



A MITEL
PRODUCT
GUIDE

MiVoice Business

System Manual for Mitel SMB Controller

Release 10.1 SP1
Document Version 1.0

July 2024

Notices

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

Trademarks

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

[®], [™] Trademark of Mitel Networks Corporation

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 About this Document.....	1
1.1 What's New in This Document.....	2
1.2 Related Documents.....	3
1.3 Download documents, system software and tools.....	5
 2 About SMB Controller.....	 6
2.1 Introduction.....	6
2.2 SMB Controller Overview.....	7
2.2.1 SMB Controller Manager.....	10
2.2.2 SMB Controller Manager user accounts.....	11
2.2.3 Display and Control Panel.....	12
2.2.4 Operating Modes.....	14
2.2.5 Configure User Access Control.....	22
2.3 Network Scenarios.....	23
2.4 Hardware Installation.....	28
2.4.1 Safety Information.....	28
2.4.2 System Components.....	31
2.4.3 Hardware.....	32
2.4.4 Mounting the SMB Controller.....	42
2.5 Power Up the SMB Controller.....	57
2.5.1 115/230 V power supply.....	57
2.5.2 Uninterruptible power supply (UPS).....	58
2.5.3 Earthing and protecting the communication server.....	59
 3 About Mitel Standard Linux.....	 61
3.1 Server Manager.....	61
 4 About MiVoice Business.....	 65
4.1 Purpose and function.....	65
4.2 Data Protection.....	65
4.3 Feature Interactions.....	66
4.3.1 Embedded Voice Mail.....	66
4.3.2 Trunks.....	67
4.3.3 Analog Loop Start (LS) Trunks.....	67
4.3.4 ONS (FXS) Devices.....	67
4.3.5 DSP Allocation.....	68
4.3.6 Loudspeaker Paging.....	69
4.3.7 Music on Hold (MOH).....	69
 5 About MiVoice Border Gateway.....	 71

6 About CloudLink Gateway.....	73
7 About Mitel Performance Analytics Probe.....	74
8 About Initial Configuration Wizard (ICW).....	75
8.1 ICW Backup and Restore.....	76
9 Deployment Steps for the MiVoice Business Solution on SMB Controller.....	77
9.1 Initial Setup of SMB Controller.....	80
9.1.1 Requirements.....	81
9.1.2 Set up Initial Network Access to the SMB Controller.....	81
9.1.3 Set Credentials for the SMB Controller.....	86
9.1.4 Identifying the Call Server for SMB Controller.....	88
9.1.5 Configure SMB Controller IP Address.....	88
9.1.6 Set Date and Time.....	90
9.1.7 Upgrading the SMB Controller Software.....	91
9.1.8 Install MSL Container.....	93
9.1.9 Initial MSL Network Setup.....	96
9.1.10 Licensing the Solution.....	104
9.1.11 Server Manager Requirements for Software Download-Blades.....	110
9.1.12 Install MiVoice Business Blade.....	110
9.1.13 Install MiVoice Border Gateway Blade.....	112
9.1.14 Install CloudLink Gateway Blade.....	116
9.1.15 Install Mitel Performance Analytics Probe Blade.....	116
9.1.16 Install Initial Configuration Wizard (ICW) Blade.....	117
9.2 Configure the Applications.....	118
9.2.1 Initial Configuration Wizard.....	118
9.2.2 Configure MiVoice Business on the SMB Controller.....	141
9.2.3 Configure MiVoice Border Gateway on the SMB Controller.....	148
9.2.4 Configure CloudLink Gateway for MSL.....	149
9.3 Integrate Applications.....	149
10 Migration.....	151
10.1 Platform Migration.....	151
10.1.1 Migrating CX-II, MXe-III, AX to SMB Controller.....	152
10.1.2 Migrating Virtual, ISS, or EX Controller from SMB Controller.....	152
10.2 Migration Tool.....	153
10.3 Migration from Pre-9.0 MiVoice Business Platform to SMB Controller.....	153
10.4 Migrating Embedded Application to offboard.....	154
10.4.1 Offloading Mitel Border Gateway + CloudLink Gateway.....	154
10.4.2 Mitel Performance Analytics Probe.....	155
11 Maintenance.....	156
11.1 Shutdown and Reboot.....	156

11.1.1 Restart the SMB Controller.....	156
11.1.2 Shutting Down the SMB Controller.....	157
11.2 Start/Stop/Restart/Uninstall the MSL Container.....	157
11.3 Restart the MSL Server.....	158
11.4 Restart the SMB Controller via SMB Controller Front Panel.....	158
11.5 Managing Multiple Admin Accounts on SMB Controller Manager.....	158
11.6 Changing the IP Addresses.....	161
11.7 Backup and Restore.....	163
11.7.1 Backup Using Server Manager.....	163
11.7.2 Backup Using MiVoice Business System Administration Tool.....	165
11.7.3 Restore Using Server Manager Backup.....	165
11.7.4 Restore Using MiVoice Business System Administration Tool.....	165
11.8 Data Maintenance.....	166
11.9 Update Software.....	166
11.9.1 System software.....	166
11.9.2 Upgrading the MSL Container.....	167
11.10 Hardware Update.....	169
11.10.1 Prerequisites.....	169
11.10.2 System Information.....	169
11.10.3 Disk Replacement.....	169
11.10.4 Replace Units.....	170
11.10.5 Replace Interface Cards.....	171
11.10.6 System Modules.....	172
11.10.7 Mainboard.....	173
11.11 Monitor the eMMC Wear.....	174

12 Troubleshooting..... 176

12.1 Factory Default Static IP Address.....	176
12.2 Factory Reset the SMB Controller.....	178
12.3 Server Manager LAN IP is locked up from the Management PC.....	179
12.4 SMB Controller Starts up Automatically.....	180
12.5 Unable to Access the Server Manager/ESM.....	181
12.6 Unable to Access the SMB Controller Manager Using the Default IP Address.....	181
12.7 Unable to Access the SMB Controller Manager through web browser using IP address provided by DHCP Server.....	182
12.8 Unable to log into the SMB Controller Manager.....	182
12.9 Web Proxy to MiVB Intermittently Fails with a 503 Error.....	182
12.10 Media Gateway Communications Error.....	183

About this Document

1

This chapter contains the following sections:

- [What's New in This Document](#)
- [Related Documents](#)
- [Download documents, system software and tools](#)

The System Manual for MiVoice Business solution on Mitel SMB Controller is intended for certified MiVoice Business technicians who are installing, upgrading, maintaining, or troubleshooting the Mitel® MiVoice Business software deployed on the SMB Controller.



Note:

In this document, it is presumed, that the Mitel SMB Controller is loaded with a MiVoice Business application software. This assumption applies, even when the expressions Mitel SMB Controller, SMB Controller, or communication server are used.

The document is also intended for planners, installers, and system managers of phone equipment. Basic knowledge of phones and IP technology is required to understand the content.

The system manual is available in the PDF format and can be printed if necessary. Navigation in PDF format is based on the topic titles, table of contents, cross references, and index. All these navigation aids are linked; that is, a mouse click takes you directly to the corresponding places in the manual. We have also ensured that the page numbering in the PDF navigation corresponds to the page numbering of the manual, making it much easier to navigate to a particular page.

Referenced menu entries and parameters appearing on terminal displays or on the user interfaces of the configuration tools are highlighted in italics and in color for a clearer orientation.

General Considerations

Information icons used in this document, such as Hazard, Warning, Caution and so on (mentioned in the [Safety Information](#)) are explained in this document for additional information and document references.



Note:

Failure to observe information identified in the notes, cautions, warnings in this document can lead to equipment faults or malfunctions or affect the performance of the system.

TIP: Additional information about the handling or alternative operation of equipment.

See also

Reference to other chapters within the document or to other documents.

1.1 What's New in This Document

This section describes changes in this document due to new and changed functionality in MiVoice Business release 10.1 SP1. The changes are summarized in the following table.

Table 1: Document Version 1.0

Feature/Enhancement	Document Updates	Location	Publishing Date
SMB Controller Noise Level, Power Requirements, and Heat Dissipation	Updated the Location Requirements section for noise level, power requirements, and heat dissipation.	Location requirements on page 44	July 2024
Multiple Admin Accounts on SMB Controller Manager	Documented the procedure to add and delete the multiple admin accounts on the SMB Controller Manager.	Managing Multiple Admin Accounts on SMB Controller Manager on page 158	July 2024
Monitor the eMMC Disk Wear	The document has been updated to include information about proactive monitoring of the wear and lifespan of the eMMC disk on the SMB Controller.	Monitor the eMMC Wear on page 174	July 2024
Password Rules	The password rules for the SMB Controller have been updated to allow for an increased number of characters and the addition of new special characters.	Set Credentials for the SMB Controller on page 86	July 2024
Server Manager Requirements for Software Download-Blades	Updated the document to include instructions on the Server Manager Requirements for Software Download-Blades.	Server Manager Requirements for Software Download-Blades on page 110	July 2024

Feature/Enhancement	Document Updates	Location	Publishing Date
DHCP servers must provide option 6 in DHCP Offer for SMBC to accept IP address from the DHCP server	Document updated to detail DHCP servers' option 6 requirement for SMBC to accept the IP address from the DHCP server.	Deployment Steps for the MiVoiceBusiness Solution on SMB Controller Set up Initial Network Access to the SMB Controller Using the DHCP provided IP Address Factory Reset the SMB Controller Unable to Access the SMB Controller Manager through web browser using IP address provided by DHCP Server	July 2024

1.2 Related Documents

Document Title	Description	Location
SMB Controller System Manual	This document	Document Center
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 running a pre-9.0 MiVB release to MiVoice Business Release 9.0 or later, or to another platform.	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 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
MiVoice Border Gateway	Provides information on how to install, maintain, configure, and get performance information for the MiVoice Border Gateway and associated products.	Document Center
Mitel Performance Analytics	Provides instructions for installing a new Mitel Performance Analytics (MPA) monitoring system as well as its operations.	Document Center
CloudLink	Provides information on how to integrate CloudLink with MiVoice Business.	Document Center

Document Title	Description	Location
MiVoice Business - Personal Data Protection and Privacy Controls	Provides product security controls and features guidance to users who are setting up MiVoice Business security processes and security controls in place to comply with data security regulations.	Document Center
AG4124 Analog Gateway Administration Guide	Provides information about the AG4124 Analog Gateway, including instructions on how to install, configure, and use the Analog Gateway.	Document Center

1.3 Download documents, system software and tools

Before you start, download the documents and applications from the proprietary Mitel sites.

Proceed as follows to organize all downloads in a common folder:

1. Download the *Documentation set* from the [Mitel document portal](#).
2. If your Mitel SMB Controller does not have internet access, download the latest MiVoice Business application software and the SMB Controller system software (for example, “*Mitel-SMBCv2_Management-1.3.0.25_Beryllium.zip*”) from the Mitel Software Download Center > MiVoice Business > MiVoice Business Release 10.0 > MiVB 10.0 > SMBC into the folder named *Mitel*.

Required tools

The following tools are required to remove and install the SMB Controller cover and for DSP installation.

- Torx T20 screwdriver for removing and installing the SMB Controller cover screws, DSP cards, and chassis grounding screw.
- Phillips #2 screwdriver for removing and installing the fan (FRU) screws.
- Slotted screwdriver for removing and installing the wall mounting screws.

About SMB Controller

2

This chapter contains the following sections:

- [Introduction](#)
- [SMB Controller Overview](#)
- [Network Scenarios](#)
- [Hardware Installation](#)
- [Power Up the SMB Controller](#)

The Mitel Small to Medium Business Controller (SMBC) is a hardware platform that supports the MiVoice Business call processing software. This topic provides a brief overview of the SMB Controller loaded with the MiVoice Business solution software, the positioning within the MiVoice Business series and the networking possibilities. It also features the system phones, the applications and the application interfaces.

2.1 Introduction

The Mitel SMB Controller is a multi-service business controller capable of running the MiVoice Business solution. The SMB Controller has been developed to continue Mitel's commitment to deliver simplified deployments for small to medium businesses or branch offices. A single SMB Controller embeds CloudLink Gateway, MiVoice Border Gateway, MiVoice Business, Mitel Performance Analytics Probe, Initial Configuration Wizard and as such provides an all-in-one solution for the SMB or branch office market. The SMB Controller is designed to integrate with a wide variety of legacy and IP systems, Mitel call control platforms, and management tools such as Mitel Performance Analytics.

The MiVoice Business Solution on the SMB Controller has been engineered to support 150 Multi-Device User Groups (MDUGs) consisting of three Members:

- Hot Desk user (HDU) or Teleworker User with 150 Registration Directory Numbers for the HDUs to log in to
- External Hot Desk user (EHDU)
- SIP User, including MiCollab Softphone user



Note:

Multi-Device User Groups (MDUGs) with three Members represents an average scenario. Some MDUGs may have more Members, and some might have fewer.

The software components of MiVoice Business Solution loaded on the SMB Controller are:

- [Mitel Standard Linux \(MSL\)](#)
 - [Server-Manager](#): Server Manager is a web-based administrator portal that provides the administrator means to manage the MSL Server and the installed applications.
 - Installation/Upgrade of the Initial Configuration Wizard Blade.
 - Launch Initial Configuration Wizard from server manager.
- [MiVoice Business](#): MiVoice Business is a call processing application that runs on several hardware platforms including the SMB Controller.
- [MiVoice Border Gateway](#): The MiVoice Border Gateway (MBG) provides advanced functionality such as Application and Web Proxy, Teleworker support, Advanced SIP Trunk proxying (including KPML), Secure Recording Connector (SRC), SIP Trunk Proxying allows connection to an external Call Recording Equipment (CRE), API and Proxy for remote applications, CloudLink Gateway, and Advanced SIP Trunk proxying (including Key Press Markup Language (KPML)¹).
- [CloudLink Gateway](#): CloudLink Gateway is a technology that enables communication between the on-premises PBX (such as MiVoice Business) and cloud-based applications such as Mitel One and Mitel MiVoice Office.
- [Mitel Performance Analytics](#): Mitel Performance Analytics (MPA) is an optional blade that provides integration with Mitel Performance Analytics Cloud Service to provide users with real-time alerts, detailed reporting and ubiquitous accessibility with secure remote access.
- Mitel Embedded Linux Software: a customized version of the Linux operating system that is specifically designed and optimized for SMB Controller. It is lightweight, easy to use and maintain, and provides a reliable and robust platform for running the Mitel software and it allows easy integration with other Mitel products and solutions.
- [SMB Controller Manager](#)
 - Controller Manager: Controller Manager is a web-based UI for configuring the SMB Controller.
- Initial Configuration Wizard Blade
 - Provisioning of MiVoice Business, MiVoice Border Gateway

2.2 SMB Controller Overview

The base operating system is Mitel Embedded Linux Distribution software running Docker software. A single Container is running Mitel Standard Linux (MSL) with the MiVoice Business (MiVB), Mitel Border Gateway (MBG), and CloudLink Gateway (CLGW), Mitel Performance Analytics Probe (MPA Probe), and Initial Configuration Wizard (ICW) Blades.

The SMB Controller:

- Allows for integration with analog devices.
- An appliance platform, ready for easy customer installation.
- Is an all-in-one solution for MiVoice Business that includes features such as voicemail, call routing, and conference calling, as well as other functionalities like Mitel Border Gateway, Mitel Cloud Gateway, Mitel Performance Analytics Probe, and Initial Configuration Wizard. It allows an easy setup and administration of the communication system and provides a web-based management.

¹ Keypad Markup Language (KPML) is used to indicate DTMF tones in SIP messaging. KPML is used by the Key Press Stimulus Package as a SIP Event Notification Package. Endpoints will send DTMF tone indications via NOTIFY messages.

Note:

As the SMB Controller does not support 802.1Q VLAN Trunks, the SMB Controller does not set an 802.1p Ethernet priority. The SMB 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 (VLAN could be a different number but it must not be tagged). 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](#).

Note:

The CloudLink Gateway Blade is installed via the MSL container, which runs sibling container in the Mitel Embedded Linux Distribution software.

To support the installation and deployment of multiple applications, an Integrated Configuration Wizard is used.

Network Deployment Rules for MiVoice Business Only

Following are some general network deployment rules that you must consider before getting started:

Two static IP addresses on the same subnet are required: one for the SMB Controller and the other for MSL (to access Server Manager and ESM; MiVoice Business application uses the same IP address).

Network Deployment Rules for MiVoice Business with the MiVoice Border Gateway

When both MiVoice Business and MiVoice Border Gateway applications are installed on the SMBC, the following are some of the Network Deployment Rules:

- The SMB Controller MiVoice Border Gateway can use the following networking profiles:
 - Co-Resident with Call Manager networking profile, which is similar to the Server-Gateway model. The WAN port must not be directly connected to the Internet. The WAN port should connect to the ISP's or customer's firewall which in turn is connected to the Internet.
 - Custom mode, which allows the MiVoice Border Gateway to be deployed in a customer's DMZ (i.e., behind an external NAT firewall).
- Deployment using all three Mitel Border Gateway NIC Interfaces is not supported on the SMB Controller Mitel Border Gateway. SIP Trunks and Teleworker Phones must be on the same WAN Interface.
- Four static IP addresses are required:
 - Three internal static IP addresses on the same LAN (one for the SMB Controller, one for MSL/ESM and one for the MiVoice Border Gateway).
 - One external static IP address on the WAN.

In addition to the platform and the embedded interfaces, the SMB Controller also supports four expansion interface cards that can provide FXO or additional FXS capability.

Ethernet Ports

On the front of the SMB Controller, there are two physical Gigabit Ethernet Ports (Eth0 and Eth1) used in this solution. Eth2 is not used.

- Eth0
 - Always used to connect to the LAN.
 - VLAN tagging is not supported.

Note:

The Eth0 Port must be connected to an external L2 Switch Port that is configured as Untagged. Connecting the Eth0 Port to an external L2 Switch Port configured as Tagged will not work.

- Three static internal IP addresses on same Subnet.

Warning:

The network interfaces of the SMB Controller should always be behind a firewall and should never be directly connected to the Internet.

- MSL Server Manager and MiVoice Business ESM.
- Mitel Border Gateway LAN Port.
- SMB Controller Manager.
- Eth1
 - Always used to connect to the ISP.
 - One static external IP address from the ISP for the Mitel Border Gateway WAN Port.
 - At initial installation, no IP address assigned to Eth1.
 - The Mitel Border Gateway requires two IP addresses: one for the ISP and one for the LAN.
 - The Server Only mode is not supported by the SMB Controller Mitel Border Gateway.

MiVoice Business Solution on the SMB Controller Block Diagram

This is an overall Block Diagram of the solution.

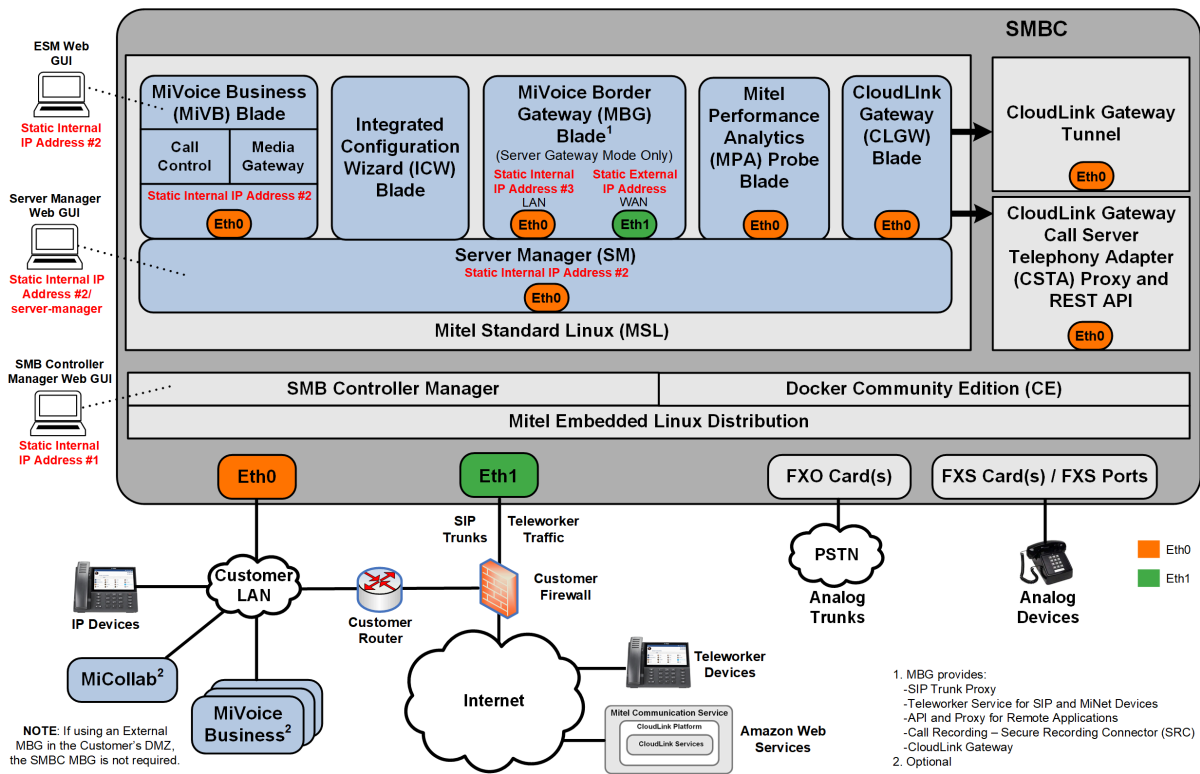


Figure 1: MiVoice Business Solution on the SMB Controller Block Diagram

Devices Supported

The MiVoice Business on SMB Controller will support all Analog Sets, IP Sets and SIP Sets that are supported on MiVoice Business application.

2.2.1 SMB Controller Manager

The SMB Controller is a pre-installed web-based configuration tool available on all Mitel SMB Controller, independent of a loaded call manager or other software application. It offers a simple, user-friendly interface and an online help for some basic configurations possibilities and maintenance tasks as follows:

- Upgrading the SMB Controller system software.
- Upgrading and managing the Mitel Embedded Linux Distribution software.
- Installing, upgrading, and managing the Mitel Standard Linux (MSL) Container for the MiVoice Business on SMB Controller project.
- Manage the IP addresses for the platform (Controller Manager)
- Manage the Primary and Secondary DNS and Domain
- Manage the Date and Time of the system

Mitel | SMB Controller Manager | SSH access is enabled | Welcome admin | English

System overview

System information

Configuration

Software

Security

Maintenance

General	
Host name	SMBCv2
Domain	mitel.com
Equipment ID (EID)	50065AE28839FCEE507BBEC753521E805920
Uptime	4d 0h 28m 34s
System time	2023-01-09 20:00
Management version	Mitel Embedded Linux Distribution 1.3.0.26 (Beryllium)
Firmware version (U-Boot / Device Tree)	0.0.0.11 / 1.1.1.0
RAM size / Disk size	8 GB / 37.98 GB
CPU clock speed	1600 MHz
Call server	MiVoice Business

	Mainboard (SMB)	CPU module (CPM-4)
Serial number	3MEFW2226D024XW	3MFFW2226A02C62
PCBA number	5601022202R	5601057301R
Revision	D / 02	A / 02
HW ID / HW version	11 / 00	03 / 01

CAREFULLY READ THE FOLLOWING AGREEMENT : [EULA](#) - INSTALLATION AND USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT

[License terms](#) for the Open Source components included in this software

Copyright © 2022 Mitel Networks Corporation - All rights reserved

Figure 2: SMB Controller Manager Landing Page

The SMB Controller file system comprises the system software, the emergency system software and the boot software. The SMB Controller Manager (including the help files) is part of the system software and in a reduced form part of the emergency system software. Usually there is no need to access the SMB Controller file system, as all needed functions are available in the SMB Controller Manager. For special cases you can access the SMB Controller file system via an SSH session.

Access: To access the login page of a brand new or a factory reset SMB Controller, enter the IP address of your SMB Controller including the port number in your browser (for example, 10.100.98.50:8443).

Table 2: Default user account SMB Controller Manager in normal mode

Username	admin
Password	admin

2.2.2 SMB Controller Manager user accounts

For the SMB Controller Manager, there are two default user accounts. One account is for initial access, when the SMB Controller is started up and runs in normal mode. The other account is used when, for any reason, the SMB Controller software is not running, correctly and the SMB Controller has to start up in emergency mode:

Default user account for initial access in normal mode

To access SMB Controller Manager the first time in normal mode, enter the following:

Table 3: Default user account SMB Controller Manager in normal mode

Username	admin
Password	admin

Note:

To prevent unauthorized access to the SMB Controller Manager, it is necessary to modify the default password during first access.

2.2.3 Display and Control Panel

The display and control panel of the SMB Controller on the front panel consists of an LED display panel and a pilot key. It is used to indicate operating states and carry out functions.

2.2.3.1 LED Display

The front panel contains an LED display field with a total of 9 labeled LEDs. It is used as an operating state and error indicator during the start-up phase and during operation.

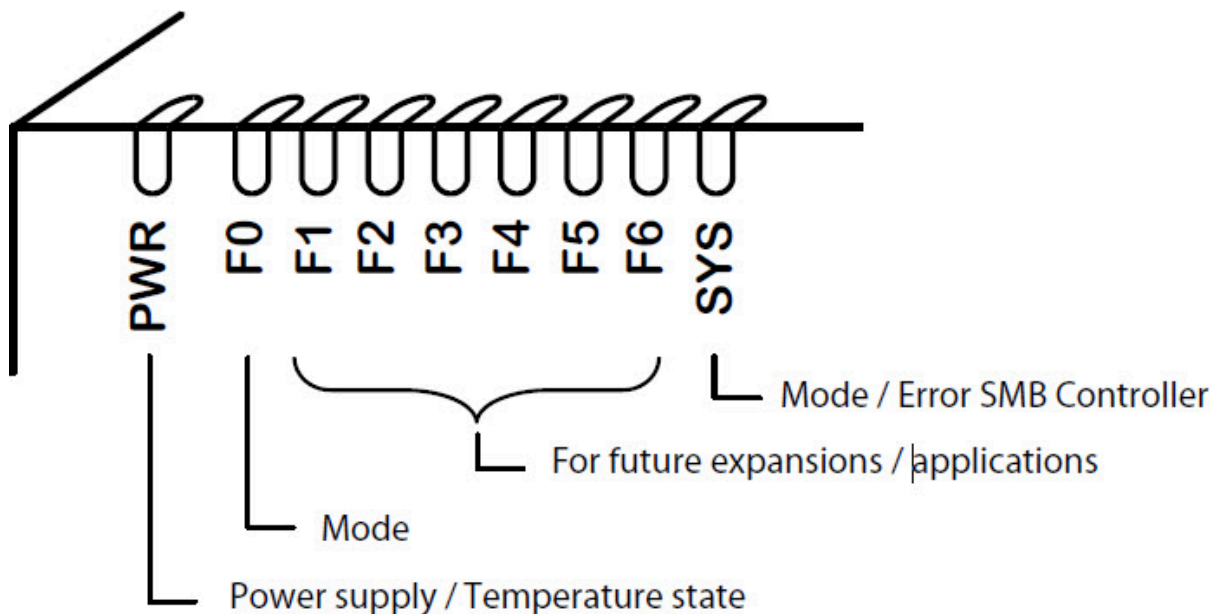


Figure 3: LED display

Each LED can take on one of four states: green (G), orange (O), red (R) and inactive. In general, the colors have the following meaning:

Table 4: Significance of the LEDs colors

Color		Meaning
Inactive		Switched off
Green		Normal operation / everything in order
Orange		Function is being carried out / is active
Red		Warning / error

The following display patterns and symbols have been defined for displaying a mode or an error of the SMB Controller or a running application (for example, MiVoice Business):

Table 5: Defined display patterns

LED activation period	Description	Symbol
Always off	Inactive	
Always on	Steady green	
Always on	Steady orange	
Always on	Steady red	
1s on / 1s off	Slowly flashing green	
1s on / 1s off	Slowly flashing orange	
1s on / 1s off	Slowly flashing red	

0.5s on / 0.5s off	Rapidly flashing green	
0.5s on / 0.5s off	Rapidly flashing orange	
0.5s on / 0.5s off	Rapidly flashing red	
	Running orange	

2.2.3.2 Pilot key (CTRL)

Pressing the pilot key carries out certain functions or switches the system to a particular mode.

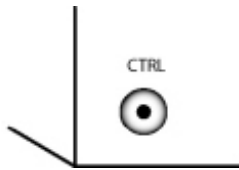


Figure 4: Pilot key

Different actions are carried out depending on how long the key is pressed and the system's current operating mode.

2.2.4 Operating Modes

For the SMB Controller we distinguish four operating modes.

Table 6: Operating modes

Operating mode	Remarks
Start-up mode	- When power is supplied - After a restart - Used as a progress indicator during start-up
Normal mode	- System is running normally - Some additional information of loaded applications might be indicated

Emergency mode	- For executing an emergency upload of the SMB Controller system software - To access the SMB Controller file system with a SSH session
Shut-down mode	- After the system is shut down - Used to safely disconnect the SMB Controller from the power supply - Shut-down mode lasts for 1.5 minutes. Thereafter the system automatically starts up again.

2.2.4.1 Start-up Mode

The start-up mode begins as soon as power is supplied or after a restart of the SMB Controller and ends when the SMB Controller enters normal mode. The LED combination patterns [1]...[5] indicate the individual start-up phases in chronological order and also serve as a progress indicator.

Table 7: Combination patterns during start-up

No.	PWR	F0	F1	F2	F3	F4	F5	F6	SYS	Duration	Meaning
[1]										~11	Power is on
[2]										~2	Time frame to start emergency mode
[3]										~2	Time frame to start Factory Default of Call Manager
[4]	 									~50	Loading SMB Controller system software
[5]											Normal mode, SMB Controller is up and running

As soon as pattern [5] is showed, the start-up phase is completed, and the SMB Controller is in normal mode. You are able to log into the SMB Controller Manager. The MiVoice Business application software is now starting up and after a while you are able to log in to MiVoice Business.

2.2.4.2 Normal Mode

The SMB Controller is in normal mode when the SMB Controller system software is up and running without error. The LED combination pattern [6] is displayed.

If there is a problem with the temperature inside the housing of the SMB Controller (overheating) and/or a problem with the fan, it is signaled with the PWR LED turning from green to orange (pattern [7]). Details of the problem can be found in the SMB Controller Manager.

If applications are loaded and running, there might be some additional information available, indicated with the LED F0 - F6. Each LED is assigned to an application. The F0 LED is assigned to the MiVoice Business application:

- If the F0 LED lights up orange (pattern [8]), the default IP address is active.
- If the F0 LED lights up red (pattern [9]), there is an error in the MiVoice Business application.

Table 8: Normal mode with additional information

No.	PWR	F0	F1	F2	F3	F4	F5	F6	SYS	Meaning
[6]										Normal mode, SMB Controller is up and running.
[7]										Normal mode, overheating. Details in the SMB Controller Manager.
[8]										Normal mode, default fixed IP address is active.
[9]										Normal mode, an error occurred.

2.2.4.3 Emergency Mode

Whenever a standard software upload of the SMB Controller system software via the SMB Controller Manager is not possible or has proved faulty, you must carry out an emergency upload. For this purpose, the SMB Controller must be set into the emergency mode.

The other main purpose of the Emergency Mode is that it allows admin user to log into the Controller Manager using the default admin password. This is useful when the user forgets the admin's user password.



Note:

Entering the emergency mode preserves SMB Controller's IP address.

In emergency mode pattern [14] is displayed.

To enter emergency mode, perform the following steps:

1. Restart the SMB Controller with the Restart button in the SMB Controller Manager System reset view.

- All applications are closed, and the SMB Controller starts up again.

OR shut-down the SMB Controller with a long click (> 5s) of the pilot key (CTRL).

- All applications are closed and SMB Controller changes into the shut-down mode and stays there for 1.5 minutes before it starts up again.

2. Press the pilot key (CTRL) while F0 lights up red during start up (pattern [11]).

- As confirmation the F0 - F6 LED are rapidly flashing red 4 times (pattern [12]).
- The SMB Controller Emergency software is loaded (pattern [13]).
- The emergency mode is entered and Pattern [14] is displayed.

Table 9: Enter emergency mode

No.	PWR	F0	F1	F2	F3	F4	F5	F6	SYS	Duration	Meaning
[10]										~11s	Power is on, begin of restart
[11]										~2s	Press pilot key to start emergency mode
[12]										~2s	Confirmation
[13]										~60	Loading SMB Controller Emergency software
[14]											Emergency mode, default fixed IP address is active

No.	PWR	F0	F1	F2	F3	F4	F5	F6	SYS	Duration	Meaning
[15]											Emergency mode, default IP address 192.168.104.13/24

Default user account in emergency mode

To access the SMB Controller Manager in emergency mode, enter the following:

Table 10: Default user account in emergency mode

Username	admin
Password	admin

Note:

The default password for emergency mode cannot be changed.

2.2.4.4 Shut-down mode

If the user has to disconnect the SMB Controller from the power supply, for example for maintenance purposes, before removing the power source, the user must execute the shut down procedure to put the SMB Controller into the shutdown mode. This approach allows the applications and the Controller Manager to save their data and to close in an orderly fashion before the controller gets powered off. The procedure comprises two main steps in the listed order:

1. [stopping the MSL container](#)
2. [initiating shut down mode](#)

Important:

Before shutting down the controller, you must stop the running MSL container to help prevent database files corruption of the MSL container and the applications running under the container, such as MiVoice Business, MBG and the CloudLink.

Note:

If the user does not disconnect the SMB Controller power supply after the LEDs F0-F6 stop flashing RED (shut-down mode), the controller will initiate its restart and execute the Normal mode.

Never disconnect the SMB Controller from the power supply to trigger a restart. This can result in data losses and prevent a restart.

Combination pattern [\[17\]](#) is displayed during shut-down mode.

Step 1: Stop the MSL Container

Requirements:

The MSL container is installed and its status is **Running**. If the MSL Container is not installed or its status is **Stopped**, skip this step and proceed with [Step 2: Enter shut-down mode](#) on page 20.

1. Log in to the SMB Controller Manager as an admin user.
2. Navigate to **Software > Applications**.
3. On the **Command** column of the MSL Container, select **Stop** from the drop-down menu.

The screenshot shows the Mitel SMB Controller Manager interface. The top navigation bar includes the Mitel logo, 'SMB Controller Manager', 'SSH access is enabled', and a user welcome message 'Welcome admin'. The left sidebar shows the navigation menu with 'System overview', 'Configuration', 'Software', 'Applications' (selected), 'System software', 'Security', and 'Maintenance'. The main content area displays 'Currently installed applications' with a table. The table has columns: Name, Version, Version (Running...), LED assignment, Command, and Status. The first row shows 'Mitel-MSL_Container' with version '11.0.105.4-1', LED assignment 'LED group F3 / F4', and status 'Running...'. The 'Command' column for this row has a dropdown menu open, showing options: 'Stop' (highlighted in red), 'Restart', and 'Uninstall'. Below the table, there is a section for 'Application files' with a table showing 'Mitel-MSL_Container-11.0.105.4-1.aarch64.rpm installed' with version '11.0.105.4-1' and size '736.38 MB (772127673 bytes)'. At the bottom, there is a 'Load application file' section with a checkbox for 'Please agree to EULA in order to load the application file' and buttons for 'Browse...' and 'Firmware server...'. The footer contains the copyright notice: 'Copyright © 2023 Mitel Networks Corporation - All rights reserved'.

- Click **OK** to confirm the request.

The MSL container will enter the **Stopping** state.

It takes about a minute or two for the MSL container and the applications (MiVoice Business, MiVoice Border Gateway, CloudLink) running in the container to shutdown orderly, after which the status of the MSL container shows as **Stopped**.

The screenshot shows the Mitel SMB Controller Manager web interface. The top navigation bar includes the Mitel logo, 'SMB Controller Manager', a red status indicator 'SSH access is enabled', and a user welcome message 'Welcome admin'. The left sidebar contains navigation links: System overview, Configuration, Software, Applications (highlighted), System software, Security, and Maintenance. The main content area displays the 'Currently installed applications' table. The table has columns for Name, Version, Version (Running...), LED assignment, Command, and Status. One application is listed: 'Mitel-MSL_Container' with version '11.0.105.4-1', LED assignment 'LED group F3 / F4', and status 'Stopped' (highlighted with a red box). Below the table, there is a section for 'Application files' showing a file 'Mitel-MSL_Container-11.0.105.4-1.aarch64.rpm.installed' with version '11.0.105.4-1' and size '736.36 MB (772127673 bytes)'. A 'Load application file' section contains a warning about the EULA and a checkbox for agreement. At the bottom, there are 'Browse...' and 'Firmware server...' buttons. The footer shows 'Copyright © 2023 Mitel Networks Corporation - All rights reserved'.

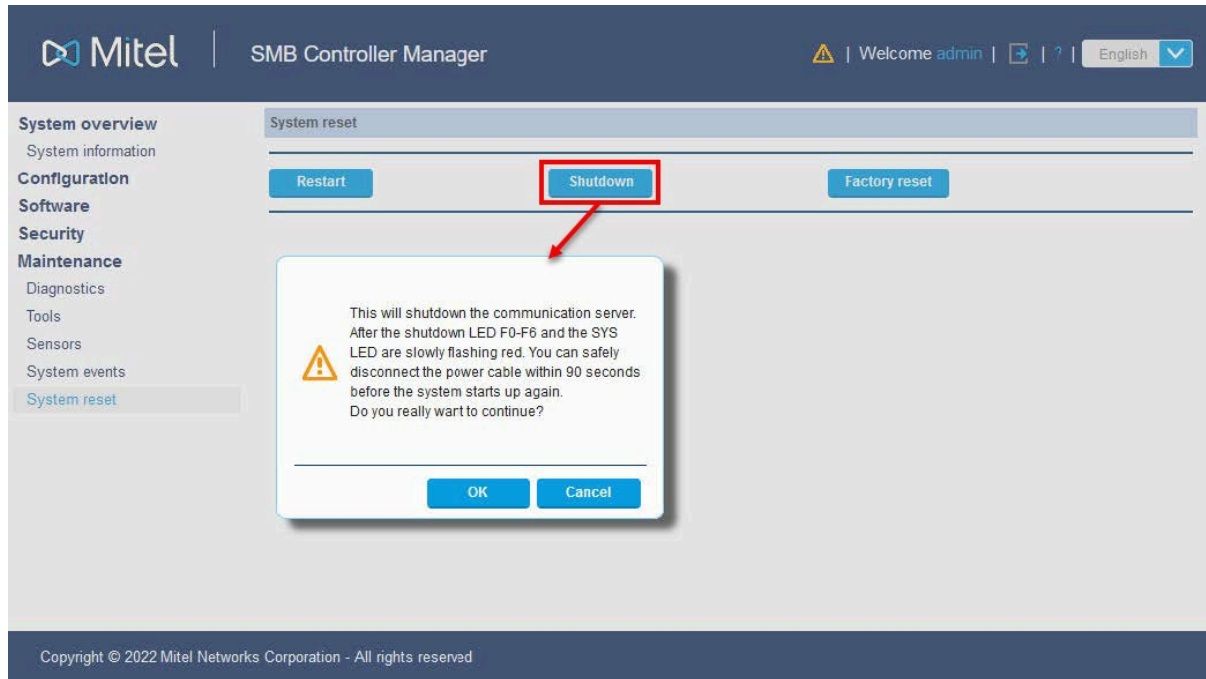
- Once the status of the MSL container has been changed to **Stopped**, proceed with the [Step 2: Enter shut-down mode](#) on page 20 to shut down the SMB Controller.

Step 2: Enter shut-down mode

Requirement:

The SMB Controller is up and running in normal mode or emergency mode.

1. Shut-down the SMB Controller with the *Shut-down* button in the SMB Controller Manager *System reset* view.



OR

Shut-down the SMB Controller with a long click (> 5s) of the pilot key (CTRL).

- The F0 - F6 LED flash orange while the applications are saving their data and are closing (pattern [\[15\]](#)).
 - The flashing orange LED stops and the LED F0 - F6 turns solid up orange. During this phase the SMB Controller is saving its data and is closing (pattern [\[16\]](#)).
 - The F0 - F6 LED and the SYS LED are slowly flashing red to indicate the shut-down mode (pattern [\[17\]](#)).
2. You can now disconnect the SMB Controller from the power supply without concerns within the next 90 seconds.

Note:
Removing the power cord before or after the controller is in shutdown mode could corrupt the database.

Note:

It is recommended to shut down the SMB Controller using the CTRL key procedure.

Table 11: LED Patterns During Shut-down Mode

No.	PWR	F0	F1	F2	F3	F4	F5	F6	SYS	Duration	Meaning
[15]										up to 5 min.	Applications are saving their data and are closing
[16]										~20s	SMB Controller is saving its data and is closing
[17]										~90s	SMB Controller is in shut-down mode Once

2.2.5 Configure User Access Control

The SMB Controller system software includes Controller Manager. The MSL System software includes Server Manager. Both the Controller Manager and the Server Manager are web-based configuration tools offer a simple, user-friendly interface and an online help for some basic configurations possibilities and maintenance tasks.

Access to both Managers configuration is password-protected. Users wanting to log in to either of the Managers are prompted for the username and password. Both managers feature default admin user.

The following table shows the subset of the configuration operations supported in each interface.

User Interface	Operation	Comments
SMB Controller Manager	SMB Controller IP Address DNS and Domain	Also contains Domain Name and DNS servers to use.

User Interface	Operation	Comments
	Install software	Installation of both system and application software.
	Date and Time	Defines NTP Server
Server Manager	MSL IP addresses	Defines LAN/WAN IP Addresses
	MSL Backup	Includes backup of applications installed in MSL (MiVoice Business + MG, MiVoice Border Gateway, Mitel Performance Analytics Probe)
	SOS Logs	Includes logs from MSL, and its installed applications (MiVoice Business + MG, MiVoice Border Gateway, CloudLink Gateway, Mitel Performance Analytics Probe)

Warning:

The MSL admin account is separate from the SMB Controller Manager admin account. Changes to the "admin" password in MSL is not reflected in SMB Controller Manager (and vice versa).

The MiVoice Business is managed by a system user in the System Administrator Tool.

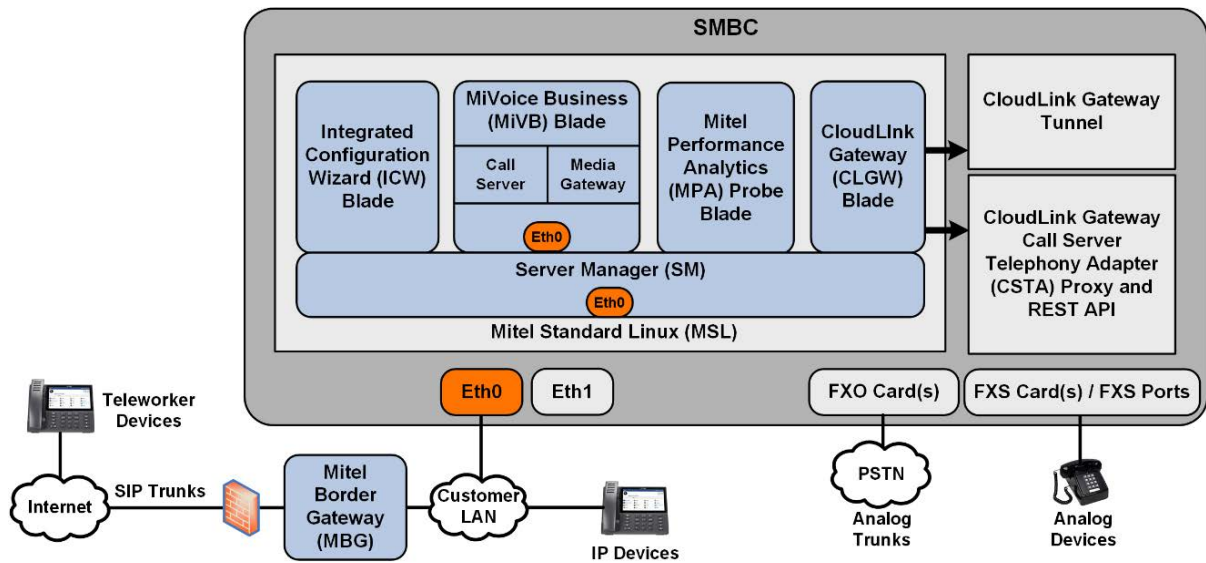
2.3 Network Scenarios

Following are some typical Network Scenario examples.

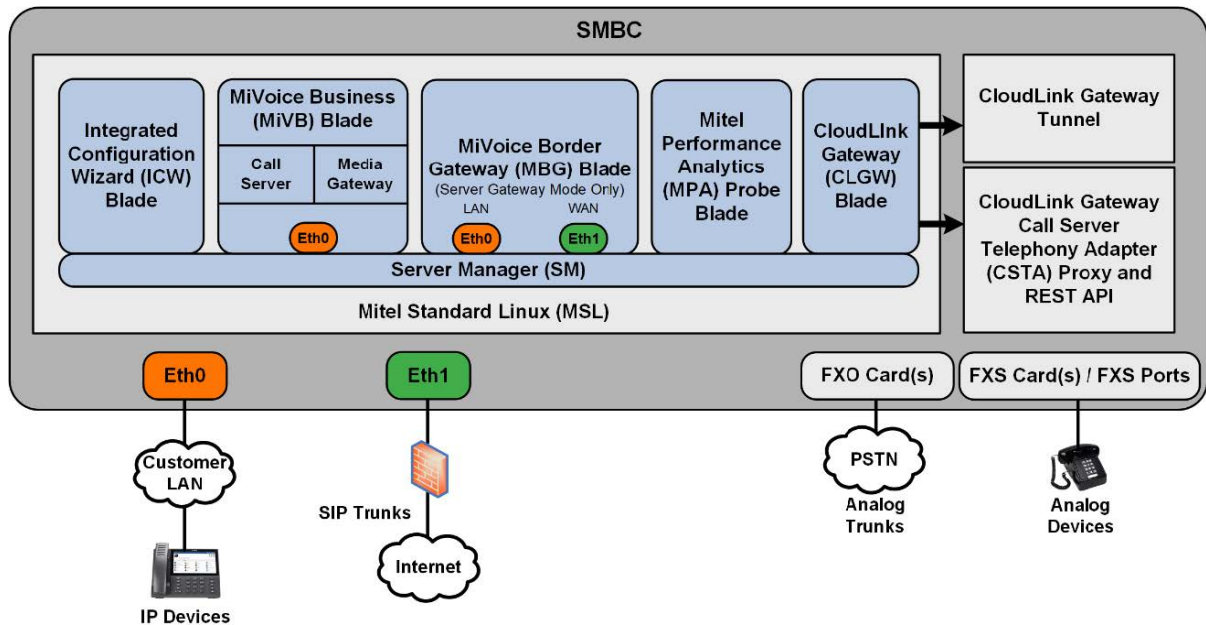
Note:

The SMB Controller does not support 802.1p ethernet priority. For more details, see [note](#) in the topic [SMB Controller Overview](#) on page 7.

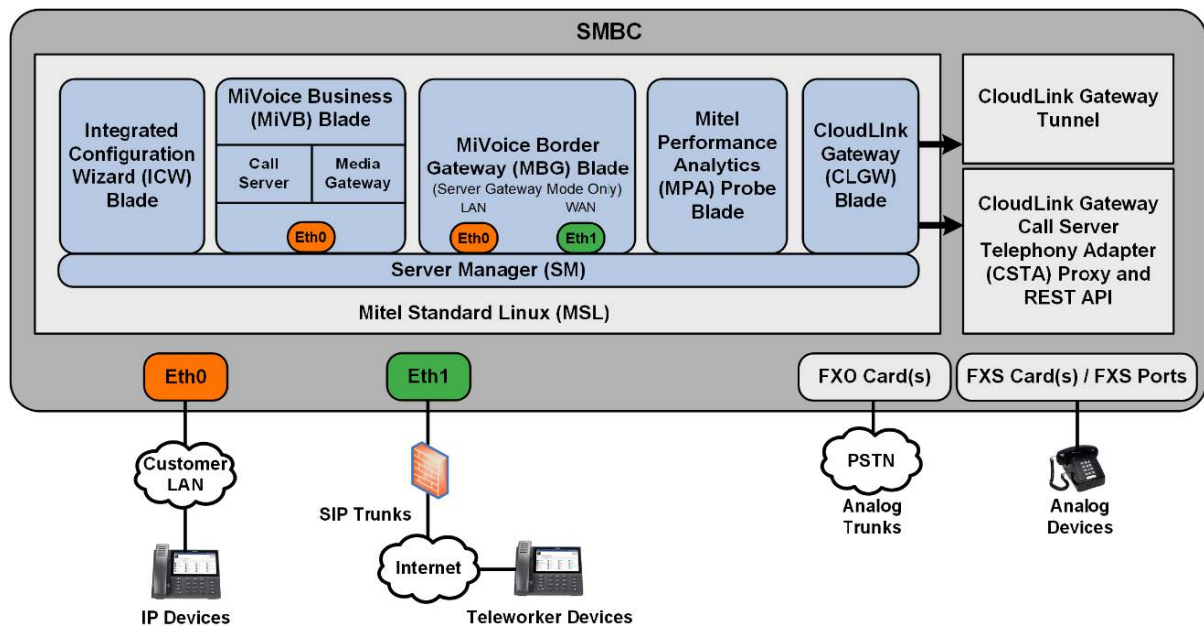
- MiVoice Business on the SMB Controller using external MiVoice Border Gateway SIP Trunks



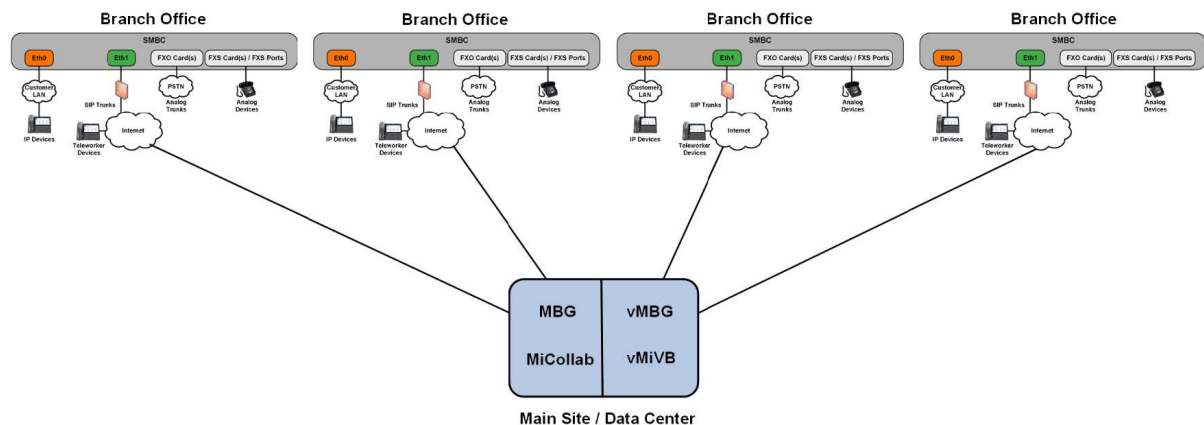
- MiVoice Business on the SMB Controller - Telephony Only using Embedded MiVoice Border Gateway SIP Trunks



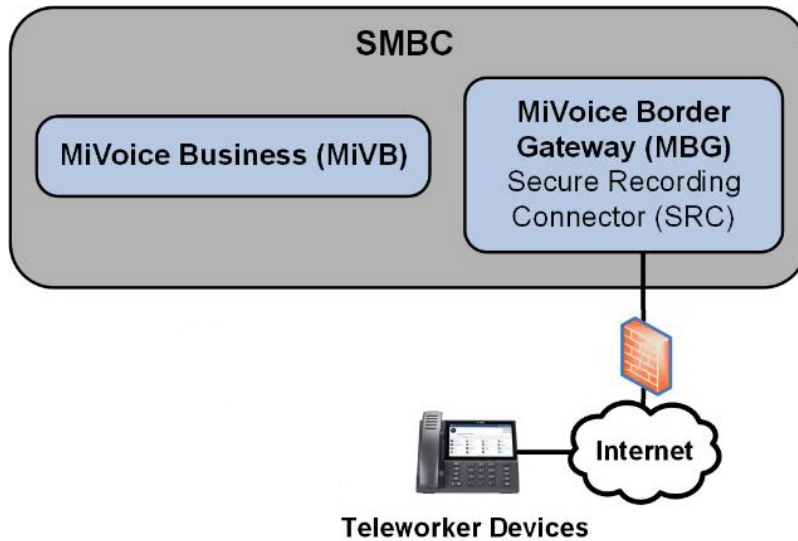
- MiVoice Business on the SMB Controller - Telephony using embedded MiVoice Border Gateway SIP Trunks with Teleworkers



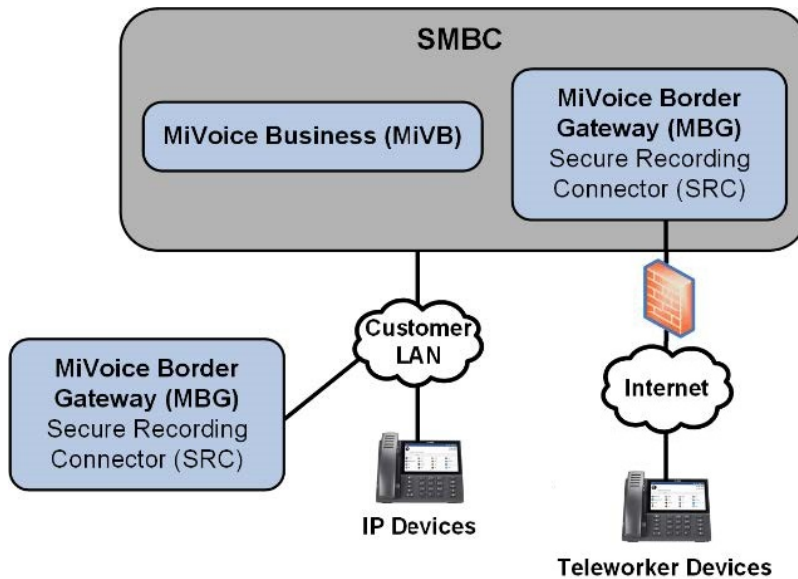
- MiVoice Business on the SMB Controller – Branch Offices with Telephony with Teleworkers



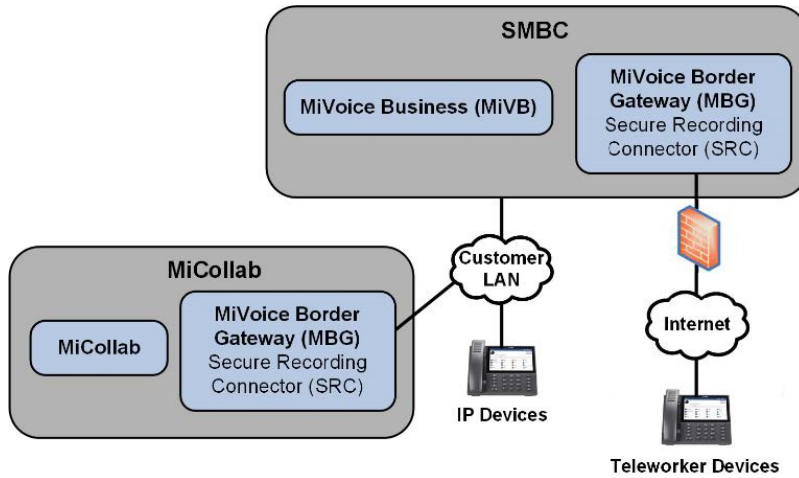
- MiVoice Business on the SMB Controller – Call Recording – External Teleworker Secure Recording Connector (SRC) function as part of the MiVoice Border Gateway Teleworker solution.



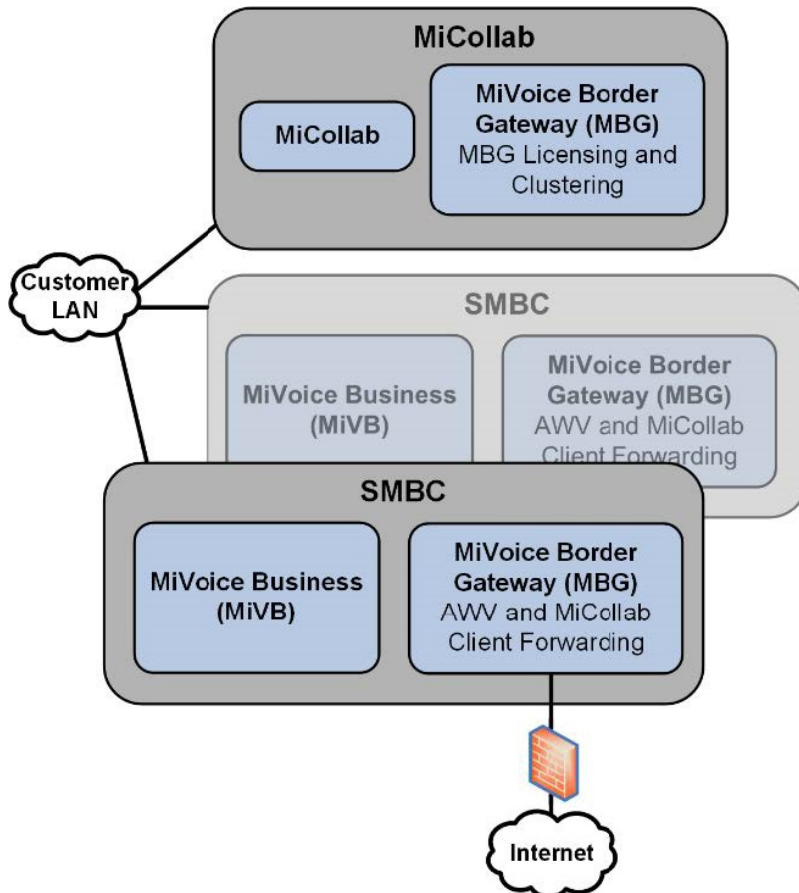
- MiVoice Business on the SMB Controller – Call Recording – Internal without MiCollab Internal Devices can be Teleworker or deploy an additional local MiVoice Border Gateway in LAN Mode.



- MiVoice Business on the SMB Controller – Call Recording – Internal with MiCollab uses the MiCollab MiVoice Border Gateway in LAN Mode as the SRC.

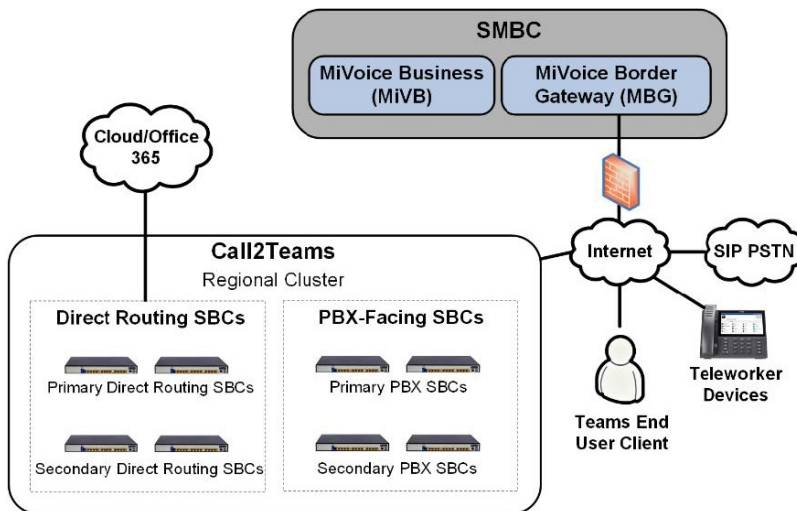


- MiCollab Integration



MiCollab Integration

- Call2Teams Solution with the SMB Controller – Multi-Tenant Cloud Service - Registers a Teams Client as a SIP Device on the existing PBX via the MiVoice Border Gateway just like a SIP Phone does.



2.4 Hardware Installation

This section describes the procedure for installing SMB Controller hardware and the conditions to be observed. It also describes mounting the Controller on a 19" rack, and the correct way to connect the earthing and the power supply.

Other topics described in this section contain instructions for fitting the system modules, interface cards, DSP cards, and the relevant wiring adapters.

Finally, the chapter also describes the network and terminal-side connection of the interfaces and the installation, powering on, and connection of system terminals.

2.4.1 Safety Information

Reference to hazards

Hazard warnings are affixed whenever there is a risk of improper handling exposing people to danger or causing damage to the MiVoice Business product. Note these warnings and follow the guidelines at all times. Take note, in particular, of the hazard warnings contained in the user information.



Warning:

Warning indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.

! CAUTION:

Caution indicates a potentially hazardous situation which, if not avoided, could cause minor or moderate injury and/or damage to the equipment or property.

These symbols may appear on the product:

	The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock.
	The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.
	Indicates ESD components. Failure to observe information identified in this way can lead to damage caused by electrostatic discharge.
	The ground symbol within a circle identifies that the product must be connected to an external conductor. Connect the product to earth ground before you make any other connections to the equipment.

Installation and operating instructions

Before you begin with the installation of the SMB Controller:

- Check that the delivery is complete and undamaged. Notify your supplier immediately of any defects; do not install or put into operation any components that may be defective.
- Check that you have all the relevant user documents at your disposal.
- Configure this product with only the assemblies specified and, in the locations, stated in the [System Components section of this user documentation](#).
- During the installation follow the installation instructions for your SMB Controller in the sequence that is given and observe all the safety warnings they contain.

⚠ CAUTION:

Failure to follow all instructions might result in improper equipment operation and/or risk of electrical shock.

- Install all wiring according to local, state, and federal electrical code requirements.
- Do not connect telecommunications cabling to the system, service the system, or operate the system with the grounding conductor disconnected.
- Ensure the AC receptacle is installed near the equipment and easily accessible.
- Use only Mitel-approved power adapters.

Any servicing, expansion, or repair work is to be carried out only by trained technical personnel with the appropriate qualifications.

Opening the SMB Controller - Safety Precautions

Be sure to observe the following safety regulations before carrying out work inside a communication server:

⚠ CAUTION:

Components, interface cards or system modules can be damaged by electrical voltage. Always shut down, then disconnect the communication server from the power supply and then wait for 3 minutes before removing the housing cover.

⚠ CAUTION:

Components can be damaged by electrostatic discharge when touched. It is strongly recommended to use an ESD earthing strap connected to the chassis of the communication server before carrying out work inside the housing. This also applies to interface cards and system modules that are no longer packed inside the ESD protective wrapping. Removed components should be stored and transported in appropriate ESD shielded packaging.

1. Disconnect the Power Supply.
2. Remove the cover.
3. Ensure that the earthing wire has been connected to to the ground terminal on the bottom plate as shown in the [Figure 5: Earthing \(Grounding\) the SMB Controller](#) on page 31.

Instructions on how to install the earthing wire are provided in the section [Earthing and protecting the communication server](#) on page 59.

4. Ensure that your ESD earthing strap is connected to ground before working inside the controller.

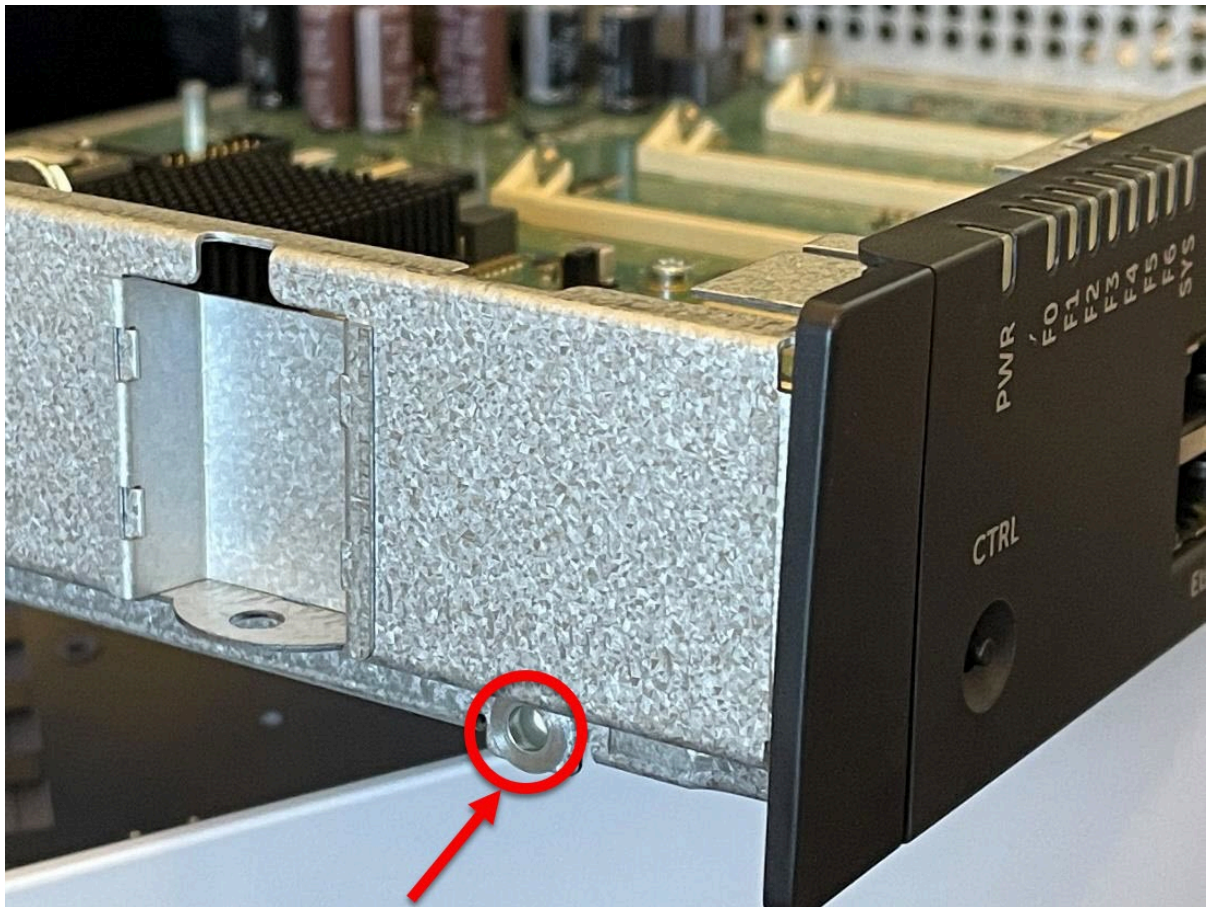


Figure 5: Earthing (Grounding) the SMB Controller

2.4.2 System Components

The following figure shows the components of the Mitel SMB Controller complete with mounting options.

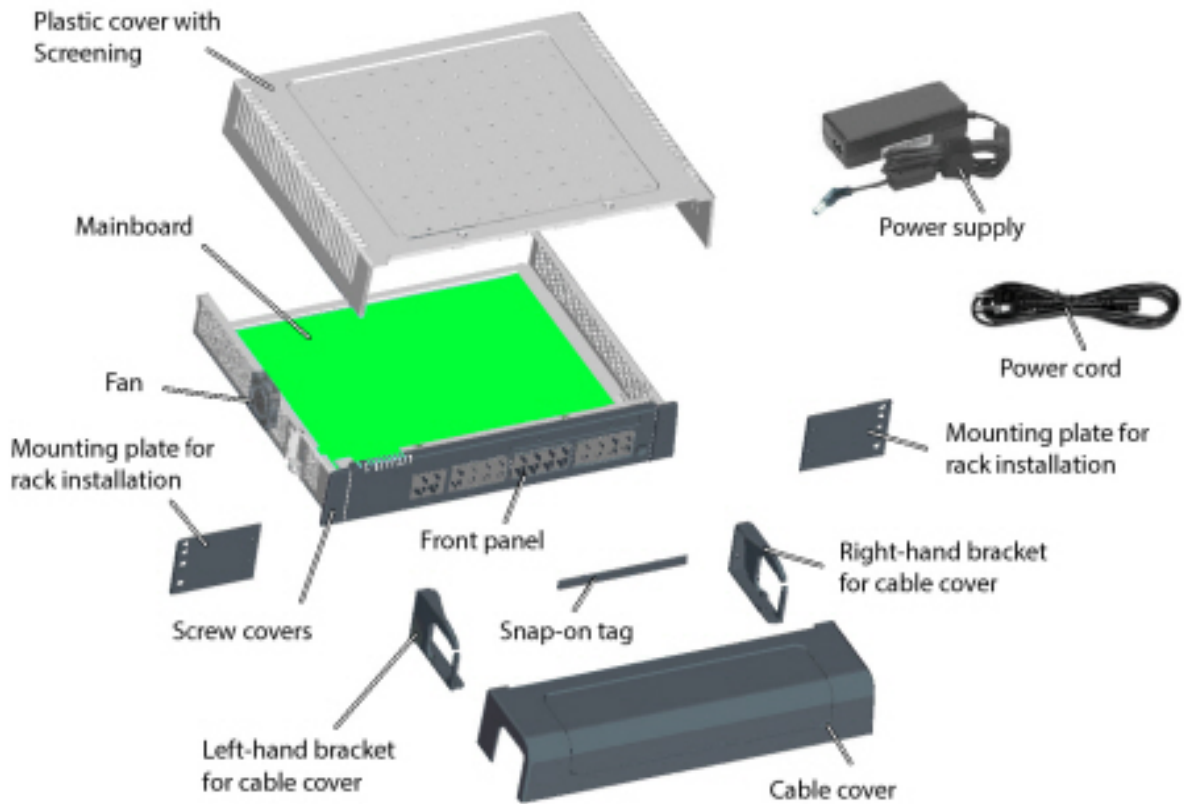


Figure 6: System components with mounting options

2.4.3 Hardware

The SMB Controller is based around an ARMv8 64-bit CPU and comes with six embedded Foreign Exchange Station (FXS) ports for analog devices.

The SMB Controller comes with an 8 GB of RAM, a 1.6 GHZ Quad Core CPU, and 38 GB of storage.

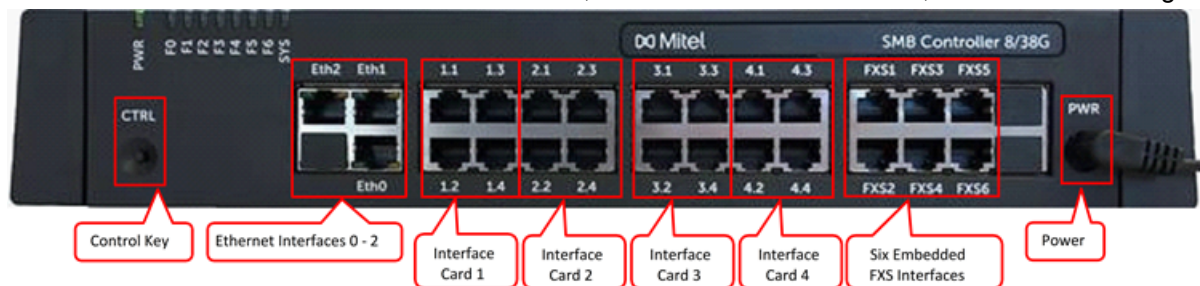


Figure 7: SMB Controller Front Panel

For networking, there are three physical networks adapters. but only two are used (Eth0 and Eth1).

Note:
Do not connect anything to Eth2.

**Note:**

There are no physical ports for Audio Inputs or Outputs for MOH and Paging. See [Music On Hold](#).

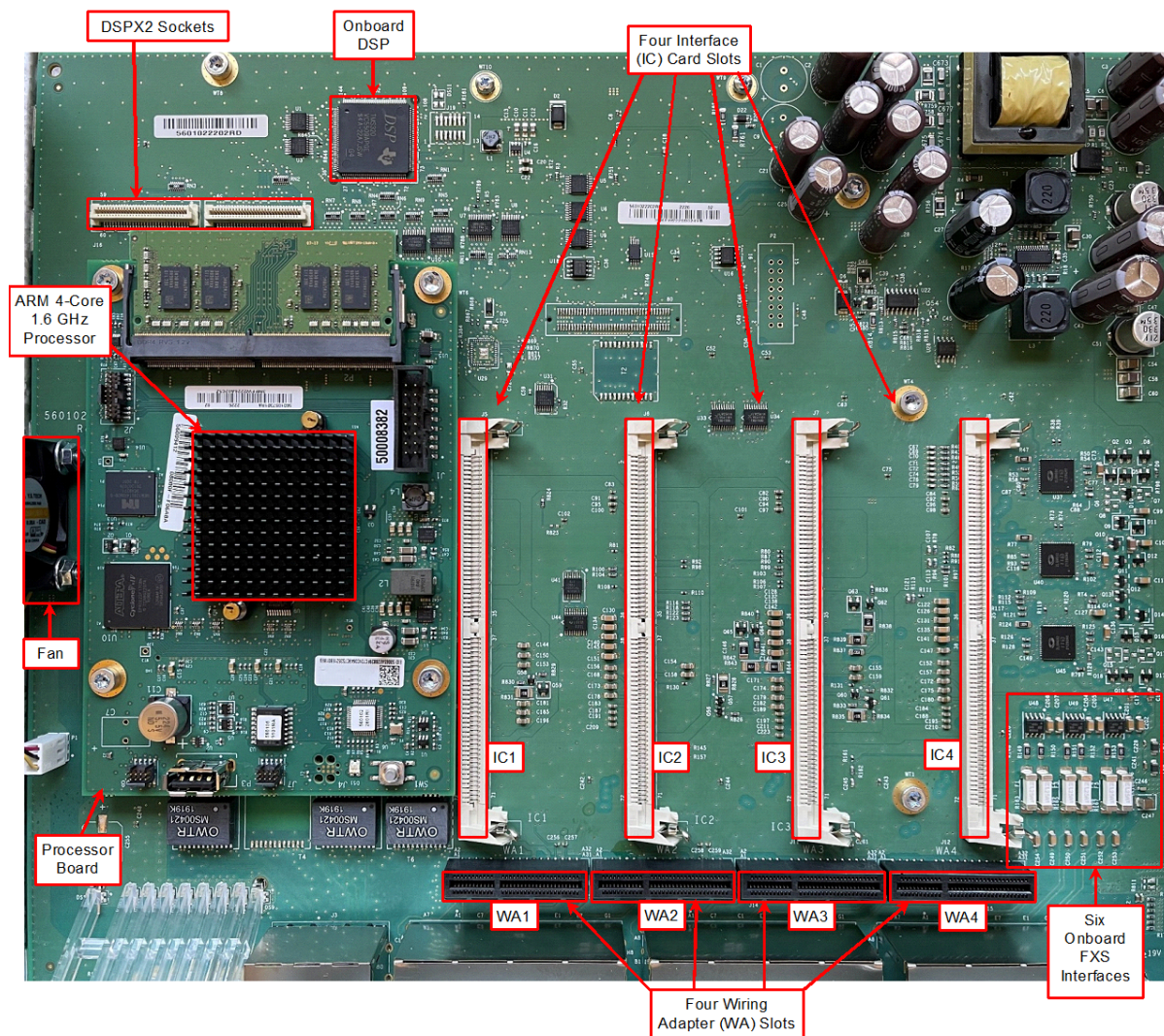


Figure 8: SMB Controller Internal

**Note:**

To install or remove Interface or DSP cards, power down the system, and unplug the power cord. Follow the proper Electrostatic Discharge (ESD) precautions. Ensure the chassis is grounded, see [Earthing \(Grounding\) the SMB Controller](#). Wait three minutes before touching the hardware. For more details see, [Installing the Interface and DSP Cards](#).

Some SMB Controller hardware information are as follows:

- The SMB Controller has an Equipment ID (EID) that is hard coded on the Processor Board.
- Four optional expansion interface cards can be installed.
- The number of supported users, Voice over Internet Protocol (VoIP) Channels, and Voice Mail / Auto Attendant Ports depends on the number of DSP Cards in the system.

2.4.3.1 Summary of Parts for MiVoice Business on SMB Controller

Part Number	Name	Comments
50008381	SMB Controller 8/38G	SMB platform
20351208	System module 2 DSPX	See section System Configurations on page 34 for information about system configurations by number of DSP cards required. Note: At least one System Module 2 DSPX resource card with part number 20351208 is required.
20350436	Expansion interface card 4 x a/b	4 FXS ports
50008254	SMB Controller Trunk card 2FXO	2 Port FXO
50008255	SMB Controller Trunk card 4FXO	4 Port FXO

2.4.3.2 System Configurations

The MiVoice Business solution on SMB Controller is recommended to be deployed as either an up to 80-user system or an up to 150-user system.

The number of supported users and the number of available VoIP channels are determined by:

- The number of DSP expansion cards installed in the system

- The number of configured VM ports
- The number of configured voice compressions.

For more information about how DSPs are used and for system configuration information, see [DSP Allocation](#).

Note:

CPQ determines the DSP card requirements.

Embedded T.38 is not supported. FAX modems can be supported by Modem-Over-IP using G.711 functionality or via an external analog gateway device, such as AG4124.

There are two options to ensure G.711 only mode on FXS/FSO:

- Assign 0 compression options in the License and Option Selection form.
- Ensure that all the SIP and IP Trunks the system interfaces with for modem calls are placed in the same Compression Zone as the system. This is provisioned in the Network Element form.

2.4.3.3 SMB Hardware Version

It is important to identify your system version before performing any maintenance or upgrades. The system hardware version is identified via a label at the bottom of the box.

The software releases needed for each hardware version are as follows:

- For Rev A hardware version, the minimum required software release is MiVoice Business version 10.0.
- For Rev B hardware version, the minimum required software release is MiVoice Business version 10.0 SP1.

Important:

It is important to ensure the correct software release is installed for your hardware version.

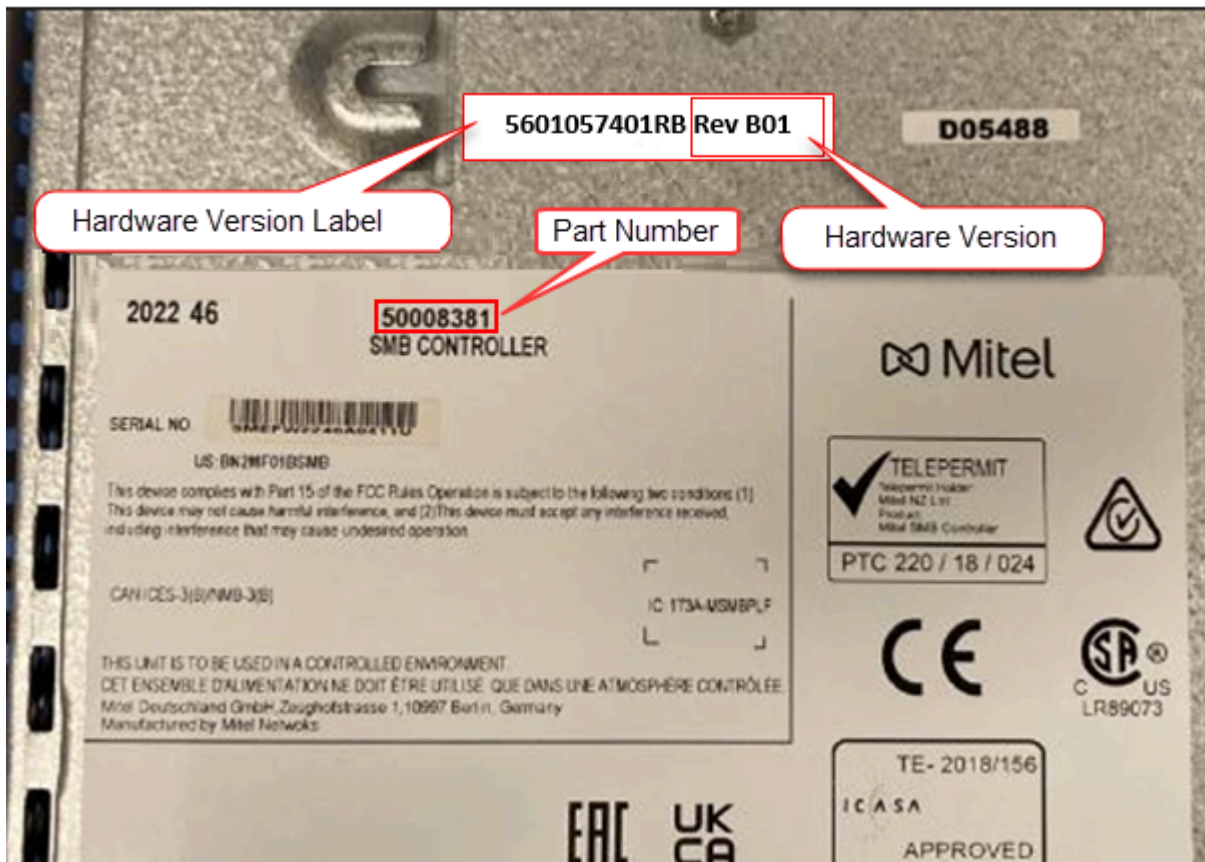


Figure 9: SMB Controller Part Number and Hardware Version Label

The label on the system denotes both the part number and hardware version number. In the above example a Rev B SMB system is shown as it is identified as a *B01* system. (*5601057401RB* is the part number).

You can also determine the installed hardware version in the System Information page on SMB Controller.

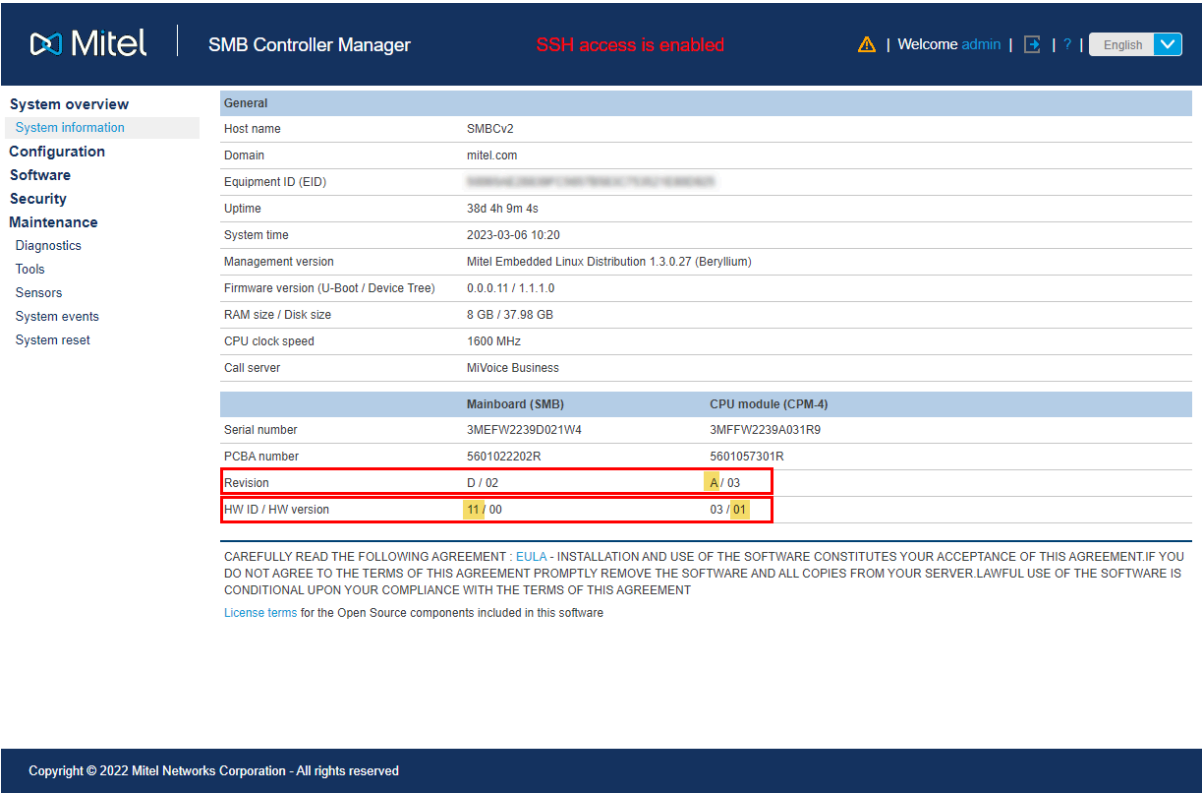


Figure 10: Hardware IDs of CPM Cards and Mainboard (Rev A)

- Rev A systems are those with a mainboard ID of 11/00 or lower and a CPU module version of 3/01.
- Rev B systems are those with a mainboard ID of 12/00 and a CPU module version of 3/02.

The [Figure 10: Hardware IDs of CPM Cards and Mainboard \(Rev A\)](#) on page 37 shows an example of Rev A system.

The [Figure 11: Hardware IDs of CPM Cards and Mainboard \(Rev B\)](#) on page 38 shows an example of Rev B system.

The screenshot shows the Mitel SMB Controller Manager web interface. The top navigation bar includes the Mitel logo, the title 'SMB Controller Manager', a warning message 'The system must be restarted to activate the new settings.', and a user welcome 'Welcome admin'. The left sidebar contains a menu with 'System overview' (selected), 'Configuration', 'Software', 'Security', and 'Maintenance'. The main content area displays 'System information' with a table of system details. Below this, there is a table comparing 'Mainboard (SMB)' and 'CPU module (CPM-4)' hardware IDs. The 'Revision' and 'HW ID / HW version' rows are highlighted with red boxes. At the bottom, there is a copyright notice for 2022 Mitel Networks Corporation.

System information	
Host name	SMBCv2
Domain	
Equipment ID (EID)	
Uptime	14m 16s
System time	2022-12-13 18:17
Management version	Mitel Embedded Linux Distribution 1.3.0.25 (Beryllium)
Firmware version (U-Boot / Device Tree)	0.0.0.11 / 1.1.1.0
RAM size / Disk size	8 GB / 37.97 GB
CPU clock speed	1600 MHz
Call server	MVoice Business

	Mainboard (SMB)	CPU module (CPM-4)
Serial number	3MEFW2302E030AA	3MFFW2305B031H5
PCBA number	5601022202R	5601057301R
Revision	E / 03	B / 03
HW ID / HW version	12 / 02	03 / 02

CAREFULLY READ THE FOLLOWING AGREEMENT - [EULA](#) - INSTALLATION AND USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT.

[License terms](#) for the Open Source components included in this software.

Copyright © 2022 Mitel Networks Corporation - All rights reserved

Figure 11: Hardware IDs of CPM Cards and Mainboard (Rev B)

2.4.3.4 Installing the Interface and DSP Cards

In addition to the platform and the embedded interfaces, the SMB Controller also supports four expansion interface cards. An interface card can be inserted into any free interface card socket.

Note:

Before opening the SMB Controller for any repair or troubleshooting, read the product information and [safety instructions](#) carefully.

To prevent damage to the components, always follow proper ESD procedures. This also applies to handling interface cards, processor cards, and system modules that are not inside ESD-protective wrapping.

To install an interface card:

1. Disconnect the power supply.
2. Remove the cover.
3. Connect the earthing wire to the ground terminal of the bottom plate, see [Earthing and protecting the communication server](#) on page 59.
4. Insert the interface cards into the IC1, IC2, IC3, and IC4 slots by placing the interface card at a slight angle into the required slot and carefully pressing the interface card down until the two metal clamps engage.
5. Insert the corresponding wiring adapters into the WA1, WA2, WA3, and WA4 sockets. See the imprint on the adapters for orientation.

6. Insert the DSP modules into the DSP Slot on the mainboard by replacing the fastening screw with the standoff supplied with the module.
7. Align the DSP module into the DSP slot and press down evenly on both connectors until they stop.

**Note:**

A maximum of three DSP modules can be stacked. At least one DSP module is required in addition to the onboard DSP.

8. Repeat steps 6 -7 for all DSP modules and then secure the final module with the fastening screw.

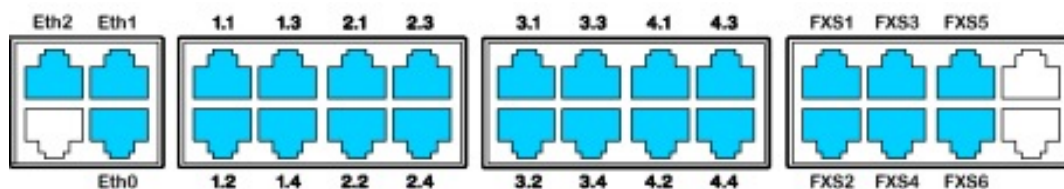
A maximum of three DSP cards can be stacked.

9. Attach the cover.

2.4.3.5 FXS terminal interfaces

The six FXS terminal interfaces of the mainboard are permanently routed to the front panel and labelled accordingly. The two remaining RJ45 sockets, which are not labelled, empty and cannot be used. With the appropriate interface cards and wiring adapters, additional FXS terminal interfaces can also be made available at the RJ45 sockets 1.x. 4.x. The possible RJ45 sockets are highlighted in color in the following figure.

Figure 12: Connection possibilities for FXS terminal interfaces



2.4.3.5.1 FXS interfaces

Feature	MiVoice Business on SMB Controller
Pulse Dialing	No
DTMF Dialing	Yes
High Voltage MWI	Yes, for on-board FXS No, for FXS expansion cards

Feature	MiVoice Business on SMB Controller
FAX	Yes
MODEM	Yes. Modem is supported via VBD
Door Phone	Yes

CAUTION:

Terminals connected to FXS interfaces can be damaged if the configuration of the system is incorrect.

Note:

Circuit type as per EN/IEC 60950: TNV-2

The following analogue terminals can be connected:

- Analogue phones with DTMF (earth key are not supported)
- Radio units for cordless phones
- Group 3 fax ²
- Answering machines
- Modem
- Music on Hold (MoH)

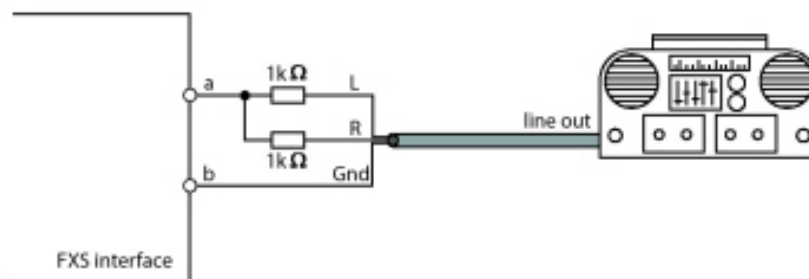


Figure 13: Connection for FXS mode Analog Music on Hold

The no-load voltage at the ports is approx. 53 VDC. The loop current is limited to 25 mA.

² Transmission with the T.38 protocol is recommended for Fax over IP.

Ports FXS1...FXS6 on the mainboard are designed for long lines and support "High voltage" for the message LED. The no-load voltage at these ports is 48 VDC. The ports of interface cards (ETAB4) have a no-load voltage of 53 VDC. The loop current is limited to 25 mA on all ports.

Table 12: Cable requirements for FXS mode: Phone/fax

	Ports FXS1...FXS6	Ports of interface cards (ETAB4)
Core pairs × cores	1 × 2	1 × 2
Stranded	only with lengths > 200 m	only with lengths > 200 m
Wire diameter, core	0.4 ... 0.8 mm	0.4 ... 0.8 mm
FXS resistance	max. 2 × 625 Ω	max. 2 × 250 Ω
Line length 0.6 mm diameter	max. 10 km	max. 4 km
Screening	not required	not required

Table 13: Specification for FXS (used for USA/Canada only)

Parameter	Interface FXS1...FXS6 of Mitel SMB Controller
OPS Loss Plan Support	No
DNIC Support	No
LS Trunk Support	Yes
LS Class Support	Yes
GS Trunk Support	No
REN per line (ONS)	2

Parameter	Interface FXS1...FXS6 of Mitel SMB Controller
Open circuit Ringing Voltage (VRMS)	Nominal = 70V (trapezoidal balance) or 40V rms (sinus wave) i Note: This setting is country dependent.
ONS Loop Length (Miles)	600 Ohm Loop (with 300 Ohm Set) 3.45 (22AWG) 2.17 (24AWG) 1.33 (26AWG)
ONS Line Feed Voltage	30V for normal 56V for long loop
ONS MWI Lamp Strike Voltage (VDC)	The following formats are supported: - High voltage (>90Vdc) i Note: This setting is country dependent. - Low voltage LED type: 12Vrms at 20Hz for 100ms - FSK - Polarity reversal

2.4.4 Mounting the SMB Controller

The SMB Controller is suitable for both wall and desktop installation as well as for mounting in a 19" rack. Different mounting sets are available for each type of installation.

2.4.4.1 Equipment supplied

The equipment supplied with the SMB Controller includes:

- Mitel SMB Controller communication server with a CPU module fitted and a fan mounted
- Set of screws for wall or desktop installation and earthing connection
- Snap-on tag
- Power supply (The power cord is a separate part and this needs to be ordered depending on country)

Part Number	Description	Country
51000582	PWR CRD C7 2.5A 250V-UK PLUG 3A FUSE	UK, Hong Kong, Ireland, Singapore, Saudi
51004990	PWR CRD C7 2.5A 250V- EURO PLUG	Europe
51011501	PWR CRD C7 2.5A 250V - AUSTRALIAN PLUG	Australia, New Zealand
51005172	PWR CRD C7 2.5A 10A 125V- NA PLUG NON POLRIZD	North American

- Product information

2.4.4.2 Mounting options

Mitel SMB Controller includes all the materials required for wall or desktop installation. Additional rack installation sets are required for a 19" rack installation.

For wall mounting, all the connecting cables can be concealed behind a cable cover. This cable cover set can be ordered as an option.

- 20350236 - SMBC Rack Mount Kit
- 20350090 - SMBC Cable Cover Kit

2.4.4.2.1 Cable cover set

Equipment supplied:

- Cable cover
- Left-hand bracket for cable cover
- Right-hand bracket for cable cover
- Screw set

2.4.4.2.2 Mitel SMB Controller rack-mounting set

Equipment supplied:

- 2 mounting plates for rack installation
- Screw set

2.4.4.3 Location requirements

The following location requirements must be observed when positioning the SMB Controller.



Warning:

Failure to observe the location requirements can cause the SMB Controller to overheat, damaging electrical components and/or the surrounding area.

Heat radiation	Do not position in direct sunlight or near radiators or near other heating sources
EMC	Do not position in strong electromagnetic fields of radiation (for example, near x-ray equipment, or welding equipment).
Heat dissipation	Rated at 35 Watts, or 119.35 BTU/hr. Do not place any object on top of the SMB Controller. Observe the clearance requirements for wall mounting and desktop installation (see minimum distance guidelines for wall mounting (front panel facing to the right) and minimum distances for wall mounting (front panel facing downwards)). In a rack installation, the space to the left and right between the SMB Controller and the wall of the 19" rack must remain empty.
Power Requirements	75 Watts
Noise Level at a distance of 1 meter, 100-1000 Hz	30 dBspl(A)
Environment	Ambient temperature 5°C to 45°C Relative humidity 30 to 80%, non-condensing

An event message is generated if the heat dissipation is insufficient. Appropriate measures must be taken immediately to improve the heat dissipation; for example, by providing the required clearances or lowering the ambient temperature.

2.4.4.4 Wall mounting

There are two variants of wall mounting. In the first variant, the front panel faces right (see [Minimum distances for wall mounting \(front panel facing to the right\)](#)); in the second, it faces downwards (see [Minimum distance guidelines for wall mounting \(front panel facing downwards\)](#)). The wall-mounting option chosen will depend on the way the cables are routed. The LED display remains visible whatever the mounting position, even when the cable cover is fitted.



CAUTION:

A wall-mounting option in which the front panel faces upwards or to the left is not permitted. Inadequate heat dissipation can damage the SMB Controller.

2.4.4.4.1 Wall-mounting procedure

Minimum distances

To ensure adequate heat dissipation, minimum distances need to be maintained with other objects such as cable ducts, cabinets or mobile objects. Maintaining minimum distances also allows the installation of the cable cover and the possibility of suspending the SMB Controller into and out of the wall-mounted screws.

The two diagrams illustrate the two wall-mounting methods.

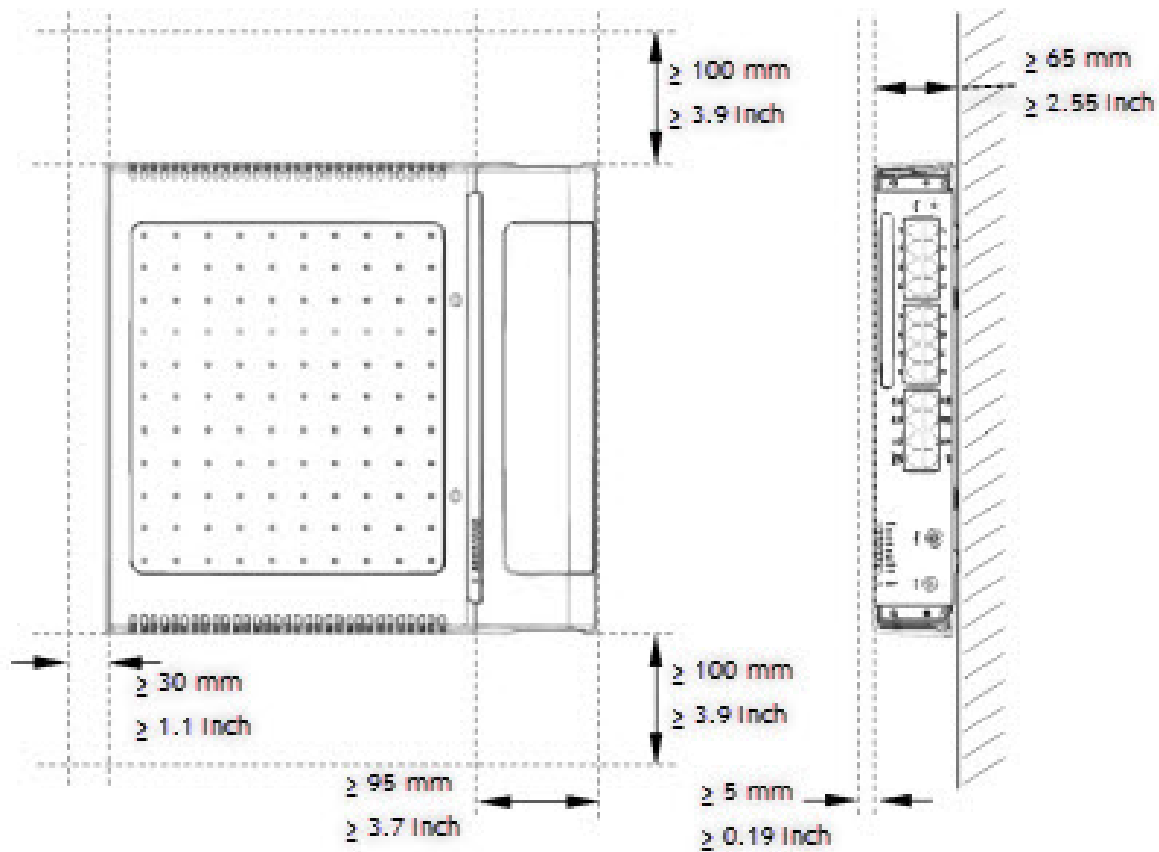


Figure 14: Minimum distances for wall mounting (front panel facing to the right)

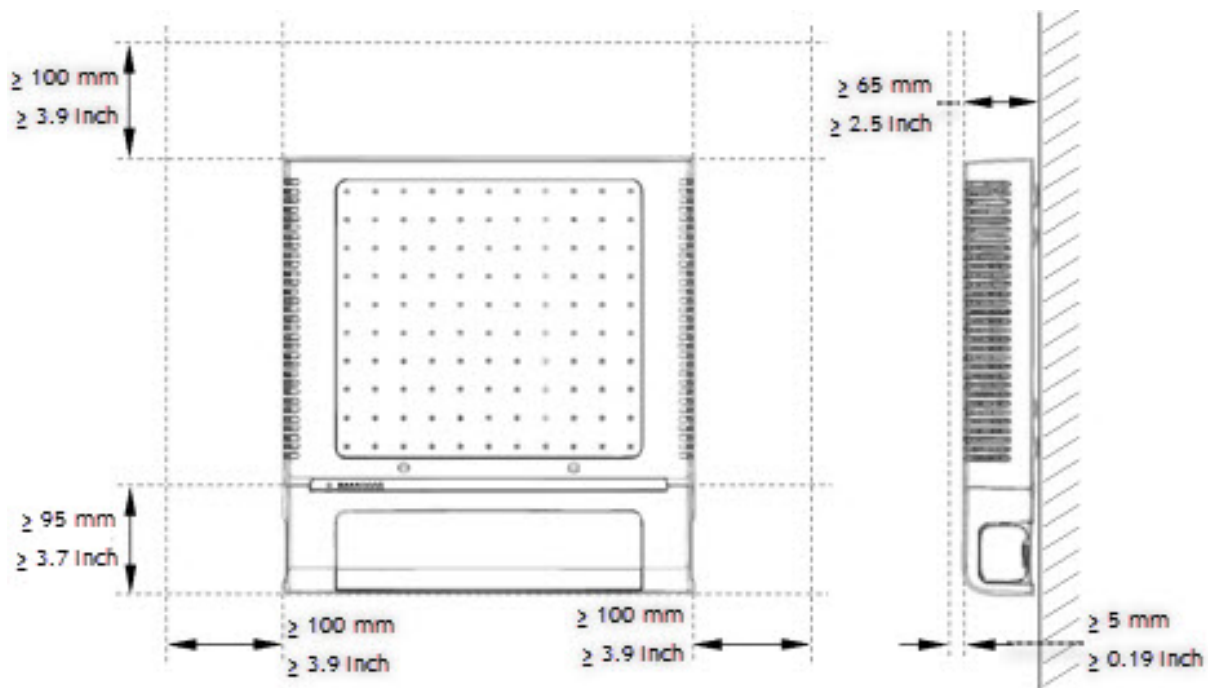


Figure 15: Minimum distances for wall mounting (front panel facing downwards)

Drilling template

The drilling template is provided in the packaging box of the communication server.

Wall-mounting procedure

Materials required:

- Screw set for wall/desktop installation
- 6 mm drill bit
- Screwdriver

To mount the SMB Controller to the wall, proceed as follows:

1. Make sure you observe the minimum distances from other objects, walls or ceilings as shown in [Minimum distances for wall mounting \(front panel facing to the right\)](#) and [Minimum distances for wall mounting \(front panel facing downwards\)](#).
2. Drill the three dowel holes.
3. Insert the dowel plugs.
4. Screw in the two shorter upper dowel screws (position A or B).
5. Shut down the SMB Controller (see [Shut-down mode](#)) and disconnect it from the power supply.



Note:

Be sure to observe the safety regulations.

6. Remove the housing cover.
7. Connect the earthing wire (see [Earthing and protecting the communication server](#) on page 59).
8. Suspend the housing of the SMB Controller from the screws.
9. To secure the SMB Controller, screw in the long lower dowel screw (position C).
10. Fit the housing cover.
11. Secure the snap-on tag to the front panel or to a suitable position on the housing cover. The holes in the housing cover are spaced in such a way that the snap-on tag can be secured both lengthways and crossways.
12. Reconnect the SMB Controller to the power supply.

2.4.4.5 Desktop installation

To protect the cable connections, the SMB Controller can also be secured using three screws. The procedure applies as for wall mounting (see [Wall-mounting procedure](#)).

CAUTION:

To ensure adequate heat dissipation, make sure that no objects are placed on top of the SMB Controller (see also Location requirements). Minimum distances must also be observed as shown in [Minimum distances for wall mounting \(front panel facing to the right\)](#).

2.4.4.6 Rack-mounting

The rack-mounting set allows the SMB Controller to be installed horizontally on a 19" rack. Be sure to observe the following:

- The SMB Controller takes up the space of 1.5 height units inside the 19" rack. (1 Unit corresponds to 44.45 mm).
- The holes in the mounting plates allow two SMB Controllers to be placed directly above each other with a space requirement of three units. Different holes in the mounting plates are used for this purpose (see the figure [Placing two SMB Controllers above each other inside a 19" rack](#)).
- The space on the left and right between the SMB Controller and the panels of the 19" rack is for heat dissipation and must remain clear.
- With interface cards that have more than 8 ports it is advisable to route the cabling via a fan-out panel (FOP) (1 height unit).

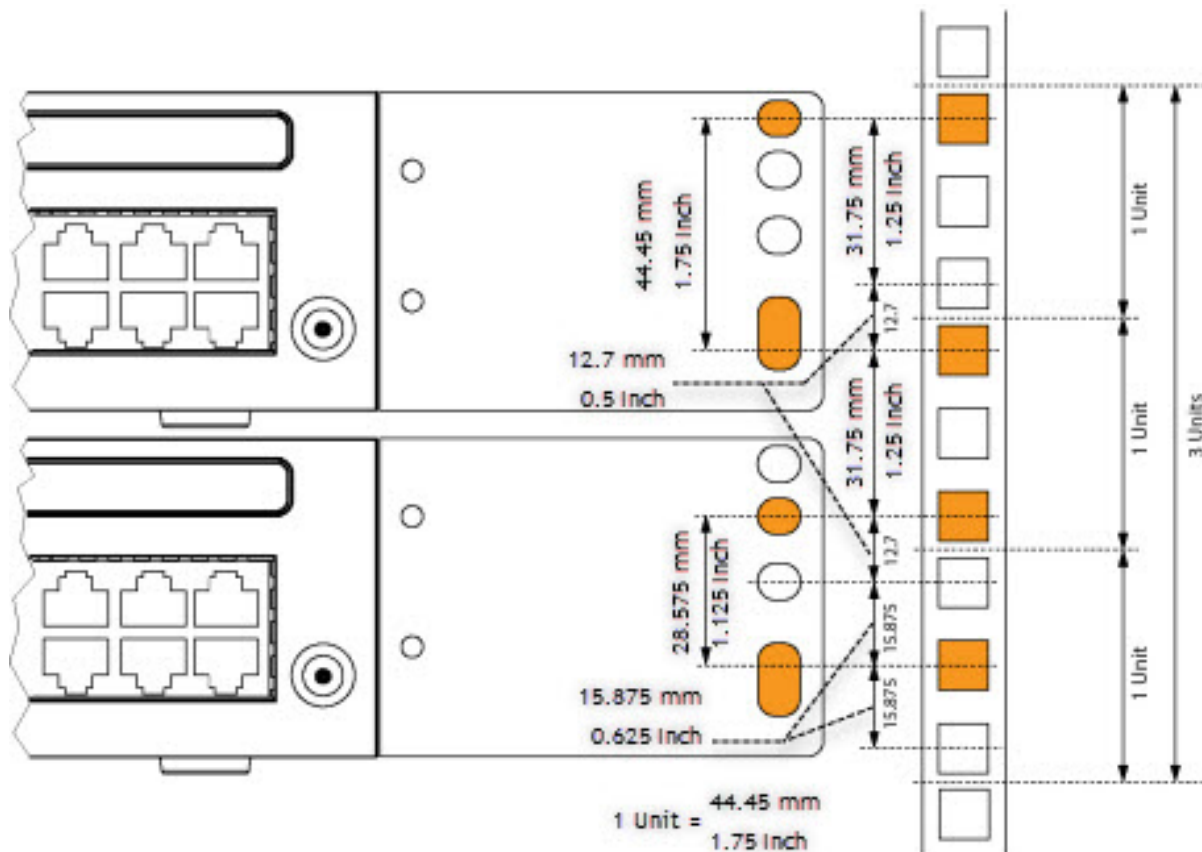


Figure 16: Placing two SMB Controllers above each other inside a 19" rack

2.4.4.6.1 Rack-mounting procedure

Materials required:

- Rack-mounting kit
- Screw set for wall/desktop installation
- Screwdriver

To rack-mount a SMB Controller, proceed as follows:

1. Pull off the screw covers on the left and right of the front panel.
2. Secure the mounting plates to the SMB Controller using the M4 screws. Make sure the front panel and the mounting plate are aligned.
3. Shut down the SMB Controller (see Shut-down mode) and disconnect it from the power supply.

 **CAUTION:**
Be sure to observe the [Safety Regulations](#).

4. Remove the housing cover.
5. Connect the earthing wire (see [Earthing and protecting the communication server](#) on page 59).
6. Fit the housing cover.
7. Secure the cage nuts in the appropriate positions in the rack's fastening rails (see [Placing two SMB Controllers above each other inside a 19" rack](#)).
8. Secure the SMB Controller to the rack's fastening rails using the M6 screws, the plastic washers and the cage nuts.
9. Fasten the snap-on tag to the front panel.
10. Reconnect the SMB Controller to the power supply.

Installing the cable cover

Materials required:

- Cable cover set
- Screwdriver

To install the cable cover, proceed as follows:

1. Pull off the screw covers on the left and right of the front panel.
2. Use the M4 screws of the cable cover set to secure the brackets for the cable cover to the SMB Controller.

Note:

The two brackets are not identical. Compare the cable brackets with the ones in Installing the brackets for the cable cover.

3. Fit the cable cover over the brackets from above until they are felt to engage.



Figure 17: Installing the brackets for the cable cover

Note:

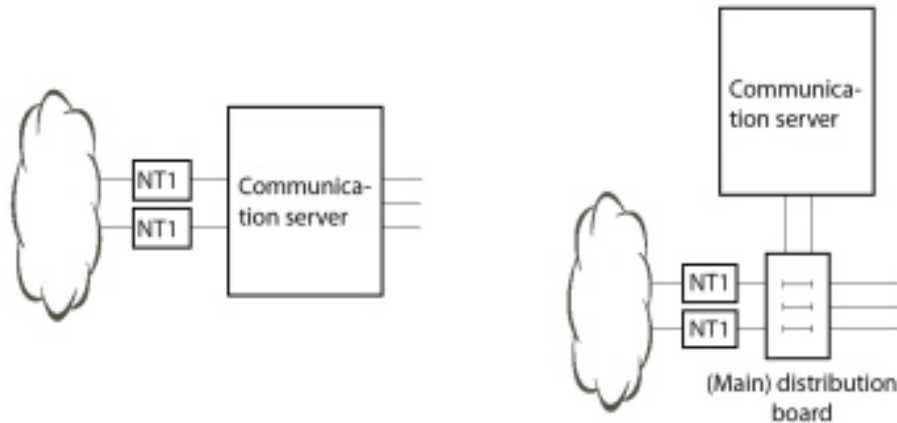
To remove the cable cover reach into the side openings of the cover, gently press the two (engaged) lugs outwards and remove the cover.

2.4.4.7 Connecting the SMB Controller

There are two possibilities for connection to the telephone network and the terminal-side cabling:

- Direct connection
- Indirect cabling via (main) distribution frame and any universal building cable installation (UBC) (see also Connecting to a UBC via a (main) distribution board (example) and Connecting to a UBC via wiring center (example)).

Figure 18: Direct cabling (left) and indirect cabling



(right)

On the front panel all the connections are made using RJ45 connectors.

2.4.4.7.1 Direct connection

Standard commercial cables are used to connect directly to the telephone network. Details can be found in the Chapter Network interfaces.

2.4.4.7.2 Indirect connection

There are two possibilities for connecting the SMB Controller indirectly to the telephone network and terminal-side cabling:

- Connection via main distribution board
- Connection to a universal building cable installation (UBC)

2.4.4.7.2.1 Connection via main distribution board

The interface sockets on the front panel and on the fan-out-panel (FOP) where applicable are connected with the (main) distribution frame or the patch panels using either patch cables or prefabricated system cables (see [Equipment Overview](#)).

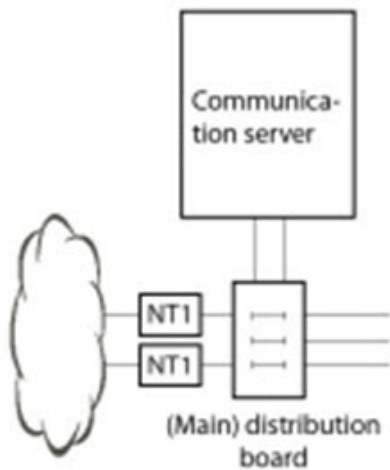


Figure 19: Connection via main distribution board

Prefabricated system cable 4 x RJ45

With terminal cards with eight or more interfaces, some or all of the RJ45 sockets are assigned four-fold on the front panel of the Mitel SMB Controller. With this cable, they can be connected without the use of a fan-out-panel (FOP). The cable is 6m long and at one extremity has four RJ45 connectors on which all the pins are wired.

Table 14: Schematic diagram of prefabricated system cable 4 x RJ45 x 8 Pin

Stranded element	Core color	Cable designation	RJ45 Pin	Port Two-wire connection
1	white	1	4	x.1a
	blue		5	x.1b
	turquoise		3	x.2a
	violet		6	x.2b
2	white		1	x.3a
	orange		2	x.3b
	turquoise		7	x.4a

Stranded element	Core color	Cable designation	RJ45 Pin	Port Two-wire connection
	violet		8	x.4b
3	white	2	4	x.1a
	blue		5	x.1b
	turquoise		3	x.2a
	violet		6	x.2b
4	white		1	x.3a
	orange		2	x.3b
	turquoise		7	x.4a
	violet		8	x.4b
5	white	3	4	x.1a
	blue		5	x.1b
	turquoise		3	x.2a
	violet		6	x.2b
6	white		1	x.3a
	orange		2	x.3b

Stranded element	Core color	Cable designation	RJ45 Pin	Port Two-wire connection
	turquoise		7	x.4a
	violet		8	x.4b
7	white	4	4	x.1a
	blue		5	x.1b
	turquoise		3	x.2a
	violet		6	x.2b
8	white		1	x.3a
	orange		2	x.3b
	turquoise		7	x.4a
	violet		8	x.4b

Prefabricated system cable 12 x RJ45

The cable is 6 m long and, at one extremity, has 12 RJ45 connectors for the interfaces on the front panel. Two of them have 4 cores; the others, 2 cores. This means the cable is suitable for connecting the following interfaces:

- 10 terminal interfaces (DSI, or FXS) or a combination thereof.

Note:

This cable cannot be used to connect Ethernet interfaces. For Ethernet interfaces, use standard commercial connecting cables.

Table 15: Schematic diagram of prefabricated system cable 12 x RJ45

Stranded element	Core color	Cable designation	RJ45 Pin	Signal Connection four-wire	Signal Connection four-wire
1	white	1	4	f	a
	blue		5	e	b
	turquoise		6	d	-
	violet		3	c	-
2	white	2	4	f	a
	blue		5	e	b
	turquoise		6	d	-
	violet		3	c	-
3	white	3	4	-	a
	blue		5	-	b
	turquoise	4	4	-	a

Stranded element	Core color	Cable designation	RJ45 Pin	Signal Connection four-wire	Signal Connection four-wire
	violet		5	-	b
4	white	5	4	-	a
	blue		5	-	b
	turquoise	6	4	-	a
	violet		5	-	b
5	white	7	4	-	a
	blue		5	-	b
	turquoise	8	4	-	a
	violet		5	-	b
6	white	9	4	-	a
	blue		5	-	b
	turquoise	10	4	-	a
	violet		5	-	b
7	white	11	4	-	a
	blue		5	-	b

Stranded element	Core color	Cable designation	RJ45 Pin	Signal Connection four-wire	Signal Connection four-wire
	turquoise	12	4	-	a
	violet		5	-	b s

2.5 Power Up the SMB Controller

The SMB Controller is powered as standard with 230 VAC or 115 VAC. To ensure that its operation is maintained even in the event of a mains outage, an external uninterruptible power supply (UPS) must be used.

2.5.1 115/230 V power supply

The SMB Controller is powered by the supplied power supply unit. The power supply unit is connected to the mains using a two-pin standard power cable.

Warning:

Hazard due to heat generation in the event of short-circuits. The mains power supply connection must be protected with 16 A maximum in countries with 230 V mains power (for instance in Europe), and with 20 A maximum in countries with 115 V mains power (for example, in North America).

Also note the following points:

- The mains connector acts as a disconnecting device and must be positioned so that it is easily accessible.

- Use only the power supply unit supplied.

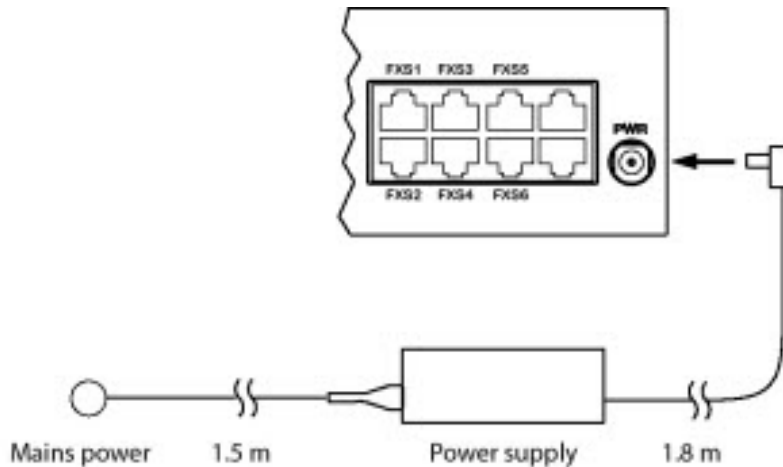


Figure 20: Powering the SMB Controller from the mains

2.5.2 Uninterruptible power supply (UPS)

The use of an external uninterruptible power supply (UPS) is recommended to ensure operation of the controller during a power failure.

The UPS battery capacity is rated according to the SMB Controller's primary power requirements and the required bridging time. The following table shows the maximum power requirements of the SMB Controller in its maximum configuration and maximum traffic volume.

Table 16: Maximum power requirements of the communication server

Communication Server	Maximum power requirements
Mitel SMB Controller	150 VA

The battery capacity required [Ah] can be calculated using the battery voltage and the maximum bridging time. It is important to note that the battery must never be allowed to become completely discharged and that in typical conditions only approx. 60% of the maximum power requirements is needed.

Note:

The uninterrupted operation of the SMB Controller is ensured if the UPS takes over the power supply within 20ms of the mains outage.

2.5.3 Earthing and protecting the communication server

The protective earth and equipotential bonding are important integral parts of the safety concept: Standard EN/IEC 62368-1 relevant to safety matters stipulates protective earthing.

CAUTION:

High leakage currents can occur as a result of connecting to the communication network. Establish an earth connection before connecting to the communications network. Disconnect the communication server from the communications network before carrying out maintenance work.

CAUTION:

Transient overvoltage can occur on the mains and on the communications network. Protect each line installation leading from the building by using one surge voltage protector per core at the isolating point (main) distribution frame or entry point into the building.

Operation on an IT current distribution system:

The communication server can be operated on an IT power distribution system as per EN/IEC 62368-1 with voltages of up to 230 VAC.

Connecting the earthing wire

The communication server's earthing connection is located at the front left on the underside and can only be connected once the housing cover has been removed. The earthing wire is secured by a screw, spring washer and serrated lock washer, which are included in the screw set of the communication server. The serrated lock washer must rest against the metal housing of the communication server.

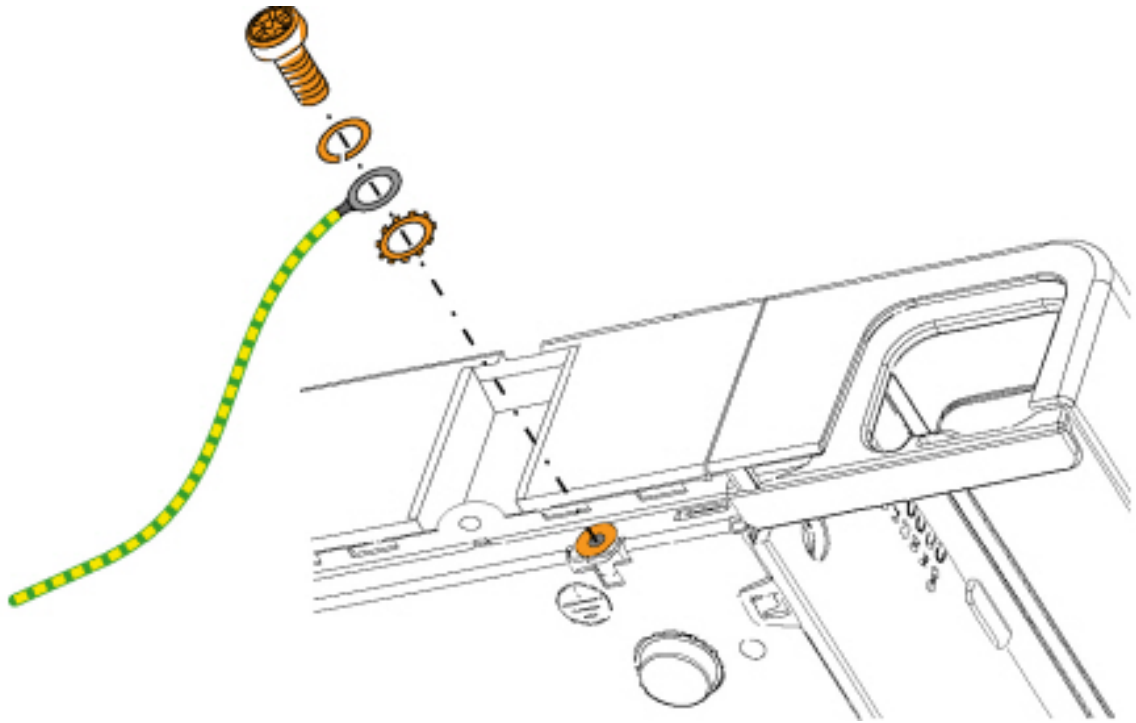


Figure 21: Earthing connection

i Note:

In the case of an indirect connection make sure that the communication server's earthing wire does not form any earth loops with the earthed cable screenings of the installation cables leading up to the (main) distribution frame. The cables should be kept as short as possible and laid out in parallel.

About Mitel Standard Linux

3

This chapter contains the following sections:

- [Server Manager](#)

Mitel Standard Linux (MSL) is an operating system that provides a base for managing the applications, and services from the Mitel Applications Management Center (AMC).

The MSL provides Server Manager Web UI that can be used to install and upgrade the blade applications, including:

- MiVoice Business (MiVB).
- MiVoice Border Gateway (MBG).
- CloudLink Gateway (CLGW).
- Mitel Performance Analytics (MPA) Probe.

MSL allows you to set IP Address(es) for MIVB/MBG, DHCP Server, Backup/Restore of the solution, and so on.

3.1 Server Manager

Server Manager is a web-based application that allows you to manage the MSL, and to perform administrative tasks on the MiVoice Business system. Server Manager is available once you install MSL Container.

Mitel | **MiVoice Business**

Applications
 MiVoice Border Gateway
 CloudLink Gateway

ServiceLink
 Blades
 Status

Administration
 Web services
 Backup
 Restore
 View log files
 Event viewer
 System information
 System monitoring
 System users
 Shutdown or reboot

Security
 Remote access
 Syslog
 Web Server
 MBG client certificates

Configuration
 IP settings
 Networks
 E-mail settings
 Google Apps
 Cloud Service Provider
 DHCP
 SNMP
 Review configuration

Miscellaneous
 Support and licensing
 Help

Welcome to the server manager

This server is a very secure, reliable and cost-effective platform for an expanding range of bu available for this platform, please contact your authorized reseller.

To perform a system administration function, click one of the links in the menu on the left of y

MiVoice Business 10.0.0.76
 MiVoice Border Gateway 11.5.0.86
 © Mitel Networks Corporation

Figure 22: Server Manager Configuration Tool

Table 17: Panels and Functionality

Grouping	Panel	Functionality
ServiceLink	Blades	Provides blade install/upgrade/removal.
	Status	Provides AMC syncs, ARID registration/de-registration, offline syncs.

Grouping	Panel	Functionality
Administration	Web services	Permits configuration of MSL's web services interface, and the clients that are permitted to use it.
	Backup	Backs up system and allows for applications to include their backups as part of the system backup.
	Restore	Restores system data and application data (if it was included in backup).
	View log files	Provides SOS report, which includes platform logs and application logs.
	Event viewer	Provides system events and allows for application integration (that is, applications can raise their own events). Used by MSL and MBG. Does NOT exist on PPC. Not used by MiVB.
	System information	
	System monitoring	
	System users	
	Shutdown or reboot	
Security	Remote access	Configure VPN (PPTP) settings, add remote management networks and configure shell access.

Grouping	Panel	Functionality
	Syslog	Configures the local syslog server to accept remote syslog events from other hosts. Can also configure sending local syslog events to remote syslog servers
	Web Server	Web server certificates
Configuration	IP settings	Configure the server name, IP addresses, Internal Network Interface (LAN), and reset network settings
	Networks	Add trusted networks and additional network routes.
	E-mail settings	
	Google Apps	
	Cloud Service Provider	
	DHCP	Configure DHCP server.
	Simple Network Management Protocol (SNMP)	Configure Simple Network Management Protocol (SNMP) support.
	Review configuration	Review Networking parameters and Domain information.
Miscellaneous	Support and licensing	EULA
	Help	

About MiVoice Business

4

This chapter contains the following sections:

- [Purpose and function](#)
- [Data Protection](#)
- [Feature Interactions](#)

Mitel® MiVoice Business is the brand name of the call-processing software that runs on several hardware platforms including industry-standard servers, virtual machines, and MiVoice Business Applications purpose-built hardware.

MiVoice Business on SMB Controller Limitations

- No support for Positive Disconnect.
- No support for Loudspeaker pager
- No support for physical Music on Hold port (MoH is supported via an FXS interface)
- Limited DSP support

Networking:

- The SMB Controller will have its own IP address, see [SMB Controller Manager](#) on page 10.
- The MiVoice Business will use the MSL LAN address. For more details, see [Initial MSL Network Setup](#) on page 96.

4.1 Purpose and function

MiVoice Business is an open, modular, and comprehensive communication solution for the business sector that integrates several communication servers of different performance and expansion capacity, an extensive telephone portfolio, and provision for accommodating expansion cards and modules. The expansions include an application server for unified communications and multimedia services, an open interface for application developers, and multiple expansion cards, and modules.

The business communication solution with all its components was developed to fully cover the communication requirements of businesses and organizations, in a way that is both user-friendly and maintenance-friendly. The individual products and components are coordinated and must not be used for other purposes or replaced by third-party products or components (unless it is to connect other approved networks, applications, and terminals to the interfaces certified specially for that purpose).

4.2 Data Protection

You are advised to perform regular MSL back up after making any changes to your configuration data.

Protection of user data

During operation, the communication system records and stores user data (for example, call data, contacts, and voice messages). Protect this data from unauthorized access by using restrictive access control:

- Restrict the number of user accounts to the minimum necessary and assign to the user accounts only those authorization profiles that are required.
- Instruct users with access rights to change their passwords on a regular basis and manage the passwords in a secure manner.

Protection against listening in and recording

The MiVoice Business communication solution comprises features that allow calls to be monitored or recorded without the parties on the call being aware. Inform your customers that these features can be used only in compliance with national data protection provisions.

Unencrypted phone calls made on the IP network can be recorded and played back by anyone with the right resources:

- Use encrypted voice transmission (Secure VoIP) whenever possible.
- Use dedicated encrypted VPN, or private network connections, between different business locations on the same private network. This will ensure secure connections in addition to encryption on the end-devices, such as IP or SIP phones.
- Use the MiVoice Border Gateway to connect Teleworker phones that are connected to the business over public networks, i.e. Internet. Teleworker phones include secure connection to and from MiVoice Border Gateway and do not require a separate VPN (allowing simple installation and mobility).

4.3 Feature Interactions

4.3.1 Embedded Voice Mail

The MiVB on the SMB Controller supports up to 16 Voice Mail Ports and 750 Voice Mailboxes. These specifications are applied to the following forms:

- VM Port Capacity
- VM Ports
- VM Greetings
- VM Mailboxes
- VM RAD Greetings



Note:

Of the 16 Voice Mail Ports available, it is recommended to provide 10 Ports for Voice Mail to support 150 Users with the remaining four supporting Auto Attendant.

4.3.1.1 Number of Voice Mail or Auto Attendant Ports

ESM has set the Voice Mail or Auto Attendant Port Limits to these values for the SMB Controller:

- Default - 6
- Minimum - 0
- Maximum - 16

4.3.1.2 Visual Voice Mail (VVM) Support in Embedded Voice Mail

Visual Voicemail (VVM) support for external applications is now extended in MiVB 10.0 to all MiVoice Business on x86, SMB Controller, and EX except PPC platforms. This extension will be used by external applications like MiCollab Enterprise and CloudLink solutions. The behavior of the Visual Voice Mail feature remains the same as it was in the MiVoice Business 9.1 Release.

4.3.2 Trunks

The MiVoice Business on SMB Controller will support the regular accompaniment of IP Trunks, SIP Trunks, and Analog Trunking.

R2 Trunks, T1 Trunks, E1 Trunks, and BRI are not supported.

Loop Tie and E&M FXO trunks are not supported.

4.3.3 Analog Loop Start (LS) Trunks

The hardware supports Analog Loop Start (LS) Trunks. The Analog Trunks can be designated as CLASS Trunks as well. These and other specifications are defined in the CO Trunk Circuit Descriptors Form.

Note:

- Analog Loop Start (LS) Trunks is also known as FXO.
- Positive Disconnect is not supported on FXO hardware

4.3.4 ONS (FXS) Devices

The SMB Controller does not support OPS Lines and does not support System Failure Transfer. The specifications are defined in the ONS/OPS Circuit Descriptor Form.

Note:

To maintain emergency services during a power outage or a Controller outage, the Administrator may want to ensure that a POTS phone with PSTN connectivity is deployed and identified as an emergency phone.

Note:

- ONS Devices are Devices connected to the FXS Ports.
- Positive Disconnect is not supported for ONS (FXS) devices.

4.3.5 DSP Allocation

The DSPs are loaded at boot time and the allocation cannot be changed at run time without a MiVoice Business reboot. The DSP allocation depends on the number of required Voice Mail/Auto Attendant ports. The number of supported VoIP channels (E2T channels) is driven by whether G.729 Compression is enabled or not.

For more details on the required DSP cards in the system, see the following table.

Configuration instance #	# of DSP expansion cards	Max # of VM ports	# of Compressions (G729)	Max # VoIP channels	Max # of phones per page group	Recommended for
1	1	6	0	20	10	80 users configuration with up to 6 VM ports
2	2	6	0	40	20	80 users configuration with up to 6 VM ports
3	2	6	1 to 24	24	12	80 users configuration with up to 6 VM ports
4	2	16	0	30	15	150 users configuration with up to 16 VM ports
5	3	16	0	50	25	150 users configuration with up to 16 VM ports
6	3	16	1 to 30	30	15	150 users configuration with up to 16 VM ports

Configuration instance #	# of DSP expansion cards	Max # of VM ports	# of Compressions (G729)	Max # VoIP channels	Max # of phones per page group	Recommended for
7	1	6	0	20	10	150 rooms + 25 staff
8	2	6	24	24	12	150 rooms + 25 staff
9	2	16	0	50	25	300 rooms + 50 staff
10	3	16	30	30	15	300 rooms + 50 staff

Note:

Configuring the number of VM ports and/or the number of voice compressions beyond the boundaries listed in the above table will result in a DSP alarm.

The MiVoice Business on SMB Controller loads DSPs during the application startup. To take effect, changes in the DSP allocation require MiVoice Business application restart.

4.3.6 Loudspeaker Paging

Since SMB Controller does not have a dedicated loudspeaker paging port, you can use any industry standard SIP or analog paging devices.

4.3.7 Music on Hold (MOH)

The SMB Controller supports Music on Hold (MOH) using the following sources:

- Analog Music on Hold using an FXS Port as Audio Input.

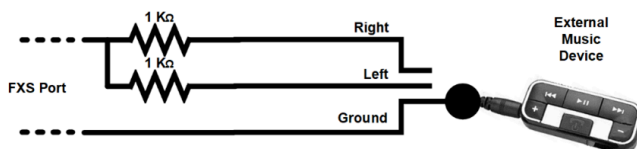


Figure 23: FXS Port MOH Circuit

- Embedded Music on Hold (up to four Music on Hold sources, up to 4 MB total RAM, and up to eight minutes of total play time.)
- Live Music on Hold over IP

i Note:

- If two to four Music-on-Hold sources are configured, additional DSP2 cards are required.

See the [DSP Allocation](#) on page 68 section of the documentation for more information on how many DSP cards are required for the SMB Controller and how they are allocated.

- If Music On Hold (MOH) is required, the number of Voicemail Port Capacity must be set to a minimum of 7 and a maximum of 16 for the usage of additional MOH sources.
- Only the FXS interfaces on the mainboard of the SMB Controller (FXS1...FXS6) support the Analog Music on Hold feature. FXS interfaces on expansion cards cannot be used.
- Use the Mitel MoH Input Adapter (50006162) for connecting the external music source to the FXS embedded port.
- The customer is responsible for all copyright matters relating to any music playback.

About MiVoice Border Gateway

5

The MiVoice Border Gateway (MBG) Blade provides advanced functionality such as Application and Web Proxy, Teleworker support, Advanced SIP Trunk proxying (including KPML), Secure Recording Connector (SRC), SIP Trunk Proxying allows connection to an external Call Recording Equipment (CRE), API and Proxy for remote applications, CloudLink Gateway, and Advanced SIP Trunk proxying (including Key Press Markup Language (KPML)³).

Note:

You must license the solution prior to installing any Blades.

MiVoice Border Gateway functions included:

- SIP Trunk proxy – for Telco Connectivity
- Teleworker – for SIP and MiNET devices
- API and Proxy for remote applications
- Call Recording –Secure Recording Connector (SRC) function
- CloudLink Gateway (CLGW)

Limitations

- The MiVoice Border Gateway Blade on SMB Controller can only use the Server Gateway Mode deployment model using the co-resident with Call Manager Networking Profile.
- The embedded MiVoice Border Gateway is scaled to support up to 150 users on the SMB Controller. Increased scaling can be obtained with an external off-board MiVoice Border Gateway.
- Customers using the embedded MiVoice Border Gateway and an off-board MiCollab must maintain the MiVoice Border Gateway capacity limitations of the SMB Controller.
- Customers with MiCollab must use an off-board MiVoice Border Gateway.

Networking

- The SMB Controller will have its own IP address on the customer LAN.
- The MiVoice Business will be using the MSL LAN address.
- The MiVoice Border Gateway must use the second LAN IP Address programmed in MSL. For more details, see [Initial MSL Network Setup](#) on page 96.
- The MiVoice Border Gateway will also use a WAN address programmed in MSL. This WAN connection is expected to be connected directly to the internet (via an ISP router). For more details, see [Initial MSL Network Setup](#) on page 96.
- The Eth1 Port is enabled and DHCP deselected in the SMB Controller Manager's IP Network Panel.

³ Keypad Markup Language (KPML) is used to indicate DTMF tones in SIP messaging. KPML is used by the Key Press Stimulus Package as a SIP Event Notification Package. Endpoints will send DTMF tone indications via NOTIFY messages.

For more information about installing and maintaining the MiVoice Border Gateway, refer to the [MiVoice Border Gateway Installation and Maintenance Guide](#) and [MiVoice Border Gateway \(MBG\) Rel 11.5 I&M Self-Study](#)

About CloudLink Gateway

6

The CloudLink Gateway (CLGW) Blade provides integration with CloudLink-based (for example, CloudLink API program or Mitel Assistant).

Limitations

- The embedded CloudLink Gateway is intended only to service the users of a single SMB Controller platform.



Note:

Larger deployments should use an offboard CloudLink Gateway

- If the MiVoice Border Gateway/CloudLink Gateway is offboard, the CloudLink Gateway is expected to be offboard too.



Note:

The CloudLink Gateway for MiVoice Office 400 on SMB Controller application (installable via [SMB Controller Manager](#)). Be sure to install the CloudLink Gateway for MiVoice Business for this installation, and not the CloudLink Gateway for MiVoice Office 400 which can run on the same hardware.

Networking

- CloudLink Gateway Blade will use the SMB Controller's ETH0 Ethernet port to access the CloudLink services. As a result, it requires access to the CloudLink Cloud Service via the Customer's Internet Gateway.



Note:

Eth0 should never be directly connected to the Internet.

For more information about the CloudLink Gateway, refer to the [CloudLink Documentation](#) and [CloudLink Onboarding for MiVoice Business](#)

About Mitel Performance Analytics Probe

7

The Mitel Performance Analytics Probe blade is an optional blade that provides integration with Mitel Performance Analytics Cloud Service. For more information about Mitel Performance Analytics, see <https://www.mitel.com/document-center/applications/analytics/mitel-performance-analytics>.

Limitations:

- The embedded Mitel Performance Analytics Probe is intended only to handle the functions and Users of a single SMB Controller. Other applications such as an external MiVoice Business, MiVoice Border Gateway, and so on require an additional external Mitel Performance Analytics Probe. Larger deployments must use an additional offboard Mitel Performance Analytics Probe.
- If the MiVoice Border Gateway/CloudLink Gateway are offboard, the Mitel Performance Analytics Probe is expected to be offboard too.
- A secondary probe is required for resiliency, along with a secondary MiVoice Business, secondary MiVoice Border Gateway, and secondary CloudLink Gateway.

Networking

- Mitel Performance Analytics Probe creates a Reverse VPN Tunnel back to the Mitel Performance Analytics Cloud Service to ensure a secure connection for data transfer. The tunnel can also provide secure access for remote management and maintenance from the Cloud Service. The VPN Connection is via the customer's Internet Gateway.

For more information about the MPA Probe, refer to the [Mitel Performance Analytics Documentation](#) and [Mitel Performance Training](#).

About Initial Configuration Wizard (ICW)

8

This chapter contains the following sections:

- [ICW Backup and Restore](#)

The Initial Configuration Wizard (ICW) Blade can be used to support the installation and deployment of the MiVoice Business and multiple applications.

The current supported deployment option for the Initial Configuration Wizard is to provision the MiVoice Business and MiVoice Border Gateway at a new installation.

For the Initial Configuration Wizard on the SMB Controller, the overall procedures are:

1. Install the MSL/Server-Manager Container.
2. License the SMB Controller via Server Manager.
3. Install the MiVoice Business Blade and MiVoice Border Gateway Blade (required only if MiVoice Border Gateway needs to be deployed).
4. Install the Initial Configuration Wizard Blade.
5. Launch the Initial Configuration Wizard from the Server Manager.

Note:

The Initial Configuration Wizard requires at least one application to provision, so the Initial Configuration Wizard Blade will be launched only if at least MiVoice Business Blade is installed.

6. On the Initial Configuration Wizard, provision MiVoice Business and the MiVoice Border Gateway.

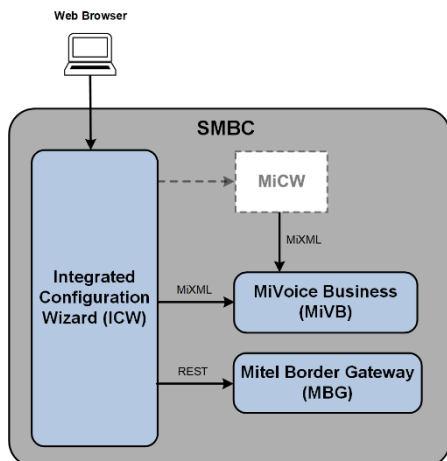


Figure 24: Initial Configuration Wizard for New System

8.1 ICW Backup and Restore

The Initial Configuration Wizard (ICW) triggers MSL scripts to perform a full MSL data backup before configuring the system. The backup file (*backup.tgz*) will be stored in the */var/cache/vucc/databases* folder of the file system. The backup file will be deleted after the configuration is completed successfully or if the Initial Configuration Wizard blade is uninstalled.

If the configuration is unsuccessful, the Initial Configuration Wizard will leave the system in a failed state for the user to troubleshoot, correct, or complete the configuration. In such a case, the backup file is retained.

The user can start a new configuration process or restore the backup data that was saved from the last run of the ICW. For more details about restoring the backup data that was saved from the last run of the ICW, see the [Configuration Options Page](#) on page 137.

After a successful configuration, users are recommended to schedule a periodic network backup from the Server Manager Backup panel for maintenance and disaster recovery.

Deployment Steps for the MiVoice Business Solution on SMB Controller

9

This chapter contains the following sections:

- [Initial Setup of SMB Controller](#)
- [Configure the Applications](#)
- [Integrate Applications](#)

MiVoice Business Solution on SMB Controller is designed to be highly flexible and fits into different deployment models because multiple embedded applications such as MiVoice Border Gateway, Mitel Performance Analytics Probe, Initial Configuration Wizard, and CloudLink Gateway can be installed along-side the MiVoice Business application.

Note:

Only certain combinations of these embedded applications are supported as the deployments are intended to service only the embedded call engine and is scaled only for the SMB market.

The following Flow Chart summarizes the deployment process. If needed, print the flow chart and use it as a checklist.

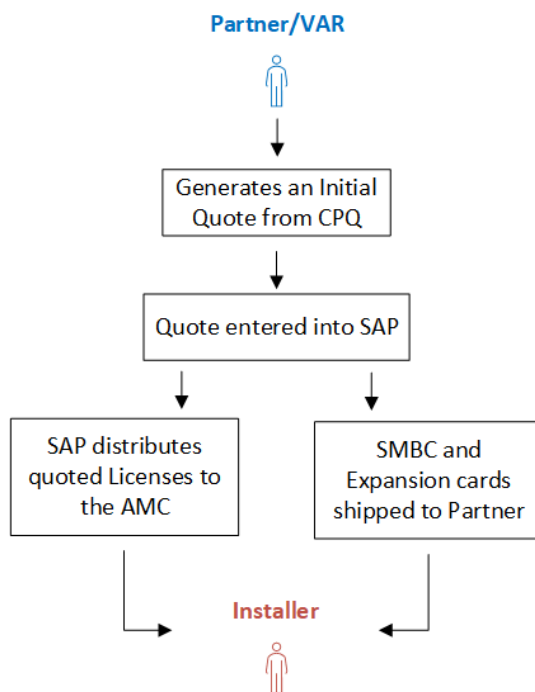


Figure 25: Steps to be performed by the partner

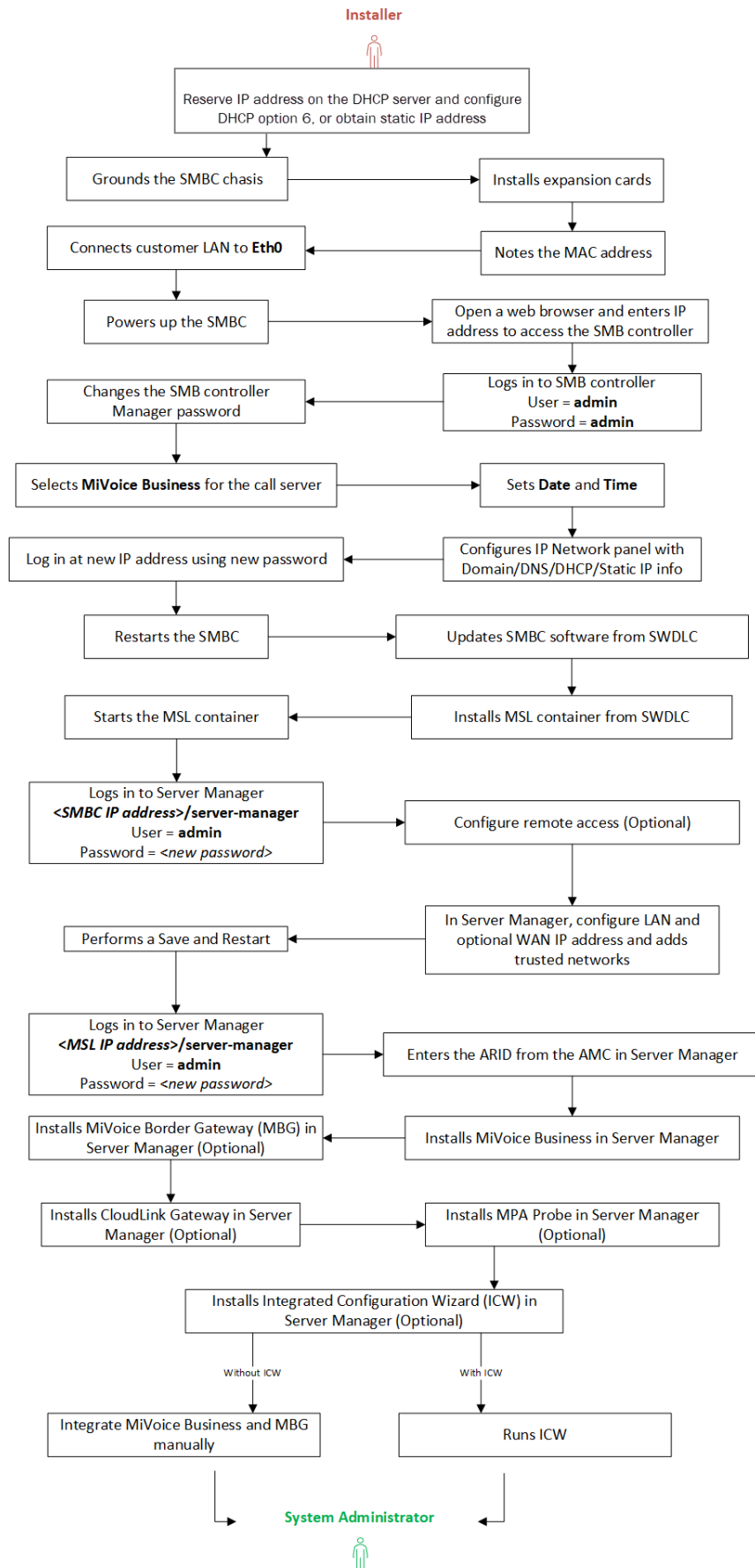


Figure 26: Steps to be performed by the installer

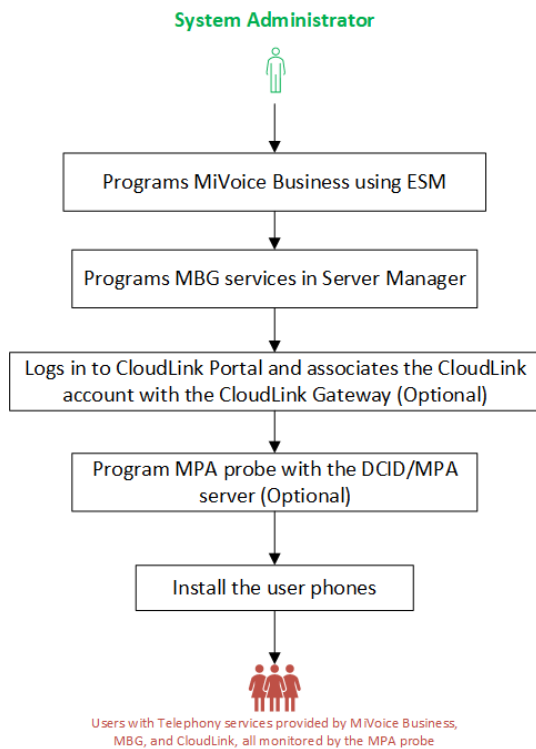


Figure 27: Steps to be performed by the system administrator

The supported combinations with MiVoice Business are shown in the following table:

MBG (MiVoice Border Gateway)	CLGW (CloudLink Gateway)	MPA Probe	Comments
No	No	No	SMB customers (MiVoice Business supports resiliency) Larger Customers that cluster with an SMB Controller for PSTN access. Can also integrate with offboard MiVoice Border Gateway/CloudLink Gateway. Customers that want integration with certain applications: For example, MiCollab.
No	No	Yes	SMB customers who require MPA integration (Standalone/resilient)
Yes	No	No	SMB customers who require SIP Trunking and/or Teleworker support (MiVoice Business and MiVoice Border Gateway support resiliency).

MBG (MiVoice Border Gateway)	CLGW (CloudLink Gateway)	MPA Probe	Comments
Yes	No	Yes	SMB customer that wants SIP Trunking and/or Teleworker support with MPA integration (MiVoice Business, MiVoice Border Gateway, and MPA Probe support resiliency).
Yes	Yes	No	SMB customers who require SIP Trunking and/or Teleworker or Cloud applications (MiVoice Business and MBG support resiliency, except CloudLink Gateway).
Yes	Yes	Yes	SMB customers who require SIP Trunking and/or Teleworker or Cloud applications with MPA integration (MiVoice Business, MiVoice Border Gateway, and MPA Probe support resiliency except CloudLink Gateway).

Note:

The Mitel Performance Analytics probe is not dependent on any other applications, but the CloudLink Gateway requires MiVoice Border Gateway to be installed..

9.1 Initial Setup of SMB Controller

The SMB Controller comes from factory with Mitel Embedded Linux Distribution OS and SMB Controller Manager software installed, but no Call Control Manager. MSL container and other Mitel applications must be installed manually.

Note:

These procedures are for a new SMB Controller or for an SMB Controller that has been Factory Reset.

This section describes the initial setup of the SMB Controller, configuring the SMB Controller's IP address, changing the initial login and password, setting the Date and Time, and configuring the DNS and Domain.

Note:

It is not possible to recover a forgotten SMB Controller Manager Admin Password. The only way to recover the SMB Controller is to put the system into [Emergency Mode](#) via CTRL Button and then initiate a [Factory Reset](#).

9.1.1 Requirements

General Requirements

- A computer with an internet browser, internet access. Partner login credentials to access Mitel [MiAccess Portal](#).

The following browsers are supported.

- Chrome
- Firefox
- Microsoft Edge
- Internet access is for licensing and software downloads.
- For SIP Trunks, you need a SIP account provided by a SIP provider.

Required Downloads

Before you start, download the required documents and applications. For details, see [Download documents, system software and tools](#) on page 5.

9.1.2 Set up Initial Network Access to the SMB Controller

A brand new or a factory reset SMB Controller starts with Eth0 in a DHCP Client mode by default and obtains its IP address from a DHCP Server. If the communication server cannot find a DHCP server within 90 seconds, it uses the default IP address, and the system is then accessible via the default IP address (192.168.104.13/255.255.255.0 with default gateway 0.0.0.0).

Table 18: Configuring the SMB Controller System IP address

Method	Enable Eth0 DHCP?	Eth0 IP addresses
Customer-provided static IP address (Highly recommended)	No, disable the DHCP	Change the Provided by customer. Change the IP address to the one the customer provided.

Method	Enable Eth0 DHCP?	Eth0 IP addresses
No DHCP server (direct Ethernet cable connection between programming PC and Eth0) (Highly recommended)	No, disable the DHCP	192.168.104.13/24 (default). Change the default IP address of the SMB Controller.
Customer-provided reserved IP address from their DHCP server and configured DHCP Option 6, Domain Name Server. (Recommended)	Yes	Provided by DHCP Server. No need to change the IP address.
Customer-provided dynamic IP address from their DHCP server and configured DHCP Option 6, Domain Name Server. (not recommended)	Yes	Provided by DHCP server. Change the IP address to the one the customer provided.

Using the Factory Default IP Address

1. Change the network adapter settings on the programming PC to the IP addresses *192.168.104.x* and the Subnet *255.255.255.0*. Do not use *192.168.104.13*. The below example uses *192.168.104.5*.

Internet Protocol Version 4 (TCP/IPv4) Properties [X]

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 104 . 5

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Figure 28: Configuring Programming PC to SMB Controller Default Subnet

2. Connect the SMB Controller directly to the computer using the Eth0 port.
3. Connect the power adapter to the socket on the front panel and to a power source (100 - 240 VAC/48 - 62 Hz).

4. When the startup is completed, the SMB Controller runs in normal mode and by default, the DHCP is enabled. The PWR LED and F0 LEDs are green, and the SYS LED is green and flashing.

Execute Factory Default static IP Address procedure to set controller's IP address to 192.168.104.13.

5. To test the connection, open a browser and enter the IP address of your SMB Controller including port number 8443. For example, *https://192.168.104.13:8443* The SMB Controller Manager login page is displayed.

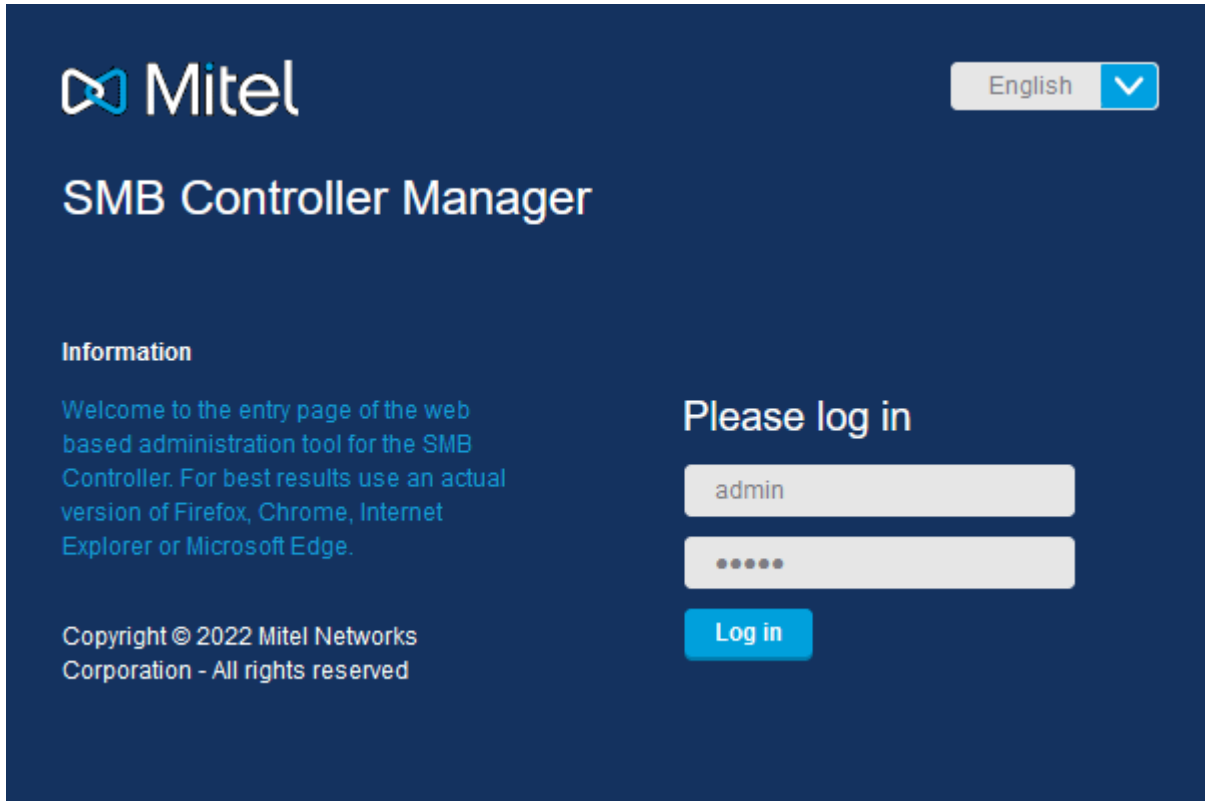


Figure 29: SMB Controller Manager Log in Page

Using the DHCP provided IP Address

The SMB Controller is accessible via an IP address provided by a DHCP server.

i Note:

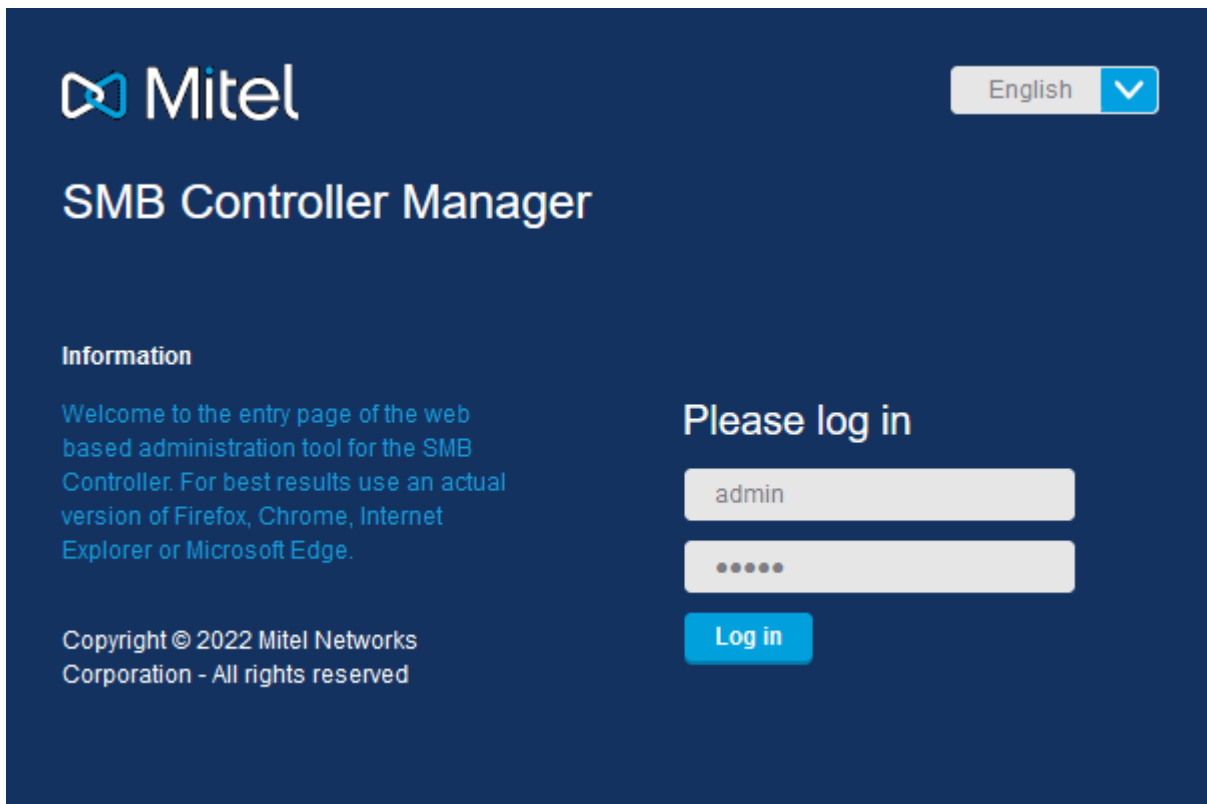
The DHCP Server must have provisioned DHCP Option 6, Domain Name Server option. Otherwise, after 90 seconds the SMB Controller will default to its static IP address 192.168.104.13/24. At that point the F0 LED will display a steady orange light and you will have to access the controller off the network as described in [Using the Factory Default IP Address](#).

Note:

It is recommended to obtain a static IP address or reserve an IP address on the DHCP server for the subnet to the SMB Controller based on its MAC address.

Following allocation of a dynamic address via DHCP, an administrator can then access the SMB Controller to program in a mutually agreed static IP address that will not conflict with the external DHCP server. Ensure that DNS is also updated accordingly.

To test the connection, open a browser and enter the IP address of your SMB Controller including the port number 8443. For example, <https://x.x.x.x.:8443>. The SMB Controller Manager login page is displayed.



Mitel

English ▼

SMB Controller Manager

Information

Welcome to the entry page of the web based administration tool for the SMB Controller. For best results use an actual version of Firefox, Chrome, Internet Explorer or Microsoft Edge.

Copyright © 2022 Mitel Networks Corporation - All rights reserved

Please log in

admin

.....

Log in

Figure 30: SMB Controller Manager Log in Page

1. Connect the Eth0 of the SMB Controller to the same subnet where the DHCP server is running.
2. Connect the power adapter to the socket on the front panel and to a power source (100 - 240 VAC/48 - 62 Hz).
3. When the startup is completed, the SMB Controller runs in normal mode. The PWR LED and F0 LEDs are green, and the SYS LED is green and flashing.

Note:

If the communication server cannot find a DHCP server within 90 seconds, it uses the default IP address and the F0 LED turns and stays orange. Now the system is accessible via the default IP address.

4. To test the connection, open a browser and enter the IP address of your SMB Controller including the port number 8443. For example, <https://x.x.x.x:8443>. The SMB Controller Manager login page is displayed.

Figure 31: SMB Controller Manager Log in Page

9.1.3 Set Credentials for the SMB Controller

1. Open a browser window and enter the IP address of your SMB Controller including the port 8443 (Example: <https://192.168.104.13:8443>).
 - The SMB Controller Manager login page is displayed.
2. Log in with the admin username and the appropriate password (default username and password is *admin*).
 - You are asked to change the password. Following are the rules for SMB Controller password:

Note:

- A password must consist of a minimum of 8 and a maximum of 255 characters.
- The password must contain a minimum of 1 uppercase character (A-Z).
- The password must contain a minimum of 1 lowercase character (a-z).
- The password must contain a minimum of 1 digit (0-9).
- The password must contain at least 1 of the following special characters: ? / < > . , - + * # = ! " \$ % & ' () : ; @ [\] ^ _ ` { | } ~ <space>
- German umlauts (e.g. ä, ö, ü) and other diacritical characters (e.g. é, à, â) are not permitted.
- The default password password is not permitted.
- The password must not be the same as the user name.

Note:

You can create up to five user accounts, with the same administrator privileges. This multiple admin account feature ensures that an alternative account will always be available. If one administrator forgets their password, others can still access the SMB Controller. This feature prevents losing access to the SMBC due to forgotten passwords..

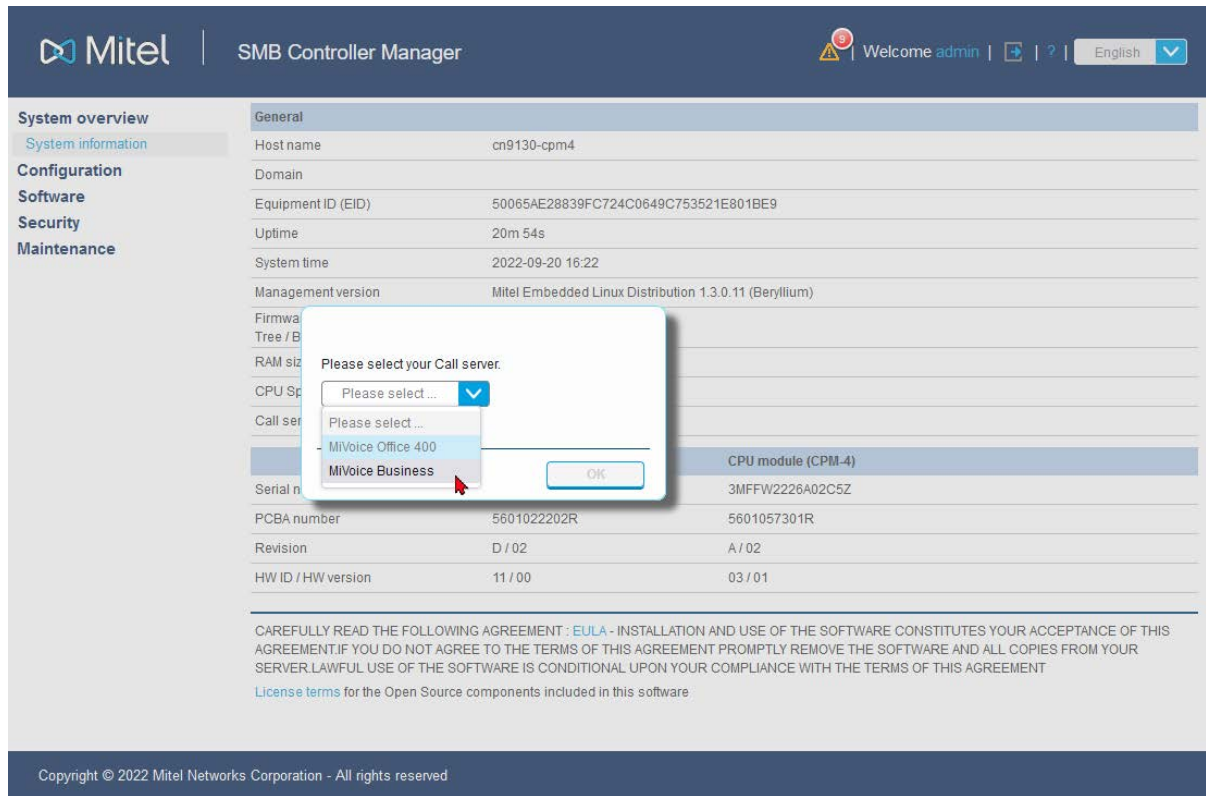
See [Managing Multiple Admin Accounts on SMB Controller Manager](#) on page 158 for more details on managing multiple user accounts on SMB Controller.

3. Click the **Change button to confirm the new password.**

The System Information page of the SMB Controller Manager is displayed, and you are prompted to select the Call Server

9.1.4 Identifying the Call Server for SMB Controller

1. Select **MiVoice Business** from the Call Server drop-down menu and then click the **OK** button.



Once the SMB Controller is ready to configure the MiVoice Business, the system info page is displayed with a message to restart the system to activate the new settings.

Note:

Do not restart the controller before configuring the IP address.

9.1.5 Configure SMB Controller IP Address

1. After you have selected MiVoice Business in the previous step, navigate to the **IP Network** page (SMB Controller Manager > *Configuration* > *IP Network*).

Note:

If the SMB Controller features its default static IP address, a pop up window appears to remind you that you must choose a different static address for your subnet. Click the OK button to continue with the configuration.

2. Configure Network settings:

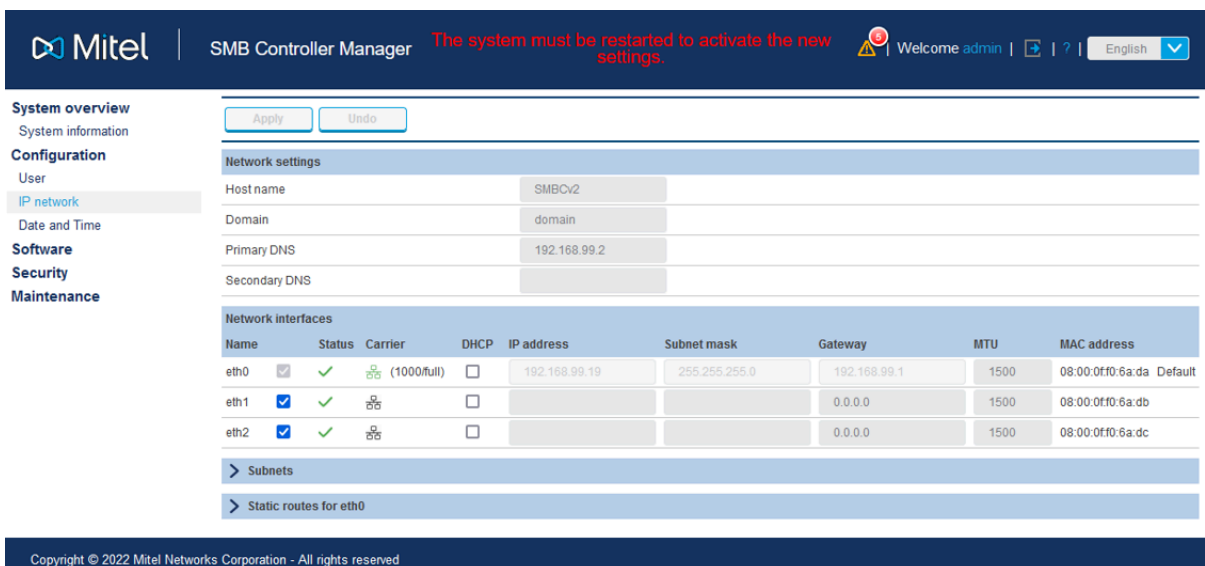
- Provide the host name, domain name in the respective fields.
- In the **Primary DNS** and **Secondary DNS** field, enter the Primary and Secondary DNS IP address.

3. Configure Network interfaces:

- If you are using static IP configuration:
 - a. Deselect the DHCP checkbox for **eth0**.
 - b. Enter the static IP address, the corresponding Subnet Mask, and the Gateway IP address.
 - c. Verify that **eth1** is enabled.
- If you are using dynamic IP configuration:
 - a. Select the DHCP checkbox for **eth0**.

Note:

You may have to re-configure IP configuration of your management PC to be able to reach the SMB Controller Manager.

• 

4. Click **Apply**. The following message is displayed.

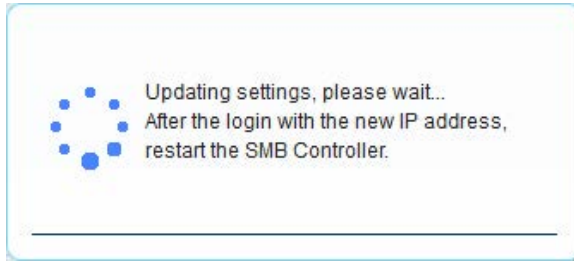


Figure 32: Restart Reminder

Once the configurations have been updated, the SMB Controller will disconnect from the current network, and it will then be reachable at the new IP address.

5. If the SMB Controller was accessed from the default IP address, perform the following:
- a. Reconfigure the network settings on the programming PC to their default values.
 - b. Enter the new IP address of your SMB Controller in the browser window including the port 8443 (Example: `http://192.168.99.19:8443`).
6. Log in with the username *admin* and your new password.
7. From the left panel, select the **Maintenance** section and then click **System reset**.
8. From the **System reset** window, click on the **Restart**.

The new settings are activated.

9.1.6 Set Date and Time

To change the Date and Time:

1. Log into the SMB Controller Manager and under **Configuration**, select **Date and Time**.
2. Modify the fields with appropriate responses.
3. Do either of the following:
 - If you are using the NTP server, do the following
 - a. Select **System time zone**.
 - b. Enable the **Time synchronisation via time server** option.
 - c. Ensure that the NTP servers specified are correct.
 - If you are not using the NTP server, do the following:
 - a. Disable the **Time synchronisation via time server** option.
 - b. Enter the system date in the **System date** field.
 - c. Enter the system time in the **System time** field.
 - d. Set the current date in the **Set current date** field.
 - e. Set the current time in the **Set current time** field.

4. Select

Mitel

SMB Controller Manager

Welcome admin | ? | English

System overview

System information

Configuration

User

IP network

Date and Time

Software

Security

Maintenance

Apply

Undo

Date and time

System date2022-09-20Set current date (Date format: YYYY-MM-DD)

System time10:12:49Set current time (Time format: 24 hours mode)

System time zone(+00:00) MST

Time synchronisation via time server using NTP (network time protocol)

Time synchronisation via time server☒

NTP servers0.mitel.pool.ntp.orgSet default NTP servers1.mitel.pool.ntp.org2.mitel.pool.ntp.org3.mitel.pool.ntp.org

Copyright © 2022 Mitel Networks Corporation - All rights reserved

Apply.

9.1.7 Upgrading the SMB Controller Software

The SMB Controller comes with Mitel Embedded Linux with SMB Controller Manager software installed. However, due to ongoing updates and product improvements. It is recommended to upgrade the SMB Controller manager firmware to the latest packages prior to installation and configuration of the applications.

Note:

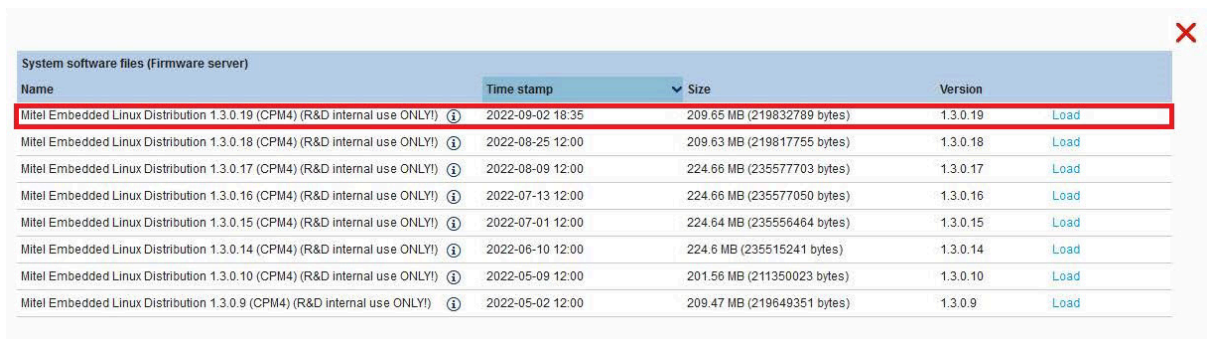
- If MSL is already installed, it might be necessary to install a new version of the same, after an update of the SMB Controller system software. For more details, see [Install MSL Container](#) on page 93.

1. Login to SMB Controller Manager.

2. Navigate to **Software - System Software** and agree to the **EULA**.

- For the SMB Controller with internet access:
 - a. Click **Firmware server...** to see a list of available SMB Controller manager firmware versions (for example, "Mitel Embedded Linux Distribution 1.3.0.27").
 - b. Click **Load** next to the required firmware version.

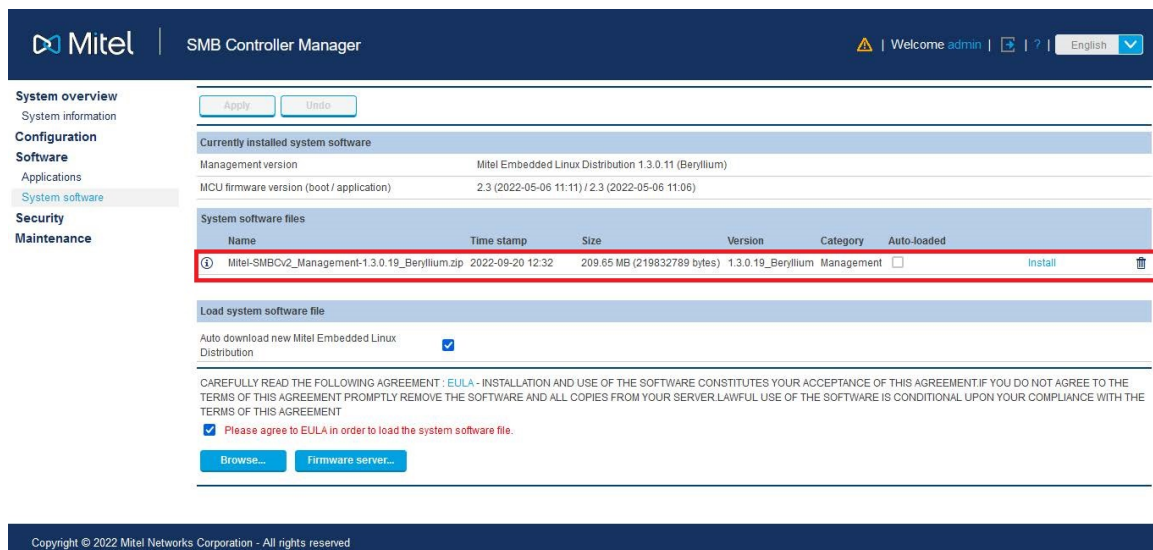
The download begins with a progress bar indicating the download progress.



Name	Time stamp	Size	Version	
Mitel Embedded Linux Distribution 1.3.0.19 (CPM4) (R&D internal use ONLY!)	2022-09-02 18:35	209.65 MB (219832789 bytes)	1.3.0.19	Load
Mitel Embedded Linux Distribution 1.3.0.18 (CPM4) (R&D internal use ONLY!)	2022-08-25 12:00	209.63 MB (219817755 bytes)	1.3.0.18	Load
Mitel Embedded Linux Distribution 1.3.0.17 (CPM4) (R&D internal use ONLY!)	2022-08-09 12:00	224.66 MB (235577703 bytes)	1.3.0.17	Load
Mitel Embedded Linux Distribution 1.3.0.16 (CPM4) (R&D internal use ONLY!)	2022-07-13 12:00	224.66 MB (235577050 bytes)	1.3.0.16	Load
Mitel Embedded Linux Distribution 1.3.0.15 (CPM4) (R&D internal use ONLY!)	2022-07-01 12:00	224.64 MB (235556464 bytes)	1.3.0.15	Load
Mitel Embedded Linux Distribution 1.3.0.14 (CPM4) (R&D internal use ONLY!)	2022-06-10 12:00	224.6 MB (235515241 bytes)	1.3.0.14	Load
Mitel Embedded Linux Distribution 1.3.0.10 (CPM4) (R&D internal use ONLY!)	2022-05-09 12:00	201.56 MB (211350023 bytes)	1.3.0.10	Load
Mitel Embedded Linux Distribution 1.3.0.9 (CPM4) (R&D internal use ONLY!)	2022-05-02 12:00	209.47 MB (219649351 bytes)	1.3.0.9	Load

- For the SMB Controller without internet access:
 - a. Click **Browse...** and select the previously downloaded firmware (for example, "Mitel Embedded Linux Distribution 1.3.0.27 (CPM4)").
 - b. Click **Open**.
 - c. The upload begins with a progress bar indicating the upload process and the name of the file is added to the list of available System Software Files.
3. Click **Install** next to the required SMB Controller manager firmware version.

The installation of the software begins with a progress bar indicating progress of the software installation.



System overview
System information

Configuration
Software
Applications
System software
Security
Maintenance

Apply Undo

Currently installed system software

Management version	Mitel Embedded Linux Distribution 1.3.0.11 (Beryllium)
MCU firmware version (boot / application)	2.3 (2022-05-06 11:11) / 2.3 (2022-05-06 11:06)

System software files

Name	Time stamp	Size	Version	Category	Auto-loaded	
Mitel-SMBCv2_Management-1.3.0.19_Beryllium.zip	2022-09-20 12:32	209.65 MB (219832789 bytes)	1.3.0.19_Beryllium	Management	☐	Install

Load system software file

Auto download new Mitel Embedded Linux Distribution ☒

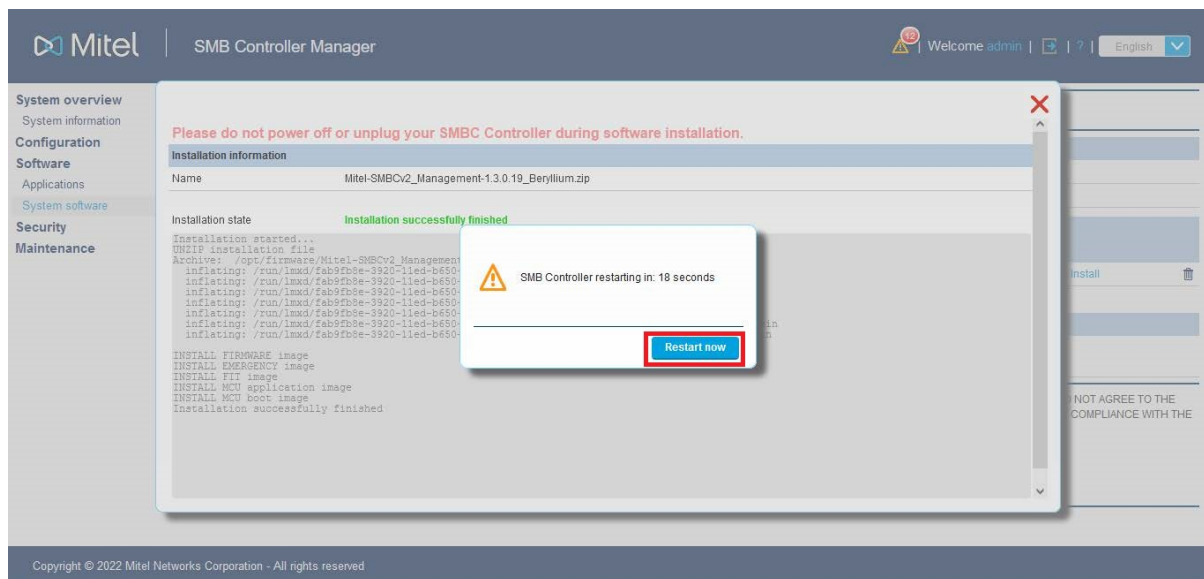
CAREFULLY READ THE FOLLOWING AGREEMENT: [EULA](#) - INSTALLATION AND USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT.

☒ Please agree to EULA in order to load the system software file.

[Browse...](#) [Firmware server...](#)

Copyright © 2022 Mitel Networks Corporation - All rights reserved

4. After a successful Installation, click the **Restart Now** button to restart the SMB Controller.



5. When the startup is completed, the SYS LED is green and flashing.

9.1.8 Install MSL Container

Note:

- Make sure that the SMB Controller software has been Upgraded to the correct version. See [Upgrading the SMB Controller Software](#) on page 91.
- Set up the SMB Controller's [date and time](#) via Controller Manager before installing MSL.

The Mitel-MSL_Container RPM file must now be installed via the SMB Controller Manager. This process assumes that the SMB Controller Manager Firmware and MCU (Boot) firmware are at the latest version. To install the MSL Container:

1. Log in to Controller Manager.

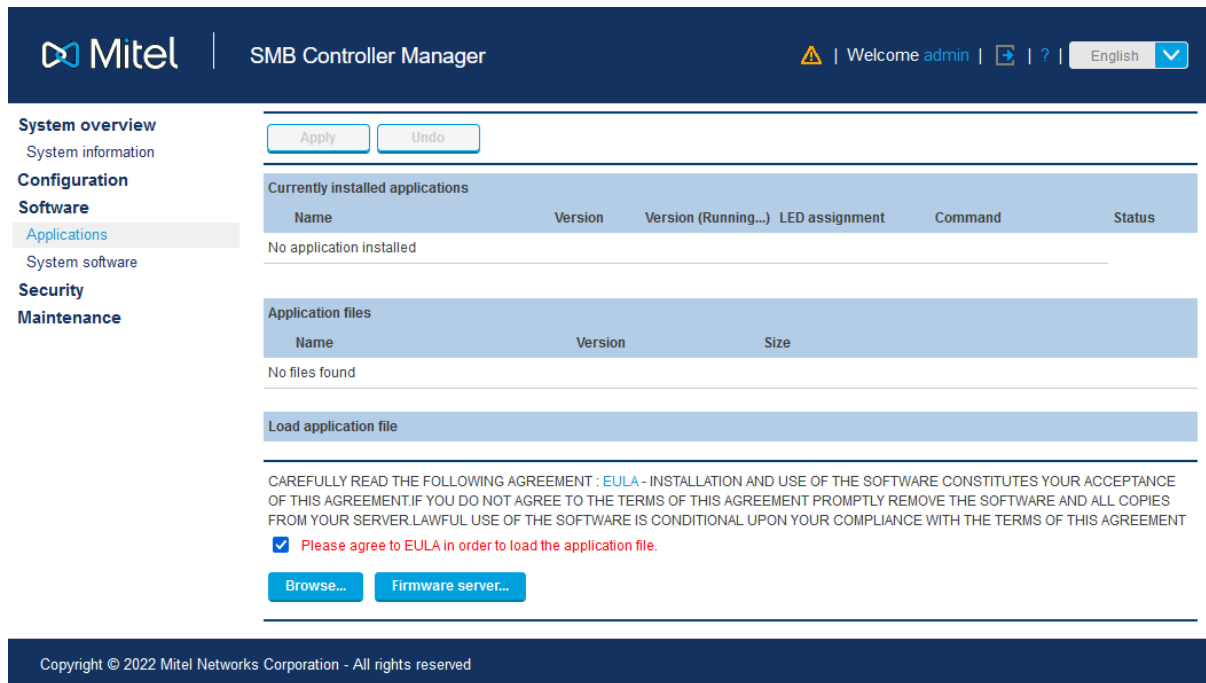


Figure 33: Controller Manager – Applications Installation

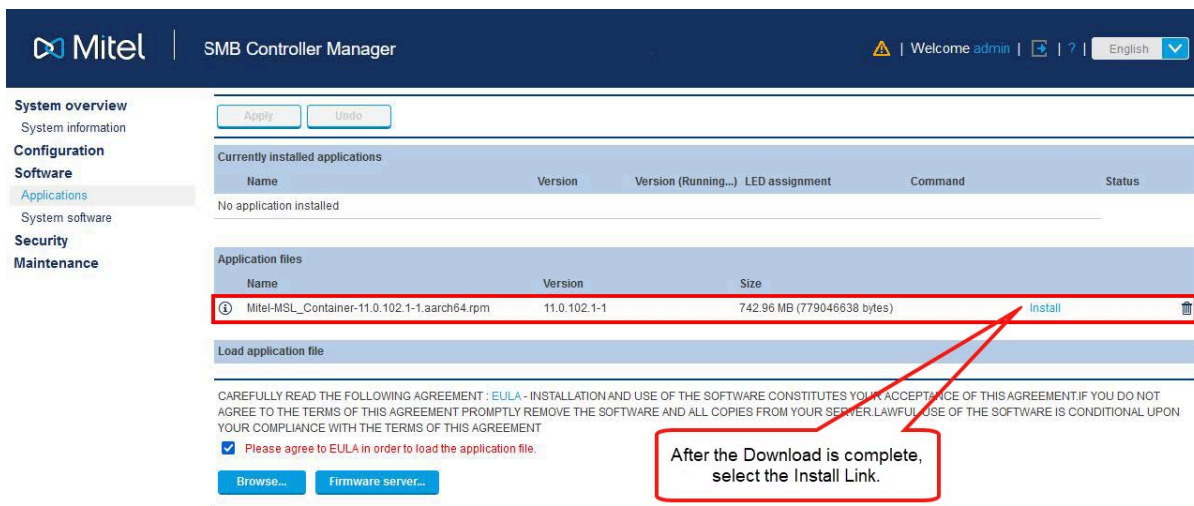
2. Go to the **Software > Applications** panel.
3. Agree to the **EULA** (End User License Agreements)
4. Select the Application to be downloaded:
 - Browse for a local RPM if you have already downloaded it.
 - Via the firmware server to download it directly from the Mitel SWDLC (Software Download center).
5. Load the Mitel-MSL-Container from the Mitel SWDLC.

Name	Time stamp	Size	Version	
Mitel-MSL_Container-11.0.102.1-1	2022-09-21 10:56	742.96 MB (779046638 bytes)	11.0.102.1-1	Load
Mitel-MSL_Container-11.0.100.1-3	2022-09-19 16:34	742.79 MB (778869063 bytes)	11.0.100.1-3	Load
Mitel-MSL_Container-11.0.100.1-2	2022-09-13 18:09	742.79 MB (778868851 bytes)	11.0.100.1-2	Load
Mitel-MSL_Container-11.0.100.1-1	2022-09-07 15:37	742.79 MB (778868737 bytes)	11.0.100.1-1	Load

Select the Load Link for the desired Firmware Load.

6. Once the application is loaded completely, close the loading window.

7. Click the **Install** link, to install the MSL Container.



Mitel | SMB Controller Manager

System overview | System information | Configuration | **Software** | Applications | System software | Security | Maintenance

Currently installed applications

Name	Version	Version (Running...)	LED assignment	Command	Status
No application installed					

Application files

Name	Version	Size	
Mitel-MSL_Container-11.0.102.1-1.aarch64.rpm	11.0.102.1-1	742.96 MB (779046638 bytes)	Install

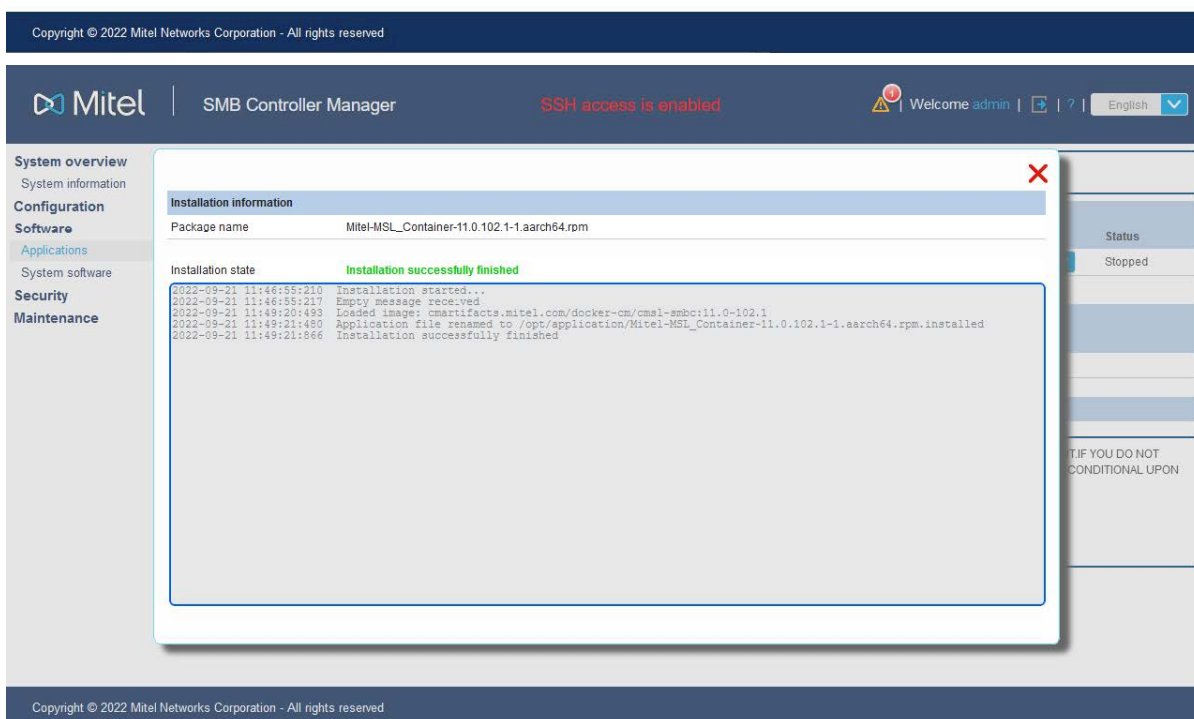
Load application file

CAREFULLY READ THE FOLLOWING AGREEMENT : [EULA](#) - INSTALLATION AND USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT.

☒ Please agree to EULA in order to load the application file.

[Browse...](#) [Firmware server...](#)

After the Download is complete, select the Install Link.



Copyright © 2022 Mitel Networks Corporation - All rights reserved

Mitel | SMB Controller Manager

SSH access is enabled

System overview | System information | Configuration | **Software** | Applications | System software | Security | Maintenance

Installation information

Package name: Mitel-MSL_Container-11.0.102.1-1.aarch64.rpm

Installation state: **Installation successfully finished**

```

2022-09-21 11:46:55:210 Installation started...
2022-09-21 11:46:55:217 Empty message received
2022-09-21 11:49:20:493 Loaded image: cmarifacts.mitel.com/docker-cm/cma1-smbc11.0-102.1
2022-09-21 11:49:21:480 Application file renamed to /opt/application/Mitel-MSL_Container-11.0.102.1-1.aarch64.rpm.installed
2022-09-21 11:49:21:866 Installation successfully finished
    
```

Status: Stopped

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT PROMPTLY REMOVE THE SOFTWARE AND ALL COPIES FROM YOUR SERVER. LAWFUL USE OF THE SOFTWARE IS CONDITIONAL UPON YOUR COMPLIANCE WITH THE TERMS OF THIS AGREEMENT.

Copyright © 2022 Mitel Networks Corporation - All rights reserved

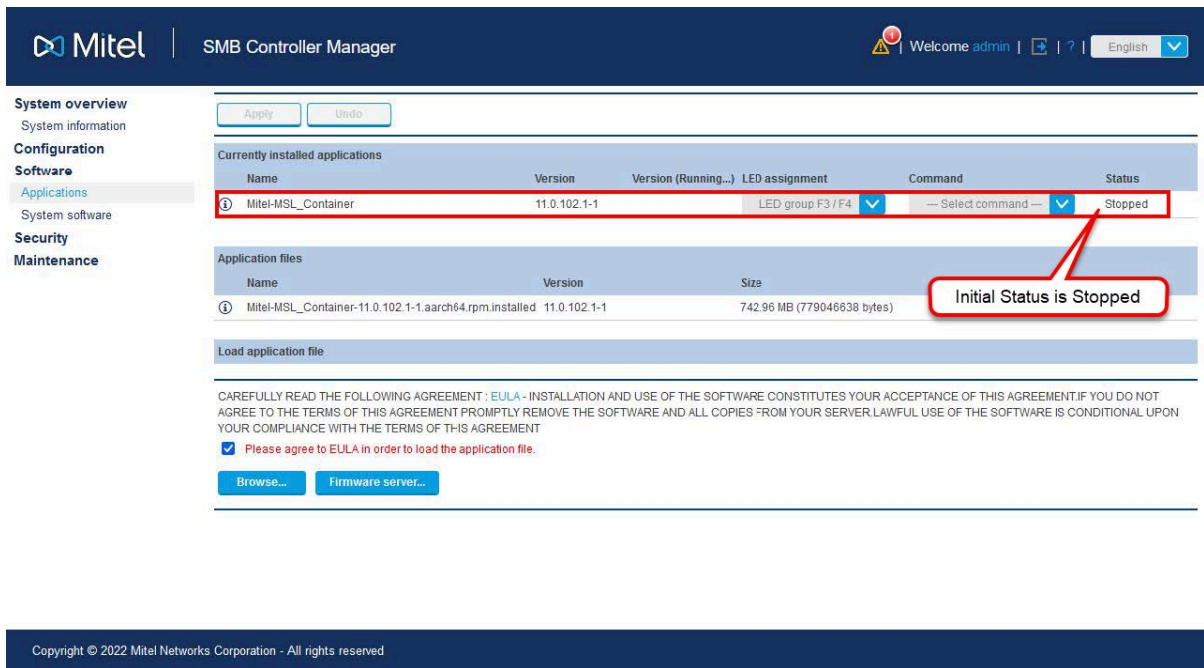


Figure 34: Installing the MSL Container

The MSL Container is initialized with the same Admin Account Password that was configured in the SMB Controller Manager.



Warning:

The MSL admin account is separate from the SMB Controller Manager admin account. Changes to the "admin" password in MSL is not reflected in SMB Controller Manager (and vice versa).

It is the responsibility of the customer to manually maintain the passwords.

After installing the MSL Container, you must manually start the MSL container.

9.1.9 Initial MSL Network Setup

The MSL requires the administrator to program the IP address and password information for the platform. The addresses required will depend on the applications:

- MiVoice Business will require a static LAN IP address.
- (Optional) MiVoice Border Gateway will require a static LAN IP and a static WAN IP address. Additionally, the ETH1 interface should be enabled in Controller Manager (DHCP disabled, and no IP address configured).

These additional IP addresses must be statically assigned and cannot be obtained using DHCP and should not be included in the DHCP server scope.

Note:

If you are using the embedded DHCP Server, make sure that there is no conflict with any existing installed DHCP server.

1. Using the web-browser, browse to: <SMB Controller IP Address>/server-manager. Note that this is the SMB Controller IP address, not the MSL IP address (as the MSL IP address is not yet programmed). This address will be used only once.

Note:

When an application is installed via Controller Manager, the WebUI releases port 80 and 443. Since MSL will be an application, it will take over these ports. This allows the administrator direct access to the Server Manager. Controller Manager is still available on port 8080 and 8443.

2. The MSL Container is initialized with the same admin password configured on the SMB Controller (when the MSL Container starts for the first time). Login with the 'admin' username and the initial admin password. The MSL admin password can be changed from the System Users page under Administration. For MSL password rules, See [Mitel Standard Linux Installation and Administration Guide](#).



Figure 35: MSL Login

CAUTION:

The MSL admin account is separate from the SMB Controller Manager admin account. Changes to the "admin" password in MSL is not reflected in SMB Controller Manager (and vice versa).

Mitel | Mitel Standard Linux admin@mitel-networks-server.mycompany.local Status: Clear

ServiceLink
Blades
Status

Administration
Web services
Backup
Restore
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reboot

Security
Remote access
Syslog
Web Server

Configuration
IP settings
Networks
E-mail settings
Google Apps
Cloud Service Provider
DHCP
SNMP
Review configuration

Miscellaneous
Support and licensing
Help

Warning: Configure IP addresses before proceeding!

Warning: Internal Interface is disabled!

Welcome to the server manager

This server is a very secure, reliable and cost-effective platform for an expanding range of business applications and services. For information about the specific applications available for this platform, please contact your authorized reseller.

To perform a system administration function, click one of the links in the menu on the left of your screen.

Mitel Standard Linux 11.0.104.1
© Mitel Networks Corporation

Figure 36: MSL Landing Page

3. Navigate to the **Remote access** panel under **Security** (Optional).

- (Optional): Add the subnet of your PC to the **Remote Management** section, and then save the remote access settings.

Mitel | Mitel Standard Linux | admin@mitel-networks-server.mycompany.local | Status: Clear

ServiceLink
Blades
Status

Administration
Web services
Backup
Restore
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reboot

Security
Remote access
Syslog
Web Server

Configuration
IP settings
Networks
E-mail settings
Google Apps
Cloud Service Provider
DHCP
SNMP
Review configuration

Miscellaneous
Support and licensing
Help

Warning: Configure IP addresses before proceeding!

Warning: Internal Interface is disabled!

Change remote access settings

Remote Management

It is possible to allow hosts on remote networks to access the server manager or login via secure shell by entering those networks here. Use a subnet mask of 255.255.255.255 to limit the access to the specified host. Any hosts within the specified range will be able to access the server manager using HTTPS. To allow secure shell access from hosts in the specified range you must also configure the Secure Shell Settings accordingly.

There are no entries yet

To add a new remote management network, enter the details below.

Network	192.168.1.0
Subnet mask	255.255.255.0

Secure Shell Settings

You can control Secure Shell access to your server. The public setting should only be enabled by experienced administrators for remote problem diagnosis and resolution. We recommend leaving this parameter set to "No Access" unless you have a specific reason to do otherwise.

Secure shell access	Allow public access (entire Internet) ▼
Allow administrative command line access over secure shell	Yes ▼
Allow secure shell access using standard passwords	Yes ▼

Save

Mitel Standard Linux 11.0.104.5
© Mitel Networks Corporation

Figure 37: Remote Access Settings (Optional)

**Warning:**

It is advised to disable the SSH access as soon as you have verified the Server Manager is accessible from the MSL IP address.

4. Navigate to the **IP Settings** panel under **Configuration**.

5. Enter the IP address information, which will be used to access MSL and MiVoice Business blade. The second IP address is required if the MiVoice Border Gateway is installed.

Mitel | Mitel Standard Linux

admin@mitel-networks-server.mitel.com Status: Clear

ServiceLink
Blades
Status

Administration
Web services
Backup
Restore
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reboot

Security
Remote access
Syslog
Web Server

Configuration
IP settings
Networks
E-mail settings
Google Apps
Cloud Service Provider
DHCP
SNMP
Review configuration

Miscellaneous
Support and licensing
Help

Warning: Configure IP addresses before proceeding!

Warning: Internal Interface is disabled!

IP addresses and hostname settings

This panel allows you to configure server name and IP addresses.
Changes to these settings will require a restart.

The hostname must contain only letters, numbers and hyphens, and must start and end with a letter or number.

Hostname: mitel-networks-server
Domain: mitel.com

The IP address, Netmask and Gateway must be in the form #.#.#.# (each # is a number from 0 to 255).
Make sure the IP addresses are not in use by any other devices and the netmasks match your existing networks.

Internal Network Interface (LAN)

Link status	down
Physical interface	eth0
Virtual interface	
MAC address	
IP address	172.19.51.215
Second IP address (Optional)	
Netmask	255.255.255.224
Gateway (Router)	172.19.51.193

Enter the LAN IP Address

Optionally enter the MBG LAN IP Address

Enter the LAN Subnet Mask IP Address

Enter the LAN Default Gateway IP Address

Reset Networks Next

Mitel Standard Linux 11.0.105.2
© Mitel Networks Corporation

Figure 38: Entering the LAN Information

6. Select **Next** to configure the Trusted Networks.
7. Configure the Trusted Networks to ensure connectivity from your PC. Additional trusted networks can be added later via the Networks panel.

Warning:

To access the Server Manager from any PC outside your local network, you must add a trusted network. Otherwise, the Server Manager will only be accessible from a browser within the local network. If a browser within the local network is not available, add a trusted network before proceeding.

Failure to do so, may result the connectivity issues from your PC.

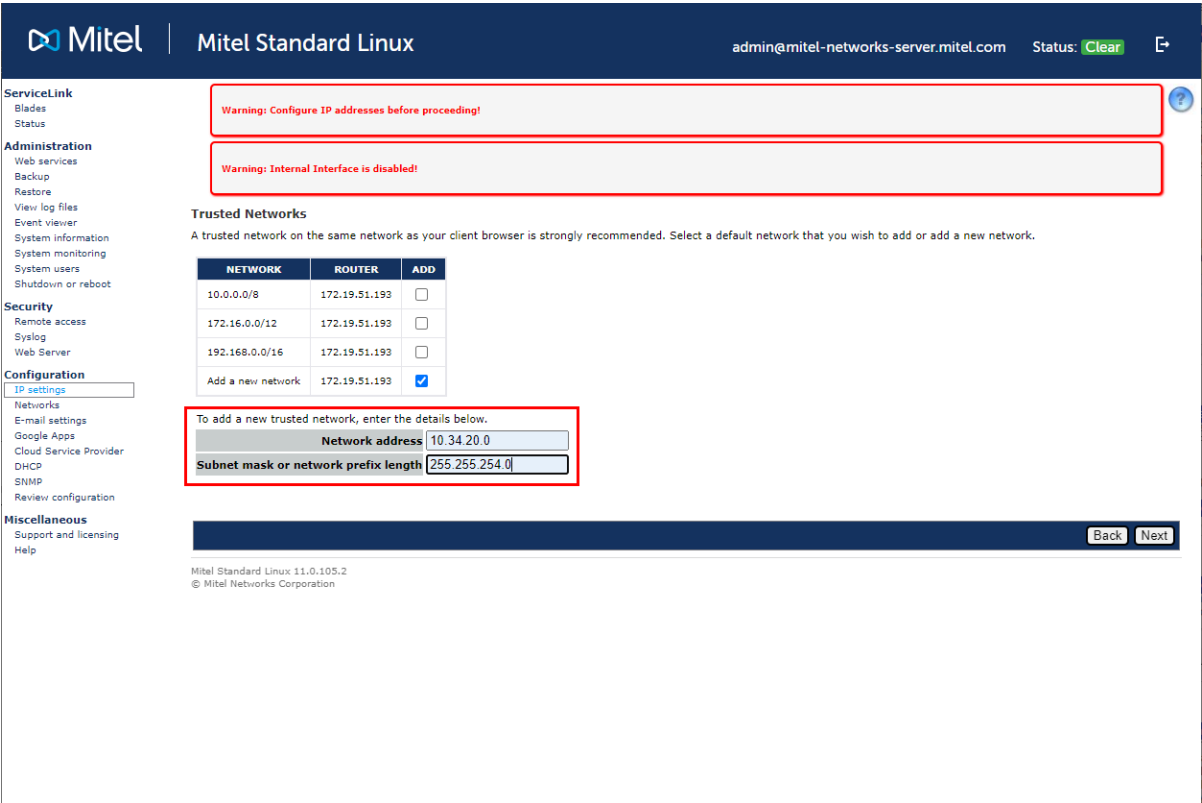


Figure 39: Adding a Trusted Network

8. Select **Next** to program the WAN interface.

9. Enable the WAN and enter the IP addresses, Netmask, and Gateway(router) (if using MiVoice Border Gateway) and then select **Next** to review the changes.

Mitel | Mitel Standard Linux

admin@mitel-networks-server.mitel.com Status: Clear

ServiceLink

- Blades
- Status

Administration

- Web services
- Backup
- Restore
- View log files
- Event viewer
- System information
- System monitoring
- System users
- Shutdown or reboot

Security

- Remote access
- Syslog
- Web Server

Configuration

- IP settings**
- Networks
- E-mail settings
- Google Apps
- Cloud Service Provider
- DHCP
- SNMP
- Review configuration

Miscellaneous

- Support and licensing
- Help

Warning: Configure IP addresses before proceeding!

Warning: Internal Interface is disabled!

External Network Interface (WAN)

External Network Interface (WAN) is required if deploying in server gateway such as deployments with MBG. Configure this interface only if needed.

Enabled	☐
Link status	down
Physical interface	eth1
Virtual interface	
MAC address	
IP address	
Netmask	255.255.255.0
Gateway (Router)	

Required if using the MBG

Back Next

Mitel Standard Linux 11.0.105.2
© Mitel Networks Corporation

Figure 40: Entering the WAN Information

Note:

If you are enabling the external Network Interface, ensure the following:

- The Eth1 Port is enabled in the SMB Controller Manager's IP Network Panel.
- The Eth1 Port has DHCP deselected in the SMB Controller Manager's IP Network Panel

10. Review the IP Addresses and Trusted Networks and then select **Save and Restart**.

The screenshot shows the Mitel Standard Linux configuration web interface. The top header includes the Mitel logo, 'Mitel Standard Linux', the user 'admin@mitel-networks-server.mitel.com', and a 'Status: Clear' button. A left sidebar lists various system management categories like ServiceLink, Administration, Security, Configuration, and Miscellaneous. The main content area is titled 'IP addresses and hostname settings' and includes a 'Review Settings' section. At the top of this section, two red-bordered warning boxes are displayed: 'Warning: Configure IP addresses before proceeding!' and 'Warning: Internal Interface is disabled!'. Below these, the 'Hostname' is set to 'mitel-networks-server'. The 'Internal Network Interface (LAN)' section shows the 'IP address' as 172.19.51.215, the 'Second IP address (Optional)' as 255.255.255.224, the 'Netmask' as 255.255.255.224, and the 'Gateway (Router)' as 172.19.51.193. The 'Trusted Networks' section has buttons for 'Active trusted networks' and 'New trusted network'. The 'External Network Interface (WAN)' section shows 'Enabled' as 'no', 'IP address' as 255.255.255.0, 'Netmask' as 255.255.255.0, and 'Gateway (Router)' as 255.255.255.0. A message at the bottom states 'The system will restart after saving the changes. Do you want to continue?'. At the very bottom, there are 'Back' and 'Save and Restart' buttons, and a footer with 'Mitel Standard Linux 11.0.105.2' and '© Mitel Networks Corporation'.

Figure 41: Summary Page

11. Wait for some time to save the new configuration and once you configuration is saved successfully, you will be prompted with the following screen.

Click **Next**.

12. Log in to the Server Manager using the MSL IP address <https://<MSL IP Address>/server-manager/>. Use the same credentials as those used to log into the SMB Controller Manager.

13. Disable the SSH access (**recommended**).

**Warning:**

It is advised to disable the SSH access as soon as you have verified the Server Manager is accessible from the MSL IP address.

- Log in to Server Manager, at <https://<MSL IP Address>/server-manager/>.
- Navigate to the **Remote Access** panel under **Security**.
- Remove the configured subnet of your PC, disable the secure shell access, and then click **Save**.

Mitel | MiVoice Business admin@smbc17-ve-in.lab.mitel.com Status: **Clear**

ServiceLink
Blades
Status

Administration
Web services
Backup
Restore
View log files
Event viewer
System information
System monitoring
System users
Shutdown or reboot

Security
Remote access
Syslog
Web Server

Configuration
IP settings
Networks
E-mail settings
Google Apps
Cloud Service Provider
DHCP
SNMP
Review configuration

Miscellaneous
Support and licensing
Help

Change remote access settings

Remote Management

It is possible to allow hosts on remote networks to access the server manager or login via secure shell by entering those networks here. Use a subnet mask of 255.255.255.255 to limit the access to the specified host. Any hosts within the specified range will be able to access the server manager using HTTPS. To allow secure shell access from hosts in the specified range you must also configure the Secure Shell Settings accordingly.

Network	Subnet mask	Number of hosts	Remove
192.168.1.0	255.255.255.0	16777216	☒

To add a new remote management network, enter the details below.

Network
Subnet mask

Secure Shell Settings

You can control Secure Shell access to your server. The public setting should only be enabled by experienced administrators for remote problem diagnosis and resolution. We recommend leaving this parameter set to "No Access" unless you have a specific reason to do otherwise.

Secure shell access

Allow administrative command line access over secure shell

Allow secure shell access using standard passwords

Save

MiVoice Business 10.0.104.5
© Mitel Networks Corporation

Figure 42: Remote Access Settings

9.1.10 Licensing the Solution

To license the solution:

Note:

- An online connection is necessary for licensing changes and software upgrades.
 - Offline activation of the ServiceLink with AMC is not supported on the SMB Controller. This limitation applies specifically to the SMB Controller and not to the SVI.
 - There is a difference between the 54005968 and 54011858 part numbers in their online/offline capabilities. Specifically, the 54005968 part number allows for both online and offline activation, while the 54011858 part number requires an online connection.
 - The server must be properly configured and licensed to the Blades Panel to display the available software blades that can be installed.
 - The MiVoice Business software may not appear on the Blades panel unless the system is back online.
-
- An online connection is necessary for licensing changes and software upgrades.
 - Offline activation of the ServiceLink with AMC is not supported on the SMB Controller. This limitation applies specifically to the SMB Controller and not to the SVI.
 - There is a difference between the 54005968 (MiVoice Business Enterprise S/W for 3300 (No Users)) and 54011858 (MiVoice Business on SMB Controller bundle) part numbers in their online/offline capabilities. Specifically, the 54005968 part number allows for both online and offline activation, while the 54011858 part number requires an online connection.
 - The server must be properly configured and licensed to the Blades Panel to display the available software blades that can be installed.
 - The MiVoice Business software may not appear on the Blades panel unless the system is back online.

1. Log in to Server Manager, at <https://<MSL IP Address>/server-manager/>.
2. Select **Status** under **ServiceLink**.
3. Enter the **Service Account ID** (ARID) from the AMC.

4. Select **Activate**.

ServiceLink Activation

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

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

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

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

Service account ID: 77987275

Address of Mitel License Server or proxy (optional): default is AMC

TCP port to use for the License Server connection (optional):

Enable offline license generation: ☐

Activate

Mitel Standard Linux 11.0.102.1
© Mitel Networks Corporation

On successful activation of the solution, the following screen will be displayed.

If the activation is unsuccessful, see the Licensing section of the [MiVoice Business Troubleshooting Guide](#) for troubleshooting.

ServiceLink Status Information

✓ **Operation status report**
Congratulations, your server has now been activated for ServiceLink.

This web panel provides updated ServiceLink status information for this server. Status information is downloaded from the Mitel License Server to this server as part of the synchronization protocol.

The display includes information about your ServiceLink account, the latest synchronization event status, and a list of services available from ServiceLink for which this server is subscribed. The display also includes the expiration date for each service and, if applicable, any error notice for that service. Click on the notice for more detailed information.

If you wish to deactivate your ServiceLink account, please click [here](#).

Your service account ID is: 77987275
Your descriptive server name is: SMBC_Pat2022
The last sync completed successfully at: Wed Sep 21 15:38:58 2022

Current ServiceLink subscription listing

Service	Status	Expires	Messages
Server activation and synchronization	Subscribed	No expiry	None
3300 ICP / MCD	Subscribed	No expiry	None

Sync

Mitel Standard Linux 11.0.102.1
© Mitel Networks Corporation

9.1.10.1 AMC Licensing

MiVoice Business on the SMB Controller relies on MSL's support of a single ARID from the AMC used for both MiVoice Business and MiVoice Border Gateway; a single ARID with multiple Sub-License Keys assigned to the MiVoice Business and MiVoice Border Gateway products.

The MSL Container will use the SMB Controller EID in place of the hardware ID.

To purchase the appropriate licenses for the SMB Controller:

1. Create an ARID.

- a. For Capex purchases, order the 54011858 MiVoice Business on SMB Controller bundle, which will include the base kits.

The contents of this bundle are listed below.

Part No.	Description	Quantity
54005748	MiVoice Business	1
54005339	MiVoice Border Gateway (includes CloudLink Gateway)	1
54004491	MiVoice Border Gateway SIP Proxy	30
54005400	MiVoice Business SIP Trunks	30
54004575	MiVoice Border Gateway Teleworker Service Users	50
54004577	MiVoice Border Gateway Teleworker Service Users	100
54003184	MiVoice Border Gateway SRC Licenses	30
54004582	MiVoice Border Gateway Compression	30
54000297	MiVoice Business Embedded Voice Mailboxes	20

Part No.	Description	Quantity
54005064	MiVoice Business - IDS Connection	1

Alternatively, the following MiVoice Business base packs could be used when on board MiVoice Border Gateway functionality is not required.

- 54005968 MiVoice Business Enterprise S/W for 3300 (No Users)
 - 54004973 MiVoice Business Enterprise S/W for 3300
 - 54005777 MiVoice Business Enterprise Hospitality S/W for 3300
2. For subscription licensing there is a flag in CPQ to indicate that the SMB Controller is being used, in which case CPQ will allocate 52003861 Subscript Base - MiVoice Business Solution SMB Controller or 52003862 Subscript Base - MiVoice Business Hospitality SMB Controller. This part is similar to the other base packs used with subscription licensing in that it is free of charge but it includes a combined MiVoice Business/MiVoice Border Gateway base kit and includes other entitlements for Teleworkers, compression licenses, SRC channels, and SIP trunks.
 3. Add items from the Purchase Order to the ARID.
 4. Optionally, add the ARID to a DLM
 - a. AMC will migrate only the MiVoice Business licenses from this ARID to the DLM. It will not touch any non-MiVoice Business licenses.
 5. Optionally, add the ARID to a ULM.
 - AMC will apply only to the UCC licenses that make sense to the ARID. This means only the MiVoice Business and Mitel Border Gateway licenses from the UCC license.

9.1.10.2 SMB Controller Licensing

Software	Licensed	Comments
MSL	No	The MSL is not licensed at this time.
MiVoice Business	Yes	All existing MiVoice Business parts will be supported on the SMB Controller.
Mitel Border Gateway	Yes	All existing Mitel Border Gateway parts will be supported on the SMB Controller.
CloudLink Gateway	No	The CloudLink Gateway is not licensed at this time.

Software	Licensed	Comments
Mitel Performance Analytics Probe	No	The Mitel Performance Analytics Probe is not licensed at this time.

9.1.10.3 MiVoice Business Licensing

The ARID used by the SMB Controller must contain an MiVoice Business base product in order to install the MiVoice Business.

The embedded MiVoice Business will not require virtualization as it accepts both virtualized and non-virtualized base packs.

The Embedded FXS and Expansion FXS/FXO cards are not licensed, and their ports will not consume any licenses.

9.1.10.4 Mitel Border Gateway Licensing

The ARID used by the SMB Controller must contain a Mitel Border Gateway base product to install the Mitel Border Gateway.

The embedded Mitel Border Gateway will not require virtualization as it accepts both virtualized and non-virtualized base packs.

Note:

CloudLink Gateway and Mitel Performance Analytics Probe do not require licenses.

The SMB Controller ARID required the MiVoice Border Gateway base package for the CloudLink Gateway blade to be visible on MSL.

9.1.10.5 UCC Licensing

The UCC Licensing Model provided by AMC revolve around an existing MiCollab solution. However, CloudLink Gateway Deployments and MiCollab Deployments may not be compatible, and as a result the UCC Licensing Model used with MiCollab may not be applicable when using CloudLink.

9.1.10.6 Subscription Licensing

The AMC supports OPEX/Subscription licensing for the MiVoice Business on the SMB Controller instance and other Applications, including regular license synchronization. CAPEX Licensing is also available.

Scenario	MiVoice Business Results	Mitel Border Gateway Results
Synchronization with AMC after subscription ends	MiVoice Business and Mitel Border Gateway will go into license violation. For "0" allocated licenses, MiVoice Business will go to a WARNING license violation, and escalate from there. For an invalid license key, MiVoice Business will go to a CRITICAL license violation	See MiVoice Border Gateway Engineering Guidelines for more details.
MSL cannot synchronize with AMC	The MiVoice Business will go to a CRITICAL license violation.	See Licensing the Solution on page 104 or MiVoice Border Gateway Engineering Guidelines for more details.

9.1.11 Server Manager Requirements for Software Download-Blades

Ensure that the firewall is configured to allow:

Note:

Use DNS lookup to verify the IP address for **blades.mitel-amc.com**, **swdlgw.mitel.com**, and **swdl.mitel.com** before configuring the firewall rules.

1. SSH connections on port 22 to **blades.mitel-amc.com** to verify licenses associated with the ARID.
2. HTTPS connections on port 443 to **swdlgw.mitel.com** to download access tokens from the Software Download Center.
3. HTTPS connections on port 443 to **swdl.mitel.com** to download the software from Content Delivery Network (CDN). As static IP addresses cannot be guaranteed by CDN, firewall rules must be configured to allow FQDN.

9.1.12 Install MiVoice Business Blade

Pre-requirements

- Installation of the [MSL Container](#).

- The solution must be licensed prior to installing any blades.

Installation Steps

1. Log in to the **Server Manager**.
2. Select the **Blades** Panel.
3. Click on the **Update list** button.
4. Find the **MiVoice Business Blade** row and select **Install**.



Mitel Standard Linux

admin@mitel-networks-server.mycompany.local Status: Clear

ServiceLink

Blades

Status

Administration

Web services

Backup

Restore

View log files

Event viewer

System information

System monitoring

System users

Shutdown or reboot

Security

Remote access

Syslog

Web Server

Configuration

IP settings

Networks

E-mail settings

Google Apps

Cloud Service Provider

DNCP

SNMP

Review configuration

Miscellaneous

Support and licensing

Help

Current list of blades

Update list

Software download center: staging.swdlgw.mitel.com

Last updated: Mon 26 Sep 2022 11:08:23 AM MST

Blade	Description	Status	Installation	Documentation
Initial Config Wizard for SHBC	DESIGN BUILD including M1VB-27195, M1VB-27193 and M1VB-32731		Install Cache (v5.1.0.30)	
			Install Cache (v5.1.0.32)	
MailWatch Probe Blade	The MPA mailprobe service is used with the MPA monitoring platform. It requires additional system resources on the host Virtual Machine. Ensure that adequate vCPU and memory are available before using this service. Refer to Mitel Virtual Appliance Deployment Guidelines and product Engineering and Solution Guidelines for details.		Install Cache (v6.5.7.2)	
			Install Cache (v6.5.8.26)	
			Install Cache (v6.5.8.28)	
			Install Cache (v6.5.9.32)	
			Install Cache (v6.6.4.115)	
			Install Cache (v10.0.0.24)	
			Install Cache (v10.0.0.25)	
			Install Cache (v10.0.0.26)	
			Install Cache (v10.0.0.27)	
			Install Cache (v10.0.0.28)	
			Install Cache (v10.0.0.28.3)	
			Install Cache (v10.0.0.29)	
			Install Cache (v10.0.0.30)	
			Install Cache (v10.0.0.31)	
			Install Cache (v10.0.0.32)	
			Install Cache (v10.0.0.33)	
			Install Cache (v10.0.0.34)	
			Install Cache (v10.0.0.35)	
			Install Cache (v10.0.0.36)	
			Install Cache (v10.0.0.37)	
			Install Cache (v10.0.0.38)	
			Install Cache (v10.0.0.39)	
			Install Cache (v10.0.0.40)	
			Install Cache (v10.0.0.41)	
			Install Cache (v10.0.0.42)	
			Install Cache (v10.0.0.43)	
			Install Cache (v10.0.0.44)	
			Install Cache (v10.0.0.45)	
			Install Cache (v10.0.0.46)	
			Install Cache (v10.0.0.47)	
			Install Cache (v10.0.0.48)	
			Install Cache (v10.0.0.49)	
			Install Cache (v10.0.0.50)	
			Install Cache (v10.0.0.50.1)	
ServiceLink	ServiceLink for MSL Container	Installed	Installed (v11.0.102.1)	

Mitel Standard Linux 11.0.102.1

© Mitel Networks Corporation

- 5.** Once the blade is installed, login to ESM using *https://<MSL IP Address>*.

6. Navigate to the **License and Option Selection** and verify the licenses and the dimensions.

License and Option Selection

Online Licensing with the Application Management Center

Application Record ID : 75682069

Licensed Options	Locally Consumed	Locally Allocated	Available for Allocation	Purchased	Local Limits	
					Licenses Allowed	Can be Over Allocated
Users						
IP Users	30	700	50	750	Unrestricted	Yes
External Hot Desk Users	0	750	0	750	Unrestricted	Yes
ACD Active Agents	0	16	0	16	Unrestricted	Yes
HTML Applications	0	750	0	750	Unrestricted	Yes
Single Line Users	3	40	10	50	Unrestricted	Yes
MiVoice Business Console Active Operators	0	0	20	0	Unrestricted	No
Multi-device Users	5	200	0	200	Unrestricted	Yes
Multi-device Suites	0	0	20	0	Unrestricted	Yes
Messaging						
Embedded Voice Mail	2	750	0	750	Unrestricted	Yes
Embedded Voice Mail PMS	1	Yes	0	1	Unrestricted	Yes

Figure 43: License and Option Selection Form

7. Either reboot the MiVoice Business to activate licenses, or perform a data restore (if you have a database you would like to restore from a prior deployment – for example, CX II migration).

Note:

If the MSL Container hasn't been configured with an address, the MiVoice Business Blade will not start. An error log will be generated and captured in syslog.

9.1.13 Install MiVoice Border Gateway Blade

To install the MiVoice Border Gateway Blade:

Pre-requirements

- License the solution prior to installing any blades.
- Installation of the [MSL Container](#).

1. Log in to the SMB Controller Manager.

- From the **Configuration** menu, select **IP network** and then enable the **eth1** port without enabling the **DHCP** in the **Network Interfaces** panel.

The screenshot shows the Mitel SMB Controller Manager web interface. The top navigation bar includes the Mitel logo, the title 'SMB Controller Manager', a status message 'SSH access is enabled', and a user welcome message 'Welcome admin'. The left sidebar contains a menu with 'System overview' (System information), 'Configuration' (User, IP network, Date and Time), 'Software', 'Security', and 'Maintenance'. The main content area is titled 'Network settings' and includes an 'Apply' button and an 'Undo' button. Below this, there are fields for 'Host name' (SMBcv2), 'Domain', 'Primary DNS' (8.8.8.8), and 'Secondary DNS' (4.4.4.4). The 'Network interfaces' section is a table with columns: Name, Status, Carrier, DHCP, IP address, Subnet mask, Gateway, MTU, and MAC address. The table lists three interfaces: eth0, eth1, and eth2. eth0 is the default interface with IP 192.168.1.108. eth1 is selected with a blue checkmark and has IP 0.0.0.0. eth2 is not selected and has IP 0.0.0.0. Below the table, there are expandable sections for 'Subnets' and 'Static routes for eth0'.

Name	Status	Carrier	DHCP	IP address	Subnet mask	Gateway	MTU	MAC address
eth0	☒	(100/full)	☐	192.168.1.108	255.255.255.0	192.168.1.1	1500	08:00:0f:f0:6a:8a Default
eth1	☒		☐			0.0.0.0	1500	08:00:0f:f0:6a:8b
eth2	☐		☒				1500	08:00:0f:f0:6a:8c

Copyright © 2022 Mitel Networks Corporation - All rights reserved

- Log in to Server Manager.
- Go to the Blades Panel.

5. Click on the **Update list** button.

Mitel | MiVoice Business | admin@mitel-networks-server.mycompany.local | Status: Clear +

ServiceLink
[Blades](#)
[Status](#)

Administration
[Web services](#)
[Backup](#)
[Restore](#)
[View log files](#)
[Event viewer](#)
[System information](#)
[System monitoring](#)
[System users](#)
[Shutdown or reboot](#)

Security
[Remote access](#)
[Syslog](#)
[Web Server](#)

Configuration
[IP settings](#)
[Networks](#)
[E-mail settings](#)
[Google Apps](#)
[Cloud Service Provider](#)
[DHCP](#)
[SNMP](#)
[Review configuration](#)

Miscellaneous
[Support and licensing](#)
[Help](#)

Current list of blades
[Update list](#)

Software download center: staging.swdlgw.mitel.com
 Last updated: Mon 24 Oct 2022 09:17:30 AM MST

Blade	Description	Status	Installation	Documentation
Mitel CloudLink Gateway	Mitel CloudLink Gateway		Install Cache (V1.2.19)	View
Initial Config Wizard for SMBC	DESIGN BUILD including MIVB-27195, MIVB-27193, MIVB-32731 and MIVB-32957		Install Cache (V5.1.0.32) Install Cache (V5.1.0.34)	
MarWatch Probe Blade	The MPA marprobe service is used with the MPA monitoring platform. It requires additional system resources on the host Virtual Machine. Ensure that adequate vCPU and memory are available before using this service. Refer to Mitel Virtual Appliance Deployment Guidelines and product Engineering and Solution Guidelines for details.		Install Cache (V6.5.7.2) Install Cache (V6.5.8.28) Install Cache (V6.5.9.32) Install Cache (V6.6.4.115)	
Blade-MiVoiceBusinessSMBC	MiVoice Business software for installation on the SMBC ARM platform.	installed	Remove (V10.0.0.55)	View
Blade-MiVoice_Border_Gateway	A secure gateway for VoIP traffic and associated Mitel applications		Install Cache (V11.0.0.224)	
			Install Cache (V11.0.0.243)	
			Install Cache (V11.0.0.250)	
			Install Cache (V11.0.0.302)	
			Install Cache (V11.0.0.304)	
			Install Cache (V11.0.0.305)	
			Install Cache (V11.0.0.308)	
			Install Cache (V11.0.0.309)	
			Install Cache (V11.0.0.311)	
			Install Cache (V11.0.0.313)	
			Install Cache (V11.5.0.49)	
			Install Cache (V11.5.0.53)	
ServiceLink	ServiceLink for MSL Container.	installed	installed (V11.0.103.1)	

MiVoice Business 10.0.0.55
 © Mitel Networks Corporation

Figure 44: MiVoice Border Gateway Blade

6. Find the MiVoice Border Gateway Blade and select install.

After the installation is complete, the **Applications** panel is displayed, and the **MiVoice Border Gateway** is listed as an application.

Installation of Blade-MiVoice_Border_Gateway V11.5.0.68 blade

Progress Overview

- Fetch package information: 100%
- Download packages: 100%
- Check for package conflicts: 100%
- Check for unresolved dependencies: 100%
- Install packages: 100%

The Blade-MiVoice_Border_Gateway V11.5.0.68 blade was successfully installed.
The blade reported:
You should now visit the application panel to configure the application.
[Clear this report](#)

Progress Details

Fetch package information	Completed successfully		
Download packages	Completed successfully		
	Blade-MiVoice_Border_Gateway-11.5.0.68-01.aarch64.rpm	2100612/2100612 bytes downloaded	100% complete
	boost-regex-1.53.0-28.el7.aarch64.rpm	273844/273844 bytes downloaded	100% complete
	libzip-0.10.1-8.el7.aarch64.rpm	48148/48148 bytes downloaded	100% complete
	mitel-hermod-2.2.16-01el7.aarch64.rpm	4219200/4219200 bytes downloaded	100% complete
	mitel-msl-ca-1.26.2-01.noarch.rpm	22480/22480 bytes downloaded	100% complete
	mitel-msl-cakeys-1.27.3-01el7.aarch64.rpm	23252/23252 bytes downloaded	100% complete
	mitel-msl-certgmt-1.26.2-01.noarch.rpm	44600/44600 bytes downloaded	100% complete

Applications
MiVoice Border Gateway

Current list of blades
[Update list](#)

Software download center: staging.swdlgw.mitel.com
Last updated: Wed 16 Nov 2022 10:46:41 AM MST

Blade	Description	Status	Installation	Documentation
Mitel CloudLink Gateway	Mitel CloudLink Gateway		Install Cache (V1.2.23)	View
			Install Cache (V1.2.24)	View
Initial Config Wizard for SMBC	Initial Config Wizard for SMBC		Install Cache (V5.1.0.32)	
			Install Cache (V5.1.0.34)	
			Install Cache (V10.0.0.1)	
			Install Cache (V10.0.0.2)	
MarWatch Probe Blade	The MPA marprobe service is used with the MPA monitoring platform. It requires additional system resources on the host Virtual Machine. Ensure that adequate vCPU and memory are available before using this service. Refer to Mitel Virtual Appliance Deployment Guidelines and product Engineering and Solution Guidelines for details.		Install Cache (V6.5.7.2)	
			Install Cache (V6.5.8.28)	
			Install Cache (V6.5.9.32)	
			Install Cache (V6.6.4.115)	
MiVoiceBusiness for SMBC	MiVoice Business software for installation in the SMBC ARM platform.	installed	Remove (V10.0.0.61) Upgrade Cache (V10.0.0.62)	View
Blade-MiVoice_Border_Gateway	A secure gateway for VoIP traffic and associated Mitel applications	installed	Remove (V11.5.0.68)	
ServiceLink	ServiceLink for MSL Container	installed	installed (V11.0.103.3) Upgrade Cache (V11.0.104.1)	

MiVoice Business 10.0.0.61
MiVoice Border Gateway 11.5.0.68
© Mitel Networks Corporation

Note:

If the MSL Container is configured with an invalid IP address settings, the MiVoice Border Gateway blade will not start. An error log will be generated and captured in the syslog.

9.1.14 Install CloudLink Gateway Blade

The CloudLink Gateway (CLGW) Blade provides integration with CloudLink-based (for example, CloudLink API program or Mitel Assistant).

Pre-requirements

The MBG Blade has been installed.

1. Log in to Server Manager.
2. Go to the Blades Panel.
3. Click on the **Update list** button.
4. Find the CloudLink Gateway Blade and select **install**.

After the installation is complete, the **Applications** panel is displayed and the **CloudLink Gateway** is listed as an application.

The screenshot shows the Mitel MiVoice Business Server Manager interface. The top navigation bar includes the Mitel logo, 'MiVoice Business', the user 'admin@mitel-networks-server.mycompany.local', and a 'Status: Clear' indicator. The left sidebar contains a menu with categories: Applications, ServiceLink, Administration, Security, Configuration, and Miscellaneous. The 'Applications' section is expanded, showing 'MiVoice Border Gateway' and 'CloudLink Gateway'. The 'CloudLink Gateway' application is selected, displaying its details. The main content area shows the 'CloudLink Gateway' title, a button to access the 'CloudLink portal', and two tables: 'Status' and 'Containers'. The 'Status' table has columns for Stage, Version, Supported Call Manager, and AccountID. The 'Containers' table has columns for Container and Version. A 'Restart' button is located at the bottom right of the application details section.

Stage	Version	Supported Call Manager	AccountID
production	1.2.24	MiVoice Business	

Container	Version
CloudLink	1.3.0.01-2554
Tunnel	2022.10.17-162

MiVoice Business 10.0.0.62
MiVoice Border Gateway 11.5.0.67
© Mitel Networks Corporation

9.1.15 Install Mitel Performance Analytics Probe Blade

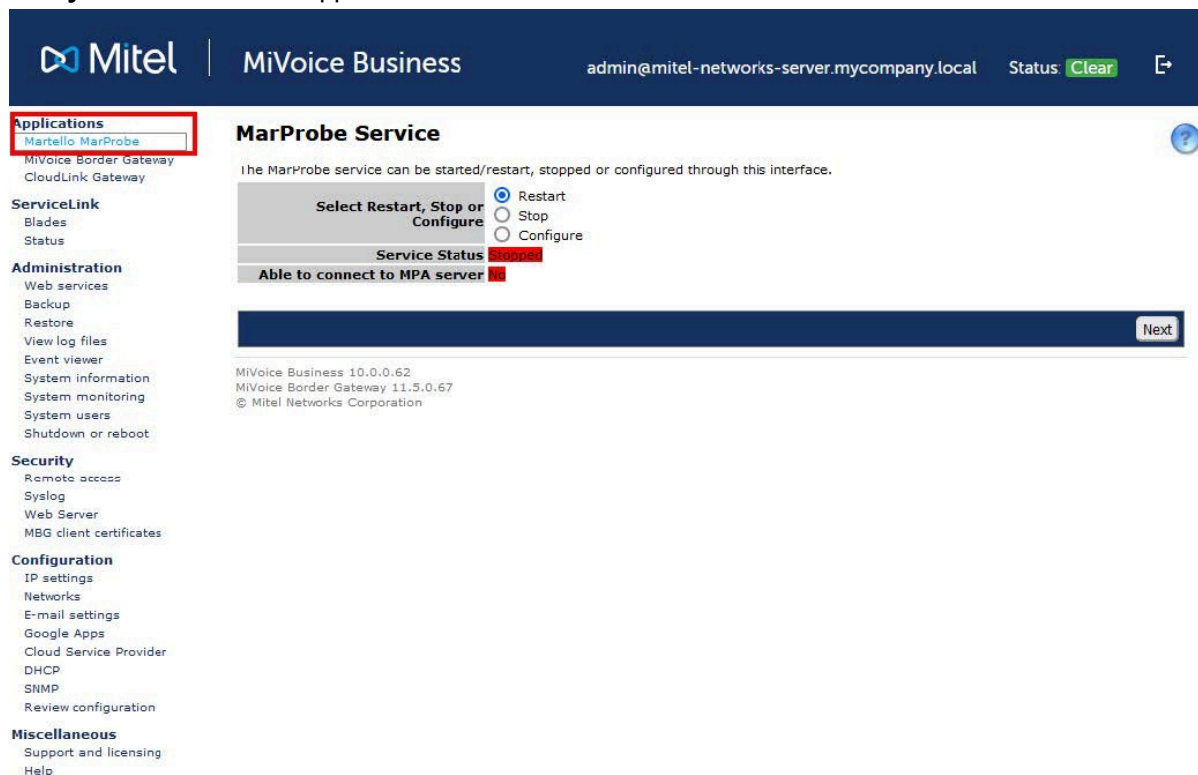
To install the Mitel Performance Analytics Probe Blade:

Pre-requirements

- Installation of the [MSL Container](#).
- The MiVoice Business Blade has been installed.

1. Log in to Server Manager.
2. Go to the Blades Panel.
3. Click on the **Update list** button.
4. Installing Find the Mitel Performance Analytics Probe Blade and select install.

After the installation is complete, the **Applications** panel is displayed, and the **Mitel Performance Analytics** is listed as an application.



9.1.16 Install Initial Configuration Wizard (ICW) Blade

To install the Initial Configuration Wizard Blade:

1. Log into Server Manager.
2. Select **Blades**.
3. Select **Install** next to the Initial Configuration Wizard Blade and follow the steps.

Note:

It is not necessary to install this blade after the MiVoice Business or MiVoice Border Gateway blades, however Initial Configuration Wizard has nothing to provision without the MiVoice Business blade. A MiVoice Business blade must be present in order for the Initial Configuration Wizard to launch.

9.2 Configure the Applications

The section in this chapter describes the web-based tool Server Manager , the web-based configuration tool Initial Configuration Wizard as well as some additional options.

9.2.1 Initial Configuration Wizard

The Initial Configuration Wizard (ICW) is used for the initial configuration of the MiVoice Business and multiple applications.

Note:

It is recommended to use the Initial Configuration Wizard to configure the MiVoice Business and other applications on SMB Controller.

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

- Review initial configuration parameters
- Select and configure Resiliency
- Configure administration email and servers
- Configure numbering plan
- Configure SIP Trunking (optional)
- Configure incoming call configuration
- Select and configure SIP provider
- Change the administrator password for MiVB
- View a summary of the configuration
- Download Logs

Note that the values shown in the following screen shots of this document are only examples.

9.2.1.1 Launch Initial Configuration Wizard

The Initial Configuration Wizard (ICW) can be accessed via Server Manager.

To access the Initial Configuration Wizard:

1. Log in to Server Manager as an admin user.
2. From the **Applications** menu, click **Initial Configuration Wizard**.

The Initial Configuration Wizard panel opens, providing a link to launch the ICW, information about the ICW status, failure reasons, and an option for downloading ICW logs.

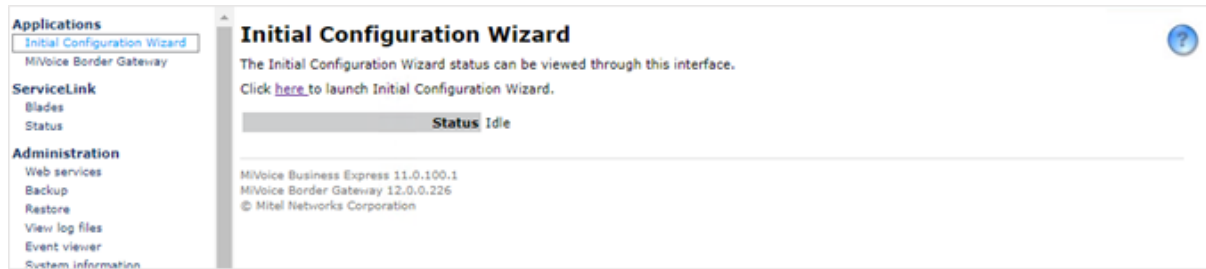


Figure 45: Initial Configuration Wizard blade panel showing Idle status

3. Click the link to launch Initial Configuration Wizard.

If the MiVoice Business blade is not installed, then this Initial Configuration Wizard page will indicate this and prevent the launch of the wizard. Launching the Initial Configuration Wizard without MiVoice Business installed on the SMB Controller is pointless as this is required for the ICW to function properly.

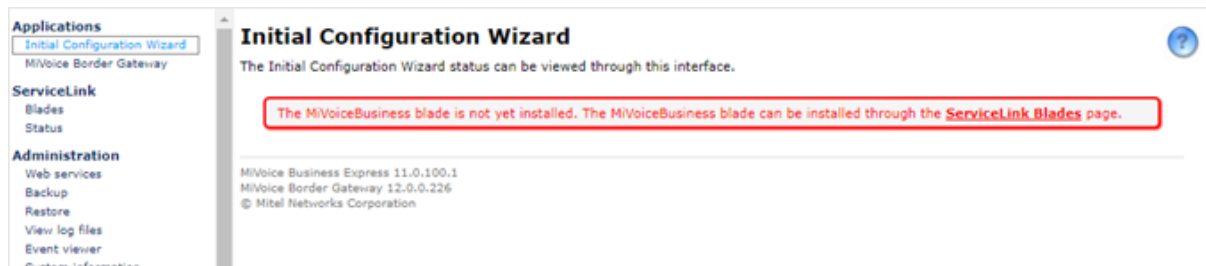


Figure 46: Initial Configuration Wizard page when MiVoice Business blade is not installed.

The Initial Configuration Wizard blade panel displays status indications as shown in the following table.

Table 19: Initial Configuration Wizard Status

Status	Meaning	User Action
Idle	ICW is not running.	Launch ICW.

Status	Meaning	User Action
Started	ICW is currently provisioning applications.	The ICW application cannot be launched by the user from the Initial Configuration Wizard panel. The link labeled here to launch the ICW will not be visible. If the user attempts to manually enter the ICW URL to launch it and clicks on the Start button again while the previous session is still in progress, the attempt will fail.
Completed	ICW has successfully provisioned applications.	User will not be able to re-run ICW
Failed	ICW failed to provision applications. Check the reason for more information on failure.	Fix the error and re-run ICW.

9.2.1.2 Welcome Page

When the Initial Configuration Wizard (ICW) is launched from the Server Manger, Welcome page opens, and the system applies default settings to the following applications:

- MiVoice Business
- MiVoice Border Gateway

Refer to the MiVoice Business system administrator online help for the standard default settings that are applied to the MiVoice Business platform.

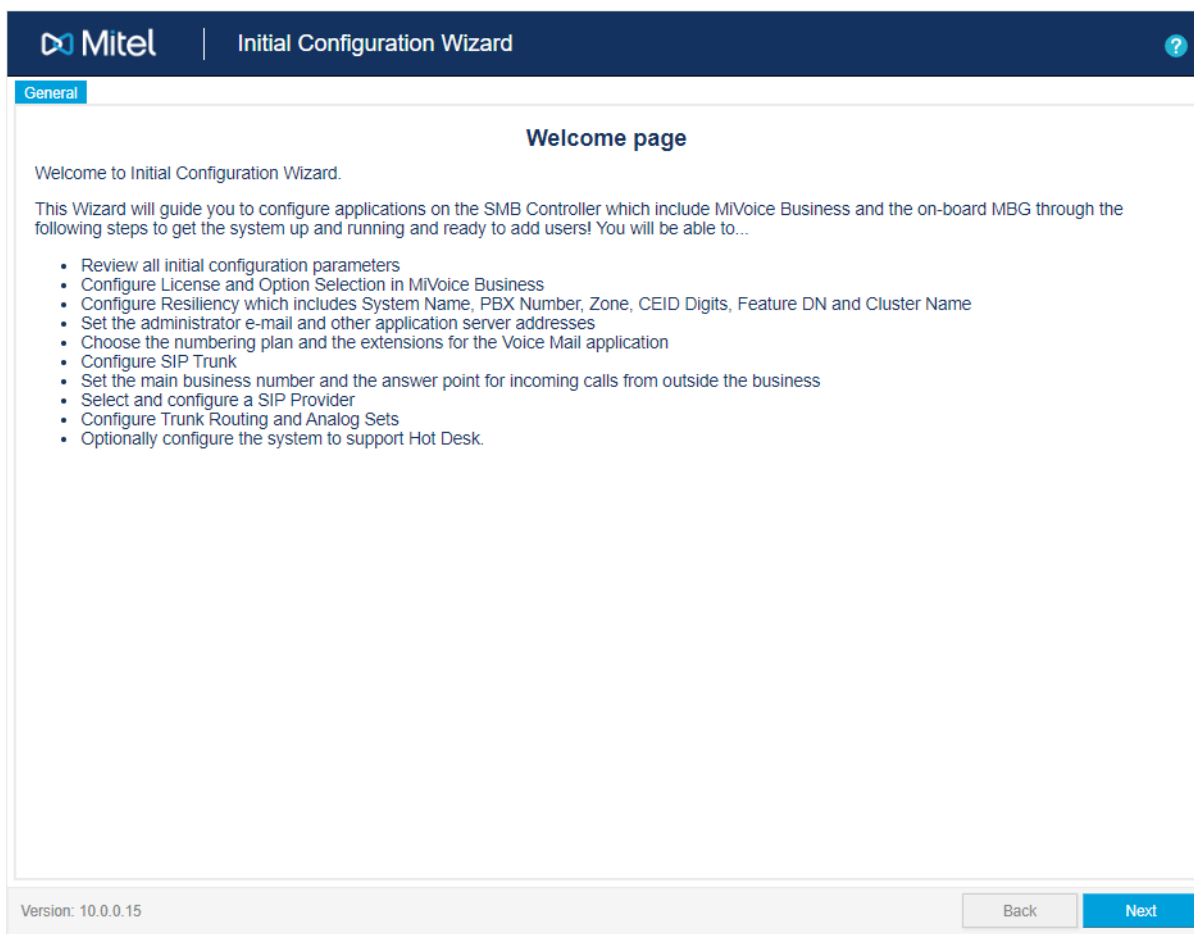


Figure 47: Welcome page for a new Initial Configuration Wizard

9.2.1.3 Credentials Page

The Credentials page is to validate MiVoice Business and Server Manager credentials.

Field	Description
MiVB Current Password	ESM system user password
MiVB New Password	To set new password for ESM system user
Confirm MiVB New Password	
Server Manager Login ID	Server Manager username and password to access resources within MSL.
Server Manager Password	

Mitel | Initial Configuration Wizard

Credentials

▼ SMB Controller

Please select a new MiVB password for your system. A strong password contains all of the following: upper case letter, lower case letter, number, non-alphanumeric character from the set @#\$%^!&+= and be at least 8 characters long. Please don't use single quotes.
It is recommended to use a consistent password between MiVB and Server Manager.

* MiVB Current Password

* MiVB New Password

* Confirm MiVB New Password

Server Manager Details

* Server Manager Login ID

* Server Manager Password

ESM system User Password

Set and Confirm new ESM system User Password

Server Manager admin User Password

Version: 10.0.0.15 Back Next

Figure 48: Credentials page for a new Initial Configuration Wizard configuration

9.2.1.4 Initial Configuration Page

The Initial Configuration Page is used to define the parameters described in the following table.

Parameter	Description
Time Zone	Time Zone specified at deployment time is displayed. Field is disabled.

Parameter	Description
Country	Country setting determines some Telephony Server default settings. The country that is displayed is derived from the timezone that you specified during deployment. If an "Other" country is chosen for the Country setting, the ICW will only partially configure the system. Additional manual configuration will be required after initial deployment.
Telecom Region	The Telecom Region determines the system's phone numbering plan and default system language. The region that is displayed is derived by the ICW from the timezone that you specified during deployment. The region defaults to North America if ICW is unable to derive a region from the timezone.
MiVB IP Address or FQDN	IP address or FQDN of the MiVoice Business telephony server (also known as the MiVoice Business address) specified during deployment. The value is pre-filled.
Licensing Key	Licensing key specified during deployment. The value is pre-populated.

i Note:

If necessary, you can select a different Time Zone, Country, and Telecom Region. If you select a Time zone that is not within one of Countries supported by the system, the Country value is set to "Other" and the Telecom Region defaults to North America.

▼ Initial Configuration i

- * Time Zone Universal ▼
- * Country United States ▼
- * Telecom Region North America ▼
- * MiVB IP Address 192.168.1.100
- * Licensing Key XXXXXXXXXX

Figure 49: Initial Configuration Page

9.2.1.5 License and Option Page

The Licensing page is used to allocate the required licenses.

▼ License and Option i

Licensed Options	Locally Consumed	Locally Allocated	Available For Allocation
IP Users	0	750	0
External HotDesk Users	0	750	0
ACD Active Agents	0	16	0
HTML Applications	0	750	0
Single Line Users	0	0	20
MiVB Console Active Operators	0	0	20
Multi-device Users	0	200	0
Multi-device Suites	0	0	20
Embedded Voice Mail	0	750	0
Embedded Voice Mail PMS	1	1	0
SIP Trunks	0	100	0
IDS Connection	0	0	1

Configuration Options

- Maximum Element per Cluster ▼
- 5560 IPT Devices Extended Key Lines ☐
- Extended PRG MDUG ☐
- Compression
- Extended Ring Group Members ☐

Figure 50: Licensing Page

9.2.1.6 Configure Resiliency Page

Resiliency is achieved by setting up a network of MiVoice Business systems in a Resilient Cluster that can direct IP Phones to route and maintain calls. The fields in the Configure Resiliency page are used for setting up this network. These fields are described in the following table.


Note:

While setting up resiliency, ensure that the resiliency parameter values such System Name, PBX Number, Zone, CEID Digits, and Feature DN values are different for the primary and the secondary MiVB applications.

Parameter	Description
MiVB System Name	Enter a unique name of up to nine characters for the network element. The field value will be defaulted to the Server Manager's hostname up to nine characters long. The user can change the default value.
IP Address	Defines the IP address of the Network Element specified during deployment. The field is auto-populated.
PBX Number	Unique identifier assigned to the Network Element. The PBX Number range is from 1 to 999.
Zone	Zone specified for the IP Voice Media Stream originating or terminating at the selected MiVoice Business system. The Zone range is from 1 to 999.
CEID Digits	Enter the Cluster Element Identifier (CEID) Digit String. Assign a unique CEID Digit Strings to each Cluster Element. In a network that is configured for the Voice Clustering (Portable Directory Number) feature, the CEID Digit String allows calls to be routed between Network Elements. The CEID Digit Strings for remote Network Elements must translate to a programmed ARS Route, ARS Route List, or ARS Route Plan for correct call routing. Up to seven digits can be used.

Parameter	Description
Feature DN	For the Local Network Element, enter a Feature Directory Number. For a Remote Network Element, enter the Feature DN that corresponds to the local Feature DN of the Remote Network Element within the Cluster. Up to seven digits can be used.
Cluster Name	Enter a unique Name for the Cluster. Up to 128 characters can be used.

▼ Configure Resiliency ⓘ

* MIVB System Name

* IP Address

* PBX Number

* Zone

* CEID Digits

Feature DN

Create Cluster

* Cluster Name

Figure 51: Configure Resiliency Page

9.2.1.7 Email and Servers Page

The **Email and Servers** page is used to configure the email and server address for sending the email messages.

Parameter	Description
Administrative E-mail Address	Enter the optional email address to which key system alerts are sent.
SMTP Mail Server	Enter the optional SMTP server address for sending email messages from one server to another.

Parameter	Description
SMTP Connection Type	Select this option to use a secure SMTP connection for sending email messages, and choose the encryption method.
SMTP Password	Enter the SMTP password for your mail server.

Figure 52: Email and Servers Page

9.2.1.8 Numbering Plan Page

Set the length from three to seven digits of the system extension numbers in the **Extension length** field of the Numbering Plan Page.

Figure 53: Numbering Plan Page

9.2.1.9 Voice Mail - Embedded Page

The following table describes the fields in the Voice Mail - Embedded Page.

Parameter	Description
Mailbox Extension Length	Set the length from (3 to 7 digits) of the Embedded Voice mail extension numbers. Defaults to the value specified in the Numbering Plan's Extension Length field.

Parameter	Description
Passcode Length	Set the length (4 to 8 digits) of the passcode length.
Voice Mail Ports	Set the number of Voice Mail ports to provision. Maximum value and default is 6.
Voice Mail Hunt Group	Extension that users dial to reach the voice mail system. Default is 7000.
Voice Mail Starting Port	First extension in the extension group. It is used by the voice mail system to connect a user to the voice mail system. Default is 7001 (up to 7030), Voicemail end port depends on voicemail port capacity.
Voice Mail Record A Call Hunt Group	Extension that users dial to reach the voice mail record-a-call system.

▼ Voice Mail - Embedded i

☒ Configure Embedded Voice Mail

Specify the number of digits for the extension length and passcode length.

* Passcode length 4 digits

Provide appropriate number of Voice Mail Ports. Total number of Voice Mail Ports + Voice Mail Record A Call Ports should not exceed the Voice Mail port capacity of 6.

* Voice Mail Ports 6

* Voice Mail Record A Call Ports 0

Specify the extensions you would like to use for the following services. You also have the option of accepting the default values displayed.

* Voice Mail Hunt Group 7000

* Voice Mail Starting Port 7001 (includes up to 7006)

Voice Mail Record A Call Hunt Group

Figure 54: Voice Mail - Embedded Page

9.2.1.10 Trunk Routing Page

The Trunk Routing Page is used to configure some standard default routes. For the Route Table, the Trunk Group defaults to SIP if MiVoice Border Gateway (MBG) is detected or, to Analog if MBG is not detected.

Figure 55: Trunk Routing Page

9.2.1.11 MBG Network Profile Page

Choose the network profile for MBG. This page is displayed only if the MBG is installed on the SMB Controller.

Parameter	Description
Co-resident with call manager configuration	Default mode for the SMB Controller platform, MBG acts in server-gateway mode.
Custom configuration	A custom configuration making use of manually set streaming addresses: • RTP ICP-side override address • RTP set-side override address

Figure 56: MBG Network Profile Page

9.2.1.12 SIP Trunks Page

The **SIP Trunks** Page is used to provision the SIP trunking connection to SIP service provider.

**Note:**

This page will be displayed only if MBG is installed on the SMB Controller.

Parameter	Description
Main Business Number	Provide the area code (three digits), city code (three digits), and phone number (four digits).
Number of digits to absorb	Select the number of leading digits to be stripped from the incoming call before the number is delivered to system call processing (for example: routing to an internal extension). Leading digits are stripped off from the left of the number. Leave blank if no digits are to be stripped off.
Digits to insert	Enter the digits that are inserted in front of the phone numbers after any leading digits have been absorbed. The digits are inserted prior to the phone numbers being sent for system call processing. Leave blank if no digits are to be inserted (optional).

Parameter	Description
SIP Service Provider	The most common Service Providers for your region are listed in a drop-down menu. A "Generic" SIP Peer Profile is also available. You can also select "Custom Profile" and import a CSV file saved from the SIP Peer Profile form of the MiVoice Business System Administration Tool: 1. Save a CSV file of a SIP Peer Profile. 2. Select Custom Profile from the drop-down menu. Click Browse and navigate to the CSV file. For partners that have access, there are canned SIP Service Profile import files available through the Mitel InfoChannel that can be used within this Initial Configuration Wizard form.
IP Address or FQDN	Enter the IP address or FQDN of the selected SIP Service Provider.
External Session Border Controller IP address or FQDN	Enter the IP address or FQDN of the External Session Border Controller (proxy server) that is provided by your SIP Service Provider.
Number of SIP channels	Displays the number of SIP channels licensed for the system. Number of SIP channels must not exceed the number of SIP trunk licenses.
Phone number(s) from Service Provider	This field is optional. If the FQDN/IP address of an incoming call does not match the FQDN/IP address of the Service Provider specified above, the MiVoice Business system will not accept the call unless the number is registered with the SIP Service Provider. Enter one or more telephone numbers that you want to register with the SIP Service Provider and check the Enable SIP Authentication box. The maximum number of digits per telephone number is 26. You can enter a mix of ranges and single numbers (for example, 6135554000-6135554400, 6135554500). The entire field is limited to 60 characters.

Parameter	Description
Call billing phone number	This number is sent as the billable number to the SIP Service Provider for SIP trunk calls. The maximum number of digits for a number is 26. Only digits 0 through 9 and no spacing between each digit are allowed (for example, 6135554000). If this instance is configured to use the same aggregated SIP Trunking Gateway as another instance, this billing number will be sent to the SIP Service provider. (Optional)
Enable SIP Authentication	If your SIP Provider requires authentication with a user name and password, select this box to authenticate the Telephone Numbers that you entered in the field above. Enter the SIP Authentication user name and password that you received from your SIP Provider.
Subscription User Name	The subscription user name can be any combination of alphanumeric and special characters, with a maximum of 48 characters.
Subscription Password	The subscription password can be any combination of alphanumeric and special characters, with a maximum of 20 characters.
Subscription Password Confirmation	Confirm the subscription password.

▼ SIP Trunks

☒ Configure Sip Trunks

* Main Business Number (232) - 342 - 2433

▼ Advanced Incoming Call Configuration

Number of digits to absorb 0 ▼

Digits to insert

* SIP Service Provider AccessLine
Choose File No file chosen

* IP Address or FQDN 10.211.26.12

External Session Border Controller IP address or FQDN

* Number of SIP channels 100

Phone number(s) from Service Provider

Call billing phone number

☐ Enable SIP Authentication

* User Name

* Password

* Confirm Password

▼ Advanced SIP Service Provider

Subscription User Name

Subscription Password

Subscription Password Confirmation

Figure 57: SIP Trunks Page

9.2.1.13 Analog Sets Page

The six Embedded FXS Ports and the 4FXS Interface Card Ports can be assigned a Directory Number from the ESM's Analog Sets Page.

The Analog Sets Page allows for a range of DNs to be assigned to the Embedded Analog FXS Ports and any installed 4FXS Interface Card.

▼ Analog Sets i

☒ Configure Embedded Analog Ports

Specify the first directory number to assign to the 6 embedded analog ports.

Extension Range 1001 - 1006

* Starting Extension 1001

Figure 58: Analog Sets Page

9.2.1.14 Optional Services Page

Hot Desking is configured in the Optional Services Page.

▼ Optional Services i

☒ Configure Hot Desk

Hot Desking allows a number of users to share one or more hot desk enabled IP phones. Specify the range of extensions to provision hot desk devices.

Extension Range None

* Starting Extension

* Number of Devices

Figure 59: Optional Services Page

Hot Desk

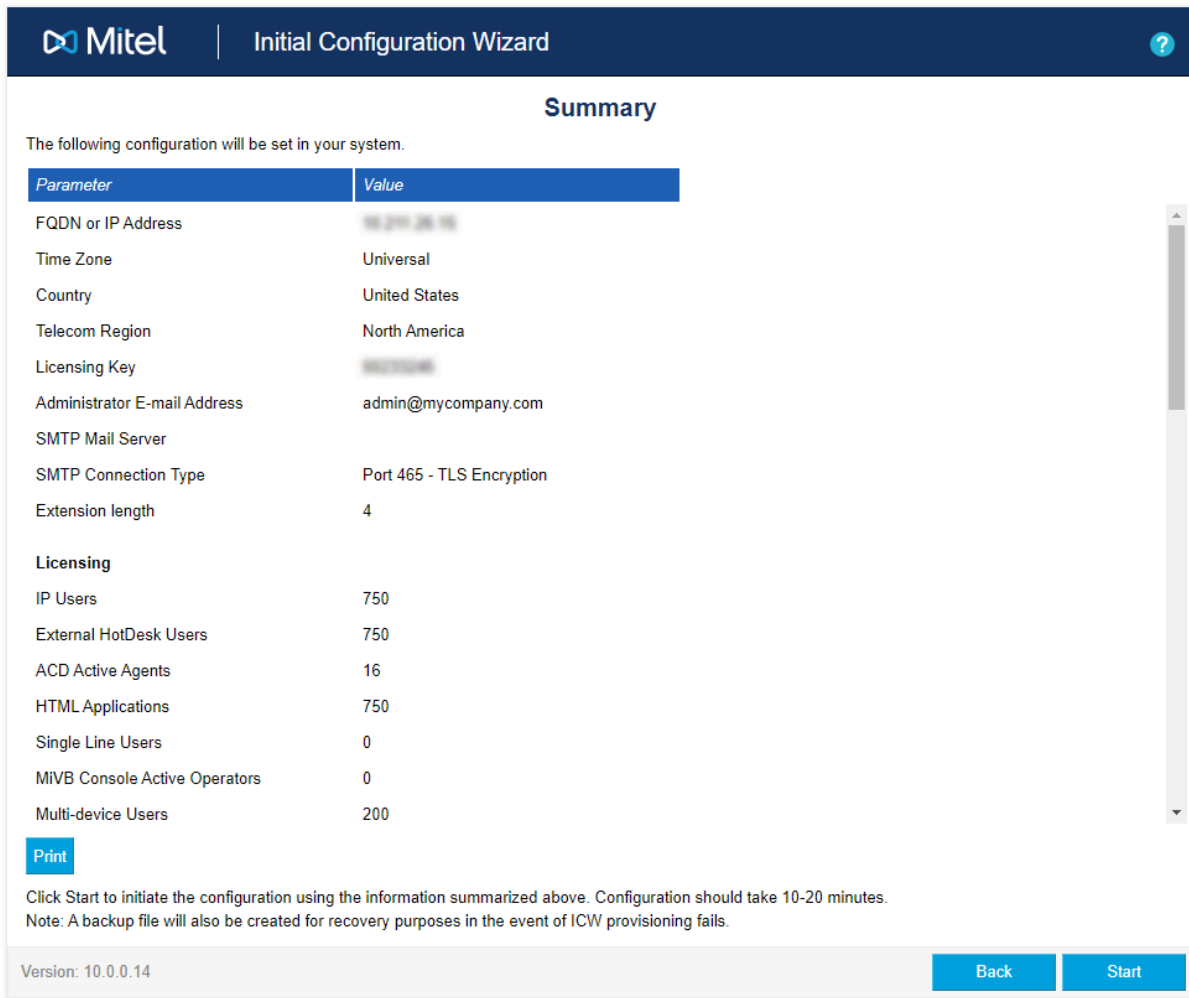
For the hot desking feature, configure the phones for which hot desking is enabled for the site. A hot desk user can log in to any hot-desk-enabled phone and the system applies the user's profile to the phone. If you have selected the Hot Desk feature, Select **Hot Desk** and complete the following:

Parameter	Description
Starting Extension	Enter the starting extension number (default 2000) of the range of numbers that the system will assign to the hot-desk-enabled phones. The hot desk extensions must be different from the extension numbers that you entered in the Numbering Plan screen (that is, the numbers must not overlap).
Number of Devices	Enter the number of phones that you want to support hot desking.

Parameter	Description
Extension Range	This field displays the range of extension numbers that the ICW assigns to the hot desk devices. The extension numbers are assigned consecutively. i Note: Ensure that the selected extension range does not conflict with the system's dialing plan.

9.2.1.15 Summary Page

The Summary Page is for reviewing the settings so that you can ensure that you have entered correct values before proceeding.



Mitel | Initial Configuration Wizard

Summary

The following configuration will be set in your system.

Parameter	Value
FQDN or IP Address	10.200.200.10
Time Zone	Universal
Country	United States
Telecom Region	North America
Licensing Key	XXXXXXXXXX
Administrator E-mail Address	admin@mycompany.com
SMTP Mail Server	
SMTP Connection Type	Port 465 - TLS Encryption
Extension length	4
Licensing	
IP Users	750
External HotDesk Users	750
ACD Active Agents	16
HTML Applications	750
Single Line Users	0
MiVB Console Active Operators	0
Multi-device Users	200

[Print](#)

Click Start to initiate the configuration using the information summarized above. Configuration should take 10-20 minutes.
 Note: A backup file will also be created for recovery purposes in the event of ICW provisioning fails.

Version: 10.0.0.14

[Back](#) [Start](#)

Figure 60: Summary Page

9.2.1.16 Configuring System Page

The Configuring System Page displays the current state of provisioning. Upon successful completion, a green check appears in the Status column for each of the listed operations. If the Initial Configuration Wizard fails to configure the system, check the logs by downloading the Initial Configuration Wizard logs of the wizard by clicking the **Download Logs** button to identify the issue.

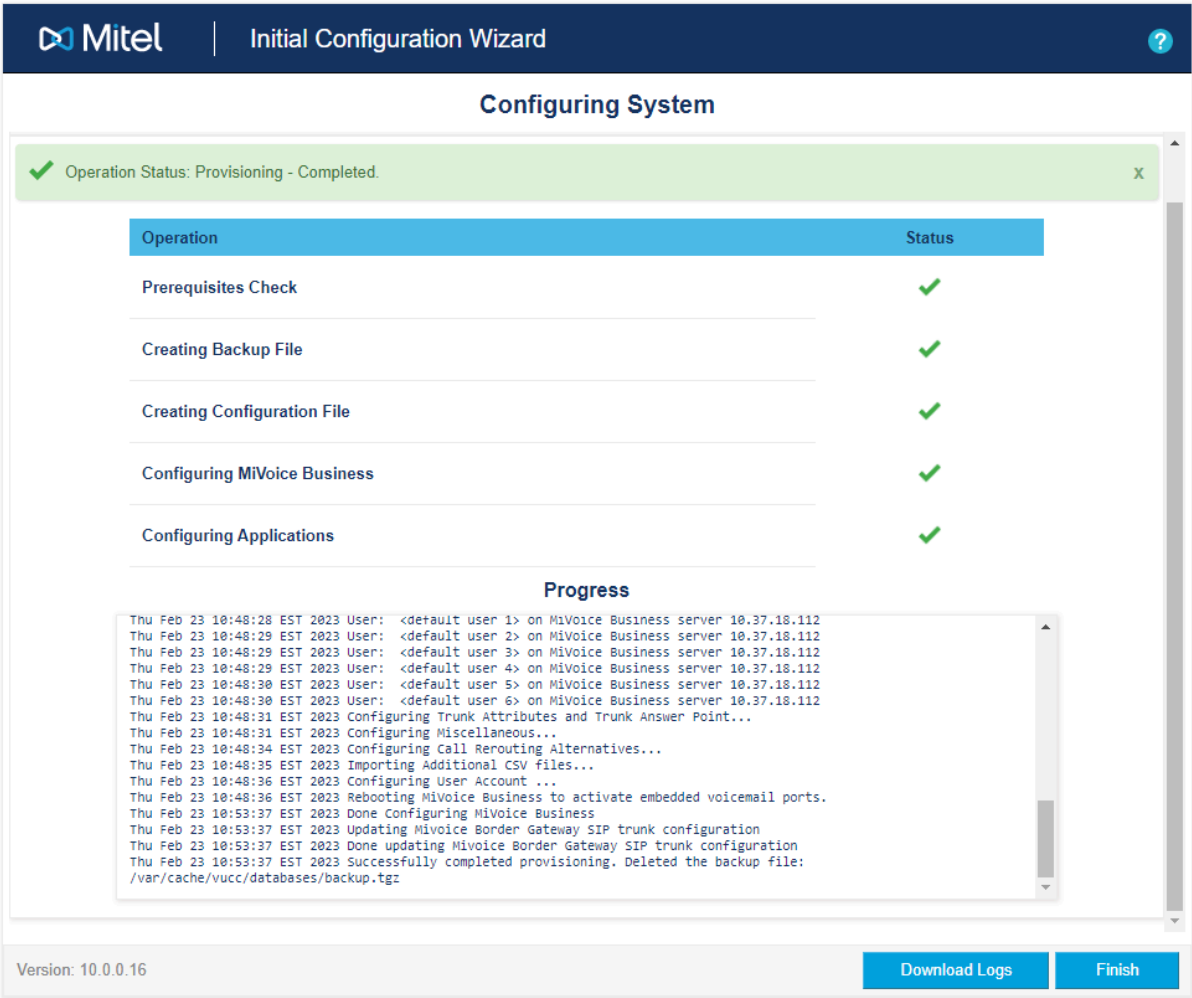


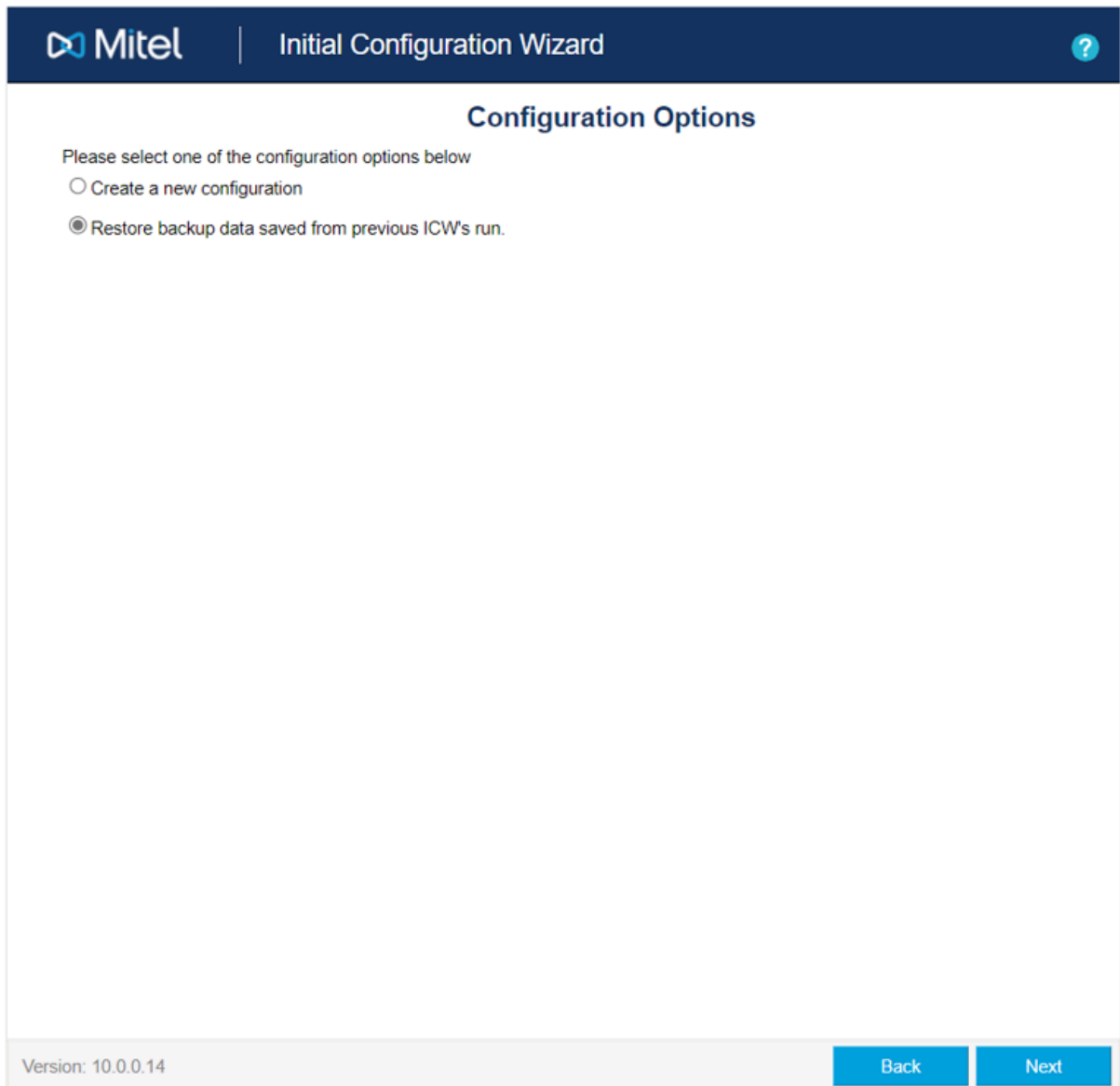
Figure 61: Configuring System Page

9.2.1.17 Configuration Options Page

If the configuration is unsuccessful, the Initial Configuration Wizard (ICW) will leave the system in a failed state for the user to troubleshoot, correct, or complete the configuration.

If the user launches the ICW again, after the user views the Welcome page, the **Configuration Options** Page opens. This page provides an option for the user to start a new configuration process or to restore the backup data that was saved from the previous ICW run.

1. Choose **Restore backup data saved from previous ICW's run.** and click the **Next** button.



The screenshot shows the 'Initial Configuration Wizard' window for Mitel. The title bar is dark blue with the Mitel logo and a help icon. The main content area is titled 'Configuration Options' and contains the instruction 'Please select one of the configuration options below'. There are two radio button options: 'Create a new configuration' and 'Restore backup data saved from previous ICW's run.', with the second option selected. At the bottom, there is a version number 'Version: 10.0.0.14' and two buttons, 'Back' and 'Next'.

Mitel | Initial Configuration Wizard ?

Configuration Options

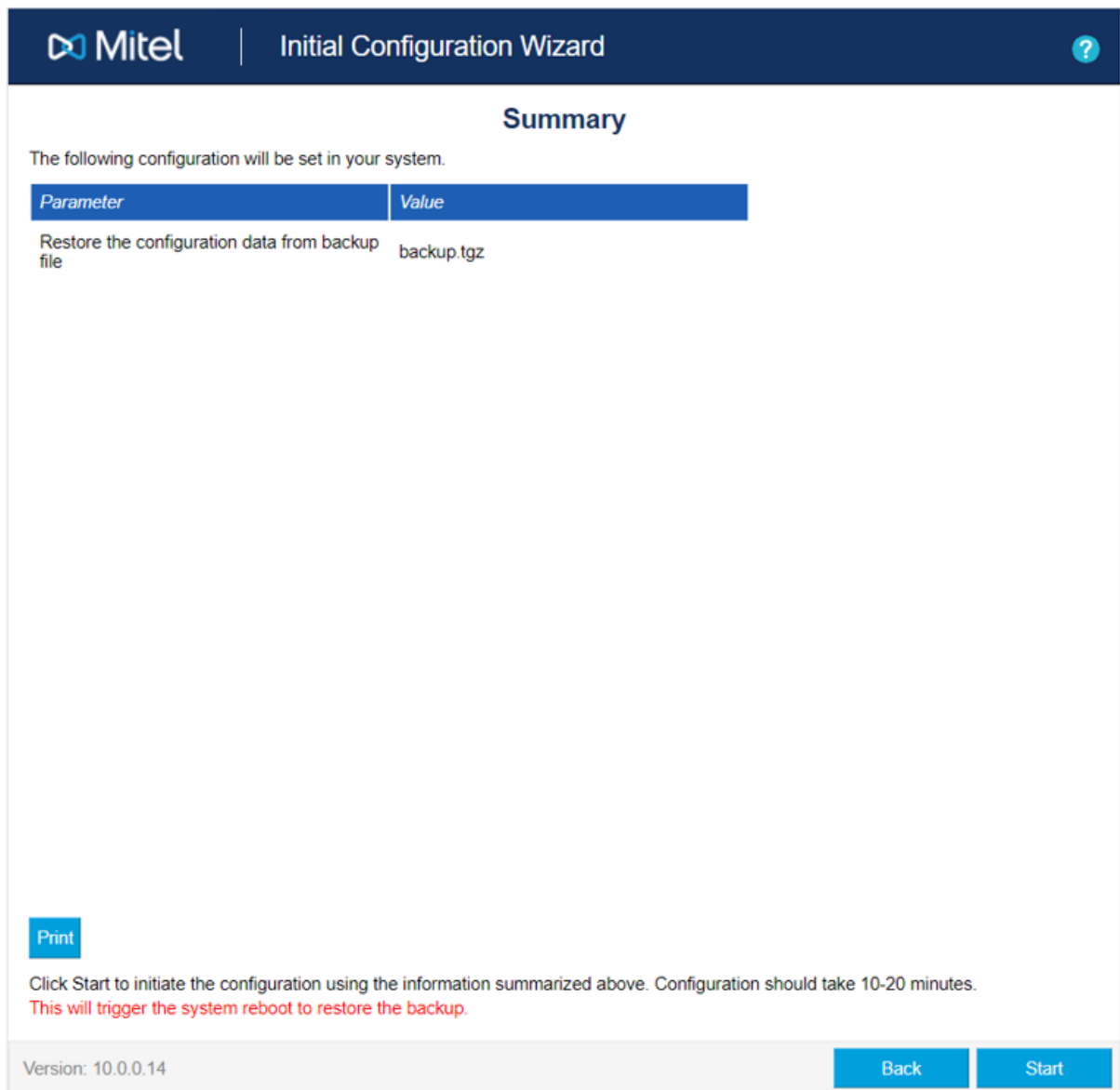
Please select one of the configuration options below

- ☐ Create a new configuration
- ☒ Restore backup data saved from previous ICW's run.

Version: 10.0.0.14 Back Next

Figure 62: Configuration Options Page

2. In the **Summary** page, click the **Start** button to restore the data.



Mitel | Initial Configuration Wizard ?

Summary

The following configuration will be set in your system.

Parameter	Value
Restore the configuration data from backup file	backup.tgz

[Print](#)

Click Start to initiate the configuration using the information summarized above. Configuration should take 10-20 minutes.
This will trigger the system reboot to restore the backup.

Version: 10.0.0.14 [Back](#) [Start](#)

Figure 63: Restore Summary Page

**Note:**

A system reboot is necessary to restore the data.

The Restoring Backup page is displayed as shown in the following figure.

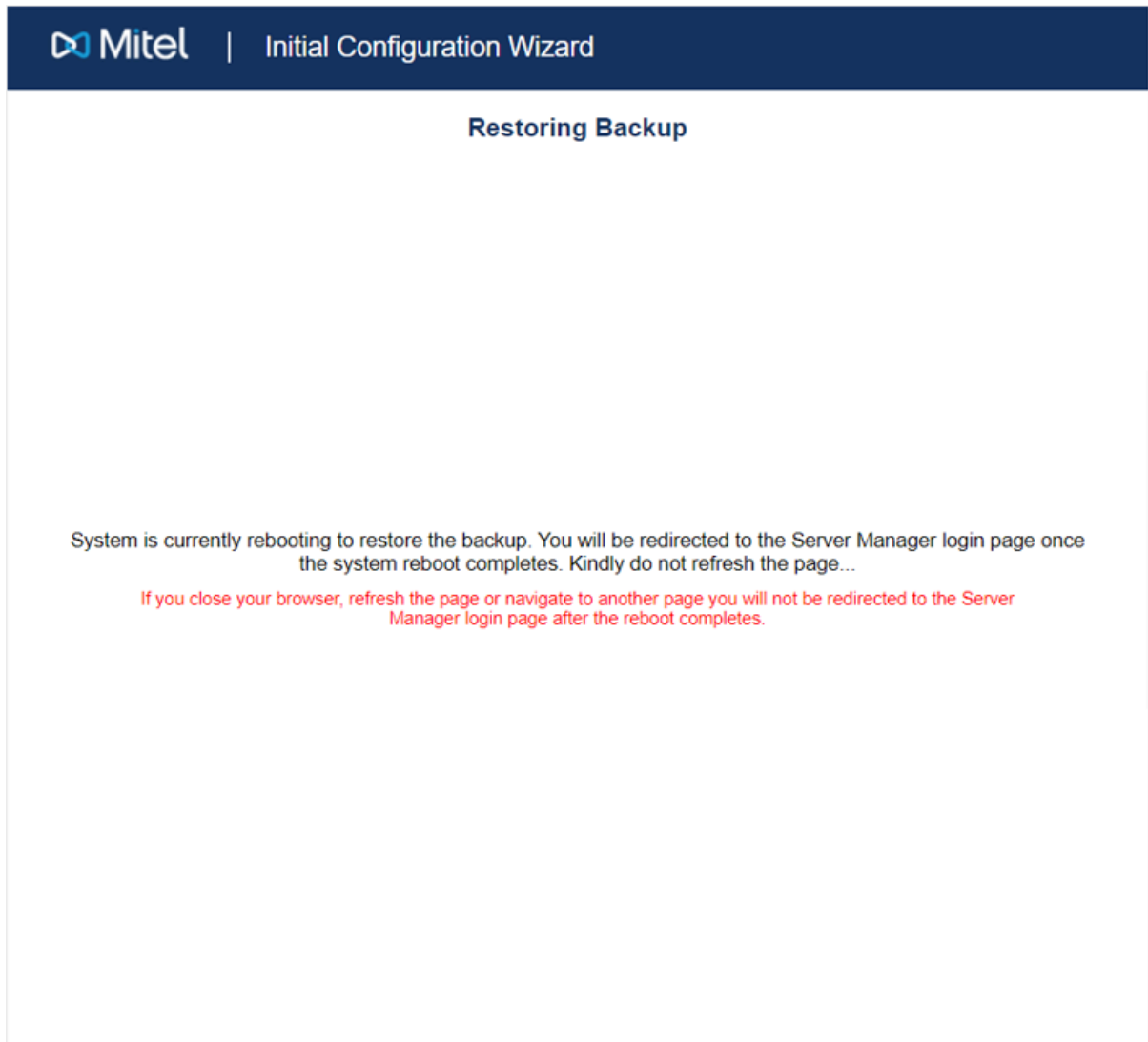


Figure 64: Restoring Backup

After the reboot is complete and the system is running, the user will be directed to the login screen of the Server Manager.

3. Log in to the Server Manager.

A red banner is displayed indicating whether the MiVB data restore is failed or is still in progress.

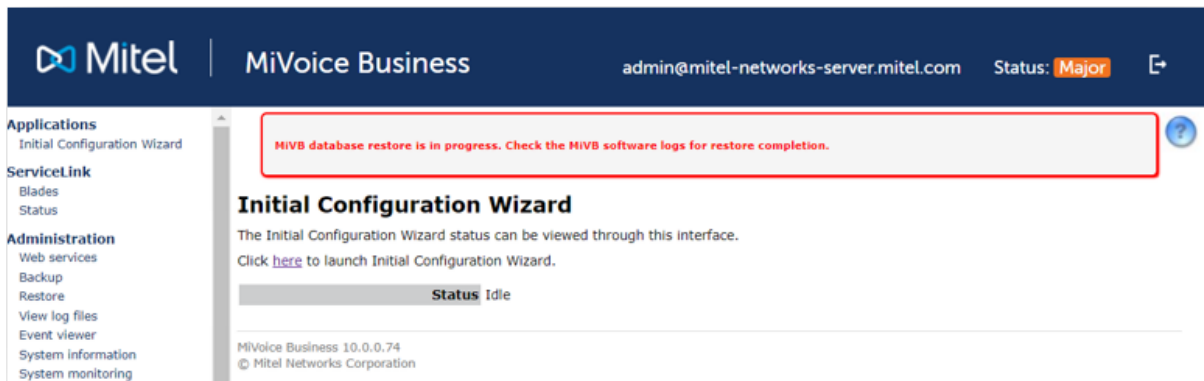


Figure 65: MiVoice Business Data Restore Status

After successful configuration, users are recommended to schedule a periodic network backup from the Server Manager Backup panel for maintenance and disaster recovery. For more details see, [Backup Using Server Manager](#) on page 163.

9.2.2 Configure MiVoice Business on the SMB Controller

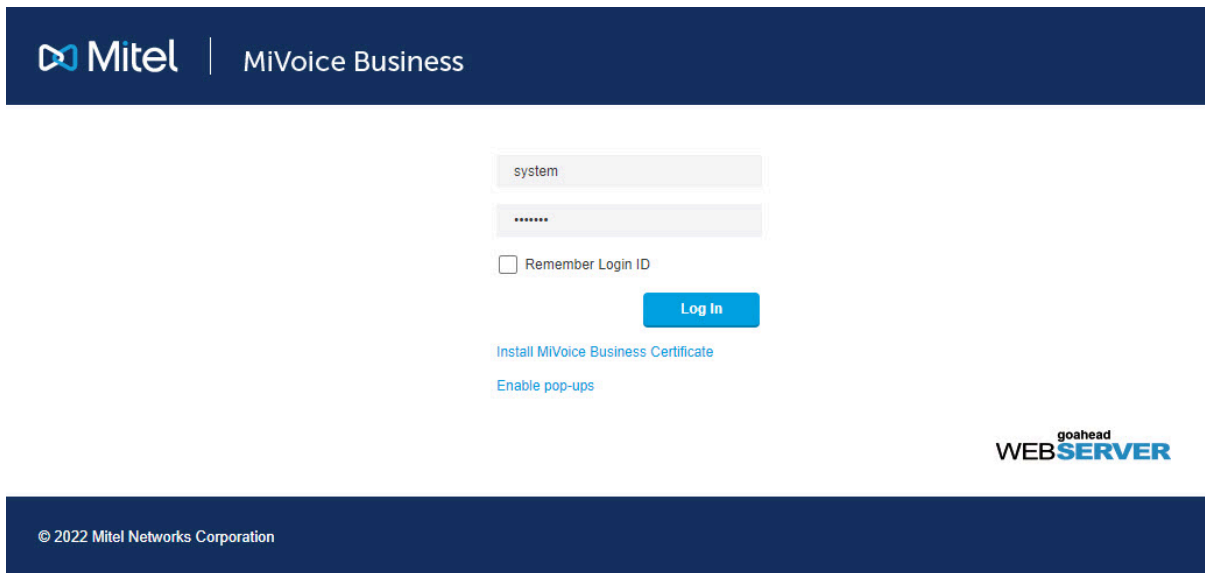
After deploying the blades, you need program the MiVoice Business system using MiVoice Business System Administration Tool.

i Note:

It is recommended to use the Initial Configuration Wizard to configure the MiVoice Business and other applications on SMB Controller.

(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.

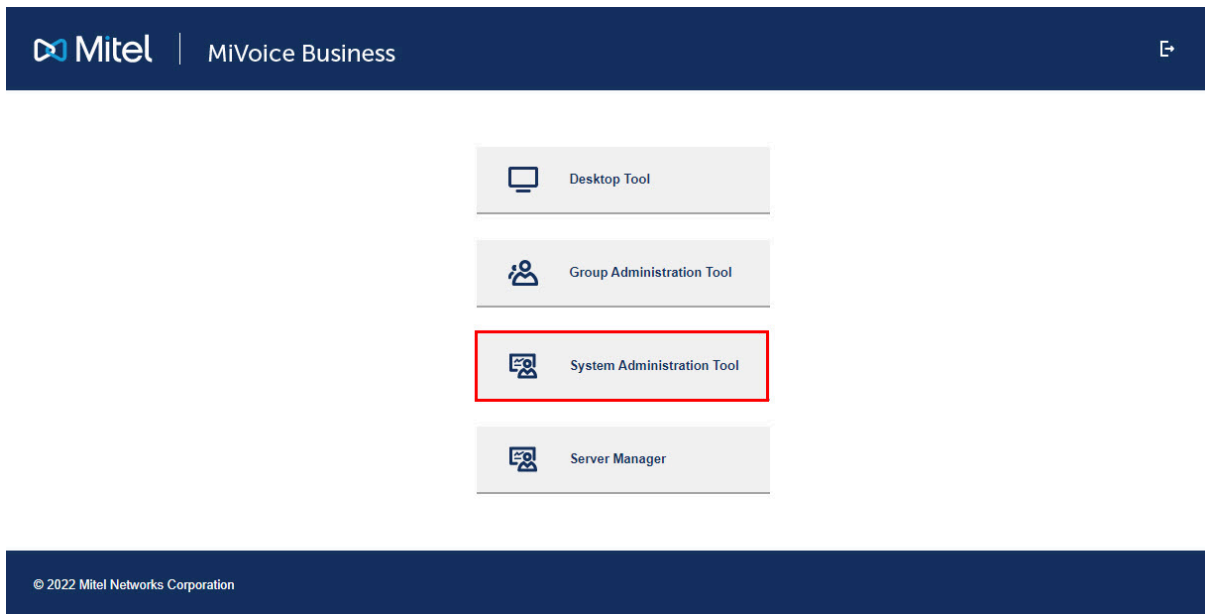
1. Log into MSL Server Manager at <https://<MSL IP Address>/>. MiVoice Business login page displays.



The login page features a dark blue header with the Mitel logo and 'MiVoice Business' text. Below the header, there is a login form with a username field containing 'system' and a password field with masked characters. A 'Remember Login ID' checkbox is present below the password field. A blue 'Log In' button is positioned to the right of the password field. Below the button, there are two links: 'Install MiVoice Business Certificate' and 'Enable pop-ups'. In the bottom right corner, there is a 'goahead WEB SERVER' logo. The footer contains the copyright notice '© 2022 Mitel Networks Corporation'.

Figure 66: MiVoice Business Login Page

2. Log in with the default username (system) and the default password (password).
3. You are asked to change the ESM password. Enter the new password. After confirmation of the new password, the MiVoice Business ESM select tool is displayed.



The ESM select tool page has a dark blue header with the Mitel logo, 'MiVoice Business', and a user icon. The main content area displays four tool options, each with an icon and a label: 'Desktop Tool' (monitor icon), 'Group Administration Tool' (group of people icon), 'System Administration Tool' (server icon, highlighted with a red border), and 'Server Manager' (server rack icon). The footer contains the copyright notice '© 2022 Mitel Networks Corporation'.

Figure 67: MiVoice Business ESM select tool

4. Select System Administrator Tool. The MiVoice Business System Administrator Tool is opened in a new window.

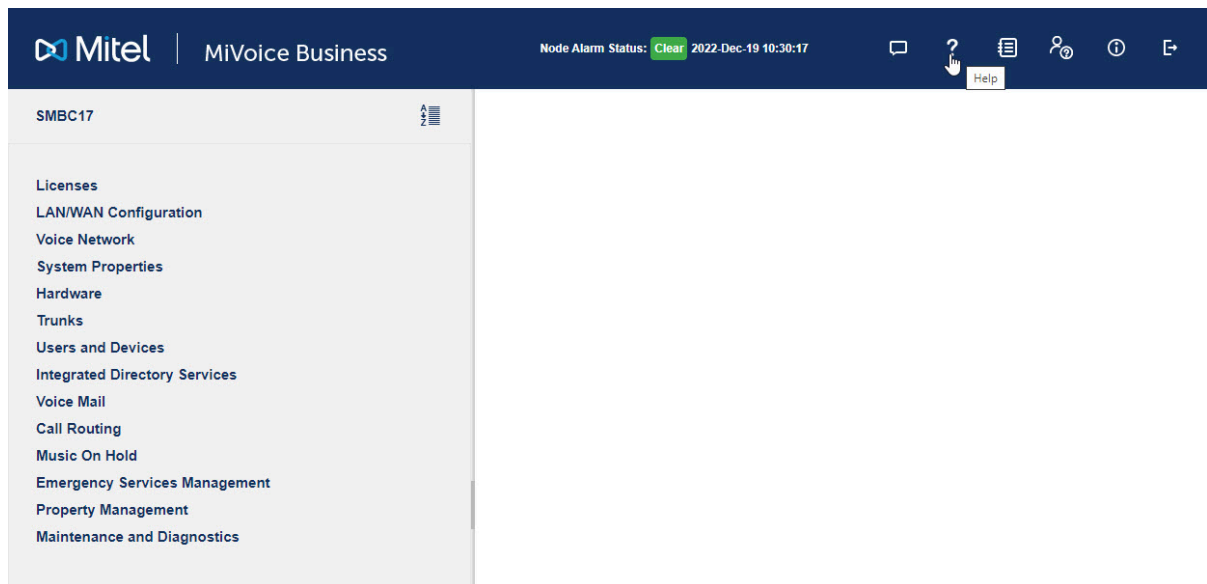


Figure 68: MiVoice Business System Administrator Tool

5. In the MiVoice Business System Administrator Tool, click the **Help** icon. The **System Administrator Tool Help** is displayed in a new window.

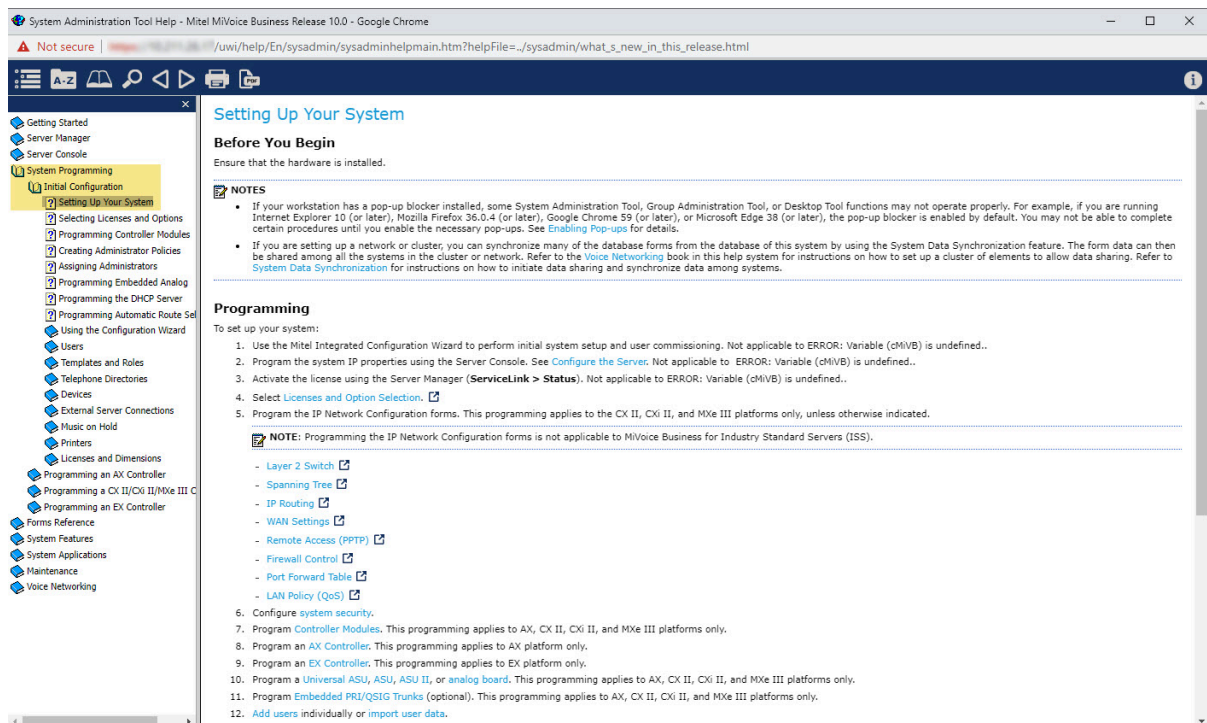


Figure 69: System Administrator Tool Help

6. In the **System Administrator Tool Help**, navigate to **System Programming > Initial Configuration > Setting Up Your System**.
7. Configure the MiVoice Business as per the instructions provided in the **Programming** section of **Setting Up Your System** topic in the **System Administrator Tool Help**.

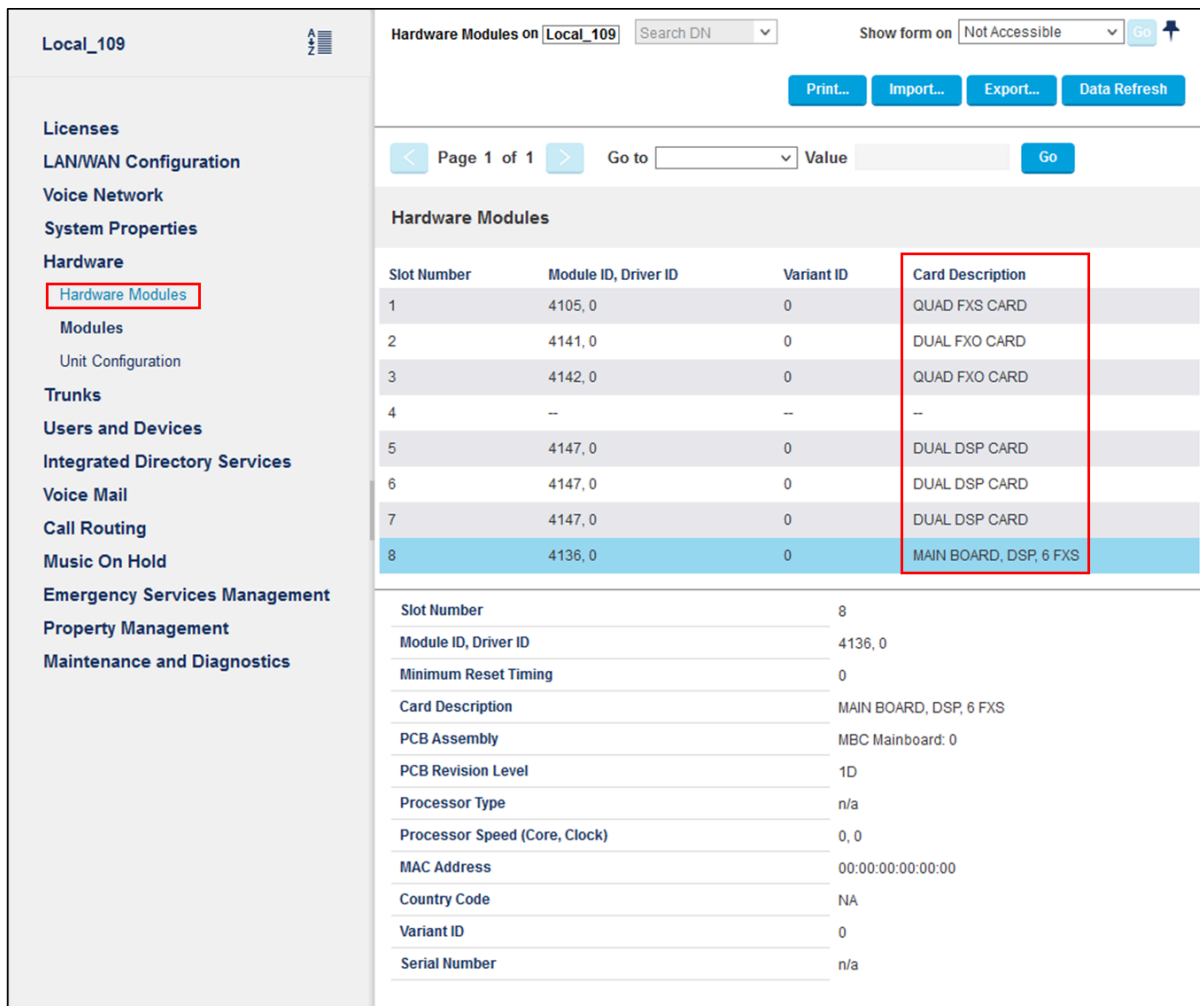
After completing the programming steps in the System Administrator Tool Help, the MiVoice Business is configured successfully.

9.2.2.1 Verify the Installed Hardware

To verify the installed hardware on the SMB Controller, you can use the Hardware Modules Form on the MiVoice Business System Administrator Tool. Hardware Modules Form is a read-only form that displays information on the installed Interface Cards, DSP Cards, and embedded FXS ports.

To verify the installed hardware:

1. Log into MSL Server Manager at <https://<MSL IP Address>/>.
2. Open the System Administrator Tool.
3. In the MiVoice Business System Administrator Tool, on the left side panel, select **Hardware Modules** from **Hardware**. The **Hardware Modules Form** is displayed.



Local_109

Hardware Modules on Local_109 Search DN Show form on Not Accessible Go

Print... Import... Export... Data Refresh

Page 1 of 1 Go to Value Go

Slot Number	Module ID, Driver ID	Variant ID	Card Description
1	4105, 0	0	QUAD FXS CARD
2	4141, 0	0	DUAL FXO CARD
3	4142, 0	0	QUAD FXO CARD
4	--	--	--
5	4147, 0	0	DUAL DSP CARD
6	4147, 0	0	DUAL DSP CARD
7	4147, 0	0	DUAL DSP CARD
8	4136, 0	0	MAIN BOARD, DSP, 6 FXS

Slot Number 8

Module ID, Driver ID 4136, 0

Minimum Reset Timing 0

Card Description MAIN BOARD, DSP, 6 FXS

PCB Assembly MBC Mainboard: 0

PCB Revision Level 1D

Processor Type n/a

Processor Speed (Core, Clock) 0, 0

MAC Address 00:00:00:00:00:00

Country Code NA

Variant ID 0

Serial Number n/a

Figure 70: Hardware Modules Form Example

9.2.2.2 Identify the Installed and Programmed Module Types

The installed and programmed module types on the SMB Controller can be identified using the Controller Module Configuration Form. Each installed module is assigned with a module number.

To identify the programmed and installed module type:

- 1. Log into MSL Server Manager at *https://<MSL IP Address>/*.
- 2. Open the System Administrator Tool.
- 3. In the MiVoice Business System Administrator Tool, on the left side panel, select **Controller Module Configuration** from **Hardware > Modules**. The **Controller Module Configuration Form** is displayed.

Local_109

Licenses

LAN/WAN Configuration

Voice Network

System Properties

Hardware

Hardware Modules

Modules

Controller Module Configuration

Unit Configuration

Trunks

Users and Devices

Integrated Directory Services

Voice Mail

Call Routing

Music On Hold

Emergency Services Management

Property Management

Maintenance and Diagnostics

Controller Module Configuration on Local_109

Search DN

Show form on Not Accessible

Go

Change

Clear

Print...

Import...

Export...

Data Refresh

Page 1 of 1

Go to

Value

Go

Controller Module Configuration

Module	Programmed Module Type	Installed Module Type	Unit	Comment
-	Embedded 6 FXS	Embedded 6 FXS	2	
1	4 Port FXS	4 Port FXS	3	
2	2 Port FXO	2 Port FXO	4	
3	4 Port FXO	4 Port FXO	5	

Figure 71: Example for Controller Module Configuration Form

Controller Module Configuration	
Module	1
Programmed Module Type	4 Port FXS
Installed Module Type	No Card Present
Unit	
Comment	

Save Cancel

Figure 72: Example for Configuring the Module

9.2.2.3 Program FXO Trunks

The installed FXO interface cards can be programmed, assign and configure the trunk number to the analog trunk card (FXO) using the Analog Trunks Form. The number of circuits displayed in the form correspond to the number of circuits on the card. The total number of circuits in the form is 16 if there are four 4 Port FXO Interface Cards installed.

To program the installed FXO interface card:

1. Log into MSL Server Manager at <https://<MSL IP Address>/>.
2. Open the System Administrator Tool.
3. In the MiVoice Business System Administrator Tool, on the left side panel, select **Analog Trunks** from **Trunks > Analog**. The **Analog Trunks Form** is displayed.
4. Select the Card Type and program the FXO interface card as required.

Here is an example of the Analog Trunks Form when two FXO interface cards are configured:

- One 2-Port FXO
- One 4-Port FXO

Local_109

Analog Trunks on Local_109 Search DN Show form on Not Accessible Go

Change Clear Print... Import... Export... Data Refresh

Page 1 of 1 Go to Value Go

Cabinet	Shelf	Slot	Circuit	Card Type	Trunk Number
4	1	1	1	2 Port FXO	
4	1	1	2	2 Port FXO	
5	1	1	1	4 Port FXO	
5	1	1	2	4 Port FXO	
5	1	1	3	4 Port FXO	
5	1	1	4	4 Port FXO	

Unit Number

Cabinet 4

Shelf 1

Slot 1

Circuit 1

Card Type 2 Port FXO

Trunk Number

Trunk Service Number

DTS Service Number

Circuit Descriptor Number

Interconnect Number

Tenant Number 1

Balance Network Setting National Complex

Trunk Category Unknown

Auto Select No

Milliwatt Trunk Number

CO Telephone Number

Figure 73: Example for Analog Trunks Form

9.2.2.4 Program FXS Devices

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.

To program the Analogue FXS ports, fill out the User and Service Configuration form:

1. Log into MSL Server Manager at <https://<MSL IP Address>/>.
2. Open the System Administrator Tool.
3. In the MiVoice Business System Administrator Tool, on the left side panel, select **User and Services Configuration** from **User and Devices**. The **User and Services Configuration Form** is displayed.
4. To add a phone, click **Add** > select **Default User and Device**.
5. Click on the tab **User Profile** > enter the name.

6. Do either of the following:

- Go to the **User and Services Configuration** form and select the **Device Type** as **Analog** and specify the **PLID** in the **Device Details** tab.
- Go to the **Analog Sets** form and select the **Card Type**.

7. 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.

8. Click **Save Changes**.

9.2.3 Configure MiVoice Border Gateway on the SMB Controller

The MiVoice Business on the SMB Controller also includes the MiVoice Border Gateway. This extends the number of deployment options available beyond MiVoice Business.

To configure the MiVoice Border Gateway the network profile should be either in **co-resident** or in **custom** mode. In custom mode, the primary LAN IP address must be excluded from the LAN bind IPs to avoid conflict with MiVoice Business.

Note:

It is recommended to use the Initial Configuration Wizard to configure the MiVoice Business and other applications on SMB Controller.

You should choose the custom mode if:

- the SMB Controller is deployed in the DMZ behind a NAT device, like a 3-port firewall.
- to instruct Teleworker sets to connect to MiVoice Border Gateway using the post-NAT IP address and to include the address in the set-side streaming address.

The icp-side streaming address will be the second LAN IP.

To configure the MiVoice Border Gateway, see the instruction provided in the [MBG Installation and Maintenance Guide](#) on Mitel Document Center.

To access the ESM management from the internet, the web proxy on the MiVoice Border Gateway must be configured with split DNS. For this to work properly you must:

- configure a private DNS server on the LAN to resolve the MiVoice Business FQDN.

For details, see the topic *Split DNS Setup* in the [MBG Installation and Maintenance Guide](#) on Mitel Document Center.

- configure a public DNS server to resolve the same private MiVoice Business FQDN to the SMB Controller WAN public IP.

For details, see the topic *Split DNS Setup* in the [MBG Installation and Maintenance Guide](#) on Mitel Document Center.

- the SMB Controller hostname needs to be different than the MiVoice Business hostname in the private/public FQDN.
- configure the MiVoice Border Gateway web proxy user and domain for MiVoice Business and other optional applications such as MiCollab, MiContact Center and Mitel Interaction Recording. For details, see the topic *Configure LAN Servers on the Web Proxy* in the [MBG Installation and Maintenance Guide](#) on Mitel Document Center.

**Note:**

If the web proxy is not configured, users accessing the SMB Controller WAN IP are redirected to server-manager.

9.2.4 Configure CloudLink Gateway for MSL

This article contains specific information for the installation and operation of the CloudLink gateway on MSL (Mitel Standard Linux).

**Note:**

It is recommended to use the Initial Configuration Wizard to configure the MiVoice Business and other applications on SMB Controller.

Reference

For more details, see [Mitel CloudLink - Deployment Guide with MiVoice Business](#) on Mitel Document Center.

9.3 Integrate Applications

The MiVoice Border Gateway services are independent from the MiVoice Business. As a result, the customer must manually configure/integrate these services:

- Teleworkers
- SIP Trunking with the MiVoice Border Gateway
- Call Recording

To manually configure these services, use the MiVoice Business System Administrator Tool.

**Note:**

It is recommended to use the Initial Configuration Wizard to configure the MiVoice Business and other applications on SMB Controller.

**Note:**

When using an offboard MiVoice Border Gateway with the CloudLink GateWay or MiCollab, the embedded MiVoice Border Gateway on the SMB Controller can still be used for SIP Trunking. Caution must be taken to ensure the MiVoice Border Gateway resources remain within the 150 User limit.

MiVoice Business with the Mitel Performance Analytics Probe

The MiVoice Business and Mitel Performance Analytics Probe are independent applications. The Mitel Performance Analytics Probe obtains a list of MiVoice Business to access from the Mitel Performance Analytics Cloud Service. The customer is responsible for programming the Mitel Performance Analytics Cloud Service accordingly. This occurs for both an embedded Mitel Performance Analytics Probe and an offboard Mitel Performance Analytics Probe.

This chapter contains the following sections:

- [Platform Migration](#)
- [Migration Tool](#)
- [Migration from Pre-9.0 MiVoice Business Platform to SMB Controller](#)
- [Migrating Embedded Application to offboard](#)

10.1 Platform Migration

The SMB Controller does not share common cards with other platforms. The MiVoice Business on the SMB Controller will only support the 4 port FXO expansion, 2 port FXS expansion, and 4 port FXS expansion cards

This means that cards supported on one platform type are not supported on another platform type. These devices do not consume any licenses during the database restore process and can be converted back to analog devices after the database restore has completed. After the device has been modified, converted to analog, or when the SIP device starts using this DN, a license is consumed.

When migrating Mx III, CX II, and AX Controllers, the platform-specific hardware (AMB/AOB, CIM, ASUs, T1/E1, Dual T1/E1, and so on) are not supported on the SMB Controller and will be ignored. Analog Devices connected to this hardware are converted to PENDING Single Line Generic SIP Devices. Analog Trunks are removed, leaving an ARS Route pointing to an empty Analog Trunk Group. To restore functionality, the Administrator must make the required changes.

Note:

The type *.dr.logfile_1 Maintenance Command can be used to dump the Call Control Restore Logs to see what data was dumped and why.

Note:

The SMB Controller can support up to 16 Voicemail ports. If the migration of a database contains more Voicemail ports than is supported on the SMB Controller, it will be reduced to 16. If there are not enough DSPs to support this configuration, DSP alarms will be raised.

Table 20: Supported migration types

From	Comments
MXe III, CXII, or AX	(NEW). Toss FXO/T1/E1. Converts FXS to PENDING Single Line Generic SIP.
Virtual, or ISS	(NEW, but not MVP) Everything is retained.
EX	(Existing) Must manually delete the EX-hardware before migration.

10.1.1 Migrating CX-II, MXe-III, AX to SMB Controller

The process to migrate MiVoice Business system installed on a MXe-III, CX-II, or AX controller to the SMB Controller platform is as follows:

1. Run the pre-migration audit, to identify any hardware that might cause an issue during the migration to the SMB Controller. For more details, see [MiVoice Business - Migration Guidelines](#).
2. Via ESM, backup the existing platform.
3. [Deploy the SMB Controller](#).
4. Configure the [SMB Controller](#).
5. Install the [MSL Container](#).
6. Install the [MiVoice Business Blade](#).
7. Restore the MiVoice Business data (via ESM).
8. (Optionally) Program the Trunk IDs against FXO/T1/E1 cards that have been automatically programmed. Assign the Trunk IDs to the appropriate TDM Trunk Groups.
9. (Optionally) Convert the PENDING Single Line Generic SIP Device to an Analog Set. Via the Analog Sets form, program the DN of a Single Line Generic SIP Device on the desired PLID.

10.1.2 Migrating Virtual, ISS, or EX Controller from SMB Controller

Refer the [Table 20: Supported migration types](#) on page 152 to see the supported migration types. The supported migration process will be:

1. Run the pre-migration audit, to identify any hardware that might cause an issue during the migration to the Virtual, ISS, or EX platform (in particular licensing concerns).
2. Via ESM, backup the MiVoice Business on SMB Controller
3. Deploy the Virtual, ISS, or EX platform
4. Restore the MiVoice Business data (via ESM).
 - All Analog Devices will be converted to Generic SIP Devices.
 - All Analog Trunks/Digital Trunks will be removed, leaving an Empty Trunk Group and ARS Routers.

For an EX:

- Program the EX Gateway.
- Convert Generic SIP Devices to an Analog FXS using the EX-cards.
- Convert any ARS Route using a Trunk Group to use the appropriate SIP Peer.

10.2 Migration Tool

The Migration Tool is used to help migrate pre-9.0 platforms to 9.0 or later. In particular, it provides:

- A Pre-Migration Audit to help identify elements of a customer database that could cause problems when migrating to a 9.0 or later Platform.
- An easy way to migrate MiVoice Business installed on an MxIII, CXII, or AX controllers to SMB controller, (back up the database, install 9.x, and restore the database on the new controller).



Note:

The purchased T.38 license will be cleared during database restore.



Note:

The Migration Tool does not support platforms already running MiVB 9.0 or later.

The Migration Tool will support SMB Controller as a target platform only when performing Pre-Migration Audit operation. It will:

- Warn about each analog device that will be converted to a PENDING Single Line Generic SIP Device, and that they will need to convert it back to an FXS, or register it as a SIP device.
- Warn about hardware that is not supported on the SMB Controller
- Warn about analog and digital trunks that are programmed on unsupported hardware
- Warn about the additional license consumption when converting an analog device to a Single Line Generic SIP Device
- Warn about the conversion of Analog Devices to PENDING Single Line Appearances.
- Warn about an Analog Device programmed as an Alert DN in the Skills Agents Groups, and ACD Express Groups. No Hunt Groups.
- Warn about irrelevant Layer 2 IP address and VLAN ID configuration.

10.3 Migration from Pre-9.0 MiVoice Business Platform to SMB Controller

The procedure for migrating a pre-9.0 MiVoice Business platform to SMB Controller:

1. Install or Upgrade the Migration Tool on your PC.
2. Run a pre-migration audit and verify that the database supports migration to MiVoice Business 9.0 or later.
 - a. Detect any unsupported hardware, and warn that they will be removed
 - b. Detect any Analog device on a card programmed onto an ASU that is not supported on the SMB Controller platform.
3. Backup the MiVoice Business data (via ESM)
4. Deploy the SMB Controller
 - a. Configure [SMB Controller](#)
 - b. Install [MSL Container](#)
 - c. Install [MiVoice Business Blade](#)
5. Restore the MiVoice Business data (via ESM).
6. Program SMB Controller specific hardware as required.

**Note:**

For more information, see the MiVoice Business - Migration Guidelines document located at [Mitel Doc Center](#).

10.4 Migrating Embedded Application to offboard

The embedded Mitel Border Gateway, CloudLink Gateway, and Mitel Performance Analytics Probe are intended to service only the embedded MiVoice Business on the SMB Controller. If a customer expands beyond the capabilities of the MiVoice Business on SMB Controller (that is, required clustering with multiple MiVoice Business, MiCollab integration, MiCC Integration) then the expectation is that the customer will migrate to use offboard Mitel Border Gateway, CloudLink Gateway, and Mitel Performance Analytics Probe applications.

**Note:**

To migrate Mitel Border Gateway and CloudLink Gateway to SMB Controller platform, you must use the Bulk Provisioning Export/Import method.

10.4.1 Offloading Mitel Border Gateway + CloudLink Gateway

In order to migrate to and offboard Mitel Border Gateway and CloudLink Gateway:

1. Take a backup via MSL.

2. From AMC:

- a.** Create a new ARID for MSL on SMB Controller and move MiVoice Business related licenses to this new ARID.
 - b.** Create new another ARID for Mitel Border Gateway and move Mitel Border Gateway related licenses to this new ARID.
 - c.** Delete the old ARID.
- 3.** Deploy offboard Mitel Border Gateway and CloudLink Gateway and synchronize with AMC.
- a.** Restore the backup taken in the first step.

4. From the SMB Controller:

- a.** Remove the Mitel Border Gateway Blade and CloudLink Gateway from the SMB Controller.
 - b.** Synchronize with AMC using the new ARID.
- 5.** Reconfigure the integration between MiVoice Business and Mitel Border Gateway (SIP Outbound Proxy) and teleworkers.
- 6.** Associate the new CloudLink Gateway with your CloudLink Account. Reconfigure the integration between CloudLink Gateway and the Mitel Border Gateway.

10.4.2 Mitel Performance Analytics Probe

To migrate to and offboard Mitel Performance Analytics Probe:

- 1.** Deploy the new offboard Mitel Performance Analytics Probe.
- 2.** Remove the embedded Mitel Performance Analytics Probe.
- 3.** Remove the Mitel Performance Analytics Probe entitlement from your ARID in AMC.

This chapter contains the following sections:

- [Shutdown and Reboot](#)
- [Start/Stop/Restart/Uninstall the MSL Container](#)
- [Restart the MSL Server](#)
- [Restart the SMB Controller via SMB Controller Front Panel](#)
- [Managing Multiple Admin Accounts on SMB Controller Manager](#)
- [Changing the IP Addresses](#)
- [Backup and Restore](#)
- [Data Maintenance](#)
- [Update Software](#)
- [Hardware Update](#)
- [Monitor the eMMC Wear](#)

This chapter describes maintaining the system and configuration data as well as updating the system software. Replacing cards, modules, and terminals are also described. The display and control panel of the SMB Controller, operations supervision using the event message concept, operating state display, and error display are also topics covered in this chapter.

11.1 Shutdown and Reboot

The SMB Controller can be Restarted, Shutdown, or Factory Reset from the SMB Controller Manager. A Shutdown initiates a graceful shutdown of the MSL Container. A Factory Reset can be performed by selecting the Factory Reset Button in the System Reset Panel.



Note:

If you cannot access the SMB Controller Manager, you can trigger system shutdown by pressing the CTRL button on the front panel and then enter Emergency Mode by pressing the CTRL button on the front panel while the F0 LED on the front panel is red during start up.

MSL can be rebooted or restarted from the MSL Container, but that will restart or shutdown the MSL and all the applications that run under the MSL only, not the complete system.

MiVoice Business can also be restarted with the Reset System Maintenance Command, but that will only reset MiVoice Business.

11.1.1 Restart the SMB Controller

To restart the SMB Controller:

- 1. Login to the SMB Controller Manager.
- 2. From the left panel, select the **Maintenance** section and then click **System reset**.
- 3. From the **System reset** window, click on the **Restart** button.

Note:
Restarting the MSL will reboot all the applications that run under the MSL

11.1.2 Shutting Down the SMB Controller

If the SMB Controller needs to be disconnected from the power supply, it must be shut down in a controlled manner. This gives the applications time to save their data and to close. The SMB Controller does not power down completely and will remain in the shut-down mode for 90 seconds before it starts up again automatically. You must remove the power cord during that time. This procedure is described in chapter [Shut-down mode](#).

11.2 Start/Stop/Restart/Uninstall the MSL Container

The MSL Container can be started/stopped by Controller Manager.

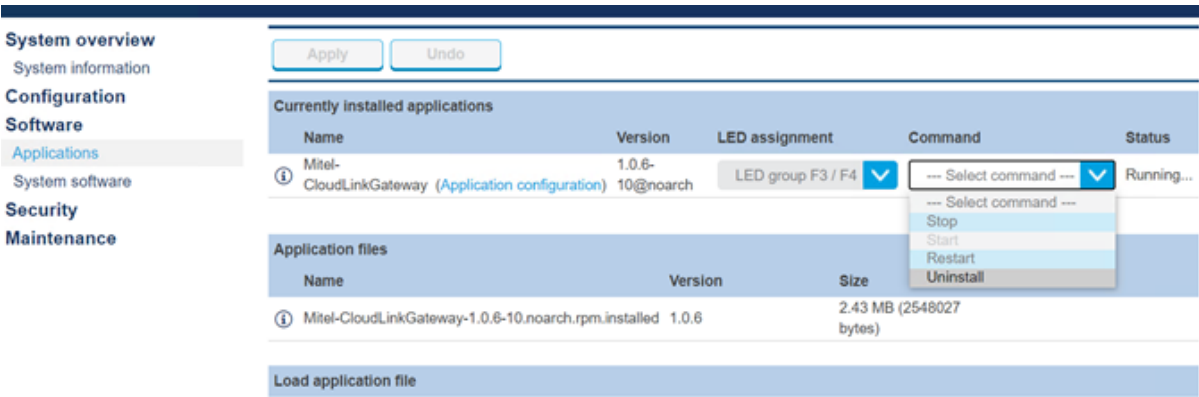


Figure 74: Controller Manager - Applications Start/Stop/Restart/Uninstall

- 1. Navigate to **Software > Applications**.
- 2. Under the **Command** column, select the operation via the drop down.
- 3. Confirm the operation.

Wait for two minutes to complete the process, even if the process state in the SMB Controller changes.

11.3 Restart the MSL Server

When the MSL server is restarted, the MSL server is rebooted and restarts all the applications that run on it.

To restart the MSL Server:

1. Log in to the MiVoice Business Server Manager.
2. From the **Administration** menu, select **Shutdown or reboot**.
3. Select the **Reboot** radio button and then click the **Perform** button.

To restart the MiVoice Business system, the System Administrator Tool maintenance commands can be used; for more details, see the System Administration Tool Online Help.

11.4 Restart the SMB Controller via SMB Controller Front Panel

Execute a shutdown of the SMB Controller using the pilot key and do not remove the power. After you trigger the shut-down with the pilot key, the controller shuts down all the applications in a controlled manner, enters shut-down mode for 1.5 minutes and then starts up again. All configuration data are preserved (see [Shut-down mode](#)). Therefore, this procedure is equivalent to restart via Restart button from the controller Manager except that it offers user the option to safely remove the power.

Note:

- Never disconnect the SMB Controller from the power supply to trigger a restart. This can result in data losses and prevent a restart.
- The restart is triggered immediately. All the active call and data connections are interrupted.

11.5 Managing Multiple Admin Accounts on SMB Controller Manager

The SMB Controller Manager platform allows you to set up multiple admin accounts, which can be customized with their own username. Up to 5 users with the same access rights can manage the service, and each can add, change, or delete accounts by the currently logged-in admin. This multiple admin account feature ensures that an alternative account will always be available. If one administrator forgets their password, others can still access the SMB Controller.

This feature prevents losing access to the SMBC due to forgotten passwords.

The password expiration time and password rules remain global for all users. This helps to enhance user management, improve security, and provide more customization options for administrators.

Note:
Only one user can be logged in to the SMBC Manager platform at a time.

To create a new account with the same privileges as an admin user:

- 1. Log into the **Server Manager**, and navigate to **Configuration > Users**.
- 2. In the **Authentication** section, re-enter current login password to verify the authentication.

Mitel

SMB Controller Manager

SSH access is enabled

55

Welcome admin

?

System overview

System information

Configuration

User

IP network

Date and Time

Software

Security

Maintenance

Undo

Authentication

Re-enter current login password

Name	New password	Confirm new password	
admin			Apply user
test1			Apply user

Add user

Copyright © 2023 Mitel Networks Corporation - All rights reserved

- 3. Click on the **Add User** button.
- A new user field will be displayed.
- 4. In the new user field, enter the new user name, set a password, and confirm the password.

Note:
It is mandatory to change this password during initial login.
See [Set Credentials for the SMB Controller](#) for the SMB Controller password rules.

5. Click on the **Apply User** button.

Mitel | SMB Controller Manager | SSH access is enabled | Welcome admin | ? |

System overview
System information

Configuration
User
IP network
Date and Time
Software
Security
Maintenance

Undo

Authentication

Re-enter current login password:

Name	New password	Confirm new password	
admin			Apply user
Test			Apply user
Test 2			Apply user

Add user

Copyright © 2023 Mitel Networks Corporation - All rights reserved

The new admin account is created now and the new user can login to the SMB Controller Manager using the new credentials.

Click the **Undo** button to cancel the current process.

Note:

- A default user named "admin" is automatically created for ease of setup.
- Up to 5 admin accounts with the same privileges can be configured.
- Each user can be assigned a customized name.
- No option to change user names without deleting and adding a new user.

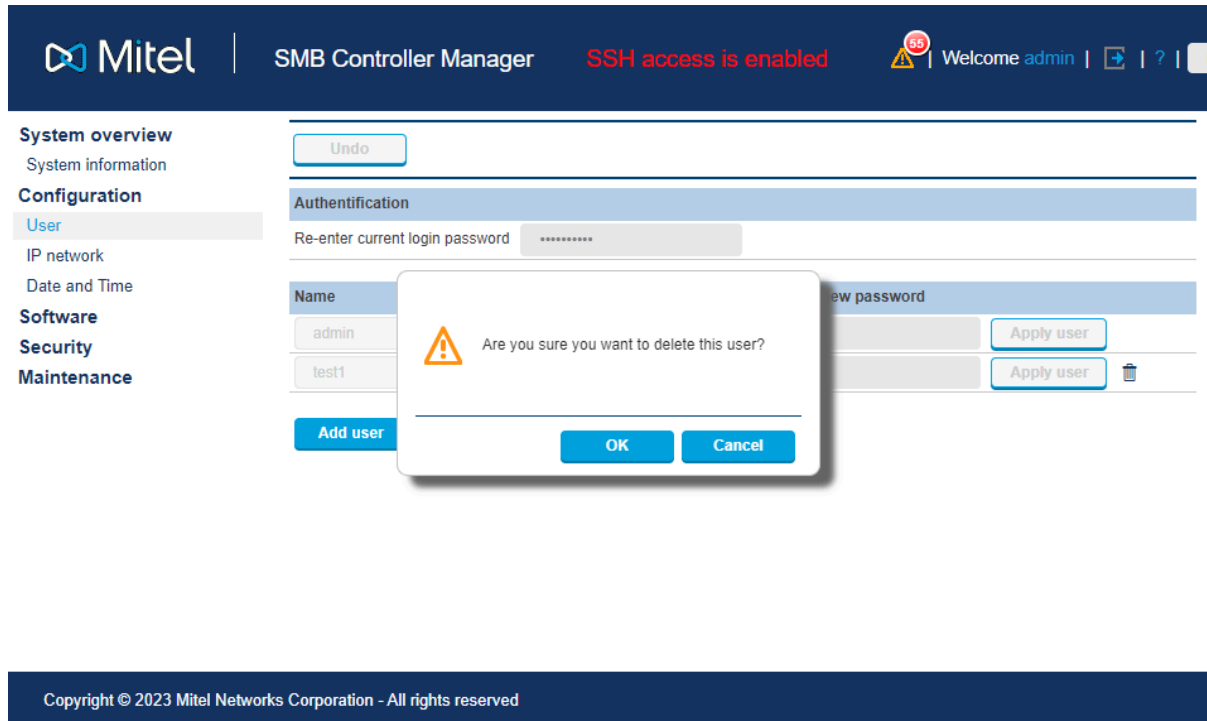
To delete an existing account (excluding the default admin account):

Note:

Self-deletion of the accounts are restricted.

You cannot delete the default "admin" user account of the system.

1. Log into the **Server Manager**, and navigate to **Configuration > Users**.
2. In the **Authentication** section, re-enter current login password to verify the authentication.
3. Click on the delete icon to the right of the account you want to delete.
4. In the confirmation box, click **OK**, to proceed with deleting the account.



Copyright © 2023 Mitel Networks Corporation - All rights reserved

11.6 Changing the IP Addresses

Typically, an Installation Technician would setup a lab network to mimic the customer network and deploy the SMBC there. If the IP Addresses need to be changed, however, follow these steps. Note that the optional WAN IP Address may not be available yet.

1. From a Programming PC on the same Subnet as the SMB Controller, log into MSL Server Manager at <https://<MSL IP Address>/server-manager>.
2. Ensure Remote Management is configured for the new network by selecting Remote Access. Ensure that the new network has at least some Subnet available to PCs that can connect and manage MSL.
3. Change the IP Address(es) of the MSL Container by selecting IP Settings and change the LAN IP address, the LAN Secondary IP address, and the WAN IP address (Optional).

Ensure the IP address are on the same subnet as the SMB Controller Manager.

4. Select **Save and Restart**.

Mitel Standard Linux | admin@mitel-networks-server.mitel.com | Status: Clear

Warning: Configure IP addresses before proceeding!

Warning: Internal Interface is disabled!

IP addresses and hostname settings

This panel allows you to configure server name and IP addresses.
Changes to these settings will require a restart.

The hostname must contain only letters, numbers and hyphens, and must start and end with a letter or number.

Hostname: mitel-networks-server
Domain: mitel.com

The IP address, Netmask and Gateway must be in the form #.#.#.# (each # is a number from 0 to 255).
Make sure the IP addresses are not in use by any other devices and the netmasks match your existing networks.

Internal Network Interface (LAN)

Enter the LAN IP Address

Optionally enter the MBG LAN IP Address

Enter the LAN Subnet Mask IP Address

Enter the LAN Default Gateway IP Address

Link status	Physical interface	Virtual interface	MAC address	IP address	Second IP address (Optional)	Netmask	Gateway (Router)
down	eth0			172.19.51.215		255.255.255.224	172.19.51.193

Previous Next

Mitel Standard Linux 11.0.105.2
© Mitel Networks Corporation

5. After a few minutes, log into the SMB Controller Manager at <https://<SMBC IP Address>:8443>.

6. Under **Configuration**, select **IP Network** and change the IP Address of the SMB Controller Manager.

7. Select **Apply**. The SMB Controller and MSL are now on the new network.

Mitel SMB Controller Manager | SSH access is enabled | Welcome admin | English

System overview
System information

Configuration
User
IP network
Date and Time

Software
Security
Maintenance

Apply Undo

Network settings

Host name	SMBCV2
Domain	
Primary DNS	8.8.8.8
Secondary DNS	4.4.4.4

Network interfaces

Name	Status	Carrier	DHCP	IP address	Subnet mask	Gateway	MTU	MAC address
eth0	☒	☒ (100/full)	☐	192.168.1.108	255.255.255.0	192.168.1.1	1500	08:00:0f10:6a:8a Default
eth1	☒	☒	☐			0.0.0.0	1500	08:00:0f10:6a:8b
eth2	☐	☒	☒				1500	08:00:0f10:6a:8c

> Subnets

> Static routes for eth0

Copyright © 2022 Mitel Networks Corporation - All rights reserved

8. For access, change the Subnet of the Programming PC to the new Subnet of the SMB Controller.

9. Ensure Trusted Networks are configured for the new network by selecting Networks. This is required if there are Applications/Phones on the internal LAN on a different Subnet that need to connect to MiVoice Business.

10. If required, add the WAN IP Address in the IP Address Panel.

11.7 Backup and Restore

Perform Solution Backups and Restores from the Server Manager. If you are backing up to or restoring from the Network, you must first configure the Network for the Backup and then configure the Network for the Restore. The Server Manager Backups and Restores include the data for all installed Applications, IP Network Settings, and so on.

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

Note:

While the Application Databases might be restored, the Applications may not be installed on the new Server Manager. When the Application is installed, its database will be restored from the saved database.

CAUTION:

The CloudLink Gateway blade data is not saved in MSL Backups.

11.7.1 Backup Using Server Manager

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

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

Network Backup and Restore

Initial Configuration Wizard will support Network Backup and Restore using the REST API for triggering the netbackup and netrestore.

The admin should configure the network backup in Server Manager before configuring the Initial Configuration Wizard. The Initial Configuration Wizard blade page in Server manager will perform a check to see if the network backup has been programmed, if not it will display an error explaining the problem and provide a link to the backup page within Server Manager. The launch of Initial Configuration Wizard will be prevented until the network backup has been configured.

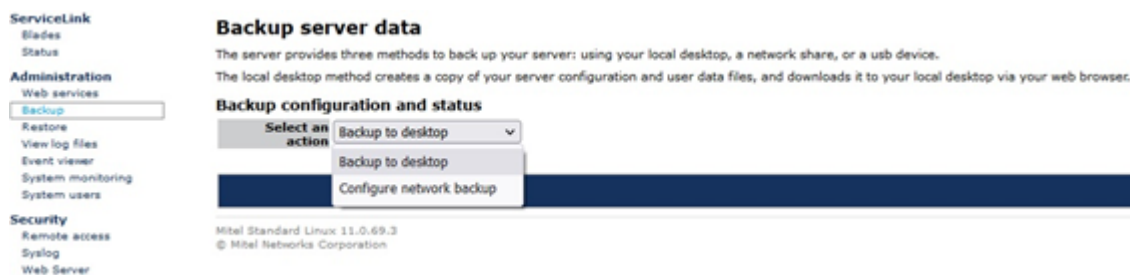
Note:

Before Initial Configuration Wizard performs any configuration, it will trigger a full backup. If any fatal error occurs during the configuration of Initial Configuration Wizard, then Initial Configuration Wizard will automatically restore this backup.

Once the Initial Configuration Wizard has successfully configured the system, a new backup will be created so that the post-Initial Configuration Wizard configuration state can also be saved.

To configure a network backup and restore:

1. Log into the **Server Manager**, and navigate to **Administration > Backup**.
2. In the **Backup server data** panel, from the **Select an action** drop-down, select **Configure network backup**.



3. Configure the network server.

Network Backups

Current system time: **Fri 12 Nov 2021 11:04:56 AM Universal**

Configure the server where the backup files will be stored. Then indicate the desired time and the frequency of the backups.

IP Address	
Username	
Password	
Domain or Workgroup Name	
Sharename	
(Optional) Sub Directory	
Maximum number of backup files to keep	10

Backup Schedule

☒ Disabled
☐ Daily Network backup time of day (hour/min) 2 00 AM
☐ Weekly Day of week Sunday
☐ Monthly Day of month 1

Backup Encryption

To encrypt the backup file enter an encryption password below. You will need to use this same password if you choose to restore this backup at a later date.

If you choose not to encrypt the backup file, leave the password fields blank. Be sure to store your backup in a secure location.

Warning: If the backup is protected by entering an encryption password and this password is forgotten, you will not be able to recover any data stored in the backup file.

Encryption Password:	
Encryption Password (verify):	

Mitel Standard Linux 11.0.69.3
© Mitel Networks Corporation

4. Make sure backup server details is reflecting in restore panel.

Make sure that the backup server details is reflected in **Restore** panel of the Server Manager.

11.7.2 Backup Using MiVoice Business System Administration Tool

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

Note:
The database backup generated from the System Administration Tool does not include the MiVoice Border Gateway or SMB Controller (host) database.

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

Note:
It is always recommended to do the backup/restore from MSL. For more details, see [MSL Installation and Administration Guide](#) on Mtel Document Center.

11.7.3 Restore Using Server Manager Backup

A previously backed up MSL Database, can be restored via the **Restore** panel in Server Manager.

Note:
MSL backup/restores are not portable between platforms. (for example, you cannot restore an AX/CX/ MXe or PRI, FSX, DSP,FXO MSL database on an SMB Controller).

11.7.4 Restore Using MiVoice Business System Administration Tool

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

Note:

It is always recommended to do the backup/restore from MSL. For more details, see [MSL Installation and Administration Guide](#) on Mitel Document Center.

11.8 Data Maintenance

11.9 Update Software

11.9.1 System software

SMB Controller system software

In some cases, it is necessary to reinstall the SMB Controller system software via the SMB Controller Manager (see [Update the SMB Controller system software](#)).

To update the MSL, see [Upgrading the MSL Container](#) on page 167.

If the SMB Controller Manager does not run anymore an Emergency Upload is required (see Emergency Upload of SMB Controller system software).

Note:

A factory reset of the SMB Controller system software or an Emergency Upload of the SMB Controller system software resets all MiVoice Business configuration data to the default values and deletes all audio data. Before you proceed to do a factory reset, create a backup of the configuration and audio data (see the chapter [Data backup](#)).

Emergency Upload of SMB Controller system software

Whenever a standard software upload of the SMB Controller system software via the SMB Controller Manager is not possible or has failed, you must carry out an Emergency Upload.

To perform an Emergency Upload, proceed as follows:

1. Set the SMB Controller to emergency mode using the control key (see Emergency mode). NOTE: If static IP address was set before, the SMB Controller should be reachable with the same IP address. Otherwise, you have to find the IP address of the SMB Controller as described in chapter Search for the SMB Controller in the IP network.
2. Open a browser window and enter the IP address of your SMB Controller including the port 8080 (Example: <http://10.100.98.43:8080>).

3. Log in with the default username (admin) and the default password (admin) for accessing the system in emergency mode.

The SMB Controller Manager is opened in a reduced emergency mode.

4. Load an SMB Controller system software (format: Mitel-SMBC_XXX-XXX.zip) and click Install.

The Emergency Upload is started.

11.9.2 Upgrading the MSL Container

The Mitel-MSL-Container software upgrade is performed from the SMB Controller Manager Software Applications page.

Note:

The MSL container in the SMB Controller Manager application is not the same as the MSL service link. MSL container only can be upgraded from SMB Controller Manager.

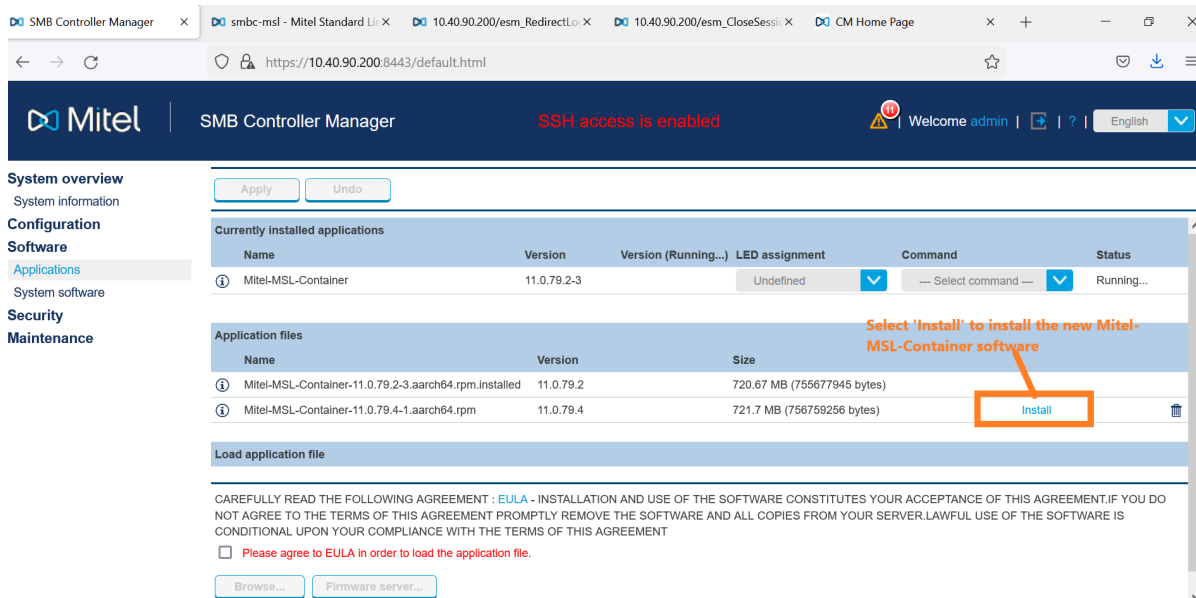
To upgrade the Container, the Administrator should follow these steps:

If a MiVoice Business Blade has been installed:

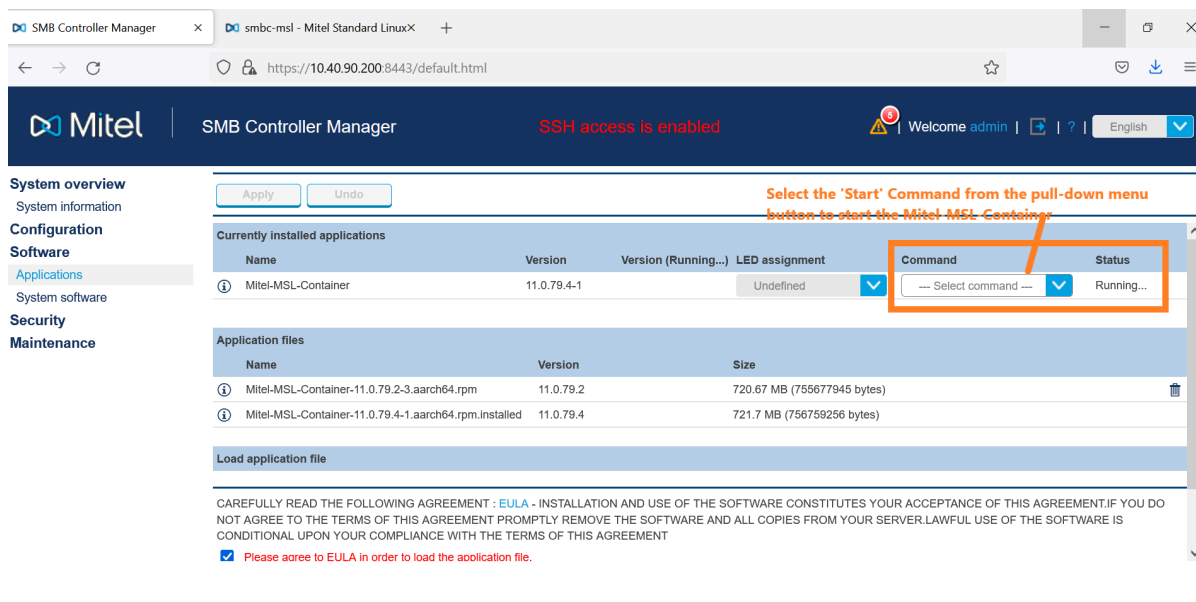
1. Sync the ARID from the Server Manager's Status Panel.
2. Log in to the MiVoice Business and issue a **RESET SYSTEM** Maintenance Command. The reboot enables the MiVoice Business to apply the Licenses.
3. Backup the Database from the Server Manager Backup. Although the upgrade automatically performs a Database Backup, this step is recommended in case the Mitel-MSL-Container upgrade fails.
4. Upgrade the Mitel-MSL-Container software by downloading the RPM from the Firmware Server in the SMB Controller Manager Software Application page.
5. After the RPM has loaded, select **Install** next to that RPM.

This will check to see if a prior MSL Container is already installed, and if so, trigger a Database Backup, install the new MSL, and trigger a Database Restore. Once the Server Manager has started, the

Administrator should ensure that the database has been restored. The Administrator should also remove the old MSL Container Application.



6. Once the RPM has been successfully loaded, the Mitel-MSL-Container can be started by selecting **Start** from the Command drop-down menu.



7. If the ARID previously synced, it should have been automatically synced with the AMC on startup of the Server Manager. If an ARID has not been synced with the AMC, then the Administrator must provide an ARID and perform the Sync from the Server Manager Status Panel.

The Blades Panel now displays the available Blades to install if the ARID has been successfully synced. The Administrator can now install the required Blades.

8. If the MiVoice Business Blade is installed after an MSL Container upgrade, a data restore should be automatically done as part of the blade installation. The Administrator should be able to browse to the MiVoice Business and to log in to ESM with the previously saved password.

If the MSL Container upgrade fails, the RPM can be loaded, installed, and started, as described in the installation instructions. Once the Server Manager is up, restore the MSL Database from the Restore Panel. The MiVoice Business Blade can then be installed from the Blades Panel. Again, the MiVoice Business database restore should be performed automatically as part of the blades installation.

11.10 Hardware Update

Hardware maintenance comprise of replacing cards, modules and terminals when there is a defect, or for an upgrade. Safety regulations must be observed, and the step-by-step procedure must be followed.

Note:

The mainboard cannot be removed. If the components on the mainboard are defective or permanently faulty, the entire communication server with the metal chassis must be replaced.

11.10.1 Prerequisites

The following steps applies for any maintenance activity which includes replacing the interface cards, system modules and the CPU module as well as to the mainboard of the SMB Controller itself.

First steps before cards are removed or added:

1. Inform all concerned users if the system has to be put out of operation during working time.
2. Shut down the SMB Controller (see [Shut-down mode](#)) and disconnect it from the power supply.
3. Wait at least 3 minutes to be sure that all components are discharged.

11.10.2 System Information

Some system information is stored separately on the CPU module. The information includes:

- The EID (Equipment Identification) serial number
- The system type
- The application software generation
- The IP address of the MiVoice Business communication server

The data on the MiVoice Business communication server is not deleted and remains available.

11.10.3 Disk Replacement

The SMB Controller does not have a field replaceable disk. The storage disk is soldered into the CPU card. When the storage disk fails, the CPU card needs to be replaced. This will also change the EID of the system (which is on the CPU Flash) which is used to license the MiVoice Business on SMB Controller.

Note:

Before opening the SMB Controller for any repair or troubleshooting, read the product information and [safety instructions](#) carefully.

To prevent damage to the components, always follow proper ESD procedures. This also applies to handling interface cards, processor cards, and system modules that are not inside ESD-protective wrapping.

If the EID changes, the admin will need to reset the hardware identifier from the AMC and re-sync the ARID from the server-manager. This may be the case if "disk replacements" are required on the SMB Controller.

Note:

In the unlikely event of a disk failure, the customer is requested to contact customer support to determine the best option to solve the issue. This may involve a replacement of a full base unit. Ensure that system backups are maintained to allow quick recovery of new hardware installation.

11.10.4 Replace Units

If the components on the controller unit needs to be replaced, the entire unit must be replaced.

Note:

Ensure that system backups are maintained to allow quick recovery of new hardware installation.

Note:

Before opening the SMB Controller for any repair or troubleshooting, read the product information and [safety instructions](#) carefully.

To prevent damage to the components, always follow proper ESD procedures. This also applies to handling interface cards, processor cards, and system modules that are not inside ESD-protective wrapping.

1. Order the new hardware unit for replacement.

2. If the replacement includes a new CPU card, the admin will need to reset the hardware identifier from the AMC and re-sync the ARID from the server-manager.
3. Install the new SMB Controller hardware, see [Hardware Installation](#) on page 28.
4. Remove the interface cards from the existing controller unit and install them on the new controller unit. See [Replacing a Defective Interface Card](#) on page 171.
5. Remove the DSP modules from the existing controller unit and install them on the new controller unit. See [Replace DSP Module](#) on page 173.
6. Configure the new SMB Controller, see [Deployment Steps for the MiVoice Business Solution on SMB Controller](#) on page 77.
7. Restore the database, see [Backup and Restore](#) on page 163.

11.10.5 Replace Interface Cards

The different card types, the number of slots and the maximum configuration are all determined by the system capacity (see the chapter Expansion Stages and System Capacity).

A number of rules have to be observed when fitting the cards (see Component mounting rules).

All configuration data is centrally stored in non-volatile Flash memory. This means that configuration data is preserved whenever a defective interface card has to be replaced by a new one.

11.10.5.1 Replacing a Defective Interface Card

A card is replaced by the same card type with the same number of ports.

Procedure:

**Note:**

Be sure to observe the Safety regulations.

1. Carry out preparations (see [Prerequisites](#) on page 169).
2. Remove the housing cover.
3. Remove the defective interface card by pressing the two lateral metal clamps outward at the same time and gently lifting the interface card.
4. Place the new interface card at a slight angle into the required slot (see [Fitting an interface card](#)).

Make sure the angled side of the interface card is facing backwards (that is, it must not project over the wiring adapter slots).

5. Carefully press the interface card downwards until the two lateral metal clamps engage.
6. Fit the housing cover.
7. Reconnect the system to the power supply.

11.10.5.2 New Card with Fewer Ports

A card is replaced by a similar card with fewer ports.

Procedure:

Change the card and put the system into operation again. Similar procedure as described in [Replacing a defective interface card](#).

The following data is deleted:

- The system and terminal configuration data of the terminals on the interfaces that are no longer present in the new configuration.
- The system configuration data of the network interfaces that are no longer present in the new configuration.

Note:

If the terminal configuration data of system terminals is deleted following the reconfiguration of a card, a warning message will appear beforehand to give you the possibility of cancelling the process. However, this is possible only if the configuration data of the original card was not already deleted beforehand.

11.10.5.3 New Card with More Ports

A card is replaced by a similar card with more ports.

Procedure:

1. Change the card and put the system into operation again. Similar procedure as described in [Replacing a defective interface card](#).
2. In the WebAdmin view *Cards and modules* (=4g) *Confirm* the new cards.
3. Configure new ports.

The system configuration data (User No., User configuration, and so on.) of the terminals on the new ports is created as new data (default values).

11.10.6 System Modules

The category system modules comprises the DSPX2 modules stacked in slot SM1.

The category system modules comprises the modules expandable as an option (DSP modules) and the mandatory RAM module.

11.10.6.1 Replace DSP Module

The following describes how to replace a DSP module if it is defective or how to replace it for another module type.

Procedure:

**Note:**

Be sure to observe the [Safety regulations](#).

1. Carry out preparations (see [Prerequisites](#) on page 169).
2. Remove the housing cover.
3. Remove the old or defective module by loosening the fastening screw and carefully pulling the module out vertically of the module slot.

**Note:**

If there are several modules fitted and the module to be replaced is not at the top most position, the spacing sleeves have to be loosened and the modules pulled. The order of the modules on the slot is relevant only if different types of modules are equipped.

4. Align the DSP Module into the DSP Slot and press down evenly on both connectors until they stop.
5. Secure the module with the fastening screw.
6. Fit the housing cover.
7. Reconnect the system to the power supply.

11.10.7 Mainboard

If the components on the mainboard are defective or permanently faulty, the entire communication server with the metal chassis must be replaced.

To replace the communication server, proceed as follows:

**CAUTION:**

Be sure to observe the [Safety regulations](#).

1. Back up the configuration data and audio data, if still possible.
2. Carry out preparations (see [Preparations](#)).

3. Remove the housing cover.
4. Remove the interface cards (see [Interface Cards](#)), the system modules (see [System modules](#)) and the wiring adapter.
5. Dismantle all the connected cables in such a way that the new communication server can be identically reconnected.

Note:

The mainboard is not dismantled. The entire unit is replaced.

6. The new communication server can now be reassembled, fitted and installed in the reverse sequence.
7. Power up the SMB Controller and upload the configuration data from a backup file back on to the communication server.

11.11 Monitor the eMMC Wear

This section provides crucial information about monitoring the wear and lifespan of the eMMC disk on the SMB Controller. This feature becomes essential due to the presence of an onboard MiVoice Border Gateway, which contributes to increased eMMC usage. The aim is to enable proactive monitoring, allowing for timely alerts to customers before potential outages occur.

The eMMC wear indication can be monitored from the Controller Manager.

1. Navigate to **Maintenance > Diagnostics**.
2. Under the **Flash disk usage** column, eMMC wear percentage is shown.
3. If the eMMC wear exceeds 90%, then the existing CPU card must be [replaced with a new CPU card](#).

Note:

The eMMC disk is not a replaceable unit, as it is embedded in the CPU card. If you want to replace the eMMC disk, you must replace the CPU card completely.

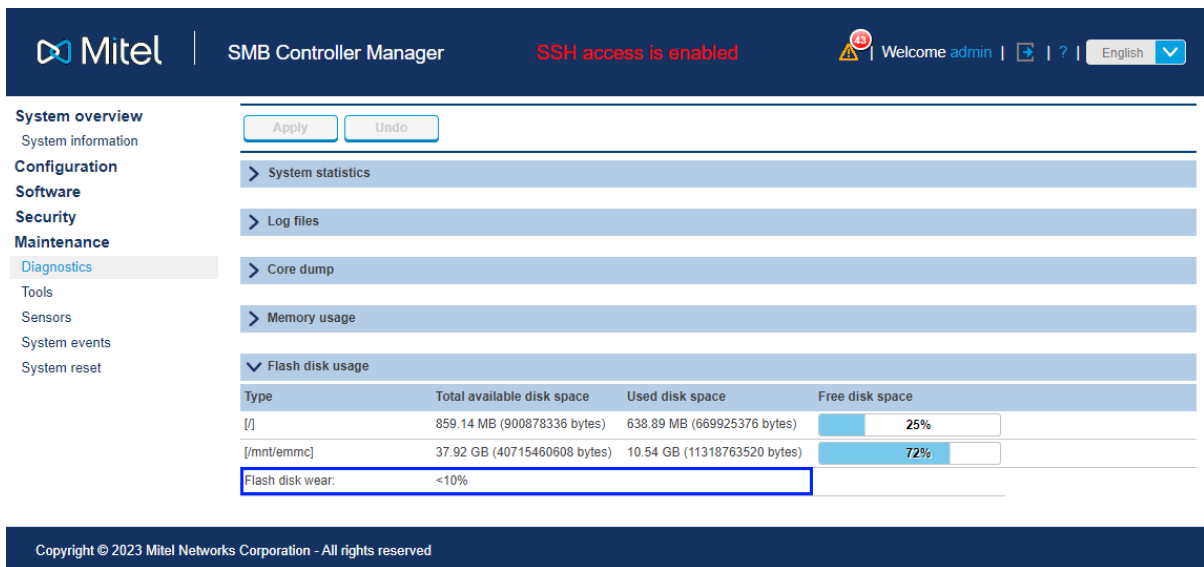


Figure 75: eMMC Wear Indication

Note:

If the eMMC wear exceeds 90%, a warning message will display: "Flash disk wear: >90% (Warning: 80% of spare blocks allocated)".

Important:

- The customer should monitor the wear regularly and replace the hardware when necessary.
- If the eMMC wear is reported as >90%, it is strongly recommended to replace the CPU Card to avoid any potential malfunctions. The eMMC is not a replaceable unit, it is embedded in the CPU card.
- The customer should take immediate action to address the wear by ordering a [replacement CPU Card](#) before the eMMC it fails. Aware that eMMC wear is a natural occurrence due to the number of read/write cycles the eMMC goes through.

This chapter contains the following sections:

- [Factory Default Static IP Address](#)
- [Factory Reset the SMB Controller](#)
- [Server Manager LAN IP is locked up from the Management PC](#)
- [SMB Controller Starts up Automatically](#)
- [Unable to Access the Server Manager/ESM](#)
- [Unable to Access the SMB Controller Manager Using the Default IP Address](#)
- [Unable to Access the SMB Controller Manager through web browser using IP address provided by DHCP Server](#)
- [Unable to log into the SMB Controller Manager](#)
- [Web Proxy to MiVB Intermittently Fails with a 503 Error](#)
- [Media Gateway Communications Error](#)

This chapter provides troubleshooting information for the SMB Controller, intended for use by Mitel certified technicians. For troubleshooting other general issues, see [MiVoice Business Troubleshooting Guide](#).

12.1 Factory Default Static IP Address

To temporarily set the IP address to its default value, so you can access the SMB controller using the default IP address. The IP configuration of the other IP interfaces (eth1, eth2,...) and all other data are preserved, only eth0 is impacted by the process.

If the IP address has not been changed in the interim, the SMB Controller will use the previous IP address from the database after a restart.

To temporarily set the IP address to its default value, follow the procedure:

1. Power up the SMB Controller.
2. There are two options:
 - A brand new or a factory reset SMB Controller starts with DHCP client enabled. If the communication server cannot find a DHCP server within 90 seconds, it deactivates the DHCP mode, and the system is then accessible via its default IP address. You can wait for 90 seconds and allow the SMB Controller to start in the Normal Mode, at which point the default IP address is set.
 - With the SMB Controller in Normal Mode or Emergency Mode, press the CTRL Button five times within 5 seconds.

Each time you press the CTRL Button, the F1 through F5 LEDs turn orange one-by-one.

After the fifth button press, the F1 through F5 LEDs are turned off and the F0 LED turns orange to indicate that the Default IP address is set.

3. Change the network adapter settings on the programming PC to the IP addresses *192.168.104.x* and the Subnet *255.255.255.0*. Do not use *192.168.104.13*. The below example uses *192.168.104.5*.

Internet Protocol Version 4 (TCP/IPv4) Properties [X]

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 104 . 5

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Figure 76: Configuring Programming PC to SMB Controller Default Subnet

4. Connect a Programming PC to the Eth0 Port.
5. You can now reach the SMB Controller from a Web Browser with the Default IP address *192.168.104.13*.

Note:

With the SMB Controller Manager now available, the system can be Factory Reset using the admin username and password if required.

12.2 Factory Reset the SMB Controller

A factory reset of the SMB Controller system software removes the MSL Container, and everything that was installed under the MSL container, all configuration data to the default values and deletes all audio data. Before you proceed to do a factory reset, take a backup of the MSL Container which includes all the configuration and audio data (see the chapter [Data backup](#)).

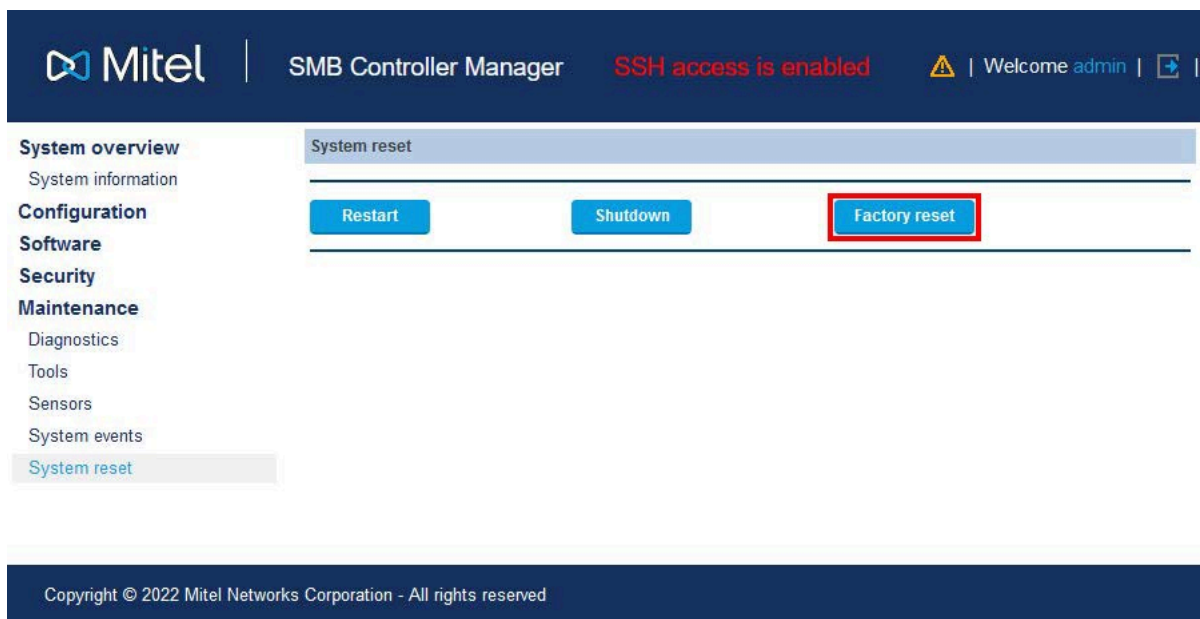
Note:

- A factory reset deletes all loaded or installed applications (inclusive the MiVoice Business application) and their configuration data from the SMB Controller. The LAN settings will be changed to DHCP. If you are performing the factory reset remotely, you must ensure that DHCP server is available for the subnet and that it has provisioned DHCP Option 6. Otherwise, the SMB Controller will default to its static IP address 192.168.104.13/24 and you will have to access the controller off the network as described in [Using the Factory Default IP Address](#).
- The factory reset is triggered immediately. All the active call and data connections are interrupted.

A factory reset of the SMB Controller is triggered in the SMB Controller Manager maintenance settings with the Factory reset button in the **System reset** view.

To factory reset the SMB Controller (Normal Mode):

1. Login to the SMB Controller Manager.
2. From the left panel, select the **Maintenance** section and then click **System reset**.
3. From the **System reset** window, click on the **Factory reset** button.



If you are unable to login to the SMB Controller Manager, see [Unable to log into the SMB Controller Manager](#) on page 182. Set the system to emergency mode, login to Controller Manager using the emergency mode username/password, and initiate a factory reset.

To factory reset the SMB Controller (Emergency Mode):

1. Set the SMB Controller into [Emergency Mode](#).
2. Login to the SMB Controller Manager using the default username and password.
3. From the left panel, select the **Maintenance** section and then click **System reset**.
4. From the **System reset** window, click on the **Factory reset** button.

12.3 Server Manager LAN IP is locked up from the Management PC

Symptom

- After initial configuration, the user was able to access the Server Manager from a local LAN IP address, but not anymore.
- During the initial configuration, the user is unable to access the Server Manager on its LAN IP address.

Remember that during the initial configuration, the user accesses the Server Manager from the IP address of the SMB Controller. Once the Server Manager LAN IP is configured, the user can access the Server Manager from the Server Manager LAN IP.

Possible Cause

The Server Manager LAN IP address is blocked.

Corrective Action

- If the Secure Shell (SSH) remote access is configured and enabled:

1. If the SSH is disabled, log into the Controller Manager as 'admin'.
2. Run the script:

```
sudo /opt/application/Mitel-MSL_Container/net-init
```

Note:

Wait until the command prompt returns after the script reconfigure all the MSL network settings in the Mitel MSL Container.

3. Exit the SSH.
4. (Optional) Disable the SSH in the Controller Manager. See step 13 of [Initial MSL Network Setup](#) on page 96.

Note:

SSH to the Controller Manager IP address is controlled by **Controller Manager > Security > Security settings**. SSH should be enabled only for troubleshooting and must be disabled immediately after use.

12.4 SMB Controller Starts up Automatically

Symptom

The SMB Controller starts up again automatically after shutting down.

Possible Cause

SMB Controller will restart in 90 seconds after reaching the shut-down mode and does not power down automatically.

Corrective Action

When the shut-down mode is reached, the SMB Controller can be disconnected from the power supply without concerns. The SMB Controller will remain in this mode for 90 seconds. For more details, see [Shut-down mode](#).

12.5 Unable to Access the Server Manager/ESM

Symptom

Unable to access the Server Manager/ESM.

Possible Cause

- Your computer might be on another subnet.
- Your computer might not be in a trusted network or in remote management network.

Corrective Action

- Ensure that your PC is on the same subnet of the SMB Controller.
- From a PC that is on a trusted network, add the computer network of the new PC to the trusted network list.
- From a PC that is on a trusted network, add your computer network to the remote management network.

12.6 Unable to Access the SMB Controller Manager Using the Default IP Address

Symptom

After configuring the SMB Controller to use its default IP address, the user is unable to access the SMB Controller Manager.

Possible Cause

- The SMB Controller not configured for default IP address.
- Your connecting PC might not be on a 192.168.104.0/24 subnet.

Corrective Action

- Try to access the SMB Controller Manager using the IP address provided by the DHCP server.

Disable the DHCP server. If the communication server cannot find a DHCP server within 90 seconds, it uses the IP address provided in the SMB Controller Manager. Try to access the SMB Controller Manager using the IP address provided in the SMB Controller Manager.

- Ensure that your PC's ethernet port is directly connected to the Eth0 port of the SMB Controller and that the PC's ethernet port is configured for 192.168.104.0/24 subnet of the SMB Controller
- Ensure that your subnet is routable to the SMBC subnet.
- Try to access the SMB Controller Manager using the correct IP address.

Reset the SMB Controller IP address to its default value. see, [Factory Default Static IP Address](#) on page 176.

12.7 Unable to Access the SMB Controller Manager through web browser using IP address provided by DHCP Server

Symptom

After configuring the SMB Controller to use DHCP to get its IP address, the user is unable to access the SMB Controller Manager.

Possible Cause

- The DHCP Server is not configured to provide DHCP option 6, Domain Name Server.

Corrective Action

- Provision DHCP option 6 on the DHCP server.

12.8 Unable to log into the SMB Controller Manager

Symptom

Unable to log into the SMB Controller Manager.

Possible Cause

Forgot or lost the SMB Controller Manager login credentials

Corrective Action

There is no way of recovering a forgotten Controller Manager admin password. Put the system into Emergency Mode, and login to Controller Manager using the emergency mode username/password

. See, [Factory Reset the SMB Controller](#) on page 178, and [Emergency Mode](#) on page 16. Use the **Factory Reset** option from the Web UI.

12.9 Web Proxy to MiVB Intermittently Fails with a 503 Error

Symptom

An error 503 - Service unavailable occurs when attempting to log into MiVoice Business through the MiVoice Border Gateway proxy from the internet.

Possible Cause

Marwatch MiVoice Border Gateway container admin password on the SMB Controller platform is incorrect.

Corrective Action

Update the server-manager admin password for the MiVoice Border Gateway container in Marwatch.

12.10 Media Gateway Communications Error

Symptom

Indicates communications error with the remoted Media Gateway.

Possible Causes

In general, remoted Media Gateway could crash if it encounters a condition it cannot handle. The crash as such generates a coredump file in /var/crash directory.

If the Media Gateway keeps continuously crashing, the reason for that could be incompatibility between MiVoice Business Blade version and SMB controller hardware version.

Corrective Actions

Make sure the installed MiVoice Business Blade version is compatible with SMB controller hardware version. Otherwise, upgrade the MiVoice Business Blade version, as well as the MSL Container version if necessary, to the minimum required version.

If the installed MiVoice Business Blade version is compatible with the SMB Controller hardware version, collect the SOS report and share it with the Product Support.

The system clears the alarm after the error condition is resolved and communication is re-established.

