MiCollab Installation and Maintenance Guide

- MiVoice Business
- MiVoice Office 250

RELEASE 8.1.1

DECEMBER 2018
NOTICE

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

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

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

Installation and Maintenance Guide
Release 8.1.1
December 2018
# Table of Contents

## CHAPTER 1: INTRODUCTION

- About MiCollab ............................................................... 3
- Deployment Configurations ............................................. 3
- Supported Communications Platforms .............................. 3
  - Platforms ................................................................. 3
  - Software Releases ..................................................... 3
- MiCollab Platforms ...................................................... 3
  - Industry Standard Server ........................................... 4
  - MiCollab Server Appliance ........................................... 4
  - MiCollab Virtual Appliance (vMiCollab) ......................... 4
- About the Mitel Integrated Configuration Wizard .................. 5
  - Overview ................................................................. 5
  - Supported Use Cases ................................................ 5
  - Unsupported Use Cases ............................................. 6
  - Requirements .......................................................... 6
  - A Note About Hunt Groups .......................................... 6
- About the Documentation Set .......................................... 7
  - MiCollab ................................................................. 7
  - MiCollab NuPoint Unified Messaging ............................. 8
  - Speech Auto Attendant .............................................. 8
  - Mitel Standard Linux ................................................ 8
  - MiVoice Border Gateway (Teleworker) ............................ 8
  - MiCollab Client ....................................................... 8
  - Mitel MiVoice Business Communications Platform ............. 8
  - Mitel MiVoice Office 250 Communications Platform .......... 8
  - Access MiCollab Product Documentation ....................... 9
  - Access Product Bulletins ............................................ 9

## CHAPTER 2: INSTALLATION & PROVISIONING WORK FLOW

- Getting Started ........................................................... 13
- Work flow ................................................................. 13
- Workflow Steps .......................................................... 14
  - Step 1: Obtain Licenses ............................................. 14
Step 2: Prepare Hardware Platform .................................................. 14
Step 3: Obtain Software ................................................................. 14
Step 4: Install or Deploy Operating Software .................................. 14
Step 5: Configure Operating Software ............................................ 14
Step 6: Install Application Software .............................................. 15
Step 7: Integrate MiCollab Client Database (optional) ..................... 15
Step 8: Perform Initial Configuration ............................................. 15
Step 9: Create or Update Users and Services Database ................. 15
Step 10: Configure System Application Settings .......................... 16
Step 11: Perform Backups ............................................................. 16
Step 12: Configure Integrated Directory Services ......................... 16

CHAPTER 3:
LICENSING

Introduction .................................................................................. 19
About AMC Licensing ................................................................. 19
   Requesting a New AMC Account .................................. 20
   Accessing your AMC Account ........................................ 20

UCC Licensing Procedure .............................................................
   Overview ................................................................. 21
   Deploying UCC Licenses ............................................... 21

Adding “à la carte” Licenses ........................................................... 29

CHAPTER 4:
INSTALL MICOLLAB SERVER

Overview .................................................................................. 33
Collect Site Information .............................................................. 34
Set Up Platform ...................................................................... 36
   MiCollab on Industry Standard Server .......................... 36
   MiCollab Server Appliance ........................................ 36
   MiCollab on Microsoft Hyper-V Virtual Machine ........ 38

Create Application Record ......................................................... 38

Obtain MSL and Application Software ...................................... 39
   Download Software ISO Files from Mitel OnLine ......... 39
   Software Downloads .................................................. 39
# Create Storage Media
- Option 1: Burn MSL ISO to CD/DVD and Copy Application ISO Images to USB Device
- Option 2: Burn Downloaded ISO Images to CD/DVDs

# Install MSL Operating System Software

# Configure the MSL Operating System
- Accept End User License
- Set Administrator Password
- Select System Timezone
- Configure Domain Name
- Configure System Name
- Enter Local Network Adapter
- Enter Local Networking Parameters
- Enable IPv6 Protocol and Address
- Select WAN Adapters
- Select Gateway IP Address
- Configure External Interface
- Configure DNS
- Activate Changes

# Install Application Software

# Configure MiCollab
- Log in to the Administrator Portal (Server Manager)
- Install Web Certificates
- Allow "Trusted Network" Access
- Set System Language
- Perform Initial Configuration of Applications

# Install MiCollab Server in LAN Mode with MiVoice Border Gateway Server(s)

## Prerequisites and Conditions

## CHAPTER 5:
**INSTALLING VIRTUAL MiCOLLAB IN A VMWARE ENVIRONMENT**

# Introduction

# About MiCollab Virtual Appliance

# Deployment Configurations
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Applications</td>
<td>57</td>
</tr>
<tr>
<td>Installation Checklist</td>
<td>57</td>
</tr>
<tr>
<td>MiCollab Virtual Appliance Installation</td>
<td>57</td>
</tr>
<tr>
<td>Review Installation Details</td>
<td>57</td>
</tr>
<tr>
<td>Requirements</td>
<td>57</td>
</tr>
<tr>
<td>Constraints</td>
<td>58</td>
</tr>
<tr>
<td>Collect Site Information</td>
<td>58</td>
</tr>
<tr>
<td>Collect Custom Template Information</td>
<td>60</td>
</tr>
<tr>
<td>Create MiCollab Application Record</td>
<td>63</td>
</tr>
<tr>
<td>Download MiCollab OVA file and Application Software</td>
<td>63</td>
</tr>
<tr>
<td>Software Downloads</td>
<td>63</td>
</tr>
<tr>
<td>Deploy vMiCollab vApp</td>
<td>64</td>
</tr>
<tr>
<td>Configure the MSL Operating System</td>
<td>64</td>
</tr>
<tr>
<td>Launch the MSL Server Console</td>
<td>64</td>
</tr>
<tr>
<td>Set Administrator Password</td>
<td>65</td>
</tr>
<tr>
<td>Select System Timezone</td>
<td>65</td>
</tr>
<tr>
<td>Configure Domain Name</td>
<td>65</td>
</tr>
<tr>
<td>Configure System Name</td>
<td>66</td>
</tr>
<tr>
<td>Enter Local Network Adapter</td>
<td>66</td>
</tr>
<tr>
<td>Enter Local Networking Parameters</td>
<td>66</td>
</tr>
<tr>
<td>Enable IPv6 Protocol and Address</td>
<td>67</td>
</tr>
<tr>
<td>Select WAN Adapters</td>
<td>67</td>
</tr>
<tr>
<td>Select Gateway IP Address</td>
<td>68</td>
</tr>
<tr>
<td>Configure External Interface</td>
<td>68</td>
</tr>
<tr>
<td>Configure DNS</td>
<td>69</td>
</tr>
<tr>
<td>Activate Changes</td>
<td>69</td>
</tr>
<tr>
<td>Enter Application Record ID and Reboot</td>
<td>69</td>
</tr>
<tr>
<td>Install Application Software</td>
<td>70</td>
</tr>
<tr>
<td>Configure vMiCollab</td>
<td>70</td>
</tr>
<tr>
<td>Log in to the Administrator Portal (Server Manager)</td>
<td>70</td>
</tr>
<tr>
<td>Install Web Certificate</td>
<td>71</td>
</tr>
<tr>
<td>Allow &quot;Trusted Network&quot; Access</td>
<td>72</td>
</tr>
<tr>
<td>Set System Language</td>
<td>73</td>
</tr>
<tr>
<td>Synchronize MiCollab Client server with MiCollab AWV Software Versions</td>
<td>74</td>
</tr>
</tbody>
</table>
Perform Initial Configuration of Applications .............................................. 74

CHAPTER 6:
INITIAL CONFIGURATION

Introduction ................................................................. 77
Collect Site Configuration Information .............................................. 77
Configure MiCollab Client Mode .................................................. 79
   CO-LOCATED MODE OR INTEGRATED MODE? ................................. 80
   Configuring Integrated Mode ...................................................... 81
      For MiCollab Server and vMiCollab Deployments: ......................... 81
Synchronize MiCollab Client server with MiCollab AWV Software Versions .......... 81
Configure Platform and Application Resources ..................................... 81
Configure Users and Services ..................................................... 82
   MiVoice Business Platform ....................................................... 82
   MiVoice Office 250 ................................................................. 82
Configure Flow Through Provisioning. ................................................. 82
System Requirements ............................................................. 83
Conditions ................................................................. 83
   Topology ......................................................................................... 85
   Departments and Locations .......................................................... 85
   Roles and Templates ................................................................. 86
   Users and Services ................................................................. 86
      Fully Qualified Domain Name (FQDN) for Cloud Deployments ........... 87
Configuration Overview ............................................................. 88
Greenfield: New MiCollab with one New MiVB Server ......................... 89
   Using MiCW .................................................................................. 89
   Manual Configuration ............................................................... 90
Greenfield: New MiCollab Server with Multiple New MiVB Servers ............. 91
   Using MiCW .................................................................................. 91
   Manual Configuration ............................................................... 92
Verify that Sharing has Started on MiCollab ........................................... 93
Check MiCollab Server Flow Through Provisioning Logs ......................... 94
Configure Integrated Directory Services .............................................. 94
Configure Application Settings .......................................................... 95
Backup Database ........................................................................... 95

CHAPTER 7:
MAINTENANCE

Upgrading MiCollab Software ................................................................. 99

Upgrade from MAS 5.0 or later to MiCollab 8.1 using Fresh Install .................. 99
  Prerequisites .................................................................................. 100
  Backup and Restore with Fresh Install .............................................. 100

Upgrade from vMAS 5.0 or later to vMiCollab 8.1 ........................................ 103
  Upgrade Prerequisites .................................................................. 103
  Deploy vMiCollab 8.1 OVA File and Restore Backup ......................... 103

Upgrade from MiCollab 8.x to MiCollab 8.y ............................................ 106

Upgrade vMiCollab Configuration ......................................................... 106

Installing Additional (Missing) Applications .......................................... 106
  Add Application from Server Manager .......................................... 106

Removing an Application during Initial Installation ......................... 107

Downgrading Application Software .................................................... 107

Performing Backups ...................................................................... 108
  Server Manager "Backup" .............................................................. 108
  Backup to Desktop ...................................................................... 108
  Schedule Backups to Network File Server ..................................... 109
  Server Manager SFTP Backup to Linux Servers ................................. 111
    Allow Access on the Backup Server ........................................... 111
    Configure an SFTP backup ......................................................... 111
  Server Console "Perform Backup" .................................................. 112
    Backing up to USB Device ......................................................... 112
    Backing up to Network File Server ........................................... 113
  Verify Backup Data ..................................................................... 113

Shutting Down MiCollab .................................................................... 114

Correcting Activation Errors .............................................................. 114

Accessing the Server Console ............................................................ 114
  About SSH (Secure Shell) ............................................................. 115
  Obtaining an SSH Client .............................................................. 116

Configuring Remote Management via MBG ....................................... 116

Viewing Log Files ........................................................................ 117
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Alarms</td>
<td>118</td>
</tr>
<tr>
<td>Conversions and Migrations</td>
<td>118</td>
</tr>
<tr>
<td>Convert a MiCollab Server Database to vMiCollab</td>
<td>118</td>
</tr>
<tr>
<td>Conditions and Constraints</td>
<td>118</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>119</td>
</tr>
<tr>
<td>Perform the Conversion</td>
<td>119</td>
</tr>
<tr>
<td>Migrate Standalone MiCollab Client to MiCollab Server or vMiCollab</td>
<td>121</td>
</tr>
<tr>
<td>Conditions and Constraints</td>
<td>121</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>121</td>
</tr>
<tr>
<td>Perform the Migration</td>
<td>122</td>
</tr>
<tr>
<td>CHAPTER 8: TROUBLESHOOTING</td>
<td></td>
</tr>
<tr>
<td>General Troubleshooting</td>
<td>127</td>
</tr>
<tr>
<td>Online Help Troubleshooting</td>
<td>131</td>
</tr>
<tr>
<td>Flow Through Provisioning Troubleshooting</td>
<td>131</td>
</tr>
<tr>
<td>vMiCollab Troubleshooting</td>
<td>133</td>
</tr>
<tr>
<td>Troubleshooting Applications</td>
<td>135</td>
</tr>
<tr>
<td>MiCollab AWV</td>
<td>135</td>
</tr>
<tr>
<td>Conferencing Error Messages for Alarm/Alert Conditions</td>
<td>142</td>
</tr>
<tr>
<td>MiCollab Client</td>
<td>143</td>
</tr>
<tr>
<td>MiVoice Border Gateway</td>
<td>144</td>
</tr>
<tr>
<td>NP-UM Troubleshooting</td>
<td>145</td>
</tr>
<tr>
<td>Google Apps Troubleshooting</td>
<td>146</td>
</tr>
<tr>
<td>Troubleshooting Licensing Errors</td>
<td>146</td>
</tr>
<tr>
<td>Troubleshooting UCC Licensing Upgrades</td>
<td>148</td>
</tr>
<tr>
<td>Troubleshooting Active Directory Problems</td>
<td>149</td>
</tr>
<tr>
<td>Problem</td>
<td>149</td>
</tr>
<tr>
<td>Possible Cause</td>
<td>149</td>
</tr>
<tr>
<td>Detecting Active Directory Delay</td>
<td>149</td>
</tr>
<tr>
<td>Corrective Action</td>
<td>151</td>
</tr>
<tr>
<td>Viewing/Collecting Log Files</td>
<td>151</td>
</tr>
<tr>
<td>Database Recovery (Restore)</td>
<td>151</td>
</tr>
<tr>
<td>Conditions and Constraints</td>
<td>151</td>
</tr>
<tr>
<td>Restoring a Database Backup</td>
<td>153</td>
</tr>
</tbody>
</table>
Access the Console Restore Menu .......................................................... 153
Restore From Another Running Server ............................................ 153
Restore From Network Share ............................................................. 154
Restore from Removable Device ....................................................... 154
Check Application Data ................................................................. 155
vMiCollab System Disaster Recovery .............................................. 155
Restoring a MiCollab Server Database to a Different Server ............ 155

APPENDIX A:
FLOW THROUGH PROVISIONING: ADDING GREENFIELD MICOLLAB TO GREENFIELD MIvb SERVERS

Overview .............................................................. 159
MiCW Use Cases .......................................................... 159
  Greenfield MiCollab with a Single Greenfield MiVB Platform ............ 159
  Run Wizard ............................................................ 159
  Greenfield MiCollab with a Single Existing MiVB Platform .......... 161
  Run Wizard ............................................................ 162
Adding Greenfield MiCollab To a New MiVB Cluster ......................... 164
  Initial Run of Wizard .................................................. 164
  Run Wizard FOR Each Additional MiVB Cluster Element .......... 166
  Last Run of Wizard Configures MiCollab ................................. 167
Greenfield MiCollab with Existing MiVB Cluster ............................ 170
  Before You Run the Wizard ............................................. 170
  Run the Wizard ........................................................ 170
  After Sharing is Started ................................................. 172

APPENDIX B:
FLOW THROUGH PROVISIONING: ADDING GREENFIELD MICOLLAB TO BROWNFIELD MIvb SERVERS

Overview .............................................................. 175
Prepare Site .............................................................. 175
  Run GDM Check and GDM Repair Commands ............................ 177
  Add Softphone Users .................................................... 178
  Migrate Full IP Users to Multi-Device User Groups ..................... 179
Obtain Licenses .......................................................... 179
Install MiCollab and Application Software .................................... 180
Provision the Network Elements ................................................. 180
Provision Application Resources .................................................. 181
Create Templates (and Roles) ................................................... 181
  Identify Users, Prime Numbers and Primary MiVoice Business .................. 182
  Identify the MiCollab Applications Service Mixes .................................. 183
  Identify Differences in the Application Service Configurations .................... 185
  Create Single-phone Templates for each User Type .................................. 186
Create CSV File and Import Using BUP ........................................... 187
Start Sharing with the MiCollab Server .......................................... 190
  Add MiCollab as Network Element ............................................... 190
  Start Sharing ............................................................................ 191
Run Reconcile Wizard .................................................................... 193
Flow Through Provisioning .......................................................... 195

APPENDIX C:
FLOW THROUGH PROVISIONING: BROWNFIELD MICOLLAB WITH BROWNFIELD MIVB SERVERS

Overview............................................................................... 198
Prepare Site ............................................................................. 199
Run GDM Check and GDM Repair Commands ..................................... 201
Start sharing with the MiCollab server ............................................ 202
Run Reconcile Wizard .................................................................. 205
Flow Through Provisioning .......................................................... 206

APPENDIX D:
FLOW THROUGH PROVISIONING: SHARING SCOPES

Supported Sharing Scopes ................................................................ 211

APPENDIX E:
OFF-LINE LICENSING AND INSTALLATION

Introduction ................................................................................ 214
Installation of vMiCollab Using Off-Line Licensing ............................... 214
Resetting The License Term ........................................................... 215
Adding Licenses ........................................................................... 216
Chapter 1

INTRODUCTION
ABOUT MICOLLAB

Mitel® MiCollab is a software solution that supports the co-residency of Mitel applications on the Mitel Standard Linux (MSL) operating system. MiCollab supports co-residency of multiple applications:
• on a single industry standard server, and
• within a virtual appliance (vApp) running in a virtualized environment.

MiCollab provides the following features for all applications:
• **Single sign-on**: a common login point
• **Administrator Portal**: a common portal for administrators to configure all applications
• **End User Portal**: a web interface portal for users to enter user-configurable information.

A base set of applications are provided in the base software package. You can then add uplift packages and add-on applications to enhance the base package. Refer to the *MiCollab Ordering Guide* for details.

DEPLOYMENT CONFIGURATIONS

Refer to the *MiCollab Engineering Guidelines* for details of the supported deployment configurations. These guidelines are available on the Mitel Customer documentation web site.

SUPPORTED COMMUNICATIONS PLATFORMS

**PLATFORMS**

MiCollab is supported for the following Mitel communications platforms:
• **MiVoice Business platforms**:
  - 3300 MXe
  - 3300 CX II and CXi II
  - MiVoice Business for Industry Standard Servers
  - MiVoice Business Virtual Appliance
• **MiVoice Office 250**

SOFTWARE RELEASES

Refer to the *MiCollab Engineering guidelines* for a table of the supported Mitel communication platform releases.

MICOLLAB PLATFORMS

MiCollab is available on the following platforms:
• Industry Standard Server
• MiCollab Server Appliance turnkey platform
MiCollab Installation and Maintenance Guide

- MiCollab Virtual Appliance running in a virtual environment

**Note:** System capacities and performance levels are dependent upon the type of MiCollab platform, the number of users, and the installed applications. Refer to *MiCollab System Capacities, Performance and Constraints* in the *MiCollab Engineering Guidelines* for details.

INDUSTRY STANDARD SERVER

This option is a small to mid-range business solution that can provide multiple MiCollab applications to up to 2500 users. Customers have the flexibility of purchasing their own MSL qualified server and then installing the MSL operating system software and MiCollab software on it. For server installations, refer to the MSL Qualified Hardware List for a list of the supported server platforms. To access this list:

2. Under **Applications and Solutions**, click **Mitel Standard Linux**.
3. Click **MSL Qualified Hardware List Rls 10.x**.

**Note:** MiCollab Release 7.0 and later software must be installed on a 64-bit server. It is not supported on a 32-bit server.

MICOLLAB SERVER APPLIANCE

This option provides a small business solution for up to 150 users. The MiCollab Server Appliance is a rack-mount Dell PowerEdge server with the MSL operating system software and MiCollab software pre-installed at Mitel. After the technician configures the server site-specific values, the MiCollab Server Appliance is ready to use. This option simplifies the installation process and reduces the time on site required to get the system up and running.

**Note:** The MiCollab Server Appliance is only available in North America and UK.

MICOLLAB VIRTUAL APPLIANCE (VMICOLLAB)

vMiCollab can be deployed

- on a virtual appliance (vApp) within the VMware vSphere Cloud Operating System, or
- on a Microsoft Hyper-V virtual machine.

MiCollab Virtual Appliance deployments on VMware are supported for

- small business multi-application
- mid-range business multi-application or single application sites
- enterprise multi-application sites
- enterprise single-application sites

MiCollab Virtual Appliance deployments on Hyper-V are supported for
• small business multi-application sites
• mid-range business multi-application or single application sites

Refer to the Virtual Appliance Deployment Guide for the virtual resource requirements.

ABOUT THE MITEL INTEGRATED CONFIGURATION WIZARD

OVERVIEW

The Mitel Integrated Configuration Wizard (MiCW) is a standalone software tool that allows you to perform initial configuration of the MiVoice Business and MiCollab systems. It supports the configuration of
• MiVoice Business clustering
• system data sharing between MiVoice Business platforms,
• user data sharing between MiCollab and MiVoice Business
• platform and system application resources, and
• roles and templates,

For MiCollab and MiVoice Business, the MiCW supports the configuration of the following application system resources:
• NuPoint Unified Messaging Voice Mail (to configure a user’s mailbox with additional options refer to the NuPoint Web Console help).
• MiVoice Border Gateway
• Speech Auto Attendant
• MiCollab AWV
• MiCollab Client.

The MiCW application software is only available from Mitel Online. You install the MiCW on a maintenance PC and enter data in the screens of wizard. The wizard creates a configuration file of the entered data that you apply to the MiCollab and MiVoice Business databases. You can run the wizard while the PC is connected to the MiCollab and the MiVoice Business platform or you can run it offline (while the PC is not connected). If you run the wizard offline, you must save the configuration file and apply it at a later time.

SUPPORTED USE CASES

You can use the Mitel Integrated Configuration Wizard to
• configure a new single MiVoice Business system and a new MiCollab system.
• configure of multiple new MiVoice Business systems with a new MiCollab system.
• configure of a single MiVoice Business system with multiple MiCollab servers. (Configure one MiCollab system per wizard session).
• start sharing and sync a MiVoice Business or MiVoice Business network with a MiCollab server to support Flow Through Provisioning.

See “Flow Through Provisioning: Adding Greenfield MiCollab to Greenfield MiVB Servers” on page 157 for specific instructions on how to use MiCW to configure MiCollab and MiVoice Business platforms.

**UNSupported USE CASES**

The MiCW does not support configuration of the following:

• multiple MiVoice Business systems beyond the first MiVoice Business in the cluster
• new applications on existing (pre-configured) MiVoice Business or MiCollab systems
• MiCollab users who will be synchronized with an IDS system. For MiCollab-IDS systems, you populate the user database by syncing it with the directory service and use Roles and Templates in the MiCollab Users and Services application to apply the licenses and services
• new services to existing MiCollab users
• MiCollab applications when data has been migrated from a standalone application. It is recommended that the application be used directly for configuration in this case
• standalone applications
• day-to-day administration
• MiVoice 5000, MiVoice MX-ONE, MiVoice Office 400, or MiVoice Office 250 platform configuration.

**REQUIREMENTS**

The following requirements apply to using the Mitel Integrated Configuration Wizard:

• MiCW 6.x.x.x supports MiCollab 8.0 with MiVoice Business 8.0 SP2
• PRI, BRI, T1/D4, and analog (non-dial-in) trunks only with the same answer point for all analog trunks

You must install the Mitel Integrated Configuration Wizard on a maintenance PC that is running the Windows 10, or Windows 8.x Pro operating system.

**Note:** For the MiCW, both 32-bit and 64-bit versions of these operating systems are supported.

**A NOTE ABOUT HUNT GROUPS**

Hunt groups must contain contiguous values if being provisioned from the MiCW; however MiCollab will support non-contiguous values if you program them manually on the MiVoice Business system and on the MiCollab application. It is recommended that you use contiguous values to facilitate troubleshooting. The important thing is to define the correct number of hunt group members, which you must derive from the MiCollab Engineering Guidelines document.
ABOUT THE DOCUMENTATION SET

The MiCollab documentation is available on the Mitel Customer Documentation web site.

MICOLLAB

- **MiCollab General Information Guide**: provides a high-level overview of the MiCollab product.
- **MiCollab Engineering Guidelines**: provides information about the characteristics, requirements, and performance of MiCollab and the supported applications.
- **MiCollab Order Guide**: provides licensing information and product part number lists.
- **Virtual Appliance Deployment Guide**: provides engineering guidelines for deploying Mitel products in a virtual infrastructure.
- **MiCollab Installation and Maintenance Guides**: provide instructions on how to install the MiCollab server and application software.
- **Platform Integration Guide**: provides instructions on how to configure the MiVoice Business and MiVoice Office 250 communication platforms to support the MiCollab applications.
- **Mitel Integrated Configuration Wizard Online Help**: provides instructions on how to use the wizard to perform initial configuration of the MiCollab and MiVoice Business.
- **MiCollab Client for Mobile Resiliency Guide**: provides information for configuring MiCollab for Mobile Client resiliency.
- **MiCollab Client Desktop MiNET Softphone - Server Independence Guide**: describes the behavior of the MiCollab Client Desktop MiNET Softphone when a user is logged into MiCollab Client and the MiCollab server is taken out of service. If the MiCollab server is taken out of service, for example due to an upgrade or hardware failure, the Desktop MiNET softphone continues to provide basic functionality.

Administrator

- **Server Manager help**: provides configuration, administration, and maintenance procedures for the MiCollab server. The MiCollab Integrated Directory Services functionality is described in this on-line help.
- **Users and Services help**: provides instructions on how to manage user data and assign or remove user services, such as MiVoice Border Gateway or Teleworker.
- **NuPoint Unified Messaging help**: is intended to help system administrators configure and maintain NuPoint Unified Messaging functionality through the web console interface.
- **MiCollab AWV help**: provides instructions on how to provision the conferencing application.
- **Mitel MetaDirectory help**: provides instructions on how to set up a Mitel Metadirectory. Mitel MetaDirectory is a Lightweight Directory Access Protocol (LDAP) server with intelligent services for comparing and presenting data. It collects employee and customers data from various sources and allows it to be searched efficiently.
End User

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

MICOLLAB NUPOINT UNIFIED MESSAGING

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

SPEECH AUTO ATTENDANT

- Refer to the *NuPoint Unified Messaging Help* for a description of the Speech Auto Attendant feature and for configuration instructions.

MITEL STANDARD LINUX

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

MIVVOICE BORDER GATEWAY (TELEWORKER)

- *Installation and Maintenance Guide with Web Proxy* describes the installation requirements and provides installation instructions for the MiVoice Border Gateway server.

MICOLLAB CLIENT

- *MiCollab Client Engineering Guidelines*
- *Administrator Guide* provides instructions on how to configure MiCollab Client on Mitel communications platforms.
- *Administrator Portal Online Help* provides information and instructions for the MiCollab Client Server administrator interface.
- *MiCollab Client Quick Reference Guide*

MITEL MIVOICE BUSINESS COMMUNICATIONS PLATFORM

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

MITEL MIVOICE OFFICE 250 COMMUNICATIONS PLATFORM

- *MiCollab Platform Integration Guide for MiVoice Office 250 platform* provides detailed instructions for integrating the NuPoint Unified Messaging software with the MiVoice Office 250.
ACCESS MICOLLAB PRODUCT DOCUMENTATION

To access MiCollab product documentation:

1. Log on to Mitel MiAccess (formerly known as Mitel Connect).
2. From the left menu, select eDocs.
3. Click Applications and then select MiCollab.

To access Mitel Knowledge Base articles:

1. Log on to Mitel MiAccess.
2. From the left menu, select Knowledge Management System. The Knowledge Base search engine opens.
3. Enter your application name in search area and click Search.

ACCESS PRODUCT BULLETINS

To access Mitel Product Bulletins:

1. Log on to Mitel MiAccess.
2. From the left menu, select InfoChannel.
3. Select Mitel - Worldwide in the drop down menu.
4. Click Products & Solutions and then select MiCollab.
5. Click Product Announcement/Bulletin (PA).
Chapter 2

INSTALLATION & PROVISIONING WORK FLOW
GETTING STARTED

1. Identify the following site requirements:
   - Deployment configuration (refer to the MiCollab Engineering Guidelines)
   - Applications
   - MiCollab platform
     - MiCollab Server
     - MiCollab Server Appliance
     - MiCollab Virtual Appliance (see the Virtual Appliance Deployment Guide)
   - Communications platform (“Supported Communications Platforms” on page 3)
   - Firewall Settings (Refer to the MiCollab Engineering Guidelines)

2. Identify the required base software part numbers and UCC user licenses. Refer to the MiCollab Ordering Guide.

3. Install and configure Mitel communication platform. See the Mitel Customer Documentation website to locate documentation for the communication platform.

4. Refer to the following diagram for an overview of the work flow steps.

WORK FLOW

The following figure summarizes the installation and provisioning workflow for MiCollab.
WORKFLOW STEPS

STEP 1: OBTAIN LICENSES

**Licenses:** Refer to “Licensing” on page 17 for MiCollab licensing requirements. Refer to the MiVoice Business Site Planning Guide, Engineering Guidelines, and Technician’s handbook for MiVoice Business licensing information.

STEP 2: PREPARE HARDWARE PLATFORM

**Communication Platform:** For new installs on a fresh site, install the communication platform and configure the system as per the documentation. Refer to the Mitel Customer Documentation web site at [http://edocs.mitel.com/default.htm](http://edocs.mitel.com/default.htm) for the latest documentation.

**MiCollab Server and MiCollab Server Appliance:** Ensure required licenses are available. Unpack the server platform. Connect installation laptop, or a physical monitor and keyboard to the network and to the MiCollab Server. Physically connect the server to network. For the Server Appliance, ensure that the default IP addresses do not conflict with an existing IP address on the network. If there is a conflict, you must change the default IP address via the MSL server manager console prior to connecting the Server Appliance to the network.

**MiCollab Virtual Appliance:** Ensure the virtualization environment meets the minimum specified requirements (see the Virtual Appliance Deployment Guide). Connect installation laptop to the network.

STEP 3: OBTAIN SOFTWARE

**MiCollab Server:** Download the Mitel Standard Linux (MSL) operating system software and MiCollab application software from Mitel Online and burn to DVDs or USB device.

**MiCollab Appliance Server:** MSL operating system and MiCollab application software are pre-installed.

**MiCollab Virtual Appliance:** For deployments on VMware vSphere, download MiCollab Virtual Appliance OVA file and optional application software to a network drive or to a folder on your vSphere Client PC. For deployments on Microsoft Hyper-V, download the MiCollab software and optional applications software.

STEP 4: INSTALL OR DEPLOY OPERATING SOFTWARE

**MiCollab Server:** Install MSL operating system software.

**MiCollab Appliance Server:** MSL operating system and application software are pre-installed.

**MiCollab Virtual Appliance:** For VMware vSphere environments deploy OVA file. For Microsoft Hyper-V, create the virtual machine with the required resources and install the MSL operating system software.

STEP 5: CONFIGURE OPERATING SOFTWARE

Configure and license MSL operating system software.
STEP 6: INSTALL APPLICATION SOFTWARE

**MiCollab Server**: Install application software from DVDs or USB device.

**MiCollab Appliance Server**: MSL operating system and MiCollab application software are pre-installed.

**MiCollab Virtual Appliance**: Install optional application software (for example, NP-UM options) from network drive or a client PC.

STEP 7: INTEGRATE MICOLLAB CLIENT DATABASE (OPTIONAL)

By default, MiCollab systems are in co-located mode.

For MiCollab systems with MiVoice Business platforms, you must configure MiCollab Client in integrated mode if Flow Through Provisioning is required. You use the MiCollab Client Integration Wizard to put a MiCollab system into integrated mode.

STEP 8: PERFORM INITIAL CONFIGURATION

**MiCollab with MiVoice Business**: Use the Mitel Integrated Configuration Wizard (MICW) to configure the platforms and system application resources. It can also be used to start sharing and synchronizing the data between the elements (required to support Flow Through Provisioning between MiCollab and MiVoice Business platforms).

**MiVoice Office 250**: Perform the required steps to integrate the communications platform with the MiCollab system. Refer to the *MiCollab Platform Integration Guide* for instructions.

- Configure application resources on the MiCollab system through the application administration interfaces.
- Configure the SIP trunking interfaces manually on the communication platform.

STEP 9: CREATE OR UPDATE USERS AND SERVICES DATABASE

Create or update the user and services database on the MiCollab system. If you are applying UCC licensing, use USP Roles and Templates to create MiCollab users.

There are several methods that you can use to provision a new MiCollab system with user and service data:

- **Flow Through Provisioning**: synchronizes updates made to the following data between the MiCollab and MiVoice Business system databases using System Data Synchronization (SDS).
- **Bulk User Provisioning Tool**: export a CSV or LDIF file of user entries from an existing communications platform and then import it into the MiCollab database using the Bulk User Provisioning Tool.
- **Manual Provisioning**: enter user data separately for each entry through the User and Services application.
- **Provisioning with IDS**: seed the Users and Services application database with the user entries and or corporate contacts from a site directory server database.
For each of the above provisioning methods, you can assign roles and templates to quickly configure user data.

**STEP 10: CONFIGURE SYSTEM APPLICATION SETTINGS**

Configure the MiCollab system application settings (for example, NP-UM ICP, NP-UM Line Groups, MiCollab AWV SIP server, and so forth) manually through the application administration interfaces. The application online help systems provide instructions on how to configure these settings.

**STEP 11: PERFORM BACKUPS**

Backup the MiCollab and communication platform databases to complete the installation.

**STEP 12: CONFIGURE INTEGRATED DIRECTORY SERVICES**

Optionally, configure Integrated Directory Services.
Chapter 3

LICENSING
INTRODUCTION

This section provides instructions on how to assign licenses to the system via the Mitel Application Management Center (AMC). Refer to the *MiCollab Order Guide* for licensing information.

MiCollab is licensed as a base package with a series of optional, add-on application user packages and system feature options. There are several base packages available depending on the required deployment model. Add-on user packages allow the licensed number of users to access the base package functionality.

The base package provides application software and basic free user licenses that allow customers to evaluate the MiCollab Client application. Customers then have the option of purchasing Unified Communications and Collaboration (UCC) and/or a la carte uplift license packages for the desired application(s) to increase capacity up to the supported system maximums as defined in the system capacity tables of the *MiCollab Engineering Guidelines*.

ABOUT AMC LICENSING

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

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

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

When you place a new order for products with the Mitel Customer Care Center, the order information is entered into the AMC system. The AMC places the purchased licenses into your licensing account for use in creating an application record. You must then log in to the AMC and create the application record; assign purchased products, features, and options to that application record; and then activate the customer’s Mitel Standard Linux (MSL) operating system (OS) before you can install the MiCollab application.

MiCollab uses the AMC to obtain licensing information, which is required for installing main base software, for installing upgrade software, and for installing system option upgrades. You must install MiCollab and then register it with the AMC online.

When you install MiCollab, MSL generates a unique Hardware ID that includes the MAC address of the server. When you connect to the AMC over the Internet, MSL uses the Hardware ID and the Application Record ID to communicate with the AMC to obtain licensing information (also called “sync”).
REQUESTING A NEW AMC ACCOUNT

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

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

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

ACCESSING YOUR AMC ACCOUNT

To access your account for the first time:

1. Go to the Mitel web site (http://www.mitel.com) and log in to your Mitel MiAccess account.
2. From the left menu, Click License Server AMC.
3. Select “Add a new AMC login”.

Figure 2: Log in to AMC
4. Enter your User ID and Password.
5. Click **Login**. For information about using the AMC, see the help.

## UCC LICENSING PROCEDURE

The Application Management Center distributes the platform and application user licenses that are contained within a Unified Communications and Collaboration (UCC) license bundle to the members of a Unified Licensing Manager (ULM) group.

### MiVoice Business Deployments

You add the following servers to a UCC License Manager group:

- 1 MiVoice Business Release 7.2 or higher OR 1 DLM
- 1 or more MiCollab Release 7.0 or higher systems
- 1 or more MBG Release 9.1 or higher systems

### OVERVIEW

The following is an overview of the main steps required to deploy UCC licenses to a site using the Applications Management Center (AMC):

- Create customer account.
- Register (purchase) products and licenses and assign them to the customer account.
- Create Application Record IDs for customer products.
- Assign base software licenses to system ARIDs.
- Set up the ULM (or DLM) group on the AMC.
- Add the system server ARIDs and GARIDs to the ULM Group.
- Assign licenses, including UCC user and SWAS licenses, to the ULM Group ARID.
- Synchronize the servers with the AMC to download licenses.

### DEPLOYING UCC LICENSES

*Note:* The screens shown in this procedure are examples only.

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

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

2. Create a Customer Account for each customer. Do not put multiple customers in a single customer account.
- Click **Customers**.
- Click the **Create Customer** button.
- Enter the end-customer information.
- Enter an e-mail address for the administrator contact.
- Enter an e-mail for the technician contact.

![Figure 3: Create Customer Account](image)

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

3. Register products and licenses for the customer site:

   - Click **Self service**.
   - Click **Register a License**.
   - Enter a Purchase Order reference number.
   - For deployments that include MiVoice Business, click + beside MiVoice Business Products. Enter the required MiVoice Business base software license and product licenses.

   **Note:** You can use the browser Find function to locate specific part numbers or license descriptions from the tables.

   - Click + beside MiCollab Products. Enter the required MiCollab base software license and product licenses.
   - Click + beside MiVoice Border Gateway Products. Enter the required standalone MBG base software license and product licenses.
   - Click + beside Mitel Unified Collaboration and Communication Products. Enter the
desired number of UCC User Licenses and the required SWAS licenses.
- Click **Next**.

**Figure 4: Selecting Licenses (Simple Example)**
4. Click **Confirm**. The system displays a list of the ordered products.

![Figure 5: Product Order List](image)

5. For integrations with MiVoice Business platforms, create Application Record IDs for your customer's MiCollab, standalone MBG, and MiVoice Business systems.

To create an ARID:

- Click **Customers**.
- Enter the name of the customer and click **Search**.
- Select the Customer ID of your customer from the Customer List and click **Create**.
- Enter a description for the Application Record (for example: ARID for AAA Corporation - MiCollab).
Licensing

25

- Click Submit.
- Click Commit. The system displays the ARID assigned to the system.
- Record the ARID.
- Repeat the above steps for each system.

6. Display the list of Application Records assigned to the customer:
   - Click Customers.
   - Enter the Customer name.
   - Click Search.
   - At the bottom of the screen, click to display a list of the ARIDs.

![Figure 6: List ARIDs](image)

7. For each system, assign the base software licenses to the system base ARIDs:
   - Click the Status icon .
   - Click the Assign Product link.
   - Enter the Purchase order number in the search criteria and click Search.
   - Click to display the Purchase order details.
- **Assign** the system's base software license to the base ARID.
- Click **Confirm** to assign the license.
- Review the licenses and record the ARID.
- Click **Done** or click **E-Mail** to notify to the administrator. You can send the notification to your technician or customer by including their email addresses.

![Assignment Confirmation - Transaction Report](image)

**Figure 7: Assign the MiCollab Base License**

8. In the Customer profile create an associated ULM Group ARID:
   - Click **Self service**.
   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name and then click **Search**.
   - Click **Add**.
   - For deployments with MiVoice Business, click the ULM button next to the MiVoice Business Base ARID.
   - Enter a description for the ULM Application Record. For example: "AAA Corporation ULM ARID".
   - Click **Submit**. The Application Record details are displayed
   - Click **Next**. The server ARIDs appear listed in the right frame of the Group Application Record.
9. Add the system server ARIDs to the ULM Group ARID:
   - Select the check boxes next to the ARIDs that you want to add.
   - Click **Add Selected Servers**.
   - Click **Add Selected Server**. The server ARIDs are added to the "ARIDs Managed by this ULM" list, and the AMC distributes the licenses to the ULM server members.
   - Click **Return to License Manager**.

**Figure 8: Create ULM Group ARID**
Figure 9: Group Application Record with Managed MiCollab ARID

10. Assign the MiVoice Business SIP trunk licenses, MBG SIP trunk licenses, UCC User and SWAS licenses to the ULM ARID:
   - Click Customers.
   - Enter the Customer name and then click Search.
   - Click beside the customer’s ID.
- Click the Status button next to the ULM ARID (for example, "AAA Corporation ULM Record").
- Click the Assign Product link.
- Enter the Purchase order number and click Search.
- Click to expand the Purchase order.
- Assign the licenses to the ULM ARID.
- Click Assign.
- Click Allocate to assign the licenses.
- Review the licenses and record the ARID.
- Click Confirm.
- Click Done.

11. Log into each member server or platform and sync with the AMC. During the sync, the AMC distributes the licenses to the servers:

**CAUTION:** After you sync a server ARID with the ULM group, you cannot remove it.

- Sync the MiCollab and MBG servers from the Status page in the Server Manager interface. You can sync the MiCollab and MBG server ARIDs in any order. All the UCC MBG license options are provided to MiCollab in the group. The MBG standalone does not get any direct UCC license options.
- Sync each MiVoice Business or DLM platform by clicking Retrieve Licenses in the License and Options Selection form of the System Administration Tool.

12. For MiVoice Business deployments, assign the UCC licenses to users through the MiCollab Users and Services application. See Managing UCC licenses in the USP online help for instructions.

### ADDING "À LA CARTE" LICENSES

To purchase and activate additional feature, user, port, trunk, or language licenses:

1. Order the required licenses from the Mitel Online Store. A new Application Record ID is sent to your AMC account.

2. In your AMC account, access the appropriate Application Record and assign the upgrade products from your license account to the Application Record. Assign any MiVoice Business User and Services licenses to the MiVoice Business ICP Application Record. The AMC upgrades your licenses on its hourly synchronization.

3. Access the server manager. See “Log in to the Administrator Portal (Server Manager)” on page 49.

4. Under ServiceLink, click Status.

5. Click the Sync button to download your AMC license upgrades.

- Teleworker and MiCollab AWV licenses are applied automatically during the synchronization.
- If you have downloaded NP-UM, SAA, or MiCollab AWV licenses, perform a system reboot to activate the new licenses.
- If you have downloaded new NP-UM language licenses, access the Users and Services
application. A warning message is displayed at the top of the Users and Services page indicating that you must enable the languages. Click **Enable**. The MiCollab system services are restarted. After a short delay, the system returns to service. Then, assign the new system language from the server manager in the MiCollab Language page of the server manager.

- The Licensing page in the server manager shows the licensing counts. The UCC licensing bundles are listed at the top of the page; the "à la carte" license counts are listed below.

**Notes:**

- If you are moving Teleworker from an existing standalone deployment to a new MiCollab Software Base deployment, apply the appropriate upgrade license to the standalone Application Record to convert it to a MiCollab Application Record. All client licenses that are currently assigned to the standalone Application Record are retained.

- When purchasing additional MiCollab NuPoint Unified Messaging licenses, ensure that you order the MiCollab version of the license, if a MiCollab version is available. If a MiCollab version of a NuPoint Unified Messaging license is not available, use the NP-UM standalone version.

- After adding new NP-UM or MiCollab AWV licenses and synchronizing with the AMC, you must reboot to update the system with the license changes.

- Moving a NuPoint Unified Messaging standalone deployment to MiCollab is not supported.
Chapter 4

INSTALL MICOLLAB SERVER
OVERVIEW

This section provides instructions for installing

- the MiCollab system software on a qualified industry standard server (sourced from the Mitel Qualified Hardware List)
- the MiCollab Server Appliance
- the MiCollab system software on a Microsoft Hyper-V virtual machine.

**Note:** If you are upgrading from a previous release, see “Upgrading MiCollab Software” on page 99. If you are installing vMiCollab, see “Installing Virtual MiCollab in a VMware Environment” on page 55.

If you are installing a MiCollab Server Appliance, you do not perform several of the installation steps (noted in the table below), because the MSL operating system and application software are pre-installed on the server.

Installation consists of the following steps:

- Collect Site Information
- Set up Platform
- Create Application Record
- Obtain MSL and MiCollab Application software - (not required for MiCollab Server Appliance)
- Install MSL Operating System software - (not required for MiCollab Server Appliance)
- Configure the MSL Operating System
- Install Application Software - (not required if installing a MiCollab Server Appliance)
- Configure MiCollab
- Perform Initial Configuration of Applications (See “Initial Configuration” on page 75).
- Integrate or Co-locate MiCollab Client Database? (See “Configure MiCollab Client Mode” on page 79).
**COLLECT SITE INFORMATION**

The following table itemizes the information you will need to enter during software installation and configuration. For an efficient installation, gather this information before you start:

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NOTES</th>
<th>ENTER YOUR INFORMATION HERE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiCollab Server or MiCollab Server Appliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Administrator Password</td>
<td>For password strength, choose a password that contains a mix of uppercase and lowercase letters, numbers, and punctuation characters. For more information, see page 43.</td>
<td></td>
</tr>
<tr>
<td>2. Domain Name</td>
<td>Names must start with a letter; can contain letters, numbers, and hyphens. For more information, see page 43.</td>
<td></td>
</tr>
<tr>
<td>3. System Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. IP address of your MiCollab server (LAN mode)</td>
<td>The local IP address of the server where you are installing MiCollab.</td>
<td></td>
</tr>
<tr>
<td>4b. IP address of your external NIC (Network Edge mode)</td>
<td>The IP address of your external Ethernet connection.</td>
<td></td>
</tr>
<tr>
<td>5. External Interface Connection</td>
<td>Cable Modem? You need to know if the ISP supplies an account name or an Ethernet address.</td>
<td>Account Name or Ethernet Address?</td>
</tr>
<tr>
<td></td>
<td>Direct Connection? You need to know the static IP address.</td>
<td></td>
</tr>
<tr>
<td>6. Gateway IP address</td>
<td>The IP address that MiCollab will use to access the network.</td>
<td></td>
</tr>
</tbody>
</table>

Page 1 of 2
7. **MiCollab AWV IP Addresses**

   There are two different configuration methods for providing access to the AWV application (installed on the MiCollab Server) from outside of the customer firewall.
   
   - For two external IP configuration: In the AWV configuration with two external IP address, obtain two external IP addresses from your Internet Service Provider (ISP). One IP address is required for the web server interface that is used to set up audio conferences. A second IP address is required for the web service that provides the conference functions, such as file sharing, desktop collaboration, keyboard chat, and so forth).
   
   - For single external IP configuration: In the AWV configuration with one external IP address, the External Port is configured with 4443. This directs the external clients to reach the Connection Point using port 4443. The result is, the connection to the web conferencing portal will be requested on port 443, and the connection to the Connection Point component will be requested on port 4443.

   For information on configuring the MiCollab AWV IP addresses based on the configuration used, see the *MiCollab Engineering Guidelines* document.

8. **Will the MiCollab (MSL) server be supplying DHCP services?**

   If the MiCollab server will supply the DHCP services, you need to provide the range of IP addresses that the server can distribute. For more information, see page 46.

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

9. **DNS Server IP address**

   Enter the IP address of your corporate DNS server. **Note:** If your DNS is supplied by your ISP, leave this setting blank.

10. **Application Record ID #**

    Create an Application Record for the MiCollab installation in your AMC license account. You will use the ID number of this Application Record to activate your MSL license. See “About AMC Licensing” on page 19 for more information. Record the generated Application Record ID.

   ---

   **“Trusted Network” Access**

   If your PBX platform or some of your users are not on the same subnet as the MiCollab server, you need to classify them as "Trusted Networks" and then allow them access.

11. **Network Address**

    The IP address of the network for which you want to allow access.

12. **Subnet mask or network prefix**

    The dot-decimal subnet mask or CIDR network prefix for the range of IP addresses you wish to allow.

13. **Router Address**

    The address of the router/gateway you will use to access the network (or subnet) to which you are granting access.
SET UP PLATFORM

MICOLLAB ON INDUSTRY STANDARD SERVER

MiCollab runs on the Mitel Standard Linux (MSL) operating system. MiCollab Server is supported on industry standard (64-bit only), hardware redundant servers. The MSL Qualified Hardware List identifies third-party manufacturer server platforms on which you can install MiCollab. Follow the manufacturer’s instructions to set up the server hardware.

To access the MSL Qualified Hardware List:
1. Go to the Mitel Customer Documentation site at http://edocs.mitel.com
2. Under Applications menu, click Mitel Standard Linux.
3. Click MSL Qualified Hardware List (PDF Version) to launch the wizard.

Note: Your server model may require modifications to the BIOS settings. If modifications are required, they will be specified in the MSL Qualified Hardware List.

Note: MiCollab Release 7.0 and later software must be installed on a 64-bit server. It is not supported on a 32-bit server.

MICOLLAB SERVER APPLIANCE

The MiCollab Server Appliance software is shipped from the factory installed on a Dell™ PowerEdge™ Rack Mount Server which includes the following:

- Intel Dual Core Microprocessor
- 8GB Error Correcting Memory
- Non-redundant 250GB (min.) SATA Hard Disk Drive
- Non-redundant Power Supply
- Dual Port Motherboard Embedded 1GB Ethernet Adapter
- Internal Optical Drive.
Follow the manufacturer’s instructions to set up the server hardware. The server BIOS comes pre-configured from Mitel Manufacturing. Should the BIOS settings become altered, verify the following table for key settings:

<table>
<thead>
<tr>
<th>BIOS SETTING</th>
<th>REQUIRED SETTINGS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main Menu =&gt; System Time Set to site time zone</td>
<td>Set to site time zone</td>
</tr>
<tr>
<td>Main Menu =&gt; System Date</td>
<td>Set to current date</td>
</tr>
<tr>
<td>Memory Settings =&gt; System Memory Testing</td>
<td>Enabled</td>
</tr>
<tr>
<td>Processor Settings =&gt; Logical Processor</td>
<td>Enabled</td>
</tr>
<tr>
<td>Processor Settings =&gt; Virtualization Technology</td>
<td>Disabled</td>
</tr>
<tr>
<td>Processor Settings =&gt; C States</td>
<td>Disabled</td>
</tr>
<tr>
<td>Processor Settings =&gt; Number of Cores per Processor</td>
<td>All</td>
</tr>
<tr>
<td>SATA Settings =&gt; SATA Controller</td>
<td>AHCI</td>
</tr>
<tr>
<td>Boot Settings =&gt; Boot Mode</td>
<td>BIOS</td>
</tr>
</tbody>
</table>
MICOLLAB ON MICROSOFT HYPER-V VIRTUAL MACHINE

Refer to the to Virtual Appliance Deployment Guide for the Microsoft Hyper-V virtual machine requirements. After you have created the Hyper-V virtual machine, follow the same installation procedure that you would use for a physical system except with a virtual product license assigned to the ARID.

Note that when you install Mitel products on Hyper-V, USB is not supported. Therefore, you must download the ISO images of the application software (for example, MSL, NPM, AWV, MBG and so forth) and either create installation disks, or copy the ISO images to a network share and mount them during installation.

CREATE APPLICATION RECORD

Create an Application Record (ARID) for this MiCollab installation in your AMC license account. You will use the ID number of this Application Record to activate your MiCollab license. See “About AMC Licensing” on page 19 for more information.

If your MiCollab system requires NuPoint Speech Auto Attendant, ensure that your ARID includes the following licensing options:

- 324: NuPoint Text To Speech Ports
- 326: Speech Ports

If these options are not enabled, the MiCollab installation screen does not list Speech Auto Attendant as an installable application.
OBTAIN MSL AND APPLICATION SOFTWARE

Note: If you are installing the MiCollab Server Appliance, skip this section. The MSL operating system and your MiCollab application software are pre-installed on a MiCollab Server Appliance.

Note: For installation on Hyper-V, USB is not supported. Therefore, you must create installation disks or copy the ISO images to a network share and mount them during installation.

MiCollab applications are installed as a product rather than as a collection of separate software blades.

If you can connect to the Application Management Center (AMC) over the internet from the site, you can install the system software directly from the AMC. The only exception is the NP-UM applications which cannot be installed directly from the AMC. However, they can be downloaded to a network share and installed.

If the site does not allow you access to the internet, or if you will be installing multiple sites, download the system software and create storage media (USB or CD/DVD).

DOWNLOAD SOFTWARE ISO FILES FROM MITEL ONLINE

You can download and copy the applications to portable storage media (USB device or CD/DVDs) and then install the software from the storage media onto the MiCollab server:

- If you install from a USB device the installation wizard simply copies the required applications, based on your Application Record ID, directly to the server hard disk. Therefore, when you use a USB device, it is faster than installing from CD/DVDs.
- If you install from CD/DVDs the installation wizard prompts you, based on your Application Record ID, to copy the required applications from the storage media into the system cache. Although, you can choose to not install an application, the applications are meant to be installed together. After all the applications are saved in system cache, the system copies the software to the server hard disk.

Before you can install MiCollab, you must obtain the MSL and MiCollab application software files. All the software installation components are available for download from Mitel MiAccess. After you obtain the files, you transfer the files to a portable storage media (CD/DVDs or USB device)

When you download the ISO files, a MD5 checksum file is also provided to verify that the download of the ISO file was successful. The MSL operating system also provides a server console menu option that allows you to MD5 checksum the contents of an inserted CD/DVD or USB device.

SOFTWARE DOWNLOADS

1. Log on to Mitel MiAccess (formerly known as Mitel Connect).
2. From left menu, select Software Downloads Center.
3. Click MiCollab.
4. Click the appropriate MiCollab Software Download version (for example select MiCollab 8.1.x.x).
6. Download the MSL, applications, and prompts software for your deployment by clicking the file links in the table. When you click a link, you are presented with a software Disclaimer.
7. Click the "I Agree [Download using Software Download Manager (Recommended)]".
8. If you don’t already have the Download Manager installed on your local PC, you are prompted to install it. The Download Manager is an Active X application that optimizes the software download speed. After you install the Download Manager, it is available for subsequent software downloads.
9. Save the downloaded software ISO images to a folder on your maintenance PC.

CREATE STORAGE MEDIA

After you download the MSL and application software, either
- burn the MSL ISO file to a CD/DVD and copy the application ISO files to a USB device of 8 GB minimum (Note that installing the application software from USB is not supported for installations on Hyper-V virtual machines).

OR
- burn each ISO file to a CD/DVD or USB device as an image (not simply copy the ISO files to the CD/DVD).

**Note:** The installation of the software is quicker if you can install the application files from a USB device.

OPTION 1: BURN MSL ISO TO CD/DVD AND COPY APPLICATION ISO IMAGES TO USB DEVICE

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

<table>
<thead>
<tr>
<th>LABEL</th>
<th>CD/DVD</th>
<th>FILE NAME DOWNLOADED</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD/DVD1</td>
<td>MSL 10.6 for MiCollab Servers</td>
<td>MSL_10.6.xx.0.i686.iso (64-bit version only)</td>
</tr>
</tbody>
</table>

3. Copy the software application images to a USB device (minimum size 8 GB). Do not change the names of the files.

<table>
<thead>
<tr>
<th>APPLICATION SOFTWARE</th>
<th>FILE NAME DOWNLOADED</th>
<th>APPROX FILE SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiCollab Application Services</td>
<td>SAS_8.1.x.xx.0.iso</td>
<td>260 MB</td>
</tr>
<tr>
<td>MiVoice Border Gateway</td>
<td>MBG_10.1.x.xx.0.iso</td>
<td>98 MB</td>
</tr>
<tr>
<td>MiCollab Client Service</td>
<td>MiCollab Client_8.1.x.x.iso</td>
<td>283 MB</td>
</tr>
</tbody>
</table>
OPTION 2: BURN DOWNLOADED ISO IMAGES TO CD/DVDS

You will require up to nine, blank, formatted CDs or DVDs. Note that the NP-UM ISO file and SAA-TTS.iso file must be burned to separate DVDs. These applications are too large for CDs. The other software images can be copied to CDs or DVDs. Each CD/DVD must be labelled with the ISO file name. The MiCollab installation script uses the ISO file name to request the software.

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

<table>
<thead>
<tr>
<th>LABEL</th>
<th>CD/DVD CONTENT</th>
<th>FILE NAME DOWNLOADED</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD/DVD1</td>
<td>MSL 10.6 for MiCollab Servers</td>
<td>MSL_10.6.xx.0.i686.iso (64-bit version only)</td>
</tr>
<tr>
<td>CD/DVD2</td>
<td>MiCollab Application Services</td>
<td>SAS_8.1.x.xx.0.iso</td>
</tr>
<tr>
<td>DVD3</td>
<td>NuPoint Unified Messaging (includes Speech to Text option)</td>
<td>NPM_Blades-DVD_1_19.1.x.xx-01.iso</td>
</tr>
<tr>
<td>DVD4</td>
<td>Speech Auto Attendant - Text to Speech</td>
<td>NPM_Blades-DVD_2_19.1.x.xx-01.iso</td>
</tr>
<tr>
<td>CD/DVD5</td>
<td>MiCollab Audio, Web and Video Conferencing</td>
<td>AWV_8.1.x.xx.iso</td>
</tr>
<tr>
<td>CD/DVD6</td>
<td>MiVoice Border Gateway</td>
<td>MBG_10.1.x.xx.0.iso</td>
</tr>
<tr>
<td>CD/DVD7</td>
<td>MiCollab Client Service</td>
<td>MiCollab Client_8.1.x.x.iso</td>
</tr>
<tr>
<td>CD/DVD8</td>
<td>MiCollab Client Deployment</td>
<td>MiCollab Client Deploy_8.1.x.x</td>
</tr>
</tbody>
</table>

INSTALL MSL OPERATING SYSTEM SOFTWARE

During the install, if you accidentally exit from the server console, you can use Secure Shell (SSH) to access the server console again (see “Accessing the Server Console” on page 114 for details).

**This procedure applies to initial installations of MiCollab software only.** If you are upgrading from a previous version of MiCollab, please ensure that you have a backup and then refer to “Upgrading MiCollab Software” on page 99 for upgrade instructions.

It takes approximately 15 minutes to install the MSL operating system software.
1. Insert the MSL software CD/DVD that you labeled as MSL_10.6.xx.0.iso in the CD/DVD drive of the server.

2. Reboot the server.
   - To reboot the server, press the server **Reset** button
   - After the server reboots, the server console launches, you are presented with the installation choices.

3. Select the following software load:
   - **MSL 10.6.xx.x SL** for a MiCollab Server

4. Depending on your model of CD/DVD drive, you may be prompted to select the installation language. Use the Space bar on the keyboard to select the desired language and select **Ok**.

5. Choose your preferred keyboard from the list (default is **us**).

6. You are prompted to test the CD/DVD media. Select **Test** to test the CD/DVD for validity and readability. The software installer runs.

7. At the **Install** option, select **Yes**.

8. Select your Time Zone from the list. Select **Ok**.

9. You are reminded to review the log file of the install. During the installation, logs are generated. After the installation is complete, the log file is saved to the root directory of the server: `/root/install.log`. Select **Next**.

10. Finishing the installation is automatic and takes only a few minutes. At the end of the process, you are prompted to remove any media and reboot the system.

11. Remove the CD/DVD media.

12. Press **Enter** to reboot. The server reboots.

**CONFIGURE THE MSL OPERATING SYSTEM**

If you are installing a MiCollab Server wait until the server reboots. If you are installing a MiCollab Server Appliance power up the server.

Now, you must configure the MSL operating system. Refer to your Site Information sheet (on page 38) while completing the entries in the following sections.

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

**ACCEPT END USER LICENSE**

Select Accept to proceed with the installation.

At the "Restore from backup?" prompt:

- Select **No** if this is your initial installation of the MiCollab Server software. Continue with the next configuration step, "Set Administrator Password"
OR

- Select **Yes** if you have a MiCollab database backup file from a
  - MAS Release 5.0 or later system database that you want to restore to this MiCollab Server deployment
  - Then, refer to “Restoring a Database Backup” on page 153 for instructions on how to complete the restore.

**CAUTION:** Before you attempt to perform a restore, review Table 8, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 152 to ensure that the operation is supported for your configuration.

**SET ADMINISTRATOR PASSWORD**

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

The Administrator password (or System password) is used to access the administrator portal or the server console. Choose a password that contains numbers, mixed upper- and lower-case letters, and punctuation characters.

After you have entered and confirmed the password, the system examines the password for strength. If it is found to be weak, you are offered the chance to change it or continue.

**SELECT SYSTEM TIMEZONE**

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

**CONFIGURE DOMAIN NAME**

- Enter the primary domain name that will be associated with the MSL server (Field defaults to “mycompany.local”).

Enter the primary domain name that will be associated with this MSL server. This domain will become the default for the web-based administrator portal. The name must start with a letter and can contain letters, numbers, and hyphens. (For example, mitel.com.) Do NOT use the default setting.

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

**CONFIGURE SYSTEM NAME**

- Enter a system name for the server (host name).

Enter a unique system name or host name for the server. The name must start with a letter and can contain letters, numbers, and hyphens (for example, Server1).

**ENTER LOCAL NETWORK ADAPTER**

MSL automatically detects your system’s Ethernet adapters (Network Interface Cards) and displays them so you can configure:
MiCollab Installation and Maintenance Guide

- a "Local" adapter (for LAN mode) or
- a "Local" adapter AND a "WAN" adapter (for Network Edge mode).

For MiCollab Appliance Server installations, refer to Figure for the location of the Network Interface Card connectors on the server.

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

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

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

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

**ENTER LOCAL NETWORKING PARAMETERS**

- Enter the local IP address for this server, or select from the default parameters provided
- Enter the subnet mask for the local network, or accept the default.

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

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

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

Enter the subnet mask for the local network. If you are adding the server to an existing network, use the subnet mask used by the local network. Otherwise, accept the default setting.

**ENABLE IPV6 PROTOCOL AND ADDRESS**

- Select **No** to limit the server to IPv4 addresses. Continue with the next configuration step “Select WAN Adapters”.

  **OR**

- Select **Yes** to enable the server to be programmed with both IPv6 and IPv4 addresses. You are then prompted to enter an IPv6 address for the LAN interface.

  **Note:** If the LAN interface does not have an IPv6 address, this field can be left blank. However, some applications (such as MBG) require entry for IPv6 operation.
In addition to the LAN interface, you can configure IPv6 addresses for the WAN interface and gateway. This enables you to deploy MSL in a network environment that supports a mixture of IPv4 and IPv6 network protocols, and to access MSL via its IPv6 interfaces.

The following table lists the options supported by IPv6 in the current release:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Manager access</td>
<td>Use https://&lt;IPv6address&gt;/server-manager.</td>
</tr>
<tr>
<td>System Monitor access</td>
<td>Use https://&lt;IPv6address&gt;/monitor.</td>
</tr>
<tr>
<td>LAN interface configuration</td>
<td>Support for one IPv6 address only (that is, you cannot configure any additional LAN interfaces with an IPv6 address at this time). Bonding is supported.</td>
</tr>
<tr>
<td>WAN interface configuration</td>
<td>Support for one IPv6 static address. Bonding is supported. (DHCP/PPPoE with IPv6 is not supported at this time.)</td>
</tr>
<tr>
<td>Trusted Networks</td>
<td>IPv6 network addresses are supported.</td>
</tr>
<tr>
<td>SSH access</td>
<td>IPv6 access supported.</td>
</tr>
<tr>
<td>Review Configuration</td>
<td>Displays IPv6 configuration.</td>
</tr>
<tr>
<td>Remote management access</td>
<td>IPv6 access supported.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>IPv6 network addresses are supported.</td>
</tr>
</tbody>
</table>

Other options, such as backup/restore, remote management, MSL firewall, port forwarding, Email, DHCP, Hostnames and address, domains and SNMP are not supported.

**SELECT WAN ADAPTERS**

MSL automatically detects any remaining unconfigured Ethernet adapters and displays them here.

- If you are deploying MiCollab in Network Edge mode (that is, with Internet access), you must configure a WAN (external) adapter. MSL offers the choice to bond two Network Interface Cards - bonding is not supported for MiCollab.

- To deploy MiCollab in Network Edge mode with conferencing, there are two different configuration methods for providing access to the AWV application (installed on the MiCollab Server) from outside of the customer firewall.
  - Two external IP configuration: Configure two external IP addresses on the WAN adapters for MiCollab AWV web collaboration support. In Network Edge mode, the MSL firewall is located in the MiCollab server that resides on the network edge. Obtain two external IP addresses from your Internet Service Provider (ISP) for the web server interface and the conference functions. The MSL firewall on the MiCollab server is pre-configured to port forward from the second external alias IP address to the MiCollab AWV service on the MiCollab server.
    - Configure WAN interface
    - Select STATIC from (static/dhcp/ppoe)
    - Enter WAN IP address of the MiCollab AWV web server interface
    - Enter WAN IP netmask
- Enter WAN alias IP address of the MiCollab AWV conference functions
- Enter WAN alias IP netmask. If you leave the WAN alias IP address blank, this screen is not presented.

• Single external IP configuration: In the AWV configuration with one external IP address, the External Port is configured with 4443. This directs the external clients to reach the Connection Point using port 4443. The result is, the connection to the web conferencing portal will be requested on port 443, and the connection to the Connection Point component will be requested on port 4443.

• If your MiCollab applications will be operating in a LAN mode, do not configure a WAN adapter. Press the space bar to clear the selection.

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

SELECT GATEWAY IP ADDRESS

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

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

CONFIGURE EXTERNAL INTERFACE

Specify how the WAN adapter will be configured according to your connection setup:

<table>
<thead>
<tr>
<th>YOUR SETUP</th>
<th>CHOOSE OPTION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Modem and your ISP has supplied an account name.</td>
<td>1 (Use DHCP and send account name).</td>
</tr>
<tr>
<td>Cable modem and your ISP has supplied an Ethernet address.</td>
<td>2 (Use DHCP and send Ethernet address).</td>
</tr>
<tr>
<td>Residential ADSL.</td>
<td>3 (Use PPP over Ethernet).</td>
</tr>
<tr>
<td>You have a static IP address.</td>
<td>4 (Use static IP address).</td>
</tr>
</tbody>
</table>

If you select Option 4:

• Enter the IP address that this server should use to access the Internet. If this server does not access the Internet, leave the setting blank

• Enter the subnet mask.

CONFIGURE DNS

• If there are specific routes out to the Internet and you want the server to do DNS lookups to other servers in the network, enter the Corporate DNS server address, click Next and then specify how name resolution is performed for the local domain (the domain configured on the MSL server):
Install MiCollab Server

- **localhost** – the localhosts file is used resolve names for the local domain while the corporate DNS server handles name resolutions for all other domains.
- **corporate** – The corporate DNS server is used to resolve names for all domains.

- Click **Next**. The MSL operating system is now configured.

**ACTIVATE CHANGES**

When you have entered all configuration information, you are prompted to activate your changes. Select **Yes** to activate changes and automatically reboot the system.

**Note:** If you receive an error message when you activate, you may have entered an incorrect network parameter. See “Correcting Activation Errors” on page 114.

**ENTER APPLICATION RECORD ID**

1. After the reboot completes, you are prompted to **enter the Application Record ID number** that you created for this installation. Although the screen says that this entry is optional, you **must** enter your Application Record ID number now. This entry initiates registration of all licensed and enabled MiCollab software applications.

**Note:** If you accidentally cancel this screen you will exit to the server console menu. You can restart the application software installation by selecting **Register for ServiceLink** from the menu. Enter your Application Record ID number to initiate registration. Then proceed to “Install Application Software” on page 47.

2. The Mitel Application Management (AMC) licensing server is located on the Internet. In order to obtain licenses, the MiCollab server requires access to the internet. If the MiCollab server is on a network that does not have access to the internet, enter the IP address of a proxy server or router that will allow it to access the internet.

3. Proceed to “Install Application Software” on page 47.

**INSTALL APPLICATION SOFTWARE**

**Note:** If you are installing the MiCollab Server Appliance, skip this section. The MSL operating system and your MiCollab application software is pre-installed on a MiCollab Server Appliance.

You can install the application software by

- downloading and installing the application software from the AMC, or
- installing the application software from local media (CD/DVDs or a USB device).

**Note:** For installation on Hyper-V, USB is not supported. Therefore, you must create installation disks of the application software.

1. In the server manager, under **ServiceLink**, click **Install Applications**.
2. Click the **Install Applications** tab.
3. If prompted, set the **PBX Type** and then click **Next**. The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.

4. Select the latest software version for installation.

5. For each application you want to install:
   a. Select the **Install** box.
   b. Select the **Download from AMC** box to download and install software from the Application Management Center.
      -or-
      Clear the **Download from AMC** box to download software from local media (CD/DVD or USB).

6. If you are installing from USB, click **Query USB Storage Devices**. The system detects and lists all of the USB devices connected to the local computer. These devices will be searched for application software when installation commences.

7. Click the **Install** button.

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

   **Note:** If you are installing NuPoint ISO files, ensure that you include the "NPUM Finalize" blade.

8. After the applications are installed, reboot the MiCollab server.


**CONFIGURE MICOLLAB**

The administrator portal is a web-based portal that provides a central location for configuring the server and applications. The administrator portal web interface provides access to the

- **Server Manager** - allows you to configure and maintain the server
- **Application Web Pages** - allow you to configure and administer the installed applications (for example NuPoint Unified Messenger).

Web browser access to MiCollab administration interfaces is provided through

- Microsoft Edge 20
- Internet Explorer 10, or 11
- Mozilla FireFox 41 or higher, or
- Google® Chrome™ (version 46 or higher)

Note that Flow Through Provisioning and Reach Through functionality are only supported in Internet Explorer and FireFox browsers.
LOG IN TO THE ADMINISTRATOR PORTAL (SERVER MANAGER)

1. On a management PC that is on the same subnet as the MiCollab server, open a browser and enter the following URL in the address bar:
   https://<Fully Qualified Domain Name of the MiCollab server or controller>/server-manager
   or
   https://<IP Address of the MiCollab server or controller>/server-manager

2. Enter User Name (default is "admin") and the system Password you created during installation, and then click Login. The administrator portal opens.

3. Do one of the following:
   • In the left-hand menu, under Applications, click an application name to open the interface of that application.
   • Click the Help link in the administrator portal for detailed server administration instructions.

4. By default, MiCollab is configured to send a Welcome E-mail to new users after you add them to the system. The e-mail provides users with their MiCollab information, such as
   - a link to the My Unified Communications web portal, and
   - login ID and password.

   See Configure Service Email in the MiCollab Administrator online help for the Welcome E-mail configuration options. In order for the system to list the Speech Auto Attendant pilot/access number in the Service E-mail, you must enter the pilot number into the Network Element screen of the USP application.

   If you choose to disable the Welcome E-mail functionality, you will need to advise users of the URL for the MiCollab End User portal:
   https://<Fully Qualified Domain Name of the MiCollab server>/portal
   or
   https://<IP Address of the MiCollab server or controller>/portal

5. Proceed to “Install Web Certificates” on page 49.

INSTALL WEB CERTIFICATES

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

To prevent these security warnings from appearing
   • install the Mitel Root CA certificate locally on each user’s client PC, or
   • purchase and install a Secure Sockets Layer (SSL) certificate from a third-party Certificate Authority (CA) on the MiCollab Server, MiVoice Border Gateway Server, or both.

For instructions on how to install the Mitel Root CA certificate (security certificate), see the Install Mitel Root Certificate topic in the MiCollab End User portal online help.
For instructions on how to install a third-party SSL certificate, refer to the Manage Web Server Certificate topic in the Server Manager online help for details.

**Note:** Restart MiCollab Client if you change the web certificate on the MiCollab server. MiCollab Clients will not be able to connect until MiCollab Client has been restarted.

- To prevent the Security Alert warning from appearing on clients on the local network, purchase a Secure Sockets Layer (SSL) certificate for the MiCollab server and then import it onto the MiCollab server.

- To prevent the Security Alert warning from appearing on remote clients, purchase a Secure Sockets Layer (SSL) certificate for the MiVoice Border Gateway Web Proxy server and then import it onto the MiVoice Border Gateway Web Proxy server.

**Note:** If you purchase a third-party certificate for the Web Proxy on the MiVoice Border Gateway server, then the purchased certificate should include "alternate names" for any URLs handled by the Web Proxy. For example, if MiCollab Client server "uca.example.com" is handled by the Web Proxy "webproxy.example.com", then the SSL certificate for "webproxy.example.com" should also include "uca.example.com" as a subject alternate name on the SSL certificate.

**ALLOW "TRUSTED NETWORK" ACCESS**

Access to the MiCollab server is restricted to your local network (or subnet) by default. If your ICP or some of your users or phones are on a different subnet than the MiCollab server, it is necessary to allow them access. First, you must configure them as a trusted local network and then you can grant them express permission.

To configure Trusted Networks:

1. Log into the MiCollab server console. The server console Welcome menu is displayed.
2. Select Manage trusted networks from the menu and select Next.
3. Select Add IPv4 trusted network or Add IPv6 trusted network and select Next.
4. Enter the Trusted Network IP address of the network to which you are granting access. (For example, 168.195.52.0). Select Next.
5. Enter the Trusted Network Mask to apply to the network address. (For example, if your network IP address is 168.195.52.0 and you want to allow access to all network IP addresses in the range from 1 to 255, enter 255.255.255.0. This allows IP addresses 168.195.52.1 through 168.195.52.255 to access your virtual appliance).
6. Enter the Trusted Network Router Address. (IP address of the router on your local network).
7. Select Next. The local network is added.
8. Repeat steps 1 through 5 to configure additional trusted networks.

To grant secure shell access to the trusted local network you have created:

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 49).
2. Navigate to **Remote Access** under the **Security** section.

3. In the **Secure Shell Access** field, select one of the following:
   - **No Access**: select this option to restrict access to your own local network
   - **Allow access only from trusted and remote management networks**: select this option to allow access to selected trusted local networks (required if using Mitel Integrated Configuration Wizard) and remote management networks. This is the recommended setting.
   - **Allow Public access (entire Internet)**: select this option to allow access to the entire Internet. This setting requires a strong SSH (admin) password; its use is NOT recommended.

4. In the **Allow administrative command line access over secure shell** field, do one of the following:
   - select **Yes** to allow users to connect to the virtual appliance and log in as "root"
   - select **No** to restrict users from logging in as "root".

5. In the **Allow secure shell access using standard passwords** field, do one of the following:
   - select **Yes** to allow users to connect to your virtual appliance using a standard password
   - select **No** to restrict virtual appliance access to users with RSA Authentication.

6. Click **Save**.

**SET SYSTEM LANGUAGE**

After the initial installation of a new system, the system language is set to US English. You can set the language of the MiCollab End User portal and the Telephone User Interface (TUI) for the MiCollab application end-users from the server manager. End users can set:

- the language of their MiCollab End User portal from their login page, and
- their prompt language from the Settings page in their portal.

The MiCollab software is installed with North American English as the default language. To change the default system language to one of the other supported languages:

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 49).
2. Under **Configuration**, click **MiCollab Language**.
3. Select the desired language from the Language drop-down box.
4. Click **Save**.
5. If NuPoint Unified Messenger application is installed, you can set up to five languages for the NuPoint system prompts. Users who call into the NuPoint auto attendant can choose to hear prompts in one of the supported languages for the duration of their call. Refer to the online help for the **MiCollab Language Settings** page for details.
6. If your system uses the Speech Auto Attendant application, set the SAA prompt language. The MiCollab system language setting does not control the prompt language used by the Speech Auto Attendant application. The MiCollab Speech Auto Attendant only supports
two languages: UK English and NA English. To change the Speech Auto Attendant language:
- Under Applications, click NuPoint Web Console.
- Under Auto Attendant, click Misc. Parameters.
- Select the desired Primary Language, and then click Save.
- Under Auto Attendant, click Data Source.
- Click Force Update.

Note: MiCollab Client (MiCollab Client) supports additional languages that are not supported by MiCollab. If MiCollab Client is configured in integrated mode, only the MiCollab languages are supported. However, MiCollab Client users can use the additional languages if MiCollab Client is deployed on MiCollab in co-located mode, even though these languages are not supported by MiCollab.

Note: For additional details regarding language support, see Configure MiCollab Language Settings in the Server Manager online help.

7. If your system uses the MiCollab Client application, ensure that the MiCollab Client server uses the same IP address as the MiCollab server.

8. If required, configure MiTeam. MiTeam provides Cloud-based collaboration features for UCC Premium users. Note that MiTeam is only supported for MiCollab Client Integrated mode. Refer to the MiCollab Client Administrator Guide for configuration requirements.

PERFORM INITIAL CONFIGURATION OF APPLICATIONS

Proceed to “Initial Configuration” on page 75.

INSTALL MICCOLLAB SERVER IN LAN MODE WITH MIVOICE BORDER GATEWAY SERVER(S)

You can use a MiCollab server in LAN mode to manage Teleworker services that are running on one or more MiVoice Border Gateway (MBG) servers located on the Network-Edge or in the DMZ. To support this configuration, you install the MiCollab server with MBG in the LAN and install the MBG servers with Teleworker in the DMZ or on the Network Edge. You then create a cluster on the MiCollab server and add the MBG servers as members of the cluster in separate cluster zones.

PREREQUISITES AND CONDITIONS

☑ The MiCollab server must be configured in LAN mode (server-only mode). MBG clustering is only supported for MiCollab systems that are configured in LAN mode.

☑ The MBG server must be installed, operational and routable to the MiCollab server.

☑ The MiCollab system must be configured with an MBG cluster to allow the data on the MBG cluster to be managed from the MiCollab application. Note that the MiCollab server can only be a member in one MBG cluster.
The MiCollab and MBG servers should all have the same MBG software release (for example, MBG Release 9.4).

The MiCollab and MBG nodes must reside in separate zones. You create a "LAN" zone for the MiCollab node and the MBG nodes remain in the "Default" zone.

After you establish the cluster, the licenses of the MiCollab and MBG servers are pooled together. However, it is recommended that you purchase all Teleworker service licenses against the external MBG servers to avoid licensing issues.

To cluster the MiCollab server with an MBG cluster of one or more external MBGs:

1. Install the MBG server(s) in the DMZ. Refer to the MBG Installation and Maintenance Guide for instructions.

2. Open port 6809 in the firewall to allow the MiCollab system to communicate remotely with the MBG server(s).

3. In the MiCollab server manager, under Applications, click MiVoice Border Gateway, click the System status tab and then click Dashboard.

4. Create a new cluster on the MiCollab (master) server:
   - In the Clustering status frame, click Create a cluster.
   - In the IP Address of current node list, select the interface or enter the IP address of the MiCollab master server (or accept the default).
   - In the IP Address of peer node list, enter the IP address of the MBG slave server (DMZ address or server-gateway WAN address). These entries establish the cluster relationship between the servers.
   - In the Cluster weight of current node field, select the cluster weight factor value to apply to the MiCollab master server for load balancing. The default value is 0. You must select a non-zero value.
   - Click Save to create the initial master/slave pair. The two new nodes are added to the Node information list as members of the "Default" cluster zone.

5. Create a new "LAN" zone:
   - Click + Zone (Add new zone).
   - In the Cluster zone name field, enter "LAN".
   - Click Save.

6. Modify the MiCollab node and add it to the "LAN" zone:
   - Click (Modify node).
   - Set the Cluster zone for current node field to "LAN".
   - Click Save.

7. Join the cluster from MBG (slave) server:
   - Log into the MBG server.
   - In the MSL server manager, click the System status tab and then click Dashboard.
   - In the Clustering status frame, click Join a cluster.
   - In the IP Address of current node list, select the interface or IP address of this server.
   - In the IP Address of peer node list, enter the IP address of the MiCollab master server.
- Click **Save**.

8. Wait for the master node to synchronize its database with the slave, which can take five minutes for newly created MBGs and up to 30 minutes for existing MBGs with large databases. When synchronization is complete, the State field on the master displays, "In sync with peer node" and the State field on the slave displays "In sync with master node."

9. For the node you have just added, click to **Modify node**.

10. In the **Cluster weight of current node** field, select a value to apply to the slave server. The default value is 0. You must select a non-zero value.

11. Click **Save**.

**Note:** By default, the slave server has a cluster weight of zero (0). If you fail to update this value, the slave server will not participate in load balancing, even if all other nodes in the cluster fail.

12. To add more MBG servers to the cluster, join the cluster from other MBG (slave) servers:
   - On the MiCollab (master) server, program the MBG(s) as new nodes in the cluster.
   - On the MBG(s), program them as slaves to the MiCollab (master) server.

**Note:** Provision Teleworker services from the MiCollab server. Do not provision them on the MBG servers; otherwise, the MiCollab and MBG databases could get out of sync.

**Note:** Mitel 6800 and 6900 Series SIP Phones can be used as Teleworker devices on a MBG in conjunction with a MiVoice Office 400 communication platform. The devices will not be visible or managed through MiCollab **Users and Services**. The system administrator is responsible to set up Mitel 6800/6900 series SIP phones using a configuration file. For instructions, see *Mitel SIP Teleworker via MBG on MiVoice Office 400 Deployment Guide*. 
Chapter 5

INSTALLING VIRTUAL MICOLLAB
IN A VMWARE ENVIRONMENT
INTRODUCTION

This chapter describes the installation of vMiCollab in a VMware environment.

ABOUT MICOLLAB VIRTUAL APPLIANCE

You can deploy the MiCollab system as a virtual appliance within a virtualized cloud environment. A MiCollab Virtual Appliance deployment supports

- Small Business multi-application sites up to 250 users
- Mid Market Business multi-application sites up to 1500 users
- Enterprise multi-application and single-application sites up to 2500 users.
- Large Enterprise multi-application and single-application sites up to 5000 users.

Refer to the MiCollab Engineering Guidelines for MiCollab Virtual Appliance capacities and performance information. Also see the Virtual Appliance Deployment Guide for engineering guidelines for deploying Mitel Virtual Appliances and applications in a virtual infrastructure.

This chapter describes the deployment of the MiCollab virtual appliance. It does not describe the setup and operation of the VMware cloud environment.

DEPLOYMENT CONFIGURATIONS

Figure 11 shows an example of a MiCollab Virtual Appliance deployment. Refer to the MiCollab Engineering Guidelines for descriptions of the supported deployments.
SUPPORTED APPLICATIONS

The following applications are supported on the MiCollab Virtual Appliance:

• NuPoint Unified Messaging
• Speech Auto Attendant
• MiCollab Client
• MiCollab AWV
• MiVoice Border Gateway (Secure Call Recording of LAN devices only)

INSTALLATION CHECKLIST

An installation consists of the following steps:

☐ Review Installation Details
☐ Collect Site Information
☐ Collect Custom Template Information
☐ Create vMiCollab Application Record ID (Virtual Appliance)
☐ Download vMiCollab OVA file and Optional Application Software
☐ Deploy MiCollab vApp
☐ Configure the MSL Operating System
☐ Enter Application Record ID and Reboot
☐ Install MiCollab Application Software Options (for example, NP-UM options) and Reboot
☐ Configure vMiCollab Virtual Appliance
☐ Perform Initial Configuration of MiCollab Applications
☐ Integrate or Collocate MiCollab Client Database?

MICOLLAB VIRTUAL APPLIANCE INSTALLATION

REVIEW INSTALLATION DETAILS

REQUIREMENTS

• Refer to the Virtual Appliance Deployment Guide for MiCollab Virtual Appliance platform requirements. Ensure that you meet or exceed the minimum resource requirements.
• Internet access to allow licensing from the Applications Management Center (AMC). Internet access must be maintained with the AMC to prevent license expiry.
• For MiCollab Virtual Appliance in Network Edge (server-gateway) deployments, you must have a WAN connection available in the network to assign to the MiCollab WAN adapter.
• A DNS server that is reachable from the platform.

CONSTRAINTS

The following constraints apply:

• You must use MiCollab Virtual Appliance base software license when you create the Application Record ID for an installation. Do not attempt to install MiCollab Virtual Appliance using an Application Record ID created from a MiCollab Server base software license; otherwise, the installation will fail.

• vMiCollab is not supported if you manually install MiCollab (that is, install the MSL and the MiCollab software into a virtual appliance and then use a vMiCollab Application Record ID to activate the software).

• Do not attempt to restore a database that has been taken from an individual application (for example, a NP-UM database) within a MiCollab Server to either a MiCollab Server system or a vMiCollab deployment.

• Refer to the Virtual Appliance Deployment Guide for constraints related to the virtual environment.

COLLECT SITE INFORMATION

Collect the following information before you start the installation:

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NOTES</th>
<th>RECORD YOUR INFORMATION HERE:</th>
</tr>
</thead>
</table>
| 1. Identify virtual environment | • VMware vSphere Standalone host  
• VMware vSphere vCenter Server | □ |
| 2. Identify MiCollab Virtual Appliance network deployment configuration | Refer to the MiCollab Engineering Guidelines for descriptions of the MiCollab deployment configurations. vMiCollab supports the following deployment configurations:  
• vMiCollab in Network Edge (server gateway) Mode  
• vMiCollab in LAN mode with a second MBG Server in DMZ:  
  - vMiCollab with second MBG Web Proxy in DMZ (2 Server deployment)  
  - vMiCollab with second MBG/Web Proxy in Network Edge mode (2 Server deployment)  
• vMiCollab in LAN Mode (Server Only) | □ |
| 3. Identify vMiCollab capacity | All applications are included with vMiCollab. The maximum user capacity is higher for sites with a single application. For single application sites, do not configure users with multiple applications; otherwise the maximum performance and capacities of the system will be reduced. | □ |
### Installing Virtual MiCollab in a VMware Environment

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NOTES</th>
<th>RECORD YOUR INFORMATION HERE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Application Record ID</td>
<td>Create an Application Record ID for the vMiCollab installation in your AMC license account. You will use this Application Record ID to activate your MiCollab license. See &quot;About AMC Licensing&quot; on page 19 for more information. Record the generated Application Record ID.</td>
<td></td>
</tr>
<tr>
<td>5. MiCollab Administrator Password</td>
<td>For password strength, choose a password that contains a mix of uppercase and lowercase letters, numbers, and punctuation characters.</td>
<td></td>
</tr>
<tr>
<td>6. Domain Name</td>
<td>Names must start with a letter; can contain letters, numbers, and hyphens. For more information, see page 65.</td>
<td></td>
</tr>
<tr>
<td>7. System Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. IP address of your vMiCollab system (LAN mode)</td>
<td>The local IP address of the vMiCollab system.</td>
<td></td>
</tr>
<tr>
<td>9. Gateway IP address</td>
<td>The IP address that vMiCollab will use to access the network.</td>
<td></td>
</tr>
</tbody>
</table>
| 10. MiCollab AWV IP Addresses | There are two different configuration methods for providing access to the AWV application (installed on the MiCollab Server) from outside of the customer firewall.  
- For two external IP configuration: In the AWV configuration with two external IP address, obtain two external IP addresses from your Internet Service Provider (ISP). One IP address is required for the web server interface that is used to set up audio conferences. A second IP address is required for the web service that provides the conference functions, such as file sharing, desktop collaboration, keyboard chat, and so forth).  
- For single external IP configuration: In the AWV configuration with one external IP address, the External Port is configured with 4443. This directs the external clients to reach the Connection Point using port 4443. The result is, the connection to the web conferencing portal will be requested on port 443, and the connection to the Connection Point component will be requested on port 4443.  
For information on configuring the MiCollab AWV IP addresses based on the configuration used, see the MiCollab Engineering Guidelines document. | |
| 11. Will the vMiCollab (MSL) vApp be supplying DHCP services? | If the MiCollab vApp will supply the DHCP services, you need to provide the range of IP addresses that the server can distribute. For more information, see page 69. | Yes | No |
| 12. DNS Server IP address | Enter the IP address of your corporate DNS server. **Note:** If your DNS is supplied by your ISP, leave this setting blank. | |
"Trusted Network" Access

If your PBX platform or some of your users are not on the same subnet as the vMiCollab vApp, you need to classify them as "Trusted Networks" and then allow them access.

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>The IP address of the network for which you want to allow access.</td>
</tr>
<tr>
<td>Subnet mask or network prefix</td>
<td>The dot-decimal subnet mask or CIDR network prefix for the range of IP addresses you wish to allow.</td>
</tr>
<tr>
<td>Router Address</td>
<td>The address of the router/gateway you will use to access the network (or subnet) to which you are granting access.</td>
</tr>
</tbody>
</table>

Note: To create a blank template for cloning, leave the following fields empty: Administrator Password, Hostname, Domain Name, LAN and WAN IP addresses. After you create the clone, you must complete these fields before you can proceed with deployment. You cannot clone an active (deployed) vMiCollab.

Table 3: Collect Custom OVA Template Information

<table>
<thead>
<tr>
<th>CONFIGURATION ITEMS</th>
<th>FIELD DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td></td>
</tr>
<tr>
<td>Restore from backup</td>
<td>If a database restore is required during deployment, ensure that you have a taken a database backup.</td>
</tr>
<tr>
<td>Localization</td>
<td></td>
</tr>
<tr>
<td>Time zone setting</td>
<td>Identify the MSL operating system time zone setting. The default is America/New York. The Time zone setting also determines your system telecommunications regional settings.</td>
</tr>
<tr>
<td>Keyboard Type</td>
<td>Identify the preferred keyboard type (default is us)</td>
</tr>
</tbody>
</table>
## Table 3: Collect Custom OVA Template Information

<table>
<thead>
<tr>
<th>CONFIGURATION ITEMS</th>
<th>FIELD DESCRIPTION</th>
<th>SITE CONFIGURATION DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Initial Administrator Password</strong></td>
<td>Record the initial administrator password for the MiCollab server manager interface. This password must be at least six characters long. After you access the MiCollab server manager, you will be prompted to change this initial password. <strong>Note:</strong> You must enter a password before you deploy the MiCollab UC; otherwise, the system will not boot up.</td>
<td><strong>Initial MiCollab Server manager Administrator Password:</strong> Final MiCollab server manager Administrator Password: <strong>Note:</strong> It is recommended that you use a strong password that contains all of the following: upper case letter, lower case letter, number, non-alphanumeric character, and be at least seven characters long. Do not use a commonly used word (for example: 'password').</td>
</tr>
<tr>
<td>Hostname</td>
<td>Set the hostname of the system.</td>
<td></td>
</tr>
<tr>
<td>Domain Name (Optional)</td>
<td>Specify the domain name for the hostname above. The default domain name is &quot;mycompany.local&quot;.</td>
<td></td>
</tr>
<tr>
<td>License Key (Optional)</td>
<td>Identify the License Key (ARID) for this system. The ARID is used by the AMC to distribute the system licenses.</td>
<td></td>
</tr>
<tr>
<td>DNS Server IP (Optional)</td>
<td>Record the DNS Server IP Address</td>
<td></td>
</tr>
<tr>
<td>Remote Network Addresses for MiCollab Server administration (Optional)</td>
<td>List the Network IP address that is allowed to access the MiCollab server and perform remote administration.</td>
<td></td>
</tr>
<tr>
<td>Remote Network Netmask (Optional)</td>
<td>Enter the Netmask associated with the remote network address.</td>
<td></td>
</tr>
<tr>
<td><strong>Network Settings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN IP Address (IP Address of the vMiCollab)</td>
<td>Record the IP address of the local (LAN) interface. This must be a valid IP address on the local LAN. <strong>Note:</strong> You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this IP address from vSphere Client. Right-click on the MiCollab and click <strong>Edit Settings.</strong> Click the <strong>Options</strong> tab, click <strong>Properties</strong> and enter the LAN IP Address.</td>
<td></td>
</tr>
<tr>
<td>LAN Netmask</td>
<td>Record the Netmask of the LAN</td>
<td></td>
</tr>
</tbody>
</table>
WAN IP Address (Optional) For Network Edge (Server-gateway) deployments, record the IP address of the external (WAN) interface. This must be a valid IP address on external WAN. For LAN only (Server-only) deployments, use an IP address of 0.0.0.0. **Note:** You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this address from vSphere Client. Right click on the MiCollab and click **Edit Settings.** Click the **Options** tab, click **Properties** and enter the WAN IP Address.

WAN Netmask (Optional) Record the Netmask of the WAN.

LAN (Optional) Optional network interface that can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.

Default Gateway IP Address Record the Gateway IP address. For Server-gateway deployments this gateway typically points to the internet. For Server-only deployments, this gateway typically points to a LAN router.
CREATE MICOLLAB APPLICATION RECORD

Create an Application Record for this MiCollab Virtual Appliance installation in your AMC license account. You will use the ID number of this Application Record to activate your MSL license. See "About AMC Licensing" on page 19 for more information.

If your MiCollab system requires NuPoint Speech Auto Attendant, ensure that your ARID includes the following licensing options:

- 324: NuPoint Text To Speech Ports
- 326: Speech Ports

**Note:** You must use vMiCollab software license "Virtual MiCollab Base SW" part number when you create the Application Record ID for a vMiCollab installation. Do not attempt to install MiCollab Virtual Appliance using an Application Record ID created from a MiCollab Server license; otherwise, the installation will fail.

DOWNLOAD MICOLLAB OVA FILE AND APPLICATION SOFTWARE

SOFTWARE DOWNLOADS

1. Log on to Mitel MiAccess (formerly known as Mitel Connect).
2. From left menu, select Software Downloads Center.
3. Click MiCollab.
4. Click the appropriate MiCollab Software Download version.
6. Download the MSL, applications, and prompts software for your deployment by clicking the file links in the table. When you click a link, you are presented with a software Disclaimer.
7. Click the "I Agree [Download using Software Download Manager (Recommended)]".
8. If you don’t already have the Download Manager installed on your local PC, you are prompted to install it. The Download Manager is an Active X application that optimizes the software download speed. After you install the Download Manager, it is available for subsequent software downloads.
9. Save the downloaded software ISO images to a folder on your maintenance PC.

<table>
<thead>
<tr>
<th>FILE CONTENTS</th>
<th>FILE FORMAT</th>
<th>FILE NAME DOWNLOADED</th>
<th>APPRrox File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>vMiCollab vApp packaged as a</td>
<td>.ova file</td>
<td>vMiCollab_8.1.x.x.ova</td>
<td>2.4 GB</td>
</tr>
<tr>
<td>virtual appliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NuPoint Unified Messaging option</td>
<td>.iso file</td>
<td>NPM_Blades-DVD_1_19.1.x.xx-01.iso</td>
<td>1.2 GB</td>
</tr>
<tr>
<td>Speech Auto Attendant and Text to</td>
<td>.iso file</td>
<td>NPM_Blades-DVD_2_19.1.x.xx-01.iso</td>
<td>2.9 GB</td>
</tr>
<tr>
<td>Speech options</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DEPLOY VMICOLLAB VAPP

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

Refer to the Mitel Virtual Appliance Deployment Guide for the deployment requirements and for additional instructions on how to deploy the virtual application.

CONFIGURE THE MSL OPERATING SYSTEM

If you deployed vMiCollab on vSphere vCenter and used the Custom Template to configure the MSL Operating System parameters, use the following procedures to review your settings. If you did not use vSphere vCenter, you must configure the MSL Operating System parameters using the procedures in this section.

LAUNCH THE MSL SERVER CONSOLE

1. Right-click on the newly created MiCollab Virtual Appliance (for example: vMiCollab 7.3.23.0 build) and select Power On.

2. Right-click on the MiCollab Virtual Appliance and select Open Console.
Installing Virtual MiCollab in a VMware Environment

3. The MSL Server Console is displayed and you are prompted to select your keyboard layout (default is us). Select the required keyboard layout and click Next.

   **Note:** If at any time you need the cursor available for other desktop activities, press the CTRL + ALT keys.

4. You are prompted to restore for backup. Click No.

5. Proceed to “Set Administrator Password” on page 65.

**SET ADMINISTRATOR PASSWORD**

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

The Administrator password (or System password) is used to access the administrator portal or the server console. Choose a password that contains numbers, mixed upper- and lower-case letters, and punctuation characters.

After you have entered and confirmed the password, the system examines the password for strength. If it is found to be weak, you are offered the chance to change it or continue.

**SELECT SYSTEM TIMEZONE**

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

**CONFIGURE DOMAIN NAME**

- Enter the primary domain name that will be associated with the MSL virtual appliance (Field defaults to “mycompany.local”).

Enter the primary domain name that will be associated with this MSL virtual appliance. This domain will become the default for the web-based administrator portal. The name must start
with a letter and can contain letters, numbers, and hyphens (for example, mitel.com). Do NOT use the default setting.

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

CONFIGURE SYSTEM NAME

• Enter a system name for the MiCollab virtual appliance (host name).

Enter a unique system name or host name for the virtual appliance. The name must start with a letter and can contain letters, numbers, and hyphens (for example, Server1).

ENTER LOCAL NETWORK ADAPTER

MSL automatically detects your system's Ethernet adapters (Network Interface Cards) and displays them so you can configure:

• a "Local" adapter (for LAN mode) or
• a "Local" adaptor AND a "WAN" adapter (for Network Edge mode).

Note that although MSL offers the choice to bond two Network Interface Cards, this option is not supported for MiCollab. An asterisk is displayed in front of the Local adapter REGARDLESS OF SERVER MODE, YOU MUST ALWAYS CONFIGURE A LOCAL (INTERNAL) ADAPTER.

• Use the up/down arrow keys to select the adapter you want to configure as local. Use the space bar to assign the adapter as Local.

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

ENTER LOCAL NETWORKING PARAMETERS

• Enter the local IP address for this virtual appliance, or select from the default parameters provided

• Enter the subnet mask for the local network, or accept the default.

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

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

Note: If you are installing virtual appliances at multiple sites within the organization, use different network addresses for each site. This simplifies later troubleshooting and VPN setups.
Enter the subnet mask for the local network. If you are adding the virtual appliance to an existing network, use the subnet mask used by the local network. Otherwise, accept the default setting.

**ENABLE IPV6 PROTOCOL AND ADDRESS**

- Select No to limit the server to IPv4 addresses. Continue with the next configuration step “Select WAN Adapters”.

OR

- Select Yes to enable the server to be programmed with both IPv6 and IPv4 addresses. You are then prompted to enter an IPv6 address for the LAN interface.

**Note:** If the LAN interface does not have an IPv6 address, this field can be left blank. However, some applications (such as MBG) require entry for IPv6 operation.

In addition to the LAN interface, you can configure IPv6 addresses for the WAN interface and gateway. This enables you to deploy MSL in a network environment that supports a mixture of IPv4 and IPv6 network protocols, and to access MSL via its IPv6 interfaces.

The following table lists the options supported by IPv6 in the current release:

<table>
<thead>
<tr>
<th>OPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Manager access</td>
<td>Use https://&lt;IPv6address&gt;/server-manager.</td>
</tr>
<tr>
<td>System Monitor access</td>
<td>Use https://&lt;IPv6address&gt;/monitor.</td>
</tr>
<tr>
<td>LAN interface configuration</td>
<td>Support for one IPv6 address only (that is, you cannot configure any additional LAN interfaces with an IPv6 address at this time). Bonding is supported.</td>
</tr>
<tr>
<td>WAN interface configuration</td>
<td>Support for one IPv6 static address. Bonding is supported. (DHCP/PPPoE with IPv6 is not supported at this time.)</td>
</tr>
<tr>
<td>Trusted Networks</td>
<td>IPv6 network addresses are supported.</td>
</tr>
<tr>
<td>SSH access</td>
<td>IPv6 access supported.</td>
</tr>
<tr>
<td>Review Configuration</td>
<td>Displays IPv6 configuration.</td>
</tr>
<tr>
<td>Remote management access</td>
<td>IPv6 access supported.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>IPv6 network addresses are supported.</td>
</tr>
</tbody>
</table>

Other options, such as backup/restore, remote management, MSL firewall, port forwarding, Email, DHCP, Hostnames and address, domains and SNMP are not supported.

**SELECT WAN ADAPTERS**

MSL automatically detects any remaining unconfigured Ethernet adapters and displays them here.

- If you are deploying MiCollab in Network Edge mode, (that is, with Internet access), you must configure a WAN (external) adapter. MSL offers the choice to bond two Network Interface Cards - bonding is not supported for MiCollab.
• To deploy MiCollab in Network Edge mode with conferencing, there are two different configuration methods for providing access to the AWV application (installed on the MiCollab Server) from outside of the customer firewall.

• Two external IP configuration: Configure two external IP addresses on the WAN adapters for MiCollab AWV web collaboration support. In Network Edge mode, the MSL firewall is located in the MiCollab server that resides on the network edge. Obtain two external IP addresses from your Internet Service Provider (ISP) for the web server interface and the conference functions. The MSL firewall on the MiCollab server is pre-configured to port forward from the second external alias IP address to the MiCollab AWV service on the MiCollab server.
  - Configure WAN interface
  - Select STATIC from (static/dhcp/ppoe)
  - Enter WAN IP address of the MiCollab AWV web server interface
  - Enter WAN IP netmask
  - Enter WAN alias IP address of the MiCollab AWV conference functions
  - Enter WAN alias IP netmask. If you leave the WAN alias IP address blank, this screen is not presented.

• Single external IP configuration: In the AWV configuration with one external IP address, the External Port is configured with 4443. This directs the external clients to reach the Connection Point using port 4443. The result is, the connection to the web conferencing portal will be requested on port 443, and the connection to the Connection Point component will be requested on port 4443.

• If your MiCollab applications will be operating in a LAN mode, do not configure a WAN adapter. Press the space bar to clear the selection.

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

SELECT GATEWAY IP ADDRESS

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

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

CONFIGURE EXTERNAL INTERFACE

Specify how the WAN adapter will be configured according to your connection setup:

<table>
<thead>
<tr>
<th>YOUR SETUP:</th>
<th>CHOOSE OPTION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable Modem and your ISP has supplied an account name.</td>
<td>1 (Use DHCP and send account name).</td>
</tr>
<tr>
<td>Cable modem and your ISP has supplied an Ethernet address.</td>
<td>2 (Use DHCP and send Ethernet address).</td>
</tr>
</tbody>
</table>
If you select Option 4:

- Enter the IP address that this server should use to access the Internet. If this server does not access the Internet, leave the setting blank
- Enter the subnet mask.

**CONFIGURE DNS**

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

**ACTIVATE CHANGES**

- When you have entered all configuration information, you are prompted to activate your changes. Select **Finish** to activate changes and automatically reboot the system.
- Proceed to “Enter Application Record ID and Reboot” on page 69.

**Note:** If you receive an error message when you activate, you may have entered an incorrect network parameter. See “Correcting Activation Errors” on page 114.

**ENTER APPLICATION RECORD ID AND REBOOT**

1. Enter the Application Record ID number that you created for this installation. Although the screen says that this entry is optional, you must enter your Application Record ID number now. This entry initiates registration of all licensed and enabled MiCollab software applications. Select **Next**.

**Note:** If you accidentally cancel this screen you will exit to the server console menu. You can restart the application software installation by selecting **Register for ServiceLink** from the menu. Enter your Application Record ID number to initiate registration. Then proceed to “Install Application Software” on page 70.

2. The Mitel Application Management (AMC) licensing server is located on the Internet. In order to obtain licenses, the MiCollab virtual appliance requires access to the internet. If the MiCollab virtual appliance is on a network that does not have direct access to the internet, you can override the default AMC address by entering the IP address of a proxy server or router that will allow access to the internet.
INSTALL APPLICATION SOFTWARE

You install Applications Software from MiCollab server manager:

1. In the server manager, under ServiceLink, click Install Applications.
2. Click the Install Applications tab.
3. Set the PBX Type and then click Next. The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.
4. Select the latest software version for installation.
5. Check the Download from AMC boxes of the required applications.
6. Click Install.

**Note:** For detailed instructions on how to install software in a virtual environment, including how to mount media (CD/DVD or USB) from a datastore, client or host device, refer to the MiCollab Administrator online help.
7. After the applications are installed, proceed to “Configure vMiCollab” on page 70.

CONFIGURE VMICOLLAB

The administrator portal is a web-based portal that provides a central location for configuring the virtual appliance and system settings. The administrator portal web interface provides access to the

• Server Manager - allows you to configure and maintain the virtual appliance
• Application Web Pages - allow you to configure and administer the installed applications (for example NuPoint Unified Messenger).

Web browser access to MiCollab administration interfaces is provided through

• Microsoft Edge 20
• Internet Explorer 10, or 11
• Mozilla FireFox 41 or higher, or
• Google Chrome (version 46 or higher)

LOG IN TO THE ADMINISTRATOR PORTAL (SERVER MANAGER)

1. On a PC on the same subnet as the vMiCollab server, open a browser and enter the following URL in the address bar:
   - https://<Fully Qualified Domain Name of the MiCollab server or controller>/server-manager
   or
   - https://<IP Address of the MiCollab server or controller>/server-manager

2. Enter User Name (default is "admin") and the system Password you created during installation, and then click Login. The administrator portal opens.
3. Do one of the following:
Installing Virtual MiCollab in a VMware Environment

4. By default, MiCollab is configured to send a Welcome E-mail to new users. The e-mail contains
   - a link to the My Unified Communications web portal, and
   - the user’s login ID, password, and passcode

   See Configure Service Information Email in the MiCollab Administrator online help for the Welcome E-mail configuration options. In order for the system to list the Speech Auto Attendant pilot/access number in the Welcome E-mail, you must enter the pilot number into the Network Element tab of the USP application.

   If you choose to disable the Welcome E-mail functionality, you will need to advise users of the URL for the MiCollab End User portal:
   - https://<Fully Qualified Domain Name of the MiCollab server>/portal
   - https://<IP Address of the MiCollab server or controller>/portal


INSTALL WEB CERTIFICATE

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

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

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

For instructions on how to install a third-party SSL certificate, refer to the Manage Web Server Certificate topic in the Server Manager online help for details.

   • To prevent the Security Alert warning from appearing on client stations on the local network, purchase a Secure Sockets Layer (SSL) certificate for the vMiCollab virtual appliance and then import it onto the vMiCollab virtual appliance.
   • To prevent the Security Alert warning from appearing on remote client stations, purchase a Secure Sockets Layer (SSL) certificate for the MBG Web Proxy server and then import it onto the MBG Web Proxy server.
ALLOW "TRUSTED NETWORK" ACCESS

Access to the vMiCollab virtual appliance is restricted to your local network (or subnet) by default. If your ICP or some of your users or phones are on a different subnet than the vMiCollab virtual appliance, it is necessary to allow them access. First, you must configure them as a trusted local network and then you can grant them express permission.

To configure Trusted Networks:

1. In the vSphere Client, right-click on the your vMiCollab appliance (for example: vMiCollab 7.3.3.0 build) and select Open Console. The vMiCollab virtual appliance console opens.
2. Log into the MiCollab server console. The server console Welcome menu is displayed.
3. Select Manage trusted networks from the menu and select Next.
4. Select Add IPv4 trusted network or Add IPv6 trusted network and select Next.
5. Enter the Trusted Network IP address of the network to which you are granting access. (For example, 168.195.52.0). Select Next.
6. Enter the Trusted Network Mask to apply to the network address. (For example, if your network IP address is 168.195.52.0 and you want to allow access to all network IP addresses in the range from 1 to 255, enter 255.255.255.0. This allows IP addresses 168.195.52.1 through 168.195.52.255 to access your virtual appliance).
7. Enter the Trusted Network Router Address. (IP address of the router on your local network).
8. Select Next. The local network is added.
9. Repeat steps 1 through 5 to configure additional trusted networks.

To grant secure shell access to the trusted local network you have created:

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 70).
3. In the Secure Shell Access field, select one of the following:
   - No Access: select this option to restrict access to your own local network
   - Allow access only from trusted and remote management networks: select this option to allow access to selected trusted local networks (required if using Mitel Integrated Configuration Wizard) and remote management networks. This is the recommended setting
   - Allow Public access (entire Internet): select this option to allow access to the entire Internet. This setting requires a strong SSH (admin) password; its use is NOT recommended.
4. In the Allow administrative command line access over secure shell field, do one of the following:
   - select Yes to allow users to connect to the virtual appliance and log in as "root"
   - select No to restrict users from logging in as "root".
5. In the Allow secure shell access using standard passwords field, do one of the following:
Installing Virtual MiCollab in a VMware Environment

- select **Yes** to allow users to connect to your virtual appliance using a standard password
- select **No** to restrict virtual appliance access to users with RSA Authentication.

6. Click **Save**.

SET SYSTEM LANGUAGE

After the initial installation of a new system, the system language is set to US English. You can set the language of the MiCollab End User portal and the Telephone User Interface (TUI) for the MiCollab application end-users from the server manager. End users can set the language of their MiCollab End User interface from their portal login page and set the prompt language from their Settings page.

The MiCollab software is installed with North American English as the default language. To change the default system language to one of the other supported languages:

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 70).

2. Under **Configuration**, click **MiCollab Language**.

3. Select the desired language from the Language drop-down box.

4. Click **Save**.

5. If your system uses the Speech Auto Attendant application, set the SAA prompt language. The MiCollab system language setting does not control the prompt language used by the Speech Auto Attendant application. The MiCollab Speech Auto Attendant only supports two languages: UK English and NA English. To change the Speech Auto Attendant language:

   - Under **Applications**, click **NuPoint Web Console**.
   - Under **Auto Attendant**, click **Misc. Parameters**.
   - Select the desired **Primary Language**, and then click **Save**.
   - Under **Auto Attendant**, click **Data Source**.
   - Click **Force Update**.

6. If required, configure MiTeam. MiTeam provides Cloud-based collaboration features for UCC Premium users. Note that MiTeam is only supported for MiCollab Client Integrated mode. Refer to the **MiCollab Client Administrator Guide** for configuration requirements.
SYNCHRONIZE MICOLLAB CLIENT SERVER WITH MICOLLAB AWV SOFTWARE VERSIONS

To support video, the MiCollab Client server must be synchronized with the latest MiCollab AWV software versions:

1. In MiCollab server manager, under Applications, click MiCollab Client Service.
2. Click Configure MiCollab Client Service.
3. Click the Collaboration tab.
4. Click the Local AWV Server link.
5. Click Sync Now. The MiCollab AWV Server and Client software versions are updated.
6. Click Save.

PERFORM INITIAL CONFIGURATION OF APPLICATIONS

Proceed to “Initial Configuration” on page 75.
Chapter 6

INITIAL CONFIGURATION
INTRODUCTION

Initial configuration consists of the following tasks:

- Collect Site Configuration Information
- Configure MiCollab Client Mode
- Configure Platform and Application Resources
  - Run the Mitel Integrated Configuration Wizard, or
  - Configure the Platform and Application Resources Manually
- Configure Users and Services
- Configure Flow Through Provisioning (MiVoice Business only)
- Configure Integrated Directory Services
- Configure Applications Settings
- Backup Database

COLLECT SITE CONFIGURATION INFORMATION

Collect the site configuration information applicable to your site and record it in the following table.

Table 5: Site Configuration Information

<table>
<thead>
<tr>
<th>STEP</th>
<th>CONFIGURATION INFORMATION</th>
<th>RECORD DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Platform and Application Resources</td>
<td>Greenfield site with New MiCollab and New MiVoice Business</td>
<td>Run MiCW (see “Flow Through Provisioning: Adding Greenfield MiCollab to Greenfield MiVB Servers” on page 157)</td>
</tr>
<tr>
<td>Configure Platform and Application Resources</td>
<td>New MiCollab server with existing supported</td>
<td>Configure Manually (see the MiCollab Platform Integration Guide).</td>
</tr>
<tr>
<td>Server Details</td>
<td>Communication platform</td>
<td>IP Address:</td>
</tr>
<tr>
<td></td>
<td>System Login:</td>
<td>Password:</td>
</tr>
<tr>
<td></td>
<td>MiCollab Server</td>
<td>Password:</td>
</tr>
<tr>
<td>MiCW off line configuration file available?</td>
<td>□ Yes</td>
<td>Filename:</td>
</tr>
<tr>
<td></td>
<td>□ No</td>
<td>File Location:</td>
</tr>
<tr>
<td>Start sharing MiVoice Business and MiCollab databases (either run MiCW or manually start sharing from a MiVoice Business element)</td>
<td>Recommended (for MiVoice Business integrations only)</td>
<td>□ Yes</td>
</tr>
</tbody>
</table>
### Table 5: Site Configuration Information

<table>
<thead>
<tr>
<th>STEP</th>
<th>CONFIGURATION INFORMATION</th>
<th>RECORD DETAILS</th>
</tr>
</thead>
</table>
| Device Resiliency  
(MiVoice Business only) | Resilient configuration with MiVoice Businesses required? Yes | |
| MiCollab Resource Provisioning  
(Voice Mail - NuPoint) | Hunt Group DN 7000  
with 4 ports starting at 6001  
MWI Type HCI Reroute:  
HCi Hunt Group extension: 6400  
Voice Mail Port: | |
| MiCollab Resource Provisioning  
(Speech Auto Attendant) | Record - A - Call licensed  
Record-A-Call Hunt Group DN 7000  
with 1 port starting at 6801 | |
| MiCollab Resource Provisioning  
(Mitel Collaboration Advanced) | Hunt Group DN 6850  
with 3 ports starting at 6851  
Web Conferencing Name  
Administrator Email  
Main Dial In Number | |
| MiCollab Resource Provisioning  
(MiCollab AWV) | Hunt Group DN 6850  
with 3 ports starting at 6851  
Web Conferencing Name  
Administrator Email  
Main Dial In Number  
Toll-Free Dial In Number  
Toll-Free Dial In Number | |
| MiCollab Client Integration | Identify required Integration Mode  
(see "Configure MiCollab Client Mode" on page 79 for details)  
Integrated?  
or  
Co-located? | |
### CONFIGURE MICOLLAB CLIENT MODE

The MiCollab Client application is supported in either of the following modes:

**Integrated Mode**: In this mode, the MiCollab system keeps the Users and Services database and MiCollab Client database synchronized so they function like a single database on the MiCollab server.

---

**Table 5: Site Configuration Information**

<table>
<thead>
<tr>
<th>STEP</th>
<th>CONFIGURATION INFORMATION</th>
<th>RECORD DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>USP Roles and Templates</td>
<td>☐ Use UCC licensing default templates?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>☐ Create roles and templates?</td>
<td></td>
</tr>
<tr>
<td>Role Name:</td>
<td>Associated Template Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Provisioning Method</td>
<td>Mitel Integrated Config Wizard,</td>
<td>☐</td>
</tr>
<tr>
<td>User Provisioning Method</td>
<td>Bulk User Import data from file, or</td>
<td>☐</td>
</tr>
<tr>
<td></td>
<td>Sync AD database with MiCollab.</td>
<td>☐</td>
</tr>
<tr>
<td>User Import File Type</td>
<td>BUPEXample CSV ☐</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSV ☐</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LDIF ☐</td>
<td></td>
</tr>
<tr>
<td>Filename</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provision MiVoice Business</td>
<td>DID Number Range</td>
<td></td>
</tr>
<tr>
<td>Advanced Features</td>
<td>MiVoice Business System Groups</td>
<td></td>
</tr>
<tr>
<td>MiCollab IDS Integration</td>
<td>Required, or</td>
<td>☐</td>
</tr>
<tr>
<td>(See Integrated Directory Services</td>
<td>Not Required</td>
<td>☐</td>
</tr>
<tr>
<td>Configuration in the Server Manager</td>
<td>Migration from existing MiVoice Business</td>
<td>☐</td>
</tr>
<tr>
<td>online help)</td>
<td>or MiCollab application IDS integration</td>
<td></td>
</tr>
</tbody>
</table>
It allows you to provision MiCollab Client services from the MiCollab Users and Services application and supports flow through provisioning of the MiCollab Client services on the MiVoice Business platform(s). This is the recommended mode for sites that meet the integration requirements. Integrated Mode is required to support MiCollab IDS.

**Co-located Mode:** Prior to MAS Release 4.0, MiCollab Client is supported only in co-located mode. In this mode, the Users and Services data and MiCollab Client data are contained in separate, independent databases on the MiCollab server. This mode is supported for sites with either MiVoice Business or MiVoice Office 250 platforms. With this mode, you must provision MiCollab Client services separately from the MiCollab Client Server application interface.

Flow through provisioning is supported for both Integrated and Co-located mode; however you cannot run the MiCollab Client Integration Wizard after Flow through provisioning has been enabled. If you are currently in Co-located mode and want to transition to Integrated mode, do this before configuring Flow Through Provisioning.

---

**Note:** After a system is in integrated mode, you can only change it back to co-located mode by re-installing MiCollab.

**Note:** Integrated Mode is recommended for sites with MiVoice Business systems.

**Note:** Vidyo integration is not supported in co-located mode.

**Note:** MiCollab Release 6.0 SP1 was your last opportunity to integrate a MiCollab Client Enterprise database with the MiCollab Users and Services database.

---

**CO-LOCATED MODE OR INTEGRATED MODE?**

Your system should remain in co-located mode only if your site requires any of the following:

- MiCollab with MiVoice Office 250 platforms
- Multiple MiCollab AWV servers
- MiCollab AWV with LDAP configuration
- MiCollab Client Integration with Active Directory
- Multiple MiCollab Client Enterprises (Note that you cannot enter integrated mode if you have an Enterprise configured)
- Digital Network Interface Card (DNIC) sets. Although co-located mode supports DNIC sets, integrated mode does NOT.
- MiCollab Client referencing non-local voicemail servers. (MiCollab Client Integrated mode only supports the MiCollab NuPoint application, so the MiCollab Client voice mail server field must be populated with the MiCollab IP address).
- Standalone MiCollab Client Server languages that are not supported by MiCollab. The following MiCollab Client Server languages are not supported by MiCollab:
  - Chinese (Simplified)
To remain in co-located mode do not run the wizard.

**CONFIGURING INTEGRATED MODE**

By default, MiCollab systems are in co-located mode. You must run the wizard to put a MiCollab system into Integrated Mode.

**Note:** Do not run the MiCollab Client Integration Wizard on a system which is either SDS sharing or was previously SDS sharing with MiVoice Business.

**Note:** Make sure you have installed latest MiCollab applications from ServiceLink > Install Applications and set the PBX type. For more details, see “Install Application Software” on page 70.

*For MiCollab Server and vMiCollab Deployments:*

1. Log into the MiCollab Server Manager.
2. Under **Configuration**, click **MiCollab Client Integration Wizard**.
3. Follow the prompts to run the wizard.

**SYNCHRONIZE MICOLLAB CLIENT SERVER WITH MICOLLAB AWV SOFTWARE VERSIONS**

To support video, the MiCollab Client server must be synchronized with the latest MiCollab AWV software versions:

**Note:** If MiCollab Client is being installed in co-located mode, you must first create an Enterprise in order to enable the MiCollab Client application interface tabs. If you ran the MiCollab Client Integration Wizard, it created an Enterprise for you.

1. In MiCollab server manager, under **Applications**, click **MiCollab Client Service**.
2. Click **Configure MiCollab Client Service**.
3. Click the **Collaboration** tab.
4. Click the **Local AWV Server** link.
5. Click **Sync Now**. The MiCollab AWV Server and Client software versions are updated.
6. Click **Save**.

**CONFIGURE PLATFORM AND APPLICATION RESOURCES**

Depending on your site topology, you either run the Mitel Integrated Configuration Wizard or perform the configuration manually through the server administration programming interfaces:
• If you are installing a Greenfield site with a new MiCollab and new MiVoice Business systems, the recommended "best practice" is to run the Mitel Integrated Configuration Wizard. The wizard also starts sharing and synchronizes the MiVoice Business and MiCollab databases. To support Flow Through Provisioning, the databases must be sharing. See “Configure Flow Through Provisioning” on page 82 for details.

• If you are installing a new MiCollab server with an existing MiVoice Business systems the recommended "best practice" is to configure the platform and applications resources manually and then start sharing the databases from the MiVoice Business.

For MiVoice Office 250, MiVoice Office 400, MiVoice 5000, or MiVoice MX-ONE communication platforms, you must configure the platform and application resources manually. See the MiCollab Platform Integration Guide for instructions.

CONFIGURE USERS AND SERVICES

MIVOICE BUSINESS PLATFORM
• “Configure Flow Through Provisioning” on page 82 (Recommended).
  or
• Manually perform user and services provisioning from the USP application.
  or
• Configure “Configure Integrated Directory Services” on page 94, if required.

MIVOICE OFFICE 250
1. Program the users on the communication platform.
2. Export the user data from the communication platform to a CSV file.
3. Import the CSV file into the MiCollab Bulk User Provisioning tool. See the Bulk Import of User Information topic in the USP application online help for instructions.
4. Assign roles and templates to the users through the Bulk User Provisioning tool.
5. Program the phone and application services on the communications platform. Because MiCollab does not support Flow Through Provisioning to these communications platforms any future user programming on MiCollab must also be manually programmed on the MiVoice Office 250 or MiVoice Office 400.

CONFIGURE FLOW THROUGH PROVISIONING

Flow Through Provisioning uses System Data Synchronization (SDS) to synchronize updates made between the MiCollab and MiVoice Business system databases. The following data is synchronized:
- Network Elements
- Roles and Templates
- Users and Service Hosting, and
- Phone Services

For MiCollab sites with MiVoice Business servers Flow Through Provisioning provides the following advantages:

• Allows you to perform user and service provisioning for a network of MiVoice Business servers from the MiCollab User and Services application. Although changes made to the phones services data on a MiVoice Business system are distributed to the other system databases in the network, including the MiCollab, the recommended "best" practice is to perform all user and service provisioning from the MiCollab USP application.

• Provides a Reconcile Wizard that migrates an existing MiVoice Business database to a newly installed MiCollab. In the case of an upgrade, this wizard also helps you reconcile any conflicting user entries, roles, and templates.

• Allows you to view and manage distribution errors and pending updates. If you make an update in the MiCollab USP database and the update is not successfully shared to all the other elements in the sharing network, a distribution error is sent to the MiCollab SDS Distribution Errors application. If the number of distribution errors exceeds an SDS alarm threshold, a data distribution alarm is generated in the server manager Event Viewer application.

• Provides single-sign on to the administration interfaces for the Mitel communications network. After you sign into the MiCollab server manager, you are granted "reach-through" access to the MiVoice Business system administration tools and vice versa.

• Supports context sensitive Reach Through from the User and Services application pages to specific MiVoice Business programming forms. You can modify specific system settings by launching the system administration tool of the MiVoice Business system that hosts the user’s phone. For example, you can reach-through to the User Configuration form and modify user parameters. SDS then shares the user updates to the other MiVoice Business systems in the network.

SYSTEM REQUIREMENTS

• MiCollab Release 7.0 or higher
• MiVoice Business Release 7.2 or higher

CONDITIONS

• Flow Through Provisioning is only supported between MiCollab systems and MiVoice Business platforms.
• MiCollab Release 7.0 or higher is required.
• MiVoice Business Release 7.2 or higher is required.
• If MiCollab Client is in co-located mode and you start sharing, then MiCollab Client must remain in co-located mode. The MiCollab Client Integration Wizard is not available after you initiate sharing from the MiVoice Business with MiCollab.
• Flow Through Provisioning is only supported from one MiCollab system. It is not supported for multiple MiCollab systems in the same SDS sharing network. You can only include one MiCollab system to share within a SDS sharing network.

• If MiCollab is managing a group of MiVoice Business systems, they must be configured within an SDS sharing cluster. All the MiVoice Business servers in the cluster must be at Release 7.2 or higher.

• Flow Through Provisioning must be enabled (started) either from the Mitel Integrated Configuration wizard or manually from a MiVoice Business platform in the cluster.

• Reach through is enabled from MiCollab USP to the MiVoice Business (MiVB) system administration tool using the MiVoice Business "system" administrator account. The MiVoice Business must have an administrator account configured in the User Authorization Profiles form with Login ID "system" and System Admin authorization set to "True".

• To support reach through navigation from MiCollab server manager to the MiVoice Business system administration tool you must download the common Mitel Root Certificate from one of the MiVoice Business servers and import it into your Internet Explorer or FireFox browser as a ‘Trusted Root Certification Authority’.

• You can reach through from MiCollab into other administration clusters provided that the MiCollab is in the same administration group that started the sharing to the MiCollab. In addition, specific forms must be shared across all elements. See “Supported SDS Sharing Scopes” on page 211 for a list of the forms that must be shared.

• The USP application allows you to manage the local MiCollab application services and the remote MiVoice Business phone services.

• The MiCollab USP database lists all the users in the MiVoice Business network. The USP application identifies the host network elements for extensions in the Phone tab and application services tabs. For example: 3001 (on Local_30) where extension3001 is hosted on network element Local_30.

• A maximum of three phones are supported in a shared MiCollab template. You cannot use a template that is programmed with more than three phones.

• If resiliency is configured for a MiVoice Business solution, data updates are sent from MiCollab to the primary controller. If the primary controller is out of service, the MiCollab USP application does not provide data updates to the secondary controller. Instead, an error message is presented in MiCollab indicating that the primary controller cannot be reached.

• Although you can view analog and DNIC phones, you cannot create them.

• Synchronization is bidirectional. Changes made to users, phones, templates, multi-device user groups, and personal ring groups in any remote MiVoice Business element in the sharing network are reflected in the MiCollab server's USP entry.

• The synchronization of MiVoice Business elements with MiCollab takes substantially longer than the synchronization of just MiVoice Business element form data.]

• If Flow Through Provisioning is enabled, IDS Integration must be enabled from MiCollab to Active Directory, not from MiVoice Business to Active Directory.
• MiVoice Business allows you to associate multiple users with the same directory number; however, MiCollab does not support this functionality. If you associate multiple users with the same directory number from the MiVoice Business User and Services Configuration form, the association is not shown in the MiCollab Users and Services application. The following SDS Distribution Error is also generated: “Cannot associate more than one user to the same phone service”.

TOPOLOGY

• You control the sharing topology of the solution from the following System Data Synchronization (SDS) forms in the MiVoice Business System Administration Tool:
  - Network Elements
  - Cluster Elements
  - Admin Groups
  - SDS Forms Comparison
  - SDS Form Sharing.

• Sharing is only supported to one cluster. It is not possible to start sharing with MiCollab from an SDS network which contains more than one MiVoice Business cluster. However, you do not have to have a cluster defined. MiCollab can perform flow through provisioning to a single MiVoice Business; however, if there are multiple MiVoice Business elements in the network which are hosting phone services, you must create a cluster before flow through provisioning can be used to manage all the MiVoice Business systems.

• All MiVoice Business controllers must be active and reachable from MiCollab when sharing is started. It is not possible to create phone services on a MiVoice Business controller which is offline. Flow through provisioning does not fall back to the resilient controller.

• The MiVoice Business server must be within the networks defined in MiCollab. If it is not, then start sharing will fail to connect to MiCollab after 60 seconds. You change the configuration from the Network Elements page in the MiCollab server manager.
• You can configure how data is shared among the MiVoice Business elements using the 'SDS Form Sharing' form in the MiVoice Business System Administration Tool. However, the flow through provisioning feature requires specific MiVoice Business forms to be shared with MiCollab, so you cannot remove sharing from these forms, nor can you share them at a scope which MiCollab cannot participate in. These restrictions are enforced by MiVoice Business. If an invalid sharing scope is selected a message is presented in MiVoice Business stating the sync has failed and to review the messages in the SDS-CC, MOM server and message logs in MiCollab. Refer to Appendix D on page 209 for the supported sharing scopes.

• The simplest supported configuration is one MiCollab server and one MiVoice Business server in a single (default) administration group with no cluster defined. If there is no cluster defined, MiCollab only shares its data with the MiVoice Business server that started sharing with MiCollab. Flow Through Provisioning is not offered to other MiVoice Business servers in this configuration even if they are included in the local administration group.

• To support Flow Through Provisioning to multiple MiVoice Business servers, a cluster must be defined. Only a single cluster is supported. MiVoice Business will not allow ‘Start Sharing’ with MiCollab if there are multiple clusters. After sharing has started with MiCollab, MiVoice Business will disallow the creation of a second cluster.

• To avoid role and template conflicts, it is recommended that you segregate the MiVoice Business servers into separate administration groups and change the sharing scope of roles and user templates to "Admin Group" before you start sharing with the first MiCollab server.

• Ensure that all MiVoice Business elements in the sharing network are configured with an IP address or FQDN. MiCollab will not support a network element unless it is provisioned with an IP address or FQDN. If a MiVoice Business element is provisioned in the network without an IP address or FQDN then sharing with MiCollab cannot be established. The Start Sharing operation will fail with a message to check the MiCollab logs.

DEPARTMENTS AND LOCATIONS
• Departments and Locations are shared by default at the network scope, although you can narrow down the scope to just the Admin Group in the 'Shared Forms Configuration' form in MiVoice Business System Administration Tool.

ROLES AND TEMPLATES
• A shared template definition is used to create phone services. Flow Through Provisioning is only able to offer the ability to create phone services on MiVoice Business servers which are sharing role and template data.

• Role and template data is shared among the MiCollab server and the MiVoice Business servers in the same Admin Group. Role and template data is not shared with other MiCollab servers (only one MiCollab server is allowed in an Admin Group). Roles and templates are merged during the synchronization process and may need to be reconciled.

• Templates can be added by either copying an existing template (in the Edit Template page) or by adding a new template. You can edit templates either in USP or MiVoice Business System Administration Tool and the changes are shared. You need to refresh the form to see changes that were made on a remote network element.
• If MiVoice Business was upgraded from Release 6.0, there may be legacy templates in the database. These templates will not be imported into MiCollab and will not appear in MiCollab USP. If you attempt to create a new template with the same name as a legacy template, an error is presented.

• USP can manage all the service components within a user and service template, but only a subset of the fields which are offered in the MiVoice Business System Administration forms are available in USP. Use Reach Through to manage the complete phone service template on the MiVoice Business (for example, to edit feature key templates).

USERS AND SERVICES
• Create users from MiCollab USP using pre-defined roles and templates. Do not create users from the MiVoice Business servers.

• The USP directory only displays phones that are assigned to users. However, the MiVoice Business supports phones that do not have users associated with them. To manage these phones from USP, add a new user to the phone or associate a user with the phone in the MiVoice Business User and Services Configuration form. After you assign a user to the phone, the user and phone will appear in the USP directory and you can add services to the user.

• You cannot assign DNIC or analog phone services to users from USP. However, DNI analog phones that have been created on the MiVoice Business system administration tool are displayed in the USP directory and can be modified or deleted.

• The USP directory does not list the following MiVoice Business directory numbers:
  - Phones that are not associated with users
  - Directory numbers that are associated with line appearances on feature keys
  - Local-only phones
  - Directory numbers that are used in certain types of hunt groups.

• It is only possible to manage multi-line MiNET and SIP devices. Single line, DNIC and analog devices cannot be created from the Users and Services application and are not listed in the directory. The same is true for other types of service such as traditional ACD agents, IP consoles, non-prime broadcast groups, and so forth.

• The Users and Services application does not manage phones which are not associated with a user.

FULLY QUALIFIED DOMAIN NAME (FQDN) FOR CLOUD DEPLOYMENTS

The following Domain Name Server (DNS) configurations are possible in Cloud solution deployments:
• MiVoice Business server may or may not be resolvable in DNS.
• MiCollab server may or may not be resolvable in DNS.
• Any of the servers which make up the solution may resolve to a different IP address inside the LAN versus out in the WAN/cloud (split DNS).
• Any of the servers may not resolve internally, but may resolve externally (partial DNS).
• An administrator may wish to make use of Reach Through outside in the cloud, inside the LAN, or through a web proxy.

• Mitel Standard Linux operating system can be configured to use a corporate (external) DNS server.

The following conditions apply to programming FQDN(s):

• When MiCollab is initially deployed, the IP address that you enter for the local (LAN) interface is added to the network element in the Network Element list. The FQDN field is initially blank.

• Enter the FQDN for the MiCollab server at any time by editing the local network element in the Network Element page. The FQDN can be the same as the host name and domain that is entered in MiCollab server console or it may be a different FQDN which is only resolvable externally.

• After Mitel Integrated Configuration Wizard adds MiVoice Business servers to the MiCollab server, you must provide the IP address. You can also provide an FQDN. This is also the case when you add MiVoice Business servers to the network.

  Note: The host name and domain entered during server commissioning may not be resolvable anywhere except inside the MSL system. For this reason, the MiCollab server will not attempt to reverse-DNS in order to ‘automatically’ detect FQDNs.

CONFIGURATION OVERVIEW

The procedure to configure Flow Through Configuration is dependent on your site configuration:

• “Greenfield: New MiCollab with one New MiVB Server” on page 89

• “Greenfield: New MiCollab Server with Multiple New MiVB Servers” on page 91

• “Flow Through Provisioning: Adding Greenfield MiCollab to Brownfield MiVB Servers” on page 173

• “Flow Through Provisioning: Brownfield MiCollab with Brownfield MiVB Servers” on page 197
GREENFIELD: NEW MICOLLAB WITH ONE NEW MIVB SERVER

The simplest supported configuration for Flow Through Provisioning is shown in Figure 14.

Figure 14: MiCollab with one MiVB Server

USING MICW

For a single greenfield MiCollab with a single greenfield MiVoice Business, you can perform the configuration from the Mitel Integrated Configuration Wizard (MiCW).

1. Install and license the MiVoice Business server using the Software Installer.

2. In the MiVoice Business SDS Form Sharing form, ensure that data is being shared at scopes that are supported for Flow Through Provisioning (see Appendix D on page 209).

3. Run the Mitel Integrated Configuration Wizard against both the MiVoice Business platform and the MiCollab system in a single session to
   - configure the MiVoice Business server.
   - automatically add the MiCollab server to the network, start sharing the databases, and synchronizes the data.
   - configure the application resources on the MiCollab server, and
   - configure the MiCollab application resources on the MiVoice Business platform.

Refer to “Greenfield MiCollab with a Single Greenfield MiVB Platform” on page 159 for detailed instructions on how to run MiCW for this configuration.
MANUAL CONFIGURATION

1. Install and license the MiVoice Business server using the Software Installer.

2. Manually provision the MiCollab and MiVoice Business application system resources. Refer to the MiCollab Platform Integration Guide.

3. Add the MiCollab server as a network element with server type MSL Server (MiCollab) to the Network Element form of the MiVoice platform:
   - Log into the System Administration Tool of the MiVoice Business platform.
   - Choose to view forms alphabetically.
   - In the left forms menu, click Network Elements.
   - Click Add and enter the MiCollab server name and IP address with type MSL Server (MiCollab). Enter the first eight characters of the MiCollab server name. The name must be unique.

4. Start sharing with the MiCollab server.
   - In the MiVoice Business SDS Form Sharing form, ensure that data is being shared at scopes that are supported for Flow Through Provisioning (see Appendix D on page 209).
   - In the Network Elements form, check the box of the MiCollab server. The PBX type is MSL Server (MiCollab) type.
   - Click Start Sharing.
   - Click OK. After the start sharing operation is complete, reload (refresh) the MiCollab server manager screen. The Data Sharing field for the MiCollab server (MSL Server) will change to YES.

This operation also synchronizes any elements in the MiCollab network element tab with the MiVoice Business Network Element form.

Note: You must enter both the MiVoice Business and MiCollab provisioning data in a single Mitel Integrated Configuration Wizard session in order to start sharing (that is, you only run the wizard once).

Note: After sharing is started, a Major alarm is generated on all the elements. On each element, configure SNMP Agent support and align the community strings to clear the alarms.

4. Proceed to “Configure Users and Services” on page 82.
5. Configure the MiCollab applications. Refer to the MiCollab application online helps for instructions.

6. Proceed to “Configure Users and Services” on page 82.

GREENFIELD: NEW MICOLLAB SERVER WITH MULTIPLE NEW MIVB SERVERS

In this topology you configure multiple MiVoice Business servers in a cluster. Phones can be created with resilient hosting on another MiVoice Business server. For a topology that includes MiCollab with multiple MiVoice Business elements, the first run of MiCW should be in "Create Cluster" mode and MiCollab properties should not be configured. The subsequent runs of MiCW should be against the other MiVB elements in "Join Cluster" mode. The last run against a MiVoice Business element should be programmed with MiCollab application resources.

![Figure 15: MiCollab Server with Multiple MiVB Servers](image-url)
USING MICW

1. Install and license the MiVoice Business servers using Software Installer.

2. In the MiVoice Business SDS Form Sharing form, ensure that data is being shared at scopes that are supported for Flow Through Provisioning (see Appendix D on page 209).

3. Run MiCW in "Create new cluster" mode against MiVoice Business B to
   - Create a new cluster, and
   - Configure the MiCollab applications resources on MiCollab and
   - Configure the MiCollab application resources on MiVoice Business B.

4. Run MiCW in "Join existing cluster" mode against MiVoice Business A (with MiVoice Business B as master) and MiCollab in a single session to
   - Add MiVoice Business server B to the cluster.
   - Join and synchronize the MiVoice Business servers.
   - Join and synchronize the MiCollab server. The wizard automatically adds all three elements to the admin group.
   - Configure the MiCollab server including MiCollab applications (MiVoice Business B can be selected as the secondary host of the resilient ports and hunt groups in the application data sections).

Refer to “Adding Greenfield MiCollab To a New MiVB Cluster” on page 164 for detailed instructions on how to run MiCW for this configuration.

Note: You must enter both the MiVoice Business and MiCollab provisioning data in a single Mitel Integrated Configuration Wizard session in order to start sharing.

At the end of the process, the MiVoice Business servers and MiCollab server are joined in an SDS network consisting of one admin group and one cluster, both MiVoice Business servers will be members of the cluster and all elements will be members of the admin group. All elements are sharing and all elements are in sync. The MiCollab applications are provisioned and running. And, the roles, templates, users and services entered in MiCollab USP are present in both MiCollab USP and MiVoice Business System Administration Tool.

Note: After sharing is started, a Major alarm is generated on all the elements. On each element, configure SNMP Agent support and align the community strings to clear the alarms.

5. Proceed to “Configure Users and Services” on page 82.

MANUAL CONFIGURATION

1. Install and license the MiVoice Business servers using Software Installer.

2. Add one of the MiVoice Business servers to the Network Elements form in the voice network of the other.

3. Create a new cluster and add both MiVoice Business elements to the cluster, providing network element IDs and cluster dialing digits.

4. Start sharing the elements from one of the MiVoice Business elements.
5. Provision the application resources on the MiVoice Business servers (set the secondary host for resiliency).

6. Add the MiCollab server as a network element with server type MSL Server (MiCollab) to the Network Element form in one of the MiVoice Business servers:
   - Log into the System Administration Tool of the MiVoice Business platform.
   - Choose to view forms alphabetically.
   - In the left forms menu, click **Network Elements**.
   - Click **Add** and enter the MiCollab server name and IP address with type MSL Server (MiCollab). The first eight characters of the MiCollab server name must be unique.

   **Note:** By default, the MiCollab server is added to the Network Element tab of Users and Services application.

7. Start sharing with the MiCollab server.
   - In the MiVoice Business SDS Form Sharing form, ensure that data is being shared at supported scopes for Flow Through Provisioning (see Appendix D on page 209).
   - In the Network Elements form, check the box of the MiCollab server.
   - Click **Start Sharing**.
   - Click **OK**. After the start sharing operation is complete, the Data Sharing field for the MiCollab server (MSL Server) will change to YES.

   This operation also synchronizes the entries in the MiCollab network element tab with the MiVoice Business Network Element form.

   **Note:** Templates are associated with the network element from which you started sharing.

   **Note:** After sharing is started, a Major alarm is generated on all the elements. On each element, configure SNMP Agent support and align the community strings to clear the alarms.

   **Note:** If the synchronization from MiVoice Business to MiCollab fails, check the error logs on MiCollab in `sdscctcurrent` directory. If synchronization failed for "Hosted User Service", run the GDM CHECK USERANDSERVICE and GDM REPAIR USERANDSERVICE maintenance commands from the MiVoice Business System Administration Tool.

8. Configure the MiCollab applications. Refer to the MiCollab application online helps for instructions.

9. Proceed to “Configure Users and Services” on page 82.

**VERIFY THAT SHARING HAS STARTED ON MICOLLAB**

To verify that sharing has started on MiCollab:

1. Log into the MiCollab server manager.
2. Under **Administration**, click **Event Viewer**.
3. Confirm that the following events are present.

4. Confirm that the following events are present:
   - Device Sync Completed
   - Device Sync Started
   - User Sync Completed
   - User Sync Started
   - Device Data Notifications Started
   - Device Data Notifications Completed
   - Problem Detected (This is a transient condition and is normal)
   - SDS Join Completes
   - SDS Join Started

CHECK MICOLLAB SERVER FLOW THROUGH PROVISIONING LOGS

The following logs are applicable to Flow Through Provisioning:

- Tomcat - web application container in which USP runs
- MOM Server: - the server that provides repository services to MiCollab
- SDS-CC - component that maintains data synchronization with MiVoice Business
- UPM - application provisioning module that maintains sync with the installed applications.

To view these logs:

1. Open a secure shell connection (SSH) to the MiCollab server.
   
   Login "root"
   Username: default

2. Run the following command:
   
   [root@micollab ~ ] # tail - F /var/log/mom-server/current /var/log/tomcat/current /var/log/sdscc/current /var/log/upm/current

CONFIGURE INTEGRATED DIRECTORY SERVICES

You can integrate the user database of a corporate directory service with the MiCollab database to minimize data entry and administration. The user data on the corporate directory server is synchronized with the MiCollab database using Lightweight Directory Access Protocol (LDAP). If Flow Through Provisioning is enabled, then MiCollab distributes the user data to the MiVoice Business platforms. Synchronization occurs in one direction only—from the directory server to MiCollab. Refer to Integrated Directory Services in the MiCollab server manager online help for instructions.

Also, see Non-Corporate Contacts for instructions on how to add contacts to the MiCollab Client corporate directory.
CONFIGURE APPLICATION SETTINGS

Configure the MiCollab system application settings (for example, NP-UM ICP, NP-UM Line Groups, AWV web conference SIP server, and so forth) manually through the application administration interfaces. Refer to the application online help for instructions.

BACKUP DATABASE

After you have programmed the site configuration data, it is recommended that you make a backup of the MiCollab system database. See “Downgrading Application Software” on page 107. System installation is now complete.
Chapter 7

MAINTENANCE
UPGRADING MICOLLAB SOFTWARE

An upgrade is when you move a MiCollab system up to a new system software release. Before you can upgrade a pre-MAS 2.2 system to MiCollab 8.1 software, the system must be at a minimum of MAS Release 5.0 and valid software assurance (SWAS) must be active.

Table 6 identifies the supported upgrades and the required procedures.

Table 6: Upgrade Procedures

<table>
<thead>
<tr>
<th>SUPPORTED UPGRADES</th>
<th>UPGRADE PROCEDURES</th>
<th>WHEN TO USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAS Server 3.0 SP1 or later to MAS Server 5.0</td>
<td>You must install the MSL operating system (you cannot use the Upgrade option) and</td>
<td>You install the MSL 10.6 operating system and then download the software applications (with the exception of the NP-UM applications) off the AMC server. Refer to the Maintenance chapter in the MAS Release 5.0 Installation and Maintenance Guide for instructions on how to upgrade from MAS 3.0 SP1 to MAS 5.0.</td>
</tr>
<tr>
<td></td>
<td>upgrade MAS Applications from AMC (page 99).</td>
<td></td>
</tr>
<tr>
<td>MAS Server 5.0 or later to MiCollab Server 8.1</td>
<td>Perform a backup and restore with fresh install</td>
<td>&quot;Upgrade from MAS 5.0 or later to MiCollab 8.1 using Fresh Install&quot; on page 99.</td>
</tr>
<tr>
<td>vMAS 5.0 or later to vMiCollab 8.1</td>
<td>Deploy vMiCollab 8.1 OVA file and restore vMAS 5.0 or higher backup (page 103)</td>
<td>This is the preferred upgrade method. You must use this procedure if you want to upgrade from a Small Business deployment to an Enterprise deployment.</td>
</tr>
<tr>
<td>MAS Server 5.0 or later to vMiCollab 8.1</td>
<td>Convert from MiCollab Server to vMAS 5.0 (page 118) and then upgrade from vMAS 5.0</td>
<td>Use these procedures to convert a MAS Server 5.0 or later system to a vMiCollab 8.1 system.</td>
</tr>
<tr>
<td></td>
<td>to vMiCollab 8.1 (page 103)</td>
<td></td>
</tr>
<tr>
<td>MiCollab 8.x to MiCollab 8.y</td>
<td>Upgrade applications from server manager Service Link &gt; Install Applications panel.</td>
<td>Use this procedure, to apply dot releases.</td>
</tr>
<tr>
<td>MiCollab 8.x Service Pack Upgrades</td>
<td>Apply service packs from server manager ServiceLink &gt; Install Applications panel.</td>
<td>Use this procedure, to apply service pack upgrades.</td>
</tr>
</tbody>
</table>

UPGRADE FROM MAS 5.0 OR LATER TO MICOLLAB 8.1 USING FRESH INSTALL

This procedure applies to MiCollab Server or MiCollab Server Appliance software upgrades. This procedure requires a backup and restore with a fresh install.

CAUTION: The Customer Service Manager (CSM) application is not supported in MAS Release 4.0 or later. If the site requires the CSM application, you must migrate the existing CSM database to a standalone CSM system before you upgrade.
PREREQUISITES

- MiCollab Release 7.0 and later software is only supported on a 64-bit server architecture.
- To upgrade to MiCollab Release 8.1, your current system must be running MAS Release 5.0 or later and valid software assurance (SWAS) must be active.
- There is a connection available to the AMC.
- To support all the available MiCollab applications, the MiCollab Server or MiCollab Server Appliance requires a minimum of 6 GB of RAM (refer to the MSL Qualified Hardware List available on Mitel OnLine).
- Ensure that the database backup file contains the same application blades as the target MiCollab 6.0 system. If the database backup file contains a different set of application blades than the target MiCollab system, none of the blades will be restored. Review Table 8 and Table 9 on page 152 to ensure that your database meets the requirements and can be restored.
- The MAS 5.0 server or later database is backed up (see “Server Manager "Backup"” on page 108).
- You have verified your MAS 5.0 or later backup file (see “Verify Backup Data” on page 113 for details).
- All administrative applications on the MiCollab server are closed.
- The MiCollab server is NOT processing calls (Upgrading should be done outside of business hours.)

BACKUP AND RESTORE WITH FRESH INSTALL

1. Purchase the required MiCollab upgrade licenses and upgrade your AMC account. Refer to the latest MiCollab Release 8.x product bulletin on Mitel Online for details. To access the MiCollab product bulletin:
   - Log on to Mitel MiAccess (formerly known as Mitel Connect).
   - From the left menu, select InfoChannel.
   - Select Mitel - Worldwide as the InfoChannel.
   - Click Products & Solutions and then click MiCollab.
   - Click Product Announcement/Bulletin (PA).
2. Download the ISO files of the latest MSL software and the MiCollab application software. Follow the instructions on page 39.
3. Transfer the MSL_10.6.xx.x.iso software and application ISO files to either CDs, DVDs, or USB. See “Create Storage Media” on page 40.
4. Back up your existing MiCollab system database. See “Performing Backups” on page 108.
5. If you plan to use an existing backup file, verify it before performing the new installation (see “Verify Backup Data” on page 113).

**Note:** If verification is not successful, you will have to repeat the backup procedure. Do NOT start an upgrade without a verified backup file.
6. Insert the MSL software CD/DVD that you labeled as MSL_10.6.xx.x.iso in the CD/DVD drive of the server.

7. Reboot the server. After the server or controller reboots, you are presented with the server console.

8. Depending on your model of CD/DVD drive, you may be prompted to select the installation language. Use the Space bar on the keyboard to select the desired language and select Ok.

9. You are prompted to test the CD/DVD media. Select Ok to test the CD/DVD for validity and readability.

10. Choose your preferred keyboard from the list (default is us).

11. You are offered the following options:

   - Reinstall System
   - Upgrade existing Mitel Networks server 10.6.x.x system

   Select Reinstall System if you are upgrading to a new hardware platform. When you select this option, any previous MSL software and configuration settings are erased and new MSL software is installed. Select Upgrade existing Mitel Networks server 10.5.x.x. system, if the current system is at MSL 10.6.x.x.

12. Select your Time Zone from the list. Select Ok and wait. After approximately 2 minutes, the screen displays a warning that your disks will be formatted and asks for confirmation.

13. Click Yes.

14. Finishing the installation is automatic and takes only a few minutes. At the end of the process, you are prompted to remove any media and reboot the system.

15. Remove the CD/DVD media.

16. Press Enter to reboot and wait. After approximately 3 minutes, you are prompted to accept the end-user license.

17. Accept the End-User License.

18. When you are prompted to Restore from Backup, insert your backup storage media (USB device or CD/DVD) or access the backup file on the network share and then select Yes.

   CAUTION: If you select No, you will have to restart this procedure from Step 6.

   Note: If the system detects that an application service is mapped to user data, the application will automatically be included in the install. Only the mandatory applications are installed. To add other applications after the upgrade is complete, see “Installing Additional (Missing) Applications” on page 106.
19. When the restore is complete, remove the USB device or CD/DVD storage media.

20. Activate your ServiceLink account (Application Record ID).
   - In the MiCollab Server manager under ServiceLink, click Status.
   - If a service account ID (Application Record ID) is displayed on the Status page, click Sync.
   - Enter your Application Record ID and click Activate.

21. If the MiCollab Client application is supported on the system, the following message appears in the server manager: The MiCollab Client Application has been detected on your system. Please use the MiCollab Client Integration Wizard prior to managing the application. Click here to cancel this warning. You can either
   - integrate the MiCollab Client database with the MiCollab system database and support MiCollab Client in integrated mode. This is the recommended mode. See "Configure MiCollab Client Mode" on page 79 for the requirements and instructions. OR
   - cancel the warning and leave the MiCollab Client database in co-located mode. OR
   - cancel the warning and then migrate a standalone MiCollab Client database onto the MiCollab system in co-located mode. See "Migrate Standalone MiCollab Client to MiCollab Server or vMiCollab" on page 121 for requirements and instructions.

22. New fields were added to the User and Services Network Element form during the upgrade. Provision these new fields with appropriate settings:
   - In MiCollab server manager, under Applications, click Users and Services
   - Click the Network Elements tab.
   - Select the Network Element and click Edit. The "Standard Phone COS" and "Record-a-Call COS" settings were restored from the backup.
   - Enter a "Default COR".
   - Enter the "Call Reroute First Alternative (CRFA)" index number. On the MiVoice Business platform, program the CRFA index number with the desired destination number.

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

24. Perform a database backup of the newly upgraded system.
WARNING: AFTER YOU UPGRADE TO MICOLLAB RELEASE 7.2 OR LATER, YOU CANNOT RESTORE A BACKUP FROM A PRE-RELEASE 7.2 SYSTEM, SO IT IS CRITICAL THAT YOU MAKE A BACKUP NOW.

25. If the MiCollab system is connected to MiVoice Office 250 or MiVoice Office 400 platform(s), you must configure port 5058 on the MiVoice Office(s) to support SIP communication from the NuPoint application.

26. For deployments with MiVoice Business Gateways, upgrade them to the latest version.

27. If you are upgrading a MiCollab with MiVoice Business site, it is recommended that you configure the network to support Flow Through Provisioning:
   - See Flow Through Provisioning in the server manager online help for an overview
   - See “Flow Through Provisioning: Brownfield MiCollab with Brownfield MiVB Servers” on page 197 for instructions.

UPGRADE FROM VMAS 5.0 OR LATER TO VMICOLLAB 8.1

UPGRADE PREREQUISITES

☑ Ensure that the virtual machine has the required resources (see the Virtual Appliance Deployment Guide).

☑ To upgrade to MiCollab Release 8.1, your current system must be running Release 5.0 or later and valid software assurance (SWAS) must be active.

DEPLOY VMICOLLAB 8.1 OVA FILE AND RESTORE BACKUP

Note: If your restore includes NP-UM feature options and SAA-TTS data, these applications are not included in the OVA file and must be installed separately. If you fail to install required applications, you will see a warning banner in the server manager that specifies that these software applications are missing.

"Data for applications NuPoint SAA & TTS, NuPoint Fax Port Enable, NuPoint Record a Call have been restored from backup but these applications are not currently installed. The system may be unstable because of this. Please install these applications as soon as possible."

Note: NuPoint Record a Call option is not a part of the OVA. Insert the NuPoint DVD One to install the NuPoint Record a Call option.

1. Download the vMiCollab 8.1.x.x OVA file, NP-UM feature options.iso file and SAA-TTS.iso file from Mitel Online to a network drive or vSphere Client PC (see page 63 for instructions).

2. Backup the vMAS 5.0 or later database to a network drive or vSphere Client PC (see “Server Console "Perform Backup”” on page 112 for instructions).

3. Deploy the vMiCollab 8.1 OVA file on the host system (see page 64 for instructions).
4. Power up the vMiCollab VM.

5. Choose your preferred keyboard from the list (default is us).

6. You are prompted to restore. When the system prompts you with "Do you wish to restore from backup?", choose one of the following options:
   - Select **Restore from network share**. Follow the prompts to specify the location of the backup file and start the restore, or
   - Select **Restore from removable device**, or
   - Select **Restore from running server option** to retrieve the configuration from an existing MiCollab server. This option shuts down the server that you are retrieving the configuration from before bringing up the new server. It configures the new system with the IP address of the old system.

7. After responding to all prompts, click **Yes** to restore the backup data.

8. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the **Decryption password**. Click **Next** and then **Yes**.

9. After MSL completes the restore, select **Reboot Now**.

10. After the vMiCollab vApp has powered up, log into the MiCollab server manager:

11. In the server manager, under **ServiceLink**, click **Install Applications**.

12. Set the **PBX Type** and then click **Next**. The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.

13. Select the latest software version for installation.

14. Check the **Download from AMC** boxes of the required applications.

15. Click **Install**.

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

**Note:** For detailed instructions on how to install software in a virtual environment, including how to mount media (CD/DVD or USB) from a datastore, client or host device, refer to the **MiCollab Administrator online help**.

16. After the applications are installed, reboot the MiCollab server.
17. After the optional software is installed, check that all applications and application data is present.

18. If the MiCollab Client application is supported on the system, the following message appears in the server manager: The MiCollab Client Application has been detected on your system. Please use the MiCollab Client Integration Wizard prior to managing the application. Click [here] to cancel this warning. You can either
   - integrate the MiCollab Client database with the MiCollab system database and support MiCollab Client in integrated mode. This is the recommended mode. See "Configure MiCollab Client Mode" on page 79 for the requirements and instructions.
   OR
   - cancel the warning and leave the MiCollab Client database in co-located mode.
   OR
   - cancel the warning and then migrate a standalone MiCollab Client database onto the MiCollab system in co-located mode. See "Migrate Standalone MiCollab Client to MiCollab Server or vMiCollab" on page 121 for requirements and instructions.

19. New fields were added to the User and Services Network Element form during the upgrade. Provision these new fields with appropriate settings:
   - In MiCollab server manager, under Applications, click Users and Services
   - Click the Network Elements tab.
   - Select the Network Element and click Edit. The "Standard Phone COS" and "Record-a-Call COS" settings were restored from the backup.
   - Enter a "Default COR".
   - Enter the "Call Reroute First Alternative (CRFA)" index number. On the MiVoice Business platform, program the CRFA index number with the desired destination number.

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

21. Ensure that your UCC V3 licenses have been upgraded to UCC V4 licenses:
   - Log into the server manager
   - Under Applications, click Licensing Information.

   If not, perform a manual sync with the AMC.
   - Under ServiceLink, click Status.
   - Click Sync.

22. Perform a database backup of the newly upgraded system.

   WARNING:AFTER YOU UPGRADE TO MICOLLAB RELEASE 7.2 OR LATER, YOU CANNOT RESTORE A BACKUP FROM A PRE-RELEASE 7.0 SYSTEM, SO IT IS CRITICAL THAT YOU MAKE A BACKUP NOW.
23. For deployments with MiVoice Business Gateways, upgrade them to the latest version.

24. If you are upgrading a MiCollab with a MiVoice Business site and Flow Through Provisioning was not previously configured, it is recommended that you configure the network to support Flow Through Provisioning.
   - See Flow Through Provisioning in the server manager online help for an overview
   - See “Flow Through Provisioning: Brownfield MiCollab with Brownfield MiVB Servers” on page 197 for instructions.

**UPGRADE FROM MICOLLAB 8.X TO MICOLLAB 8.Y**

You can upgrade within the same release (for example, from MiCollab 8.0 to 8.0 SP1 or from MiCollab 8.0 to 8.1) from the MiCollab server manager ServiceLink > Install Applications panel. Refer to the online help for instructions.

*Note: You cannot upgrade the system from MiCollab 7.0 (MSL 10.3) or 7.1 (MSL 10.4) to MiCollab Release 7.2 or 7.3 (MSL 10.5) using a USB. You must upgrade to MSL 10.5 using a CD or DVD before you can use a USB to install the application software.*

**UPGRADE VMICOLLAB CONFIGURATION**

To upgrade a from a vMiCollab configuration (for example, from Small Business configuration to a Mid Market user configuration):

1. Obtain a database backup from the current system.
2. Deploy the vMiCollab OVA. During deployment, set the configuration to the new size (for example Mid Market configuration).
3. Shut down the current system and start the newly deployed vMiCollab system.
4. Restore the database.

*Note: You cannot simply add more resources (vCPU, RAM, and so forth) so that the virtual machine meets the vMiCollab configuration specification and then apply additional licenses. There are different reservations required for each configuration in the OVA.*

**INSTALLING ADDITIONAL (MISSING) APPLICATIONS**

You can use the MiCollab server manager to add applications that you did not select for installation during the initial install using the server manager.

**ADD APPLICATION FROM SERVER MANAGER**

1. Log into MiCollab server manager.
2. Under ServiceLink, click Install Applications.
3. Click the Install Applications tab.
4. Select the latest software version for installation.
5. Scroll through the table and locate the blade for the application/service that you are adding to the system.

6. For each application/service you want to install:
   a. Select the **Install** box.
   b. Select the **Download from AMC** box to download and install software from the Application Management Center.
      -or-
      Clear the **Download from AMC** box to download software from local media (CD/DVD or USB).

7. If you are installing from USB, click **Query USB Storage Devices**. The system detects and lists all of the USB devices connected to the local computer. These devices will be searched for application software when installation commences.

8. Click **Install**.

9. If required, you will be prompted to insert any optional software CD/DVDs. Click **Continue**. Progress is displayed

   **Note:** If you are installing NuPoint ISO files, ensure that you include the "NPUM Finalize" blade.

10. Installing a blade creates new menu items in the navigation menu to allow you to administer the application/service.

11. After you install a blade, launch the associated online help from the application/service. The online help provides information on how to program and use the blade.

12. For MiCollab applications, such as MiCollab Client or MiCollab AWV, you can quickly apply the new service to the users by updating the User and Services template with the new service. Then apply the template to the users.

### REMOVING AN APPLICATION DURING INITIAL INSTALLATION

MiCollab Applications cannot be removed once installed. After an application is installed on the MiCollab server, it cannot be removed without re-installing using the fresh install procedure. If you no longer want an installed application on the MiCollab server, you must perform a fresh install without a restore. During the install, do not select the application that you want to remove.

### DOWNGRAADING APPLICATION SOFTWARE

Downgrading MiCollab software to a previous (lower) release (for example, from Release 7.3 to 7.2) is not supported.
PERFORMING BACKUPS

There are several methods that you can use to back up system data (including all server configuration data, application configuration data, user settings, messages, and greetings):

- **Server Manager "Backup"**: allows you to perform back ups to a local desktop computer or schedule backups to a network file server
- **Server Console "Perform Backup"**: allows you to back up to a USB device or to a network file server
- **VMware Tools**: For vMiCollab deployments, you can use the methods listed above to obtain a vMiCollab database backup. In addition, you can use VMware tools to obtain a backup of the vMiCollab OVA file. Refer to the Virtual Appliance Deployment Guide for instructions.

Notes:

1. You can use different filenames for backup files, but the filename must not contain spaces and the file extension must be either .tgz (unencrypted) or .aes256 (encrypted).
2. To ensure that MiCollab has consistent Network Element (ICP) information, you must use these MSL backup procedures. If you restore backups that were created from inside the individual applications, incorrect Network Element data may be restored to the MiCollab server.
3. To restore the data, you must transfer the backup file to a storage medium (USB device or network share).
4. If MiCollab is deployed in LAN only mode with Teleworker running remotely on an MBG server in the DMZ, you should back up both the MiCollab server database and the MBG server database at the same time.
5. If your site uses Google Integration features (such as, calendar integration), it is recommended that you record the integration settings that are entered in Google Apps configuration tabs and store these settings in a file with the backup. These settings are not retained in the backup.

SERVER MANAGER "BACKUP"

BACKUP TO DESKTOP

Use this procedure to save your system backup to a file or device on your desktop computer or maintenance PC if your MiCollab system has only one application installed.

A "Backup to desktop" saves all of the data to a single, large compressed file and is therefore limited by the maximum file size of the client operating system. For example, if you are backing up data to a Windows client that uses the FAT file system (the default for many versions of Windows), you are limited to a maximum file size of 2 GB. Other file systems may have a larger limit. If the backup file exceeds the maximum file size of the client operating system, it cannot be properly restored.

1. Log into the Administrator portal (server manager). See page 49 for instructions.
2. Under Administration, click Backup.
3. Select the Backup to desktop option.
4. Click Perform. MSL prepares the system for backup and displays the following:
The "Operation status report" with the estimated backup size. Ensure that your browser and target file system support downloads of this size.

The "Backup Encryption" option.

5. (Optional) To encrypt the backup file, enter an Encryption Password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. The encrypted backup file is identifiable with an .aes256 extension.

Note: You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

6. Click Download Backup File.

7. When prompted to Open or Save, click Save.

8. In the file download window that appears:
   - Name the file and then select the location where the file will be saved. Note that the filename of the backup must not contain any spaces; otherwise, you will receive an error when you attempt to restore it.
   - Click Save.
   - In the Download Complete Window, click Close.
   - After saving, you can copy the backup file to a CD/DVD or USB storage device, if required. The backup file is identifiable by its extension, either .tgz (unencrypted) or .aes256 (encrypted).

SCHEDULE BACKUPS TO NETWORK FILE SERVER

Use this option to

• perform immediate system backups to a Network File Server
• schedule daily, weekly, or monthly system backups to a Network File Server.
• Two file-sharing protocols are supported: SMB/CIFS and SFTP.

Use this option if your system has more than one application installed.

Note: You can only have one backup scheduled on the server. To cancel an existing backup schedule, select Disabled and then click Update.

Note: If your site uses Google Integration features (such as, calendar integration), it is recommended that you record the integration settings that are entered in Google Apps configuration tabs of the server manager in a file. These settings are not retained in the backup.

Before you can perform network backups, you must create a shared folder on the Network File Server that allows network users to write to the folder. For example, to create a shared folder on a PC running Windows 8:

1. Right-click on the desktop and select New and then select Folder.

2. Name the folder, for example: "MiCollab Backups".
3. Right-click on the folder and select Properties.
4. Click the Sharing tab.
5. Click Share.
6. Select "Everyone" and click Add.
7. Set the Permission level to Read/Write.
8. Click Share.
9. Click Done.

Next, specify the Network File Server and shared folder in the MiCollab server manager interface:

1. Log into the MiCollab server manager.
2. Under Administration, click Backup.
3. From the Select an action list, click Configure network backup.
4. Click Perform.
5. Identify the server where the backup file will be stored.
   - Enter the IP address of the file server where the backup will be stored.
   - Enter the Sharename of the shared folder where the backup file will be stored. (For example, "MiCollab Backups".) You must set the permissions of the shared folder to allow network users to write files to the folder.
   - Enter an Optional Sub Directory for the backup file, if desired. The specified directory must exist in the share folder. The field accepts multi-level directories; for example "MiCollab/Sept/backups". If you leave this field blank, the system stores the file in the root directory of the specified network share.
   - Enter the Username to use when connecting to the backup server.
   - Enter the Domain or Workgroup Name of the server. (For example, mitel.com.)
   - Enter the Password to use when connecting to the backup server.
   - (Optional) Select the Maximum number of backup files to keep (1-999) on the server. When the number of stored files reaches this maximum count, the oldest version is deleted.
   - Click Update.

To perform an immediate backup

1. Click Backup Now.

To schedule backups to a network file server:

1. Under Administration, click Backup.
2. From the Select an action list, click Configure network backup.
3. Click Perform.
4. Select the frequency with which you want to perform backups. Backup file names will include timestamps, for example: mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz).
To disable regularly scheduled backups, click **Disabled**.

- For Daily backups, select a time of day (hour, minute, AM/PM)
- For Weekly backups, select a time of day, and day of the week
- For Monthly backups, select a time of day, and day of month

5. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters.

**Note:** You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

6. Click **Save** to save the backup password and schedule information.

**SERVER MANAGER SFTP BACKUP TO LINUX SERVERS**

Secure File Transfer Protocol (SFTP) is supported for backups over the network to Linux/Unix servers, including to another MSL server. You use the Network Backup option in the web-based server manager to perform SFTP backups.

**Allow Access on the Backup Server**

To ensure that the backup server accepts access from the source server, perform the following steps on the backup (or destination) server:

- For backups to the WAN interface, enable **remote access** for the source network.
- For backups to the LAN interface, set up the source server as a **local network**.
- In both cases, you must enable **Secure Shell (SSH)** access on the destination server, including the following settings:
  - Allow administrative command line access over secure shell set to **Yes**.
  - Allow secure shell access using standard passwords set to **Yes**.

When the backup is complete, return the SSH settings to **No** and disable SSH access.

**Note:** SFTP backups are **not** supported from the server console Backup menu.

**Configure an SFTP backup**

1. In the server manager, under **Administration**, click **Backup**.

2. Select **Configure network backup** and click **Perform**.

3. In the Network Backups screen, enter the

   - IP address of the backup server
   - Username and password of a valid user on the backup server who has access to the required directory.
• Domain and Sharename are not required. (If a Sharename is entered, MSL will attempt to connect to it using Samba (i.e. Windows backup). If that connection fails, MSL will then attempt an SFTP connection.)

4. (Optional) You can enter a sub-directory where the file will be stored. For SFTP backups, if a directory is not specified, the file is stored in the / directory.

5. (Optional) To encrypt the backup file, enter an Encryption Password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters.

**Note:** You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

6. Click Save. When a valid configuration is entered, the Backup Now button appears.

7. Click Backup Now or configure a backup schedule and click Save.

**Note:** The backup server must accept access from the server you want to back up. For MSL servers, configure the Local Networks and SSH Access of the backup server accordingly.

8. Upon successful completion, MSL displays the path to the backup file.

### SERVER CONSOLE "PERFORM BACKUP"

You can save your system backup to a network file server or to a USB storage device, such as a memory stick. Any USB storage device that is formatted as FAT32 (DOS), EXT3 (Linux), or NTFS (Windows and Linux) is compatible. Optionally, you can encrypt the backup file if you are saving it to a USB device from the server console.

The backup file size limit for a USB or network backup is set by the destination file system: 4 GB for a FAT32, 2 TB (terabyte or trillion bytes) for NTFS, and 16 GB to 16 TB for EXT3 (depending on file system block size). The current MSL EXT3 block size is 4096 bytes which allows file sizes of 2 TB.

1. Access the server console Welcome menu (see page 114).
2. Log in as "admin".
3. From the console, select the option to **Perform backup**.
4. Select a destination for the backup file:
   - Backup to USB Device
   - Backup to Network File Server.

### BACKING UP TO USB DEVICE

1. Select **Backup to a USB Device**.
2. At the prompt, insert the USB device in the MiCollab server (if not already in place) and then click Next.
3. When prompted, enter a filename for the backup file (default is 'mslserver'). Note that the filename of the backup must not contain any spaces, otherwise, you will receive an error.
when you attempt to restore it. The file extension, either .tgz (unencrypted) or .aes256 (encrypted), is added automatically.

4. (Optional) To encrypt the backup file, enter an encryption password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. Click Next.

**Note:** You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.

5. MSL displays an estimate of the size of your backup. Click Proceed.

6. When the backup is complete, remove the USB device when prompted. Click Continue.

7. Re-mount the USB device and verify that the backup has been performed successfully using the verification procedure listed under “Verify Backup Data” on page 113.

**BACKING UP TO NETWORK FILE SERVER**

1. Select **Backup to a network file server**.

2. Enter the **IP address** of the file server where the backup will be stored.

3. Enter the **domain** or workgroup name of the server. (For example, mitel.com.)

4. Enter the name of the **shared folder** where the backup file will be stored. (For example, "MiCollab Backups"). You must set the permissions of the shared folder to allow network users to write files to the folder.

5. Enter an **optional sub directory** for the backup file, if desired. The specified directory must exist in the share folder. The field accepts multi-level directories; for example "MiCollab/Sept/backups". If you leave this field blank, the system stores the file in the root directory of the specified network share.

6. Enter the **username** to use when connecting to the backup server.

7. Enter the **password** to use when connecting to the backup server. Estimated backup size and available storage space are displayed.

8. Click **Next**. A progress bar indicates backup status. When the backup is complete, file verification is performed automatically.

**VERIFY BACKUP DATA**

When backing up to a USB device or when using a pre-existing backup file, it is important to verify the file before starting a restore procedure. If your backup file cannot be verified, then it cannot be used to restore system information.

To verify a backup file:

1. Access the server console Welcome menu (see page 114).

2. Log in as "admin".

3. From the console menu, select the option to **Verify backup file**.
4. At the prompt, insert your USB device. (Note: if your USB device was left mounted after your last backup, you must remove it and re-mount it now.)

5. From the list, select your storage device type and then click OK. Verification of the file is confirmed. If you receive an error message, you cannot use this backup file for the restore. Check your storage media and try the backup procedure again. See the MiCollab for MiVoice Business - Engineering Guidelines for a list of supported USB devices.

SHUTTING DOWN MICOLLAB

If you need to shut down or reboot, use the Reboot or Shutdown screen to ensure that the shutdown sequence occurs gracefully, preserving all configuration and information on the server. There is a similar function in the MSL console. Note that this screen initiates the shutdown or reboot immediately after you click Perform.

CORRECTING ACTIVATION ERRORS

If you receive an error message while activating MSL, you may have entered an incorrect parameter.

To check and correct a network parameter:

1. Access the server console Welcome menu (see page 114).
2. In the server console menu, select the option to Configure the Server.
3. Review and correct parameters as required.
4. When complete, depending on the parameter changed, you are prompted to reboot the server or you receive a message that activation is complete.
5. After reboot (or confirmation message), launch the administrator portal (see page 48).
6. Under ServiceLink, click Status. You are prompted to enter your Service Account ID.
7. Enter your Application Record ID number and then click Activate.
8. Continue with "Install Application Software" on page 47, starting at step 2.

ACCESSING THE SERVER CONSOLE

To access the server console locally, log into the server console by entering the MiCollab login name and password:

Login: admin
Password: (as programmed during MSL install)

Note: When you use the MSL server console, to ensure that your entered information is not lost, always press the Alt keyboard key to recover from power saving mode or screen saver mode. Do not press the Space bar or Return keyboard key when the terminal screen has gone blank.
You can also access the MiCollab server console using remote secure shell (SSH) access. However, before you can access the server console remotely, you must enable the following options through the Administrator Portal:

1. Log into the Administrator Portal (see page 49).
3. Under Secure Shell Settings, set the following parameters:
   - Set the Secure Shell Access field to "Allow access only from trusted and remote management networks"
   - Set the Allow administrative command line access over secure shell to "Yes"
   - Set the Allow secure shell access using standard passwords to "Yes".
4. Click Save.

ABOUT SSH (SECURE SHELL)

SSH (secure shell) provides a secure, encrypted way to log into a remote machine across a network, or to copy files from a local machine to a server. Programs such as telnet and FTP transmit passwords in plain, unencrypted text across the network or the Internet. SSH provides a secure way to log in or copy files. For more information about SSH Communications Security and its commercial products, visit http://www.ssh.com/.

OpenSSH, included in MSL, is a version of the SSH tools and protocol. The server provides the SSH client programs as well as an SSH server daemon and supports the SSH2 protocol. After SSH is enabled, you can connect to the server by launching the SSH client on the remote system. Ensure that it is pointed to the external domain name or IP address for the server. In the default configuration, you will be prompted for your user name. Enter "admin" and the administrative password. The interface opens in the server console. From here you can change the server configuration, access the server manager through a text browser or perform other server console tasks.

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. If you do enable SSH access, you have two configuration options:

- **Allow administrative command line access over secure shell** - This allows someone to connect to the server and log in as "root" with the administrative password. The user has full access to the underlying operating system. This can be useful if someone is providing remote support for the system, but in most cases we recommend setting this to No.

- **Allow secure shell access using standard passwords** - If you choose Yes, users will be able to connect to the server using a standard user name and password. This may be a concern from a security point of view, in that someone wishing to break into the system could connect to the SSH server and repeatedly enter user names and passwords in an attempt to find a valid combination. A more secure way to allow SSH access is called RSA Authentication and involves the copying of an SSH key from the client to the server.

Note: By default, only two user names can be used to log in remotely to the server: "admin" (to access the server console) and "root" (to use the Linux shell). Regular users are not permitted to log into the server.
OBTAINING AN SSH CLIENT

A number of different free software programs provide SSH clients for use in a Windows or Macintosh environment. Several are extensions of existing telnet programs that include SSH functionality. Two different lists of known clients can be found online at the following web sites:

- http://www.openssh.com/windows.html, and

PuTTY is a "free" SSH client recommended for interoperating with OpenSSH from Windows and can be obtained at http://www.openssh.com/windows.html

A commercial SSH client is available from SSH Communications Security at: http://www.ssh.com/buy/.

CONFIGURING REMOTE MANAGEMENT VIA MBG

You can configure secure remote access for clients on the internet to the MiCollab server manager interface through a standalone MBG server. The following requirements apply:

- MiCollab is deployed in either LAN mode or Network Edge (server-gateway) mode
- Standalone MBG server is deployed in either in the DMZ or Network Edge mode
- Standalone MBG server requires the Remote Proxy Services application.

**Note:** A proxy loopback configuration, where the admin proxy is set up on itself on the network edge is not supported

To configure remote access to the MiCollab system:

1. Log into the MSL server manager on the standalone MBG server.
3. On the Domain list tab, click Add new proxied domain and add the MiCollab server. In the MiCollab support field, check the End user and Admin boxes. Refer to the associated online help for detailed step-by-step instructions.
4. Next, click the User tab and add user accounts (usernames, passwords, and email addresses) for remote management access. Refer to the associated online help for detailed step-by-step instructions.

To remotely access the MiCollab server manager or MiCollab End User portal:

1. Open a MiCollab supported browser and enter one of the following URLs:
   - Enter the https://<Fully Qualified Domain Name of the MiCollab server>/server-manager to access the server-manager login page,
   - Enter the https://<Fully Qualified Domain Name of the MiCollab server> to access the My Unified Communications login page.
2. You are prompted for your remote access username and password.
3. After you enter your credentials correctly, the login page is displayed.
4. Log in using your MiCollab credentials.

To add Users to Standalone MBG for Remote Access:
1. In the server manager, under Applications, click Remote Proxy Services.
2. On the Users tab, click Add new user.
3. Select Active.
4. In the Username field, enter the username used for authentication when accessing the application interface.
5. In the Password field, enter the user's password used for authentication when accessing the application interface.
6. In the Confirm Password field, re-type the user's password.
7. In the First Name field, type the user's first name.
8. In the Last Name field, type the user's last name.
9. In the Email address field, type the user's email address.
10. In the Add permission list, select the application interfaces you want this user to access, and then click Add. Use Shift+Click and Ctrl+Click to select multiple applications.

**Note:** In this release, select permissions only for the "Admin interfaces". In a future release, it will be possible to select "User interfaces".

11. To automatically activate the user at a later date and time, enter the Deferred activation Date and Time.
12. To automatically de-activate the user at a later date and time, enter the Expiry Date and Time.
13. Click Save.

**VIEWING LOG FILES**

You can use the View Log Files feature of the MiCollab server to help in troubleshooting system performance. Adjusting the default settings provides custom log reports.

To view log files:
1. Access the administrator portal.
2. Under Administration, click View Log Files.
3. Refer to the MiCollab Server Manager online help for information about setting log file preferences.
For more Troubleshooting diagnostics, see “Troubleshooting” on page 125, and the following documentation for each application:

<table>
<thead>
<tr>
<th>APPLICATION</th>
<th>ONLINE HELP TOPIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitel Collaboration Advanced</td>
<td>See Troubleshooting chapter in the MiCollab AWV Configuration and Maintenance Manual and “MiCollab AWV” on page 135</td>
</tr>
<tr>
<td>NuPoint Unified Messaging</td>
<td>“Troubleshooting Applications” on page 135</td>
</tr>
<tr>
<td>MiVoice Border Gateway</td>
<td>“MiCollab Client” on page 143</td>
</tr>
</tbody>
</table>

**VIEWING ALARMS**

You can view the current alarm state of the Teleworker application and recent events that the system has recorded.

To view events:
1. Access the administrator portal.
2. Under Administration, click **Event Viewer**.
3. Refer to the MiCollab online help for information about event viewer preferences.

**CONVERSIONS AND MIGRATIONS**

This section provides instructions on how to

- Convert a MAS Server Release 4.0 or later database to a MiCollab Virtual Appliance (vMiCollab) system
- Migrate a standalone MiCollab Client database to a MiCollab Server or MiCollab Virtual Appliance system.

**CONVERT A MICOLLAB SERVER DATABASE TO VMICOLLAB**

You can convert a MAS Release 4.0 or later database from a MiCollab Server to a MiCollab Virtual Appliance Release 7.1 or later deployment using the Restore option in the server console.

**CAUTION:** Before you attempt to perform the conversion, review Table 8, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 152 to ensure that the conversion is supported for your configuration.

**CONDITIONS AND CONSTRAINTS**

The following conditions and constraints apply:

- You can only convert MAS Release 4.0 or later database backups to vMiCollab deployments. Conversions from releases prior to Release 4.0 are not supported.
- All application data programmed in the vMiCollab database is overwritten by the backup data during the restore operation. The data in the backup is not merged with the existing database in the vMiCollab system.
• If the vMiCollab system has additional applications that are not included in the restored database, these application databases will not contain any data after the restore. They will be blanked out during the restore.

• Before you convert, ensure that the existing MiCollab system does not exceed the vMiCollab capacity limits. Refer to the MiCollab for MiVoice Business - Engineering Guidelines for vMiCollab capacities.

BEFORE YOU BEGIN

Ensure that you have completed the following tasks before you begin the conversion:

- Ensure conversion is supported for your deployment configuration
  - Review Table 8, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 152 to ensure that the database restore operation is supported for your configuration. If the restore operation is NOT supported, DO NOT PROCEED with the conversion.

- Purchase required licensing
  - Contact your dealer or VAR and request to have PN 54005389, “MiCollab Server to Virtual MiCollab Conversion” added to your Application Record ID. To support vMiCollab, your Application Record ID must include PN 54005389.
  - Ensure that you record your Application Record ID and have it available before you begin the conversion.

- Download the latest OVA file and application software from Mitel Online.
  - See “.” on page 63 for instructions.
  - If your deployment requires Nupoint Unified Messaging options or the SAA-TTS option, you must also download these ISO files to separate DVDs or to a USB device.

- Deploy vMiCollab but do not power up the vMiCollab Virtual Machine (VM).
  - Install the vMiCollab system by deploying the new vMiCollab OVA file. See “Deploy vMiCollab vApp” on page 64.
  - Do not power up the VM at this time.

- Backup your MiCollab Server database
  - Obtain a database backup from the MiCollab Server and save it to a USB device or a network drive. See “Performing Backups” on page 108 for instructions.

PERFORM THE CONVERSION

Schedule the conversion to occur during off business hours because a service outage occurs during the conversion:

1. Shut down the MiCollab Server system. See “Shutting Down MiCollab” on page 114 for instructions.

2. Launch the vSphere Client application on the network PC.
   - Click Start -> All Programs.
   - Click VMware -> VMware vSphere Client.
   - Enter the IP address or hostname of the Hypervisor ESX/ESXi Host server or
Enter the IP address or hostname of the vCenter Server.
- Enter your username and password.
- Click OK.

3. Right-click on the virtual MiCollab appliance (for example: vMiCollab 7.1.1.0 build) and select Open Console. The vMiCollab console opens within the vSphere Client.

4. Power on the vMiCollab VM by clicking the green arrow button in the toolbar. The MSL bootup is displayed on the screen.

5. Choose your preferred keyboard from the list (default is us) and click Next.

6. When the system prompts you with “Do you wish to restore from backup?“:
   - Select Restore from Backup.
   - Select Restore from removable device and insert your USB key when prompted
   - Select Restore from network share. Follow the prompts to specify the location of the backup file and start the restore, or
   - Select Restore from running server option to retrieve the configuration from the existing MiCollab server. This option shuts down the server that you are retrieving the configuration from before bringing up the new server. It configures the new system with the IP address of the old system.

7. After responding to all prompts, click Yes to restore the backup data.

8. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the Decryption password. Click Next and then Yes.

9. After MSL completes the restore, select Reboot Now. The system takes approximately 20 minutes to reboot.

   **Note:** If the screen times out and goes blank press the Alt keyboard key to restore the screen. Do not press the Enter key.

10. After the vMiCollab vApp has powered up, log into the MiCollab server manager:

11. In the server manager, under ServiceLink, click Install Applications.

12. Click the Install Applications tab.

13. Set the PBX Type and then click Next. The list of licensed applications, services and security patches for the currently installed version of MiCollab appears.

14. Select the latest software version for installation.

15. Check the Download from AMC boxes of the required applications.

16. Click Install.

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

17. After the applications are installed, reboot the MiCollab server.

18. After the optional software is installed, check that all applications and application data is present.
MIGRATE STANDALONE MICOLLAB CLIENT TO MICOLLAB SERVER OR VMICOLLAB

You can migrate (import) a standalone UCA version 5.0 or higher database to a MiCollab Server Release or vMiCollab Release system.

There are several options:

• Install the MiCollab system on a new 64-bit server and restore the MiCollab Client standalone database.
• Restore the MiCollab Client database to an existing MiCollab 64-bit server.

CONDITIONS AND CONSTRAINTS

The following conditions and constraints apply to the migration:

• MiCollab Release 7.2 and higher is only supported on 64-bit server architecture.
• The UCA Server database must be a version 5.0 or higher database.
• MiCollab Client migration does not support UCC licensing. The migrated users consume "à la carte" licenses when they are migrated to MiCollab.
• You can only migrate data from a MiCollab Client system to a MiCollab deployment; you cannot migrate data from a MiCollab deployment to a MiCollab Client system.
• Database migration from MiCollab Client Server Appliance is not supported.
• A MiCollab Server must have a minimum of 6 GB of RAM to support the MiCollab Client application.
• Refer to the Engineering Guidelines "Performance and Capacities" section for the maximum number of MiCollab Client users supported by your deployment configuration.
• You must have an active software assurance license or have purchased the "MiCollab Add-on to MiCollab Client" part number.
• MiCollab Client user licenses are transferred from the MiCollab Client standalone system to the MiCollab system after you have migrated the MiCollab Client database.
• When you import the data, any existing MiCollab Client data on the MiCollab system will be overwritten.

BEFORE YOU BEGIN

☐ Purchase the required upgrade part number and apply it to your Application Record ID:
  - MiCollab Add-on to MiCollab Client - PN 54005444
  or
  - vMiCollab Add-on to MiCollab Client - PN 54005445
☐ Ensure that you record your Application Record ID and have it available before you begin the migration.
☐ Schedule the migration to occur after business hours. MiCollab Client services will be down during the migration.
PERFORM THE MIGRATION

1. Obtain a backup of the MiCollab Client Server database from the MSL Server Manager Backup page. Save the backup to a network file server. Refer to “Schedule Backups to Network File Server” on page 109 for instructions.

2. Shut down the MiCollab Client server.

3. Install MiCollab Release software:
   - Install MiCollab Server (page 31). During the installation of the MSL operating system, you must access the MiCollab server manager and install the application software. See “Install Application Software” on page 47.
   
   or

   - Install vMiCollab (page 55). You must install vMiCollab by deploying the OVA file.

4. After the install is complete, MiCollab is running with the MiCollab Client application.

5. Log into the MiCollab Administrator portal (server manager). See page 49 for instructions.

6. Under Applications, click MiCollab Client.

7. In the Import Data File field, click the Browse button and navigate to the MiCollab Client version 5.0 or later database file (for example, smeserver.tgz).

8. When prompted to Open or Save, click Open.

9. Click Import Mitel UC Server Configuration.

10. Send a broadcast email to MiCollab Client client users informing them that they must point their client to the MiCollab FQDN. Send users the MiCollab FQDN along with the following instructions:

    For Desktop Clients:
    - Open the Control Panel, open Programs and Features, right-click on Mitel MiCollab Client, and click Change.
    - In the Setup Wizard window, click Next.
    - In the Change, Repair, or Remove Installation window, click Change.
    - In the Custom Setup window, click Next.
    - In the UC Advanced Configuration window, enter the MiCollab FQDN in the MiCollab Client Hostname field and then click Next.
    - In the Ready to Change Mitel MiCollab Client window, click Change. The setup runs.
    - Click Finish.
    - Click Yes to restart your system.

    For Mobile Clients:
    - Select the MiCollab Client Mobile Client application.
    - Select Settings.
    - Select Account Options
    - Enter the MiCollab FQDN in the Server IP field.
11. If your site does not use MiVoice Office 250 systems and if you do not require Active Directory Integration with MiCollab Client, integrate the MiCollab Client database with the Users and Services application. See “Configure MiCollab Client Mode” on page 79 for instructions.
Chapter 8

TROUBLESHOOTING
### GENERAL TROUBLESHOOTING

The following tables list scenarios you may encounter when installing/using MiCollab and application software.

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| Error 404 - File Not Found when accessing the MiCollab End User portal via VPN | VPN is on a different subnet from the MiCollab server so the IP address of VPN connection must be added to the list of Trusted Networks | To find your VPN IP address:  
1. Access the server manager  
2. Under Administration, click View Log Files  
3. From the Choose a log file to view list, click httpd/error_log  
4. Scan the logs for your VPN IP address  
5. Follow the instructions on page 50 to allow Trusted Network access for your VPN |
| One way audio | ICP or phones may be on a different subnet than the MiCollab server | Set up the Trusted Networks so that the IP address of each ICP and phone on your network falls within one of the IP ranges configured within the Trusted Networks panel. See page 50 |
| Network Connectivity problems in Network Edge mode | Incorrect ethernet card connection | Use the administrator portal to reassign the internal and external ethernet cards |
| User information not available after removing NP-UM mailbox using method other than via USP | After the removal of NP-UM mailboxes using methods other than the USP, the information for that user will be temporarily unavailable to the USP and an error will be presented. An audit occurs between NP-UM and USP every five minutes to correct and update data | Allow the system to complete its audit by waiting five minutes before accessing the user's information |
| Cannot receive system admin e-mail notifications or send e-mail invitations for MiCollab AWV conferences when using a mail exchange server | If you are using a mail exchange server, email notifications from the MiCollab AWV server require you to delegate email processing to your mail exchange server. | • In the server manager, under Configuration, click Email  
• Under Delegate Mail Server, in the Address of internal mail server field, enter the IP address of your mail exchange server |
| The software version for an MiVoice Business element is not listed in the USP Network Elements tab. | The MiCollab system was unable to retrieve the version information from the MiVoice Business element because the "SNMP Read Only Community" field on the MiVoice Business is not set to "Default". | 1. Log into the MiVoice Business System Administration Tool of the network element.  
2. Set the "SNMP Read Only Community" field in the MiVoice Business SNMP Configuration form to "Default". |
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error message: &quot;Sorry there was an error while processing your request. Please report this to your Administrator.&quot; OR PC hangs when trying to install software from CD/DVD</td>
<td>If you have logged out of the server console by answering &quot;No&quot; to the &quot;Do you want to install software from CD&quot; prompt, you may have interrupted the install sequence</td>
<td>Reboot the server. Log in as admin and select the server console option to Install software from CD/DVD</td>
</tr>
<tr>
<td>Error Message: Failed: Failed to insert tuple to CUS_USER_CONFIG. MiXML error: MimaRC-Insert-Tuple-Failed</td>
<td>When adding new users (single adds or bulk import), you may accidentally exceed the number of IP Device licenses available</td>
<td>To verify license quantities: 1. In the MiVoice Business System Administration Tool, select System Configuration 2. Select System Capacity and then System Capacity Display 3. Check the number of IP Licenses Purchased. If your import/adds cause the number of users to exceed the number of IP Licenses Purchased, you must postpone the import/add until more licenses are purchased</td>
</tr>
<tr>
<td>Error Message: Fatal Error Caught, Can’t call method “prop” on an undefined value at /usr/lib/perl5/site_perl/esmit/h/Blades/Blade.pm line 1005 when installing NP-UM Prompts</td>
<td>The CD/DVD drive is unable to read information from the CD/DVD</td>
<td>Ensure that the CD/DVD is clean and smudge-free</td>
</tr>
<tr>
<td>SAA TUI reports experiencing &quot;Technical Difficulty&quot; and &quot;Your call will be transferred to an operator.&quot; when you speak the Department prompt</td>
<td>Department name may have been programmed with an apostrophe included</td>
<td>In the MiCollab USP or the NuPoint application, edit the Department name so it does not include an apostrophe</td>
</tr>
<tr>
<td>While you are in the Server Manager Administrator portal or MiCollab End User portal you receive the following error message: &quot;The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.</td>
<td>A software update is in progress. During the software update, the tomcat server restarts. While the restart is in progress, you cannot use the Administrator portal and MiCollab End User portal web interfaces.</td>
<td>Wait approximately 5 minutes until the tomcat server has finished restarting.</td>
</tr>
<tr>
<td>SYMPTOM</td>
<td>POSSIBLE CAUSE</td>
<td>CORRECTIVE ACTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>You cannot log into the NP-UM web console.</td>
<td>The system is over provisioned with voice mailboxes (that is, the number of provisioned mailboxes exceeds the number of NP-UM user licenses)</td>
<td>To return these applications to their normal state, you must purchase additional NP-UM user licenses or delete the extra mailboxes. You must reduce the number of mailboxes to be equal to, or lower than, the number of available licenses</td>
</tr>
<tr>
<td>You cannot log into the MiCollab AWV administration application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>You can log into the NP-UM TUI, but you will be unable to access the administrative options.</td>
<td>One or more of the NuPoint software application blades are not licensed correctly. To see the blades that failed to install, re-install NuPoint software application.</td>
<td>Apply the licensing part number(s) for the unlicensed NP-UM blade(s) to the MiCollab application record. See “Installing Additional (Missing) Applications” on page 106. Then repeat the application installation procedure. See “Installing Additional (Missing) Applications” on page 106.</td>
</tr>
<tr>
<td>You are attempting to install additional software applications using the MSL text console &quot;Install Application Software from CD/DVD&quot;. The display only indicates that NuPoint needs to be installed. You cannot proceed with the installation.</td>
<td>An error occurred while the system was preparing for a restore Check the message log for more information. You may have cleared (or never set) an Application Record Identifier (ARID).</td>
<td>For a MiCollab server: 1. Re-install MSL. 2. When prompted to do so, restore the backup. For a vMiCollab deployment: 1. Re-install the vMiCollab OVA. 2. Enter the ARID when prompted to do so. 3. Repeat the restore.</td>
</tr>
<tr>
<td>When performing a restore, you get the following error message: &quot;Error preparing for system restore&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>During a software update using the MSL text console &quot;Update Mitel Application Software&quot;. The display only indicates that NuPoint needs to be installed. You cannot proceed with the software updates.</td>
<td>One or more of the NuPoint software application blades are not licensed correctly. To see the blades that failed to install, re-install NuPoint software application.</td>
<td>Apply the licensing part number(s) for the unlicensed NP-UM blade(s) to the MiCollab application record. See “Installing Additional (Missing) Applications” on page 106. Then repeat the software update installation procedure. See “Performing Backups” on page 108.</td>
</tr>
<tr>
<td>Users and administrators are unable to access the MiCollab web portals (for example, MiCollab End-User Portal) using Internet Explorer 10.</td>
<td>In MiCollab Release 7.1, the TLS 1.0 security protocol is enabled by default. If you disable support for TLS 1.0, users will be unable to access the MiCollab web portals using Internet Explorer 9 and 10.</td>
<td>Upgrade to Internet Explorer 11.0. OR Enable TLS 1.1 and 1.2 in your Internet Explorer 10 browser: 1. Select Tools &gt; Internet Options &gt; Advanced &gt; Security. 2. Enable Use TLS 1.1 3. Enable Use TLS 1.2 4. Click Apply and then OK.</td>
</tr>
</tbody>
</table>
When you boot up a MiCollab system running on a DL360 G6 server, the following error messages appear:

**[Firmware bug]:** The Bios has corrupted hw-PMU resources (MSR 38d is 30)
**ERST: Failed To Get Error Log Address Range**

The Broadcom NC382T PCI Express Dual Port NICS were both detected with 00:00:... MAC addresses.

1. Upgrade the Firmware to HP Service Pack DL 360 2013.02.0 or higher.
2. In the MiCollab server console, ensure that you reset the mapping of the on-board NICs (see “Enter Local Network Adapter” on page 43 for details).

MiVoice Conference Unit is not functioning correctly.

The current SIP Device Capabilities settings do not support the MiVoice Conference.

When you select a device type of “UC Endpoint” the SIP Device Capabilities number defaults to 71. However, the settings assigned to 71 do not fully support the MiVoice Conference Unit.

1. In USP, change the default SIP Device Capabilities number from 71 to a value between 1 to 60.
2. On the communications platform, program the assigned SIP Device Capabilities number with the settings required to support the MiVoice Conference Unit.
3. See the MiVoice Conference Unit Administrator’s Guide on the Mitel Customer Documentation site for the required settings.

Users and administrators are unable to access the MiCollab web portals (for example, MiCollab End-User Portal) using Internet Explorer 9 or 10.

In MiCollab Release 7.1 or later, the TLS 1.0 security protocol is enabled by default. If you have disabled support for TLS 1.0, users will be unable to access the MiCollab web portals using Internet Explorer 9 and 10.

Upgrade to Internet Explorer 11.0.
OR
Enable TLS 1.1 and 1.2 in your Internet Explorer 10 browser:
1. Select **Tools > Internet Options > Advanced > Security**.
2. Enable **Use TLS 1.1**
3. Enable **Use TLS 1.2**
4. Click **Apply** and then **OK**.

You see the following alarm in server manager: "I/O problems detected!"
Or, you receive an e-mail from the server indicating an I/O or file system problem.

The system is experiencing problems which has led to switching to read-only file system.
This issue can be caused by slow network connections, heavy disk I/O or problems with the data storage.

Reboot the MiCollab server.

When you attempt to access the MiCollab End User portal login page, you receive a "500 Internal Server Error" in your browser.

Issue with browser cookies
Clear your browser cache.
## ONLINE HELP TROUBLESHOOTING

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents is not present or not functioning correctly in Internet Explorer 10 or 11</td>
<td>Help compatibility issues with Internet Explorer 10 or 11.</td>
<td>Put the browser in compatibility mode. For Internet Explorer 10, click the Compatibility View icon located in the browser address bar on the right side.</td>
</tr>
<tr>
<td>Help topic text is not appearing in Internet Explorer</td>
<td>Google Chrome does not support webhelp files when they are run locally on your PC. The webhelp must be running on a web server in order to support Google Chrome.</td>
<td>Open the webhelp from the MiCollab application, or To open webhelp files locally on your PC, use a supported Internet Explorer browser version or a supported Firefox browser version.</td>
</tr>
<tr>
<td>Cannot display online help in Google Chrome browser locally.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| In the online help, numbered steps are ordered incorrectly and text formatting is inconsistent. | You need to modify your Internet Explorer compatibility settings.               | 1. In the Internet Explorer toolbar, click Tools and then click Compatibility View Settings.  
2. Check the Display all websites in Compatibility View.  
3. Click Close.                                                      |

## FLOW THROUGH PROVISIONING TROUBLESHOOTING

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Start Sharing operation fails with a message to check the MiCollab logs.</td>
<td>One or more MiVoice Business elements are provisioned in the network without an IP address or FQDN. Sharing with MiCollab cannot be established unless all MiVoice Business elements in the network are provisioned with an IP address or FQDN.</td>
<td>Configure all MiVoice Business elements in the sharing network are configured with either an IP address or FQDN. Then perform the Start Sharing operation.</td>
</tr>
<tr>
<td>Flow Through Provisioning updates that you make to users on the MiVB are not being updated in the MiCollab database.</td>
<td>The update has not been applied yet.</td>
<td>Wait approximately 2 minutes. The system can take several minutes before the updates are applied.</td>
</tr>
<tr>
<td>SYMPTOM</td>
<td>POSSIBLE CAUSE</td>
<td>CORRECTIVE ACTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Unable to Reach Through to MiVoice Business</td>
<td>MiVoice Business &quot;system&quot; administrator account is not configured</td>
<td>Reach through is enabled from MiCollab USP to the MiVoice Business (MiVB) system administration tool using the MiVoice Business &quot;system&quot; administrator account. Configure an administrator account in the User Authorization Profiles form with Login ID &quot;system&quot; and System Admin authorization set to &quot;True&quot;.</td>
</tr>
<tr>
<td>During a Start Sharing operation you receive an error messaging indicated that Synchronization Failed.</td>
<td>One or more MiVoice Business forms are shared at the wrong scope.</td>
<td>Access the MiVoice Business SDS Form Sharing form and set the correct scopes. See “Supported Sharing Scopes” on page 211.</td>
</tr>
</tbody>
</table>
| Incomplete phone services are present in the MiVoice Business. database. | While Flow Through Provisioning was turned off, you performed a restore on MiCollab or you made changes to phone services on the MiVoice Business. Afterwards, you performed a sharing and sync resulting in incomplete phone services on the MiVoice Business. | 1. Delete the incomplete phone service from the primary MiVoice Business.  
2. Perform a sync operation from the MiVoice Business to MiCollab with the "Overwrite" option selected. This operation removes the incomplete phone data from MiCollab. |
| A template in the templates form displays the following error message in red text: "This template is not valid on MiCollab: This MiVoice Business template has incomplete MiCollab services associated with it." | A restore was performed using a database backup which did not contain templates that are currently on the MiVoice Business. The Reconcile Wizard has marked these templates as invalid. | Delete the invalid templates from the MiVoice Business. |
| You run the MiConfiguration Wizard against a brownfield MiVoice Business (not recommended) and you receive the following error message: "Failure detected during MiVoice Business reconcile execution: [Database GUID normalization failed.]" | SDS is not enabled in MiVoice Business System Options form. | Enable SDS in the MiVoice Business System Options form. Then, run the MiConfiguration Wizard again. |
### VMICOLLAB TROUBLESHOOTING

The following issues are specific to Virtual MiCollab deployments:

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiCollab system performance is slow.</td>
<td>You have taken snapshots of vMiCollab. vMiCollab system performance is degraded if snapshots are present on the platform.</td>
<td>Delete all vMiCollab snapshots from system.</td>
</tr>
<tr>
<td>Unable to connect to a CD/DVD drive when you are attempting to install optional application software (for example, NP-UM features).</td>
<td>In the vMiCollab Virtual Machine Properties Hardware screen, under Host Device, the drop-down menu displays &quot;CD/DVD Drive 1 - Device unavailable&quot;.</td>
<td>Select a valid CD/DVD drive from the list of devices.</td>
</tr>
</tbody>
</table>
| After importing (restoring) an vMiCollab OVF template backup file, system performance and voice quality is poor. | Network adapter type is set incorrectly. After importing an OVF template file, the network adapter type is reset to default. The network adapter must be reset to type VMXNET3. | Set the network adapter to type VMXNET3.:
1. In the vSphere Client, click the vMiCollab App properties Hardware tab.
2. Select Network adapter 1 from the Hardware list.
3. Click Remove.
4. Click Add.
5. From the "Adapter type" drop-down menu, select VMXNET3.
6. Click Next and then click OK. |
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice quality issues</td>
<td>vMiCollab is installed in the vSphere environment using Thin provisioning.</td>
<td>Reinstall vMiCollab and select Thick provisioning during the install wizard.</td>
</tr>
<tr>
<td></td>
<td>Thin provisioning can cause voice quality issues due to disk sharing.</td>
<td></td>
</tr>
<tr>
<td>VMware environment is not configured with</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the required resources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vMiCollab features not working as expected</td>
<td>Invalid license. You have installed MiCollab on a virtual machine, but you do</td>
<td>1. Contact your authorized Reseller to purchase a virtualization license and obtain a Application Record ID.</td>
</tr>
<tr>
<td></td>
<td>not have a virtualization license.</td>
<td>2. In your AMC account, access the appropriate Application Record and assign the license.</td>
</tr>
<tr>
<td></td>
<td>In the Server Manager, click the Licensing Information page. If your license</td>
<td>3. Log into the Server Manager.</td>
</tr>
<tr>
<td></td>
<td>is invalid a red warning message will appear near the top of the web page.</td>
<td>4. Under ServiceLink, click Status.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Click Sync.</td>
</tr>
</tbody>
</table>

1. Log into the MiCollab server manager.  
2. Under Administration, click Virtualization.  
3. Run the Mitel Virtualization diagnostics. Refer to the online help for instructions.  
4. Collect the Virtualization logs from the server manager View Log Files page.  
5. Send the compressed log file to Mitel Product Support for analysis.
TROUBLESHOOTING APPLICATIONS

MICOLLAB AWV

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>After initial configuration of a MiCollab with MiVoice Business deployment, AWV is not functioning. Logs similar to the following are being constantly generated on the MiVoice Business:</td>
<td>Mitel Integrated Configuration Wizard was run against MiVoice Business and MiCollab in separate sessions. When you run the Mitel Integrated Configuration Wizard, if you configure both the MiVoice Business and the MiCollab in the same MiCW session, the wizard automatically creates a common SIP password. This password is assigned in both the MiCollab AWV SIP Server Configuration page and in the MiVoice Business User and Devices &gt; User and Device Configuration &gt; Access and Authentication &gt; SIP Password fields. However, if you run the Mitel Integrated Configuration Wizard, separately against the MiVoice Business and the MiCollab systems, the SIP passwords will not match and AWV will not function.</td>
<td>1. Log into the MiCollab server manager and configure a SIP Password in the MiCollab AWV SIP Server Configuration page. 2. Log into the MiVoice Business System Admin tool and program the same SIP password against the AWV SIP Ports in the User and Devices &gt; User and Device Configuration &gt; Access and Authentication &gt; SIP Password fields.</td>
</tr>
</tbody>
</table>

5 INFO 2015/05/07 16:45:43 MOBILITY General Maintenance(0) Hot Desk: 6851 unlocked by DISA TIMER timeout

6 INFO 2015/05/07 16:45:43 MOBILITY General Maintenance(0) Hot Desk: 6852 unlocked by DISA TIMER timeout

7 INFO 2015/05/07 16:45:43 MOBILITY General Maintenance(0) Hot Desk: 6853 unlocked by DISA TIMER timeout

User receives the following error message when upgrading MiCollab AWV client:

**The executable could not be downloaded from server to the PC in https url mode.**

**Check with local IT to see if there have been changes in OS/certificates. Determine if other https urls are accessible from that PC browser.**

1. From the user’s PC, do Winscp to the server ip as root.
   **Note:** If the server ip cannot be FTPed, then download from the server and copy it to the PC by other means.
2. Go to `/usr/awc/connpoint/content`.
3. Download the `MCAClient.msi` to local directory.
4. Run the msi file.
   If the user sees a permission issue when moving the files to the AppData folder, then run the msi as admin option.
   **Note:** To run the msi as admin, download the `MCAClient-admin.exe` file instead of the `MCAClient.msi` in step 3.
5. Verify the new client is installed on the user’s PC.
## Troubleshooting

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| The MiCollab AWV Conferencing Client does not upgrade, or does not upgrade in a timely fashion. | The Windows Installer or Registry is corrupt or is missing files. When MiCollab AWV Conferencing Client detects an existing version, it instructs Microsoft Windows Installer to remove the existing version first. If this uninstall fails, the MiCollab AWV upgrade will also fail. | You must uninstall the existing MiCollab AWV Conferencing Client installer manually before you can perform the upgrade.  
1. Log into Windows as the user who installed the MiCollab AWV Conferencing Client.  
2. Copy the exact version of the installed mcaclient.msi in the installed path (for example, C:\Users\%username%\AppData\Local\Mitel\MCAClient).  
3. Open the Windows Control Panel, click the Add/Remove programs icon and remove the MiCollab AWV Conferencing Client.  
4. Remove the registry key and delete installed copy of software from the installed path:  
   a. Type regedit in Run to reach the registry.  
   b. Type the following path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall.  
   c. Search for "MiCollab Audio, Web and Video Conferencing Client".  
   d. Remove the key containing this value.  
   e. Go to C:\Users\%username%\AppData\Local\Mitel\MCAClient folder and remove the files.  
   OR  
   1. Install Microsoft Fix It (Cleanup Utility). This utility is available from Microsoft.com at the following URL: http://support.microsoft.com/mats/Program_Install_and_Uninstall/.  
   2. Run Microsoft Fix It; select and remove MiCollab Audio, Web and Video Conferencing Client. |

### Registry Sections that contain keys pertaining to the Collaboration Client:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- HKEY_CURRENT_USER\Software\Microsoft\Installer\Products

To remove the CC 2.0 program settings (preferences) from the registry, remove the following key.

- HKEY_CURRENT_USER\Software\Inter-Tel\DesktopClient32
**SYMPTOM** | **POSSIBLE CAUSE** | **CORRECTIVE ACTION**  
--- | --- | ---  
End users are unable to log into MiCollab AWV conferences. | If MiCollab AWV user accounts are duplicated on both the MiCollab server and an LDAP server, end users will be unable to log into MiCollab AWV conferences. | Create and manage MiCollab AWV user accounts on the MiCollab server or on a LDAP server. You cannot use both methods on the same MiCollab installation.  
Some characters in the e-mail invitation do not display correctly for all languages. | The user has Outlook 2003 or settings are not configured in Outlook 2007 and 2010 to convert the characters correctly. | Change the international settings in Outlook for the UTF-8 mailto protocol. Refer to the MiCollab Audio, Web and Video Conferencing User Help for details.  
The Mitel Conferencing tab in Outlook does not retain the server URL and user password. | Windows 7 includes enhancements to security that require Administrator privileges to write to the folder where the OFT information is saved. | Unless the user has the necessary privileges, they will need to type the server URL and user password every time they want to access MiCollab Audio, Web and Video Conferencing through their Outlook calendar.  
When trying to log on by typing the user name and password the screen returns to the log on page. | Internet Explorer cookies are case sensitive. When the user logs on, the cookie is not set up with the same case and the user is denied access. | Make sure the cookie and username/password use the same case.  
The user logs on successfully but is returned to the log on page when attempting to perform any action within MiCollab Audio, Web and Video Conferencing. | The URL does not match the URL in the Internet Explorer cookies. It is likely that the URL used to connect to MiCollab Audio, Web and Video Conferencing is only a partial of the required URL. | Make sure the cookie uses the entire URL.  
Users will not see expected text on some popup windows. For example, "Documents" tab shows the word "Browse" using IE or Firefox but shows "Choose File" and "No file chosen" using Chrome. | The display language of some popup windows and buttons is determined by the version of operating system installed as well as the web browser being used. For example, Spanish version of Windows is required for specified buttons/popups to be displayed in Spanish. | Use the correct language version of Windows to see those prompts displayed in the selected MiCollab Audio, Web and Video Conferencing language.  
A "Connection to Server not complete" message is displayed when attempting to join a Web conference. | After performing an upgrade for the MiCollab Audio, Web and Video Conferencing blade, Web conferencing may not fully restart. | Log on the MiCollab Audio, Web and Video Conferencing Administrator Portal, and save the Web Conferencing Settings. A reboot is recommended after completing any application blade update.
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| MiVoice Business users are experiencing voice quality issues on AWV conference calls. | Compression is enabled. If compression is enabled, the call uses the lowest quality Codec (for example G.729).                                                                                               | Ensure that compression is disabled. With MiVoice Business systems, you can create network zones to manage compression and bandwidth.  
  • To ensure adequate voice quality on calls within zones, ensure that compression is disabled for intra-zone calls  
  • To ensure adequate voice quality on calls between zones on a MiVoice Business Release 7.2 or later system, configure the zones in a Group Zone. When you configure zones in the same Group Zones, the endpoints are forced to use higher quality audio compression codecs for calls between zones.  
  Refer to the MiVoice Business System Administration tool online help provided with the Network Zones form for details. |
| The MiCollab Audio, Web and Video Conferencing Client does not upgrade, or the upgrade is slow to complete. | When the MiCollab Audio, Web and Video Conferencing Client detects an existing version, it instructs Microsoft Windows Installer to remove the existing version first. If this operation fails, the MiCollab Audio, Web and Video Conferencing Client upgrade fails. | The installer or Registry could be corrupt or is missing files.  
  Uninstall the existing MiCollab Audio, Web and Video Conferencing Client manually before you upgrade the client.  
  1. Log into Windows as the user who is trying to install the MiCollab Audio, Web and Video Conferencing Client.  
  2. Verify that the existing MiCollab Audio, Web and Video Conferencing Client will not uninstall using Add/Remove Programs.  
  4. Run the utility; select and remove the MiCollab Audio, Web and Video Conferencing Client.  
  If the MiCollab Audio, Web and Video Conferencing Client does not uninstall, search through the registry keys (see Note below) and remove the keys that are related to the MiCollab Audio, Web and Video Conferencing Client. You will see MiCollab Audio, Web and Video Conferencing Client 1.0 information in the frame on the right-hand side when you have found the correct keys. |
### MiCollab Installation and Maintenance Guide

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user has an existing tab for an appointment form (such as “Web Conferencing”) and they run the Outlook Form install. A new form is not installed for Collaboration.</td>
<td>The installation makes the form available, but the install does not force a new tab to appear in Outlook.</td>
<td>The corrective action will help only if the previous Outlook form is part of a different software application. If the existing default Outlook form belongs to the previous version of MiCollab Audio, Web and Video Conferencing, the default form must be removed before the new form can be installed. Follow these steps: open the Outlook Calendar Appointment &gt; “Tools” Menu &gt; “Forms” Option &gt; “Choose Form” Option &gt; Look in “Calendar” &gt; Select “Collaborate” When you choose “Collaborate,” it replaces your “Web Conferencing” appointment form/tab.</td>
</tr>
<tr>
<td>The conference leader receives an error message when trying to add a participant’s outside phone number (not extension) using the Web interface.</td>
<td>The conference leader attempted to add an outside phone number and did not use the correct dialing format.</td>
<td>The conference leader must type the complete phone number that includes country code and area code, if applicable, with an outside number when adding a participant to the conference using the Web interface.</td>
</tr>
<tr>
<td>An operator error message is audible in the conference: “It is not necessary to dial a 1 when dialing this number.” The audio may be different, depending on the service provider.</td>
<td>Dial Access String (DAS) rules have not been set up correctly.</td>
<td>Add additional DAS rules to allow for the +1 to be stripped out from the local number. For example, 602 and 480 are two of the area codes for Phoenix, Arizona. For these area codes, add the following DAS Rules:</td>
</tr>
</tbody>
</table>

#### DAS Rules

<table>
<thead>
<tr>
<th>DAS Rule 1</th>
<th>DAS Rule 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>`s/\d+1(602</td>
<td>480)</td>
</tr>
</tbody>
</table>

The result: any phone number starting with 1602 or 1480 will have the leading “1” stripped off, replacing it with a “9,” the number, @, and then the IP address. For example, assuming that the phone number to be dialed is 1-602-555-1212 and the IP address configured in TCP/IP Settings is 192.168.22.55: 16025551212 becomes 96025551212@192.168.22.55 |
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calls dialed from MiCollab Audio, Web and Video Conferencing fail.</td>
<td>DAS rules contain errors.</td>
<td>Check DAS rules for typing errors (missing dots, slashed, etc.).</td>
</tr>
<tr>
<td>An attempt to create a three-way call with two users and a conference fails. The two users are briefly connected to one another, but then that call drops as well. Other users on the conference hear garbled voice while the failure is occurring.</td>
<td>SIP default settings are incorrect.</td>
<td>Use the default SIP settings.</td>
</tr>
<tr>
<td>One-way audio is experienced when the MiCollab Audio, Web and Video Conferencing server makes an outbound call using the MiVoice Office 250 PBX.</td>
<td>The Speech Encoding settings are incorrect.</td>
<td>The Speech Encoding Setting must be set to G.711 Mu-Law for UK installations.</td>
</tr>
<tr>
<td>When in a conference on an Android Xoom tablet, the sharing viewer flickers constantly if the shared area contains a blinking cursor.</td>
<td>The cause of this issue is unknown.</td>
<td>There is no solution for this issue.</td>
</tr>
<tr>
<td>If a user un-installs a previously installed version of MiCollab AWV client and then clicks Share in the web client, the browser displays Page not found error.</td>
<td>Previous information remains in the mitelCollab cookie.</td>
<td>User should remove the mitelCollab cookie from their browser. For example, in Google Chrome: 1. From the Google toolbar, click Settings 2. Click Show advanced settings. 3. Under Privacy, click Content Settings . . . 4. Under Cookies, click All cookies and site data. 5. Choose the MiCollab server and cookie (mitelCollab), click x to remove and then click Done.</td>
</tr>
<tr>
<td>Users running MiCollab Desktop Client Release 7.0 or earlier client are unable to upgrade the MiCollab AWV client to Release 7.1</td>
<td>User is attempting to upgrade the MiCollab AWV client to Release 7.1 from a MiCollab Desktop Client Release 7.0 or earlier client. This upgrade path is not supported.</td>
<td>User should upgrade to MiCollab Client Release 7.1 first, then perform the AWV client upgrade. OR User should upgrade the AWV client from the AWV portal or through the AWV Desktop Client Launcher.</td>
</tr>
<tr>
<td>UC 360 unable to connect to AWV conference.</td>
<td>TLSv1.0 is disabled.</td>
<td>Enable TLSv1.0 on the MiCollab server.</td>
</tr>
</tbody>
</table>
CONFERENCING ERROR MESSAGES FOR ALARM/ALERT CONDITIONS

The following table provides the error messages for alarm and alert conditions that may arise when using MiCollab Audio, Web and Video Conferencing. These messages are sent to General Alarm or General Alert e-mail addresses configured in System Options.

Table 7: Conferencing Error Messages for Alarm/Alert Conditions

<table>
<thead>
<tr>
<th>MESSAGE</th>
<th>SUBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>No trunks available (trunkalert)</td>
<td>“Enterprise alarm” Message = “no phone trunks are operational”</td>
<td>No VOIP ports available to make or receive calls.</td>
</tr>
<tr>
<td>database restart (alert)</td>
<td>“Enterprise alert” Message = “database restart at HH:MM:SS MM/DD/YYYY”</td>
<td>The Database service was restarted at the specified time.</td>
</tr>
<tr>
<td>mux restart (alert)</td>
<td>“Enterprise alert” Message = “Sip multiplexor restart at HH:MM:SS MM/DD/YYYY”</td>
<td>The muxer application was restarted at the specified time.</td>
</tr>
<tr>
<td>tp240driver restart (alert)</td>
<td>“Enterprise alert” Message = “phone trunk driver restart at HH:MM:SS MM/DD/YYYY”</td>
<td>The main call server was restarted at the specified time.</td>
</tr>
<tr>
<td>Fewer than n ports are still available (trunkalert)</td>
<td>“Enterprise alert” Message = “only %d ports are currently unused at %s”, $nlines, HH:MM:SS MM/DD/YYYY”</td>
<td>This is a number of ports available threshold alert.</td>
</tr>
<tr>
<td>Some trunk line went down (trunkalert)</td>
<td>“Enterprise alert” Message = “trunk lines %d went down HH:MM:SS MM/DD/YYYY”</td>
<td>Specified trunk ID went out of service.</td>
</tr>
</tbody>
</table>
Table 7: Conferencing Error Messages for Alarm/Alert Conditions (continued)

<table>
<thead>
<tr>
<th>MESSAGE</th>
<th>SUBJECT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some trunk line(s) came up (trunkalert)</td>
<td>“Enterprise info” Messages = “trunk lines $linecode ($resultCode) came up HH:MM:SS MM/DD/YYYY”</td>
<td>Trunk(s) ID are now in service at the specified time.</td>
</tr>
</tbody>
</table>

**MICOLLAB CLIENT**

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| MiCollab Client loses connection with the MiCollab server. | The client’s Login ID was changed. | 1. Re-deploy the client  
2. Send the user a fresh deployment email so the new Login ID can be communicated to the client. |
| After an upgrade from to MiCollab 7.1, clients are unable to connect. | MiVoice Business Gateway requires upgrading. | Upgrade MiVoice Business Gateway to the latest software version. |
| When you attempt to run the MiCollab Client Integration Wizard, the following error message is displayed “WmiAppException creating new enterprise: Tenant license exceeded.” | You have selected the PBX Type and installed the application software in the **Install and Upgrade Applications** panel. However, the system has not received its MiCollab Client license from the Application Management Center (AMC) yet, so the wizard is unable to run. | Wait at least 7 minutes and then restart the MiCollab Client wizard again. |
| One-way audio is occurring in the following connection: A MiCollab Client mobile (iOS or Android) user places a call through the MiVoice Border Gateway to a user on a communications platform (for example MiVoice MX-ONE). The called party does not receive audio from the MiCollab Client mobile user. | The packetization time on either the MiVoice Border Gateway and/or the communication platform is not set correctly to support MiCollab client. If you are using G.729 with MiCollab Client, the packetization time must be set to support 20 ms. | On the MiVoice Border Gateway:  
1. Log into the server manager.  
2. Under **System Configuration >Settings**, ensure that RTP framesize is set to **Dynamic**.  
Log into the communication platform management interface. Ensure that the system is set to support  
• G.729 codec  
• 20 ms packetization |
## MIVOICE BORDER GATEWAY

### Calls made from a MiCollab for Mobile client to a 3-digit extension are sent out the PSTN instead of going to the extension

The extension number conflicts with an emergency number that is pre-configured in the user’s deployment profile. Emergency numbers are exempt from any special routing and are dialed directly.

The following emergency numbers are pre-configured:
000,110,112,118,119,911,999

Although it is not recommended, emergency numbers that are not applicable to the user's region can be deleted from the user’s profile if the emergency number (for example, 119) conflicts with an existing dialing string (for example, extension 119). Before you delete an emergency number, you should be certain that the user will not be traveling to a region that uses it.

To modify the emergency numbers in a user’s deployment profile:
1. Log into the server manager.
2. Under Applications, click MiCollab Client Deployment.
3. Click Deployment Profiles.
4. Modify the user’s profile.
5. In the Emergency number field, modify the numbers as required. Multiple emergency numbers must be separated with commas and no spaces.
6. Click Save.

### SIP Teleworker devices are not functioning

SIP devices are denied access to the LAN by the MBG server. In the MBG application, the "Restrict SIP Devices" option under the Advanced Settings tab is set to True (enabled).

If this option was disabled in MBG R6.0 or earlier, it will be enabled when you upgrade to MBG R6.1 or later. As a result, you will lose SIP service.

To restore SIP service:
- Leave the option enabled and add the phones to the SIP Device List.
- or -

Under the Advanced Settings tab, click Settings and then click Edit. Set the "Restrict SIP Devices option to False.

**Note:** For security, this option should disabled only on a temporary basis.

### Red Warning dialog appears in all Teleworker pages of the Users and Services Provisioning application. The warning indicates that you must create a cluster from MiCollab.

MiCollab server is configured in LAN mode with the Teleworker application, but it is not clustered with a MiVoice Border Gateway (MGB)

The MiCollab server is a member of multiple MBG clusters. The MiCollab server can only belong to one MBG cluster.

When you deploy MiCollab in LAN mode with Teleworker, you must cluster the MiCollab server with an MBG server that is running Teleworker in the DMZ. The MiCollab can only belong to one MBG cluster. The cluster must be programmed in the Teleworker Clustering tab with a weight of zero

See “Install MiCollab Server in LAN Mode with MiVoice Border Gateway Server(s)” on page 52.
## NP-UM TROUBLESHOOTING

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clicking on NP-UM mailbox presents a blank screen</td>
<td>Mailbox does not have PWG FCOS</td>
<td>Contact your Administrator. Your mailbox is in the wrong Class of Service</td>
</tr>
<tr>
<td>Message Waiting Indication lamps on MiVoice Business system phones turn off before users have listened to their voice messages.</td>
<td>The SUPERSET Callback Message Cancel Timer on the MiVoice Business system is set to 24 hours. When this timer expires, the MiVoice Business system cancels the message waiting indication and turns off the lamps.</td>
<td>Set the SUPERSET Callback Message Cancel Timer field to blank: 1. Log into the System Administration Tool on the MiVoice Business System. 2. Access the Shared System Options form. 3. Blank out the SUPERSET Callback Message timer field. After you set this field to blank, message indication will not be cancelled by the system until the user has listened to the messages.</td>
</tr>
<tr>
<td>Clicking a NP-UM voice message in the MiCollab End User portal results in a blank screen with an icon indicating &quot;applet not found&quot;</td>
<td>Windows Media Player is not selected as the default player</td>
<td>Set Windows Media Player to be your default player: 1. Close Internet Explorer 2. Right-click in Windows Explorer. 3. Click <strong>Tools</strong> and then click <strong>Folder Options</strong> 4. On the File Types tab, scroll to WAV files 5. Click <strong>Change</strong> and select <strong>Windows Media Player</strong> from the list 6. Click <strong>OK</strong> 7. Open Windows Media Player 8. Click <strong>Tools</strong> and then <strong>Options</strong>. (If the Tools menu does not appear, click the Media Player icon in the upper left to view.) 9. On the File Types tab, ensure the WAV file check box is selected 10. Click <strong>OK</strong></td>
</tr>
<tr>
<td>For the Call Director - Alternate Transfer feature, users who are transferred to the alternate number do not hear the Timeout message if their call is unanswered. Instead, they hear the Message Center Main Menu.</td>
<td>NuPoint on MiCollab is integrated to a MiVoice Office 250.</td>
<td>None. When NuPoint on MiCollab is integrated with a MiVoice Office 250, the Timeout Message for the Call Director -- Alternate Transfer feature is not supported.</td>
</tr>
</tbody>
</table>
GOOGLE APPS TROUBLESHOOTING

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitel Google App (for example AWV Google Calendar Integration) is not</td>
<td>Browser incompatibility</td>
<td>Ensure that you are running the applications in a recent version of Google Chrome.</td>
</tr>
<tr>
<td>functioning correctly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Calendar is out of sync with MiCollab AWV.</td>
<td>After creating a new conference event, the user quickly closed Google</td>
<td>Delete the event from Google Calendar and then re-create it.</td>
</tr>
<tr>
<td></td>
<td>Calendar or the internet browser before the new event was added to AWV.</td>
<td></td>
</tr>
<tr>
<td>Mitel Google Apps are not functioning after a data restore or an upgrade.</td>
<td>Google App configuration settings are not included in a database backup.</td>
<td>Re-enter the configuration settings in the MiCollab server manager under</td>
</tr>
<tr>
<td></td>
<td>Therefore, during a data restore or upgrade, the configuration settings are</td>
<td>Configuration&gt;Google Apps</td>
</tr>
<tr>
<td></td>
<td>not maintained.</td>
<td></td>
</tr>
<tr>
<td>User does not have Google Gadget functionality</td>
<td>Users must install and configure the functionality on their computer.</td>
<td>Resend the Service Information (Welcome) Email the user. It provides instructions.</td>
</tr>
</tbody>
</table>

TROUBLESHOOTING LICENSING ERRORS

When administering licenses in your AMC account, you may receive an error message. The following table contains possible error messages, their meanings, and possible solutions:

<table>
<thead>
<tr>
<th>ERROR ID:</th>
<th>ERROR MESSAGE:</th>
<th>POSSIBLE PROBLEM:</th>
<th>POSSIBLE SOLUTION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>01201</td>
<td>Demo kit base level products can only be applied to servers one-at-a-time</td>
<td>You may be trying to add a demo kit to a server that already has one active demo kit</td>
<td>Recheck the Application Records for the relevant server</td>
</tr>
<tr>
<td>01205</td>
<td>This product can only be assigned to an Application Record under the same end customer as its related/bundled parts; &lt;company name&gt;</td>
<td>Some products (for example, YA) include MiVoice Business user and device licenses for the YA purchaser. You may be trying to assign these user and device licenses to a customer other than the original purchaser</td>
<td>Assign related/bundled licenses to the appropriate customer account as listed in the error message</td>
</tr>
<tr>
<td>01210</td>
<td>This product attempts to deliver an invalid application type for this application record</td>
<td>You may be trying to add another base product to an Application Record that already has a base product applied. (For example, you cannot add a Teleworker starter kit to an Application Record that has a MiVoice Business starter kit applied.)</td>
<td>Each base product requires a separate Application Record</td>
</tr>
<tr>
<td>ERROR ID:</td>
<td>ERROR MESSAGE:</td>
<td>POSSIBLE PROBLEM:</td>
<td>POSSIBLE SOLUTION:</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>01211</td>
<td>This application record already has a base service level product attached.</td>
<td>You may be trying to add another base product to an Application Record that already has the same base product applied. (For example, you cannot add a MiVoice Business 20-user starter kit to an Application Record that has a 40-user starter kit applied.)</td>
<td>Each base product requires a separate Application Record.</td>
</tr>
<tr>
<td>01213</td>
<td>This product is missing a required base product component that must be attached to this application record first</td>
<td>You may be trying to install a subsidiary license (for example, an IP Phone License) to an Application Record that has no base product assigned If you are adding licenses to a legacy system (3300 ICP system licensed prior to April/05 or SX-200 system licensed prior to April/06), it is possible that your Application Record has not been transferred</td>
<td>Ensure that a base product (for example MiVoice Business or YA starter kit) is installed before you attempt to add subsidiary licenses Every effort has been made to load all legacy data files but it is possible that some systems were missed. Send an email to the AMC and request that your application record be loaded from legacy data files</td>
</tr>
<tr>
<td>01220</td>
<td>The number of application records that can apply this product has already been reached.</td>
<td>You may be trying to add products beyond the maximum number of times allowed. (For example, by default, only one Teleworker demo kit is allowed. You cannot add an Application Record for another demo kit for the same Customer.)</td>
<td>--</td>
</tr>
<tr>
<td>01221</td>
<td>This product has already been used the maximum allowed for this application record</td>
<td>You may be trying to use a product beyond the maximum number of times allowed. (For example, some reward programs offer free product incentives. The number of these products per Application Record may be limited.)</td>
<td>Contact the AMC for further assistance</td>
</tr>
<tr>
<td>01230</td>
<td>This product requires an active <code>&lt;name of service&gt;</code> service component</td>
<td>You may be trying to apply an extension to a product that has expired. (For example, your Teleworker starter kit is over one year old. You cannot attach a Teleworker Support extension to this record.)</td>
<td>Ensure that you purchase extension products before the expiration of the base product</td>
</tr>
</tbody>
</table>
UCC V3 license bundles were introduced in MiCollab Release 6.0. Providing that you have active Software Assurance, all UCC V1 and V2 licenses are automatically converted to UCC V3 licenses during an upgrade to Release 6.0. If your system had UCC V1 licenses that were converted to UCC V3 licenses, it is recommended that you assign the newly converted bundles to the users who were previously using the UCC V1 licenses.

To identify users who were previously using UCC V1 licenses and assign them with the UCC V3 license bundles:

1. Run the UCC license identification script. This script scans the users and services in the MiCollab database and identifies users, who likely should be assigned with Basic, Entry, Standard, and Premium UCC V3 license bundles. The results of the script are saved to a CSV file. For example, the script may detect that the user Joe Smith appears to have Entry user services, Tom Jones has Standard services, and Bob Green has Premium services.

2. Open the CSV file.

3. Edit the file. Align the users with the correct license bundles.

4. Run the script again to associate the V3 bundles with the users. The script does not change the users’ services, it just associates the bundle with the user. For example, Joe Smith is associated UCC V3 Entry bundle; Tom Jones is associated with UCC V3 Standard bundle, and Bob Green is associated with UCC V3 Premium bundle.

<table>
<thead>
<tr>
<th>ERROR ID</th>
<th>ERROR MESSAGE</th>
<th>POSSIBLE PROBLEM</th>
<th>POSSIBLE SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>01240</td>
<td>Activation of this product will exceed the maximum number of licenses for this application record</td>
<td>You may be exeeding the maximum number of users that your base equipment is designed to accommodate. (For example, Teleworker is designed for 500 users. You cannot activate more than 500 licenses.)</td>
<td>Your product may need upgrade</td>
</tr>
<tr>
<td>01242</td>
<td>The products already attached to this application record are not valid for this extension product</td>
<td>You may be applying an extension product that is not compatible with the products already in the Application Record. (For example, you cannot add a Teleworker Support extension if your Application Record does not include a Teleworker starter kit.)</td>
<td>Ensure that you are applying the correct extension product to the correct Application Record</td>
</tr>
<tr>
<td>01280</td>
<td>This application record is using a multiple-year product that requires uplift binding determination</td>
<td>You may have an Application Record containing a product that applies to multiple years. (For example, the 6040 Office Server Suite.) When you try to add a license to the Application Record, it is not clear to which product year you wish to apply it</td>
<td>Contact the AMC for further assistance</td>
</tr>
</tbody>
</table>
5. Update each user's services from the User and Services application.

TROUBLESHOOTING ACTIVE DIRECTORY PROBLEMS

PROBLEM

1. When the administrator attempts to add an Active Directory user to MiCollab Users and Services application using the Bulk User Provisioning tool, an error is displayed.

   AND/OR

2. After users change their Active Directory password, they are unable to log into MiCollab.

POSSIBLE CAUSE

Latency or delay in the network is preventing Active Directory from responding to a search request from MiCollab. Without the search request results, MiCollab cannot add an Active Directory user.

DETECTING ACTIVE DIRECTORY DELAY

To detect any delay or latency on the Active Directory network at a site, use the "ldapsearch" command. This command opens a connection to an LDAP server and performs a search using specified parameters. The required parameters are:

- LDAP Root DN (or binddn)
- LDAP Root Password (or credentials)
- Login ID for an AD/IDS user.

Find the LDAP root DN and root password by executing the following Linux command in a shell console or a putty window:

```
[root@vmas-server]# more /etc/openldap/slapd.conf|grep binddn
```

Example output:

```
idassert-bind bindmethod=simple binddn="cn=root,dc=maslab,dc=mitel,dc=com"
credentials=d6d7a634-740a-4428-a162-3f7465f4fcdc
```

Replace the "binddn", "credentials", and "login ID" parameters that are marked with angle brackets in the following LDAP search command with the site values:

```
time ldapsearch -x -b "dc=virtual,dc=metadirectory" -D "<binddn>" -w "credentials" "(sAMAccountName=<login ID>)"
```

The following example uses these values:

- Bind DN: cn=root,dc=maslab,dc=mitel,dc=com
- Credentials: d6d7a634-740a-4428-a162-3f7465f4fcdc
- User login ID: testuser
Using the above values, the LDAP search command will be as follows:

```

time ldapsearch -x -b "dc=virtual,dc=metadirectory" -D "cn=root,dc=maslab,dc=mitel,dc=com" -w "d6d7a634-740a-4428-a162-3f7465f4fcdc" "(sAMAccountName=testuser)"
```

The output for the above LDAP search is listed below. The execution time is shown at the end of the display.

```
# extended LDIF
#
# LDAPv3
# base <dc=virtual,dc=metadirectory> with scope subtree
# filter: (sAMAccountName=testuser)
# requesting: ALL
#
#
# testuser Test, ad1.virtual.metadirectory
dn: cn=testuser Test,dc=ad1,dc=virtual,dc=metadirectory
  objectClass: top
  objectClass: person
  objectClass: organizationalPerson
  objectClass: USER
  cn: testuser Test
  sn: Test
  telephoneNumber: 1889
  givenName: testuser
  distinguishedName: cn=testuser Test,dc=ad1,dc=virtual,dc=metadirectory
  displayName: testuser
  name: testuser Test
  OBJECTGUID:: wajo7V3pCE6akVkmcf1Yw==
  sAMAccountName: testuser
  USERPRINCIPALNAME: testuser
  mail: testuser@test.com
  <SNIP>

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```
CORRECTIVE ACTION

Reduce the latency in your network such that the sum of the "real", "user", and "sys" parameters is less than 15 seconds.

VIEWING/COLLECTING LOG FILES

To assist in troubleshooting, you can either view or download the log files generated by the services running on MiCollab. You access log files from the Administration > View logs file page in the MiCollab server manager. Refer to the online help for instructions.

DATABASE RECOVERY (RESTORE)

This section provides procedures for

- MiCollab Server, MiCollab Server Appliance, and vMiCollab database recovery
- vMiCollab system disaster recovery
- Restoring a database to a different server

CONDITIONS AND CONSTRAINTS

The following conditions and constraints apply to database restores:

- In order to restore a backup to a MiCollab Server, the backup must contain the same applications as those installed on the server.
- Do not attempt to restore a database
  - that has been taken from a LAN mode (server-only) configuration to a Network Edge (server-gateway) configuration
  - that has been taken from a Network Edge (server-gateway) configuration to a LAN mode (server-only) configuration.
- Do not attempt to restore a database that has been taken from an individual application (for example, a NP-UM database) within MiCollab to either a MiCollab Server system or a vMiCollab deployment.
- All application data programmed in the MiCollab database is overwritten by the backup data during the restore operation. The data in the backup is not merged with the existing database in the MiCollab system.
- You cannot restore a vMiCollab OVA file from a newer vSphere platform to a platform with an older version of vSphere. For example, you cannot restore a vMiCollab OVA file that was exported from a vSphere 5.5 platform to a vSphere 5.1 platform.
The following table summarizes the MiCollab backup and restore scenarios that are supported:

**Table 8: Supported Backup and Restore Scenarios (after upgrade to Release 6.0)**

<table>
<thead>
<tr>
<th>BACKUP CONTENTS</th>
<th>CONFIGURATION ON TARGET SYSTEM</th>
<th>ADDITIONAL NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>All applications on MiCollab 6.0 Server or higher</td>
<td>All applications on MiCollab 6.0 Server system</td>
<td>To upgrade to MiCollab Release 6.0, your current system must be running MAS Release 4.0 SP1 or higher. After a MiCollab system has been upgraded to Release 6.0 and the backup restored, you can no longer restore a pre-release 6.0 backup. Therefore ensure that you obtain a backup immediately after you upgrade to MiCollab Release 6.0.</td>
</tr>
<tr>
<td>Subset of applications on MiCollab 6.0 system or higher</td>
<td>Same subset of applications as backup on MiCollab 6.0 system</td>
<td></td>
</tr>
<tr>
<td>Subset of applications on MiCollab 6.0 Server system or higher.</td>
<td>All applications on a newly installed (virgin) vMiCollab 6.0 deployment</td>
<td></td>
</tr>
<tr>
<td>MiCollab backup with all applications from a system deployed in Network Edge (server-gateway) mode</td>
<td>MiCollab system deployed in LAN (server-only) mode</td>
<td>You must reconfigure the system to LAN mode after the restore</td>
</tr>
<tr>
<td>MiCollab backup with all applications from a system deployed in LAN (server-only) mode</td>
<td>MiCollab system deployed in Network Edge (server-gateway) mode</td>
<td>You must reconfigure the system to Network Edge mode after the restore</td>
</tr>
</tbody>
</table>

The following table summarizes the MiCollab backup and restore configurations that are NOT supported.

**Table 9: Unsupported Backup and Restore Scenarios**

<table>
<thead>
<tr>
<th>BACKUP CONTENTS</th>
<th>CONFIGURATION ON TARGET SYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>All applications on MiCollab 6.0 system or higher</td>
<td>Some but not all applications on MiCollab 6.0 system</td>
</tr>
<tr>
<td>Subset of applications on MiCollab 6.0 or higher</td>
<td>Different subset of applications as backup on MiCollab 6.0</td>
</tr>
<tr>
<td>MiCollab 6.0 backup</td>
<td>MiCollab 4.0 or MiCollab 5.0 system</td>
</tr>
<tr>
<td>vMiCollab OVA file exported from a vSphere 5.5 platform</td>
<td>vSphere 5.1 platform</td>
</tr>
</tbody>
</table>
RESTORING A DATABASE BACKUP

You can restore a MiCollab Server, MiCollab Appliance, or vMiCollab system database from the server console using any of the following methods:

• restore from running server
• restore from removable device
• restore from network share

ACCESS THE CONSOLE RESTORE MENU

1. Log into the server console. See “Accessing the Server Console” on page 114.
2. From the Welcome menu, select the Restore from Backup option. The “Restore after Reboot” screen appears.
3. Select Reboot Now.
4. Wait for the system to reboot.
5. At the “Do you wish to restore from backup?” prompt, select Yes.
6. Select the restore method:
   - Restore from another running server
   - Restore from network share
   - Restore from removable device

RESTORE FROM ANOTHER RUNNING SERVER

If you are replacing an existing MSL 9.x server (physical or virtual), you can pull configuration and application data from it while it is still running and restore the data to a new MSL 10.x server.

The restore process automatically shuts down the old server.

Conditions:

• Installing the same ARID on new physical hardware will require a Hardware ID reset.
• If the two servers are on:
  - Connected networks (i.e. there is no router between them), both servers must have the same subnet mask applied.
  - Different networks, MSL will request a gateway/router IP address to use for access. When the restore is complete, the new server must be reconfigured for its own network because it will have inherited the network configuration of the running server.

CAUTION: Booting up the original server again after the restore procedure will result in IP address conflicts.
RESTORE FROM NETWORK SHARE

MSL Releases 10.0 and later support backups over the network to Linux/Unix servers, including to another MSL server, using the Network Backup option in the web-based server manager.

MSL 10.3 supports restore of SFTP backups using the console-based “Restore” option. You can restore application and configuration data during a fresh install of MSL at the “Do you want to restore from backup?” prompt. You can also force a restore “on demand”.

1. In the server console of the server that you are restoring, select **Restore from backup**.
2. A warning message is displayed and then the server reboots.
3. When the restore options are displayed, select **Restore from network share**.
4. Select the network interface to use for the restore (i.e. the network interface that has a connection (direct or indirect) to the network file share server).
5. Enter the IP address of the MSL server and the subnet mask to apply:
6. Enter the IP address of the network share server that contains the backup file.
7. If the file server is on a different network than the MSL server, MSL prompts you to enter the gateway IP address to use to access the backup server.
8. Enter the Windows login domain or workgroup of the backup server. (Leave this blank when restoring SFTP backups.)
9. Enter the shared folder name where the backup file is stored. If multiple backup files are stored, you must select the one you want to restore. (Leave this blank when restoring SFTP backups.)
10. Optionally, you can enter a subdirectory or path in which to store the backup file. (For SFTP backups, if you have created a folder on the backup server (e.g. “/backups”), then enter the path to that folder here.) Or press Next to skip this step.

**Note:** If you do not enter a sub-directory here for SFTP backups, the file is stored in the “/” folder by default.

11. Enter the username and password required to log in to the backup server
12. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the **Decryption password**. Click **Next** and then **Yes**.
13. A progress bar is displayed for the restore procedure. When the restore is complete, the server reboots to activate your restored configuration settings.
14. Proceed to “Check Application Data” on page 155.

RESTORE FROM REMOVABLE DEVICE

1. Follow the prompts to identify the backup file, and start the database backup.
2. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the **Decryption password**. Click **Next** and then **Yes**.
Troubleshooting

The Progress screen displays the data transfer progress.

**Note:** The filename of the backup must not contain any spaces; otherwise, you will receive an error when you attempt to restore it.

3. If you are restoring a database from a USB device and if "boot from USB" is enabled in the computer BIOS, you must remove the USB memory stick after the data transfer progress bar reaches 100%.

4. Proceed to “Check Application Data” on page 155.

**CHECK APPLICATION DATA**

1. After the reboot is complete log into the server manager and check to ensure that all application data is present.

**Note:** If the restored database contains data from MiCollab applications that are not installed on the MiCollab server, a red warning message is displayed in the server manager interface: "Data for applications NuPoint SAA & TTS, NuPoint Fax Port Enable, NuPoint Record a Call have been restored from backup, but these applications are not currently installed. The system may be unstable because of this. Please install these applications as soon as possible." Refer to “Installing Additional (Missing) Applications” on page 106 for instructions on how to install the missing applications.

2. If MiCollab is deployed in LAN only mode with Teleworker running remotely on an MBG server in the DMZ, you must also restore the MBG server with the current database; otherwise, the databases will be out of sync.

3. If your site uses Google Integration features (such as, calendar integration), re-enter the configuration settings in the Google Apps configuration tabs of the server manager interface.

**VMICOLLAB SYSTEM DISASTER RECOVERY**

You can recover a vMiCollab system database on the same virtual machine by deploying the latest vMiCollab OVF file, restoring your vMiCollab database backup, and then installing the latest MiCollab application software.

- Refer to the Mitel [Virtual Appliance Deployment Guide](#) for instructions on how to deploy the OVF file.
- See “Database Recovery (Restore)” on page 151.
- See “Install Application Software” on page 70.

**RESTORING A MICOLLAB SERVER DATABASE TO A DIFFERENT SERVER**

Use the following procedure to restore a

- MiCollab 5.0 or later database to a MiCollab 7.1 server, or a
- MiCollab 7.1 database to a MiCollab 7.1 system on different server hardware.
To restore a database from Server A to a different Server B:

1. Perform a database backup from Server A to a USB device or network server. See “Server Manager "Backup"” on page 108 for instructions.

2. Clear your Hardware ID from the AMC. See “Backup and Restore with Fresh Install” on page 100 for instructions.

3. After you receive an email from Mitel Technical Support stating that the Hardware ID has been cleared from Server A, you can proceed with the migration to Server B. Note that after the Hardware ID is cleared from Server A, it will continues to function.

4. Install MSL 10.3.x.x. on Server B.

5. At the "Do you wish to restore from backup?" prompt, select Yes.
   - Select Restore from network share. Follow the prompts to specify the location of the backup file and start the restore,
   - Select Restore from removable device, or
   - Select Restore from running server option to retrieve the configuration from the existing MiCollab server. This option shuts down the server that you are retrieving the configuration from before bringing up the new server. It configures the new system with the IP address of the old system.
   - If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the Decryption password. Click Next and then Yes.
   - After MSL completes the restore of the Server A database to Server B, the MSL operating system reboots.

6. At the root prompt (or using SSH) login as Admin and select Configure this server to review MSL server configuration settings.

7. Review the settings without changing any parameters and then reboot the server. This step changes the MAC address in the MSL database.

   Note: Server B now has the same FQDN and IP address as Server A.

8. After system reboots, log into the server manager. See “Log in to the Administrator Portal (Server Manager)” on page 29 for instructions.

9. Deactivate and then re-activate your ServiceLink account (Application Record ID)
   - Under ServiceLink, click Status.
   - If a service account ID (Application Record ID) is displayed on the Status page, click the here link and then click Deactivate.
   - Enter your Application Record ID and click Activate.

10. At the root prompt (or using SSH), login to the server console as Administrator and select Install MiCollab from CD/DVD. Install the MiCollab Application software from CD/DVD or USB.

11. Under Administration, click Shutdown or Reconfigure. Select Reboot from the drop-down menu and then click Perform. After the reboot is complete, the MiCollab system is operational with the database contained in backup.
Appendix A

FLOW THROUGH PROVISIONING:
ADDING GREENFIELD MICOLLAB TO
GREENFIELD MIVB SERVERS
OVERVIEW

The Mitel Integrated Configuration Wizard (MiCW) supports the initial configuration of MiCollab with MiVoice Business (MiVB) platforms for the following deployments:

- Greenfield (new) MiCollab with a single greenfield MiVB platform
- Greenfield MiCollab with a single existing MiBV platform
- Greenfield MiCollab with greenfield MiVB cluster (with or without resiliency)
- Greenfield MiCollab with existing MiVB cluster (with or without resiliency)

For MiCollab with a single MiVoice Business platform deployments, you must enter both the MiVoice Business and MiCollab provisioning data in a single Mitel Integrated Configuration Wizard session in order to start sharing and enable Flow Through Provisioning (that is, you only run the wizard once).

For MiCollab with multiple MiVoice Business deployments, you must run the MiCW against each MiVoice Business element to configure them into a cluster. Then, you run MiCW against one of the MiVoice Business servers and MiCollab (in a single MiCW session) to join MiCollab into the cluster and configure the MiCollab application settings. After you complete the wizard, MiCollab and the MiVB network elements are sharing data and Flow Through Provisioning is enabled.

The MiCW application software is only available from Mitel Online. You install the MiCW on a maintenance PC and enter data in the screens of the wizard. The wizard creates a configuration file of the entered data that you apply to the MiCollab and MiVoice Business databases. See “About the Mitel Integrated Configuration Wizard” on page 5 for more information.

Note: You must configure the MiVoice Business and MiCollab in a single MiCW session to start sharing data and enable Flow Through Provisioning. In addition, MiCW creates a common SIP Password (unseen in the MiCW interface) and applies it to both the MiCollab AWV SIP Server Configuration and the MiVoice Business AWV ports. If you run the Mitel Integrated Configuration Wizard separately against the MiVoice Business and MiCollab, the SIP passwords will not match and AWV will not function.

MICW USE CASES

GREENFIELD MICOLLAB WITH A SINGLE GREENFIELD MIVB PLATFORM

In this deployment scenario, you are configuring a greenfield (new) MiCollab with a single greenfield (new) MiVB platform. You run the Mitel Integrated Configuration Wizard once to

- configure the MiVoice Business server
- configure the MiCollab application resources on the MiVoice Business platform
- configure the application resources on the MiCollab server, and
- automatically add the MiCollab as a Network Element in MiVB and perform data sharing and sync

RUN WIZARD

1. In the Start Configuration page, select Create a new Configuration and click Next.
2. In the System Parameters page
- Complete the MiVB system parameters.
- Check the **Configure MiVoice Business System Data** box.
- Select the **MiCollab** option box.
- Enter the MiCollab IP address.

### System Parameters

Identify the MiVoice Business, the MiCollab and general site information by entering the required information.

**MiVoice Business**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>[Input Field]</td>
</tr>
<tr>
<td>IP Address</td>
<td>[Input Field] (MiVoice Business IP Address after configuration)</td>
</tr>
<tr>
<td>Hostname or FQDN</td>
<td>[Input Field]</td>
</tr>
<tr>
<td>Platform</td>
<td>[Virtual MiVB]</td>
</tr>
<tr>
<td><strong>Configure MiVoice Business System Data</strong></td>
<td>[Checkbox]</td>
</tr>
</tbody>
</table>

**MiCollab**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>[Input Field]</td>
</tr>
</tbody>
</table>

**Figure 16: System Parameters**

3. Complete the General Site information on the System Parameters page as required by the site and click **Next**.

4. Complete the following pages based on the site requirements: Licenses and System Options, Local Area Network Connection, and the MiVoice Business System Settings.

5. In the Applications page
   - Select **Single MiVoice Business**
   - Select the required MiCollab applications.
Flow Through Provisioning: Adding Greenfield MiCollab to Greenfield MiVB Servers

Applications

Select the type of solution you want to configure:
Clear the Configure MiVoice Business System Information check box if the MiVoice Business has already been configured. You cannot use this option if any programming changes to the system were made since commissioning. For more information, click here.

Select the type of network configuration for the MiVoice Business:

- Single MiVoice Business
- MiVoice Business Cluster
  - Create new non-resident cluster
  - Create new cluster for resident users and services
  - Join existing cluster
  - Modify existing cluster element

Select the applications that are part of your solution:

- Hot Desk Devices
- Voice Mail
  - Embedded
  - MiCollab NuPoint VM
- Mobility Services - Dynamic Extension
- MiCollab Speech Auto Attendant
- Teleworker
- MiCollab Audio, Web and Video

Figure 17: Applications Page - Join MiCollab into Cluster

6. Configure the MiVoice Business and Application resources.

**Note:** Do not add any users or services via the Automatically Generate and Users and Services page.

7. Save and apply the configuration. MiCW automatically adds the MiCollab as a Network Element in MiVB and performs data sharing and synchronization.

**Note:** After sharing is started, a Major alarm is generated on both elements. On each element, configure SNMP Agent support and align the community strings to clear the alarms.

8. Proceed to “Configure Users and Services” on page 82.

GREENFIELD MICOLLAB WITH A SINGLE EXISTING MIVB PLATFORM

In this deployment scenario, you are configuring a greenfield MiCollab with a single existing (brownfield) MiVB platform. You run the Mitel Integrated Configuration Wizard once to

- configure the MiCollab application resources on the MiVoice Business platform
- configure the application resources on the MiCollab server, and
- automatically add the MiCollab as a Network Element in MiVB and perform data
sharing and sync

RUN WIZARD

1. In the Start Configuration page, select **Create a new Configuration** and click **Next**.

2. In the System Parameters page:
   - Complete the MiVB system parameters.
   - Check the **Configure MiVoice Business System Data** box.
   - Check the **MiCollab** option box.
   - Enter the MiCollab IP address.

3. Complete the General Site information on the System Parameters page as required by the site and click **Next**.

4. Complete the following pages based on the site requirements: Licenses and System Options, Local Area Network Connection, and the MiVoice Business System Settings.

5. In the Applications page
   - Select **Single MiVoice Business**
   - Select the required MiCollab applications.
Flow Through Provisioning: Adding Greenfield MiCollab to Greenfield MiVB Servers

Applications

Select the type of solution you want to configure.
Clear the Configure MiVoice Business System information check box if the MiVoice Business has already been configured. You cannot use this option if any program changes to the system were made since commissioning. For more information, click Help.

Select the type of network configuration for the MiVoice Business

Network Configuration
- Single MiVoice Business
- MiVoice Business Cluster
  - Create new non-resilient cluster
  - Create new cluster for resilient users and services
  - Join existing cluster
  - Modify existing cluster element

Select the applications that are part of your solution

- Hot Desk Devices
- Voice Mail
  - Embedded
  - MiCollab Hybrid UM
- Mobility Services - Dynamic Extension
- MiCollab Speech Auto Attendant
- Teleworker
- MiCollab Audio, Web and Video

Figure 19: Applications Page - Join MiCollab into Cluster

6. Save and apply the configuration. MiCW automatically adds the MiCollab as a Network Element in MiVB and performs data sharing and synchronization.

Note: After sharing is started, a Major alarm is generated on all the elements. On each element, configure SNMP Agent support and align the community strings to clear the alarms.

7. Log into the MiCollab server manager and run the Data Reconcile Wizard.
ADDING GREENFIELD MICOllAB TO A NEW MIVB CLUSTER

In this deployment scenario, you are adding a greenfield MiCollab to a new resilient MiVB cluster that has two or more greenfield MiVB platforms. You must run the wizard once for each element.

INITIAL RUN OF WIZARD

During the first run of the wizard, you create a cluster. If you are configuring resiliency, you must create the cluster on the secondary controller (for example, Mivb_2nd). On the next run, you configure the primary controller (for example Mivb_prim) with MiCollab in Join Cluster mode.

1. In the Start Configuration page, select Create a new Configuration and click Next.

2. In the System Parameters page, complete the MiVB system parameters.
   - Check the Configure MiVoice Business System Data box
   - Do not check the MiCollab box.

3. Complete the General Site information on the System Parameters page as required by the site and click Next.

4. Complete the following pages based on the site requirements: Licenses and System Options, Local Area Network Connection, and the MiVoice Business System Settings.

5. In the Applications page, select MiVoice Business Cluster, and select
   - Create new non-resilient cluster, or
   - Create a new cluster for resilient users and services.
   - For non-resilient deployments, ensure the MiCollab Applications are unchecked.
   - For resilient deployments, all Applications are unchecked and disabled by default.
6. Complete the wizard to configure the MiVB element.
RUN WIZARD FOR EACH ADDITIONAL MIVB CLUSTER ELEMENT

Next, run the MiCW against each additional MiVB element to join them with the cluster. For resilient deployments, this MiCW run configures the primary controller (Mivb_prim) for the previously configured secondary element (Mivb_2nd).

1. In the Start Configuration page, select Create a new Configuration and click Next.

2. In the System Parameters page complete the MiVB system parameters.
   - Check the Configure MiVoice Business System Data
   - Do not check the MiCollab option box.

   **System Parameters**

<table>
<thead>
<tr>
<th>MiVoice Business (required)</th>
</tr>
</thead>
<tbody>
<tr>
<td>* System Name: Mivb_prim</td>
</tr>
<tr>
<td>* IP Address: 192.168.1.22</td>
</tr>
<tr>
<td>** Hostname or FQDN</td>
</tr>
<tr>
<td>** Platform: Virtual MiVB</td>
</tr>
<tr>
<td>* Configure MiVoice Business System Data</td>
</tr>
</tbody>
</table>

   **Figure 23: System Parameters - for additional MiVB Element**

3. Complete the General Site information as required.

4. Complete the Licenses and System Options, Local Area Network Connection, and the MiVoice Business System Settings based on the site requirements.

5. In the Applications page select MiVoice Business Cluster and Join existing cluster. Leave the MiCollab application options disabled.

   **Applications**

<table>
<thead>
<tr>
<th>Select the type of solution you want to configure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear the Configure MiVoice Business System Information check box if the MiVoice Business has already been configured. You cannot use this option if any programming changes to the system were made since commissioning. For more information, click Help.</td>
</tr>
</tbody>
</table>

   **Select the type of network configuration for the MiVoice Business**

   - Single MiVoice Business
   - MiVoice Business Cluster
     - Create new resilient cluster
     - Create new cluster for resilient users and services
     - Join existing cluster
     - Modify existing cluster elements

   **Select the applications that are part of your solution**

   - Hot Desk Devices
   - Voice Mail - Embedded
   - Mobility Services - Dynamic Extension

   **Figure 24: Applications Page - Join Additional MiVB to Cluster**
6. In the "MiVoice Business Join Cluster" page, enter all the mandatory fields for "Mivb_prim" (primary controller) and then enter the IP address of Mivb_2nd (secondary controller) in the Master Element IP Address as shown in figure below.

![MiVoice Business Join Cluster](image)

**Note:** This procedure specifically requires the secondary controller to be nominated as the SDS master when joining the primary controller. This is intentional.

7. Complete the wizard to configure the element.

8. Repeat steps 1 to 7 above for each additional MiVB in the cluster.

**LAST RUN OF WIZARD CONFIGURES MICOLLAB**

Lastly, run the MiCW against MiCollab to join it into the cluster and configure the MiCollab application settings. After you complete the wizard, MiCollab and the MiVB network elements are sharing data.

1. In the Start Configuration page, select **Create a new Configuration** and click **Next**.

2. In the System Parameters page:
   - Check the **Configure MiVoice Business System Data** box
- Check the **MiCollab** box.
- Enter the MiCollab IP address.

### System Parameters

Identify the MiVoice Business, the MiCollab and general site information by entering the required information:

**MiVoice Business**

- **System Name:** MiVb_2nd
- **F Address:** 192.168.1.2
- **Hostname or FCDN:**
- **Platform:**
  - [ ] Configure MiVoice Business System Data
- **MiCollab**
  - **IP Address:** 192.168.1.23

**Figure 26: System Parameters Page - Configuring MiCollab**

3. Complete the General Site information as required for the site and click **Next**.

4. In the Applications page,
   - For the Network Configuration, select **MiVoice Business Cluster - modify existing cluster element**.
   - Select the MiCollab applications for your solution.

### Applications

Select the type of solution you want to configure. Clear the Configure MiVoice Business System Information check box if the MiVoice Business has already been configured. You cannot use this option if any programming changes to the system were made since commissioning. For more information, click Help.

**Select the type of network configuration for the MiVoice Business**

- **Network Configuration:**
  - Single MiVoice Business
  - MiVoice Business Cluster
    - Create new non-resilient cluster
    - Create new cluster for resilient users and services
    - Join existing cluster
    - Modify existing cluster element

**Select the applications that are part of your solution**

- [ ] Hot Desk Devices
- [ ] Voice Mail
- [ ] Embedded
- [ ] MiCollab NuPoint UM
- [ ] Mobility Services - Dynamic Extension
- [ ] MiCollab Speech Auto Attendant
- [ ] Teleservice
- [ ] MiCollab Audio, Web and Video

**Figure 27: Select MiCollab Applications**
5. In the MiVoice Business Cluster Definition page, add the names of the MiVB cluster elements:

![MiVoice Business Cluster Definition Image]

Figure 28: Define MiVoice Business Elements in Cluster

6. Configure the MiCollab Application resources.

**Note:** Do not add any users or services via the Automatically Generate and Users and Services page.

7. If any MiCollab applications like NuPoint were selected in "Application Resources and Options" page, select the IP address of the secondary controller (Mivb_2nd) from the drop-down menu. This is shown in the figure below.

![Application Resources and Options Image]

Figure 29: Select IP Address of Secondary MiVoice Business Controller

8. Save and apply the configuration. MICW automatically adds the MiCollab as a Network Element in MiVB and performs data sharing and synchronization.
9. Proceed to “Configure Users and Services” on page 82.

GREENFIELD MICOllAB WITH EXISTING MIVB CLUSTER

In this deployment scenario, you are configuring a greenfield MiCollab with two or more existing (brownfield) MiVB platforms in a cluster. You must run the wizard once for each element.

BEFORE YOU RUN THE WIZARD

1. Ensure that the MiVoice Business element databases are in sync by performing a sync from one MiVoice Business element to all the other MiVoice Business elements in the network.
2. Export the user data from one of the MiVB elements in the sharing network to a CSV file.
3. If your site uses custom Feature Access Codes or Class of Service Options, export the data from these forms to CSV files.
4. Create roles and templates in MiCollab that correspond to the service levels to be assigned to the users.
5. Import the CSV of user entries into the USP Bulk User Provisioning (BUP) tool and assign roles to the users.
6. Add the users with their roles to the MiCollab USP directory from the BUP tool.

RUN THE WIZARD

Run the wizard to add MiCollab to the cluster via one of the MiVB elements.
1. In the Start Configuration page, select Create a new Configuration and click Next.
2. In the System Parameters page
   - Complete the MiVB system parameters.
   - Check the Configure MiVoice Business System Data box.
   - Select the MiCollab option box.
   - Enter the MiCollab IP address.

Figure 30: System Parameters - First Run
3. Complete the General Site information on the System Parameters page as required by the site and click **Next**.

4. Complete the following pages based on the site requirements: Licenses and System Options, Local Area Network Connection, and the MiVoice Business System Settings.

5. In the Applications page,
   - For the Network Configuration, select **Join Existing Cluster**
   - Select the MiCollab applications for your solution.

### Applications

Select the type of solution you want to configure.
Clear the Configure MiVoice Business System Information check box if the MiVoice Business has already been configured. You cannot use this option if any programming changes to the system were made since commissioning. For more information, click Help.

Select the type of network configuration for the MiVoice Business:

- Single MiVoice Business
- MiVoice Business Cluster
  - Create new non-resilient cluster
  - Create new cluster for resilient users and services
  - Join existing cluster
  - Modify existing cluster element

Select the applications that are part of your solution:

- Hot Desk Devices
- Voice Mail
  - Embedded
  - MiCollab NuPoint UV
- Mobility Services - Dynamic Extension
- MiCollab Speech Auto Attendant
- Teleworker
- MiCollab Audio, Video and Video

**Figure 31: Join Existing Cluster**

6. Configure the MiCollab Application resources.

**Note:** Do not add any users or services via the Automatically Generate and Users and Services page.

7. In the MiVoice Business - Advanced Configuration page, import CSV files of MiVB system form settings (for example, COS or FAC settings).

8. Save and apply the configuration. MiCW automatically adds the MiCollab as a Network Element in MiVB and performs data sharing and synchronization.

9. Log into the MiCollab server manager and run the Data Reconcile Wizard.
AFTER SHARING IS STARTED

After sharing has started, it is recommended that you:

1. Provide a login ID and password and a set registration and replacement code for any MiVoice Business elements added to MiCollab from MiVoice Business. The former is used to modify hot desk passcodes and the latter is used to register application soft-phones.

2. Review the shared template definitions in MiVoice Business and add MiVoice Business programming for templates added to MiVoice Business from MiCollab. MiVoice Business-specific programming such as feature keys can be added and will be used when MiCollab creates phones using these templates. For example, consider adding multi-call feature to UC endpoint devices or other feature keys.
Appendix B

FLOW THROUGH PROVISIONING:
ADDING GREENFIELD MICOLLAB TO
BROWNFIELD MIVB SERVERS
OVERVIEW

Flow Through Provisioning uses System Data Synchronization (SDS) to synchronize updates made between the MiCollab and MiVoice Business system databases. The following data is synchronized:

- user and services data
- network elements
- departments and locations, and
- roles, and templates.

This procedure describes how to configure Flow Through Provisioning when you are adding a new MiCollab server to a site with existing (Brownfield) MiVoice Business servers. The following is an overview of the main tasks:

- Prepare site
- Install MiCollab and application software
- Configure network elements on MiCollab
- Provision application ports
- Create templates (and roles)
- Create CSV file and import using Bulk User Provisioning Tool
- Start sharing
- Run Reconcile Wizard

CAUTION: Perform this procedure during off business hours.

PREPARE SITE

1. Ensure that you have recent database backups of the MiVoice Business systems or MiVoice Business Express system.
2. Ensure that the MiVoice Business platforms that you want to support Flow Through Provisioning are sharing data. Ensure that SDS is enabled in MiVB System Options form.
3. Ensure that the MiVoice Business element databases are in sync by performing a Sync from one MiVoice Business element to all the other MiVoice Business elements in the network:
   - Log into the System Administration Tool of one of the MiVoice Business elements in the sharing network.
   - Access the Network Elements form.
   - Check the boxes of all the other network elements in the sharing network.
Figure 32: Check the Boxes of the Other Network Elements

- Click **Sync**.
- Under **Shared Forms to be Synchronized**, check the **User**, **Service Hosting** and **Templates** boxes.
- Under **Synchronize Options**, select **Merge**.

Confirm Synchronization

The shared data from Local_173 will be synchronized to the following (3) Network Element(s):

- Local_177
- Local_181
- Local_185

Select the Shared Forms to be Synchronized:

Note: You configure the data that is shared in each of these forms, using the Shared Forms Configuration form.

Synchronization Options:

- **Merge** (The synchronization operation will combine data from the Master and Slave, where applicable)
- **Overwrite** (Master’s data will overwrite the Slave’s data, where applicable)

View Form Sync Info

Resilient User-Device Policy

- Only Synchronize data where Local_173 is the PRIMARY host for resilient devices.
- Synchronize data where Local_173 is either the PRIMARY or SECONDARY host for resilient devices.

Figure 33: Select the Forms to be Synchronized

- Click **OK** to perform the synchronization.
Flow Through Provisioning: Adding Greenfield MiCollab to Brownfield MiVB Servers

4. It is recommended that you resolve outstanding SDS distribution errors on every MiVoice Business platform prior to upgrading them. On every MiVoice Business in the sharing network:
   - Log into the MiVoice Business system administration tool.
   - Choose to view forms alphabetically.
   - In the left forms menu, click SDS Distribution Errors - All.
   - Select Display all and then click Retrieve.

   The SDS Distribution Errors form displays any synchronization delays and errors that occur when changes are propagated to other network elements in your sharing network. This form shows the status of pending updates and updates that were not distributed successfully to other network elements. SDS Distribution Errors must be resolved to keep your network elements synchronized.

   To resolve the pending updates or errors:
   - Click Retry to retry the update. "Retrying" appears before the Reason field in the record. Click Data Refresh. If the update is successful the update record disappears from the list. If the update is unsuccessful, the update error record will be updated with the new time stamp.
   - Click Force Change to update the remote node with the record from the local node. (This action only applies to conflict errors).
   - Click Login to launch the system administration tool of the remote system. You can then manually fix the error through the System Administration Tool of the remote element. Click Data Refresh to update the main window. After you have corrected the error on the remote element, you may have to delete the error record on the local element. Go back to the SDS Distribution Errors form on the local element, select the error record and click Delete.

5. Upgrade the MiVoice Business platform(s) to Release 7.2 or later.

RUN GDM CHECK AND GDM REPAIR COMMANDS

Run the GDM Check and GDM Repair maintenance commands on each MiVoice Business network element immediately prior to start sharing.

1. Log into the MiVoice Business system administration tool.
2. Choose to view forms alphabetically.
3. In the left forms menu, click Maintenance Commands.
4. Enter the GDM REPAIR USERANDSERVICE command.
5. Enter the GDM CHECK USERANDSERVICE command again to ensure that no data inconsistencies are found.
ADD SOFTPHONE USERS

If you have several MiVoice Business users who require SIP softphones, it is recommended that you add them manually through USP after you have configured Flow Through Provisioning. However, if there are many users who require softphones, use the following procedure to add the softphones to the MiVoice Business database:

1. Export the Users and Services Configuration form from each MiVoice Business system to CSV files to obtain the user entries.
2. Open the contents of each CSV file in an Excel spreadsheet (or similar spreadsheet application).
3. For each user that requires a softphone, locate the user in the file.
4. Copy and paste the user row below the existing user’s entry.
5. Delete the existing user’s entry.
6. Modify the data as follows:
   - In the Device Type cell for the user, change the device type to "UC Endpoint".
   - In the SIP Password cell, enter a SIP Password for the user up to 26 ASCII characters including numeric, alphanumeric, and special characters.
   - Set the COS cell to a Class of Service that supports SIP softphones.
   - Set the SIP Device Capabilities to 71 (default).
   - Blank out the Hosted User Service Guid for the new phone.
   - Extension Numbers must be unique.
   - Service Label must match a Service Label in MiCollab Users and Services.
Flow Through Provisioning: Adding Greenfield MiCollab to Brownfield MiVB Servers

MIGRATE FULL IP USERS TO MULTI-DEVICE USER GROUPS

To convert a large number of full service IP Phone users to Multi-Device User Groups (MDUG):

1. Log into the MiVoice Business system administration tool.
2. Access the Multi-device User Groups form.
3. Click Import.
4. Download a copy of the Import spreadsheet.
5. Save a copy of the 3300ICPImportSpreadsheet.tar.gz file.
6. Unzip the 3300ICPImportSpreadsheet.tar.gz file.
7. Open the spreadsheet folder and launch the 3300ICPImportSpreadsheet.xls file in Excel.
8. Select the Multi-Device user group form. You may have to click Options and enable Macros & Active X.
9. Enter the directory numbers that you want to use to create Multi-device User Groups. The order does not matter.
   
   Note: The import spreadsheet tool applies a Standard group type which you can modify to External Twin if required.

10. Import the spreadsheet of directory numbers into the MiVB system administration tool.

OBTAIN LICENSES

Create an Application Record IDs and assign licenses through the Application Management Center. Refer to "Licensing" on page 17 for instructions.
INSTALL MICOLLAB AND APPLICATION SOFTWARE

Refer to “Install MiCollab Server” on page 31 for instructions on how to install the MiCollab system software:

- on a qualified industry standard server, or
- on a Microsoft Hyper-V virtual machine.

Refer to “Installing Virtual MiCollab in a VMware Environment” on page 55 for instructions on installing MiCollab in a VMware environment.

Run the MiCollab Client Integration Wizard to configure the server in integrated mode (see “Configure MiCollab Client Mode” on page 79). Flow Through Provisioning is only supported for MiCollab Client integrated mode. Before running the wizard, ensure that you select the Synchronize Dynamic Extension Only option on the MiCollab Client Service Configuration > Synchronization tab to prevent pulling in all the MiVoice Business user accounts into the MiCollab Client database.

PROVISION THE NETWORK ELEMENTS

Configure MiCollab with the MiVoice Business network elements for Flow Through Provisioning.

1. Log into the MiCollab server manager.

2. Under Applications, click Users and Services.

3. Click the Network Element tab.

4. Click Add.

5. Complete the MiVoice Business Network Element fields.
   - Refer to the help for field descriptions.
   - Check the Use NuPoint UM IP Integration Licenses if the Network Element will support the NuPoint UM application ports.

6. If the system includes the NP-UM application, complete the following:
   - Enter the “Call Reroute First Alternative Number”.
   - Enter the “NP-UM voice mail hunt group number” in the “Call Forward Destination Directory Number” field.
   - Enter the hunt group number for the HCI Reroute Hunt Group. (This hunt group is used to enable MWI lamp on stations with mailboxes via the MiTAI application interface.)

7. Click Save.

8. If you are adding the first network element to the list, you are prompted to associate the element with the default UCC templates. If you select Yes, the network element field for the primary phone in the default templates is automatically set to the name of this network element. If you select No, you must create custom templates and associate them with this element.

9. After you save your changes to the Network Elements tab, if the network element supports the NP-UM application ports, you must activate the changes.
At the top of the screen, click the NuPoint activation link. Click OK. Complete the process of activation. Click Return to Server Manager in the left-hand menu.

PROVISION APPLICATION RESOURCES

Refer to the MiCollab Platform Integration Guide for instructions on how to configure the MiCollab application resources for the MiVoice Business platform.

CREATE TEMPLATES (AND ROLES)

You need to create MiCollab user templates that reflect the MiCollab service mixes that you want to assign to each user.

Each MiCollab template is assigned to a MiVoice Business network element, so you will need to create a set of templates for each network element. You create a template by saving a copy of one of the default templates and then modifying it.

Tip: Minimize the number of different service mixes to simplify the data migration.

This task requires that you:

• Identify the users, their primary phone numbers, and host primary MiVoice Business.
• Identify the MiCollab application service mixes that you want to assign to users
• Identify any differences in the application service configurations
• Create single-phone templates for each user type.

IDENTIFY USERS, PRIME NUMBERS AND PRIMARY MIVOICE BUSINESS

1. Log into the MiVoice Business system administration tool.
2. Export the Network Element form data to a CSV file and open it in Excel.
3. Export the Users and Services Configuration form to a CSV file and open it in Excel.
4. In the Users and Services Configuration file, open the Find and Replace function.
5. Get a Network Element ID (GUID) and its corresponding Home Element Name from the Network Element CSV file and then enter them into the Find and Replace function in the Users and Services Configuration CSV.
6. Use the Find and Replace function to replace the Network Element IDs (GUIDs) with their Home Element names.

7. Sort the data on the Home Element Name and save the file.
8. Repeat the above step for each MiVoice Business network element.
IDENTIFY THE MICOLLAB APPLICATIONS SERVICE MIXES

For example, how many users will require:
- MiCollab Client, NP-UM, AWV and Teleworker?
- MiCollab Client, NP-UM and AWV?
- MiCollab Client and NP-UM?
- only MiCollab Client?

Table 10 provides lists services that you could program into custom templates for the purpose of importing the MiVoice Business users into the MiCollab database.

<table>
<thead>
<tr>
<th>TEMPLATE PURPOSE</th>
<th>TEMPLATE CONTENTS</th>
<th>SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>For an Entry-level user</td>
<td>1 User</td>
<td>UCC license bundle set to &quot;UCC Entry User for Enterprise (Vx.0)&quot;</td>
</tr>
<tr>
<td></td>
<td>1 Phones</td>
<td>Primary Phone: Desk Phone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Secondary Phone: EHDU Phone</td>
</tr>
<tr>
<td></td>
<td>Include MiCollab Client Entry</td>
<td>Feature Profile: UCC (Vx.0) Entry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Desk phone extension: None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Soft phone extension: None</td>
</tr>
<tr>
<td></td>
<td>1 NuPoint Mailbox</td>
<td>NuPoint mailbox license with Call Director and Standard and Advanced UM licensing</td>
</tr>
<tr>
<td>For a Standard-level user</td>
<td>1 User</td>
<td>UCC license bundle set to &quot;UCC Standard User for Enterprise (Vx.0)</td>
</tr>
<tr>
<td></td>
<td>1 Phones</td>
<td>Primary Phone: Desk Phone</td>
</tr>
<tr>
<td></td>
<td>Include MiCollab Client Standard</td>
<td>Feature Profile: UCC (Vx.0) Standard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Desk phone extension: Primary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Soft phone extension: Other</td>
</tr>
<tr>
<td></td>
<td>1 NuPoint Mailbox</td>
<td>NuPoint mailbox license with call director and Standard and Advanced UM licensing</td>
</tr>
<tr>
<td></td>
<td>1 Teleworker</td>
<td>Teleworker Service available for one phone</td>
</tr>
<tr>
<td></td>
<td>Include Audio, Web and Video Conferencing</td>
<td>Access for primary phone</td>
</tr>
</tbody>
</table>
In Table 11 identify the various combinations of applications that users will require and enter the number of users for each service mix. It’s recommended that you use service mixes that closely resemble the UCC User default templates and licensing bundles.

### Table 11: Identify MiCollab Application Service Mixes

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>APPLICATION SERVICE MIXES</th>
<th>NUMBER OF USERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry</td>
<td>NuPoint UM and MiCollab Client</td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>NuPoint UM, MiCollab Client, Audio Web and Video, and Teleworker</td>
<td></td>
</tr>
<tr>
<td>Premium</td>
<td>NuPoint UM, MiCollab Client, Audio Web and Video, and three Teleworker</td>
<td></td>
</tr>
</tbody>
</table>
IDENTIFY DIFFERENCES IN THE APPLICATION SERVICE CONFIGURATIONS

For example:

- In NP-UM there can be differences in the FCOS and Unified Messaging settings.
- In MiCollab Client, there can be differences in feature profiles.

Identify any differences in the services configurations of NuPoint UM and MiCollab Client. Within NuPoint configurations there are FCOS and Unified Messaging differences. Within MiCollab Client there can be feature profile differences.

Tip: To simplify configuration, minimize the number of variants.

Table 12: Identify MiCollab Application Service Mixes

<table>
<thead>
<tr>
<th>SERVICE MIX VARIANT</th>
<th>NUPOINT</th>
<th>MICOLLAB CLIENT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FCOS</td>
<td>STD UM</td>
</tr>
<tr>
<td>Entry Variant 1</td>
<td>14</td>
<td>No</td>
</tr>
<tr>
<td>Variant 2</td>
<td>14</td>
<td>Yes</td>
</tr>
<tr>
<td>Variant 3</td>
<td>14</td>
<td>No</td>
</tr>
<tr>
<td>Variant 4</td>
<td>14</td>
<td>Yes</td>
</tr>
<tr>
<td>Variant 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Variant 6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: FCOS 14 is the NuPoint default. If you assign a different FCOS you will need to configure it.
CREATE SINGLE-PHONE TEMPLATES FOR EACH USER TYPE

Create templates for each combination of MiVB network element and service mix by making copies of the default UCC User templates.

For example:

- **P72 Entry**: MiCollab Client deskphone and NP-UM FCOS 14
- **P72 Standard**: MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV
- **P72 Premium**: MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV, 3 Teleworkers, and Vidyo
- **P73 Entry**: MiCollab Client deskphone and NP-UM FCOS 14
- **P73 Standard**: MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV
- **P73 Premium**: MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV, and 3 Teleworkers

![Figure 38: Example Template](image)
To create a template:
1. Log into the MiCollab server manager
2. Under Applications click Users and Services.
3. Click User Templates.
4. Select a default UCC template (for example: UCC V4.0 Standard) and click Edit.
5. Click Copy.
6. Enter a label for the new template.
7. Enter a description.
8. Enter the template information. Refer to the online help for field descriptions.
9. Click Save.
10. Record the templates in the following table.

Table 13: List MiCollab Application Templates

<table>
<thead>
<tr>
<th>TEMPLATE</th>
<th>HOME ELEMENT</th>
<th>PHONE SERVICE</th>
<th>APPLICATION SERVICE MIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>P72 Entry</td>
<td>P72</td>
<td>1</td>
<td>MiCollab Client deskphone and NP-UM FCOS 14</td>
</tr>
<tr>
<td>P72 Standard</td>
<td>P72</td>
<td>1</td>
<td>MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV</td>
</tr>
<tr>
<td>P72 Premium</td>
<td>P72</td>
<td>1</td>
<td>MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV, and 3 Teleworkers</td>
</tr>
<tr>
<td>P73 Entry</td>
<td>P73</td>
<td>1</td>
<td>MiCollab Client deskphone and NP-UM FCOS 14</td>
</tr>
<tr>
<td>P73 Standard</td>
<td>P73</td>
<td>1</td>
<td>MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV</td>
</tr>
<tr>
<td>P73 Premium</td>
<td>P73</td>
<td>1</td>
<td>MiCollab Client deskphone, NP-UM FCOS 14, Advanced UM, AWV, and 3 Teleworkers</td>
</tr>
</tbody>
</table>

CREATE CSV FILE AND IMPORT USING BUP

1. Log into the System Administration Tool on each MiVoice Business network element and export the Users and Services Configuration form data.
2. In the MiCollab server manager, under Applications click Users and Services.
3. Click the Bulk User Provisioning tab.
4. Click **Tools**, click **Download Example CSV File**, scroll down to the bottom of the screen, and then click **Open**. The file (BUPExample.csv) opens in Excel. The BUPExample.csv file is shown below:

![BUPExample.csv File](image)

**Figure 39: BUPExample.csv File**

5. Copy the user data from the exported USC files into the import file spreadsheet columns, starting at row 2. Table 14 shows how the BUP file headings map to the USC form headings.

**Notes:**
- Do not modify or overwrite the first row of header data in the spreadsheet. If you modify the first row of data, the import will fail.
- The maximum import file size is 5000 entries.
- Do not import AWV or NP-UM ports (that is, do not include AWV or NP-UM ports in the BUP Import spreadsheet).
- The sync and reconcile operation that runs at the end of the start sharing process assigns the users’ phone services (for example: Device Type) from the MiVoice Business database to the MiCollab user entries.
- Ensure that an appropriate role is assigned to each user.
- Enter Roles carefully -- Roles are case sensitive.
- Only include a SIP Password if the user’s primary phone is a SIP device.
- Add each network element users in a separate BUP Import Spreadsheet file.
- In MiVoice Business, Login IDs are case sensitive (so, smithF and smithf are two unique Login IDs). However in MiCollab, Login IDs are not case sensitive (so, smithF and smithf are the same Login ID). To avoid conflicts during the synchronization, ensure that all Login IDs consist of a unique set of characters.
- Ensure that you do not assign a SIP Password to MiNET phones. If you enter a SIP Password in the CSV file and the Prime DN is not a SIP phone the Bulk User Provisioning (BUP) tool returns an error. You cannot correct this error in the BUP tool because the SIP Password field is not displayed. You must correct the error in the CSV file and import it again.
Flow Through Provisioning: Adding Greenfield MiCollab to Brownfield MiVB Servers

6. Click the Office Button, click **Save As**, click **Other Formats** and then save the file type as CSV (comma delimited) (*.csv).

7. If you are prompted to "keep the workbook in this format", click **Yes**. Close the file.

8. Click **Tools** and then click **Import from File**. The Import from File window opens.

9. Select **Import Bulk Add CSV File**.

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

11. Select the file and click **Open**.

**Note:** Ensure that you disable Skype plug-ins before you import records using the Bulk User Provisioning tool. Skype plug-ins can cause the BUP import process to be very slow or in extreme cases stop functioning.

12. Click **Import**. The data from the CSV file is imported.

13. Correct any errors that are displayed in the BUP file. Invalid entries are indicated with error icons:

---

**Table 14: USC File Headings Mapped to Bulk User Provisioning (BUP) File Headings**

<table>
<thead>
<tr>
<th>BUP FILE COLUMN HEADING</th>
<th>USC FILE COLUMN HEADING</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>First Name</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last Name</td>
</tr>
<tr>
<td>Login ID</td>
<td>First Name</td>
</tr>
<tr>
<td>Email Address</td>
<td>Email</td>
</tr>
<tr>
<td>Role</td>
<td>Not applicable - you need to create roles on MiCollab and specify one of the roles in the BUP file.</td>
</tr>
<tr>
<td>Prime Phone</td>
<td>Number</td>
</tr>
<tr>
<td>Secondary Phone</td>
<td>Number (of user's second phone)</td>
</tr>
<tr>
<td>External Number</td>
<td></td>
</tr>
<tr>
<td>DID Number</td>
<td>DID Service Number</td>
</tr>
<tr>
<td>SIP Password</td>
<td>SIP Password</td>
</tr>
</tbody>
</table>

---

**Figure 40: BUP Import Spreadsheet**

- Click the Office Button, click **Save As**, click **Other Formats** and then save the file type as CSV (comma delimited) (*.csv).
- If you are prompted to "keep the workbook in this format", click **Yes**. Close the file.
- Click **Tools** and then click **Import from File**. The Import from File window opens.
- Select **Import Bulk Add CSV File**.
- Click **Browse** and navigate to the CSV file.
- Select the file and click **Open**.
- **Note:** Ensure that you disable Skype plug-ins before you import records using the Bulk User Provisioning tool. Skype plug-ins can cause the BUP import process to be very slow or in extreme cases stop functioning.
- Click **Import**. The data from the CSV file is imported.
- Correct any errors that are displayed in the BUP file. Invalid entries are indicated with error icons:
indicates a field entry error. To display the error, hover your cursor over the icon. The error message provides the corrective action. Typical errors include "Role does not exist".

indicates a data import failure. To display the error, click the icon for details. The error report provides the corrective action. If multiple errors exist against the update, click Next.

Click the icon next to an entry to review a detailed summary of any errors. You must resolve the errors before you can save an entry to the directory.

### Users and Services

The Users and Services directory allows you to maintain user data and assign or remove user services. The directory lists the usernames and office numbers of users installed on the server as application blade and are licensed.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Bulk User Add</th>
<th>OP</th>
<th>First Name</th>
<th>Last Name</th>
<th>Login ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>David</td>
<td>Babineau</td>
<td>babinet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>Ed</td>
<td>Bignone</td>
<td>bignone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>Norman</td>
<td>Clarke</td>
<td>clarken</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>Rocky</td>
<td>Dickerson</td>
<td>dickerson</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>Wayne</td>
<td>Fry</td>
<td>fry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>James</td>
<td>Lerche</td>
<td>lerche</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>David-A</td>
<td>Smith</td>
<td>smithd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A</td>
<td>Daum</td>
<td>Smith</td>
<td>smithd</td>
</tr>
</tbody>
</table>

Figure 41: Detailed Error Summary

14. Click the box in the table header to Select All entries.

15. Click Save.

16. Click the Users tab and check to ensure that all the entries are listed correctly.

### START SHARING WITH THE MICOLLAB SERVER

### ADD MICOLLAB AS NETWORK ELEMENT

1. Log into the System Administration Tool of any one of the MiVoice Businesses.

2. Access the Network Elements form.

3. Click Add.
4. Enter the MiCollab system name. If the MiCollab system name is longer than eight characters in length, enter only the first eight characters of the name.
5. Set the Type to MSL Server (MiCollab).
6. Enter the FQDN or IP address of the MiCollab server.
7. Click **Save**.

**START SHARING**

1. In the MiCollab server manager, under **Configuration**, ensure that the **Networks** page is configured to allow MiCollab and the MiVoice Business network elements to connect.
2. Log into the System Administration Tool of one of the MiVoice Business systems.
3. In the SDS Form Sharing form, ensure that data is being shared at scopes that are supported for Flow Through Provisioning (see Appendix D on page 209).
4. Access the **Network Elements** form.
5. In the MiVoice Business **Network Elements** form, check the box of the MiCollab server network element.
6. Click **Start Sharing**.

**Note:** MiCollab templates are associated with the network element from which you started sharing.

**Note:** If the synchronization from MiVoice Business to MiCollab fails, check the error logs on MiCollab in `sdscrcurrent` directory. If synchronization failed for "Hosted User Service", run the GDM CHECK USERANDSERVICE and GDM REPAIR USERANDSERVICE maintenance commands from the MiVoice Business System Administration Tool.

7. Click **OK**.
8. If a reconcile is required, you will receive the message shown in Figure 42. The MiVoice Business system will also have error logs indicating this status.
After the start sharing operation is complete, reload (refresh) the MiCollab server manager screen. The Data Sharing field for the MiCollab server (MSL Server) will change to YES and the SDS Distribution Errors and Reconcile Wizard pages are added to the left-hand menu.

If you receive the message show in Figure 44, the sync is still in progress and you need to wait for it to complete before you can run the Reconcile Wizard. Exit the wizard and try again later.
1. In the server manager, under **Configuration**, click **Reconcile Wizard**. Ensure that you are the only administrator using the wizard. Only one administrator should access the Reconcile Wizard at a time.

---

**CAUTION:** While a reconcile operation is in progress, changes to users and services should not be made from any of the administration tools (for example, MiCollab USP, MiVoice Business system administration tool, and so forth).
2. Make backups of the MiCollab and MiVoice Business system databases before running this wizard. Click the links to access the system backup functions.

3. Check the **Backups Recommended** box. You must check this box to enable the **Next** button.

4. Click **Next** to step through the wizard pages. Refer to the online help for information on the pages.

   **Note:** If you navigate away from the reconcile wizard or click Abort prior to the execution phase, then the analysis must be repeated when you open the wizard again. You must complete the Reconcile Wizard in order for the USP database on the MiCollab to start sharing and become synchronized with the MiVoice Business databases.

5. Review the Analysis Summary carefully. Optionally, click **Save Report** and save a copy of the Analysis Summary to your PC.

6. If there are "Operations for Review" listed, review them to ensure that these operations will have the desired result.

7. If there are "Unresolvable Operations" listed, you can choose to manually reconcile the unresolved operations and click **Rerun Analysis**. On subsequent runs of the analysis, unresolved operations that you manually corrected are not listed.

8. The wizard performs the "Automatic Operations" automatically after you start the reconcile.

9. Click **Reconcile** and then click **Ok**. The wizard generates a Reconcile Summary of the failed, unresolved, and successful operations.

10. Review the Reconcile Summary. Optionally, click **Save Report** and save a copy of the Reconcile Summary to your PC.
11. If there are failed operations listed, you can choose to manually reconcile the failed operations and run the wizard again. On subsequent runs of the analysis, any failed operations that you manually corrected are not listed.

12. Click Finish.

13. Check the Distribution Error application (in Users and Services application) for any distribution errors or pending updates and if any are present, resolve them.
   - Under Administration, click SDS Distribution Errors. The pending updates and errors are listed.
   - Click Reload to refresh the table. If new distribution errors occur while you are viewing the table, the table is not updated automatically. You must click Reload to see the latest view.
   - Refer to the online help for instructions on how to resolve Distribution Errors.

FLOW THROUGH PROVISIONING

The MiCollab and MiVoice Business are now fully synchronized. It is recommended that you provision users and services from the MiCollab Users and Services application only.

Note: The AWV and NP-UM ports from the MiVoice Business database may be listed in the MiCollab USP directory. Do not delete these ports from USP. They should not be assigned any services.

After sharing has started, it is recommended that you:

1. Provide a login ID and password and a set registration and replacement code for any MiVoice Business elements added to MiCollab from MiVoice Business. The former is used to modify hot desk passcodes and the latter is used to register application soft-phones.

2. Review the shared template definitions in MiVoice Business and add MiVoice Business programming for templates added to MiVoice Business from MiCollab. MiVoice Business-specific programming such as feature keys can be added and will be used when MiCollab creates phones using these templates. For example, consider adding multi-call feature to UC endpoint devices or other feature keys.
Appendix C

FLOW THROUGH PROVISIONING:
BROWNFIELD MICOLLAB WITH
BROWNFIELD MIVB SERVERS
OVERVIEW

Flow Through Provisioning uses System Data Synchronization (SDS) to synchronize updates made between the MiCollab and MiVoice Business system databases. The following data is synchronized:

• user and services data
• network elements
• departments and locations, and
• roles and templates.

This procedure describes how to configure a site that has an existing (Brownfield) MiCollab server and existing (Brownfield) MiVoice Business servers with Flow Through Provisioning.

Prior to MiCollab Release 7.0, Single Point Provisioning was supported. If Single Point Provisioning was enabled, user provisioning data that the administrator entered on the MiCollab server (user profile information, phone services, and application services) was automatically provisioned on the MiVoice Business system(s). However, data was updated in one direction only -- from MiCollab to the MiVoice Business servers.

If Single Point Provisioning was not enabled the administrator had to manually program the user provisioning data on both the MiCollab and MiVoice Business systems. Sites that have not be using Single Point Provisioning may experience a greater number of synchronization errors.

After you upgrade to MiCollab Release 7.0 or later system or after you restore a pre-Release 7.0 MiCollab database to a MiCollab Release 7.0 or later system, Single Point of Provisioning is disabled and Flow Through Provisioning is not configured. You must configure Flow Through Provisioning using the procedure described in this appendix.

Note: MiCollab Release 6.0 supports Single Point of Provisioning with MiVoice Business Release 7.2.

CAUTION: Perform this procedure during off business hours.
PREPARE SITE

1. Flow through provisioning is supported for both Integrated and Co-located mode; however you cannot run the MiCollab Client Integration Wizard after Flow through provisioning has been enabled. If you are currently in Co-located mode and want to transition to Integrated mode, do this before you configure Flow Through Provisioning.

2. Ensure that you have recent backups of the MiCollab and MiVoice Business databases.

3. Ensure that the MiVoice Business platforms that you want to support Flow Through Provisioning are sharing data. Ensure that SDS is enabled in MiVB System Options form.

4. Ensure that the MiVoice Business element databases are in sync by performing a Sync from one MiVoice Business element to all the other MiVoice Business elements in the network:
   - Log into the System Administration Tool of one of the MiVoice Business elements in the sharing network.
   - Access the Network Elements form.
   - Check the boxes of all the other network elements in the sharing network.

   ![Network Elements Table]

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>PRX Number/Cluster Element ID</th>
<th>FQDN or IP Address</th>
<th>Data Sharing</th>
<th>Version</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local_173</td>
<td>3300 ICP</td>
<td>173</td>
<td>10.39.37.173</td>
<td>---</td>
<td>14.0.0.71</td>
<td>1</td>
</tr>
<tr>
<td>Local_177</td>
<td>3300 ICP</td>
<td>177</td>
<td>10.39.37.177</td>
<td>YES</td>
<td>14.0.0.71</td>
<td>1</td>
</tr>
<tr>
<td>Local_181</td>
<td>3300 ICP</td>
<td>181</td>
<td>10.39.37.181</td>
<td>YES</td>
<td>14.0.0.71</td>
<td>1</td>
</tr>
<tr>
<td>Local_185</td>
<td>3300 ICP</td>
<td>185</td>
<td>10.39.37.185</td>
<td>YES</td>
<td>14.0.0.71</td>
<td>1</td>
</tr>
</tbody>
</table>

   Figure 46: Check the Boxes of the Other Network Elements

   - Click Sync.
   - Under Shared Forms to be Synchronized, check the User, Service Hosting and Templates boxes.
   - Under Synchronize Options, select Merge.
Figure 47: Select the Forms to be Synchronized

- Click OK to perform the synchronization.

5. It is recommended that you resolve all outstanding SDS distribution errors on every MiVoice Business platform prior to upgrading them. On every MiVoice Business in the sharing network:
   - Log into the MiVoice Business system administration tool.
   - Choose to view forms alphabetically.
   - In the left forms menu, click SDS Distribution Errors - All.
   - Select Display all and then click Retrieve.

The SDS Distribution Errors form displays any synchronization delays and errors that occur when changes are propagated to other network elements in your sharing network. This form shows the status of pending updates and updates that were not distributed successfully.
to other network elements. SDS Distribution Errors must be resolved to keep your network elements synchronized.

To resolve the pending updates or errors:

- Click **Retry** to retry the update. "Retrying" appears before the Reason field in the record. **Click Data Refresh.** If the update is successful the update record disappears from the list. If the update is unsuccessful, the update error record will be updated with the new time stamp.

- Click **Force Change** to update the remote node with the record from the local node. (This action only applies to conflict errors).

- Click **Login** to launch the system administration tool of the remote system. You can then manually fix the error through the System Administration Tool of the remote element. **Click Data Refresh** to update the main window. After you have corrected the error on the remote element, you may have to delete the error record on the local element. Go back to the SDS Distribution Errors form on the local element, select the error record and click **Delete**.

6. Upgrade the MiVoice Business platform(s) to Release 7.2 or later.

7. Ensure that your UCC V3 licenses have been upgraded to UCC V4 licenses:
   - Log into the server manager
   - Under **Applications**, click **Licensing Information**.

   If not, perform a manual sync with the AMC.
   - Under **ServiceLink**, click **Status**.
   - Click **Sync**.

8. Reach through is enabled from MiCollab USP to the MiVoice Business (MiVB) system administration tool using the MiVoice Business "system" administrator account. Ensure that the MiVoice Business systems have an administrator account configured in the User Authorization Profiles form with Login ID "system" and System Admin authorization set to "True".

9. It is possible to program non-existent phones (for example MiNET devices) in the USP application against voice mail boxes, speed calls, hunt group numbers, and non-prime broadcast groups. This allows you to search for the directory number in the USP directory and find the user assigned with the feature. If you have programmed non-existent phones in the Users and Services application, the Reconcile Wizard will assign them with a "Phantom" device type during the reconcile. MiCollab entries that are assigned with the "Phantom" device type are not shared or synchronized with the MiVoice Business via Flow Through Provisioning.

   **CAUTION:** Do not create users in the MiVoice Business system administration tool while the data is in a partially reconciled state. Otherwise, the users will be duplicated in the User and Services directory.

**RUN GDM CHECK AND GDM REPAIR COMMANDS**

Run the GDM Check and GDM Repair maintenance commands on each MiVoice Business network element **immediately prior to start sharing**.

1. Log into the MiVoice Business system administration tool.
2. Choose to view forms alphabetically.
3. In the left forms menu, click **Maintenance Commands**.
4. Enter the GDM REPAIR USERANDSERVICE command.
5. Enter the GDM CHECK USERANDSERVICE command again to ensure that no data inconsistencies are found.

![Figure 48: GDM CHECK USERANDSERVICE Command Successful Result](image)

**START SHARING WITH THE MICOLLAB SERVER**

1. In the MiCollab server manager, under **Configuration**, ensure that the **Networks** page is configured to allow MiCollab and the MiVoice Business network elements to connect.
2. Log into the System Administration Tool of one of the MiVoice Business systems.
3. In the SDS Form Sharing form, ensure that data is being shared at scopes that are supported for Flow Through Provisioning (see Appendix D on page 209).
4. Access the **Network Elements** form.
5. Click **Add**.
6. Enter the MiCollab system name. If the MiCollab system name is longer than eight characters in length, enter only the first eight characters of the name.
7. Set the Type to MSL Server (MiCollab).
8. Enter the FQDN or IP address of the MiCollab server.
9. Click **Save**.
10. Check the box of the MiCollab server network element.
11. Click **Start Sharing**.

**Note:** The MiCollab templates are associated with the network element from which you started sharing.
12. Click OK.

13. If a reconcile is required, you will receive the message shown in Figure 49. This message indicates that the servers are not in fully synchronized or reconciled. The MiVoice Business system will also have error logs indicating this status.

![Figure 49: Message Indication Reconcile Required](image)

14. After the start sharing operation is complete, reload (refresh) the MiCollab server manager screen. The Data Sharing field for the MiCollab server (MSL Server) will change to YES and the SDS Distribution Errors and Reconcile Wizard pages are added to the left-hand menu.

**Note:** If the synchronization from MiVoice Business to MiCollab fails, check the error logs on MiCollab in `/sdsc/current` directory. If synchronization failed for "Hosted User Service", run the GDM CHECK USERANDSERVICE and GDM REPAIR USERANDSERVICE maintenance commands from the MiVoice Business System Administration Tool.
15. If you receive the message shown in Figure 51, the sync is still in progress and you need to wait for it to complete before you can run the Reconcile Wizard. Click OK, exit the wizard and try again later.

Figure 50: Reconcile Wizard and SDS Distribution Errors Pages

Reconcile Wizard

Figure 51: Sync in Progress
RUN RECONCILE WIZARD

At the end of the start sharing process, the ‘Reconcile Wizard’ runs. This may be automatic as long as the data has been entered completely and accurately; otherwise, you will need to log into MiCollab server manager and manually run the Reconcile Wizard to identify and resolve any data conflicts.

1. In the server manager, under Configuration, click Reconcile Wizard. Ensure that you are the only administrator using the wizard. Only one administrator should access the Reconcile Wizard at a time.

   **CAUTION:** While a reconcile operation is in progress, changes to users and services should not be made from any of the administration tools (for example, MiCollab USP, MiVoice Business system administration tool, and so forth).

2. Make backups of the MiCollab and MiVoice Business system databases before running this wizard. Click the links to access the system backup functions.

3. Check the Backups Recommended box. You must check this box to enable the Next button.

4. Click Next to step through the wizard pages. Refer to the online help for information on the pages.

   **Note:** If you navigate away from the reconcile wizard or click Abort prior to the execution phase, then the analysis must be repeated when you open the wizard again. You must complete the Reconcile Wizard in order for the USP database on the MiCollab to start sharing and become synchronized with the MiVoice Business databases.
5. Review the Analysis Summary carefully. Optionally, click **Save Report** and save a copy of the Analysis Summary to your PC.

6. If there are "Operations for Review" listed, review them to ensure that these operations will have the desired result.

7. If there are "Unresolvable Operations" listed, you can choose to manually reconcile the unresolved operations and click **Rerun Analysis**. On subsequent runs of the analysis, unresolved operations that you manually corrected are not listed.

8. The wizard performs the "Automatic Operations" automatically after you start the reconcile.

9. Click **Reconcile** and then click **Ok**. The wizard generates a Reconcile Summary of the failed, unresolved, and successful operations.

10. Review the Reconcile Summary. Optionally, click **Save Report** and save a copy of the Reconcile Summary to your PC.

11. If there are failed operations listed, you can choose to manually reconcile the failed operations and run the wizard again. On subsequent runs of the analysis, any failed operations that you manually corrected are not listed.

12. Click **Finish**.

13. Check the Distribution Error application (in Users and Services application) for any distribution errors or pending updates and if any are present, you can resolve them.
   - Under **Administration**, click **SDS Distribution Errors**. The pending updates and errors are listed.
   - Click **Reload** to refresh the table. If new distribution errors occur while you are viewing the table, the table is not updated automatically. You must click Reload to see the latest view.
   - Refer to the online help for instructions on how to resolve Distribution Errors.

**FLOW THROUGH PROVISIONING**

The MiCollab and MiVoice Business are now fully synchronized. It is recommended that you provision users and services from the MiCollab Users and Services application only.

**Note:** The AWV and NP-UM ports from the MiVoice Business database may be listed in the MiCollab USP directory. Do not delete these ports from USP. They should not be assigned any services.

**Note:** You cannot provision a login ID in the MiCollab Users and Services application if the same login ID is already provisioned in the MiVoice Business User Authorization form. The system will generate an error.

After sharing has started, it is recommended that you:
1. Provide a login ID and password and a set registration and replacement code for any
MiVoice Business elements added to MiCollab from MiVoice Business. The former is used
to modify hot desk passcodes and the latter is used to register application soft-phones.

2. Review the shared template definitions in MiVoice Business and add MiVoice Business
programming for templates added to MiVoice Business from MiCollab. MiVoice Busi-
ness-specific programming such as feature keys can be added and will be used when
MiCollab creates phones using these templates. For example, consider adding multi-call
feature to UC endpoint devices or other feature keys.
Appendix D

FLOW THROUGH PROVISIONING:

SHARING SCOPES
SUPPORTED SHARING SCOPES

Before you start sharing with MiCollab, access the SDS Form Sharing form on the MiVoice Business and ensure that the SDS forms and data are being shared at supported scopes.

The following table lists the SDS forms and data that require specific sharing scopes in order to support Flow Through Provisioning with MiCollab. Form categories that are not listed are not restricted to any specific setting.

In a multi-administration group SDS cluster, if the highlighted forms below are shared across All Network Elements, then you can reach through into other administration groups from MiCollab. MiCollab must be in the same administration group as the MiVoice Business that started the sharing.

Table 15: Supported SDS Sharing Scopes

<table>
<thead>
<tr>
<th>FORM CATEGORY</th>
<th>SHARE RECORDS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General System</strong></td>
<td></td>
</tr>
<tr>
<td>Call Recognition Service</td>
<td>All 3300 ICP</td>
</tr>
<tr>
<td>Network Element – 3300 Network Element Properties</td>
<td>All 3300 ICP*</td>
</tr>
<tr>
<td>Network Elements</td>
<td>All Network Elements*</td>
</tr>
<tr>
<td>Network Element FQDN</td>
<td>All Network Elements*</td>
</tr>
<tr>
<td><strong>System Level Call Handling</strong></td>
<td></td>
</tr>
<tr>
<td>Ring Groups</td>
<td>Resilient Pair*</td>
</tr>
<tr>
<td>Hunt Groups</td>
<td>Resilient Pair*</td>
</tr>
<tr>
<td>Personal Ring Groups</td>
<td>Resilient Pair*</td>
</tr>
<tr>
<td>Personal Ring Groups - Members</td>
<td>Resilient Pair*</td>
</tr>
<tr>
<td>Multi-device User Groups</td>
<td>Resilient Pair*</td>
</tr>
<tr>
<td>Multi-device User Groups - Members</td>
<td>Resilient Pair*</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td></td>
</tr>
<tr>
<td>User Definition</td>
<td>All Network Elements</td>
</tr>
<tr>
<td><strong>Device Level Resiliency</strong></td>
<td></td>
</tr>
<tr>
<td>Associated Directory Numbers</td>
<td>Any</td>
</tr>
<tr>
<td>Call Routing</td>
<td>Any</td>
</tr>
<tr>
<td>CESID Assignment</td>
<td>Any</td>
</tr>
<tr>
<td>Device Data</td>
<td>Resilient Pair</td>
</tr>
<tr>
<td><strong>Service Hosting</strong></td>
<td></td>
</tr>
<tr>
<td>Local-only Directory Number List</td>
<td>All Cluster Elements</td>
</tr>
<tr>
<td><strong>Service Hosting</strong></td>
<td></td>
</tr>
<tr>
<td>Templates</td>
<td>All Network Elements</td>
</tr>
<tr>
<td>FORM CATEGORY</td>
<td>SHARE RECORDS</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>User Roles</td>
<td>All Network Elements</td>
</tr>
<tr>
<td>User and Service Templates</td>
<td>All Network Elements</td>
</tr>
<tr>
<td>Templates (Pre-7.1)</td>
<td>All Network Elements</td>
</tr>
<tr>
<td>User Simple Templates</td>
<td>All Network Elements</td>
</tr>
<tr>
<td>User and Service Templates -- Template IDs</td>
<td>All Network Elements</td>
</tr>
<tr>
<td>Key Templates</td>
<td>All Network Elements</td>
</tr>
</tbody>
</table>

* Fixed, cannot be edited in SDS Form Sharing Form
Appendix E

OFF-LINE LICENSING AND INSTALLATION
INTRODUCTION

This appendix describes off-line licensing and installation for customers who are unable to connect to the Mitel Applications Management Center (AMC) via the internet due to security concerns. Typically, off-line licensing is available to large customers with MiCollab virtual deployments in server-only mode. Note that the optional blades (NuPoint Unified Messaging and Speech Auto Attendant applications) cannot be installed with off-line licensing and installation.

Off-line licensing is available for a set duration of time. Before your licensing term expires, the system generates warnings indicating that you must re-sync the MiCollab system ARID.

**Note:** If you allow your licensing to expire, then after you re-sync your system ARID, you must reboot the system in order to restart the MiCollab applications.

INSTALLATION OF vMiCollab USING OFF-LINE LICENSING

The following procedure describes how to perform off-line activation of licenses from the server manager using a maintenance PC.

To install vMiCollab using off-line licensing:

1. Obtain an Application Record ID (or service account ID) from your authorized reseller.
2. Download the MiCollab OVA file only (see page 63). The NuPoint Messenger and Speech Auto Attendant applications are not supported for off-line licensing and installation.
3. Deploy the vMiCollab vApp (see page 64). If you are deploying on vSphere vCenter, leave the Application Record ID field in the Custom Template blank.
4. Configure or Review the MSL Operating System Settings (see page 64)
   - If you deployed vMiCollab on vSphere vCenter and used the Custom Template to set the MSL Operating System parameters, review the settings in the server console.
   - If you did not use vSphere vCenter, you must configure the MSL Operating System parameters in the server console. When you are prompted for the Application Record ID, leave it blank.
5. Log into the server manager of the maintenance PC, under **ServiceLink**, click **Status**.
6. Enter your Application Record ID (also called Service account ID).
7. Select **Enable off-line license generation**.
8. Click **Activate** to request an off-line licensing file. The Operation status report page is displayed.
9. Click **Download license request file** (license_request.zip).
10. In the file download dialog, click **Save** and save the zip file to a portable storage medium on the maintenance PC.
11. Remove the portable storage device and go to an Internet-connected PC.
12. On the Internet-connected PC, extract the contents of the zip file to a temporary folder.
13. Open the folder and double-click the sync.bat file to execute handshake and synchronization with the AMC.

14. Synchronization occurs with the AMC and the sync.bat file creates a license.zip file containing license files from the AMC. (If you receive a security warning during this process, click Run.)

15. Save the license.zip file to the portable storage device.

16. Remove the storage device from the Internet-connected PC and return to the maintenance PC.

17. Insert the storage device in the maintenance PC.

18. In the server manager of the maintenance PC, under ServiceLink, click Status. Beside Upload license file, click Choose File.

19. In the file upload dialog, browse to the license.zip file that was created by executing the sync.bat file, then click Ok to select the file to be uploaded.

20. Click Upload license file to install the synchronized license key file and activate the purchased options.

21. Transfer the new zip file back to maintenance PC used to access server manager (if applicable).

22. Click Upload license file to upload the license response back into MiCollab.

**Note:** Save your sync.bat file to a portable storage device or PC, in case you want to add additional licenses offline to the system in the future.

**Note:** You cannot install the NuPoint and SAA applications while the system is off-line. If the system cannot access the AMC, installation of these application blades will fail. You must install these applications while the system is online.

**Note:** A virtual application license which is synced off-line will expire after the licensing term. Prior to expiry there will be a series of alarms raised at incremental severity as the expiry time nears. You must sync the system with license file again to clear the alarm and re-enable the licensing.

23. Select the PBX Type from the MiCollab Server Manager.
   - In the server manager, under ServiceLink, click Install Applications.
   - Click the Install Applications tab.
   - Set the PBX Type and then click Next. The list of licensed applications, services, and security patches for the currently installed version of MiCollab appears.

24. Off-line licensing is complete.

### RESETTING THE LICENSE TERM

You will receive MiCollab alarms near the end of the licensing term that indicates that you must re-sync your system with the licensing file. The following alarms can appear:

- Minor: Mitel Applications Suite (MiCollab) licenses expire in 8 days.
- Major: Mitel Applications Suite (MiCollab) licenses expire in 5 days.
- Critical: Mitel Applications Suite (MiCollab) licenses expire in 2 days.
To reset the license term, log into the server manager.

1. Under **ServiceLink**, click **Status** and then click **Sync**. The alarm will be cleared and your licenses are re-enabled for another term.

2. Perform a system reboot to restart your applications.

**Note:** If you allow your licensing to expire, then after you re-sync your system ARID, you must reboot the system in order to restart the MiCollab applications.

### ADDING LICENSES

Before you can add new licenses, you must generate an off-line license request:

1. Contact the order desk and purchase the new licenses. The new licenses will be assigned against your ARID in the AMC.

2. If you saved your sync.bat file (from initial installation) you can use it to add new licenses to the system. From an internet connected PC, double-click the sync.bat file to execute handshake and synchronization with the AMC.

**Note:** If you cannot find the sync.bat file from initial installation, you must generate a new one. Perform Step 5 to Step 22 of “Installation of vMiCollab Using Off-Line Licensing” on page 214.

3. Synchronization occurs with the AMC and the sync.bat file creates a license.zip file containing license files from the AMC. (If you receive a security warning during this process, click **Run**.)

4. Save the license.zip file a portable storage device.

5. Remove the storage device from the Internet-connected PC and return to the maintenance PC.

6. Insert the storage device in the maintenance PC.

7. Log into the server manager of the maintenance PC.

8. Under **ServiceLink**, click **Status**.

9. Click **Sync** to generate an offline license request. The **Upload license file** and **Download licensing refresh** file buttons are displayed.

10. Beside **Upload license file** click **Browse**.

11. In the file upload dialogue, browse to the license.zip file that was created when you executed the sync.bat file. Click **Save** to select the file to be uploaded.

12. Click **Upload license file** to install the synchronized license key file and activate the purchased licenses.

### UPGRADE

You do not need to re-sync your licenses during an upgrade.
Logs
   viewing and collecting 149
M
Maintenance 99
MiCollab
   overview 3
MiCollab Client
   migrating 52
MiCollab Client Integration Wizard
description 79
MiCollab End User portal 49, 71
MiCollab Server Appliance 36
description 4
MiCollab Virtual Appliance
description 4
MiCW
description 5
new MiCollab with a new MiVB cluster 164
new MiCollab with a single existing MiVB platform 161
new MiCollab with a single new MiVB platform 159
new MiCollab with existing MiVB cluster 170
use cases 159, 180
Mitel
   Application Management Center 19
   application record ID 61
   Knowledge Base articles 9
   Root CA certificate 49, 71
   Standard Linux, installing operating system 41
Mitel Configuration Wizard
description 5
new MiCollab with a new MiVB cluster 164
new MiCollab with a single existing MiVB platform 161
new MiCollab with a single new MiVB platform 159
new MiCollab with existing MiVB cluster 170
use cases 159, 180
MiVoice Border Gateway
troubleshooting 143
MSL
   activation errors 114
   configure software 42
   configure software on vMiCollab 64
download software 39
install software 40, 63, 180
installing operating system 41
Qualified Hardware List 4
qualified hardware list, accessing 36
MSL software, obtaining 39
N
Network elements
   identification 180
O
Online help, troubleshooting 131
OpenSSH 115
Overview, of vMiCollab install 57
OVF 64
P
Packages, software 3
Password, administrator 43
PBX interoperability 5
PC server 36
Platform, setting up 36
PuTTY 116
Q
Qualified hardware list, accessing 36
R
Restore
disaster recovery 151
Root CA certificate 49, 71
Secure shell 41, 115
Secure Sockets Layer 49, 71
Server
   console, accessing 114
   set up 36
Server Appliance 36
Server manager, accessing 49, 70
Server platforms 3
Server, industry standard 4
ServiceLink 47, 69
Site information, collecting 34
Software
   application installation 47
download, 39
Install Applications, 47
Install optional vMiCollab applications 70
labeling CD/DVDs 40, 41
licensed packages 3
obtaining 39
upgrade 99
upgrading MiCollab software 99
vMiCollab application installation 70
SSH 41, 115
Telnet 115
Troubleshooting
   Licensing 131
   licensing errors 146
   MiVoice Border Gateway 143
   online help 131
Upgrade
   application suite licenses 29
   MiCollab software 99
V
   vApp
deployment 64
   vMiCollab
deployment configurations 56
   installation requirements and constraints 57
   supported applications 57
   vApp deployment 64
Web certificates, installation 49, 71
Work flow
   for existing site 14
   for new site 13