MiCollab - Installation and Maintenance Guide

- MiVoice Office 400
- MiVoice 5000
- MiVoice MX-ONE

RELEASE 7.3
JANUARY 2017
NOTICE

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

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

Trademarks

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

Installation and Maintenance Guide
Release 7.3
January 2017

©, ™ Trademark of Mitel Networks Corporation
© Copyright 2017, Mitel Networks Corporation
All rights reserved
# Table of Contents

## CHAPTER 1: INTRODUCTION

- About MiCollab .......................................................... 3
- Deployment Configurations ........................................... 3
- Supported Communications Platforms .............................. 3
  - Platforms ............................................................... 3
  - Software Releases ................................................... 3
- MiCollab Platforms ..................................................... 3
  - Industry Standard Server .......................................... 4
  - MiCollab Virtual Appliance (vMiCollab) .......................... 4
- About the Documentation Set ......................................... 4
  - MiCollab ..................................................................... 5
  - MiCollab NuPoint Unified Messaging .............................. 6
  - Speech Auto Attendant ............................................... 6
  - Mitel Standard Linux .................................................. 6
  - MiVoice Border Gateway (Teleworker) ............................ 6
  - MiCollab Client .......................................................... 6
- Access MiCollab Product Documentation ............................ 6
- Access Product Bulletins ................................................. 7

## CHAPTER 2: INSTALLATION & PROVISIONING WORK FLOW

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

Introduction ............................................................ 17
About AMC Licensing ................................................. 17
  Requesting a New AMC Account ................................. 18
  Accessing your AMC Account ..................................... 18
UCC Licensing Procedure ........................................... 19
  Overview .............................................................. 19
  Deploying UCC Licenses ............................................ 19
Adding "à la carte" Licenses ........................................ 26

CHAPTER 4: INSTALL MICOLLAB SERVER

Overview .............................................................. 31
Collect Site Information ............................................. 32
Set Up Platform ....................................................... 33
  MiCollab on Industry Standard Server .......................... 33
  MiCollab on Microsoft Hyper-V Virtual Machine .......... 33
Create Application Record ......................................... 34
Obtain MSL and Application Software ............................ 34
  Download Software ISO Files from Mitel OnLine .......... 34
  Software Downloads .............................................. 35
Create Storage Media ............................................... 35
  Option 1: Burn MSL ISO to CD/DVD and Copy Application ISO Images to USB Device .... 36
  Option 2: Burn Downloaded ISO Images to CD/DVDs .... 36
Install MSL Operating System Software ......................... 37
Configure the MSL Operating System ............................ 37
  Accept End User License ........................................ 38
  Set Administrator Password ..................................... 38
  Select System Timezone .......................................... 38
  Configure Domain Name .......................................... 38
  Configure System Name .......................................... 39
  Enter Local Network Adapter .................................... 39
  Enter Local Networking Parameters ............................. 39
  Enable IPv6 Protocol and Address .............................. 40
# Table of Contents

- Select WAN Adapters .................................................. 40
- Select Gateway IP Address ............................................. 41
- Configure External Interface .......................................... 41
- Configure DNS ................................................................. 41
- Activate Changes .............................................................. 41
- Enter Application Record ID ............................................. 42
- Install Application Software ............................................. 42
- Configure MiCollab ........................................................... 43
- Log in to the Administrator Portal (Server Manager) ............... 43
- Install Web Certificates .................................................... 44
- Allow “Trusted Network” Access ......................................... 44
- Set System Language ......................................................... 45
- Configure Port 5058 .......................................................... 46
- Perform Initial Configuration of Applications ......................... 47
- Install MiCollab Server in LAN Mode with MiVoice Border Gateway Server(s) ............................................. 47
- Prerequisites and Conditions ............................................. 47

## CHAPTER 5: INSTALLING VIRTUAL MIPLATFORM IN A VMWARE ENVIRONMENT

- Introduction ..................................................................... 50
- About MiCollab Virtual Appliance ....................................... 50
  - Deployment Configurations ............................................. 50
  - Supported Applications .................................................. 51
- Installation Checklist ........................................................ 51
- MiCollab Virtual Appliance Installation ............................... 51
- Review Installation Details ................................................ 51
  - Requirements ................................................................ 51
  - Constraints .................................................................. 52
- Collect Site Information ..................................................... 52
- Collect Custom Template Information .................................. 53
- Create MiCollab Application Record .................................... 56
- Download MiCollab OVA file and Application Software .......... 56
  - Software Downloads ...................................................... 56
- Deploy vMiCollab vApp ...................................................... 57
- Configure the MSL Operating System ................................... 57
Launch the MSL Server Console .............................................. 57
Set Administrator Password .................................................. 58
Select System Timezone ....................................................... 58
Configure Domain Name ....................................................... 58
Configure System Name ....................................................... 59
Enter Local Network Adapter ............................................... 59
Enter Local Networking Parameters ..................................... 59
Enable IPv6 Protocol and Address ......................................... 60
Select WAN Adapters .......................................................... 60
Select Gateway IP Address .................................................. 61
Configure External Interface ............................................... 61
Configure DNS ................................................................. 61
Activate Changes .............................................................. 61
Enter Application Record ID and Reboot ................................. 62
Install Application Software .................................................. 62
Configure vMiCollab ............................................................ 62
Log in to the Administrator Portal (Server Manager) ..................... 63
Install Web Certificate .......................................................... 63
Allow “Trusted Network” Access ............................................ 64
Set System Language ......................................................... 65
Configure Port 5058 ............................................................. 66
Synchronize MiCollab Client server with MiCollab AWV Software Versions ................................................................. 66
Perform Initial Configuration of Applications ............................. 66

CHAPTER 6: INITIAL CONFIGURATION

Introduction ........................................................................... 69
Collect Site Configuration Information .................................... 69
Configure MiCollab Client Mode ............................................. 71
     Configuring Integrated Mode ............................................. 71
     For MiCollab Server Deployments: .................................. 71
     For vMiCollab Deployments: .......................................... 71

Synchronize MiCollab Client server with MiCollab AWV Software Versions ................................................................. 72

Configure Platform and Application Resources .......................... 72
Configure Users and Services ................................................. 72
<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiVoice Office 400</td>
</tr>
<tr>
<td>MiVoice 5000 OR MiVoice MX-ONE</td>
</tr>
<tr>
<td>Configure Integrated Directory Services</td>
</tr>
<tr>
<td>Configure Application Settings</td>
</tr>
<tr>
<td>Backup Database</td>
</tr>
<tr>
<td><strong>CHAPTER 7: MAINTENANCE</strong></td>
</tr>
<tr>
<td>Upgrading MiCollab Software</td>
</tr>
<tr>
<td>Upgrade to MiCollab 7.3 using Fresh Install</td>
</tr>
<tr>
<td>Prerequisites</td>
</tr>
<tr>
<td>Backup and Restore with Fresh Install</td>
</tr>
<tr>
<td>Upgrade to vMiCollab 7.3</td>
</tr>
<tr>
<td>Upgrade Prerequisites</td>
</tr>
<tr>
<td>Deploy vMiCollab 7.3 OVA File and Restore Backup</td>
</tr>
<tr>
<td>Upgrade from MiCollab 7.x to MiCollab 7.y</td>
</tr>
<tr>
<td>Upgrade vMiCollab Configuration</td>
</tr>
<tr>
<td>Installing Additional (Missing) Applications</td>
</tr>
<tr>
<td>Add Application from Server Manager</td>
</tr>
<tr>
<td>Removing an Application during Initial Installation</td>
</tr>
<tr>
<td>Downgrading Application Software</td>
</tr>
<tr>
<td>Performing Backups</td>
</tr>
<tr>
<td>Server Manager &quot;Backup&quot;</td>
</tr>
<tr>
<td>Backup to Desktop</td>
</tr>
<tr>
<td>Schedule Backups to Network File Server</td>
</tr>
<tr>
<td>Server Manager SFTP Backup to Linux Servers</td>
</tr>
<tr>
<td>Allow Access on the Backup Server</td>
</tr>
<tr>
<td>Configure an SFTP backup</td>
</tr>
<tr>
<td>Server Console &quot;Perform Backup&quot;</td>
</tr>
<tr>
<td>Backing up to USB Device</td>
</tr>
<tr>
<td>Backing up to Network File Server</td>
</tr>
<tr>
<td>Verify Backup Data</td>
</tr>
<tr>
<td>Shutting Down MiCollab</td>
</tr>
<tr>
<td>Correcting Activation Errors</td>
</tr>
<tr>
<td>Accessing the Server Console</td>
</tr>
</tbody>
</table>
About SSH (Secure Shell) ................................................................. 92
Obtaining an SSH Client ............................................................. 93
Configuring Remote Management via MBG ............................. 93
Viewing Log Files ................................................................. 94
Viewing Alarms ................................................................. 95
Conversions and Migrations ................................................... 95
Convert a MiCollab Server Database to vMiCollab .................. 95
  Conditions and Constraints .................................................. 95
  Before You Begin ............................................................. 96
  Perform the Conversion ...................................................... 96
Migrate Standalone MiCollab Client to MiCollab Server or vMiCollab .................................................. 98
  Conditions and Constraints .................................................. 98
  Before You Begin ............................................................. 98
  Perform the Migration ...................................................... 99

CHAPTER 8: TROUBLESHOOTING

General Troubleshooting .................................................. 103
Online Help Troubleshooting ............................................... 106
vMiCollab Troubleshooting ................................................ 107
Troubleshooting Applications ........................................... 109
MiCollab AWV ........................................................................ 109
  Conferencing Error Messages for Alarm/Alert Conditions ..... 114
MiCollab Client ................................................................. 116
MiVoice Border Gateway ..................................................... 117
NP-UM Troubleshooting ..................................................... 118
Google Apps Troubleshooting ............................................ 118
Troubleshooting Licensing Errors ....................................... 119
Troubleshooting UCC Licensing Upgrades ......................... 121
Troubleshooting Active Directory Problems ....................... 122
  Problem .............................................................................. 122
  Possible Cause ............................................................... 122
  Detecting Active Directory Delay ..................................... 122
  Corrective Action ............................................................ 124
Viewing/Collecting Log Files .............................................. 124
Database Recovery (Restore) ................................................................. 124
Conditions and Constraints .............................................................. 124
Restoring a Database Backup ............................................................ 126
  Access the Console Restore Menu ................................................. 126
  Restore From Another Running Server ......................................... 126
  Restore From Network Share ....................................................... 127
  Restore from Removable Device .................................................. 127
  Check Application Data .............................................................. 128
vMiCollab System Disaster Recovery .................................................. 128
Restoring a MiCollab Server Database to a Different Server ................... 128

APPENDIX A: OFF-LINE LICENSING AND INSTALLATION

  Introduction .................................................................................. 132
  Installation of vMiCollab Using Off-Line Licensing ......................... 132
  Resetting The License Term ......................................................... 133
  Adding Licenses .......................................................................... 134
  Upgrade ....................................................................................... 134
Chapter 1

INTRODUCTION
ABOUT MICOLLAB

Mitel® MiCollab is a software solution that supports the co-residency of Mitel applications on the Mitel Standard Linux (MSL) operating system. MiCollab supports co-residency of multiple applications:

• on a single industry standard server, and
• within a virtual appliance (vApp) running in a virtualized environment.

MiCollab provides the following features for all applications:

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

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

DEPLOYMENT CONFIGURATIONS

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

SUPPORTED COMMUNICATIONS PLATFORMS

PLATFORMS

MiCollab is supported for the following Mitel communications platforms:

• MiVoice Office 400
• MiVoice 5000
• MiVoice MX-ONE

SOFTWARE RELEASES

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

MICOLLAB PLATFORMS

MiCollab is available on the following platforms:

• Industry Standard Server
• MiCollab Virtual Appliance running in a virtual environment
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.

MICOLLAB VIRTUAL APPLIANCE (VMICOLLAB)

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

MiCollab Virtual Appliance deployments on VMware are supported for
- small business multi-application
- mid-range business multi-application or single application sites
- enterprise multi-application sites
- enterprise single-application sites

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

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

ABOUT THE DOCUMENTATION SET

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

- **MiCollab General Information Guide**: provides a high-level overview of the MiCollab product.

- **MiCollab Engineering Guidelines** provides information about the characteristics, requirements, and performance of MiCollab and the supported applications.

- **MiCollab Order Guide** provides licensing information and product part number lists.

- **Virtual Appliance Deployment Guide** provides engineering guidelines for deploying Mitel products in a virtual infrastructure.

- **MiCollab Installation and Maintenance Guides** provide instructions on how to install the MiCollab server and application software.

- **Platform Integration Guide**: provides instructions on how to configure the MiVoice Office 400, MiVoice 5000, and MiVoice MX-ONE communication platforms to support the MiCollab applications.

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

- **MiCollab Client Desktop MiNET Softphone - Server Independence Guide** describes the behavior of the MiCollab Client Desktop MiNET Softphone when a user is logged into MiCollab Client and the MiCollab server is taken out of service. If the MiCollab server is taken out of service, for example due to an upgrade or hardware failure, the Desktop MiNET softphone continues to provide basic functionality.

**Administrator**

- **Server Manager help** provides configuration, administration, and maintenance procedures for the MiCollab server. The MiCollab Integrated Directory Services functionality is described in this on-line help.

- **Users and Services help** provides instructions on how to manage user data and assign or remove user services, such as MiVoice Border Gateway or Teleworker.

- **NuPoint Unified Messaging help** is intended to help system administrators configure and maintain NuPoint Unified Messaging functionality through the web console interface.

- **MiCollab AWV help** provides instructions on how to provision the conferencing application.

- **Mitel MetaDirectory help** provides instructions on how to set up a Mitel Metadirectory. Mitel MetaDirectory is a Lightweight Directory Access Protocol (LDAP) server with intelligent services for comparing and presenting data. It collects employee and customers data from various sources and allows it to be searched efficiently.

**End User**

- **MiCollab End User Portal Online Help** provides you with instructions on how to configure your portal settings and use the communication applications.

- **MiCollab AWV Quick Reference Guide** provides procedures on how to set up and use the conferencing features.
MICOLLAB NUPOINT UNIFIED MESSAGING

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

SPEECH AUTO ATTENDANT

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

MITEL STANDARD LINUX

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

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

• *MiCollab Client Engineering Guidelines*
• *Administrator Guide* provides instructions on how to configure MiCollab Client on Mitel communications platforms.
• *Administrator Portal Online Help* provides information and instructions for the MiCollab Client Server administrator interface.
• *MiTeam Reference Guide*: provides user information for Mitel’s Cloud-based collaboration tool.
• *MiCollab Client Quick Reference Guide*

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
   - MiCollab platform
     - MiCollab Server
     - MiCollab Virtual Appliance (see the Virtual Appliance Deployment Guide)
   - Communications platform (“Supported Communications Platforms” on page 3)
   - Firewall Settings (Refer to the MiCollab Engineering Guidelines)

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

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

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

WORK FLOW

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

STEP 1: OBTAIN LICENSES

Licenses: Refer to “Licensing” on page 15 for MiCollab licensing requirements.

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.

MiCollab Server: 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.

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

STEP 3: OBTAIN SOFTWARE

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

MiCollab 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 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 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, MiVoice MX-ONE, and MiVoice Office 400 platforms, you must configure MiCollab Client in integrated mode.

STEP 8: PERFORM INITIAL CONFIGURATION

MiCollab with MiVoice 5000, MiVoice MX-ONE, MiVoice Office 400:

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:

- **Bulk User Provisioning Tool**: export a CSV or LDIF file of user entries from an existing communications platform and then import it into the MiCollab database using the Bulk User Provisioning Tool.
- **Manual Provisioning**: enter user data separately for each entry through the User and Services application.
- **Provisioning with IDS**: seed the Users and Services application database with the user entries and or corporate contacts from a site directory server database.

For each of the above provisioning methods, you can assign roles and templates to quickly configure user data.

STEP 10: CONFIGURE SYSTEM APPLICATION SETTINGS

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

STEP 11: PERFORM BACKUPS

Backup the MiCollab and communication platform databases to complete the installation.
STEP 12: CONFIGURE INTEGRATED DIRECTORY SERVICES

Optionally, configure Integrated Directory Services.
Chapter 3

LICENSING
INTRODUCTION

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

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

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

ABOUT AMC LICENSING

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

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

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

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

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

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

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

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

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

ACCESSING YOUR AMC ACCOUNT

To access your account for the first time:

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

![Figure 2: Log in to AMC](image-url)
4. Enter your User ID and Password.
5. Click **Login**. For information about using the AMC, see the help.

**UCC LICENSING PROCEDURE**

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

**MiVoice 5000, MiVoice MX-ONE and MiVoice Office 400 Deployments**

For these deployments, you add the following servers to a UCC License Manager group:

- 1 or more MiCollab Release 7.0 or higher systems
- 1 or more MBG Release 9.1 or higher systems

The MiVoice 5000, MiVoice MX-ONE, and MiVoice Office 400 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 the AMC.
- Add the system server ARIDs to the ULM Group.
- Assign licenses, including UCC user and SWAS licenses, to the ULM Group ARID.
- Synchronize the servers with the AMC to download licenses.

**DEPLOYING UCC LICENSES**

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

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

**Note:** While you are using the AMC interface, if you click the browser back button, you may need to refresh your browser to redisplay the screen.
2. Create a Customer Account for each customer. Do not put multiple customers in a single customer account.
   - Click Customers.
   - Click the Create Customer button.
   - Enter the end-customer information.
   - Enter an e-mail address for the administrator contact.
   - Enter an e-mail for the technician contact.

3. Register products and licenses for the customer site:
   - Click Self service.
   - Click Register a License.
   - Enter a Purchase Order reference number.

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

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

**Figure 4: Selecting Licenses (Simple Example)**

4. **Click Confirm.** The system displays a list of the ordered products.

**Figure 5: Product Order List**
5. For integrations with MiVoice 5000, MX-ONE, MiVoice Office 400 platforms, create Application Record IDs for the MiCollab and standalone MBG systems.

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

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

6. Display the list of Application Records assigned to the customer:
- Click Customers.
- Enter the Customer name.
- Click Search.
- At the bottom of the screen, click to display a list of the ARIDs.
7. For each system, assign the base software licenses to the system base ARIDs:
   - Click the Status icon.
   - Click the Assign Product link.
   - Enter the Purchase order number in the search criteria and click Search.
   - Click to display the Purchase order details.
   - Assign the system's base software license to the base ARID.
   - Click Confirm to assign the license.
   - Review the licenses and record the ARID.
   - Click Done or click E-Mail to notify to the administrator. You can send the notification to your technician or customer by including their email addresses.

8. In the Customer profile create an associated ULM Group ARID:
- Click **Self service**.
- Under **Tasks**, click **Assign a License**.
- Enter the Customer Name and then click **Search**.
- Click 📝.
- For deployments with MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 400 click the ULM button next to the MiCollab Base ARID.
- Enter a description for the ULM Application Record. For example: "AAA Corporation ULM ARID".
- Click **Submit**. The Application Record details are displayed
- Click **Next**. The the server ARIDs appear listed in the right frame of the Group Application Record.

![Figure 8: Create ULM Group ARID](image)

9. Add the system server ARIDs to the ULM Group ARID:
   - Select the check boxes next to the ARIDs that you want to add.
   - Click **Add Selected Servers**.
   - Click **Add Selected Server**. The server ARIDs are added to the "ARIDs Managed by this ULM" list, and the AMC distributes the licenses to the ULM server members.
   - Click **Return to License Manager**.
10. Assign the UCC User and SWAS licenses to the ULM ARID:
   - Click Customers.
   - Enter the Customer name and then click Search.
   - Click beside the customer’s ID.
- Click the Status button next to the ULM ARID (for example, "AAA Corporation ULM Record".
- Click the Assign Product link.
- Enter the Purchase order number and click Search.
- Click to expand the Purchase order.
- Assign the licenses to the ULM ARID.
- Click Assign.
- Click Allocate to assign the licenses.
- Review the licenses and record the ARID.
- Click Confirm.
- Click Done.

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

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

- Sync the MiCollab and MBG servers from the Status page in the Server Manager interface. You can sync the MiCollab and MBG server ARIDs in any order. All the UCC MBG license options are provided to MiCollab in the group. The MBG standalone does not get any direct UCC license options.
- You do not sync MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 400 platforms with the AMC. These communication platforms obtain their licenses from a different software licensing server.

12. For MiVoice 5000, MiVoice MX-ONE, or MiVoice Office 400 deployments, you will assign the UCC licenses to users from the 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.

**ADDING "À LA CARTE" LICENSES**

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

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

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

3. Access the server manager. See “Log in to the Administrator Portal (Server Manager)” on page 43.

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 system software on a Microsoft Hyper-V virtual machine.

**Note:** If you are upgrading from a previous release, see “Upgrading MiCollab Software” on page 77. If you are installing vMiCollab, see “Installing Virtual MiCollab in a VMware Environment” on page 49.

Installation consists of the following steps:

- Collect Site Information
- Set up Platform
- Create Application Record
- Obtain MSL and MiCollab Application software
- Install MSL Operating System software
- Configure the MSL Operating System
- Install Application Software
- Configure MiCollab
- Perform Initial Configuration of Applications (See "Initial Configuration" on page 67).
- Integrate or Co-locate MiCollab Client Database? (See “Configure MiCollab Client Mode” on page 71).
**COLLECT SITE INFORMATION**

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

<table>
<thead>
<tr>
<th>ITEM</th>
<th>NOTES</th>
<th>ENTER YOUR INFORMATION HERE:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MiCollab Server</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Administrator Password</td>
<td>For password strength, choose a password that contains a mix of uppercase and lowercase letters, numbers, and punctuation characters. For more information, see page 38.</td>
<td></td>
</tr>
<tr>
<td>2. Domain Name</td>
<td>Names must start with a letter; can contain letters, numbers, and hyphens. For more information, see page 38.</td>
<td></td>
</tr>
<tr>
<td>3. System Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. IP address of your MiCollab server (LAN mode)</td>
<td>The local IP address of the server where you are installing MiCollab.</td>
<td></td>
</tr>
<tr>
<td>5. External Interface Connection</td>
<td>Cable Modem? You need to know if the ISP supplies an account name or an Ethernet address. Account Name or Ethernet Address?</td>
<td>Direct Connection? You need to know the static IP address.</td>
</tr>
<tr>
<td>6. Gateway IP address</td>
<td>The IP address that MiCollab will use to access the network.</td>
<td></td>
</tr>
<tr>
<td>7. MiCollab AWV IP Addresses</td>
<td>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).</td>
<td></td>
</tr>
<tr>
<td>8. Will the MiCollab (MSL) server be supplying DHCP services?</td>
<td>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 41.</td>
<td>Yes</td>
</tr>
<tr>
<td>9. DNS Server IP address</td>
<td>Enter the IP address of your corporate DNS server. <strong>Note:</strong> If your DNS is supplied by your ISP, leave this setting blank.</td>
<td></td>
</tr>
<tr>
<td>10. Application Record ID #</td>
<td>Create an Application Record for the MiCollab installation in your AMC license account. You will use the ID number of this Application Record to activate your MSL license. See “About AMC Licensing” on page 17 for more information. Record the generated Application Record ID.</td>
<td></td>
</tr>
</tbody>
</table>
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 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 17 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

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
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.

CREATE STORAGE MEDIA

After you download the MSL and application software, either

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

  OR

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

Note: The installation of the software is quicker if you can install the application files from a USB device.
OPTION 1: BURN MSL ISO TO CD/DVD AND COPY APPLICATION ISO IMAGES TO USB DEVICE

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

<table>
<thead>
<tr>
<th>LABEL</th>
<th>CD/DVD CONTENT</th>
<th>FILE NAME DOWNLOADED</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD/DVD1</td>
<td>MSL 10.5 for MiCollab Servers</td>
<td>MSL_10.5.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_7.3.x.xx.0.iso</td>
<td>260 MB</td>
</tr>
<tr>
<td>MiVoice Border Gateway</td>
<td>MBG_9.4.xx.0.iso</td>
<td>98 MB</td>
</tr>
<tr>
<td>MiCollab Client Service</td>
<td>MiCollab Client_7.3.x.x.iso</td>
<td>283 MB</td>
</tr>
<tr>
<td>MiCollab Audio, Web and Video Conferencing</td>
<td>AWV_6.3.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_20.0.x.xx-01.iso</td>
<td>1.0 GB</td>
</tr>
<tr>
<td>MiCollab Client Deployment</td>
<td>MiCollab Client Deploy_1.1.x.x</td>
<td></td>
</tr>
</tbody>
</table>

OPTION 2: BURN DOWNLOADED ISO IMAGES TO CD/DVDS

You will require up to seven, blank, formatted 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 10.5 for MiCollab Servers</td>
<td>MSL_10.5.xx.0.i686.iso (64-bit version only)</td>
</tr>
<tr>
<td>CD/DVD2</td>
<td>MiCollab Application Services</td>
<td>SAS_7.3.x.xx.0.iso</td>
</tr>
<tr>
<td>DVD3</td>
<td>NuPoint Unified Messaging (includes Speech to Text option)</td>
<td>NPM_Blades-DVD_1_20.0.x.xx-01.iso</td>
</tr>
<tr>
<td>CD/DVD5</td>
<td>MiCollab Audio, Web and Video Conferencing</td>
<td>AWV_6.3.x.xx.iso</td>
</tr>
<tr>
<td>CD/DVD6</td>
<td>MiVoice Border Gateway</td>
<td>MBG_9.4.x.0.iso</td>
</tr>
<tr>
<td>CD/DVD7</td>
<td>MiCollab Client Service</td>
<td>MiCollab Client_7.3.x.x.iso</td>
</tr>
<tr>
<td>CD/DVD8</td>
<td>MiCollab Client Deployment</td>
<td>MiCollab Client Deploy_1.1.x.x</td>
</tr>
</tbody>
</table>
INSTALL MSL OPERATING SYSTEM SOFTWARE

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

During the install, if you accidentally exit from the server console, you can use Secure Shell (SSH) to access the server console again (see “Accessing the Server Console” on page 92 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 77 for upgrade instructions.

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

1. Insert the MSL software CD/DVD that you labeled as MSL_10.5.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 10.5.xx.x SL** for a MiCollab Server
4. Depending on your model of CD/DVD drive, you may be prompted to select the installation language. Use the Space bar on the keyboard to select the desired language and select **Ok**.
5. Choose your preferred keyboard from the list (default is **us**).
6. You are prompted to test the CD/DVD media. Select **Test** to test the CD/DVD for validity and readability. The software installer runs.
7. At the **Install** option, select **Yes**.
8. Select your Time Zone from the list. Select **Ok**.
9. You are reminded to review the log file of the install. During the installation, logs are generated. After the installation is complete, the log file is saved to the root directory of the server: /root/install.log. Select **Next**.
10. Finishing the installation is automatic and takes only a few minutes. At the end of the process, you are prompted to remove any media and reboot the system.
11. Remove the CD/DVD media.
12. Press **Enter** to reboot. The server reboots.

CONFIGURE THE MSL OPERATING SYSTEM

If you are installing a MiCollab Server wait until the server reboots.
Now, you must configure the MSL operating system. Refer to your Site Information sheet (on page 34) 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 126 for instructions on how to complete the restore.

**CAUTION:** Before you attempt to perform a restore, review Table 7, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 125 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.
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)

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

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

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

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

CONFIGURE EXTERNAL INTERFACE

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

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

If you select Option 4:
• Enter the IP address that this server should use to access the Internet. If this server does not access the Internet, leave the setting blank
• Enter the subnet mask.

CONFIGURE DNS

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

ACTIVATE CHANGES

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

Note: If you receive an error message when you activate, you may have entered an incorrect network parameter. See “Correcting Activation Errors” on page 91.
ENTER APPLICATION RECORD ID

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

   **Note:** If you accidentally cancel this screen you will exit to the server console menu. You can restart the application software installation by selecting **Register for ServiceLink** from the menu. Enter your Application Record ID number to initiate registration. Then proceed to “Install Application Software” on page 42.

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

3. Proceed to “Install Application Software” on page 42.

INSTALL APPLICATION SOFTWARE

You can install the application software by

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

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

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

2. Click the **Install Applications** tab.

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

4. Select the latest software version for installation.

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

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

7. Click the **Install** button.
8. After the applications are installed, reboot the MiCollab server.
9. Proceed to “Configure MiCollab” on page 43.

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 Web browser access to MiCollab administration interfaces is provided through

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

LOG IN TO THE ADMINISTRATOR PORTAL (SERVER MANAGER)

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

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

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

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

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

   If you choose to disable the Welcome E-mail functionality, you will need to advise users of the URL for the MiCollab End User portal:
   https://<Fully Qualified Domain Name of the MiCollab server>/portal
5. Proceed to "Install Web Certificates" on page 44.

INSTALL WEB CERTIFICATES

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

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

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

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

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

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

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

ALLOW "TRUSTED NETWORK" ACCESS

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

To configure Trusted Networks:

1. Log into the MiCollab server console. The server console Welcome menu is displayed.
2. Select **Manage trusted networks** from the menu and select **Next**.

3. Select **Add IPv4 trusted network** or **Add IPv6 trusted network** and select **Next**.

4. Enter the **Trusted Network IP** address of the network to which you are granting access. (For example, 168.195.52.0). Select **Next**.

5. Enter the **Trusted Network Mask** to apply to the network address. (For example, if your network IP address is 168.195.52.0 and you want to allow access to all network IP addresses in the range from 1 to 255, enter 255.255.255.0. This allows IP addresses 168.195.52.1 through 168.195.52.255 to access your virtual appliance).

6. Enter the **Trusted Network Router Address**. (IP address of the router on your local network).

7. Select **Next**. The local network is added.

8. Repeat steps 1 through 5 to configure additional trusted networks.

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

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 43).

2. Navigate to **Remote Access** under the **Security** section.

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

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

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

6. Click **Save**.

**SET SYSTEM LANGUAGE**

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

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

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 43).
2. Under **Configuration**, click **MiCollab Language**.
3. Select the desired language from the Language drop-down box.
4. Click **Save**.
5. If NuPoint Unified Messenger application is installed, you can set up to five languages for the NuPoint system prompts. Users who call into the NuPoint auto attendant can choose to hear prompts in one of the supported languages for the duration of their call. Refer to the online help for the **MiCollab Language Settings** page for details.
6. If your system uses the Speech Auto Attendant application, set the SAA prompt language. The MiCollab system language setting does not control the prompt language used by the Speech Auto Attendant application. The MiCollab Speech Auto Attendant only supports two languages: UK English and NA English. To change the Speech Auto Attendant language:
   - Under **Applications**, click **NuPoint Web Console**.
   - Under **Auto Attendant**, click **Misc. Parameters**.
   - Select the desired **Primary Language**, and then click **Save**.
   - Under **Auto Attendant**, click **Data Source**.
   - Click **Force Update**.

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

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

7. If your system uses the MiCollab Client application, ensure that the MiCollab Client server uses the same IP address as the MiCollab server.
8. If required, configure MiTeam. MiTeam provides Cloud-based collaboration features for UCC Premium users. Note that MiTeam is only supported for MiCollab Client Integrated mode. Refer to the **MiCollab Client Administrator Guide** for configuration requirements.

**CONFIGURE PORT 5058**

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 67.

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 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. You then create a cluster on the MiCollab server and add the MBG servers as members of the cluster in separate cluster zones.

PREREQUISITES AND CONDITIONS

☑ The MiCollab server must be configured in LAN mode (server-only mode). MBG clustering is only supported for MiCollab systems that are configured in LAN mode.
☑ The MBG server must be installed, operational and routable to the MiCollab server.
☑ The MiCollab system must be configured with an MBG cluster to allow the data on the MBG cluster to be managed from the MiCollab application. Note that the MiCollab server can only be a member in one MBG cluster.
☑ The MiCollab and MBG servers should all have the same MBG software release (for example, MBG Release 9.4).
☑ The MiCollab and MBG nodes must reside in separate zones. You create a “LAN” zone for the MiCollab node and the MBG nodes remain in the “Default” zone.
☑ After you establish the cluster, the licenses of the MiCollab and MBG servers are pooled together. However, it is recommended that you purchase all Teleworker service licenses against the external MBG servers to avoid licensing issues.

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

1. Install the MBG server(s) in the DMZ. Refer to the MBG Installation and Maintenance Guide for instructions.
2. Open port 6809 in the firewall to allow the MiCollab system to communicate remotely with the MBG server(s).
3. In the MiCollab server manager, under Applications, click MiVoice Border Gateway, click the System status tab and then click Dashboard.
4. Create a new cluster on the MiCollab (master) server:
   - In the Clustering status frame, click Create a cluster.
   - In the IP Address of current node list, select the interface or enter the IP address of the MiCollab master server (or accept the default).
   - In the IP Address of peer node list, enter the IP address of the MBG slave server (DMZ address or server-gateway WAN address). These entries establish the cluster
relationship between the servers.

- In the Cluster weight of current node field, select the cluster weight factor value to apply to the MiCollab master server for load balancing. The default value is 0. You must select a non-zero value.
- Click Save to create the initial master/slave pair. The two new nodes are added to the Node information list as members of the "Default" cluster zone.

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

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

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

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

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

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

11. Click Save.

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

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

**Note:** Provision Teleworker services from the MiCollab server. Do not provision them on the MBG servers; otherwise, the MiCollab and MBG databases could get out of sync.
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.
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.
- 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 LAN mode with a second MBG Server in DMZ:  
  - vMiCollab with second MBG Web Proxy in DMZ (2 Server deployment)  
• vMiCollab in LAN Mode (Server Only) |  |
| 3. Identify vMiCollab capacity | All applications are included with vMiCollab. The maximum user capacity is higher for sites with a single application. For single application sites, do not configure users with multiple applications; otherwise the maximum performance and capacities of the system will be reduced. |  |
| 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 17 for more information. Record the generated Application Record ID. |  |
Before you begin deployment, collect and record the data specified in Table 2. 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 2: 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>
<tr>
<td>Application</td>
<td></td>
<td></td>
</tr>
</tbody>
</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. |                               |
### Table 2: 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>Remote Network Netmask (Optional)</td>
<td>Enter the Netmask associated with the remote network address.</td>
<td></td>
</tr>
<tr>
<td><strong>Network Settings</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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                                                      |                        |
| WAN IP Address (Optional)               | For LAN only (Server-only) deployments, use an IP address of 0.0.0.0.  
**Note:** You can leave this field blank if you are creating a blank template of the OVA file for cloning. However, you must set it before powering up the virtual appliance. You can set this address from vSphere Client. Right click on the MiCollab and click **Edit Settings**. Click the **Options** tab, click **Properties** and enter the WAN IP Address. |                        |
| WAN Netmask (Optional)                  | Record the Netmask of the WAN                                                      |                        |
| LAN (Optional)                          | Optional network interface that can be used to connect a management application or to route the SIP Proxy to an isolated SIP Proxy network. |                        |
| Default Gateway IP Address              | Record the Gateway IP address. For Server-gateway deployments this gateway typically points to the internet. For Server-only deployments, this gateway typically points to a LAN router. |                        |
CREATE MICOLLAB APPLICATION RECORD

Create an Application Record for this MiCollab Virtual Appliance installation in your AMC license account. You will use the ID number of this Application Record to activate your MSL license. See “About AMC Licensing” on page 17 for more information.

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

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

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

DOWNLOAD MICOLLAB OVA FILE AND APPLICATION SOFTWARE

SOFTWARE DOWNLOADS

1. Log on to Mitel 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.

<table>
<thead>
<tr>
<th>Table 3: Software Download Files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FILE CONTENTS</strong></td>
</tr>
<tr>
<td>vMiCollab Deployments</td>
</tr>
<tr>
<td>vMiCollab vApp packaged as a</td>
</tr>
<tr>
<td>virtual appliance</td>
</tr>
<tr>
<td>NuPoint Unified Messaging</td>
</tr>
<tr>
<td>option</td>
</tr>
</tbody>
</table>
DEPLOY VMICOLLAB VAPP

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

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

CONFIGURE THE MSL OPERATING SYSTEM

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

LAUNCH THE MSL SERVER CONSOLE

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

2. Right-click on the MiCollab Virtual Appliance and select Open Console.
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 58.

**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.
Installing Virtual MiCollab in a VMware Environment

**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) Note that although MSL offers the choice to bond two Network Interface Cards, this option is not supported for MiCollab. An asterisk is displayed in front of the Local adapter.

Regardless of server mode, you must always configure a Local (internal) adapter.

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

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

**ENTER LOCAL NETWORKING PARAMETERS**

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

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

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

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

Enter the subnet mask for the local network. If you are adding the virtual appliance to an existing network, use the subnet mask used by the local network. Otherwise, accept the default setting.
ENABLE IPV6 PROTOCOL AND ADDRESS

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

OR

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

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

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

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

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

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

SELECT WAN ADAPTERS

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

- If 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 62.

**Note:** If you receive an error message when you activate, you may have entered an incorrect network parameter. See “Correcting Activation Errors” on page 91.
ENTER APPLICATION RECORD ID AND REBOOT

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

Note: If you accidentally cancel this screen you will exit to the server console menu. You can restart the application software installation by selecting Register for ServiceLink from the menu. Enter your Application Record ID number to initiate registration. Then proceed to “Install Application Software” on page 62.

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

INSTALL APPLICATION SOFTWARE

You install Applications Software from MiCollab server manager:

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

2. Click the Install Applications tab.

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

4. Select the latest software version for installation.

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

6. Click Install.

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

7. After the applications are installed, proceed to “Configure vMiCollab” on page 62.

CONFIGURE VMICOLLAB

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

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

Web browser access to MiCollab administration interfaces is provided through
• Microsoft Edge 20
• Internet Explorer 10, or 11
• Mozilla FireFox 41 or higher, or
• Google Chrome (version 46 or higher)

LOG IN TO THE ADMINISTRATOR PORTAL (SERVER MANAGER)

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

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

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

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


INSTALL WEB CERTIFICATE

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

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

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

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

• To prevent the Security Alert warning from appearing on client stations on the local network, purchase a Secure Sockets Layer (SSL) certificate for the vMiCollab virtual appliance and then import it onto the vMiCollab virtual appliance.

• To prevent the Security Alert warning from appearing on remote client stations, purchase a Secure Sockets Layer (SSL) certificate for the MBG Web Proxy server and then import it onto the MBG Web Proxy server.

ALLOW "TRUSTED NETWORK" ACCESS

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

To configure Trusted Networks:

1. In the vSphere Client, right-click on the your vMiCollab appliance (for example: vMiCollab 7.3.3.0 build) and select Open Console. The vMiCollab virtual appliance console opens.

2. Log into the MiCollab server console. The server console Welcome menu is displayed.

3. Select Manage trusted networks from the menu and select Next.

4. Select Add IPv4 trusted network or Add IPv6 trusted network and select Next.

5. Enter the Trusted Network IP address of the network to which you are granting access. (For example, 168.195.52.0). Select Next.

6. Enter the Trusted Network Mask to apply to the network address. (For example, if your network IP address is 168.195.52.0 and you want to allow access to all network IP addresses in the range from 1 to 255, enter 255.255.255.0. This allows IP addresses 168.195.52.1 through 168.195.52.255 to access your virtual appliance).

7. Enter the Trusted Network Router Address. (IP address of the router on your local network).

8. Select Next. The local network is added.

9. Repeat steps 1 through 5 to configure additional trusted networks.

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

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)” on page 63).


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:

1. Log into the Administrator Portal (see “Log in to the Administrator Portal (Server Manager)" on page 63).

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.

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

**CONFIGURE PORT 5058**

If the MiCollab system is connected to a MiVoice Office 250, MiVoice Office 400, 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 67.
INTRODUCTION

Initial configuration consists of the following tasks:

- Collect Site Configuration Information
- Configure MiCollab Client Mode
- Configure Platform and Application Resources
- Configure Users and Services
- 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>STEP</th>
<th>CONFIGURATION INFORMATION</th>
<th>RECORD DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Platform and Application Resources</td>
<td>New MiCollab server with existing supported communication platform</td>
<td>Configure Manually (see the MiCollab Platform Integration Guide).</td>
</tr>
<tr>
<td>Server Details</td>
<td>Communication platform</td>
<td>IP Address:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System Login:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password:</td>
</tr>
<tr>
<td></td>
<td>MiCollab Server</td>
<td>Password:</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>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>
</tbody>
</table>
### Table 4: Site Configuration Information

<table>
<thead>
<tr>
<th>STEP</th>
<th>CONFIGURATION INFORMATION</th>
<th>RECORD DETAILS</th>
</tr>
</thead>
<tbody>
<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></td>
<td>Toll-Free Dial In Number</td>
<td></td>
</tr>
<tr>
<td>MiCollab Client Integration</td>
<td>Identify required Integration Mode (see &quot;Configure MiCollab Client Mode&quot; on page 71 for 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>
<tr>
<td>USP Roles and Templates</td>
<td>□ Use UCC licensing default templates?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>□ Create roles and templates?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Role Name:</td>
<td>Associated Template Name</td>
</tr>
<tr>
<td>User Provisioning Method</td>
<td>Bulk User Import data from file, or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>□</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sync AD database with MiCollab.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>□</td>
<td></td>
</tr>
<tr>
<td>User Import File Type</td>
<td>BUPEXample CSV □</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CSV □</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LDIF □</td>
<td></td>
</tr>
<tr>
<td>Filename</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File location</td>
<td></td>
<td></td>
</tr>
</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.

**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.

---

**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 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.

---

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 to 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:

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

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

CONFIGURE USERS AND SERVICES

MIVOICE OFFICE 400

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

6. Configure “Configure Integrated Directory Services” on page 73 if required.

MIVOICE 5000 OR MIVOICE MX-ONE

Refer to the MiCollab Platform Integration Guide for instructions.

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). Refer to Integrated Directory Services in the MiCollab server manager online help for instructions. Also, see Non-Corporate Contacts for instructions on how to add contacts to the MiCollab Client corporate directory.

CONFIGURE APPLICATION SETTINGS

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

BACKUP DATABASE

After you have programmed the site configuration data, it is recommended that you make a backup of the MiCollab system database. See “Downgrading Application Software” on page 85. 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 7.3 software, the system must be at a minimum of MAS Release 5.0 and valid software assurance (SWAS) must be active.

Table 5 identifies the supported upgrades and the required procedures.

Table 5: Upgrade Procedures

<table>
<thead>
<tr>
<th>SUPPORTED UPGRADES</th>
<th>UPGRADE PROCEDURES</th>
<th>WHEN TO USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiCollab 7.x to MiCollab 7.y</td>
<td>Upgrade applications from server manager Service Link &gt; Install Applications panel.</td>
<td>Use this procedure, to apply dot releases.</td>
</tr>
<tr>
<td>MiCollab 7.3 Service Pack Upgrades</td>
<td>Apply service packs from server manager ServiceLink &gt; Install Applications panel.</td>
<td>Use this procedure, to apply service pack upgrades.</td>
</tr>
</tbody>
</table>

UPGRADE TO MICOLLAB 7.3 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 7.3, 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 7 and Table 8 on page 125 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 86).
✓ You have verified your MAS 5.0 or later backup file (see “Verify Backup Data” on page 91 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.)

MiCollab Client integrates with a MiVoice 5000 or MiVoice MX-ONE communication platform using CSTA protocol. In MiCollab Release 7.1 and later, a CSTA proxy server is provided with the MiCollab MSL/Linux operating system.

If you have MiCollab Release 7.0 deployed with a MiVoice 5000 or MiVoice MX-ONE communications platform and you are upgrading to MiCollab Release 7.3 or later, you no longer require a separate Blustar server to support MiCollab Client. **Ensure that you either shut down the Blustar server or disconnect it from MiCollab before you upgrade to MiCollab Release 7.1 or later:**

- If the Blustar server is only supporting CSTA integration between MiCollab Client and the communication platform, shut down the Blustar server before upgrading MiCollab.
- If the Blustar server is supporting the CSTA integration and also providing additional customer functionality, disconnect the Blustar server from MiCollab prior to upgrading. To disconnect, log into the Web Admin portal of the Blustar server. Delete the MiCollab IP Address from the CSTA Proxy Configuration page, then click **Save**.
- After the upgrade, the MiCollab CSTA Proxy supports the MiCollab Client integration with the MiVoice 5000 or MiVoice MX-ONE.

**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 Connect.
   - Click 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 34.

3. Transfer the MSL_10.5.xx.x.iso software and application ISO files to either CDs, DVDs, or USB. See “Create Storage Media” on page 35.

4. Back up your existing MiCollab system database. See “Performing Backups” on page 85, 5.

5. If you plan to use an existing backup file, verify it before performing the new installation (see “Verify Backup Data” on page 91).

   **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_10.5.xx.x.iso in the CD/DVD drive of the server.

7. Reboot the server. After the server or controller reboots, you are presented with the server console.
8. Depending on your model of CD/DVD drive, you may be prompted to select the installation language. Use the Space bar on the keyboard to select the desired language and select Ok.

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

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

11. You are offered the following options:
   - Reinstall System
   - Upgrade existing Mitel Networks server 10.5.x.x system

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

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

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

**21.** If the MiCollab Client application is supported on the system, the following message appears in the server manager: The MiCollab Client Application has been detected on your system. Please use the **MiCollab Client Integration Wizard** prior to managing the application. Click [here to cancel this warning](#). You can either
  - integrate the MiCollab Client database with the MiCollab system database and support MiCollab Client in integrated mode. This is the recommended mode. See “Configure MiCollab Client Mode” on page 71 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 98 for requirements and instructions.

**22.** New fields were added to the User and Services Network Element form during the upgrade. Provision these new fields with appropriate settings:
  - In MiCollab server manager, under **Applications**, click **Users and Services**
  - Click the **Network Elements** tab.
  - Select the Network Element and click **Edit**. The “Standard Phone COS” and "Record-a-Call COS” settings were restored from the backup.
  - Enter a "Default COR".

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

**24.** Perform a database backup of the newly upgraded system.

**WARNING:** AFTER YOU UPGRADE TO MI-COLLAB RELEASE 7.2 OR LATER, YOU CANNOT RESTORE A BACKUP FROM A PRE-RELEASE 7.2 SYSTEM, SO IT IS CRITICAL THAT YOU MAKE A BACKUP NOW.

**25.** If the MiCollab system is connected to MiVoice Office 250 or MiVoice Office 400 platform(s), you must configure port 5058 on the MiVoice Office(s) to support SIP communication from the NuPoint application.
UPGRADE TO VMICOLLAB 7.3

UPGRADE PREREQUISITES

- Ensure that the virtual machine has the required resources (see the Virtual Appliance Deployment Guide).
- To upgrade to MiCollab Release 7.3, your current system must be running Release 5.0 or later and valid software assurance (SWAS) must be active.

DEPLOY VMICOLLAB 7.3 OVA FILE AND RESTORE BACKUP

1. Download the vMiCollab 7.3.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 56 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 89 for instructions).
3. Deploy the vMiCollab 7.3 OVA file on the host system (see page 57 for instructions).
4. Power up the vMiCollab VM.
5. Choose your preferred keyboard from the list (default is us).
6. You are prompted to restore. When the system prompts you with "Do you wish to restore from backup?", choose one of the following options:
   - Select Restore from network share. Follow the prompts to specify the location of the backup file and start the restore, or
   - Select Restore from removable device, or
   - Select Restore from running server option to retrieve the configuration from an existing MiCollab server. This option shuts down the server that you are retrieving the configuration from before bringing up the new server. It configures the new system
with the IP address of the old system.

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

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

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

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

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

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

13. Select the latest software version for installation.

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

15. Click **Install**.

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

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

17. After the optional software is installed, check that all applications and application data is present.

18. If the MiCollab Client application is supported on the system, the following message appears in the server manager: The MiCollab Client Application has been detected on your system. Please use the **MiCollab Client Integration Wizard** prior to managing the application. Click **here** to cancel this warning. You can either

   - integrate the MiCollab Client database with the MiCollab system database and support MiCollab Client in integrated mode. This is the recommended mode. See “Configure MiCollab Client Mode” on page 71 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 98 for requirements and instructions.

19. New fields were added to the User and Services Network Element form during the upgrade. Provision these new fields with appropriate settings:

   - In MiCollab server manager, under **Applications**, click **Users and Services**
   - Click the **Network Elements** tab.
   - Select the Network Element and click **Edit**. The “Standard Phone COS” and “Record-a-Call COS” settings were restored from the backup.
- Enter a "Default COR".
- Enter the "Call Reroute First Alternative (CRFA)" index number. On the MiVoice Business platform, program the CRFA index number with the desired destination number.

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

21. Ensure that your UCC V3 licenses have been upgraded to UCC V4 licenses:
   - Log into the server manager
   - Under Applications, click Licensing Information.
     If not, perform a manual sync with the AMC.
   - Under ServiceLink, click Status.
   - Click Sync.

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

WARNING: AFTER YOU UPGRADE TO MICOLLAB RELEASE 7.3, YOU CANNOT RESTORE A BACKUP FROM A PRE-RELEASE 7.0 SYSTEM, SO IT IS CRITICAL THAT YOU MAKE A BACKUP NOW.

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

UPGRADE FROM MICOLLAB 7.X TO MICOLLAB 7.Y

You can upgrade within the same release (for example, from MiCollab 7.0 to 7.0 SP1 or from MiCollab 7.2 to 7.3) from the MiCollab server manager ServiceLink > Install Applications panel. Refer to the online help for instructions.

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

UPGRADE VMICOLLAB CONFIGURATION

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

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

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

### INSTALLING ADDITIONAL (MISSING) APPLICATIONS

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

**ADD APPLICATION FROM SERVER MANAGER**

1. Log into MiCollab server manager.
2. Under ServiceLink, click **Install Applications**.
3. Click the **Install Applications** tab.
4. Select the latest software version for installation.
5. Scroll through the table and locate the blade for the application/service that you are adding to the system.
6. For each application/service you want to install:
   a. Select the **Install** box.
   b. Select the **Download from AMC** box to download and install software from the Application Management Center.
      -or-
      Clear the **Download from AMC** box to download software from local media (CD/DVD or USB).
7. If you are installing from USB, click **Query USB Storage Devices**. The system detects and lists all of the USB devices connected to the local computer. These devices will be searched for application software when installation commences.
8. Click **Install**.
9. If required, you will be prompted to insert any optional software CD/DVDs. Click **Continue**. Progress is displayed

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

10. Installing a blade creates new menu items in the navigation menu to allow you to administer the application/service.
11. After you install a blade, launch the associated online help from the application/service. The online help provides information on how to program and use the blade.
12. For MiCollab applications, such as MiCollab Client or MiCollab AWV, you can quickly apply the new service to the users by updating the User and Services template with the new service. Then apply the template to the users.

REMOVING AN APPLICATION DURING INITIAL INSTALLATION

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

DOWNGRADING APPLICATION SOFTWARE

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

PERFORMING BACKUPS

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

• **Server Manager "Backup"**: allows you to perform back ups to a local desktop computer or schedule backups to a network file server

• **Server Console "Perform Backup"**: allows you to back up to a USB device or to a network file server

• **VMware Tools**: For vMiCollab deployments, you can use the methods listed above to obtain a vMiCollab database backup. In addition, you can use VMware tools to obtain a backup of the vMiCollab OVA file. Refer to the Virtual Appliance Deployment Guide for instructions.

Notes:

1. You can use different filenames for backup files, but the filename must not contain spaces and the file extension must be either .tgz (unencrypted) or .aes256 (encrypted).

2. To ensure that MiCollab has consistent Network Element (ICP) information, you must use these MSL backup procedures. If you restore backups that were created from inside the individual applications, incorrect Network Element data may be restored to the MiCollab server.

3. To restore the data, you must transfer the backup file to a storage medium (USB device or network share).

4. If MiCollab is deployed in LAN only mode with Teleworker running remotely on an MBG server in the DMZ, you should back up both the MiCollab server database and the MBG server database at the same time.

5. If your site uses Google Integration features (such as, calendar integration), it is recommended that you record the integration settings that are entered in Google Apps configuration tabs and store these settings in a file with the backup. These settings are not retained in the backup.
SERVER MANAGER "BACKUP"

BACKUP TO DESKTOP

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

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

1. Log into the Administrator portal (server manager). See page 43 for instructions.
2. Under Administration, click Backup.
3. Select the Backup to desktop option.
4. Click Perform. MSL prepares the system for backup and displays the following:
   - The "Operation status report" with the estimated backup size. Ensure that your browser and target file system support downloads of this size.
   - The "Backup Encryption" option.
5. (Optional) To encrypt the backup file, enter an Encryption Password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. The encrypted backup file is identifiable with an .aes256 extension.
6. Click Download Backup File.
7. When prompted to Open or Save, click Save.
8. In the file download window that appears:
   - Name the file and then select the location where the file will be saved. Note that the filename of the backup must not contain any spaces; otherwise, you will receive an error when you attempt to restore it.
   - Click Save.
   - In the Download Complete Window, click Close.
   - After saving, you can copy the backup file to a CD/DVD or USB storage device, if required. The backup file is identifiable by its extension, either .tgz (unencrypted) or .aes256 (encrypted).

SCHEDULE BACKUPS TO NETWORK FILE SERVER

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

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

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

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

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

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

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

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

**To perform an immediate backup**

1. Click **Backup Now**.

**To schedule backups to a network file server:**

1. Under **Administration**, click **Backup**.
2. From the **Select an action** list, click **Configure network backup**.
3. Click **Perform**.
4. Select the frequency with which you want to perform backups. Backup file names will include timestamps, for example: `mslserver_<hostname>_yyyy-mm-dd_hh-mm.tgz`.
   - To disable regularly scheduled backups, click **Disabled**.
   - For Daily backups, select a time of day (hour, minute, AM/PM)
   - For Weekly backups, select a time of day, and day of the week
   - For Monthly backups, select a time of day, and day of month
5. (Optional) To encrypt the backup file, enter an **Encryption Password**, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters.

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

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

**SERVER MANAGER SFTP BACKUP TO LINUX SERVERS**

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

**Allow Access on the Backup Server**

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

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

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

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

**Configure an SFTP backup**

1. In the server manager, under Administration, click Backup.
2. Select Configure network backup and click Perform.
3. In the Network Backups screen, enter the
   - IP address of the backup server
   - Username and password of a valid user on the backup server who has access to the required directory.
   - Domain and Sharename are not required. (If a Sharename is entered, MSL will attempt to connect to it using Samba (i.e. Windows backup). If that connection fails, MSL will then attempt an SFTP connection.)
4. (Optional) You can enter a sub-directory where the file will be stored. For SFTP backups, if a directory is not specified, the file is stored in the / directory.
5. (Optional) To encrypt the backup file, enter an Encryption Password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters.
   **Note**: You will be prompted to enter the password when you restore from backup. If you fail to remember the password, you will not be able to restore the data contained in the backup file.
6. Click Save. When a valid configuration is entered, the Backup Now button appears.
7. Click Backup Now or configure a backup schedule and click Save.

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

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

**SERVER CONSOLE "PERFORM BACKUP"**

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

The backup file size limit for a USB or network backup is set by the destination file system: 4 GB for a FAT32, 2 TB (terabyte or trillion bytes) for NTFS, and 16 GB to 16 TB for EXT3 (depending on file system block size). The current MSL EXT3 block size is 4096 bytes which allows file sizes of 2 TB.
1. Access the server console Welcome menu (see page 92).
2. Log in as "admin".
3. From the console, select the option to **Perform backup**.
4. Select a destination for the backup file:
   - Backup to USB Device
   - Backup to Network File Server.

**BACKING UP TO USB DEVICE**

1. Select **Backup to a USB Device**.
2. At the prompt, insert the USB device in the MiCollab server (if not already in place) and then click **Next**.
3. When prompted, enter a filename for the backup file (default is 'mslserver'). Note that the filename of the backup must not contain any spaces, otherwise, you will receive an error when you attempt to restore it. The file extension, either .tgz (unencrypted) or .aes256 (encrypted), is added automatically.
4. (Optional) To encrypt the backup file, enter an encryption password, and then re-enter it. To create a strong password, use a mix of characters, numbers and symbols, plus both upper and lower case characters. Click **Next**.

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

5. MSL displays an estimate of the size of your backup. Click **Proceed**.
6. When the backup is complete, remove the USB device when prompted. Click **Continue**.
7. Re-mount the USB device and verify that the backup has been performed successfully using the verification procedure listed under “Verify Backup Data” on page 91.

**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 92).
2. Log in as "admin".
3. From the console menu, select the option to **Verify backup file**.
4. At the prompt, insert your USB device. (Note: if your USB device was left mounted after your last backup, you must remove it and re-mount it now.)
5. From the list, select your storage device type and then click **OK**. Verification of the file is confirmed. If you receive an error message, you cannot use this backup file for the restore. Check your storage media and try the backup procedure again. See the MiCollab for Communications Platforms - 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 92).
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 43).
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 42, 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 43).
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/](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](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](http://www.openssh.com/windows.html)

A commercial SSH client is available from SSH Communications Security at: [http://www.ssh.com/buy/](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 Standalone MBG server is deployed in either in the DMZStandalone MBG server requires the Remote Proxy Services application.

**To configure remote access to the MiCollab system:**

1. Log into the MSL server manager on the standalone MBG server.
2. Under **Applications**, click **Remote Proxy Services**.
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 101, 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 109</td>
</tr>
<tr>
<td>NuPoint Unified Messaging</td>
<td>“Troubleshooting Applications” on page 109</td>
</tr>
<tr>
<td>MiVoice Border Gateway</td>
<td>“MiCollab Client” on page 116</td>
</tr>
</tbody>
</table>

**VIEWING ALARMS**

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

To view events:

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

**CONVERSIONS AND MIGRATIONS**

This section provides instructions on how to
- Convert a MAS Server Release 4.0 or later database to a MiCollab Virtual Appliance (vMi-Collab) system
- Migrate a standalone MiCollab Client database to a MiCollab Server or MiCollab Virtual Appliance system.

**CONVERT A MICOLLAB SERVER DATABASE TO VMICOLLAB**

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

**CAUTION:** Before you attempt to perform the conversion, review Table 7, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 125 to ensure that the conversion is supported for your configuration.

**CONDITIONS AND CONSTRAINTS**

The following conditions and constraints apply:
• You can only convert MAS Release 4.0 or later database backups to vMiCollab deployments. Conversions from releases prior to Release 4.0 are not supported.

• All application data programmed in the vMiCollab database is overwritten by the backup data during the restore operation. The data in the backup is not merged with the existing database in the vMiCollab system.

• If the vMiCollab system has additional applications that are not included in the restored database, these application databases will not contain any data after the restore. They will be blanked out during the restore.

• Before you convert, ensure that the existing MiCollab system does not exceed the vMiCollab capacity limits. Refer to the MiCollab for Communications Platforms - 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 7, “Supported Backup and Restore Scenarios (after upgrade to Release 6.0),” on page 125 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 56 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 57.
  - 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 85 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 91 for instructions.
2. Launch the vSphere Client application on the network PC.
   - Click Start -> All Programs.
   - Click VMware -> VMware vSphere Client.
   - Enter the IP address or hostname of the Hypervisor ESX/ESXi Host server or Enter the IP address or hostname of the vCenter Server.
   - Enter your username and password.
   - Click OK.

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

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

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

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

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

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

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

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

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

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

12. Click the Install Applications tab.

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

14. Select the latest software version for installation.

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

16. Click Install.
17. After the applications are installed, reboot the MiCollab server.

18. After the optional software is installed, check that all applications and application data is present.

MIGRATE STANDALONE MICOLLAB CLIENT TO MICOLLAB SERVER OR VMICOLLAB

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

There are several options:

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

CONDITIONS AND CONSTRAINTS

The following conditions and constraints apply to the migration:

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

BEFORE YOU BEGIN

- Purchase the required upgrade part number and apply it to your Application Record ID:

Note: The MiVoice Business Express ISO and NuPoint ISO files are not available from the AMC for download. You must install them from a network share or from DVDs. Refer to the Install Applications page online help for instructions.
- MiCollab Add-on to MiCollab Client - PN 54005444
or
- vMiCollab Add-on to MiCollab Client - PN 54005445

☐ Ensure that you record your Application Record ID and have it available before you begin the migration.

☐ Schedule the migration to occur after business hours. MiCollab Client services will be down during the migration.

PERFORM THE MIGRATION

1. Obtain a backup of the MiCollab Client Server database from the MSL Server Manager Backup page. Save the backup to a network file server. Refer to “Schedule Backups to Network File Server” on page 86 for instructions.

2. Shut down the MiCollab Client server.

3. Install MiCollab Release software:
   - Install MiCollab Server (page 29). During the installation of the MSL operating system, you must access the MiCollab server manager and install the application software. See “Install Application Software” on page 42.
   or
   - Install vMiCollab (page 49). 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 43 for instructions.

6. Under Applications, click MiCollab Client.

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

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

9. Click Import Mitel UC Server Configuration.

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

For Desktop Clients:

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

*For Mobile Clients:*

- Select the **MiCollab Client Mobile Client** application.
- Select **Settings**.
- Select **Account Options**
- Enter the MiCollab FQDN in the Server IP field.

11. If your site does not use MiVoice Office 250 systems and if you do not require Active Directory Integration with MiCollab Client, integrate the MiCollab Client database with the Users and Services application. See “Configure MiCollab Client Mode” on page 71 for instructions.
Chapter 8

TROUBLESHOOTING
## GENERAL TROUBLESHOOTING

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

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| Error 404 - File Not Found when accessing the MiCollab End User portal via VPN | VPN is on a different subnet from the MiCollab server so the IP address of VPN connection must be added to the list of Trusted Networks | To find your VPN IP address:  
1. Access the server manager  
2. Under Administration, click **View Log Files**  
3. From the **Choose a log file to view** list, click **httpd/error_log**  
4. Scan the logs for your VPN IP address  
5. Follow the instructions on page 44 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 44 |
| 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 | |
<p>| 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 | If you have logged out of the server console by answering &quot;No&quot; to the &quot;Do you want to install software from CD&quot; prompt, you may have interrupted the install sequence | Reboot the server. Log in as admin and select the server console option to Install software from CD/DVD |</p>
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Message: Fatal Error Caught, Can’t call method “prop” on an undefined value at /usr/lib/perl5/site_perl/es♠/Blades/Blade.pm line 1005 when installing NP-UM Prompts</td>
<td>The CD/DVD drive is unable to read information from the CD/DVD</td>
<td>Ensure that the CD/DVD is clean and smudge-free</td>
</tr>
<tr>
<td>SAA TUI reports experiencing &quot;Technical Difficulty&quot; and &quot;Your call will be transferred to an operator.&quot; when you speak the Department prompt</td>
<td>Department name may have been programmed with an apostrophe included</td>
<td>In the MiCollab USP or the NuPoint application, edit the Department name so it does not include an apostrophe</td>
</tr>
<tr>
<td>While you are in the Server Manager Administrator portal or MiCollab End User portal you receive the following error message: &quot;The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.</td>
<td>A software update is in progress. During the software update, the tomcat server restarts. While the restart is in progress, you cannot use the Administrator portal and MiCollab End User portal web interfaces.</td>
<td>Wait approximately 5 minutes until the tomcat server has finished restarting.</td>
</tr>
<tr>
<td>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 84. Then repeat the application installation procedure. See “Installing Additional (Missing) Applications” on page 84.</td>
</tr>
</tbody>
</table>
### Troubleshooting

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
</table>
| When performing a restore, you get the following error message: "Error preparing for system restore" | 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. |
| 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 84. Then repeat the software update installation procedure. See “Performing Backups” on page 85. |
| Users and administrators are unable to access the MiCollab web portals (for example, MiCollab End-User Portal) using Internet Explorer 10. | In MiCollab Release 7.1, the TLS 1.0 security protocol is enabled by default. If you disable support for TLS 1.0, users will be unable to access the MiCollab web portals using Internet Explorer 9 and 10. | Upgrade to Internet Explorer 11.0.  
OR  
Enable TLS 1.1 and 1.2 in your Internet Explorer 10 browser:  
1. Select **Tools > Internet Options > Advanced > Security**.  
2. Enable **Use TLS 1.1**  
3. Enable **Use TLS 1.2**  
4. Click **Apply** and then **OK**. |
| When you boot up a MiCollab system running on a DL360 G6 server, the following error messages appear:  

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

The Broadcom NC382T PCI Express Dual Port NICS were both detected with 00:00:.... MAC addresses. | 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 39 for details). |
<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>MiVoice Conference Unit is not functioning correctly.</td>
<td>The current SIP Device Capabilities settings do not support the MiVoice Conference. When you select a device type of &quot;UC Endpoint&quot; the SIP Device Capabilities number defaults to 71. However, the settings assigned to 71 do not fully support the MiVoice Conference Unit.</td>
<td>1. In USP, change the default SIP Device Capabilities number from 71 to a value between 1 to 60. 2. On the communications platform, program the assigned SIP Device Capabilities number with the settings required to support the MiVoice Conference Unit. 3. See the MiVoice Conference Unit Administrator's Guide on the Mitel Customer Documentation site for the required settings.</td>
</tr>
<tr>
<td>Users and administrators are unable to access the MiCollab web portals (for example, MiCollab End-User Portal) using Internet Explorer 9 or 10.</td>
<td>In MiCollab Release 7.1 or later, the TLS 1.0 security protocol is enabled by default. If you have disabled support for TLS 1.0, users will be unable to access the MiCollab web portals using Internet Explorer 9 and 10.</td>
<td>Upgrade to Internet Explorer 11.0. OR Enable TLS 1.1 and 1.2 in your Internet Explorer 10 browser: 1. Select Tools &gt; Internet Options &gt; Advanced &gt; Security. 2. Enable Use TLS 1.1 3. Enable Use TLS 1.2 4. Click Apply and then OK.</td>
</tr>
<tr>
<td>You see the following alarm in server manager: &quot;I/O problems detected!&quot; Or, you receive an e-mail from the server indicating an I/O or file system problem.</td>
<td>The system is experiencing problems which has led to switching to read-only file system. This issue can be caused by slow network connections, heavy disk I/O or problems with the data storage.</td>
<td>Reboot the MiCollab server.</td>
</tr>
<tr>
<td>When you attempt to access the MiCollab End User portal login page, you receive a &quot;500 Internal Server Error&quot; in your browser.</td>
<td>Issue with browser cookies</td>
<td>Clear your browser cache.</td>
</tr>
</tbody>
</table>

**ONLINE HELP TROUBLESHOOTING**

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents is not present or not functioning correctly in Internet Explorer 10 or 11</td>
<td>Help compatibility issues with Internet Explorer 10 or 11.</td>
<td>Put the browser in compatibility mode. For Internet Explorer 10, click the Compatibility View icon located in the browser address bar on the right side.</td>
</tr>
<tr>
<td>Help topic text is not appearing in Internet Explorer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Troubleshooting

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot display online help in Google Chrome browser locally.</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>In the online help, numbered steps are ordered incorrectly and text formatting is inconsistent.</td>
<td>You need to modify your Internet Explorer compatibility settings.</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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>SYMPTOM</td>
<td>POSSIBLE CAUSE</td>
<td>CORRECTIVE ACTION</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Voice quality issues</td>
<td>vMiCollab is installed in the vSphere environment using <strong>Thin</strong> provisioning. Thin provisioning can cause voice quality issues due to disk sharing.</td>
<td>Reinstall vMiCollab and select <strong>Thick</strong> provisioning during the install wizard.</td>
</tr>
</tbody>
</table>
|                                              | VMware environment is not configured with the required resources.              | 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. |
| 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>User receives the following error message when upgrading MiCollab AWV client: The executable could not be downloaded from server to the PC in https url mode.</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.&lt;br&gt;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.&lt;br&gt;2. Go to /usr/awc/connpoint/content.&lt;br&gt;3. Download the MCAClient.msi to local directory.&lt;br&gt;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.&lt;br&gt;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. |
### 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 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. 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>
<tr>
<td>The MiCollab Audio, Web and Video Conferencing Client does not upgrade, or the upgrade is slow to complete.</td>
<td>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.</td>
<td>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. 3. Install the Windows Installer Clean Up Utility, available for download from Microsoft.com. 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.</td>
</tr>
<tr>
<td>The user has an existing tab for an appointment form (such as “Web Conferencing”) and they run the Outlook Form install. A new form is not installed for Collaboration.</td>
<td>The installation makes the form available, but the install does not force a new tab to appear in Outlook.</td>
<td>The corrective action will help only if the previous Outlook form is part of a different software application. If the existing default Outlook form belongs to the previous version of MiCollab Audio, Web and Video Conferencing, the default form must be removed before the new form can be installed. Follow these steps: open the Outlook Calendar Appointment &gt; “Tools” Menu &gt; “Forms” Option &gt; “Choose Form” Option &gt; Look in “Calendar” &gt; Select “Collaborate” When you choose “Collaborate,” it replaces your “Web Conferencing” appointment form/tab.</td>
</tr>
</tbody>
</table>
## Troubleshooting

<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</td>
<td>The conference leader attempted to add an outside phone number and did not</td>
<td>The conference leader must type the complete phone number that includes</td>
</tr>
<tr>
<td>participant’s outside phone number (not extension) using the Web</td>
<td>use the correct dialing format.</td>
<td>country code and area code, if applicable, with an outside number when adding a</td>
</tr>
<tr>
<td>interface.</td>
<td></td>
<td>participant to the conference using the Web interface.</td>
</tr>
<tr>
<td>An operator error message is audible in the conference: &quot;It is not</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</td>
</tr>
<tr>
<td>necessary to dial a 1 when dialing this number.&quot; The audio may be</td>
<td></td>
<td>number.</td>
</tr>
<tr>
<td>different, depending on the service provider.</td>
<td></td>
<td>For example, 602 and 480 are two of the area codes for Phoenix, Arizona. For</td>
</tr>
<tr>
<td></td>
<td></td>
<td>these area codes, add the following DAS Rules:</td>
</tr>
<tr>
<td></td>
<td>DAS Rule 1 5/%+1(602.)9/=9/@&lt;primary internal IP address&gt;/f</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DAS Rule 2 5/%+1(480.)9/=9/@&lt;primary internal IP address&gt;/f</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The result: any phone number starting with 1602 or 1480 will have the leading</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;1&quot; stripped off, replacing it with a &quot;9,&quot; the number, @, and then the IP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>address.</td>
<td>For example, assuming that the phone number to be dialed is 1-602-555-1212 and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the IP address configured in TCP/IP Settings is 192.168.22.55: 16025551212 becomes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
<td>SIP default settings are incorrect.</td>
<td>Use the default SIP settings.</td>
</tr>
<tr>
<td>fails. The two users are briefly connected to one another, but then</td>
<td></td>
<td></td>
</tr>
<tr>
<td>that call drops as well. Other users on the conference hear garbled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>voice while the failure is occurring.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>One-way audio is experienced when the MiCollab Audio, Web and Video</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>Conferencing server makes an outbound call using the MiVoice Office 250</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PBX.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When in a conference on an Android Xoom tablet, the sharing viewer</td>
<td>The cause of this issue is unknown.</td>
<td>There is no solution for this issue.</td>
</tr>
<tr>
<td>flickers constantly if the shared area contains a blinking cursor.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 6: Conferencing Error Messages for Alarm/Alert Conditions

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>If a user un-installs a previously installed version of MiCollab AWV client and then clicks Share in the web client, the browser displays Page not found error.</td>
<td>Previous information remains in the mitelCollab cookie.</td>
<td>User should remove the mitelCollab cookie from their browser. For example, in Google Chrome: 1. From the Google toolbar, click Settings 2. Click Show advanced settings. 3. Under Privacy, click Content Settings . . . 4. Under Cookies, click All cookies and site data. 5. Choose the MiCollab server and cookie (mitelCollab), click x to remove and then click Done.</td>
</tr>
<tr>
<td>Users running MiCollab Desktop Client Release 7.0 or earlier client are unable to upgrade the MiCollab AWV client to Release 7.1</td>
<td>User is attempting to upgrade the MiCollab AWV client to Release 7.1 from a MiCollab Desktop Client Release 7.0 or earlier client. This upgrade path is not supported.</td>
<td>User should upgrade to MiCollab Client Release 7.1 first, then perform the AWV client upgrade. OR User should upgrade the AWV client from the AWV portal or through the AWV Desktop Client Launcher.</td>
</tr>
<tr>
<td>UC 360 unable to connect to AWV conference.</td>
<td>TLSv1.0 is disabled.</td>
<td>Enable TLSv1.0 on the MiCollab server.</td>
</tr>
</tbody>
</table>

**Note:** The following Registry Sections contain keys pertaining to the MiCollab Audio, Web and Video Conferencing 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

### 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>&quot;Enterprise alarm&quot; Message = &quot;no phone trunks are operational&quot;</td>
<td>No VOIP ports available to make or receive calls.</td>
</tr>
</tbody>
</table>
### Table 6: 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>database restart (alert)</td>
<td>“Enterprise alert” Message = “database restart at HH:MM:SS MM/DD/YYYY”</td>
<td>The Database service was restarted at the specified time.</td>
</tr>
<tr>
<td>mux restart (alert)</td>
<td>“Enterprise alert” Message = “Sip multiplexor restart at HH:MM:SS MM/DD/YYYY”</td>
<td>The muxer application was restarted at the specified time.</td>
</tr>
<tr>
<td>tp240driver restart (alert)</td>
<td>“Enterprise alert” Message = “phone trunk driver restart at HH:MM:SS MM/DD/YYYY”</td>
<td>The main call server was restarted at the specified time.</td>
</tr>
<tr>
<td>Fewer than n ports are still available (trunkalert)</td>
<td>“Enterprise alert” Message = “only %d ports are currently unused at %s$, %lines, HH:MM:SS MM/DD/YYYY”</td>
<td>This is a number of ports available threshold alert.</td>
</tr>
<tr>
<td>Some trunk line went down (trunkalert)</td>
<td>“Enterprise alert” Message = “trunk lines %d went down HH:MM:SS MM/DD/YYYY”</td>
<td>Specified trunk ID went out of service.</td>
</tr>
<tr>
<td>Some trunk line(s) came up (trunkalert)</td>
<td>“Enterprise info” Messages = “trunk lines %linecode ($resultCode) came up HH:MM:SS MM/DD/YYYY”</td>
<td>Trunk(s) ID are now in service at the specified time.</td>
</tr>
</tbody>
</table>
## MICOLLAB CLIENT

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>After you upgrade MiCollab from Release 7.0 to Release 7.1 or later in a deployment that supports either a MiVoice 5000 or a MiVoice MX-ONE communications platform, MiCollab Client is not functioning correctly.</td>
<td>BluStar server was not shut down or disconnected from MiCollab prior to the upgrade. The MiCollab CSTA Proxy that is included with MiCollab Release 7.1 is conflicting with the BluStar server CSTA functionality.</td>
<td>1. Shut down the BluStar server. OR Disconnect the BluStar server by logging into the BluStar Web Admin Portal, deleting the MiCollab IP Address from the CSTA Proxy Configuration page, and then clicking Save. 2. Log into MiCollab server manager. 3. Access the MiCollab Client Service Perform Server Diagnostic page. 4. Stop and then restart the MiCollab CstaProxy service.</td>
</tr>
<tr>
<td>MiCollab Client loses connection with the MiCollab server.</td>
<td>The client’s Login ID was changed.</td>
<td>1. Re-deploy the client 2. Send the user a fresh deployment email so the new Login ID can be communicated to the client.</td>
</tr>
<tr>
<td>When you attempt to run the MiCollab Client Integration Wizard, the following error message is displayed “WmiAppException creating new enterprise: Tenant license exceeded.”</td>
<td>You have selected the PBX Type and installed the application software in the Install and Upgrade Applications panel. However, the system has not received its MiCollab Client license from the Application Management Center (AMC) yet, so the wizard is unable to run.</td>
<td>Wait at least 7 minutes and then restart the MiCollab Client wizard again.</td>
</tr>
<tr>
<td>One-way audio is occurring in the following connection: A MiCollab Client mobile (iOS or Android) user places a call through the MiVoice Border Gateway to a user on a communications platform (for example MiVoice MX-ONE). The called party does not receive audio from the MiCollab Client mobile user.</td>
<td>The packetization time on either the MiVoice Border Gateway and/or the communication platform is not set correctly to support MiCollab client. If you are using G.729 with MiCollab Client, the packetization time must be set to support 20 ms.</td>
<td>On the MiVoice Border Gateway: 1. Log into the server manager. 2. Under System Configuration &gt;Settings, ensure that RTP framesize is set to Dynamic. Log into the communication platform management interface. Ensure that the system is set to support • G.729 codec • 20 ms packetization</td>
</tr>
</tbody>
</table>
### MIVOICE BORDER GATEWAY

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calls made from a MiCollab for Mobile client to a 3-digit extension are sent out the PSTN instead of going to the extension</td>
<td>The extension number conflicts with an emergency number that is pre-configured in the user's deployment profile. Emergency numbers are exempt from any special routing and are dialed directly. The following emergency numbers are pre-configured: 000, 110, 112, 118, 119, 911, 999</td>
<td>Although it is not recommended, emergency numbers that are not applicable to the user's region can be deleted from the user's profile if the emergency number (for example, 119) conflicts with an existing dialing string (for example, extension 119). Before you delete an emergency number, you should be certain that the user will not be traveling to a region that uses it. To modify the emergency numbers in a user's deployment profile: 1. Log into the server manager. 2. Under Applications, click MiCollab Client Deployment. 3. Click Deployment Profiles. 4. Modify the user’s profile. 5. In the Emergency number field, modify the numbers as required. Multiple emergency numbers must be separated with commas and no spaces. 6. Click Save.</td>
</tr>
</tbody>
</table>

### SIP Teleworker devices are not functioning

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Teleworker devices are not functioning</td>
<td>SIP devices are denied access to the LAN by the MBG server. In the MBG application, the &quot;Restrict SIP Devices&quot; 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.</td>
<td>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 &quot;Restrict SIP Devices option to False. Note: For security, this option should disabled only on a temporary basis.</td>
</tr>
</tbody>
</table>

<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.</td>
<td>MiCollab server is configured in LAN mode with the Teleworker application, but it is not clustered with a MiVoice Border Gateway (MGB) The MiCollab server is a member of multiple MBG clusters. The MiCollab server can only belong to one MBG cluster.</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 belong to one MBG cluster. The cluster must be programmed in the Teleworker Clustering tab with a weight of zero See &quot;Install MiCollab Server in LAN Mode with MiVoice Border Gateway Server(s)&quot; on page 47.</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>
<tr>
<td>Clicking a NP-UM voice message in the MiCollab End User portal results in a blank screen with an icon indicating &quot;applet not found&quot;</td>
<td>Windows Media Player is not selected as the default player.</td>
<td>Set Windows Media Player to be your default player: 1. Close Internet Explorer 2. Right-click in Windows Explorer. 3. Click <strong>Tools</strong> and then click <strong>Folder Options</strong> 4. On the File Types tab, scroll to WAV files 5. Click <strong>Change</strong> and select <strong>Windows Media Player</strong> from the list 6. Click OK 7. Open Windows Media Player 8. Click <strong>Tools</strong> and then <strong>Options</strong>. (If the Tools menu does not appear, click the Media Player icon in the upper left to view.) 9. On the File Types tab, ensure the WAV file check box is selected 10. Click OK</td>
</tr>
<tr>
<td>For the Call Director - Alternate Transfer feature, users who are transferred to the alternate number do not hear the Timeout message if their call is unanswered. Instead, they hear the Message Center Main Menu.</td>
<td>NuPoint on MiCollab is integrated to a MiVoice Office 250.</td>
<td>None. When NuPoint on MiCollab is integrated with a MiVoice Office 250, the Timeout Message for the Call Director – Alternate Transfer feature is not supported.</td>
</tr>
</tbody>
</table>

## GOOGLE APPS TROUBLESHOOTING

<table>
<thead>
<tr>
<th>SYMPTOM</th>
<th>POSSIBLE CAUSE</th>
<th>CORRECTIVE ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitel Google App (for example AWV Google Calendar Integration) is not functioning correctly</td>
<td>Browser incompatibility</td>
<td>Ensure that you are running the applications in a recent version of Google Chrome.</td>
</tr>
</tbody>
</table>
TROUBLESHOOTING LICENSING ERRORS

When administering licenses in your AMC account, you may receive an error message. The following table contains possible error messages, their meanings, and possible solutions:

<table>
<thead>
<tr>
<th>ERROR ID</th>
<th>ERROR MESSAGE</th>
<th>POSSIBLE PROBLEM</th>
<th>POSSIBLE SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>01201</td>
<td>Demo kit base level products can only be applied to servers one-at-a-time</td>
<td>You may be trying to add a demo kit to a server that already has one active demo kit</td>
<td>Recheck the Application Records for the relevant server</td>
</tr>
<tr>
<td>01205</td>
<td>This product can only be assigned to an Application Record under the same end customer as its related/bundled parts; &lt;company name&gt;</td>
<td>Some products (for example, YA) include MiVoice Business user and device licenses for the YA purchaser. You may be trying to assign these user and device licenses to a customer other than the original purchaser</td>
<td>Assign related/bundled licenses to the appropriate customer account as listed in the error message</td>
</tr>
<tr>
<td>01210</td>
<td>This product attempts to deliver an invalid application type for this application record</td>
<td>You may be trying to add another base product to an Application Record that already has a base product applied. (For example, you cannot add a Teleworker starter kit to an Application Record that has a MiVoice Business starter kit applied.)</td>
<td>Each base product requires a separate Application Record</td>
</tr>
<tr>
<td>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>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>01213</td>
<td>This product is missing a required base product component that must be attached to this application record first</td>
<td>You may be trying to install a subsidiary license (for example, an IP Phone License) to an Application Record that has no base product assigned. If you are adding licenses to a legacy system (3300 ICP system licensed prior to April/05 or SX-200 system licensed prior to April/06), it is possible that your Application Record has not been transferred.</td>
<td>Ensure that a base product (for example MiVoice Business or YA starter kit) is installed before you attempt to add subsidiary licenses. Every effort has been made to load all legacy data files but it is possible that some systems were missed. Send an email to the AMC and request that your application record be loaded from legacy data files.</td>
</tr>
<tr>
<td>01220</td>
<td>The number of application records that can apply this product has already been reached.</td>
<td>You may be trying to add products beyond the maximum number of times allowed. (For example, by default, only one Teleworker demo kit is allowed. You cannot add an Application Record for another demo kit for the same Customer.)</td>
<td>--</td>
</tr>
<tr>
<td>01221</td>
<td>This product has already been used the maximum allowed for this application record</td>
<td>You may be trying to use a product beyond the maximum number of times allowed. (For example, some reward programs offer free product incentives. The number of these products per Application Record may be limited.)</td>
<td>Contact the AMC for further assistance.</td>
</tr>
<tr>
<td>01230</td>
<td>This product requires an active '&lt;name of service&gt;' service component</td>
<td>You may be trying to apply an extension to a product that has expired. (For example, your Teleworker starter kit is over one year old. You cannot attach a Teleworker Support extension to this record.)</td>
<td>Ensure that you purchase extension products before the expiration of the base product.</td>
</tr>
<tr>
<td>01240</td>
<td>Activation of this product will exceed the maximum number of licenses for this application record</td>
<td>You may be exceeding the maximum number of users that your base equipment is designed to accommodate. (For example, Teleworker is designed for 500 users. You cannot activate more than 500 licenses.)</td>
<td>Your product may need upgrade.</td>
</tr>
</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.
TROUBLESHOOTING ACTIVE DIRECTORY PROBLEMS

PROBLEM
1. When the administrator attempts to add an Active Directory user to MiCollab Users and Services application using the Bulk User Provisioning tool, an error is displayed.

AND/OR
2. After users change their Active Directory password, they are unable to log into MiCollab.

POSSIBLE CAUSE
Latency or delay in the network is preventing Active Directory from responding to a search request from MiCollab. Without the search request results, MiCollab cannot add an Active Directory user.

DETECTING ACTIVE DIRECTORY DELAY
To detect any delay or latency on the Active Directory network at a site, use the "ldapsearch" command. This command opens a connection to an LDAP server and performs a search using specified parameters. The required parameters are:

• LDAP Root DN (or binddn)
• LDAP Root Password (or credentials)
• Login ID for an AD/IDS user.

Find the LDAP root DN and root password by executing the following Linux command in a shell console or a putty window:

```
[root@vmas-server]# more /etc/openldap/slapd.conf | grep binddn
```

Example output:

```
idassert-bind bindmethod=simple binddn="cn=root,dc=maslab,dc=mitel,dc=com"
credentials=d6d7a634-740a-4428-a162-3f7465f4fcdc
```

Replace the "binddn", "credentials", and "login ID" parameters that are marked with angle brackets in the following LDAP search command with the site values:

```
time ldapsearch -x -b "dc=virtual,dc=metadirectory" -D "<binddn>" -w "credentials" (sAMAccountName=<login ID>)
```

The following example uses these values:

• Bind DN: cn=root,dc=maslab,dc=mitel,dc=com
• Credentials: d6d7a634-740a-4428-a162-3f7465f4fcdc
• User login ID: testuser

Using the above values, the LDAP search command will be as follows:
time ldapsearch -x -b "dc=virtual,dc=metadirectory" -D "cn=root,dc=maslab,dc=mitel,dc=com" -w "d6d7a634-740a-4428-a162-3f7465f4fcdc" "(sAMAccountName=testuser)"

The output for the above LDAP search is listed below. The execution time is shown at the end of the display.

# extended LDIF
#
# LDAPv3
# base <dc=virtual,dc=metadirectory> with scope subtree
# filter: (sAMAccountName=testuser)
# requesting: ALL
#

# testuser Test, ad1.virtual.metadirectory
dn: cn=testuser Test,dc=ad1,dc=virtual,dc=metadirectory
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: USER
cn: testuser Test
sn: Test
telephoneNumber: 1889
givenName: testuser
distinguishedName: cn=testuser Test,dc=ad1,dc=virtual,dc=metadirectory
displayName: testuser
name: testuser Test
OBJECTGUID:: wajo7V3pCE6akVkmcf1Yw==
sAMAccountName: testuser
USERPRINCIPALNAME: testuser
mail: testuser@test.com
<SNIP>

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1

real 0m0.942s
user 0m0.003s
CORRECTIVE ACTION

Reduce the latency in your network such that the sum of the "real", "user", and "sys" parameters is less than 15 seconds.

VIEWING/COLLECTING LOG FILES

To assist in troubleshooting, you can either view or download the log files generated by the services running on MiCollab. You access log files from the Administration > View logs file page in the MiCollab server manager. Refer to the online help for instructions.

DATABASE RECOVERY (RESTORE)

This section provides procedures for

- MiCollab Server 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 7: 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 8: 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 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 92.
2. From the Welcome menu, select the Restore from Backup option. The "Restore after Reboot" screen appears.
3. Select Reboot Now.
4. Wait for the system to reboot.
5. At the "Do you wish to restore from backup?" prompt, select Yes.
6. Select the restore method:
   - Restore from another running server
   - Restore from network share
   - Restore from removable device

RESTORE FROM ANOTHER RUNNING SERVER

If you are replacing an existing MSL 9.x server (physical or virtual), you can pull configuration and application data from it while it is still running and restore the data to a new MSL 10.x server.

The restore process automatically shuts down the old server.

Conditions:

• Installing the same ARID on new physical hardware will require a Hardware ID reset.
• If the two servers are on:
  - Connected networks (i.e. there is no router between them), both servers must have the same subnet mask applied.
  - Different networks, MSL will request a gateway/router IP address to use for access. When the restore is complete, the new server must be reconfigured for its own network because it will have inherited the network configuration of the running server.

CAUTION: Booting up the original server again after the restore procedure will result in IP address conflicts.
RESTORE FROM NETWORK SHARE

MSL Releases 10.0 and later support backups over the network to Linux/Unix servers, including to another MSL server, using the Network Backup option in the web-based server manager.

MSL 10.3 supports restore of SFTP backups using the console-based “Restore” option. You can restore application and configuration data during a fresh install of MSL at the “Do you want to restore from backup?” prompt. You can also force a restore “on demand”.

1. In the server console of the server that you are restoring, select Restore from backup.
2. A warning message is displayed and then the server reboots.
3. When the restore options are displayed, select Restore from network share.
4. Select the network interface to use for the restore (i.e. the network interface that has a connection (direct or indirect) to the network file share server).
5. Enter the IP address of the MSL server and the subnet mask to apply:
6. Enter the IP address of the network share server that contains the backup file.
7. If the file server is on a different network than the MSL server, MSL prompts you to enter the gateway IP address to use to access the backup server.
8. Enter the Windows login domain or workgroup of the backup server. (Leave this blank when restoring SFTP backups.)
9. Enter the shared folder name where the backup file is stored. If multiple backup files are stored, you must select the one you want to restore. (Leave this blank when restoring SFTP backups.)
10. Optionally, you can enter a subdirectory or path in which to store the backup file. (For SFTP backups, if you have created a folder on the backup server (e.g. “/backups”), then enter the path to that folder here.) Or press Next to skip this step.

**Note:** If you do not enter a sub-directory here for SFTP backups, the file is stored in the “/” folder by default.

11. Enter the username and password required to log in to the backup server
12. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the Decryption password. Click Next and then Yes.
13. A progress bar is displayed for the restore procedure. When the restore is complete, the server reboots to activate your restored configuration settings.
14. Proceed to “Check Application Data” on page 128.

RESTORE FROM REMOVABLE DEVICE

1. Follow the prompts to identify the backup file, and start the database backup.
2. If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the Decryption password. Click Next and then Yes.
The Progress screen displays the data transfer progress.

**Note:** The filename of the backup must not contain any spaces; otherwise, you will receive an error when you attempt to restore it.

3. If you are restoring a database from a USB device and if "boot from USB" is enabled in the computer BIOS, you must remove the USB memory stick after the data transfer progress bar reaches 100%.

4. Proceed to “Check Application Data” on page 128.

**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 84 for instructions on how to install the missing applications.

2. If MiCollab is deployed in LAN only mode with Teleworker running remotely on an MBG server in the DMZ, you must also restore the MBG server with the current database; otherwise, the databases will be out of sync.

3. If your site uses Google Integration features (such as, calendar integration), re-enter the configuration settings in the Google Apps configuration tabs of the server manager interface.

**VMICOLLAB SYSTEM DISASTER RECOVERY**

You can recover a vMiCollab system database on the same virtual machine by deploying the latest vMiCollab OVF file, restoring your vMiCollab database backup, and then installing the latest MiCollab application software.

- Refer to the Mitel Virtual Appliance Deployment Guide for instructions on how to deploy the OVF file.
- See "Database Recovery (Restore)" on page 124.
- See “Install Application Software” on page 62.

**RESTORING A MICOLLAB SERVER DATABASE TO A DIFFERENT SERVER**

Use the following procedure to restore a

- MiCollab 5.0 or later database to a MiCollab 7.1 server, or a
- MiCollab 7.1 database to a MiCollab 7.1 system on different server hardware.
To restore a database from Server A to a different Server B:

1. Perform a database backup from Server A to a USB device or network server. See "Server Manager "Backup"" on page 86 for instructions.

2. Clear your Hardware ID from the AMC. See “Backup and Restore with Fresh Install” on page 78 for instructions.

3. After you receive an email from Mitel Technical Support stating that the Hardware ID has been cleared from Server A, you can proceed with the migration to Server B. Note that after the Hardware ID is cleared from Server A, it will continues to function.

4. Install MSL 10.3.x.x. on Server B.

5. At the "Do you wish to restore from backup?" prompt, select Yes.
   - Select Restore from network share. Follow the prompts to specify the location of the backup file and start the restore,
   - Select Restore from removable device, or
   - Select Restore from running server option to retrieve the configuration from the existing MiCollab server. This option shuts down the server that you are retrieving the configuration from before bringing up the new server. It configures the new system with the IP address of the old system.
   - If the backup file has been encrypted (identifiable with an .aes256 extension), you will be prompted to enter the Decryption password. Click Next and then Yes.
   - After MSL completes the restore of the Server A database to Server B, the MSL operating system reboots.

6. At the root prompt (or using SSH) login as Admin and select Configure this server to review MSL server configuration settings.

7. Review the settings without changing any parameters and then reboot the server. This step changes the MAC address in the MSL database.

   **Note:** Server B now has the same FQDN and IP address as Server A.

8. After system reboots, log into the server manager. See “Log in to the Administrator Portal (Server Manager)” on page 29 for instructions.

9. Deactivate and then re-activate your ServiceLink account (Application Record ID)
   - Under ServiceLink, click Status.
   - If a service account ID (Application Record ID) is displayed on the Status page, click the here link and then click Deactivate.
   - Enter your Application Record ID and click Activate.

10. At the root prompt (or using SSH), login to the server console as Administrator and select Install MiCollab from CD/DVD. Install the MiCollab Application software from CD/DVD or USB.

11. Under Administration, click Shutdown or Reconfigure. Select Reboot from the drop-down menu and then click Perform. After the reboot is complete, the MiCollab system is operational with the database contained in backup.
INTRODUCTION

This appendix describes off-line licensing and installation for customers who are unable to connect to the Mitel Applications Management Center (AMC) via the internet due to security concerns. Typically, off-line licensing is available to large customers with MiCollab virtual deployments in server-only mode. Note that the optional blades (NuPoint Unified Messaging and Speech Auto Attendant applications) cannot be installed with off-line licensing and installation.

Off-line licensing is available for a set duration of time. Before your licensing term expires, the system generates warnings indicating that you must re-sync the MiCollab system ARID.

Note: If you allow your licensing to expire, then after you re-sync your system ARID, you must reboot the system in order to restart the MiCollab applications.

INSTALLATION OF vMICOLLAB USING OFF-LINE LICENSING

The following procedure describes how to perform off-line activation of licenses from the server manager using a maintenance PC.

To install vMiCollab using off-line licensing:

1. Obtain an Application Record ID (or service account ID) from your authorized reseller.
2. Download the MiCollab OVA file only (see page 56). The NuPoint Messenger and Speech Auto Attendant applications are not supported for off-line licensing and installation.
3. Deploy the vMiCollab vApp (see page 57). If you are deploying on vSphere vCenter, leave the Application Record ID field in the Custom Template blank.
4. Configure or Review the MSL Operating System Settings (see page 57)
   • If you deployed vMiCollab on vSphere vCenter and used the Custom Template to set the MSL Operating System parameters, review the settings in the server console.
   • If you did not use vSphere vCenter, you must configure the MSL Operating System parameters in the server console. When you are prompted for the Application Record ID, leave it blank.
5. Log into the server manager of the maintenance PC, under ServiceLink, click Status.
6. Enter your Application Record ID (also called Service account ID).
7. Select Enable off-line license generation.
8. Click Activate to request an off-line licensing file. The Operation status report page is displayed.
9. Click Download license request file (license_request.zip).
10. In the file download dialog, click Save and save the zip file to a portable storage medium on the maintenance PC.
11. Remove the portable storage device and go to an Internet-connected PC.
12. On the Internet-connected PC, extract the contents of the zip file to a temporary folder.
13. Open the folder and double-click the sync.bat file to execute handshake and synchronization with the AMC.

14. Synchronization occurs with the AMC and the sync.bat file creates a license.zip file containing license files from the AMC. (If you receive a security warning during this process, click Run.)

15. Save the license.zip file to the portable storage device.

16. Remove the storage device from the Internet-connected PC and return to the maintenance PC.

17. Insert the storage device in the maintenance PC.

18. In the server manager of the maintenance PC, under ServiceLink, click Status. Beside Upload license file, click Choose File.

19. In the file upload dialog, browse to the license.zip file that was created by executing the sync.bat file, then click Ok to select the file to be uploaded.

20. Click Upload license file to install the synchronized license key file and activate the purchased options.

21. Transfer the new zip file back to maintenance PC used to access server manager (if applicable).

22. Click Upload license file to upload the license response back into MiCollab.

**Note:** Save your sync.bat file to a portable storage device or PC, in case you want to add additional licenses offline to the system in the future.

**Note:** You cannot install the NuPoint and SAA applications while the system is off-line. If the system cannot access the AMC, installation of these application blades will fail. You must install these applications while the system is online.

**Note:** A virtual application license which is synced off-line will expire after the licensing term. Prior to expiry there will be a series of alarms raised at incremental severity as the expiry time nears. You must sync the system with license file again to clear the alarm and re-enable the licensing.

23. Select the PBX Type from the MiCollab Server Manager.
   - In the server manager, under ServiceLink, click Install Applications.
   - Click the Install Applications tab.
   - Set the PBX Type and then click Next. The list of licensed applications, services, and security patches for the currently installed version of MiCollab appears.

24. Off-line licensing is complete.

**RESETTING THE LICENSE TERM**

You will receive MiCollab alarms near the end of the licensing term that indicates that you must re-sync your system with the licensing file. The following alarms can appear:

- Minor: Mitel Applications Suite (MiCollab) licenses expire in 8 days.
- Major: Mitel Applications Suite (MiCollab) licenses expire in 5 days.
- Critical: Mitel Applications Suite (MiCollab) licenses expire in 2 days.
To reset the license term, log into the server manager.

1. Under ServiceLink, click Status and then click Sync. The alarm will be cleared and your licenses are re-enabled for another term.

2. Perform a system reboot to restart your applications.

**Note:** If you allow your licensing to expire, then after you re-sync your system ARID, you must reboot the system in order to restart the MiCollab applications.

### ADDING LICENSES

Before you can add new licenses, you must generate an off-line license request:

1. Contact the order desk and purchase the new licenses. The new licenses will be assigned against your ARID in the AMC.

2. If you saved your sync.bat file (from initial installation) you can use it to add new licenses to the system. From an internet connected PC, double-click the sync.bat file to execute handshake and synchronization with the AMC.

**Note:** If you cannot find the sync.bat file from initial installation, you must generate a new one. Perform Step 5 to Step 22 of “Installation of vMiCollab Using Off-Line Licensing” on page 132.

3. Synchronization occurs with the AMC and the sync.bat file creates a license.zip file containing license files from the AMC. (If you receive a security warning during this process, click Run.)

4. Save the license.zip file a portable storage device.

5. Remove the storage device from the Internet-connected PC and return to the maintenance PC.

6. Insert the storage device in the maintenance PC.

7. Log into the server manager of the maintenance PC.

8. Under ServiceLink, click Status.

9. Click Sync to generate an offline license request. The Upload license file and Download licensing refresh file buttons are displayed.


11. In the file upload dialogue, browse to the license.zip file that was created when you executed the sync.bat file. Click Save to select the file to be uploaded.

12. Click Upload license file to install the synchronized license key file and activate the purchased licenses.

### UPGRADE

You do not need to re-sync your licenses during an upgrade.
A
Activation errors 91
Administrator
  password 38, 54
Alarms, viewing 95
AMC 17
Application
  record id 54
  record ID number 17, 42
  record ID number for vMiCollab 62
  record, creating 34
  record, creating for vMiCollab 56
  software, obtaining 34
  web pages 43, 62
Applications
  software installation 42
  software packages 3
  supported for vMiCollab 51
  vMiCollab software installation 62
ARID 17, 54

B
Backup, to USB 89

C
CD/DVDs
  software labeling 36
Certificate Authority 44, 64
Certificate, root certificate installation 44, 63
Client system, requirements 43, 62
Co-located mode, for MiCollab Client 71
Configuration
  determining deployment requirements 32
  DHCP server 41
  DHCP server, 61
  DNS server 41
  DNS server, 61
  MSL 56
  MSL, 36
  system name 38
  system name, 58
Configurations, vMiCollab deployment 50
Console, accessing 92

D
Deployment configurations, for vMiCollab 50
Deployment, determining requirements 32
DHCP 41, 61
Disaster recovery 124
DNS server 41, 61
Documentation set
  About 4
  accessing online 6, 7
  MBG 6
  MiCollab 5
  MiCollab Client 6
  Mitel Standard Linux 6
  MiVoice Office 250 6
  NP-UM 6
  NuPoint 4
  Speech Auto Attendant, 6
  Teleworker 4

E
Event viewer 95

F
FTP 92

G
Greenfield site, provisioning 11

H
Hardware
  accessing qualified hardware list 33
  platforms 3
Help troubleshooting 106

I
Industry standard server 4
Installation
  application software 42
  checklist for vMiCollab install 51
  overview 31
  overview of vMiCollab install 50
  vMiCollab application software 62
Integrated mode, for MiCollab Client 71
Introduction
  overview of MiCollab 3

K
Knowledge base articles, accessing 6

L
Licenses
  troubleshooting 119
V
vApp
deployment 57
vMiCollab
deployment configurations 50
installation requirements and constraints 51
supported applications 51

W
Web certificates, installation 44, 63
Work flow
for existing site 12
for new site 11

vApp deployment 57