Mitel 1023 SIP Terminals for MiVoice MX-ONE

INSTALLATION INSTRUCTIONS

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 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.

1 GENERAL

This document is valid for Mitel 1023 i when installing this phone model in a MX-ONE environment.

Figure 1: Mitel 1023

The product number is DBC 41023/110.

1.1 SCOPE

This document describes how to install and configure the Mitel 1023 terminals in a MX-ONE Service Node (SN) environment.

1.2 GLOSSARY

Some expressions:

Table 1 Expressions

Expression	Description
IPP	IP Phone SW Server Configuration Management Application for Windows.
LAN port	Port to be connected to a PC. In the other Mitel IP phones this port is called the PC port
WAN port	Port to be connected to the local network. In the other Mitel IP phones this port is called the LAN port

2 DELIVERY METHOD

The phones are delivered in a box with a handset, handset cord and a quick installation guide.

The configuration file must be adapted for each site and has to be loaded into the phone.

3 CABLING

The cables shall be connected to the inlets according to the figure.

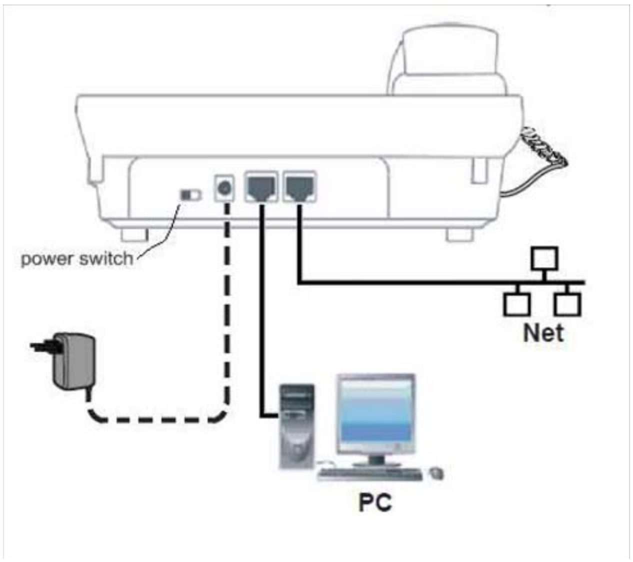


Figure 2: Cabling for Mitel 1023

The outlet marked **WAN** shall be connected to the local network. If a PC shall be used, it shall be connected to the outlet marked **LAN**.

4 POWER EQUIPMENT

Mitel 1023 is powered from power over Ethernet (PoE) according to IEEE 802.3af or from an AC/DC adapter 5V.

Table 2 Power classes for the different phone models

Device	Power Consumption	Power Class
1023	1.5 W in idle 1.8 W in active call	1

Explanation of power classes:

- 0 - classification is not implemented.
- 1 - less than 3.84 W
- 2 - less than 6.49 W

Table 3 AC/DC adapters

Product Number	Description
87L00038AAA-A00	EU.This product consists of a kit with 10 adapters.
87L00038BAA-A00	US. This product consists of a kit with 10 adapters.

5 SETTING UP THE SOFTWARE SERVER

The software and configuration files used by the phone is stored on a software server and downloaded to the phone during power up. Setting up the software server comprises the following steps:

- Installing the software server.
- Creating a directory structure on the server.

When the software server is installed and the directory structure created, the phone software can be stored on the server. For information on how to store phone software on the server, see 8.1 Installing New Phone Software on the Software Server on page 12.

5.1 INSTALLING THE SOFTWARE SERVER

The recommendation is to use an http server. Installation of the software server is done according to the documentation of the HTTP server. Both PC and Unix versions are supported. Below follows some remarks about different servers:

- When using Windows® Server, the **.z** and **.cfg** file types must be enabled. Follow the steps below to enable these file types:

  In **IIS Manager**, select **DefaultWEB Site**. Then select **Properties** and edit **HTTP header**. Apply the following settings:

  – **Associated extension: .cfg** and **.z**

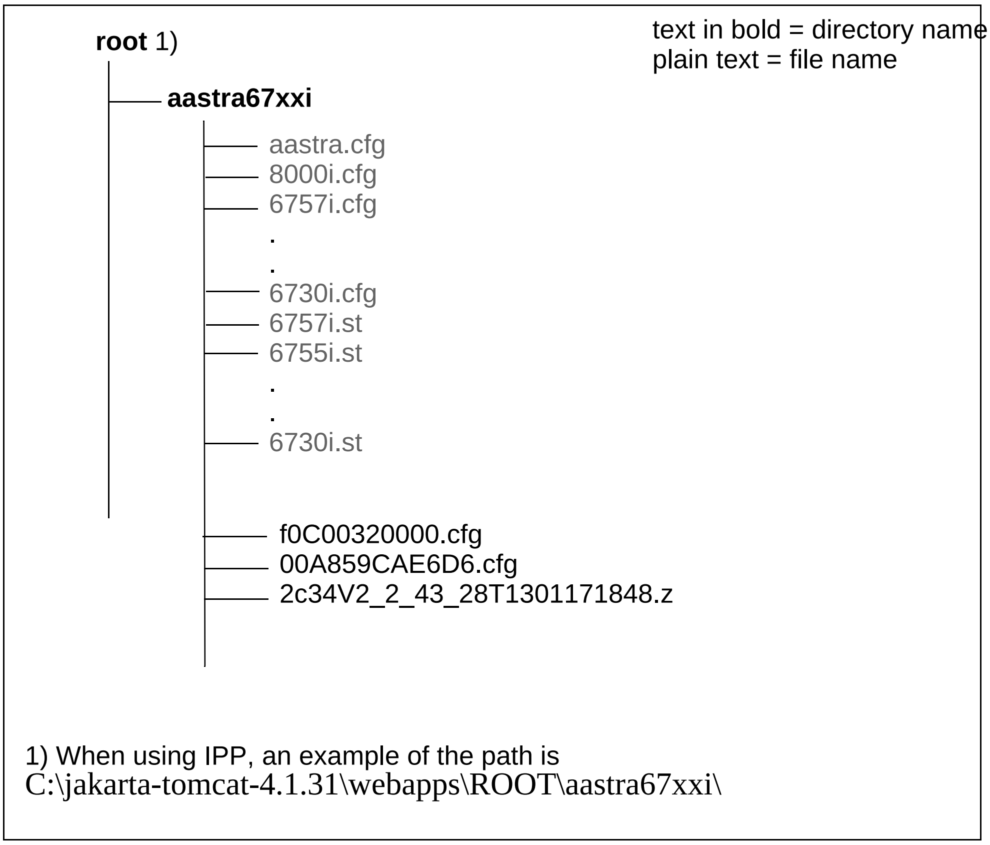
  – **Content type (MIME): application/octet-stream**.
- Apache on Microsoft® Windows® or Redhat® Linux 5.2.
- IP Phone SW Server Configuration Management Application for Windows (CXC 109 0055/1) also called IPP. This application is using a Tomcat http server. IPP is mandatory when using the IP Phone Configuration File in MX-ONE Service Node Manager for creating the configuration files for Mitel 6900, 6800, 6700, 7400 or MiVoice 442x. This Tomcat server can also be used to host the software files for Mitel 1023 phones.

Note: When storing the files on the software server, make sure that the files are transferred in binary mode, otherwise the file can be modified by the transfer tool and the size be changed. In this case the telephone will not load the file.

5.2 CREATING A DIRECTORY STRUCTURE

When the customer shall have mixed terminal models with Mitel 1023 and Mitel 6900/6800/6700, the recommendation is to store the firmware and configuration file(s) for Mitel 1023 under the same directory as the Mitel 6x00 terminals.

The reason is that the same set up of the DHCP option defining the URL to the software server can be used.



1) When using IPP, an example of the path is
C:\jakarta-tomcat-4.1.31\webapps\ROOT\aastra67xxi\

Figure 3: Directory structure

6 MANAGE THE CONFIGURATION FILES IN MX-ONE SERVICE NODE MANAGER

There is no support yet in **MX-ONE Service Node Manager** (SNM) for creating the configuration file for Mitel 1023.

7 HOW TO START A NEW PHONE

The phone is delivered with default settings for an IP network. These settings must be adapted to the local network.

Most settings in the phone can be controlled by the configuration file, available on the software server. When the phone is powered up, the configuration file is downloaded to the phone from the software server.

7.1 CONNECTING THE PHONE TO A NETWORK USING DHCP

When the phone is delivered from the factory, DHCP is enabled.

To be able to connect the phone to a network, the following parameters must be configured:

- **Verify that DHCP is enabled.** Press 🔧 > **Network** > **WAN** > **Net Mode** and check that DHCP is enabled.
- **The phone's IP address**, **subnet mask**, and **default gateway**. When using DHCP, these parameters are configured automatically.
- **The IP address of the software server**. This address is configured automatically using DHCP, or manually from the phone. If DHCP is used for providing this parameter, the DHCP server must be configured before the phones can connect to the network. For information on how to configure the DHCP server for providing the phone with the IP address to the software server, see 15.1 Data from DHCP on page 31.
- **The IP address of the sip server**. This address is configured using the configuration file or manually from the phone, see section 11.8 Setting the IP Address of the SIP Proxy / Registrar on page 19.

Edit the configuration file, store it on the software server and connect the phones to the network. Start the telephone.

Press the scroll down navigation key ▼ and verify that the display shows DHCP, IP address for the phone and the IP address for the default gateway.

Next step is to register the phone, see section 7.3 Register the Phone to the SIP Server on page 11.

7.2 CONNECTING THE PHONE USING STATIC IP ADDRESS

When connecting the phone to a network not using DHCP, network parameters in the phone are configured manually after the phone is started:

- **Change to static IP settings.** Press 🔧 > **Network** > **WAN** > **Net Mode** and select **Static IP**.
- **Set the static IP settings.** Press 🔧 > **Network** > **WAN** > **Static IP Settings**. Enter the phone's IP address, subnet mask, default gateway and IP address to the DNS server.
- **The IP address of the software server**. If DHCP is not used, this IP address must be manually entered into each phone, see section 11.7 Setting the IP Address of the Software Server on page 19.

- **The IP address of the sip server**. This address is configured using the configuration file or manually from the phone, see section 11.8 Setting the IP Address of the SIP Proxy / Registrar on page 19.

Press the scroll down navigation key ▼ and verify the IP address for the phone and the IP address for the default gateway.

Next step is to register the phone, see section 7.3 Register the Phone to the SIP Server on page 11.

7.3 REGISTER THE PHONE TO THE SIP SERVER

The IP address of the SIP server must have been defined in the phone before the procedure below can be used.

The directory number and PIN code (if applicable) must be entered into the phone. This can be done by the end-user or by the system administrator:

1. Press the 🔧 key. Scroll down to **User Logon** and press **Enter**.
2. Enter the Phone Number.
3. Scroll down one step and enter the PIN code (if applicable). Press **More** and then press **Logon**.
4. If the registration is successful, the extension number is shown on the top line in the idle menu.
5. Make a phone call to check that the registration is ok.

One alternative is to set the directory number and PIN code via the web interface.

8 MANAGING IP PHONE SW

8.1 INSTALLING NEW PHONE SOFTWARE ON THE SOFTWARE SERVER

By updating the phone software files on the software server, the phones are updated when restarted. The following files need to be stored on the software server:

2c34V2_2_43_14T20120928181435.z

The application firmware for the phones. This file includes English, Chinese and Portuguese. The file name consists of:
2c34 = product id for the Aastra application
V2_2 = Version 2.2
43_14 = build number
20120928181435 = time stamp
z = file extension

2c34V2_2_43_14T20120928181435_ES_FR_EN.z

The application firmware for the phones but with other languages than the default languages. In this example English, French and Spanish.

f0C03200000.cfg

Common configuration file. This file contains the configuration parameters for all 1023 phones in the system. The configuration file has to be adapted for each installation.
The template file is stored in MX-ONE under **/etc/opt/eri_sn/aastraSIPphones/**.

<mac>.cfg

MAC-oriented configuration file. This file contains configuration parameters for a certain phone.

The template is stored in MX-ONE under
/etc/opt/eri_sn/aastraSIPphones/

8.2 INSTALLING THE FIRMWARE / CONFIGURATION FILES

When the phone starts or reboots, the phone fetches the configuration file from the software server.

If the firmware shall be updated, see section 8.4 Firmware upgrade on page 13.

If the system administrator wants that the phone shall read in the updated configuration files there are the following options to reboot the phone:

MX-ONE command

- extension_unregistration. The telephone restarts and registers again automatically.

Phone UI

- Press ⚙ , scroll down to **Reboot System** and select **Reboot**

Web UI

- Log in to the web interface. Click on **MAINTENANCE** > **REBOOT** > **Reboot**

8.3 FACTORY DEFAULT

If all the settings via the configuration file or menus shall be erased, there are 2 alternative:

Alternative 1. - Phone UI

Do as follows:

Press SETUP, scroll down to System Config and switch input mode from 2aB->123, and type the password (default is 22222).

Scroll down to Factory Reset.

Press Enter-> Reset -> Yes.

Alternative 2. - Post mode

1. When the phone is starting up, press the **# ke**y. **Post mode** is shown in the display.
2. Press the sequence ***#168**. A confirmation message is shown in the display.

8.4 FIRMWARE UPGRADE

In the configuration file there is a parameter (Auto Image Version) defining the version number.

If this version number is different compared to the one in the firmware in the phone memory, the new firmware will be loaded.

The version number in the Auto Image Version parameter shall match the version number in the file name of the application.

The following parameters must be in the configuration file if the telephones shall download firmware:

<AUTOUPDATE CONFIG MODULE>
Auto Image URL: http://192.168.0.1/Aastra/V2_2_43_14T20120928181435.z

Firmware upgrade can be done in one of the following ways:

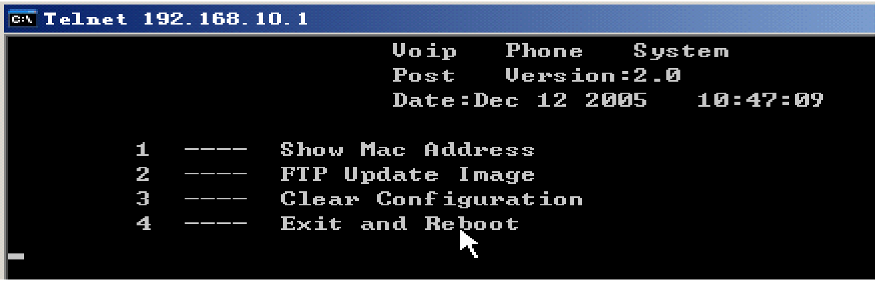
- Web UI: **MAINTENANCE** > **Update > Web Update**
- The phone will automatically look for firmware update and configuration files during the boot process.
- MX-ONE command: **extension_unregistration**.

Note: When the firmware is upgraded, the display shows **Downloading** and then **Updating**. If the power is disconnected while **Updating** is shown, the firmware in the flash memory will be corrupt.

8.4.1 REPAIR OF CORRUPT FIRMWARE

If the firmware in the flash memory is corrupt, follow the flow below to load it to the flash:

- Connect a PC to the LAN port of the phone.
- Disconnect and connect the power.
- Press # while the phone is starting: Post Mode is shown in the LCD display.
- Use Telnet with the address: 192.168.10.1
- The following is shown in the PC:

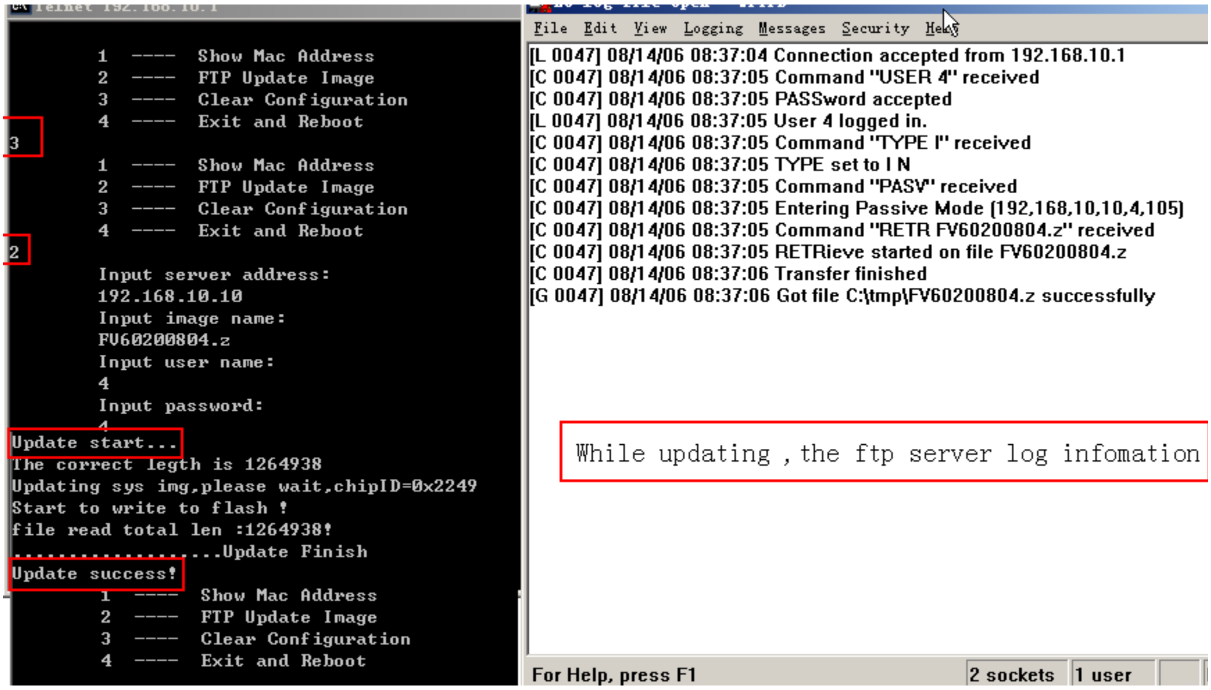


```
Telnet 192.168.10.1
                              Voip    Phone    System
                              Post    Version:2.0
                              Date:Dec 12 2005    10:47:09

          1  ----  Show Mac Address
          2  ----  FTP Update Image
          3  ----  Clear Configuration
          4  ----  Exit and Reboot
_
```

Figure 4: Config page

- Enter 3 to clear the configuration.
- Enter 2 to update the firmware by follow the procedure in the picture below:



```
        1  ----  Show Mac Address
        2  ----  FTP Update Image
        3  ----  Clear Configuration
        4  ----  Exit and Reboot
3
        1  ----  Show Mac Address
        2  ----  FTP Update Image
        3  ----  Clear Configuration
        4  ----  Exit and Reboot
2
        Input server address:
        192.168.10.10
        Input image name:
        FU60200804.z
        Input user name:
        4
        Input password:
        4
Update start...
The correct legth is 1264938
Updating sys img,please wait,chipID=0x2249
Start to write to flash !
file read total len :1264938!
...................Update Finish
Update success!
        1  ----  Show Mac Address
        2  ----  FTP Update Image
        3  ----  Clear Configuration
        4  ----  Exit and Reboot
```

```
[L 0047] 08/14/06 08:37:04 Connection accepted from 192.168.10.1
[C 0047] 08/14/06 08:37:05 Command "USER 4" received
[C 0047] 08/14/06 08:37:05 PASSword accepted
[L 0047] 08/14/06 08:37:05 User 4 logged in.
[C 0047] 08/14/06 08:37:05 Command "TYPE I" received
[C 0047] 08/14/06 08:37:05 TYPE set to I N
[C 0047] 08/14/06 08:37:05 Command "PASV" received
[C 0047] 08/14/06 08:37:05 Entering Passive Mode (192,168,10,10,4,105)
[C 0047] 08/14/06 08:37:05 Command "RETR FV60200804.z" received
[C 0047] 08/14/06 08:37:05 RETRieve started on file FV60200804.z
[C 0047] 08/14/06 08:37:06 Transfer finished
[G 0047] 08/14/06 08:37:06 Got file C:\tmp\FV60200804.z successfully
```

While updating , the ftp server log infomation

Figure 5: Download the new firmware

8.5 VIEWING SOFTWARE VERSION

It is possible to display the versions of the software units.

Phone UI

- Select 🔧 > **System Info** > **Firmware**

Web UI

- Log in to the web interface. The software version is shown at the bottom of the first page (BASIC)**.**

MX-ONE

- MX-ONE command: **extension_info -d all --terminal-info**

9 RESTART / RESTORE

There are the following options:

- Restart the phone.
- Restore to factory default. The phone gets the same data as when leaving the factory and removes any saved directory files.

9.1 RESTART

Phone UI

- Press 🔧 , scroll down to **Reboot System** and press **Enter**.
- Select **Reboot**.

Web UI

- Log in to the web interface. Click on **MAINTENANCE** > **REBOOT** > **Reboot**

From MX-ONE

- **extension_unregistration**. The telephone restarts and registers again automatically

9.2 RESTORE TO FACTORY DEFAULT

Phone UI

- Press 🔧 > **System Config** and enter the administrator password. Scroll down to **Factory Reset** and select **Reset.**

10 ENTERING ADMINISTRATOR MODE

Phone UI

- Press (menu) key
- Scroll down and select **System Config**
- Enter the administrator password: 22222 (which is the default password but can be changed)

Web UI

There is only an administrators mode, not any end-user mode.

- Find the IP address of the telephone by pressing the down navigation key.
- Enter the IP address to the telephone into the address field in the web browser in the PC and press enter.
- Log in to the web interface by enter
  User name: **admin**
  Password: **22222** (which is the default password)

11 CONFIGURING THE PHONE

This chapter describes how to configure the phone from the phone menus as an administrator.

This chapter also covers the configuration via the configuration files.

The parameters can be set in any of the configuration files, but in this section it is the recommended placing that is described. If one parameter occurs in several configuration files, it is always the last read parameter value that the telephone uses.

11.1 SETTINGS MODE

To enter into settings mode in the phone user interface:

- Press (menu key)

To enter the web user interface:

- Find the IP address of the telephone by pressing the down navigation key.
- Enter the IP address to the telephone into the address field in the web browser in the PC and press enter.
- Log in to the web interface by enter
  User name: **admin**
  Password: **22222** (which is the default password)

11.2 SETTINGS IN THE CONFIGURATION FILES

The template configuration file shall be used and it shall be adapted with the necessary adaptation for the site.

The template file file can be fetched from:

/etc/opt/eri_sn/aastraSIPphones/

11.3 AUTOMATIC LAN ACCESS CONTROL

The IEEE802.1x standard is used for port access control authentication. The LAN switch must support IEEE802.1x signaling and there must be a RADIUS server handling the authentication, according to EAP-MD5. If the authentication is successful, the phone gets access to the LAN and continues with the ordinary start sequence.

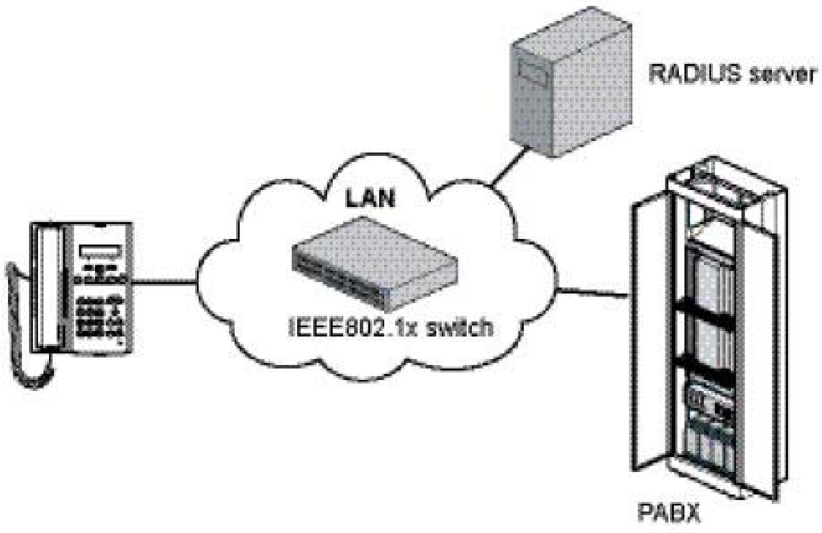


Figure 6: Components in LAN access control

Before the authentication the phone cannot get access to the LAN or even get the IP address from the DHCP server. The authentication is performed periodically (intervals as defined by the LAN switch). If the LAN switch does not support IEEE802.1x, the phone will start in the ordinary way.

When a PC is connected to the PC port in the phone, at present the 1023 phone does not support the PC port authentication.

The following parameters are used for the LAN access control:

Xsup User:
Xsup Password:
Xsup DevUnit: 1 # 0=Disable the function, 1=Enable the function

To set the data via the web UI:

Network > **WAN** > **802.1x Settings**

11.4 LLDP-MED

The telephones have support for Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED).

When LLDP is enabled, VLAN settings via LLDP has priority over other ways to set VLAN data.

The telephone sends also information in the outgoing LLDP packets for inventory management, allowing network administrators to track their network devices, and determine their characteristics such as:

- Telephone model (Mitel 1023), hardware revision, firmware revision, serial number.
- IP address, MAC address of the phone
- System name and system description = “Aastra IP Phone”
- Power consumption

When the phone is up and running and receives a changed LAN identity in the LLDP message, the telephone uses this new VLAN identity, but there is no automatic reboot to start a new DHCP negotiation.

The parameters for LLDP-MED in the configuration file are:

# The phone sends LLDP messages. 0=Disable LLDP, 1=Enable LLDP

LLDP Transmit :1

# The time interval between sending LLDP packets, 1-3600 sec

LLDP Refresh Time : 60

# The phone uses the received LLDP data

LLDP Learn Policy : 1

If LLDP is disabled in the configuration file in a running system and if LLDP shall be enabled, the configuration file with the changed LLDP parameter must be read in from the existing VLAN configuration before the telephone can get the new VLAN information via LLDP.

The LLDP data can be set via the web UI:

NETWORK > **QOS&VLAN** > **Link Layer Discovery Protocol LLDP Settings**

11.5 ENABLING / DISABLING DHCP

Follow the steps below to enable or disable DHCP:

Press 🔧 > **Network** > **WAN** > **Net Mode** and select **DHCP** or select **Static IP.**

11.6 SETTING THE PHONE'S IP ADDRESS

If DHCP is used, the phone's IP address is set automatically, using the DHCP server. To be able to set the phone's IP address manually, DHCP must first be disabled on the phone, see section 11.5 Enabling / Disabling DHCP on page 19

Press 🔧 > **Network** > **WAN** > **Static IP Settings**.

11.7 SETTING THE IP ADDRESS OF THE SOFTWARE SERVER

To download the phone software from the software server, the phone must be configured with the IP address to the software server. This IP address can be set using one of the following alternatives:

- Manually from the phone UI; 🔧 > **System Config** and enter the password > scroll down to **Auto Provision > Protocol HTTP** is recommended **> Mode** where **After Reboot** is recommended > **Server > File Name.**
- Automatically using DHCP, see 15.1 Data from DHCP on page 31.

11.8 SETTING THE IP ADDRESS OF THE SIP PROXY / REGISTRAR

The phone is configured with the IP address of the SIP proxy using one of the following methods:

1. In the common configuration file with the following parameters:
   SIP1 Register Addr :
   SIP1 Register Port : 5060
   SIP1 Enable Reg : 1
2. In the MAC-oriented configuration file **<mac>**.
3. Phone UI: 🔧 > **System Config** > **SIP Set** > Select line > **Basic SIP** > **Registrar Address.** Enter the IP address to the sip server and **Enable Register**. Press **Save**.
4. Web UI: Log in to the web interface. Click on **VOIP** > **SIP** > **Server Address** > **Apply**.

11.9 USING VIRTUAL LAN (VLAN)

The following VLAN data can be set:

- Enable VLAN tagging
- VLAN identity

The following configuration alternatives are available:

- LLDP, see section 11.4 LLDP-MED on page 18.
- Common configuration file with the parameters:
  #0=disable, 1= enable
  Enable VLAN : 1
  VLAN ID :
  #PC port, 1=disabled, 0=follow the LAN port, 2=enabled
  Enable PVID : n

  PVID value:
- Web UI: **Network** > **QOS&VLAN** > **WAN Port VLAN Settings** and **Network** > **QOS&VLAN** > **LAN Port VLAN Settings**
- Phone UI: **Network** > **QOS&VLAN** > **WAN LAN > VLAN** (on; off)

11.10 SETTING TIME AND DATE

Time and date are set via the SNTP protocol from a time server.

The time and data format is possible to change.

The following configuration alternatives are available:

- Common configuration file with the following parameters:
  SNTP Server :
  Second SNTP Server:
  Enable SNTP: 1
  #27 is Central European Time. For other values see web UI.
  Time Zone : 27
- Phone UI. 🔧 > **User Config** > **scroll down to Time&Date.** Enter the IP address to the SNTP server, the time format, time zone and daylight saving
- Web UI: Click on **NETWORK** > **Time & Date >** enter the IP address to the SNTP server, the time format, time zone and daylight saving date.

The recommendation is to use MX-ONE server 1 as the SNTP server. Second SNTP server can be any other reachable time server.

11.11 LANGUAGE SETTINGS

The language for the display texts can be changed via the configuration file, web interface or the key pad.

The application module contains three languages, the one included when the phone is delivered contains English, Chinese and Portuguese.

If another language is wanted, another application has to be loaded into the phone.

Change the language in the telephone:

- **Phone UI**. 🔧 > **User Config > Language Set** and switch to the wanted language.
- **Web UI**: Click on **Basic** > **Language**
- **Configuration file**:

  Default UI :m

  m = the number of the wanted default language.

  1= English
  2= Chinese
  3= German
  4= French
  6= Spanish
  7= Italian
  8= Portuguese

Some text strings are sent out from the PBX to the telephone. To order the PBX to send out the right language enter from the telephone:

***08*n#** where n is the language number in MX-ONE.

Although it is possible to select Chinese for the text strings locally in the phone, the text strings from the PBX cannot be in Chinese

11.12 USING SHORTCUT KEYS

There are no programmable keys in these phones.

11.13 SOFTKEYS

There are three softkeys below the display. These have different functions dependent on the traffic case.

When using the template configuration file, the softkeys adapted for a MX-ONE environment is shown.

The parameters for setting this in the configuration file are:

```
Desktop Softkey :history;
Talking Softkey    :new;hold;end;
Ringing Softkey    :accept;reject;
Alerting Softkey   :none;none;end;
```

XAlerting Softkey :xfer;none;end;
Waiting Softkey   :hold;conf;end;accept;

It is possible to change this for a certain phone via the Web UI:

FUNCTION KEY > **SOFTKEY**

Softkey mode:

- More: enable the settings option of softkeys.
- Disabled: default softkeys are shown.

Screen, the different traffic cases:

- Desktop, Ringing, Trying, Talking etc.

Select the wanted soft keys.

11.14 INITIATING DATA FROM MX-ONE PROVISIONING MANAGER

MX-ONE Provisioning Manager (PM) can be used to initiate data for this phone model. Select family = Mitel 1023. Other type. Note that this telephone model has no programmable function keys.

11.15 DIAL PLAN

To be able to use procedures (* n #), the possibility to send the number by pressing the hash key must be disabled. This is done via the configuration file with the parameter:

```
# 0=disable
Dial by pound: 0
```

It can also be done for one terminal via the web UI:

PHONE > **DIAL PLAN** disable **Press “#” to Send**.

11.16 AUTHENTICATION CODE SHALL NOT BE VISIBLE

When entering a service code procedure containing an authorization and PIN code, it is not possible to prevent the authorization or PIN code to be stored in the logs.

11.17 INQUIRY

A softkey must be set to have the possibility to initiate the second call, see also section 11.13 Softkeys on page 21.

Web UI:

PHONE > **SOFTKEY** > **Talking** > **New Call (New)** (to enable the Call soft key).

Configuration file:

Talking Softkey :new;hold;end;

Enable the Call softkey (called new as parameter value)

11.18 FREE ON SECOND LINE

If the phone shall be able to receive calls on another line although there already is a call on line 1, call waiting must be enabled. The soft keys for handling this traffic case must also be defined, see also section 11.13 Softkeys on page 21.

Web UI:

PHONE > **FEATURE** > **Enable Call Waiting**

PHONE > **SOFTKEY** > **Ringing** > **Answer** (to enable the Answer soft key).

Configuration file:

Ringing Softkey   :accept;reject;

Enable the Answer softkey (called accept as parameter value)

11.19 DIVERSION / CALL FORWARD

The recommendation is to use the call forwarding feature in the PBX, set by the service code procedure (for example *21*n#) from the phone, to get the advantage of all MX-ONE features.

To disable the *local* call forwarding function in the phone:

- Common configuration file with the parameter:
  # 0=disabled
  FWD Typ : 0
- **Phone UI:** 🔧 **> Call Service >** scroll down to **Call Forward >** select the line **>** set **Mode = OFF**
- **Web UI:** Click on **VOIP** > **Advanced SIP Settings** > set **Forward Type = Disabled**.

11.20 DO NOT DISTURB (DND)

It is possible to activate individual DND with the service code procedure (*27#) from the terminals. The recommendation is to use the DND function in the PBX to get advantage of all MX-ONE features. The extension must have a certain category to be allowed to activate individual DND. When the feature is activated the forwarding of calls to the extension is dependent on the settings in MX-ONE. No settings in the telephone is necessary for this feature. See also MiVoice MX-ONE Feature List.

To disable the *local* call forwarding function in the phone:

- Common configuration file with the parameter:
  P1 Enable DND : 0 # 0=disabled
- **Phone UI:** 🔧 **> Call Service >** scroll down to **DND >** set **DND= OFF**
- **Web UI:** Click on **Phone** > **Feature** > **Feature Settings > DND**

It is possible to activate group do not disturb from the telephone with a service code procedure. The extension must have a certain category to be allowed to activate group DND. No settings in the telephone is necessary for this feature. See also MiVoice MX-ONE Feature List.

11.21 CONFIGURING RING SIGNALS

The adaptation of the ring signals for internal / external calls and for call back is not possible.

It is possible to chose between a number of predefined ring signal types:

- **Phone UI:** 🔧 **> User Config > Ring Settings > Ringer Type**
- **Web UI:** Click on **Phone** > **Audio** > **Default Ring Type**

11.22 CONFIGURING PRESENCE SERVICES

The absence reason has to be set from the phone by using the service code procedure (for example *23*n#) from the phone.

When message diversion is active, a text message is shown in the display.

Note: It is necessary to set the time and date format in MX-ONE for the different absence reasons. Use command:

extension_text with parameter **ics-time-format**

See operational directions for Generic Extension.

11.23 USING THE PHONE AS AN OPERATOR MEDIA DEVICE (OMD)

Not applicable.

11.24 CENTRAL STORAGE OF USER SPECIFIC DATA

Not applicable.

11.25 CONFIGURING THE DIFFSERV PARAMETER

Diffserv is a model for handling of priority, based on the type of service (TOS) field in the IP packet heading.

The DSCP value can be defined in the configuration file with the parameters:

```
# 0=disable, 1=enable
Enable diffServ :0
# 46 is the default value
Singalling DSCP :46
# 46 is the default value
Voice DSCP :46
```

The DSCP value for one telephone can be set via the web UI:

NETWORK > **QOS&VLAN**

11.26 SELECTION OF TRANSPORT ADDRESSES (PORT NUMBERS)

The table below shows the default port numbers.

Table 4 UDP/TCP ports used by the phone

Type of signalling	Minimum	Maximum	Comment
RTP	10000	10398	Limitation can be introduced via the configuration file
RTCP			
SIP	5060	5060	
SIP TLS	1024	2024	
http	80	80	

11.27 REGISTRATION DISTRIBUTION

In the MX-ONE concept called HLR (Home Location Register) server, the configuration is a part of the initial REGISTER procedure. The phones will as the main rule be registered in their home server, but if the HLR server has reached its limit, an alternative server will be able to accept the registration.

The Mitel 1023 phone does not have support for registration distribution. This means that the system administrator has to handle the balancing of the registration load “manually” by defining different sip servers via different configuration files.

11.28 REDUNDANCY

The redundancy feature can be implemented by using the *SIP1 and SIP2 Register Addr* as a backup group. The following parameters in the configuration file are concerned:

# MX-ONE server 1
SIP1 Register Addr :192.105.88.10

# This name can be any name but must be equal to SIP2 Sip Name

SIP1 Sip Name :MXone

# MX-ONE server 2

SIP2 Register Addr :192.105.88.11

# This name can be any name but must be equal to SIP1 Sip Name
SIP2 Sip Name :MXone

In the example above the following happens at registration:

- the phone tries to register towards server 1 and if it is not possible towards server 2.
- at re-registration the phone tries server 1 and if it does not work keeps the registration towards server 2.

11.29 USING DNS SRV RESOURCE RECORDS

DNS SRV resource records can be used to implement redundancy.

The following parameter in the configuration file has to be enabled the use of DNS SRV records:SIP1 DNS SRV 1When the SIP1 Register Addr is set to the SRV record name, the phone performs a SRV lockup and retrieves a list of SIP registrar servers. It is recommended to specify the SIP registrar servers in the FQDN format. The most common scenario is to initiate the telephony servers (LIMs) in the SRV records. The telephones will register to these servers accordingto the priority in the SRV records.

11.30 REGISTRATION AT BRANCH OFFICES

The branch office scenario means that the telephones are registered to PBX in the main office and if the connection to the main office fails, the phones shall register to a local SIP server.

When the connection to the main office is working again, the telephones shall register towards this PBX again.

This can be implemented in a similar way as for redundancy, see section 11.28 Redundancy on page 25.

DNS SRV resource records can also be used, see section 11.29 Using DNS SRV Resource Records on page 26.

One scenario can be:

- The main site is a three servers system
- A branch office with a local SIP server
- SRV records with the three servers in the main site are used withSIP1 Register Addr
- The branch office SIP server is defined (with the IP address or FQDN) in SIP2 *Register Addr*

The phones in the branch office will register to the server with highest priority in the SRV record. If this server is out of order the server with second priority will be used. If there is no connection to the main site, the telephones will register to branch node defined in SIP2 *Register Addr*. When the phones are registered in the branch node they will continuously test if any server in the main node answers and in this case the phones willswitch back to the main node.

11.31 VOICE MAIL

When a user has got a voice mail and the message waiting key is flashing, the user can listen to his voice mail by pressing this key. The telephone will send the *32# procedure to the system.

The parameters in the configuration file are:

```
SIP1 Subscribe : 1 ; 1=subscribe of MWI messages
SIP1 MWI Num : *32#
```

11.32 CORPORATE DIRECTORY

It is not possible to access Mitel CMG corporate directory.

11.33 REMOTE PHONE BOOK

Remote Phone Book when the end user searches in this directory, one hundred records of the remote directory are downloaded into the phone and the search is done locally in the phone.Five different remote directories can be defines. The directory file shall be in .xml format. Store the .xml files on a ftp server. Example from the configuration file:

--Xml PhoneBook-- :

XML-PBook1 Name : Customers_England

XML-PBook1 Addr: ftp://192.105.106.1/aa

stra/customer_en.xml

XML-PBook1 Auth: username:password

XML-PBook1 Policy: 0 XML-PBook1 SipLine : 0

XML-PBook1 Addr : username:password. The user identity (or user account) and password under which the phone book files are stored on the FTP server.
It is possible to use several levels of the phone book files. For an example how the phone book files can look like and be linked together, see the attachments to this Installation Instructions pdf file.11.34 Contacts (Local Phone Book). The contacts are stored locally in the telephone. Maximum 500 contacts can be stored. The end user initiates the contacts via the phone menu.

To create your own xml files that to be used as external phone books, you must have the following 3 templates, such as:

1) Beijing_names.xml
2) Beijing_level_2.xml
3) PhoneBook_top_level.xml

11.33.1 CONTACTS (LOCAL PHONE BOOK)

The contacts are stored locally in the telephone. Maximum 500 contacts can be stored. The end user initiates the contacts via the phone menu.

11.34 CALL PARK POOL

For a detailed description of the Call Park Pool feature in an MX-ONE environment, see operational directions for Call Park Pool.

No configuration in the phone is needed for this feature.

12 PASSWORDS AND PIN CODES

The following passwords or PIN codes are used when working with these phones:

- PIN code for registering the phones to MX-ONE. The user can change the PIN code with the procedure: *74*old PIN*new PIN#.

  When the user has entered this, the new PIN has to be entered in the phone as well, see 7.3 Register the Phone to the SIP Server on page 11. Otherwise the phone will send the old PIN code after the next reboot.

  It is recommended to use PIN code to avoid that an end-user can log on with another end-user's directory number.
- Administrator password for accessing the phone using the phone's web interface or the phone menus.

12.1 CHANGING THE ADMINISTRATOR PASSWORD

The default user name is: **admin**

The default password is **22222**.

To change the user name and password for the web interface, the following parameters in the configuration file are affected:

```
Account1 Name : admin
Account1 Password :22222
#To let the system administrator see all the menus
Account1 Level :10
```

The password for the phone user interface can be changed via the following parameter in the configuration file:

```
Menu Password :22222
```

Note: If the configuration file cannot be read by the phone, the default password for the phone user interface is 123.

12.2 WEB INTERFACE PASSWORDS FOR END USERS

The recommendation is that the end users shall not be allowed to use the phone's Web interface. The reason is that the user can change the IP settings, which can cause problems in the network.

This is the reason why the user name and password is not described in the end user documentation.

13 EMERGENCY CALLS

There is no menu for un-register these phones which means that they are normally always registered. If the phone is not registered to the PBX, it is not possible to make emergency calls.

14 QUALITY OF SERVICE (QOS)

It is not possible to view the QoS statistics via MX-ONE.

15 DHCP SERVER

15.1 DATA FROM DHCP

The phone has support for DHCP by which the following IP configuration data can be provided:

- Own IP address, subnet mask and default gateway, received in the DHCP standard fields (1 and 3).
- URL to the software server. The path to the firmware to be downloaded from the software server can also be provided as well as the protocol to be used. The recommendation is to use DHCP option 66 (TFTP server name).

  There is support for DHCP option 43 (vendor specific information field) also, but the phone does not support DHCP option 60 (vendor class identifier), which means that it is not possible to define option 43 for this specific phone model. One other problem with option 43 is that it must be enabled before it can be used, which causes problem at new installation.

15.2 DHCP SETTINGS FOR OPTION 66

Enter the URL to the software server in the DHCP server.

Enable the DHCP option in the phone:

- **Configuration file:** The parameter is:
  DHCP Option : 66
- **Phone UI:** 🔧 > **System Config** and enter the password > scroll down to **Auto Provision > Protocol** and select **DHCP option 66.**
- **Web UI:** Click on **Maintenance** > **Auto Provision** > **DHCP Option Settings** and select **DHCP option 66.**

16 SECURITY

This phone model has support for SRTP and has TLS support of the SIP signaling.

16.1 ENCRYPTED CONFIGURATION FILES

Not supported.

16.2 HOW TO ENABLE SRTP IN MITEL 1023

The steps to enable SRTP are:

- MX-ONE: For setup of security and security policy, see operational directions VoIP Security (82/15431-ANF90114) in the CPI library.
- The feature in the phone can be enabled via the configuration file:

```
SIP1 MedCrypto : 1
SIP1 MedCrypto Key:
# SIP1 SRTP Auth-Tag shall always be set to 1
SIP1 SRTP Auth-Tag : 1
```

  The crypto key parameter is optional. If it is not defined, the phone will generate a key randomly. This is the recommended option. If the crypto key is set, it shall consist of 40 characters.

- It can also be set manually via the web UI:

  Web UI: **VOIP** > **SIP** > **Advanced SIP Settings**

  Select **RTP Encryption** and **RTP Encryption Key** (if applicable)

16.3 HOW TO ENABLE TLS FOR SIGNAL ENCRYPTION IN MITEL 1023

Do as follows:

1. **In MX-ONE:** For setup of security and security policy, see Operational directions VoIP Security (82/15431-ANF90114) in the CPI library.
2. The feature in the phone can be enabled via the configuration file:

```
SIP1 Register Port :5061
SIP1 Proxy Port    :5061
#SIP1 Transport value: 0-UDP 1-TCP 3-TLS
SIP1 Transport     :3
```

Set manually via the web UI

- **Web UI:** VOIP > SIP > Basic Settings

  Set Server Port: 5061

- **Web UI:** VOIP > SIP > Advanced SIP Settings

  Set Transport Protocol option to TLS

17 TROUBLESHOOTING

It is possible to create a file with all the current settings in the telephone. Use the web interface to initiate the dump: **MAINTENANCE** > **CONFIG** > **Backup Configuration.**

Syslog is a protocol which is used to record the log messages with a client/server mechanism. The syslog server receives the messages from clients and classifies them based on priority and type. The syslog is initiated from the web interface: **MAINTENANCE** > **SYSLOG** > **Syslog Settings.**

The messages will be written into the log by some rules which the administrator can configure:

- Level 0 = emergency. The telephone cannot work
- Level 1 = alert.
- Level 2 = critical.
- Level 3 = error.
- Level 4 = warning.
- Level 5 = notice.
- Level 6 = info.
- Level 7 = degug. This level can only be displayed in when using Telnet. This level is only intended for R&D.

18 LIMITATIONS

The following features are **not** supported:

- **MNS**. Monitoring of other telephones.
- **EDN**. Extra Directory Number.
- **SCA**. Shared Call Appearance.
- **Headset**. There is no support for headset.
- **Expansion Module**. There is no support for any expansion module