Installation and Maintenance Guide

RELEASE 7.0
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

Mitel is a registered trademark of Mitel Networks Corporation.
Windows and Microsoft are trademarks of Microsoft Corporation.
Dell is a trademark of Dell Inc.
PowerEdge is a trademark of Dell Inc.
VMware, vMotion, vCenter, vCloud, vSphere, ESX, and ESXi are trademarks of VMware Incorporated.
Google and the Google logo are registered trademarks of Google Inc.
Chrome is a trademark of Google Inc.
Skype is a trademark of Skype or related entities
Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.
CHAPTER 1: INTRODUCTION

About MiCollab ................................................................. 3
Deployment Configurations ............................................... 3
Supported Communications Platforms ............................... 3
Platforms ............................................................................. 3
Software Releases ............................................................. 3
MiCollab Platforms ............................................................. 4
Industry Standard Server .................................................... 4
MiCollab Server Appliance .................................................. 4
MiCollab Virtual Appliance (vMiCollab) ............................. 5
Supported Applications ....................................................... 5
MiVoice Business Communication Platforms ...................... 5
MiVoice 5000, MiVoice MX-One, and MiVoice Office 250 Platforms .......................................................... 6
Client Station Support ......................................................... 6
About the Mitel Integrated Configuration Wizard ................... 6
Overview .............................................................................. 6
Supported Use Cases .......................................................... 7
Unsupported Use Cases ......................................................... 7
Requirements ....................................................................... 8
A Note About Hunt Groups .................................................. 8
About the Documentation Set .............................................. 8
MiCollab .............................................................................. 8
MiCollab NuPoint Unified Messaging ................................... 9
Speech Auto Attendant ......................................................... 9
Mitel Standard Linux .......................................................... 9
MiVoice Border Gateway (Teleworker) ................................. 9
MiCollab Client ................................................................. 9
Mitel MiVoice Business Communications Platform ............... 10
Mitel MiVoice Office 250 Communications Platform ............. 10
Access MiCollab Product Documentation ............................ 10
Access Product Bulletins ..................................................... 10

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 ......................... 15
  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 .................................. 19
    Accessing your AMC Account ..................................... 20
  Software Assurance ..................................................... 20
  vMiCollab Licensing Detection and Violation Mode .......... 21

UCC Licensing ............................................................. 21
  UCC Licensing Rules .................................................. 22
  UCC Licensing Tiers ................................................... 24
  MiCollab PC Client Capabilities by UCC Bundle ............. 26
  UCC Licensing for MiCollab AWV ................................. 26
  UCC Licensing Part Numbers ....................................... 27
  UCC Licensing Procedure ............................................ 29
    Overview .............................................................. 29
    Deploying UCC Licenses ........................................... 29
  Effect OF UPGRADING ON UCC Licensing .................... 36
  Trusted Service Support .............................................. 36

License Packages .......................................................... 37
  MiCollab Base Packages ............................................. 38
  MiCollab and vMiCollab Base Add-on to MiCollab Client .... 38
  Uplift Packages ........................................................ 38
# Table of Contents

NuPoint Unified Messaging .......................................................... 38  
MBG-Teleworker ............................................................................. 40  
MBG-Secure Recording Connector .................................................... 40  
Mitel Collaboration Advanced .......................................................... 41  
  MiCollab AWV Uplift Licensing Details ............................................. 41  
  For MiVoice Business Systems ......................................................... 41  
  For MiVoice Office 250 .................................................................. 42  
  For MiVoice Office 250 Digital .......................................................... 42  
  Introduce MiCollab AWV Web-only for all PBX Integrations .............. 42  
  MiCollab AWV Enhanced Video License .......................................... 42  
MiCollab Client ............................................................................... 43  

Adding "à la carte" Licenses ............................................................. 43  

## CHAPTER 4: INSTALL MICOLLAB SERVER

Overview ......................................................................................... 47  
Collect Site Information ................................................................. 48  
Set Up PlatForm .............................................................................. 49  
  MiCollab on Industry Standard Server ........................................... 49  
  MiCollab Server Appliance ............................................................. 49  
  MiCollab on Microsoft Hyper-V Virtual Machine ............................. 51  
Create Application Record ............................................................. 51  
Obtain MSL and Application Software ............................................ 52  
  Download Software ISO Files from Mitel OnLine ......................... 52  
  Software Downloads for MiVoice Business .................................. 53  
  Software Downloads with MiVoice MX-ONE ................................ 53  
  Software Downloads with MiVoice 5000 ....................................... 53  
Create Storage Media ...................................................................... 53  
  Option 1: Burn MSL ISO to CD/DVD and Copy Application ISO Images to USB Device ........................................... 54  
  Option 2: Burn Downloaded ISO Images to CD/DVDs .................... 54  
Install MSL Operating System Software ......................................... 55  
Configure the MSL Operating System ............................................. 56  
  Accept End User License ............................................................. 56  
  Set Administrator Password ......................................................... 56  
  Select System Timezone ............................................................... 57  
  Configure Domain Name .............................................................. 57  
  Configure System Name ............................................................... 57  
  Enter Local Network Adapter ....................................................... 57
Enter Local Networking Parameters ............................................. 57
Enable IPv6 Protocol and Address .............................................. 58
Select WAN Adapters ............................................................... 59
Select Gateway IP Address ....................................................... 59
Configure External Interface ..................................................... 59
Configure DNS ........................................................................... 60
Activate Changes ....................................................................... 60
Enter Application Record ID ..................................................... 60
Install Application Software ...................................................... 61
Install Applications Software From Server Manager .................... 61
Installing Application Software from CD/DVDs or USB device .... 62
Configure MiCollab ................................................................. 63
Log in to the Administrator Portal (Server Manager) ..................... 64
Install Web Certificates .............................................................. 64
Allow “Trusted Network” Access ............................................... 65
Set System Language ................................................................ 66
Configure Port 5058 (for NON-MiVoice Business only) ............... 67
Perform Initial Configuration of Applications .......................... 67
Install MiCollab Server in LAN Mode with MiVoice Border Gateway Server(s) .............. 67
Prerequisites and Conditions ...................................................... 68

CHAPTER 5: INSTALLING VIRTUAL MICOLLAB IN A VMWARE ENVIRONMENT

Introduction ............................................................................. 72
About MiCollab Virtual Appliance .............................................. 72
Deployment Configurations ....................................................... 72
Supported Applications ............................................................. 73
Installation Checklist ............................................................... 73

MiCollab Virtual Appliance Installation .................................. 73
Review Installation Details ....................................................... 73
Requirements ........................................................................... 73
Constraints ................................................................................. 74
Collect Site Information ........................................................... 74
Collect Custom Template Information ....................................... 76
Create MiCollab Application Record ...................................... 79
Download MiCollab OVA file and Application Software .......... 79
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Downloads for MiVoice Business</td>
<td>79</td>
</tr>
<tr>
<td>Software Downloads with MiVoice MX-ONE</td>
<td>79</td>
</tr>
<tr>
<td>Software Downloads with MiVoice 5000</td>
<td>79</td>
</tr>
<tr>
<td>Deploy vMiCollab vApp</td>
<td>80</td>
</tr>
<tr>
<td>Configure the MSL Operating System</td>
<td>80</td>
</tr>
<tr>
<td>Launch the MSL Server Console</td>
<td>80</td>
</tr>
<tr>
<td>Set Administrator Password</td>
<td>81</td>
</tr>
<tr>
<td>Select System Timezone</td>
<td>82</td>
</tr>
<tr>
<td>Configure Domain Name</td>
<td>82</td>
</tr>
<tr>
<td>Configure System Name</td>
<td>82</td>
</tr>
<tr>
<td>Enter Local Network Adapter</td>
<td>82</td>
</tr>
<tr>
<td>Enter Local Networking Parameters</td>
<td>83</td>
</tr>
<tr>
<td>Enable IPv6 Protocol and Address</td>
<td>83</td>
</tr>
<tr>
<td>Select WAN Adapters</td>
<td>84</td>
</tr>
<tr>
<td>Select Gateway IP Address</td>
<td>84</td>
</tr>
<tr>
<td>Configure External Interface</td>
<td>85</td>
</tr>
<tr>
<td>Configure DNS</td>
<td>85</td>
</tr>
<tr>
<td>Activate Changes</td>
<td>85</td>
</tr>
<tr>
<td>Enter Application Record ID and Reboot</td>
<td>85</td>
</tr>
<tr>
<td>Install Optional Application Software</td>
<td>86</td>
</tr>
<tr>
<td>Install Applications Software From Server Manager</td>
<td>86</td>
</tr>
<tr>
<td>Installing Application Software from CD/DVDs or USB device</td>
<td>86</td>
</tr>
<tr>
<td>Configure vMiCollab</td>
<td>88</td>
</tr>
<tr>
<td>Log in to the Administrator Portal (Server Manager)</td>
<td>89</td>
</tr>
<tr>
<td>Install Web Certificate</td>
<td>89</td>
</tr>
<tr>
<td>Allow &quot;Trusted Network&quot; Access</td>
<td>90</td>
</tr>
<tr>
<td>Set System Language</td>
<td>91</td>
</tr>
<tr>
<td>Configure Port 5058 (for MiVoice Office 250 only)</td>
<td>92</td>
</tr>
<tr>
<td>Synchronize MiCollab Client server with MiCollab AWV Software Versions</td>
<td>92</td>
</tr>
<tr>
<td>Perform Initial Configuration of Applications</td>
<td>92</td>
</tr>
</tbody>
</table>

**CHAPTER 6: INITIAL CONFIGURATION**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>95</td>
</tr>
<tr>
<td>Collect Site Configuration Information</td>
<td>95</td>
</tr>
<tr>
<td>Configure MiCollab Client Mode</td>
<td>97</td>
</tr>
</tbody>
</table>
CO-LOCATED MODE OR INTEGRATED MODE? .................................................. 98
Configuring Integrated Mode ......................................................................... 99
  For MiCollab Server Deployments: ............................................................. 99
  For vMiCollab Deployments: ..................................................................... 99
Synchronize MiCollab Client server with MiCollab AWV Software Versions .......... 99
Configure Platform and Application Resources ................................................. 99
Configure Users and Services ....................................................................... 100
  MiVoice Business Platform ....................................................................... 100
  MiVoice Office 250 .................................................................................. 100
  MiVoice 5000 or MiVoice MX-ONE ............................................................ 100
Configure Flow Through Provisioning ............................................................. 101
System Requirements .................................................................................. 101
Conditions .................................................................................................... 102
  Topology ................................................................................................... 103
  Departments and Locations ....................................................................... 104
  Roles and Templates .................................................................................. 104
  Users and Services .................................................................................... 105
  Fully Qualified Domain Name (FQDN) for Cloud Deployments ................. 105
Configuration Overview .............................................................................. 106
Greenfield: New MiCollab with one New MiVB Server .................................. 107
  Using MiCW ............................................................................................. 107
  Manual Configuration ................................................................................ 108
Greenfield: New MiCollab Server with Multiple New MiVB Servers .............. 109
  Using MiCW ............................................................................................. 110
  Manual Configuration ................................................................................ 110
Verify that Sharing has Started on MiCollab ................................................... 111
Check MiCollab Server Flow Through Provisioning Logs .............................. 112
Configure Integrated Directory Services ......................................................... 112
Configure Application Settings .................................................................... 113
Backup Database .......................................................................................... 113

CHAPTER 7: MAINTENANCE

Upgrading MiCollab Software ........................................................................ 117
Upgrade from MAS 5.0 or later to MiCollab 7.0 using Fresh Install ................. 118
  Prerequisites .............................................................................................. 118
  Backup and Restore with Fresh Install ....................................................... 119
# Table of Contents

Upgrade from vMAS 5.0 or later to vMiCollab 7.0 .................................................. 122
  Upgrade Prerequisites ......................................................................................... 122
  Deploy vMiCollab 7.0 OVA File and Restore Backup ....................................... 122
Upgrade from MiCollab 7.x to MiCollab 7.y ......................................................... 126
Upgrade from MiCollab 7.0 to MiCollab 7.0 SPx .................................................. 127
Upgrade vMiCollab Configuration ......................................................................... 127
Installing Additional (Missing) Applications ......................................................... 128
  Add Application from Server Manager ............................................................. 128
  Add Application from Server Console ............................................................. 128
Removing an Application during Initial Installation ............................................. 130
Performing Backups ............................................................................................... 130
  Server Manager "Backup" .................................................................................. 130
  Backup to Desktop .............................................................................................. 130
  Schedule Backups to Network File Server ....................................................... 131
  Server Manager SFTP Backup to Linux Servers .................................................. 133
    Allow Access on the Backup Server ............................................................... 133
    Configure an SFTP backup ............................................................................ 133
  Server Console "Perform Backup" ...................................................................... 134
  Backing up to USB Device ............................................................................... 134
  Backing up to Network File Server ................................................................... 134
  Verify Backup Data ........................................................................................... 135
Shutting Down MiCollab ......................................................................................... 135
Correcting Activation Errors .................................................................................. 135
Accessing the Server Console ............................................................................. 136
  About SSH (Secure Shell) ................................................................................. 136
  Obtaining an SSH Client ................................................................................... 137
Configuring Remote Management via MBG ......................................................... 137
Viewing Log Files ................................................................................................. 139
Viewing Alarms ................................................................................................... 139
Conversions and Migrations ............................................................................... 139
  Convert a MiCollab Server Database to vMiCollab ......................................... 140
    Conditions and Constraints ......................................................................... 140
    Before You Begin ......................................................................................... 140
Perform the Conversion .............................................................. 141
Migrate Standalone MiCollab Client to MiCollab Server or vMiCollab ......................... 142
  Conditions and Constraints ....................................................... 142
  Before You Begin ................................................................... 143
  Perform the Migration ............................................................... 143
Upgrading Users with UCC V1 Licenses to UCC V4.0 or Later Licenses ...................... 144
  UBAT Script Usage ................................................................. 144
  Overview of Procedure ............................................................ 144
  Export and Analyze a CSV File of Current Licensing ............................................. 145
  Review and Modify CSV File ....................................................... 145
  Import CSV File ................................................................... 145

CHAPTER 8: TROUBLESHOOTING

  General Troubleshooting .......................................................... 149
  Online Help Troubleshooting ..................................................... 152
  Flow Through Provisioning Troubleshooting ......................................................... 153
  vMiCollab Troubleshooting ......................................................... 154
  Troubleshooting Applications ....................................................... 156
    MiCollab AWV ................................................................... 156
      Conferencing Error Messages for Alarm/Alert Conditions ................................. 162
    MiVoice Border Gateway .......................................................... 163
    NP-UM Troubleshooting ........................................................... 165
    Google Apps Troubleshooting ....................................................... 166
  Troubleshooting Licensing Errors .................................................................. 166
  Troubleshooting UCC Licensing Upgrades ......................................................... 168
  Viewing/Collecting Log Files ................................................................ 169
  Database Recovery (Restore) .................................................................. 169
  Conditions and Constraints .................................................................. 169
  Restoring a Database Backup .................................................................. 171
    Access the Console Restore Menu ....................................................... 171
    Restore From Another Running Server ....................................................... 171
    Restore From Network Share ................................................................... 172
    Restore from Removable Device .................................................................. 172
    Check Application Data ................................................................... 173
  vMiCollab System Disaster Recovery .................................................................. 173
  Restoring a MiCollab Server Database to a Different Server ................................. 173
# APPENDIX A: FLOW THROUGH PROVISIONING: ADDING GREENFIELD MI-COLLAB TO GREENFIELD MI-VB SERVERS

Overview ......................................................................................................................... 177

MiCW Use Cases ............................................................................................................. 177
Greenfield MiCollab with a Single Greenfield MiVB Platform ........................................ 177
  Run Wizard .................................................................................................................. 177
Greenfield MiCollab with a Single Existing MiVB Platform ............................................. 179
  Run Wizard .................................................................................................................. 180
Adding Greenfield MiCollab To a New MiVB Cluster ...................................................... 182
  Initial Run of Wizard .................................................................................................... 182
  Run Wizard FOR Each Additional MiVB Cluster Element .......................................... 184
  Last Run of Wizard Configures MiCollab ................................................................... 185
Greenfield MiCollab with Existing MiVB Cluster ............................................................ 188
  Before You Run the Wizard ......................................................................................... 188
  Run the Wizard ........................................................................................................... 188
  After Sharing is Started ............................................................................................. 190

# APPENDIX B: FLOW THROUGH PROVISIONING: ADDING GREENFIELD MI-COLLAB TO BROWNFIELD MI-VB SERVERS

Overview ......................................................................................................................... 193

Prepare Site ...................................................................................................................... 193
  Run GDM Check and GDM Repair Commands ............................................................ 194
  Add Softphone Users ................................................................................................. 195
Obtain Licenses .................................................................................................................. 195
Install MiCollab and Application Software ...................................................................... 195
Provision the Network Elements ..................................................................................... 196
Provision Application Resources ..................................................................................... 197
Create Templates (and Roles) ........................................................................................ 197
  Identify Users, Prime Numbers and Primary MiVoice Business .................................. 198
  Identify the MiCollab Applications Service Mixes ...................................................... 199
  Identify Differences in the Application Service Configurations ................................ 201
  Create Single-phone Templates for each User Type ................................................... 202
Create CSV File and Import Using BUP ....................................................................... 203
Start Sharing with the MiCollab Server ......................................................................... 206
APPENDIX C: FLOW THROUGH PROVISIONING: BROWNFIELD MiCollab WITH BROWNFIELD MIVB SERVERS

Overview ................................................................. 215
Prepare Site ............................................................ 215
Run GDM Check and GDM Repair Commands ......................... 217
Start sharing with the MiCollab server ................................ 218
Run Reconcile Wizard .................................................. 220
Flow Through Provisioning ............................................. 222

APPENDIX D: FLOW THROUGH PROVISIONING: SHARING SCOPES

Supported Sharing Scopes ............................................. 225
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 “License Packages” on page 37 for a listing of the package contents.

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
• MiVoice 5000
• MiVoice MX-ONE

SOFTWARE RELEASES

MiCollab 7.0 software supports

• MiVoice Business Releases:
  - MCD 5.0 with latest SP
  - MiVoice Business 6.0 with latest SP
  - MiVoice Business 7.0 with latest SP
- MiVoice Business 7.1 with latest SP
- MiVoice Business 7.2 (required for Flow Through Provisioning)

• MiVoice Office 250 Releases
  - 5000 CP 5.0
  - MiVoice Office 250 Release 5.1
  - MiVoice Office 250 Release 6.1 with latest SP (recommended)

• MiVoice 5000 Release 6.1 SP2 and MiVoice 5000 Manager version 3.1 SP2 and higher

• MiVoice MX-ONE Release 6.0 SP2

**Note:** For communications platform compatibility with MiCollab and Mitel Integrated Configuration (MiCW) versions, see the *Requirements* section of “About the Mitel Integrated Configuration Wizard” on page 6.

**MICOLLAB PLATFORMS**

MiCollab is available on the following platforms:

- Industry Standard Server
- MiCollab Server Appliance turnkey platform
- MiCollab Virtual Appliance running in a virtualized 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 R210 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.
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 sites to up to 250 users,
  • mid-range business multi-application or single application sites up to 1500 users
  • enterprise multi-application sites up to 5000 users.
  • enterprise single-application sites (MiCollab Client or AWV) up to 5000 users.

MiCollab Virtual Appliance deployments on Hyper-V are supported for
  • small business multi-application sites to up to 250 users,
  • mid-range business multi-application or single application sites up to 1500 users.

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

SUPPORTED APPLICATIONS

The applications supported by a MiCollab installation are dependent on the following criteria:
  • Communications platform
  • Deployment configuration, and
  • MiCollab platform

MIVOICE BUSINESS COMMUNICATION PLATFORMS

For the supported MiVoice Business communications platforms, the following MiCollab applications are supported:
  • NuPoint Unified Messaging
  • Speech Auto Attendant
  • MiCollab Client in either integrated or co-located mode; see page 97 for a description of these modes.
  • MiCollab Audio, Web, and Video (AWV) Conferencing.
  • MiVoice Border Gateway (Teleworker, SIP Trunking, and Secure Recording Connector Services) with Web Proxy
  • MiVoice for Skype™ for Business
• Vidyo

**Note:** The Speech Navigation option is only supported if NuPoint Unified Messaging is the only installed application. This restriction applies to both the MiCollab server and virtual MiCollab. Although all applications are installed in the vMiCollab OVA, if you only apply NuPoint licenses (à la carte) then it is considered a single application installation.

MIVOICE 5000, MIVOICE MX-ONE, AND MIVOICE OFFICE 250 PLATFORMS

The following MiCollab applications are supported:

• NuPoint Unified Messaging
• Speech Auto Attendant (MiVoice Office 250 only)
• MiCollab Client
• MiCollab Audio, Web and Video (AWV) Conferencing
• MiVoice Border Gateway (Teleworker Service only) with Web Proxy
• MiVoice for Skype for Business
• Vidyo

**Note:** The MiVoice Border Gateway SIP Trunking and Secure Recording Connector services are not supported on the MiVoice Office 250 platform.

**Note:** The Speech Auto Attendant application is not supported on the MiVoice 5000 and MiVoice MX-ONE.

CLIENT STATION SUPPORT

MiCollab clients (for example, MiCollab End User portal, MiCollab System Administrator portal, MiCollab AWV clients, and so forth) are supported on various operating systems. Refer to the MiCollab Engineering Guidelines for details.

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 175 for specific instructions on how to use MiCW to configure MiCollab and MiVoice Business platforms.

UNRELATED 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, or MiVoice Office 250 platform configuration.

REQUIREMENTS

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

• MiCW 5.3.x.x supports MiCollab 7.0 with MiVoice Business 7.2 and its SPs
• 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 8 Pro, Windows 7 (Professional, Business, or Ultimate), Windows XP Professional 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 Engineering Guidelines provides information about the characteristics, requirements, and performance of MiCollab and the supported applications.
• Virtual Appliance Deployment Guide provides engineering guidelines for deploying Mitel products in a virtual infrastructure.
• MiCollab Installation and Maintenance Guide (this guide) provides installation instructions for the MiCollab software and for the supported applications.
• MiCollab Platform Integration Guide provides instructions on how to configure the MiVoice Business, MiVoice Office 250, MiVoice 5000, and MiVoice MX-ONE 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.

Note: You can configure MiCollab with the MiVoice Business using the Mitel Integration Configuration Wizard. See “Flow Through Provisioning: Adding Greenfield MiCollab to Greenfield MiVB Servers” on page 175.
Introduction

- *MiCollab Client for Mobile Resiliency Guide* provides information for configuring MiCollab for Mobile Client resiliency.

**Administrator**
- *Server Manager help* provides configuration, administration, and maintenance procedures for the MiCollab server.
- *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.

**End User**
- *MiCollab End User Portal Online Help* provides 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.

**MIVOICE 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**
- *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.
MITEL MIVOX BUSINESS COMMUNICATIONS PLATFORM
- MiVoice Business System Administration Tool Online Help provides instructions on how to configure and program MiVoice Business platforms.

MITEL MIVOX OFFICE 250 COMMUNICATIONS PLATFORM
- Mitel MiVoice Office 250 and NuPoint Messenger Integration Guide 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 Connect.
2. Click Mitel Online.
4. Click Applications and then click MiCollab.

To access Mitel Knowledge Base articles:
1. Log on to Mitel OnLine.
2. Click Support, under Technical Support, click Mitel Knowledge Base. The Knowledge Base search engine opens.
3. From the Product list, select your application name and click Search.

ACCESS PRODUCT BULLETINS

To access Mitel Product Bulletins:
1. Log on to Mitel Connect.
2. Click Mitel Online.
4. Click the link to access a list of recent product bulletins.
Chapter 2

INSTALLATION & PROVISIONING

WORK FLOW
GETTING STARTED

1. Identify the following site requirements:
   - Deployment configuration (refer to the MiCollab Engineering Guidelines)
   - Applications (see “Supported Applications” on page 5)
   - MiCollab platform (“MiCollab Platforms” on page 4)
     - MiCollab Server
     - MiCollab Server Appliance, or
     - 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 “License Packages” on page 37.

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 work flow 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


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 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 copy to USB device or network share.

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 environments, 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 MiVoice 5000 and MiVoice MX-ONE platforms, you must configure MiCollab Client in integrated 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).

MiCollab with MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 250: The MiCW does not support these platforms so you must

- 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).
MiCollab Installation and Maintenance Guide

- **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

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 UCC and/or à 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
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 OnLine account.
2. Point to Purchasing. Under Licensing click AMC.
3. Click Go to the Applications Management Center (AMC).
4. Sign in with your unique AMC username and password to establish your "single sign on". On subsequent visits, you access your AMC account directly after signing in to Mitel OnLine.
5. For information about using the AMC, click the online Help link in your AMC account.

SOFTWARE ASSURANCE

The Mitel Software Assurance (SWAS) Program is a subscription-based service that provides customers with access to new software releases, software upgrades, and product support services for all users (ports) on a given application record. The Mitel Applications Management Center (AMC) manages the entitlement of the Software Assurance Program, determining whether a given application record ID for a customer is entitled to a specific software installation or upgrade. Initial product purchase includes 90 days of Software Assurance. The program can then be renewed for your chosen term. (Discounted rates are applied to multi-year renewals.)

Your Authorized Mitel Reseller will contact you before the expiry of your Software Assurance term to assist you with the renewal process. When you have decided upon a renewal term (from 1 day to 4 years), your Mitel Reseller will supply a price quotation. Upon acceptance of the quotation, your Mitel Reseller places your order and your Software Assurance is renewed within minutes. Note: If your Software Assurance plan has expired, you can still renew it, but there will be a re-enlistment fee.

Under the SWAS program, software upgrades are provided at no additional cost without any of the new features or functionality that are available in the base upgrade package. To obtain
the new features and functionality available in a software release, you must purchase the MiCollab base software package.

Refer to the latest Software Assurance Product Bulletin for the latest information. To access the SWAS bulletins:
- Log into Mitel Online
- Under Services, click Software Assurance and Support.

**VMICOLLAB LICENSING DETECTION AND VIOLATION MODE**

vMiCollab appliances must maintain online connectivity to the AMC at all times. Loss of AMC connectivity for a short period of time is tolerated by the system. However, AMC connectivity must be re-established without delay in order to maintain access to all system functions and features. If AMC connectivity is lost for an extended period of time, an automatic email alert is generated and sent to the named Channel Partner AMC account administrator. If AMC connectivity is not re-established, then the virtual appliance system goes into license violation mode and certain capabilities are no longer accessible.

Mitel recognizes that in some deployment situations, it is not practical to implement online connectivity to the AMC from each virtual appliance deployed at a customer’s site. For this reason, Mitel supports the ability to proxy online AMC connectivity from each virtual appliance through a single named proxy within the customer data center environment. This enables AMC online connections to be managed and controlled from one central point within the data center rather than from each individual product.

**UCC LICENSING**

Unified Communications and Collaboration (UCC) licensing helps to simplify the selling and ordering process because it bundles the platform and application user licenses together. For example, instead of ordering a MiVoice Business user license and multiple individual applications licenses for each MiCollab user, you order a single UCC license per user. The existing “à la carte” licensing options are still available; however, UCC licensing offers the following benefits:
- Simplifies the licensing of a MiCollab user by bundling application user licenses.
- Offers a significant pricing discount over “à la carte” licenses.
- Provides tiered functionality with progressive discounts. The following UCC user licenses are available:
  - UCC Basic license
  - UCC Entry license
  - UCC Standard license
  - UCC Premium license.
- In all cases, each UCC user license includes a Call manager user license with multiple device support (number of devices supported at each UCC tier depends on the Call Manager to which MiCollab is being deployed).
- Software assurance is more cost effective: The Mitel Software Assurance (SWAS) Program is a subscription-based service that provides customers with access to new software re-
leases, software upgrades, and product support services for all users (ports) on a given application record. Under the SWAS program, software upgrades are provided at no additional cost without any of the new features or functionality that are available in the base upgrade package.

• In the case of MiVoice Business platforms, 100-user license packs are available for Entry, Standard and Premium licenses with discounted pricing for volume.

UCC LICENSING RULES

The following rules apply to UCC Licensing:

• MiCollab Release 7.0 supports V4.x Enterprise UCC User Licenses only. UCC Business licenses are no longer available for UCC V4.x licensing. After an upgrade to MiCollab Release 7.0, 3.x Enterprise licenses are automatically converted to V4.0 Enterprise licenses. However, you must upgrade UCC Business V3.x to UCC 4.x Enterprise licenses through the Application Management Center (AMC).

• UCC V4.0 licensing is supported with MiCollab Release 7.0 and above. Providing that you have active Software Assurance, all earlier UCC licenses are automatically converted to UCC V4.0 licenses during an upgrade to Release 7.0. The MiCollab server only updates the users’ license bundles with the new entitlements. It does not automatically assign the services to the user. After an upgrade, you must update the services for each user. If your system had UCC V2 or V3 licenses that were converted to UCC V4.0 licenses, it is recommended that you assign the newly converted bundles to the same users who were previously using the UCC V2 or V3 licenses.

• After licenses have been converted, you update the users’ MiCollab Client Profiles using the Edit user functionality. New users are provisioned based on UCC V4 template definitions available on the system after the upgrade to MiCollab 7.0.

• UCC licensing is not supported for standalone Mitel applications.

• Hardware (controllers, phones), base system software, service provider interconnect licenses, and certain system options remain separately purchasable licenses.

• "à la carte" licenses remain available. Installed platform user licenses can be converted to the UCC Basic designation (process depends on the Call Manager that MiCollab is deployed against). This change facilitates upgrades to Entry, Standard, or Premium bundles.

• You can add UCC licenses to an existing MiCollab system. UCC licensing can be applied to a system which has existing "à la carte" licenses.

• There is no migration of existing "à la carte" licenses to UCC licenses.

• MiCollab licenses in the UCC license bundle can only be applied to one MiCollab application record in the AMC.

• You cannot split a UCC license bundle and deploy the application licenses across different users within a system. Nor can you split a UCC license bundle across multiple MiCollab systems that have the same user.

• Only add phone and applications services from USP. Do not add them from the application interfaces. This could result in license violations.
• When a UCC license bundle is assigned to a user, all the services provided in that bundle are consumed by that user, even if the services are not configured.

• When you configure a new user with a UCC license bundle, MiCollab fully configures the user’s phones and groups on the MiVoice Business (if Flow Through Provisioning is enabled). However, if you change a bundle for a user, you may be required to update the user’s ring group programming on the MiVoice Business. When MiCollab is deployed with a MiVoice 5000 or MiVoice MX-ONE, the administrator provisions MiCollab users from the call manager administrator interface by assigning a role to the user.

• If all the available UCC license bundles for a specific bundle type (Basic, Entry, Standard, or Premium) are in use, you will receive an error message if you attempt to assign another one of those license bundles (that is, you cannot assign a bundle to a user if the in-use bundle count is already equal to the licensed bundle count).

• The system displays licensing information in the server-manager interface under Applications on the Licensing Information page.

• **For MiVoice Business integrations**: If you downgrade the UCC license bundle of an existing user (for example, from Entry to Basic, from Standard to Entry, or from Premium to Standard) from the USP application, the system will not delete any of the services. Instead, MiCollab attempts to apply any available "à la carte" licenses to support the extra services. If "à la carte" licenses are not available, then a license violation is generated. If you if you downgrade the role from the call, the services will be deleted.

• **For MiVoice 5000 or MiVoice MX-ONE integrations**: If you downgrade the UCC license bundle of an existing user (for example, from Entry to Basic, from Standard to Entry, or from Premium to Standard) from the platform’s call manager interface, the user’s services are deleted.

• If you have different types of upgrade licenses (for example, "Basic to Entry", "Entry to Standard", and "Standard to Premium") available on the system, apply the highest upgrade licenses first. For example, upgrade the Standard users to Premium licenses first, before you upgrade the Entry users to Standard licenses.

• To use the MBG Teleworker licenses that are included in the UCC Standard and Premium Licenses, the MiCollab and MBG servers must be clustered.
**UCC LICENSING TIERS**

There are four tiers of UCC licensing: Basic, Entry, Standard, and Premium. There are also two UCC licensing versions:

- Use UCC V4.0 Enterprise licenses
  - with all MiCollab Release 7.0 systems, and
  - with all MiCollab Release 6.0 and later systems that manage a network of communication platforms.

- Use Business UCC V3.0 licenses for MiCollab systems with Release 6.0 SP2 and earlier that support standalone MiVoice Business systems.

**CAUTION:** Licensing is subject to change. Refer to the MiCollab Product Bulletins for the latest information.

<table>
<thead>
<tr>
<th>LICENSES INCLUDED</th>
<th>V4.0 UCC LICENSE BUNDLES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BASIC</td>
</tr>
<tr>
<td>MiVoice Business user license only</td>
<td>Entitles user to MiCollab Basic Client</td>
</tr>
<tr>
<td>MiVoice Business Multi-device user license (not applicable to MiVoice 5000 or MX-ONE)</td>
<td>No</td>
</tr>
<tr>
<td>MiVoice 5000 or MX-ONE Multi-device user license (not applicable to MiVoice Business)</td>
<td>No</td>
</tr>
<tr>
<td>NuPoint mailbox license with call director</td>
<td>No</td>
</tr>
<tr>
<td>Standard and Advanced UM license</td>
<td>No</td>
</tr>
<tr>
<td>MiCollab Client desktop and web client with Instant Messaging (also see “MiCollab PC Client Capabilities by UCC Bundle” on page 26)</td>
<td>Yes</td>
</tr>
<tr>
<td>MiCollab AWV and collaboration access</td>
<td>No</td>
</tr>
<tr>
<td>MBG Teleworker license, MiCollab Client MiNET and SIP softphone license</td>
<td>No</td>
</tr>
<tr>
<td>MiCollab Client deskphone license</td>
<td>No</td>
</tr>
<tr>
<td>MiCollab Client web license (see Note 1)</td>
<td>Yes (Basic features only)</td>
</tr>
</tbody>
</table>
Licensing

Notes:

1. With an additional MiVoice Business user license, you can configure a UCC Entry user with a Multi-device User Group.

2. Basic licenses also include the MiCollab Client desktop and web client with just the Instant Messaging Presence feature. Entry licenses provide IM and Voice presence. Standard and Premium licenses provide MiCollab Client desktop and web client with full MiCollab Client feature functionality.

3. A Standard license provides video functionality. A Premium license includes the standard video functionality and the advanced Vidyo feature. Vidyo provides higher resolution video as well as some advanced features. Vidyo and MiCollab integration also requires the Vidyo Portal API License PN5130264.

4. Optional license PN54006550 adds MiCollab Client Mobile functionality to an Entry bundle.

5. Optional license PN54006551 adds MiCollab Client Softphone functionality to an Entry bundle.

<table>
<thead>
<tr>
<th>LICENSES INCLUDED</th>
<th>V4.0 UCC LICENSE BUNDLES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>BASIC</td>
</tr>
<tr>
<td>MiCollab Client softphone license (see Note 1)</td>
<td>No</td>
</tr>
<tr>
<td>MiCollab Client Mobile SIP for Softphone</td>
<td>No</td>
</tr>
</tbody>
</table>
MICOLLAB PC CLIENT CAPABILITIES BY UCC BUNDLE

Table 2: MiCollab PC Client Capabilities

<table>
<thead>
<tr>
<th>PC UC CLIENT CAPABILITIES</th>
<th>BASIC (FREE)</th>
<th>ENTRY BUNDLE</th>
<th>STANDARD &amp; PREMIUM BUNDLES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Statue &amp; Calendar Integration</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>PC Softphone</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Ad hoc Collaboration Launch</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Call Handoff</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Launchpad</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Hot Desking from client</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Knowledge Management</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>OfficeLink (Make call on other device)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Presence (IM / Voice / Video)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Click to Call from UCA Contacts</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Contact Management &amp; Grouping</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Voice Features: Auto Answer / DND / Call Forwarding / Incoming Call Notification</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IM Chat</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Call History</td>
<td>Missed only</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Visual Voice Mail</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Web Window (RSS)</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Desk Phone Button Programming</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Import Contacts (Outlook, Google)</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

UCC LICENSING FOR MICOLLAB AWV

The following UCC Licensing conditions apply to the MiCollab AWV application:

- MiCollab AWV is licensed by port. Each port enables one simultaneous audio and web connection in the system. For example, a 10-party conference would require 10 ports.

- The system includes nine ports plus an additional port for every 10 Standard UCC User licenses. If the system has no Standard or Premium UCC User licenses, then no ports are included with the system. Typical configurations use one audio port for every 10 MiCollab AWV users.

- The AMC uses a set of pre-defined rules to deliver audio and web collaboration entitlement:

  The number of ports are based on the number of UCC Standard or Premium licenses that are assigned to users.

  The following licenses are provisioned for every 10 Standard UCC Users:

  1 x Communications Platform Connection User
  1 x MiCollab AWV Web Port, 1 x Audio Port, 1 x HDCodec Port

  The following licenses are provisioned for every 5 Premium UCC Users:
1 x Communications Platform Connection User
1 x MiCollab AWV Web Port, 1 x Audio Port, 1 x HDCodec Port

For example: 11 UCC Standard licenses earns 11 audio and web collaboration ports at no additional charge

- A total of 21 UCC Standard licenses earns 12 audio and web collaboration ports at no additional charge.
- A conferencing port is comprised of 1 audio port, 1 web port, and 1 H.264 video port.
- A UCC Entry license does not include a conferencing license so it does not include any audio and web conferencing ports.
- If required, you can purchase additional ports separately to achieve the customer’s required quantity, depending on the end-customers particular business requirements for simultaneous audio conferencing.

UCC LICENSING PART NUMBERS

Table 3: UCC Licenses

<table>
<thead>
<tr>
<th>LICENSES</th>
<th>PART NUMBER</th>
<th>NUMBER REQUIRED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MIVOICE BUSINESS INTEGRATIONS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>User</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCCV4.0 Entry User x1</td>
<td>54006539</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Standard User x1</td>
<td>54006542</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Premium User x1</td>
<td>54006545</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Entry User x100</td>
<td>54006541</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Standard User x100</td>
<td>54006544</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Premium User x100</td>
<td>54006547</td>
<td></td>
</tr>
<tr>
<td><strong>User Licenses - Service Provider Subscription Fulfilment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP Subscript License-UCCv4.0 Entry Users x50</td>
<td>54006122</td>
<td></td>
</tr>
<tr>
<td>SP Subscript License-UCCv4.0 Stnd Users x50</td>
<td>54006117</td>
<td></td>
</tr>
<tr>
<td>SP Subscript License-UCCv4.0 Prem Users x50</td>
<td>54006118</td>
<td></td>
</tr>
<tr>
<td><strong>User Licenses - Service Provider CAPEX</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP Capex License - UCCv4.0 Entry User x1</td>
<td>54006119</td>
<td></td>
</tr>
<tr>
<td>SP Capex License - UCCv4.0 Standard User x1</td>
<td>54006120</td>
<td></td>
</tr>
<tr>
<td>SP Capex License - UCCv4.0 Premium User x1</td>
<td>54006121</td>
<td></td>
</tr>
<tr>
<td><strong>Uplift</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Basic to v4.0 Entry</td>
<td>54006553</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Basic to v4.0 Standard (available in Release 7.1 and later)</td>
<td>54006704</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Basic to v4.0 Premium (available in Release 7.1 and later)</td>
<td>54006705</td>
<td></td>
</tr>
<tr>
<td>UCCv4.0 Entry to v4.0 Standard</td>
<td>54006548</td>
<td></td>
</tr>
</tbody>
</table>
## MiCollab Installation and Maintenance Guide

### Licenses

| UCCv4.0 Standard to v4.0 Prem | 54006549 |

### MiVoice 5000 Integrations

<table>
<thead>
<tr>
<th>User</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UCCv4.0 Entry User x1</td>
<td>51303523</td>
</tr>
<tr>
<td>UCCv4.0 Standard User x1</td>
<td>51305324</td>
</tr>
<tr>
<td>UCCv4.0 Premium User x1</td>
<td>51303525</td>
</tr>
<tr>
<td>UCCv4.0 Entry User x100</td>
<td>51303701</td>
</tr>
<tr>
<td>UCCv4.0 Standard User x100</td>
<td>51303702</td>
</tr>
<tr>
<td>UCCv4.0 Premium User x100</td>
<td>51303705</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Uplift</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UCCv4.0 Basic to v4.0 Entry</td>
<td>51303528</td>
</tr>
<tr>
<td>UCCv4.0 Basic to v4.0 Standard (available in Release 7.1 and later)</td>
<td>51304210</td>
</tr>
<tr>
<td>UCCv4.0 Basic to v4.0 Premium (available in Release 7.1 and later)</td>
<td>51304211</td>
</tr>
<tr>
<td>UCCv4.0 Entry to v4.0 Standard</td>
<td>51303526</td>
</tr>
<tr>
<td>UCCv4.0 Standard to v4.0 Prem</td>
<td>51303527</td>
</tr>
</tbody>
</table>

### MiVoice MX-One Integrations

<table>
<thead>
<tr>
<th>User</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UCCv4.0 Entry User x1</td>
<td>51303535</td>
</tr>
<tr>
<td>UCCv4.0 Standard User x1</td>
<td>51303536</td>
</tr>
<tr>
<td>UCCv4.0 Premium User x1</td>
<td>51303537</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Uplift</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>UCCv4.0 Basic to v4.0 Entry</td>
<td>51303540</td>
</tr>
<tr>
<td>UCCv4.0 Basic to v4.0 Standard (available in Release 7.1 and later)</td>
<td>51304212</td>
</tr>
<tr>
<td>UCCv4.0 Basic to v4.0 Premium (available in Release 7.1 and later)</td>
<td>51304213</td>
</tr>
<tr>
<td>UCCv4.0 Entry to v4.0 Standard</td>
<td>51303538</td>
</tr>
<tr>
<td>UCCv4.0 Standard to v4.0 Prem</td>
<td>51303539</td>
</tr>
</tbody>
</table>

### Software Assurance Support (SWAS)

| Standard SWAS: UCC Virtual Appliance Base | 54005936 |
| Premium SWAS: UCC Virtual Appliance Base | 54005937 |
| Standard SWAS: UCC Virtual Appliance Base for SP CAPEX | 54005938 |
| Premium SWAS: UCC Virtual Appliance Base for SP CAPEX | 54005939 |

### Other

| MiCollab Mobile Client Option | 54006550 |
| MiCollab Client PC Softphone Option | 54006551 |

**Note:** Premium SWAS must be applied as an upgrade to Standard SWAS (that is, you cannot apply Premium SWAS outright; it must be applied to a system that has Standard SWAS).
UCC LICENSING PROCEDURE

The Application Management Center distributes the platform and application user licenses that are contained within a 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 MBG Release 9.1 or higher (optional)

MiVoice 5000 and MX-ONE Deployments

You add the following servers to a UCC License Manager group:
- 1 MiCollab Release 7.0 or higher system
- 1 MBG Release 9.1 or higher (optional)

The MiVoice 5000 and MX-ONE communication platforms do not receive licenses from the Applications Management Center (AMC). Therefore, they are not added to UCC Licensing Manager groups.

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 group on AMC.
- Add the system server ARIDs and GARIDs to the ULM group.
- Assign licenses, including UCC user and SWAS licenses, to the ULM 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 login User ID
   - Enter your Password.
2. Create a Customer Account for each customer. Do not put multiple customers in a single customer account.
   - Under **Systems**, 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.
   - Click **Submit** and click **Confirm**.

![Create Customer Record (TEST: Mitel Internal)](image)

**Figure 2: Create Customer Account**

3. Register products and licenses for the customer site:
   - 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. Use the browser Find function to locate specific part numbers or license descriptions.
   - Click + beside MiCollab Products. Enter the required MiCollab base software license and product licenses.
   - Click + beside Mitel Standard Linux Standalone 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** and then click **Confirm**.

**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.
4. Create Application Record IDs for your customer’s MiCollab, standalone MBG, and MiVoice Business systems. If you are integrating with a MiVoice 5000 or MX-ONE, only create ARIDs for the MiCollab and standalone MBG. To create an ARID:
   - Under **Systems**, click **Customers**.
   - Enter the name of the customer and click **Retrieve**.
   - Select the Customer ID of your customer from the Customer List and click **Create App Record**.
   - Enter a description for the Application Record (for example: PPP Industries MiCollab ARID) and click **Submit**.
   - Click **Next** and the system displays a ARID for your customer’s system.
   - Record the ARID.
   - Repeat the above steps for each system.
Figure 4: Create ARIDs

5. For each system, assign the base software license to the system’s base ARID:
   - Under Tasks, click Assign a License.
   - Enter the Customer Name in the Name field and then click Retrieve.
   - Click + beside the customer’s ID.
   - Select the option button next to the Base ARID and then click Assign.
   - Enter the Purchase order number in the Search Criteria and click Retrieve.
   - Click + to expand the Purchase order.
   - Assign the system’s base software license to the base ARID.
   - Click Confirm to assign the licenses.
   - Review the licenses and record the ARID.
   - Click Done or click E-Mail Report to notify to the administrator. You can send the notification to your technician or customer by including their email addresses.
6. In the Customer profile create an associated ULM Group ARID:
   - Under **Tasks**, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
   - Click + beside the customer’s ID.
   - For deployments with MiVoice Business, select the option button next to the MiVoice Business Base ARID.
     For deployments with MiVoice 5000 or MX-ONE, select the option button next to the MiCollab Base ARID.
   - Click the **Create ULM Record** button.
   - Enter a description for the ULM Application Record. For example: "ABC Corporation ULM ARID".
   - Click **Submit**. The system displays the newly created ARID at the top of the screen.
   - Record the ULM ARID.
   - Click **Next**. The server ARIDs appear listed in the right frame of the Group Application Record.
Figure 6: Create ULM Group ARID

7. 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.
8. If you are deploying a MiVoice Business platform, assign the MiVoice Business SIP trunk licenses, MBG SIP trunk licenses, UCC User and SWAS licenses to the ULM ARID:
   - Under Tasks, click **Assign a License**.
   - Enter the Customer Name in the Name field and then click **Retrieve**.
   - Click + beside the customer’s ID.
   - Select the option button next to the ULM ARID (for example, "ABC Corporation ULM Record" and then click **Assign**.
   - Enter the Purchase order number in the Search Criteria and click **Retrieve**.
   - 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.

9. 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.

- You do not sync MiVoice 5000 or MiVoice MX-ONE platforms with the AMC. The MiVoice 5000 and MiVoice MX-ONE obtain their licenses from the GIM.

10. 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, or

For MiVoice 5000 or MX-ONE deployments, you will assign the UCC licenses to users from the MiVoice 5000 or MiVoice MX-ONE administrator management interfaces by applying roles to the users. Roles are associated with templates. The template applies the UCC licensing bundle to the user’s MiCollab profile.

EFFECT OF UPGRADING ON UCC LICENSING

When you upgrade to MiCollab Release 7.0 with

• MiVoice Business 7.1, UCC v3 Standard and Premium licenses are upgraded to UCC v4 licenses. UCC v3 Entry licenses remain at UCC v3.

• MiVoice Business 7.2, UCC v3 Entry, Standard, and Premium licenses are upgraded to UCC v4 licenses. However, the number of external hot desk licenses that were provided by the UCC v3 Entry licenses remains the same.

TRUSTED SERVICE SUPPORT

The MiCollab NuPoint Unified Messaging application is supported as a Trusted Service (application) on MiVoice Business platforms. Trusted services do not require MiVoice Business IP user licenses to register and provide services to the MiVoice Business platform. Instead, they validate themselves to the MiVoice Business using an encrypted handshake. Because the NuPoint service is trusted, this reduces the need to include MiVoice Business user licenses in the MiCollab base packs and NuPoint mailbox uplift licenses.

In order to be trusted, the voicemail port directory numbers (DNs) must be assigned with a "Trusted Service" level on the MiVoice Business platform:

• For new MiCollab with MiVoice Business installations that are configured using Mitel Integrated Configuration Wizard, the "Full Service" level is applied by default to the DNs on the MiVoice Business platform.

• To manually configure trusted service, assign the "Trusted Service" level to the voice mail port DNs in the User and Services Configuration form of the MiVoice Business System Administration Tool and then restart the NuPoint application from the NuPoint console to re-register the application ports.

NuPoint will then authenticate itself to the MiVoice Business using SSL certificates, and an MiVoice Business license will be freed for other uses. For more information, see the NuPoint UM Technician’s Handbook and the MiVoice Business System Administration Tool Help.

Note the following:

• Trusted MiCollab applications connect to the MiVoice Business system services through port 6803 on the MiVoice Business platform.
Licensing

- Trusted Service directory numbers are programmed on the same forms and fields as Full Service directory numbers.
- Although Trusted Services do not consume IP user licenses, they do consume other licenses (such as EDHU or HTML licenses) when they are programmed with additional functionality.

LICENSE PACKAGES

The following sections detail the software licensing packages and provides an overview of the functionality provided in each package:

- Refer to the MiCollab Engineering Guidelines for descriptions of the supported platforms and deployment configurations.
- Refer to Product Bulletin PB 20110051 for MiCollab upgrade and migration licensing details.

The following table lists the MiCollab base, add-on, and upgrade licensing packages.

<table>
<thead>
<tr>
<th>SOFTWARE PACKAGE</th>
<th>PLATFORM(S)</th>
<th>PART NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BASE PACKAGES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MiCollab Base SW for Free MiCollab Client</td>
<td>MiVoice Business, MiVoice Office 250, MiVoice 5000, MiVoice MX-ONE</td>
<td>54005963</td>
</tr>
<tr>
<td>MiCollab Base SW (Full)</td>
<td>MiVoice Business and MiVoice Office 250</td>
<td>54005441</td>
</tr>
<tr>
<td>MiCollab Virtual Appliance for MiVoice Business</td>
<td>MiVoice Business, MiVoice 5000, MiVoice MX-ONE</td>
<td>54005442</td>
</tr>
<tr>
<td>MiCollab Virtual Appliance for MiVoice Office 250</td>
<td>MiVoice Office 250</td>
<td>54005799</td>
</tr>
<tr>
<td>MiCollab Server Appliance for MiVoice Business (NA)</td>
<td>MiVoice Business</td>
<td>52002722</td>
</tr>
<tr>
<td>MiCollab Server Appliance for Mitel MiVoice Office 250 (NA)</td>
<td>MiVoice Office 250</td>
<td>52002723</td>
</tr>
<tr>
<td><strong>MiCollab Base Add-on to MiCollab Client</strong></td>
<td>MiVoice Business and MiVoice Office 250</td>
<td>54005444</td>
</tr>
<tr>
<td>MiCollab add-on to MiCollab Client</td>
<td>MiVoice Business and MiVoice Office 250</td>
<td>54005445</td>
</tr>
<tr>
<td><strong>UPGRADES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MiCollab 2.2 base kit to MiCollab 3.0/4.0 base kit upgrade</td>
<td>MiVoice Business and MiVoice Office 250</td>
<td>54005447</td>
</tr>
<tr>
<td>vMiCollab 2.2 to vMiCollab 3.0/4.0 base kit upgrade</td>
<td>MiVoice Business</td>
<td>54005449</td>
</tr>
<tr>
<td>MiCollab AWV HD Codec Upgrade</td>
<td>MiVoice Business and MiVoice Office 250</td>
<td>54005475</td>
</tr>
<tr>
<td>MiCollab AWV HD Codec + Web Collaboration license</td>
<td>MiVoice Business and MiVoice Office 250</td>
<td>54005477</td>
</tr>
<tr>
<td>MiCollab Base SW for Free MiCollab Client to Full MiCollab Base</td>
<td>MiVoice Office 250</td>
<td>54005964</td>
</tr>
<tr>
<td><strong>DATABASE MIGRATIONS</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note: The "MiCollab Server to Virtual MiCollab Conversion" part number allows you to convert a MiCollab Server to a vMiCollab for either MiVoice Business or MiVoice Office 250 platforms.

Note: Only MBG Teleworker service is supported for MiVoice Office 250 platforms. The MBG SIP Trunking, MBG Secure Recording Connector, and MBG Web Proxy services are not supported on MiVoice Office 250 platforms.

### MICOLLAB BASE PACKAGES

The following MiCollab base packages are available:

- MiCollab Base SW -- P/N 54005441
- Virtual MiCollab Base SW -- P/N 54005442
- MiCollab Server Appliance MiVoice Business (NA) -- P/N 52002722
- MiCollab Server Appliance MiVoice Office 250 (NA) -- P/N 52002723

The Base SW packages provide the following licenses:

- 6 SIP Peering VM Ports for NP-UM
- 6 MiVoice Business Application Connection licenses

### MICOLLAB AND VMICOLLAB BASE ADD-ON TO MICOLLAB CLIENT

MiCollab add-on to MiCollab Client (PN 54005444)

- 6 SIP Peering VM Ports for NP-UM
- 6 MiVoice Business Application Connection licenses

vMiCollab add-on to MiCollab Client (PN 54005445)

- 6 MiVoice Business Application Connection licenses

### UPLIFT PACKAGES

**NUPOINT UNIFIED MESSAGING**

The following user uplift packages are available for MiVoice Business systems:

- 1 user mailbox license and 1 personal call director license (PN 54004762)
- 10 user mailbox licenses, 10 personal call director licenses, 1 application connection license (PN 54005610)
- 50 user mailbox license, 50 personal call director licenses, 3 application connection licenses (PN 54005611)
- 250 user mailbox license, 250 personal call director licenses, 10 application connection licenses (PN 54005612)
• 500 user mailbox license, 500 personal call director licenses, 15 application connection licenses (PN 54005613)

The following user uplift packages are available for the MiVoice Office 250 integration via the MiVoice Office 250 Gateway:
• 1 user mailbox license and 1 personal call director license (PN 54004767)
• 10 user mailbox licenses, 10 personal call director licenses, and one SIP Peering license (PN 54004768)
• 50 user mailbox license, 50 personal call director licenses, and 3 SIP Peering licenses (PN 54004769)

You can also purchase Standard UM licenses, Advanced UM licenses, and Speech Directory entries in bundles of one, ten, and fifty. The Advanced UM licenses are specific to the MiCollab product. The other bundles are NuPoint standalone application part numbers that are available to MiCollab customers:

NuPoint Standard UM standalone part numbers (parts listed under NuPoint, available for MiCollab)
• 1 NuPoint Standard UM User (PN 54004107)
• 10 NuPoint Standard UM Users (PN 54004108)
• 50 NuPoint Standard UM Users (PN 54004109)

NuPoint Advanced UM standalone part numbers (MiCollab specific numbers)
• 1 MiCollab NPUM Advanced UM User Uplift (PN 54004222)
• 10 MiCollab NPUM Advanced UM User Uplift (PN 54004052)
• 50 MiCollab NPUM Advanced UM User Uplift (PN 54004223)

Note: Advanced System Enablement is included in the MiCollab base software.

NuPoint Speech Directory standalone part numbers
• 1 Entry NPUM Speech AA Directory Uplift (1 Entries) (PN 54004054)
• 10 Entries NPUM Speech AA Directory Uplift (PN 54004055)
• 50 Entries NPUM Speech AA Directory Uplift (PN 54003293)

MiCollab NuPoint Misc Port part numbers
• NuPoint Misc App Port (54004961)
• NuPoint TTS port (PN 54002692)
• Speech AA port (PN 54003292)
• NPM IP FAX Port Enable (PN 54002375)

NuPoint FAX part numbers
• NuPoint Outbound FAX 1 User (PN 54004110)
• NuPoint Outbound FAX 10 User (PN 54004111)
• NuPoint Outbound FAX 50 User (PN 54004112)

NuPoint Feature Options
• NPM IP-Voice Mail Networking (PN 54001624)
• NPM IP-Voice IP-Record-A-Call (PN 54001627)
• NPM IP-TDM Memo Full Edition (PN 54001640)
• NPM IP-Competitive TUI Kit (PN 54001641)
• NPM IP Miscellaneous Applications (PN 54001636)
• NPM Call Detail Recorder (PN 54001637)
• NPM IP-Full Language Uplift (PN 54001637)
• Enable Presence (PN 54003298)
• NP Speech Navigation Enablement (NP 54005861)
• NP Speech Navigation 10 Users (PN 54005862)
• NP G.729 System Enablement (PN54005863)

NuPoint Speech to Text (STT) Enablement License (PN 54005322)
Note that this license is only compatible with MAS Release 4.0 and later systems. You cannot apply this license to pre-MAS Release 4.0 systems.

NuPoint STT Auto Transaction Credits
• 180 credits (6-month expiry) - (PN 54005647)
• 360 credits (12-month expiry) - (PN 54005648)

MBG-TELEWORKER

The following Teleworker user uplift packages are available for MiVoice Business:
• 1 MBG Teleworker Service User (PN 54004572)
• 10 MBG Teleworker Service Users (PN 54004573)
• 50 MBG Teleworker Service Users (PN 54004575)
• 100 MBG Teleworker Service Users (PN 54004577)
• SIP Trunking Channel (PN 54004491)
• MBG 5 Session Compression License (PN 54004582)

MBG-SECURE RECORDING CONNECTOR

The following TAP licenses are available to enable Secure Recording Connector for user devices:
• Secure Recording Connector Single License (PN 54003182)
• Secure Recording Connector Single 10-License Pack (PN 54003183)
• Secure Recording Connector Single 50-License Pack (PN 54003184)

MiCollab AWV Uplift Licensing Details

For each MiCollab AWV Uplift License purchased, you can create 20 MiCollab AWV user accounts on the system. The number of concurrent conference users, for all conferences, is equal to one user per one MiCollab AWV Uplift License. You can set up many MiCollab AWV user accounts, but for licensing purposes the product restricts the total number of concurrent conference participants. The following table identifies the communication platform license requirements:

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>LICENSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiVoice Business system</td>
<td>• One application connection license per MiCollab AWV Uplift License (included with MiCollab AWV uplift license)</td>
</tr>
<tr>
<td>Mitel MiVoice Office 250</td>
<td>• One Category C License per MiCollab AWV Uplift License (included with MiCollab AWV uplift license)</td>
</tr>
<tr>
<td></td>
<td>• One IP Enabler Unit License per MiCollab AWV Uplift License, or One IP Enabler System License (one IP Enabler Unit License is included with MiCollab AWV uplift license)</td>
</tr>
<tr>
<td></td>
<td>• System OAI Events License (not included with MiCollab AWV uplift license)</td>
</tr>
<tr>
<td></td>
<td>• System OAI Third-party Call Control License (not included with MiCollab AWV uplift license)</td>
</tr>
</tbody>
</table>

For MiVoice Business Systems

MiCollab AWV Audio Only

• 1 MiCollab AWV audio uplift license and 1 MiVoice Business application connection license (PN 54005614)
• 10 MiCollab AWV audio uplift licenses and 10 MiVoice Business application connection licenses (PN 54005615)
• 50 MiCollab AWV audio uplift licenses and 50 MiVoice Business application connection licenses (PN 54005616)

MiCollab AWV Audio and Web

• 1 MiCollab AWV audio uplift and web uplift license and 1 MiVoice Business application connection license (PN 54005617)
• 10 MiCollab AWV audio uplift and web uplift licenses and 10 MiVoice Business application connection licenses (PN 54005618)
• 50 MiCollab AWV audio uplift and web uplift licenses and 50 MiVoice Business application connection licenses (PN 54005619)
MiCollab Installation and Maintenance Guide

For MiVoice Office 250

MiCollab AWV Audio Only

• 1 MiCollab AWV audio only user license 5K (PN 54003981)
• 10 MiCollab AWV audio only user licenses 5K (PN 54003982)
• 50 MiCollab AWV audio only user licenses 5K (PN 54003983)

MiCollab AWV Audio and Web

• 1 MiCollab AWV audio and web license 5K (PN 54003984)
• 10 MiCollab AWV audio and web licenses 5K (PN 54003985)
• 50 MiCollab AWV audio and web licenses 5K (PN 54003986)

For MiVoice Office 250 Digital

MiCollab AWV Audio Only

• 1 MiCollab AWV audio uplift license, 1 Single Unit IP enabling license, 1 CAT C license (PN 54003973)
• 10 MiCollab AWV audio uplift licenses, 10 Single Unit IP enabling licenses, 10 CAT C licenses (PN 54003974)
• 50 MiCollab AWV audio uplift licenses, 50 Single Unit IP enabling licenses, 50 CAT C licenses (PN 54003975)

MiCollab AWV Audio and Web

• 1 MiCollab AWV audio uplift and web uplift license, 1 Single Unit IP enabling license, 1 CAT C license (PN 54003976)
• 10 MiCollab AWV audio uplift and web uplift licenses, 10 Single Unit IP enabling licenses, 10 CAT C licenses (PN 54003977)
• 50 MiCollab AWV audio uplift and web uplift licenses, 50 Single Unit IP enabling licenses, 50 CAT C licenses (PN 54003978)

Introduce MiCollab AWV Web-only for all PBX Integrations

MiCollab AWV Web Only

• 1 MiCollab AWV web uplift (PN 54004621)
• 10 MiCollab AWV web uplift (PN 54004622)
• 50 MiCollab AWV web uplift (PN 54004623)

MiCollab AWV Enhanced Video License

For MiCollab AWV v4.00 or later Collaboration Clients, these licenses provide the higher resolution video that is supported by the H.264 codec:

• 54005475 MiCollab: 1 MiCollab AWV HD Codec Uplift - Discounted uplift license required for customers who purchased a web collaboration license in MCA Release 3.9 and are upgrading to a later MiCollab AWV Release.
**MICOLLAB CLIENT**

- 1 MiCollab Client Deskphone License (PN 54004266)
- 50 MiCollab Client Deskphone Licenses (PN 54004267)
- 1 MiCollab Client Softphone License (PN 54004268)
- 50 MiCollab Client Softphone Licenses (PN 54004269)
- MiCollab Client Deskphone and Softphone License (PN 54004281)
- MiCollab Client Server Peering License (PN 54005380)
- MiCollab Client Server Federation License (PN 54005381)
- 1 MiCollab Client Mobile for Smart Device License (PN 54005598)
- 50 MiCollab Client Mobile for Smart Device Licenses (PN 54005599)
- 1 MiCollab Client Standalone Client Smart Device License (PN 54005601)
- MiCollab Client Console Option (PN 54004823)
- MiCollab Client MiNET and SIP Softphone License (PN54005830)
- MiCollab Client Deskphone/Softphone and SIP Softphone License (PN 540005831)
- MiCollab Client Mobile Smart Device SIP License Add-on (PN 540005832)
- MiCollab Client Mobile Standalone SIP License Add-on (PN 54005833)
- SIP MiCollab Client Softphone Add-on License (PN 54005829)
- MiCollab Client MiNet and SIP Softphone License (PN 54005830)
- Add-on UCC Premium MiCollab Client Mobile for SIP and Video (PN 54005887)
- Add-on UCC Premium Mobility Fixed Mobile Convergence (FMC) (PN 54005888)
- Add-on MiCollab Client Mobility SIP Softphone and Video (PN 5400889)
- Add-on MiCollab Client Mobility Fixed Mobile Convergence (FMC) (PN54005890)

**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.

---

**Note:** Ensure that the number of enhanced video licenses equals the number of web conference port licenses. If you have a fewer number of enhanced video licenses than you have web collaboration port licenses, you will lose the additional port licenses. Also, you must restart MiCollab AWV in order to activate these licenses.
3. Access the server manager. See “Log in to the Administrator Portal (Server Manager)” on page 64.

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 117. If you are installing vMiCollab, see “Installing Virtual MiCollab in a VMware Environment” on page 71.

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 93).
- Integrate or Co-locate MiCollab Client Database? (See “Configure MiCollab Client Mode” on page 97).
# 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>
</table>

### MiCollab Server or MiCollab Server Appliance

1. **Administrator Password**  
   For password strength, choose a password that contains a mix of uppercase and lowercase letters, numbers, and punctuation characters. For more information, see page 56.

2. **Domain Name**  
   Names must start with a letter; can contain letters, numbers, and hyphens. For more information, see page 57.

3. **System Name**

4. **IP address of your MiCollab server (LAN mode)**  
   The local IP address of the server where you are installing MiCollab.

4b. **IP address of your external NIC (Network Edge mode)**  
   The IP address of your external Ethernet connection.

5. **External Interface Connection**  
   Cable Modem? You need to know if the ISP supplies an account name or an Ethernet address.  
   Direct Connection? You need to know the static IP address.

6. **Gateway IP address**  
   The IP address that MiCollab will use to access the network.

7. **MiCollab AWV IP Addresses**  
   If installing the MiCollab AWV application in a MiCollab server, 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).  
   You configure the two MiCollab AWV IP addresses for Network Edge deployments. See the MiCollab Engineering Guidelines document for deployment configurations.

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 60.

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.
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 and Solutions, click Mitel Standard Linux.
3. Click MSL Qualified Hardware List (Web 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™ R210 Rack Mount Server which includes the following:
MiCollab Installation and Maintenance Guide

- Intel Core i3 Microprocessor
- 8GB 1333 MHz ECC DDR3 Memory
- Non-redundant 250 GB SATA Hard Disk Drive
- Non-redundant Power Supply
- Dual Port Motherboard Embedded Ethernet Adapter
- Internal DVD-ROM Drive.

Figure 8 shows the front view. Figure 9 shows the location of the Local and WAN network interfaces on the rear panel.

Follow the manufacturer’s instructions to set up the server hardware. Table 5 lists the required BIOS settings for the Dell PowerEdge R210 Rack-mount server:
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 Connect. 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 FOR MIVOICE BUSINESS
1. Log on to Mitel Connect.
2. Click Mitel Online.
3. Click Technical and then click Software Downloads.
4. Click MiCollab.
5. Click the appropriate MiCollab Software Download version.
7. 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.
8. Click the "I Agree [Download using Software Download Manager (Recommended)]".
9. If you don’t already have the Download Manager installed on your local PC, you are prompt-
ed 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.
10. Save the downloaded software ISO images to a folder on your maintenance PC.

SOFTWARE DOWNLOADS WITH MIVOICE MX-ONE
1. Log in to Mitel Connect.
2. Select Knowledge Base.
3. Under Applications, select MiCollab. The Service Advice for the release of MiCollab 7.0
is in section “Service Pack/Advice 2015”.

SOFTWARE DOWNLOADS WITH MIVOICE 5000
1. Log in to Espace France (https://support.mitel.fr).
2. Click Espace technique.
3. Click Produits then Logiciel (Products then Software)
4. Navigate through Applications/MiCollab.
5. Click the download link for your software package.

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
  install lat ions on Hyper-V virtual machines).
OR

- burn each ISO file to a CD/DVD 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 10.3 for MiCollab Servers</td>
<td>MSL_10.3.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_7.0.x.xx.0.iso</td>
<td>260 MB</td>
</tr>
<tr>
<td>MiVoice Border Gateway</td>
<td>MBG_9.1.xx.0.iso</td>
<td>98 MB</td>
</tr>
<tr>
<td>MiCollab Client Service</td>
<td>MiCollab Client_7.0.x.x.iso</td>
<td>283 MB</td>
</tr>
<tr>
<td>MiCollab Audio, Web and Video Conferencing</td>
<td>AWV_6.x.x.xx.iso</td>
<td>135 MB</td>
</tr>
<tr>
<td>NuPoint Unified Messaging (includes Speech to Text option)</td>
<td>NPM_Blades-DVD_1_18.x.x.xx-01.iso</td>
<td>1.0 GB</td>
</tr>
<tr>
<td>Speech Auto Attendant - Text to Speech</td>
<td>NPM_Blades-DVD_2_18.x.x.xx-01.iso</td>
<td>2.0 GB</td>
</tr>
<tr>
<td>MiCollab Client Deployment</td>
<td>MiCollab Client Deploy_1.0.x.x</td>
<td></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 10.3 for MiCollab Servers</td>
<td>MSL_10.3.xx.0.i686.iso (64-bit version only)</td>
</tr>
<tr>
<td>CD/DVD2</td>
<td>MiCollab Application Services</td>
<td>SAS_7.0.x.xx.0.iso</td>
</tr>
</tbody>
</table>
Install MiCollab Server

During the install, if you accidently exit from the server console, you can use Secure Shell (SSH) to access the server console again (see “Accessing the Server Console” on page 136 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 117 for upgrade instructions.

It takes approximately 15 minutes to install the MSL operating system software.

1. Insert the MSL software CD/DVD that you labelled as MSL_10.3.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 10.3.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.

Note: If you are installing the MiCollab Server Appliance, skip this section. The MSL operating system is pre-installed on a MiCollab Server Appliance.
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 51) 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 171 for instructions on how to complete the restore.

**CAUTION:** Before you attempt to perform a restore, review Table 11, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 170 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:
• a "Local" adapter (for LAN mode) or
• a "Local" adaptor AND a "WAN" adapter (for Network Edge mode).

For MiCollab Appliance Server installations, refer to Figure 9 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.

- If you are deploying MiCollab in a Network Edge mode with MiCollab AWV, you must 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.

- 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>
</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 to 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 135.

**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 and then select the **Install MiCollab Software** menu option.

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. The system checks with the Application Management Center (AMC) and presents a list of the MiCollab versions that you can install on the system. This list is obtained from the AMC and is determined by your Application Record ID.

4. Select the MiCollab version that you want to install:
   - Use the up and down keyboard arrows to highlight a version in the list.
   - Select OK.

5. Select the type of ICP that is connected to this MiCollab server: MiVoice Business, MiVoice Office 250, MiVoice 5000, MiVoice MX-ONE. Select OK.
   OR
   Select the type of installation All Applications (for MiVoice Business, MiVoice Office 250, MiVoice 5000, MiVoice MX-ONE) or Subset of Applications (MiVoice Office 250).

6. Proceed to “Install Application Software” on page 61.

**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 server manager, or
- installing the application software from 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. |

**INSTALL APPLICATIONS SOFTWARE FROM SERVER MANAGER**

1. In the server manager, under ServiceLink, click Install Applications.
2. Select the required network element type.
3. Install the application software from the Install Applications panel in the MiCollab server manager. You can choose to install the application software from CD/DVDs, network share, or download software blades from the Application Management Center (AMC). Refer to the Install Applications panel online help for instructions.

| 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. |

4. Proceed to “Configure MiCollab” on page 63.
INSTALLING APPLICATION SOFTWARE FROM CD/DVDS OR USB DEVICE

If you install all the software from CD/DVDs, it takes approximately 20 minutes to copy the full suite of MiCollab application software to the server cache, and approximately 90 minutes to install a full suite of MiCollab applications from cache to the server hard drive. If you install the application software from a USB device the software does not have to be cached, so it takes approximately 90 minutes to install the full suite of MiCollab applications.

WARNING: IF YOU INSTALL THE SOFTWARE FROM A USB DEVICE, DO NOT REMOVE THE DEVICE DURING THE FULL 90 MINUTE INSTALLATION PERIOD. EACH ISO FILE IS INSTALLED DIRECTLY FROM THE USB DEVICE. IF THE USB DEVICE IS ACCIDENTALLY REMOVED BEFORE INSTALLATION IS COMPLETE, YOU MUST RE-INSTALL FROM MSL.

To install the application software:

1. Select the applications that you want to install:
   - Use the up and down keyboard arrows to navigate the list, or press the first letter of an application on the keyboard to highlight it for selection
   - Press the keyboard space bar to select (X) or deselect an application for installation. If your Application Record ID includes NP-UM feature options, these will also be listed.
   - Selected the desired applications and NP-UM feature options.
   - Select OK.

2. The system presents a confirmation screen that lists the applications that you have selected for installation. Select Continue.

3. The "Use USB Storage Device?" screen is displayed.

4. Install the application software from the storage media (CD/DVDs or USB device).

   To install from a USB device:
   - Select Yes. The "Insert USB Storage Devices" screen is displayed.
   - Insert the USB device in the MiCollab Server USB connector and select Scan Devices. Choose the USB stick and select Yes.
   - Select Continue. The system begins installing the software to the server hard drive. DO NOT remove the USB device until the software installation is complete (approximately 90 minutes).
   - Skip to Step 5.

   To install from CD/DVDs:
   - Select No.
   - The system checks with the AMC and displays the required versions (volume labels) of the application installation software. Select Continue.
   - The CD/DVDs must be labelled with the application ISO file name and version. The MiCollab installation checks the CD/DVD content. If the software on CD/DVD does not have correct version, the MiCollab install will not continue until a valid CD/DVD is inserted.
   - Ensure that the CD/DVDs are clean before you insert them in the drive. If the system presents an Input/Output error, you need to clean the CD/DVD.
Install MiCollab Server

- Insert an applications software CD/DVD in the drive. You can copy the CD/DVDs to the server cache in any order.

- Select Continue. The application software is copied from the CD/DVD to the server disk cache. If you insert a CD/DVD with a volume label that does not match the required volume label, an error message is displayed. You must download the correct version of software from Mitel Online and copy it to a CD/DVD in order to install the application.

- When the application is successfully cached, select Next. Insert the next CD/DVD and repeat the process until all the application CD/DVDs have been copied to the server cache.

- After all the specified application software volumes are copied to the server cache, select Next. The server begins installing the software. The screen displays a bar that indicates the progress of the software installation.

5. When the system has finished installing all the application software, the following message is displayed: "Successfully completed application installation". If you installed the application software from a USB device, REMOVE the USB device from the MiCollab server before proceeding.

6. Select Next and you return to the server console menu.

   CAUTION: If you installed the application software from a USB device, ensure that you disconnect it from the server before you reboot.

7. After the application software is installed, reboot the server from the server console Reboot, reconfigure, or shutdown menu. Select the Reboot option, and then click OK and Yes.

   To complete software installation, and to ensure that all services are started, you must reboot the server.

8. After the reboot is complete, proceed to "Configure MiCollab" on page 63.

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

- Internet Explorer 9, 10, or 11
- Mozilla® FireFox® 33 or higher, or
- Google® Chrome™ (version 38 or higher)
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
   - 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
   - https://<IP Address of the MiCollab server or controller>/portal

5. Proceed to “Install Web Certificates” on page 64.

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 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 64).
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 (such as British English, Canadian French, European French, Dutch, Latin American Spanish, German, Swedish, Finnish, or Norwegian):

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 64).
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.

**CONFIGURE PORT 5058 (FOR NON-MIVOICE BUSINESS ONLY)**

If the MiCollab system is connected to a MiVoice Office 250, MiVoice 5000, or MiVoice MX-ONE platform, you must configure port 5058 on the communication platform to support SIP communication from the NuPoint application. The NP-UM application uses port 5058 for SIP communication.

**PERFORM INITIAL CONFIGURATION OF APPLICATIONS**

Proceed to “Initial Configuration” on page 93.

**INSTALL MICOLLAB 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

- 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 version of the MBG application on MiCollab should match the versions of the MBG server software. This will ensure that all features are supported on both servers.
- MiCollab system must be configured with an MBG cluster to allow the data on the MBG cluster to be managed from the MiCollab application.
- The Teleworker application must be installed on the MiCollab server and the MBG servers. The servers should have the same MBG software version.
- 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 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 Business 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.
   - 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 and put the MiCollab server in this 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".
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 node field, select a value to apply to the slave server.

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.
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 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 10 shows an example of a MiCollab Virtual Appliance deployment. Refer to the MiCollab Engineering Guidelines for descriptions of the supported deployments.

![Figure 10: Sample MiCollab Virtual Appliance Deployment](image-url)
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 site 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.

- **Small Business Multi-App (250 users)**
- **Mid-Market Multi-App (1500 users)**
- **Enterprise Multi-App (up to 5000 users)**
- **Enterprise Single-App (up to 5000 users)**

### 4. Application Record ID

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 “About AMC Licensing” on page 19 for more information. Record the generated Application Record ID.

### 5. MiCollab Administrator Password

For password strength, choose a password that contains a mix of uppercase and lowercase letters, numbers, and punctuation characters.

### 6. Domain Name

Names must start with a letter; can contain letters, numbers, and hyphens. For more information, see page 82.

### 7. System Name

### 8. IP address of your vMiCollab system (LAN mode)

The local IP address of the vMiCollab system.

### 9. Gateway IP address

The IP address that vMiCollab will use to access the network.

### 10. MiCollab AWV IP Addresses

If installing the MiCollab AWV application in a MiCollab vApp, obtain two external IP addresses from your Internet Service Provider (ISP). One IP address is required for the MiCollab AWV web server interface that is used to set up audio conferences. A second IP address is required for the MiCollab AWV web service that provides the conference functions, such as file sharing, desktop collaboration, keyboard chat, and so forth.

You configure the two MiCollab AWV IP addresses based on the configuration used. See the MiCollab Engineering Guidelines document for deployment configurations.

### 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 85.

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

### 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.
Before you begin deployment, collect and record the data specified in Table 6. You will need this information in order to successfully deploy the OVA.

**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 6: 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>Administration</td>
<td></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>
<td></td>
</tr>
<tr>
<td>Localization</td>
<td></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>
<td></td>
</tr>
<tr>
<td>Keyboard Type</td>
<td>Identify the preferred keyboard type (default is us)</td>
<td></td>
</tr>
</tbody>
</table>
Installing Virtual MiCollab in a VMware Environment

<table>
<thead>
<tr>
<th>CONFIGURATION ITEMS</th>
<th>FIELD DESCRIPTION</th>
<th>SITE CONFIGURATION DATA</th>
</tr>
</thead>
</table>
| Initial Administrator Password | 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. **Note:** You must enter a password before you deploy the MiCollab UC; otherwise, the system will not boot up. | Initial MiCollab Server manager Administrator Password:  
Final MiCollab server manager Administrator Password:  
**Note:** 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'). |
| Hostname | Set the hostname of the system. | |
| Domain Name (Optional) | Specify the domain name for the hostname above. The default domain name is "mycompany.local". | |
| License Key (Optional) | Identify the License Key (ARID) for this system. The ARID is used by the AMC to distribute the system licenses. | |
| DNS Server IP (Optional) | Record the DNS Server IP Address | |
| Remote Network Addresses for MiCollab Server administration (Optional) | List the Network IP address that is allowed to access the MiCollab server and perform remote administration. | |
| Remote Network Netmask (Optional) | Enter the Netmask associated with the remote network address. | |
| **Network Settings** | | |
| LAN IP Address (IP Address of the vMiCollab) | Record the IP address of the local (LAN) interface. This must be a valid IP address on the local LAN. **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 IP address from vSphere Client. Right-click on the MiCollab and click **Edit Settings.** Click the **Options** tab, click **Properties** and enter the LAN IP Address. | |
| LAN Netmask | Record the Netmask of the LAN | |

Table 6: Collect Custom OVA Template Information
Table 6: 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>WAN IP Address (Optional)</td>
<td>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. <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 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 WAN IP Address.</td>
<td></td>
</tr>
<tr>
<td>WAN Netmask (Optional)</td>
<td>Record the Netmask of the WAN.</td>
<td></td>
</tr>
<tr>
<td>LAN (Optional)</td>
<td>Optional network interface that can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network.</td>
<td></td>
</tr>
<tr>
<td>Default Gateway IP Address</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
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 FOR MIVOICE BUSINESS

1. Log on to Mitel Connect.
2. Click Mitel Online.
3. Click Technical and then click Software Downloads.
4. Click MiCollab.
5. Click the appropriate MiCollab Software Download version.
7. 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.
8. Click the "I Agree [Download using Software Download Manager (Recommended)]".
9. 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.
10. Save the downloaded software ISO images to a folder on your maintenance PC.

SOFTWARE DOWNLOADS WITH MIVOICE MX-ONE

1. Log in to Mitel Connect.
2. Select Knowledge Base.
3. Under Applications, select MiCollab. The Service Advice for the release of MiCollab 7.0 is in section “Service Pack/Advice 2015”.

SOFTWARE DOWNLOADS WITH MIVOICE 5000

1. Log in to Espace France (https://support.mitel.fr).
2. Click **Espace technique**.
3. Click **Produits** then **Logiciel (Products then Software)**
4. Navigate through Applications/MiCollab.
5. Click the download link for your software package.

<table>
<thead>
<tr>
<th>Table 7: Software Download Files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FILE CONTENTS</strong></td>
</tr>
<tr>
<td>vMiCollab Deployments</td>
</tr>
<tr>
<td>NuPoint Unified Messaging option</td>
</tr>
<tr>
<td>Speech Auto Attendant and Text to Speech options</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 7.2.23.0 build) and select **Power On**.
2. Right-click on the MiCollab Virtual Appliance and select **Open Console**.

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 81.

**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>
</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.
- If you are deploying MiCollab in a Network Edge mode with MiCollab AWV, you must 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 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.

- 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>
<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):
  - ***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 85.

**Note:** If you receive an error message when you activate, you may have entered an incorrect network parameter. See "Correcting Activation Errors" on page 135.

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**.
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.

3. The system checks with the Application Management Center (AMC) and presents a list of the MiCollab versions that you can install on the system. This list is obtained from the AMC and is determined by your Application Record ID.

4. Select the MiCollab Suite version that you want to install:
   - Use the up and down keyboard arrows to highlight a version in the list.
   - Select OK.

5. Select the type of ICP that is connected to this MiCollab server: MiVoice Business, MiVoice Office 250, MiVoice 5000, or MiVoice MX-ONE. Select OK. OR Select the type of installation All Applications (for MiVoice Business, MiVoice Office 250, MiVoice 5000, MiVoice MX-ONE) or Subset of Applications (MiVoice Office 250).

6. If you are prompted to install optional NP-UM applications, proceed to “Install Optional Application Software” on page 86. Otherwise, proceed to “Configure vMiCollab” on page 88.

### INSTALL OPTIONAL APPLICATION SOFTWARE

#### INSTALL APPLICATIONS SOFTWARE FROM SERVER MANAGER

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

2. Install the application software from the Install Applications panel in the MiCollab server manager. You can choose to install the application software from CD/DVDs, network share, or download software blades from the Application Management Center (AMC). Refer to the Install Applications panel online help for instructions.

   **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.

3. Proceed to “Configure vMiCollab” on page 88.

### INSTALLING APPLICATION SOFTWARE FROM CD/DVDS OR USB DEVICE

To install optional application software (for example, NP-UM feature options):

1. In the MiCollab Server Console screen, select the applications that you want to install:
- Use the up and down keyboard arrows to navigate the list, or press the first letter of an application on the keyboard to highlight it for selection.
- Press the keyboard space bar to select (X) or deselect a feature option for installation.
- After you have selected the desired feature options, select OK.

2. The system presents a confirmation screen that lists the applications that you have selected for installation. Select Continue.

3. The "Use USB Storage Device?" screen is displayed.
   - To install the optional NP-UM optional software from a USB device, click Yes. The "Insert USB Storage Devices" screen is displayed.
   - To install the software from DVD or a vSphere Datastore.iso file you must select No.

4. In the vSphere Client Application, right-click on the vMiCollab instance (for example: vMiCollab 7.2.3.0 build) and then click Edit Settings. The vMiCollab Virtual Machine Properties window opens.

5. Click the vMiCollab Virtual Hardware tab. You must set the desired method for installing the application software in this screen (Datastore, CD/DVD, or USB stick). Click the Help button for instructions on how to use this screen.

![Figure 13: vMiCollab Virtual Machine Properties Hardware](image)

6. Return to the MiCollab Server Console window and install the software:
- If you are installing from USB stick, insert the USB stick. From the "Insert USB Storage Devices" screen, click **Scan Devices**. The "USB Devices Found" screen displays the USB device. Select **Continue** and follow the console prompts.
- If you are installing from a datastore click **Continue** and follow the console prompts.
- If you are installing from CD/DVDs, click **Continue** and follow the console prompts. Insert the CD/DVDs when instructed to do so.

7. After the system finishes installing all the application software, the following message is displayed: "Successfully completed application installation". **If you installed the application software from a USB device, REMOVE the USB device from the MiCollab server before proceeding.**

8. Select **Next** and you return to the server console menu.

9. After the application software is installed, perform a reboot the server from the server console **Reboot, reconfigure, or shutdown** menu. Select the **Reboot** option, and then click **OK** and **Yes**.

To complete software installation, and to ensure that all services are started, you must reboot the server.

10. After the reboot is complete, disconnect the CD/DVD drive or USB device. To maximize vMiCollab system performance, it is recommended that you disconnect the CD/DVD drive or USB stick from the vMiCollab virtual appliance when they are not required. For example, to remove the CD/DVD drive:
    - In the vSphere Client Application, right-click on the vMiCollab instance (for example: vMiCollab 7.2.3.0 build) and then click **Edit Settings**.
    - Click the **Hardware** tab.
    - Select "CD/DVD Drive 1" in the Hardware list.
    - Under Device Status, clear the **Connected** check box. Ensure that the **Connect at power on** check box is also unchecked.

11. Proceed to “Configure vMiCollab” on page 88.

**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

- Internet Explorer 9, 10, or 11
- Mozilla® FireFox® 33 or higher, or
- Google Chrome (version 38 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:
   - 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. The e-mail contains
   - a link to the My Unified Communications web portal, and
   - the user’s login ID, password, and passcode

   See Configure Welcome 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
   or
   - https://<IP Address of the MiCollab server or controller>/portal

5. Proceed to “Install Web Certificate” on page 89.

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 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 7.2.3.0 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 89).


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 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 (such as British English, Canadian French, European French, Dutch, Latin American Spanish, German, Swedish, Finnish, or Norwegian):

1. Log into the Administrator Portal (see "Log in to the Administrator Portal (Server Manager)" on page 89).

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**.

**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 details regarding language support, see Configure MiCollab Language Settings in the Server Manager online help.

**CONFIGURE PORT 5058 (FOR MIVOICE OFFICE 250 ONLY)**

If the MiCollab system is connected to a MiVoice Office 250 platform, MiVoice 5000, or MiVoice MX-ONE communication platform, you must configure port 5058 on the communication platform to support SIP communication from the NuPoint application.

**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 93.
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>
<thead>
<tr>
<th>Table 8: Site Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STEP</strong></td>
</tr>
<tr>
<td>Site Topology</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Server Details</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>MiCW off line configuration file available?</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
### Table 8: Site Configuration Information

<table>
<thead>
<tr>
<th>STEP</th>
<th>CONFIGURATION INFORMATION</th>
<th>RECORD DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start sharing MiVoice Business and MiCollab databases</td>
<td>Recommended (for MiVoice Business integrations only)</td>
<td>Yes</td>
</tr>
<tr>
<td>(either run MiCW or manually start sharing from a MiVoice Business</td>
<td></td>
<td></td>
</tr>
<tr>
<td>element)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Resiliency</td>
<td>Resilient configuration with MiVoice Businesses required?</td>
<td>Yes</td>
</tr>
<tr>
<td>(MiVoice Business only)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MiCollab Resource Provisioning (Voice Mail - NuPoint)</td>
<td>Hunt Group DN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with 4 ports starting at</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MWI Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HCl Reroute:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HCl Hunt Group extension: 6400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Voice Mail Port:</td>
<td></td>
</tr>
<tr>
<td>MiCollab Resource Provisioning (Speech Auto Attendant)</td>
<td>Record - A - Call licensed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Record-A-Call Hunt Group DN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with 1 port starting at</td>
<td></td>
</tr>
<tr>
<td>MiCollab Resource Provisioning (Mitel Collaboration Advanced)</td>
<td>Hunt Group DN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with 3 ports starting at</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web Conferencing Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administrator Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main Dial In Number</td>
<td></td>
</tr>
<tr>
<td>MiCollab Resource Provisioning (MiCollab AWV)</td>
<td>Hunt Group DN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with 3 ports starting at</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Web Conferencing Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administrator Email</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main Dial In Number</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Toll-Free Dial In Number</td>
<td></td>
</tr>
<tr>
<td>MiCollab Client Integration</td>
<td>Identify required Integration Mode (see “Configure MiCollab Client Mode” on page 97 for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>details)</td>
<td>Integrated?</td>
</tr>
<tr>
<td></td>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Co-located?</td>
<td></td>
</tr>
</tbody>
</table>
Initial Configuration

Table 8: 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>
</tbody>
</table>

Role Name: Associated Template Name

<table>
<thead>
<tr>
<th>Role Name</th>
<th>Associated Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Provisioning Method</th>
<th>Mitel Integrated Config Wizard, Bulk User Import data from file, or Sync AD database with MiCollab. User Import File Type</th>
<th>BUPEXample CSV</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✗ Mitel Integrated Config Wizard, ✗ Bulk User Import data from file, or ✗ Sync AD database with MiCollab. BUPEXample CSV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✗ CSV ✗ LDIF</td>
<td></td>
</tr>
</tbody>
</table>

Filename
File location

Provision MiVoice Business
Advanced Features

<table>
<thead>
<tr>
<th>DID Number Range</th>
<th>MiVoice Business System Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

MiCollab IDS Integration
(See Integrated Directory Services Configuration in the Server Manager online help)

<table>
<thead>
<tr>
<th>Required, or</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Required</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Migration from existing MiVoice Business or MiCollab application IDS integration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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. This mode is only supported for MiCollab with MiVoice Business systems. 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. Integrated Mode is required for sites with MiVoice 5000 or MiVoice MX-ONE communication platforms.

**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)
  - Chinese (Traditional)
  - Italian
  - Portuguese (Brazil)
  - Spanish (European)

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.

For MiCollab Server Deployments:
1. Under Configuration, click MiCollab Client Integration Wizard.
2. Follow the prompts to run the wizard.

For vMiCollab Deployments:
1. Log into the MiCollab server manager.
2. Under Servicelink, click Install Applications.
3. Click the Install Applications tab.
4. Select the PBX type in the panel and click Next. You must set the PBX type in order complete the wizard.
5. Under Configuration, click MiCollab Client Integration Wizard.
6. 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 101 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.

• If you are installing a non-MiVoice Business platform, for example a MiVoice Office 250, MiVoice 5000, or MiVoice MX-ONE, you must configure the platform and application resources manually. Flow Through Provisioning is not supported for non-MiVoice Business platforms. See the MiCollab Platform Integration Guide for instructions.

CONFIGURE USERS AND SERVICES

MIVOICE BUSINESS PLATFORM

• “Configure Flow Through Provisioning” on page 101 (Recommended).

  or

• Manually perform user and services provisioning from the USP application.

  or

• Configure “Configure Integrated Directory Services” on page 112, 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 the MiVoice Office 250 any future user programming on MiCollab must also be manually programmed on the MiVoice Office 250.

6. Configure “Configure Integrated Directory Services” on page 112 if required.

MIVOICE 5000 OR MIVOICE MX-ONE

Refer to the MiCollab Platform Integration Guide for instructions.
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

- Flow Through Provisioning is only supported between MiCollab systems and MiVoice Business platforms.

- MiCollab Release 7.0 or later is required.

- MiVoice Business Release 7.2 or later is required.

- In MiCollab Release 7.0, Flow Through Provisioning is only supported from one MiCollab system. It is not supported for multiple MiCollab systems in the same SDS sharing network.
• If MiCollab is managing a group of MiVoice Business systems, they must be configured in 
a single administration group within an SDS sharing cluster. All the MiVoice Business 
servers in the cluster must be at Release 7.2 or later.

• Flow Through Provisioning must be enabled (started) either from the Mitel Integrated Con-
figuration wizard or manually from a MiVoice Business platform in the administration group 
of the cluster.

CONDITIONS

• Flow Through Provisioning is only supported between MiCollab systems and MiVoice Busi-
ness platforms.

• MiCollab Release 7.0 or later is required.

• MiVoice Business Release 7.2 or later is required.

• MiCollab Client must be configured in integrated mode.

• In MiCollab Release 7.0, Flow Through Provisioning is only supported from one MiCollab 
system. It is not supported for multiple MiCollab systems in the same SDS sharing network.

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

• Flow Through Provisioning must be enabled (started) either from the Mitel Integrated Con-
figuration wizard or manually from a MiVoice Business platform in the administration group 
of 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 Mi-
Voice 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 this 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’.

• 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 appli-
cation 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 223 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 107
- “Greenfield: New MiCollab Server with Multiple New MiVB Servers” on page 109
- “Flow Through Provisioning: Adding Greenfield MiCollab to Brownfield MiVB Servers” on page 191
- “Flow Through Provisioning: Brownfield MiCollab with Brownfield MiVB Servers” on page 213
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](image)

**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 223).

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 177 for detailed instructions on how to run MiCW for this configuration.
4. Proceed to “Configure Users and Services” on page 100.

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.

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

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 223).
   - 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:** MiCollab 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.
5. Configure the MiCollab applications. Refer to the MiCollab application online helps for instructions.

6. Proceed to “Configure Users and Services” on page 100.

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.

**Note:** If the synchronization from MiVoice Business to MiCollab fails, check the error logs on MiCollab in **sdsccl/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.

![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 223).

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 182 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 100.

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 223).
   - 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 `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.

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

9. Proceed to “Configure Users and Services” on page 100.

**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:

- Topmcat - 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 “Performing Backups” on page 130. 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 7.0 software, the system must be at a minimum of MAS Release 5.0 and valid software assurance (SWAS) must be active.

- Upgrade part numbers (PN 54005447 or 54005449) are required to upgrade from MAS 2.2 to MAS 3.0 SP1.
- Upgrade part numbers are not required to upgrade from MAS Release 3.0 SP1 to MAS 5.0.
- Upgrade part numbers are not required to upgrade from MAS Release 5.0 or above to MiCollab Release 7.0.

**Note:** MAS 3.0 SP1 and later servers require a minimum of 6 GB of RAM to run all supported applications. MAS 2.2 Servers require minimum of 4 GB of RAM. However, you can upgrade a MAS 2.2 Server to a higher software release and run the system with 4 GB of RAM if you do not install the MiCollab Client application. Before you can install MiCollab Client, your MiCollab Server must have a minimum of 6 GB of RAM.

Table 9 identifies the supported upgrades and the required procedures.

<table>
<thead>
<tr>
<th>SUPPORTED UPGRADES</th>
<th>UPGRADE PROCEDURES</th>
<th>WHEN TO USE</th>
</tr>
</thead>
</table>
| MAS 2.2 to MAS 3.0 SP1           | To upgrade from MAS 2.2 to 3.0 SP1 software, you must apply one of the following part numbers to your ARID:  
• MAS Server 2.2 to 3.0 SP1 - PN 54005447  
• vMAS 2.2 to vMAS 3.0 SP1 - PN 54005449 | You must upgrade to MAS 3.0 SP1 before you can upgrade to MAS 5.0. Refer to the Maintenance chapter in the MiCollab Release 4.0 Installation and Maintenance Guide for instructions on how to upgrade from MAS 2.2 to MAS 3.0 SP1. |
| MAS Server 3.0 SP1 or later to MAS Server 5.0 | You must install the MSL operating system (you cannot use the Upgrade option) and then upgrade MAS Applications from AMC (page 118). | You install the MSL 10.0 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. |
| MAS Server 5.0 or later to MiCollab Server 7.0 | Perform a backup and restore with fresh install | "Upgrade from MAS 5.0 or later to MiCollab 7.0 using Fresh Install" on page 118. |
| vMAS 5.0 or later to vMiCollab 7.0 | Deploy vMiCollab 7.0 OVA file and restore vMAS 5.0 or higher backup (page 122) | 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. |
UPGRADE FROM MAS 5.0 OR LATER TO MICOLLAB 7.0 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 7.0, 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 11 and Table 12 on page 170 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 130).
- You have verified your MAS 4.0 or later backup file (see “Verify Backup Data” on page 135 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.)
☑ UCC User Business Licenses have been converted to UCC User Enterprise licenses. See "Trusted Service Support" on page 36.

BACKUP AND RESTORE WITH FRESH INSTALL

1. Purchase the required MiCollab upgrade licenses and upgrade your AMC account. Refer to the latest MiCollab Release 7.x product bulletin on Mitel Online for details. To access the MiCollab product bulletin:
   - Log into Mitel Online
   - Under Products, click MiCollab.
   - Under Related Links, click MiCollab Product Bulletins.

2. Download the ISO files of the latest MSL software and the MiCollab application software. Follow the instructions on page 52.

3. Transfer the ISO files to storage media (CD/DVDs or USB). See “Create Storage Media” on page 53.

4. Back up your existing MiCollab system database. See “Performing Backups” on page 130.

5. If you plan to use an existing backup file, verify it before performing the new installation (see “Verify Backup Data” on page 135).

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_10.3.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.

Note: If you are installing the upgrade on a new hardware platform, you must clear the MiCollab address of the old server platform by stepping through all the screens without changing any options. Then select Save to clear the MiCollab address of the old server platform.

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 10.3.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 10.3.x.x. system, if the current system is at MSL 10.3.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 128.

- **Note:** If you are restoring the database to new server hardware or to a server that has a different MAC address for eth0, the MSL system may present a red warning error message: "ignoring eth0 due to unexpected MAC address". The server will not have network connectivity at this point. In order to proceed, you must log into the server console as administrator, select **Configure this server** menu option, step through all the pages without making any changes, and allow the server to reboot.

19. When the restore is complete, remove the USB device or CD/DVD storage media.

20. 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 **Sync**.
   - Enter your Application Record ID and click **Activate**.

21. Log into the server console and upgrade the MiCollab applications.

22. 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 97 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 142 for requirements and instructions.

23. 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.

24. 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.

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

WARNING: AFTER YOU UPGRADE TO MICOLLAB RELEASE 7.0, YOU CANNOT RESTORE A BACKUP FROM A PRE-RELEASE 7.0 SYSTEM, SO IT IS CRITICAL THAT YOU MAKE A BACKUP NOW.

26. If the MiCollab system is connected to MiVoice Office 250 platform(s), you must configure port 5058 on the MiVoice Office(s) to support SIP communication from the NuPoint application. For MiCollab Server and vMAS Release 4.0 SP1 and later, the NP-UM application uses port 5058 for SIP communication.

27. If you upgraded to MiCollab Release 7.0 with MiVoice Business Release 7.2, the UCC V3 Entry licenses are converted to UCC V4 Entry licenses. The UCC V4 Entry licenses have a Multi-Device User Group instead of an IP User license and external hot desk license. If you are upgrading a MiCollab with a MiVoice Business site, you may receive a licensing violation error on the MiVoice Business, because the system will have more IP user licenses allocated than were purchased.
   - Log into the MiVoice Business system, access the Licensing and Option Selection form.
   - Set the Locally Allocated field for the IP Users to the number of purchased licenses.
   - Set the Locally Allocated field for the Multi-Device Users to the number of purchased licenses.
   - Click Save.
   - Click OK to the licensing messages. The licensing violation error is cleared.
28. 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 213 for instructions.

UPGRADE FROM VMAS 5.0 OR LATER TO VMICOLLAB 7.0

UPGRADE PREREQUISITES

- Ensure that the virtual machine has the required resources (see the Virtual Appliance Deployment Guide).
- To upgrade to MiCollab Release 7.0, your current system must be running Release 5.0 or later and valid software assurance (SWAS) must be active.
- UCC User Business Licenses have been converted to UCC User Enterprise licenses. See “Trusted Service Support” on page 36.

DEPLOY VMICOLLAB 7.0 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. For example: 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.

1. Download the vMiCollab 7.0.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 80 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 134 for instructions).
3. Deploy the vMiCollab 7.0 OVA file on the host system (see page 80 for instructions).

**Note:** If you are upgrading from MAS Release 5.0 to MiCollab Release 6.0 or later, ensure that you select the correct deployment configuration for the site. In MAS Release 5.0, the Enterprise configuration supported up to 1500 users. With MiCollab Release 6.0 or later, select the Mid-market configuration for a site up to 1500 users.

**Note:** To support a large Enterprise (2500 or 5000-user multi-application capacity or 5000-user single application capacity) you must manually increase the VMware resources for the MiCollab virtual machine. Deploy the OVA using the "Enterprise" configuration. Before you power up the virtual machine, edit the virtual machine settings and increase the Virtual Hardware resources to the requirements that are specified in the Virtual Appliance Deployment Guide.

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 MSL completes the restore, select Reboot.

8. After the vMiCollab vApp has rebooted, log into the server console by entering the MiCollab login name and password:
   - Login: admin
   - Password: (as programmed during the MSL installation)

9. In the server console Welcome menu, use the up and down keyboard arrows to select Install MiCollab Software and then select Next.

10. The "Use USB Storage Device?" screen is displayed.
    - To install the optional NP-UM optional software from a USB device, click Yes. The "Insert USB Storage Devices" screen is displayed.
    - To install the software from DVD or a vSphere Datastore.iso file you must select No.

11. The MiCollab Server Console screen lists the lists the applications that will be installed. Select Continue.

12. In the vSphere Client Application, right-click on the vMiCollab instance (for example: vMiCollab 7.2.3.0 build) and then click Edit Settings. The vMiCollab Virtual Machine Properties window opens.

13. Click the vMiCollab Virtual Machine Properties Hardware tab. You must set the desired method for installing the application software in this screen (Datastore, CD/DVD, or USB stick). Click the Help button for instructions on how to use this screen.

14. Return to the MiCollab Server Console window and install the software:
    - If you are installing from USB stick, insert the USB stick. From the "Insert USB Storage Devices" screen, click Scan Devices. The "USB Devices Found" screen displays the USB device. Select Continue and follow the console prompts.
    - If you are installing from a datastore click Continue and follow the console prompts.
    - If you are installing from CD/DVDs, click Continue and follow the console prompts. Insert the CD/DVDs when instructed to do so. If using multiple disks, you must disconnect from the first disk and mount the next disk.

15. After the system finishes installing all the application software, the following message is displayed: "Successfully completed application installation". If you installed the application software from a USB device, REMOVE the USB device from the MiCollab server before proceeding.

16. Select Next and you return to the server console menu.
17. After the application software is installed, perform a reboot the server from the server console Reboot, reconfigure, or shutdown menu. Select the Reboot option, and then click OK and Yes.

To complete software installation, and to ensure that all services are started, you must reboot the server.

18. After the reboot is complete, disconnect the CD/DVD drive or USB device. To maximize vMiCollab system performance, it is recommended that you disconnect the CD/DVD drive or USB stick from the vMiCollab virtual appliance when they are not required. For example, to remove the CD/DVD drive:

- In the vSphere Client Application, right-click on the vMiCollab instance (for example: vMiCollab 7.2.3.0 build) and then click Edit Settings.
- Click the Hardware tab.
- Select "CD/DVD Drive 1" in the Hardware list.
- Under Device Status, clear the Connected check box. Ensure that the Connect at power on check box is also unchecked.

19. 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 97 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 142 for requirements and instructions.

20. 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.

21. 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.

22. 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**.

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

**WARNING:** AFTER YOU UPGRADE TO MICOLLAB RELEASE 7.0, YOU CANNOT RESTORE A BACKUP FROM A PRE-RELEASE 7.0 SYSTEM, SO IT IS CRITICAL THAT YOU MAKE A BACKUP NOW.

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

25. If you upgraded to MiCollab Release 7.0 with MiVoice Business Release 7.2, the UCC V3 Entry licenses are converted to UCC V4 Entry licenses. The UCC V4 Entry licenses have a Multi-Device User Group instead of an IP User license and external hot desk license. If you are upgrading a MiCollab with a MiVoice Business site, you may receive a licensing violation error on the MiVoice Business, because the system will have more IP user licenses allocated than were purchased.
   - Log into the MiVoice Business system, access the **Licensing and Option Selection** form.
   - Set the Locally Allocated field for the IP Users to the number of purchased licenses.
   - Set the Locally Allocated field for the Multi-Device Users to the number of purchased licenses.
   - Click **Save**.
   - Click **OK** to the licensing messages. The licensing violation error is cleared.

26. If you are upgrading a MiCollab with a 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 213 for instructions.
UPGRADE FROM MICOLLAB 7.X TO MICOLLAB 7.Y

Use this procedure to upgrade within the same release (for example, from MiCollab 7.0 to 7.1). After MSL is at Release 10.3, you can use this procedure to upgrade MSL and the MiCollab applications from the AMC.

Note: This procedure applies to both MiCollab Server and vMiCollab platforms.

Note: If you want to upgrade a vMiCollab system by re-deploying OVA file, do not use this procedure. Instead, refer to “Deploy vMiCollab 7.0 OVA File and Restore Backup” on page 122 for instructions.

The following conditions apply:

- MSL operating system must be at Release 10.3 or later.
- If the MSL version of the upgrade is greater than the installed version, you must upgrade MSL. For MiCollab Server deployments, you have the choice of upgrading MSL from the MSL ServiceLink (as documented in the procedure below) or from the MSL CD. To upgrade MSL using a CD, you would
  - Insert the MSL CD
  - Reboot MiCollab
  - Upgrade MSL as per upgrade procedures.
  - Reboot MiCollab. Then, complete the “To install a software upgrade within the same release” procedure given below.
- All application versions that comprise a MiCollab software upgrade must be installed (that is, you cannot install an upgrade for just a specific application).
- You will need to insert the MSL CD/DVD during the install.
- Software upgrades for all applications, with the exception of the NP-UM options, SAA-TTS applications, are downloaded from the Mitel AMC. You must download the NP-UM options, and SAA-TTS application upgrades from Mitel Online and copy them to DVDs.
- During a software upgrade, the MiCollab tomcat server restarts. The restart takes approximately 5 minutes. While the restart is in progress, the Administrator portal and MiCollab End User portal interfaces do not function. The following error message is displayed on these interfaces during the restart: "The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later."

To install a software upgrade within the same release

1. For vMiCollab deployments, export the vMiCollab OVA file from vSphere Client before you start the update. Then, if you encounter issues, you can import the OVA file to restore the system.
2. Access the server console Welcome menu (page 136).
3. Use the up and down keyboard arrows to select Upgrade MiCollab Software and then select Next. The system connects to the AMC and checks for updates. The MiCollab application versions to which you can update your applications are listed in the display.
4. After you select a newer MiCollab version and select **OK**, the console lists the applications that will be updated.

**Note:** If updates are not required the console screen displays: "There are no applications to be updated". Click **OK** to return to the server console Welcome menu.

5. Select **Continue**.

6. The "Use USB storage device?" screen is displayed.
   - To install from USB, select **Yes**. The "Insert USB Storage Devices" screen is displayed. Insert the USB device and select **Scan Devices**. The system detects and displays the connected USB device. Select **Yes**.
   - To install from DVD, click **No** and follow the console prompts.

7. The screen displays a list of the applications that will be updated. Select **Continue**.

8. The system begins downloading the updates from the AMC. A progress bar at the bottom of the screen indicates the percent complete.
   - If a MSL Servicelink upgrade is required, the system will prompt you to insert the MSL software CD/DVD.
   - If a NP-UM or SAA-TTS upgrade is required, the system will prompt you to insert the storage media.

9. When the applications are downloaded, the screen displays "Successfully downloaded the required application software from blades.mitel-amc.com." and the updated applications are listed.

10. Select **Next**. The system begins upgrading the applications. A progress bar appears on the screen. When the system has finished installing the software updates, the following message is displayed "Successfully completed application installation."

11. Click **Next** to return to the server console menu.

12. Reboot the server.

**UPGRADE FROM MICOLLAB 7.0 TO MICOLLAB 7.0 SPX**

You can perform service pack upgrades from the MiCollab server manager **Install and Upgrade Software** panel. Refer to the online help for instructions.

**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 add applications that you did not select for installation during the initial install using either of the following methods:

- add application from server manager, or
- add application from server console.

**ADD APPLICATION FROM SERVER MANAGER**

1. Log into MiCollab server manager.

2. Under **ServiceLink** click **Install and Upgrade Applications**.

3. Click **Update List** to retrieve the latest list of available blades from the Mitel Application Management Center (AMC).

4. Scroll through the list and locate the blade for the feature that you are adding to the system.

5. Do one of the following:
   - To install a new blade immediately, click the **Install** link beside it.
   - To download a blade for installation at a later time, click the **Cache** link beside it.
     Complete the installation process by clicking the **Install** link.

6. Installing a blade creates new menu items in the navigation menu to allow you to administer the blade.

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

8. 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.

**ADD APPLICATION FROM SERVER CONSOLE**

1. Download the application software and burn the ISO images to a CD/DVD or copy to a USB stick.

2. Access the server console Welcome menu (see page 136).

3. Select **Install MiCollab Applications**.
4. Select the applications that you want to install:
   - Use the up and down keyboard arrows to navigate the list, or press the first letter of an application on the keyboard to highlight it for selection
   - Press the keyboard space bar to select (X) or deselect an application for installation. If your Application Record ID includes NP-UM feature options, these will also be listed.
   - After you have selected the desired applications and NP-UM feature options, select OK.

5. The system presents a confirmation screen that lists the applications that you have selected for installation. Select Continue.

6. The "Use USB Storage Device?" screen is displayed.

7. Install the application software from the storage media (USB stick or CD/DVDs).
   To install from USB stick
   - Select Yes. The "Insert USB Storage Devices" screen is displayed.
   - Insert the USB stick in the MiCollab Server USB connector and select Scan Devices. The system detects and displays the connected USB device. Select Yes. The system lists the applications that will be installed.
   - Select Continue. The system begins installing the software to the server hard drive. DO NOT remove the USB device until the software installation is complete (approximately 90 minutes).
   - Skip to Step 8.
   To install from CD/DVDs
   - Insert the applications software CD/DVD. Select Continue. The application software is copied from the CD/DVD to the server disk cache.
   **CAUTION:** If you select Cancel, you will need to start the application installation over again. However, the system retains any application software that was fully cached on the hard disk and the time required to complete the installation will be reduced.
   - Select Next. Insert the next CD/DVD and repeat the process until all the application CD/DVDs have been copied to the server cache.
   - After the system has copied all the application software to the server cache, the screen displays "Successfully cached the required application software from CD/DVD <volume label>". Select Next. The system begins installing the application software.

8. After the application software is installed, the screen displays "Successfully completed application installation". **If you installed the application software from a USB stick, REMOVE the USB stick from the MiCollab server before proceeding.**

9. Select Next to return to the server console menu.
   **CAUTION:** If you installed the application software from a USB stick, ensure that you disconnect it from the server before you reboot.

10. Reboot the server using server console option Reboot, reconfigure, or shutdown.

11. Update your MiCollab user templates in the Users and Services provisioning of the MiCollab server manager to include the new services.
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.

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 .tgz.
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 64 for instructions.
2. Under Administration, click Backup.
3. Select the Backup to desktop option.
4. Click Perform. MSL prepares the system for backup. The "Backup to desktop - Operation status report" screen is displayed with the estimated backup size.
5. Ensure that your browser and target file system support downloads of this size and then click Begin Download.
6. When prompted to Open or Save, click Save.
7. 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.

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.

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 7:

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. Click **Save**.

### 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. Optionally, 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. Click **Save**. When a valid configuration is entered, the **Backup Now** button appears.
6. Click **Backup Now** or configure a backup schedule and click **Save**.
7. 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.

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 136).
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 .tgz extension is automatically added.
4. MSL displays an estimate of the size of your backup. Click **Proceed**.
5. When the backup is complete, you are prompted to remove the USB storage device.
6. 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 135.

**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 136).
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 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 136).
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 63).

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 61, 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 64).


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 147, 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 156</td>
</tr>
<tr>
<td>NuPoint Unified Messaging</td>
<td>“Troubleshooting Applications” on page 156</td>
</tr>
<tr>
<td>MiVoice Border Gateway</td>
<td>“MiVoice Border Gateway” on page 163</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 3.0 SP1 or later database to a MiCollab Virtual Appliance (vMiCollab) Release 7.0 or later system
- Migrate a standalone MiCollab Client database to a MiCollab Server or MiCollab Virtual Appliance Release 7.0 or later 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 7.0 or later deployment using the Restore option in the server console.

CAUTION: Before you attempt to perform the conversion, review Table 11, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 170 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 7.0 or later 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 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 11, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 170 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 80 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 80.
- 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 130 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 135 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 6.3.1.0 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 MSL completes the restore, select Reboot. 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.

8. After the vMiCollab vApp has powered up, log into the server console by entering the MiCollab login name and password:
   - Login: admin
   - Password: (as programmed during the MSL installation in the backup database)
9. Select **Configure this server** from the server console menu.
   - Step through all the screens and review your settings.
   - If the new vMiCollab system requires a different IP address than the previous MiCollab Server system, enter the new IP address when prompted.
   - Select **Reboot the system**.

10. Next, install the optional NP-UM applications if required. See “Install Optional Application Software” on page 86.

11. After the optional software is installed and the system has rebooted, log into the server manager and 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 7.0 or vMiCollab Release 7.0 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 7.0 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 MiCollab 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 7.0 Add-on to MiCollab Client" part number.
- MiCollab Client user licenses are transferred from the MiCollab Client standalone system to the MiCollab 7.0 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 7.0 Add-on to MiCollab Client - PN 54005444
  - vMiCollab 7.0 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 131 for instructions.
2. Shut down the MiCollab Client server.
3. Install MiCollab Release 7.0 software:
   - Install MiCollab Server (page 45). During the installation of the MSL 10.3 operating system, you must choose the Install MiCollab Software option
   - Install vMiCollab (page 71). 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 64 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:
    - On Windows XP, open the Control Panel, click Add/Remove Programs, click Mitel MiCollab Client, and then click Change/Remove.
    - On Windows 7 or Windows 8, 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 97 for instructions.

UPGRADING USERS WITH UCC V1 LICENSES TO UCC V4.0 OR LATER LICENSES

The User Bundle Analysis Tool (UBAT) script allows you to
- identify users who are assigned UCC V1 licenses, and
- upgrade the UCC V1 users to UCC V4.0 or later licenses

UBAT SCRIPT USAGE

/usr/mas/bin/ubat.sh [-c][-e <export file>] [-i <import file>] [-q <where's them SQL scripts at>] [-r <report file>] [-v]

- c Remove any intermediate tables created. Do this only after you have imported.
- e Export user bundles info to a CSV file. Specify the output file.
- i Import user bundles info from a CSV file. Specify the file name.
- q Directory where the needed SQL scripts can be found. Default is .
- r Report file containing result of import.
- v Verbosity on

OVERVIEW OF PROCEDURE

To upgrade users who are assigned with UCC V1 licenses to UCC V4.0 or later licenses, you must
- Export and analyze a CSV file of the current system license usage
- Review the CSV file and modify the licenses as required
- Import the modified CSV file
EXPORT AND ANALYZE A CSV FILE OF CURRENT LICENSING

1. Log into the MiCollab server console as root.
   
   login: root
   password: ******

2. At the command prompt, enter the following command:
   
   [root@mivtesting ~] ubat -e <filename>
   
   The system exports a CSV file of all users on the system to the following location:
   
   /var/tmp/<filename>
   
   A summary of the user licensing is displayed.

3. Download the file from the server to your laptop or a network drive using a utility, such as WinSCP. WinSCP is an open source free SFTP client and FTP client for Windows. Its main function is the secure file transfer between local and remote computer.

REVIEW AND MODIFY CSV FILE

1. Open the CSV file in a spreadsheet program (for example, Excel) and review the contents. The file lists all the users on the system, their licensing bundle (if any) and the services assigned to each user.

2. Review the file to determine which users require their licenses upgraded. Ensure that you have the required number of licenses available on the system.

3. Edit the CSV file in Excel. Change the licensing bundles for the users as required and save the file.

IMPORT CSV FILE

1. Copy the modified CSV back to the /var/tmp directory on the MiCollab server:

2. Enter the following command to import your changes:

   ubat -i <filename>
   
   The system displays a summary of the user licensing. If listed correctly, enter Y to proceed. The licensing bundles specified in the import file are applied to the system.

3. Enter Y to clean up the temporary files.
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 65 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 65 |
| 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 “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/per15/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 “Your call will be transferred to an operator.” 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: “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></td>
<td></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>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 128. Then repeat the application installation procedure. See “Installing Additional (Missing) Applications” on page 128.</td>
</tr>
</tbody>
</table>
| When performing a restore, you get the following error message:          | 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). | 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. |
| “Error preparing for system restore”                                      |                                                                                |                                                                                  |
| During a software update using the MSL text console "Update Mitel Application Software". The display only indicates that NuPoint needs to be installed. You cannot proceed with the software updates. | 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. | 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 128. Then repeat the software update installation procedure. See “Performing Backups” on page 130. |
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)
ERT: Failed To Get Error Log Address Range

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

MiVoice Conference Unit is not functioning correctly.

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| Server is not running a compatible firmware version for the MiCollab system. | 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 57 for details). | |

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.

<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>
### Troubleshooting

#### FLOW THROUGH PROVISIONING TROUBLESHOOTING

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</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** | | |
| **SYMPTOM** | **POSSIBLE CAUSE** | **CORRECTIVE ACTION** |
| The **Start Sharing** operation fails with a message to check the MiCollab logs. | 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. | Configure all MiVoice Business elements in the sharing network are configured with either an IP address or FQDN. Then perform the **Start Sharing** operation. |
| Flow Thorough Provisining updates that you make to users on the MiVB are not being updated in the MiCollab database. | The update has not been applied yet. | Wait approximately 2 minutes. The system can take several minutes before the updates are applied. |
| Unable to Reach Through to MiVoice Business | MiVoice Business "system" administrator account is not configured | Reach through is enabled from MiCollab USP to the MiVoice Business (MiVB) system administration tool using the MiVoice Business "system" administrator account. Configure an administrator account in the User Authorization Profiles form with Login ID "system" and System Admin authorization set to "True". |
| During a Start Sharing operation you receive an error messaging indicated that Synchronization Failed. | One or more MiVoice Business forms are shared at the wrong scope. | Access the MiVoice Business SDS Form Sharing form and set the correct scopes. See “Supported Sharing Scopes” on page 225. |
| 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. |
## 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>
<tr>
<td>After importing (restoring) an vMiCollab OVF template backup file, system performance and voice quality is poor.</td>
<td>Network adapter type is set incorrectly. After a importing an OVF template file, the network adapter type is reset to default. The network adapter must be reset to type VMXNET3.</td>
<td>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 &quot;Adapter type&quot; drop-down menu, select MXNET3. 6. Click Next and then click OK.</td>
</tr>
<tr>
<td>Voice quality issues</td>
<td>vMiCollab is installed in the vSphere environment using Thin provisioning. Thin provisioning can cause voice quality issues due to disk sharing.</td>
<td>Reinstall vMiCollab and select Thick provisioning during the install wizard.</td>
</tr>
<tr>
<td>VMware environment is not configured with the required resources.</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
## Troubleshooting

vMiCollab features not working as expected

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| vMiCollab features not working as expected | Invalid license. You have installed MiCollab on a virtual machine, but you do not have a virtualization license. In the Server Manager, click the **Licensing Information** page. If your license is invalid a red warning message will appear near the top of the web page. | 1. Contact your authorized Reseller to purchase a virtualization license and obtain a Application Record ID.  
2. In your AMC account, access the appropriate Application Record and assign the license.  
3. Log into the Server Manager.  
4. Under **ServiceLink**, click **Status**.  
5. Click **Sync**. |
# 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.</td>
<td>Mitel Integrated Configuration Wizard was run against MiVoice Business and MiCollab in separate sessions.</td>
<td>1. Log into the MiCollab server manager and configure a SIP Password in the MiCollab AWV SIP Server Configuration page.</td>
</tr>
<tr>
<td>Logs similar to the following are being constantly generated on the MiVoice Business:</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>5 INFO 2015/05/07 16:45:43 MOBILITY General Maintenance(0) Hot Desk : 6851 unlocked by DISA TIMER timeout</td>
<td>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>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>
<tr>
<td>6 INFO 2015/05/07 16:45:43 MOBILITY General Maintenance(0) Hot Desk : 6852 unlocked by DISA TIMER timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7 INFO 2015/05/07 16:45:43 MOBILITY General Maintenance(0) Hot Desk : 6853 unlocked by DISA TIMER timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8 WARNING 2015/05/07 16:46:13 SSP General Maintenance(0) Temporary Lockout of SIP Registration for sip:6851@10.46.33.62/sip:6851@10.46.33.62 due to 932 '403 Authentication Failures'. Failed Connection was just attempted by SrcIP[10.46.33.68:6064<a href="http://10.46.33.68:6064">http://10.46.33.68:6064</a>], ViaIP[10.46.33.68:6064<a href="http://10.46.33.68:6064">http://10.46.33.68:6064</a>], ContactIP[10.46.33.68:6064<a href="http://10.46.33.68:6064">http://10.46.33.68:6064</a>]</td>
<td>1. Log into the MiCollab server manager and configure a SIP Password in the MiCollab AWV SIP Server Configuration page.</td>
<td></td>
</tr>
</tbody>
</table>
User receives the following error message when upgrading MiCollab AWV client:

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User receives the following error message when upgrading MiCollab AWV client:</td>
<td>The executable could not be downloaded from server to the PC in https url mode.</td>
<td>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.</td>
</tr>
<tr>
<td>1. From the user's PC, do Winscp to the server ip as root. <strong>Note:</strong> If the server ip cannot be FTPed, then download from the server and copy it to the PC by other means.</td>
<td>2. Go to /usr/awc/connpoint/content.</td>
<td>3. Download the MCAClient.msi to local directory.</td>
</tr>
<tr>
<td>1. From the user’s PC, do Winscp to the server ip as root. <strong>Note:</strong> If the server ip cannot be FTPed, then download from the server and copy it to the PC by other means.</td>
<td>2. Go to /usr/awc/connpoint/content.</td>
<td>3. Download the MCAClient.msi to local directory.</td>
</tr>
<tr>
<td>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. <strong>Note:</strong> To run the msi as admin, download the MCAClient-admin.exe file instead of the MCAClient.msi in step 3.</td>
<td>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. <strong>Note:</strong> To run the msi as admin, download the MCAClient-admin.exe file instead of the MCAClient.msi in step 3.</td>
<td></td>
</tr>
<tr>
<td>5. Verify the new client is installed on the user's PC.</td>
<td>5. Verify the new client is installed on the user's PC.</td>
<td></td>
</tr>
<tr>
<td>SYMPTOM</td>
<td>POSSIBLE CAUSE</td>
<td>CORRECTIVE ACTION</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</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
## Troubleshooting

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>End users are unable to log into MiCollab AWV conferences.</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Some characters in the e-mail invitation do not display correctly for all languages.</td>
<td>The user has Outlook 2003 or settings are not configured in Outlook 2007 and 2010 to convert the characters correctly.</td>
<td>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.</td>
</tr>
<tr>
<td>The Mitel Conferencing tab in Outlook does not retain the server URL and user password.</td>
<td>Windows 7 includes enhancements to security that require Administrator privileges to write to the folder where the OFT information is saved.</td>
<td>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.</td>
</tr>
<tr>
<td>When trying to log on by typing the user name and password the screen returns to the log on page.</td>
<td>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.</td>
<td>Make sure the cookie and username/password use the same case.</td>
</tr>
<tr>
<td>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.</td>
<td>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.</td>
<td>Make sure the cookie uses the entire URL.</td>
</tr>
<tr>
<td>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.</td>
<td>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 (IE or Firefox vs Chrome). For example, Spanish version of Windows is required for specified buttons/popups to be displayed in Spanish.</td>
<td>Use the correct language version of Windows to see those prompts displayed in the selected MiCollab Audio, Web and Video Conferencing language.</td>
</tr>
<tr>
<td>A “Connection to Server not complete” message is displayed when attempting to join a Web conference.</td>
<td>After performing an upgrade for the MiCollab Audio, Web and Video Conferencing blade, Web conferencing may not fully restart.</td>
<td>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.</td>
</tr>
<tr>
<td>SYMPTOM</td>
<td>POSSIBLE CAUSE</td>
<td>CORRECTIVE ACTION</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| 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 key sections (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. |
| 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. | The installation makes the form available, but the install does not force a new tab to appear in Outlook. | 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  
--> "Tools" Menu  
--> "Forms" Option  
--> "Choose Form" Option  
--> Look in "Calendar"  
--> Select "Collaborate"  
When you choose "Collaborate," it replaces your "Web Conferencing" appointment form/tab. |
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>
<tr>
<td></td>
<td></td>
<td><strong>DAS Rules</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>DAS Rule 1</strong> <code>\(\text{\textbf{5/10/1602.}}\text{\textbf{.}}\text{\textbf{9/31@primary internal IP address}}}\)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>DAS Rule 2</strong> <code>\(\text{\textbf{5/10/16480.}}\text{\textbf{.}}\text{\textbf{9/31@primary internal IP address}}}\)</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<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>
</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>
<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</td>
<td>“Enterprise alert” Message = “only %d ports are currently unused at %s”, 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 10: 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>

---

### MVOICE BORDER GATEWAY

#### SYMPTOM

<table>
<thead>
<tr>
<th>TELEWORKER USERS ARE EXPERIENCING ONE-WAY AUDIO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POSSIBLE CAUSE</strong></td>
</tr>
</tbody>
</table>
| You have logged into the MiCollab server manager and changed the MiCollab system IP address. After the system reboots all applications except Teleworker are functioning correctly. Teleworker users are experiencing one-way audio. | You must sync the MiCollab system with the AMC to fix this issue:  
1. Log into the MiCollab Server Manager.  
2. Under **ServiceLink**, click **Status**.  
3. Click **Sync**.  
4. Under **Applications**, click **Remote Teleworker Solution**.  
5. Click the Advanced tab.  
6. Ensure the new MiCollab system IP address is displayed in the "RTP Icpside Address Override Default" field.  
7. Click the Dashboard tab and start Teleworker service.  
8. Click the Clustering tab.  
9. Click Join to rejoin the cluster. |

#### SIP TELEWORKER DEVICES ARE NOT FUNCTIONING

<table>
<thead>
<tr>
<th><strong>SIP TELEWORKER DEVICES ARE NOT FUNCTIONING</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POSSIBLE CAUSE</strong></td>
</tr>
</tbody>
</table>
| 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. |
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 with a weight of zero</td>
<td>MiCollab server is configured in LAN mode with the Teleworker application, but it is not clustered with a MiVoice Border Gateway (MGB)</td>
<td>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 be clustered with one MBG server. The cluster must be programmed in the Teleworker Clustering tab with a weight of zero. See “Upgrade from vMAS 5.0 or later to vMiCollab 7.0” on page 122</td>
</tr>
</tbody>
</table>
### NP-UM TROUBLESHOOTING

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>After upgrading to MAS Release 4.0 SP1 or later, users on MiVoice Office 250 are unable to call into their NP-UM voice mailboxes.</td>
<td>Port 5058 on the MiVoice Office 250 is not configured to support SIP communication from the NuPoint application.</td>
<td>Configure port 5058 on the MiVoice Office 250(s) to support SIP communication from the NuPoint application.</td>
</tr>
<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>
</tbody>
</table>
| Message Waiting Indication lamps on MiVoice Business system phones turn off before users have listened to their voice messages. | 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. | 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. |
| Clicking a NP-UM voice message in the MiCollab End User portal results in a blank screen with an icon indicating "applet not found" | Windows Media Player is not selected as the default player                   | Set Windows Media Player to be your default player:  
  1. Close Internet Explorer  
  2. Right-click in Windows Explorer.  
  3. Click **Tools** and then click **Folder Options**  
  4. On the File Types tab, scroll to WAV files  
  5. Click **Change** and select **Windows Media Player** from the list  
  6. Click OK  
  7. Open Windows Media Player  
  8. Click **Tools** and then **Options**. (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 **OK** |
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 functioning correctly</td>
<td>Browser incompatibility</td>
<td>Ensure that you are running the applications in a recent version of Google Chrome.</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 Calendar or the internet browser before the new event was added to AWV.</td>
<td>Delete the event from Google Calendar and then re-create it.</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. Therefore, during a data restore or upgrade, the configuration settings are not maintained.</td>
<td>Re-enter the configuration settings in the MiCollab server manager under Configuration&gt;Google Apps</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>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>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>01211</td>
<td>This application record already has a base service level product attached. Multiple base kits not allowed</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>
</tbody>
</table>
TROUBLESHOOTING UCC LICENSING UPGRADES

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.

5. Update each user's services from the User and Services application.

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 11: 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 12: 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 136.
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. A progress bar is displayed for the restore procedure. When the restore is complete, the server reboots to activate your restored configuration settings.
13. Proceed to “Check Application Data” on page 173.

RESTORE FROM REMOVABLE DEVICE

1. Follow the prompts to identify the backup file, and start the database backup. 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.

2. 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%.
3. Proceed to “Check Application Data” on page 173.

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 128 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 synch.

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 for instructions.

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 7.0 server, or a
- MiCollab 7.0 database to a MiCollab 7.0 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 130 for instructions.

2. Clear your Hardware ID from the AMC. See “Backup and Restore with Fresh Install” on page 119 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.
- 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 6 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 MICOllLAB 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. * Denotes required fields

<table>
<thead>
<tr>
<th>System Name:</th>
<th>MiVb</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address:</td>
<td>192.168.1.2</td>
</tr>
</tbody>
</table>

* (MiVoice Business IP Address after configuration)

<table>
<thead>
<tr>
<th>Hostname or FQDN:</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>* Platform:</th>
<th>Virtual MiVb</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring MiVoice Business System Data</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MiCollab</th>
</tr>
</thead>
</table>

| IP Address: | 192.168.1.23 |

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 Help.

Select the type of network configuration for the MiVoice Business

- Single MiVoice Business
- MiVoice Business Cluster
  - Create new non-redundant 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
  - Encoded
  - MiCollab NUPoint UM
- 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 100.

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
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.
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.
Flow Through Provisioning: Adding Greenfield MiCollab to Greenfield MiVB Servers

6. Complete the wizard to configure the MiVB element.

Figure 21: Applications Page - Create new non-resilient cluster

Figure 22: Applications Page - Create new cluster for resilient users and services
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.

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.

Figure 23: System Parameters - for additional MiVB Element

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.

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.
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.

5. In the MiVoice Business Cluster Definition page, add the names of the MiVB cluster elements:
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.

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 100.
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.

![System Parameters - First Run](image)

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 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 NoPoint VM
- Mobility Services - Dynamic Extension
- MiCollab Speech Auto Attendant
- Teleworker
- MiCollab Audio, Web 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.
2. Ensure that the MiVoice Business platforms that you want to support Flow Through Provisioning are sharing data.
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.
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.

![Figure 32: GDM CHECK USERANDSERVICE Command Successful Result](image-url)
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. 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).

6. After adding the desired SIP softphone entries, import the CSV files back into their respective MiVoice Business User and Services Configuration forms.

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 45 for instructions on how to the MiCollab system software.
MiCollab Installation and Maintenance Guide

- 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 71 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 97). Flow Through Provisioning is only supported for MiCollab Client integrated mode.

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 MIVOECE 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Last Name</th>
<th>Number</th>
<th>Location</th>
<th>Role</th>
<th>Email</th>
<th>Prim Phone</th>
<th>Direct Prim</th>
<th>Home Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>E. Smith</td>
<td>Smith</td>
<td>123</td>
<td>Office</td>
<td>User</td>
<td>Smith</td>
<td>555-1234</td>
<td></td>
<td>MN25</td>
</tr>
<tr>
<td>J. Jones</td>
<td>Jones</td>
<td>456</td>
<td>Warehouse</td>
<td>User</td>
<td>Jones</td>
<td>666-5432</td>
<td></td>
<td>MN27</td>
</tr>
<tr>
<td>L. Johnson</td>
<td>Johnson</td>
<td>789</td>
<td>Factory</td>
<td>User</td>
<td>Johnson</td>
<td>777-6543</td>
<td></td>
<td>MN25</td>
</tr>
</tbody>
</table>

Figure 35: Find and Replace in User and Services Configuration Data

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 13 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 UCC license bundle set to &quot;UCC Entry User for Enterprise (Vx.0)&quot;</td>
<td>Primary Phone: Desk Phone&lt;br&gt;Primary Phone: EHDU Phone&lt;br&gt;Feature Profile: UCC (Vx.0) Entry&lt;br&gt;Desk phone extension: None&lt;br&gt;Soft phone extension: None</td>
</tr>
<tr>
<td>1 Phones</td>
<td>Primary Phone: Desk Phone&lt;br&gt;Secondary Phone: EHDU Phone</td>
<td></td>
</tr>
<tr>
<td>Include MiCollab Client Entry</td>
<td>Feature Profile: UCC (Vx.0) Entry&lt;br&gt;Desk phone extension: None&lt;br&gt;Soft phone extension: None</td>
<td></td>
</tr>
<tr>
<td>1 NuPoint Mailbox</td>
<td>NuPoint mailbox license with Call Director and Standard and Advanced UM licensing</td>
<td></td>
</tr>
<tr>
<td>For a Standard-level user</td>
<td>1 User UCC license bundle set to &quot;UCC Standard User for Enterprise (Vx.0&quot;</td>
<td>Primary Phone: Desk Phone&lt;br&gt;Primary Phone: EHDU Phone&lt;br&gt;Feature Profile: UCC (Vx.0) Standard&lt;br&gt;Desk phone extension: Primary&lt;br&gt;Soft phone extension: Other</td>
</tr>
<tr>
<td>1 Phones</td>
<td>Primary Phone: Desk Phone</td>
<td></td>
</tr>
<tr>
<td>Include MiCollab Client</td>
<td>Feature Profile: UCC (Vx.0) Standard&lt;br&gt;Desk phone extension: Primary&lt;br&gt;Soft phone extension: Other</td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>NuPoint mailbox license with call director and Standard and Advanced UM licensing</td>
<td></td>
</tr>
<tr>
<td>1 Teleworker</td>
<td>Teleworker Service available for one phone</td>
<td></td>
</tr>
<tr>
<td>Include Audio, Web and Video</td>
<td>Access for primary phone</td>
<td></td>
</tr>
<tr>
<td>Conferencing</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In Table 14 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 14: 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>

Table 13: Sample UCC User Template Functionality

<table>
<thead>
<tr>
<th>TEMPLATE PURPOSE</th>
<th>TEMPLATE CONTENTS</th>
<th>SERVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCC V4.0 Premium</td>
<td>1 User</td>
<td>UCC license bundle set to “UCC Premium User for Enterprise (Vx.0)”</td>
</tr>
<tr>
<td></td>
<td>3 Phones</td>
<td>Primary Phone: Desk Phone</td>
</tr>
<tr>
<td></td>
<td>Include MiCollab Client Premium</td>
<td>Feature Profile: UCC (Vx.0) Premium Desk phone extension: Primary 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>3 Teleworker</td>
<td>Teleworker service available for up to three phones</td>
</tr>
<tr>
<td></td>
<td>Include Audio, Web and Video Conferencing</td>
<td>Access for primary phone</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 15: 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

![Edit User Template](image)

**User Template - P73 Premium**

- Label: P73 Premium
- Description: Copy of the default template for the UCC Premium

**User Information**

- UCC Bundle: UCC Premium User for Enterprise (V4.0)
- Department: <empty>
- Location: <empty>
- Prompt Language: System Default - English (United States)
- Password: 
  - Same as Primary Phone Extension
  - Randomly Generate
  - Use this value
- TUI Passcode: 
  - Same as Primary Phone Extension
  - Randomly Generate
  - Use this value
  - IDS Manageable

**Service Information**

- Include Primary Phone

- Service Label: Deskphone
- Network Element: P73
- Secondary Element: <empty>
- CESID: <empty>
- Use DID Service Number as Outgoing DID Number
- Device Type: 64x0e IP
- Include Teleworker Service
- Service Level: Full
- Zone ID: 1
- Call Coverage Service Number: 1

**Figure 36: Example Template**
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 16: 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>Examples only:</td>
<td></td>
<td></td>
<td></td>
</tr>
<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:

![Figure 37: BUPExample.csv File](image)

5. Copy the user data from the exported USC files into the import file spreadsheet columns, starting at row 2. Table 17 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.
Figure 38: BUP Import Spreadsheet

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:
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 who have been installed on the server as an application blade and are licensed.

<table>
<thead>
<tr>
<th>Mode</th>
<th>Bulk User Add</th>
<th>First Name</th>
<th>Last Name</th>
<th>Login ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>David</td>
<td>Babineau</td>
<td>Babineau</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Ed</td>
<td>Biman</td>
<td>Biman</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Norman</td>
<td>Clarion</td>
<td>Clarion</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Ricky</td>
<td>Dickerson</td>
<td>Dickerson</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Wayne</td>
<td>Pry</td>
<td>Pry</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>James</td>
<td>Lerche</td>
<td>Lerche</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>David-A</td>
<td>Smith</td>
<td>SmithD</td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>Dean</td>
<td>Smith</td>
<td>smithD</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 39: 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 223).

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 `sdscc/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.

7. Click **OK**.

8. If a reconcile is required, you will receive the message shown in Figure 40. The MiVoice Business system will also have error logs indicating this status.
9. 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.

10. If you receive the message show in Figure 42, 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.
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, 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
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 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 continues to support 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.

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.
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. In your AMC account, convert UCC User V3 licenses to UCC V4 User Licenses. See “Trusted Service Support” on page 36.

8. 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**.

9. 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".

10. 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 44: GDM CHECK USERANDSERVICE Command Successful Result](image-url)
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 223).

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.

   **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.

12. Click OK.

13. If a reconcile is required, you will receive the message shown in Figure 45. 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.
Flow Through Provisioning: Brownfield MiCollab with Brownfield MiVB Servers

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.

15. If you receive the message shown in Figure 47, 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.
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.

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 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 settings.

**Table 18: 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>Service Hosting</td>
<td></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>Service Hosting</td>
<td>All Network Elements</td>
</tr>
<tr>
<td><strong>Templates</strong></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>FORM CATEGORY</td>
<td>SHARE RECORDS</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td><strong>Templates (Pre-7.0)</strong></td>
<td></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
A
Activation errors 135
Administrator
  password 56, 77
Alarms, viewing 139
AMC 19
Application
  record id 77
  record ID number 19, 60
  record ID number for vMiCollab 85
  record, creating 51
  record, creating for vMiCollab 79
  software, obtaining 52
  web pages 63, 88
Application support, communication platforms 6
Applications
  software installation 61
  software packages 3
  supported for vMiCollab 73
  vMiCollab software installation 86
ARID 19, 77

B
Backup, to USB 134

C
CD/DVDs
  software labeling 54
Certificate Authority 64, 89
Certificate, root certificate installation 64, 89
Client system, requirements 63, 88
Co-located mode, for MiCollab Client 98
Configuration
  configuration wizard 6
  determining deployment requirements 48
  DHCP server 60
  DHCP server, 85
  DNS server 60
  DNS server, 85
  MSL 80, 195
  MSL, 54
  system name 57
  system name, 82
Configurations, vMiCollab deployment 72
Console, accessing 136

D
Deployment configurations, for vMiCollab 72
Deployment, determining requirements 48
DHCP 60, 85
Disaster recovery 169
DNS server 60, 85
Documentation set
  About 8
  accessing online 10
  MBG 9
  MiCollab 8
  MiCollab Client 9
  Mitel Standard Linux 9
  MiVoice Office 250 10
  NP-UM 9
  NuPoint 8
  Speech Auto Attendant, 9
  Teleworker 8

E
Element identification 196
Event viewer 139

F
FTP 136

G
Greenfield site, provisioning 13

H
Hardware
  accessing qualified hardware list 49
  platforms 4
Help troubleshooting 152

I
Industry standard server 4
Installation
  application software 61
  checklist for vMiCollab install 73
  overview 47
  overview of vMiCollab install 72
  vMiCollab application software 86
Integrate mode, for MiCollab Client 97
Introduction
  overview of MiCollab 3

K
Knowledge base articles, accessing 10
Licenses
- troubleshooting 166
- upgrading 43
- Local network settings 57
- Local network settings, for vMiCollab 83
- Logging into server manager 64, 89

Logs
- viewing and collecting 169

Maintenance 117
MiCollab
- overview 3
MiCollab Client
- migrating 67
- part numbers 38
MiCollab Client Integration Wizard
- description 97
MiCollab End User portal 64, 89
MiCollab Server Appliance 49
- description 4
MiCollab Virtual Appliance
- description 5
MiCW
- description 6
- new MiCollab with a new MiVB cluster 182
- new MiCollab with a single existing MiVB platform 179
- new MiCollab with a single new MiVB platform 177
- new MiCollab with existing MiVB cluster 188
- use cases 177, 196
Mitel
- Application Management Center 19
- application record ID 77
- Knowledge Base articles 10
- Root CA certificate 64, 89
- software assurance program 21
- Standard Linux, installing operating system 55
Mitel Configuration Wizard
- description 6
- new MiCollab with a new MiVB cluster 182
- new MiCollab with a single existing MiVB platform 179
- new MiCollab with a single new MiVB platform 177
- new MiCollab with existing MiVB cluster 188
- use cases 177, 196
MiVoice 5000
- supported versions 4
- MiVoice Border Gateway
  - troubleshooting 163
MiVoice Business
- supported versions 3
MiVoice MX-ONE
- supported versions 4
MiVoice Office 250
- supported versions 4
MSL
- activation errors 135
- configure software 56
- configure software on vMiCollab 80
- download software 52
- install software 54, 80, 195
- installing operating system 55
- Qualified Hardware List 4
- qualified hardware list, accessing 49
MSL software, obtaining 52

Mitel Configuration Wizard
- description 6
- new MiCollab with a new MiVB cluster 182
- new MiCollab with a single existing MiVB platform 179
- new MiCollab with a single new MiVB platform 177
- new MiCollab with existing MiVB cluster 188
- use cases 177, 196
MiVoice 5000
- supported versions 4

Mitel Configuration Wizard
- description 6
- new MiCollab with a new MiVB cluster 182
- new MiCollab with a single existing MiVB platform 179
- new MiCollab with a single new MiVB platform 177
- new MiCollab with existing MiVB cluster 188
- use cases 177, 196
MiVoice 5000
- supported versions 4

Mitel Configuration Wizard
- description 6
- new MiCollab with a new MiVB cluster 182
- new MiCollab with a single existing MiVB platform 179
- new MiCollab with a single new MiVB platform 177
- new MiCollab with existing MiVB cluster 188
- use cases 177, 196
MiVoice 5000
- supported versions 4

Mitel Configuration Wizard
- description 6
- new MiCollab with a new MiVB cluster 182
- new MiCollab with a single existing MiVB platform 179
- new MiCollab with a single new MiVB platform 177
- new MiCollab with existing MiVB cluster 188
- use cases 177, 196

MIVoice 5000
- supported versions 4

Mitel Configuration Wizard
- description 6
- new MiCollab with a new MiVB cluster 182
- new MiCollab with a single existing MiVB platform 179
- new MiCollab with a single new MiVB platform 177
- new MiCollab with existing MiVB cluster 188
- use cases 177, 196

Online help, troubleshooting 152
OpenSSH 136
Overview, of vMiCollab install 73
OVF 80

Packages, software 3
Part numbers
- for SWA 28
Password, administrator 56
PBX interoperability 6
PC server 49
Platform, setting up 49
PuTTY 137

Qualified hardware list, accessing 49

Reboot, reconfigure, or shutdown 63
Reboot, reconfigure, or shutdown vMiCollab 88, 124
Restore
- disaster recovery 169
Root CA certificate 64, 89
S
Secure shell  55, 136
Secure Sockets Layer  64, 89
Server
  console, accessing  136
  set up  49
Server Appliance  49
Server manager, accessing  64, 89
Server platforms  4
Server, industry standard  4
ServiceLink  60, 86
Site information, collecting  48
Software
  application installation  61
  download, 52
  Install Applications,  61
  Install optional vMiCollab applications  86
  labeling CD/DVDs  54
  licensed packages  3
  obtaining  52
  upgrade  117
  upgrading MiCollab software  117
vMiCollab application installation  86
Software assurance program  21
SSH  55, 136
SWA
  description  21
  part numbers  28
T
telnet  136
Troubleshooting
  Licensing  152
  licensing errors  166
  MiVoice Border Gateway  163
  online help  152
U
Upgrade
  application suite licenses  43
  MiCollab software  117
V
vApp
  deployment  80
vMiCollab
  deployment configurations  72
  installation requirements and constraints  73
  supported applications  73
  vApp deployment  80
W
Web certificates, installation  64, 89
Work flow
  for existing site  14
  for new site  13