

MiVoice Conference/Video Phone

RELEASE 2.1, SP7

ADMINISTRATION GUIDE



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>.

MiVoice Conference/Video Phone Administration Guide

Release 2.1, SP7

December 2017

®,™ Trademark of Mitel Networks Corporation

© Copyright 2017, Mitel Networks Corporation

All rights reserved

Chapter 1: New features

New Features and Enhancements	3
-------------------------------------	---

Chapter 2: Introduction

Introduction	9
Identifying the Product Variant.	10
MiVoice Conference Phone	10
MiVoice Video Phone	11
About This Document	11
Related Documentation	11

Chapter 3: Recommended Configurations

Recommended Configurations	15
Conference Room	15
Teleworker Home Office	15
Executive Office Side Table	15
Revolabs Microphone Placement	17

Chapter 4: Quick Start

Introduction	23
Before You Start	23
Conference/Video Phone Interfaces	23
Launching Advanced Settings using the Phone Interface	24
Accessing The Phone Using The Web Interface	25
Obtain Network Settings	26
Configure Static IP addresses	26
Upgrading Software	27
Download the Software	27
Set Up the HTTP/HTTPS Server and Upgrade Software	27
Configure SIP Settings	28
Import/Export Configuration Files	29

HTTP Import	29
USB or SD Card Import	29
Minimal Configuration File for Video Conferencing	30
Minimal Configuration File for Audio Conferencing	31

Chapter 5: **Configuration**

Introduction	35
Auto-configuration of the phone	36
Launching Settings	37
Advanced Settings	38
Configure System Settings	40
SIP Settings	41
Apps Settings	47
Network Settings	48
Contacts Settings	52
Dial Plan	61
Video Settings	63
RDP Settings	64
VNC Settings	65
History Settings	66
Extension Microphone Settings	67
Advanced Settings Password	68
Camera Settings	69
Country Variant	76
Dialpad Settings	77
Licensing and Backup Import/Export	78
Upgrade System Software	82
Debug Settings	86
Web Server Settings	87
Reboot	88
Factory Reset	89
Sound	90
Display	91
Language & Keyboard Settings	92

Date & Time	93
Maintenance Routine	93
Conference/Video Phone Used as Teleworker	94
Troubleshooting	97

Chapter 6: MiVoice Business Configuration

Programming MiVoice Business	101
User and Device Configuration	102
SIP Device Capabilities: SDP Options	107

Chapter 7: MiVoice Office 250 Configuration

MiVoice Office 250 Configuration	111
Mivoice Office 250 System Programming	111
Conference Phone Programming	113

Appendix A: ONVIF Device Manager

ONVIF Device Manager.....	117
---------------------------	-----

Appendix B: Web Server

Conference Phone /Video Phone Web Server	125
Logs Collection	127
Ethernet Trace	128
Configuration	129
Reboot	131

Appendix C: Mass Deployment

Mass Deployment of Conference/Video Phone.....	135
Requirements	135
Programming/Configuration Steps	137

Appendix D: XML File Format

XML File Format	143
Parameter Model	143

XML Tags and Attributes	143
User Configuration	144
Country Variant	144
Certificate	144
Contacts Translation Plan Rules	145
Dial Plan Settings	145
Video Quality Settings	145
Timezone Values	145
Browser Bookmarks	149
Administrator Password	149

Appendix E: Mass Deployment Configuration File Reference

Chapter 1

New features

New Features and Enhancements

This section of the document briefly describes the new features and enhancements available on the MiVoice™ Conference Phone and MiVoice Video Phone with Release 2.1 software.

Release 2.1, SP7

- The application join.me™ is no longer supported.
- The SD Card Upgrade capability is removed from the Chapter 5: Configuration.
- The Web browser is disabled by default. See the Chapter 5: Configuration — “Advanced Settings” on page 38.

Release 2.1, SP6

- Updated support for camera versions — see “Ethernet Camera Firmware” on page 70.
- Updated RDP Settings — see “RDP Settings” on page 64.

Release 2.1, SP5

- Support for the import of contacts from MiVoice Business and MiVoice Office 250 in formatted CSV files. These files can be imported from either USB flash drive or from the HTTP configuration server — see “Contacts Settings” on page 52.
- Support for WV-SPN311 camera — see “Ethernet Camera Firmware” on page 70.
- Support for OfficeWRX™ — replaced Smart Office 2 in “Apps Settings” on page 47.
Note: OfficeWRX does not support Dropbox™ or Box.net.
- Removed ADB startup for normal operations.
- Removed the ability to enable ADB through advanced settings.
- Removed the ability to enable ADB through cfg file.

Release 2.1, SP4

- Software fixes only.

Release 2.1, SP3

- Support for Panasonic WV-SPN310 camera — see “Ethernet Camera Firmware” on page 70.
- The setting Upgrade System Software has a new option “Trust All HTTPS Servers”. You can enter https:// in the HTTP Server Address — see “HTTP Server Upgrade” on page 82.
- Ability to upgrade a MiVoice Conference Phone to a MiVoice Video Phone by applying a purchased license file — see “Upgrade Audio to Video License” on page 80.
- Support for a configurable NTP server— see “Date & Time” on page 92.
- Swedish language support — see “Language & Keyboard Settings” on page 91.
- Mitel Redirection and Configuration Service (RCS) for auto-configuration of the MiVoice Conference/Video phone — see “Auto-configuration of the phone” on page 36.
- New Mitel product branding.

Note: Once the MiVoice Video phone is upgraded to 2.1 SP3, it cannot be downgraded.

Release 2.1, SP2

- New and updated LDAP Server Settings:
 - LDAP Search Base setting— see “LDAP (Auto) Search Base” on page 57.
 - LDAP Search filter changes — see “LDAP Search Filter” on page 57.
- Updates to the XML Configuration File based on the new LDAP settings — see “Mass Deployment Configuration File Reference” on page 151.
- With 2.1, SP1, the \$ and & characters are not supported in any System Settings parameters and in the mass deployment XML cfg file.
- The Web Server now allows the XML configuration file to be uploaded directly to the Conference/Video Phone. As well, the current settings can be downloaded, edited locally and then uploaded to apply any required changes. See “Import Settings Directly” on page 130.
- The UC360 Collaboration Point has been rebranded and is now referred to as the MiVoice Conference Phone and/or the MiVoice Video Phone. It is shortened to Conference Phone or Video Phone depending on the context. It is also referred to as phone.

Conference/Video Phone Release 2.1, SP1

- New SIP Settings — see “SIP Settings” on page 41.
 - Display Name under Account - name of the caller sent during calls that may be shown on the other party's display.
 - Firewall Traversal (STUN and ICE) - enhances SIP call media establishment over the internet when behind NAT firewalls.
 - SPAM Call Filter - allows the Conference/Video Phone to ignore incoming calls that do not originate from the programmed SIP Server.
 - SRTP - supports secure audio.
- LDAP Server Settings change - the **Connect to MBG** button has been removed and this option has been added in the drop down menu in Communications Security type. See “LDAP Settings” on page 54.
- New settings in MiVoice Business Configuration — see “MiVoice Business Configuration” on page 99.
- Updates to the XML Configuration File based on the new SIP settings — see “Mass Deployment Configuration File Reference” on page 151.
- Rebranding name changes: Mitel Communications Directory (MCD) to MiVoice Business and Mitel Border Gateway to MiVoice Border Gateway.

Conference/Video Phone Release 2.1

- Sound — can enable audible clicks for all selections and keyboard input.
See “Sound” on page 89.
- Apps Settings — enables or disables any of the apps that are currently implemented on the Conference/Video Phone. New apps include

- MiCollab Conference
- Cisco™ WebEx® Meetings
- Remote VNC Pro

See “Apps Settings” on page 47 for more information.

- New SIP Settings
 - Security - ability to install trusted root certificates (see “Security” on page 45)
 - Transport - support TLS transport (see “Transport” on page 42)
- VNC Settings — allows the Conference/Video Phone to connect to and control non-MS Windows computers as RDP (Remote Desktop Protocol) does for MS Windows computers. Apple Mac computers which come with a VNC (Virtual Network Connection) server already installed and Linux/Unix computers can use the RemoteVNC application on the Conference/Video Phone. This app is turned off by default.

See “VNC Settings” on page 65 for more information.

- Extension microphones — enables the settings for an Extension Microphone (Revolabs only) if installed. See “Extension Microphone Settings” on page 67 for more information.
- Conference/Video Phone Web Server — enables a Remote Diagnostic Web Application that allows you to access debug and diagnostics through a web service on the Conference/Video Phone. From the Remote Diagnostic Web page, the Administrator can download a configuration XML file.

See “Web Server Settings” on page 86 and “Web Server” on page 123 for more information.

- Mass deployment — The Mass Deployment feature allows an administrator configure multiple units all at once without manually changing the settings for each unit. The Conference/Video Phone settings can be exported to a configuration XML file. This file can be edited. That file can then be imported manually through "Backup Import/Export" via the HTTP server. The HTTP server can be manually configured or automatically populated via DHCP.

See “Mass Deployment” on page 133.

Chapter 2

Introduction

Introduction

Mitel offers two products variants:

- MiVoice™ Conference Phone
- MiVoice Video Phone

The MiVoice Conference Phone and the MiVoice Video Phone are all-in-one multimedia collaboration appliances that provide multi-party audio and/or video conferencing, in-room presentation display, and remote collaboration for personal office meeting areas and conference rooms.

MiVoice Conference Phone (formerly MiVoice Conference Unit) is designed to provide businesses of all sizes (and markets) with a rich, multi-party audio conference and collaboration experience.

The MiVoice Video Phone (formerly MiVoice Video Unit) combines in-room presentation display, multi-party audio conferencing and video collaboration for remote participants in an easy-to-use device.

Both the MiVoice Conference Phone and the MiVoice Video Phone have a large 7-inch color multi-touch display screen. The LCD display has a resolution of 1024 x 600 and has a backlight with adjustable brightness.



It has a patented beam forming microphone array that delivers 360° audio clarity for all participants. It automatically locates the talker in the room and attenuates background noise by adjusting the microphone sensitivity towards the current talker. It provides visual indication of the active speaker.


USB and Micro SD connectors are provided on the side of unit for quickly accessing files and presentations.



Identifying the Product Variant

The product variant is indicated on the main phone screen: Video Enabled Conferencing (Video Phone) or Audio Enabled Conferencing (Conference Phone).

To see the software version of the phone:

1. Press  to display the Menu bar, and then press .
The Software Version is displayed in the lower right-hand corner.
2. Ensure that the phone contains the most recent Release 2.1 software.
3. If you need to upgrade the software version, see “Upgrade System Software” on page 82.
4. You will see one of the following product variants in the middle of the display

These product variants are described below.

MiVoice Conference Phone

The Conference Phone provides basic Telephony and Conference features and applications:

- HD audio with 4-party audio bridge
- 16 beam forming microphones
- In-room presentation display (Mitel MiCollab Conference, Browser, Cisco WebEx Meetings, Remote RDP, Remote VNC, and OfficeWRX™)

MiVoice Video Phone

The Video Phone supports all the features of the Conference Phone, plus the following:

- HD audio with 4-party audio and HD video bridge
- Presentation display to remote participants
- Point-to-point video

This document includes procedures for both the MiVoice Conference Phone and the MiVoice Video Phone.

About This Document

This document provides the information that you need to configure the various settings on the phone, for example, the network settings, the SIP settings, the camera settings, and so forth. It also describes procedures to back up and import settings, and upgrade the software.

For more detailed information, see the following chapters:

- how to launch **Settings** and configure Advanced settings for the phone - see “Configuration” on page 33
- how to configure MiVoice Business settings for the phone - see “Programming MiVoice Business” on page 101
- how to configure settings for the MiVoice Office 250 - see “MiVoice Office 250 Configuration” on page 111

Related Documentation

See the following documents for more information on the MiVoice Conference/Video Phone.

- **MiVoice Conference/Video Phone User Guide** — describes how to use the Conference and/or Video Phone to make and receive calls, launch the various applications, and display and share presentations.
- **MiVoice Conference/Video Phone Installation Guide** — provides instructions on how to physically connect the Conference Phone or Video Phone.
- **Revolabs HD™ Dual Channel System Microphone Installation Guide** — provides instructions on how to install the Revolabs HD Single/Dual Channel Wireless Microphone system. It also provides guidelines on charging, placing, and using the extension microphones on the MiVoice Conference/Video Phone.
- **Conference/Video Phone Universal Camera Mount Installation Guide** — provides instructions on how to mount the Conference/Video Phone universal camera mounting bracket and camera to the display monitor.
- **MiVoice Conference/Video Phone Quick Reference** — provides basic procedures on how to make conference calls, handle calls, and do in-room and remote presentations.
- **MiVoice Conference/Video Phone Engineering Guidelines** — provides information on the Conference/Video Phone engineering requirements.

- **MiVoice Business System Administration Tool Online Help** — Refer to this online help system for instructions on how to program SIP devices on the MiVoice Business system.
- **Redirection and Configuration Service (RCS) User Guide** — Refer to this guide on the RCS service that offers touchless deployment of Mitel devices.

To access MiVoice Conference/Video Phone and system-specific documentation:

1. In your browser, go to <http://www.edocs.mitel.com>.
2. Select a documentation suite from the following drop-down menus:
 - **Applications -> Conferencing and Collaboration -> MiVoice Conference/Video Phones**
 - End User Documents
3. Log in if asked to do so.
4. To view a document, click on the document title.

Chapter 3

Recommended Configurations

Recommended Configurations

The section of the document describes the recommended configurations for the Conference/Video Phone.

- “Conference Room” on page 15
- “Teleworker Home Office” on page 15
- “Executive Office Side Table” on page 15

Conference Room

- Install and configure the Conference Phone or Video Phone following the guidelines in the *MiVoice Conference/Video Phone Engineering Guidelines*. See the sections **Initial Setup** and **Conference Rooms and Office Recommendations**.
- Place the Revolabs Extension Microphones as recommended in the *“Revolabs Microphone Placement”* on page 17.
- Configure the extension microphone settings on the Conference/Video Phone. See “Extension Microphone Settings” on page 67.

Teleworker Home Office

To use the Conference/Video Phone in a Teleworker home office, refer to the following information:

- See the section “Conference/Video Phone Used as Teleworker” on page 93 in this guide.
- See the section **Teleworker and MiVoice Border Gateway Deployments** in the *MiVoice Conference/Video Phone Engineering Guidelines* as well Bandwidth Requirements and MBG configuration.

Executive Office Side Table

Ensure that the Conference/Video Phone is set up in office mode by programming a personal ring group on the MiVoice Business. Also, program a hand-off key on the user’s desk phone so that they can hand off calls answered on their desk phone over to the Conference/Video Phone.

Configuring MiVoice Business

1. Open ESM on MiVoice Business.
2. Click on the Users and Services Configuration Menu.
3. Click on the Group Programming Menu.
4. Click open the Personal Ring Group form.
5. Click Add.
6. Under Personal Ring Group field, enter the DN of the Desk phone to be in the ring group.
7. Click Save.
8. To add a Conference/Video Phone to the ring group, select the Personal Ring Group you previously created.

9. Click on Add Member.
10. Add the Conference/Video Phone DN you want to be in the ring group.
11. Click Save.

Configuring the Desk phone for Handoff

To program the Handoff key on the Desk phone:

1. From the desk phone, press the Superkey.
2. Press Settings.
3. Select the key you want to program.
4. Scroll through the features list and select the Handoff feature and Save.

To handoff your desk phone to the Conference/Video Phone

1. Place an incoming call to the Desk phone extension.

Both the Desk phone and Conference/Video Phone will ring.

2. Answer from the Desk phone.
3. Select the Handoff Key.

The Conference/Video Phone will ring.

4. Answer the Conference/Video Phone.

The Conference/Video Phone will then be connected to the originating call.

Revolabs Microphone Placement

The following diagrams illustrate the placement of the microphones for different layouts: single microphone, two microphones (angled and straight), and U-shaped conference table. All microphones should be placed flat on the table.

Figure 1: Conference Table with Single Microphone

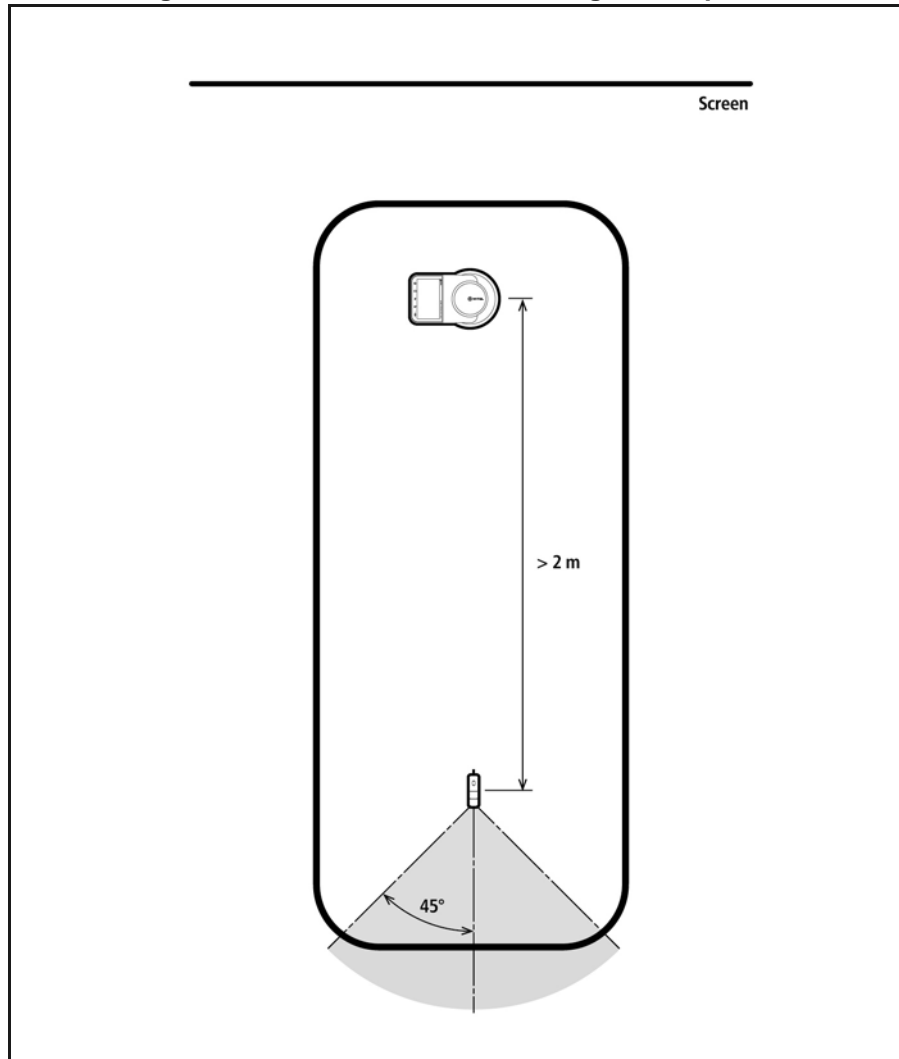


Figure 2: Conference Table with Two Microphones (Angled)

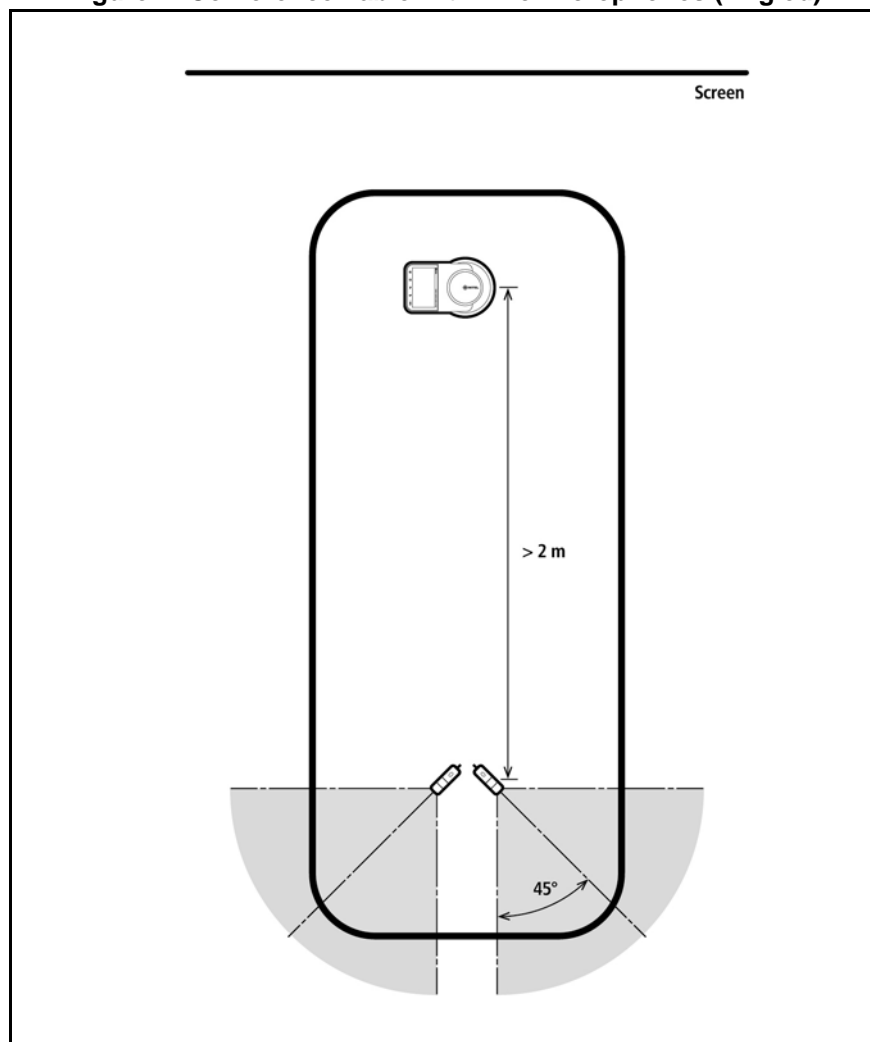


Figure 3: Conference Table with Two Microphones (Straight)

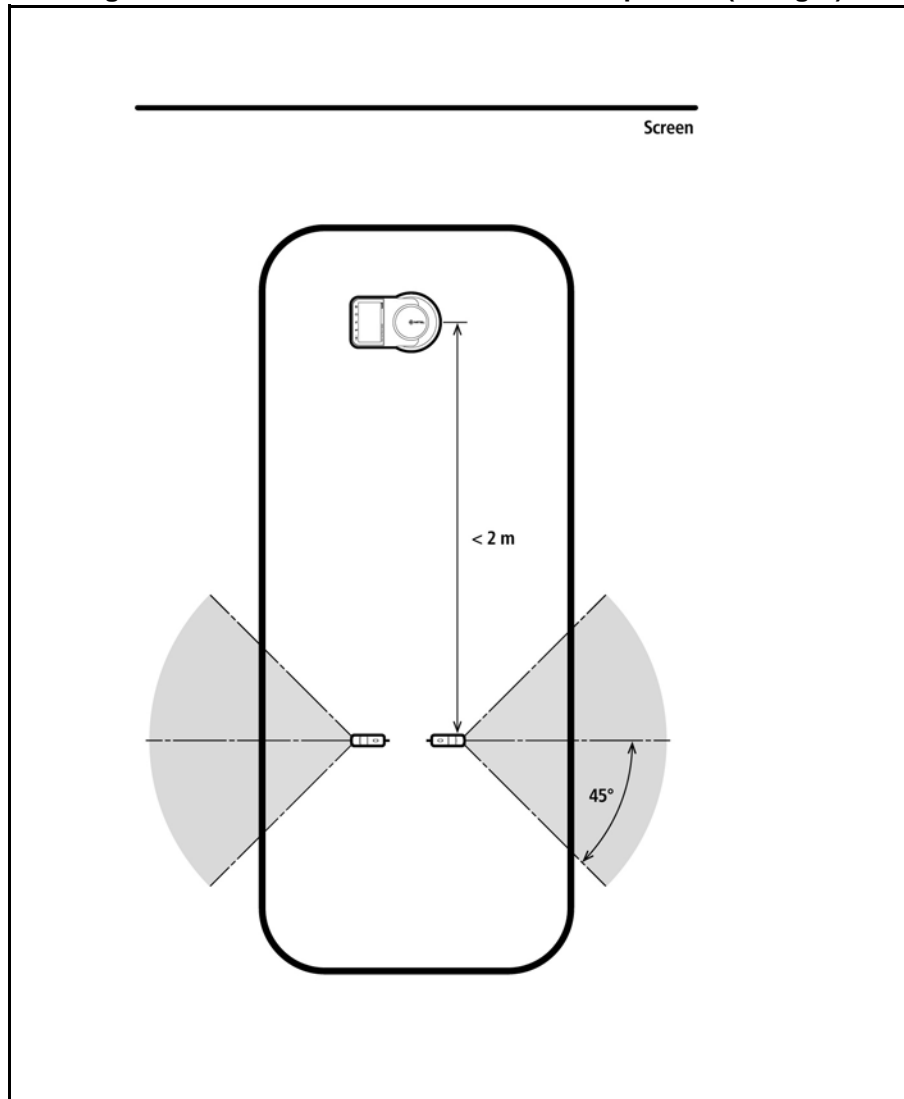
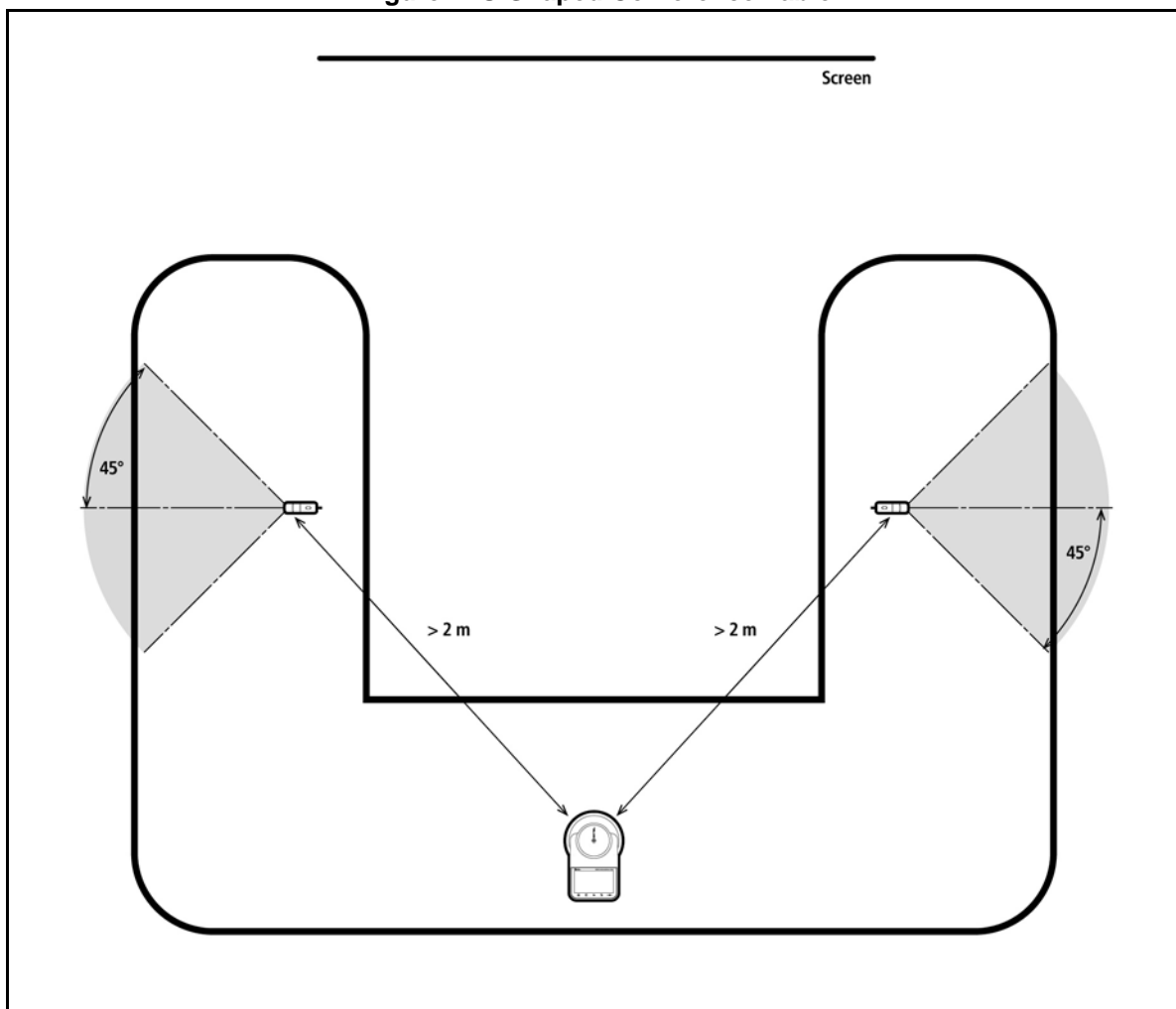


Figure 4: U-Shaped Conference Table



Chapter 4

Quick Start

Introduction

This chapter provides quick setup procedures for configuring the Conference/Video Phone. It contains the following sections:

- “Before You Start” on page 23
- “Conference/Video Phone Interfaces” on page 23
- “Launching Advanced Settings using the Phone Interface” on page 24
- “Accessing The Phone Using The Web Interface” on page 25
- “Obtain Network Settings” on page 26
- “Configure Static IP addresses” on page 26
- “Upgrading Software” on page 27
- “Configure SIP Settings” on page 28
- “Import/Export Configuration Files” on page 29

Refer to the following documents for more information:

- *MiVoice Conference/Video Phone User Guide* for a description of the Conference/Video Phone, its interface, how to make and receive video calls, and set up remote collaboration.
- *MiVoice Conference/Video Phone Installation Guide* for instructions on physically connecting the MiVoice Conference Phone or Video Phone.
- *MiVoice Conference/Video Phone Engineering Guidelines* for information on various configuration settings and Conference/Video Phone engineering requirements.

Before You Start

Ensure that the MiVoice Conference/Video Phone is installed properly and is connected to a local area network (LAN).


Refer to the *MiVoice Conference/Video Phone Installation Guide* for instructions on physically connecting the MiVoice Conference Phone or Video Phone.

Conference/Video Phone Interfaces

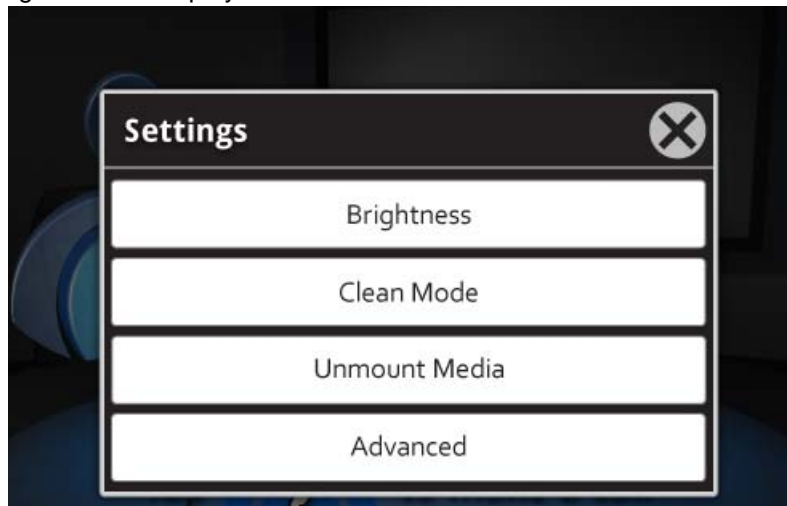
You can configure the phone using

- the phone’s touch screen (see “Launching Advanced Settings using the Phone Interface” on page 24), or
- the phone’s web interface (see “Upgrading Software” on page 27)

Launching Advanced Settings using the Phone Interface

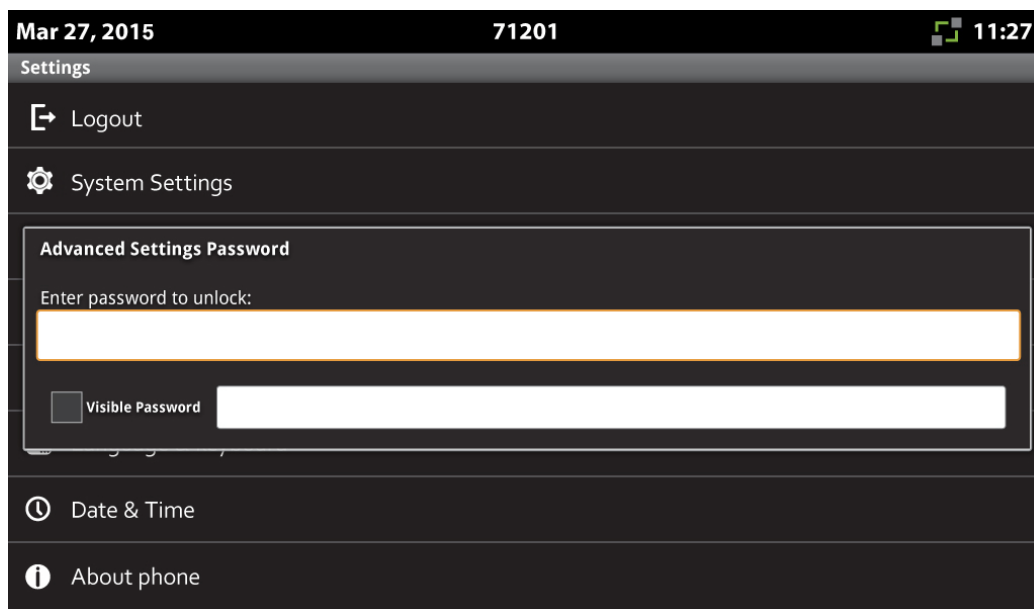
1. Press  to display the Menu bar.
2. Press **Settings** .

The following screen is displayed:



3. Press **Advanced**.

The following screen is displayed.



4. Enter the password.

The default password is "admin". It is highly recommended that you use a different password.

5. Press **OK**.

The Advanced Settings screen is displayed.



Accessing The Phone Using The Web Interface

Once the Web Server is enabled, you can enter the IP address of the phone in a browser to access its configuration interface.

1. From the **Advanced Settings** screen, press **System Settings**.
2. Press **Web Server Settings** and ensure the **Web Server Enabled** box is checked.
3. Enter the phone's IP address in a web browser, such as IE, Chrome, or Firefox to open the phone web interface.

See "Web Server" on page 123 for details on how to use the Web Server to configure the phone.

Obtain Network Settings

You must obtain the phone's IP address in order to configure the phone.

1. From the **Advanced Settings** screen, press **System Settings**.
2. Press **Network Settings**.
3. Press **View Current** and write down the Phone's IP Address.

Configure Static IP addresses

If you do not have a DHCP server, you can configure static IP addresses.

1. From the **Advanced Settings** screen, press **System Settings**.
2. Press **Network Settings**.
3. Press **Modify Static**.
4. Enter the static IP addresses.

Upgrading Software

Prerequisite: Obtain the URL of the HTTPS server from which the software files will be downloaded.

The Conference/Video phone firmware contains two files:

- uc360_x.x.x.x.zip — where x.x.x.x is the upgrade load version
- upgrade.xml


You can download the software from Mitel OnLine by following the instructions below.

Download the Software

1. Log on to Mitel OnLine.
2. Move your cursor over **Support** and under **Technical Support**, click **Software Downloads**.
3. Click on **IP Desktop Devices** and click on **UC360 Collaboration Point - Software Download**.
4. Select the appropriate software to download.
5. When you click on the software to download, a "Disclaimer" is displayed that prompts "I agree..." or "I disagree". Click the appropriate response.
6. Select a location on your PC to store the downloaded software.

Set Up the HTTP/HTTPS Server and Upgrade Software


You must place the firmware files on an HTTP/HTTPS server in order to upgrade the software on the phone.

1. Press **Settings** , then press **Advanced**.
2. Press **System Settings**.
3. Select **Upgrade system S/W**.
4. Select **Software HTTP Server Address** and enter the IP address of the HTTP server where new software loads are stored. You can enter https:// in the HTTP Server Address.
5. Enable **Trust All HTTPS Servers**, (if necessary).
6. Press **Save**.
7. Select **Upgrade system S/W now**.
8. Select **HTTP**.

You will see a series of messages. This can take several minutes; the phone will power off and then on. The phone will reboot and load the new software.

Configure SIP Settings

In order to make and receive calls, the SIP settings must be set up. For more details, refer to “Configure SIP Settings” on page 28.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **SIP Settings**.

Enter the parameters listed in the table below.

Parameter	Comments
Server Address	The IP address (IPv4) or the FQDN format address of the SIP server.
Username	The SIP user's ID. It is typically the DN (extension number) assigned on the SIP server.
Display Name	Enter the name to be sent during calls that may be shown on the other party's display. Only use alphanumeric characters and space for display names.
Login Name	SIP Authentication name; this can be different from the username.
Login Password	SIP Authentication password.
Transport	Transport type; the default is UDP.
Proxy Server Address	Optional, depending on if the phone and the SIP server require the proxy server for SIP message routing.

Import/Export Configuration Files

The phone support two types of configuration files: generic and device-specific.


- MN_GENERIC.cfg
- MN_MAC.cfg

The phone can be programmed to automatically attempt to download the configuration files each time it boots up or at specific time of day. In addition to the automatic downloads, you can import/export configuration files using one of two methods:

- HTTP Import
- USB or SD Card Import/Export

HTTP Import


You will need to configure the HTTP Server first, and then import the configuration files.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Licensing and Backup Import/Export**.
5. Press **HTTP Import**.
6. Press **Configuration HTTP Server Address** and enter the address of the configuration HTTP server, and press **Save**.
7. Select **HTTP Import Now**.

The phone downloads the specific configuration files from the designated server.

USB or SD Card Import

You can import/export configuration files using a USB or SD card.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Licensing and Backup Import/Export**.
5. Insert the SD card or USB flash drive.

This option opens a Backup Import/Export window.

6. Enter the filename to which you want to export or import settings.
7. Enter the password.

The filename can be any valid filename. The password is the Admin password for the phone.

8. Click the option you wish to use.

- You can export/save a backup of the current settings to a file on an SD card or USB flash drive.
- You can import/load an existing backup of settings from a file on the SD card or USB flash drive.

Import/Export using the SD and USB cards will import/export the binary database and the set-specific configuration files. If you want to explicitly import the set-specific configuration file, you need to input the MN_MAC.cfg in the **Enter filename** field.

Minimal Configuration File for Video Conferencing

This is an example of the minimal configuration file that can be used for video conferencing.

```
<?xml version='1.0' encoding='UTF-8' standalone='yes' ?>
<Parameter Model="UC360">
  <user_list>
    <User ID="2025" DispName="2025" Pwd="1234" AuthName="2025"
ProxySvr="10.40.190.21" ProxyPort="5060" ProxyScheme="2" OutSvr=""
OutPort="5060" DialURIOutboundProxySvr="" DialURIOutboundProxyPort="5060" />
  </user_list>
  <audio_codec_list>g722,g722.1,g711u,g711a</audio_codec_list>
  <video_codec_list>h264highprofile,h264baseprofile</video_codec_list>
  <camera Enable="1" Address="10.35.21.113" Port="0" AuthName="polaris"
Pwd="mitel"></camera>
</Parameter>
```

Notes

- The configuration file is designed in XML format. Malformed XML format will be rejected by the phone.
- The best way to edit the phone configuration file is to export one from an existing phone first and then change the parameters from there.
- The parameters in the MN_Generic.cfg and MN_MAC.cfg files can be duplicated. The policy is the later parameter will overwrite the former ones. The phone will download the MN_Generic.cfg first, then the set specific files.
- If the parameters are missing in the configuration files, default values will be used in the phone.

Minimal Configuration File for Audio Conferencing

This is an example of a configuration file that can be used for audio conferencing.

```
<?xml version='1.0' encoding='UTF-8' standalone='yes' ?>
<Parameter Model="UC360">
  <user_list>
    <User ID="2020" DispName="2020" Pwd="1234" AuthName="2020"
ProxySvr="10.40.190.21" ProxyPort="5060" ProxyScheme="2" OutSvr=""
OutPort="5060" DialURIOutboundProxySvr="" DialURIOutboundProxyPort="5060" />
  </user_list>
  <audio_codec_list>g722,g722.1,g711u,g711a</audio_codec_list>
</Parameter>
```

This is the minimal configuration values for audio conferencing. However, if the phone has been previously programmed to support video as described in “Video Settings” on page 63, the existing settings for video are still valid. Therefore, unless you remove the video codecs from the settings, or add the following parameter, you can still make video calls.

```
<video_codec_list> </video_codec_list>
```


Chapter 5

Configuration

Introduction

This chapter provides detailed procedures for configuring the following advanced settings for the Conference/Video Phone:

- Sound — See “Sound” on page 89.
- SIP Settings — See “SIP Settings” on page 41.
- Apps Settings — See “Apps Settings” on page 47.
- Network Settings — See “Network Settings” on page 48.
- Contacts Settings — See “Contacts Settings” on page 52.
- Dial Plan Settings — See “Dial Plan” on page 61.
- Video Settings — See “Video Settings” on page 63.
- RDP Settings — See “RDP Settings” on page 64.
- VNC Settings — See “VNC Settings” on page 65.
- History Settings — See “History Settings” on page 66.
- Extension Microphone Settings — See “Extension Microphone Settings” on page 67.
- Advanced Settings Password — See “Advanced Settings Password” on page 68.
- Camera Settings — See “Camera Settings” on page 69.
- Country Variant — See “Country Variant” on page 76.
- Dialpad Settings — See “Dialpad Settings” on page 77.
- Licensing and Backup Import/Export — See “Licensing and Backup Import/Export” on page 78.
- Upgrade System S/W — See “Upgrade System Software” on page 82.
- Debug Settings — See “Debug Settings” on page 85.
- Web Server Settings — See “Web Server Settings” on page 86.
- Reboot — See “Reboot” on page 87.
- Factory Reset — See “Factory Reset” on page 88.

Refer to the following documents for more information:

- *MiVoice Conference/Video Phone User Guide* for a description of the Conference/Video Phone, its interface, how to make and receive video calls, and set up remote collaboration.
- *MiVoice Conference/Video Phone Installation Guide* for instructions on physically connecting the MiVoice Conference Phone or Video Phone.
- *MiVoice Conference/Video Phone Engineering Guidelines* for information on various configuration settings and Conference/Video Phone engineering requirements.
- *Redirection and Configuration Service (RCS) User Guide* for more information on the auto-configuration of the MiVoice Conference/Video Phone.

Auto-configuration of the phone

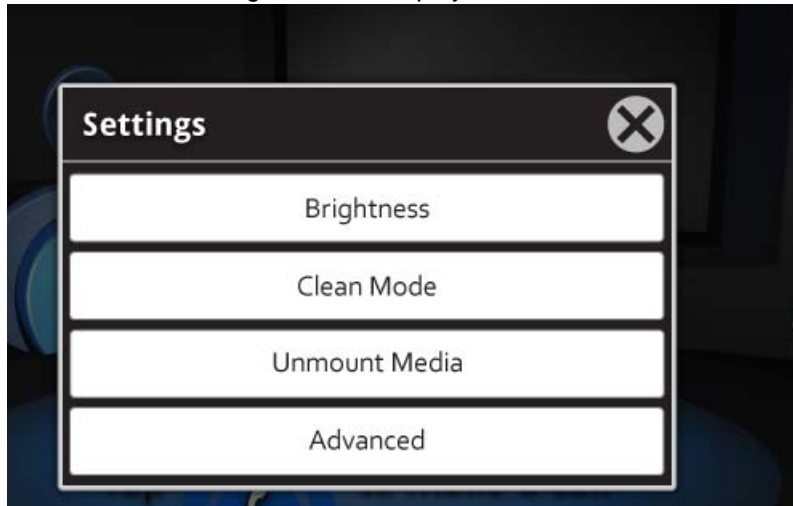
The Mitel Redirection and Configuration Service (RCS) is a service that offers Service Providers the option of auto-configuring devices when they are first powered up. Mitel's RCS eases the issues Service Providers face with mass deployments. By simply entering the MAC address of a device into the Global RCS server, upon initial boot-up, the device can be routed to its assigned server for configuration. See the *Redirection and Configuration Service (RCS) User Guide*.

The MiVoice Video/Conference Phone will contact the RCS server when it is booted up from factory default if there is no automatic provisioning of the configuration server URL from DHCP or static programming. This mechanism provides a fallback source for the configuration server URL. See "Mass Deployment" on page 133 for more details on the XML configuration files and supported DHCP options.

Launching Settings

1. Press  to display the Menu bar.
2. Press **Settings** .

The following screen is displayed:



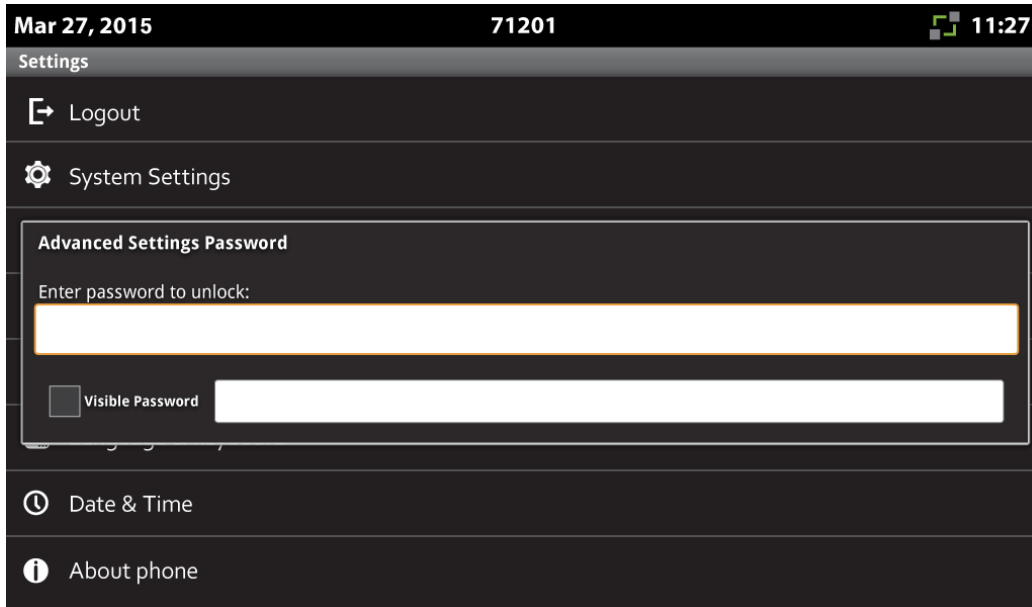
Refer to the *MiVoice Conference/Video Phone User Guide* for details on adjusting the brightness, cleaning the phone screen, and unmounting media.

For Advanced settings, see "Advanced Settings" on page 38.

Advanced Settings

1. From the **Settings**  menu, press Advanced.

The following screen is displayed.



2. Enter the password.

The default password is "admin". It is highly recommended that you use a different password.

3. Press **OK**.

The Advanced Settings screen is displayed.



You have the following choices:

- Logout
- System Settings
- Sound (see “Sound” on page 89)
- Display (see “Display” on page 90)
- Applications
- Storage
- Language & Keyboard (see “Language & Keyboard Settings” on page 91)
- Date and Time (see “Date & Time” on page 92)
- About phone


If you forget the password, you can hold down the Back key for 5 seconds. This will launch a Mitel customized Factory Data Reset window which requires confirmation before resetting the phone to factory data defaults. See “Factory Reset” on page 88.

Note: Do not change the Date and Time while in a call. This may cause the phone to reboot.

You may cancel out of the Factory Data Reset at this screen by using the Back key or the Cancel button. Reset to factory defaults allows the administrator access to the phone using the default password. Once reset, the software load reverts to the factory load, and the phone’s site-specific settings will need to be reconfigured.


Note: The factory load browser that was enabled by default earlier is now disabled by default.

Configure System Settings

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.

You can set/adjust the following settings:

- SIP Settings
- Apps Settings
- Network Settings
- Contacts Settings
- Dial Plan Settings
- Video Settings
- RDP Settings
- VNC Settings
- History Settings
- Extension Microphone Settings
- Advanced Settings Password
- Camera Settings
- Country Variant
- Dialpad Settings
- Licensing and Backup Import/Export
- Upgrade System S/W
- Debug Settings
- Web Server Settings
- Reboot
- Factory Reset

You can press the HOME key  or the Back key twice to quit out of **Settings** and return to Conference app.

SIP Settings

The Conference/Video Phone supports the SIP protocol. As a result, it is capable of operating with a number of third-party SIP Servers and SIP end points such as SIP phones, Audio Conference Units and Video Conference Units.

SIP Servers and Endpoints

As well, the phone supports a number of third-party video conferencing services. The phone user can access these services with SIP URI dialing.

Mitel maintains a SIP Centre of Excellence (SIP CoE); the CoE performs interoperability testing between third-party devices and services and Mitel SIP devices. The CoE generates documents that cover the results of the interoperability tests and how the phone and Cloud services should be configured for successful interoperation.

For the complete list of devices that Conference/Video Phone can interoperate with, please refer to the Knowledge Base article called *Mitel Technical Reference Guide: Mitel Compatibility and Third-Party Certification Reference Guide for Mitel Products, 08-5159-00014*.

This Reference Guide can be found on Mitel On-Line under **Support -> Technical Support > SIP Centre of Excellence**. The Reference Guides provide the Administrator with the following type of information:

- Configuration recommendations for the Conference/Video Phone and the Mitel MiVoice Business.
- Configuration recommendations for the Conference/Video Phone and third-party SIP Servers and SIP end points.
- A list of potential interoperability and/or feature limitations.


Prerequisites

- Before configuring SIP settings, ensure that MiVoice Business programming or MiVoice Office 250 programming is completed. See “Programming MiVoice Business” on page 101 or “MiVoice Office 250 Configuration” on page 111.
- Obtain the SIP Server address name, User Name, and Login Name from the User and Device Configuration form.
- Ensure that the SIP server is configured to support E.164 dialing in order to correctly translate the + into the country exit code. Refer to the SIP Server’s Administration/Configuration Guide.
- For MiVoice Border Gateway specific settings, see “Conference/Video Phone Used as Teleworker” on page 93.

Note: The \$ and the & characters are not supported in any of the System Settings menus. These characters are also not supported in the mass deployment XML cfg file.

- For a Conference/Video Phone or UC360 Release 2.1 or older, if the \$ or the & character has been used to configure any System Settings parameters, that programming will be invalid once upgraded to Release 2.1 SP1, and the device will stop functioning properly.

- Update the SIP server and camera programming to configurations that do not include the \$ or & and then reprogram the Conference/Video Phone System Settings parameters accordingly.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **SIP Settings**.

Account

Under **Account**, set the following parameters:

1. Enter the Server Address — the IP address (IPv4) or the FQDN format address of the SIP server.
2. Enter the Username — the SIP user's ID. It is typically the DN (extension number) assigned on the SIP server.
3. Enter the Display Name — enter the name to be sent during calls that may be shown on the other party's display. Only use alphanumeric characters and space for display names.

Authentication

Under **Authentication**

1. Enter the login name — typically the DN.
2. Enter the password — typically the DN.

Transport

Three transport types are supported:

- TLS — enable/disable TLS secure protocol.
- TCP — enable/disable TCP protocol.
- UDP — enable/disable UDP protocol.

Only the selected (check box) transport types will be connected if they are available on the server.

They may be toggled individually to enabled or disabled, and in any combination with one restriction. That restriction is that at least one must be enabled and thus the unit will automatically enable UDP if all are disabled. The single currently active transport is indicated by a star (*) e.g. TLS as illustrated in the example below.

*Enable/disable TLS secure protocol (Enabled)**

If the connection and/or registration fails for the currently active transport, the next highest in precedence, which is enabled becomes the active transport. The process continues until the registration succeeds. Any change to this or other registration affecting configuration will restart the process.

Media

Under **Media**, set the following parameters:

- Audio CODEC List — specify the preferred order for audio CODEC usage.
- Video CODEC List — specify the preferred order for video CODEC usage.

The default order is

- h264highprofile
- h264baseprofile

The order is important as the top most codec entry is the preferred one when the call is being negotiated.

If the phone is using URI dialing, only the H.264 baseline profile CODEC is supported.

Note: A reboot is required after changing the video codecs

To configure a codec:

- Enabled codecs are shown at the top of the list in green and disabled codecs are listed at the bottom in grey.
- Long press a codec entry to the right of its icon to obtain a popup to select enable or disable a codec.
- Press the icon to the left of any codec, then drag and drop to re-order the codec list.

On a system software upgrade from an earlier version to Release 2.0:

- If the old H264 codec was disabled, then both of the new video codecs will be disabled.
- If the old H264 codec was enabled, then the default configuration, as described, will be in effect.

The Video Phone must be reset if the H.264 video codec is not enabled, and has been enabled for the first time.

G.729a is disabled by default and it is recommended that it should remain disabled on Video Phones. This ensures the best audio quality. If G.729a is required, an administrator can enable it manually.

Refer to the section on CODECs and bandwidth in the *MiVoice Conference/Video Phone Engineering Guidelines* for more information.

- Packet Time — set the preferred packet time from 20 ms to 100 ms in 10 ms increments. A packet time of 20 ms is recommended. **Note:** Certain CODECS may only operate in 20 ms increments.

- SRTP — Secure audio is supported via SRTP. There are three values for the SRTP mode:
 - SRTP Disabled - Real Time Transport Protocol (RTP) is used. Voice packets between endpoints are not secure.
 - SRTP and RTP - SRTP will be used if it is available; otherwise, RTP is used. SRTP is Secure RTP, which uses encryption and authentication for security.
 - SRTP only - calls will only connect using SRTP and cannot fall back to RTP. If the other end does not support SRTP, then the call will fail.
- Session Maximum Packet Rate — Some SIP servers may have problems processing SDP (Session Description Protocol) messages used to control media establishment, which includes a Session level *maxprate*. This setting is disabled by default, but can be enabled using this setting.

Firewall Traversal

The Firewall Traversal configuration options should only be used in configurations when specified in a SIP Center of Excellence Interoperation report.

- ICE — SIP Internet Connectivity Establishment. The ICE setting is automatically set to disabled (default) and the check box is greyed out if the STUN Server Address is empty.
- STUN Server Address — Session Traversal Utilities for NAT. Enter the STUN server IP address (IPv4) or the FQDN format address along with the port number, which defaults to port 3478. The MiVoice Conference/Video Phone supports STUN on UDP.

ICE must be enabled to use STUN with ICE to enhance SIP call media establishment over the internet when behind NAT firewalls.

Misc

- **Registration Time Out** — the SIP registration time out value in seconds. It is recommended to leave this at the factory default setting of 300 seconds.
- **Keep Alive Interval** — the SIP keep-alive interval in seconds. It is recommended to leave this at the factory default setting of 0, which is disabled.
- **Proxy Server Address** — the SIP Proxy server IP address (IPv4) if you have a server that is used when interoperating with a 3rd party server, for example, BroadSoft. See the Mitel SIP Centre of Excellence (SIP CoE).
- **Proxy Server address for Dial URI** — the internal IP address of the gateway or SIP Outbound Proxy server address in the format FQDN | IP [:port]. This is the address of the SBC.

The Proxy Server (SBC) needs to be configured so that it can support the Transport Settings selected. For example, if the transport setting TLS is selected, the Proxy Server needs to support TLS transport in order for calls to work.

- **SPAM Call Filter** — allows incoming calls only from the programmed SIP Server.

In previous versions of the Conference/Video Phone software, there was an option to specify DTMF mode. In the current version, the phone supports both out-of-band (as per RFC 2833) and in-band DTMF signaling mechanisms. The phone uses Session Description Protocol (SDP) messages to negotiate with its SIP peer to determine which DTMF mechanism should be used.

By default, the phone will offer/answer its ability to support out-of-band DTMF (telephone-event per RFC 2833) in SDP messages sent to the SIP peer.

If the SIP peer also supports the out-of-band capability, then the phone will use the out-of-band mechanism to send DTMF digits. However, if the peer does not indicate that it supports telephone-event in its SDP messages, then the phone will fall back to using the in-band DTMF mechanism, which will insert the DTMF tones in the audio RTP stream.

Security

- **TLS Server Validation** — enable or disable the validation of TLS connections with installed certificate authority certificates.
- **Install Certificates From External Storage** — install a user or CA certificate and keys for validating TLS connections.
- **Remove All Installed Certificates** — remove all installed user and CA certificates and keys.

TLS Server Validation

When TLS Server Validation is enabled, the certificate supplied by the SIP Server when using the TLS transport during the TLS handshake is validated against the list of trusted root certificate installed on the phone.

The Mitel root certificate is the single entry in this certificate list by default on the phone.

Install Certificates From External Storage

You can install new certificates from any.crt file (for example, mat_ca.crt in PEM format) or p12 file (PKCS12 format) in the following locations: the root directory of a USB drive, the root directory or download directory of an sdcard.

If there are multiple.crt and/or.p12 files, you will see a list of files to choose from. Note that the list indicates the path, including the device on which each file is present.

Upon successful installation of a certificate, the selected file is deleted on the external storage device and will no longer appear in the above list.


If only a single file is found, you see only the information on any certificate found in that file and have the option to name the certificate. The same process occurs with a file selected from the above list.

Remove All Installed Certificates

If the administrator confirms they want to remove all installed certificates after selecting that option, then the default Mitel certificate is the only that remains in the list.

Apps Settings

The Apps Settings allows you to enable or disable any of the shareable applications that are currently implemented on the phone.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Apps Settings**.

A list of all the currently installed apps will be displayed. Each app has its own check box. You can enable each check box as desired by tapping the check box to check or uncheck it.

A check mark in the box enables the associated app. If there is no check mark in the box, then the associated app is disabled.

The available apps are the following:

- Mitel MiCollab Conference
- Browser
- OfficeWRX
- Files
- Cisco WebEx Meetings
- RemoteRDP
- RemoteVNC (disabled by default)

Note: If a USB keyboard is connected to the phone, **Num Lock** does not function.

No Apps Enabled

If the administrator chooses to disable all apps, then the **Present** icon on the main screen will be disabled and grayed out so that pressing them will have no effect.

Software Upgrade and App Settings Defaults

When the UC360 software is upgraded from version 2.0.x to 2.1.x software, the default settings for each app will be set to enabled, except for Remote VNC. When the upgrade from 2.0.x to 2.1.x occurs, new database entries are created for the Apps Settings and the default values are set. Subsequent software upgrades will not need to reference the default values, and will use the existing values from the database.

Network Settings

If installing the Conference/Video Phone with a MiVoice Business, it may be easier to use static VLAN and QoS values by manually entering the information into the phone Network Settings menu rather than obtaining parameters via DHCP or other methods.

However, if you choose to have a DHCP server provide these values to the phone, it should be noted that the MiVoice Business DHCP server may not support a field for defining L2 and L3 QoS values for Multimedia Conferencing. In this case, the L2 and L3 QoS values for Multimedia Conferencing will need to be statically programmed.

Where possible, the DHCP values are displayed below the entry.

DHCP (value) - This indicates the value was not programmed by the administrator and was obtained via DHCP from the network. Static values programmed by the administrator don't have this encapsulation.

For example:


Default Gateway IP Address
DHCP (10.33.36.1)

The Default Gateway IP Address is obtained from the DHCP server and the value is shown in parentheses.

Static values programmed by the administrator are not shown in parentheses.

Software HTTP Server Address
10.33.36.132

Note: The Conference/Video Phone does not support the Windows 2000 server for DHCP.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Network Settings**.

The following options are available as listed below.

View Current

All the items below are initially retrieved from the DHCP, except the MAC address. Some of these options may be overridden by the Static settings.

SIP Server

The IP address (IPv4) or the FQDN format address of the SIP server.

SIP Proxy Server

The IP address (IPv4) of the SIP Proxy server.

Mac Address

The hardware address associated with the network interface on the phone.

Phone IP Address

The phone requires an IP address. This is an IPv4 address and it is recommended that the address selected be in the same subnet as the local ethernet camera.

Default Gateway IP Address

This is the IP address (IPv4) of the gateway (or default router) that allows access to other subnets.

Subnet Mask

Consult with the network administrator as to how this should be set.

VLAN ID

This field is used by the administrator to set the VLAN ID. The default setting for this field is no value (blank).

Note: If a VLAN ID is not entered into this field, then the L2 priority settings will not take effect.

L2 Priority Voice

This screen allows the administrator to set the L2 priority for Voice packets. A value of 6 is recommended. For further details, see section on phone Quality of Service Settings.

L2 Priority Signaling

This screen allows the administrator to set the L2 priority for Signaling packets. A value of 3 is recommended. For further details, see section on phone Quality of Service Settings.

L2 Priority Multimedia

This screen allows the administrator to set the L2 priority for Multimedia packets. A value of 4 is recommended. For further details, see section on Conference/Video Phone Quality of Service Settings.

DSCP Voice

This screen allows the administrator to set the L3 priority for Voice packets. A value of 46 is recommended. For further details, see section on Conference/Video Phone Quality of Service Settings.

DSCP Signaling

This screen allows the administrator to set the L3 priority for Signaling packets. A value of 24 is recommended. For further details, see section on Conference/Video Phone Quality of Service Settings.

DSCP Multimedia

This screen allows the administrator to set the L3 priority for Multimedia packets. A value of 34 is recommended. For further details, see section on Conference/Video Phone Quality of Service Settings.

Software HTTP Server

The location of the server used for the software upgrade files.

Configuration HTTP Server

The location of the configuration server used for mass deployment configuration files.

DNS Server 1

This is the IP address (IPv4) of the first DNS server.

IPA Server

This is the IP address (IPv4) of the IPA server. The IPA (IP Phone Analyzer) is a Mitel product that can be used to assist with debugging phone and network issues.

NTP Server

NTP (Network Time Protocol) allows the phone to set its time of day clock. The phone will access the default server at the URL - *2.android.pool.ntp.org* - on the internet to obtain the current time of day.

Modify Static

Modify these values based on your network requirements.

802.x Protocol

802.1X Settings can be set as required or left blank.

The Conference/Video Phone supports the IEEE 802.1x standard for port based network access control with EAP-MD5. EAP (Extensible Authentication Protocol) is an authentication protocol that can be used to control network access at the port level.

Devices that authenticate through 802.1x require a user name and password before being allowed access to network. If the administrator configures the L2 Switch for port access control, then the phone, when connected to this port, will prompt the user for an account name and password if one has not already been entered or if the information saved in the phone is invalid.

If incorrect 802.1X credentials are programmed, the MiVoice Video phone will fail to connect to the network. This will be indicated by the network icon.

Hardware

This menu allows the administrator to display the following values:

- LAN Port Speed
- LAN Port Duplex

Tools and Features

This menu allows the administrator to enable or disable a number of network-related protocols.

- DHCP: It is recommended that this be enabled.
- CDP: It is recommended that this be enabled.
- LLDP: It is recommended that this be enabled.
- 802.1x: If the administrator wants authentication performed before allowing network access, then this should be enabled.
- Enable Firewall Filter: It is recommended that the firewall filter be enabled.
- VLAN Enabled: When this check box is on, VLAN tagging information (if available) will be obtained from the various sources. When the check box is off, no VLAN tagging information will be used. (The default value is for Enable VLAN to be off.)
- Ping Test IP Address: Allows a user to ping a network IP address.
- DCHP Trace: Allows a user to perform a DCHP trace.

See the *MiVoice Conference/Video Phone Engineering Guidelines* for details on these options.

Contacts Settings


For corporate directory access, the MiVoice Conference/Video Phone can use CSV (Comma Separated Value) files or LDAP. You can configure the phone to populate the corporate contacts from CSV files or from an LDAP server. The default is LDAP.

The Conference/Video Phone imports contacts only from CSV files that are formatted as generated by either the MiVoice Business Telephone Directory export or from the MiVoice 250 Phone - Individual export. For more details, see the *MiVoice Business System Administration Tool Help* or the *MiVoice Office 250 Feature and Programming Guide*. UTF-8 characters are not supported in these CSV files.

The MiVoice Conference/Video phones support a maximum LDAP Directory size of 20,000 entries with pictures and 40,000 entries without pictures.

If the LDAP directory size exceeds the maximum, a partial directory will be downloaded and available for use.

Enable CSV Import

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Contacts Settings**.
5. Enable the checkbox **Populate from CSV file**.

Once enabled, the following two menu entries are available that allow immediate import of the Corporate Directory CSV files: **Import Contacts from USB** and **Import Contacts from HTTP Configuration Server**.

When this setting is enabled, along with the checks on the HTTP configuration server for Mass Deployment configuration files MN_Generic.cfg and MN_XXXXXXXXXXXXX.cfg on boot up, a further check is made for directory CSV files MN_Generic.csv and MN_XXXXXXXXXXXXX.csv (where the X's represent the 12-character hexadecimal MAC address of the specific phone). These CSV files are parsed to populate the Corporate Contacts.

If an error occurs with the CSV import (for example, a missing file, incorrect file), the contacts list remains empty. Check the following:

- Verify the format of the CSV file: Only CSV files that are formatted as generated by either the MiVoice Business Telephone Directory export or from the MiVoice 250 Phone - Individual export are supported. For more details, see the *MiVoice Business System Administration Tool Help* or the *MiVoice Office 250 Feature and Programming Guide*.
- Verify the CSV file names: The directory CSV files must be MN_Generic.csv and MN_XXXXXXXXXXXXX.csv (where the X's represent the 12-character hexadecimal MAC address of the specific phone).
- Verify that the CSV file is in the correct location. For an http download, place the CSV files in the same directory as the cfg files. When importing a CSV file from a USB flash drive or SD card, the files must be placed in the \uc360\backups directory.

Import Contacts from USB

Ensure that the USB flash drive contains one or both of the following files:

- MN_Generic.csv
 - MN_XXXXXXXXXXXX.csv (where the X's represent the 12-character hexadecimal MAC address of the specific phone)
1. Insert a USB flash drive containing the CSV files listed above.
 2. Press **Import Contacts from USB** to copy the CSV files from the USB drive.

This triggers the replacement of the current Corporate Contacts with those from the files.

Import Contacts from HTTP Configuration Server

1. Ensure the configuration server is programed as described in “HTTP Import” on page 79.
2. Obtain one or more CSV files from the MiVoice Business or MiVoice Office 250.
3. Edit them as required to remove any unwanted entries, and split into generic and phone-specific CSV files, and rename them following the guidelines below:
 - MN_Generic.csv
 - MN_XXXXXXXXXXXX.csv (where the X's represent the 12-character hexadecimal MAC address of the specific phone)
4. Place these files on the HTTP server.
5. Press **Import Contacts from HTTP Configuration Server** to import them into the Corporate Contacts.

To Enable LDAP Import

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Contacts Settings**.
5. Ensure the **Populate from CSV file** is unchecked.

LDAP Settings

You can enter the following information below in order to login and retrieve the corporate directory list. Some settings are enabled by default. Note that **Populate from CSV file** must not be enabled to access these settings.

1. Select **LDAP Server Settings** and enter the following information.
2. Enter the Directory Server IP Address or Host Name (FQDN address of the server).
3. Enter the Communication Security Type:
 - None (port 389)
 - StartTLS (port 389)
 - SSL (port 636)
 - MBG - see "Communications Security Type - MBG" on page 55.

All server certificates are permitted for StartTLS and SSL Communications Security Types.

4. Enter the User Login.
5. Enter the User Password.

Note: If the administrator changes the LDAP username or password, and the Contacts are already loaded, the phone automatically clears the data and loads the Contacts using the new credentials.

6. LDAP Search Base - enabled (see "LDAP (Auto) Search Base" on page 57).
7. Enter the LDAP Search Directory (see "LDAP Search Directory" on page 56).
8. Enter the LDAP Search Filter (see "LDAP Search Filter" on page 57).
9. Enter the First name attribute (see "Programmable LDAP Attributes and Labels" on page 57).

Communications Security Type - MBG

When connecting to LDAP or Active Directory server through the MiVoice Border Gateway (MBG):

- Enter the MiVoice Border Gateway IP address in the Directory Server IP address field.
- Select the MBG (port 35010) for the Communications Security Type. Only valid MBG server certificates are permitted for this Communication Security Type.

For more details, see “Conference/Video Phone Used as Teleworker” on page 93. MBG configuration is required if using MBG. See the *MiVoice Border Gateway (MBG) On-line Help*.

Enable/Disable Use Pictures

The **Use Pictures** option turns on/off pictures displayed in the Contacts application. This is to support situations where the global contacts database does not have any profile pictures.

The picture size displayed in the Contacts application is restricted to 64 x 48. Therefore, photos stored in the AD must be resized. You can use one of the following freeware tools to resize the photos:

Photo upload tool

Name: CodeTwo Active Directory Photos

Link: <http://www.codetwo.com/freeware/active-directory-photos/>

Photo resize tool

Name: FastStone Photo Resizer 3.1

Link: <http://www.faststone.org/FSResizerDetail.htm>

LDAP Search Directory

The LDAP Search directory field can be programmed using LDAP attributes to search a semi-colon delimited list of specific directories or using wildcard * to search for all directories. Some examples are given below.

Search for the list in this directory	Search String
Users	ou=Users
NA -> Users Accounts	ou=User Accounts,ou=NA
NA -> Users1 & NA -> User2	ou=Users1,ou=NA; ou=Users2,ou=NA
All directories	*

Note that the search uses a filter for (objectCategory=person) so this must be specified for each entry on the LDAP server to be found by the phone. The following attributes are requested for each matched entry found on the LDAP server.

Attribute Name	Description
cn (+)	Common-Name
userAccountControl (*)	User Account Control
givenName (-)(&)	First Name
sn (-)(&)	Last Name (surname)
telephonenumber (&)	Office Phone Number
homephone (&)	Home Phone Number
pager (&)	Pager Number
mobile (&)	Mobile Number
thumbnailPhoto (#)	Active Directory thumbnail picture

(-) Must have a non-blank name. At least one of these values in a record from the LDAP server must be non-blank otherwise the record is discarded.

(+) Mandatory field, record discarded if not found or if cn is not unique.

(*) Will discard disabled accounts.

(#) Only requested from the LDAP server when the option "Use Pictures" is enabled for LDAP Server configuration.

(&) There are six LDAP configuration settings, one for each attribute name that can be programmed. The default values are shown in the table above in those cases.

LDAP Search Filter

The default search uses a filter for (objectCategory=person) and this must be specified for each entry on the LDAP server to be found by the Conference/Video Phone. This may be changed via the LDAP Search Filter configuration to any valid RFC4515 string representation of a search filter.

Programmable LDAP Attributes and Labels

There are six settings for the LDAP attributes that default to the values listed in the table above.

- First Name Attribute
- Last Name Attribute
- Office Number Attribute [;Contact Label]
- Home Number Attribute [;Contact Label]
- Pager Number Attribute [;Contact Label]
- Mobile Number Attribute [;Contact Label]

The four contact numbers entries can also optionally override the UI label used for that number in the contact details dialog, for example:

ipPhone;MiVoice Video

This represents a configuration with the attribute privateNumber being associated with the label "Private Number" and this setting could for example replace homePhone in the Home Number Attribute setting.

The label in the contacts details dialog contains a finite amount of display space. Choose a string short enough to maintain a reasonable space for the contacts numbers following the label.

Since a variable font is used, the number of characters that fit may depend on the mix of characters and their cases. As a guide, 15 mainly lower case characters fits well.

Specifying an empty value for any one of these fields results in the default being applied for that field. The labels normally come from automatically translated string resources, but if you program an optional label, then effectively you must handle your own translation for that label by providing the label appropriate to the language setting of the phone.

LDAP (Auto) Search Base

By default, all LDAP searches are from a base detected from the first naming context returned by the server as part of its rootDSE, if supplied by the server. The setting for Auto Search Base, enabled by default, can be used to disable this.

When Auto Search Base is disabled, the LDAP Search Base setting may be edited to manually specify the search base. When Auto Search Base is enabled, the LDAP Search Base setting is greyed out and the value shown is that automatically obtained from the server when a connection is made.

LDAP Server Updates

This option allows the phone to get contacts list updates from Active Directory. You have the following choices to get the updates.

Get updates now

- From the LDAP Server Updates menu, press **Get updates now**.

The Contacts list will be updated right away.

Note: A user may need to reload the LDAP entries from the LDAP server after a reboot or upgrade. LDAP entries are not re-loaded from the LDAP server if they already exist on the phone.

Schedule updates

- From LDAP Server Updates menu, press **Schedule updates**.

This allows you to schedule the day of the week and time for getting updates automatically from Active Directory.

Use the Clear button to clear out the current settings in order to schedule a new day and time.

If you attempt to set a time that conflicts with other scheduled updates, you will receive the message "This time is reserved. Please select a different time."

Contact Translations Plan

The Contact translations plan adds dialing prefixes to phone numbers that are contained in the Contacts directory so that they can be directly dialed on the connected phone system.

1. Press **Contacts Settings**.
2. Press **Translation Plan Settings**.
3. Enter the rules for the Contact Translations Plan.

The translation plan supports up to 5 different dialing prefixes for phone numbers listed in the Contacts directory.

Each prefix has one or more rules when matched causes the prefix digits to be dialed before the phone number in the Contacts directory. Note that matches that start with a + for E164 numbers will strip the leading + from a Contacts directory number before dialling after the prefix digits.

If there aren't any matches to the rules, no prefix digits are dialed.

Writing rules

- To match a specific digit or * or # enter it directly.
- To match any digit or * or # enter an X or x.
- A + may be entered as the first character of a match rule for E164 support.
- A ? may be entered as the last character of a match rule to match zero or more digits.
- To add additional rules for the same prefix separate with a semicolon. For example, 10 digit numbers starting with area codes 613 and 343 match with the rule 613XXXXXXX;343XXXXXXX


Some examples are shown below.

- 4 digit extension dialing with a 7 prefix.
- 613 area code number of 10 digits dialing with a 9 prefix.
- long distance dialing with 10 digit dialing with a 91 prefix.
- long distance 1+10 digits dialing with a 9 prefix.
- three digit extensions starting with 1XX, 2XX, 3XX dialing with a 70 prefix.

Mitel LDAP Translation Plan Settings	
Rule 1	Prefix
XXXX	7
Rule 2	Prefix
613XXXXXXXXXX	9
Rule 3	Prefix
XXXXXXXXXX	91
Rule 4	Prefix
1XXXXXXXXXX	9
Rule 5	Prefix
1XX;2XX;3XX	70
<div>Save Cancel</div>	

Dial Plan

The Dial Plan settings feature speed Dial Pad dialing by initiating a call as soon as the entered number matches one of the administrator-specified rules. When no rules match, pressing the Call button starts the call.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Dial Plan Settings**.
5. Enter the rules for the various dialing plans.

The dial plan settings supports up to 5 lines of rules that when matched initiates the call.

Writing rules

- To match a specific digit or * or # enter it directly.
- To match any digit or * or # enter an X or x.
- To add additional rules on the same line separate with a semicolon. For example, 10 digit numbers starting with area codes 613 and 343 match with the rule 613XXXXXXX;343XXXXXXX.

Dial plan notes

- Use care when designing a dial plan and verify the rules work as intended.
- Use rules without leading digits very carefully. A rule such as XXXX will prevent the phone from dialing any phone number longer than 4 digits since any 4 digit number will match.
- Useful to add rules like 911 emergency, 0 operator.

Dial plan example:

To support the following dialing sequences:

- Support 3-digit extensions from 000-899.
- Support 10-digit long distance calling using prefix 91.
- Support local calls to area code 613 and 343 with prefix 9.

Create your dial plan as follows:

Rule1 -> extensions 000-899

0XX;1XX;2XX;3XX;4XX;5XX;6XX;7XX;8XX

Rule 2 -> 1+10 digits dialing

91XXXXXXXXXX

Rule 3 -> 10 digit local dialing area code 613 and 343

9613XXXXXXXX;9343XXXXXXXX

Note: The Dialing Plan does not restrict dialing, but facilitates dialing by eliminating the wait for the inter-digit time-out.

The screenshot displays the 'Mitel Dial Plan Settings' window. It contains five rules, each with a text input field. Rule 1 is highlighted with an orange border and contains the text '0XX;1XX;2XX;3XX;4XX;5XX;6XX;7XX;8XX'. Rule 2 contains '91XXXXXXXXXX'. Rule 3 contains '9613XXXXXXXX;9343XXXXXXXX'. Rules 4 and 5 have empty input fields. At the bottom are 'Save' and 'Cancel' buttons.


Rule	Dial Plan
Rule 1	0XX;1XX;2XX;3XX;4XX;5XX;6XX;7XX;8XX
Rule 2	91XXXXXXXXXX
Rule 3	9613XXXXXXXX;9343XXXXXXXX
Rule 4	
Rule 5	

Video Settings

Video Settings allow you to adjust video bandwidth parameters for both the uplink and downlink LAN connections. The video settings menu also allows you to enable or disable the Dynamic Bandwidth Allocation (DBA) capability introduced in Release 2.0.

DBA is an algorithm the Conference/Video Phone uses to reduce packet loss on a congested communication link. DBA will lower the phone's transmitted bit rate according to the packet loss feedback it receives from the remote end, the end goal being that a reduction in the transmission rate should alleviate congestion and packet loss.


DBA relies on the RTCP protocol. At the time of writing, the MiVoice Border Gateway does not support the RTCP protocol. As a result, if the phone is connected to an MiVoice Border Gateway, you should disable the DBA feature on the phone.

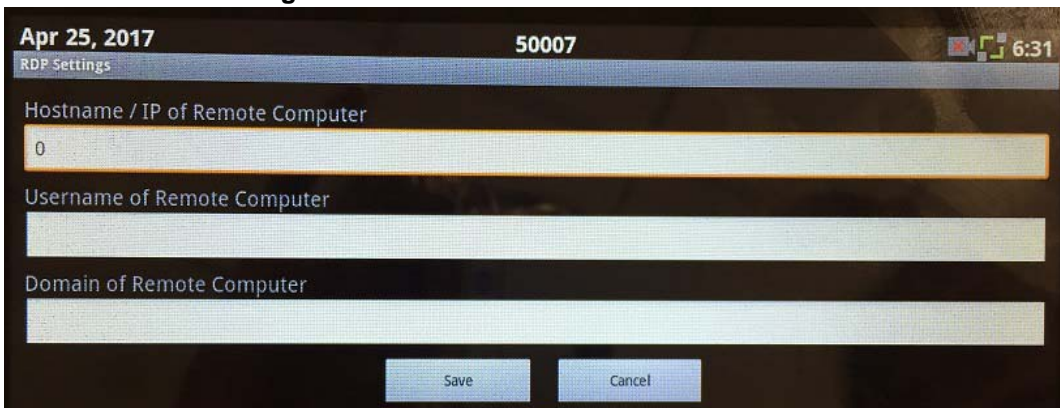
1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Select **Video Settings**.
5. Select the bandwidth for the video quality: High, Medium, or Low.
6. Enable **Dynamic Bandwidth Allocation**, if desired.
7. Click **Save**.

See the *MiVoice Conference/Video Phone Engineering Guidelines* for details on Dynamic Bandwidth Allocation.

RDP Settings

The RDP Settings allow you to set a Preset Remote Computer for phone. This allows the user to press a Connect button and open the RDP session for the Preset computer.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Select **RDP Settings**.




5. Enter the following fields:
 - Hostname/IP Address
Note: By default, the value is 0.
 - Username of Remote Computer
 - Domain of Remote Computer
6. Press **Save**.

See Displaying and Sharing Presentations in the *MiVoice Conference/Video Phone User Guide* for more information.

VNC Settings

The VNC Settings allows the user to enter the pre-set host computer name or IP address displayed in RemoteVNC application. Also the user can set or clear the key mapping selection for Apple Mac or non-Apple Mac computers.


The check box selects the key mapping used for the host computer by the RemoteVNC application. When the box is selected, the application maps the ALT key to the Mac command key and the Windows key to the Mac option key. This allows the phone user to use Mac keyboard functions. When the check box is deselected normal key mapping is in effect.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Select **VNC Settings**.

Ensure that the Apple Mac operating system is upgraded to Mavericks (10.9). Otherwise, it may not respond when logging on through the RemoteVNC.

History Settings

The History Settings allow you to enable or disable the Clear History prompt (replaced with the Close All Apps Icon). It is highly recommended that Close All Apps be enabled in conference rooms.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Select **History Settings**.
5. Select **Clear History Prompt**.


The Close All Apps action stops application sharing, logs the user off the RDP or OfficeWRX session, and clears any states in the Conference Application.

When Close All Apps is disabled, the phone does not prompt the user to clear the session history. Only the Close All Apps icon will be available to manually clear the session history. This configuration is preferable for an executive office environment where the phone is not typically shared with other users.

When Close All Apps is enabled, the phone will prompt the user when a conference call ends. This configuration is recommended for conference room environments where the phone is used by many people.

Extension Microphone Settings


The Extension Microphone Settings allow you to enable the appropriate setting if Extension Microphones are installed.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Select **Extension Microphone Settings**.
5. Select either **NA Microphone installed** or **EU Microphone installed**.

The default is **Not Installed** if extension microphones are not installed. Only Revolabs extension microphones are supported. Refer to the *Revolabs HD Dual Channel System Microphone Installation Guide*.

Advanced Settings Password

You need to enter a password to access Advanced Settings.


1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Select **Advanced Settings Password**.

A window opens allowing you to enter a new password.

5. Enter the new password.
6. Re-enter the password to confirm the password.
7. Select the option for **Visible Password**, if desired.
8. Press **OK**.

The password must be between 4-10 characters in length and is case sensitive. The default password is admin.

Camera Settings

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Camera Settings**.

The Network Camera setting provides the following functions and settings:

- Search — Discover local cameras.
 - The Search function invokes the Camera Discovery Protocol that will search for any available cameras in the phone's subnet. When a camera is found, its IP address is displayed on the phone screen.
 - The Camera Discovery Protocol is a non-routable protocol; it only works when the camera and the phone are on the same subnet.
 - Additionally, you can use the ONVIF Device Manager to define the camera name and location. This is not required, but will give you additional information to differentiate between multiple cameras of the same maker and model listed in the **Discovered Cameras** list. See *Appendix C: ONVIF Device Manager* for more information.

Note: If the camera location name contains a semicolon, for example, AXIS M1104;ConfRm 54485, the text before the semicolon will not display in the Discovered Camera list. You will only see ConfRm 54485. Use other punctuation instead if necessary.

- Enabled — Enables or disables the ethernet camera.
- IP Address/Host Name.
 - This is the IP address (IPv4) or host-domain name of the ethernet camera. The IP address may have previously been manually programmed into the ethernet camera or the camera may have obtained the address from a DHCP server.
 - If a DNS server is being employed, then the ethernet camera can be addressed with the host name of the camera. The DNS server will perform the IP address lookup based on the host name.
 - If the camera is using DHCP, then use the camera manufacturer-provided utility to find the IP address.
- Port — enter the ONVIF port number set in the camera. If unknown, leave the port number blank. The phone will use the default ONVIF port internally.
- Username — Sets the username for access to the ethernet camera. Use the name created when you installed the camera. See “Setting Up and Configuring Video Phone Cameras” on page 70.
- Password — Sets the password for access to the ethernet camera. Use the password created when you installed the camera. See “Setting Up and Configuring Video Phone Cameras” on page 70.

Setting Up and Configuring Video Phone Cameras

Follow the instructions in the camera's Installation Guide to set up the camera. You will need the camera's IP address, username and password in order to configure Camera settings in the Video Phone.

Use the software CD supplied with the camera or download the software from the camera's website. See the appropriate section below for your camera type.

Ethernet Camera Firmware

It is important to ensure that the ethernet cameras are running the correct versions of firmware.

- The Panasonic cameras must run the minimum version of firmware shown in the Table below.
- The AXIS cameras MUST run a specific version of firmware; see the Table below for the Required Firmware Revision.
- The Sony cameras must run the minimum version of firmware shown in the Table below; however, the Sony cameras can be run with newer versions of firmware.

Note: Required Firmware for Release 2.1, SP4 is the same as Release 2.1, SP3.

Ethernet Camera	Required Firmware Revision, Release 2.1, SP6	Required Firmware Revision, Release 2.1, SP5	Required Firmware Revision, Release 2.1, SP3	Required Firmware Revision, Release 2.1, SP2	Required Firmware Revision, Release 2.1, SP1	Required Firmware Revision, Release 2.1, SP0
AXIS M1054	5.50.3.8	5.50.3.4	5.50.3	5.50.3 (See Note)	5.50.3 (See Note)	5.50.3 (See Note)
AXIS: M1104	5.50.3.4	5.50.3	5.50.3	5.50.3 (See Note)	5.50.3 (See Note)	5.50.3 (See Note)
Sony CH-110	1.86	1.85	1.85	1.82	1.82	1.82
Sony CH-120	1.86	1.85	1.85	1.82	1.82	1.82
Panasonic WV-SP105	2.40	2.15	2.1	2.01	2.01	1.82
Panasonic WV-SP305	Not supported	2.13	2.1	2.02	2.01	1.83
Panasonic WV-SPN310	Not supported	2.00	1.71	Not supported		
Panasonic WV-SPN311	Not supported	2.00	Not supported			
Panasonic WV-SPN311A	2.54					

Note: ONVIF user required. See "Create an ONVIF User in Axis" on page 71.

Table 1: Cameras and Minimum Firmware

Setting up the AXIS Camera

It is recommended that you use the AXIS IP Utility and AXIS Camera Management to set up the AXIS camera. These free applications are available on the AXIS Network Product CD supplied with the camera, or can be downloaded from www.axis.com/techsup. See your AXIS Camera Installation Guide for more details.

If you are using an Axis camera, depending on when you purchased the camera, it may be necessary to reinstall the camera's firmware. It may require an upgrade or a downgrade to ensure that the Axis camera is running the exact revision of firmware shown. If necessary you can obtain a copy of the required firmware at Mitel On-Line.

For the Axis camera, if you have upgraded from pre-5.40 firmware to 5.40.9.2 or newer, you must do the following:

- Perform a factory restore on the camera and setup an ONVIF user for security.
- Add the username and password to the Video Phone Camera Settings.

Perform Factory Restore on Axis Camera

1. Open AXIS Camera Management software.
2. Select the **Setup** Menu.
3. Go to **System Options -> Maintenance**.
4. Click **Restore**.

Wait a few minutes for the camera to reset. After the camera has rebooted, login again. Now you must add the ONVIF user.

Create an ONVIF User in Axis

1. In Axis Camera Management, access the **Setup** Menu.
2. Go to **System Options -> Security**.
3. Click **ONVIF**.
4. Add a user: enter the username, password, and select Administrator as the User Group.

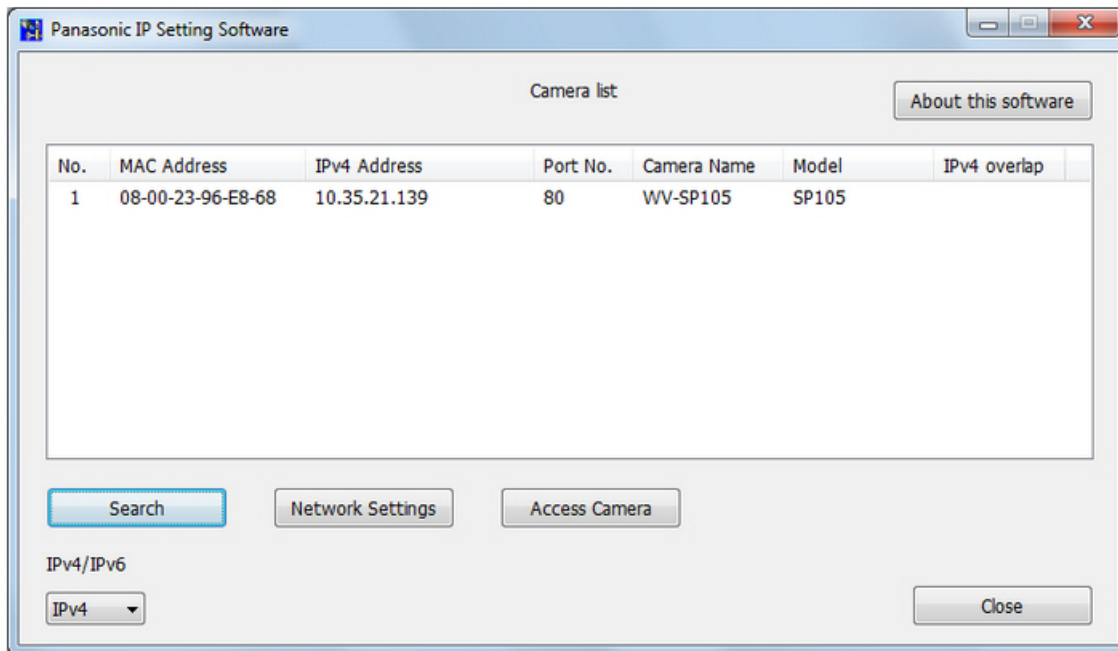
This is the username and password to be used in the Video Phone Camera Settings.

Setting up the Panasonic Camera

Follow the instructions in the Panasonic Installation Guide to set up the camera. Use the software provided on the Panasonic Product CD supplied with the camera or download the software from the Panasonic website. After you have set up the camera, follow the additional instructions below. The instructions below provide an example for the WV-SP105, but are the same for the WV-SP305.

Configuring the Panasonic WV-SP105 - Network Setup

1. Run the Panasonic IP Setting Software and locate the camera IP address.
2. Select the camera that you are configuring, and click Network Settings.



3. In the Network Settings screen, set the network parameters as shown below. Click **Save**.

Network Settings

Network Settings: ☐ StaticIP ☒ DHCP
☐ Auto(AutoIP) ☐ Auto(Advanced)

Port No.: 80

IPv4 Address: 10 . 35 . 21 . 147

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 10 . 35 . 21 . 1

DNS: ☒ Auto ☐ Manual

Primary DNS: 0 . 0 . 0 . 0

Secondary DNS: 0 . 0 . 0 . 0

☒ Wait for camera restarting.

Save Back

4. Click **Access Camera** from the Panasonic IP Settings software initial screen (see above).
The software redirects the settings to a new web browser. You will see the live video from the camera.
5. Click the **Setup** button and provide the login name and password (default "admin", and "12345" according to the user's manual) to login to the setup window.
6. Upgrade the camera to latest firmware version.
 - Click **Maintenance -> Upgrade** to check your camera firmware version.
 - You can download the latest release from the Panasonic website.

WV-SP105 Network Camera - Windows Internet Explorer

http://10.35.21.161/admin/index.html?Language=0

Network Camera WV-SP105

Advanced func. User mng. Server Network Schedule Maintenance

System log Upgrade Status Default reset

Model no.	WV-SP105		
MAC address	08-00-23-9B-CB-1F		
Serial no.	LKV02250		
Firmware version	1 Application	:	1.66
	2 Image data	:	2.01

7. After the upgrade is completed, go back to the Setup menu.

Configuring the Panasonic WV-SP105 - Image Setup

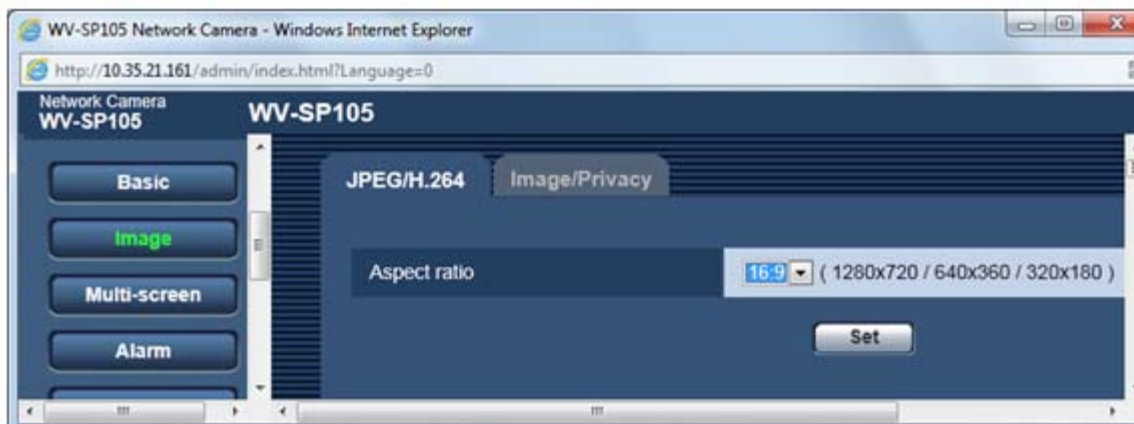
1. Click **Image** and set the following parameter:

Scroll down the screen until you see the items that need to be configured.

- Aspect ratio: 16:9
- H.264(1): Transmission priority: Constant bit rate
- Image quality: Low (motion priority)

Note: For the Panasonic WV-SPN310 and WV-SPN311, for the Aspect ratio: 16:9, chose 1:3 mega pixel [16:9] (30fps).

2. Click **Set**.



The camera is ready to use. See “Camera Settings” on page 69 to configure the Video Phone camera settings.

Light Control Mode 50 Hz 60 Hz Compensation

When flicker is caused by fluorescent lighting, a setting allows the camera to automatically compensate for the flicker. Select 50 Hz or 60 Hz corresponding to the location where the camera is in use.

If necessary, to accommodate fluorescent lights:

1. Click the **Image -> Image/Privacy** tab.
2. Under Light Control Mode, select the required settings.

Camera Security

The System Administrator may want to ensure that the camera cannot be controlled by unauthorized individuals and that video streams cannot be accessed by unauthorized individuals.

To secure the camera, the System Administrator should consult the camera vendor's documentation, in particular:

- There may be the ability to set 'root' passwords in order to control access to camera configuration parameters.
- There may be the ability to set HTTP and RTSP passwords.
- The camera may support an IP address filter or an access control list; both are mechanisms that control which IP addresses are allowed to connect with the camera.
- The camera may support the IEEE 802.1x authentication protocol.
- The administrator may want to disable the camera's NAT firewall traversal abilities.
- The administrator may want to disable anonymous viewer login capabilities.
- The Video Phone only supports "Digest" authentication. When selecting the Authentication Mode, enable Digest authentication in the cameras.

See Ethernet Cameras in the *MiVoice Conference/Video Phone Engineering Guidelines* for more detailed information.

Country Variant

The Country Variant option allows you to select a specific country or region in order to enable the progress tones for that country.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Country Variant**.
5. Select the country for which progress tone are required.


The Conference/Video Phone can be configured to generate country-specific call progress tones. Tone plans for the following counties and/or regions are supported.

- Australia
- France
- Germany
- Italy
- Latin America (Argentina, Chile, Mexico)
- Netherlands
- New Zealand
- North America (Canada, USA)
- Portugal
- Spain
- UK

In some cases, the phone can be deployed in countries that are not included in the above list. In these cases, regional office personnel will be able to suggest the country selection that will provide the most suitable tone plan.

Dialpad Settings

The Dialpad Settings allows you to enable the dialpad to be displayed as the home screen on the phone. This setting is disabled by default.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Dialpad Settings**.
5. Select the checkbox to enable **Display Dialpad** automatically.
6. Select **Idle Time Before Displaying the Dialpad** and set the duration of the idle time before the dialpad is automatically displayed.

You can set it to a minimum of 5 seconds and a maximum of 120 seconds, inclusive.

Licensing and Backup Import/Export


You can use the Licensing and Backup Import/Export setting to do the following:

- Import or export files from an SD card or USB flash drive.
- Import a license allowing an upgrade of a MiVoice Conference Phone to a MiVoice Video Phone.

For full details on mass deployment, see “Mass Deployment” on page 133.

Note: When importing a settings file from a USB flash drive or SD card, the files must be placed in the \uc360\backups directory.

Import/Export Settings

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Licensing and Backup Import/Export**.
5. Press **USB or SD Card Import/Export**.
6. Insert the SD card or USB flash drive.

This option opens a Licensing and Backup Import/Export window.

7. Enter the filename to which you want to export or import settings.
 8. Enter the password.
 9. Click the option you wish to use.
- You can export/save a backup of the current settings to a file on an SD card or USB flash drive.
 - You can import/load an existing backup of settings from a file on the SD card or USB flash drive.

WARNING: MAKE SURE YOU UNMOUNT THE SD CARD OR USB FLASH DRIVE BEFORE REMOVING IT.

Unmount SD Card or USB Flash Drive

1. Press **Settings** .
2. Select **Unmount Media**.
3. Select **SD Card** or **USB Flash Drive**.
4. Remove the SD card or USB Flash Drive.

HTTP Import

The HTTP Import setting opens a new window and has the following options:

- HTTP Import Now — check for new configuration files from the programmed HTTP Server Address.
- Configuration HTTP Server Address — enter the address of the HTTP server.
- Trust All HTTPS Servers — (optional) enable this option if an HTTPS server is used as the Configuration HTTP server.

An HTTPS URI may be specified for the configuration server URI to employ secure SSL HTTPS XML configuration file transfer. By default, the SSL certificate of the server must be signed by a trusted root CA (Certificate Authority) included in the standard list of trusted root CAs in Android Gingerbread 2.3.4 (with the addition of the Mitel root CA). If not, a certificate error is displayed when a download is attempted.

Servers using either a self-signed certificate or one signed by a CA (Certificate Authority) not in the trusted root CA list require this setting to be enabled.

- Time of day for XML Import — the time is fixed to 02:00 AM, the time of the daily reboot.

USB or SD card Import/Export

Pressing the **USB or SD card Import/Export** button goes to the window that allows the user to import or export the configuration settings to USB or SD card. On an export to USB or SD both the encrypted version of the settings backup file and an editable XML file are created. The XML file name is the MAC address.

Upgrade Audio to Video License

The MiVoice Conference Phone can be upgraded to the MiVoice Video Phone by applying a license file.

Each MiVoice Conference Phone supports one license file that is bound to its MAC address. The name of the license file contains the MAC address of the MiVoice Conference Phone, and the suffix .lic.

For example:

<MAC>.lic - 08000F6D9471.lic


Once a MiVoice Conference Phone has been upgraded to a MiVoice Video Phone, the license remains intact even after software upgrades.

Note: Only software release 2.1 SP3 and up support the upgrade license procedure.

You can upgrade the license using the following methods:

- USB flash drive - see "Import License File Using USB Flash Drive" on page 80.
- HTTP(S) download - "Import License File Using HTTP Import" on page 81.

Import License File Using USB Flash Drive

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Licensing and Backup Import/Export**.
5. Press **USB or SD Card Import/Export**.
6. Insert the USB flash drive.

You do not need to enter a filename or password to import a license file.


Note: When importing a license file from a USB flash drive, the files must be placed in the \uc360\backups directory.

7. Press **Import License File from USB flash drive**.

You will see a message, "License Import Success!" when finished. The MiVoice Conference Phone automatically reboots and is upgraded to a MiVoice Video Phone.

You will see Video Enabled Conferencing on the main conference screen.

Import License File Using HTTP Import

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Licensing and Backup Import/Export**.
5. Press **HTTP Import**.
6. Press **Configuration HTTP Server Address** and ensure that it contains the address for the location of the license file. This file is in the same directory as the configuration files. See “HTTP Configuration Server” on page 135 for more details.
7. Press **HTTP Import Now**.

The license file downloads and the MiVoice Conference Phone is upgraded to a MiVoice Video Phone.

You will see Video Enabled Conferencing on the main conference screen.

License File Upgrade Using Automatic Download

When the HTTP(S) Server address is configured, the phone checks for the configuration and license files upon boot up. If a license file exists, it checks the time stamp of the file. Only a new or modified license file is automatically downloaded and applied to the phone.

Upgrade System Software

You have several options for upgrading the system software as new software loads from Mitel become available: USB flash drive and HTTP. Additionally, you can enable Auto Upgrade, Auto Polling, and the set the Upgrade time.


Important: When upgrading from Release 1.0, it is necessary to use an SD card or HTTP Server. When upgrading from 2.0 and up, USB Flash Drive is supported as well.

Important: It is recommended to back up the Conference/Video Phone and maintain a copy of the backup files in a safe location.

Note: The Conference/Video Phone system only supports FAT formatted USB drives. USB drives with U3 formatting will not be recognized by the phone. Write-protected enabled USB drives are not supported.

USB Flash Drive (Supported on Release 2.0 and up)

The USB flash drive must contain the file named upgrade.xml and the upgrade file package in the top-level folder, typically named uc360_x.x.x.x.zip, where x.x.x.x is the upgrade load version. Mitel will supply these files with each new software load. The upgrade.xml file name will contain the new software load version.

1. Insert the USB flash drive with the software upgrade.
2. Press **Settings**  , then press **Advanced**.
3. Press **System Settings**.
4. Select **Upgrade system S/W**.
5. Select **Upgrade system S/W now**.
6. Select **USB Flash**.


You will see a series of messages. This can take several minutes; the Conference/Video Phone will power off and then on. The phone will reboot and load the new software.

7. Unmount the USB flash drive (see “Unmount SD Card or USB Flash Drive” on page 78)

Note: You can abort the software upgrade by pressing the Home  button.

HTTP Server Upgrade

You can upgrade the software using an HTTP Server.

1. Press **Settings**  , then press **Advanced**.
2. Press **System Settings**.
3. Select **Upgrade system S/W**.
4. Select **Software HTTP Server Address** and enter the IP address of the HTTP server where new software loads are stored and press **Save**.
5. Select **Upgrade system S/W now**.


6. Select HTTP.

You will see a series of messages. This can take several minutes; the phone will power off and then on. The phone will reboot and load the new software.

HTTPs Server Upgrade

You can upgrade the software using an HTTPS Server.

An HTTPS URI may be specified for the configuration server URI to employ secure SSL HTTPS XML configuration file transfer. By default, the SSL certificate of the server must be signed by a trusted root CA (Certificate Authority) included in the standard list of trusted root CAs in Android Gingerbread 2.3.4 (with the addition of the Mitel root CA). If not, a certificate error is displayed when a download is attempted.

1. Press **Settings**  , then press **Advanced**.
2. Press **System Settings**.
3. Select **Upgrade system S/W**.
4. Select **Software HTTP Server Address** and enter the IP address of the HTTPS server where new software loads are stored and press **Save**.
5. Select **Trust All HTTPS Servers** (if necessary), and press **Save**.
6. Select **Upgrade system S/W now**.
7. Select **HTTP**.

You will see a series of messages. This can take several minutes; the phone will power off and then on. The phone will reboot and load the new software.


HTTP Server Upgrade via MAS/MiVoice Border Gateway

When the phone is programmed as a Teleworker device, use the following instructions to upgrade the phone software.

1. Login to the MAS server at the root level using an application that allows file transfers.
2. Copy the phone load and upgrade files to the /home/e-smith/files/ibays/Primary/html directory.
3. On the phone, set the HTTP Upgrade IP address to the WAN-side IP setting of the MiVoice Border Gateway.
4. Perform a phone upgrade using the normal upgrade procedure.

Auto Upgrade

You can enable automatic upgrades. This also check for upgrades on a reboot. As well, you can enable Auto polling, which checks daily for new software.

1. Press **Settings** , then press **Advanced**.
2. Press **System Settings**.
3. Select **Upgrade system S/W**.
4. Enable **Auto Upgrade**.

Auto Upgrades are now enabled.


5. Enable **Auto Polling**.
6. Select **Upgrade time**.
7. Enter the time for the upgrade.
8. Tap **Set**.

Avoid setting an auto upgrade time that conflicts with the following:

- The system reboot at 2:00 AM.
- Scheduled LDAP updates.

If you attempt to set a time that conflicts with other scheduled updates, you will receive the message "This time is reserved. Please select a different time."

Debug Settings


1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Debug Settings**.

You have the following options:

- Debugging - By default, debug logging is enabled.
 - Logging Level - Warning is the default Logging Level.
 - Kernel Messages - Enabled.
 - Debug log size.
 - Automatic Ethernet Trace - automatically starts an ethernet trace when network congestion occurs (default is disabled).
 - Manual Ethernet Trace - starts an ethernet trace when the user presses the Start Ethernet Trace button (default is disabled).
 - When enabled, phone will invoke a tcpdump to capture an Ethernet trace when network impairment is detected and/or manually (on demand by the user).
 - Logging level elevated during capture duration.
 - Ethernet trace duration: 60 seconds or 100MB (whichever comes first).
 - Last five captures are retained.
 - Traces are copied to SD card through existing log copy mechanism.
 - Copy Logs to SD - copies logs to an SD card.
 - Copy Logs to USB Flash Drive - copies logs to a USB flash drive.
- Note:** Do not exit Settings while copying logs to the SD card or USB flash drive. Doing so will interrupt the copying process and it will not complete.
- Development - for internal use only.
 - Custom Video Settings - for debug purposes and not recommended to be used.
 - Legacy Interop Mode - this option is used if the phone is experiencing problems interoperating with non-Mitel based servers. By default, this setting is not enabled. Do not enable it unless advised by Mitel Technical Support. While troubleshooting, it is also recommended to enable H.264 base profile to improve interoperation with non-Mitel based servers.
 - Always mirror primary display to HDMI - this option allows the phone to mirror the phone on the HDMI display is for demo and training purposes only.

Web Server Settings


This setting enables a Remote Diagnostic Web Application that allows you to access debug and diagnostics through a web service on the phone.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Press **Web Server Settings**.

This setting is disabled by default. For more details, see *Appendix B: Conference/Video Phone Web Server*.

Reboot

This option allows you to perform a soft reboot, that is, reset the phone while preserving logging and maintaining power to the phone.

1. Press **Settings** .
2. Press **Advanced**.
3. Press **System Settings**.
4. Select **Reboot**.
5. Select **Yes**.

The phone reboots. This is a warm boot and it does not power off the phone.

Factory Reset

1. Press **System Settings**.
2. Select **Factory Reset**.

You will be able to cancel out of the window or confirm that the phone will have all the settings return to the factory defaults, including the password. The following items will be included.

- Default password
- Default network settings
- Default SIP settings
- Default volume
- Default screen brightness
- Debug logging default will be OFF
- Default screen saver timeout value


You will have the option to also reset the current software load back to the original factory load that shipped with the phone.

If using mass deployment (xml cfg) to update the phone, perform a second reset after doing a factory data reset.

WARNING: BACK UP THE CURRENT CONFERENCE/VIDEO PHONE SETTINGS BEFORE RESETTNG TO FACTORY DEFAULTS.

Sound

You can enable audible clicks for all selections and keyboard input:

1. Press **Settings** .
2. Press **Advanced**.
3. Press **Sound**.
4. Tap **Audible Selection** to enable the sound.

The default is off.

Display

To access the Display settings:

1. Press **Settings**, then press **Advanced**.
2. Press **Display**.

You can configure the Brightness and Screen timeout.

To adjust the Brightness of the Conference/Video Phone Display

1. Press **Brightness**.
2. Moving the slider to the left or right.
3. Click **OK**.

To configure Screen Timeout

1. Press **Screen timeout**.
2. Select the **Screen Saver** timeout interval.

You can choose one of the following mutually exclusive radio button options: 15 seconds, 30 seconds, 1 minute, 2 minutes, 10 minutes and 30 minutes. The default timeout is 2 minutes.

The screen will timeout if the phone is continuously idle for the time-out period that was configured. This means that none of the following events occur: touch, key press, incoming call, on a call, or share presentation. The administrator will be logged off.

When the timeout occurs, the screen will go dim and the blue LEDs on the conference unit will flash in a clockwise rotating pattern. Each LED is on for two seconds until there is a user activity or an incoming call is received. The followings actions would be considered as a user activity:

- Press **Home** .
- Click or move the USB mouse.
- Press any keys on the USB keyboard.

Language & Keyboard Settings

To access the Language & Keyboard settings:

1. Press **Settings**, then press **Advanced**.
2. Press **Language & keyboard**.
3. Press **Select language**.

You can select a keyboard language independent from the displayed language. For example, the displayed language could be English but the keyboard language could be French. It is also possible to have multiple keyboard languages selected. The user swipes the spacebar key to switch the keyboard language.

The Conference/Video Phone supports the following languages:

- Deutsch
- English
- Espanol (Espana)
- Espanol (Estados Unidos)
- Francais (Canada)
- Francais (France) - see "Configuring the AZERTY Keyboard" on page 92.
- Italiano
- Nederlands
- Portugues (Brasil)
- Portugues (Portugal)
- Svenska (Swedish)

It is best to connect the external keyboard while the phone is powered off. Then power on the phone. Alternatively, you can reboot the phone after the keyboard has been connected.

Configuring the AZERTY Keyboard

Ensure the external AZERTY keyboard is installed before following the steps below:

1. Press **Settings**, then press **Advanced**.
2. Press **Language & keyboard**.
3. Press **Android keyboard** and select **Input Languages**.
4. Select **Francais (France)**.
5. Go back to **Language & keyboard**.
6. Press **Select language**.
7. Press **Francais (France)**.

You will be asked to confirm the change. Select **Yes**, and the phone will reboot.

If a user selects French (France) as the language, the AZERTY keyboard is the only supported external keyboard. If French language and an external QWERTY keyboard is desired, the user should switch language to French (Canada).

When the language is set to French (France) and the user is in the Contacts app, a touch screen keyboard is not available. Only the external AZERTY keyboard is supported.

Date & Time

To configure the date and time:

1. Press **Settings**, then press **Advanced**.
2. Press **Date & Time**.
3. Press **Select Time Zone** and select the desired time zone.
4. Press **Use 24-hour format** to toggle on or off.
5. Press **Select Date Format** and select the desired date format.
6. Enable **Use NTP time** when available.

NTP (Network Time Protocol) allows the phone to set its time of day clock. The phone will access the default server at the URL - *2.android.pool.ntp.org* - on the internet to obtain the current time of day. A customer can also use DHCP Option 42 for an NTP server.

If an NTP server is not programmed in Settings, and an NTP server is not obtained from DHCP, the default NTP server is used. If an NTP server is programmed in Settings, it is used even if an NTP server is obtained via DHCP.

Maintenance Routine

The MiVoice Video phone performs a regular maintenance routine daily at 2AM. As part of this routine, the device will reset. If the device is in use at that time, the maintenance routine will be deferred until the next day, unless the display is on only as a result of an application being shared on the HDMI display.

Conference/Video Phone Used as Teleworker

If MiVoice Border Gateway (MBG) is part of the MiVoice Business setup for teleworker, the parameters need to be set as described in the sections below.

The MBG must also be configured. See the *MiVoice Border Gateway (MBG) On-line Help*.

For detailed information on the physical connectivity, refer to the *MiVoice Conference/Video Phone Engineering Guidelines*.

Note: For correct operation with the phone, the MiVoice Border Gateway must be running a minimum of MBG 7.1 SP1 software or later.

SIP Settings

Account

1. Enter the SIP Server Address — the MiVoice Border Gateway server address.
2. Enter the Username — the SIP users's ID (programmed in MiVoice Border Gateway).
3. Enter the Login Name — the DN.

Video Codec

For a teleworker with a Video Phone communicating via MiVoice Border Gateway, the **h264highprofile** should be disabled. Only **h264baseprofile** should be enabled. This is because High Profile is less tolerant to network impairment conditions that can occur over the public internet.

For the Dial URI functionality, only the **h264baseprofile** is supported.

Keep Alive Interval

If the phone is used as a Teleworker set, the Keep Alive Interval should be set to 10 seconds to keep the NAT mapping refreshed.

Network Settings

The phone Network Settings for MiVoice Border Gateway may be added in manually through the Settings application or acquired via DHCP. SOHO users will generally need to manually supplement the parameters given by their DHCP Server such as MiVoice Border Gateway (SIP Server) address and DNS address.

LDAP/AD Settings

LDAP Server Settings

1. Enter the IP address of the MiVoice Border Gateway in the Directory Server field.
2. Select **MBG** as the Communication Security Type
3. Select **Save**.

Camera Settings (IP Connectivity)

For a Video Phone, the IP camera and the Video Phone must be on the same subnet to allow local switching between them. This eliminates possible packet loss and ensures high-quality video. It also allows the phone to automatically discover the IP camera (through ONVIF) when the Search capability is used in the Camera Settings.

Video Settings

The Video Phone defaults to a maximum transmission bit rate of 1.5Mbps but can be manually configured to transmit at a maximum 1Mbps or 512Kbs.

The Video Quality Downlink and Uplink settings are the following:

- High - 1.5 Mbs
- Medium - 1 Mbs
- Low - 512 Kbs

By default, the Video configuration settings are symmetric, that is, whatever level is set applies to both downlink and uplink. Some ISP's offer asymmetric downlink bandwidth speeds from the internet, and uplink bandwidth speeds to the internet. The phone allows for this in its Video Settings.

The Video Phone can be configured to transmit to its uplink at a different bit rate than what it offers to receive on its downlink. Check the "Cable/DSL" box and set the uplink speed independently of the downlink setting.

SOHO endpoints should strive to minimize their video bandwidth usage to ensure a high quality voice experience. Mitel recommends a Minimum/Low 512kbs bandwidth setting for both Downlink and Uplink. However, remote endpoints may choose to transmit higher bit rates and consume additional bandwidth.

Bandwidth Requirements Peer-to-Peer

The Video Phone defaults to a maximum transmission bit rate of 1.5Mbps. Video Phone SOHO endpoints connected to the internet via an MiVoice Border Gateway can support 64kbs codecs: G722.1, G711 u-law, and G711 alaw.

There is no guarantee that the remote endpoint will reduce its transmission bit rate so the downlink minimum requirement is 2Mbps. The minimum Video Phone bandwidth requirement for high-quality voice and video in peer-to-peer mode is as follows:

- High (default 1.5 Mbs video) requires a 2Mbps uplink connection to the internet.
- Mid (1 Mbs video) requires a 1.5Mbps uplink connection to the internet
- Min (512 Kbs video) requires a 1Mbps uplink connection to the internet.

Dynamic Bandwidth Allocation (DBA)

DBA is an algorithm the Video Phone uses to lower its transmitted bit rate according to the packet loss feedback it receives from the remote end. Since the Video Phone is connected to the remote end via an MiVoice Border Gateway, the phone should have its DBA disabled.

Disable Enable Dynamic Bandwidth Adaptation under Video Settings.

Troubleshooting

The chart below lists some issues the user may encounter.

Troubleshooting Chart

Problem	Resolution
<p>Bluetooth on the Conference/Video Phone is not supported</p> <p>If a user turns on Bluetooth services, the phone gets into an unknown state.</p>	<p>Click force close and the unit recovers and goes back to the browser.</p> <p>The bluetooth icon is now present in the upper right toolbar.</p> <p>A downgrade is required to recover and get rid of the bluetooth icon.</p>
<p>Cisco WebEx Upgrade Prompt</p> <p>If a user gets the prompt to upgrade the Webex app, and they confirm the upgrade, it does nothing.</p> <p>The user is restricted from upgrading the app on the Conference/Video Phone.</p> <p>Because WebEx is a 3rd party application, the phone cannot prevent this prompt from occurring.</p>	<p>The user can always manually pull up the prompt when they toggle the more options menu on the top left of the app.</p>
<p>Remote VNC - MAC not responding</p> <p>Apple Mac computers not waking up when attempting to log on through a remote client (VNC).</p>	<p>Upgrade the Mac operating system to Mavericks (10.9).</p>
<p>Shortcuts in Browser Don't Work</p> <p>ALT and Left Arrow and ALT and Right Arrow cause the Conference/Video Phone to freeze.</p>	<p>The phone appears to be frozen but is not. To get out of this state, issue the same ALT + arrow key sequence. It has to be the same right or left arrow key used to start the buffer session.</p> <p>The phone will then cycle through all the selections and key presses up to stopping the buffer session. A manual reset of the phone will also clear the buffer session.</p>
<p>Num Lock doesn't work when a USB keyboard is connected to the Conference/Video Phone</p> <p>If a user tries to use any function with Num Lock enabled on a USB keyboard, the functions do not work in the available apps on the phone.</p>	<p>See the <i>MiVoice Conference/Video Phone User Guide</i>: Appendix A - External Keyboard: Supported Keys</p>

Chapter 6

MiVoice Business Configuration

Programming MiVoice Business

This section describes how to program the MiVoice Business settings for the Conference/Video Phone.

The Conference/Video Phone is a SIP device and is programmed on the MiVoice Business. Licensing is also required on the MiVoice Business for the SIP Device. Refer to the *MiVoice Conference/Video Phone Engineering Guidelines* for more details on licensing.

The information provided below is based on MCD Release 5.0 SP2 PR1 (the minimum MCD release supporting the Conference/Video Phone) and may change; however, these instructions will still aid you in programming the phone for use on the MiVoice Business.

User and Device Configuration

Program the following information in the **User and Device Configuration** form in MiVoice Business.

User Profile

1. Select **User and Device Configuration**.
2. Select the **User Profile** tab.
3. Fill in the following fields:
 - **Last Name:** Enter the last name
 - **First Name:** Enter the first name

The screenshot displays the 'User and Services Configuration' interface. On the left, a navigation tree shows 'Users and Devices' expanded, with 'User and Services Configuration' selected. The main panel shows the 'User Profile' tab for user 'Peter Hillier'. The 'Last Name' field is populated with 'Hillier' and the 'First Name' field with 'Peter'. Red arrows highlight these fields. Other fields include 'Department', 'Location', 'Role' (a dropdown menu), 'Language' (set to 'English'), 'Email', 'IDS-Manageable' (checked), 'Prime Phone Service' (set to 'Phone Service'), 'Desktop Admin Access' (unchecked), 'Login ID', 'Password', and 'Confirm Password'.

Service Profile

Configure the Conference/Video Phone as an Endpoint on the MiVoice Business under the Service Profile tab.

1. Select the **Service Profile** tab.
2. Fill in the following fields:
 - **Number:** The DN Number. This number should be the same as the one configured in “Login Name” under “SIP Settings” in the Conference/Video Phone.
 - **Device Type:** UC Endpoint

The screenshot displays the 'User and Services Configuration' interface. On the left is a navigation tree with categories like Licenses, LAN/WAN Configuration, Voice Network, System Properties, Hardware, Trunks, and Users and Devices. The 'Users and Devices' section is expanded, showing 'User and Services Configuration' and 'Attendants'. The main area shows configuration for 'Peter Hillier' (Phone Service (74796)). The 'Service Profile' tab is selected, indicated by a red arrow. The configuration fields are as follows:

Field	Value
Number	74796
Service Label	Phone Service
Directory Name	Hillier, Peter
Prime Name	<input checked="" type="radio"/> No <input type="radio"/> Yes
Privacy	<input checked="" type="radio"/> No <input type="radio"/> Yes
Hot Desking User	<input checked="" type="radio"/> No <input type="radio"/> Yes
Device Type	UC Endpoint
Service Level	Full
Home Element	Local_55
Secondary Element	Not Assigned
Local-only DN	<input type="checkbox"/>
ACD Enabled	<input type="checkbox"/>

Red arrows point to the 'Service Profile' tab, the 'Number' field, and the 'Device Type' dropdown menu.

Service Details

SIP Device Capabilities 71 is the default and contains the programming suitable for the Conference/Video Phone.

- Select the **Service Details** tab under User and Device Configuration.
- No changes are necessary..

The screenshot displays the 'User and Services Configuration' interface. On the left, a navigation tree shows 'Users and Devices' expanded, with 'User and Services Configuration' selected. The main area shows configuration for 'Peter Hillier' (Phone Service 74796). The 'Service Details' tab is active, showing various service parameters. Two red arrows highlight the 'Save Changes' button and the 'SIP Device Capabilities' field, which is set to '71'.

	Day	Night 1	Night 2
Class of Service	10	10	10
Class of Restriction	1	1	1
External Hot Desking Enabled	<input checked="" type="radio"/> No <input type="radio"/> Yes		
External Hot Desking Dialing Prefix			
External Hot Desking Number			
DID Service Number			
Use DID Number for Outgoing Calls	<input type="checkbox"/>		
CPN Substitution Number			
Billing Number			
Personal Speedcall Allocation			
Zone Assignment Method	Default		
Zone ID	1		
SIP Device Capabilities	71		
Interconnect Number	1		
Tenant Number	1		
Lock Default Configuration	<input checked="" type="radio"/> No <input type="radio"/> Yes		
Max Call History Records	0		
Non-Busy Extension	<input checked="" type="radio"/> No <input type="radio"/> Yes		
Call Coverage Service Number	1		

Access and Authentication

1. Select the **Access and Authentication** tab under User and Device Configuration.
2. Enter a **SIP Password** and re-enter the same PIN number in **Confirm SIP Password**.

This will be the same as the Login Password configured in the Conference/Video Phone under SIP Settings.

The screenshot displays the 'User and Services Configuration' interface. On the left is a navigation tree with categories like Licenses, LAN/WAN Configuration, Voice Network, System Properties, Hardware, Trunks, and Users and Devices. The 'Users and Devices' section is expanded, showing 'User and Services Configuration' as the selected item. The main panel shows configuration for 'Peter Hillier' (Phone Service 74796). The 'Access and Authentication' tab is active, with other tabs like 'User Profile', 'Service Profile', 'Device Details', 'Service Details', 'Phone Applications', and 'Keys' visible. The 'Access and Authentication' tab contains fields for 'User PIN', 'Confirm User PIN', 'SIP Password', 'Confirm SIP Password', 'Wireless PIN', and 'Confirm Wireless PIN'. Red arrows point to the 'SIP Password' and 'Confirm SIP Password' fields, which both contain five dots, indicating they are required to be the same.

Multiline Support

In order to support the multi-line conference, you need to program the multi-call feature in the MiVoice Business.

1. Select the **Keys** tab under User and Device Configuration.

User and Services Configuration

Add by Role : Default

Peter Hillier

Phone Service (74796)

Save Changes Cancel

User Profile Service Profile Device Details Service Details

Access and Authentication Phone Applications **Keys**

Clear All Keys Clear Key

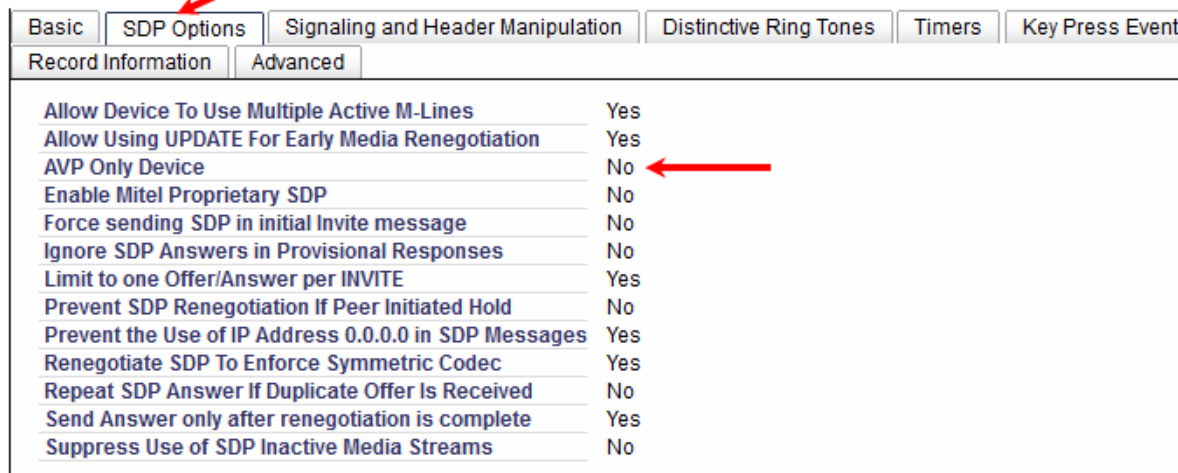
Button Number	Label	Line Type	Button URL Directory Number	Ring Type	MiXML Application Feature	Phone Application Feature
2 !	74796 Multicall	Multicall	74796	Ring	Not Assigned	
3 !	74796 Multicall	Multicall	74796	Ring	Not Assigned	
4		Not Assigned			Not Assigned	
5		Not Assigned			Not Assigned	
6		Not Assigned			Not Assigned	
7		Not Assigned			Not Assigned	
8		Not Assigned			Not Assigned	
9		Not Assigned			Not Assigned	
10		Not Assigned			Not Assigned	
11		Not Assigned			Not Assigned	
12		Not Assigned			Not Assigned	

2. There must be at least three lines (prime + 2 lines) so that the Conference/Video Phone can support conference calls. The following fields must be programmed:
 - Label: Any string
 - Line Type: Multicall
 - Button Directory Number: Same as your DN
 - Ring Type: Ring.

SIP Device Capabilities: SDP Options

You can find this form from View Alphabetically -> SIP Device Capabilities.

1. Select the SIP Device Capabilities form.
2. Select the **SDP Options** tab under SIP Device Capabilities.
3. Disable the following setting:
 - AVP Only Device (if you are using SRTP from/to a device)



Basic	SDP Options	Signaling and Header Manipulation	Distinctive Ring Tones	Timers	Key Press Event
Record Information Advanced					
Allow Device To Use Multiple Active M-Lines		Yes			
Allow Using UPDATE For Early Media Renegotiation		Yes			
AVP Only Device		No			
Enable Mitel Proprietary SDP		No			
Force sending SDP in initial Invite message		No			
Ignore SDP Answers in Provisional Responses		No			
Limit to one Offer/Answer per INVITE		Yes			
Prevent SDP Renegotiation If Peer Initiated Hold		No			
Prevent the Use of IP Address 0.0.0.0 in SDP Messages		Yes			
Renegotiate SDP To Enforce Symmetric Codec		Yes			
Repeat SDP Answer If Duplicate Offer Is Received		No			
Send Answer only after renegotiation is complete		Yes			
Suppress Use of SDP Inactive Media Streams		No			

Timers

For the Timers, the set the **Session Time** to 3600.



Basic	SDP Options	Signaling and Header Manipulation	Distinctive Ring Tones	Timers	Key Press Event
Record Information Advanced					
Registration Period Minimum		300			
Session Timer		3600			
Session Timer: Local as Refresher		No			
Subscription Period		3600			
Subscription Period Minimum		300			
Subscription Period Refresh (%)		80			
Invite Ringing Response Timer		0			

For the remaining tabs, leave them at default settings (i.e. nothing enabled). The remaining tabs include:

- Key Press Event
- Record Information
- Advanced

Chapter 7

MiVoice Office 250 Configuration

MiVoice Office 250 Configuration

The following section describes the hardware and the system programming required for the MiVoice Office 250 on the Conference Phone:

The following hardware is needed to set up the Conference Phone on the MiVoice Office 250:

- MiVoice Conference Phone (Part Number 50006580)
- MiVoice Conference Phone power supply large brick
- Two Ethernet cables
- One available Category F licenses for SIP device (required for the)
- Conference/Video Phone Collaboration Point/MiVoice Conference Phone version 1.0 SP2 and higher
- Mitel 5000 CP Release 5.1 SP4 and higher, or Mitel 5000 CP Release 6.0

The following features are supported:

- Audio bridge with in-room collaboration using an HDMI monitor or projector
- SIP Peer-to-Peer audio
- Up to four calls of any combination of internal and external

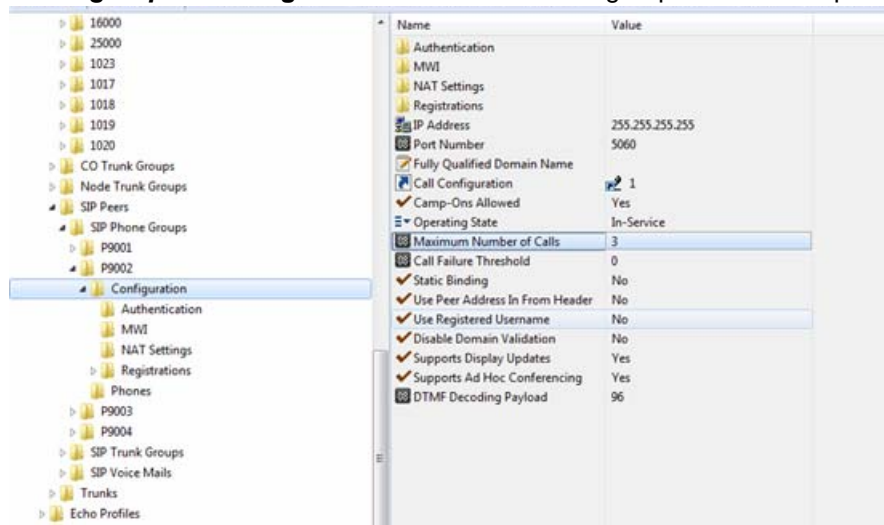
Mivoice Office 250 System Programming

1. In Database Programming, go to **System/Devices and Feature Codes/Phones**.
2. In the right-side pane, right-click and select **Create SIP phone**.

The following screen is displayed:



3. For security reasons, you may want to change the password so it is not the extension number; make a note of the password.
4. In **System -> Devices and Feature Codes**, click **Phones**.
5. In the right-side pane, configure the SIP phone settings that would normally be configured for other types of telephones to allow outgoing access.
6. After creating the SIP phone, the MiVoice Office 250 Database Programming automatically creates a SIP Phone Group with a default configuration profile.
7. Go to **System -> Devices and Feature Codes -> SIP Peers -> SIP Phone Groups/<the SIP Phone group> -> Configuration**. The <SIP Phone group> in the example below is P9001





8. In the right-side pane, click **Maximum Number of Calls**, and select **4** from the adjacent drop-down list. No other changes are required under this profile.

See the *MiVoice Office 250 Features and Programming Guide* for further information.

Conference Phone Programming


Follow the steps below to program the Conference Phone with the MiVoice Office 250 Server Address, User Name and Login Name.

1. Press  to display the Menu bar.
2. Press Settings .
3. Press Advanced.
4. Enter the password. (Tapping in this area will bring up on-screen keyboard, if a physical keyboard is not attached.)

The default password is "admin".

5. Press **OK**.
6. Tap **Date and Time**.
7. Enable **Use NTP time when available**.

Ensure that 2.android.pool.ntp.org is accessible on the network.

8. Press .
9. Press **System Settings**.
10. Tap **SIP Settings**.
11. Enter the **Server Address**. This is the IP address of the MiVoice Office 250 base processor.

Note: If using PS1, then enter the MiVoice Office 250 PS1 IP address instead of the base processor.
12. Enter the **Username**. This is the Extension number on MiVoice Office 250.
13. Enter the **Login Name**. This is the Extension number on MiVoice Office 250.
14. Enter the **Login Password**. This is the Extension number of the MiVoice Office 250 by default, unless it was changed.
15. Tap the Back key to Exit.

At this point, the Conference Phone will be functional for placing and receiving calls. After exiting the Conference Phone programming, it will take a few minutes for the network connection to cycle and establish the SIP registration. If for some reason it fails to register, confirm the password for the SIP extension on the MiVoice Office 250 and make sure it matches on the Conference Phone. A power cycle of the Conference Phone may be required after confirming the credentials.

Appendix A

ONVIF Device Manager

ONVIF Device Manager

In order to use the camera discovery feature in Camera Settings effectively, it is useful to define the camera name and location. This information can be used to differentiate between multiple cameras of the same make and model.

ONVIF Device Manager can be used to change the camera name and location.

Downloading ONVIF Device Manager

The ONVIF Device Manager can be found at

- <http://synesis.ru/en/surveillance/downloads>

The latest version can be downloaded from

- <http://sourceforge.net/projects/onvifdm/>

System Requirements:

- OS: Windows XP SP3/Windows Vista/Windows 7
- Prerequisite: Microsoft .NET 4.0. Available at
 - <http://www.microsoft.com/net/>

Installing Microsoft .NET4.0

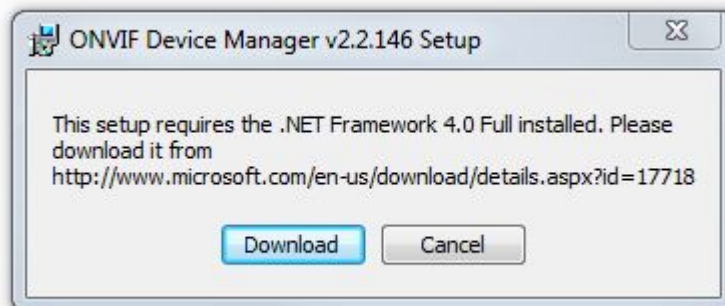
It is recommended to install Microsoft .NET 4 before running the ONVIF Device Manager Setup.

This procedure is optional as some Windows systems may already have it installed.

1. Download Microsoft .NET 4 from <http://www.microsoft.com/net/>
2. Run the ONVIF Device Manager Setup.

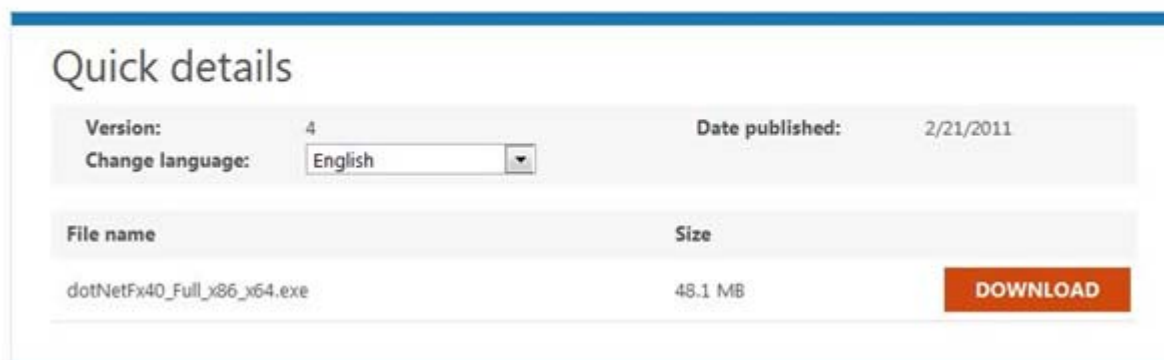
The setup will verify if .NET 4 is installed. If it is .NET is installed, see “Installing the ONVIF Device Manager” on page 119.. If it is not, you will be asked to download it.

3. Click Download.



The Microsoft .NET 4 website is displayed.

The Microsoft .NET Framework 4 redistributable package installs the .NET Framework runtime and associated files that are required to run and develop applications to target the .NET Framework 4.

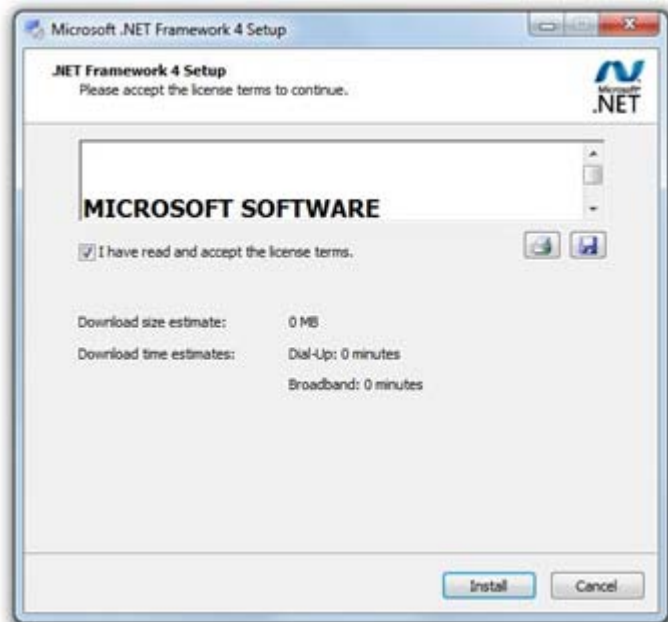


The ONVIF Device Manager installation requires .NET 4 to continue. The current installation of ONVIF must be terminated. You must restart the installation after .NET 4 is installed.

4. Click **Finish**.



- Next, run the Microsoft .NET 4 installer that you downloaded.



- Read the license terms, then select the checkbox.
- Click Install. The installation will then proceed.
- When the installation is completed, click Finish.

Installing the ONVIF Device Manager

- Click on the ONVIF Device Manager Set up .exe.
- Click Next



- Specify the location installation on the next screen. The default is acceptable. Click Next.
- Click Install.
- When the installation is completed, click Finish.

Changing the Camera Name and Location in ONVIF

Giving cameras a distinguished name and location will help you identify Discovered Cameras in Camera Setting (see “Camera Settings” on page 69)

1. Open the ONVIF Device Manager.

The ONVIF compliant devices/cameras are detected automatically and are shown in the list in the left pane.

2. If your device is not found, verify that your computer and network camera are in the same subnet. Click Refresh..
3. Log in with the ONVIF user name and password. Use the user name and password you set up in the camera.
4. Click Log in.



5. Select your camera.
6. Click the Identification button from the list of menu options in the upper right corner.



7. Change the name and location to descriptive values that will help identify its location. Click Apply.

For example:

Name: AXIS M1104 - Conference/Video Phone 54485

Location: Room 5A

Note: If the camera location name contains a semicolon, for example, AXIS M1104;Conference/Video Phone 54485, the text before the semicolon will not display in the Discovered Camera list. You will only see Conference/Video Phone 54485. Use other punctuation instead if necessary.

The screenshot displays the ONVIF web interface. On the left, the 'Device list' table contains several entries. The entry 'AXIS M1104 - UC360 54485' is highlighted. The main panel shows the 'Identification' settings for this device. The 'Name' field is set to 'AXIS M1104 - UC360 54485' and the 'Location' field is set to 'Room 5A'. Other fields like 'Manufacturer', 'Model', 'Hardware', 'Firmware', 'Device ID', 'IP address', 'MAC address', 'ONVIF version', and 'URL' are also visible. The 'Apply' button is at the bottom right of the 'Identification' section.

Device list	AXIS M1104 - UC360 54485	Identification
<input type="text" value="Name, location or address"/> <input type="button" value="Cancel"/>	Identification Time settings Maintenance Network settings User management Certificates System log Web page Events	<input type="text" value="Name: AXIS M1104 - UC360 54485"/>
AXIS M1104 UC360 53022 Firmware: 5.21beta4 Address: 169.254.24.125 Location: 5th floor VE		<input type="text" value="Location: Room 5A"/>
AXIS M1054 - UC360 54488 Firmware: 5.21 Address: 169.254.109.221 Location: 5th floor VE lab	<input type="button" value="Refresh"/>	<input type="text" value="Manufacturer: AXIS"/>
AXIS M1104 - UC360 54485 Firmware: 5.21beta4 Address: 169.254.99.5 Location: Room 5A	<input type="button" value="Live video"/> <input type="button" value="Video streaming"/> <input type="button" value="Profiles"/>	<input type="text" value="Model: AXIS M1104"/>
AXIS M1104 - UC360 54487 Firmware: 5.40.9.2 Address: 169.254.112.103 Location: 5th floor VE lab		<input type="text" value="Hardware: 179.6"/>
AXIS M1104 UC360 53028 Firmware: 5.21beta4 Address: 10.37.64.106 Location:		<input type="text" value="Firmware: 5.21beta4"/>
AXIS M1104 UC360 53029 Firmware: 5.21beta4 Address: 169.254.117.61 Location:		<input type="text" value="Device ID: 00400C00B2D"/>
AXIS M1054 - UC360 54486 Firmware: 5.40.9.2 Address: 169.254.107.84 Location: 5th floor VE lab		<input type="text" value="IP address: 10.37.64.104, 169.254.99.5"/>
<input type="button" value="Add"/> <input type="button" value="Refresh"/>		<input type="text" value="MAC address: 00-40-0C-09-8B-2D"/>
		<input type="text" value="ONVIF version: 1.0"/>
		<input type="text" value="URL: http://169.254.99.5/onvif/service"/>
		<input type="button" value="Apply"/> <input type="button" value="Cancel"/>

You will now see the newly-name camera in the list of discovered cameras in the Video Phone Camera Settings when using the Camera Search function.

Appendix B

Web Server

Conference Phone /Video Phone Web Server

The Remote Diagnostic Web Application allows you to access debug and diagnostics through a web service on the Conference/Video Phone. See “Web Server Settings” on page 86 for information on how to enable this service. It is disabled by default. The features of this application require an up-to-date browser - IE11 or a current version of Firefox are recommended.

1. Enter the IP address of the Conference/Video Phone you wish to access in a web browser.

The landing page shows some basic information about the phone to confirm that you have accessed the correct phone.

2. Next, click **Diagnostics**.

A security warning will likely be presented by the browser unless the Mitel Root Certificate was previously installed.



You may choose to ignore the security warning and proceed, but will likely be issued with the warning each time you access diagnostics or your browser may allow you to add a security exception. Installing the Mitel Root CA is only done once for your browser and will allow the browser to authenticate any Conference/Video Phone or any other Mitel signed server without continual security warnings.

- Click on the link *Install the Mitel Root Certificate* at the bottom of the landing page.
 - This action opens a page “Installing the Mitel Root Certificate” that describes how to download and install a Mitel Root Certificate on Firefox, IE, Opera and Chrome.
 - Install the Mitel Root Certificate following the instructions provided.
3. If the username and password have not already been entered, you will see a login page.

Enter the user name and password and click **Login**.

The main diagnostics page is displayed.

Note that there is currently only a single valid username - admin. The password is the same used to access **Advanced Settings**.

There is a four minute inactivity timeout when on the diagnostics page which will result in an automatic logout and throw the user to a logged out page. When on other pages such as directory listings the authenticated session again times out after four minutes - this does not result in an immediate redirection to the logged out page, rather when the administrator tries to access diagnostics or other files requiring authentication there is a redirect to the login page.

You will see Diagnostics Page (see illustration on the next page) with the following tabs:

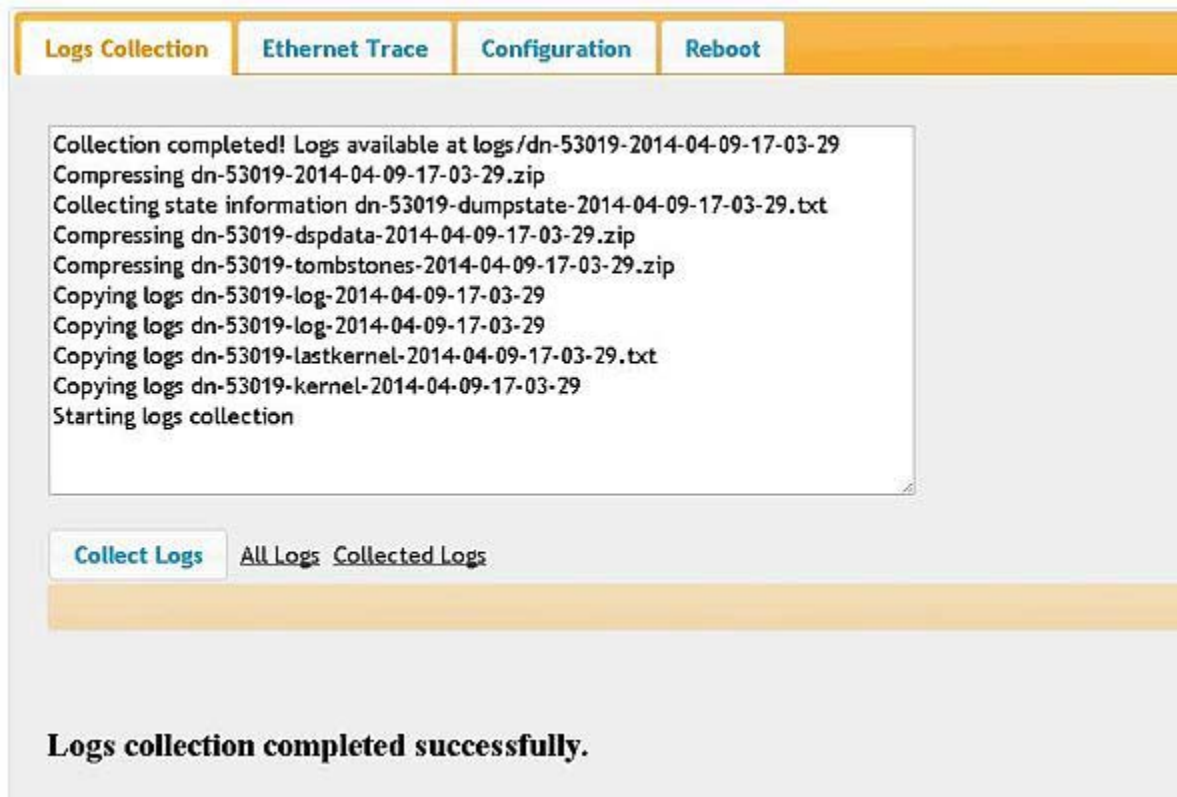
- Logs Collection
- Ethernet Trace
- Configuration
- Reboot

Logs Collection

The Logs collection tab has a button to initiate the collection and packaging of the diagnostics logs. This package is also available at the Debug Setting /Copy Logs to ...

The Logs progress message normally seen on the Conference/Video Phone display appears in the text box. Rather than copying logs to USB or SD card, when completed an additional link (Collected Logs) is presented to the logs package just generated.

There are two links (All Logs) and (Collected Logs) that can be used to browse the generated logs directories. Note that these open a new browser tab for file system navigation.



The screenshot shows a web interface with a top navigation bar containing four tabs: "Logs Collection" (highlighted in orange), "Ethernet Trace", "Configuration", and "Reboot". Below the tabs is a large text box containing the following log messages:

```
Collection completed! Logs available at logs/dn-53019-2014-04-09-17-03-29
Compressing dn-53019-2014-04-09-17-03-29.zip
Collecting state information dn-53019-dumpstate-2014-04-09-17-03-29.txt
Compressing dn-53019-dspdata-2014-04-09-17-03-29.zip
Compressing dn-53019-tombstones-2014-04-09-17-03-29.zip
Copying logs dn-53019-log-2014-04-09-17-03-29
Copying logs dn-53019-log-2014-04-09-17-03-29
Copying logs dn-53019-lastkernel-2014-04-09-17-03-29.txt
Copying logs dn-53019-kernel-2014-04-09-17-03-29
Starting logs collection
```

Below the text box is a "Collect Logs" button and two links: "All Logs" and "Collected Logs". The "Collected Logs" link is underlined. At the bottom of the interface, a message states: **Logs collection completed successfully.**

When browsing the directories of log results, you can click on the zip file to download the logs package and if there are any ethernet trace files they will be available in the tcpdump directory and also available for download.

The "All Logs" link accesses the directory listing all logs package directories stored on the Conference/Video Phone. A maximum of five logs packages are allowed on the phone, deleting the oldest as more are collected.

Ethernet Trace

Ethernet trace (which collects tcpdump info on the network and temporarily enables debug logs) can be started from the Ethernet Trace tab. This is the same operation that is available from the Settings menu on the Conference/Video Phone.

Again there is a link to the files directory allowing the just collected or previous retained tcpdumps to be downloaded. Note that these files can be very large and the Conference/Video Phone retains a maximum of 500MB of ethernet trace in this directory. Also note that the Logs Collection moves files from here to the logs package directories. While the trace is in progress, a message appears next to the status at the top of the page.



Configuration

Export Settings

Currently, the Conference/Video Phone supports the collection and downloading of the configuration XML file from the Conference/Video Phone using the **Export Settings** button and a link which pops up beside that when the XML file is available. This can be used to view or download the XML file.

A message indicates the progress/completion of the collection process and the link appears when the xml file is available. Note that the file is named MN_MAC.cfg (MAC is the MAC of the phone as shown in the top info line) to correspond to the file name used by the Mass Deployment configuration scheme

Note that Internet Explorer 10 and Internet Explorer 11 default the "save target as" file with an .xml extension rather than keeping the .cfg extension. You can change the file extension in the Save dialog to .cfg

The screenshot shows a web interface with a top navigation bar containing four tabs: "Logs Collection", "Ethernet Trace", "Configuration" (which is active), and "Reboot". Below the tabs, there are several buttons and a text field. The "Export Settings" button is highlighted in blue. To its right is a link labeled "Collected Configuration XML". Below these, there is a button labeled "Import Settings via HTTP Server" followed by a text field for "Server Url (optional)". Below that is a button labeled "Import CSV Directory via HTTP Server" followed by a note: "Note that the Contacts Settings / Populate from CSV File checkbox must be enabled for CSV Directory to be applied". At the bottom, there are two buttons: "Select File to Import" and "Upload File : Please Select First".

Import Settings via HTTP Server

The **Import Settings via HTTP Server** button can be used to request that the Conference/Video Phone download and apply the configuration of its Mass Configuration XML files from an HTTP Server. By default, the phone will use the programmed static or DHCP configuration HTTP server to query for the Mass Configuration XML files and apply them in the normal sequence - MN_GENERIC.cfg and MN_MAC.cfg (where MAC is MAC of phone e.g. MN_08000F73811C.cfg).

However, an optional Server URL is provided to set an independent URL and override any statically configured or DHCP value on the Conference/Video Phone. This field may specify a directory on the server.

1.2.3.4/xmlDirectory

in which to locate the above two files or it may specify a full pathname to a single cfg file

1.2.3.4/xmlDirectory/configFile.cfg

Import CSV Directory via HTTP Server

The **Import Setting via HTTP Server** button downloads and applies the configuration from the HTTP server but does not force the CSV Directory contacts files to be reloaded from the server. The

CSV Directory files are downloaded only if the **Populate from CSV file** in Contacts Settings is off, and the new configuration (just downloaded and applied) sets it to on.

The **Import CSV Directory via HTTP Server** button downloads the CSV Directory files. This option makes this request regardless of whether the setting **Populate from CSV file** in Contact Settings is off or on. However, the contacts in the CSV files only populate the Contacts application if **Populate from CSV file** is on.

Import Settings Directly

The XML configuration file can be uploaded directly to the Conference/Video Phone. First, select a cfg file directly from your local machine's file system by pressing the **Select File to Import** button. When a file is successfully selected, the **Upload File** button will be enabled. Pressing the active **Upload File** button will upload the cfg file and import the contained settings to the Conference/Video Phone.

The screenshot shows a web interface with a top navigation bar containing four tabs: "Logs Collection", "Ethernet Trace", "Configuration" (which is highlighted in orange), and "Reboot". Below the tabs, there are several interactive elements:

- An "Export Settings" button followed by a link "Collected Configuration XML".
- An "Import Settings via HTTP Server" button followed by a text input field labeled "Server Url (optional)".
- An "Import CSV Directory via HTTP Server" button followed by a note: "Note that the Contacts Settings / Populate from CSV File checkbox must be enabled for CSV Directory to be applied".
- A "Select File to Import" button followed by a disabled button labeled "Upload File : Please Select First".

The current settings can be downloaded using the Export Settings download link, edited locally then uploaded to apply any required changes.

When configuration download (or upload (see "Import Settings Directly" on page 130)) completes, if as a result the setting **Populate from CSV file** is changed from off to on, a check is made on the HTTP configuration server for CSV Directory files. These files are downloaded if they have been modified since the last download. Once the files are downloaded, the Contacts application parses the CSV file(s) and populates the contacts into the Contacts application.

If the setting **Populate from CSV file** is off, then the Contacts application contacts are downloaded from a configured LDAP server after configuration download (or upload) completes. See "Contacts Settings" on page 52 for more information.

Reboot

The administrator may request a reboot of the phone. There are two options: standard and forced.

The standard reboot will request a reboot but will be rejected if the phone is in use. This is indicated to the administrator in a status response including the reason the reboot was rejected.

The forced reboot can be used to force a reboot in the case that the phone is busy or left in a busy state. In either case, the Conference/Video Phone wakes its display and displays the reboot countdown. The countdown is also reflected on the status line of the web page.

The countdown can still be interrupted, for reboot or forced reboot, directly on the Conference/Video Phone using the cancel icon on the reboot countdown screen, or remotely by the administrator using the **Cancel Reboot** button on the web page. Feedback on the web page will indicate if this has happened.



Appendix C

Mass Deployment

Mass Deployment of Conference/Video Phone

In order to deploy a large number of Conference/Video Phones in an office, there are ways to configure them without physical access to each phone. The Conference/Video Phone uses configuration files (programmed offline) for setting up its configuration at boot-up time. See “Mass Deployment Configuration File Reference” on page 151 for an example of the types information to included in the Conference/Video Phone XML Configuration File.

Requirements

See the following requirements below for mass deployment of Conference/Video Phone.

MiVoice Business or 3rd Party SIP Server

This server provides the SIP Registrar. If MiVoice Business is not be used, the Conference/Video Phone needs a 3rd party SIP Registrar.

MiVoice Business or 3rd Party DHCP Server

This server is used to provide the IP address (Static IP address can also be assigned) of the phones. DHCP options 125/43 and option 66 can be used to specify separate URI's for firmware upgrade and mass deployment XML configuration files. This enables phones to upgrade firmware and apply configuration from a factory default state.

HTTP Configuration Server

An HTTP server is used to host the configuration files. When the Conference/Video Phone is configured with an HTTP server, the phone will check for any changes to its XML configuration file on boot up.

This server may also host CSV files holding corporate contacts for the Contacts application. If the setting **Populate from CSV file** (contacts_use_csv in the cfg files) is enabled in the configuration then the phone checks the configuration server for files name MN_Generic.csv and MN_XXXXXXXXXX.csv (where the X's represent the 12-character hexadecimal MAC address of the specific phone).

The configuration files should be placed in an HTTP server directory and that URI can be statically programmed as the HTTP Configuration Server Address under:

Settings -> Advanced -> System Settings -> Backup Import/Export -> HTTP Import -> Configuration Server Address

Alternatively, if that static setting is left blank (as it is by default) the URI can be sourced from DHCP options 125, 43 or 66.

Note: The HTTP Configuration Server can be the same server as the HTTP S/W Upgrade Server. A single server or separate servers are possible as the URI's are independent.

An HTTPS URI may be specified for the configuration server URI to employ secure SSL HTTPS XML configuration file transfer.

Note by default that the SSL certificate of the server must be signed by a trusted root CA (Certificate Authority) included in the standard list of trusted root CA's in Android Gingerbread 2.3.4 (with the addition of the Mitel root CA). Otherwise, a certificate error will be indicated when a download is attempted.

Servers using either a self-signed certificate or one signed by a CA not in that trusted root CA lists require the following setting to be enabled:

Settings -> Advanced -> System Settings -> Backup Import/Export -> HTTP Import / Trust All HTTPS

Adding .cfg and .lic extension for IIS HTTP Server

You must add the .cfg and .lic extension in the MIME settings of the Microsoft Internet Information Services (IIS) HTTP server.

1. Open the Control Panel, then open Administrative Tools.
2. Click on IIS Manager.
3. Click on MIME Types.
4. Click Add.
5. Enter .cfg in the File Name Extension field.
6. Enter text/xml in the MIME type field and click OK.
7. Repeat same procedure for .lic extension.

HTTP S/W Upgrade Server

An HTTP server is used to host the firmware and software upgrade files. When Auto Upgrade is enabled, a phone will check daily at a specified time or on reboot, if the software revision in the upgrade.xml in the upgrade server url directory matches the current software revision. If the revision don't match and the upgrade file is found, it is downloaded using HTTP and the software upgrade will be applied.

Configuration Files

These are XML-based files containing the Conference/Video Phone's configuration, stored on the HTTP server.

- **Generic file** - This file (**MN_Generic.cfg**) is used to apply attributes globally, to all phones.
- **Specific file** - These files are used to apply features/attributes to specific phones. At a minimum this file should supply the SIP registration information for a specific phone. There should be one per phone that is to be mass deployed and remotely configured via XML files.
 - **MN_XXXXXXXXXXXX.cfg** (where the X's represent the 12-character hexadecimal MAC address of the specific phone). Configuration is automatically downloaded at phone boot-up if the file has been modified since any previous download.

The Generic file is loaded first. The MAC address-specific file is loaded next and overwrites any duplicated settings in the Generic file. See "XML File Format" on page 141 XML File for more details.

Programming/Configuration Steps

STEP 1: DHCP Server Settings

HTTP Configuration Server URI

Add the string:

id:ipphone.mitel.com;cfg_uri=[http[s]://][hostname|IP][:port_number]/path/to/config/directory

in option 125/43 (MiVoice Business provides an option to configure vendor-specific info in option 43, but not in option 125.)

Alternatively, DHCP option 66 can also be used to provide the URI. Note that either HTTP or HTTPS may be used for the `cfg_uri` value, but only HTTP for the `sw_uri`.

Order of precedence of options:

- Static overrides DHCP
- Option 125 `cfg_uri`
- Option 43 `cfg_uri`
- Option 66
- Option 125 `sw_uri`
- Option 43 `sw_uri`

HTTP S/W Upgrade Server URI

Add the string:

id:ipphone.mitel.com;sw_uri=[http[s]://][hostname|IP][:port_number]/path/to/firmware/directory

in option 125/43. Alternatively DHCP option 66 can also be used to provide the URI.

Order of precedence of options:

- Static overrides DHCP
- Option 125 `sw_uri`
- Option 43 `sw_uri`
- Option 66

Note: One of either option 125 or 43 must be used not both. Option 125 takes precedence over 43 and if present any contents of option 43 are ignored. Note also that `sw_uri` can be used to configure both the configuration URI and the S/W upgrade URI.

Notes on URI format

[http[s]://] hostname | IP [:port_number] /path/to/config/directory

hostname is the FQDN (Fully Qualified Domain Name) of the HTTP server

IP is the dotted IP address of the server e.g. 10.33.67.89

[] brackets around an item indicate it is optional so port_number is optional

| separates a list of options, e.g. hostname | IP

Here are some examples:

http://1.2.3.4/Conference/Video PhoneFirmware

1.2.3.4:8888/Conference/Video PhoneFirmware

https://myserver.mitel.com/Conference/Video Phone/FirmwareDirectory

STEP 2: Creation of the Configuration files

The configuration files are required to be hosted on the HTTP server. Here are the steps to create the files.

Obtain a template file and create MN_Generic.cfg

1. Install one Conference or Video Phone and configure it manually through the its administration interface.
2. Make a backup of the configuration file (.cfg backup) on the USB flash drive using Settings -> Advanced -> Backup Import/Export -> USB or SD card Import/Export. You will need to know the admin password to create this file - the default is admin.

This creates the correct directory tree structure.

Note that filename you provide (for example, backup) will be use to create two files. The file with the name specified (e.g. backup) is a binary file. The file needed is "MN_<MAC Addr>.cfg" located under /UC360/backups on the USB or SD card.

It is also possible to obtain this file using a browser by enabling the Web Server under Settings -> Advanced -> Web Server Settings -> Web Server Enabled. If you do this, though, the Web Server will be enabled in the XML configuration file you download and must be disabled by editing the file if the desire is to have it disabled for all phones.

3. Copy the .lic file to /UC360/backups on the USB flash drive. Import the license file.
4. If in the Advanced Settings, use the HOME key to Settings dialog and from there use "Unmount Media" to cleanly unmount the USB / SD card.
5. Copy that entire "known working" configuration file to a text editor like notepad and save it as MN_Generic.cfg.
6. Remove all entries in MN_Generic.cfg that will be set in MN_<MAC Addr>.cfg files, i.e. those values that are not going to be generic to all Conference/Video Phone's or other Mitel sets that use the same mass deployment mechanism. One entry that should certainly be removed is <user_list> which is phone specific.

Configure Per Phone Specific attributes in MN_<MAC Addr>.cfg files

1. Create MN_<MAC Addr>.cfg files for all phones using their MAC Address using that 'known working' configuration file minus the entries we leave in the file MN_Generic.cfg.
2. Using the user-extension specific information <user_list> removed from the above saved MN_Generic.cfg file. Enter the USER ID in <user_list>. Refer below for an example.
3. Put these files (MN_Generic.cfg and the MN_<Mac Addr>.cfg files) on the HTTP Server in the directory configured in "STEP 1: DHCP Server Settings" on page 137.

STEP 3: Configuring DN

Configure the DN using the steps below.

1. Connect the power cable to the Conference/Video Phones.
2. At boot-up, each phone will do the following:
 - Request and download the MN_Generic.cfg configuration file from the HTTP server and overwrite existing setting values with all the generic file values.
 - Request and download its specific configuration file MN_<MAC Addr>.cfg from the HTTP server, and overwrite existing settings values with all the defined values in this configuration file.

Notes: If the Conference/Video Phone requests a configuration file that is not on the HTTP server, settings on the phone do not change.

When a Conference/Video Phone uses configuration files, you can still change settings manually; however, if these settings are also defined in the configuration files, the files overwrite manual settings the next time the phone reboots if the file is modified after the manual changes were applied.

If the HTTP Server does not support sending a valid LastModified timestamp with the response to GET the XML file then the check for modification before downloading is presumed to indicate a change to the XML file and it will always be downloaded.

When using mass deployment (xml cfg) to update the phone, perform a second reset after doing a factory data reset.

Appendix D

XML File Format

XML File Format

The Conference/Video Phone implementation of the XML file format contains a list of tags arranged according to their correspondence to the phone menu hierarchy of **Settings -> Advanced -> System Settings** menus, plus some user settings (currently only Browser app settings).

See “Mass Deployment Configuration File Reference” on page 151 for a listing of all menu settings and their possible values.

Note: The \$ and the & characters are not supported in the mass deployment XML cfg file.

Parameter Model

A mass deployment XML cfg file must start with a section as follows:

```
<Parameter Model="UC360">
```

This tag must exist in the XML file, and if it is not found a warning log is issued on the Conference/Video Phone and the rest of the file will not be processed. All tag and attributes within this XML element are used to specify the phone configuration.

XML Tags and Attributes

The settings are applied incrementally such that a value set from MN_<MAC Addr>.cfg will override any value previously set via MN_Generic.cfg. For the above example, some of the debug setting attributes could be specified in MN_Generic.cfg and others in MN_<MAC Addr>.cfg. If a value is specified in both, the last set wins i.e. the value in MN_<MAC Addr>.cfg.

Parsing of tags and attributes values applies validation rules to the same level as applied by the Advanced Settings user interface, i.e. if you can set it via the GUI then it is considered valid by the XML parser. Any invalid values will not be applied to the active configuration and will result in a warning log.

Configuration File Time Conflicts

For Configuration file time conflicts, a message is displayed during the XML import indicating a conflict. The following conditions are checked:

- If the S/W upgrade time is within 30 minutes before or after the 2:00 AM reboot, a message is displayed and the S/W upgrade time is not imported.
- If the LDAP update time in the XML file is within 30 minutes before or after the 2:00 AM reboot time, a message is displayed and the LDAP update time is not imported.
- If the S/W update time is within 30 minutes before or after the LDAP update time, a message is displayed and the S/W update time is imported, but the LDAP time is not imported.

User Configuration

A single `user_list` tag containing a single `User` tag is required to provide user configuration. It is optional. If there are either multiple `user_list` tags or multiple `User` tags then warning logs will be issued on the Conference/Video Phone and only the first `User` tag entry of the first `user_list` entry will be used. This should be used in the `MN_<MAC Addr>.cfg` file. For example:

```
<user_list>
<User ID="1234" DispName = "Susan Brown" Pwd="4321" AuthName="1234"
ProxySvr="10.44.180.33" ProxyPort="5060" ProxyScheme="1,2" OutSvr=""
OutPort="5060"/></user_list>
```

Tag	Attribute	Validation Rule
User	ID	Any string
	DispName	Any string
	Pwd	Any string
	AuthName	Any string
	ProxySvr	Any string
	ProxyPort	Empty or number, ignored if ProxySvr not set
	OutSvr	Any string
	OutPort	Empty or number, ignored if OutSvr not set
	ProxyScheme	Any comma separated list of 1,2,3 (e.g. "1" or "1,2")
	DialURIOutboundProxySvr	Any string
	DialURIOutboundProxyPort	Empty or number, ignored if not set

Country Variant

The Country Variant for North America is mapped to US when we generate XML, but we support US or CA to map to North America for parsing.

Certificate

Note that the certificates value may contain multiple certificates in PEM format, each beginning with the standard header.

```
-----BEGIN CERTIFICATE-----
```

which always starts a certificate. These certificates are root certificates and are used for when SIP transport TLS is configured for server certificate validation. The Mitel Root CA certificate is included by default.

Contacts Translation Plan Rules

The first five ldap_translation Rules are processed; any more entries will generate warning logs and be otherwise ignored. Note that a Rule must always be accompanied by its corresponding Prefix. The Prefix may be empty but it must always be there, otherwise warning logs will be issued that the entry is invalid.

Dial Plan Settings

The first five dialpl DigitDials are processed; any more entries will generate warning logs and be otherwise ignored.

Video Quality Settings

Video_quality settings that can be set from XML represent a subset of the values configurable from the Advanced Settings. Specifically settings available from **Debug Settings -> Custom Video Settings** are not included. Instead the full set of uplink+downlink bit rate, resolution and frame rate are set from the subset as they are for **Advanced Settings -> Video Settings**. Note that when CableDSL is enabled the link is considered asymmetric and uplink and downlink settings are applied independently from the values for Uplink and Link respectively. Conversely when disabled the uplink values are overridden by the downlink values to achieve a symmetric bandwidth configuration, so in this case the Uplink value is irrelevant.

Timezone Values

The timezone value must be one of the following timezone ids. The tag values are what is displayed in the **Advanced Settings -> Date & time settings -> Select time zone list** for the default locale.

```
<timezones>

<timezone id="Pacific/Majuro">Marshall Islands</timezone>

<timezone id="Pacific/Midway">Midway Island</timezone>

<timezone id="Pacific/Honolulu">Hawaii</timezone>

<timezone id="America/Anchorage">Alaska</timezone>

<timezone id="America/Los_Angeles">Pacific Time</timezone>

<timezone id="America/Tijuana">Tijuana</timezone>

<timezone id="America/Phoenix">Arizona</timezone>

<timezone id="America/Chihuahua">Chihuahua</timezone>

<timezone id="America/Denver">Mountain Time</timezone>

<timezone id="America/Costa_Rica">Central America</timezone>

<timezone id="America/Chicago">Central Time</timezone>
```

<timezone id="America/Mexico_City">Mexico City</timezone>

<timezone id="America/Regina">Saskatchewan</timezone>

<timezone id="America/Bogota">Bogota</timezone>

<timezone id="America/New_York">Eastern Time</timezone>

<timezone id="America/Caracas">Venezuela</timezone>

<timezone id="America/Barbados">Atlantic Time</timezone>

<timezone id="America/Manaus">Manaus</timezone>

<timezone id="America/Santiago">Santiago</timezone>

<timezone id="America/St_Johns">Newfoundland</timezone>

<timezone id="America/Sao_Paulo">Brasilia</timezone>

<timezone id="America/Argentina/Buenos_Aires">Buenos Aires</timezone>

<timezone id="America/Godthab">Greenland</timezone>

<timezone id="America/Montevideo">Montevideo</timezone>

<timezone id="Atlantic/South_Georgia">Mid-Atlantic</timezone>

<timezone id="Atlantic/Azores">Azores</timezone>

<timezone id="Atlantic/Cape_Verde">Cape Verde Islands</timezone>

<timezone id="Africa/Casablanca">Casablanca</timezone>

<timezone id="Europe/London">London, Dublin</timezone>

<timezone id="Europe/Amsterdam">Amsterdam, Berlin</timezone>

<timezone id="Europe/Belgrade">Belgrade</timezone>

<timezone id="Europe/Brussels">Brussels</timezone>

<timezone id="Europe/Sarajevo">Sarajevo</timezone>

<timezone id="Africa/Windhoek">Windhoek</timezone>

<timezone id="Africa/Brazzaville">W. Africa Time</timezone>

<timezone id="Asia/Amman">Amman, Jordan</timezone>

<timezone id="Europe/Athens">Athens, Istanbul</timezone>

<timezone id="Asia/Beirut">Beirut, Lebanon</timezone>

```
<timezone id="Africa/Cairo">Cairo</timezone>

<timezone id="Europe/Helsinki">Helsinki</timezone>

<timezone id="Asia/Jerusalem">Jerusalem</timezone>

<timezone id="Europe/Minsk">Minsk</timezone>

<timezone id="Africa/Harare">Harare</timezone>

<timezone id="Asia/Baghdad">Baghdad</timezone>

<timezone id="Europe/Moscow">Moscow</timezone>

<timezone id="Asia/Kuwait">Kuwait</timezone>

<timezone id="Africa/Nairobi">Nairobi</timezone>

<timezone id="Asia/Tehran">Tehran</timezone>

<timezone id="Asia/Baku">Baku</timezone>

<timezone id="Asia/Tbilisi">Tbilisi</timezone>

<timezone id="Asia/Yerevan">Yerevan</timezone>

<timezone id="Asia/Dubai">Dubai</timezone>

<timezone id="Asia/Kabul">Kabul</timezone>

<timezone id="Asia/Karachi">Islamabad, Karachi</timezone>

<timezone id="Asia/Oral">Ural'sk</timezone>

<timezone id="Asia/Yekaterinburg">Yekaterinburg</timezone>

<timezone id="Asia/Calcutta">Kolkata</timezone>

<timezone id="Asia/Colombo">Sri Lanka</timezone>

<timezone id="Asia/Katmandu">Kathmandu</timezone>

<timezone id="Asia/Almaty">Astana</timezone>

<timezone id="Asia/Rangoon">Yangon</timezone>

<timezone id="Asia/Krasnoyarsk">Krasnoyarsk</timezone>

<timezone id="Asia/Bangkok">Bangkok</timezone>

<timezone id="Asia/Shanghai">Beijing</timezone>

<timezone id="Asia/Hong_Kong">Hong Kong</timezone>
```

```
<timezone id="Asia/Irkutsk">Irkutsk</timezone>

<timezone id="Asia/Kuala_Lumpur">Kuala Lumpur</timezone>

<timezone id="Australia/Perth">Perth</timezone>

<timezone id="Asia/Taipei">Taipei</timezone>

<timezone id="Asia/Seoul">Seoul</timezone>

<timezone id="Asia/Tokyo">Tokyo, Osaka</timezone>

<timezone id="Asia/Yakutsk">Yakutsk</timezone>

<timezone id="Australia/Adelaide">Adelaide</timezone>

<timezone id="Australia/Darwin">Darwin</timezone>

<timezone id="Australia/Brisbane">Brisbane</timezone>

<timezone id="Australia/Hobart">Hobart</timezone>

<timezone id="Australia/Sydney">Sydney, Canberra</timezone>

<timezone id="Asia/Vladivostok">Vladivostok</timezone>

<timezone id="Pacific/Guam">Guam</timezone>

<timezone id="Asia/Magadan">Magadan</timezone>

<timezone id="Pacific/Auckland">Auckland</timezone>

<timezone id="Pacific/Fiji">Fiji</timezone>

<timezone id="Pacific/Tongatapu">Tonga</timezone>

</timezones>
```

(*6) locale - de_DE|en_US|es_ES|es_US|fr_CA|fr_FR|it_IT|nl_NL|pt_BR|pt_PT

CommentDisplayedSetting

German (Germany)Deutschde_DE

English (US)Englishen_US

Spanish (Spain)Español (España)es_ES

Spanish/USEspañol (Estados Unidos)es_US

French (Canada)Français (Canada)fr_CA

French (France)Français (France)fr_FR

Italian (Italy)Italianoit_IT

NetherlandsNederlandsnl_NL

Portuguese (Brazil)Portugues (Brazil)pt_BR

Portuguese (Portugal)Portugues (Portugal)pt_PT

Svenska (Swedish)sv_SE

Browser Bookmarks

There may be multiple browser_bookmarks tags in an XML cfg file each with multiple bookmark entries. Each entry MUST contain both the Name and Url attributes as a pair to be considered a valid bookmark otherwise the entry is ignored and a warning log is raised.

```
<browser_bookmarks>
```

```
<bookmark Name=<Any String> " Url=<Any String> />
```

```
</browser_bookmarks>
```

Only bookmarks which have a difference in the combined name/title and url are added to the browser's bookmarks i.e. duplicates that are already configured on the phone are ignored. Consequently the XML cfg files can be used to add to or change bookmarks on a phone but not to erase them.

Administrator Password

Note that the administrator password is not stored in the XML cfg files as plain text. It is a decimal representation of the SHA-256 hash of the password. This is not easy to generate manually, there are online tools that could be used to do this or simply use a Conference/Video Phone and export its XML cfg using the procedure outline previously.

```
<admin_passwd>
```

```
45550759484573394543112345748812748452036940046205246282360354971636510013881
```

```
</admin_passwd>
```


Appendix E

Mass Deployment Configuration File

Reference

Mass Deployment Configuration File Reference

MiVoice Conference/Video Phone Software, Release 2.1, SP5

NOTES:

Quotes " are literal.

[are to be replaced with the content]

[also have keys and values with alternating patterns separated with |

System Settings

SIP Settings

Account	Server Address	<user list><ProxySvr="[IP]" ProxyPort="[PORT]"></User></user list>	Username and Login Name must be the same
	Username	<user list><User ID="[USER NAME]"></User></user list>	
	Display Name	<user list><User DispName="[DISPLAY NAME]"></User></user list>	
Authentication	Login Name	<user list><User Authname="[LOGIN NAME]"></User></user list>	Proxyscheme is a comma separate list e.g. "1,2,3" Example shows only UDP enabled Example shows only TCP enabled Example shows only TLS enabled
	Login Password	<user list><User Pwd="[PASSWORD]"></User></user list>	
Transport	UDP	<user list><User ProxyScheme="1"></User></user list>	
	TCP	<user list><User ProxyScheme="2"></User></user list>	
	TLS	<user list><User ProxyScheme="3"></User></user list>	
Media	Audio Codec List	<audio_codec_list>g711u,g711a,g722,g722.1</audio_codec_list>	Ordered list of g722,g722.1,g711u,g711a, g729a ordered list e.g. h264highprofile,h264baseprofile Time in milliseconds 10 20 30 40 50 60 70 80 90 100
	Video Codec List	<video_codec_list>h264highprofile,h264baseprofile</video_codec_list>	
	Packet Time	<audio_packet_size>[PACKET TIME]</audio_packet_size>	
	DTMF Mode	<dtmf_type>[0:automatic 2:outband only 3:inband only]</dtmf_type>	
Firewall Traversal	SRTP	<srtpp>0 1 2</srtpp>	
	Session maxprate	<session_maxprate_enable>[0:disable 1:enable]</session_maxprate_enable>	
	ICE	<ice_enable>[0:disabled 1:enabled]</ice_enable>	
	STUN Server Address	<stunip>"[STUN SERVER URL - can include port]" </stunipp>	

MiVoice Conference/Video Phone Administration Guide

SIP Settings (cont'd)

Misc	Registration Timeout	<register_expire>[REGISTRATION TIMEOUT]</register_expire>	Timeout in seconds, minimum allowed is 30 0 is disabled, nonzero is enabled
	Keepalive Interval	<keepalive_interval>[KEEPALIVE INTERVAL SECONDS]</keepalive_interval>	
	SPAM Call Filter	<spam_call_filter_enable>[0:disabled 1:enabled]</spam_call_filter_enable>	
	Proxy Server Address	<user list><User OutSvr="[IP FQDN]" OutPort="[PORT]"></User></user list>	
	Proxy Server Address for Dial URI (Outbound proxy)	<user list><User DialURIOutboundProxySvr="[IP FQDN]" DialURIOutboundProxyPort="[PORT]"></User></user list>	

Security

	TLS Server Validation	<tls_server_validation>[0:disabled 1:enabled]</tls_server_validation>	
	Install Certificates from External Storage	<certificates>{list of trusted CA root certificates in PEM format}</certificates>	

Apps Settings

	<apps app_name=[0:disabled 1:enabled]> </apps>	app_name is one of RemoteRdp OfficeWrks Browser RemoteVNC Webex MitelMCA Specify one or more apps that are to be enabled or disabled. Note: MitelMCA is the MiCollab Conference App
--	---	---

Network Settings

Modify Static	Phone IP	<ipadr>[PHONE IP]</ipadr>	
	Gateway IP	<ipgateway>[GATEWAY IP]</ipgateway>	
	Subnet Mask	<ipmask>[SUBNET MASK]</ipmask>	
	VLAN Id	<vlanid>[VLAN ID]</vlanid>	
	L2 Priority Voice	<layer2_priority Voice="[L2 PRIORITY VOICE]"</layer2_priority>	
	L2 Priority Signal	<layer2_priority Signalling="[L2 PRIORITY SIGNALLING]"</layer2_priority>	
	L2 Priority Multimedia	<layer2_priority Multimedia="[L2 PRIORITY MULTIMEDIA]"</layer2_priority>	
	DSCP Voice	<dscp Voice="[DSCP VOICE]"</dscp>	
	DSCP Signalling (inconsistent with L2 Priority)	<dscp Signalling="[DSCP SIGNALLING]"</dscp>	
	DSCP Multimedia	<dscp Multimedia="[DSCP MULTIMEDIA]"</dscp>	
	DNS Server 1	<ipdns>[DNS SERVER 1]</ipdns>	
	IPA Server	<ipipa>[IPA SERVER]</ipipa>	
802.1X EAP TLS	EAPType and SCEPProxy	<protocol_802_1x Username = "" Pwd = "" EAPType = "MD5" or "TLS" SCEPProxy = "" />	password (Pwd) is only required for EAPType="MD5" and SCEPProxy URL string is only required for EAPType="TLS".
802.1X Protocol	Username	<protocol_802_1x Username="[802.1X USERNAME]"></eight_zero_two_dot_one_x>	
	Password	<protocol_802_1x Pwd="[802.1X PASSWORD]"></eight_zero_two_dot_one_x>	
802.1X EAP TLS	Username	<protocol_802_1x Username="[802.1X USERNAME]"></eight_zero_two_dot_one_x>	
	Password	<protocol_802_1x Pwd="[802.1X PASSWORD]"></eight_zero_two_dot_one_x>	
Tools and Features	DHCP	<dhcpenable>[0:disabled 1:enabled]</dhcpenable>	
	CDP	<cdpenable>[0:disabled 1:enabled]</cdpenable>	
	LLDP	<lldpenable>[0:disabled 1:enabled]</lldpenable>	
	802.1x	<protocol_802_1x_enable>[0:disabled 1:enabled]</protocol_802_1x_enable>	
	Enable Firewall Filter	<firewallenable>[0:disabled 1:enabled]</firewallenable>	
	Enabled VLAN	<vlanenable>[0:disabled 1:enabled]</vlanenable>	

Contacts Settings			
Populate from CSV file		<contacts_use_csv>>[0:disabled 1:enabled]<</contacts_use_csv>	
LDAP Server Settings	Directory Server IP Address or Host Name [:port]	<ldap Svr="[DIRECTORY SERVER IP ADDRESS OR HOST NAME][:PORT]"></ldap>	LDAP, Active Directory, or MBG Server Address
	LDAP Search Base	<ldap SearchBase="[LDAP Search Base]"></ldap>	
	LDAP Search Directory	<ldap SearchDirectory="[LDAP Search Directory]"></ldap>	
	Communication Security Type	<ldap SecurityType="[0 1 2]"></ldap>	
	LDAP Search Filter	<ldap SearchFilter="[LDAP Search Filter]"></ldap>	
	User Login	<ldap AuthName="[USER LOGIN]"></ldap>	
	User Password	<ldap Pwd="[USER PASSWORD]"></ldap>	
	Use Pictures	<ldap Pictures="[0:disabled 1:enabled]"></ldap>	
	Auto Search Base	<ldap AutoSearchBase="[0:disabled 1:enabled]"></ldap>	
	Enable MBG Connection	<ldap ConnectMBG="[0:disabled 1:enabled]"></ldap>	
Translation Plan	Rule 1	<contacts_translation Rule="[RULE 1 TEXT]" Prefix="[RULE 1 PREFIX]">Rule 1</rule>	SecurityType 0 = None (port 389) 1=SSL (port 636) 2=StartTLS (port 389) For MBG Security Type, use ConnectMBG=1 attribute which overrides this security type. When ConnectMBG = 0 attribute SecurityType specifies the communication security type. When ConnectMBG = 1, the communication security type is MBG (port 35010). ; supported X supported 0123456789*# supported [] no t supported First 5 rules are supported. Old tag ldap_translation also supported.
	Rule 2	<contacts_translation Rule="[RULE 2 TEXT]" Prefix="[RULE 2 PREFIX]">Rule 2</rule>	
	Rule 3	<contacts_translation Rule="[RULE 3 TEXT]" Prefix="[RULE 3 PREFIX]">Rule 3</rule>	
	Rule 4	<contacts_translation Rule="[RULE 4 TEXT]" Prefix="[RULE 4 PREFIX]">Rule 4</rule>	
	Rule 5	<contacts_translation Rule="[RULE 5 TEXT]" Prefix="[RULE 5 PREFIX]">Rule 5</rule>	

Schedule Updates	Day of Week	<ldap UpdateDayOfWeek="[1:Sunday 2:Monday 3:Tuesday 4:Wednesday 5:Thursday 6:Friday 7:Saturday]"></ldap>	0:None
	Time	<ldap UpdateTime="[UPDATE TIME IN 24 HR FORMAT]"></ldap>	
	Occurrence	<ldap UpdateFrequency="[0:off 1:weekly]"></ldap>	
Dial Plan Settings			
	Rule 1	<dialpl DigitDial="[RULE 1 TEXT]">Rule 1</dialpl>	; supported X supported 0123456789*# supported [] not supported First 5 rules are supported.
	Rule 2	<dialpl DigitDial="[RULE 2 TEXT]">Rule 2</dialpl>	
	Rule 3	<dialpl DigitDial="[RULE 3 TEXT]">Rule 3</dialpl>	
	Rule 4	<dialpl DigitDial="[RULE 4 TEXT]">Rule 4</dialpl>	
	Rule 5	<dialpl DigitDial="[RULE 5 TEXT]">Rule 5</dialpl>	
Video Settings			
	Video Quality Downlink and Video Quality Uplink	<video_quality Link="[MIN MID MAX]" Uplink="[MIN MID MAX]"></video_quality>	MAX BITRATE 1536kbps / MID BITRATE 1024 kbps/ MIN BITRATE 512kbps
	Dynamic Bandwidth Adaption & Cable/DSL	<video_quality CableDSL="[0:disable 1:enable]" DynamicAdaptation="[0:disabled 1:enabled]"></video_quality>	
RDP Settings			
	Hostname / IP of Remote Computer	<rdp Endpoint=[IP FQDN of REMOTE COMPUTER]></rdp_endpoint>	
	Username and Domain for the RDP Preset Remote Computer	<rdp Endpoint="" Username="" Domain="" />	
VNC Settings			
	Hostname / IP of Remote Computer	<vnc Endpoint=[IP/FQDN of REMOTE COMPUTER]> AppleMac=[0:disabled 1:enabled]</vnc_endpoint>	
History Settings			
	Enable Clear History Prompt	<clear_history_prompt>[0:disable 1:enable]</clear_history_prompt>	
Extension Microphone Settings			

MiVoice Conference/Video Phone Administration Guide

Set extension microphone mode	<extension_microphone>[...]</extension_microphone>	0:Not Installed NA:NA Microphone Installed EU:EU Microphone Installed
-------------------------------	--	---

Advanced Settings Password

Password	<admin_passwd>[ADVANCED SETTINGS PASSWORD]</admin_passwd>	Refer to note about SHA-256 hash - with recommendation to not change password through xml
----------	---	---

Camera Settings

Enabled	<camera Enable="[0:disabled 1:enabled]"></camera>	
IP Address/Host Name	<camera Address="[IP ADDRESS/Host Name]"></camera>	
Port	<camera Port="[PORT]"></camera>	
Username	<camera AuthName="[USERNAME]"></camera>	
Password	<camera Pwd="[PASSWORD]"></camera>	

Country Variant

Tone Plan Selection	<tonecode>[COUNTRY CODE]</tonecode>	AU (Australia) FR (France) DE (Germany) IT (Italy) Latin America <=> MX (Mexico) NL (Netherlands) US <= North America, CA or US => North America NZ (New Zealand) PT (Portugal) ES (Spain) GB (United Kingdom)
---------------------	-------------------------------------	---

Dialpad Settings

Display Dialpad Automatically Idle Time Before Dsplaying Dialpad	<dialpad_settings Enable="[0:disabled 1:enabled]"></dialpad_settings> <dialpad_settings HomeScreenIdleTime="5-120"></dialpad_settings>	
--	---	--

Licensing Backup Import/Export

HTTP Server Address	<http_cfg ServerUrl="[HTTP SERVER URL – can include port & path]"	Statically configured address overrides any value from DHCP
Trust All HTTP Servers	<http_cfg TrustAllHosts="[0:disable 1:enable]"></http_cfg>	

Upgrade System SW

HTTP Server Address	<http_download>[HTTP SERVER IP PORTION]</http_download> <http_port>[HTTP SERVER PORT NUMBER]</http_port>	httpport not required. port number default is 80. A value will only be provided if explicitly set in the port part of the HTTP URL. Conversely having no port set here means the default port (80) is used.
Trust All HTTP Servers	<https_swupgrade_trust_all_hosts>[0:disable 1:enable]</https_swupgrade_trust_all_hosts>	N.B. Conference/Video Phone, will check on reboot as well. upgrade auto will not prompt user
Auto Upgrade	<http_upgrade>[0:disable 1:upgrade on 2:upgrade auto]></http_upgrade>	
Auto Polling	<firmware_abs_enable>[0:disable 1:enable]</firmware_abs_enable>	
User Confirmation	<http_upgrade_user_confirm>[0:disable 1:upgrade on]></http_upgrade>	
Upgrade Time	<firmware_abs_timer_hr>[24 HOUR FORMAT HOUR]</firmware_abs_timer_hr> <firmware_abs_timer_min>[MINUTE]</firmware_abs_timer_min>	

Debug Settings

Debugging (Debug Logging)	<debug LogDebugging="[0:disable 1:enable]"></debug>	Verbose(2), debug(3), info(4), warn(5), error(6)
Debugging Level	<debug LogLevel="[Verbose Debug Information Warning Error]"></debug>	
Kernel Messages	<debug LogKernelMessages="[0:disable 1:enable]"></debug>	
Debug Logs Size	<debug LogSize="[SIZE IN MB]"></debug>	
Automatic Ethernet Trace (Congestion)	<debug AutoEthernetTrace="[0:disable 1:enable]"></debug>	
Manual Ethernet Trace (User Button Enable)	<debug UserEthernetTrace="[0:disable 1:enable]"></debug>	
Development		
eXoSIP Log Level	<debug SipLogLevel="[0:Disabled 1 2 3 4 5 6 7:verbose]"></debug>	
Debug DSP	<debug DspDebug="[0:disable 1:enable]"></debug>	
Disable DSP auto reboot	<debug DisableDspCriticalReboot="[0:off/reboot enabled 1:on/reboot disabled]"></debug>	

MiVoice Conference/Video Phone Administration Guide

Legacy Interop Mode Always mirror primary to HDMI	<debug LegacyInteropMode="[0:disable 1:enable]"></debug> <debug MirrorDisplay="[0:disable 1:enable]"></debug>	
--	--	--

Web Server Settings

Web Server Enable	<web_server Enable="[0:Disabled 1:Enabled]"></web_server>	Remote diagnostics web server
-------------------	---	-------------------------------

Sound

Audible selection (Play sound when making screen selection)	<audible_key_press_feedback>"[0:disable 1:enable]"</audible_key_press_feedback>	
---	---	--

Display

Brightness	<screen_brightness>[LCD BRIGHTNESS]</screen_brightness>	Range 30-255
Screen Timeout	<screen_timeout>[...]</screen_timeout>	15 30 60 120 600 1800

Language & Keyboard

Select Language	<lancode>[LANGUGAGE CODE]</lancode>	Deutsch – de_DE English – en_US Espanol (Espana) – es_ES Espanol (Estados Unidos) – es_US French (Canada) – fr_CA French (France) – fr_FR Italiano – it_IT Nederlands – nl_NL Portugues (Brazil) – pt_BR Portugues (Portugal) – pt_PT
-----------------	-------------------------------------	--

Keyboard Settings

Show settings key	<keyboard SettingsKeyControl="[0:hidden 1:shown 2:automatic]"></keyboard>	
Input Languages (Alternate keyboards sliding on spacebar)	<keyboard InputLanguages="[COMMA SEPARATED LIST OF VALID COUNTRY CODES FROM LANCODE]"></keyboard>	
Android Keyboard	<keyboard PopupOnTouch="[0:disable 1:enable]"></keyboard>	
Touch to correct words	<keyboard TouchForCorrections="[0:disable 1:enable]"></keyboard>	

Data & Time

Select Time Zone	<time_zone_name>[NAME OF TIMEZONE FROM ANDROID LIST]></time_zone>	0:24 hour format 1:12 hour AM/PM format {empty} mm/dd/yyyy dd/mm/yyyy yyyy/mm/dd
Use 24-hour format	<time_format>[...]></time_format>	
Select Date Format	<date_format>[...]</date>	
Use NTP time when available	<sntp_enable>[0:disable 1:enable]</sntp_enable>	
Set NTP Server Address	<ntp_server1></ntp_server1>	

Browser User Settings

Set Search Engine	<browser_settings SearchEngine="[google yahoo bing]"></browser_settings>	Configured in Browser app
Show Security Warnings	<browser_settings ShowSecurityWarnings="[0:disable 1:enable]"></browser_settings>	
Remember Passwords	<browser_settings RememberPasswords="[0:disable 1:enable]"></browser_settings>	
Remember Form Data	<browser_settings RememberFormData="[0:disable 1:enable]"></browser_settings>	
Accept Cookies	<browser_settings AcceptCookies="[0:disable 1:enable]"></browser_settings>	
Set Home Page	<browser_settings Homepage="[URL]"></browser_settings>	Latin-1:ISO-8859-1 UTF-8:Unicode GBK:Chinese Big5:Chinese SO-2022-JP:Japanese SHIFT-JIS:Japanese EUC-JP:Japanese
Block Pop-Up Windows	<browser_settings BlockPopupWindows="[0:disable 1:enable]"></browser_settings>	
Text Encoding	<browser_settings TextEncoding="[...]"></browser_settings>	
Open Pages in Overview	<browser_settings OpenPagesInOverview="[0:disable 1:enable]"></browser_settings>	
Default Zoom	<browser_settings DefaultZoom="[FAR MEDIUM CLOSE]"></browser_settings>	
Text Size	<browser_settings TextSize="[SMALLEST SMALLER NORMAL LARGER LARGEST]"></browser_settings>	
Stored Bookmarks	<browser_bookmarks><bookmark Name="name" Url="[BOOKMARK URL]"></bookmark></browser_bookmarks>	

Mitel MCA app

	<mca_settings ServerIndex="[Index of active server, starting at 0]" ServerList="[ServerEntry0;ServerEntry1;ServerEntry2;]"></mca_settings>	Configured in MCA app e.g. ServerIndex="1" indicates active server is ServerEntry1
--	--	---

