.1: System Software Troubleshooting (Continued) (Sheet 4 of 4)

Symptom	Possible Cause	Corrective Action
<ul style="list-style-type: none"> A Backup from the Server Manager (Administration > Backup) fails MiVoice Business software logs indicate an issue with mimx or the EX system 	Mismatch in: <ul style="list-style-type: none"> Passwords between MiVoice Business and the EX Controller The EX host address, and the address stored by MiVoice Business. 	<p>The ex-audit script detects:</p> <ul style="list-style-type: none"> a mismatch in mxTarget (EX Controller) ip address and ip0 property (MiVB) ip address failure to initialize mimx (<code>mivbMimxKeystoreInit</code>) improper file permissions for mimx folder whether mimx has the proper settings to access the MiVB whether mimx has the proper settings to access the EX Controller whether the EX firmware matches the recommended version in the EX Blade software <p>Run the ex-audit script to check for any potential installation issues:</p> <ol style="list-style-type: none"> Log in to the system through SSH (for example, through PuTTY) as the <i>root</i> user. Run the following command: <pre>/usr/ex/bin/ex-audit m5_ip_addr</pre> <p>Any issues are displayed with an “INFO:” text; usually, the command suggests using the '-a' option to repair the error. The '-f' option is suggested for a special case (see Step 4).</p> If the “INFO:” text suggests the '-a' option, run the following command: <pre>/usr/ex/bin/ex-audit -a m5_ip_addr</pre> If the audit detects that both <code>mxTarget</code> and the mimx have not been initialized, run the command with the '-af' option: <pre>/usr/ex/bin/ex-audit -af m5_ip_addr</pre> After running the '-a' or '-af' options, try the ex-audit script again to check for issues. If the following text is present: “Failed to communicate with mxTarget”, there may be a password mismatch. Access the EX Controller and ensure that SNMP v2 is enabled. Then, use the ex-audit command with the '-r' option: <pre>/usr/ex/bin/ex-audit -r m5_ip_addr</pre> <p>This resets the passwords to default1 on both the mimx and EX Controller. Access the Server Manager and reset the admin password to align the credentials for some applications. If SNMP v2 was previously disabled, access the EX Controller and disable it.</p>

Reset/Default Button

The **Reset/Default** button can be used to perform a factory or partial reset of the EX controller while the unit is powered on.

The **Reset/Default** button will generate different actions depending on the duration of time the button is held.

Pressing Time	Action	Comment	LED Pattern
2 to 6 seconds	Restarts the EX Controller.	No changes are made to the EX Controller settings.	Power1 blinking, all other LEDs Off.
7 to 11 seconds	Initiates a Partial Reset of the EX Controller	Restarts the unit in a known and static state while keeping most of the configuration unchanged.	All LEDs blinking, 1 cycle per second, 50% duty.
12 to 16 seconds	Initiates a Factory Reset of the EX Controller	Reverts the unit to its default factory settings. For more information, see Factory Reset .	All LEDs steady On.
17 seconds and more	No action is taken. This is useful if you accidentally pushed the button and do not need an action to be applied.	The action is ignored.	All LEDs will become Off after blinking and being steady on.

Partial Reset

You can perform a partial reset of the EX Controller to:

- Reset the password of the EX Controller Web GUI. For example, if you have forgotten the password.
- Contact the unit in a known state when you can no longer access the EX Controller Web GUI. For example, due to modified configuration. In such case, you can manage the EX Controller using the Rescue Network Interface. The Rescue Network Interface is bound to the WAN port ETH1 of the unit and accessible through the IP address 192.168.0.1. (IPv4) or an IPv6 Link Local address.

The Rescue Network Interface is used for:

- Completing the configuration of a new unit.
- Modifying existing configuration.

By default, the Rescue Network Interface is disabled. When a partial reset is performed, the Rescue Network Interface becomes enabled and the **Power** and **Ready** LEDs are blinking at 1Hz with 75% duty and all other LEDs are off. Once the configuration has been modified to solve the problem that required the partial reset, it is important to disable the Rescue Network Interface to make sure that you are no longer working in the Rescue Network Interface.

Partial reset on a new EX Controller does not modify its configuration. However, a partial reset performed on an EX Controller already in use will:

- Rollback Local Firewall settings that are not yet applied.
- Add a Local Firewall rule to allow complete access to the Rescue Network Interface.
- Rollback NAT settings that are not yet applied.
- Cancel the changes that were being modified but not yet applied to the configuration.
- Add NAT rule to allow complete access to the Rescue interface.
- Disable any Network Interface in conflict with the Network Rescue Interface.
- Configure and enable the Rescue Network Interface to:
 - use the link as the default value used by Uplink Network interface
 - set the IP address to 192.168.0.1 and the Network Mask to 255.255.255.0
 - set the IPv6 link-local address on all network links. The IPv6 link-local address can be underneath the EX Controller.

A partial reset will also modify the following parameters and preserve the values below even after the Rescue Network Interface has been disabled.

Service	Parameter	Default Value
AAA	Users.Password	<i>admin</i> and <i>pubic</i> users from profile are restored with their factory password. All other user names keep their password.
	Users.AccessRights	User(s) from profile are restored with their factory rights.
	ServicesAaaType (table)	Each service will be configured to use Local authentication and no accounting mechanism.
CLI	EnableTelnet	Disable
	TelnetPort	23
	EnableSsh	Enable
	SshPort	22
	InactivityTimeOut	15
HOC	ManagementInterface	Rescue
SNMP	Port	161
	EnableSnmpV1	Enable
	EnableSnmpV2	Enable
	EnableSnmpV3	Enable
Web	ServerPort	80
	SecureServerPort	443

To perform a partial reset of an EX Controller:

1. On a controller that is powered on, insert a small unbent paper clip into the hole of the **Reset/Default** button located at the front of the unit.
2. Press and hold the **Reset/Default** button for 7 to 12 seconds until all LEDs are blinking.
3. When all the LEDs are blinking, remove the paper clip.

NOTE: The Power LED starts blinking.

4. After you perform the partial reset, the **admin** and **public** passwords are set to factory defaults.
5. Set the Server Manager *admin* user password as the password for the *mimx* user and resolve any networking issue before disabling the Rescue Network Interface. See the corrective action described for [Telephony cards are not listed in the Hardware Modules form in the MiVoice Business System Administration Tool](#) on how to set the Server Manager *admin* user password as the password for the *mimx* user.
6. Disable the Rescue Network Interface:
 - a. [Log in to the EX Controller Web GUI](#).
 - b. Click **Management > Misc**.
 - c. From the **Network Interface** drop-down menu, select the interface that will be used to manage the EX controller unit.

NOTE: If the Rescue Network interface is enabled, the **Management** interface will be inaccessible after you disable the Rescue Network interface.
 - d. Click **Apply**.
 - e. Click **Network > Interfaces**.
 - f. From **Rescue Network Configuration**, in the **Activation** list, select **Disable**.
 - g. Click **Apply**.The EX Controller unit will be inaccessible on the newly configured static IP address or on the DHCP server.
7. Log in to the Server Manager and reset the password to synchronize the user account passwords with the Server Manager password.
8. Enable SNMP v1 and v2 from Server Manager (**Configuration > SNMP**).

Factory Reset

Depending on the DGW firmware version running on the EX Controller, the factory reset defaults the controller's IP scheme and deletes the persistent configuration parameters of the unit, including:

- MiVoice Business virtual machine and its database¹
- MiVB.img and MiVB.cfg files¹
- User files stored in the File service
- Certificates, except for the factory installed ones
- Log files of the File service

¹A factory reset on EX Controllers running DGW firmware lower than 45.1.1870 does not fully restore to its default settings, that is, the MiVoice Business virtual machine, database, MiVB.img and MiVB.cfg files are left undeleted in the controller. However, with EX Controllers running DGW firmware 45.1.1870, a

factory reset restores the controller to its default settings. Therefore, it is recommended to upgrade to the DGW firmware 45.1.1870 by upgrading the MiVoice Business EX software to the version 9.0.3.15_2 using Server Manager.

Factory reset must be performed on an EX Controller unit that is isolated from the network with access to a DHCP server. If the unit cannot find a DHCP server, it sends requests indefinitely.

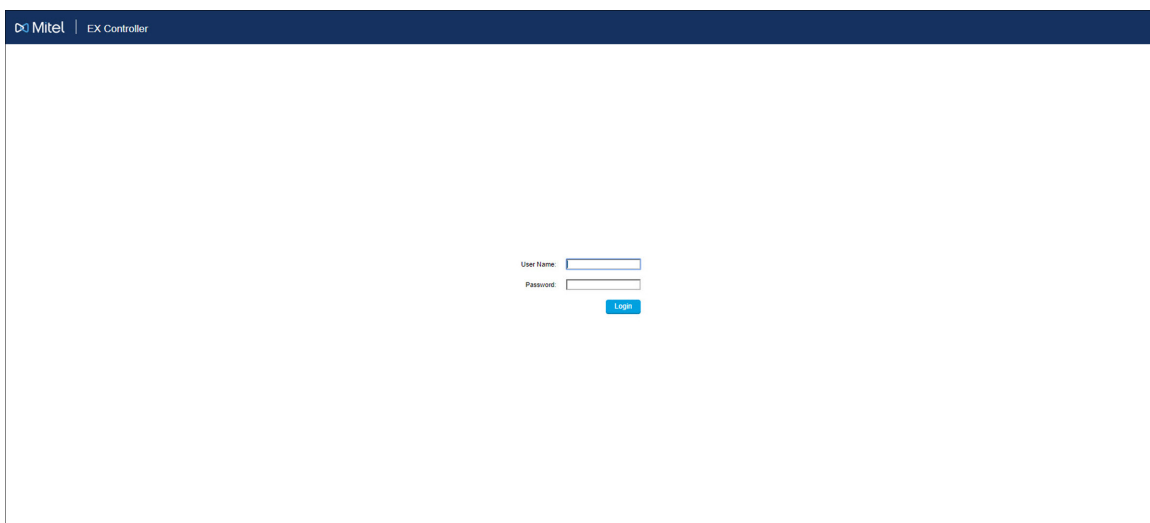
NOTE: Restoring factory default settings erases the deployment parameters.

To perform a factory reset of the EX Controller running DGW firmware version 45.1.1870 or higher:

1. On a controller that is powered on, insert a small unbent paper clip into the hole of the **Reset/Default** button located at the front of the unit.
2. Press and hold the **Reset/Default** button for 12 to 16 seconds until all the LEDs are steadily on. The controller unit reboots with the default IP address 192.168.0.10 accessible through **ETH2-ETH5** of the EX Controller.
3. Continue with [Accessing the EX Controller Deployment Tool](#).

To perform a factory reset of the EX Controller running DGW firmware version lower than 45.1.1870:

1. On a controller that is powered on, insert a small unbent paper clip into the hole of the **Reset/Default** button located at the front of the unit.
2. Press and hold the **Reset/Default** button for 12 to 16 seconds until all the LEDs are steadily on. The controller unit reboots with the default IP address 192.168.0.10 accessible through **ETH2-ETH5** of the EX Controller.
3. Assign a static IP address to your PC using the following IP scheme:
 - IP address: 192.168.0.100
 - Subnet mask: 255.255.255.0
 - Gateway IP address: 192.168.0.1
4. Connect an RJ45 Ethernet cable from the PC's Ethernet interface to any one of the ports **ETH2 - ETH5** of the EX Controller.
5. Enter the IP address 192.168.0.10 in the address bar of your browser to access the EX Controller Web GUI.



The EX Controller Web GUI login page is displayed.

6. In the **User Name** field, type **Public**.
7. Leave the **Password** field empty.
8. Click **Login**.

The EX Controller Web GUI home page is displayed.

Mitel | EX Controller

System | Network | SBC | Management | Reboot

Information | Services | Hardware | Event Log | Local Log | Packet Capture | Diagnostic | VM

• **Information**

Current Status	
Device Identification:	EX Controller
Firmware:	Dgw 44.3.1746
Profile:	STNL-MT-D2000-155
MAC Address:	0090f80bdc88
Serial Number:	000400001M318170017
Number of DSPs:	0
Storage Memory (in use/total):	18.3 GB / 60 GB
Volatile Memory (in use/total):	2.3 GB / 8 GB
System Uptime (D:HH:MM:SS):	12:19:04:19
System Time (DD/MM/YYYY HH:MM:SS):	28/11/2019 02:34:15

Licences	
CWMP/TR-069	
SBC Licence for 3 concurrent sessions	
Virtual Machine Licence	

Activate Licence	
Licence Key:	<input type="text"/>

Apply

9. Delete **MiVB.img** and **MiVB.raw** files:
 - a. Click **Management > File**. The **File** page is displayed.
 - b. From the **VM Files** table, click to delete **vm/images/MiVB.cfg** and **vm/images/MiVB.raw** files.



NOTE: Do not delete **vm/images/exdeploy.cfg** and **vm/images/exdeploy.img** files.

VM files			
Name	Description	Size	
vm/images/exdeploy.cfg	Virtual Machine configuration file	1 KB	—
vm/images/exdeploy.img	Virtual Machine image file	8.7 GB	—
vm/images/MIVB.cfg	Virtual Machine configuration file	1 KB	—
vm/images/MIVB.raw	Virtual Machine image file	31.3 GB	—
4 file(s)		Total: 40 GB / Available: 5.6 GB	


A confirmation message is displayed.

- c. Click **OK** to delete the files.

10. Start the Deployment Tool virtual machine:

- a. Click **System > VM**. The **Virtual Machine** page is displayed.
- b. Under **Virtual Machine Configuration** section, change **Startup** option to **Auto** for the **exdeploy** virtual machine configuration.

The screenshot shows the Mitel EX Controller interface. The top navigation bar includes tabs for System, Network, SBC, ISDN, POTS, SIP, Media, Telephony, Call Router, Management, and Reboot. Below this, a sub-navigation bar has tabs for Information, Services, Hardware, Endpoints, Event Log, Local Log, Packet Capture, Diagnostic, and VM. The VM tab is selected, displaying the 'Virtual Machines' section. This section contains three sub-sections: 'Virtual Machine Status', 'Virtual Machine Configuration', and 'Virtual Machine Creation'. The 'Virtual Machine Status' table shows a single VM named 'exdeploy' with a state of 'Starting'. The 'Virtual Machine Configuration' section shows the 'exdeploy' VM with a 'Startup' option set to 'Manual'. The 'Virtual Machine Creation' section shows a form to create a new VM with fields for Name, RAM, Storage, Image Format, and Number of Cores.

- c. Click  to start the Deployment Tool virtual machine. After a minute, refresh the page. The **State** under the **Virtual Machine Status** changes to **Starting** from **Stopped**. After a minute, the **Virtual Machine Status** changes to **Started**.
- d. Continue with
 - i. [Accessing the EX Controller Deployment Tool](#).
 - ii. [Updating the EX Controller Deployment Tool](#).
 - iii. [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#).

Reset the System Administration Tool Password

Overview

If you are unable to log in to the System Administration Tool as the *system* user, then you can reset the password for *system*.

Procedure

1. Log in to the system through SSH (for example, through PuTTY) as the *root* user.
2. Run the following command to reset the *system* password:
mcdDebug ResetLoginPassword system
3. Press CTRL + C to exit the mcdDebug shell.
4. Run the **logout** command to log out of the system:

Appendix A: Assigning a Static IP Address to the EX Controller Deployment Tool

If a DHCP server is not available on the network on which you want to deploy the EX Controller or if you are unable to access the Deployment Tool using a DHCP server, then you can access the Deployment Tool by assigning a static IP address to the Deployment Tool either *manually* or *using a USB flash drive*.

Assigning a static IP address manually

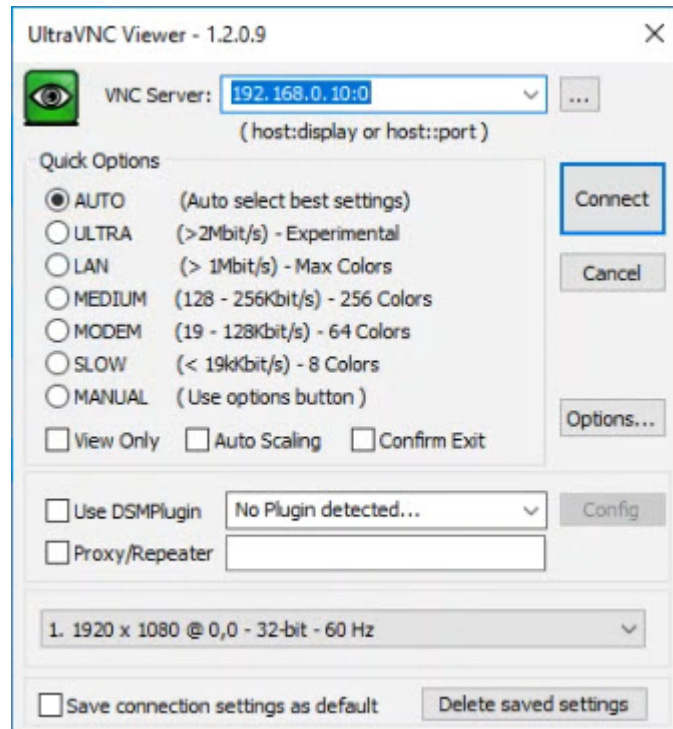
Prerequisites

- An RJ45 Ethernet cable for connection between the EX Controller and Layer2 switch.
- Download and install the latest version of UltraVNC Viewer (or VNC Viewer) application installed on the deployment PC.

Procedure

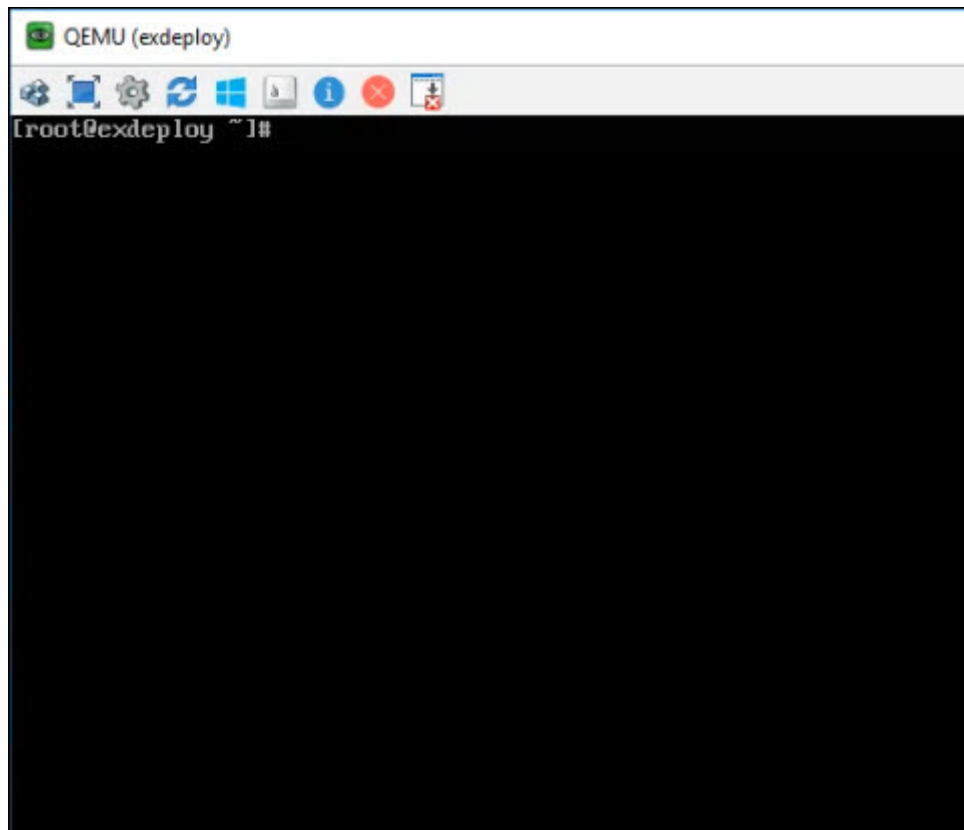
To manually assign a static IP address to the Deployment Tool:

1. Assign a static IP address to your deployment PC using the following IP scheme:
 - IP address: 192.168.0.100
 - Subnet mask: 255.255.255.0
 - Gateway IP address: 192.168.0.1
2. Power on the EX Controller.
3. Connect an RJ45 Ethernet cable from the deployment PC's Ethernet interface to one of the **ETH2 - ETH5** ports of the EX Controller.
4. From the deployment PC, start **UltraVNC Viewer**.
5. In the **VNC Server** field, enter < **Default IP address of the EX Controller Web GUI** > :0. The default IP address of the EX Controller Web GUI is **192.168.0.10**.



6. Click **Connect**.

The Deployment Tool virtual machine console is displayed.

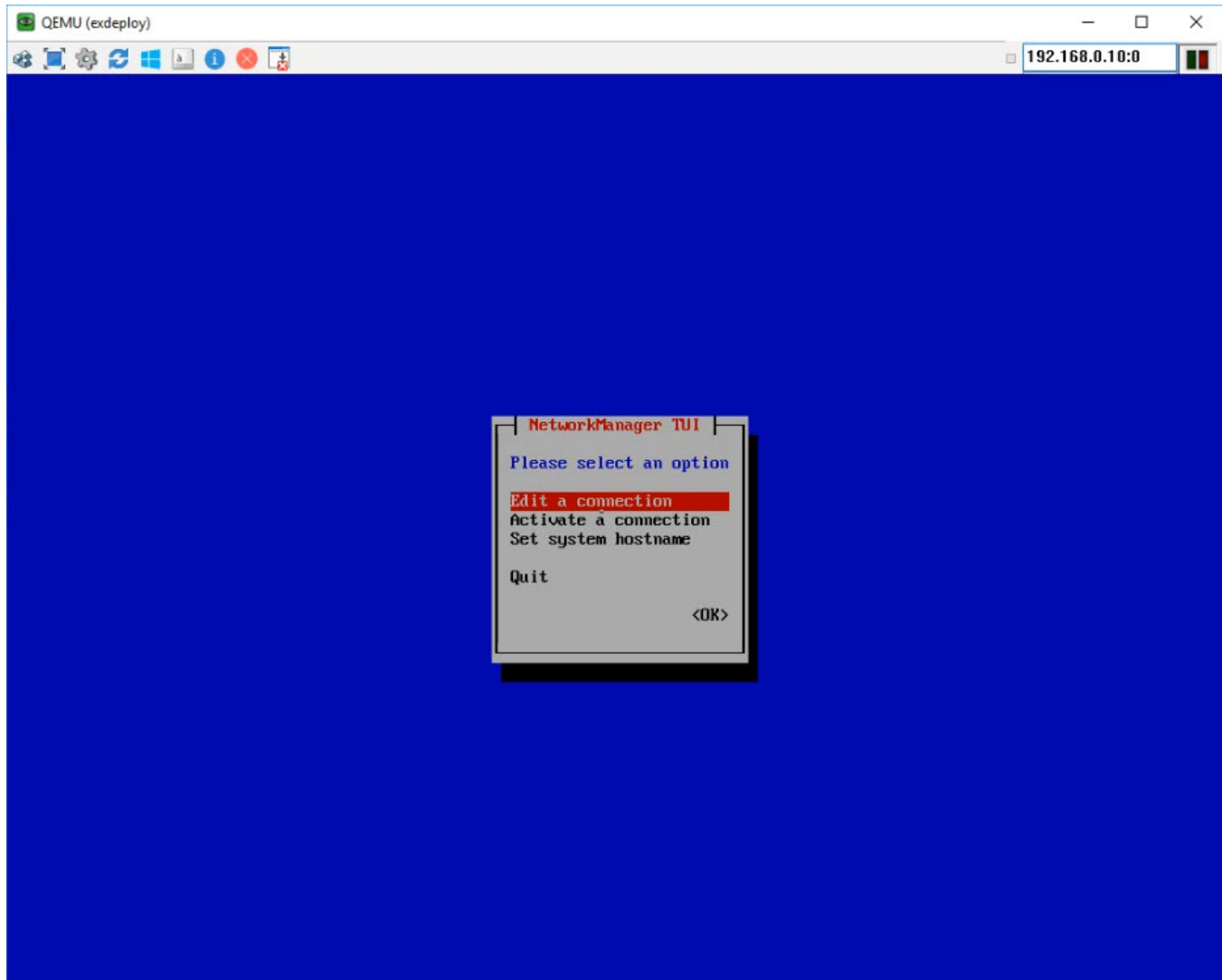


7. Log in as *root* user. The default password for *root* user is **default**.
8. Execute the following command to set **ens4** to a static setting:

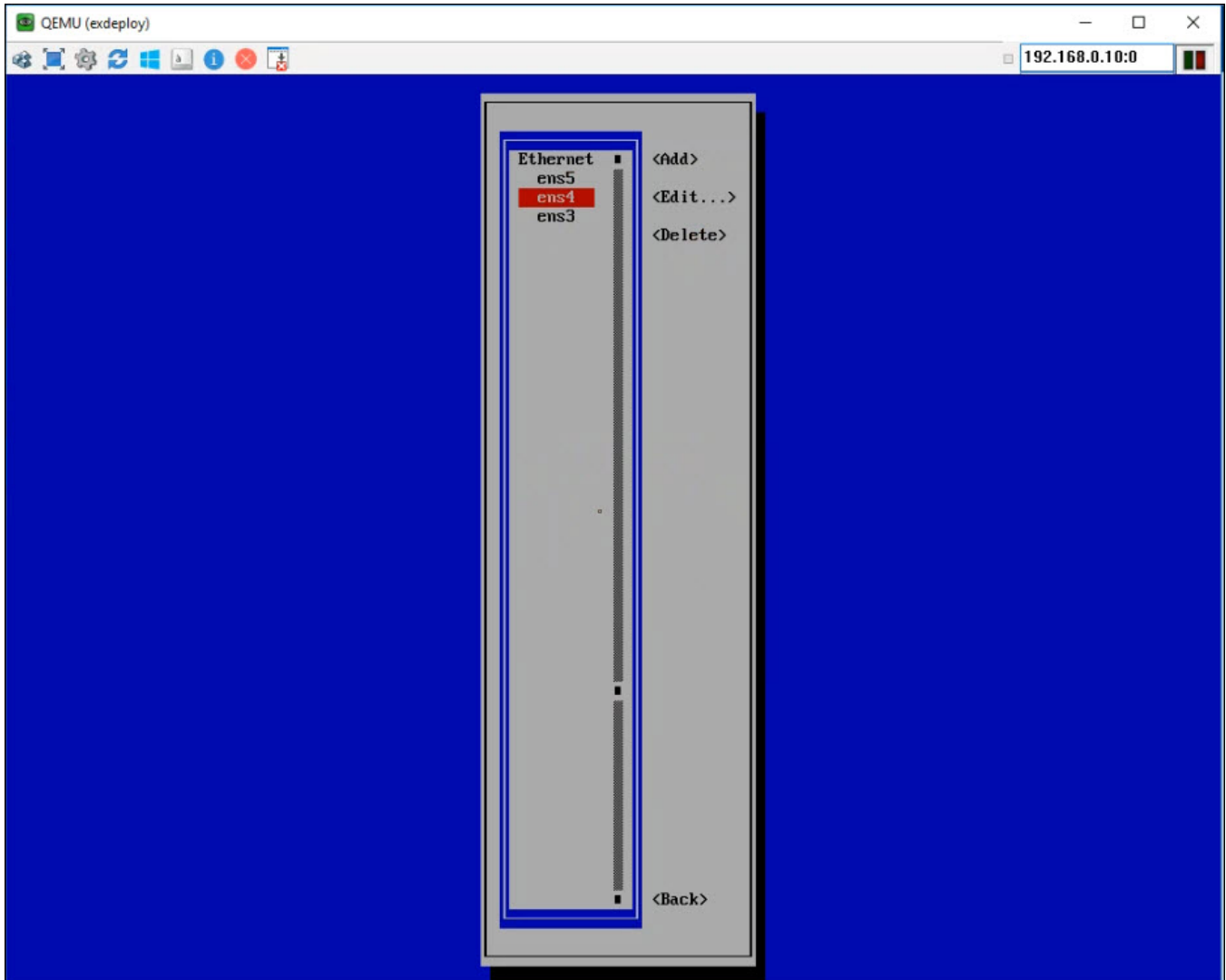
```
nmtui
```

The Network manager TUI screen is displayed.

9. From the options, select **Edit a connection** and press Enter.



10. From **Ethernet**, select **ens4** and select **Edit** to edit the LAN interface of the Deployment Tool virtual machine.



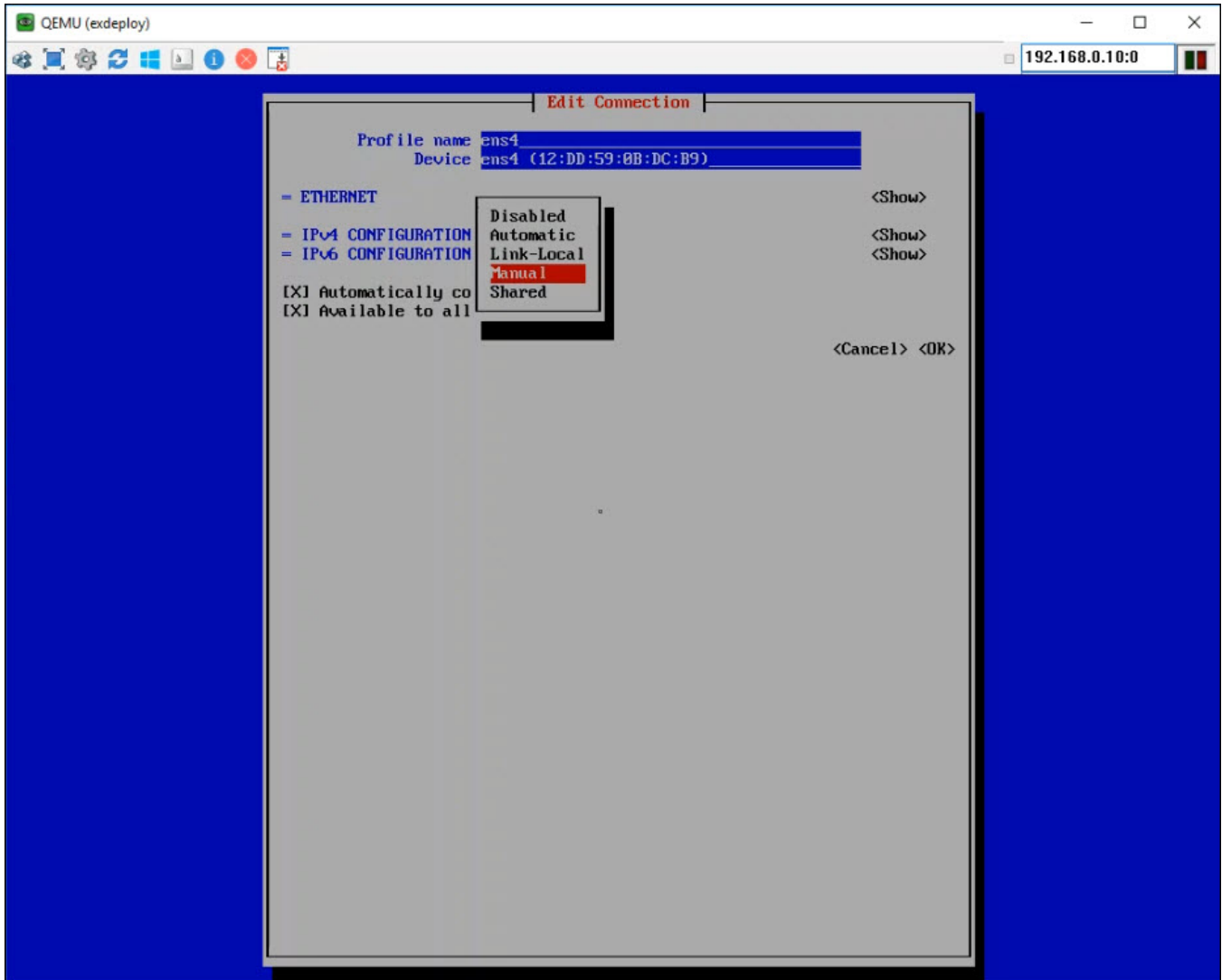
NOTE: The **ens3** option is used to edit the WAN interface, and the **ens5** option is used to edit the private interface that communicates with the EX Controller. Do **NOT** modify these options.

11. Press Enter.

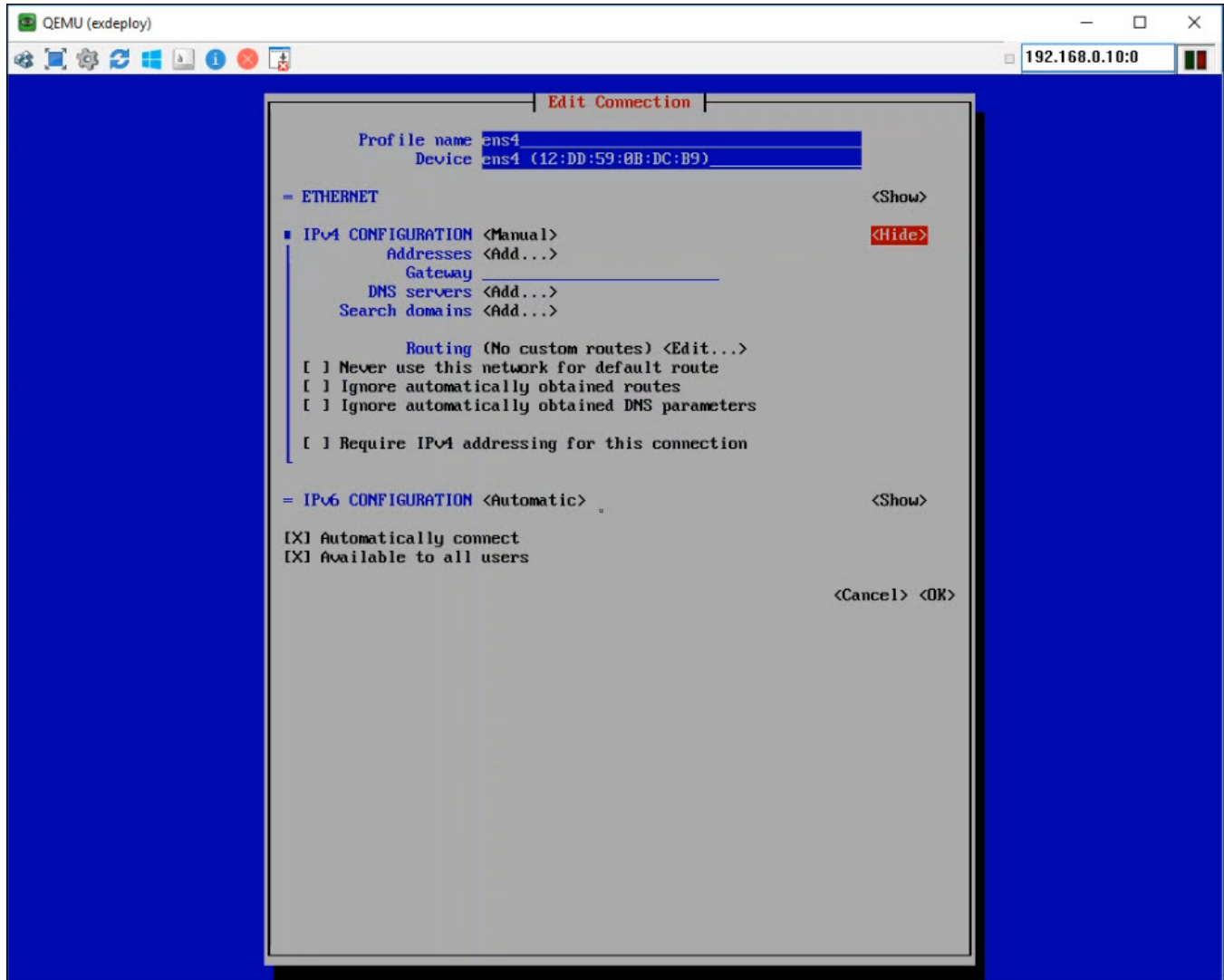
The **Edit Connection** screen is displayed.

12. Navigate to **IPv4 CONFIGURATION <Automatic>**, and press Enter.

13. From the dialog box, select **Manual**.



14. Select **<Show>** next to **IPv4 CONFIGURATION**, press Enter to expand the IP address configuration section.



15. Enter the following:

- a. **Addresses**—An available static IP address in the LAN for the Deployment Tool virtual machine.
NOTE: You can also enter a private IP address, such as 192.168.x.x, which can be accessed by the deployment PC only through 192.168.x.x interface.
- b. **Gateway**—Gateway IP address of the LAN.

16.

17. Select **OK** and press Enter.

The Network Manager TUI screen is displayed.

18. Click **Back** to save the configuration.

19. Click **Quit** to exit the Network Manager TUI screen.

The Deployment Tool virtual machine console is displayed.

20. Restart the network stack by executing the following command at the prompt for the changes to take effect:

```
systemctl restart network
```

21. Verify that the Deployment Tool virtual machine has the specified static IP address. Run the **ifconfig** command and verify whether the correct IP is assigned to **ens4**.

```

V2 192.168.0.10:0 (QEMU (exdeploy)) - VNC Viewer
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 12:c4:95:0b:dc:be txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 417 bytes 79548 (77.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.37.27.85 netmask 255.255.255.0 broadcast 10.37.27.255
    inet6 fe80::688c:63f4:f6fd:dbd prefixlen 64 scopeid 0x20<link>
    ether 12:c4:95:0b:dc:bf txqueuelen 1000 (Ethernet)
    RX packets 2566 bytes 157204 (153.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 375 bytes 64160 (62.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 169.254.10.2 netmask 255.255.255.0 broadcast 169.254.10.255
    inet6 fe80::416d:509e:884b:fbf7 prefixlen 64 scopeid 0x20<link>
    ether 12:c4:95:0b:dc:c8 txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 718 (718.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 124 bytes 10703 (10.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@exdeploy ~]#
    
```

22. Do one of the following:

- If you have specified a static IP address from the LAN, then do the following:
 - i. Disconnect the Ethernet connection between your deployment PC and the controller.
 - ii. Connect an RJ45 Ethernet cable from any one of the **ETH2** to **ETH5** ports of the EX Controller to the Layer2 switch on the LAN.
 - iii. Revert your deployment PC's IP scheme to **Obtain an IP address automatically**.
 - iv. Connect an RJ45 Ethernet cable from your deployment PC to the to the Layer2 switch on the same LAN.
- If you have specified a private network address (192.168.x.x), leave the EX Controller connected to the deployment PC.

23. Open a web browser (recommended Mozilla Firefox and Google Chrome), and type the IP address (specified in **step 15 (a)**) in the address bar, and press Enter.

The EX Controller Deployment Tool home page is displayed.

Mitel EX Controller Deployment - Deploying Help | Update | Reboot v1.1.13.0

Recall Progress Options

Platform variant

Call Manager type: MIVB

Call Manager image: Choose File No file chosen

USB:

General Settings

ARID: 42226718

Call Manager FQDN: ex41.vlab.local

Distinguished name: cn=ex41, ou=R&D, o=Mitel, l=Kanata, st=Ontario, c=CA

IPv4 DNS servers: 10.44.17.11, 10.44.17.31

IPv4 trusted network address: 10.0.0.0/8

Restore via console ☐

Enable secure EX Controller access ☐

24. Continue with [Updating the EX Controller Deployment Tool](#).

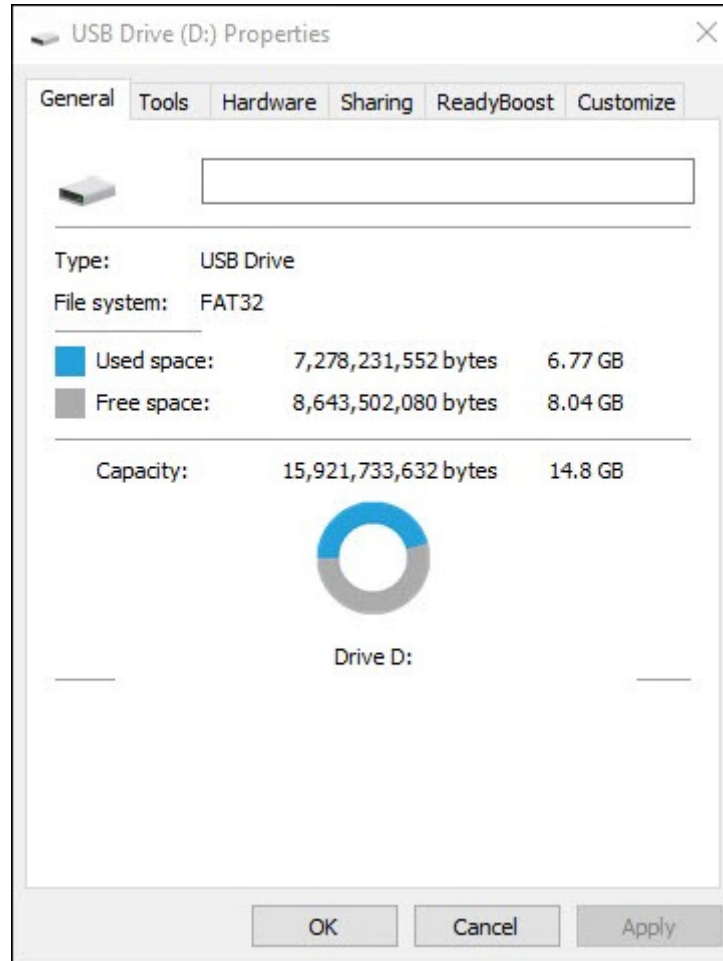
Assigning a static IP address by using a USB flash drive

NOTE: New installations are pre-installed with the EX deployment tool Version 1.1.13.0 or higher.

Prerequisites

- A USB flash drive with minimum 8-GB memory with FAT32 file system.

NOTE: To verify the file system of the USB flash drive, insert the USB flash drive into your PC. Right-click the USB flash drive, and click **Properties**.



Procedure

1. Copy the downloaded files **exdeploy-x.x.x.x.zip** and **MiVB-9.x.x.x-yy.img.zip** from your deployment PC to the USB flash drive.
2. Create a **lan.cfg** file with the static IP address and gateway IP address in the following format and copy the file to the USB flash drive:

addr=<static IP address/CIDR>
gateway=<IP address>
For example:
addr=10.38.75.41/24
gateway=10.38.75.1
3. Connect the USB flash drive to either port 6 or port 7 of the EX Controller. See [Connection Interfaces and LEDs](#).
4. Continue with either [upgrading the EX Controller Deployment tool](#) or proceed with a deployment.

Appendix B: Programming an R2 Trunk

Programming an R2 trunk

The Channel Associated Signaling (CAS) is a method of signaling where each traffic channel has a dedicated signaling channel. The signaling for a particular traffic circuit is permanently associated with that circuit. The EX Controller unit uses the R2 CAS protocol. This is a compelled sequence multi-frequency code signaling. In R2 signaling, the equipment units at the exchanges that send and receive digits, and the signaling between these units are usually referred to as register and inter-register signaling.

To program an R2 trunk on an EX Controller:

1. Log in to the EX Controller Web GUI with user name *admin* and enter the password that you use for logging in to the Server Manager. For more information about how to log in to EX Controller Web GUI, see [Log in to the EX Controller Web GUI](#).
2. Navigate to the **System > Hardware** tab.
3. Scroll down to the **PRI Ports Configuration** section.
4. In the **Signaling** drop-down list, select **R2**.

The screenshot shows the EX Controller Web GUI interface. At the top, there are tabs for System, Network, SIP Proxy, SBC, ISDN, POTS, SIP, Media, and Telephony. Below these are sub-tabs for Information, Services, Hardware, Endpoints, Event Log, Local Log, and Packet Capture. The 'Hardware' sub-tab is selected. Under 'Hardware', there are sections for Clock Reference Status, Clock Reference Configuration, PRI Ports Status, and PRI Ports Configuration. The 'PRI Ports Configuration' section contains a table with the following data:

Port	Line Type	Signaling
Slot1/E1T1	E1	Isdn

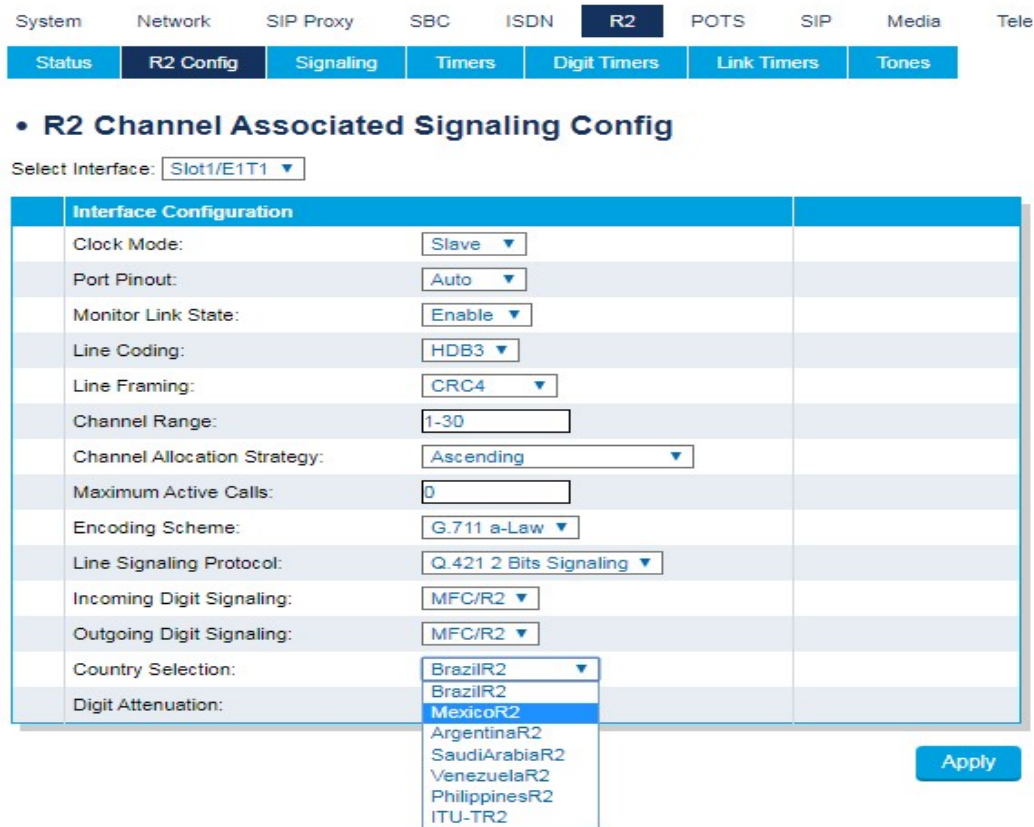
Below the table, there is a configuration section for 'Slot1/E1T1'. It has a 'Line Type' dropdown set to 'E1' and a 'Signaling' dropdown set to 'Isdn'. The 'Signaling' dropdown is open, showing options: 'Isdn', 'R2', and 'E&M'. The 'R2' option is highlighted. An 'Apply' button is located at the bottom right of the configuration section.

5. Click **Apply** to apply the changes.

6. Click the **restart the unit** link at the top of the page to restart the unit.

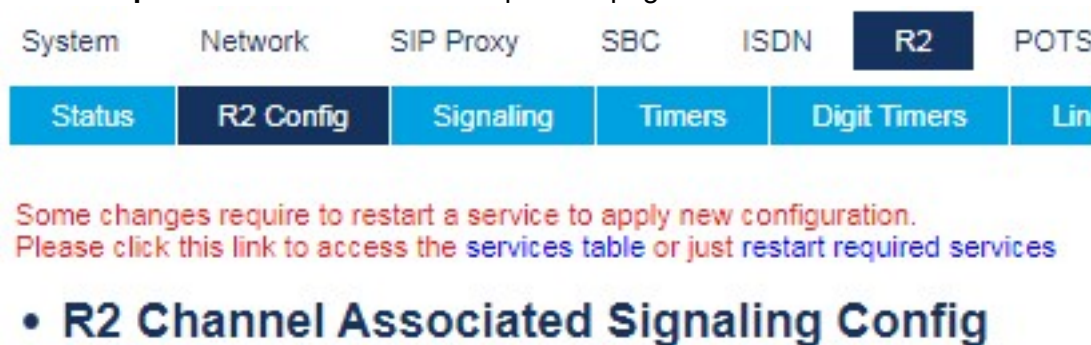


7. Click **Reboot**. The Controller takes approximately 2 minutes to reboot.
8. Log in to the EX Controller Web GUI after the reboot is complete.
9. Navigate to the **R2 > R2 Config** tab.
10. From the **Country Selection** list, select your country.



11. Click **Apply**.

12. Click **restart required services** link at the top of the page to restart.

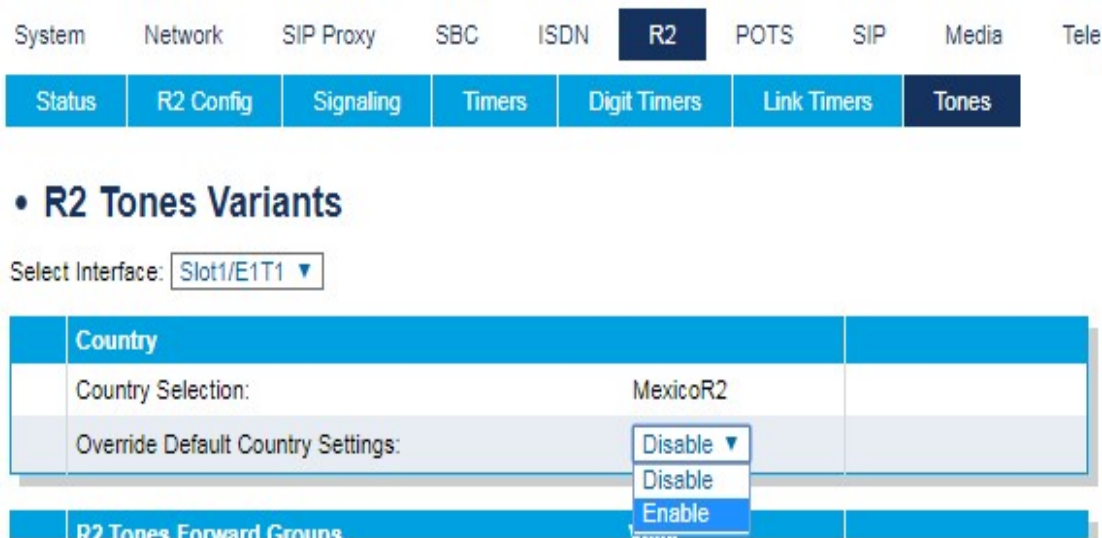


The EX Controller is now configured with R2 trunk with default settings.

Customize default settings

You can customize the default settings for Signaling, Timers, Digit Timers, Link Timers and Tones for the R2 trunk. The following steps describe the procedure for customizing Tones:

1. Log in to the EX Controller Web GUI.
2. Navigate to **R2 > Tones**.
3. In the **Override Default Country Settings** list, select **Enable**.



4. Scroll to the bottom of the page and click **Reset to default** to update the settings for your country.
5. Click the **restart required services** link at the top of the page to restart.
6. Change the settings according to your service provider's recommendations.
7. Click **Apply** to apply the change.
8. Click **restart required services**.

You can similarly customize the settings for Signaling, Timers, Digit Timers and Link Timers. **Enable** the **Override Default Country Settings** and customize the settings according to your service provider's recommendations.

Appendix C: Enabling USB Ports for the Deployment Tool


The Deployment Tool version 1.1.13 supports installation of MiVoice Business software image and upgrade of the Deployment Tool using a USB flash drive. This requires the USB ports on the EX Controller to be enabled for the Deployment Tool. For EX Controllers that do not have the version 1.1.13 pre-installed, the USB ports are disabled for the Deployment Tool by default.

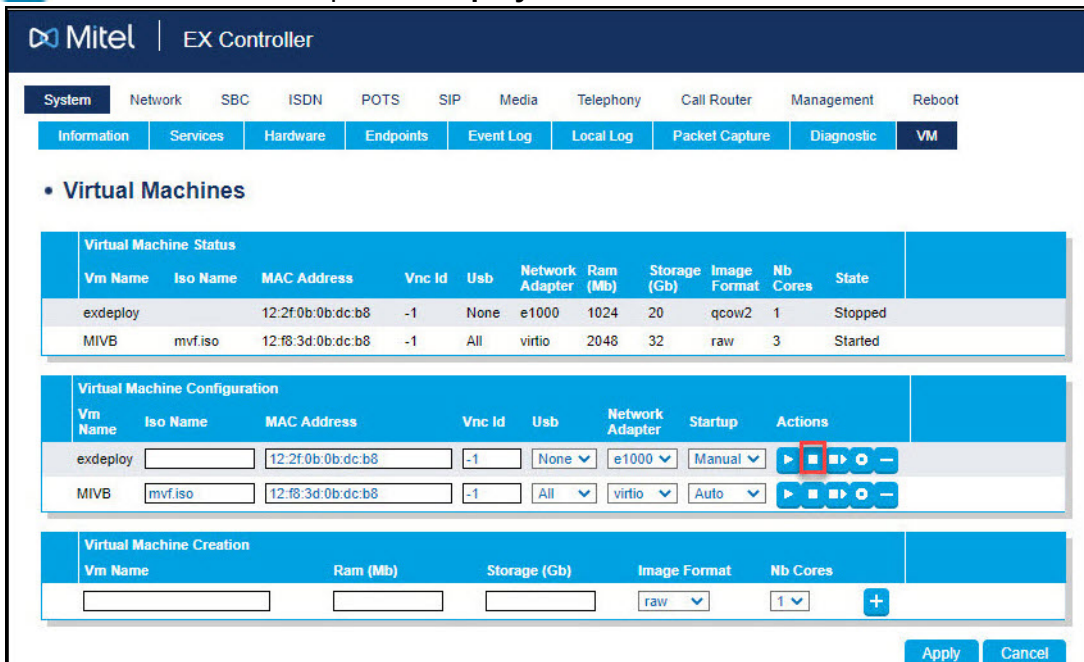
Procedure

Perform the following procedure to check and enable the USB port for the Deployment Tool, and to allow the Deployment Tool to use all three CPU cores:

1. [Upgrade the Deployment Tool](#) to version 1.1.13 or later.
2. [Log in to the EX Controller Web GUI](#).
3. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

4. Click  under **Actions** to stop the **exdeploy** virtual machine.



Mitel | EX Controller

System Network SBC ISDN POTS SIP Media Telephony Call Router Management Reboot

Information Services Hardware Endpoints Event Log Local Log Packet Capture Diagnostic VM


• Virtual Machines

Virtual Machine Status										
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State
exdeploy		12:2f:0b:0b:dc:b8	-1	None	e1000	1024	20	qcow2	1	Stopped
MIVB	mvf.iso	12:f8:3d:0b:dc:b8	-1	All	virtio	2048	32	raw	3	Started

Virtual Machine Configuration								Actions	
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup			
exdeploy		12:2f:0b:0b:dc:b8	-1	None	e1000	Manual			
MIVB	mvf.iso	12:f8:3d:0b:dc:b8	-1	All	virtio	Auto			

Virtual Machine Creation				
Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores
			raw	1

Apply Cancel

5. Change the **Usb** list corresponding to **MIVB** from **None** to **All**, and then click **Apply**. If **All** is already selected in the **Usb** list, skip this step.
6. Click  corresponding to **exdeploy** to start the **exdeploy** virtual machine.

7. Navigate to **Management > File**. If you are accessing the EX Controller using HTTP (not HTTPS), click **Activate unsecure file importation from the Web browser**.



8. Scroll down to the **VM files** table, click **vm/images/exdeploy.cfg** to download the exdeploy.cfg file to your PC.

VM files		
Name	Description	Size
vm/images/factory/exdeploy.cfg	Factory Virtual Machine configuration file (read-only)	1 KB
vm/images/factory/exdeploy.img	Factory Virtual Machine image file (read-only)	2.6 GB
vm/images/exdeploy.cfg	Virtual Machine configuration file	1 KB
vm/images/exdeploy.snapshot	Virtual Machine snapshot image file	6.3 GB
vm/images/MIVB.cfg	Virtual Machine configuration file	1 KB
vm/images/MIVB.raw	Virtual Machine image file	31.3 GB
6 file(s)		Total: 40.2 GB / Available: 3 GB

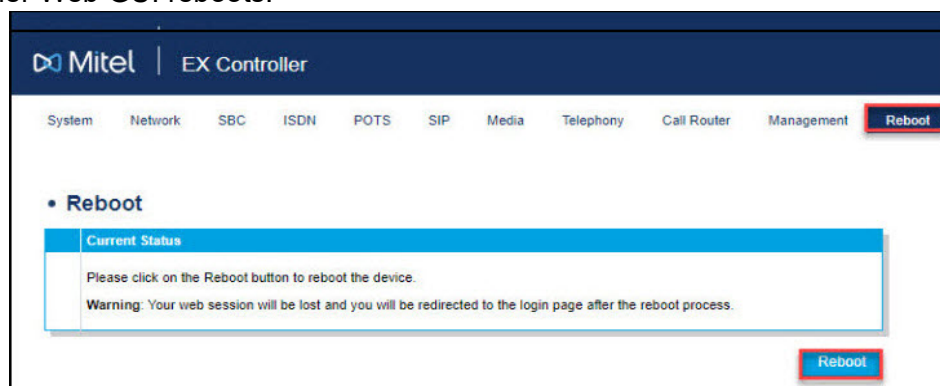
9. Open the **exdeploy.cfg** file using an editor (For example, Notepad) and change **CpuCount** to **3**.
10. Save the **exdeploy.cfg** file.
11. Scroll down to the **Import File Through Web Browser** table, select **vm/images**, in the **Path** list, click **Choose File**, select the updated **exdeploy.cfg** file, and then click **Import**.

Import File Through Web Browser	
Path	File
vm/images/	Choose File exdeploy.cfg

Import

NOTE: Do not copy the same **exdeploy.cfg** file to different EX systems as each EX has a unique date in the file.

12. After the **exdeploy.cfg** file is imported, click the **Reboot** tab and then click the **Reboot** button. The EX Controller Web GUI reboots.



13. After the EX Controller Web GUI reboots, [Log in to the EX Controller Web GUI](#).
14. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

15. In the **Virtual Machine Status** table, verify that the **Nb Cores** column for **exdeploy** shows **3**.

Virtual Machine Status

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State
exdeploy		12:37:91:0b:dc:b8	-1	All	e1000	1024	20	qcow2	1	Stopped
MIVB	mvf.iso	12:df:4c:0b:dc:b8	-1	All	virtio	2048	32	raw	3	Started

Virtual Machine Configuration

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
exdeploy		12:37:91:0b:dc:b8	-1	All	e1000	Manual	[Start] [Stop] [Restart] [Refresh] [Delete]
MIVB	mvf.iso	12:df:4c:0b:dc:b8	-1	All	virtio	Auto	[Start] [Stop] [Restart] [Refresh] [Delete]

Virtual Machine Creation

Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores
			raw	1

Apply Cancel

16. If the **MiVB** virtual machine was already installed, then by default, the **exdeploy** virtual machine does not start after the EX Controller reboots. To start the **exdeploy** virtual machine, stop the **MiVB** virtual machine, wait and refresh the page until the **MiVB** virtual machine is stopped, and then start the **exdeploy** virtual machine.
17. If you want to deploy MiVoice Business or upgrade the EX Controller Deployment Tool, copy the downloaded files **exdeploy-x.x.x.x.zip** and **MiVB-9.x.x.x-yy.img.zip** from your deployment PC to the USB flash drive.
18. If you want to [assign a static IP address for the EX Controller Deployment Tool](#), then create a **lan.cfg** file with the static IP address and gateway IP address in the following format and copy the file to the USB flash drive:
- ```
addr=<static IP address/CIDR>
gateway=<IP address>
For example:
addr=10.38.75.41/24
gateway=10.38.75.1
```
19. Insert the USB flash drive into either port 6 or port 7 of the EX Controller. See [Connection Interfaces and LEDs](#).
20. Continue with [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#).

# Appendix D - Programming Enterprise Gateway Trunks and Analogue FXS Ports

## Programming Enterprise Gateway Trunks

The Enterprise Gateways form is used to configure the IP address and the SNMP details of the EX controller.

**NOTE:** This form is applicable only to the EX Controller.

Before You Begin

Ensure you have the following information:

- When you add an EX Controller to the Enterprise Gateways form, if the Auto Program Trunk Profiles option is selected:
  - a. The system identifies the available endpoints on the EX controller and a trunk profile for each type of trunk endpoint is created.
  - b. The trunk endpoints in the Gateway Trunks form are auto-assigned to each of the trunk profiles based on the trunk types.
  - c. SIP Peer Network Elements and SIP Peer Profiles are created with the same names as the Gateway Trunk Profiles.

## Conditions

- The data changes performed on the Mediatrix Web Management Interface are not reflected in the System Administration tool or the Server Manager.
- You can only program one EX controller using this form.
- You cannot delete the entry for the local Enterprise Gateway.
- Use the SNMP credentials to configure the EX Controller.

## Programming PRI

Fill out the forms below in the order listed.

1. Trunk Attributes form - to check for an unused Trunk Attribute entry click **Trunks > Trunk Attributes**.
2. Gateway Trunk Descriptors form -
  - To program click Trunks > Enterprise Gateways > Gateway Trunk Descriptors from the left navigation pane.
  - Click the unprogrammed entry and click Change
  - Configure the line type to T1 or E1
    - NOTE:** If you change Line Type, the EX Controller (host) needs to be rebooted.
  - Configure Signaling to Isdn, R2, or Eam
  - Configure Endpoint Type to Te or Nt
  - Click Save

**3. Gateway Trunk Profiles form -**

- To program click Trunks > Enterprise Gateways > Gateway Trunk Profiles from the left navigation pane.
- Click Add, enter the Name, enter the unused Trunk Service Number.
- Click Save.

**4. Gateway Trunks form -**

- To program click Trunks > Enterprise Gateways > select an entry > change the E1T1 endpoint and select the Gateway Trunk Profiles name

**5. Gateway Configuration Scripts form -**

- To program click Trunks > Enterprise Gateways > Gateway Configuration Scripts.
- Select slot
- Click on the drop down menu of the Default Configuration Files, to select an appropriate
- Mitel per slot for the PSTN circuit
- Click Execute

**6. ARS Routes - ARS continues to be provisioned in the traditional manner by assigning a route to a digit or digit string. Complete the following fields in this form:**

- Select SIP Trunk/Enterprise Gateway from the pull-down list in Routing Medium.
- Select a Gateway Trunk Profile name from the SIP Peer Profile pull-down list.

## Programming FXO

Fill out the forms below in the order listed.

**1. Trunk Attributes form - To check for an unused Trunk Attribute entry click Trunks > Trunk Attributes.****2. Gateway Trunk Descriptors form - To view the status click Trunks > Gateway Trunk Descriptors > select an entry > click Change.****3. Gateway Trunk Profiles form -**

- To program click Trunks > Enterprise Gateways > Gateway Trunk Profiles from the left navigation pane
- Click Add, enter the Name, enter the unused Trunk Service Number
- Click Save

**4. Gateway Trunks form - To program click Trunks > Enterprise Gateways > select/change the FXO endpoint and select the Gateway Trunk Profiles name.****5. Gateway Configuration Scripts form (Optional)**

- To program click Trunks > Enterprise Gateways > Gateway Configuration Scripts.
- Select slot
- Click on the drop down menu of the Default configuration files, to select an appropriate Mitel per slot for the PSTN circuit
- Click Execute

**6. ARS Routes - ARS continues to be provisioned in the traditional manner by assigning a route to a digit or digit string. Complete the following fields in this form:**

- Select SIP Trunk/Enterprise Gateway from the pull-down list in Routing Medium.
- Select a Gateway Trunk Profile name from the SIP Peer Profile pull-down list.

**NOTE:** After successfully adding a Gateway Trunk Profile, Network Elements and SIP PeerProfile forms will have entries with the same Gateway Trunk Profiles name.

## Programming Analogue FXS Ports

The User and Services Configuration form combines the functions of several system forms into a single form; however, you can still access and use the individual forms.

### Programming

Fill out the form User and Service Configuration to program Analogue FXS Port:

- Click User and Devices > User and Services Configuration from the left navigation pane.
- To add a phone, click Add > select Default User and Device
- Click on the tab User Profile > enter the name
- Click on the tab Service Profile > enter the number. Set the device type to AnalogFXS
- Click on the tab Device Details. By default the first Endpoint ID is selected but, you can manually select the required Endpoint ID from the drop down.
- Click Save Changes.