Technical Publications

February 19

MX-E Installation Manual

Author: Zultys Technical Support Department

Zultys, Inc. 785 Lucerne Sunnyvale, California, USA 94085 www.zultys.com

Contents

Revision History:

	Date	Notes
	January 2017	Initial Release
	January 2017	Updated rear panel functions, added RAID manager to front panel identification.
	July 2017	Added Release 13 features: MX-E redundancy, SRTP, User portal features, return customer routing, unmanaged device password. Clarified MoH playlist operation.
	August 2017	Added power specifications
	February 2019	Added two Zultys supplied HDD replacement instructions

1. MX-E Description

The Zultys MX-E system is a high performance enterprise grade unified communications server that addresses the requirements of medium to large enterprise customers. The MX-E system features:

- Three(3) hot swappable hard disk drives
- Dual redundant hot swappable power supplies
- RAID 1 hard disk drive configuration
- Three(3) cooling fans
- Three(3) interface slots for expansion modules
- Two(2) - 10/1000 Ethernet interfaces
- Two(2) - USB interfaces
- One(1) - Auxiliary (console) interface
- 2x16 Liquid Crystal Display(LCD) with four(4) control buttons

The Zultys MX-E is offered in three(3) configurations from the factory:

1) MX-E

This system is capable of supporting up to 300 users and up to 300 SIP trunks at G.711.

2) MX-E+

This system is capable of supporting up to 1000 users and up to 1000 SIP trunks at G.711.

3) MX-E ++

This system is capable of supporting up to 2000 users and up to 2000 SIP trunks at G.711.

1.1 MX-E System Capacities

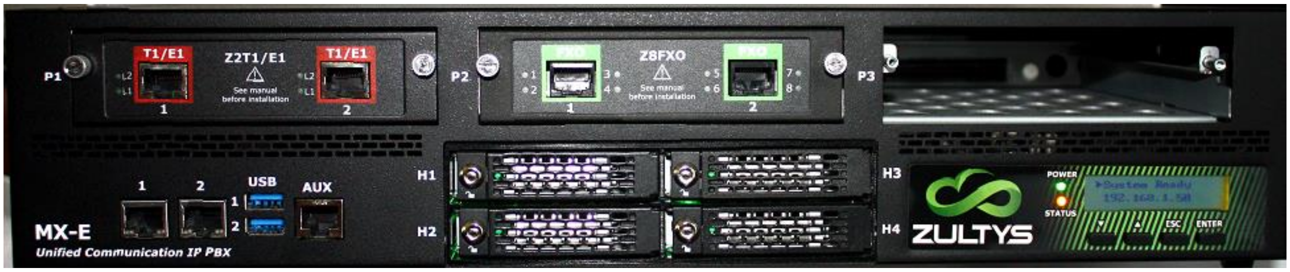
	MX-E	MX-E+	MX-E++
Users (subscribers)	300	1000	2000
Simultaneous sessions	300	1000	2000
Simultaneous registrations	1200	4000	4000
Paging groups	100	256	300
Operator groups	100	256	400
ACD or hunt groups	100	256	400
Automated attendants	100	150	200
Simultaneous accesses to AA or VM	100	256	400
Voice mail storage (hours)	1000	1000	1000
Call recording storage (hours)	150	300	600
Maximum SIP trunks	300	1000	2000
E1/T1/PRI module	3	3	3
Octal FXO module (4/8 ports)	3	3	3
Octal FXS module (4/8 ports)	3	3	3
Call Recording Sessions	300	1000	2000
Conference Participants	100	256	256
Conference Rooms	33	85	85
G.729 sessions	300	1000	2000

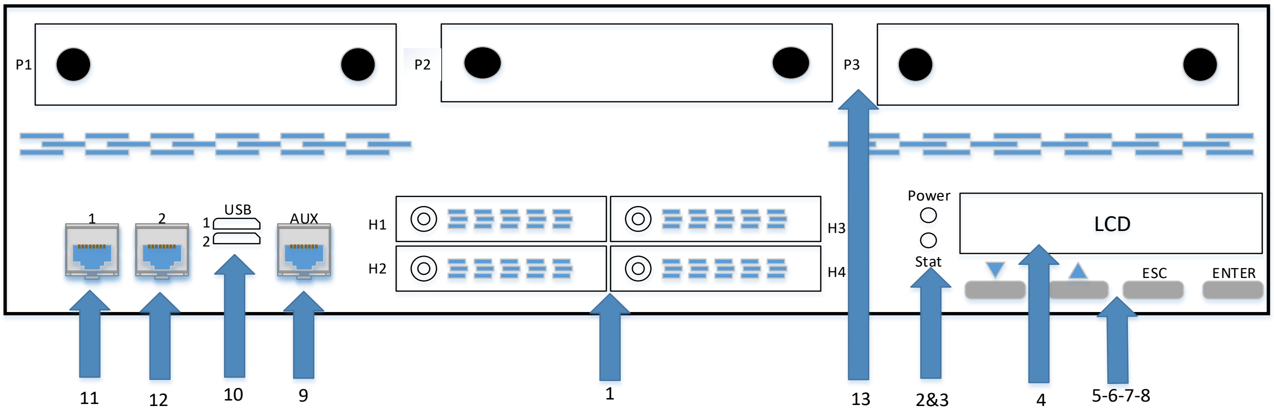
Basic MXIE	300	1000	2000
Advanced MXIE	300	1000	2000
Fax termination	64	64	100
Max number of simultaneous calls per all Outbound campaigns	100	256	256
MSEC Users	300	1000	2000
Max number of logged in Zultys Mobile Communicator users	300	1000	2000
CSTA client licenses	300	1000	2000
Desktop Integration	300	1000	2000
CRM User access	300	1000	2000

1.2 Power specifications/Dimensions

AC Input voltage, universal	100-240 VAC
Frequency	47-63 Hz
AC Input current (max)	4.5 A
Power (max)	180 watts
Typical Power (idle)	90 watts
Width	17.3”
Depth	18.1”
Height	3.46”
Weight	35 pounds

1.3 Front Panel of the MX-E


P1
T1/E1
Z2T1/E1
See manual before installation
T1/E1
1
2
P2
FXO
Z8FXO
See manual before installation
FXO
P3
1
2
USB
AUX
H1
H2
H3
H4
MX-E
Unified Communication IP PBX
ZULTYS
POWER
STATUS
ESC
ENTER



1 – *Hard Disk Drives(H1/H2/H3)* – Main, RAID-1, and a spare hard disk drive are provided. The Hard disk drive provides storage for voice mail, auto attendants, and system software. The MX-E is not operational without a hard disk drive. **Hard disk drives are hot swappable!**

Note: H4 is a solid state system drive that is not intended to be removed and is locked from the factory. The MX-E system utilizes this hard disk drive for system file operations. Do not remove this drive from service unless instructed by technical support!

Note: In the event that both the main and RAID drives become inoperable, you must contact Technical Support for an RMA on the hard disk drives. Installing a hard disk drive from another MX-E system will NOT bring the system to full functional status.

2 – *Power LED*

3 – *Status(Stat) LED*

4 – *LCD Display*

5-6-7-8 – LCD control keys – See section 1.5 for a description of the LCD control keys and how they interact with the LCD.

9 – *Auxiliary Connector(AUX)* – Serial Port connection (special cable included)

10 – *USB Connectors(USB)* – Can be used to connect to APC UPS devices. APC devices with PowerChute software will signal a low battery condition to the MX-E.

11 – *Ethernet LAN port(1)* – A 10/1000 Base-T Ethernet circuit which also serves as the console port.

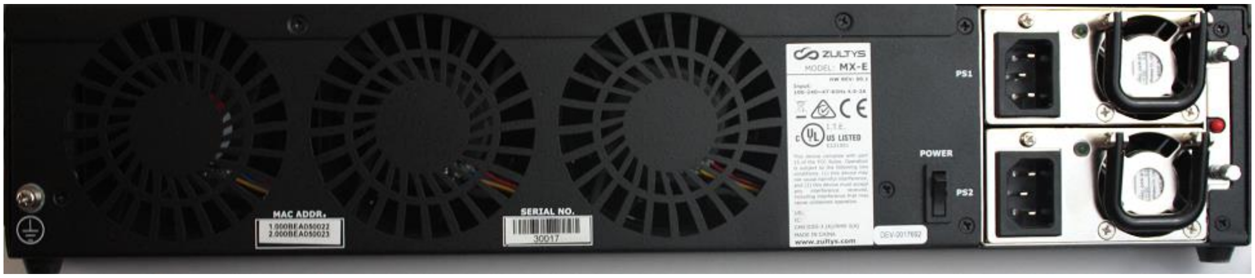
12 – *Ethernet WAN port(2)* – A 10/1000 Base-T circuit.

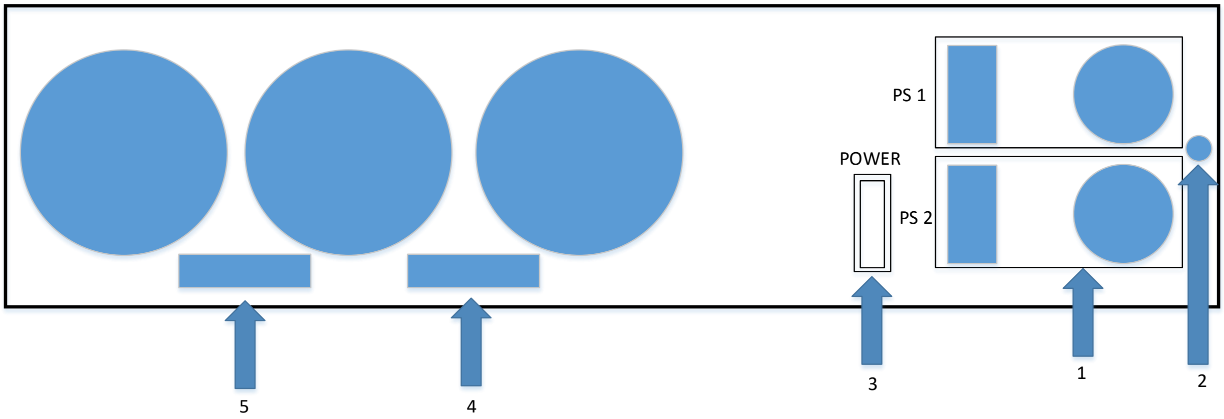
13 – *Interface slots(P1/P2/P3)* – Three slots for installing optional interface modules. Available modules include:

- FXO: 4 or 8 circuit analog exchange-side circuits.
- FXS: 4 or 8 circuit analog subscriber-side circuits.
- PCM: one or two circuit digital T1/E1/PRI exchange-side circuits.

1.4 Rear Panel of the MX-E

The rear panel, shown below, contains the power supplies, power switch, alarm silence button, and system information.





1 – *Dual Redundant Hot Swappable Power Supplies* (*PS 1/PS 2*). *Has the 117 Vac input connector, LED status*

NOTE! Both power cables must be plugged into AC power sources. Failure to do so will create an audible alarm condition. In the event of a power supply failure, the audible alarm will sound until the faulty power supply is replaced or the Power Supply Alarm Silence button is pressed.

2 – Power Supply Alarm Silence *button*

3 – *Power Button* – This powers the system on. It is not recommended to power the MX-E system down using the switch. Utilize the LCD control or MX Administrator software to initiate a graceful shutdown.

4 – *Serial Number* – Identifies the main chassis. Refer to this number to identify the system when obtaining service or returning the system for repair or replacement

5 – *MAC Address* – Identifies the MAC address of the MX-E unit.

1.5 Liquid Crystal Display (LCD)

This chapter describes MX-E LCD functions. The MX-E has a 2 line x 16 character Liquid Crystal Display (LCD) on the front panel. The LCD is used to display various system information at boot time and normal runtime. In addition, there are four (4) buttons below the LCD that are used to navigate through LCD menus during runtime. Two (2) of these buttons can be used to place the system in console mode during boot.

1.5.1 LCD during boot process:

```
SYSTEM BOOTINNG
```

```
LOADING APP
```

```
LOADING CONFIG
```

When the boot process is complete, the system will go to a normal Idle display

```
SYSTEM READY
XXX.XXX.XXX.XXX
```

Where: XXX indicates the IP address of the system

1.5.2 LCD during normal system operation:

Idle display

```
SYSTEM READY
XXX.XXX.XXX.XXX
```

Where: XXX indicates the IP address of the system

Pressing the DOWN arrow button will scroll through all the IP addresses in the system as well as the serial number, software version, and CS (customer support server) connection status:

```
XXX.XXX .XXX.XXX
XXX.XXX .XXX.XXX
```

```
SERIAL XXXXX
SW: X X. X. XXX
```

```
CS STATUS

```

Pressing the ENTER button at the system ready prompt will present a menu of sub items. Use the DOWN arrow to scroll through the sub-menu of options:

```
ONCONSOLE MODE
CONNECT TO CS
```

```
SYSTEM RESTART
SYSTEM SHUTDOWN
```

Pressing the ENTER button at the Console Mode On prompt will present a confirmation prompt. Press ENTER to place the system into console mode.

CONFIRM CONSOLE

Pressing the ENTER button at the Connect to CS prompt will present a confirmation prompt. Press ENTER to place the system into customer service mode.

CONFIRM CS

Pressing the ENTER button at the System Restart prompt will present a confirmation prompt. Press ENTER to restart the system.

CONFIRM RESTART

Pressing the ENTER button at the System Shutdown prompt will present a confirmation prompt. Press ENTER to shut the system down gracefully.

CONFIRM SHUTDOWN

The ESC button will return you to a previous menu or to the home screen depending on where you are in menu navigation.

1.6 LED Functions

Power – This LED will light Green when the system is powered on. It remains on during normal operation and extinguishes when the system is powered down.

Status – This LED will flash intermittently during normal operation indicating various processing activity.

Drive - This LED (located on each hard disk drive) will flash intermittently indicating hard disk drive (HDD) activity.

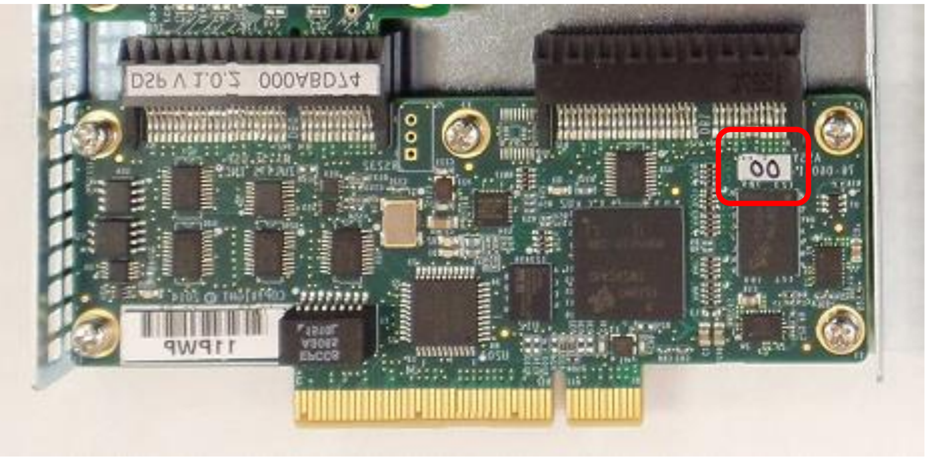
2. MX-E Circuits

MX-E interface modules ARE NOT interchangeable with MX30 or MX250 interface modules. MX-E interface modules ARE compatible with MX-SE interface modules.

Note! Certain revisions of MX-SE modules will not function in MX-E systems. To determine if an existing MX-SE module is compatible, locate the DSP circuit board on the module. There will be a revision code of either “00” or “10”

00 = Not compatible

10 = Compatible



2.1 10/1000 Base-T

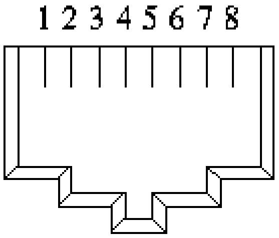
The MX-E has two 10/1000 Base-T Ethernet circuits labeled 1 and 2. Power over Ethernet is not provided on either circuit. These interfaces are in “Routing Mode” and cannot be changed to bridging mode.

- **Ethernet LAN Port (1)** connects to your local area network and provides data connectivity for the enterprise. This port serves as the console circuit, as described in Console Mode. Changing the IP address is done in Provision\System Settings\IP Addresses
- **Ethernet WAN Port (2)** can be used to implement ALG/SBC through a second IP address.

RJ45 ports connect Ethernet circuits to the MX-E and can auto-detect and adapt to the CAT5 cable configuration (straight or crossover). Changing the IP address is done through View\Interfaces. Select and right click on Ethernet 2, select Interface Information, select Configure form the IP Information tab, right click on the IP address and select Edit.

RJ45 Connector Pin Placement

(10/1000 Ethernet Circuit)

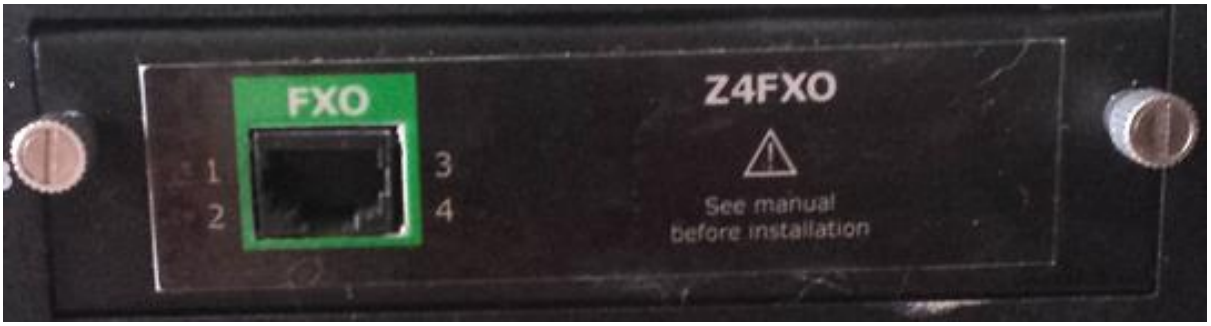


2.2 Analog FXO

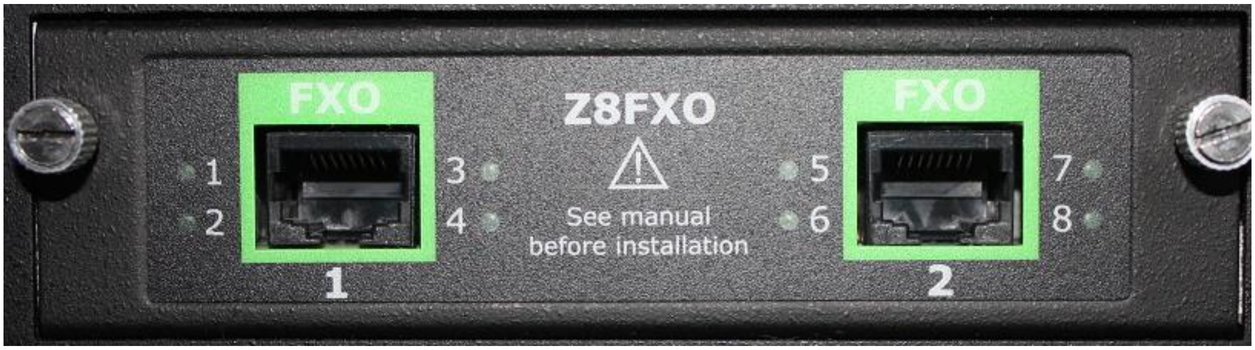
The MX-E supports a four port FXO module or an eight port FXO module through the interface slot. REN is 0.4.

The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any *combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five. / L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.*"

- The FXO4 module, shown below, provides four analog exchange-side circuits.



- The FXO8 module, shown below, provides eight analog exchange-side circuits.



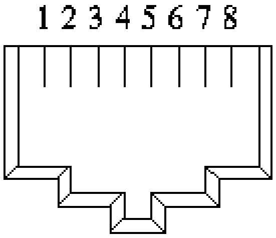
Modules provide two-wire exchange side circuits that connect to central office lines through RJ45 connectors and are configured for one of several analog protocols through the MX Administrator Interface.

LED indications are provided that indicate the status of each circuit.

Circuit State	LED Indication
Idle	Extinguished

Ringing/In Use	Solid green

Below table and image show the placement and function of RJ45 connector pins for the FXO4 and FXO8 circuit modules.



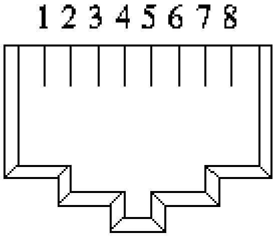
Pin	Function
1	TIP 2
2	RING 2
3	TIP 3
4	RING 1
5	TIP 1
6	RING 3
7	TIP 4
8	RING 4

Note: No analog calibration is required on FXO ports of the MX-E system!

2.3 Analog FXS

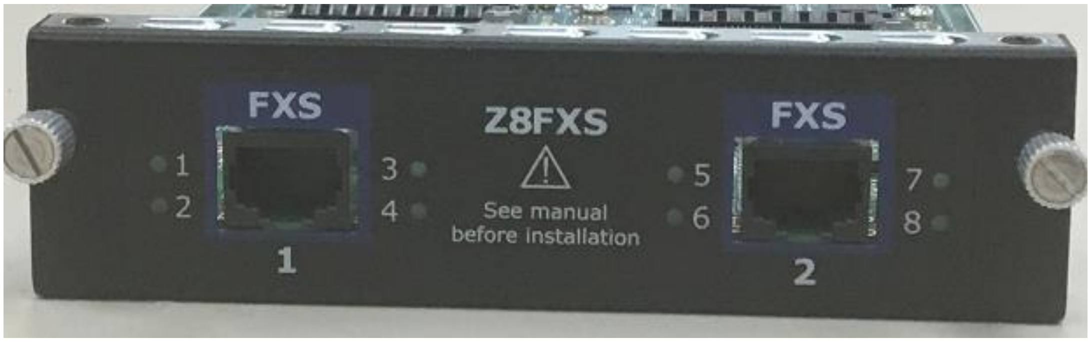
The MX-E supports either a four port or eight port FXS module through the interface slot.

- Below table and image show the placement and function of RJ45 connector pins for the FXS4 circuit module.

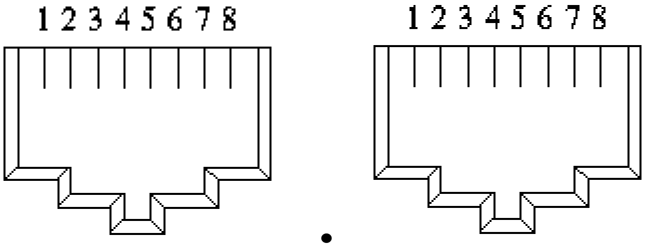


Pin	Function
1	TIP 2
2	RING 2
3	TIP 3
4	RING 1
5	TIP 1
6	RING 3
7	TIP 4
8	RING 4

- The FXS8 module, shown below, provides eight analog interface circuits.



- Below table and image show the placement and function of RJ45 connector pins for the FXS8 circuit module.



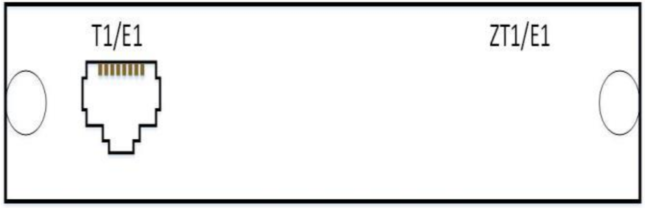
Pin	Function
1	TIP 2
2	RING 2
3	TIP 3
4	RING 1
5	TIP 1
6	RING 3
7	TIP 4
8	RING 4

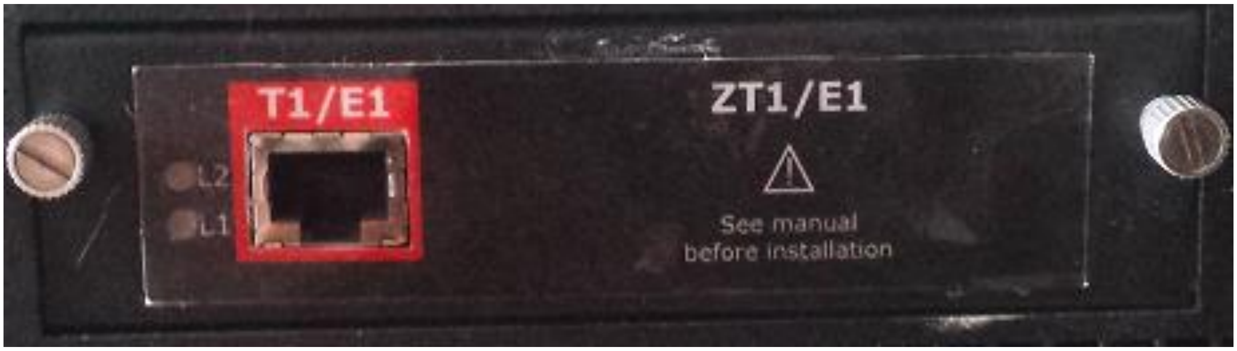
2.4 PCM Module

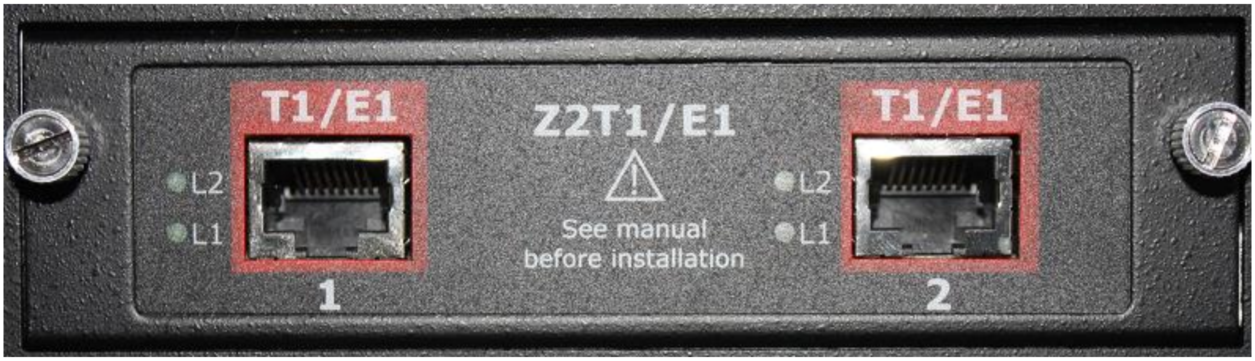
The MX-E supports one PCM module per interface slot. The module has one or two full duplex circuits that can be configured as either T1(1.544Mps)

/E1(2.048Mbps) /PRI (23B+D, 1.544Mbps). The circuit uses one of several supported PSTN protocols, i.e. ISDN, CAS, MFCR2. The circuit type and protocol are configured in MX-E Administration.

Pin assignments of the PCM module:

Pin	Signal Name	Circuit	Source	RJ45 Connector Diagram
1	Received Data, ring	BAa	Facility	
2	Received Data, tip	BAb	Facility	
3	unconnected	AA	-	
4	Transmitted Data, ring	BBa	MX-E	
5	Transmitted Data, tip	BBb	MX-E	
6	unconnected	AA	-	
7	unconnected	AA	-	
8	unconnected	AA	-	





4. Shutting Down the MX-E

To shut down the MX-E:

1. Initiate a System Shutdown operation using one of the following methods:
   - Select ***Maintenance → Shutdown*** from the User Interface, choose a shutdown option from the displayed list, then press the OK button.
   - Use the LCD buttons to navigate to the System Shutdown menu item:

   Press the ENTER button at the System Ready prompt

```
> SYSTEM READY
```

   Use the DOWN arrow button to scroll to the System Shutdown prompt:

```
> SYSTEM SHUTDOWN
```

   Press the ENTER button to select system shutdown:

```
> CONFIRMSHUTDOWN
```

   Press the ENTER button to confirm the system shutdown.

2. Wait until the Power and Status LEDs off.
3. Remove power from the DC input.

Power to the MX-E is not removed until the power cord is physically unplugged from the chassis.

Shutting down the MX-E in this manner terminates Linux and all applications properly.

A *Hard Shutdown* terminates MX-E functions without gracefully shutting down applications or properly terminating Linux. Removing the DC input power or pressing the Power button while the system is normally operating executes a hard shutdown.

Performing a Hard Shutdown is strongly discouraged. Operations are instantly terminated, data will be lost, and the Flash Memory and HDD contents may be corrupted.

5. Console Mode

Console mode provides access to the MX-E in a predefined state for configuring the system IP address or recovering the Administrator password. The MX-E defines two console modes:

- Boot Time Console Mode is entered as you start up the MX-E. You can configure the main IP address and recover the Master Administrator password from this mode.
- Run Time Console mode is entered during normal MX-E operation. Technical support personnel can monitor system behavior when the system is in this mode.

Ensure that the Ethernet cables are disconnected from the MX-E before entering console mode.

When the MX-E is in console mode, you can connect a computer to the LAN Ethernet Port. The IP address that accesses the MX-E depends on the console mode of operation.

5.2 Boot Time Console Mode

The following procedure places the MX-E into Boot Time Console Mode:

1. Disconnect the Ethernet ports from your system.

Failure to do so may disturb other devices on the LAN.

2. Ensure power to the MX-E is shut down.
3. Press and hold the ENTER button under the LCD display.
4. While pressing the button, press and release the power button on the rear of the unit.
5. Release the ENTER button when the LCD displays:

```
CONSOLE MODE?
```

6. Press the ENTER button to place the system into console mode.
7. Configure your PC's network interface with an IP address of 192.168.1.103 and a subnet mask of 255.255.255.0. Connect your PC directly to the LAN Ethernet Port.
8. To access the MX-E, open the MX-E Admin User Interface at IP address 192.168.1.100 using one of the following case sensitive Login-Password combinations:
   - Login name: MX-E user previously configured with administrator rights. Password: text string configured as password for the user.
   - Login name: **Administrator.** Password: **zultys**

This option permits access when the Administrator password is unknown and users with administrator rights are unavailable. You can change the Administrator password in this mode, if you know the current Administrator Password.

5.2.1 To exit console mode and resume normal operations

To exit the console mode you must properly shut down and power cycle the MX-E, by using the reboot command.

1. Disconnect the PC from the console port.
2. Reconfigure PC to obtain its TCP/IP address automatically.
3. Reconnect the PC and the MX-E to the network.

5.2.2 Run Time Console Mode

If you are unable to access your system through MX-E Administrator, you can allow Zultys Technical Support to access your system by entering Run Time Console Mode. You should enter Run Time Console Mode only as instructed by a member of Zultys Technical Support.

Invoking Console mode during normal operation puts the MX-E into console mode without changing its IP addresses.

To put the MX-E into console mode during normal operation:

Pressing the ENTER button at the System Ready prompt will present a menu of sub items. Use the DOWN arrow to scroll through the sub-menu of options until Console Mode On is highlighted. Press ENTER:

```
ON CONSOLE MODE
 CONNECT TO CS
```

Press the ENTER button at the confirmation prompt to enter console mode

```
 CONFIRM CONSOLE
```

To exit console mode, press and hold the Down arrow button for two seconds. The MX-E exits console mode, as indicated by the normal idle LCD.

6. Preparation

The MX-E is designed to be permanently installed in a network room or office. You must carefully install the MX-E system to ensure its proper operation.

This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel. *Installation by unqualified individuals may result in bodily injury and damage to the MX-E and surrounding equipment.*

6.2 Installation Safety Notes

These are the safety considerations for using the Zultys MX-E hardware. Read these notices before installing or using your phone system.

Important This notice contains special information that should not be ignored.

Warning This notice indicates that if a specific or practice is not correctly followed, permanent damage to the MX-E and personal injury may result.

Danger This notice warns you of imminent hazard to yourself and others if proper procedures are not followed.

Important Ultimate disposal of this product should be handled according to all national laws and regulations.

Danger Do not work on the system or connect or disconnect cables during periods of lightning activity.

Warning The separate protective earthing terminal provided on this product shall be permanently connected to earth.

Danger Disconnect telecommunication network connectors before removing cover.

Warning To reduce the risk of fire, use only 26 AWG or larger (e.g., 24 AWG) UL listed or CSA Certified Telecommunication Line Cord for all telecommunication circuits.

Danger Disconnect DC input connector before servicing.

Warning This unit is designed to work with telephone power system.

Safety Instructions - Rack Mount:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

Replaceable batteries:

CAUTION: Risk of Explosion if Battery is replaced by an Incorrect Type. Dispose of Used Batteries According to the Instructions.

Telephone line cord:

CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord

Supplementary Earthing Conductor:

When FXS Card is installed in the MX-E, Supplementary Earthing conductor shall be installed prior to connection to AC Mains.

6.3 Selecting a Site

The following criteria must be considered when selecting a site for your MX-E system.

The MX-E must be installed in a secure location with access restricted to qualified personnel. Placing the MX-E in a location accessible by unqualified individuals may result in bodily injury and damage to the MX-E and surrounding equipment.

- Temperature: Install the MX-E where the temperature remains between 0°C and 40°C.

Operating the MX-E in temperatures below 0°C or above 40°C voids your warranty and *may result in bodily injury and damage to the MX-E or surrounding equipment*.

- Ventilation: The MX-E requires space on both sides for ample air flow. Ensure the MX-E has space on both sides for ventilation.

Do not cover the interface slot and openings on the equipment. These are provided for ventilation and protection against overheating.

- **Cable Lengths**: Cable placement to associated equipment is an important site criterion. MX-E Circuit Cables shows the minimum and maximum length of any cables you connect to the MX-E.
- **Other Site Requirements**: Select a site where liquids or objects will not fall onto the equipment and that foreign objects will not be drawn into the ventilation holes.

6.4 Power Requirements

The total power input for the MX-E is W.

Disconnect 2 power supply cords before servicing

6.5 Electrostatic Discharge (ESD) Precautions

Almost all electronic components can be damaged by ESD during handling. Component damage can occur at ESD voltages as low as 50 V. A person walking across a nylon carpet can easily generate voltages in excess of 5,000 V.

Observe the following guidelines to help prevent ESD damage when installing or servicing the MX-E system or any other electronic device.

- Assemble or disassemble equipment only in a static-free work area.
- Use conductive work surfaces, such as an antistatic mat, to dissipate static charge.
- Wear a conductive wrist strap and lab coat to dissipate static charge accumulation.
- Minimize handling of assemblies and components.
- Keep replacement parts in their original anti-static packaging.
- Remove plastic, foam, vinyl, paper, and other static-generating materials from the work area.
- Use tools that do not create ESD.
- Do not handle connector pins or touch onboard components.

⚠ You can easily damage the MX-E by failing to follow these instructions. You may delay installation or cause equipment to prematurely fail. Such failure may lead to a disruption of the service provided by the equipment and void your warranty.

6.6 Serial Number

Verify the serial numbers of each item and compare them with the serial numbers on the packing lists. The serial number is a five digit alphanumeric code printed on a white barcode label on the rear panel. See section 1.2 to locate the serial number on the back of the MX-E.

7. Mounting the MX-E

Zultys recommends installing the MX-E in the same secured wiring closet as the networking equipment to which it connects. Typical devices connecting to the MX-E include the LAN switch and the provisioning computer.

The MX-E can be rack mounted, placed on a network shelf in the IT rack, or on top of a table or desk. Ensure the table or desk is properly mounted to the floor or has properly fitted stabilizers so it cannot move and will not tip over. Zultys recommends installing the system in the IT rack using the supplied rack brackets/screws.

NOTE!	**Leave space at the rear of the system for cables and for personnel installing the system.**

8. Connecting to the MX-E

8.2 Initial System Configuration

The MX-E IP address is view or configured through the User Interface. To view the IP address, select Provision → System Settings, then access the IP Addresses panel. If the IP Address (Main) data field is empty, the system uses 192.168.1.100 as the IP Address. The MX-E uses the same address for the Main and RTP IP address.

Before connecting the MX-E to your network, the Main and Internal IP addresses should be written on the IP Addresses panel on the front of the MX-E.

8.3 Startup Log

The web browser interface provides a log that lists the steps performed during the startup sequence. Open the web browser interface by starting your web browser and entering the main IP address (192.168.1.100 for an un-configured system) in the address field. To open the Start Up Log, click on Start Up Log on the Web Browser Interface.

8.4 Initial System Configuration Procedure

This procedure sets the IP addresses on a system where the main IP address is not specified on the IP Addresses panel.

1. Disconnect the MX-E Ethernet ports from all devices and networks.
2. Ensure power is removed from the MX-E.
3. Boot up the system, following the procedure in Booting Up the MX-E.

Alternatively, enter console mode by following the procedure described in Section 5.2.

1. Configure your computer with an IP address of 192.168.1.105 and a subnet mask of 255.255.255.0.

2. Connect your PC to the Ethernet LAN port 1.
3. If the MX-E Administrator is not installed on the computer, open your HTML browser, enter the IP address *192.168.1.100* , then click on Download Administration UI and open the file to install the software. If the Zultys MX-E Administrator Login panel appears, skip to step 5.
4. Double click the MX-E Admin icon to display the Zultys MX-E Administrator Login panel.
5. Enter the following values in the Login panel (logins and passwords are case sensitive):
6. **Login**: Administrator
7. **Password**: zultys
8. **URL**: 192.168.1.100
9. Run the Setup Wizard located under Provision → Wizard

8.4.1 Obtaining MX-E Administrator

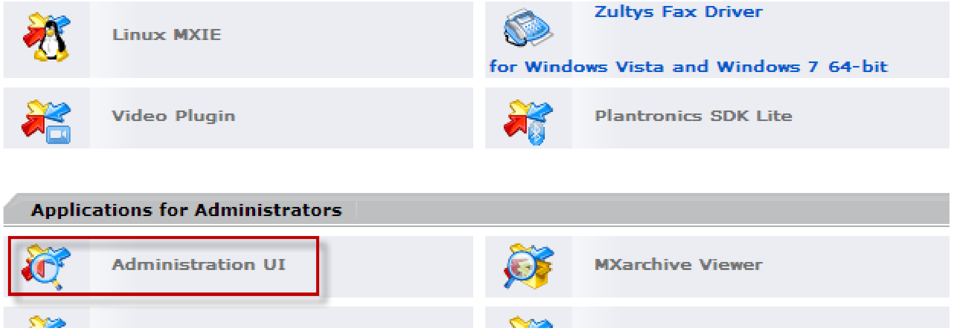
The MX-E is configured from the MX-E Administrator application.

MX-E Administrator allows the system administrator to configure all functions of MX-E including:

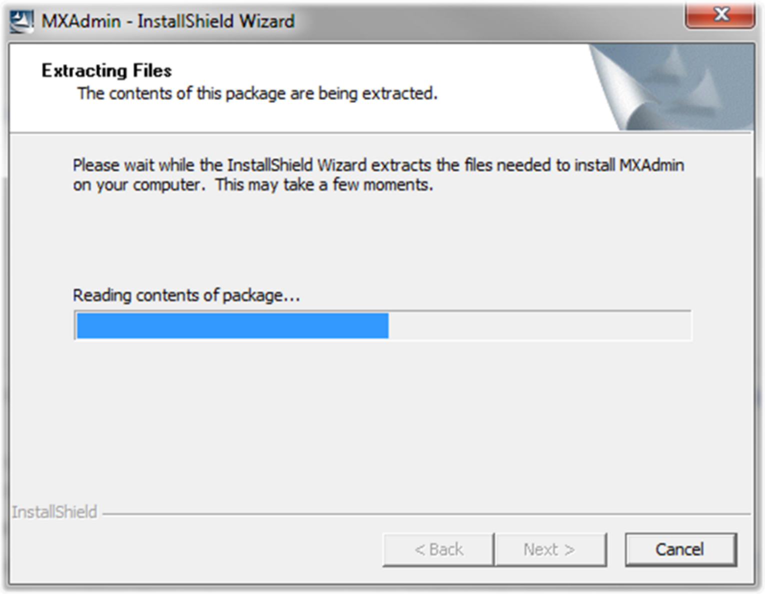
- Provision the system so that it can be connected to voice services.
- Configure the data communications functions so that MX-E fits into, or is the central part of, the LAN.
- Specify the devices and users that can access MX-E and its features.
- Define how the auto attendant (AA) and voice mail operate.
- Monitor the status of the functions of MX-E and the devices connected to it.

To download and install the MX-E Administrator application for MX-E, open a browser, type the main IP address of MX-E and press Enter.

Click on the *Administration UI* link to begin downloading MX-E Administrator application.



Open the installation file and complete the installation process.


MXAdmin - InstallShield Wizard

Extracting Files

The contents of this package are being extracted.

Please wait while the InstallShield Wizard extracts the files needed to install MXAdmin on your computer. This may take a few moments.

Reading contents of package...

Once the installation is finished, the login window appears.

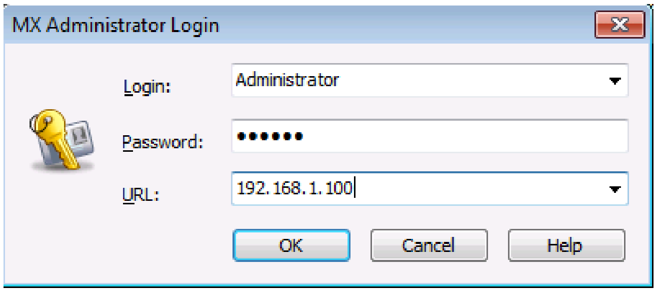
To login into MX-E Administrator, use the default login credentials.

- Login entries may be entered directly or selected from a drop-down menu that lists recent entry attempts. A valid login must match the user name as configured in the MX-E user list.
- Passwords must be typed exactly as configured for the specified user. Passwords are case sensitive.
- URL specifies the IP address of the system that you wish to access. This entry may be a numerical address or a configured name for the system.

The entry may be entered directly or selected from a drop-down menu that lists recent entry attempts.

Note: Login and Password are case sensitive

- *Login*: Administrator
- *Password*: zultys
- Type the IP of 192.168.1.100 in the *URL* line.


MX Administrator Login

Login: Administrator

Password: ••••••

URL: 192.168.1.100

Click *OK* to open MX-E Administrator.

Once the wizard finishes, and you click the reboot button, the User Interface will lose connection with the MX-E as it shuts down.

1. Disconnect the PC from the Ethernet LAN port.
2. Configure PC to obtain its TCP/IP address automatically.
3. Connect the PC and the MX-E to the network.
4. Exit the MX-E Administrator, as it will continue to connect to the 192.168.1.100 address
5. Login to the MX-E Admin User Interface software, entering the configured IP address as the URL in the Login panel, to complete the system provisioning and configuration.

9. Connecting the MX-E to the Network

9.2 Cables Required for Installation

The number and types of cables required for your system depends on the enabled system options and your network configuration. See MX-E Circuit Cables which lists the cables that may be required.

MX-E Circuit Cables

Cable and Connector	*Max Qty*	*Used to connect* to	Minimum Distance	Maximum Distance
RJ45 cables	2	Analog circuits to PSTN (FXO)	0	1 km (3000 ft)
RJ45, 568A wiring, Cat 5	*2*	*Ethernet to an IP-enabled device, firewall, or provisioning console**	0	100 m (300 ft)

* Ethernet cable wiring must comply with EIA/TIA 568A for the CAT5 10/1000Base-T Ethernet. Crossover cables comply with EIA/TIA 568A in all aspects except signals on pins 1 and 3 at one end appear on pins 2 and 6 at the other end.

To reduce the risk of fire, use only 0.4 mm (26 AWG) or larger wire for all telecommunications circuits.

9.3 Connecting Procedure

Refer to Front Panel *of the MX-E* to locate and identify all MX-E ports.

Connect the MX-E to the LAN through the Ethernet LAN port.

1. Connect all subscriber stations:

   Connect IP phones or devices enabled with softphones to the LAN through a switch.

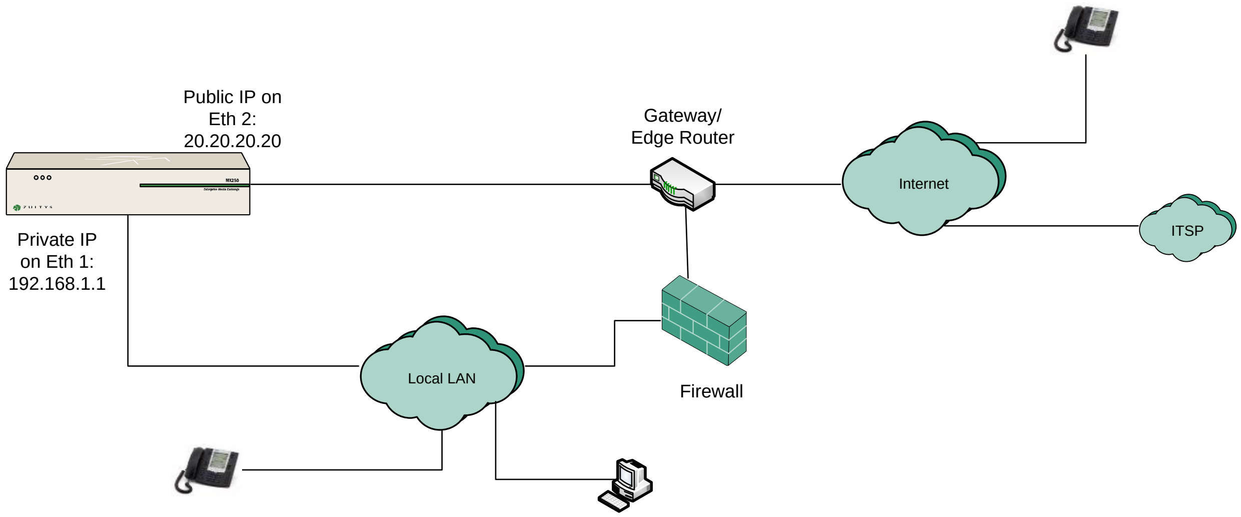
2. Connect voice lines to the PSTN
3. Connect to the IP WAN: If you connect to the WAN using external equipment you can connect the external equipment to the MX-E using the WAN Ethernet port.
4. Ensure that power is not provided to the system.
5. Connect the ac input to a power source, as specified by *Power Requirements.*, using the ac power supply with the system.

Always use the provided power cords to power the MX-E; contact your Zultys representative if this is unsuitable. The provided power cord has a separate ground (earth) connector and must be inserted in a power socket that provides a protective ground (earth) contact. Do not use an extension cord that does not carry the protective grounding conductor. *Keep the power cord properly connected at all times, even if the MX-E is not powered by the ac mains.*

The power supply cord is used as the main disconnect device. Ensure the power socket is located or installed near the equipment and is easily accessible. Do not place objects on the power cord. Run the power cord so people cannot step on or trip on the power cord. Overloading wall outlets may result in electric shock.

10. Configuring the MX-E for Routing Mode:

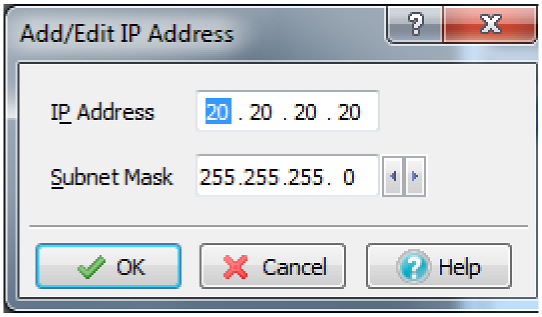
10.2 Configuring the MX-E for Routing Mode



MX-E: For the MX-E, the Ethernet 2 (WAN interface) is always configured in Routing mode and thus there are no settings to change the mode of operation from Bridging to Routing.

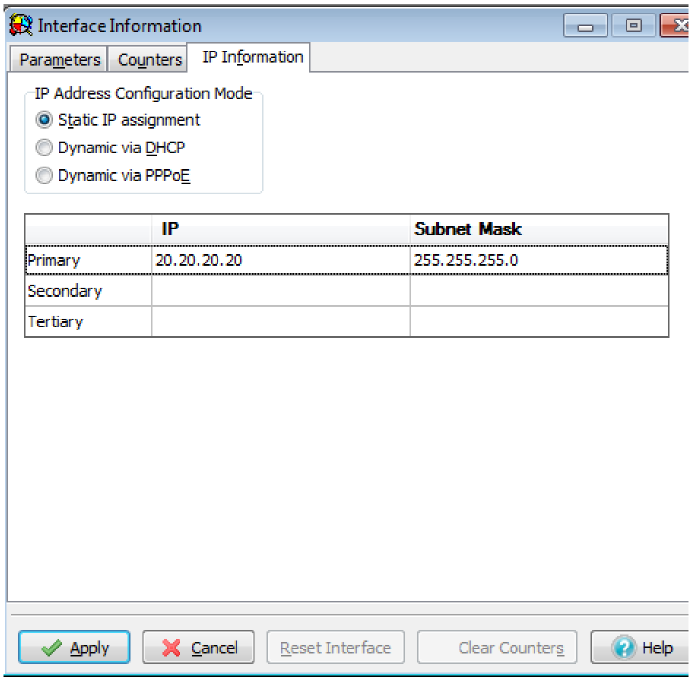
10.3 Configuring Ethernet Port 2 for an external IP Address

1. From the MX-E Administrator select *View → Interfaces*.
2. From the View pull-down menu, Select Interfaces.
3. From the Interface menu, double-click on Ethernet 2. This will display the Interface Information screen for Ethernet Port 2.
4. Click on the IP Information Tab, and click on Configure
5. Right-click in the Primary field and click on Add.
6. Configure the you public IP (in this example we will use 20.20.20.20:
   - IP Address: 20.20.20.20
   - Subnet Mask: 255.255.255.0
7. Click on OK to return to the previous menu
8. Click on Apply to save your changes.



IP Address: 20 . 20 . 20 . 20

Subnet Mask: 255.255.255. 0



IP Address Configuration Mode

● Static IP assignment

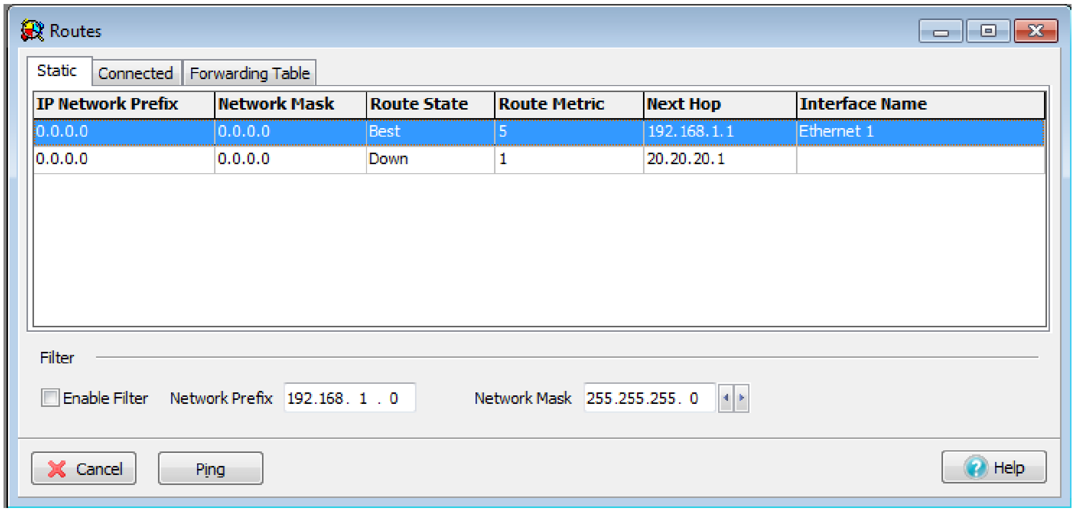
○ Dynamic via DHCP

○ Dynamic via PPPoE

	IP	Subnet Mask
Primary	20.20.20.20	255.255.255.0
Secondary		
Tertiary		

10.4 Set up routing tables

Access the MX-E routing table from the MX-E Administrator, View → Routes menu. If you previously assigned the default gateway when in console mode you will not be able to modify the first table entry with a metric of 5. You will need to boot back into console mode and remove the default gateway. As a work around you can create an additional entry with a lower metric.



IP Network Prefix	Network Mask	Route State	Route Metric	Next Hop	Interface Name
0.0.0.0	0.0.0.0	Best	5	192.168.1.1	Ethernet 1
0.0.0.0	0.0.0.0	Down	1	20.20.20.1	

Filter

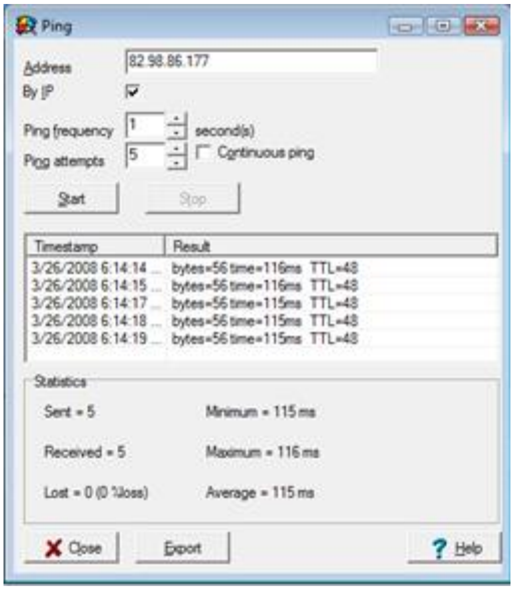
□ Enable Filter Network Prefix 192.168. 1 . 0 Network Mask 255.255.255. 0

Create a route that sets all IP addresses to go out to the internet (0.0.0.0 subnet 0.0.0.0) and set the next hop (the outside router) to be 20.20.20.21.

Test to verify the DNS and IP works correctly for the MX-E by using the ping function. This insures that the MX-E itself can reach the internet, and that the DNS lookups work correctly. If the MX-E cannot get out to the internet, nothing else will be able to.

10.4.1 Test Routing Options

The Ping function can be launched from the routes screen, by clicking on the "*Ping*" button.



Address 82.98.86.177

By IP ☑

Ping frequency 1 second(s)

Ping attempts 5 □ Continuous ping

Timestamp	Result
3/26/2008 6:14:14 ...	bytes=56 time=116ms TTL=48
3/26/2008 6:14:15 ...	bytes=56 time=116ms TTL=48
3/26/2008 6:14:17 ...	bytes=56 time=115ms TTL=48
3/26/2008 6:14:18 ...	bytes=56 time=115ms TTL=48
3/26/2008 6:14:19 ...	bytes=56 time=115ms TTL=48

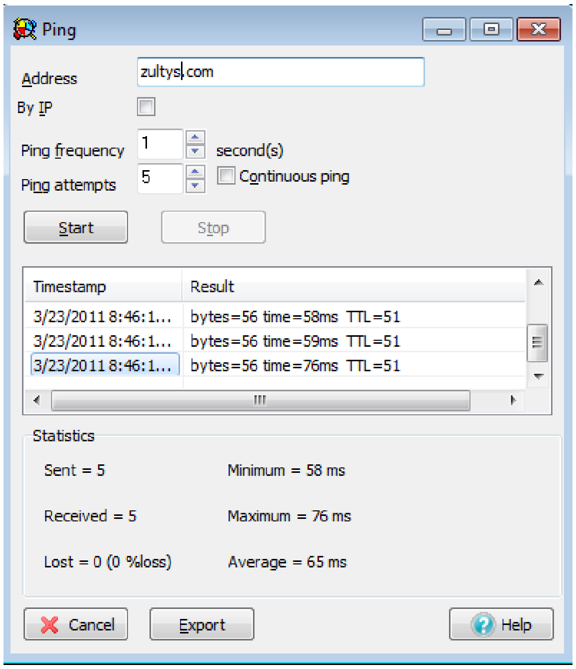
Statistics

Sent = 5 Minimum = 115 ms

Received = 5 Maximum = 116 ms

Lost = 0 (0 %loss) Average = 115 ms

If this works, check it by name, to verify that the DNS portion is working as well. Remove the check mark for By IP, and change the address to Zultys.com, and click Start.



Address zultys.com

By IP □

Ping frequency 1 second(s)

Ping attempts 5 □ Continuous ping

Timestamp	Result
3/23/2011 8:46:1...	bytes=56 time=58ms TTL=51
3/23/2011 8:46:1...	bytes=56 time=59ms TTL=51
3/23/2011 8:46:1...	bytes=56 time=76ms TTL=51

Statistics

Sent = 5 Minimum = 58 ms

Received = 5 Maximum = 76 ms

Lost = 0 (0 %loss) Average = 65 ms

11. SBC

The purpose of the Session Border Controller feature introduced in MX-E firmware v5.0 is to facilitate the successful passage of SIP signaling and RTP media streams through the Network Address Translation (NAT) function commonly implemented in broadband gateways and corporate firewalls.

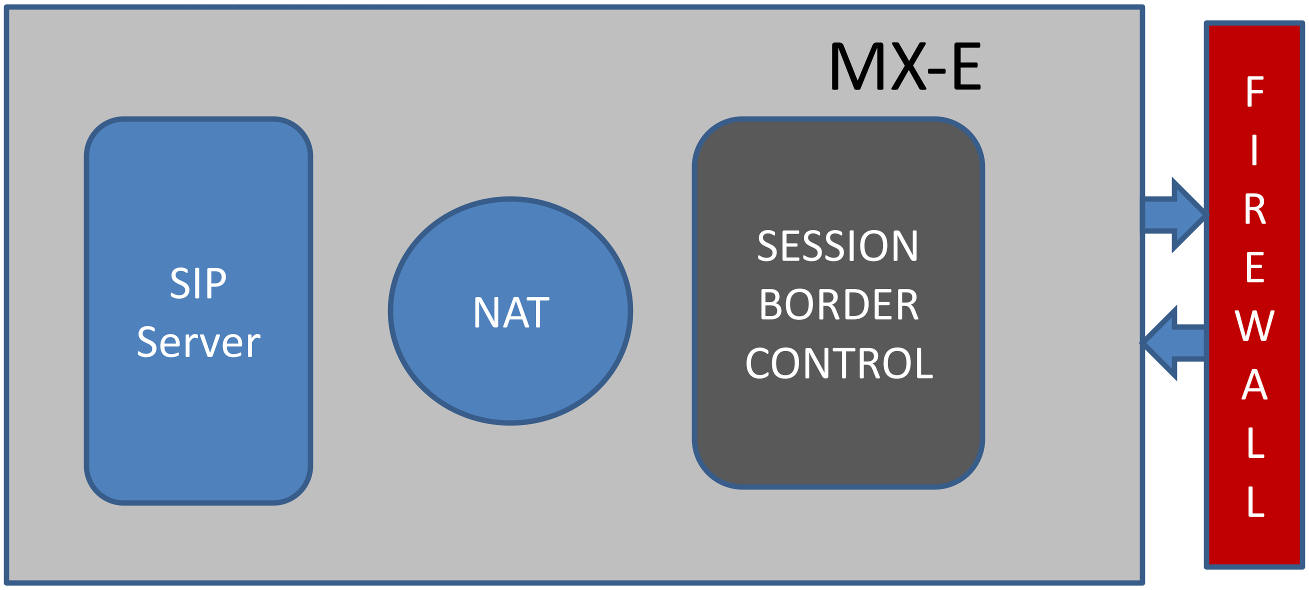
The key purpose of NAT is to allow multiple network devices (Hosts) on a Private Network to connect to the Internet via a single public IP address. This process inherently provides a level of protection for Hosts located on the private network as all unsolicited packets sent from external Hosts are prevented from accessing the internal network Hosts.

General information about Network Address Translation may be viewed at: http://en.wikipedia.org/wiki/Network_address_translation

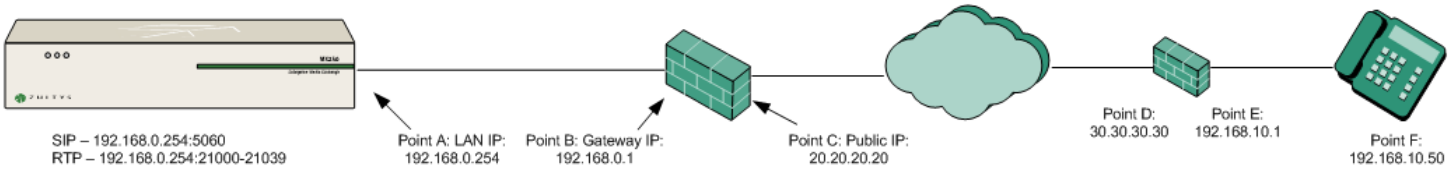
Routers and Broadband Gateways that implement NAT re-write the IP address and port information contained within IP packets and keep track of network conversations ensuring that traffic is able to flow in each direction for many applications such as web surfing or sending email.

An undesired impact of NAT is that it detrimentally impacts protocols that contain embedded network address details within their application data. The industry standard Session Initiation Protocol (SIP) used by advanced VoIP IP-PBX systems such as the Zultys MX-E system is one such protocol.

The Session Border Controller function included as standard in MX-E firmware v5.0 onwards supports Near-End NAT Traversal to allow the MX-E system to be deployed behind the corporate firewall while still allowing external SIP devices to connect and Far-End NAT Traversal to facilitate connection of remote phones such as those deployed at remote offices, employee homes and roaming sales people connecting from Wi-Fi hotspots, which are deployed behind broadband gateways and firewalls without the need for complex Virtual Private Networks (VPN).

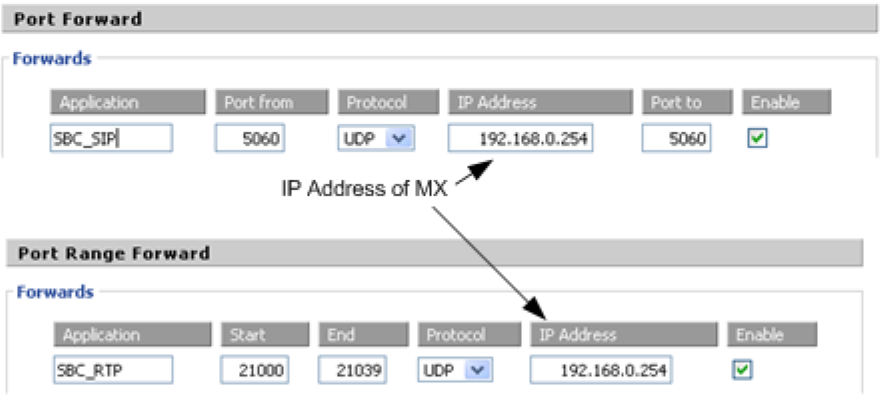


11.2 Configuration settings for the MX-E when behind a firewall


SIP – 192.168.0.254:5060
RTP – 192.168.0.254:21000-21039
Point A: LAN IP: 192.168.0.254
Point B: Gateway IP: 192.168.0.1
Point C: Public IP: 20.20.20.20
Point D: 30.30.30.30
Point E: 192.168.10.1
Point F: 192.168.10.50

11.2.1 Edge Firewall/Router modifications

The edge router must be configured to port forward all necessary packets for the services you plan on using (TFTP, SIP and RTP to name a few) from the external interface to the internal IP address of MX-E system. The images below show the Port Forwards relevant to SIP and RTP



Port Forward

Forwards

Application	Port from	Protocol	IP Address	Port to	Enable
SBC_SIP	5060	UDP	192.168.0.254	5060	☑

IP Address of MX

Port Range Forward

Forwards

Application	Start	End	Protocol	IP Address	Enable
SBC_RTP	21000	21039	UDP	192.168.0.254	☑

SBC_SIP: ‘Port From’ is the external port at which SIP signaling will be received from remote devices, generally this will be Port 5060 but may be another port if desired. ‘Port To’ is the port at which MX-E is configured to receive SIP signaling, generally this will always be 5060.

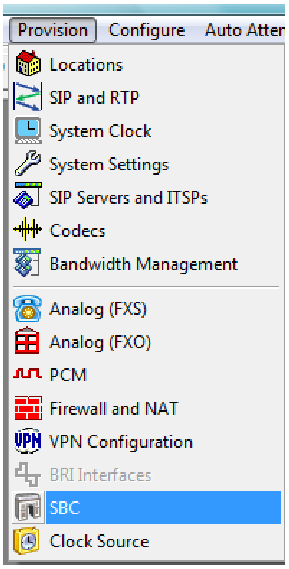
SBC_RTP: The external port range at which RTP packets will be received from remote devices. Many firewalls only support forwarding a port range to the same port range on the internal network, as per the above screenshot. In this example the external port range of 21000-21299 is forwarded to the MX-E system at IP 192.168.0.254:21000-21039.

11.2.2 Remove previous External IPs if necessary

Set the MX-E into bridging mode remove any existing routing mode setting and public address if previously configured. Unplug WAN interface cable if previously used. MX-E removes any public IP, disable and unplug WAN interface if previously used.

11.2.3 Configure SBC

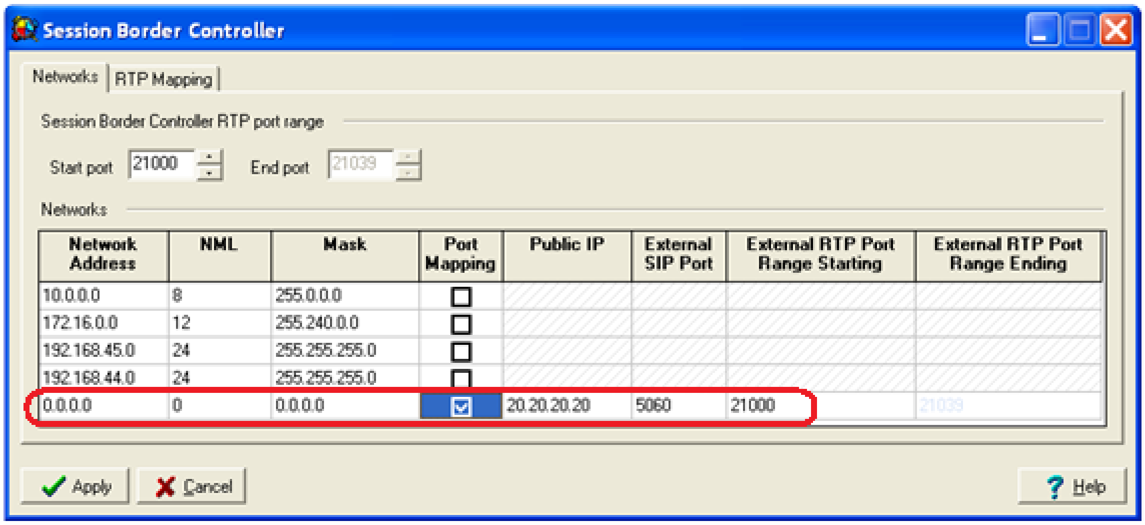
In the MX-E Administrator select *Provision → SBC.*



- Session Border Controller RTP port range – This setting determines the RTP port range used by MX-E on the internal side of network.
- Set check in the *Port Mapping* check box for the relevant Network. Generally this will be the 0.0.0.0/0 network, depending upon your

network architecture other networks may be defined and configured for Port Mapping.

- Set the Public IP to that of the WAN side of Firewall, point C on the diagram shown in Section 11.2. This is the IP address that all external devices will communicate with
- Set external SIP Port to that you configure port forwarding for (usually port 5060)
- Set the 'External RTP Port Range Starting' to correspond with the 'From Port Range' configured for forwarding on the firewall. This is the port range external devices will send RTP packets to

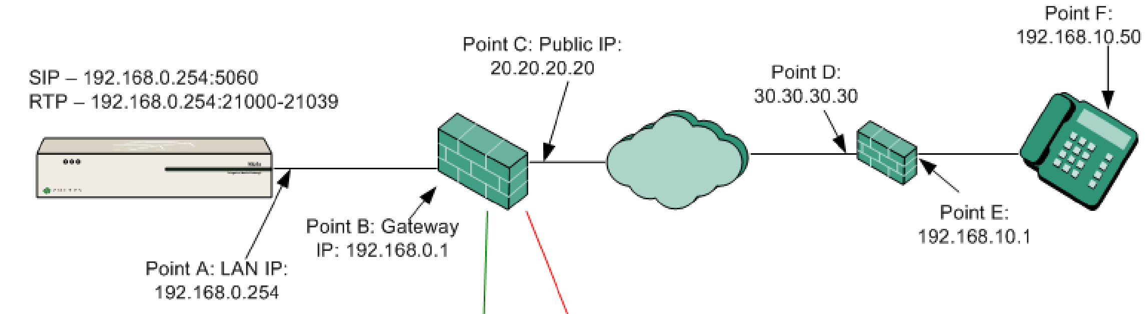


Session Border Controller RTP port range

Start port 21000 End port 21039

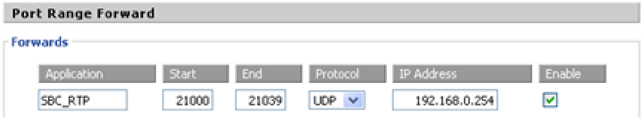
Networks

Network Address	NML	Mask	Port Mapping	Public IP	External SIP Port	External RTP Port Range Starting	External RTP Port Range Ending
10.0.0.0	8	255.0.0.0	□				
172.16.0.0	12	255.240.0.0	□				
192.168.45.0	24	255.255.255.0	□				
192.168.44.0	24	255.255.255.0	□				
0.0.0.0	0	0.0.0.0	☑	20.20.20.20	5060	21000	21039


SIP – 192.168.0.254:5060
RTP – 192.168.0.254:21000-21039
Point C: Public IP: 20.20.20.20
Point D: 30.30.30.30
Point F: 192.168.10.50
Point B: Gateway IP: 192.168.0.1
Point A: LAN IP: 192.168.0.254
Point E: 192.168.10.1

Session Border Controller RTP Port Range
This setting determines the Port range used by the SBC to send and receive Voice packets when communicating to external networks. The setting is independent of the "External RTP Port Range Starting" and Ending parameters although they may be set to the same value if the edge firewall does not support forwarding a Port range to a different Port range.

Edge Firewall - Port Forward settings

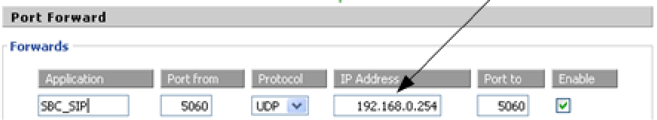


Port Range Forward

Forwards

Application	Start	End	Protocol	IP Address	Enable
SBC_RTP	21000	21039	UDP	192.168.0.254	☑

IP Address of MX

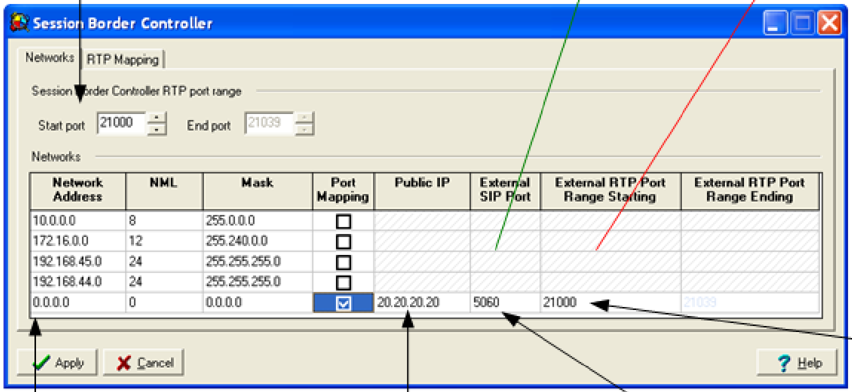


Port Forward

Forwards

Application	Port from	Protocol	IP Address	Port to	Enable
SBC_SIP	5060	UDP	192.168.0.254	5060	☑

External RTP Port Range Starting | Ending: This parameter must match the Port Forwards for RTP configured on the edge Firewall. The port range is independent of the "SBC RTP Port Range" but may be the same port numbers in the case where the edge Firewall does not support forwarding a port range to a different port range. MX will use this parameter to build the information that indicates to the far end what port to send RTP voice packets to.



Session Border Controller

Session Border Controller RTP port range

Start port 21000 End port 21039

Networks

Network Address	NML	Mask	Port Mapping	Public IP	External SIP Port	External RTP Port Range Starting	External RTP Port Range Ending
10.0.0.0	8	255.0.0.0	☐				
172.16.0.0	12	255.240.0.0	☐				
192.168.45.0	24	255.255.255.0	☐				
192.168.44.0	24	255.255.255.0	☐				
0.0.0.0	0	0.0.0.0	☑	20.20.20.20	5060	21000	21039

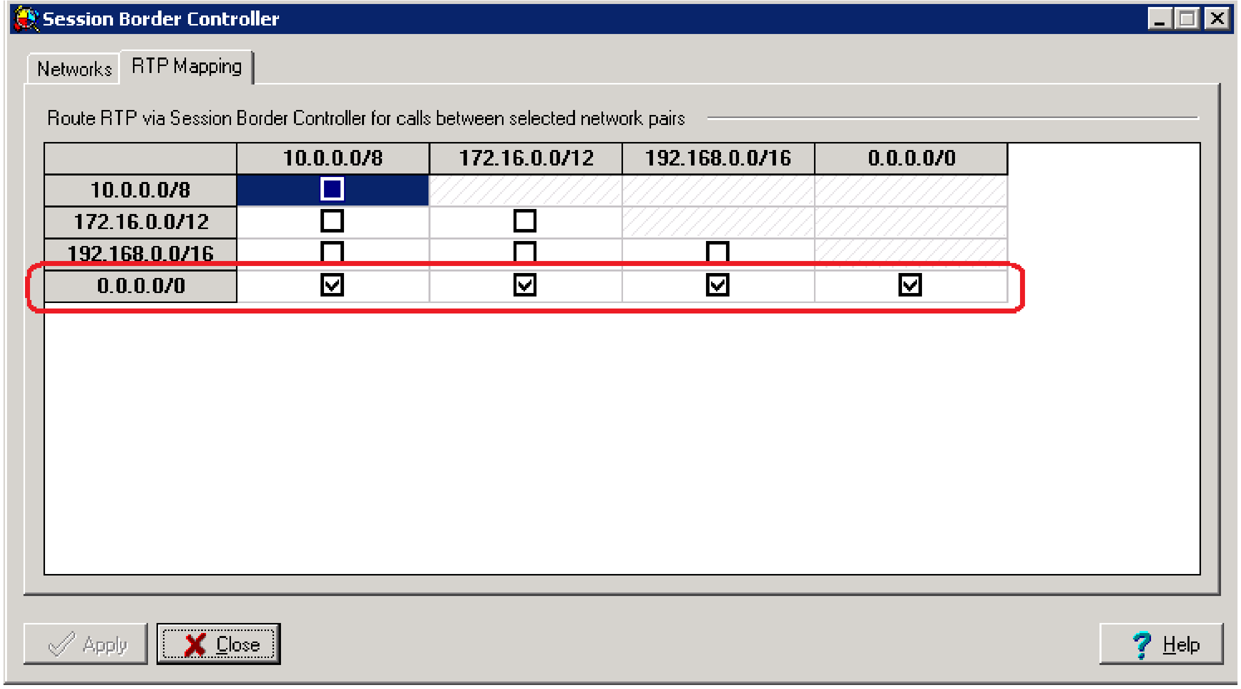
Networks: Port Mapping may be selectively applied to defined Networks. The Default 0.0.0.0/0 network effectively covers all external networks.

Public IP: Set to value of Point C. This IP address will be used as the Layer 7 SIP Source IP address for all SIP packets sent from MX. The NAT function of Firewall will rewrite the IP Layer Source IP to match thus resulting in a valid SIP Packet on the public side of firewall.

External SIP Port: The port to which external IP phones or ITSPs are sending SIP packets. Generally this will be Port 5060 and the edge Firewall will be set to forward Port 5060 to Port 5060 of the IP of MX system.

If a different External SIP Port is used then the external SIP Phones must be provisioned to use the alternate port. For example if the External SIP port is set to 6000, the firewall must forward external Port 6000 to <MX_IP_Address>:5060

Place a check mark in each of the networks you wish to provide Application Layer Gateway (ALG) for the RTP (Voice packets) via SBC to and from the WAN (Outside world).

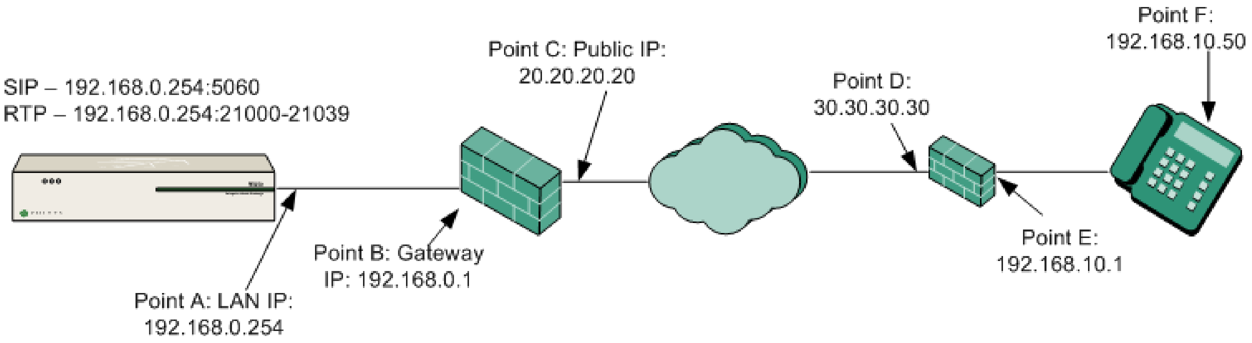


Route RTP via Session Border Controller for calls between selected network pairs

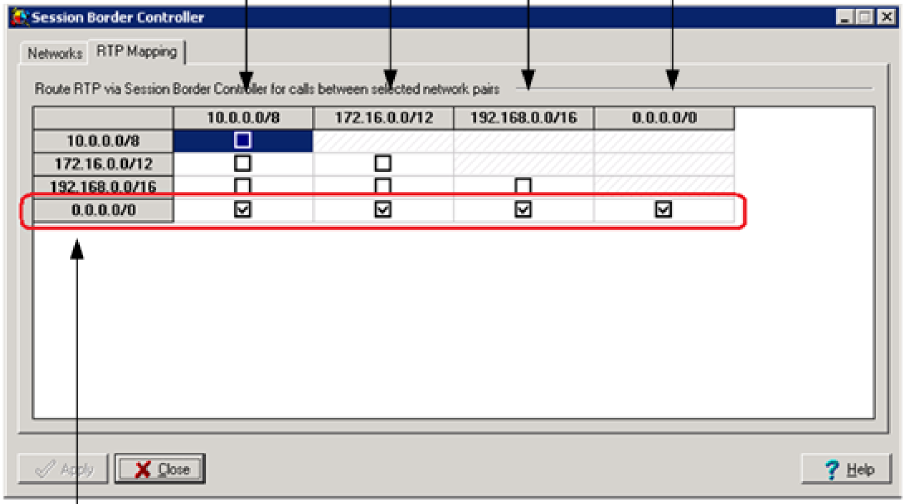
	10.0.0.0/8	172.16.0.0/12	192.168.0.0/16	0.0.0.0/0
10.0.0.0/8	□			
172.16.0.0/12	□	□		
192.168.0.0/16	□	□	□	
0.0.0.0/0	☑	☑	☑	☑

11.3 Routing Mode (MX-E with Public IP directly connected to the internet)

Routing mode is still an available option. Routing mode is when the MX-E is placed in the DMZ with a public IP on one side and a private IP on the other side. The MX-E performs all NAT and routing of packets to the internet. For further information on Routing Mode please refer to Routing_Mode.pdf document number 00000066 from technical support.



Terminating Networks: Calls originating from these networks in the Vertical column that terminate in the Horizontal column will be mapped through the MX when a check mark is placed in the box. If the box is left empty the audio will not be mapped through the MX.



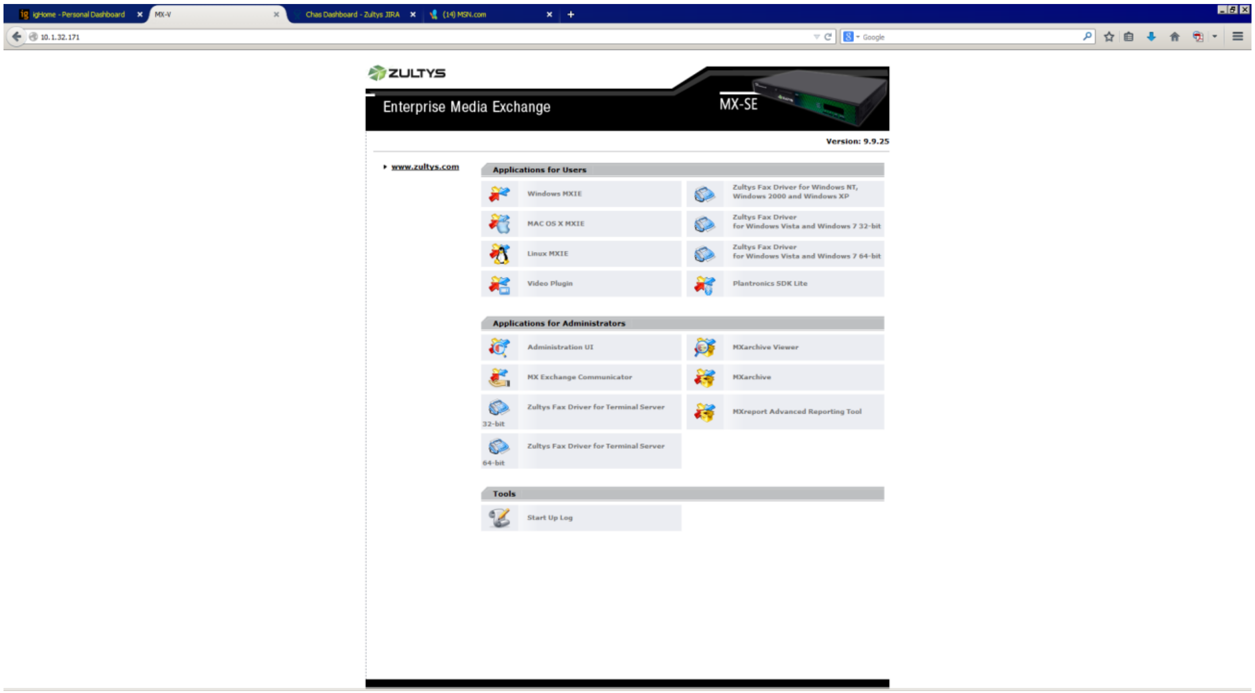
Route RTP via Session Border Controller for calls between selected network pairs

	10.0.0.0/8	172.16.0.0/12	192.168.0.0/16	0.0.0.0/0
10.0.0.0/8	□			
172.16.0.0/12	□	□		
192.168.0.0/16	□	□	□	
0.0.0.0/0	☑	☑	☑	☑

Originating Networks: Calls originating from these networks in the Vertical column that terminate in the Horizontal column will be mapped through the MX when a check mark is placed in the box. If the box is left empty the audio will not be mapped through the MX.

12. Installing the MX-E Administrator User Interface

1. Launch a web browser (Internet Explorer).
2. Enter **192.168.1.100** in the address field to connect to the MX-E (when in console mode)


igHome - Personal Dashboard
MX-V
Chas Dashboard - Zultys JIRA
(14) MSN.com
10.1.32.171
Google
ZULTYS
Enterprise Media Exchange
MX-SE
Version: 9.9.25
www.zultys.com
Applications for Users
Windows MXIE
MAC OS X MXIE
Linux MXIE
Video Plugin
Zultys Fax Driver for Windows NT, Windows 2000 and Windows XP
Zultys Fax Driver for Windows Vista and Windows 7 32-bit
Zultys Fax Driver for Windows Vista and Windows 7 64-bit
Plantronics SDK Lite
Applications for Administrators
Administration UI
MX Exchange Communicator
Zultys Fax Driver for Terminal Server
32-bit
Zultys Fax Driver for Terminal Server
64-bit
MXarchive Viewer
MXarchive
MXreport Advanced Reporting Tool
Tools
Start Up Log

3. Click on Download MX-E Administration UI link and run the installer.
4. Follow the prompts of the Installation Wizard
5. The Installation Shield will automatically install the MX-E Administrator and create a shortcut on your desktop.

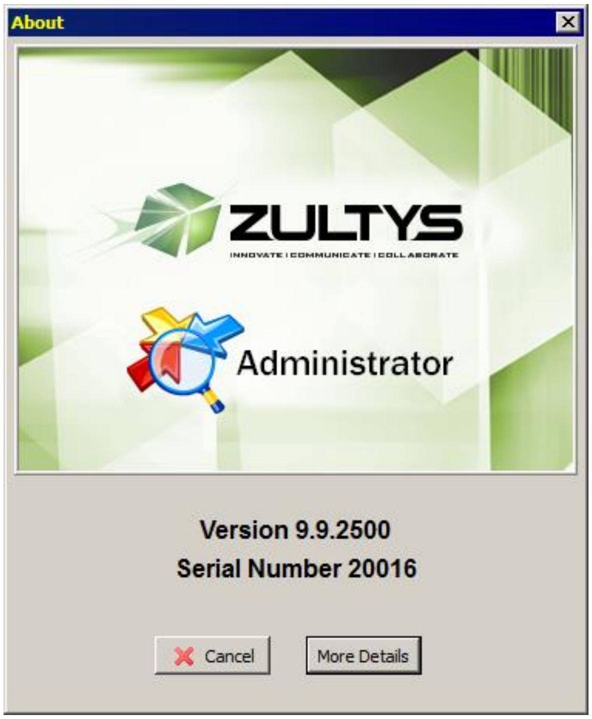
13. Verifying System Software Version

The MX-E's operating system is shipped from the factory with the current build on it. However, due to time spent in the distribution channel it may be necessary to update your MX-E to most current version.

13.2 Obtaining Current software version on your MX-E

1. From the Help pull-down menu, select about
2. The current build of software will be displayed as shown below

NOTE!	**The MX-E system REQUIRES software version 10.0 or greater to operate. Earlier software versions are not compatible with MX-E system.**



Version 9.9.2500

Serial Number 20016

13.3 Obtaining Current software release information

The current version of released software is always available on the Zultys Knowledge Base http://kbs.zultys.com/ (KBS).

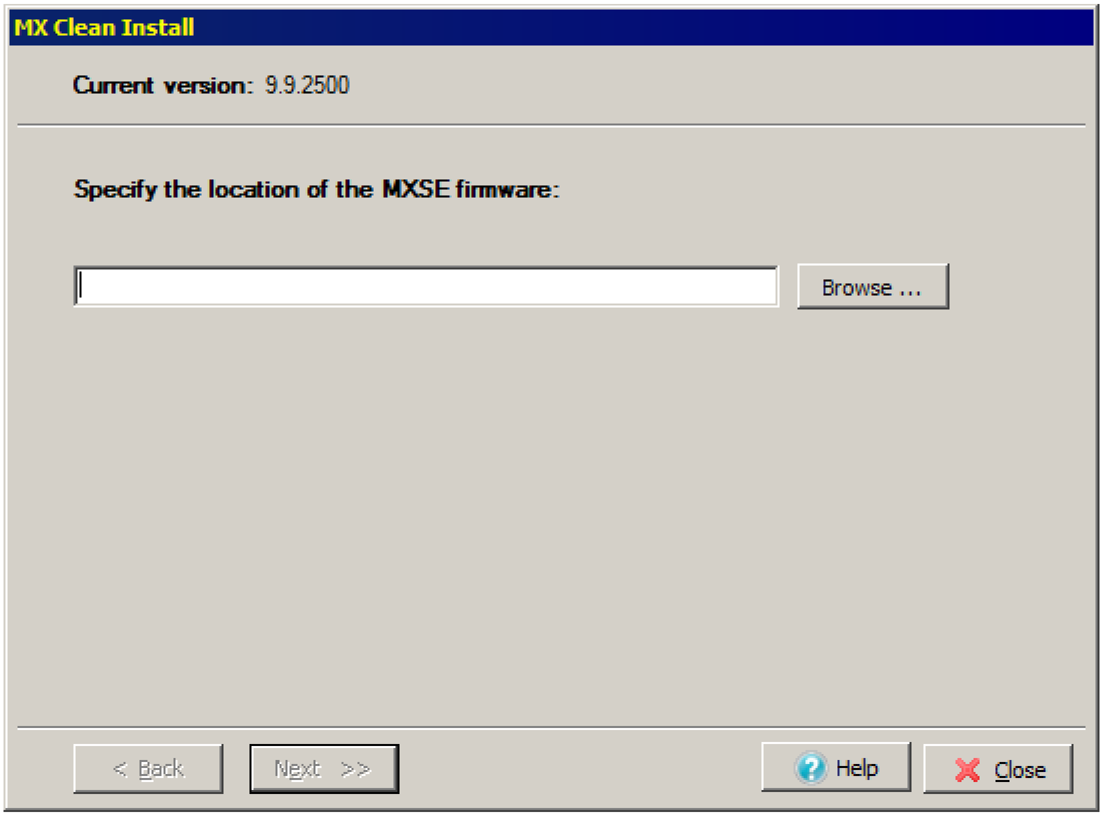
1. Log into the KBS and click on Firmware
2. A list of currently available firmware is listed for the MX-E.
3. Compare the version of software that is currently on your MX-E to the version that is available for download.
    - If they are the same, you don't have to do anything.
    - If they are different, you should download the current version of code and perform a clean install on your MX-E.

14. Performing a Clean Install

A clean install is used to re-initialize a box and to install a specific version of software, while not taking it completely back to the factory defaults. Information that is not reset includes IP Address and NTP server address.

NOTE! Prior to performing a clean install, go to the KBS site and download the "MX-E Manufacturing Image" in the Product Software/Firmware area. Download the .zip file and extract the .tar file to the same folder where the firmware RPM files are stored.

1. Launch the MX-E Administrator user interface
2. From the_Maintenance pull-down menu, select Clean Install.
3. You will be prompted to locate the version of software that you want to install.

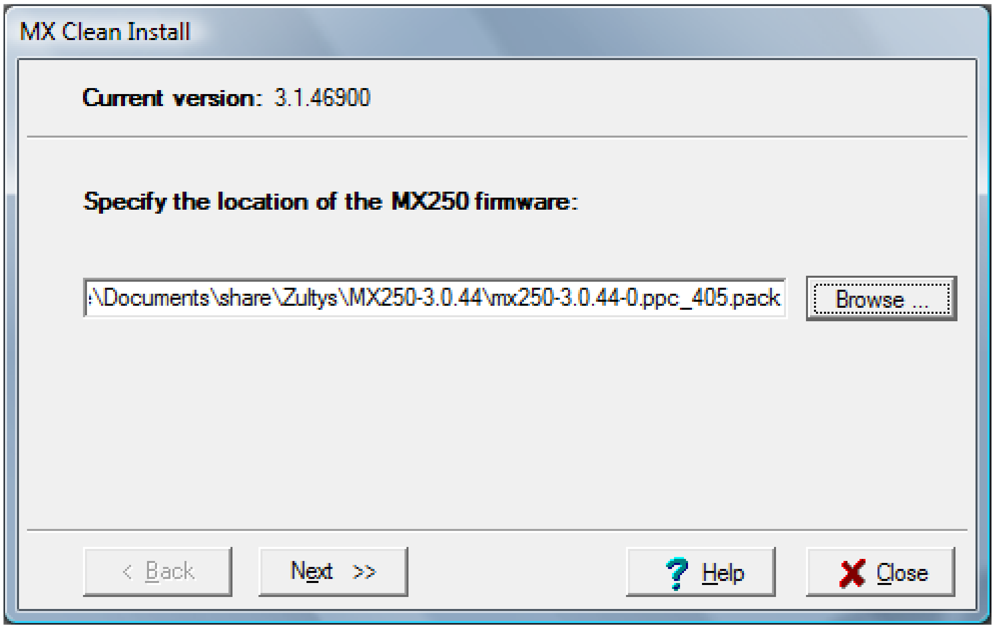


Current version: 9.9.2500

Specify the location of the MXSE firmware:

4. Click on the Browse button to bring up the browse window.

5. Navigate to the files you unzipped in the previous step.



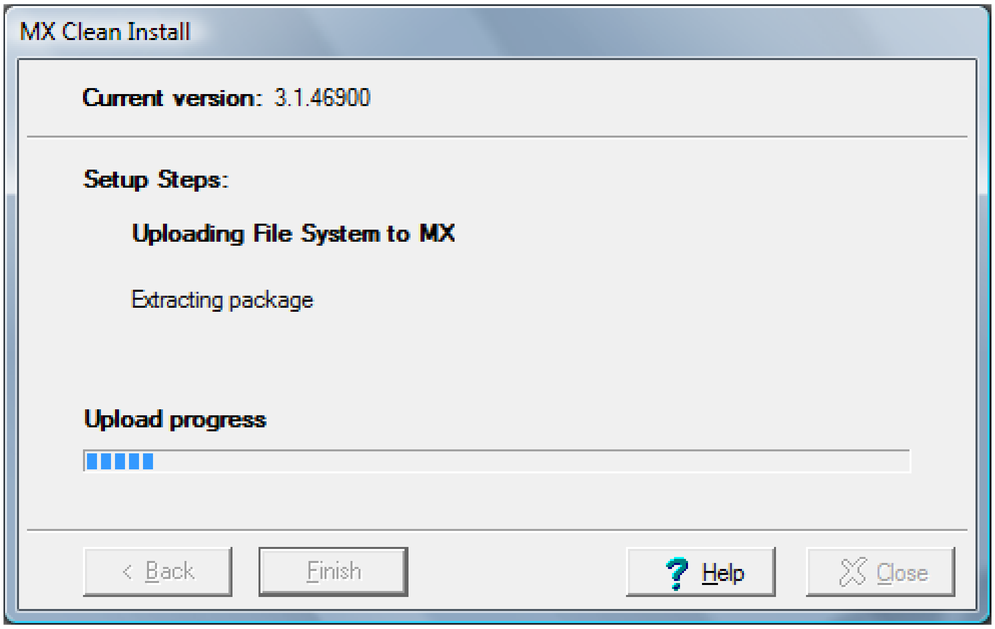
MX Clean Install

Current version: 3.1.46900

Specify the location of the MX250 firmware:

:\Documents\share\Zultys\MX250-3.0.44\mx250-3.0.44-0.ppc_405.pack

6. Choose Next to continue the upgrade process using the specified software.
   This will start the process; all files will be uploaded from your PC to the MX-E that are required for the clean install
7. This results in the MX-E User Properties window with progress bar.



MX Clean Install

Current version: 3.1.46900

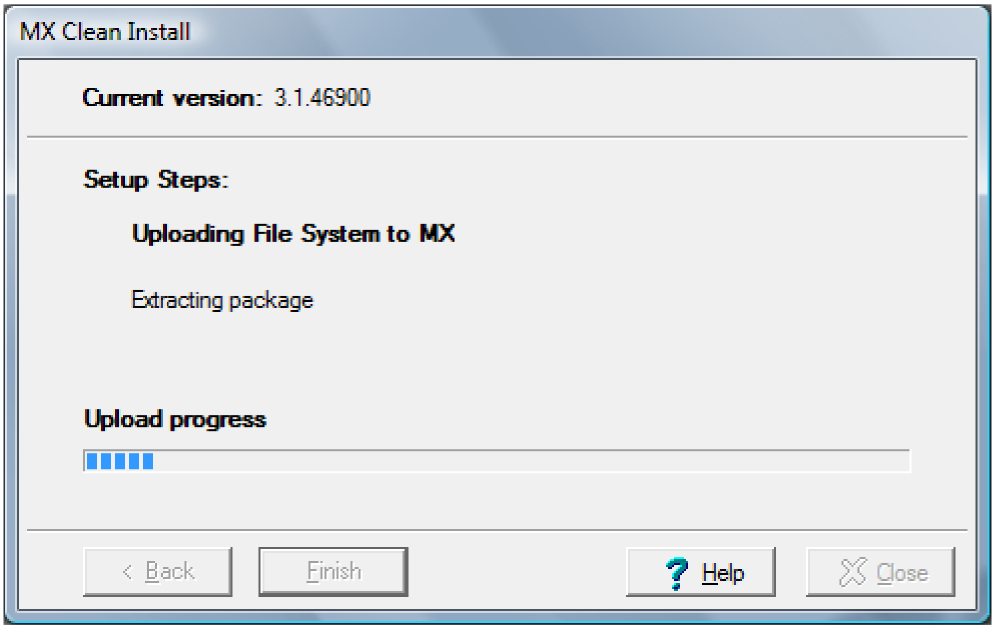
Setup Steps:

Uploading File System to MX

Extracting package

Upload progress

8. This results in the MX-E User Properties window with progress bar.



MX Clean Install

Current version: 3.1.46900

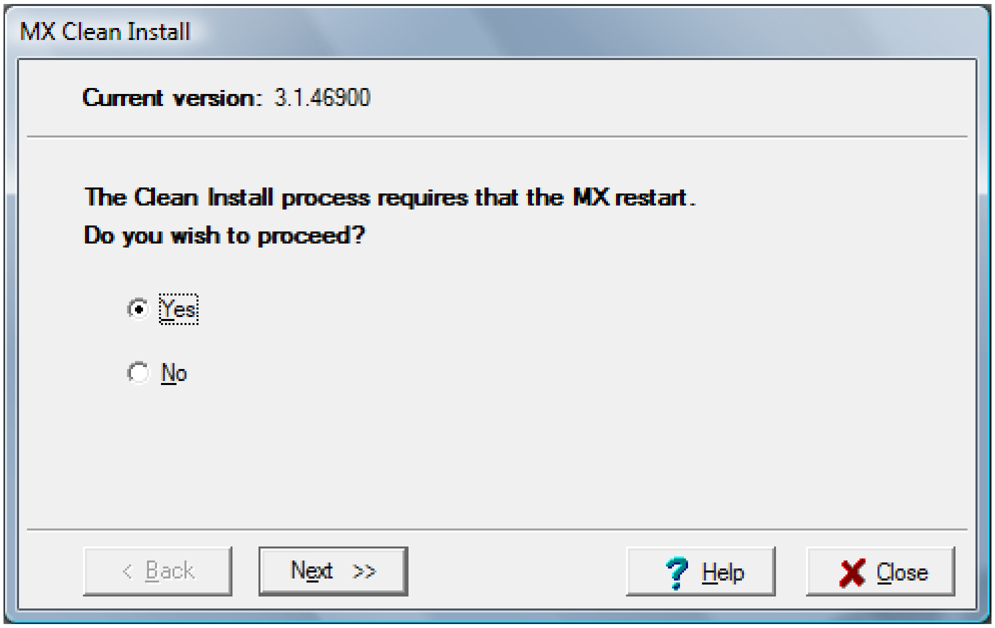
Setup Steps:

Uploading File System to MX

Extracting package

Upload progress

9. When all steps are completed successfully the system you will be prompted to restart the system.



MX Clean Install

Current version: 3.1.46900

The Clean Install process requires that the MX restart.
Do you wish to proceed?

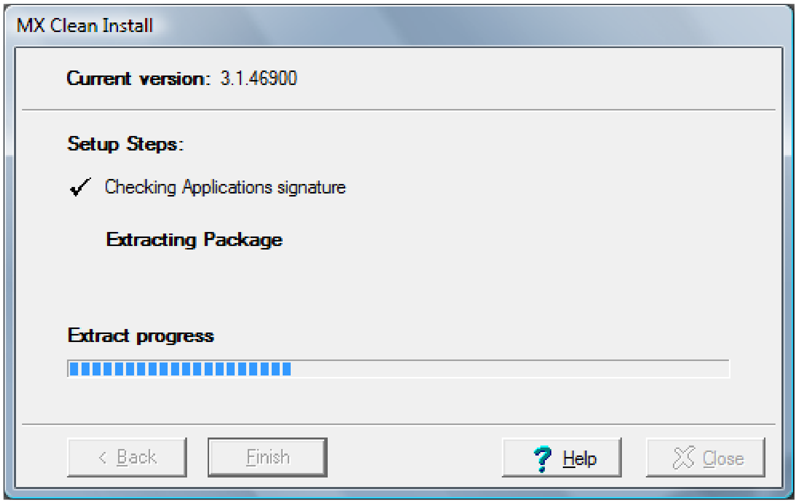
● Yes

○ No

Up to this point, the MX-E continues to operate in normal mode, and calls are still going through. Once you press the system restarts, the system resets and any incoming or outgoing calls are blocked. This is effectively the point of no return.

The first upload step uploads the software to the MX-E.

The MX-E will unpack all files:



MX Clean Install

Current version: 3.1.46900

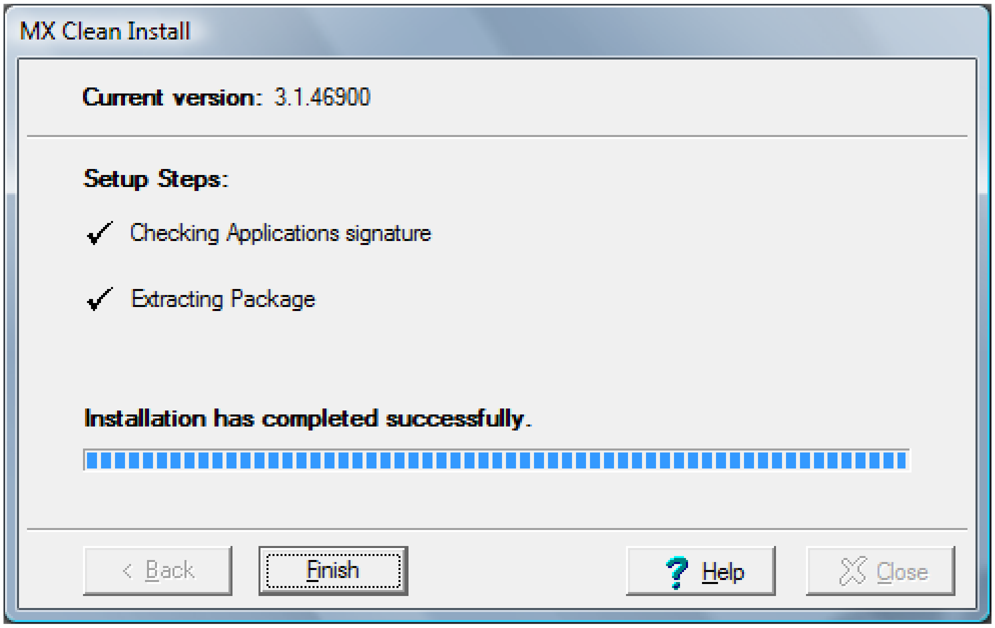
Setup Steps:

✓ Checking Applications signature

Extracting Package

Extract progress

Once all files are unpacked the MX-E will start to install the default system. The system will be off line during the install:



MX Clean Install

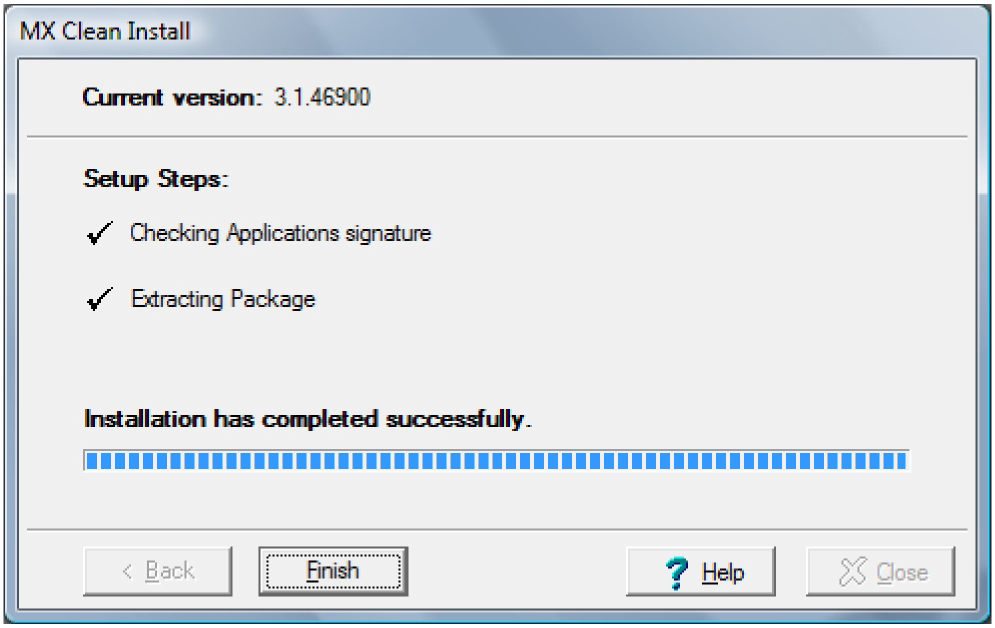
Current version: 3.1.46900

Setup Steps:

✓ Checking Applications signature

✓ Extracting Package

Installation has completed successfully.



MX Clean Install

Current version: 3.1.46900

Setup Steps:

✓ Checking Applications signature

✓ Extracting Package

Installation has completed successfully.

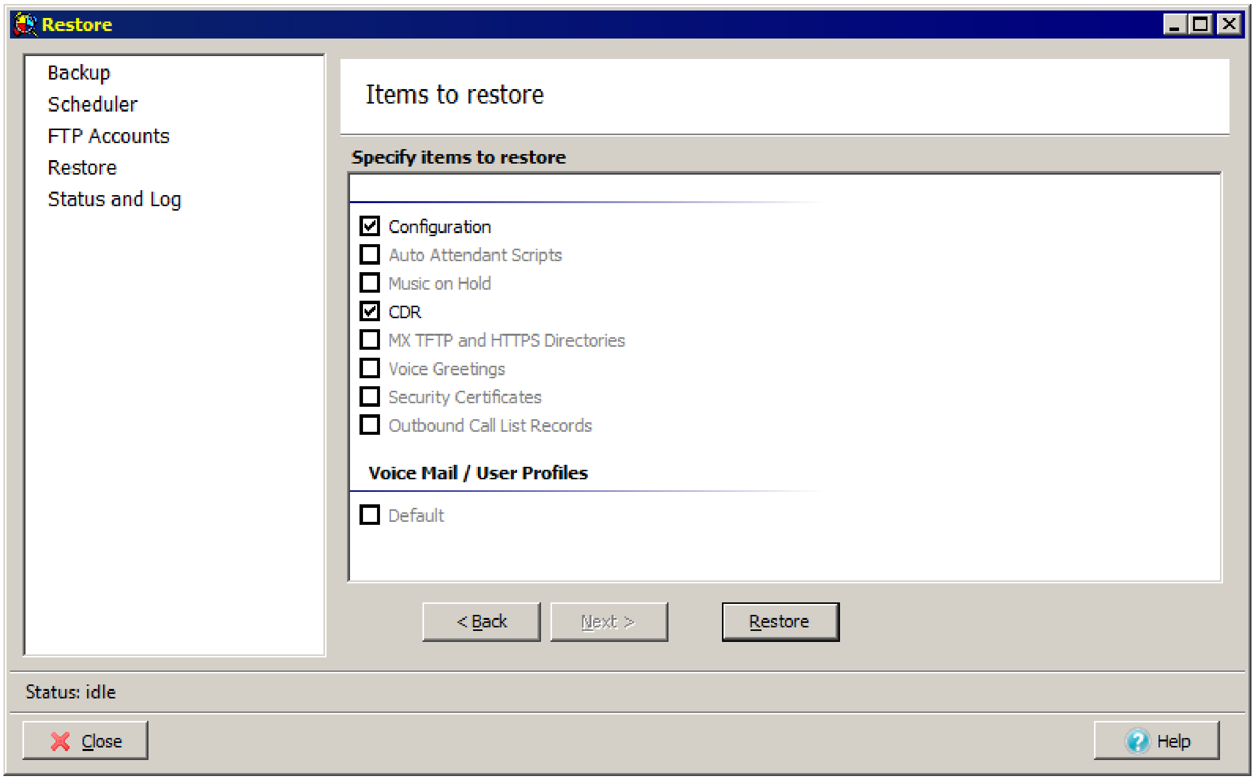
The system can take anywhere from 2 minutes to 3 minutes to restart, depending on the size of the database

Like before, you will be prompted to update your MXIE and MX-E Administrator.

***Note**: Do not try to update your MXIE and your MX-E Administrator at the same time.*

14.2 Restoring a Saved Configuration

1. Click on "Maintenance" and select "Restore"
2. Check the box next to "Configuration"



Specify items to restore

☑ Configuration
□ Auto Attendant Scripts
□ Music on Hold
☑ CDR
□ MX TFTP and HTTPS Directories
□ Voice Greetings
□ Security Certificates
□ Outbound Call List Records

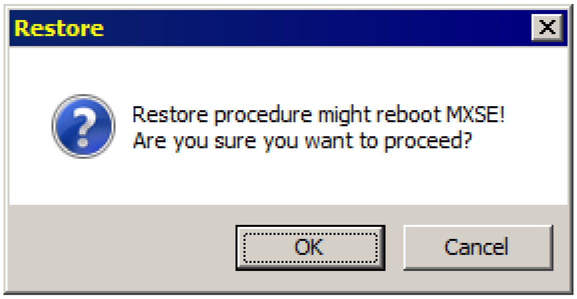
Voice Mail / User Profiles

□ Default

Status: idle

Note: You can restore the Configuration or you can restore everything else. To completely restore your configuration, you must repeat this process twice. After each restore, the system will restart.

3. For "Location" Browse to the location where you backed up the configuration
4. Then Click "Restore"
5. A pop-up screen will appear. You must click on yes to continue.



Restore procedure might reboot MXSE!
Are you sure you want to proceed?

6. Once the restore is complete, you will lose connection with the MX-E for about two minutes as the system restarts.

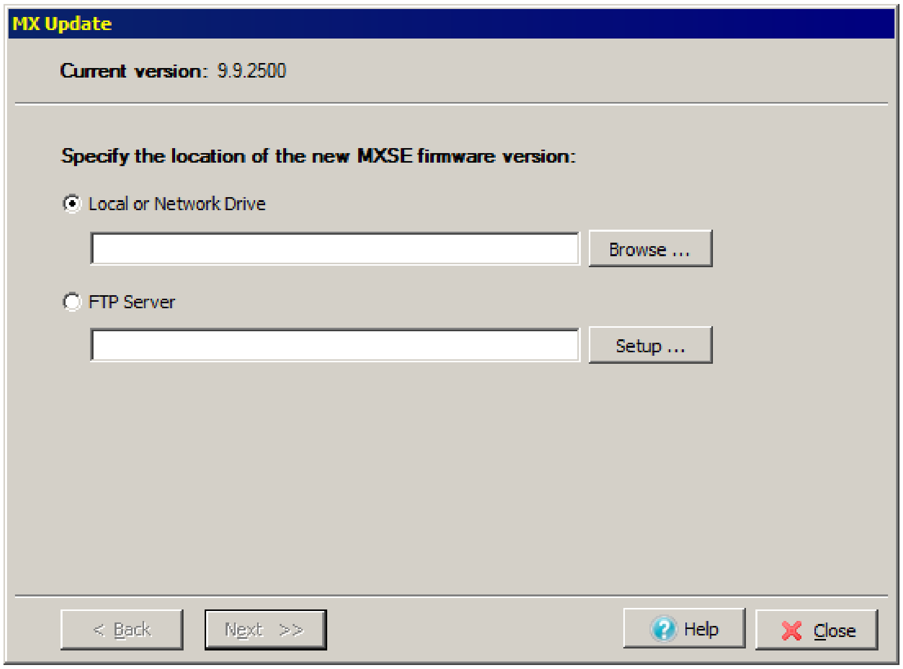
7. Once completed, you will need to repeat the process to restore the rest of the system parameters

15. Updating the software on the MX-E

Periodically, it is necessary to update the software on a system. Zultys offers two methods of performing this task. The first is to update the software to a specific level and the second is to perform a "clean" installation of a specific version of software. Updating software allows you to go from version of software to a newer version gracefully. Meaning that if you update the software on your system the configuration database for a specific system is updated as a part of the update sequence. The other method, the clean installation, allows you to go from one version of software to the next, but also cleans out much of the configuration database in the process. The other advantage of the "clean" installation is that it will allow you to install any version of software on the box.

15.2 Updating the system software version:

1. From the "Maintenance" menu select "Update Firmware"
2. The Update window appears.



MX Update

Current version: 9.9.2500

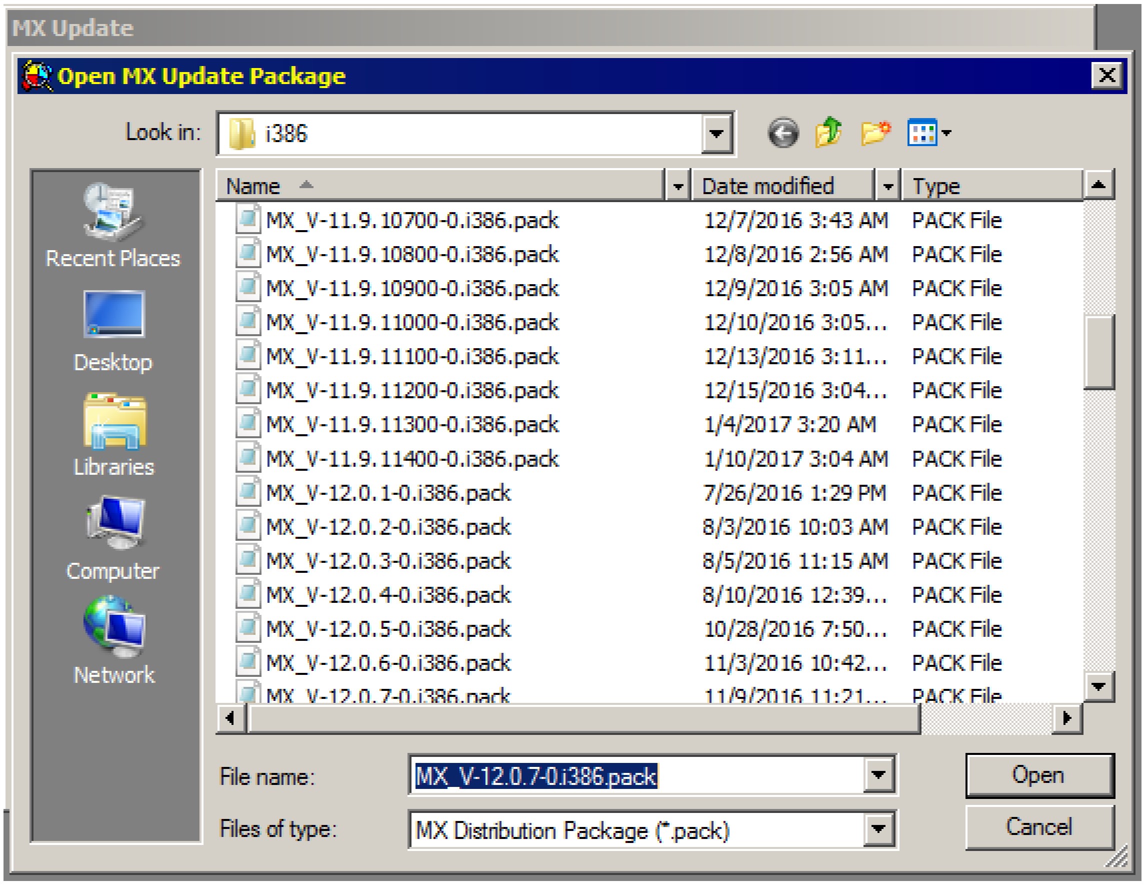
Specify the location of the new MXSE firmware version:

● Local or Network Drive

○ FTP Server

3. Click on the "Browse" button

4. Click on the Browse button to bring up the browse window.



Look in: i386

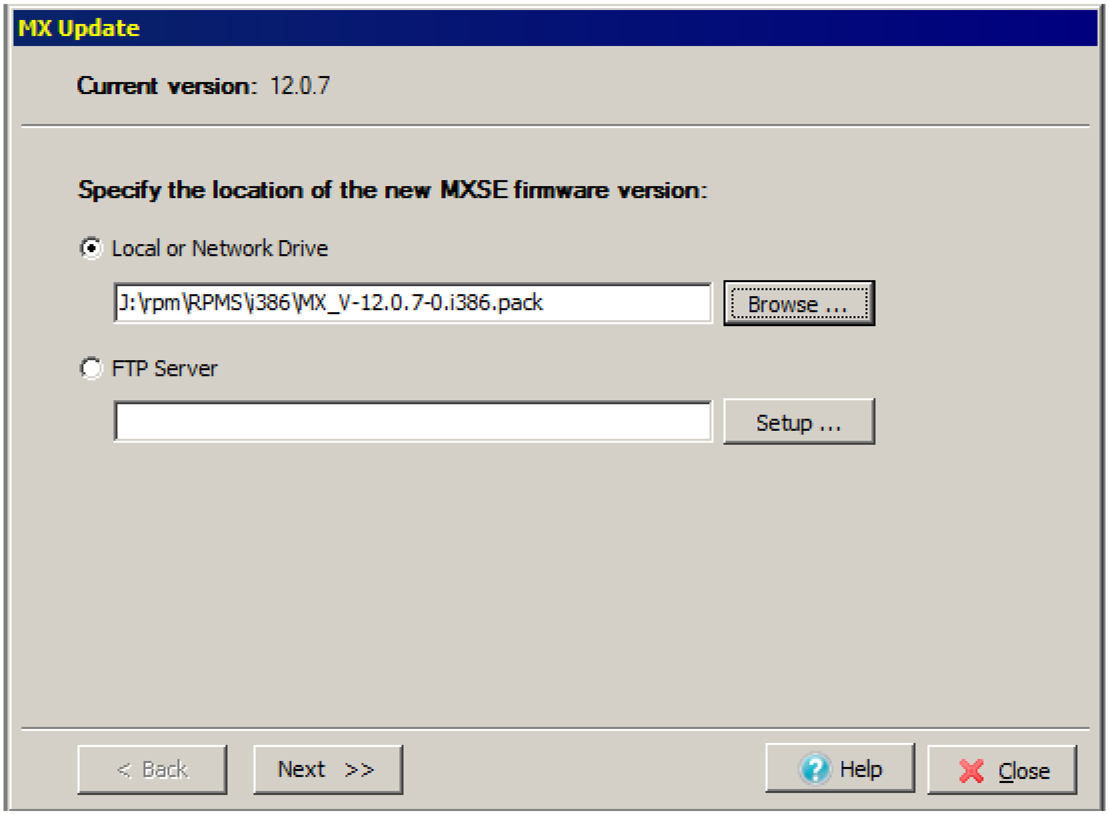
Name	Date modified	Type
MX_V-11.9.10700-0.i386.pack	12/7/2016 3:43 AM	PACK File
MX_V-11.9.10800-0.i386.pack	12/8/2016 2:56 AM	PACK File
MX_V-11.9.10900-0.i386.pack	12/9/2016 3:05 AM	PACK File
MX_V-11.9.11000-0.i386.pack	12/10/2016 3:05...	PACK File
MX_V-11.9.11100-0.i386.pack	12/13/2016 3:11...	PACK File
MX_V-11.9.11200-0.i386.pack	12/15/2016 3:04...	PACK File
MX_V-11.9.11300-0.i386.pack	1/4/2017 3:20 AM	PACK File
MX_V-11.9.11400-0.i386.pack	1/10/2017 3:04 AM	PACK File
MX_V-12.0.1-0.i386.pack	7/26/2016 1:29 PM	PACK File
MX_V-12.0.2-0.i386.pack	8/3/2016 10:03 AM	PACK File
MX_V-12.0.3-0.i386.pack	8/5/2016 11:15 AM	PACK File
MX_V-12.0.4-0.i386.pack	8/10/2016 12:39...	PACK File
MX_V-12.0.5-0.i386.pack	10/28/2016 7:50...	PACK File
MX_V-12.0.6-0.i386.pack	11/3/2016 10:42...	PACK File
MX_V-12.0.7-0.i386.pack	11/9/2016 11:21...	PACK File

File name: MX_V-12.0.7-0.i386.pack

Files of type: MX Distribution Package (*.pack)

5. Navigate to the directory where you stored the latest software image
6. Open the image by clicking on the “pack” file and clicking Open

7. The software version file browser window updates.



MX Update

Current version: 12.0.7

Specify the location of the new MXSE firmware version:

● Local or Network Drive

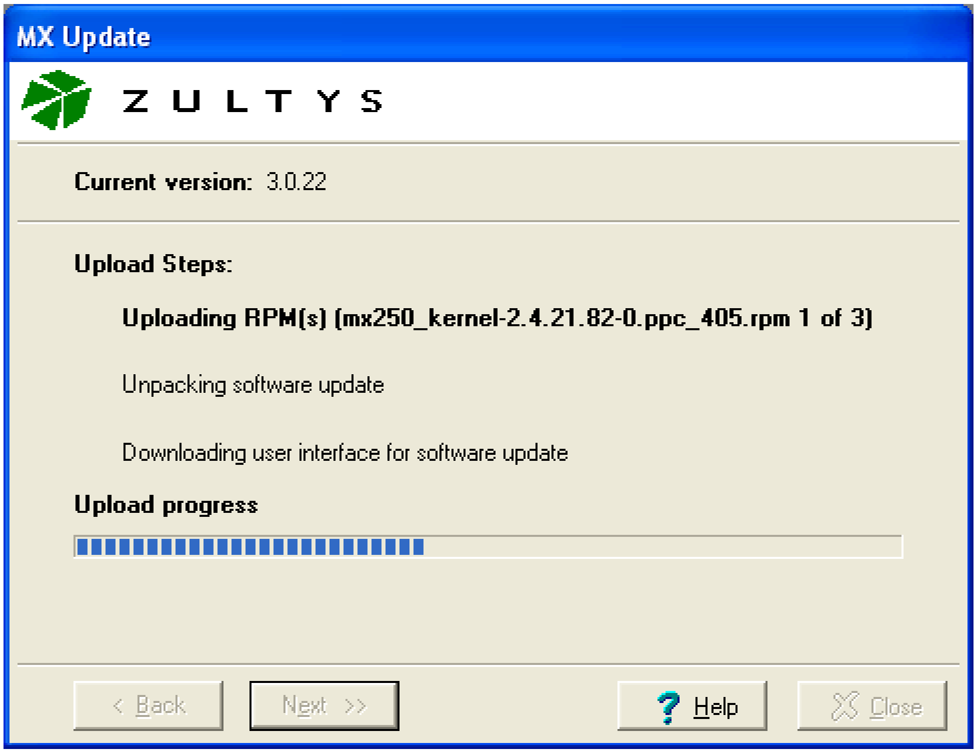
J:\rpm\RPMS\i386\MX_V-12.0.7-0.i386.pack

○ FTP Server

Software images are stored as multiple Linux RPM files to maintain portability and simplify upgrades. The Linux Operating System running on the MX-E includes an rpm utility that manages, installs, upgrades and removes RPM software packages. The RPM files that make up an upgrade package are listed in the .pack file.

8. Choose Next to continue the upgrade process using the specified software

9. This results in the MX-E User Properties window with progress bar.



Current version: 3.0.22

Upload Steps:

Uploading RPM(s) (mx250_kernel-2.4.21.82-0.ppc_405.rpm 1 of 3)

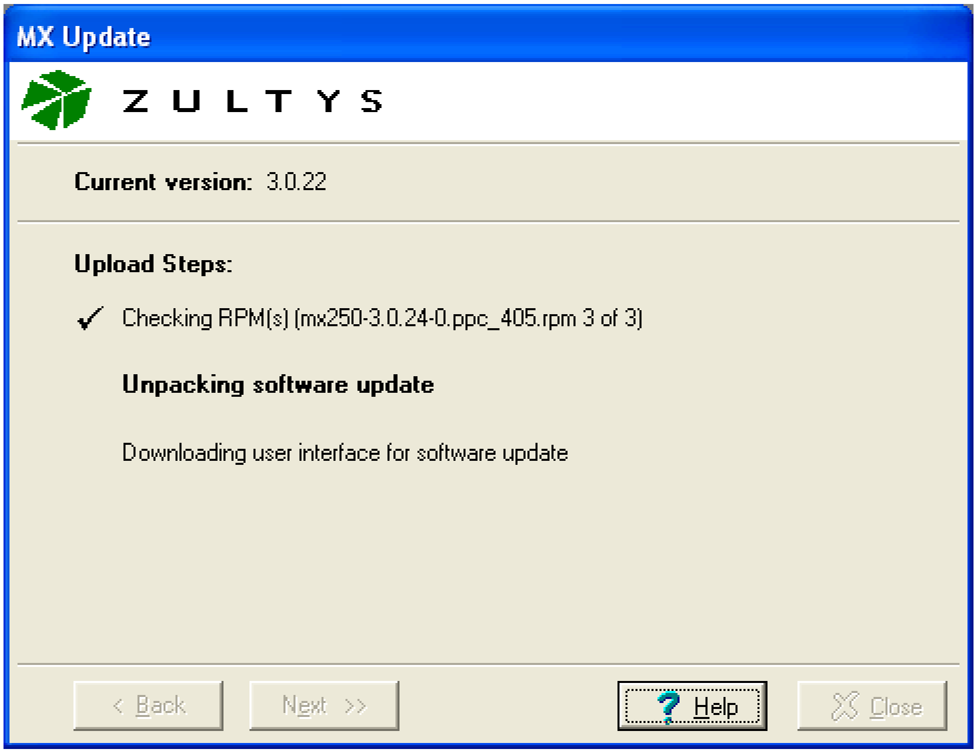
Unpacking software update

Downloading user interface for software update

Upload progress

The first upload step uploads the software to the MX-E.

The second upload step unpacks and installs the software into the proper directories.



MX Update

Current version: 3.0.22

Upload Steps:

✓ Checking RPM(s) (mx250-3.0.24-0.ppc_405.rpm 3 of 3)

Unpacking software update

Downloading user interface for software update

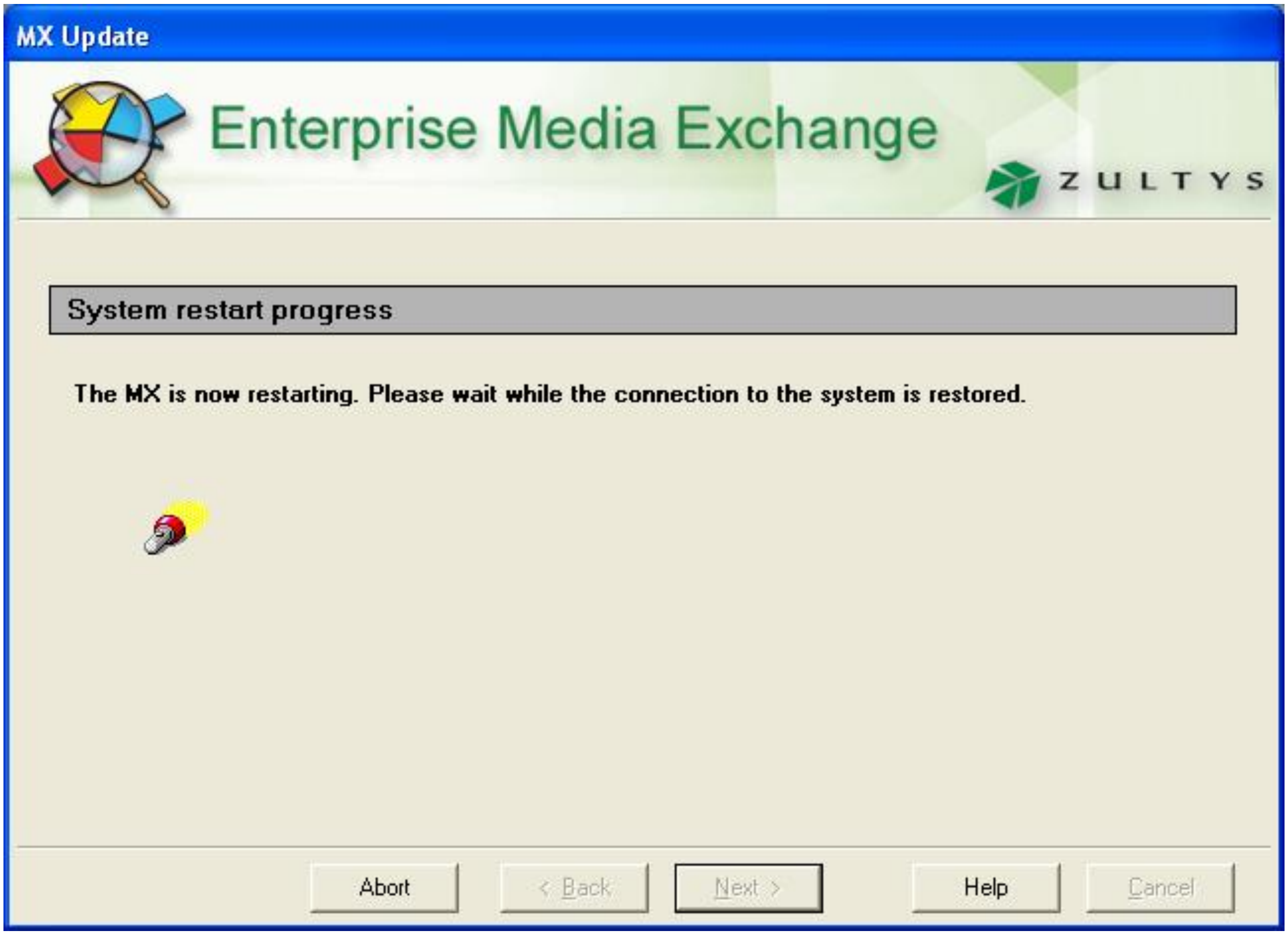
The third step downloads the new Administrator GUI onto your PC from the MX-E

The running step will be shown in **Bold Print**

As each step completes, the Bold Text will go back to normal and a check mark will appear at the beginning of the line to indicate completion.

When all steps are completed successfully the system will restart

This takes you to the System restart progress window.



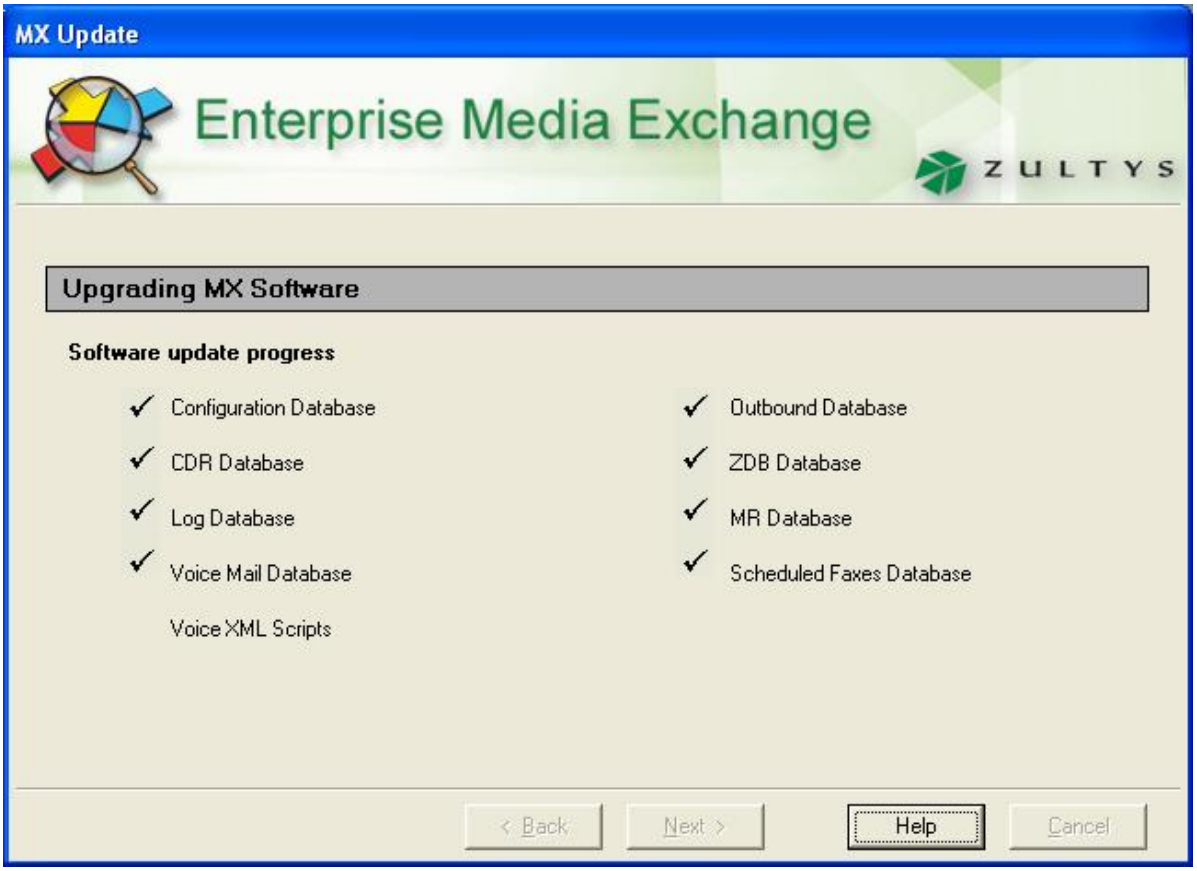
System restart progress

The MX is now restarting. Please wait while the connection to the system is restored.

Up to this point, the MX-E continues to operate in normal mode, and calls are still going through. Once you press the system restarts, the system resets and any incoming or outgoing calls are blocked. This is effectively the point of no return (other than rolling back to the previous software release).

The system can take anywhere from 2 minutes to 3 minutes to restart, depending on the size of the database

After system restart is complete, the database will be upgraded.



Upgrading MX Software

Software update progress

✓ Configuration Database

✓ CDR Database

✓ Log Database

✓ Voice Mail Database

Voice XML Scripts

✓ Outbound Database

✓ ZDB Database

✓ MR Database

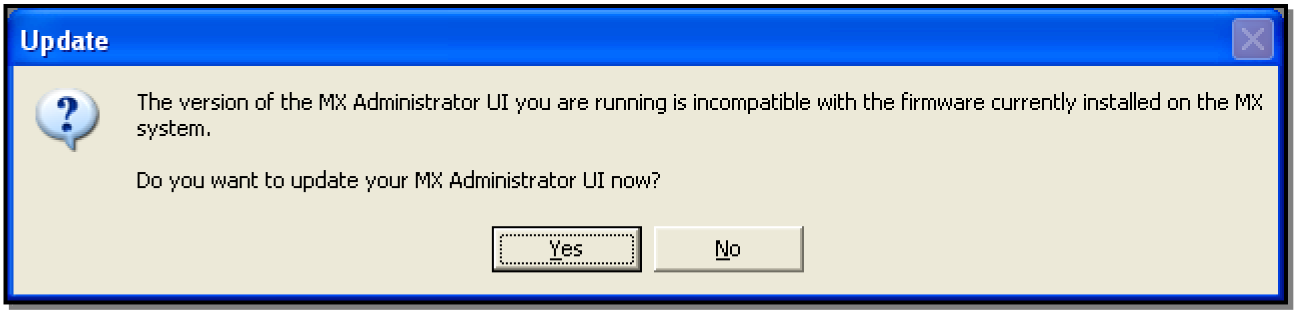
✓ Scheduled Faxes Database

Click Next when the button goes active to complete the MX-E upgrade process

15.3 Upgrading the MX-E Administrator User Interface

As the MX-E Administrator and MXIE are tied to the specific version of software on the box, the next step is to update this software.

1. After Clicking Finish, the application will automatically prompt you to upgrade your Administrative User Interface
2. The MX-E Administrator upgrade window appears.

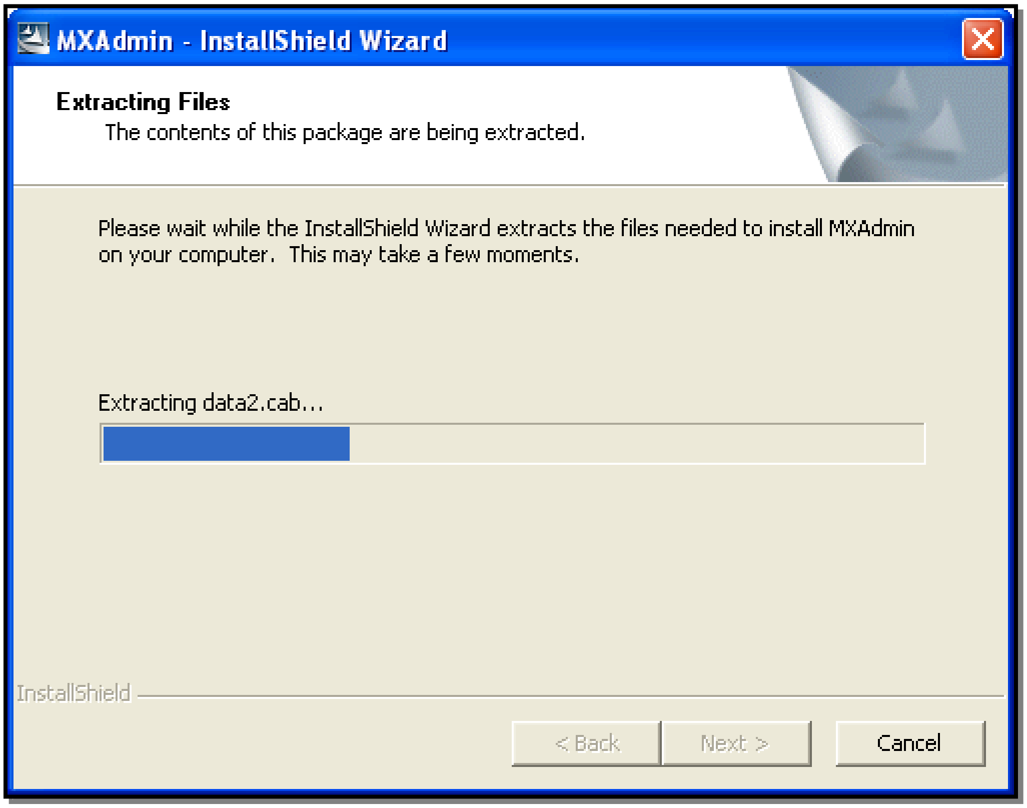


Update

The version of the MX Administrator UI you are running is incompatible with the firmware currently installed on the MX system.

Do you want to update your MX Administrator UI now?

1. Click Yes to run InstallShield and the MX-E Administrator upgrade program.



MXAdmin - InstallShield Wizard

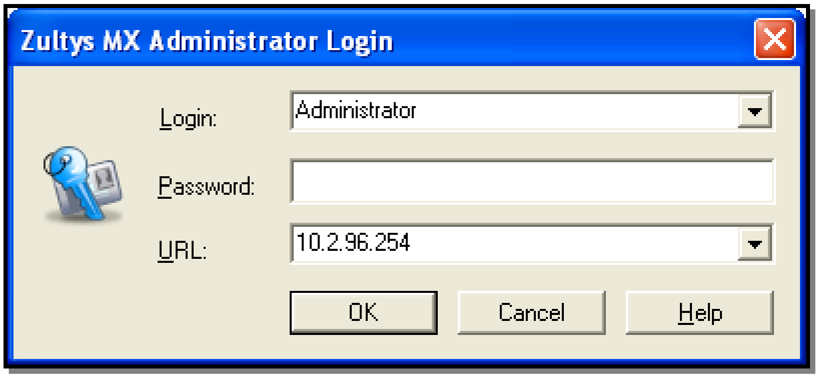
Extracting Files

The contents of this package are being extracted.

Please wait while the InstallShield Wizard extracts the files needed to install MXAdmin on your computer. This may take a few moments.

Extracting data2.cab...

3. When complete, the MX-E Administrator login appears.



Login: Administrator

URL: 10.2.96.254

4. Login as normal to Administer the MX-E

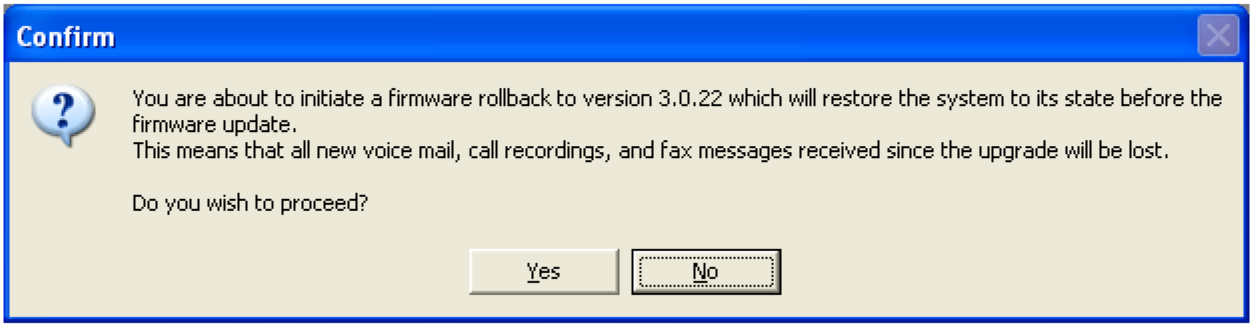
If you start the MXIE, you will also be prompted to upgrade it to the latest MX-E compatible version. The MXIE also uses InstallShield and follows the same upgrade procedure as the MX-E Administrator.

15.4 Performing a System Rollback:

The MX-E keeps two images of software on the system. This can be thought of as the active version and the previous version. Rolling back to the previous version of software is largely the same as a graceful update, but it is the only way that you can go to a previous version of software while keeping the configuration of the system.

Rolling back to the previous version:

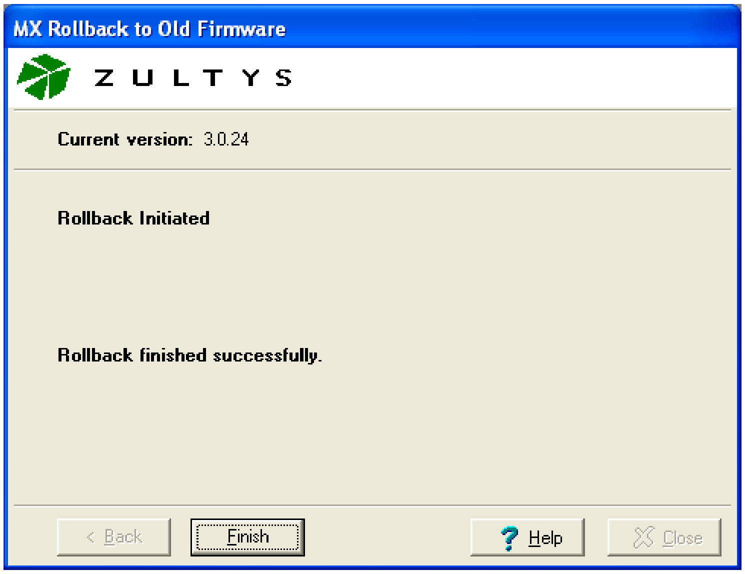
1. From the Maintenance pull-down menu, select Rollback to Old Software
2. Click Next.
3. Select Yes



You are about to initiate a firmware rollback to version 3.0.22 which will restore the system to its state before the firmware update.
This means that all new voice mail, call recordings, and fax messages received since the upgrade will be lost.

Do you wish to proceed?

You will see a progress screen to let you know that the rollback has begun.



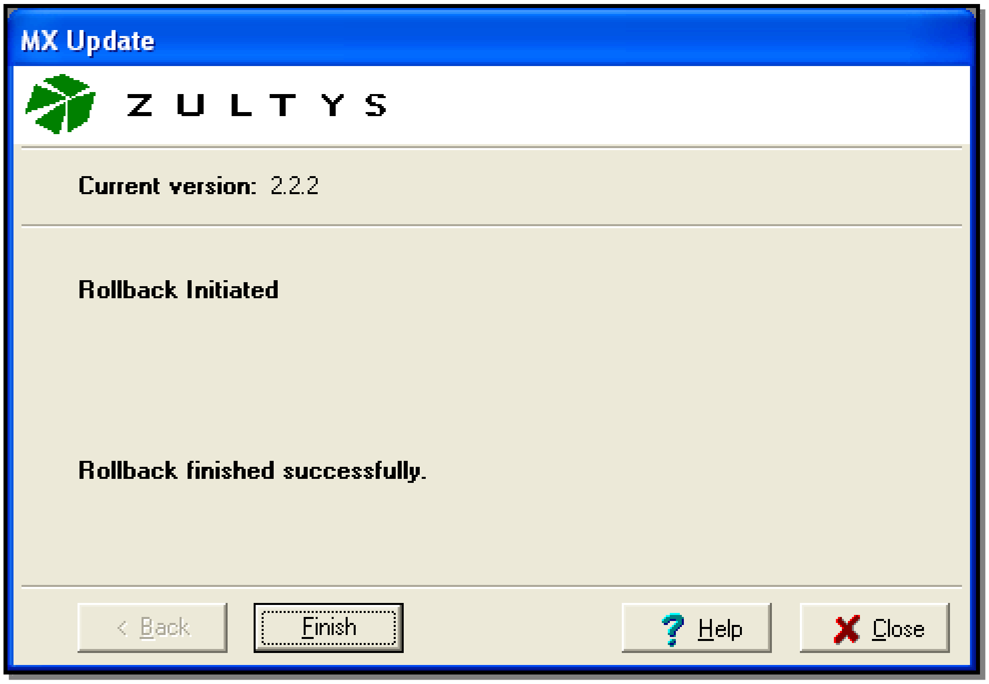
MX Rollback to Old Firmware

Current version: 3.0.24

Rollback Initiated

Rollback finished successfully.

Once the rollback has completed, you will be prompted to click Finish.



MX Update

Current version: 2.2.2

Rollback Initiated

Rollback finished successfully.

Like before, you will be prompted to update any MX-E Administrator or MXIE that you have running.

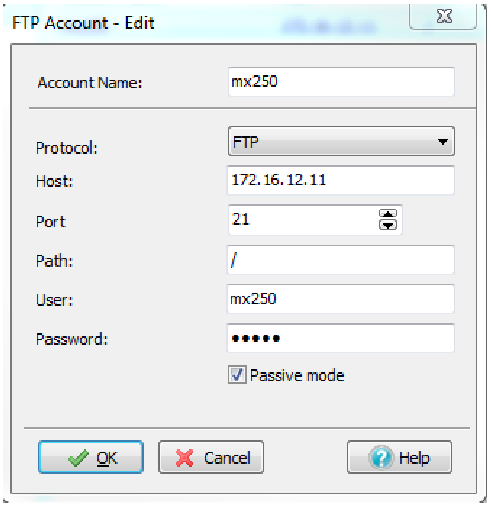
16. Backup and Restore:

Backup and restore allows the system administrator to create an archive copy a systems configuration, the voicemail and the faxes associated with a specific system. There are two methods of backing a system up: either a manual backup or a scheduled backup. After a system is backed up, it represents a specific correlation between the system software and the database that is configured on that software. For this reason, any attempt to restore a configuration to a system running a different operating system will fail.

16.2 FTP Accounts

The MX-E will use FTP/FTPs/SFTP for all automatic backups, and the same FTP/FTPs/SFTP accounts can be used for manual backups. Only manual backups can be backed up to a local server drive via the MX-E Administrator.

When using SFTP or FTPs remember to upload any required SSL certificates under Certificate Management to the MX-E.



FTP Account - Edit

Account Name: mx250

Protocol: FTP

Host: 172.16.12.11

Port 21

Path: /

User: mx250

Password: •••••

☑ Passive mode

Name: Account name used to reference this account

Protocol:

- FTP
- FTPs
- SFTP

Host: IP or URL for the FTP Server

Port: Port Used

Path: Path on FTP Server

User: Username

Password: Password

Passive Mode: Enable Passive Mode

16.2.1 FTP

Standard FTP is supported by the MX-E, and does not require any certificates to be loaded to the MX-E.

When configuring the MX-E to use FTP, use port 21.

16.2.2 SFTP

SFTP ("SSH FTP") is based on SSH (Secure Shell) version 2. It uses the same communication channels and encryption mechanisms as SSH. SFTP is fully supported by the MX-E starting with Version 8 of the MX-E Firmware. Valid certificates must be manually loaded to the MX-E.

16.2.3 FTPs

FTPS ("FTP over SSL") is based on the legacy FTP protocol, with an additional SSL/TLS encryption layer. There are several implementations of FTPS, including those with "implicit SSL" where a distinct service listens for encrypted connections, and "explicit SSL" where the connection runs over the same service and is switched to an encrypted connection by a protocol option. In addition, there are several potential combinations of what parts of an FTPS connection are actually being encrypted, such as "only encrypted login" or "encrypted login and data transfer". FTPs is fully supported by the MX-E starting with Version 8 of the MX-E Firmware. Valid certificates must be manually loaded to the MX-E.

When configuring the MX-E to use FTPs, use port 21.

16.3 Backup

The MX-E offers several different back up options, each of which can be configured to create a backup procedure to safe guard your system.

- Manual
- Automatic
  - Daily
  - Weekly
  - Monthly

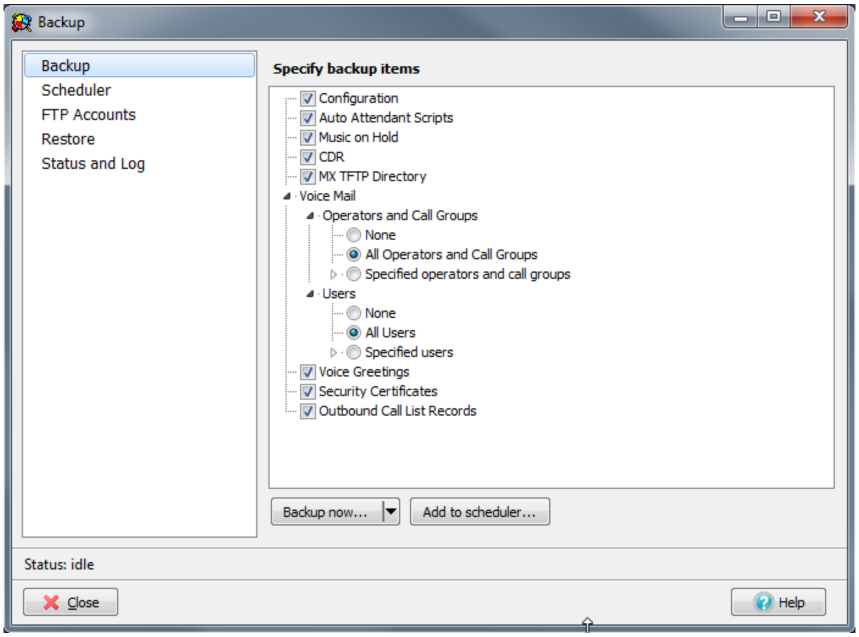
⚠ Backups on the MX-E are version specific that is if you back up a MX-E you must restore it back to the same version of MX-E. If you try to restore to a different version a warning will let you know you cannot restore to this MX-E.

16.3.1 Manual Backup

Manual back is used to manually back up your system. This must be done manually each time and will be stored on a drive or FTP Server you have access to from the pc running the MX-E Administrator. This drive can be a local drive to the pc or a network drive.

To manually back up your system go to *Maintenance →Backup* in the MX-E Administrator.

On the Backup Navigation option, select the item(s) you wish to manually backup by placing a checkmark in the box next to the item(s) you wish to backup. You may expand the selection options by clicking on the arrows to the right of some of the selections that may be expanded.

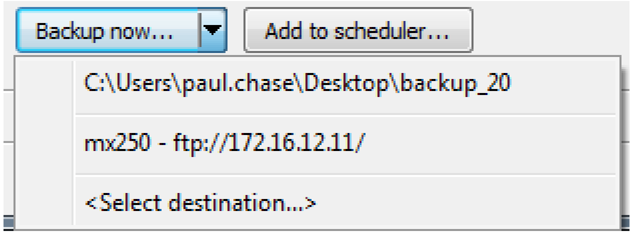


Specify backup items

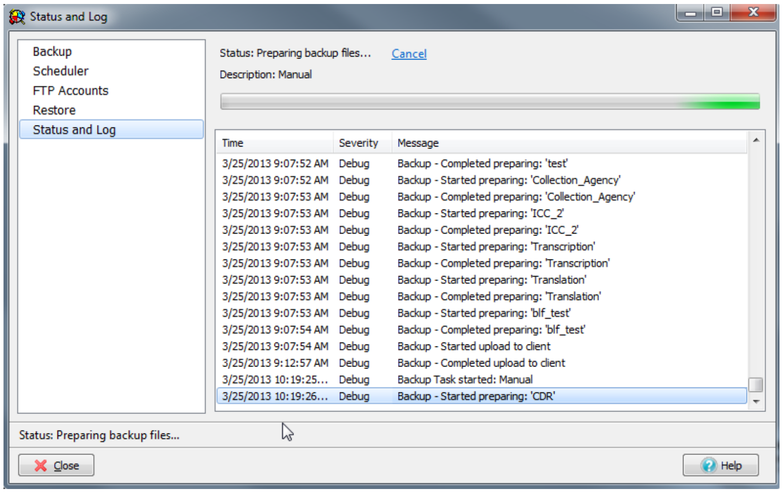
- ☑ Configuration
- ☑ Auto Attendant Scripts
- ☑ Music on Hold
- ☑ CDR
- ☑ MX TFTP Directory
- Voice Mail
  - Operators and Call Groups
    - ○ None
    - ● All Operators and Call Groups
    - ○ Specified operators and call groups
  - Users
    - ○ None
    - ● All Users
    - ○ Specified users
- ☑ Voice Greetings
- ☑ Security Certificates
- ☑ Outbound Call List Records

Status: idle

Once you have identified all the selections you wish to manually backup, click the backup now button at the bottom of the screen, or if you have manually backed up the system or a have FTP server already defined you may click the down arrow to select one of the previously defined locations, or define a new location.


Backup now…
Add to scheduler…
C:\Users\paul.chase\Desktop\backup_20
mx250 - ftp://172.16.12.11/
<Select destination...>

Once a selection has been defined, the screen will update to indicate the backup process



Status: Preparing backup files...

Description: Manual

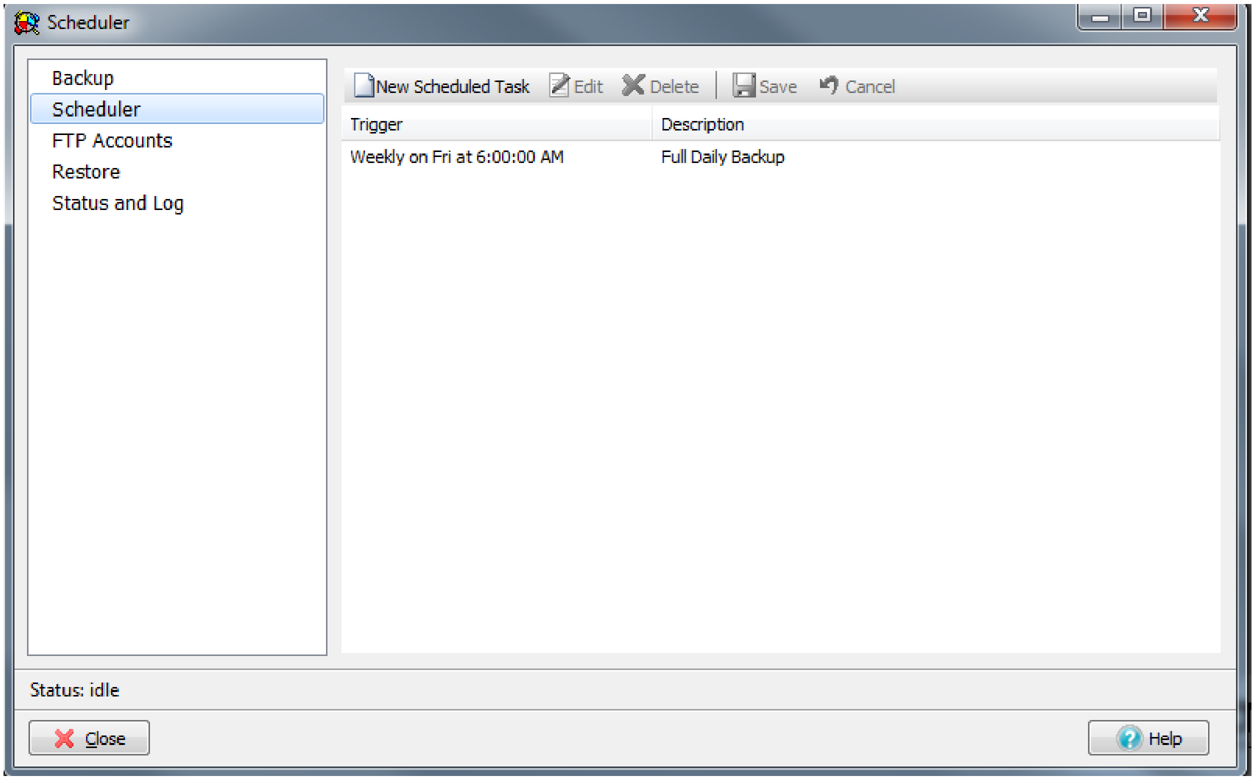
```
Time                 Severity  Message
3/25/2013 9:07:52 AM  Debug    Backup - Completed preparing: 'test'
3/25/2013 9:07:52 AM  Debug    Backup - Started preparing: 'Collection_Agency'
3/25/2013 9:07:53 AM  Debug    Backup - Completed preparing: 'Collection_Agency'
3/25/2013 9:07:53 AM  Debug    Backup - Started preparing: 'ICC_2'
3/25/2013 9:07:53 AM  Debug    Backup - Completed preparing: 'ICC_2'
3/25/2013 9:07:53 AM  Debug    Backup - Started preparing: 'Transcription'
3/25/2013 9:07:53 AM  Debug    Backup - Completed preparing: 'Transcription'
3/25/2013 9:07:53 AM  Debug    Backup - Started preparing: 'Translation'
3/25/2013 9:07:53 AM  Debug    Backup - Completed preparing: 'Translation'
3/25/2013 9:07:53 AM  Debug    Backup - Started preparing: 'blf_test'
3/25/2013 9:07:54 AM  Debug    Backup - Completed preparing: 'blf_test'
3/25/2013 9:07:54 AM  Debug    Backup - Started upload to client
3/25/2013 9:12:57 AM  Debug    Backup - Completed upload to client
3/25/2013 10:19:25...  Debug   Backup Task started: Manual
3/25/2013 10:19:26...  Debug   Backup - Started preparing: 'CDR'
```

Status: Preparing backup files...

Once the backup is finished the log will update with “Completed, upload to the client” message, and the status will return to idle.

16.3.2 Automatic Backup

The MX-E also offers the ability to automatically backup to an FTP server by scheduling a backup task. To schedule a backup task, select *Maintenance →* Backup in the MX-E Administrator.



Trigger	Description
Weekly on Fri at 6:00:00 AM	Full Daily Backup

Status: idle

From the Scheduler navigation option on the left you can

- Create a New Scheduled Task
- Edit an Existing Scheduled Task
- Delete an Existing Scheduled Task

By clicking on the appropriate icon

New Scheduled Task

Clicking on the New Scheduled Task icon New Scheduled Task opens a window in which you select the appropriate items to backup, and the schedule you wish to back them up on, as well as the location to back up to.

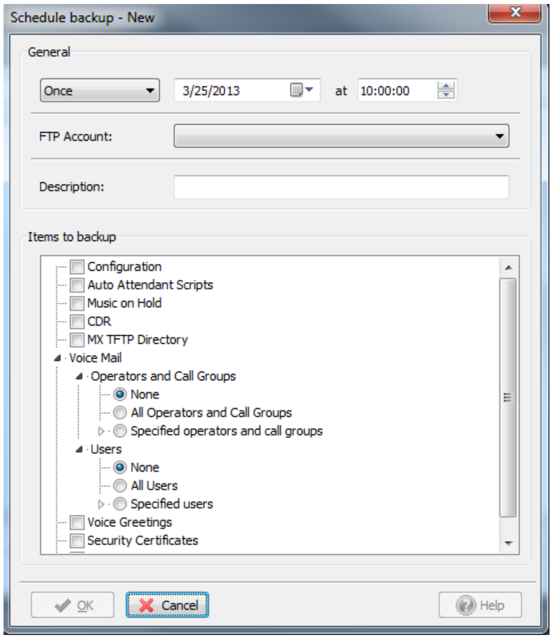
Backup Options

- Once
  - Day of the year
  - Hour of the Day
- Daily
  - Hour of the Day
- Weekly
  - Day of the week
  - Hour of the Day
- Monthly
  - Day of the Month
  - Hour of the Day

Description: Description of the Task

FTP Account: Select defined FTP Account

Items to backup: Select the items you wish to backup in this scheduled task



Schedule backup - New

General

Once ▾ 3/25/2013 at 10:00:00

FTP Account:

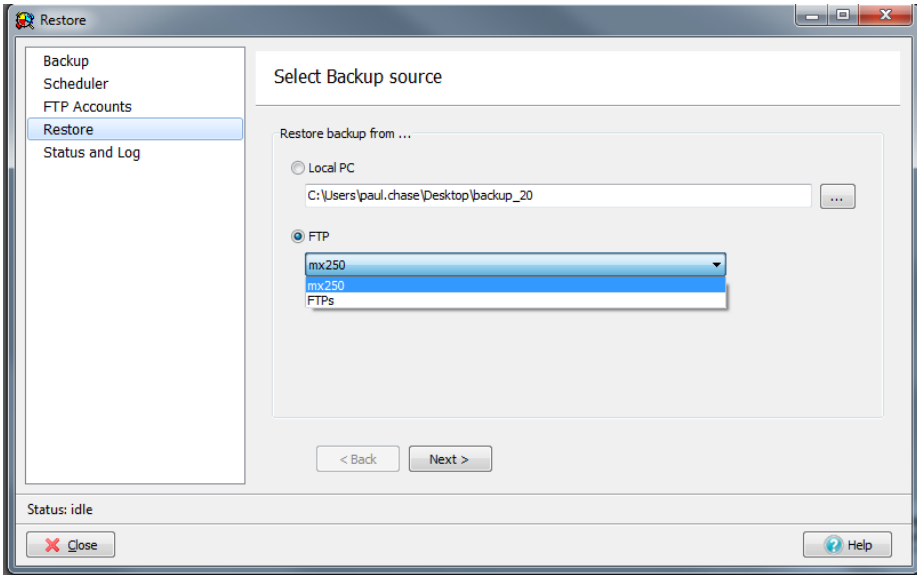
Description:

Items to backup

- □ Configuration
- □ Auto Attendant Scripts
- □ Music on Hold
- □ CDR
- □ MX TFTP Directory
- Voice Mail
  - Operators and Call Groups
    - ● None
    - ○ All Operators and Call Groups
    - ○ Specified operators and call groups
  - Users
    - ● None
    - ○ All Users
    - ○ Specified users
- □ Voice Greetings
- □ Security Certificates

Once you have scheduled a backup it will appear on the scheduler, it is important to remember to press the "Save" Save icon after making any changes to the schedule.

16.4 Restore Backup



16.4.1 Identifying the backup version

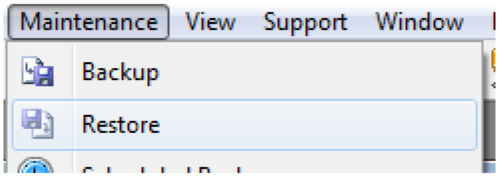
To identify the version a backup is from by opening the backup folder and review the `ver` file which can be opened by any text editing application, review the fw_version which will indicate the MX-E Version the backup is from.

This version file will also provide valuable information on the date and time the backup was created, as well other information about the MX-E, and process used to create the backup.

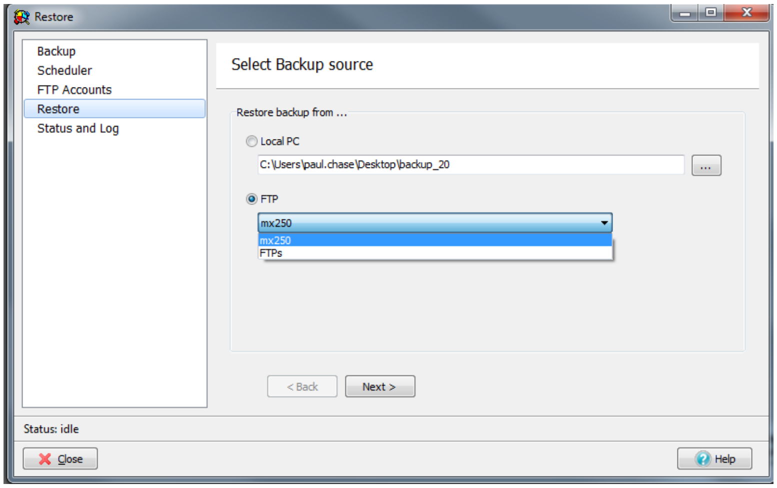
```
[compatibility]
ver=2
fw_version=7.9.3700
fw_internal_version=7.9.3700
platform=MX-E

[info]
creation_time=Mon Mar 25 12:45:56 2013
type=Manual
MX-E_IP=192.168.1.1
SN=11xxx

[items]
8.3466084948209567190=NPR_Hunt
4=CDR
9.-1585194337608583521=5041
8.3466084947344308350=Answering_Service
```

16.4.2 Performing the restore process

In the MX-E Administrator click on Maintenance → Restore.



Then select the appropriate backup source and file.



Restore backup from ...

○ Local PC

C:\Users\paul.chase\Desktop\backup_20

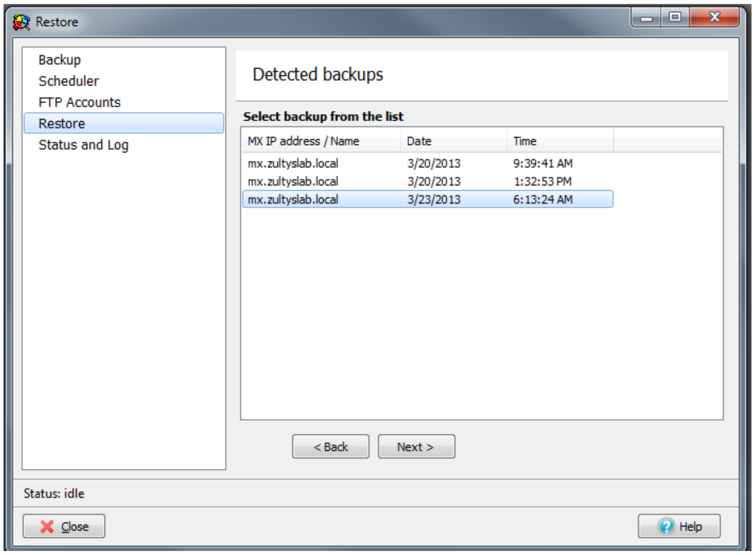
● FTP

mx250

mx250
FTPs

Status: idle

Select the appropriate backup set.



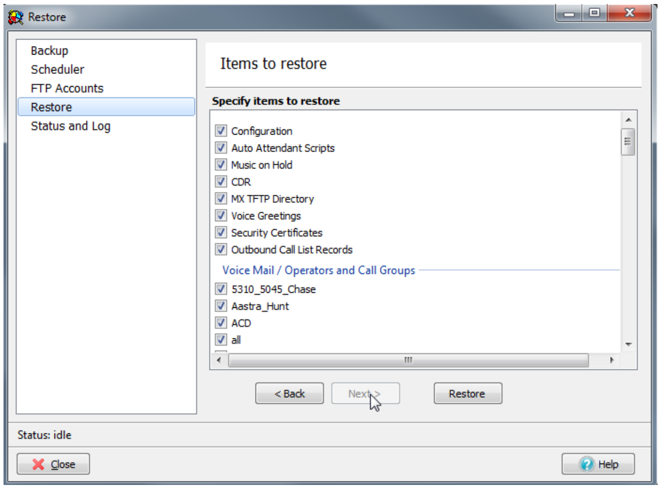
Detected backups

Select backup from the list

MX IP address / Name	Date	Time
mx.zultyslab.local	3/20/2013	9:39:41 AM
mx.zultyslab.local	3/20/2013	1:32:53 PM
mx.zultyslab.local	3/23/2013	6:13:24 AM

Status: idle

Select the appropriate items to restore.



Items to restore

Specify items to restore

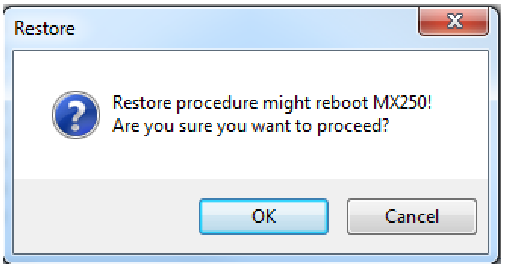
- ☑ Configuration
- ☑ Auto Attendant Scripts
- ☑ Music on Hold
- ☑ CDR
- ☑ MX TFTP Directory
- ☑ Voice Greetings
- ☑ Security Certificates
- ☑ Outbound Call List Records

Voice Mail / Operators and Call Groups

- ☑ 5310_5045_Chase
- ☑ Aastra_Hunt
- ☑ ACD
- ☑ all

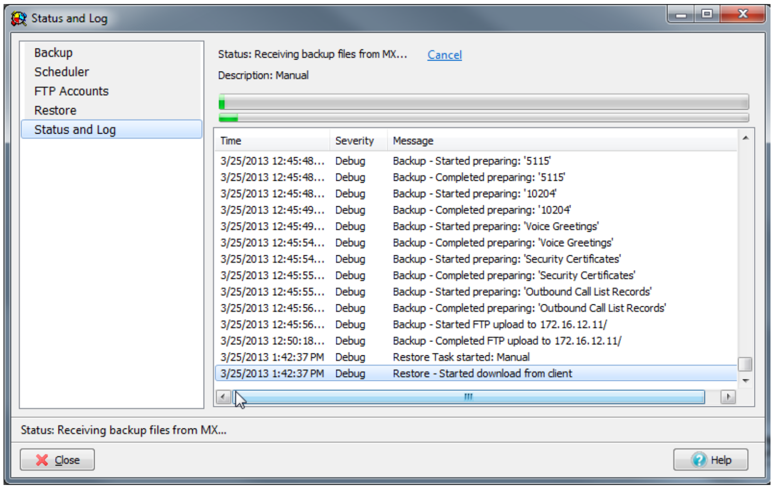
Status: idle

Click ok to the warning that the backup may trigger a reboot of the MX-E



Restore procedure might reboot MX250!
Are you sure you want to proceed?

The screen will update with progress indicators, and log entries identifying the process of the restore process.



Status: Receiving backup files from MX... Cancel

Description: Manual

```
Time                  Severity  Message
3/25/2013 12:45:48... Debug     Backup - Started preparing: '5115'
3/25/2013 12:45:48... Debug     Backup - Completed preparing: '5115'
3/25/2013 12:45:48... Debug     Backup - Started preparing: '10204'
3/25/2013 12:45:49... Debug     Backup - Completed preparing: '10204'
3/25/2013 12:45:49... Debug     Backup - Started preparing: 'Voice Greetings'
3/25/2013 12:45:54... Debug     Backup - Completed preparing: 'Voice Greetings'
3/25/2013 12:45:54... Debug     Backup - Started preparing: 'Security Certificates'
3/25/2013 12:45:55... Debug     Backup - Completed preparing: 'Security Certificates'
3/25/2013 12:45:55... Debug     Backup - Started preparing: 'Outbound Call List Records'
3/25/2013 12:45:56... Debug     Backup - Completed preparing: 'Outbound Call List Records'
3/25/2013 12:45:56... Debug     Backup - Started FTP upload to 172.16.12.11/
3/25/2013 12:50:18... Debug     Backup - Completed FTP upload to 172.16.12.11/
3/25/2013 1:42:37 PM  Debug     Restore Task started: Manual
3/25/2013 1:42:37 PM  Debug     Restore - Started download from client
```

Status: Receiving backup files from MX...

17. Replacing the Hard Disk Drive

The MX-E system utilizes three(3) field serviceable Hard Disk Drives for storage of voice messages, CDR data, call recordings. Should the need arise to replace the drive, the following instructions are provided.

To replace the hard disk drive in the MX-E:

- Open the hard disk drive cover by sliding the lock to eject the existing hard disk drive. This is done by moving the lock button on the hard disk drive door to the right.

Drive Door

Eject Button

Eject Button moved to the right, opening the drive door

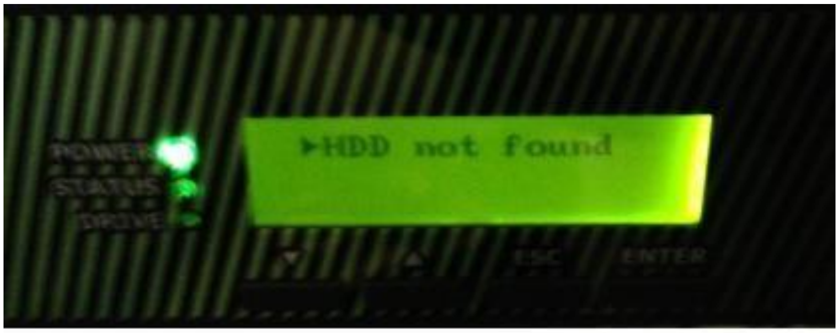
- Remove the failed hard disk drive from the unit.

- Install the new hard disk drive in the unit. (note: push the drive in using your finger as far as it will go and then use the hard disk drive door to seat the drive. The door should fully close and latch when the drive is secured.

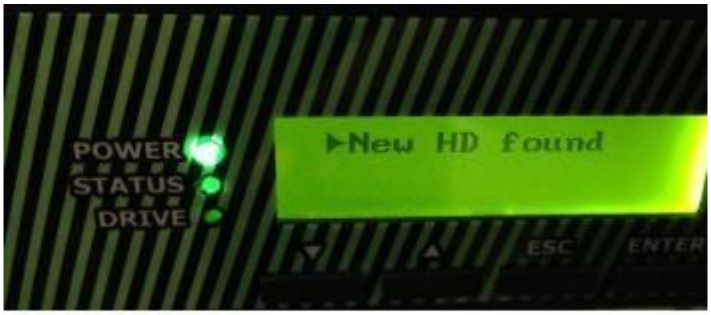
LCD Display States of Hard Disk Drive:

The LCD will display up to three(3) states to indicate Hard Disk Drive Status on power up:

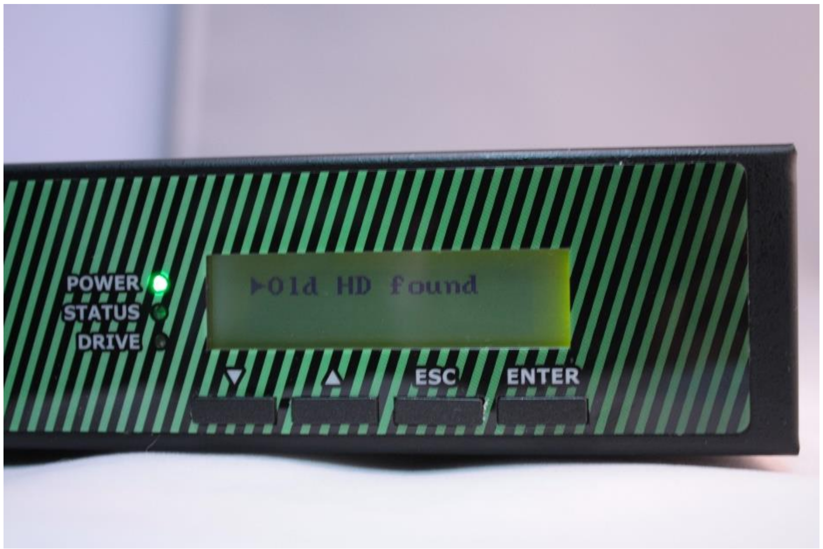
1) No drive or failed hard disk drive:
   The LCD will indicate HDD not found in the event of an improperly installed or failed hard disk drive installed in the MX-E.



2) Blank hard disk drive inserted:
   The LCD will indicate New HD found in the event of a blank hard disk drive installed in the MX-E.



3) Drive that has MX-E software installed on it:
   The LCD will indicate Old HD found in the event of a hard disk drive with MX-E software installed in the MX-E.

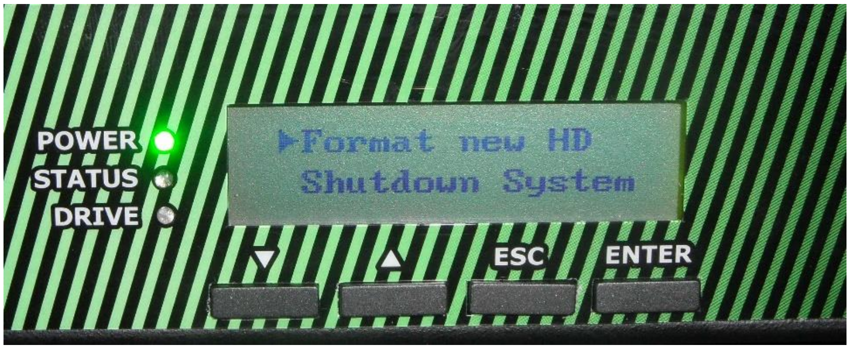


Note: If you remove a working MX-E Hard Disk Drive and simply re-install it, without attempting installation of another Hard Disk Drive, the system will boot normally. The system will then be ready to process calls.

Format Hard Disk Drive:

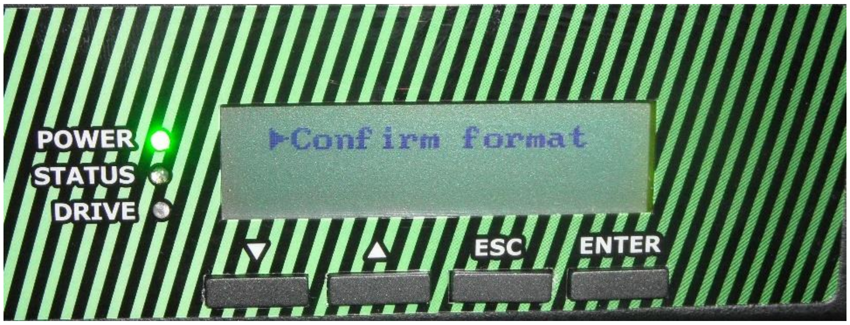
After powering up, while at 1 of the three states described in the previous section, perform the following to proceed:

1) Press the ENTER button at any state.



```
▶Format new HD
 Shutdown System
```

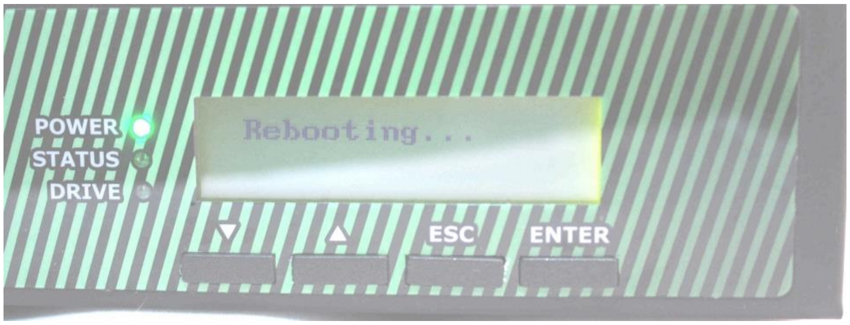
2) Press the ENTER button at the Format new HD prompt.



```
▶Confirm format
```

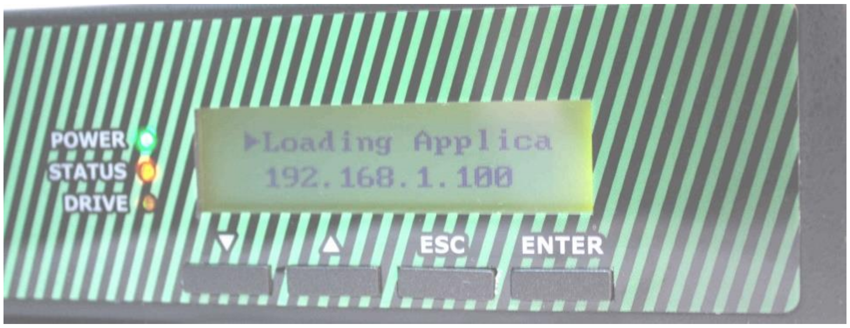
3) Press the ENTER button at the Confirm Format prompt.

4) The system will reboot and then the screen will be blank during the reformat process. During this time, the DRIVE LED will light solid.

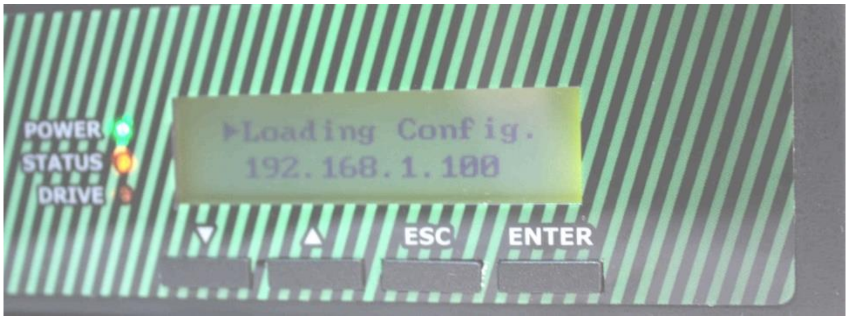


```
Rebooting...
```

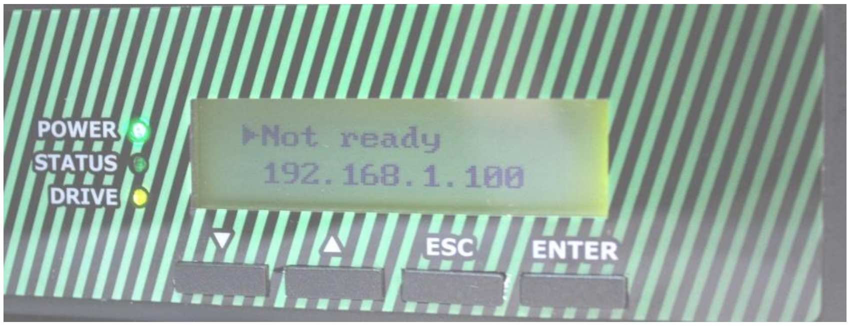
5) Once the system has formatted the Hard Disk Drive, you will see the Application Loading and Configuration Loading displays.



```
▶Loading Applica
 192.168.1.100
```



```
▶Loading Config.
 192.168.1.100
```



```
▶Not ready
 192.168.1.100
```

The system will display System Ready and the IP Address indicating the system is online and ready to process calls.

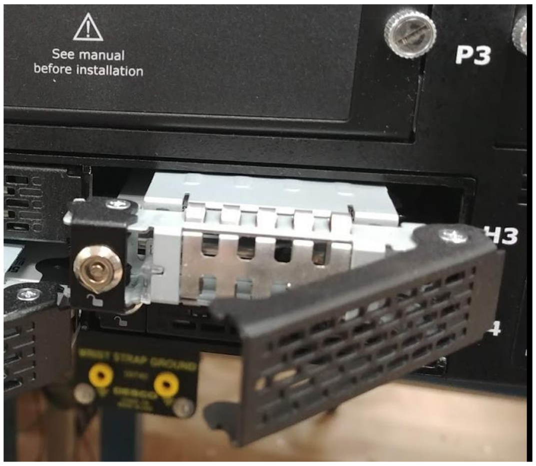
Notes:

1) If you remove an MX-E hard disk drive and install another MX-E hard disk drive, installing the original MX-E hard disk drive will result in the drive being reformatted!

2) Zultys only supports Hard Disk Drives supplied by Zultys. Third party Hard Disk Drives are not supported by Zultys.

Replacing two HDDs in MX-E with the two pre-programmed HDDs sent from Zultys

1. Turn MX-E off.
2. Remove HDDs H1 and H2 from unit.
3. Un-plug HDD in H3 but keep it in the tray

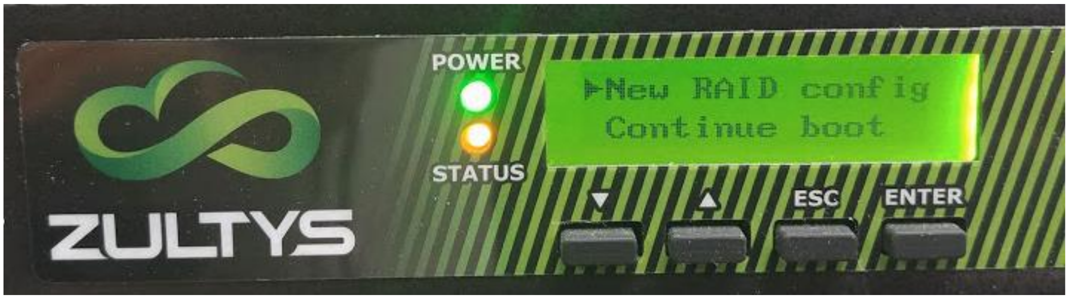


4. Only insert replacement HDD labeled H1 into H1 slot.

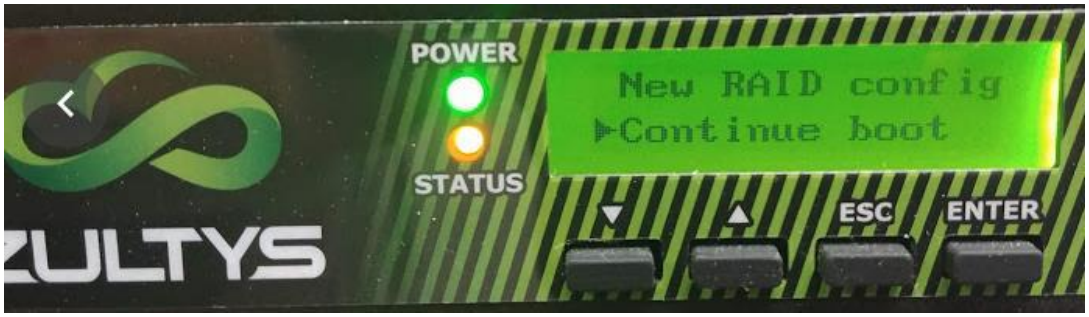
   Make sure replacement HDD matches the MX-E serial number and position H1.

5. Turn on MX-E.

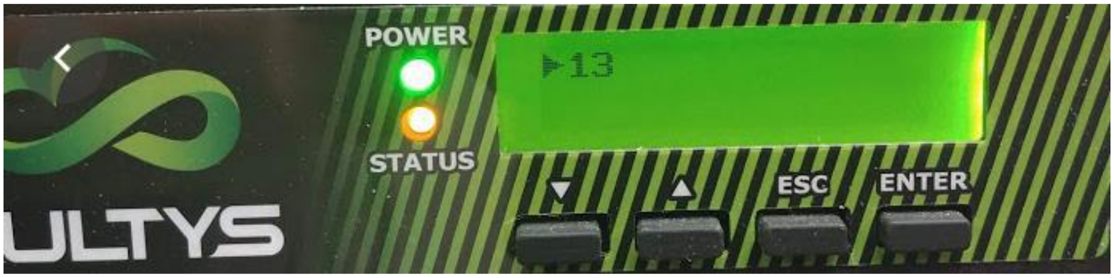
6. After a minute the LCD should display:



7. Press the down key to set cursor on “Continue boot” and press **ENTER** key.



   You will see:



8. Press **ENTER** key. The system will boot up.

9. Once MX-E boots up, shutdown the unit.

10. Insert replacement HDD labeled H2 into H2 slot.

    Make sure replacement HDD matches the MX-E serial number and position H2.

11. Reinsert HDD H3.

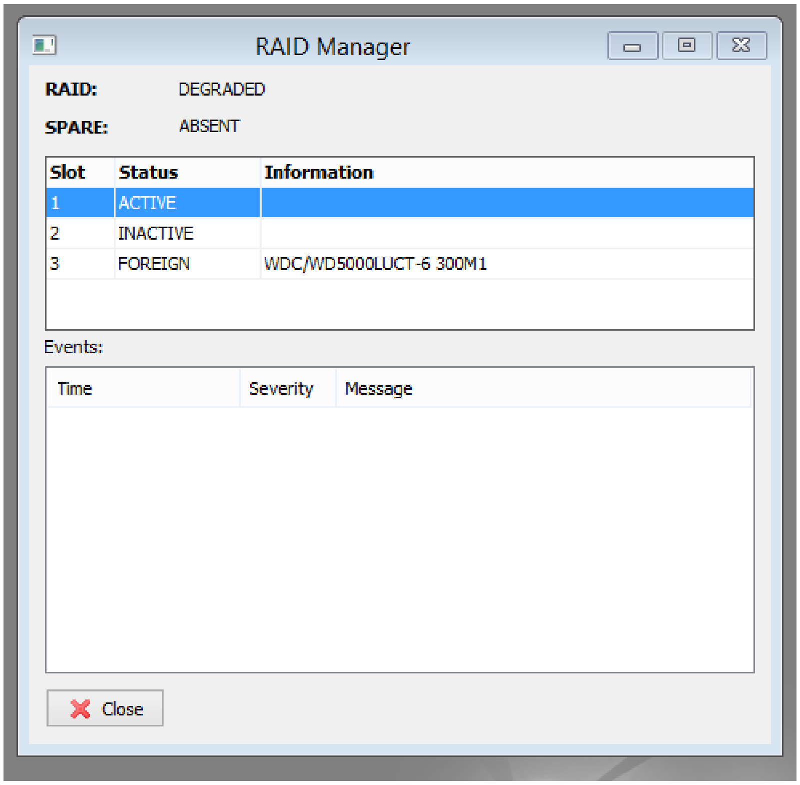
12. Turn unit on.

13. Repeat steps 6-9.

14. Once system is in Ready state. Log in with MX Admin.

    Note the IP will be 192.168.1.100.

15. In MX Admin go to View->Raid Manager. You will see:



RAID: DEGRADED

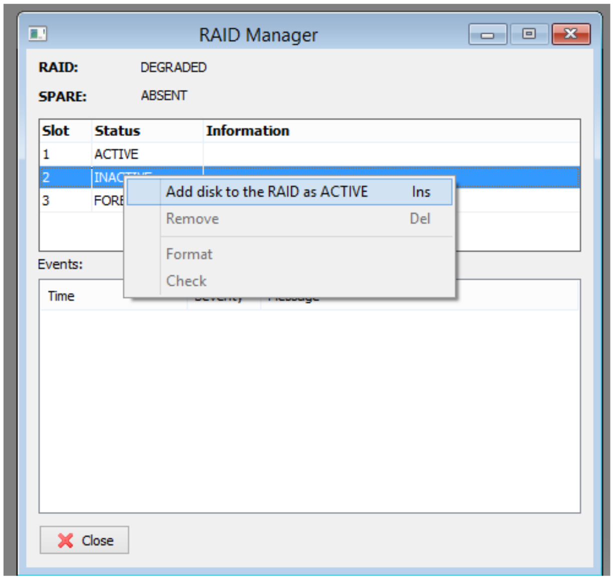
SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	
2	INACTIVE	
3	FOREIGN	WDC/WD5000LUCT-6 300M1

Events:

Time	Severity	Message

16. Right click on Slot 2 and press “Add disk to the RAID as ACTIVE”.

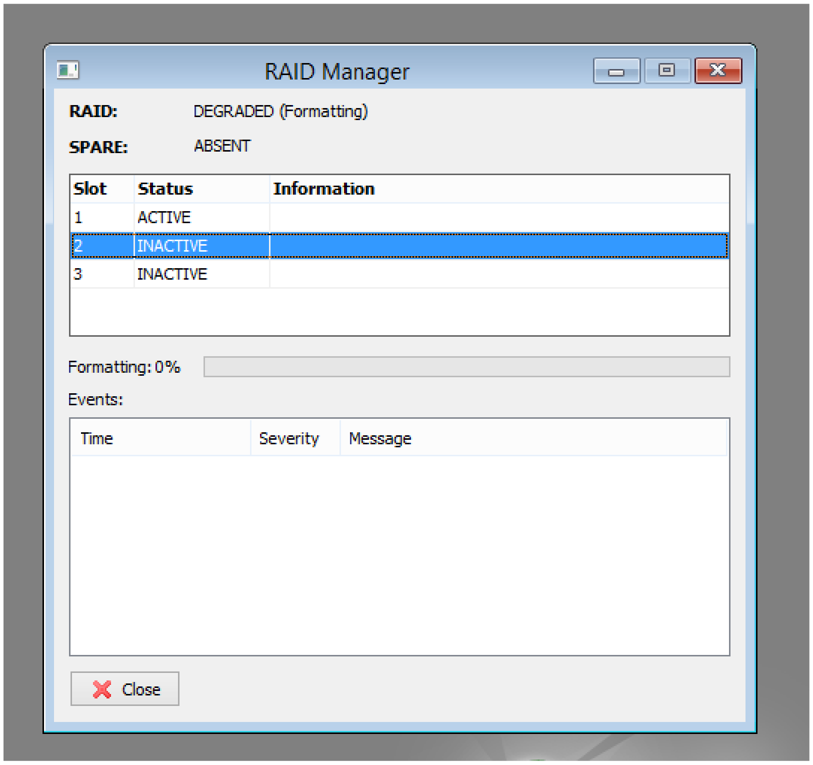


RAID: DEGRADED

SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	
2	INAC	
3	FORE	

17. The drive will start reformatting:



RAID: DEGRADED (Formatting)

SPARE: ABSENT

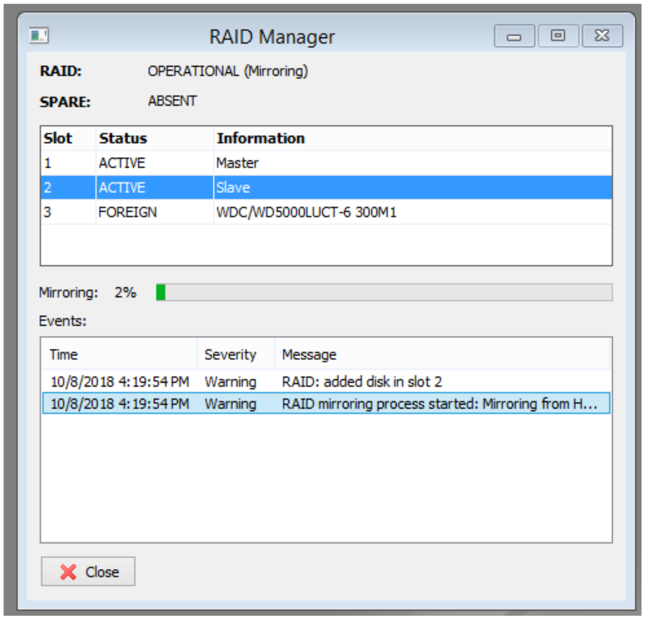
Slot	Status	Information
1	ACTIVE	
2	INACTIVE	
3	INACTIVE	

Formatting: 0%

Events:

Time	Severity	Message

18. After a couple of minutes, the drive will start mirroring:



RAID: OPERATIONAL (Mirroring)

SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	Master
2	ACTIVE	Slave
3	FOREIGN	WDC/WD5000LUCT-6 300M1

Mirroring: 2%

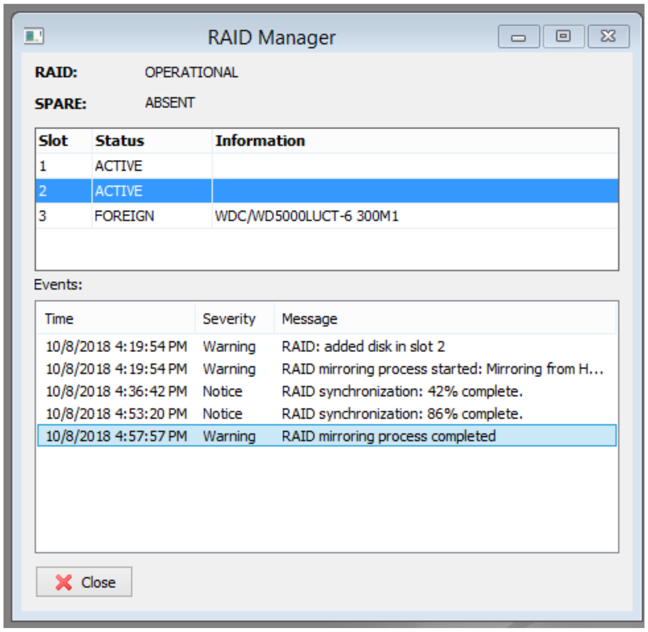
Events:

Time	Severity	Message
10/8/2018 4:19:54 PM	Warning	RAID: added disk in slot 2
10/8/2018 4:19:54 PM	Warning	RAID mirroring process started: Mirroring from H...

19. Mirroring processes may take up to an hour.

If adding disk as active fails repeat steps 16 – 18.

20. Once mirroring is finished you will see:



RAID: OPERATIONAL

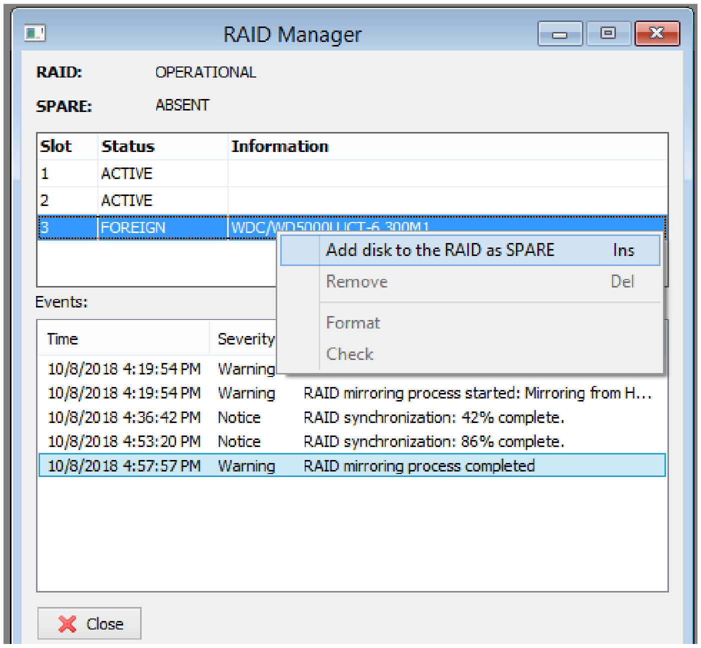
SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	
2	ACTIVE	
3	FOREIGN	WDC/WD5000LUCT-6 300M1

Events:

Time	Severity	Message
10/8/2018 4:19:54 PM	Warning	RAID: added disk in slot 2
10/8/2018 4:19:54 PM	Warning	RAID mirroring process started: Mirroring from H...
10/8/2018 4:36:42 PM	Notice	RAID synchronization: 42% complete.
10/8/2018 4:53:20 PM	Notice	RAID synchronization: 86% complete.
10/8/2018 4:57:57 PM	Warning	RAID mirroring process completed

21. Right click on Slot 3 and press “Add disk to the RAID as SPARE”.



RAID: OPERATIONAL

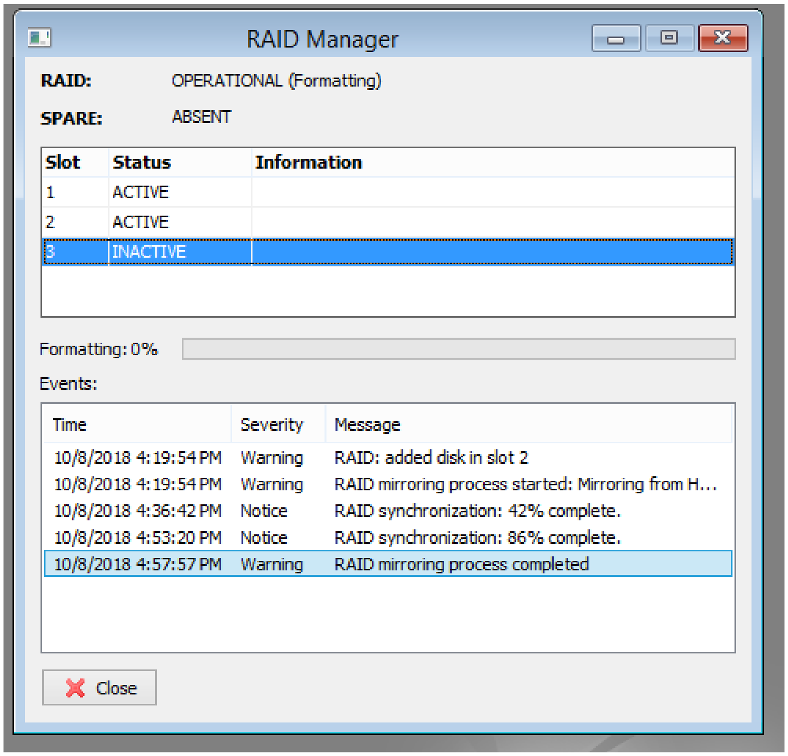
SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	
2	ACTIVE	
3	FOREIGN	WDC/WD5000LUCT-6 300M1

Events:

Time	Severity	
10/8/2018 4:19:54 PM	Warning	
10/8/2018 4:19:54 PM	Warning	RAID mirroring process started: Mirroring from H…
10/8/2018 4:36:42 PM	Notice	RAID synchronization: 42% complete.
10/8/2018 4:53:20 PM	Notice	RAID synchronization: 86% complete.
10/8/2018 4:57:57 PM	Warning	RAID mirroring process completed

22. The H3 HDD will reformat:



RAID: OPERATIONAL (Formatting)

SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	
2	ACTIVE	
3	INACTIVE	

Formatting: 0%

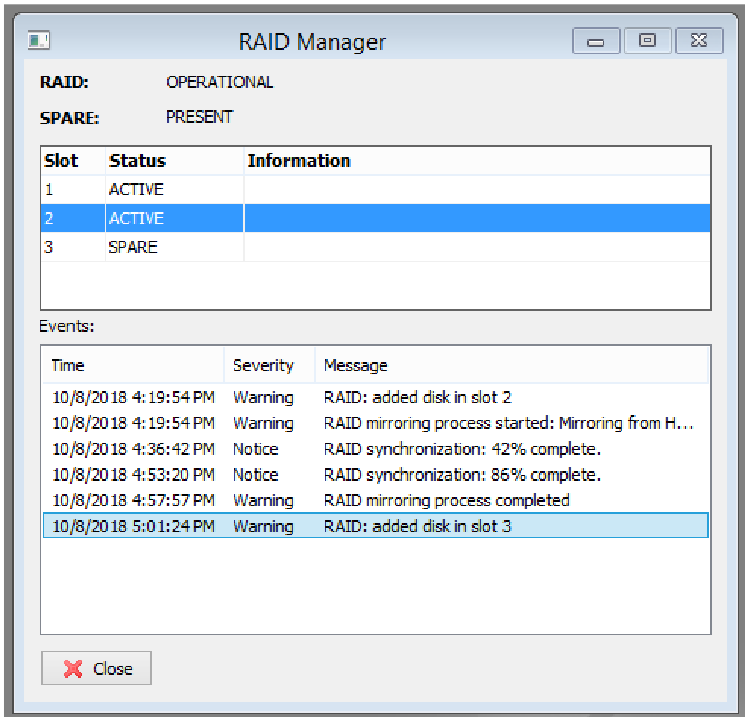
Events:

Time	Severity	Message
10/8/2018 4:19:54 PM	Warning	RAID: added disk in slot 2
10/8/2018 4:19:54 PM	Warning	RAID mirroring process started: Mirroring from H…
10/8/2018 4:36:42 PM	Notice	RAID synchronization: 42% complete.
10/8/2018 4:53:20 PM	Notice	RAID synchronization: 86% complete.
10/8/2018 4:57:57 PM	Warning	RAID mirroring process completed

23. After a couple of minutes reformatting will complete.

    If adding disk as spare fails, repeat steps 21-22.

24. Once complete RAID Manager will show:



RAID Manager

RAID: OPERATIONAL

SPARE: PRESENT

Slot	Status	Information
1	ACTIVE	
2	ACTIVE	
3	SPARE	

Events:

Time	Severity	Message
10/8/2018 4:19:54 PM	Warning	RAID: added disk in slot 2
10/8/2018 4:19:54 PM	Warning	RAID mirroring process started: Mirroring from H...
10/8/2018 4:36:42 PM	Notice	RAID synchronization: 42% complete.
10/8/2018 4:53:20 PM	Notice	RAID synchronization: 86% complete.
10/8/2018 4:57:57 PM	Warning	RAID mirroring process completed
10/8/2018 5:01:24 PM	Warning	RAID: added disk in slot 3

18. Restricted Boot Mode

The MX-E is capable of booting up and processing calls in the event of not finding a Hard Disk Drive on boot. This feature is called restricted mode boot. This feature allows the system to continue to process calls until the defective HDD can be replaced.

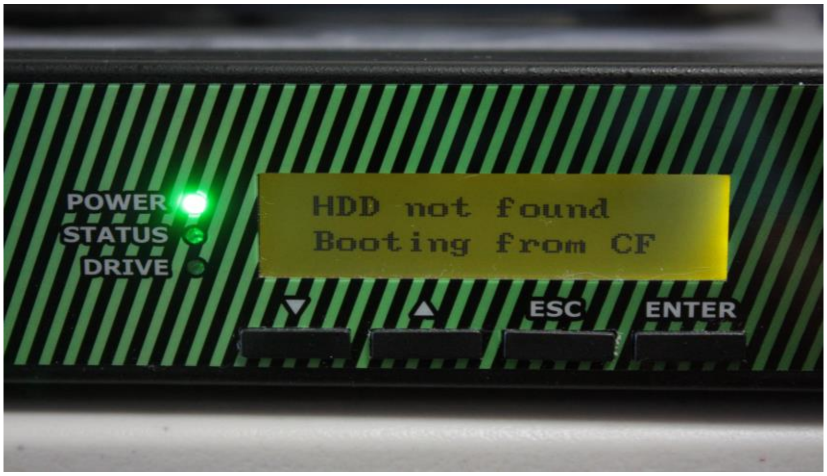
There are limitations in system functionality when running in restricted mode. These limitations are:

- No voice mail messages can be left or sent by users/call groups
- No on demand or automatic call recordings will be recorded/saved
- No CDR records are stored. This will affect MXreport and Archive Server operations.
- Cannot re-record/record AA, call group announcements, or MoH files.

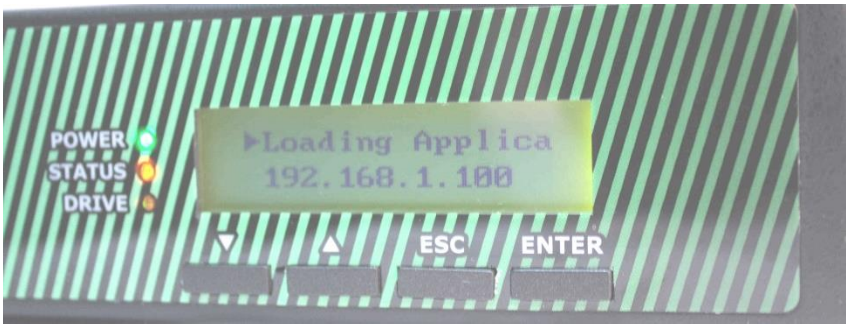
The system will provide the following functionality in restricted mode:

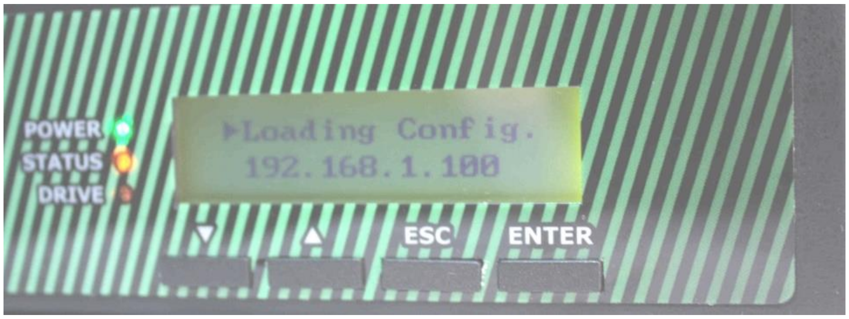
- Incoming/outgoing calls can be received/placed
- Existing AA/Call Group Announcements/MoH files will play

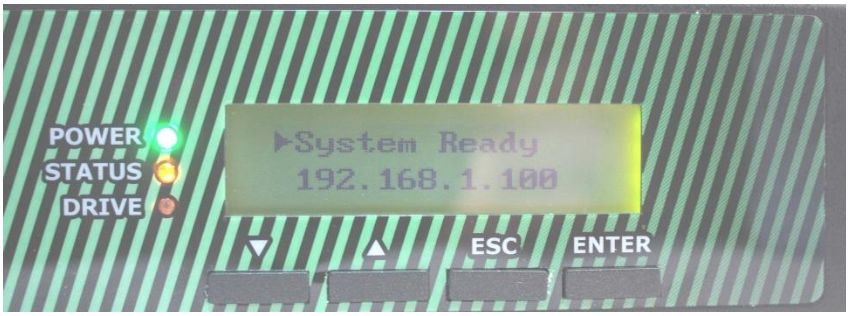
The boot process for restricted mode on the LCD will show as follows:



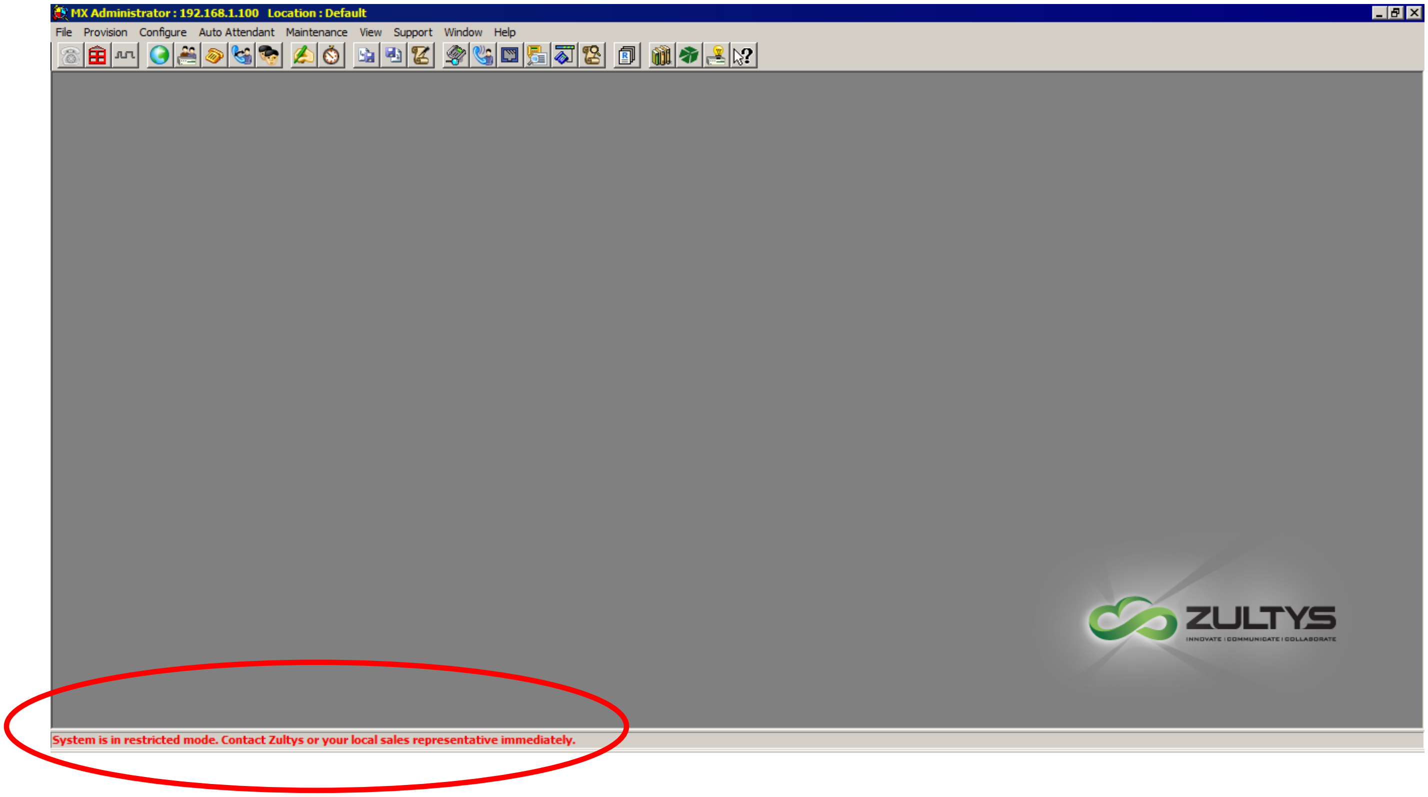
HDD not found
Booting from CF


POWER
STATUS
DRIVE
▶Loading Applica
192.168.1.100
▼
▲
ESC
ENTER


POWER
STATUS
DRIVE
▶Loading Config.
192.168.1.100
▼
▲
ESC
ENTER


POWER
STATUS
DRIVE
▶System Ready
192.168.1.100
▼
▲
ESC
ENTER

The MX-E Administrator will display a message indicating the system is in restricted mode *("System is in restricted mode. Contact Zultys or your local sales representative immediately")*. The message will flash at the bottom of the screen repeatedly as follows:


MX Administrator : 192.168.1.100 Location : Default
File
Provision
Configure
Auto Attendant
Maintenance
View
Support
Window
Help
ZULTYS
INNOVATE | COMMUNICATE | COLLABORATE

System is in restricted mode. Contact Zultys or your local sales representative immediately.

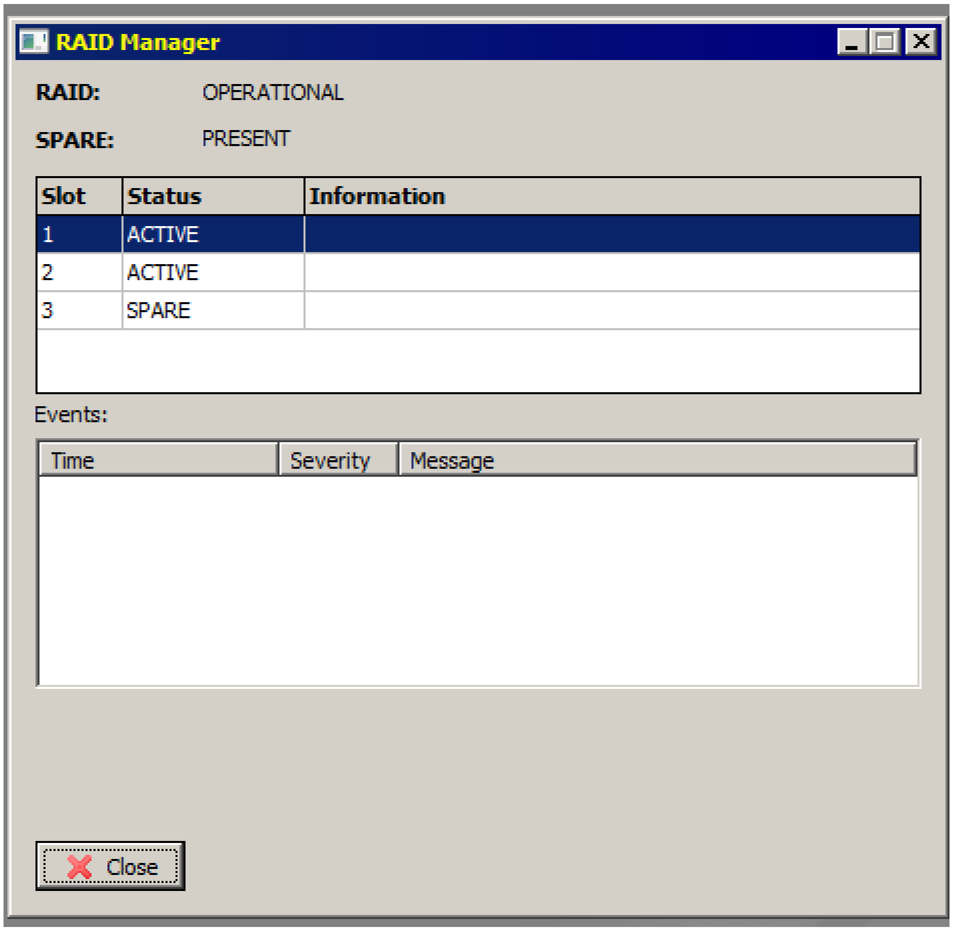
19. MX-E RAID

The RAID (redundant array of independent disks) feature provides hard disk drive redundancy in the MX-E system. The MX-E system has three(3) hard disk drive slots. Typically, H1 and H2 are set to be in a RAID configuration and H3 is designated as a spare drive in the event of an H1/H2 failure.

In the event of a hard disk drive failure, a redundant hard disk drive will take over for the failed drive to allow the system to boot and operate. In addition, the MX-E can have a spare drive installed and "at the ready" in the event of a failed hard disk. In this case, the spare drive becomes part of the RAID configuration taking the place of the failed disk drive.

In the MX-E system, hard disk drive 1(H1) and hard disk drive 2(H2) are configured as RAID members. Disk activity is mirrored between these drives. Hard disk drive 3(H3) is initially configured to be used as a spare drive. If there is a drive failure of H1 or H2, H3 will switch and become a RAID member. Disk activity is now mirrored between the active drive and H3 at this point.
This will continue until the user assigns a new RAID member (H1/H2) after the faulty drive is corrected/replaced.

MX-E Administrator is utilized to view and configure the RAID function. The area is in Maintenance\View\RAID Manager:



RAID: OPERATIONAL

SPARE: PRESENT

Slot	Status	Information
1	ACTIVE	
2	ACTIVE	
3	SPARE	

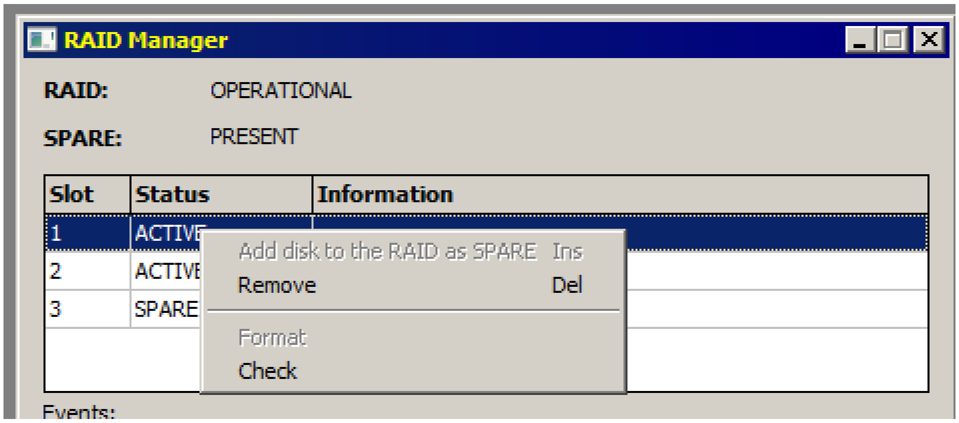
Events:

Time	Severity	Message

RAID Manager Designation	MX-E Front Panel Designation
Slot 1	H1
Slot 2	H2
Slot 3	H3

- **RAID**: [Operational], [Operational, mirroring], [Degraded]
- **Spare**: [Present], [Absent]
- **Slot**: Displays the slot number and the status of the drive in the slot
- **Status** Empty (*should be grayed out*) RAID Active, RAID Spare, RAID Faulty, Foreign
- **Mirroring**: *Percentage, If RAID is mirroring show progress*
- **Events Displays the syslog events associated with the RAID operation**

Right click a particular drive slot to view/change drive options:



RAID Manager

RAID: OPERATIONAL

SPARE: PRESENT

Slot	Status	Information
1	ACTIVE	
2	ACTIVE	
3	SPARE	

Events:

Options that are available:

Add disk to the RAID as a spare drive

Remove the drive from the RAID configuration

Format the drive

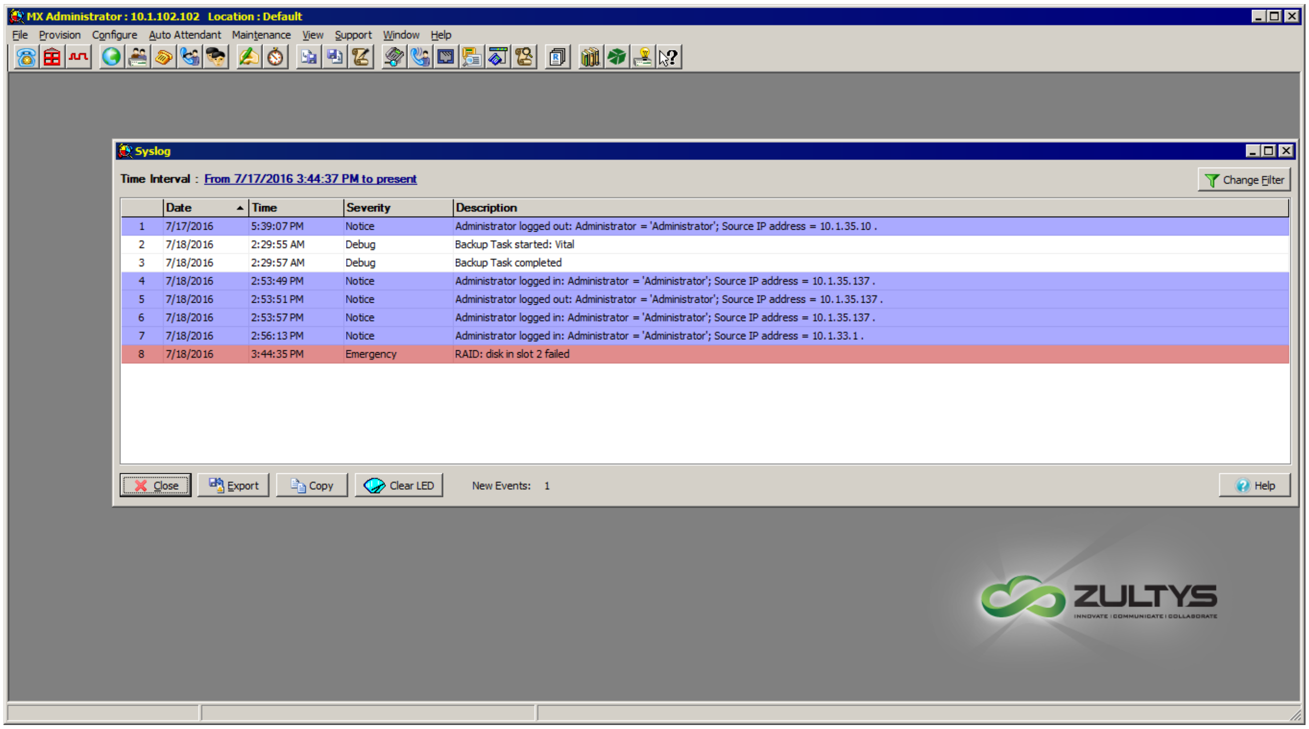
> ***Note that all information on the drive will be erased when the format procedure is done!***

Check the drive. This performs a disk check of the drive.

Failure Scenario

This example will show the results in the Raid Manager when a hard disk drive fails. In this example H2 was purposely failed.

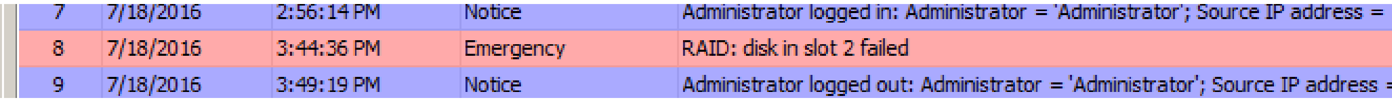
When the failure occurs, a syslog message is generated:


MX Administrator : 10.1.102.102 Location : Default
File Provision Configure Auto Attendant Maintenance View Support Window Help
Syslog
Change Filter
Close
Export
Copy
Clear LED
Help

Time Interval : From 7/17/2016 3:44:37 PM to present

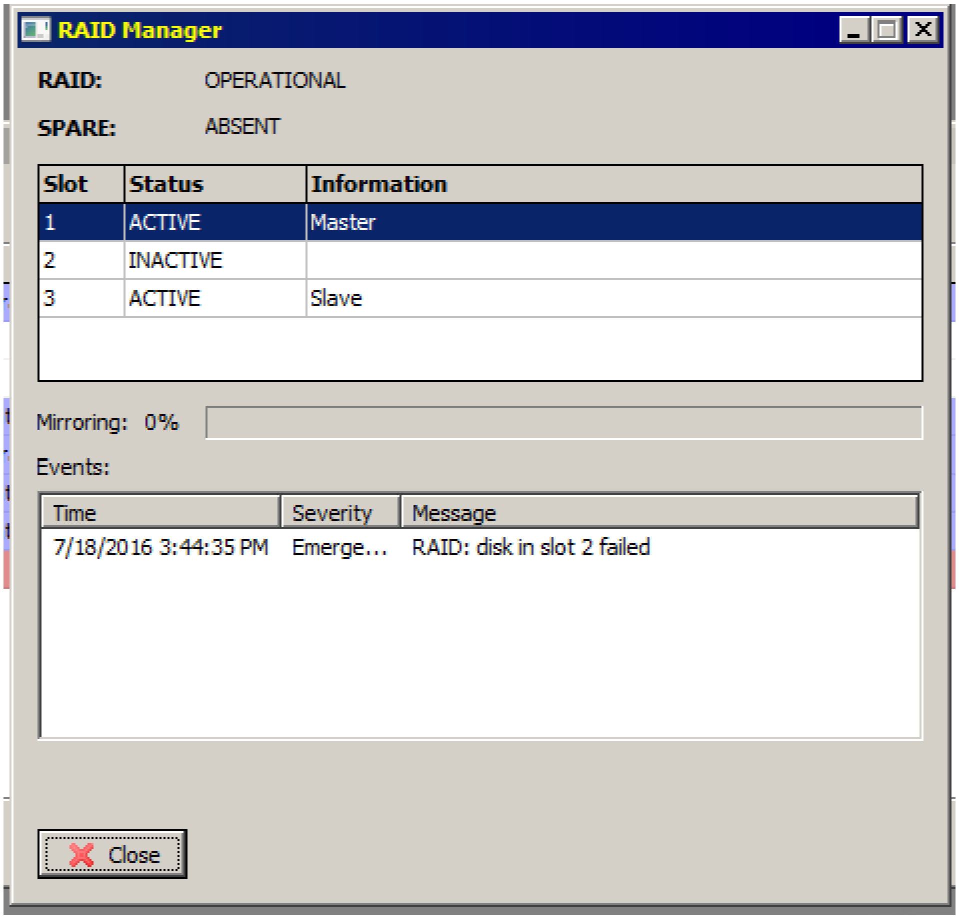
	Date	Time	Severity	Description
1	7/17/2016	5:39:07 PM	Notice	Administrator logged out: Administrator = 'Administrator'; Source IP address = 10.1.35.10 .
2	7/18/2016	2:29:55 AM	Debug	Backup Task started: Vital
3	7/18/2016	2:29:57 AM	Debug	Backup Task completed
4	7/18/2016	2:53:49 PM	Notice	Administrator logged in: Administrator = 'Administrator'; Source IP address = 10.1.35.137 .
5	7/18/2016	2:53:51 PM	Notice	Administrator logged out: Administrator = 'Administrator'; Source IP address = 10.1.35.137 .
6	7/18/2016	2:53:57 PM	Notice	Administrator logged in: Administrator = 'Administrator'; Source IP address = 10.1.35.137 .
7	7/18/2016	2:56:13 PM	Notice	Administrator logged in: Administrator = 'Administrator'; Source IP address = 10.1.33.1 .
8	7/18/2016	3:44:35 PM	Emergency	RAID: disk in slot 2 failed

New Events: 1



7	7/18/2016	2:56:14 PM	Notice	Administrator logged in: Administrator = 'Administrator'; Source IP address =
8	7/18/2016	3:44:36 PM	Emergency	RAID: disk in slot 2 failed
9	7/18/2016	3:49:19 PM	Notice	Administrator logged out: Administrator = 'Administrator'; Source IP address =

The RAID Manager will display the following information:



RAID Manager

RAID: OPERATIONAL

SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	Master
2	INACTIVE	
3	ACTIVE	Slave

Mirroring: 0%

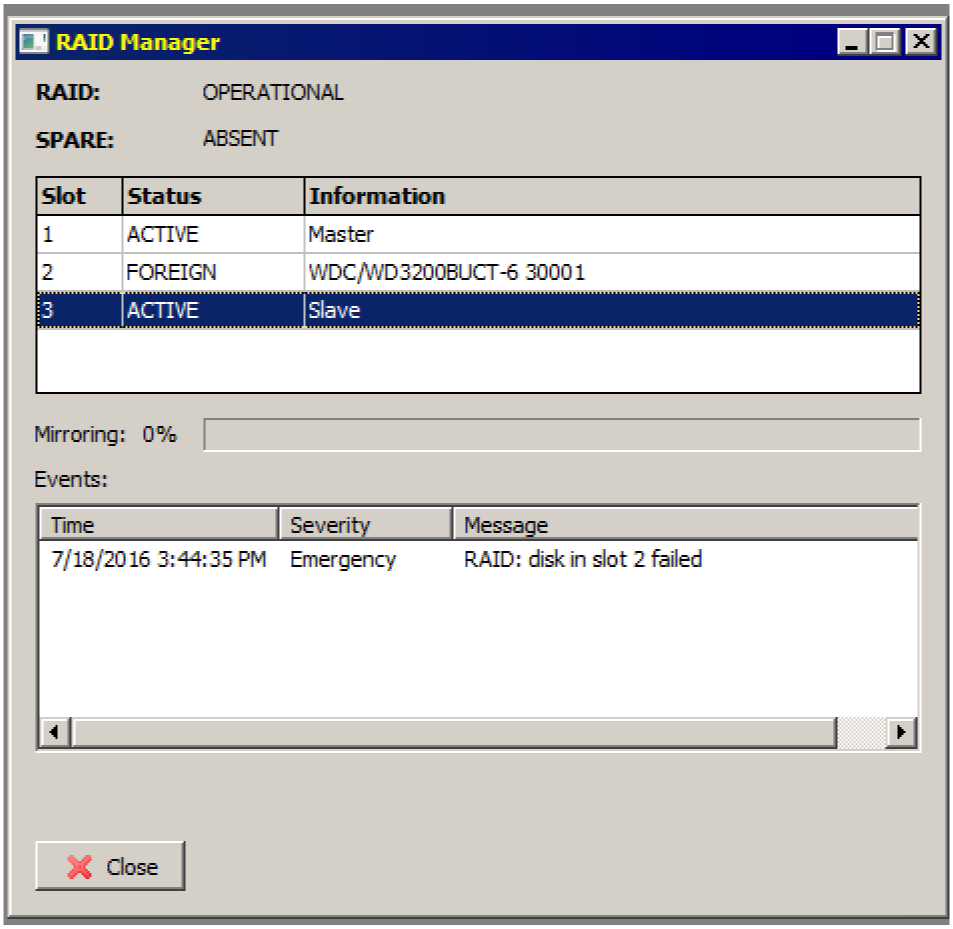
Events:

Time	Severity	Message
7/18/2016 3:44:35 PM	Emerge...	RAID: disk in slot 2 failed

Note that H2 is now INACTIVE due to the failure. H3 is now the slave drive in the RAID configuration.
Also, the syslog failure event is shown in the Events area of the RAID Manager.

The system will now start to mirror content from H1 to H3. The mirroring status will be reflected in the progress bar.

A replacement hard disk drive is now added to H2. The system detects the drive and dispositions it as FOREIGN.



RAID: OPERATIONAL

SPARE: ABSENT

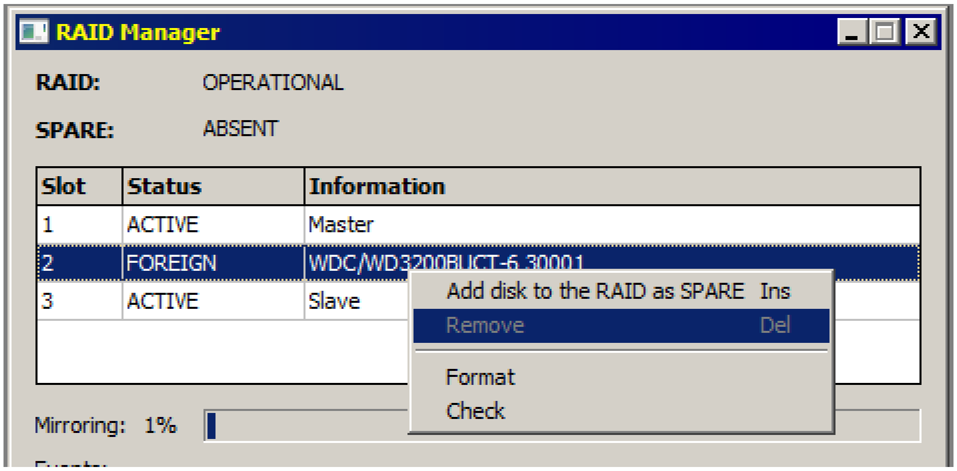
Slot	Status	Information
1	ACTIVE	Master
2	FOREIGN	WDC/WD3200BUCT-6 30001
3	ACTIVE	Slave

Mirroring: 0%

Events:

Time	Severity	Message
7/18/2016 3:44:35 PM	Emergency	RAID: disk in slot 2 failed

Right click the replacement disk drive and select “Add disk to the RAID as SPARE”



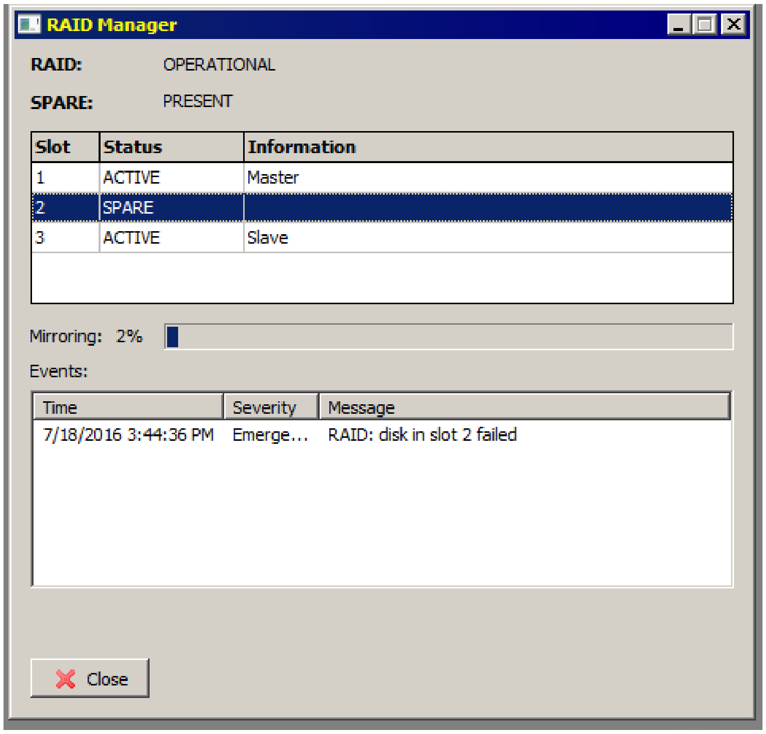
RAID: OPERATIONAL

SPARE: ABSENT

Slot	Status	Information
1	ACTIVE	Master
2	FOREIGN	WDC/WD3200BUCT-6 30001
3	ACTIVE	Slave

Mirroring: 1%

The drive will be dispositioned as a spare drive.



RAID: OPERATIONAL

SPARE: PRESENT

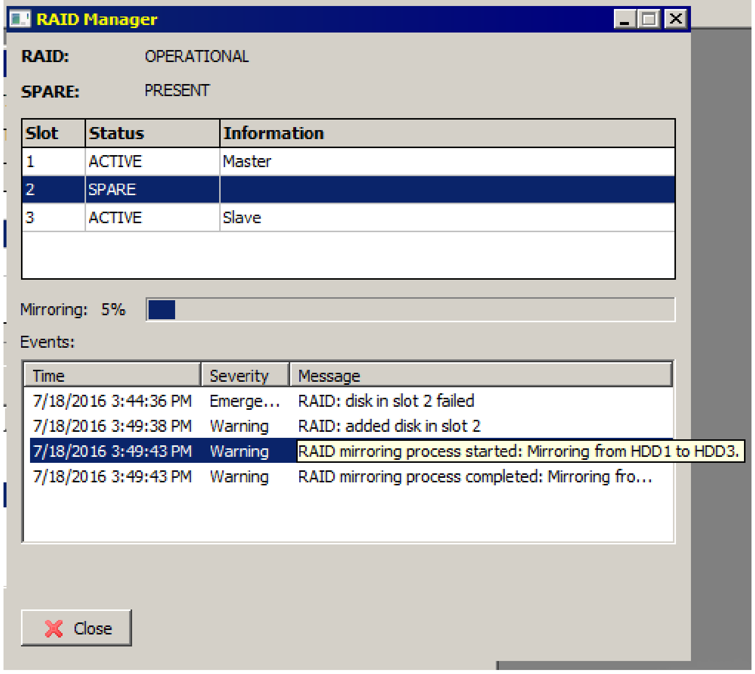
Slot	Status	Information
1	ACTIVE	Master
2	SPARE	
3	ACTIVE	Slave

Mirroring: 2%

Events:

Time	Severity	Message
7/18/2016 3:44:36 PM	Emerge...	RAID: disk in slot 2 failed

The RAID Manager will display all activity on the RAID configuration. Here you can see the message that a hard disk drive was added in slot 2 as well as the mirroring process updates.



RAID: OPERATIONAL

SPARE: PRESENT

Slot	Status	Information
1	ACTIVE	Master
2	SPARE	
3	ACTIVE	Slave

Mirroring: 5%

Events:

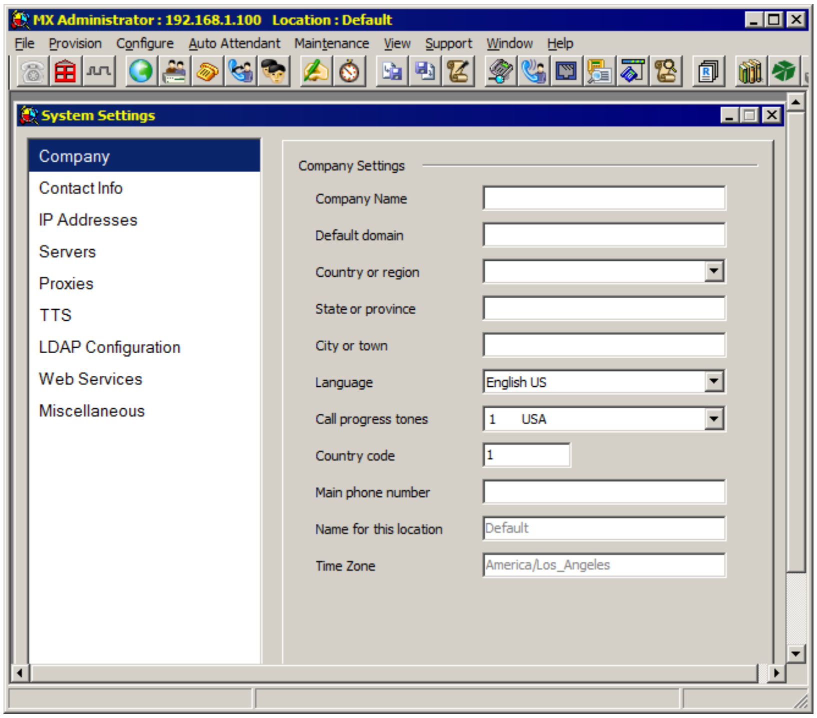
Time	Severity	Message
7/18/2016 3:44:36 PM	Emerge...	RAID: disk in slot 2 failed
7/18/2016 3:49:38 PM	Warning	RAID: added disk in slot 2
7/18/2016 3:49:43 PM	Warning	RAID mirroring process started: Mirroring from HDD1 to HDD3.
7/18/2016 3:49:43 PM	Warning	RAID mirroring process completed: Mirroring fro...

20. Using the Setup Wizard for System Configuration

The setup wizard will guide you through the next few steps. To access the setup wizard select Provision → Wizard:

20.2 Provisioning System Settings

1. Click on "Provision" and select "Wizard"
2. For "Company Name" The Company Name is verified when configuring MX-E network.
3. Enter "Default domain" , this should be the Main IP of the MX-E, or an FQDN that resolves to the MX-E
4. Select a country
5. Enter a state
6. Enter a city or Town
7. Language "English US" If a language Pack was previously installed, you may select it from the pull-down menu.
8. For "Default codec" select **µ-law** (µ-law is the standard codec in North America)
9. For "Call progress tones" select **1 | USA**
10. For "Country code" enter **1**
11. Enter "Main phone number"
    - The Main Phone number is the number presented as the Caller ID Number unless the user has a DID Number or User Caller ID assigned and they are configured to present their DID number in their user profile.


MX Administrator : 192.168.1.100 Location : Default
File Provision Configure Auto Attendant Maintenance View Support Window Help
System Settings

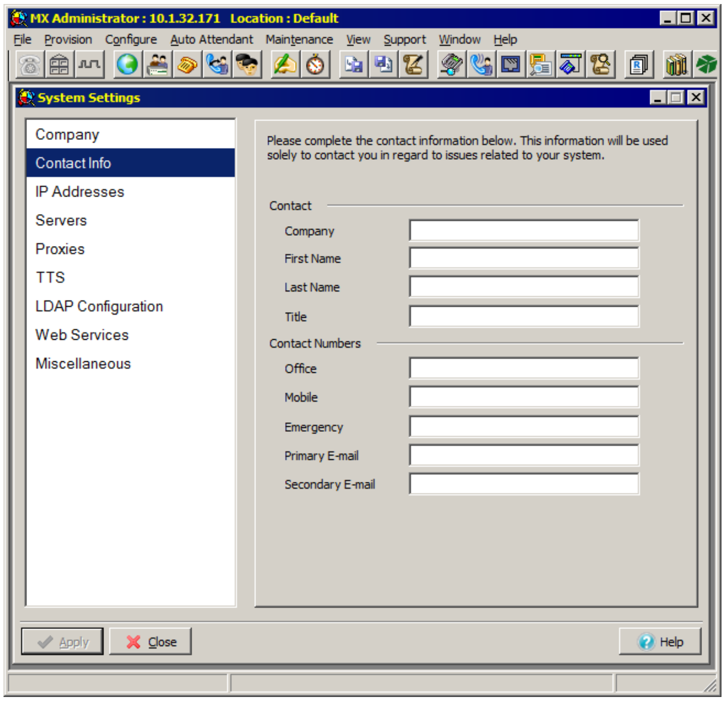
Company
Contact Info
IP Addresses
Servers
Proxies
TTS
LDAP Configuration
Web Services
Miscellaneous

Company Settings

Company Name	
Default domain	
Country or region	
State or province	
City or town	
Language	English US
Call progress tones	1 USA
Country code	1
Main phone number	
Name for this location	Default
Time Zone	America/Los_Angeles

20.3 System Settings – Contact Info

This information is only used when connected to the support server. It will be used to contact you if there is a problem with the system. It is recommended that the contact information be of the Channel Partner AND reflect the company name where the system is installed.


MX Administrator : 10.1.32.171 Location : Default
File Provision Configure Auto Attendant Maintenance View Support Window Help
System Settings
Apply
Close
Help

Company
Contact Info
IP Addresses
Servers
Proxies
TTS
LDAP Configuration
Web Services
Miscellaneous

Please complete the contact information below. This information will be used solely to contact you in regard to issues related to your system.

Contact

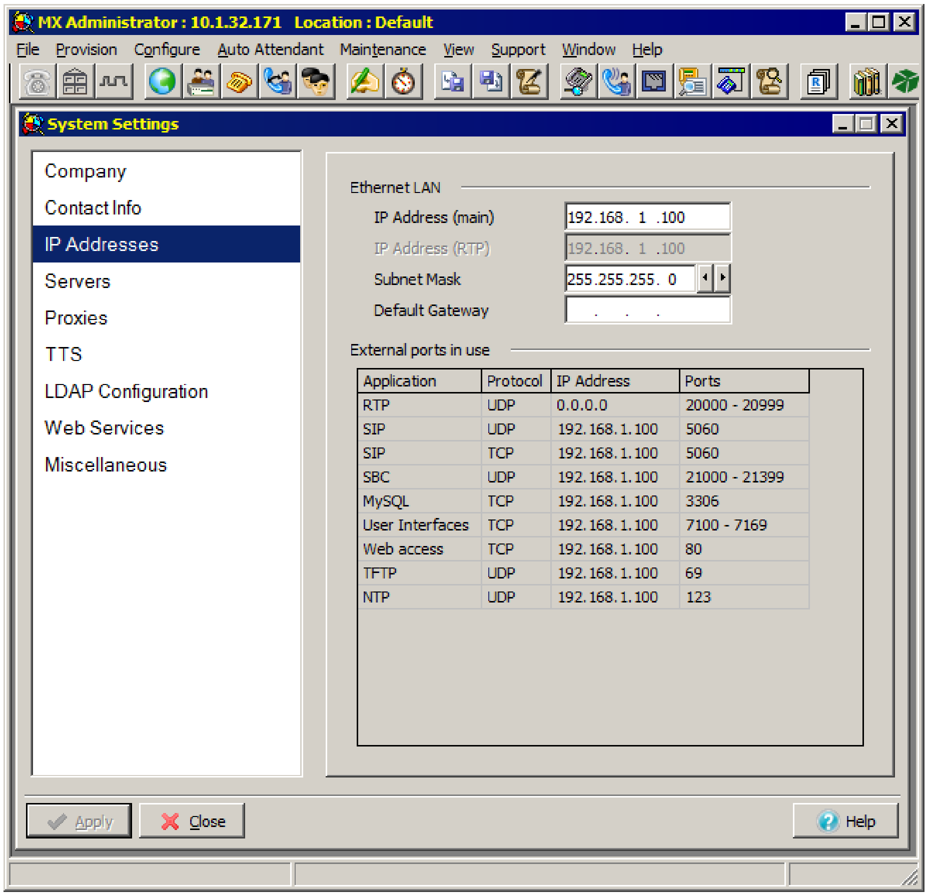
Company	
First Name	
Last Name	
Title	

Contact Numbers

Office	
Mobile	
Emergency	
Primary E-mail	
Secondary E-mail	

20.4 Configuring the MX-E's IP Address:

1. Select IP Addresses
2. Enter the IP Address obtained from the Administrator to be associated with the MX-E.
   - Main IP Address: Used for all connections to the MX-E
   - RTP IP Address: used for RTP communication only
   - Subnet Mask: Subnet mask for the local network


MX Administrator : 10.1.32.171 Location : Default
File Provision Configure Auto Attendant Maintenance View Support Window Help
System Settings
Company
Contact Info
IP Addresses
Servers
Proxies
TTS
LDAP Configuration
Web Services
Miscellaneous
Apply
Close
Help

Ethernet LAN

IP Address (main) 192.168. 1 .100

IP Address (RTP) 192.168. 1 .100

Subnet Mask 255.255.255. 0

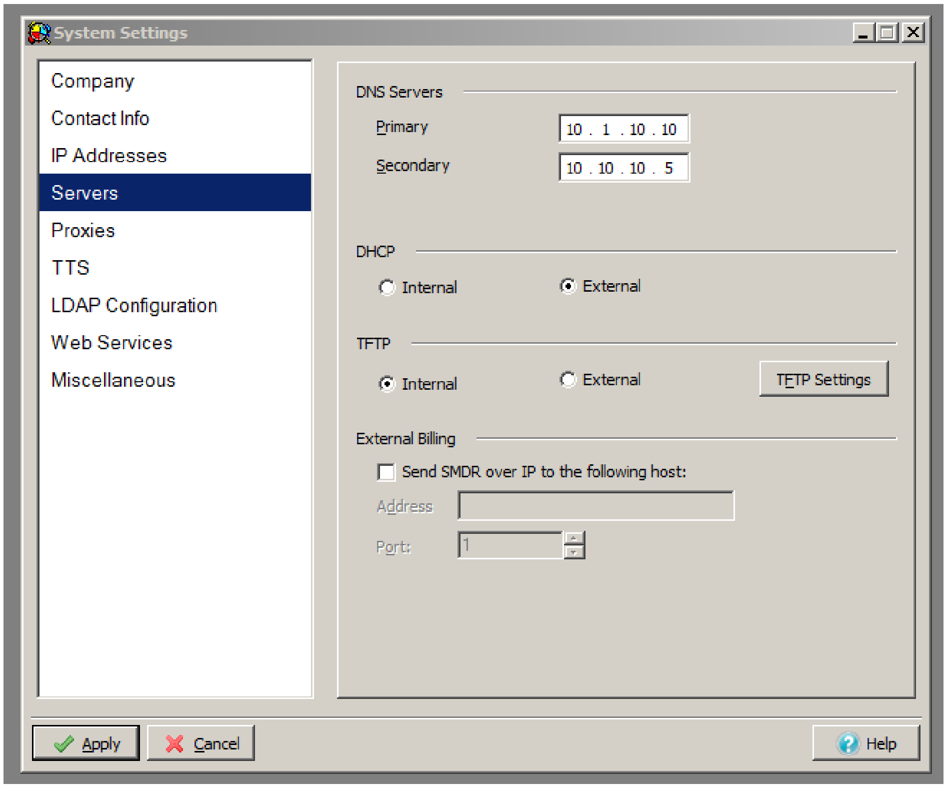
Default Gateway . . .

External ports in use

Application	Protocol	IP Address	Ports
RTP	UDP	0.0.0.0	20000 - 20999
SIP	UDP	192.168.1.100	5060
SIP	TCP	192.168.1.100	5060
SBC	UDP	192.168.1.100	21000 - 21399
MySQL	TCP	192.168.1.100	3306
User Interfaces	TCP	192.168.1.100	7100 - 7169
Web access	TCP	192.168.1.100	80
TFTP	UDP	192.168.1.100	69
NTP	UDP	192.168.1.100	123

Note: All IP Addresses must be outside the scope of any DHCP Server.

20.5 System Settings – Servers



DNS Servers

Primary 10 . 1 . 10 . 10

Secondary 10 . 10 . 10 . 5

DHCP

○ Internal ● External

TFTP

● Internal ○ External

External Billing

□ Send SMDR over IP to the following host:

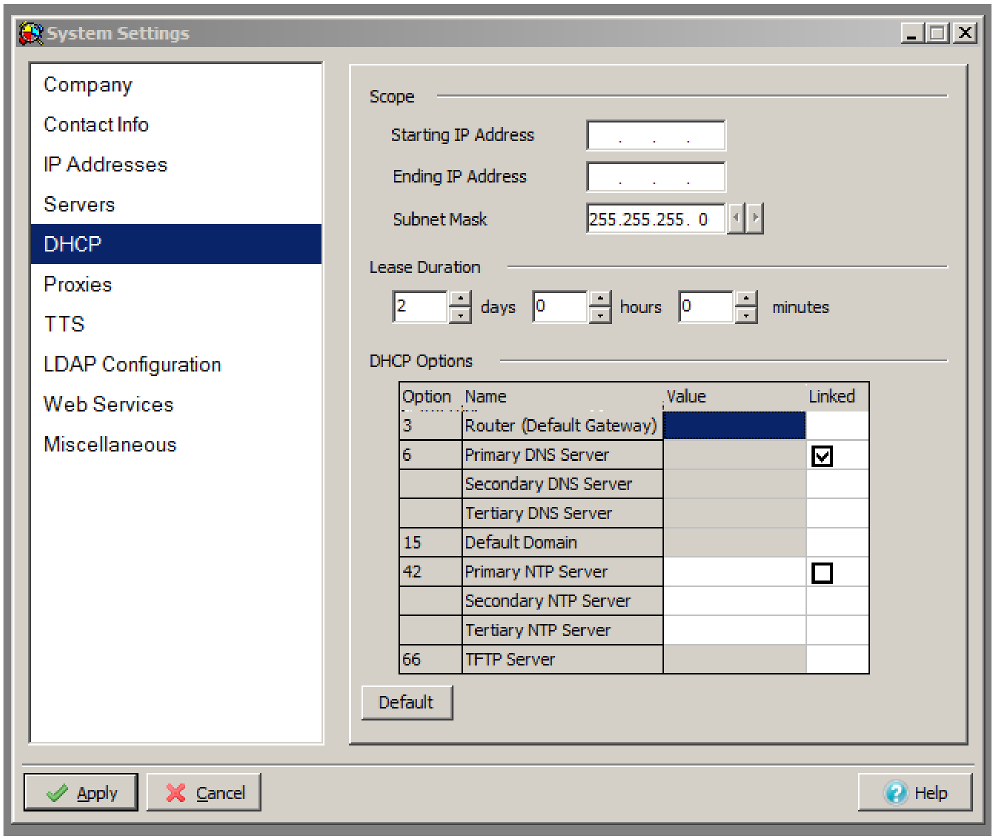
Address

Port: 1

1. Select Servers
2. Fill in the DNS server address
3. Set the “DHCP” to internal or external.

   Prior to Release 11.0.2, the MX-E did not support an internal DHCP server. Release 11.0.2 and higher versions provide internal DHCP server support.

   The DHCP menu choice appears only when DHCP is set to internal, that is the MX-E is providing DHCP to the network. If there is an existing DHCP server, this MUST be set to External.



Scope

Starting IP Address: . . .

Ending IP Address: . . .

Subnet Mask: 255.255.255. 0

Lease Duration

2 days 0 hours 0 minutes

DHCP Options

Option	Name	Value	Linked
3	Router (Default Gateway)		
6	Primary DNS Server		☑
	Secondary DNS Server		
	Tertiary DNS Server		
15	Default Domain		
42	Primary NTP Server		□
	Secondary NTP Server		
	Tertiary NTP Server		
66	TFTP Server		

Note: There are two options for configuring the system's DHCP settings: Manually and Automatically.

Manually Configuring DHCP Settings:

- Set the first IP address to be served
- Set the last IP address to be served
- Set option 3, Router (Default Gateway) to the edge router
  - Set option 6, DNS server to a valid DNS server available from the network administrator
  - Set option 42, NTP server to a valid NTP server available from the network administrator

Automatic Configuration of DHCP Settings:

- Click on the "Default" Button located below the DHCP Options field.

4. Set “TFTP” to **Internal**

   –

5. External Billing: Allows the MX-E system to send billing to an external station message-detail recording (SMDR) host. To enable, place a check in the Send SMDR over IP filed, then enter the AI Address and TCP port .

20.6 Configuring Proxies:

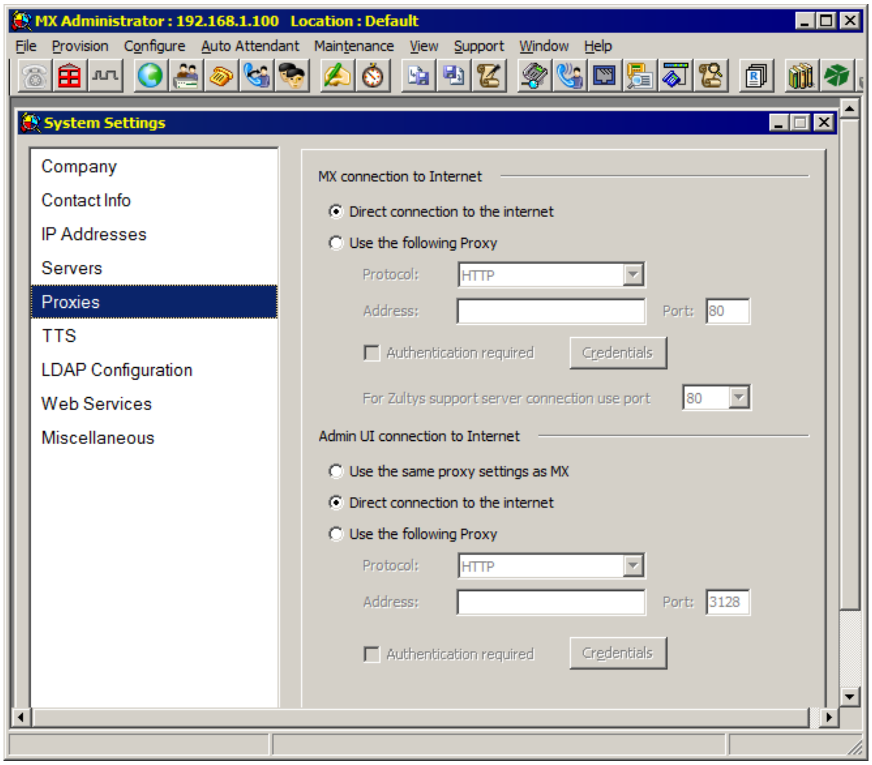
Both the MX-E and the MX-E Administrator must access the Internet to convert Text to Speech, or to communicate with external servers such as ITSPs. The MX-E uses real-time text to speech conversion in the Advanced Auto Attendant and the MX-E Administrator uses Text to speech conversion to generate scripts for Auto Attendants.

Select the Proxies Tab of the System Properties screen.

- Configuring the MX-Es connection to the Internet:
  - If the MX-E has direct access to the Internet, select Direct Connection.
  - If the MX-E must use a proxy server to access the Internet configure the desired Proxy server.

Note: if the Proxy server requires authentication, put a check in the Authentication required box and then enter the login information by clicking on Credentials.

- Configuring the MX-E Administrator’s connection to the Internet:
  - Similar to the MX-E, your choices are to use the same settings as the MX-E, Allow direct connection or to enter a different proxy server.


MX Administrator : 192.168.1.100 Location : Default
File Provision Configure Auto Attendant Maintenance View Support Window Help
System Settings
Company
Contact Info
IP Addresses
Servers
Proxies
TTS
LDAP Configuration
Web Services
Miscellaneous

MX connection to Internet

● Direct connection to the internet

○ Use the following Proxy

Protocol: HTTP

Address: Port: 80

□ Authentication required Credentials

For Zultys support server connection use port 80

Admin UI connection to Internet

○ Use the same proxy settings as MX

● Direct connection to the internet

○ Use the following Proxy

Protocol: HTTP

Address: Port: 3128

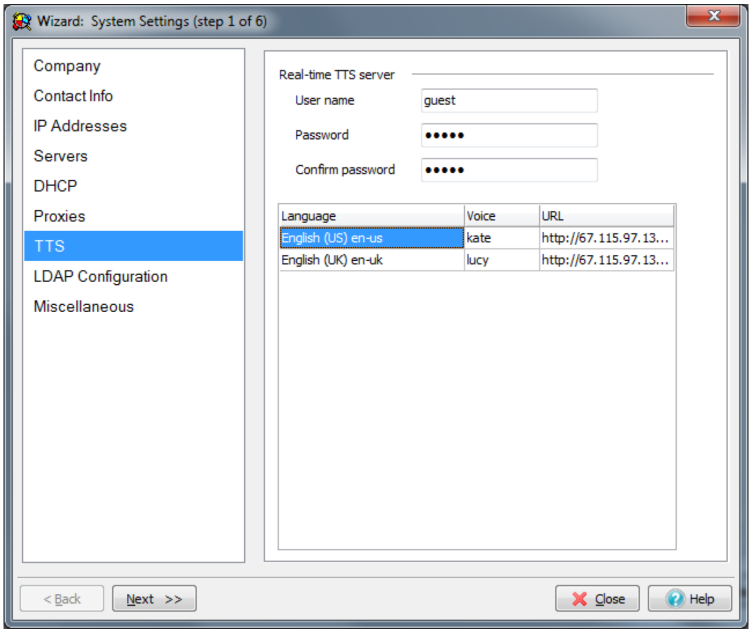
□ Authentication required Credentials

20.7 Configuring real-time TTS Server Settings:

You can configure the real-time text-to-speech (TTS) server to use either a local TTS or to use the standard TTS server located at Zultys.

To configure the MX-E to use the TTS server at Zultys please refer to the figure below:

- Enter the User Name: **guest**
- Enter and re-enter the Password: **guest**
- Right-click and add a new language option:
  - select the desired language:
  - Select the desired Voice:
  - Enter the URL: **http://67.115.97.13/tts.asp**



Real-time TTS server

User name: guest

Password: •••••

Confirm password: •••••

Language	Voice	URL
English (US) en-us	kate	http://67.115.97.13...
English (UK) en-uk	lucy	http://67.115.97.13...

20.8 LDAP Integration

With LDAP authentication, users can login using the same password whether by local area network, intranet, e-mail, etc.

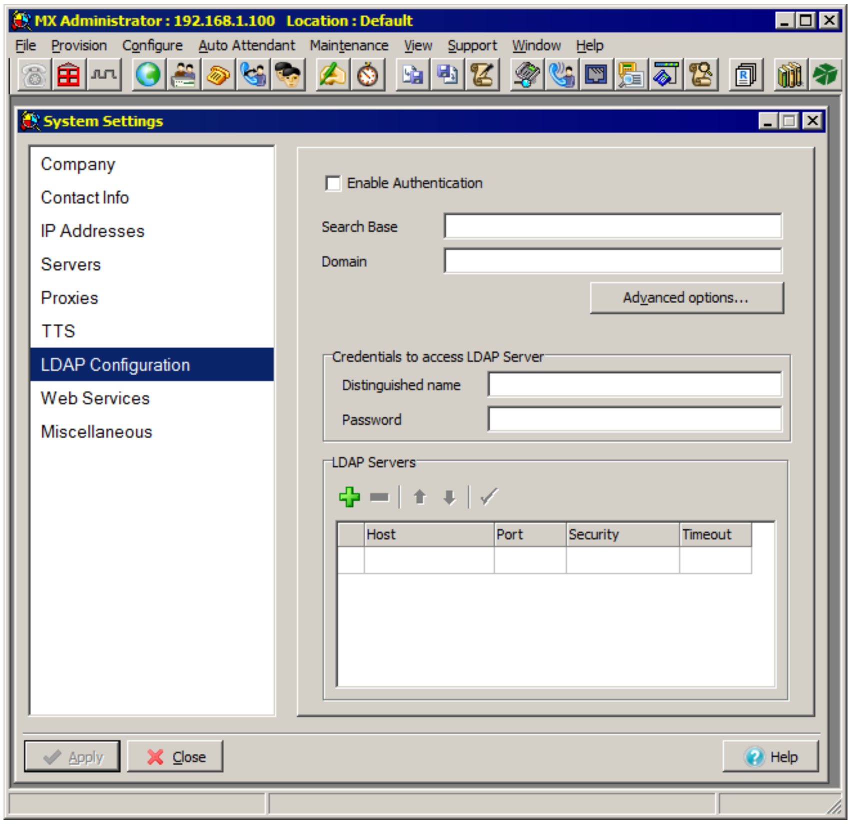
To use LDAP authentication, LDAP service first must be enabled on each MX-E PBX.

An LDAP authentication privilege then is assigned to each user. Through the MX-E Administrator, an administrator can configure a user's profile to authenticate either by using a local password, which is stored and verified on the MX-E, or from an LDAP server. An LDAP authentication privilege can be removed at any time from the user's profile, as well.

Users with LDAP authentication use their domain passwords to login to the MXIE unified communications interface.

Administrators with LDAP authentication use their domain passwords to login to the MX-E Administrator.

No LDAP cache is used by the MX-E and there is no automatic fail-over to local passwords. If an LDAP server is unreachable, authentication cannot be provided to users or administrators and their login attempt will be rejected. A best practice is to use two or more LDAP servers to achieve redundancy and reliability in case of an LDAP server failure.



1. Click on the checkbox to *Enable Authentication*.

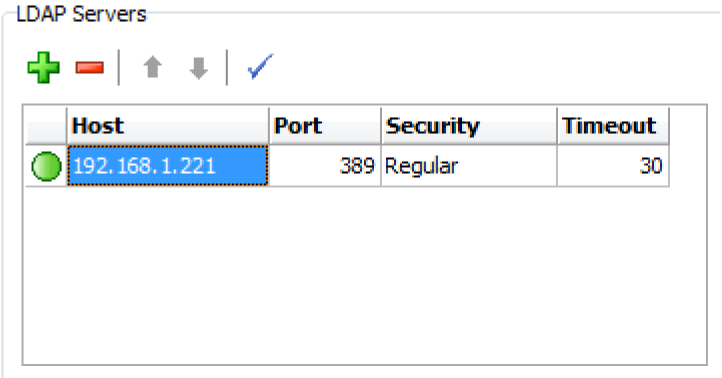
2. Key in the data fields.

   - **Search Base**: This is the LDAP path to where all the users reside in the LDAP directory
   - **Domain**: This is the LDAP domain
   - **Distinguished Name**: Name/Account used to log into the LDAP directory to search for user credentials
   - **Password**: Password associated with the distinguished name

3. In the *LDAP Servers* block, click on the green + button (✚), to add an LDAP server.

4. Enter data for *Host*, *Port*, *Security* and *Timeout.*

   - **Host**: IP of FQDN of LDAP Server
   - **Port**: Port used to communicate with the LDAP server
   - **Security**: Security options
     - **Regular**: unencrypted communications
     - **SSL/TLS**: SSL/TLS Protocol used in encryption
     - **Start TLS**: StartTLS Protocol used in encryption
   - **Timeout**: time out in seconds



LDAP Servers

	Host	Port	Security	Timeout
●	192.168.1.221	389	Regular	30

5. For redundancy, additional servers should be added. If one server is unreachable, the MX-E system automatically will attempt to use a secondary server. Click on the ✚ button again to add additional servers.

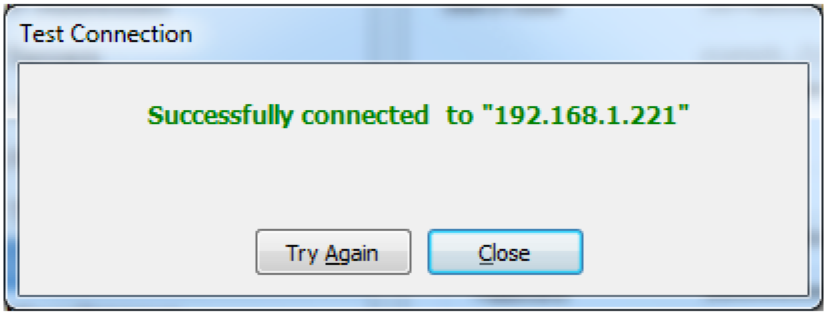
6. Click on the **Apply** button when done.

20.8.1 Removing a connection/server

To remove a server highlight server entry and click on the red minus sign (▬), there is no warning, it is simply removed.

20.8.2 Testing a connection/server

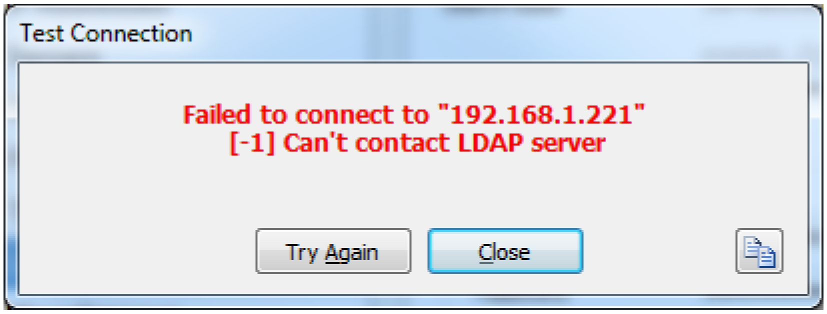
Clicking on the blue check mark (✓), will allow you to test the connection to the LDAP server, if it is a successful connection the following message will be displayed.



Test Connection

Successfully connected to "192.168.1.221"

If the test fails to connect to the LDAP server the following message will be displayed, and it will indicate the reasons for failing.



Test Connection

Failed to connect to "192.168.1.221"
[-1] Can't contact LDAP server

20.8.3 Reordering the servers

You can change the order of the connections/servers by highlighting the appropriate server and clicking the up and down arrows (⬆ ⬇).

20.8.4 LDAP System Service Status

The status of the connection between the MX-E and the LDAP server is indicated by a green circular icon next to the LDAP server entry in the LDAP server table. If the connection is lost between the MX-E and the LDAP server the circular icon will change to a grey color to indicate it is not able to communicate with the LDAP Server.

20.9 Configuring Misc. Tab Settings:

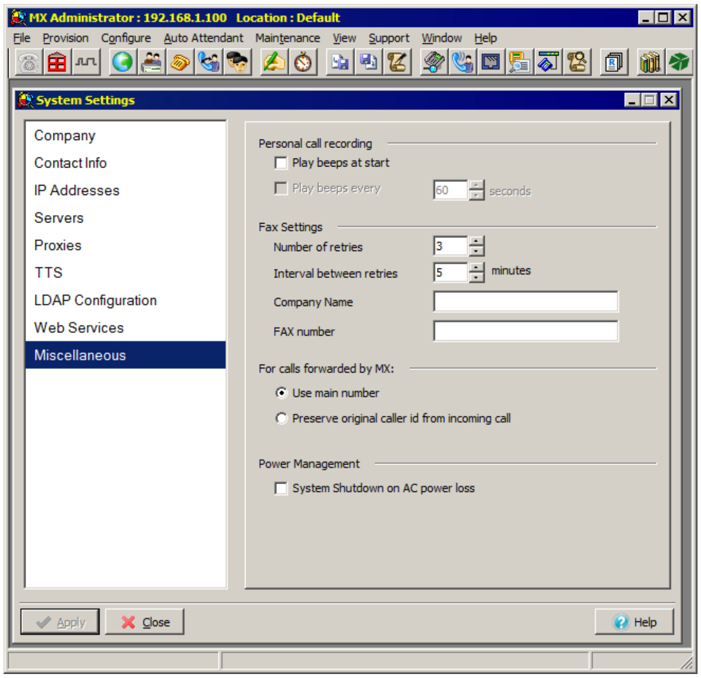
The Misc. Tab allows you to configure various settings: First if you need to play a call recording tone and how often, second the number of retries the Fax server will attempt, third the callerID handling of calls forwarded by the MX-E, and lastly, system shutdown on a power loss.

1. From the System Settings screen click on the Misc. Tab.
2. Configuring Personal Call Recording tones:
   - If you are required to play a call recording tone, put a check in the Play Beeps at start box.
   - Configure how often you want to play the beeps
3. Configuring Fax Server Settings:
   - Configure the desired number of retries
   - Configure the desired interval
   - Default company name
   - Default company fax number
4. Configuring the phone number passed by the MX-E when forwarding calls
   - Use main number or Preserve original caller ID.

5. Configure if the system shuts down on AC power loss.
   - This is used on the MX-E with the APC PowerChute shutdown kit. The MX-E will shut down when it receives a low battery signal from the APC UPS unit.

Note: The carrier must support this functionality

When finished, click on Apply and the system will restart.


MX Administrator : 192.168.1.100 Location : Default
File Provision Configure Auto Attendant Maintenance View Support Window Help
System Settings
Company
Contact Info
IP Addresses
Servers
Proxies
TTS
LDAP Configuration
Web Services
Miscellaneous
Apply
Close
Help

Personal call recording

□ Play beeps at start

□ Play beeps every 60 seconds

Fax Settings

Number of retries 3

Interval between retries 5 minutes

Company Name

FAX number

For calls forwarded by MX:

● Use main number

○ Preserve original caller id from incoming call

Power Management

□ System Shutdown on AC power loss

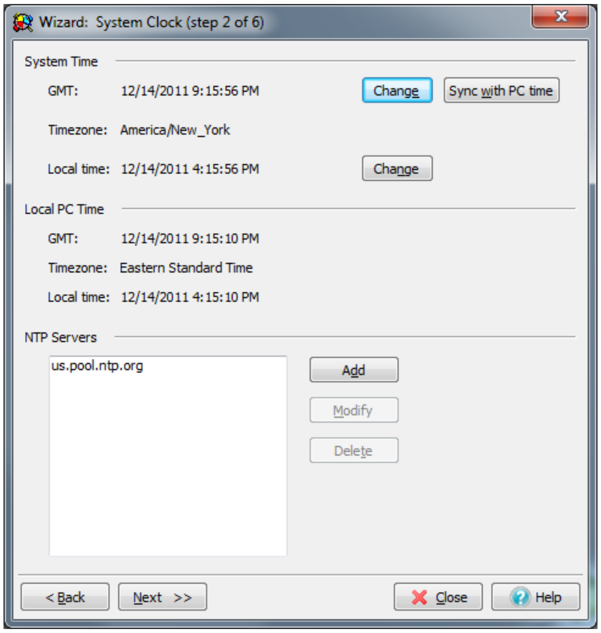
20.10 Setting the System Clock

With an MX-E the procedure is to set the date and time manually and reboot the MX-E. After the MX-E has booted up, the Network Time Protocol (NTP) server(s) should be specified. The MX-E functions both as an NTP Client synchronized to an external NTP Server and also as an NTP Server providing time information to connected telephones. It is critical in MXnetwork that all nodes have the same time.

Note: *NTP will not be able to synchronize if the time difference between the MX-E internal clock and the time returned from the server is too great. That is why the time is set manually before specifying the NTP servers. NTP Time Servers can be found using any search engine and looking for NTP Server. This website is also a valuable reference:* http://support.ntp.org/bin/view/Servers/WebHome

20.10.1 Syncing MX-E with Local PC Clock

1. Go to Provision → System Clock.
2. Click on the Sync with PC Time button.



System Time

GMT: 12/14/2011 9:15:56 PM

Timezone: America/New_York

Local time: 12/14/2011 4:15:56 PM

Local PC Time

GMT: 12/14/2011 9:15:10 PM

Timezone: Eastern Standard Time

Local time: 12/14/2011 4:15:10 PM

NTP Servers

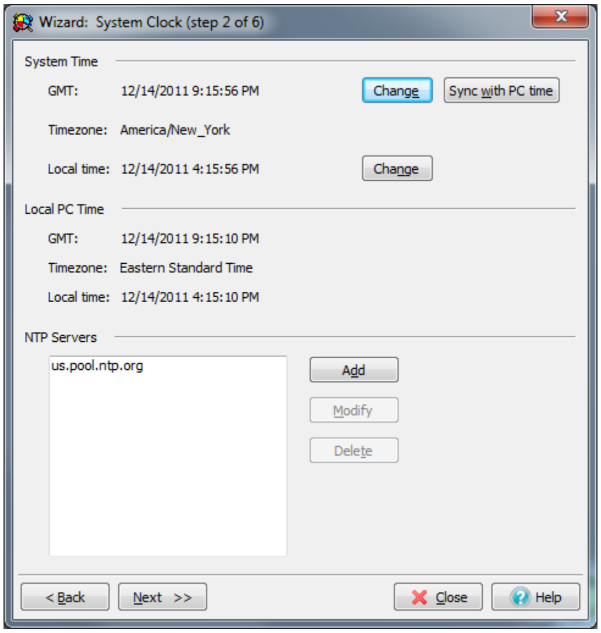
us.pool.ntp.org

20.10.2 Adding NTP Servers:

NTP is a protocol designed to synchronize the clocks of computers over a network. Time is inherently important to the function of routers and networks. It provides the only frame of reference between all devices on the network. This makes synchronized time extremely important. Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible. When it comes to security, if you cannot successfully compare logs between each of your routers and all your network servers, you will find it very hard to develop a reliable picture of an incident. Finally, even if you are able to put the pieces together, unsynchronized times, especially between log files, may give an attacker with a good attorney enough wiggle room to escape prosecution.

Once the MX-E has been synchronized to local time, it is possible to add a NTP Server.

1. From the NTP Server area, select add.
2. Add the following NTP Servers.
   - us.pool.ntp.org
3. Click Next.



Wizard: System Clock (step 2 of 6)

System Time

GMT: 12/14/2011 9:15:56 PM

Timezone: America/New_York

Local time: 12/14/2011 4:15:56 PM

Local PC Time

GMT: 12/14/2011 9:15:10 PM

Timezone: Eastern Standard Time

Local time: 12/14/2011 4:15:10 PM

NTP Servers

us.pool.ntp.org

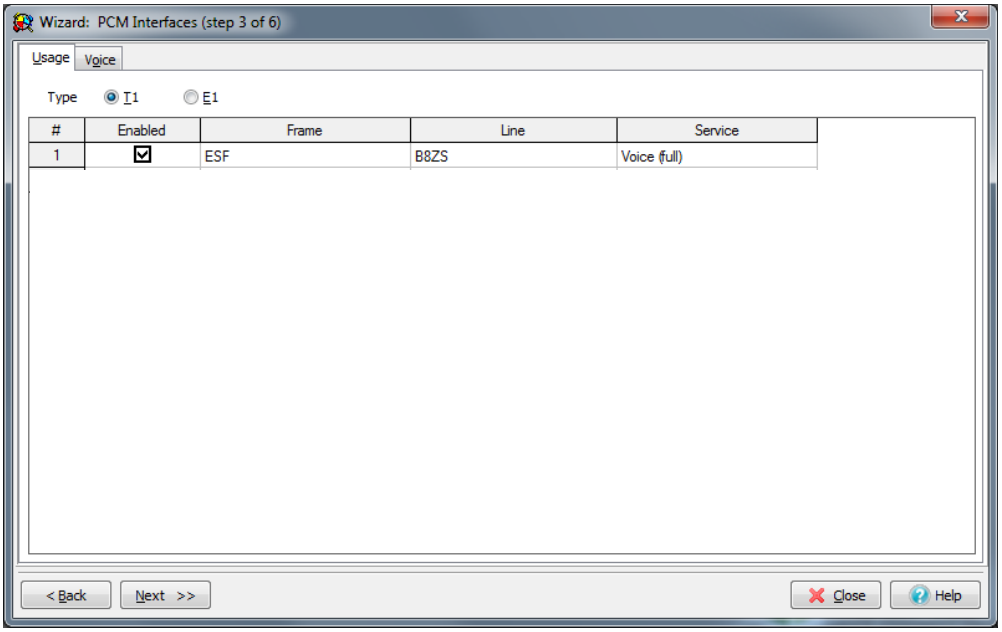
20.11 Provisioning the PCM Usage

One PCM Card (DTE) can be configured to support either T1 or E1 Line Protocols. The port can then be configured independently to support the appropriate Framing and Line Coding Protocols. Further, the port can be configured to support Voice (Full) or Voice (Fractional) service.

20.12 Provisioning Usage:

Click Next, if your MX-E is provisioned with a PCM card, you will be given the option to configure it. If no PCM card is installed, this step will be skipped.

1. Click on the check box for port 1 to enable
2. Click on “Line” and select a line type
3. Click on “Frame” and select a frame type
4. Select service type



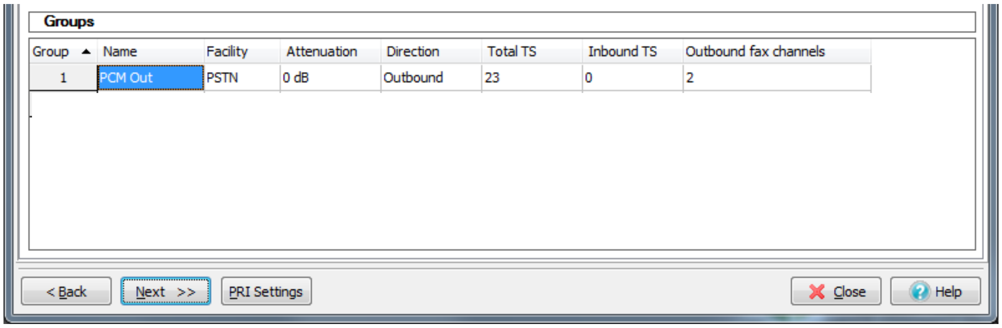
Wizard: PCM Interfaces (step 3 of 6)

Type ● T1 ○ E1

#	Enabled	Frame	Line	Service
1	☑	ESF	B8ZS	Voice (full)

20.13 Provisioning the PCM Voice Usage

Under the “Groups” heading.



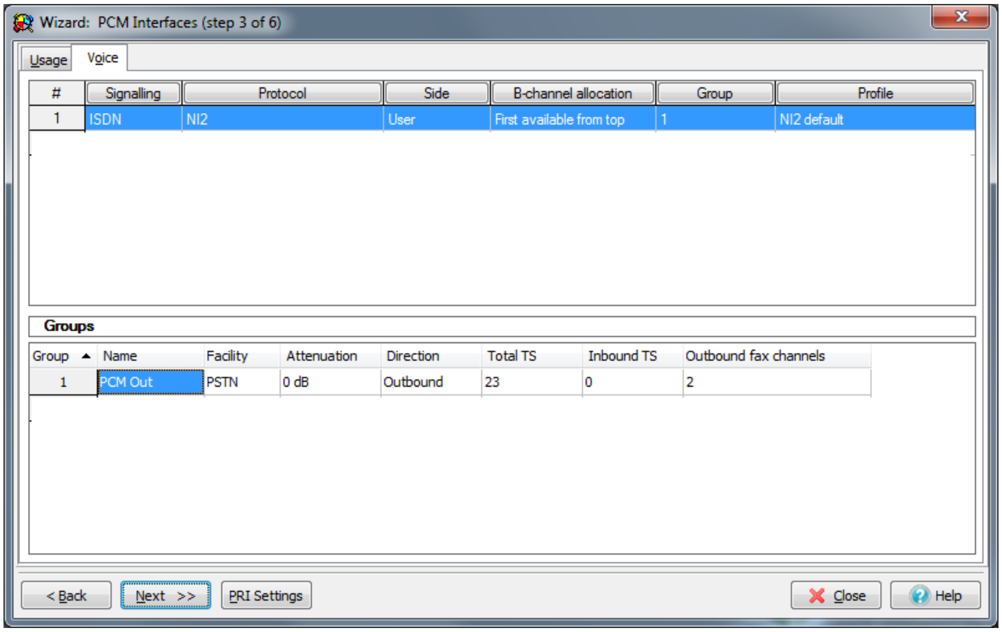
Groups

Group ▲	Name	Facility	Attenuation	Direction	Total TS	Inbound TS	Outbound fax channels
1	PCM Out	PSTN	0 dB	Outbound	23	0	2

1. Double click on the default group and change name from default
2. Click on the “Facility” field and select facility type
3. Click on the “Inbound TS” field and enter of time slots to reserve for incoming calls only
4. Click on Outbound FAX channels and enter of time slots to reserve for faxes
5. Configuring Individual Interfaces
   - In row 1 (port 1) set the “Signaling” type
   - In row 1 (port 1) change the “Protocol” type
   - In row 1 (port 1) change the “Side”

Note: “Side” configures the port for a specific protocol language. In the Case of ISDN, the Network side uses the “NT” protocol while the User side uses the “TE” protocol.

- In row 1 (port 1) enter the “group” with number



#	Signalling	Protocol	Side	B-channel allocation	Group	Profile
1	ISDN	NI2	User	First available from top	1	NI2 default

Group	Name	Facility	Attenuation	Direction	Total TS	Inbound TS	Outbound fax channels
1	PCM Out	PSTN	0 dB	Outbound	23	0	2

20.14 Provisioning the Analog FXO circuits

Click Next, if your MX-E is provisioned with a FXO card, you will be given the option to configure it. If no FXO card is installed, this step will be skipped.

20.14.1 Configuring Groups:

1. Under the “Group” area change the Default Group name to PSTN
2. Right click to add a new Group
3. Set the number of DID digits to be equal to the number of digits the internal extension numbers are for all groups

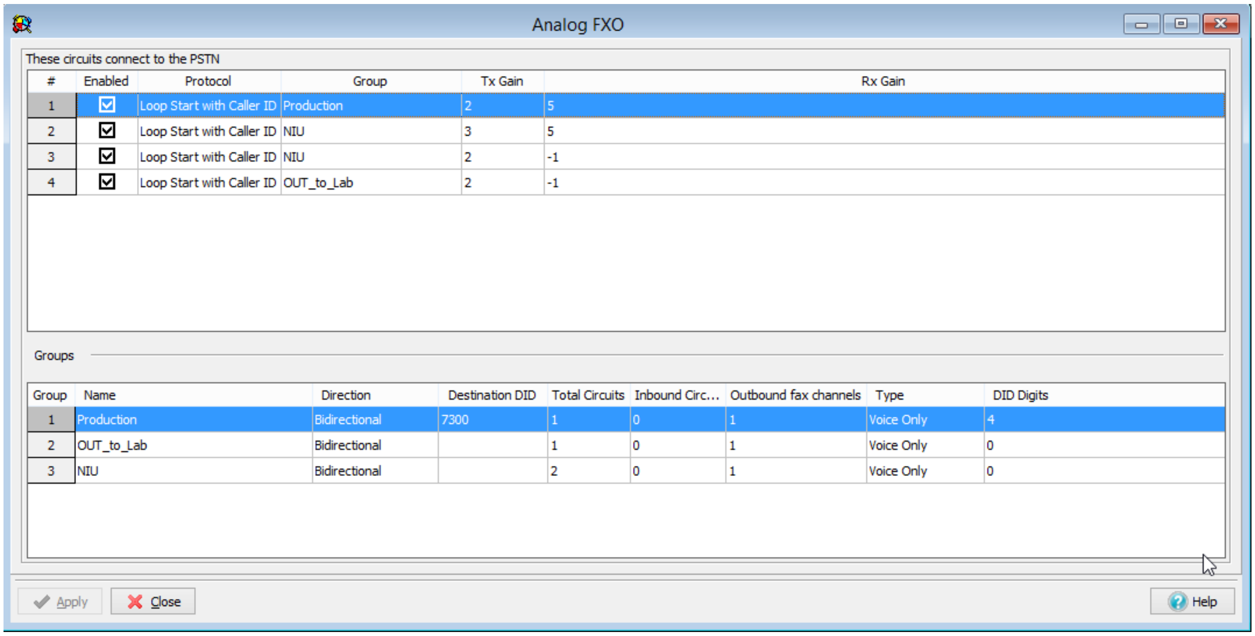
Note: No analog calibration is required on FXO ports of the MX-E system!

Note: Ports configured as “Fax Only” are internally connected to the MX-E Fax Server allowing specific FXO circuits to be routed to ACD group fax boxes. The association is configured in the “ACD & Operators” screen.

Note: If a Group is configured as Inbound, it will not be available as a resource in the Dial Plan

20.14.2 Configuring Ports:

1. Enable all ports that will be used
2. Select the signaling Protocol
   - Loop Start
   - Loop Start with no dial tone
   - Loop Start with Caller ID
   - Ground Start
   - Ground Start with Caller ID
   - Loop Start with DID
   - Loop Start Battery Reversal
3. Select the appropriate group the trunks will belong to
4. In the Destination DID enter in the extension/voice service number the trunk will ring to



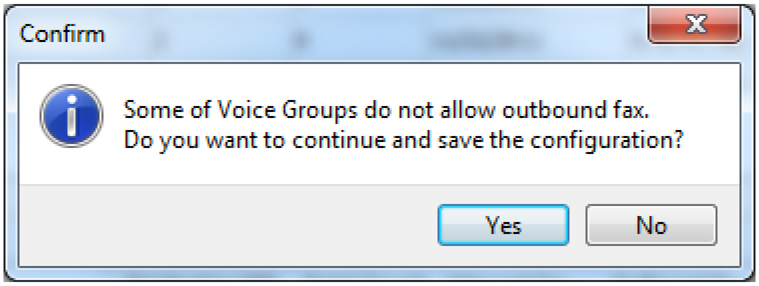
These circuits connect to the PSTN

#	Enabled	Protocol	Group	Tx Gain	Rx Gain
1	☑	Loop Start with Caller ID	Production	2	5
2	☑	Loop Start with Caller ID	NIU	3	5
3	☑	Loop Start with Caller ID	NIU	2	-1
4	☑	Loop Start with Caller ID	OUT_to_Lab	2	-1

Groups

Group	Name	Direction	Destination DID	Total Circuits	Inbound Circ...	Outbound fax channels	Type	DID Digits
1	Production	Bidirectional	7300	1	0	1	Voice Only	4
2	OUT_to_Lab	Bidirectional		1	0	1	Voice Only	0
3	NIU	Bidirectional		2	0	1	Voice Only	0

5. You will be prompted that you will need to assign the FAX Groups.



Confirm

Some of Voice Groups do not allow outbound fax.
Do you want to continue and save the configuration?

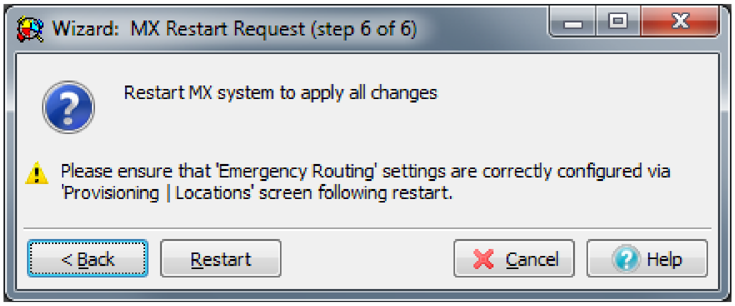
6. Click on OK to continue and the system will reboot.

20.15 Provisioning the Analog FXS circuits

RESERVED

20.16 Reboot

After the wizard complete you will need to reboot the system



Wizard: MX Restart Request (step 6 of 6)

Restart MX system to apply all changes

Please ensure that 'Emergency Routing' settings are correctly configured via 'Provisioning | Locations' screen following restart.

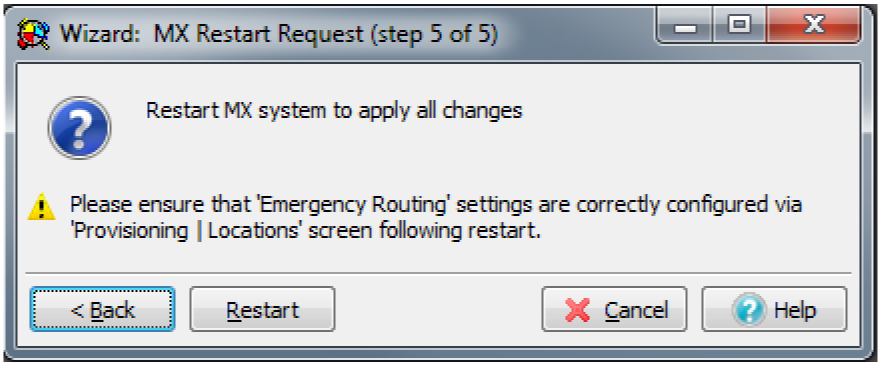
1. Click Restart. (The MX-E will re-boot)
2. The MX-E will re-boot in normal mode and can now be reconnected to the corporate network

   At this time, connect both your PC and the MX-E to a switch.

21. Location / Emergency Calling

The most important part of the installation is configuration of the locations table in the MX-E. The locations table is responsible for handing all emergency calling (911 Calls). If the locations table is not setup or setup incorrectly emergency calling (911 calls) may fail. It is the responsibility of the installer to verify that emergency calling is properly setup and tested before leaving the site.

When the Provisioning Wizard is finished it will alert the installer that after the reboot they should provision the locations table and emergency calling.

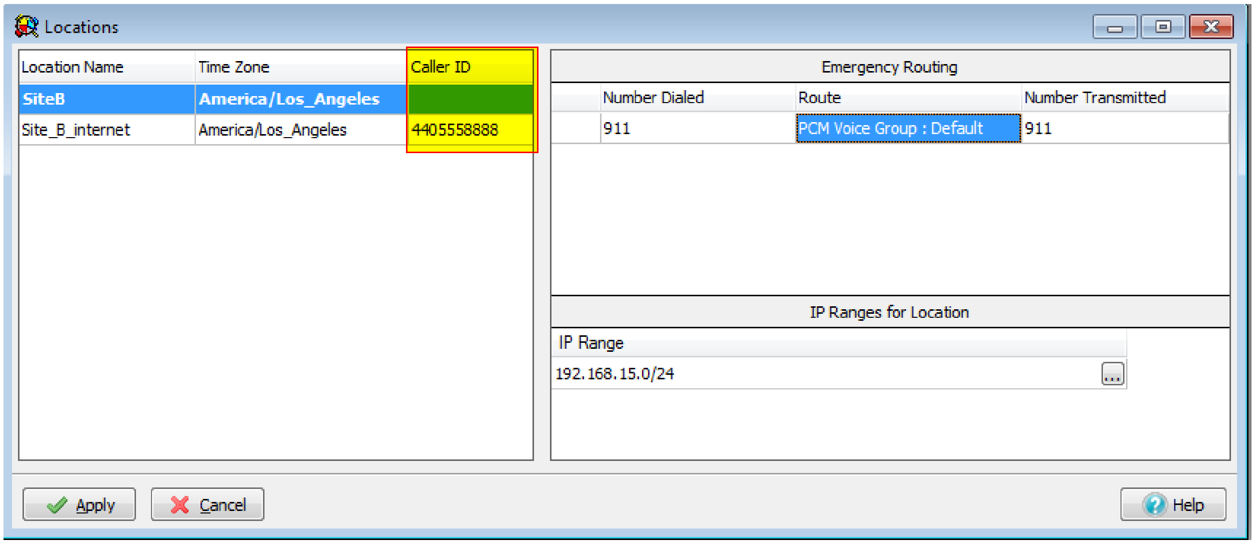

Wizard: MX Restart Request (step 5 of 5)

Restart MX system to apply all changes

Please ensure that 'Emergency Routing' settings are correctly configured via 'Provisioning | Locations' screen following restart.

21.2 Emergency Calling

When an Emergency Call is placed (911 call) the Caller ID configured under Provision → Locations, that number is sent as CID. Should the call be disconnected or the Emergency operator calls that number back the call is automatically routed by the MX-E to the phone or extension of the last user who called 911 from the specific location will ring.


Locations

Location Name	Time Zone	Caller ID
SiteB	America/Los_Angeles	
Site_B_internet	America/Los_Angeles	4405558888

Emergency Routing

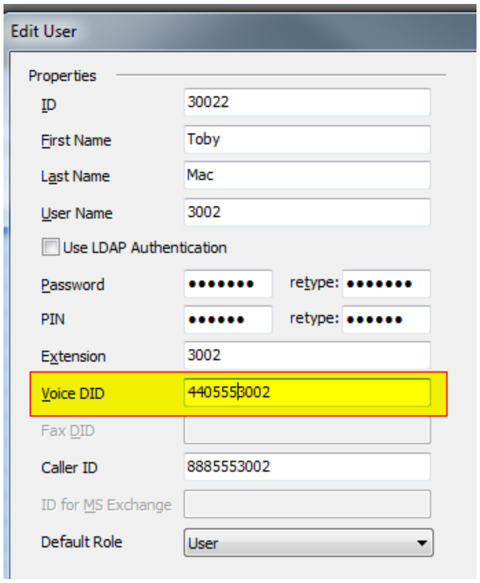
Number Dialed	Route	Number Transmitted
911	PCM Voice Group : Default	911

IP Ranges for Location

IP Range
192.168.15.0/24

This Caller ID number MUST be a dedicated number for this purpose, and cannot be the main number of the company.

If there is no Caller ID and an Emergency Call is placed the MX-E will send the users DID (the DID placed in the users DID field) as Caller ID, even if there is Caller ID configured to the particular user. Calling back will be routed to the particular user, since his/her DID is called.



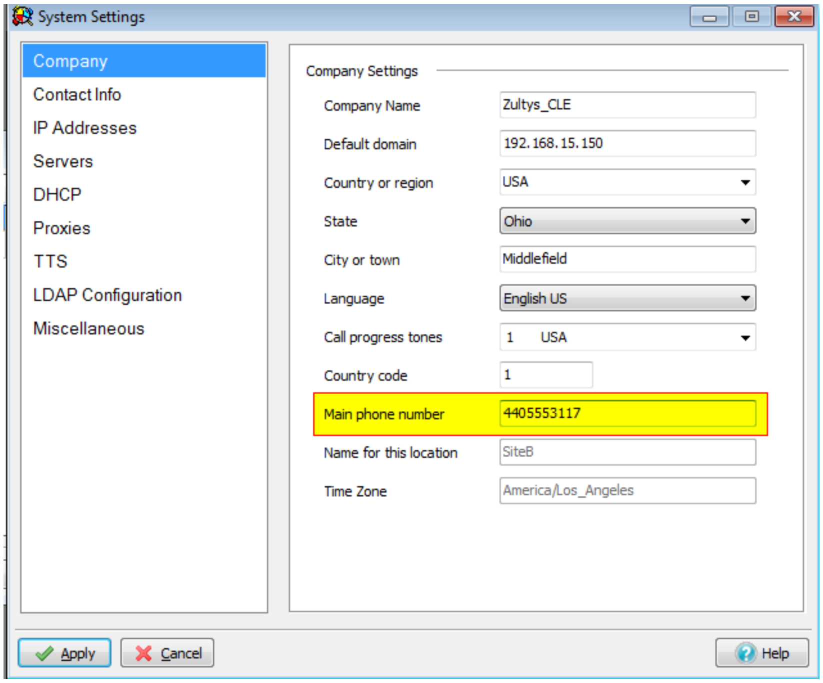
Edit User

Properties

ID	30022		
First Name	Toby		
Last Name	Mac		
User Name	3002		
□ Use LDAP Authentication			
Password	•••••••	retype:	•••••••
PIN	••••••	retype:	••••••
Extension	3002		
Voice DID	4405553002		
Fax DID			
Caller ID	8885553002		
ID for MS Exchange			
Default Role	User		

If there is no DID, no Provision → Locations Caller ID, the Caller ID will be the main company number (as provisioned under Provision → System Settings –

Company Main Number field). Calling back to the main number will use the default routing for calls with unrecognized DID.



System Settings

Company Settings

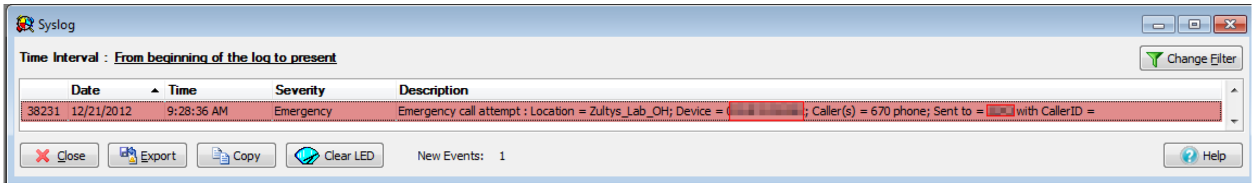
Company Name	Zultys_CLE
Default domain	192.168.15.150
Country or region	USA
State	Ohio
City or town	Middlefield
Language	English US
Call progress tones	1 USA
Country code	1
Main phone number	4405553117
Name for this location	SiteB
Time Zone	America/Los_Angeles

911 dial plans for all locations MUST be configured. Having 911 entries in the normal dial plan does not mark the call as Emergency call. The call will have no priority over the other calls; there will be no pop-up for Operations with information about this call.

21.3 Emergency Call Notification and Actions

When an Emergency Call is placed the following happens automatically by the MX-E

21.3.1 Syslog Event is created in the MX-E's event log



Syslog

Time Interval : From beginning of the log to present

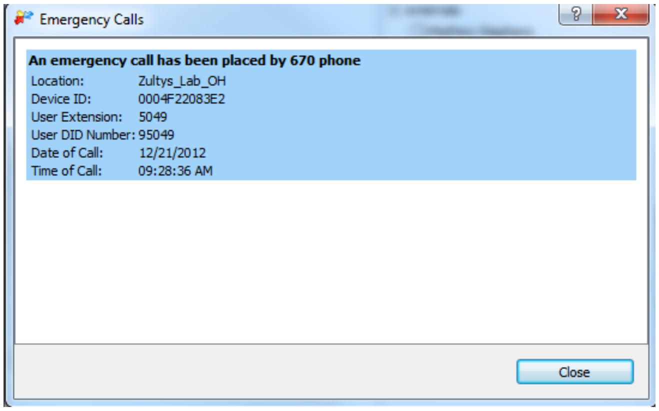
	Date	Time	Severity	Description
38231	12/21/2012	9:28:36 AM	Emergency	Emergency call attempt : Location = Zultys_Lab_OH; Device = ([redacted]; Caller(s) = 670 phone; Sent to = [redacted] with CallerID =

New Events: 1

The description of the event will include the Devices Location, the user assigned to the device and the device ID.

21.3.2 Agents of Operator groups receive IM notification

All agents of an Operator group will receive the following IM indicating an emergency call was placed. No configuration is required; Operator Groups (and only operator groups) automatically receive this IM.

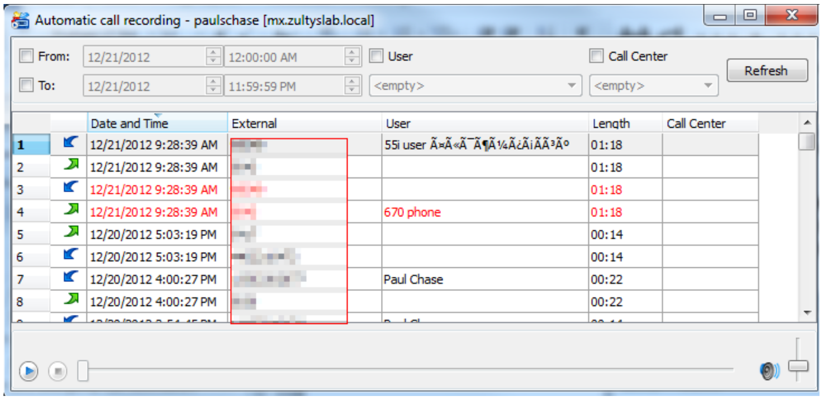


An emergency call has been placed by 670 phone

Location:	Zultys_Lab_OH
Device ID:	0004F22083E2
User Extension:	5049
User DID Number:	95049
Date of Call:	12/21/2012
Time of Call:	09:28:36 AM

21.3.3 Calls Automatically Recorded

Emergency calls are automatically recorded by the MX-E, and does not require a recording license. If the user has access to Emergency Call Recordings in their user profile, they will be listed in RED type



□ From: 12/21/2012 12:00:00 AM □ User □ Call Center
□ To: 12/21/2012 11:59:59 PM <empty> <empty>

		Date and Time	External	User	Length	Call Center
1	↙	12/21/2012 9:28:39 AM	[redacted]	55i user Ã¤Ã«Ã¯Ã¶Ã¼Ã¿Ã¡ÃÃ³Ãº	01:18	
2	↗	12/21/2012 9:28:39 AM	[redacted]		01:18	
3	↙	12/21/2012 9:28:39 AM	[redacted]		01:18	
4	↗	12/21/2012 9:28:39 AM	[redacted]	670 phone	01:18	
5	↗	12/20/2012 5:03:19 PM	[redacted]		00:14	
6	↙	12/20/2012 5:03:19 PM	[redacted]		00:14	
7	↙	12/20/2012 4:00:27 PM	[redacted]	Paul Chase	00:22	
8	↗	12/20/2012 4:00:27 PM	[redacted]		00:22	

21.3.4 Trunks Automatically Freed

If all trunks are in use when an Emergency Call is placed, the MX-E will automatically free a trunk in the trunk group defined by the Emergency Call Routing table to place the Emergency Call.

21.4 Emergency Numbers

Emergency numbers are used to contact emergency service providers. Although these providers are typically external to the enterprise, some companies may have an internal department to service these calls. Emergency dialing rules, as configured on the Locations panel, allow users to dial a number without waiting for a second dial tone. If the rule specifies an external number, the MX-E will drop other calls if necessary to set up the emergency call.

The MX-E allows you to define more than one rule for governing emergency numbers. There are two reasons for having multiple rules.

- Multiple rules allow you to specify internal and external emergency services. For example, one number can call an internal paramedic team while another rule calls an external police or fire department.
- Multiple rules support users located in physical locations separate from the MX-E deployment site.

Users connected to the MX-E at a remote location from the MX-E may require emergency numbers that are different from those that service the MX-E location. For example, suppose you have the MX-E in Sunnyvale, California with a user working from a Chicago branch office; the remote user is connected over a VPN to the MX-E.

When a user in Sunnyvale dials 911, the MX-E routes the call to the PSTN and dials 911. When a user in Chicago dials 911, the MX-E dials a long distance number to call the emergency services that serves the Chicago location.

The method that the MX-E employs to determine the location of a user that makes an emergency voice call depends upon the device used to make the call. MXIE provide login options that allow a user to specify the physical location of the device. This selection must accurately reflect the user’s physical position so that emergency services can be dispatched appropriately.

You can also perform emergency chats with phone numbers that are routed to an internal destination.

21.4.1 Emergency Call Location from a ZIP Phone

Zultys IP phones allow the normal location for each phone is specified in the MX-E Administrator device profile panels (Configure → Devices) and that normal location.

21.4.2 Emergency Call Location from MXIE

When logging into MXIE, the user is asked to specify his or her location. When the user dials an emergency number, as configured in the Locations Emergency Routing table, the MX-E transmits the number listed for the number as defined for the user's location.

21.4.3 Conflicting Emergency Call Locations from MXIE and the Phone

If a user tries to bind MXIE to a Zultys IP Phone that has a different location selection, the binding will fail. MXIE will report "In order to bind, the MXIE and the phone must have the same location selection."

21.4.4 Emergency Call Location from Other Devices:

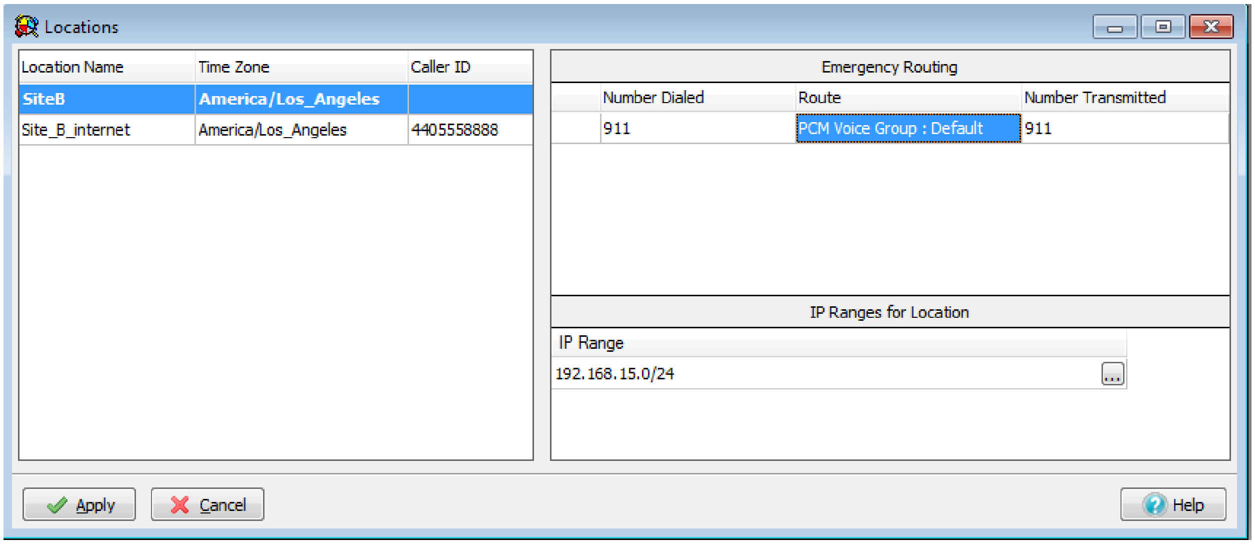
When using other devices, the MX-E will use the following criteria (listed in highest to lowest order of importance) to determine the user's location:

1. MXIE location and binding
2. Subnet or IP address range
3. Default location for MX-E

21.5 Location Table

The Locations panel, as shown in below, identifies the name and time zone location of all enterprise sites serviced by the MX-E, defines Emergency Service contacts for each location, and specifies the range of valid IP addresses for each location. Location names configured in this panel are referenced by other User Interface windows. See System Locations for guidelines on setting up your location settings. To access the Locations window, select Provision → Locations from the main menu. You can specify a maximum of 128 locations on an MX-E system.

This table lists the name, time zone location, connection type, and available bandwidth for each enterprise site served by the MX-E. The first line in the table identifies the primary enterprise location. The table displays this entry in bold typeface.



Location Name	Time Zone	Caller ID
SiteB	**America/Los_Angeles**	
Site_B_internet	America/Los_Angeles	4405558888

Emergency Routing

Number Dialed	Route	Number Transmitted
911	PCM Voice Group : Default	911

IP Ranges for Location

IP Range
192.168.15.0/24

21.5.1 Locations Table Field Definitions

- **Location Name**: This parameter specifies the name of the enterprise site. Each location/site in the enterprise that has a unique IP address should have a new location created for it, unless it is within the same building.
- **Time Zone**: This parameter specifies the time zone where the enterprise site is located. This time zone field is used to identify the time zone for all ZIP2xN phones.
- **Caller ID**: This parameter configures the ANI (Automatic Number Identification), a system utilized by telephone companies to identify the DN (Directory Number) of a calling subscriber that is presented to the carrier when an Emergency Call is placed by the location.

21.5.2 Managing Location Entries

To add an entry to the Locations table, right click the mouse while pointing the cursor in the table and select New. After adding a new location, all SIP devices on the system should be rebooted.

To edit the location name of a current entry, double click in the cell of the name that you wish to change.

To change the Time Zone setting of a current entry, click in the cell of the Time Zone setting, then press the edit button on the right side of the cell to access the Time Zones panel.

To delete an entry from the Locations table, select the entry to be deleted, right click the mouse, and select Delete.

21.5.3 Emergency Routing Table

The Emergency Routing table specifies dialing rules for contacting emergency service providers for each location. Using multiple dialing rules allow you to specify unique emergency numbers for each emergency service provider at every enterprise site.

21.5.4 Managing Dial Rules

Each row within the table lists one emergency dial rule. Rules are created or deleted by right-clicking the mouse while the cursor is pointing in this table. To view the emergency numbers available for an MX-E location, highlight that site within the locations table.

21.5.5 Field Definitions

Each Emergency dialing rule comprises the three parameter settings listed in the table.

- Number Dialed specifies the digit set that, when dialed by a user at the specified location, activates the dialing rule.
- Route specifies the MX-E facility that will transmit the emergency phone number configured by the row.
- Number Transmitted specifies the phone number sent by the MX-E to contact the emergency service provider. The system sends these digits whenever a user located at the specified location dials the digits listed in the Number Dialed column.

To add an emergency contact, right click the mouse while pointing in the Emergency Routing table and select New Phone.

To add an alternate route for an existing emergency number, right click the mouse and select New Route.

To remove an emergency contact or route from the table, highlight the entity to be removed, right click the mouse while pointing in the Emergency Routing table, and select Delete Phone (to remove a number) or Delete Route (to remove an alternate route)

21.6 IP Ranges for Location

The IP Ranges for Location table lists the valid IP Addresses defined for each MX-E location. To view the valid addresses for a site, highlight that location in the Locations table.

The IP Addresses are listed in a set of ranges. Each range is defined either by two IP Addresses or by an IP Address and a Subnet Mask. The IP Range table displays both types of definitions.

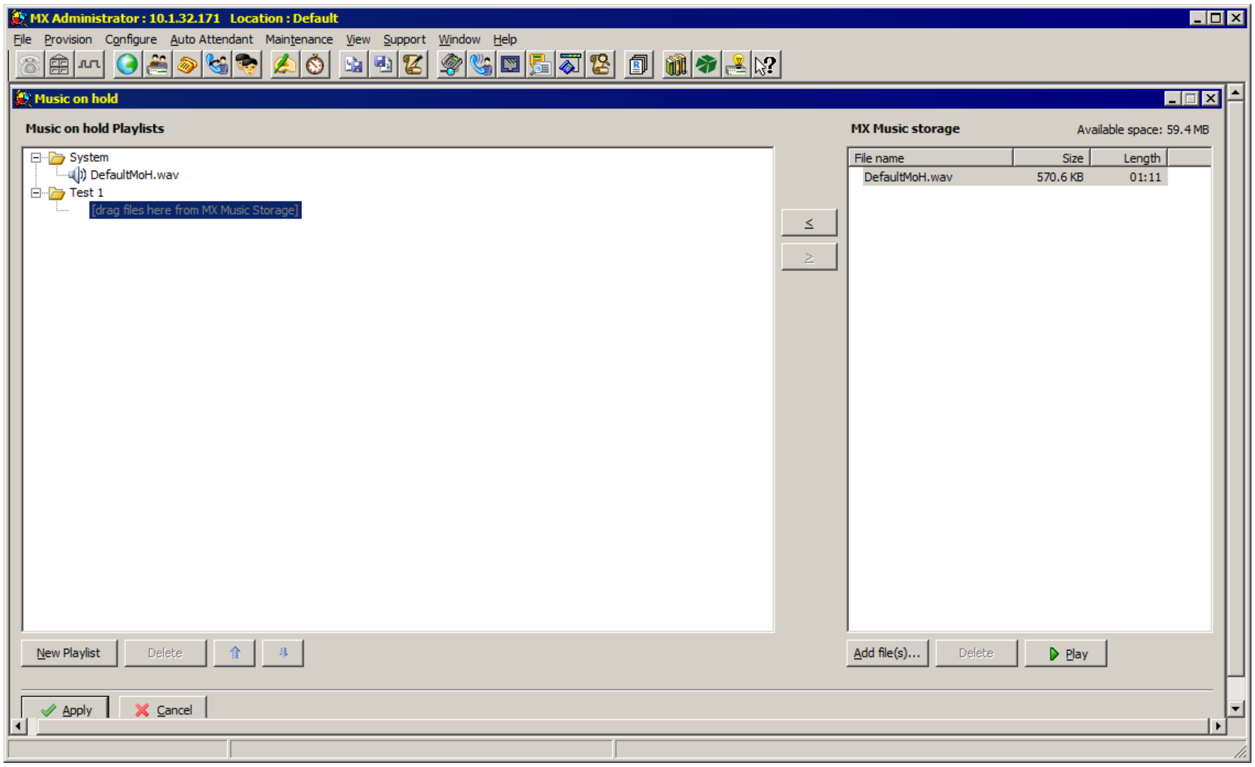
To add, edit, or delete an IP address range for a Location, right click the mouse while pointing in the IP Ranges for Location and select the appropriate option. Pressing New or Edit opens the Edit IP Range panel.

Important: Locations panel changes do not take effect until you press the Apply button. If you press the Cancel button before pressing Apply, all pending changes to the panel are disregarded. Pressing the Apply button saves all pending changes.

22. Music on Hold

Music on Hold is configured in the form of a playlist from MX-E Administrator. To access the configuration window click on Configure and select Audio.

The Music on Hold window appears. This window is divided into two parts. The left side of the window displays the Music on Hold Playlists, and the right side displays the MX-E Music Storage.



22.2 Managing Files in the MX-E Music storage

The MX-E Music Storage displays all audio files that have been uploaded to the MX-E for use as Music on Hold.

- To add more audio files click on the Add File(s) button.

  NOTE: Audio files must be in µ-law format (CCITT u-law, 8 bit, 8 kHz, mono), and must not exceed 15MB. The maximum amount of storage space on the MX-E designated for the audio files is 50MB on MX-E. For suggestions on how to convert audio files to the required format see Appendix A.

- To sort the files in the MX-E Music Storage by name, size or length, click on the column heading.
- To delete audio files that are not currently used in any playlist from the MX-E Music Storage press the Delete button.
- To listen to an audio file, select the file and click the Play button.

- To download an audio file from the MX-E Music Storage, right-click on an audio file and click on Download File(s).
- Click the Apply button to save any changes.

22.3 Configuring System Playlist

The Music on Hold Playlists box contains the System playlist. This is the default playlist for the MX-E system. It plays continuously and calls can enter it at any point in the playlist.

Select the Play Files checkbox and customize the System playlist with the files uploaded to MX-E Music Storage:

1. Drag and drop files from the MX-E Music Storage to add them to a playlist or select a file and press the Add "<" button. The same audio file can be used multiple times.
2. If necessary, select an audio file and press the Remove ">" button, to remove it from the playlist.
3. Drag and drop a file within the playlist to change its position. The files are played in the order in which they are displayed.
4. Click the Apply button to save any changes.

22.4 Configuring New Playlists

Multiple playlists can be created. These playlists will always start at the beginning when a call is first placed on hold. If a call is placed on hold for a second time, the music on hold will resume from the position it was at before the call was picked up and so on for each new hold.

1. Create a new playlist by clicking the New Playlist button and typing in a name for the playlist.

   WARNING: The playlist name cannot be changed once it has been created.
2. Drag and drop files from the MX-E Music Storage to add them to a playlist or select the file and press the Add "<" button. The same audio file can be used multiple times.

3. If necessary, select an audio file and press the Remove “>” button, to remove it from the playlist.
4. Drag and drop a file within the playlist to change its position. The files are played in the order in which they are displayed.
5. Click the Apply button to save any changes.

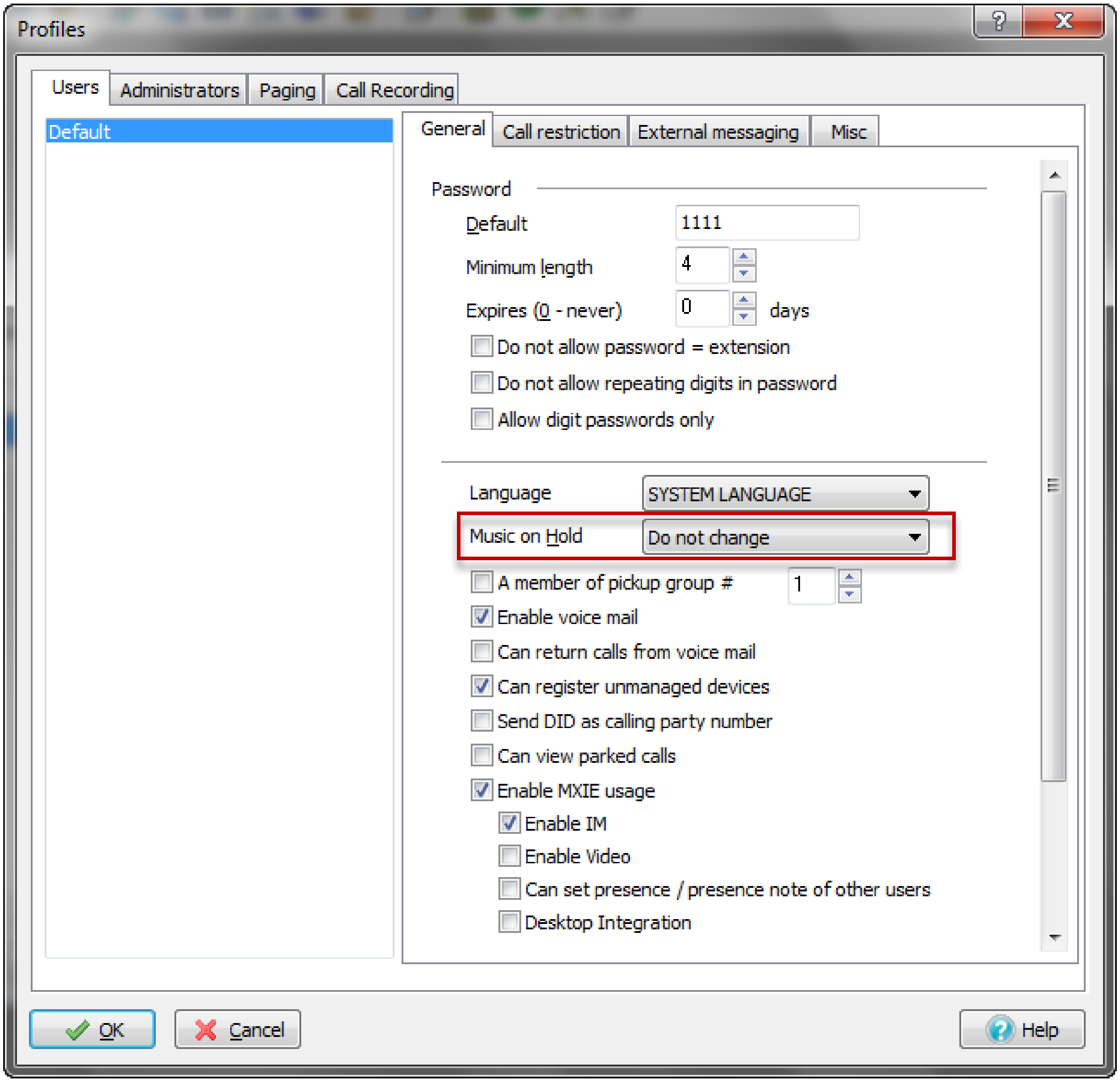
22.5 Assigning Playlists

The music on hold playlist used when a call is placed on hold is determined by the playlist assigned to the call. The playlist assignment is configured in the user profile of the answering user, the settings of the call group (Operator/ACD/Hunt/ICC Group) to where the call is routed or via the transfer action of an automated attendant.

22.5.1 Assigning a Playlist to a User Profile

Select Configure → Users.

In the User window select a user and click on the Profile button.



Password

Default: 1111

Minimum length: 4

Expires (0 - never): 0 days

□ Do not allow password = extension

□ Do not allow repeating digits in password

□ Allow digit passwords only

Language: SYSTEM LANGUAGE

Music on Hold: Do not change

□ A member of pickup group # 1

☑ Enable voice mail

□ Can return calls from voice mail

☑ Can register unmanaged devices

□ Send DID as calling party number

□ Can view parked calls

☑ Enable MXIE usage

☑ Enable IM

□ Enable Video

□ Can set presence / presence note of other users

□ Desktop Integration

In the General tab select a playlist from the Music on Hold drop-down list. The available options are:

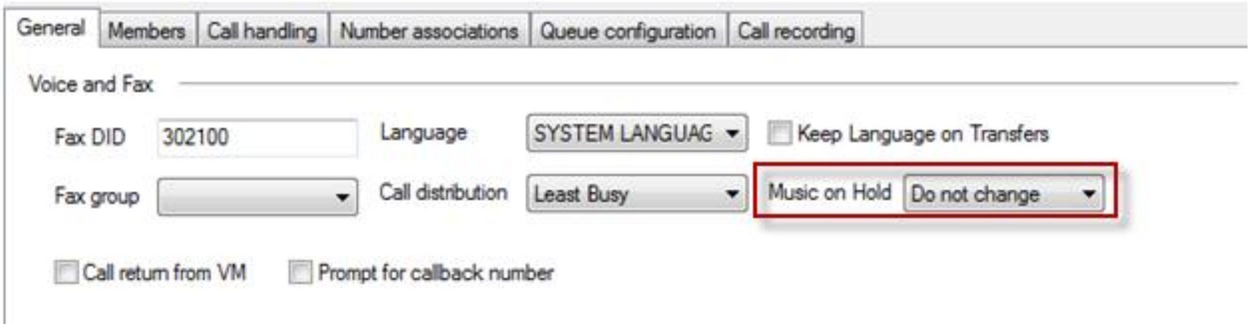
- Do Not Change - If the call is directed to this user through a transfer, it will continue to listen to the same music on hold as its previous destination. If this is the call's initial destination, it will use the System playlist.
- System – Use the System playlist for calls routed to this user.

- Playlist name – Calls routed to this user will use the selected playlist.

Click OK to save changes.

22.5.2 Assigning a Playlist to a Call Group

Select Configure → Operator and Call Groups.



Fax DID 302100

Language SYSTEM LANGUAG

☐ Keep Language on Transfers

Fax group

Call distribution Least Busy

Music on Hold Do not change

☐ Call return from VM

☐ Prompt for callback number

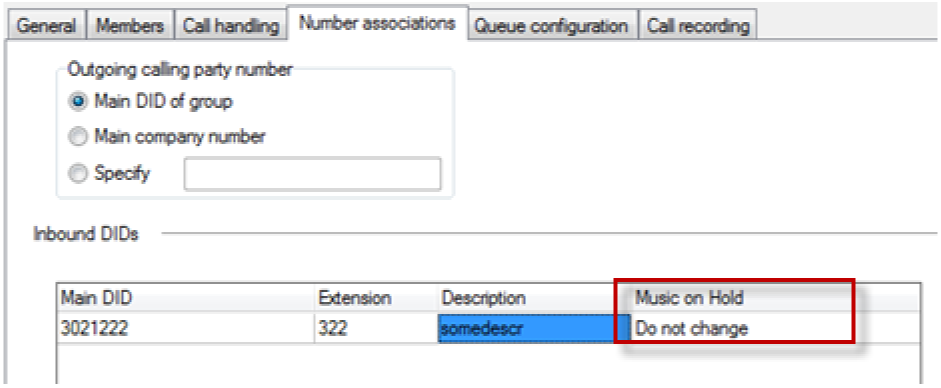
In the General tab select a playlist from the Music on Hold drop-down list. The available options are:

- Do Not Change – If the call is directed to this call group through a transfer, it will continue to listen to the same music on hold as its previous destination. If this is the call's initial destination, it will use the System playlist.
- System – Use the System playlist for calls routed to this call group.
- Playlist name – Calls routed to this call group will use the selected playlist.

Click OK to save changes.

22.5.3 Assigning a Playlist to a Call Group Number Association

Select Configure → Operator and Call Groups.



Outgoing calling party number

● Main DID of group
○ Main company number
○ Specify

Inbound DIDs

Main DID	Extension	Description	Music on Hold
3021222	322	somedescr	Do not change

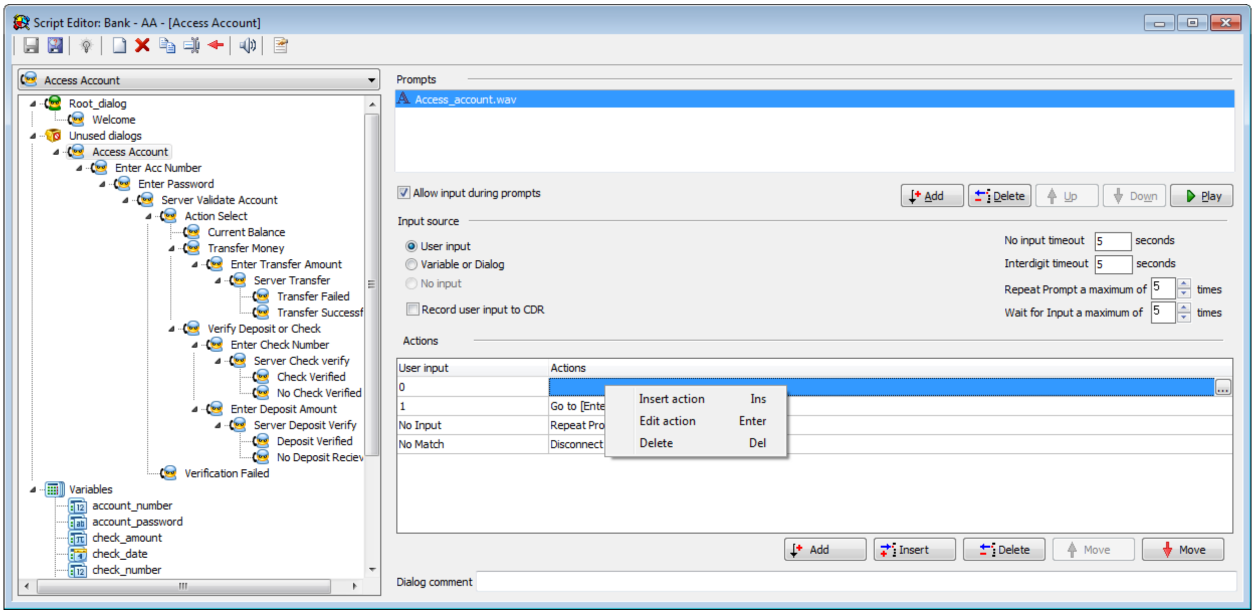
In the Number Associations tab, select a playlist in the Music on Hold column. The available options are:

- Do Not Change – If the call is directed to this call group number through a transfer, it will continue to listen to the same music on hold as its previous destination. If this is the call's initial destination, it will use the System playlist.
- System – Use the System playlist for calls routed to this call group number association number.
- Playlist name – Calls routed to this call group number association will use the selected playlist.

Click OK to save changes.

22.5.4 Assigning a Playlist through an Auto Attendant

The transfer action of the auto attendant provides a mechanism to change the Music on Hold playlist assigned to a call at the time of transfer. Auto attendant scripts are created and edited by going to Auto Attendants → Scripts.



Script Editor: Bank - AA - [Access Account]

Prompts: Access_account.wav

☑ Allow input during prompts

Input source: ● User input ○ Variable or Dialog ○ No input

☐ Record user input to CDR

No input timeout 5 seconds

Interdigit timeout 5 seconds

Repeat Prompt a maximum of 5 times

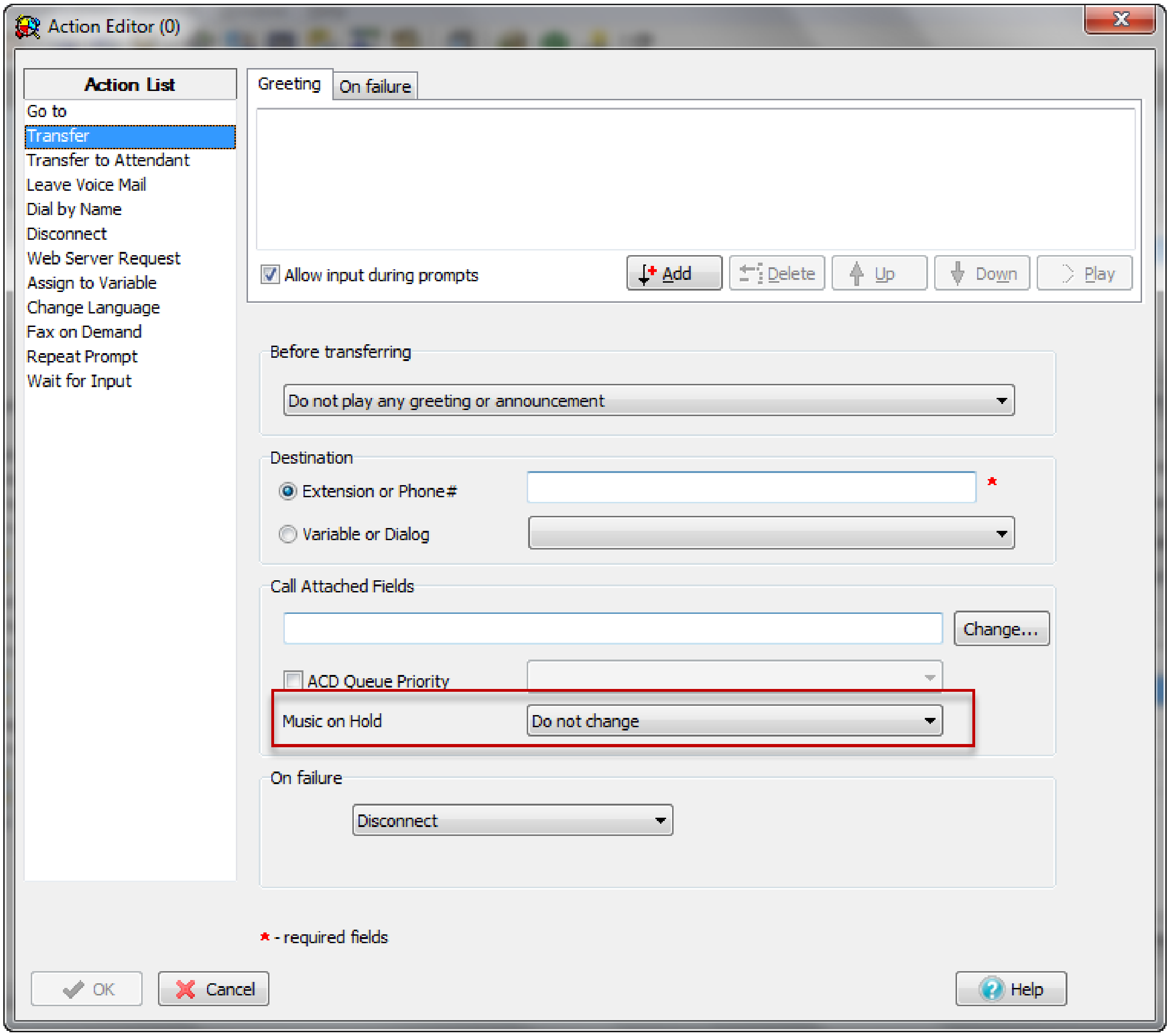
Wait for Input a maximum of 5 times

Actions

User input	Actions
0	
1	Go to [Ente
No Input	Repeat Pro
No Match	Disconnect

Dialog comment

In the Action Editor window select the Transfer action and define the greeting and transfer parameters.



In the Call Attached Fields section, select the required playlist from the Music on Hold drop-down list. The available options are:

- Do Not Change – If the call is directed to this auto attendant through a transfer, it will continue to listen to the same Music on Hold as its previous destination following this transfer. If this is the call's initial destination, it will use the System playlist following this transfer.
- System – Use the System playlist following this transfer.
- Playlist name – Calls will use the selected playlist following this transfer.

Click OK to save changes.

22.6 Playlist Assignment Rules

Playlist assignment is governed by the following rules:

- When a call first arrives it is always assigned the System playlist.
- If the MX-E system cannot find the playlist by name, it uses the System playlist.
- On transfer to a user or a call group destination where Do Not Change is set as a playlist for Music on Hold, the call will continue to listen to the playlist it has been assigned at its earlier destination.
- On transfer to a user or a call group destination where any other playlist besides Do Not Change is set, the call will change to the music on hold playlist defined for the new destination.
- For System playlist configured to use WAV files, the playlist is played continuously and calls can enter it at any point in the playlist. If the System playlist reaches the end of the last file in its list and no calls are currently on hold, the next call that uses the System playlist will hear the first file from the beginning.
- Playlists other than System playlist, start playing from the beginning. If a call is placed on hold for a second time, the music on hold will resume from the position it was at before the call was retrieved from hold the first time and so on for each new hold.
- Parking a call does not change the playlist assignment. The playlist assigned to the call before it was parked is maintained at least until the call is retrieved from park.
- Upon performing the following operations: pickup, direct pickup and pickup from hold, if the new user or call group destination has an assigned playlist other than Do Not Change, the new playlist is assigned to the call.

22.7 Limitations

The Music on Hold Assignment function is bound by the following limitations:

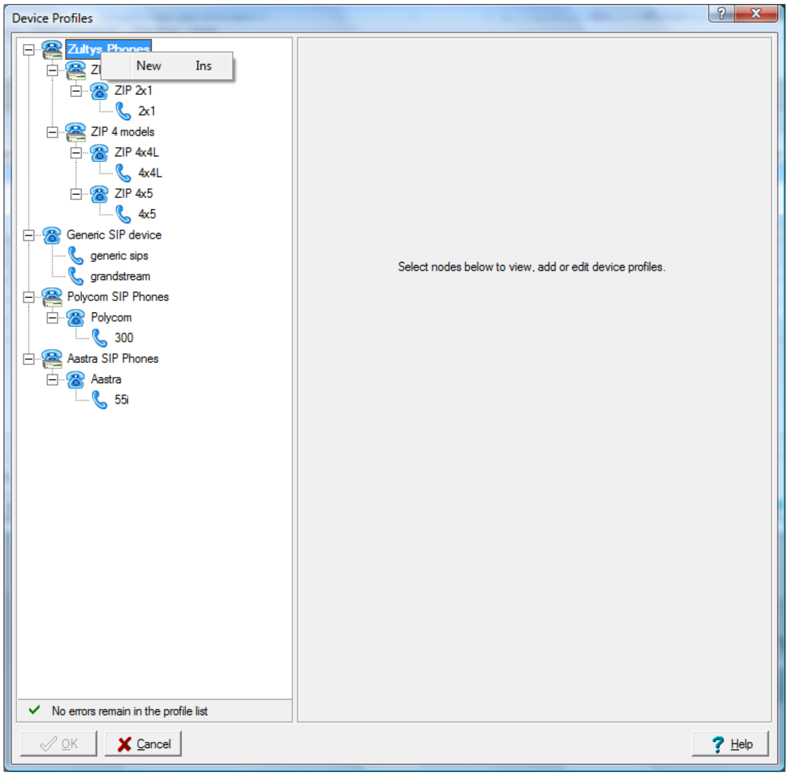
- The system doesn't allow for automatic sharing of playlists between MX-E systems in an MXnetwork configuration.
- The total number of playlists that can be configured for an MX-E system is 64.
- The number of calls that can simultaneous access the System playlist is unlimited.
- The number of calls that can simultaneous access playlists other than the System playlist is limited to 10 calls on MX-E.
- If this limit is reached, calls above the limit will use the System playlist.

23. Adding Devices - ZIP5

23.2 Create Profile for ZIP5 phone

To create a new ZIP5 series phone profile:

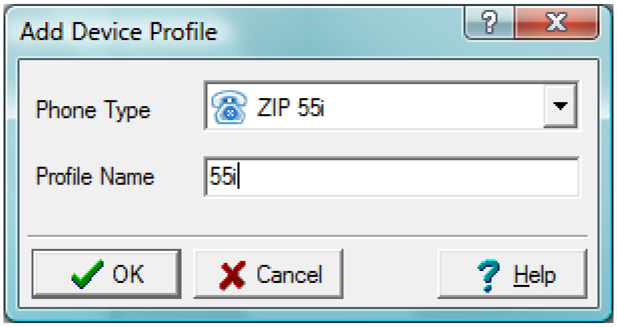
1. In MX-E Administrator, select Configure, then Devices.
2. Click the Profile button in the Managed Devices window
3. Right-click Zultys Phones and select New to create a new device profile in Device Profiles window



Select nodes below to view, add or edit device profiles.

No errors remain in the profile list

4. Select ZIP5 series phone in the Add Device Profile popup window.



Phone Type: ZIP 55i

Profile Name: 55i

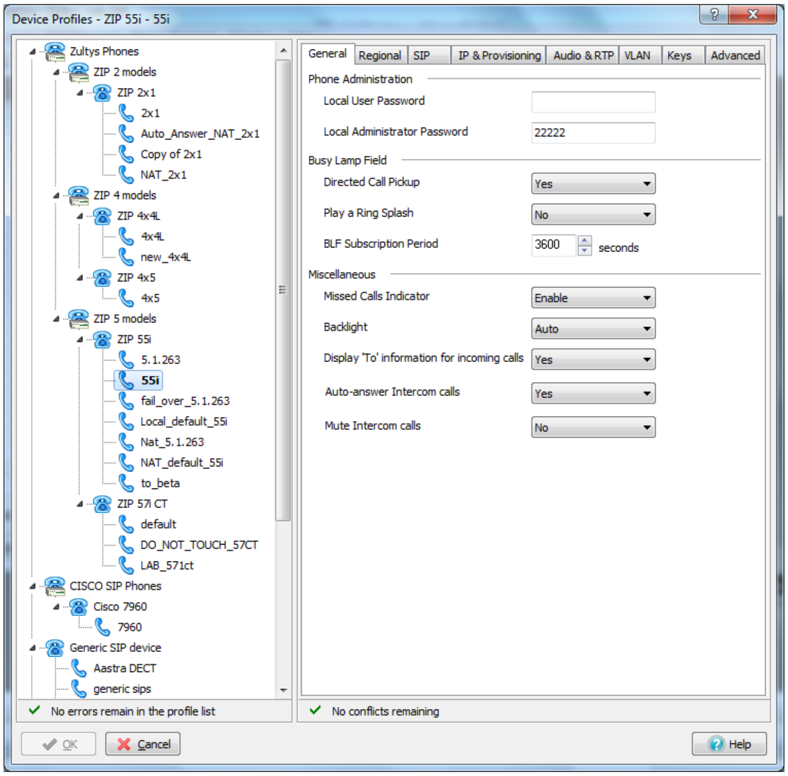
5. Type in a profile name; in this screenshot 55i was used.

23.3 Profile Tabs

The device profile for each phone is divided into several tabs. Each tab configures different aspects of the profile itself.

23.3.1 General Tab

The General tab contains Phone Administration, used to set passwords for configuration of both the web and the phone interfaces, Busy Lamp Field and Miscellaneous setting.



- Zultys Phones
  - ZIP 2 models
    - ZIP 2x1
      - 2x1
      - Auto_Answer_NAT_2x1
      - Copy of 2x1
      - NAT_2x1
  - ZIP 4 models
    - ZIP 4x4L
      - 4x4L
      - new_4x4L
    - ZIP 4x5
      - 4x5
  - ZIP 5 models
    - ZIP 55i
      - 5.1.263
      - **55i**
      - fail_over_5.1.263
      - Local_default_55i
      - Nat_5.1.263
      - NAT_default_55i
      - to_beta
    - ZIP 57i CT
      - default
      - DO_NOT_TOUCH_57CT
      - LAB_571ct
- CISCO SIP Phones
  - Cisco 7960
    - 7960
- Generic SIP device
  - Aastra DECT
  - generic sips

✓ No errors remain in the profile list

Phone Administration

Local User Password	
Local Administrator Password	22222

Busy Lamp Field

Directed Call Pickup	Yes
Play a Ring Splash	No
BLF Subscription Period	3600 seconds

Miscellaneous

Missed Calls Indicator	Enable
Backlight	Auto
Display 'To' information for incoming calls	Yes
Auto-answer Intercom calls	Yes
Mute Intercom calls	No

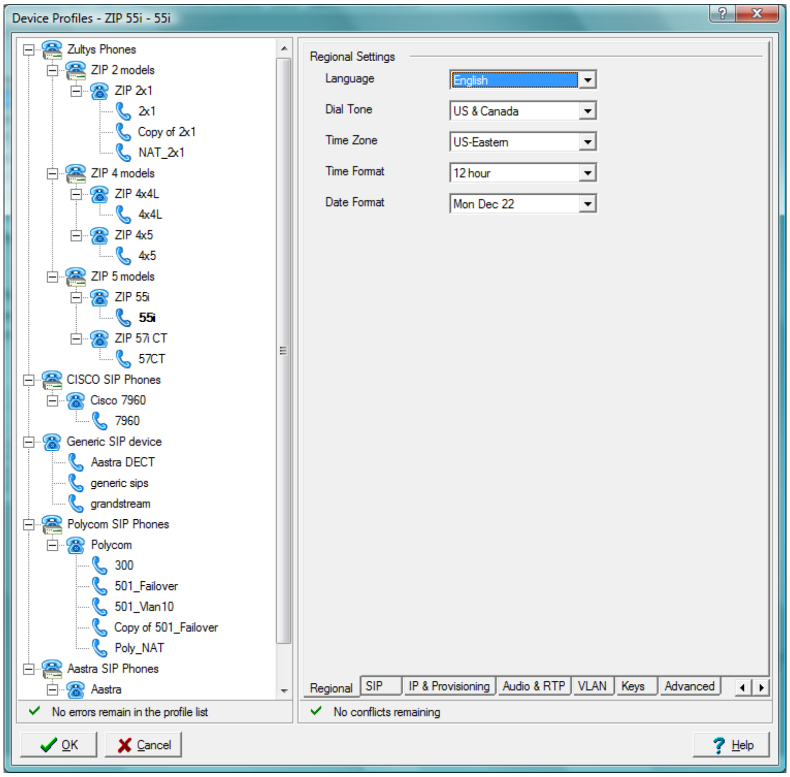
✓ No conflicts remaining

- **Local User Password**: The user password for the web interface and the local interface of the ZIP5 Phone. By default, this password is not set.
- **Local Administrator Password**: The Administrator password for the web interface and the local interface of the ZIP5 phone. By default it is 22222.
- **Directed Call Pickup:** Enables Directed Call Pickup of the stations monitored by the BLF buttons.
- **Play a Ring Splash**: If enabled, the phone plays a Call Waiting tone when off-hook or a Splash Ring when on-hook for each BLF programmed on the phone.

- **BLF Subscription Period**: The period a Busy Lamp Field registration will last before renewing.
- **Missed Calls Indicator**: If enabled, the missed call display message is turned on. (**Note:** to clear this message you must have a callers list button defined or have the hard key on the phone)
- **Backlight**: Backlight settings for the models of ZIP5 that supports the backlight feature.
- **Display "To" information for incoming calls**: If enabled, the "To" header is shown on the phone's display for incoming calls (helpful if the phone is a member of multiple call groups or multiple users are assigned to the phone).
- **Auto-Answer Intercom calls**: Enables the ability for the phone to receive intercom calls. An intercom call is defined as a call to a phone that is automatically answered on the speakerphone (or headset).
- **Mute Intercom calls**: If enabled, mute will engage when an intercom call is received. The user must press Mute to disable the muting manually in order to respond back to the caller.

23.3.2 Region tab

The Regional tab contains settings for the phone’s location.



Regional Settings

Language: English

Dial Tone: US & Canada

Time Zone: US-Eastern

Time Format: 12 hour

Date Format: Mon Dec 22

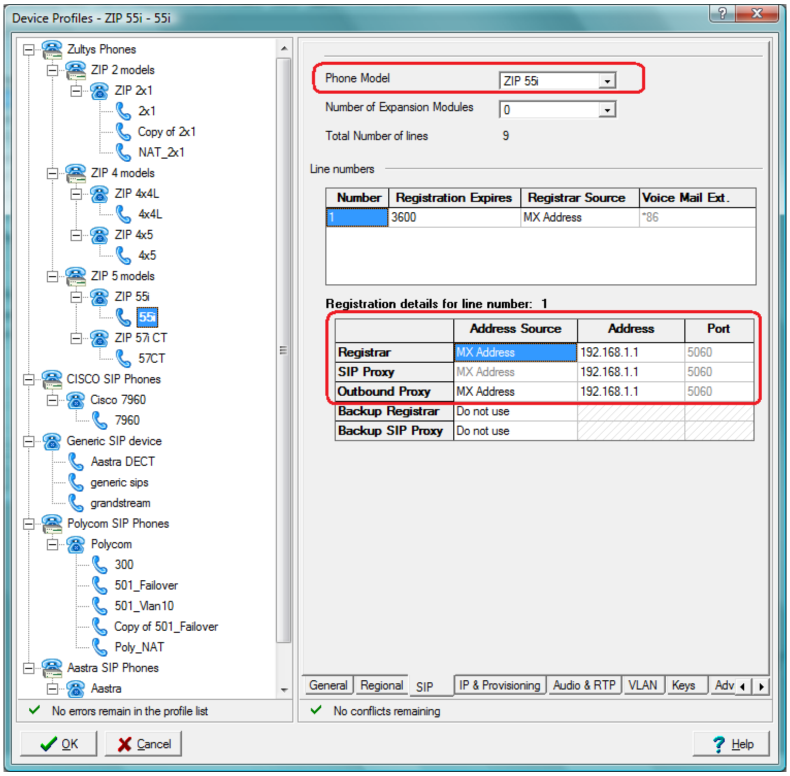
✓ No errors remain in the profile list

✓ No conflicts remaining

On this tab you will set the regional information such as

- **Language**: Language displayed on the phone’s display.
- **Dial Tone**: The type of dial tone used by the phone.
- **Time Zone**: The time zone this phone is in.
- **Time Format**: The format in which time is displayed by the phone.
- **Date Format**: The format in which date is displayed by the phone.

23.3.3 Sip Tab



✓ No errors remain in the profile list

Phone Model: ZIP 55i
Number of Expansion Modules: 0
Total Number of lines: 9

Line numbers

Number	Registration Expires	Registrar Source	Voice Mail Ext.
1	3600	MX Address	*86

Registration details for line number: 1

	Address Source	Address	Port
Registrar	MX Address	192.168.1.1	5060
SIP Proxy	MX Address	192.168.1.1	5060
Outbound Proxy	MX Address	192.168.1.1	5060
Backup Registrar	Do not use		
Backup SIP Proxy	Do not use		

✓ No conflicts remaining

The SIP Tab contains settings for the type of ZIP5 phone used and the registration addresses.

23.3.3.1 Phone Types

This option is automatically filled based on the ZIP5 phone type and cannot be changed.

23.3.3.2 Line numbers

The ZIP5 can handle multiple line numbers, or multiple registrations, the number will depend on the model of ZIP5 phone. A single registration will allow calls to be received or made from each of the physical hard line keys on the device. In most cases only one registration is required.

Voice Mail Ext. is grayed out and automatically filled by the MX-E.

23.3.3.3 Registration Details

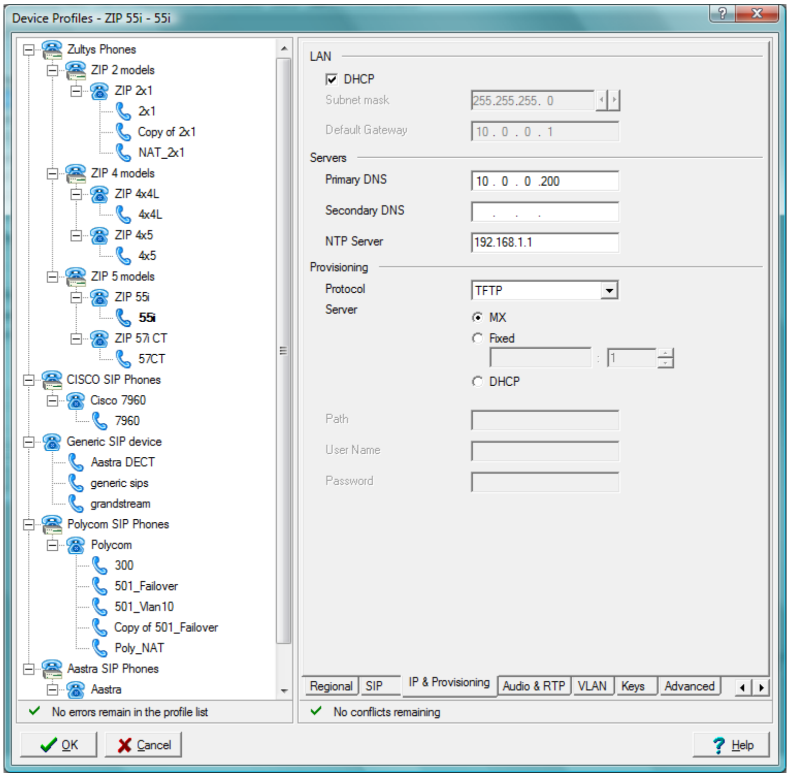
The Registrar, SIP Proxy, and Outbound Proxy all must be set to MX-E Address.

WARNING: Failure to do this will not allow you to make outgoing calls.

Address and port number are grayed out, and are not changeable when using the MX-E Address.

23.3.4 IP & Provisioning Tab

The IP and Provisioning tab contains settings for defining the IP address, DNS Servers, NTP Server, and Provisioning method.



LAN

☑ DHCP

Subnet mask: 255.255.255. 0

Default Gateway: 10 . 0 . 0 . 1

Servers

Primary DNS: 10 . 0 . 0 .200

Secondary DNS: . . .

NTP Server: 192.168.1.1

Provisioning

Protocol: TFTP

Server: ● MX ○ Fixed : 1 ○ DHCP

Path:

User Name:

Password:

✓ No errors remain in the profile list

✓ No conflicts remaining

23.3.4.1 LAN

Select whether the IP information is obtained from DHCP or statically assigned to the phone

23.3.4.2 Servers

Define the DNS Server and the NTP Servers.

23.3.4.3 Provisioning

Select the provisioning method from the following:

- TFTP
- FTP
- HTTP
- HTTPS

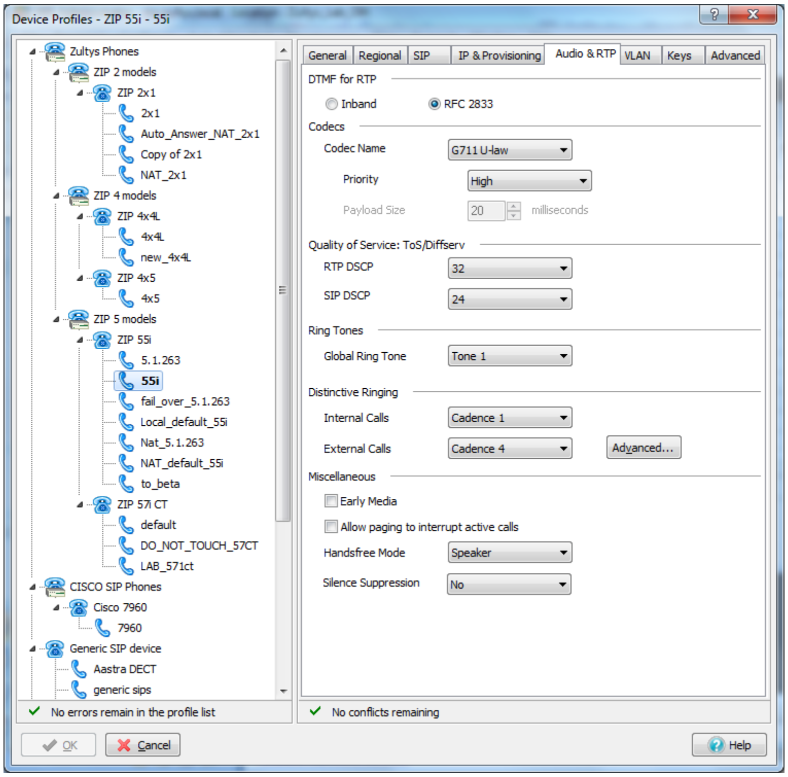
It is recommended that you use TFTP and select MX-E as the server. This enables the MX-E to build the configuration files, correctly name them and save them on the MX-E's TFTP Server. The MX-E only supports HTTP and TFTP.

If you choose to change this, type in the IP address and port number, or select DHCP to allow this information to come from the DHCP Server.

Depending on the Provisioning option, Path, User Name, and Password options become active.

23.3.5 Audio & RTP

The Audio and RTP Tab contains setting on how the audio and RTP will be handled by the phone.



DTMF for RTP

○ Inband ● RFC 2833

Codecs

Codec Name: G711 U-law

Priority: High

Payload Size: 20 milliseconds

Quality of Service: ToS/Diffserv

RTP DSCP: 32

SIP DSCP: 24

Ring Tones

Global Ring Tone: Tone 1

Distinctive Ringing

Internal Calls: Cadence 1

External Calls: Cadence 4

Miscellaneous

□ Early Media

□ Allow paging to interrupt active calls

Handsfree Mode: Speaker

Silence Suppression: No

✓ No errors remain in the profile list

✓ No conflicts remaining

23.3.5.1 DTMF for RTP

Use the default of RFC 2833. Sending DTMF inband is not supported by the MX-E, and should not be chosen.

23.3.5.2 Codecs

Choose the default codec for this device from the drop-down list.

Possible Codecs are:

- G711µ – Law
- G711a – Law
- G729A

Set the priority to High, and select Silence Suppression.

23.3.5.3 Ring Tones

Select a ring tone from the list of ring tones available for this phone model.

23.3.5.4 Distinctive Ringing

Select ring tones for Internal Calls and External Calls from the list of ring tones available for this phone model.

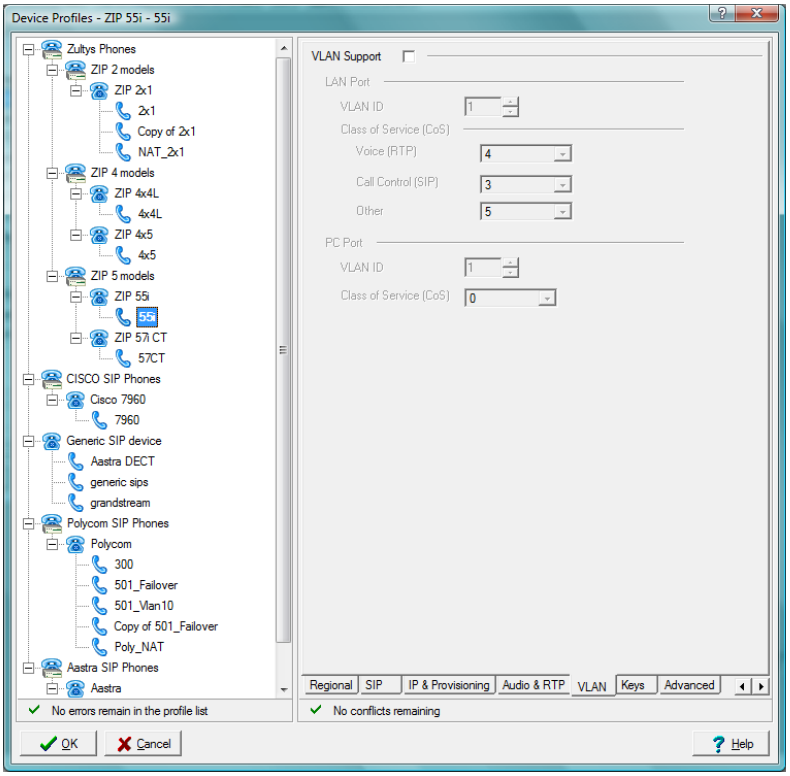
The Advance button allows you to customize the ring tone by adjusting the frequency, and cadence.

23.3.5.5 Miscellaneous

- **Early Media**: Select to enable Early Media for the phone.
- **Allow paging to interrupt active calls**: This option, when enabled, will put active calls on hold when a page is made to the phone to allow the page to be heard.
- **Handsfree Mode**: Select from the list of settings to control the mode of the speaker button which can be used for headset operation.
- **Silence Suppression**: Enables silence suppression.

23.3.6 VLAN Tab

The VLAN tab contains settings for configuring VLAN support for this phone. The settings in this tab differ depending on the ZIP5 phone model.



VLAN Support ☐

LAN Port

VLAN ID: 1

Class of Service (CoS)

Voice (RTP): 4

Call Control (SIP): 3

Other: 5

PC Port

VLAN ID: 1

Class of Service (CoS): 0

✓ No errors remain in the profile list

✓ No conflicts remaining

23.3.6.1 VLAN Support

Enables VLAN support for this device.

23.3.6.2 LAN Port

Choose which VLAN the phone will be on, and set the Class of Service (CoS) for this VLAN. This section only affects the LAN Port of the phone, not the PC Port.

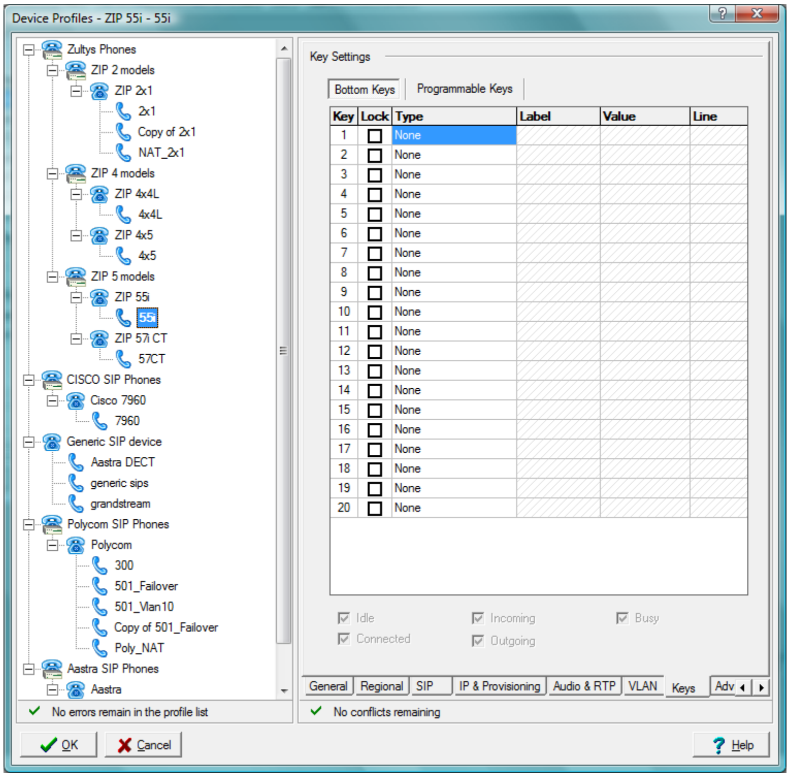
23.3.6.3 PC Port

Choose the VLAN that the PC Port will run on, and it's CoS.

23.3.7 Keys Tab

The Keys tab contains setting for custom soft keys for the phone. The number of keys, and position (Bottom Keys or Upper Keys) allowed on the phone will differ depending on ZIP5 Phone Model.

Keys can also be programmed for individual phones by clicking the Key Provisioning button in the device configuration screen, see section 23.3.10.



Key	Lock	Type	Label	Value	Line
1	□	None			
2	□	None			
3	□	None			
4	□	None			
5	□	None			
6	□	None			
7	□	None			
8	□	None			
9	□	None			
10	□	None			
11	□	None			
12	□	None			
13	□	None			
14	□	None			
15	□	None			
16	□	None			
17	□	None			
18	□	None			
19	□	None			
20	□	None			

☑ Idle ☑ Incoming ☑ Busy
☑ Connected ☑ Outgoing

✓ No errors remain in the profile list

✓ No conflicts remaining

23.3.7.1 Key

The number of the physical key on the phone.

23.3.7.2 Lock

Block the end user from modifying this key from the phone's interface or the web interface by selecting this checkbox.

23.3.7.3 Type

Select the type of key. Available options are:

- **None**: This softkey or programmable key is disabled

- **Speed dial**: This softkey or programmable key is configured for speed dial use.
- **Do Not Disturb**: This softkey or programmable key is configured for "do not disturb" use.
- **BLF**: This softkey or programmable key is configured for Busy Lamp Field (BLF) use. A user can dial out on a BLF configured softkey:
  - Max of 50 BLF per phone
  - Max of 500 to 600 per system
  - Max of 64 stations monitoring the same phone
- **Park Monitored:** This softkey or programmable key is configured to monitor a Park ID. If a call is parked to an ID the button monitoring it will light up.
- **This key type is included in the BFL count for the systemLogin (Call Group):** This softkey or programmable key is configured as a Login button to call groups (ACD/ICC/Operator). When the user presses this button they will be asked to enter in their Voicemail Password, and then be logged into the group. The key will light up to indicate they are logged in. Pressing it again will log them out of the call group. The value is <user extension number>.<group extension number>
  - This key type is included in the BFL count for the system
- **Mailbox MWI**: This softkey or programmable key is configured to indicate if there is a message waiting for the monitored mail box. Pressing the key will take the user to the login for that mail box.
  - This key type is included in the BFL count for the system
- **Park (auto)**: This softkey or programmable key is configured as a park key to park an incoming call. The MX-E will automatically select a park ID and display it on the phone and in MXIE.

- **Park (manual)**: This softkey or programmable key is configured as a park key to park an incoming call. The user will have to manually select a park ID and it will be displayed on the phone and in MXIE.
- **Pickup**: This softkey or programmable key is configured as a pickup key to pick up a parked call.
- **Directory**: This softkey or programmable key is configured to access the directory listing stored on the phone. This directory must be updated manually on the phone or via a configuration file.
- **XML Directory**: This softkey or programmable key is configured to access the directory listing stored on the phone. This directory is automatically populated and managed by the MX-E and requires no up keep.
- **Callers List**: This softkey or programmable key is configured to access the list of missed and received calls.
- **Services**: This softkey or programmable key is configured to pull up a directory of the following options:
    - Web Aps
    - Directory
    - Caller List
    - Voicemail
- **Voicemail**: This softkey or programmable key is configured to access the MX-E voice mail.
- **Page/Intercom**: This softkey or programmable key is configured to access the page server followed but the page group ID to make a page or can be followed by an extension number to intercom.
- **Empty**: This softkey or programmable key is configured to force a blank entry on the IP phone display for a specific softkey.
- **Save**: This softkey or programmable key is configured to save entries for speed dial tables. Must be in position 5 for a 53e phone.

- **Delete**: This softkey or programmable key is configured to delete entries for speed dial tables. Must be in position 6 for a 53e phone.
- **Conference**: This softkey or programmable key is configured for a local phone conference. The ZIP5 phone support 2 callers and yourself for a total of 3 party conferences.
- **MX-E Conference**: This softkey or programmable key is configured to start or join an MXconference.
- **Transfer**: This softkey or programmable key is configured to create a transfer for phones that do not have a hard key for transfer (for example 51i phone).

23.3.7.4 Label

This is what the user will see on the display of the phone for a programed key, if supported.

23.3.7.5 Value

The value for this key depends on the type of key selected. For example:

- If BLF is selected, this value is the extension number.
- If Park is selected, the value is callpark.

23.3.7.6 Line

This value is used to determine which registration this key acts on. Normally this will always be 1.

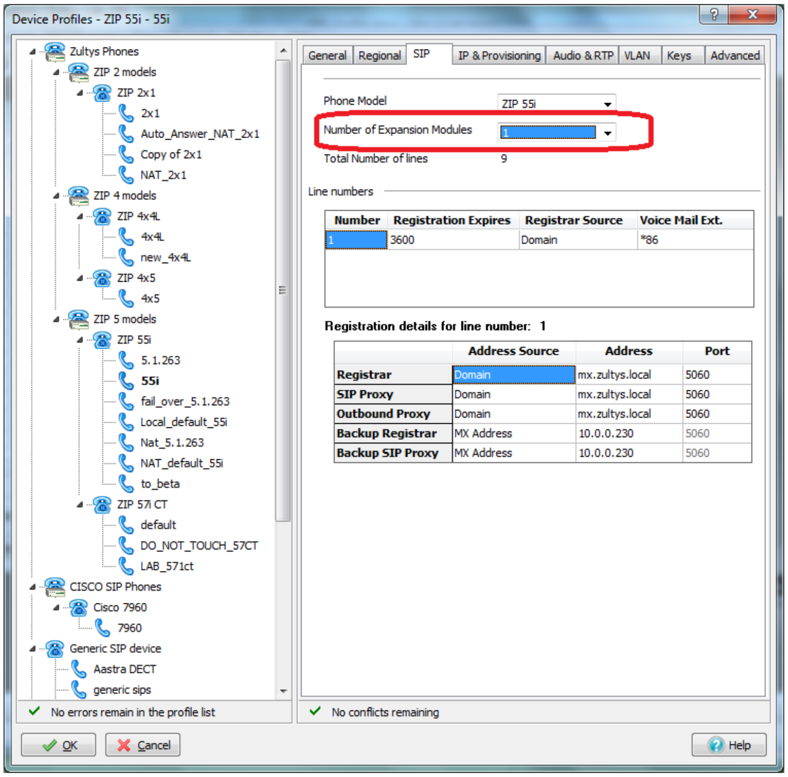
23.3.7.7 Key Availability to User

Select when each key is available to users by selecting the check boxes on the bottom of this tab.

- o **Idle**: Key is available when the phone is idle.
- o **Incoming**: Key is available when the phone is ringing on an incoming call.
- o **Busy**: Key is available when the phone is busy (off-hook).
- o **Connected**: Key is available when a call is currently connected.
- o **Outgoing**: Key is available when a call is being placed.

23.3.7.8 Programming Soft Keys for Add On Modules

Enable the number of expansion modules to use in the SIP tab, and program the keys for them in the Keys tab.



Phone Model: ZIP 55i
Number of Expansion Modules: 1
Total Number of lines: 9

Line numbers

Number	Registration Expires	Registrar Source	Voice Mail Ext.
1	3600	Domain	*86

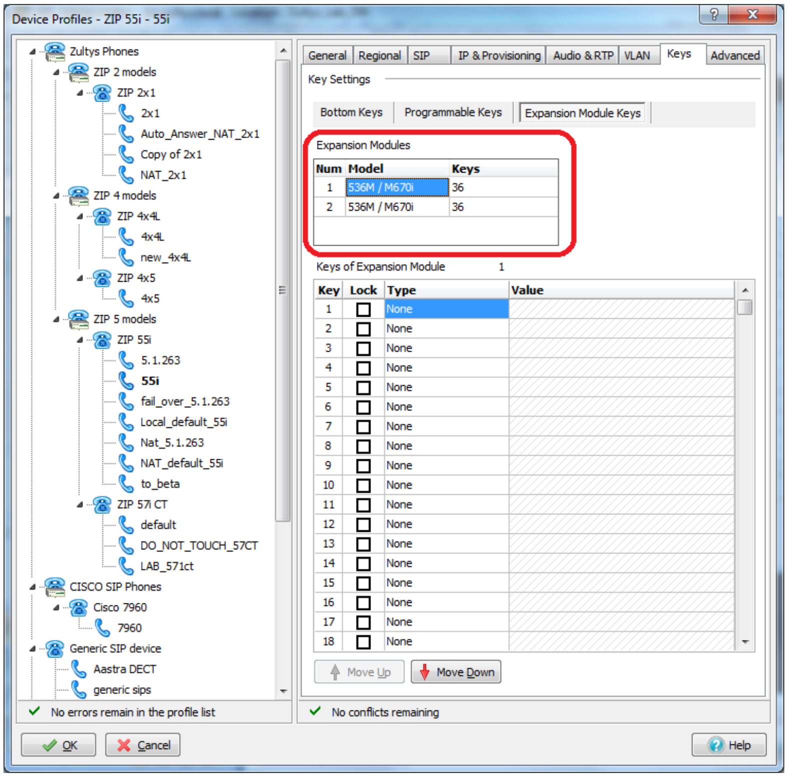
Registration details for line number: 1

	Address Source	Address	Port
Registrar	Domain	mx.zultys.local	5060
SIP Proxy	Domain	mx.zultys.local	5060
Outbound Proxy	Domain	mx.zultys.local	5060
Backup Registrar	MX Address	10.0.0.230	5060
Backup SIP Proxy	MX Address	10.0.0.230	5060

✓ No errors remain in the profile list

✓ No conflicts remaining

Select the extension module from the extension module type selection.



Expansion Modules

Num	Model	Keys
1	536M / M670i	36
2	536M / M670i	36

Keys of Expansion Module 1

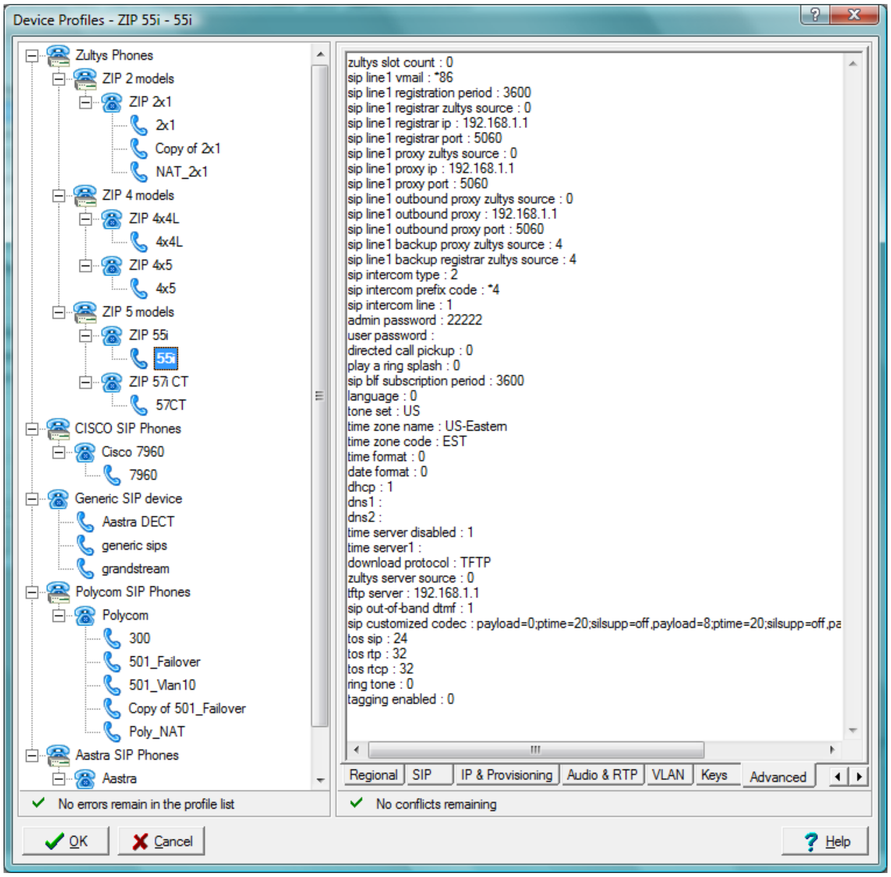
Key	Lock	Type	Value
1	□	None	
2	□	None	
3	□	None	
4	□	None	
5	□	None	
6	□	None	
7	□	None	
8	□	None	
9	□	None	
10	□	None	
11	□	None	
12	□	None	
13	□	None	
14	□	None	
15	□	None	
16	□	None	
17	□	None	
18	□	None	

✓ No errors remain in the profile list

✓ No conflicts remaining

23.3.8 Advanced Tab

This tab contains the actual configuration file. From here you can make your own custom changes to the configuration file. Note that making changes in the other tabs may remove any custom entries.



```
zultys slot count : 0
sip line1 vmail : *86
sip line1 registration period : 3600
sip line1 registrar zultys source : 0
sip line1 registrar ip : 192.168.1.1
sip line1 registrar port : 5060
sip line1 proxy zultys source : 0
sip line1 proxy ip : 192.168.1.1
sip line1 proxy port : 5060
sip line1 outbound proxy zultys source : 0
sip line1 outbound proxy : 192.168.1.1
sip line1 outbound proxy port : 5060
sip line1 backup proxy zultys source : 4
sip line1 backup registrar zultys source : 4
sip intercom type : 2
sip intercom prefix code : *4
sip intercom line : 1
admin password : 22222
user password :
directed call pickup : 0
play a ring splash : 0
sip blf subscription period : 3600
language : 0
tone set : US
time zone name : US-Eastern
time zone code : EST
time format : 0
date format : 0
dhcp : 1
dns1 :
dns2 :
time server disabled : 1
time server1 :
download protocol : TFTP
zultys server source : 0
tftp server : 192.168.1.1
sip out-of-band dtmf : 1
sip customized codec : payload=0;ptime=20;silsupp=off,payload=8;ptime=20;silsupp=off,pa
tos sip : 24
tos rtp : 32
tos rtcp : 32
ring tone : 0
tagging enabled : 0
```

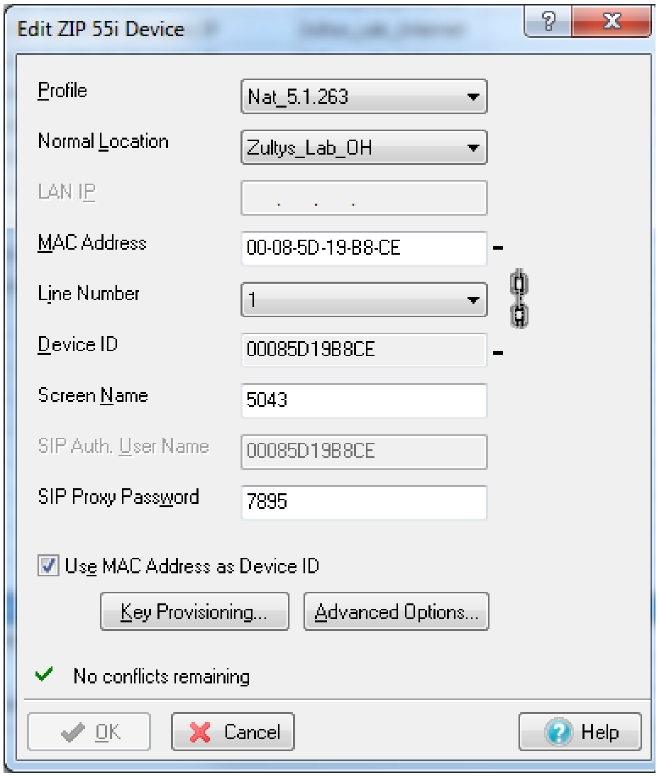
23.3.9 Park and Paging

Calls can be parked and later picked up from the ZIP5 phones. If park (manual) is used, user must provide the Park ID at the time of call park operation, the Park ID should be within the call park range configured on the MX-E (under Phone Services in Configure). There should be a Park button defined on the phone (auto, manual, or monitored) and a Pickup button.

Users with ZIP5 phones assigned / bound to them can receive paging announcements. Due to the nature of SIP based paging, the number of ZIP5 devices associated with a paging group should be limited to 32 devices. This can be further limited by the number of available sessions.

23.3.10 Device Configuration

From the device configuration screen you can edit the keys per device by clicking the Key Provisioning button. Clear the Use check box to allow overwriting the profile button options.

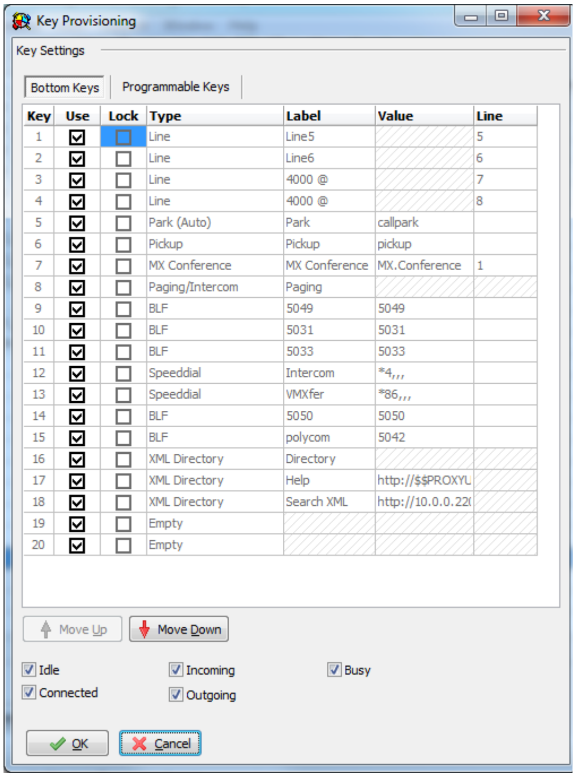


Edit ZIP 55i Device

Profile	Nat_5.1.263
Normal Location	Zultys_Lab_OH
LAN IP	. . .
MAC Address	00-08-5D-19-B8-CE
Line Number	1
Device ID	00085D19B8CE
Screen Name	5043
SIP Auth. User Name	00085D19B8CE
SIP Proxy Password	7895

☑ Use MAC Address as Device ID

✓ No conflicts remaining



Key Provisioning

Key Settings

Key	Use	Lock	Type	Label	Value	Line
1	☑	□	Line	Line5		5
2	☑	□	Line	Line6		6
3	☑	□	Line	4000 @		7
4	☑	□	Line	4000 @		8
5	☑	□	Park (Auto)	Park	callpark	
6	☑	□	Pickup	Pickup	pickup	
7	☑	□	MX Conference	MX Conference	MX.Conference	1
8	☑	□	Paging/Intercom	Paging		
9	☑	□	BLF	5049	5049	
10	☑	□	BLF	5031	5031	
11	☑	□	BLF	5033	5033	
12	☑	□	Speeddial	Intercom	*4,,,	
13	☑	□	Speeddial	VMXfer	*86,,,	
14	☑	□	BLF	5050	5050	
15	☑	□	BLF	polycom	5042	
16	☑	□	XML Directory	Directory		
17	☑	□	XML Directory	Help	http://$$PROXYU	
18	☑	□	XML Directory	Search XML	http://10.0.0.22(	
19	☑	□	Empty			
20	☑	□	Empty			

☑ Idle ☑ Incoming ☑ Busy
☑ Connected ☑ Outgoing

23.3.11 Languages

The ZIP5 phones can support multiple languages. To enable these languages on the phone please download the correct language pack and copy them to the MX-E TFTP server. In the Advanced tab of the profile for the phone, modify the following lines to enable a menu for the user to pick the language from, and set the default language. This is automatically set in the Language field in the Regional tab.

```
language : 0 (where the number indicates the language defined
below, default is 0 for English)
```

```
language 1: lang_de.txt
language 2: lang_es.txt
language 3: lang_es_MX-E.txt
language 4: lang_fr.txt
language 5: lang_fr_ca.txt
language 6: lang_it.txt
language 7: lang_pt.txt
language 8: lang_pr_br.txt
language 9: lang_ru.txt
```

Languages 1 through 4 are the menu options for languages. Language x is the default language (where 0 is the default English option). Not all languages are available for all phones.

24. Adding Devices – ZIP3

This document covers the steps required to provision, deploy and manage the Zultys ZIP 33i IP phones with a Zultys MX-E system. ZIP 33i phones are supported in MX-E Release 7.2.1 and later, prior to this release there is no support for ZIP 33i phones.

In general the steps required to successfully deploy a ZIP 33i phone are:

- Upload the current ZIP 33i firmware ROM file to the TFTP server of the MX-E system. The current firmware release is available from the Zultys Knowledge Base System (http://kbs.zultys.com). Refer to section 24.1.14.
- Create a ZIP 33i device profile with the relevant settings including selection of the firmware version to be used by the ZIP 33i phones. Refer to section 24.1.
- Add the ZIP 33i devices to the MX-E system and assign the appropriate device profile. Refer to section 24.1.11.
- Add new users to the MX-E system if required then assign the newly provisioned devices to their respective users.
- To use automatic provisioning ensure the DHCP server is correctly configured to provide Option 66. Refer to Section 24.1.6.3.

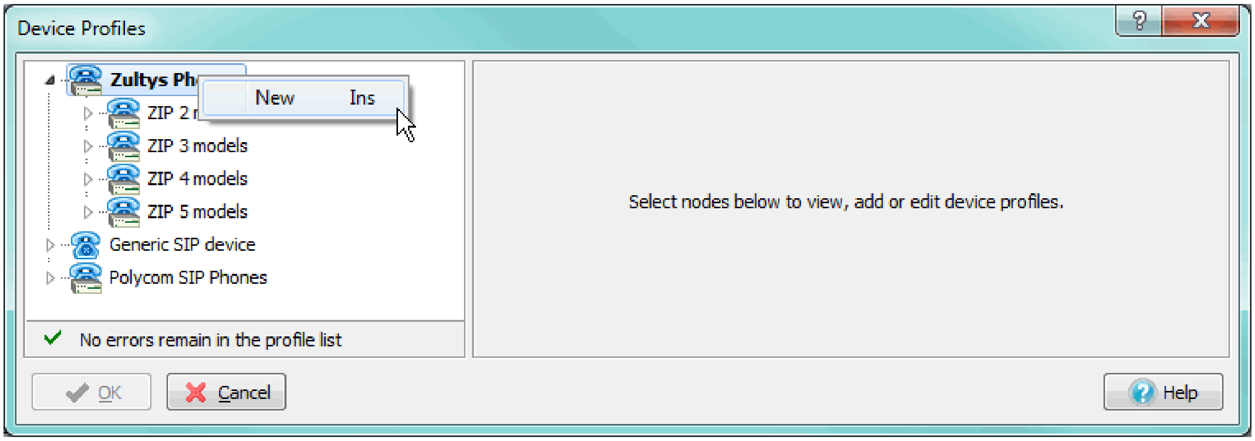
24.1 Creating a Device Profile

A Device Profile defines a common set of configuration options that will be applied to all phones that are allocated a particular Device Profile. This greatly simplifies the management of deployed phones as changes only need to be performed in one place.

Prior to creating a new Device Profile the system administrator should ensure that the current ZIP 33i firmware ROM file has been uploaded to the TFTP server of the MX-E system. Refer to section 24.1.14 for further information.

To create a new ZIP 33i device profile:

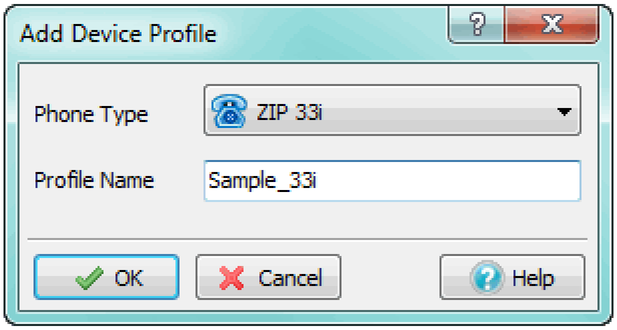
1. In MX-E Administrator, select **Configure → Devices.**
2. Click the **Profile** button in the Managed Devices window.
3. In the Device Profiles window Right-click Zultys Phones and select **New** to create a new device profile.



No errors remain in the profile list

Select nodes below to view, add or edit device profiles.

4. In the Add Device Profile window set the **Phone Type** to ZIP 33i.



Add Device Profile

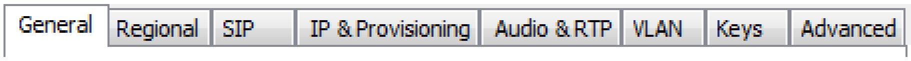
Phone Type: ZIP 33i

Profile Name: Sample_33i

5. Type a **Profile Name**, in the screenshot above **Sample_33i** is used.

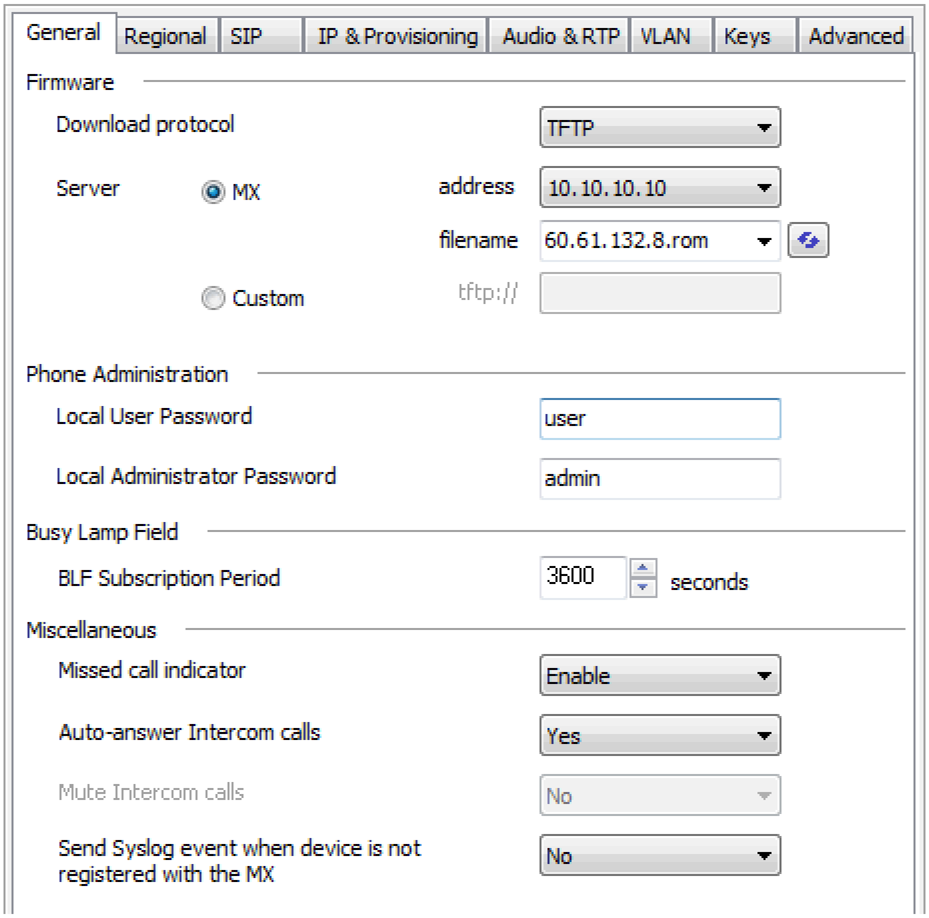
24.1.1 Overview of Profile Tabs

The device profile for each phone is divided into several tabs. Each tab configures different aspects of the profile.



24.1.2 General Tab

The General tab contains settings related to firmware version and updating, password settings and various miscellaneous settings.



Firmware

Download protocol: TFTP

Server ● MX address: 10.10.10.10

filename: 60.61.132.8.rom

○ Custom tftp://

Phone Administration

Local User Password: user

Local Administrator Password: admin

Busy Lamp Field

BLF Subscription Period: 3600 seconds

Miscellaneous

Missed call indicator: Enable

Auto-answer Intercom calls: Yes

Mute Intercom calls: No

Send Syslog event when device is not registered with the MX: No

- **Download protocol**: Defines the protocol used by the phone to download new firmware.
  - **None** – Phone will not check for new firmware on power up
  - **TFTP** – Phone will use TFTP (Trivial File Transfer Protocol) to download firmware image on power up if different to the currently installed version. This is the default setting.
  - **HTTP** – Phone will use HTTP (Hyper Text Transfer Protocol) to download firmware image on power up if different to the currently installed version. HTTP may perform more reliably over poor quality links.
- **Server**: Defines the address of server where firmware image is stored

  - **MX-E** – Select when the internal TFTP/HTTP server of the MX-E system is to be used, this will be the case for most deployments. For HTTP TCP port 8080 is used
    - **Address** – Lists the MX-E systems IP addresses including LAN, WAN and SBC Port Mapping addresses if configured. For external phones connecting to a WAN or SBC address you may need to configure port forwarding on external routers.
    - **Filename** – Lists the compatible firmware images stored on the MX-E TFTP server. Select the desired filename from the dropdown. If the files stored on the TFTP have recently been changed by another system administrator press the **Refresh** button to update the list. If the field background is red the corresponding file is not present on the TFTP server and thus the phone will be unable to access the file. Files are uploaded to the TFTP server via the TFTP Settings window accessible from the **Configure → Devices** screen. Refer to section 24.1.14 for further information about the firmware upgrade process.
  - **Custom** – Select when an external TFTP/HTTP server is to be used. In the corresponding address field type the full path and filename. For HTTP both the address and port may be defined.
    TFTP example – 192.168.1.100/60.61.132.8.rom
    HTTP example –
    192.168.1.100:8080/tftpphone/60.61.132.8.rom

- **Phone Administration**: Set passwords used to access various restricted sections of phone interface and web interface.

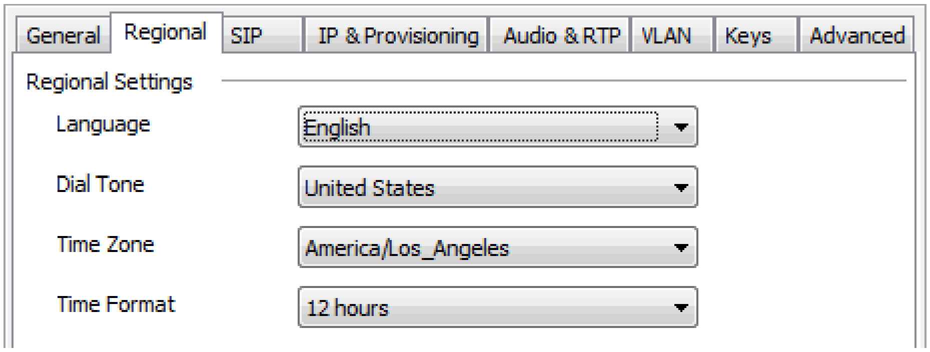
  - **Local User Password** – Password to access User level restricted sections. Default is 'user'. If the field is left blank then no password is required.
  - **Local Administrator Password** – Password to access Administrator level restricted sections. Default is 'admin'. If the field is left blank then no password is required.

- **Busy Lamp Field**
  - **BLF Subscription Period**: The period in seconds a Busy Lamp Field subscription will last before phone re-subscribes. Default is '3600'.

- **Miscellaneous**:
  - **Missed Call Indicator** – When enabled the phone will display the number of missed calls on the idle screen and also store caller details for the missed calls in the Call Log. When disabled no missed call indication will be displayed and the phone will not store any information about the missed call in the Call Log.
  - **Auto-answer Intercom calls** – When set to Yes the phone will automatically answer received Intercom calls. When set to No the phone will ring when an Intercom call is received. Default is Yes.
  - **Mute Intercom calls** – This setting is fixed at No. The microphone will always be enabled when an intercom call is answered.
  - **Send Syslog event when device is not registered with the MX-E** – When set to Yes, in the event that the phone fails to register / re-register, a message will appear in the Syslog of the MX-E alerting the system administrator to a potential issue with the phone or network. Default is No.

24.1.3 Regional tab

The Regional tab contains settings related to phone location including language, dial tone, time zone and time format.



Regional Settings

Language: English

Dial Tone: United States

Time Zone: America/Los_Angeles

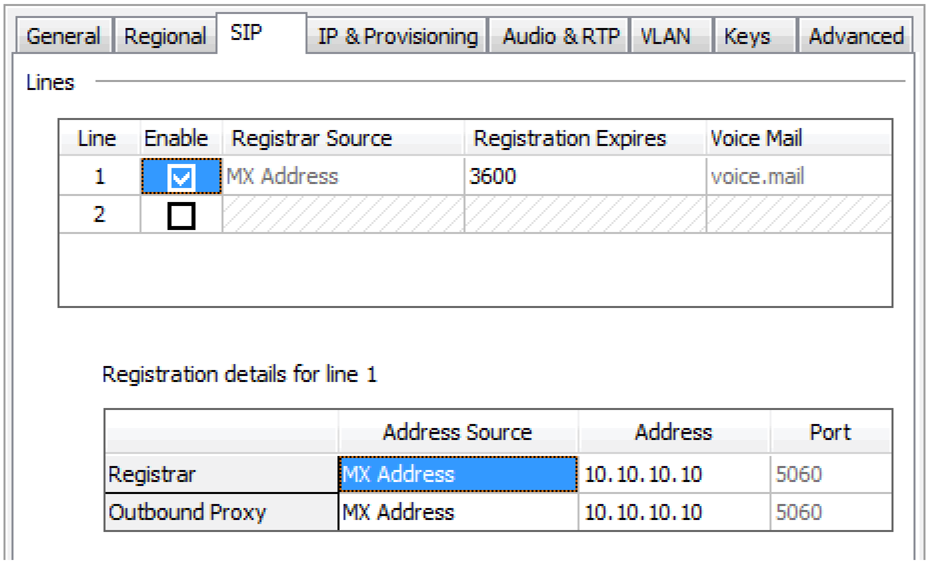
Time Format: 12 hours

The settings on this screen will automatically populate based on the default location setting of the MX-E. If required change the settings to suit the phones location.

- **Language**: Language for telephone user interface (TUI) of the phone.
- **Dial Tone**: Determines the dial tone and call progress tones generated by the phone.
- **Time Zone**: The time zone the phone is located in. Time zones will also generally impact DST dates.
- **Time Format**: Time display format, 12 or 24 hour.

24.1.4 SIP Tab

The SIP Tab contains settings related to the registration addresses.



Lines

Line	Enable	Registrar Source	Registration Expires	Voice Mail
1	☑	MX Address	3600	voice.mail
2	□			

Registration details for line 1

	Address Source	Address	Port
Registrar	MX Address	10.10.10.10	5060
Outbound Proxy	MX Address	10.10.10.10	5060

24.1.5 Lines

The ZIP 33i supports two independent SIP Registrations. In most cases only one registration is required. ‘Line’ registrations should not be confused with the number of Line Keys or Call Appearances configured via the ‘Keys’ tab. Multiple calls may be handled via a single registration.

- **Enable** – Select checkbox to enable Line
- **Registrar Source** – Defines the source of Registrar (SIP Server) address. Line 1 Registrar Source is always MX-E Address. The actual Registrar address is defined in the Registration Details section.
- **Registration Expires** – Defines the registration period in second. Default is 3600.
- **Voice Mail** – Defines the voice mail service number / URI related to the Line. Default is ‘voice.mail’ and fixed when Registrar Source is MX-E Address.

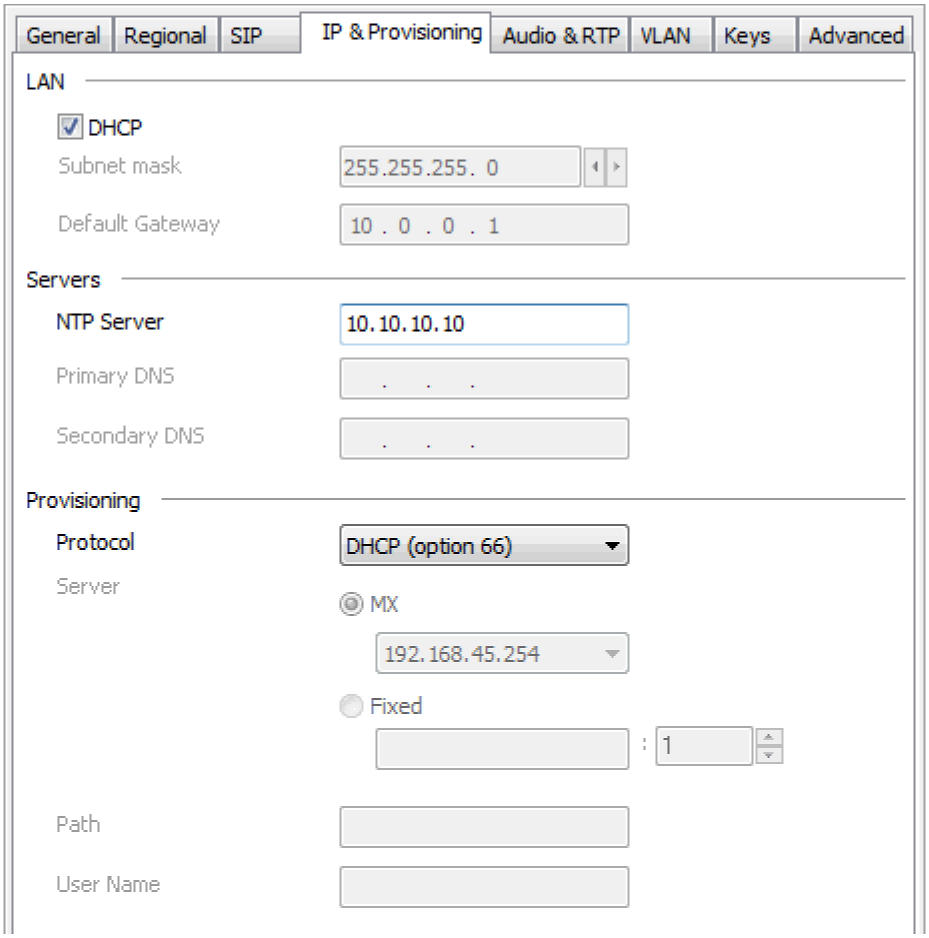
The ‘Registration details’ section defines the server address information related to the Line currently selected in the top section of the screen.

- **Registrar**: Settings related to SIP Registrar address

  - **Address Source** – Defines the source for Address setting. Line 1 is always MX-E Address.
  - **Address** – Defines the Registrar address. When Address Source is MX-E Address the dropdown will list all LAN, WAN and SBC addresses configured on the MX-E system. For phones deployed within the corporate network the LAN address of MX-E system should be selected. If using a WAN or SBC address the network must be configured appropriately to allow external phones to connect.
  - **Port** – Defines the port used for SIP signaling.
- **Outbound Proxy**: Settings related to Outbound Proxy address
  - **Address Source** – Defines the source for Address setting.
  - **Address** – Defines the Outbound Proxy address. For applications where the phone is registering to an MX-E this address should be the same as the Registrar address.
  - **Port** – Defines the port used for SIP signaling.

24.1.6 IP & Provisioning Tab

The IP and Provisioning tab contains settings for defining the IP address, DNS Servers, NTP Server, and Provisioning method.



LAN

☑ DHCP

Subnet mask: 255.255.255. 0

Default Gateway: 10 . 0 . 0 . 1

Servers

NTP Server: 10.10.10.10

Primary DNS: . . .

Secondary DNS: . . .

Provisioning

Protocol: DHCP (option 66)

Server: ● MX 192.168.45.254

○ Fixed : 1

Path:

User Name:

24.1.6.1 LAN

Select whether the IP address information is obtain automatically via DHCP or statically defined in the phone. If static addressing is used this screen defines the subnet mask and default gateway parameters, the IP address of the phone is defined in the **Edit Device** screen. Use of DHCP addressing is recommended.

24.1.6.2 Servers

Define the NTP Server and DNS Server addresses.

- **NTP Server** – Address of NTP time server that phone will synchronize its clock with. By default the field is populated with the main IP address of the MX-E system. To have the phone obtain the NTP server address via DHCP Option 42 leave this field blank and ensure the DHCP server has Option 42 correctly configured to point to a suitable NTP server. The MX-E system functions as an NTP server.
- **Primary DNS** / **Secondary DNS** – Address of DNS servers. If DHCP option is selected the DNS addresses will be obtained from DHCP server.

24.1.6.3 Provisioning

Define the protocol that phones use to download their configuration files. When using an external DHCP server, Option 66 must be configured to provide the IP address of the MX-E system for automatic provisioning of a new phone to function. If Option 66 is not enabled on the DHCP server the provisioning server address must be manually configured on the phone via the web interface or phone menu.

Overview of provisioning server options:

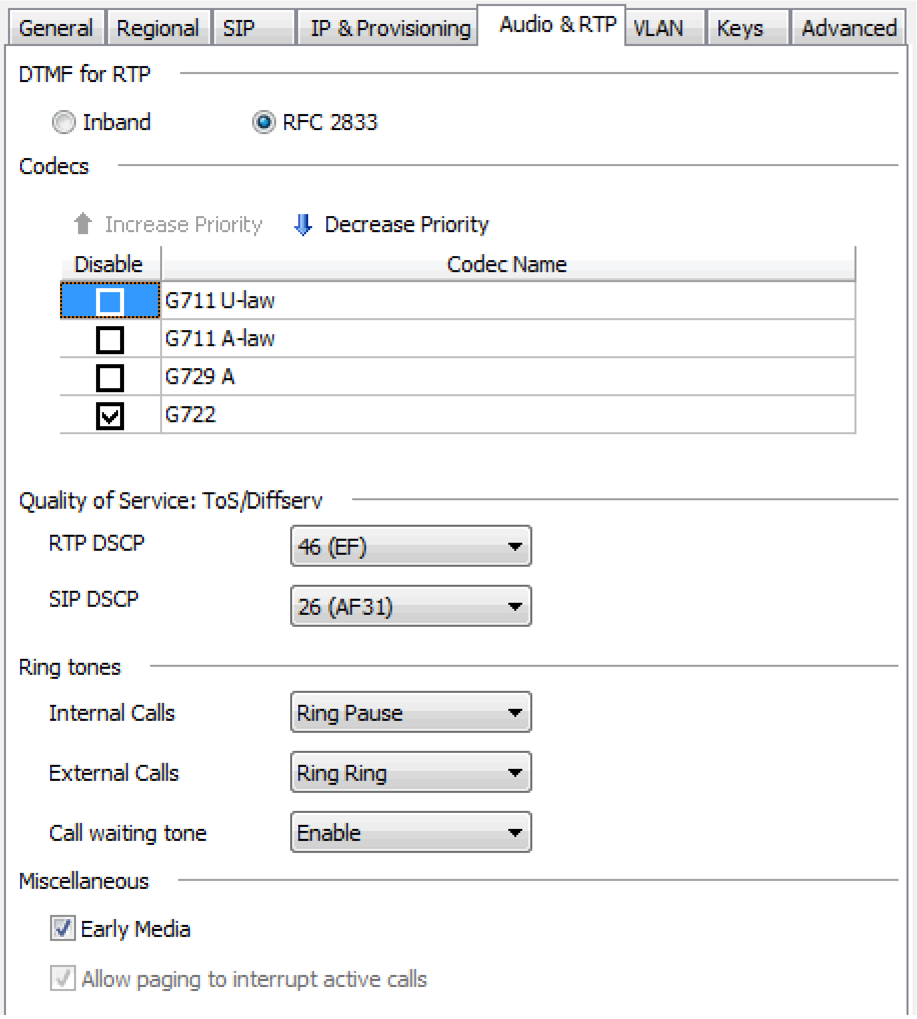
- **Protocol**: Select desired protocol to be used for configuration file download
    - **DHCP (option 66)** – Phone will obtain the TFTP server address via DHCP option 66 and then download its configuration file using TFTP. The DHCP server must have option 66 configured with the IP address of the MX-E system. This is the default setting.
    - **TFTP** – When selected the phone will download its configuration file using TFTP from the address specified in the Server section. For most applications the Server will be set to MX-E. For this option to work, the phone must initially be able to locate and connect to the MX-E TFTP server based on DHCP option 66, alternatively the address shown in the

‘URL preview’ may be manually entered via the phone’s menu or web interface.

- **FTP** - When selected the phone will download its configuration file using FTP from the address specified in the Server section. An external FTP server is required and external TFTP server option must be configured on the MX-E. The User Name field must be populated with the User Name and Password of the FTP account in the format *username:password*. For this option to work, the phone must initially be able to locate and connect to the MX-E TFTP server based on DHCP option 66, otherwise the Auto Provisioning URL setting on the phone must be manually populated with the text shown in the URL preview field.
- **HTTP** – When selected the phone will download its configuration file using HTTP from the address specified in the Server section. For most applications the Server will be set to MX-E. For this option to work, the phone must initially be able to locate and connect to the MX-E TFTP server based on DHCP option 66, alternatively the address shown in the ‘URL preview’ may be manually entered via the telephone’s menu.
- **HTTPS** - When selected the phone will download its configuration file using HTTPS from the address specified in the Server section. An external HTTPS server is required and external TFTP server option must be configured on the MX-E. For this option to work, the phone must initially be able to locate and connect to the MX-E TFTP server based on DHCP option 66, alternatively the address shown in the ‘URL preview’ may be manually entered via the telephone’s menu.

24.1.7 Audio & RTP

The Audio and RTP Tab contains setting related to DTMF, codecs, layer 3 QoS tagging, ring tones and miscellaneous settings.



DTMF for RTP

○ Inband ● RFC 2833

Codecs

Increase Priority · Decrease Priority

Disable	Codec Name
□	G711 U-law
□	G711 A-law
□	G729 A
☑	G722

Quality of Service: ToS/Diffserv

RTP DSCP: 46 (EF)

SIP DSCP: 26 (AF31)

Ring tones

Internal Calls: Ring Pause

External Calls: Ring Ring

Call waiting tone: Enable

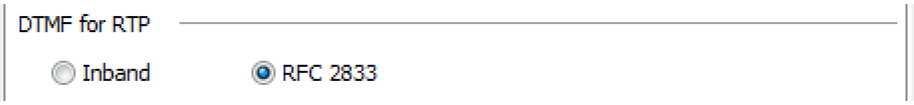
Miscellaneous

☑ Early Media

☑ Allow paging to interrupt active calls

24.1.7.1 DTMF for RTP

Use the default of RFC 2833. Sending DTMF inband is not supported by the MX-E and should not be selected.

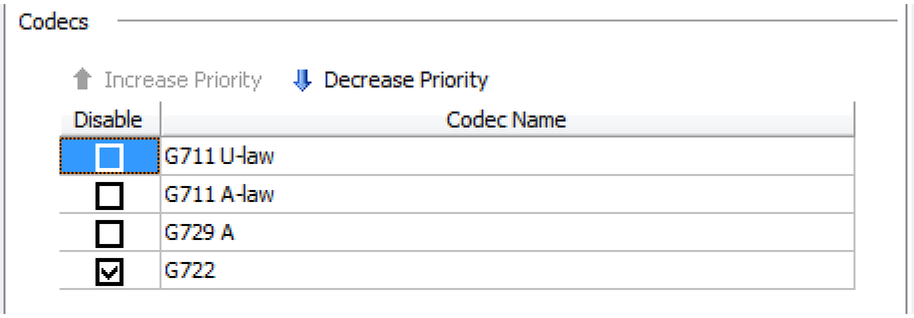


DTMF for RTP

○ Inband ● RFC 2833

24.1.7.2 Codecs

The Codecs section defines which codecs are enabled and their priority order.



Disable	Codec Name
□	G711 U-law
□	G711 A-law
□	G729 A
☑	G722

The codec at the top of the list has the highest priority. Codecs which have the **Disable** box checked are disabled.

Available codecs and the default ordering:

- G.711 µ-Law
- G.711 A-Law
- G.729a
- G.722 (Disabled by default)

To change priorities select the codec and then press the **Increase Priority** or **Decrease Priority** buttons as required. To disable a codec check the **Disable** box.

The default codec settings are suitable for most deployment scenarios. Which codec is ultimately used for a call depends on a combination of the device profile, MX-E codec profile for the location(s) and the ITSP/SIP Trunk codec profile settings if applicable.

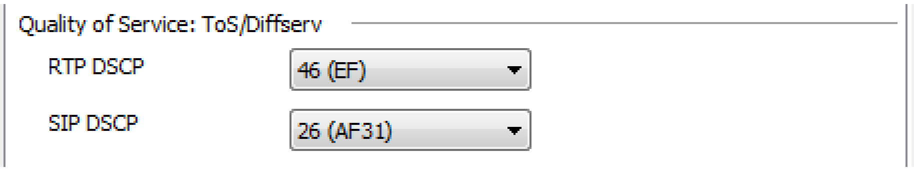
For international regions where ITSP's and SIP Trunk providers prefer to use G.711 A-Law, if the codec profile on MX-E has G.711 A-Law as the highest priority it may be desirable to also make G.711 A-Law the highest priority on the phone.

G.722 is a wideband codec which may be negotiated only between IP phones connected to the same MX-E system. The codec profile on the

MX-E system must be set to ‘Don’t Care’ to allow G.722 to be negotiated. It is recommended to leave this codec disabled.

24.1.7.3 Quality of Service: ToS/Diffserv

The Quality of Service (QoS) section defines the settings for Layer 3 DSCP packet tagging.



Quality of Service: ToS/Diffserv

RTP DSCP 46 (EF)

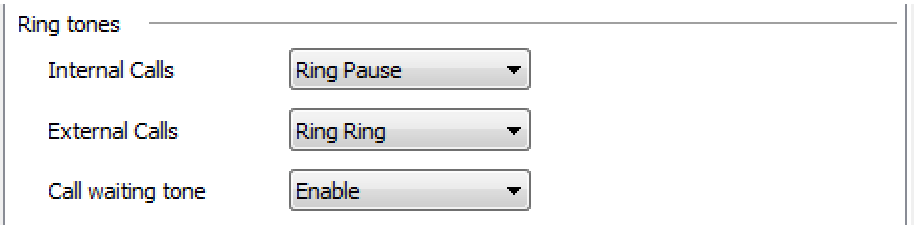
SIP DSCP 26 (AF31)

DSCP may also be referred to as Diffserv or Type of Service (ToS) tagging. RTP and SIP packets may be tagged with different DSCP values. The underlying network must be provisioned to recognize DSCP/ToS tags and prioritize the packets accordingly.

- **RTP DSCP** – Default value 46 (EF)
- **SIP DSCP** – Default value 26 (AF31)

24.1.7.4 Ring Tones

The Ring Tones section defines the ring tone settings and Call waiting tone.



Ring tones

Internal Calls Ring Pause

External Calls Ring Ring

Call waiting tone Enable

The phone has 8 built-in ring tones and supports distinctive ringing so that the user may easily differentiate between ringing internal and external calls.

The default ring tone settings in a newly created profile are based on the Time Zone setting for the Default Location of the MX-E system as defined on the **Provision →Locations** screen, thus for most deployments the default settings are appropriate.

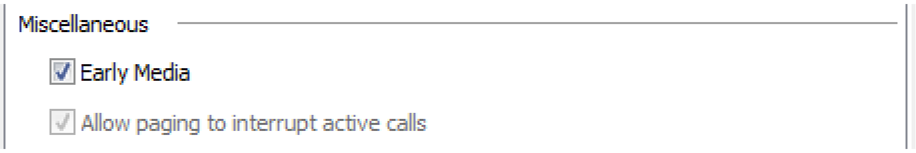
For US locations Internal Calls are assigned a **Ring** tone, and External Calls are assigned a **Ring Pause** tone.

For Australia, New Zealand, UK and related countries Internal Calls are assigned a **Ring Pause** tone, and External Calls are assigned a **Ring** tone.

For regions where no specific association is defined the default settings will be the same as for the US.

24.1.7.5 Miscellaneous

The Miscellaneous section defines settings related to Early Media support and Paging calls.



Miscellaneous

☑ Early Media

☑ Allow paging to interrupt active calls

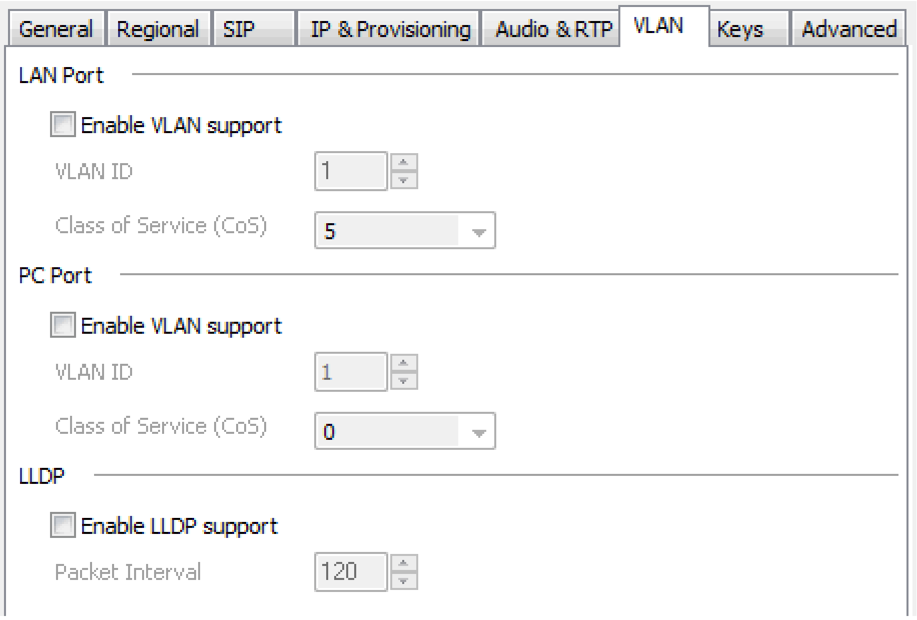
- **Early Media**: Select to enable Early Media for the phone. Early Media is a SIP mechanism which allows for inband audio to be passed through to the phone prior to the call reaching a connected state. By default this option is enabled.
- **Allow paging to interrupt active calls**: This setting is always enabled and may not be edited. Any paging call received by the phone will interrupt an active call if present. The active call will be placed on hold.

24.1.8 VLAN Tab

The VLAN tab contains settings related to VLAN tagging and LLDP support.

The phone incorporates a 2 port managed switch with the ability for voice and data traffic to use different Virtual LAN’s. VLAN settings may be configured via the profile options or automatically using LLDP (Link Layer Discovery Protocol).

When defining the VLAN settings in the profile care must be taken to ensure that once the phone downloads its configuration file it will be able to contact the MX-E system. If it cannot due to a mismatch between the VLAN settings stored in the phone and the configuration of the network, the phone will need to be factory reset via the **Menu** → **Settings** → **Advanced** → **Reset Factory** screen of phone.



LAN Port

☐ Enable VLAN support

VLAN ID: 1

Class of Service (CoS): 5

PC Port

☐ Enable VLAN support

VLAN ID: 1

Class of Service (CoS): 0

LLDP

☐ Enable LLDP support

Packet Interval: 120

24.1.8.1 LAN Port

When VLAN support is enabled for the LAN Port, all phone related packets transmitted from the LAN port will be tagged with the defined **LAN port VLAN ID** and **Class of Service (CoS)** value.

All phone related packets received from the access network must be tagged with the same VLAN ID. Effectively this can be thought of as the Voice VLAN.

24.1.8.2 PC Port

When VLAN support is enabled for the PC Port, untagged packets that enter the PC Port will be tagged with the defined **PC port VLAN ID** as they egress from the LAN port of the phone. All packets received at the LAN port which are tagged with the ID defined for the PC port will be passed to the PC port. Effectively this can be thought of as the Data VLAN. If the Data VLAN is untagged on the access network then this option should be disabled.

24.1.8.3 LLDP

As an alternative to explicitly defining the VLAN ID's for the LAN and PC ports, the Link Layer Discovery Protocol (LLDP) may be used if supported by the access switch. LLDP allows the VLAN settings to be defined at the access switch and automatically pushed to the phone.

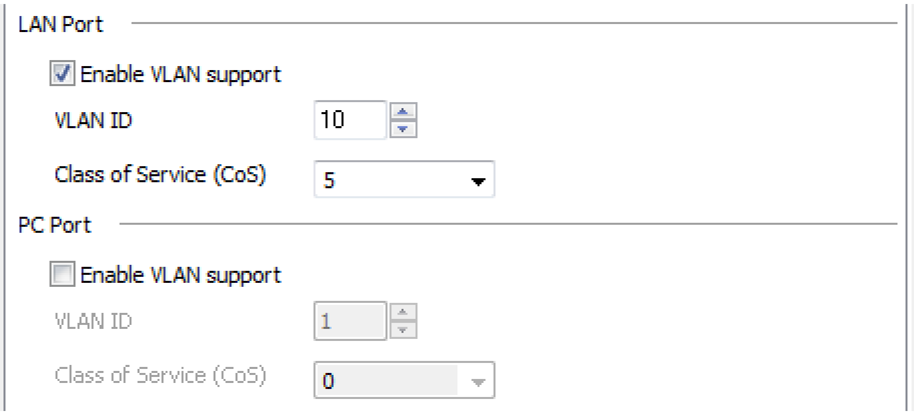
The advantage of using LLDP is that VLAN settings are determined at power up and do not rely on parameters stored in the phone, this removes the risk of the phone downloading a configuration that is invalid for the network it is connected to.

When LLDP is enabled the phone broadcasts an LLDP request on power up and then at the defined **Packet Interval**. The default period is 120 seconds.

24.1.8.4 VLAN Configuration Examples

The following examples relate to manually defining the VLAN settings via the Device Profile.

- **Tagged Voice VLAN, Untagged Data VLAN** – For many deployments that use VLAN tagging, packets related to the voice VLAN will be tagged and those related to the data VLAN will be untagged and treated as part of the native VLAN by the access switch. For the configuration shown below the Voice VLAN ID is 10 and the Data VLAN is untagged.



LAN Port

☑ Enable VLAN support

VLAN ID 10

Class of Service (CoS) 5

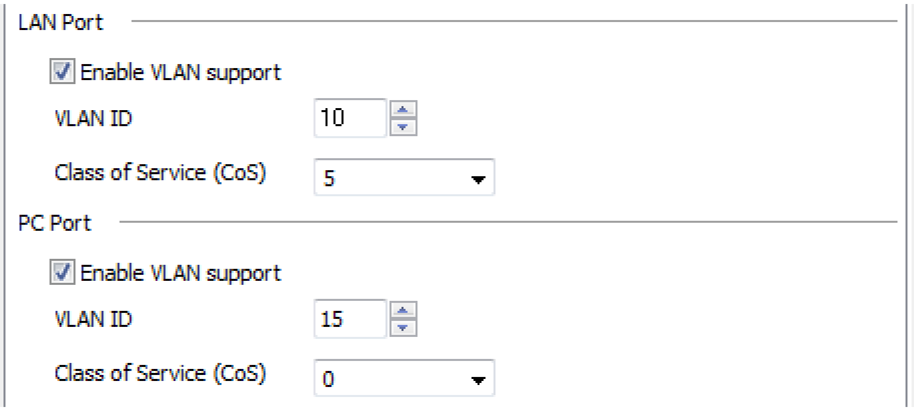
PC Port

□ Enable VLAN support

VLAN ID 1

Class of Service (CoS) 0

- **Tagged Voice VLAN, Tagged Data VLAN** – For the case where both voice and data packets are tagged as they egress and ingress at the LAN port the phone must have VLAN's enable for both the LAN and PC ports. For the configuration shown below the Voice VLAN ID is 10 and the Data VLAN ID is 15.



LAN Port

☑ Enable VLAN support

VLAN ID 10

Class of Service (CoS) 5

PC Port

☑ Enable VLAN support

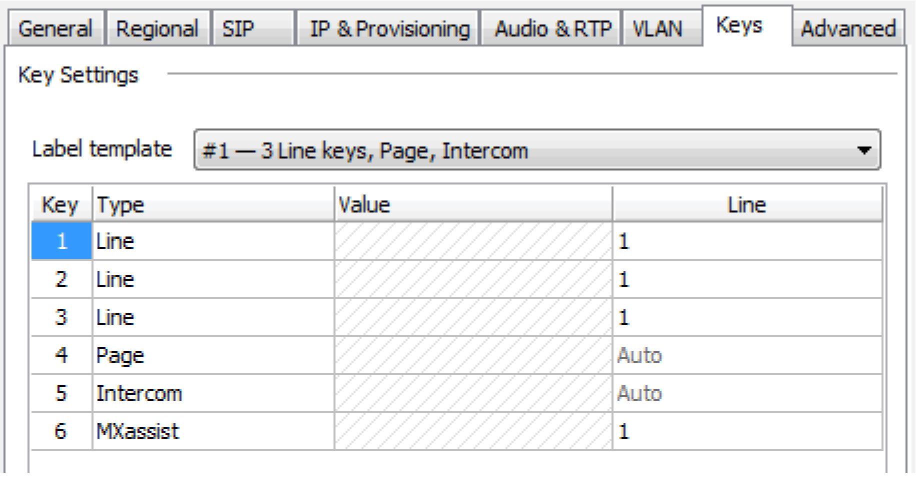
VLAN ID 15

Class of Service (CoS) 0

24.1.9 Keys Tab

The Keys tab contains setting related to the 6 programmable keys.

The key settings defined in a device profile are applied to all phones assigned the profile. Keys settings may be modified on a per phone basis by clicking the **Key Provisioning** button in the **Edit Device** screen, see section 24.1.11.



Key Settings

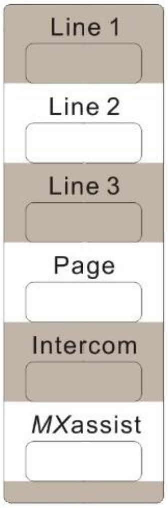
Label template: #1 — 3 Line keys, Page, Intercom

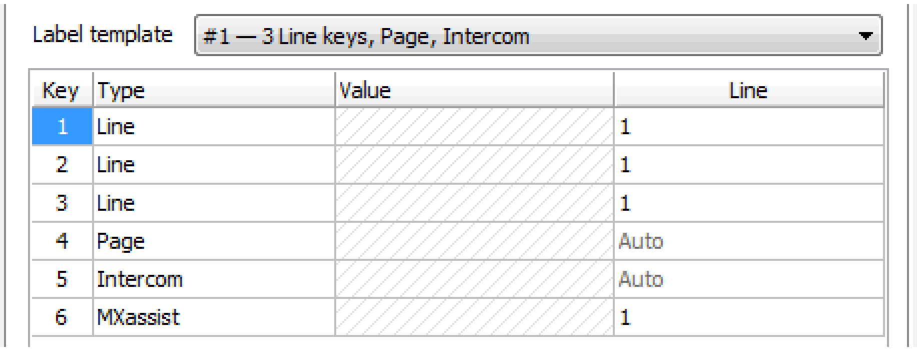
Key	Type	Value	Line
1	Line		1
2	Line		1
3	Line		1
4	Page		Auto
5	Intercom		Auto
6	MXassist		1

24.1.9.1 Label Template

The phone includes 3 pre-printed labels to cover common deployment scenarios. Select the template from the dropdown which matches the label installed on the phone. When one or more of the keys are changed from that defined by the selected template, the **Label template** dropdown will display **Custom**. Any key may be modified as required to suit the requirements of the deployment.

Label #1 – 3 Line keys, Page, Intercom (Factory installed label)

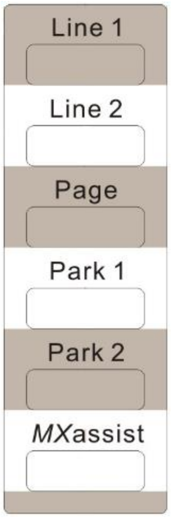


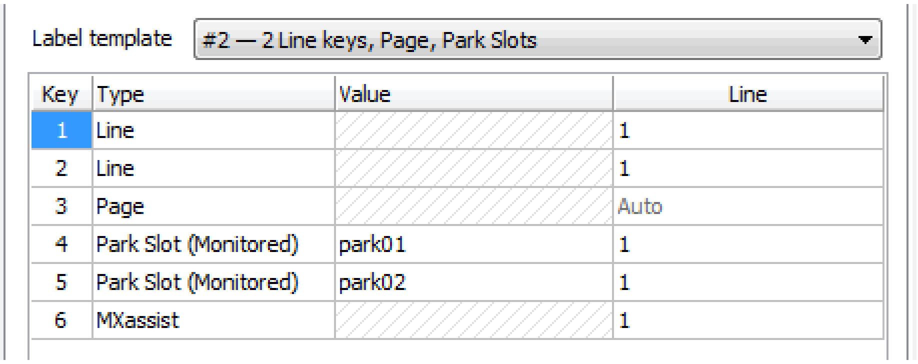


Label template: #1 — 3 Line keys, Page, Intercom

Key	Type	Value	Line
1	Line		1
2	Line		1
3	Line		1
4	Page		Auto
5	Intercom		Auto
6	MXassist		1

Label #2 – 2 Line keys, Page, Park Slots

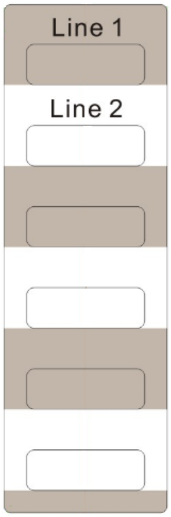


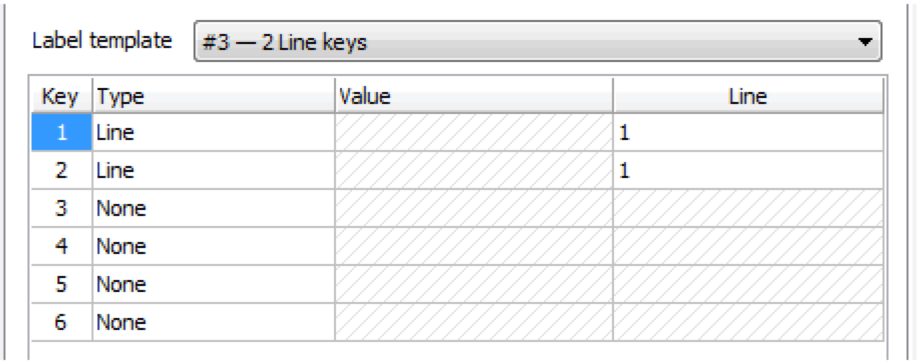


Label template: #2 — 2 Line keys, Page, Park Slots

Key	Type	Value	Line
1	Line		1
2	Line		1
3	Page		Auto
4	Park Slot (Monitored)	park01	1
5	Park Slot (Monitored)	park02	1
6	MXassist		1

Label #3 – 2 Line keys





Label template: #3 — 2 Line keys

Key	Type	Value	Line
1	Line		1
2	Line		1
3	None		
4	None		
5	None		
6	None		

24.1.9.2 Type

Select the type of key. Available options are:

- **BLF**: Defines a Busy Lamp Field (BLF) key to monitor a User or Call Group extension. **Value** is the extension number to monitor. **Line** determines the SIP registration that the BLF is associated with.

  The LED will flash when the monitored extension is ringing, pressing the flashing key will pick-up the ringing call. When the monitored User is on a call the LED will be solid red. Pressing the key when the LED is off initiates a call to the defined extension number.

Prefixing the extension number value with '+' will enable Hold indication on the key such that when the monitored user places a call on hold the LED will flash. Refer to KBS issue 11179 for further information about '+BLF'.

System wide maximums for key types that utilize BLF mechanism:

  - Maximum of 500 to 600 per system
  - Maximum of 64 stations monitoring the same extension

- **BLF (Monitor only)**: This key functions the same as 'BLF' with the exception of call pick-up. Pressing the key when it is flashing will not pick-up the ringing call.
  - This key type is included in the BLF count for the system
- **Intercom**: Facilitates an intercom call to a user extension. The called phone will automatically answer (if configured to do so in the profile) and a two-way conversation is established.
  Usage: Press key, display indicates **Dial: Intercom.** , enter the target extension number followed by **# Send.**
- **Line**: Defines a call appearance key for a specific SIP line registration. Value is the SIP line associated with the key, for most deployments this will be **1**. As an example if 3 keys are configured as **Line** for Line #1, the user will have 3 call appearance keys for SIP registration 1. At least one key must be configured as type **Line**, up to 6 keys may be configured as type **Line.**
- **Login (Call Group):** Allows the defined user to log into a defined Call Group (Operator/ACD/ICC) by pressing the key. Value must be in the format of **<group>.<user>**, where **<group>** is the Call Group extension number and **<user>** is the extension number of the user to be logged into the Call Group.
  Usage: When the button is pressed the user will be prompted to enter their voice mail password (also referred to as PIN), if the correct password is entered the call will be terminated and the LED

will become solid red. Pressing the key again will log the user out of the Call Group and the LED will turn off.

  - This key type is included in the BLF count for the system

- **Mailbox MWI**: Monitors the voice mailbox of the configured extension number. **Value** is the extension number of the mailbox to be monitored, it may be a User or Call Group extension number. The LED is solid red when there is one or more unread voice mail messages. For user extensions only the LED will flash when a caller is currently leaving a message, pressing the flashing LED will retrieve the caller. Pressing the key when either off or solid red will access the associated mailbox and prompt for password.
  - This key type is included in the BLF count for the system
- **MX-E Conference**: Provides access to MXconference service to start or join an MXconference call. MX-E system must have MXconference licenses.
- **MX-assist**: Provides access to the MXassist automated attendant service which provides help to users. To use this feature an Automated Attendant with the name 'MXassist' must be configured on the system.
- **None**: Programmable key is disabled.
- **Page**: Facilitates a call to a paging group. Care should be taken to ensure the number of ZIP 33i and ZIP 5-series phones in a paging group does not exceed 16 devices on an MX-E.
  Usage: Press key, display indicates **Dial: Page.**, enter the paging group number followed by **# Send**. After the prompt or tone begin your page.
- **Page/Intercom**: Dual purpose key that facilitates a page call to a paging group or an intercom call to an extension depending upon the number entered. Refer to Page key section above for additional details about paging.
  Usage: Press key, display indicates the Page Server extension

number (generally ***4**), for a paging call enter a 2 digit paging group extension number followed by **# Send**, for an intercom call enter the target user extension (must be 3 digits or longer) followed by **# Send**.

- **Park Slot (Monitored)**: Monitors a Park Slot, also referred to as a Park ID. In the **Value** field dropdown select the **Park ID** to monitor. When a call is currently parked at the monitored ID, the related key will flash red on all phones configured to monitor the same ID. Pressing the flashing key retrieves the parked call. When on a call pressing the key will park the call to the associated park ID.
  - This key type is included in the BLF count for the system
- **Prefix**: The Prefix key is similar to a speed dial key, when pressed the screen will display the **Prefix Value**, the user may then enter additional digits followed by **# Send** to initiate a call to the complete number.
- **Speed dial**: When pressed the phone initiates a call to the number/URI defined in the **Value** field.

24.1.9.3 Value

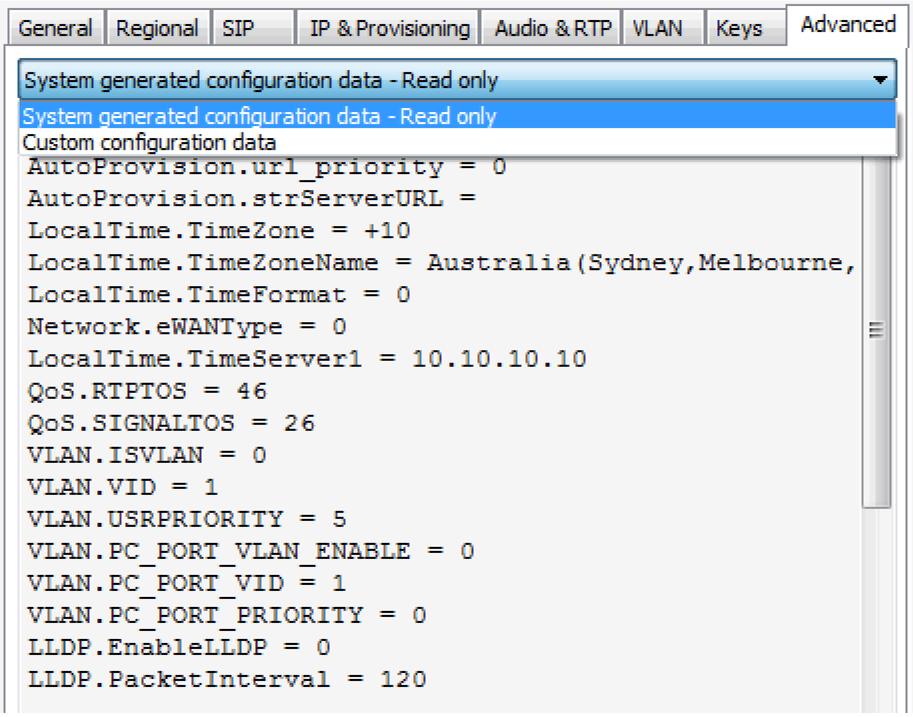
Where a key requires additional parameters such as an extension number this is entered into the **Value** field. Refer to the Key descriptions above for additional information.

24.1.9.4 Line

This parameter determines the SIP Line registration that the key is associated with. Possible selections are 1, 2 and Auto. For most deployments the Line setting will be 1 for keys that allow selection of the line number. For keys where the Auto selection is selected the phone will automatically select the SIP Line to use based on the call scenario. For key types Intercom, Page, Page/Intercom and Prefix the Line setting is always Auto.

24.1.10 Advanced Tab

The Advanced tab provides a view of the data that will be stored in the device specific <MAC>.cfg file when a device is provisioned with this Device Profile. In addition the screen provides the ability to add custom configuration data for phone options that are not exposed in the Device Profile GUI. Custom configuration data must be entered with the correct syntax including section headings. Parameters entered in the Custom screen will generally over-ride the same parameter defined in the system generated configuration data. In the event that custom settings are required Zultys Technical Support will advise the correct format for the settings.



System generated configuration data - Read only

System generated configuration data - Read only
Custom configuration data

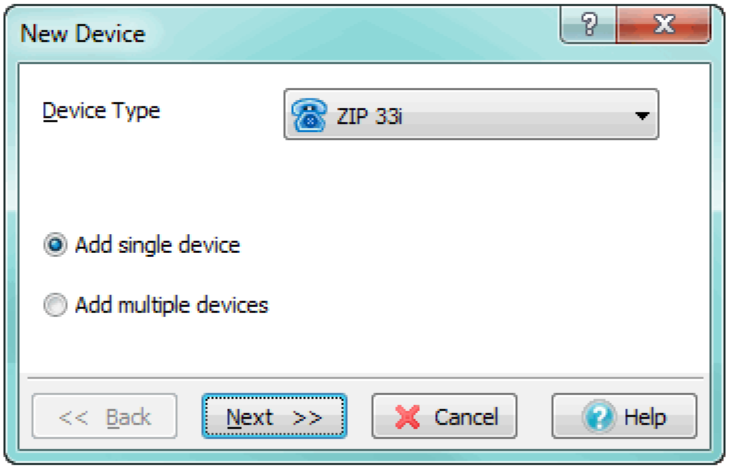
```
AutoProvision.url_priority = 0
AutoProvision.strServerURL =
LocalTime.TimeZone = +10
LocalTime.TimeZoneName = Australia(Sydney,Melbourne,
LocalTime.TimeFormat = 0
Network.eWANType = 0
LocalTime.TimeServer1 = 10.10.10.10
QoS.RTPTOS = 46
QoS.SIGNALTOS = 26
VLAN.ISVLAN = 0
VLAN.VID = 1
VLAN.USRPRIORITY = 5
VLAN.PC_PORT_VLAN_ENABLE = 0
VLAN.PC_PORT_VID = 1
VLAN.PC_PORT_PRIORITY = 0
LLDP.EnableLLDP = 0
LLDP.PacketInterval = 120
```

24.1.11 Adding a Device

Once a ZIP 33i Device Profile has been created, one or more phones may be provisioned on the MX-E system.

To add a ZIP 33i Device (phone) in MX-E Administrator:

1. Select **Configure** → **Devices** or click the **Managed Devices** icon .
2. Right click in the **Managed Devices** screen and select **Insert**, alternatively press the Insert key on keyboard.
3. In the **New Device** screen set the **Device Type** to **ZIP 33i** and press **Next.** The **Add multiple devices** option allows for multiple phones to be added via a list of MAC addresses. This document only covers the **Add single device** process.

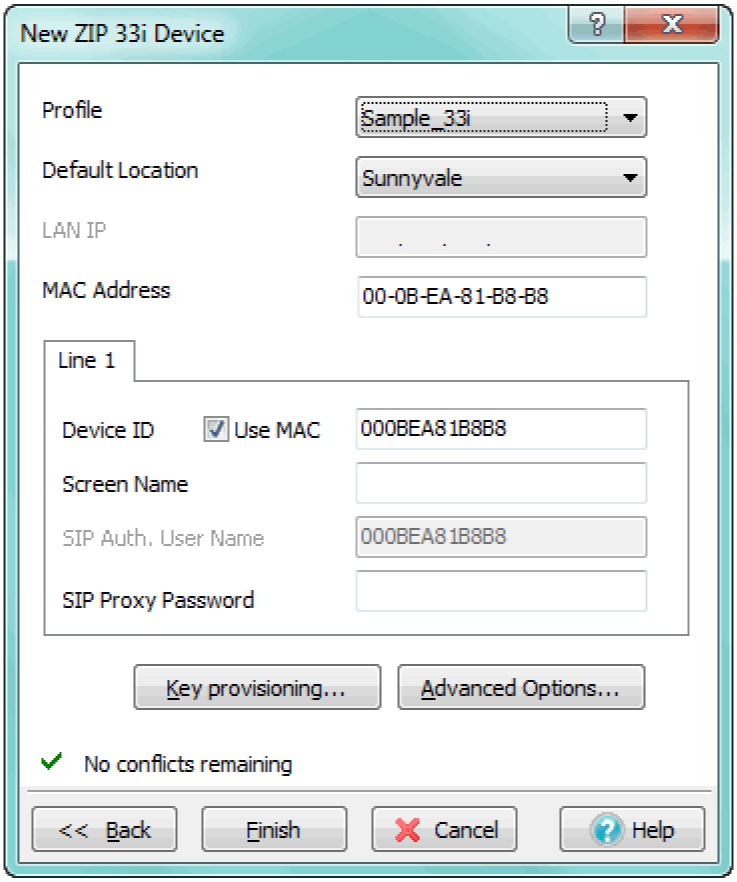


Device Type: ZIP 33i

● Add single device

○ Add multiple devices

4. In the **New ZIP 33i Device** screen, select the **Profile**, **Default Location** and enter the **MAC Address** of the phone being provisioned. The **Device ID** by default will be set to the MAC address, uncheck **Use MAC** if an alternative Device ID is to be used. The Screen Name will be displayed on the idle screen of the phone, if left blank the Device ID will be displayed.



New ZIP 33i Device

Profile	Sample_33i
Default Location	Sunnyvale
LAN IP	. . .
MAC Address	00-0B-EA-81-B8-B8

Line 1

Device ID ☑ Use MAC	000BEA81B8B8
Screen Name	
SIP Auth. User Name	000BEA81B8B8
SIP Proxy Password	

✓ No conflicts remaining

5. **SIP Proxy Password**: If the phone is to be deployed externally a SIP Proxy Password must be set, the same password must be manually entered into the phone either via the Telephone User Interface (TUI) or the phones webpage. Once the phone has downloaded its configuration file perform the following steps to store the SIP password in the phone:

   a. Via phone user interface: Press **Menu**, **3-Settings**, **2-Advanced**, enter admin password for phone (default is 'admin'), **1-Accounts**, select line to configure (usually Line 1), then press **Tick** key, arrow down to 'Password', type in SIP password and press **Tick** to accept, press **Menu** until back at idle screen.

   b. Via web interface: Obtain the IP address of phone by pressing the **Tick** key while phone is displaying Idle screen. Browse to the IP address of phone. Select **Account tab**, from the

Account dropdown select the **Account** to be edited (usually Account 1). In the Password field enter the SIP password. Press **Confirm** at the bottom of the screen to save the setting.

6. Key provisioning: If the Programmable Key settings defined in the Device Profile are to be customized for this device click **Key provisioning** and adjust the key settings as required.
7. Advanced Options: The Advanced Options screen allows custom configuration data to be added to the device specific configuration file. Generally there is no requirement to do so.
8. Press **Finish** then **Apply** to save the device configuration information to the MX-E system. The <MAC>.cfg file will be automatically created and stored on the TFTP server.
9. Depending on the Provisioning option selected (refer to section 24.1.6.3) and network configuration, when the phone is connected to the network and powered up it will automatically download its configuration file and register.

24.1.12 Fixed function keys

To facilitate easy access to common functions, the ZIP 33i phone has a range of dedicated function keys. A brief explanation of these keys appears below. Please refer to the ZIP 33i User’s Guide for detailed information.

Menu – Access the phone features and settings menu

DND – Enable / Disable Do Not Disturb. When enabled, any call offered to the phone will be rejected with a 486 BUSY response.

Park – Access the Park/Pickup feature. Pressing the **Park** key during an active call results in the call being parked and the system allocated Park ID being displayed on screen. Pressing the **Park** key when the phone is idle or off hook but not on an active call prompts the user to enter a Park ID to retrieve a parked call. Press **# Send** to initiate call after entering ID.

Directory – Provides access to the local directory stored on the phone.

Call Log – Provides access to the call log of the phone. When pressed the "All calls" list is displayed, left and right cursor keys switch between all, missed, inbound, outbound and forwarded call logs.

X / End Call – When a call is active pressing this key disconnects the call. The key also acts as a delete key when entering information and a cancel or back key during menu operations.

Message – Provides access to the voice mail service of the MX-E system. Also acts as Message Waiting Indicator (MWI). Key is illuminated green when one or more unread voice mail messages are available for the user. The red status LED of the phone will also flash when an unread voice mail message is present.

Headset – Enables headset mode. When illuminated green the headset mode is active and calls answered via the line keys or MXIE will utilize the headset. In addition pressing the key while an incoming call is ringing will answer the call and route the audio to the headset. Optional headset must be connected.

Conference – Facilitates setup of local 3 way conference calls.
Usage: Press **Conference** during an active call. The call will be placed on hold. Enter the number of the second party and then press **# Send**. Press **Conference** again when the second party answers. All parties are now joined in the conference. Note: To conference two existing calls, place one call on hold then press **Conference** while the other call is active.

Hold – When a call is active pressing this key places the call on hold. Press again to retrieve call.

Mute – Enable/disable the microphone during an active call.

Transfer – Facilitates call transfer operations.
Usage:

- Blind Transfer: Press **Transfer** during an active call. The call is placed on hold. Enter the number you want to transfer to. Press **Transfer**.

  - Attended Transfer: Press **Transfer** during an active call. The call is placed on hold. Enter the number you want to transfer to and then press **# Send**. Press **Transfer** when ready to complete the transfer or **X key** to cancel transfer.

Redial – Facilitates redialing of recently called numbers.
Usage: Press **Redial** to enter the Dialed Calls list, press **Up** or **Down** keys to select the desired call and then press **Redial** or **# Send**. To access other areas of the Call History use **Left** and **Right** keys.
Press **Redial** twice when the phone is idle to call the last dialed number.

Speaker – Press the **Speaker** key when a call is ringing to answer in handsfree mode.

24.1.13 Controlling Configurations

24.1.13.1.1 Configuration methods

The ZIP 33i phone may be configured via the following methods:

- As a managed device in MX-E Administrator (The method detailed in this document)
- Web interface of phone
- Menu of phone

Provisioning a phone as a managed device on the MX-E system automatically generates a configuration file on the MX-E's TFTP server with the name <MAC>.cfg. For example for phone with MAC address 000BEA81B8B8, the filename is 000bea81b8b8.cfg.

⚠ Any manual configuration changes performed via the web interface or the menu of the phone will take precedence over the configuration options defined in the configuration file downloaded from the MX-E TFTP server.

If a phone has been manually configured via the web interface or phone menu, the phone must be Factory Reset to fully restore automatic provisioning. Refer to section 24.1.15.1.1.

24.1.13.1.2 Phone Initialization

Upon power-up a new or un-configured phone will initialize as follows:

- Request IP address and Option 66 (TFTP server address) from DHCP server.
- Request zip33i_common.cfg file from TFTP server.
- Request <MAC>.cfg file from TFTP server.
- Request new firmware ROM image file from TFTP server if defined in cfg file.
- Complete power-up and register with MX-E system based on settings defined in cfg files.

The **zip33i_common.cfg** file referred to above may be used to apply custom configuration settings to all ZIP 33i phones connected to an MX-E system. Generally there is no requirement to use this file.

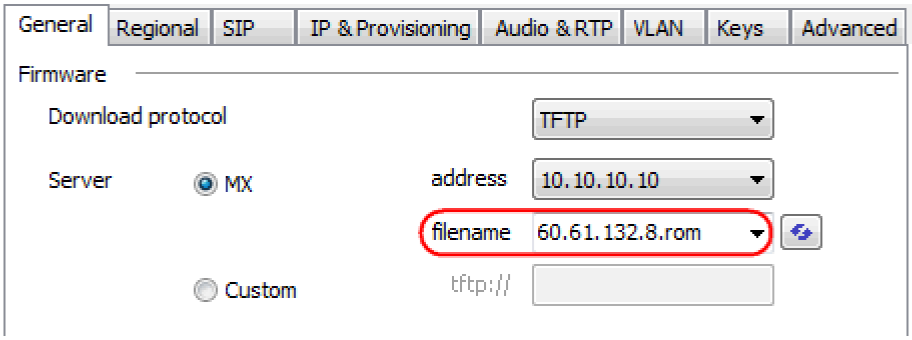
24.1.14 Upgrading Firmware

24.1.14.1.1 Upgrading firmware via Device Profile

When a ZIP 33i is provisioned as a managed device via MX-E Administrator, the firmware version of the phone is determined by the Firmware filename defined in the Device Profile. The corresponding firmware ROM file must be uploaded to the TFTP server of the MX-E system. Firmware ROM files are available for download the Zultys Knowledge Base System (http://kbs.zultys.com).

To upgrade/change the firmware version of a ZIP 33i phone perform the following steps:

1. From **Configure → Devices** screen press the TFTP Settings... button.
2. Copy the <version>.rom file (EG: 60.61.132.8.rom) to the TFTP server. Press **Close.** Note: All ZIP 33i firmware image files have the format 60.x.x.x.rom (EG: 60.61.132.8.rom).
3. Open the **Device Profile** associated with the Device that is to be updated.
4. In the **filename** field located on the **General tab** select the filename of file uploaded in step 2.



Firmware

Download protocol: TFTP

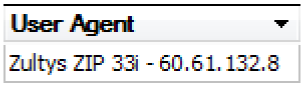
Server: ● MX ○ Custom

address: 10.10.10.10

filename: 60.61.132.8.rom

tftp://

5. Press **OK** then **Apply** to save changes to MX-E.
6. Select the device to be updated from the device list. Multiple devices may be selected via standard Windows Shift+Click and Ctrl+Click keyboard controls.
7. Click the Update button to send the update request to each phone that is currently registered to the MX-E system.
8. Alternatively power cycle or power up each phone to trigger a firmware update.
9. Once complete the firmware version may be checked via the User Agent field of **View → Device Status** screen.



User Agent
Zultys ZIP 33i - 60.61.132.8

24.1.14.1.2 Upgrading firmware via Web interface

For cases where the phone is not provisioned as a managed device or cannot access the TFTP server, the firmware may be updated via the phones web interface.

To upgrade the firmware via the web interface of phone perform the following steps:

1. Browse to the IP address of the phone. The IP address may be found by pressing the **Tick** key at the idle screen.
2. Enter the **username** 'admin' and the administration **password**, default password is 'admin'.
3. From the top menu select the **Phone tab**.
4. From the left menu select **Upgrade**.

5. Select **Browse** and browse to the ROM file, then select **Open**.
6. Select **Upgrade.** To proceed with upgrade press **OK** on the warning popup.
7. Do not disconnect power or exit webpage until the phone has restarted.
8. Once the upgrade is complete the webpage will be refreshed (assuming the IP address of the phone has not changed during restart).
9. The current firmware version is displayed on the **Phone →Upgrade** webpage and also on the **Status** webpage.

Note that if after the upgrade the phone downloads a configuration file that defines a different firmware version, the phone will immediately upgrade to the version defined in the configuration file.

⚠ **Warning**: Once the download process for the new firmware starts you must not disconnect power or restart the phone. If the process is interrupted, the phone will lose all firmware and the emergency recovery process will need to be performed. Contact your Authorized Zultys Channel Partner or Zultys Technical Support should this situation arise.

24.1.15 Troubleshooting Tips and Tools

24.1.15.1.1 Factory resetting phone

Should an invalid configuration be downloaded to or set on the phone it may be necessary to perform a factory reset. Resetting the phone to factory defaults removes all configuration settings from the phone including those applied via the web interface and menu of the phone.

Steps to Factory Reset a phone:

- Press **Menu**
- Select **3-Settings**
- Select **2-Advanced**
- Enter Admin **password.** Default password is ‘admin’
- Select **4-Reset Factory**
- Screen will display **Reset to Factory?**, press **Tick** key to proceed with reset. Screen will display **Please wait Reset..**
- Phone will now perform initialization per section 24.1.13.1.2.

24.1.15.1.2 Phone does not use the configuration file on TFTP server

If the ZIP 33i phone does not use the configuration file, or some settings defined in the configuration file do not appear to be used, check the following:

- Make sure you have not previously configured the phone using the web interface or the phone interface. Any option manually configured from the web interface or the phone interface will take precedence over the values contained in the configuration file downloaded from the TFTP server.
- Make sure the MAC address defined in MX-E Administrator matches the MAC address of the phone. To check the MAC on the phone press the **Tick** button while the idle screen is displayed, then press the **Down** arrow to display MAC address.
- Confirm the DHCP Server is providing the IP address of the TFTP server in Option 66. If Option 66 is not being used the phone must be manually configured with the provisioning server address.
- Phone was previously configured via the web or phone interface.
    - Reset the phone to factory defaults and configure using a configuration file from the MX-E.

24.1.15.1.3 How to check if configuration file is downloaded

A simple way to confirm if a phone is downloading its configuration file is to change the **Screen Name** set in the **Edit Device** screen. Apply the change then power cycle the phone. If the screen name displayed on the phone changes to the new value defined via MX-E Administrator then the phone is correctly downloading the configuration file from the MX-E system.

24.1.15.1.4 Performing network packet capture on the phone

The ZIP 33i phone has the ability to perform a packet capture in pcap format which is compatible with Wireshark. To facilitate a packet capture perform the following steps:

1. Browse to the IP address of the phone. The IP address may be found by pressing the **Tick** key at the idle screen.

2. Enter the **username** ‘admin’ and the administration **password**, default password is ‘admin’.
3. From the top menu select the **Phone tab**.
4. From the left menu select **Upgrade**.
5. In the **PCAP Trace** section click Start.
6. To stop the packet capture click Stop.
7. To export the captured information click Export and save the file to an appropriate location.
8. The file may now be opened in Wireshark or similar packet analysis applications.

24.1.15.1.5 Capturing Syslog information

The ZIP 33i phone has the ability to generate Syslog information that may assist Zultys Technical Support with investigation of issues. This information may be stored locally on the phone or output to an external Syslog server. If instructed to do so you may enable the Syslog feature by one of the following methods:

24.1.15.1.6 Capturing Syslog information locally on phone

1. Browse to the IP address of the phone. The IP address may be found by pressing the **Tick** key at the idle screen.
2. Enter the **username** ‘admin’ and the administration **password**, default password is ‘admin’.
3. From the top menu select the **Phone tab**.
4. From the left menu select **Configuration**.
5. Set **Export System Log** option to **Local**.
6. Set **SystemLogLevel** to the value requested by Zultys Technical Support. The higher the number the more detailed the information captured.
7. Press Confirm to accept changes.
8. To save stored events click Export and select a location to save file to.

24.1.15.1.7 Enabling Syslog output to external server via web interface

This setup requires an external syslog server, it is assumed the system administrator has setup a suitable syslog server.

1. Browse to the IP address of the phone. The IP address may be found by pressing the **Tick** key at the idle screen.
2. Enter the **username** ‘admin’ and the administration **password**, default password is ‘admin’.
3. From the top menu select the **Phone tab**.
4. From the left menu select **Configuration**.
5. Set **Export System Log** option to **Server**.
6. Enter the IP address of the external syslog server in the Server Name field.
7. Set **SystemLogLevel** to the value requested by Zultys Technical Support. The higher the number the more detailed the information captured.
8. Press Confirm to accept changes.
9. The phone will now send Syslog messages to the configured Syslog server address.

24.1.15.1.8 Enabling Syslog output to external server via configuration file

This setup requires an external syslog server, it is assumed the system administrator has setup a suitable syslog server.

1. Create a new Device Profile to be used by the phone under test. Generally the easiest way to do this is by creating a duplicate of the current profile.
2. On the **Advanced tab** of the Profile select **Custom configuration data.**
3. Enter the following custom configuration parameters –

   ```
   [ cfg:/phone/config/system.ini,reboot=0 ]
   SYSLOG.SyslogdIP = 192.168.1.100
   [ cfg:/phone/config/user.ini,reboot=0 ]
   PhoneSetting.LogLevel = 5
   ```

   Replace the IP address with the address of your external Syslog server. Set the **LogLevel** to a value between 1 and 6 as advised by Zultys Technical Support.
4. Press **OK** then **Apply** to accept the Profile changes.
5. Assign the Profile to the device under test.

6. Select the device in the device list and press **Update** to trigger the phone to download the new configuration file.
7. The phone will now send Syslog messages to the configured Syslog server address.

Once the required syslog information is captured the phone should be returned to the default settings of Local and Level 3.

24.1.16 Emergency Recovery Mode

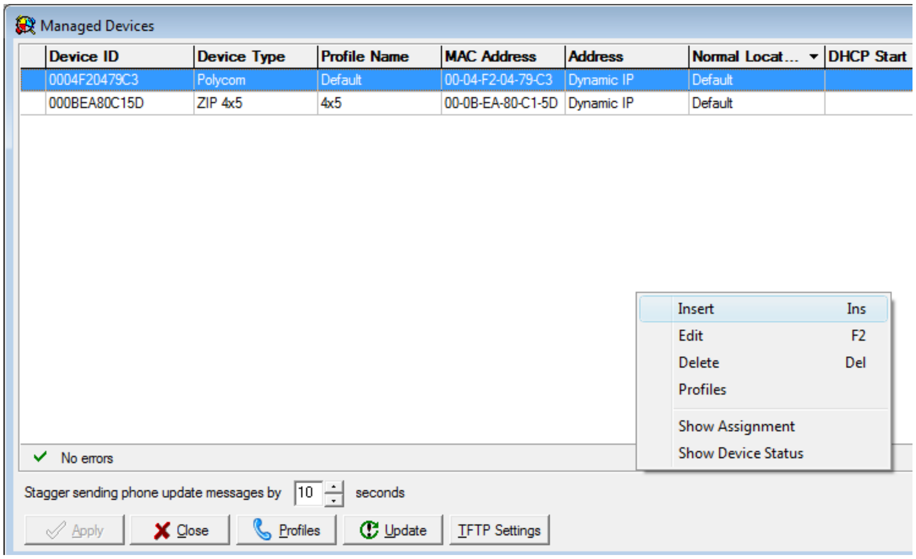
In the event that the phone is unable to initialize following a failed firmware upgrade due to power loss or similar, it may be possible to use the Emergency Recovery Mode to reload the firmware.

For assistance with this process please contact your Zultys Authorized Channel Partner or Zultys Technical Support.

25. Adding Devices – ZIP2x2

25.1 Add the device as a Managed Device

In the MX-E Administrator, go to *Provision* → *Devices*, a table of devices already assigned to the system. On the table right click and choose *Insert*.



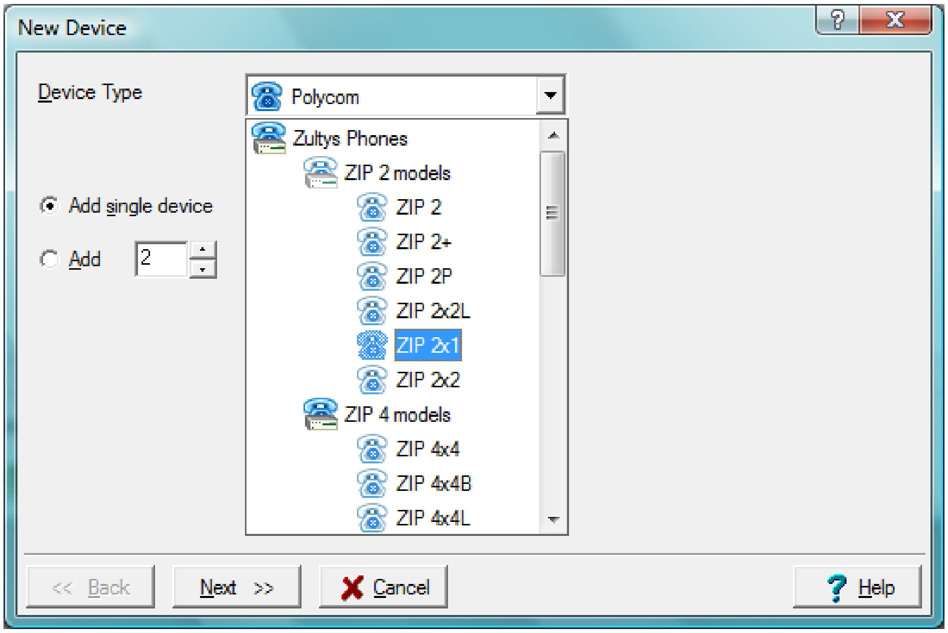
Managed Devices

Device ID	Device Type	Profile Name	MAC Address	Address	Normal Locat...	DHCP Start
0004F20479C3	Polycom	Default	00-04-F2-04-79-C3	Dynamic IP	Default	
000BEA80C15D	ZIP 4x5	4x5	00-0B-EA-80-C1-5D	Dynamic IP	Default	

✓ No errors

Stagger sending phone update messages by 10 seconds

Choose a device type from the drop down



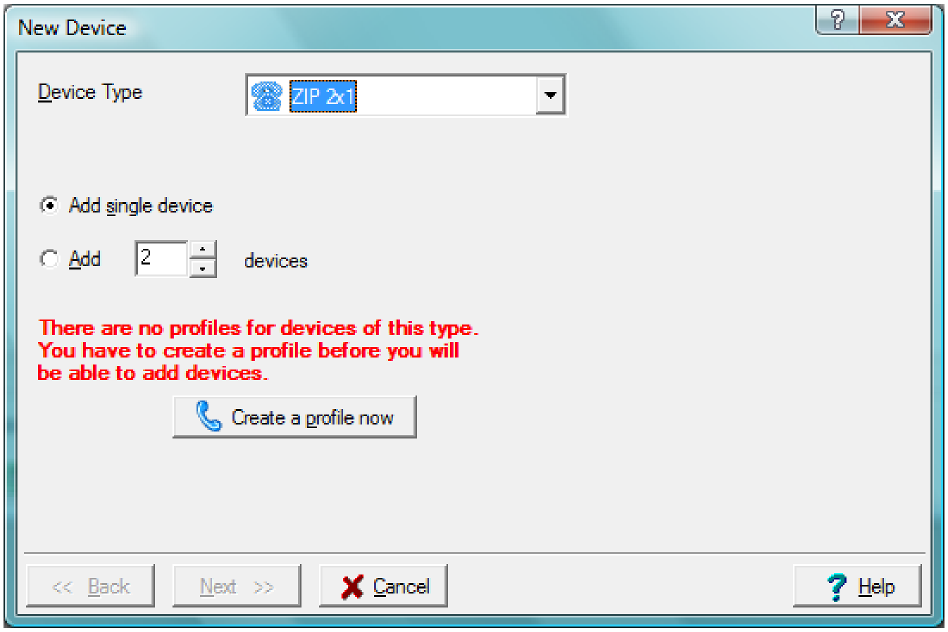
Device Type: Polycom

● Add single device

○ Add 2

And click *Next>>*.

If no profile is defined it will warn you that you need to create one.



Device Type: ZIP 2x1

● Add single device

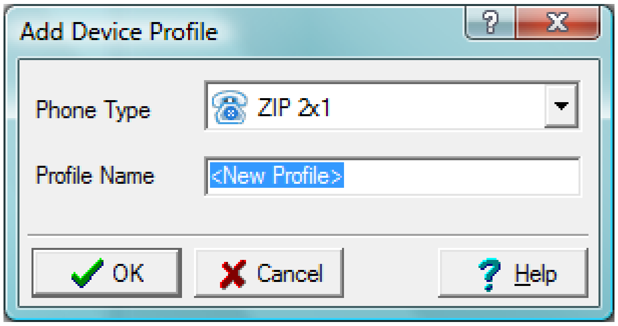
○ Add 2 devices

There are no profiles for devices of this type. You have to create a profile before you will be able to add devices.

To create a profile click *Create a profile now*.

25.2 Create a profile

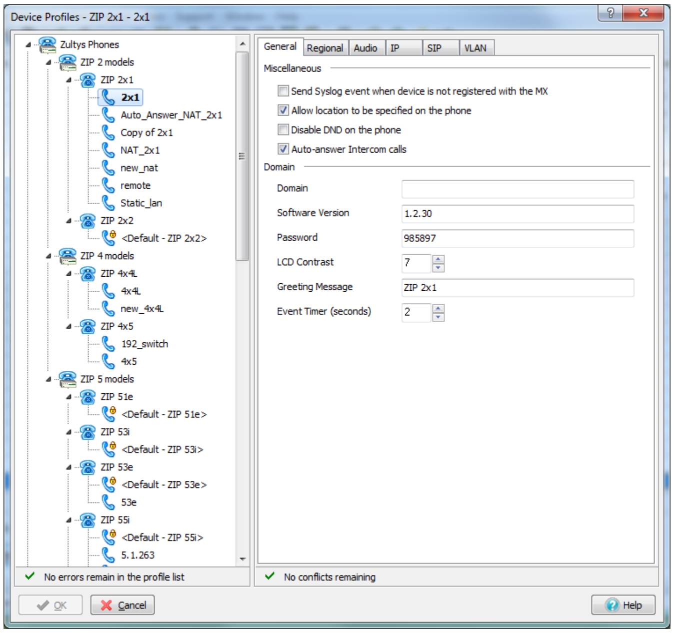
Click on the create profile now button, and assign it a name.


Add Device Profile

Phone Type: ZIP 2x1

Profile Name: <New Profile>

Once a name is given the profile screen is displayed.


Device Profiles - ZIP 2x1 - 2x1

- Zultys Phones
  - ZIP 2 models
    - ZIP 2x1
      - 2x1
      - Auto_Answer_NAT_2x1
      - Copy of 2x1
      - NAT_2x1
      - new_nat
      - remote
      - Static_lan
    - ZIP 2x2
      - <Default - ZIP 2x2>
  - ZIP 4 models
    - ZIP 4x4L
      - 4x4L
      - new_4x4L
    - ZIP 4x5
      - 192_switch
      - 4x5
  - ZIP 5 models
    - ZIP 51e
      - <Default - ZIP 51e>
    - ZIP 53i
      - <Default - ZIP 53i>
    - ZIP 53e
      - <Default - ZIP 53e>
      - 53e
    - ZIP 55i
      - <Default - ZIP 55i>
      - 5.1.263

Miscellaneous

☐ Send Syslog event when device is not registered with the MX
☑ Allow location to be specified on the phone
☐ Disable DND on the phone
☑ Auto-answer Intercom calls

Domain

Domain	
Software Version	1.2.30
Password	985897
LCD Contrast	7
Greeting Message	ZIP 2x1
Event Timer (seconds)	2

✓ No errors remain in the profile list

✓ No conflicts remaining

25.2.1 General Tab

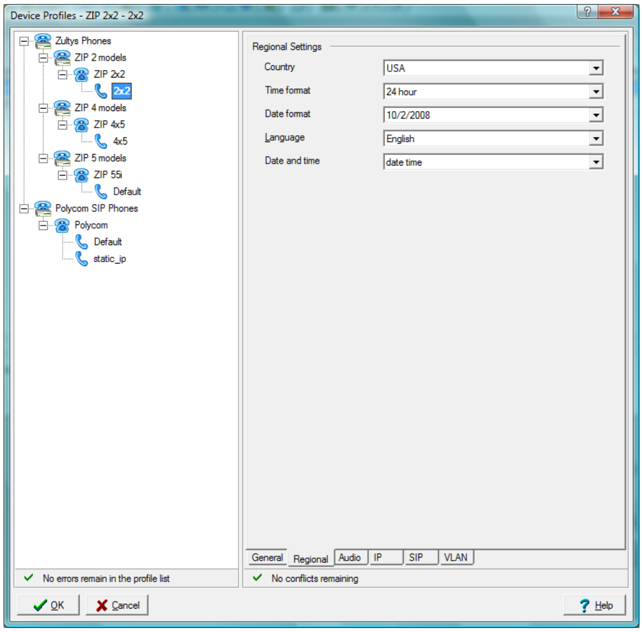
On the general tab the following fields are given

- **Software Version**: This is the software version that the phone is running. To upgrade the firmware on a Zip 2xN phone you must update this field with the version of choice.
- **Password**: This parameter specifies password required to change the protected settings. Valid passwords contain four to fifteen numeric (0-9) digits. Default password is 985897. If you change the password on the phone and also specify the password in the configuration file, the next time the phone boots up (or is sent an update request) it will take the password from the configuration file. The password in the configuration file therefore overwrites whatever was in the phone. If you do not want to overwrite whatever is in the phone, leave the password field blank. The configuration file then does not overwrite the password stored in the phone.
- **LCD Contrast**: The parameter alters the contrast of the LCD at the top of the phone. Valid settings range from 1 to 20; default value is 7.
- **Greeting Message:** This is the message that the top row of the LCD displays when the phone is idle. This parameter is not available on the ZIP2x2L, ZIP2+, and ZIP2P. These phones do not support a greeting message.
- **Event Timer**: Specifies the duration, in seconds, that some error messages and information screens are displayed on the LCD. Valid settings range from 2 to 10. Default value is 2.
- **Reject Instant Messages**: When set, this parameter programs the phone to reject all incoming instant messages.
- **Domain**: This parameter specifies the domain in which the phone resides. Used for manual configuration when DHCP is not enabled or the DHCP server does not return the domain (DHCP option 15).
- **Send Syslog event when device is not registered with the MX-E**: Select this option to program the MX-E to generate a Syslog event when a

device with this profile is not registered with the MX-E. The parameter does not affect the operation or configuration of the phone.

- **Allow Location to be specified on the phone**: Select this option to allow users to specify their MX-E location from the phone.
- **Disable DND:** Select this option to disable the DND button on the phone.
- **Auto-answer Intercom calls**: Select this option to allow users to intercom the phone.

25.2.2 Regional Tab



Device Profiles - ZIP 2x2 - 2x2

Regional Settings

Country: USA

Time format: 24 hour

Date format: 10/2/2008

Language: English

Date and time: date time

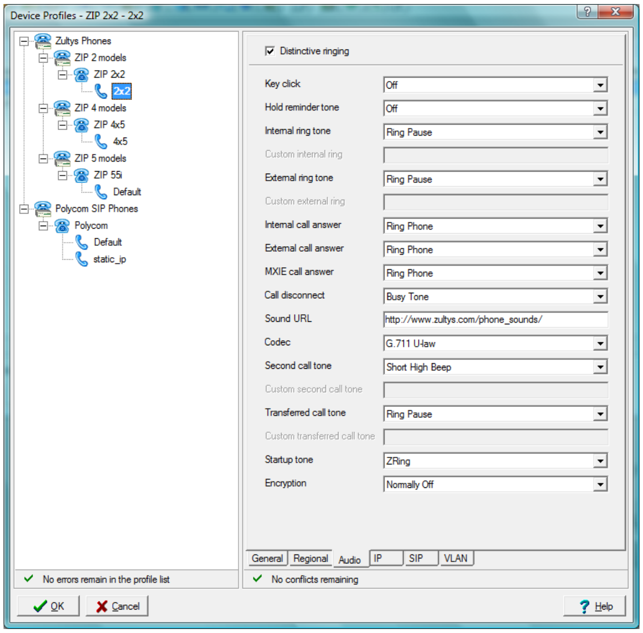
✓ No errors remain in the profile list

✓ No conflicts remaining

- **Country**: Specifies the call progress tones used by the phone, as defined by country variation.
- **Time Format**: This parameter specifies the format used by the LCD to display time.
- **Date Format**: This parameter specifies the format used by the LCD to display the date.
- **Language**: This parameter specifies the language that the phone uses to display phone settings on the LCD.

- **Date and Time**: This parameter specifies the display order of the date and time on the LCD.
- **Number Format**: This parameter specifies the calculator format settings for the decimal point and thousands delimiter.

25.2.3 Audio tab



☑ Distinctive ringing

Key click	Off
Hold reminder tone	Off
Internal ring tone	Ring Pause
Custom internal ring	
External ring tone	Ring Pause
Custom external ring	
Internal call answer	Ring Phone
External call answer	Ring Phone
MXIE call answer	Ring Phone
Call disconnect	Busy Tone
Sound URL	http://www.zultys.com/phone_sounds/
Codec	G.711 U-law
Second call tone	Short High Beep
Custom second call tone	
Transferred call tone	Ring Pause
Custom transferred call tone	
Startup tone	ZRing
Encryption	Normally Off

✓ No errors remain in the profile list

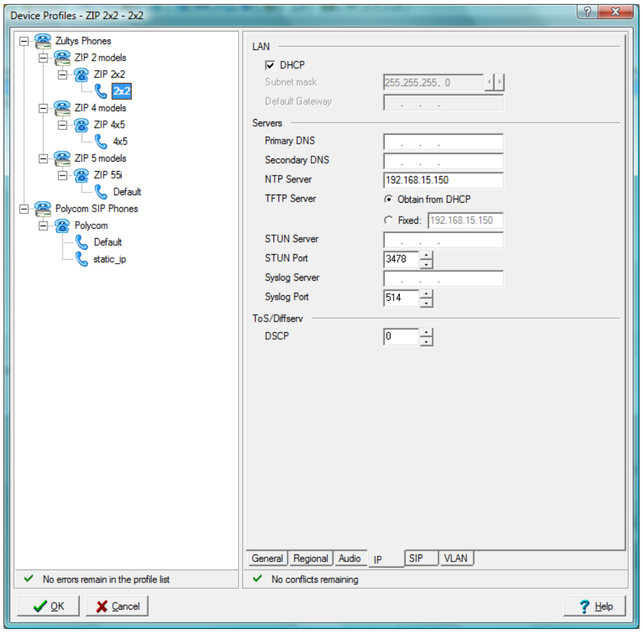
✓ No conflicts remaining

- **Distinctive Ringing**: When enabled, this parameter specifies the use of different ring tones for internal and external calls.
- **Key Click**: This parameter specifies the tone that the phone emits when you press a button or a non-numeric key.
- **Hold Reminder Tone**: This parameter specifies the tone that the phone plays when it has a call on hold. This tone is played once every 30 seconds.
- **Internal Ring Tone**: This parameter specifies the ring tone for calls received from phones inside the enterprise.
- **Custom Internal Ring**: This parameter specifies the file that provides the call waiting tone for internal calls when External Ring Tone is set to custom.

- **External Ring Tone**: This parameter specifies the ring tone for calls received from phones outside the enterprise.
- **Custom External Ring**: This parameter specifies the file that provides the call waiting tone for external calls when External Ring Tone is set to custom.
- **Internal Call Answer**: This parameter programs the phone to automatically go off hook for internal calls after one ring. Select Auto Answer to route the call through your external speaker. Select Auto Answer Hook to route the call through your headset. Select Ring Phone to play the internal ring tone until you take the phone off hook or a system call handling routine sends the call to an operator or your voice mail.
- **External Call Answer**: This parameter programs the phone to automatically go off hook for external calls after one ring. Select Auto Answer to route the call through the external speaker. Select Auto Answer Hook to route the call through the headset. Select Ring Phone to play the external ring tone until you take the phone off hook or a system call handling routine sends the call to an operator or your voice mail.
- **MXIE Call Answer:** This parameter programs the phone to automatically go off hook after one ring for outbound calls that you dial from MXIE. Select Auto Answer to route the call through your external speaker. Select Auto Answer Hook to route the call through your headset. Select Ring Phone to play the internal ring tone until you take the phone off hook.
- **Call Disconnect**: This parameter programs the phone behavior after the other party disconnects a call. Select Busy Tone to program the phone to play a busy tone for five seconds after the other party disconnects from a phone call. Select Busy Tone Timeout to program the phone to play a busy tone for five seconds after the other party disconnects from the call. Select Silent to program the phone to disconnect the phone without playing any tone.
- **Sound URL**: This parameter specifies the http directory location for files that define custom ring tones. Valid setting is http://<name of directory>.

- **Codec**: This parameter specifies the speech encryption standard (G.711 or G.729) and companding method used by the configured phones. This parameter is not available on the ZIP2x2L, ZIP2+, and ZIP2P.
- **Second Call Tone**: This parameter specifies the call waiting tone that is played when you are talking on the phone and the phone receives another call. This parameter is not available on the ZIP2x2L, ZIP2+, and ZIP2P.
- **Custom Second Call Tone**: This parameter specifies the file that provides the second call tone when Second Ring Tone is set to custom. This parameter is not available on the ZIP2x2L, ZIP2+, and ZIP2P.
- **Startup Tone**: This parameter specifies the tone that the phone emits when the phone is powered.
- **Encryption**: This parameter specifies the encryption mode for phones configured by the profile. This parameter is not available on the ZIP2x2L, ZIP2+, and ZIP2P.

25.2.4 IP Tab


Device Profiles - ZIP 2x2 - 2x2

LAN

☑ DHCP

Subnet mask: 255.255.255. 0

Default Gateway: . . .

Servers

Primary DNS: . . .

Secondary DNS: . . .

NTP Server: 192.168.15.150

TFTP Server: ● Obtain from DHCP ○ Fixed: 192.168.15.150

STUN Server: . . .

STUN Port: 3478

Syslog Server: . . .

Syslog Port: 514

ToS/Diffserv

DSCP: 0

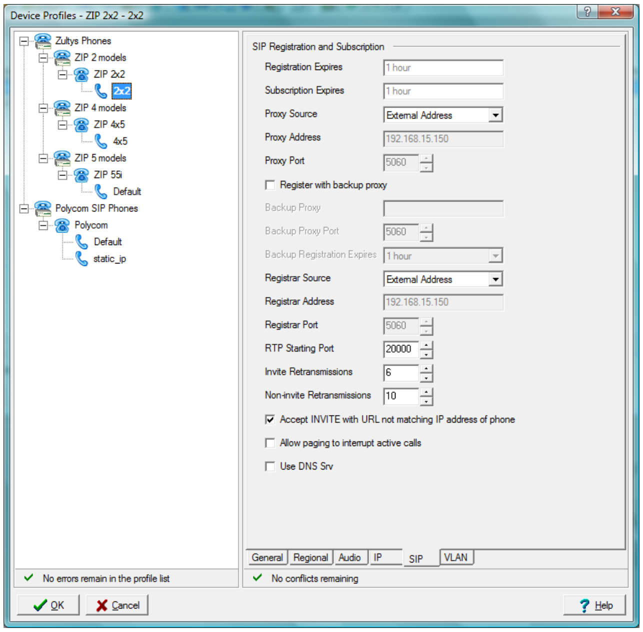
✓ No errors remain in the profile list

✓ No conflicts remaining

- **DHCP**: When this parameter is selected, phone uses DHCP to configure network settings: IP address, subnet mask, domain name, default gateway, DNS servers, NTP server address, and TFTP server address.

- **Subnet Mask**: This parameter is used for manually configuring the phone when DHCP is not enabled.
- **Default Gateway**: This parameter is the IP address of the gateway that is used for manual configuration when DHCP is not selected or DHCP does not provide the default gateway (DHCP option 3).
- **Primary DNS**: This parameter is the IP address of the primary DNS Server. Used for manual configuration when DHCP is not selected or DHCP does not return DNS Server (DHCP option 6).
- **Secondary DNS**: This parameter is the IP address of the secondary DNS Server that is used for manual configuration when DHCP is not selected or DHCP does not return a valid address.
- **NTP Server**: This parameter is the IP address of the NTP server used for manual configuration when DHCP is not enabled or DHCP does not return NTP server (DHCP option 42).
- **TFTP Server**: This parameter specifies the source of the TFTP Server Address. Select Obtain from DHCP to automatically receive the address from the DHCP server; the DHCP option must be selected to use this option. To specify a fixed TFTP address, select the second radio button and enter an IP address in the data entry box.
- **STUN Server**: This parameter specifies the IP address of the STUN server. This parameter is not available on the ZIP 2x2L, ZIP 2+, and ZIP 2P.
- **STUN Port**: This parameter specifies the port number of the STUN server. Valid settings range from 1025 to 65535. This parameter is not available on the ZIP 2x2L, ZIP 2+, and ZIP 2P.
- **DSCP**: This parameter is the Layer 3 QoS setting. This value is placed in the ToS byte of the IP header of all voice packets sent from the phone’s microprocessor if VLANs are enabled.

25.2.5 SIP Tab



SIP Registration and Subscription

Registration Expires: 1 hour
Subscription Expires: 1 hour
Proxy Source: External Address
Proxy Address: 192.168.15.150
Proxy Port: 5060
☐ Register with backup proxy
Backup Proxy:
Backup Proxy Port: 5060
Backup Registration Expires: 1 hour
Registrar Source: External Address
Registrar Address: 192.168.15.150
Registrar Port: 5060
RTP Starting Port: 20000
Invite Retransmissions: 6
Non-invite Retransmissions: 10
☑ Accept INVITE with URL not matching IP address of phone
☐ Allow paging to interrupt active calls
☐ Use DNS Srv

✓ No errors remain in the profile list

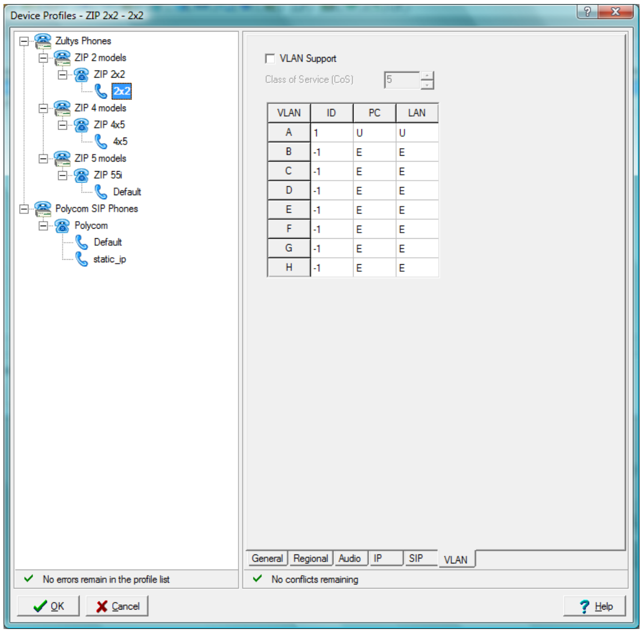
✓ No conflicts remaining

- **Registration Expires**: This parameter specifies the time period, in seconds, after which a REGISTRATION expires.
- **Subscription Expires**: This parameter specifies the time period, in seconds, after which a SUBSCRIPTION expires.
- **Proxy Source**: This parameter specifies the source for the Proxy Address.
  - **External Address**: Proxy address set to IP Address (main) in IP Address panel of System Settings window.
  - **Specified**: Proxy address is entered in data entry box.
  - **Domain**: Proxy address set to Default Domain in Company panel of System Settings window.
- **Proxy Address**: This parameter specifies the IP address of the SIP proxy server that will be used by the phone.
- **Proxy Port**: This parameter is the port of the SIP proxy that is used by the phone. Valid settings range from 1025 to 65535. Default value is 5060.
- **Register with Backup Proxy**: When this checkbox is selected, the phone registers with backup proxy at startup.

- **Backup Proxy**: This parameter is the backup SIP server proxy address value. If primary proxy server fails to operate, the phone attempts to switch to the backup proxy.
- **Backup Proxy Port**: This parameter is the backup SIP server proxy port value. Valid settings range from 1025 to 65535.
- **Backup Registration Expires**: This parameter specifies the time period, in seconds, after which a REGISTRATION with the backup proxy server expires.
- **Registrar Source**: This parameter specifies the source for the Registrar Address.
  - External Address: Registrar address set to IP Address (main) in IP Address panel of System Settings window.
  - Specified: Registrar address is entered in data entry box.
  - Domain: Registrar address set to Default Domain in Company panel of System Settings window.
- **Registrar Address**: This parameter is the SIP registrar server address. When this value is set, phone attempts to register with this server instead of proxy.
- **Registrar Port**: This parameter is the SIP Registrar server port.
- **RTP Starting Port**: This parameter specifies the starting port number for RTP/RTCP transmissions. Valid settings range from 1026 to 64528. The starting port must always be an even number and should not be set to same value as phone SIP port or the proxy port.
- **Invite Retransmissions**: This parameter specifies the number of unsuccessful INVITE retransmissions before phone switches to backup proxy. Valid settings range from 1 to 6.
- **Non-invite Retransmissions**: This parameter specifies the number of unsuccessful retransmissions (other than INVITE) before the phone switches to backup proxy. Valid settings range from 1 to 10.

- **Accept INVITE with URL not matching IP Address**: This parameter instructs the phone to accept INVITE requests that specify a destination other than that of the phone.
- **Allow Paging to Interrupt Active Calls**: This parameter instructs the phone to play an incoming page message even during an active call.
- **Use DNS Srv**: This parameter configures the phone to resolve the SIP Proxy IP address through DNS SRV records.

25.2.6 VLAN Tab



☐ VLAN Support

Class of Service (CoS) 5

VLAN	ID	PC	LAN
A	1	U	U
B	-1	E	E
C	-1	E	E
D	-1	E	E
E	-1	E	E
F	-1	E	E
G	-1	E	E
H	-1	E	E

✓ No errors remain in the profile list

✓ No conflicts remaining

- **VLAN Support**: Selecting this checkbox enables VLAN support within the ZIP2x2.
- **Class of Service (CoS)**: This parameter configures the Class of Service (CoS) at layer 2 for the phone port. Valid if phone port is defined as a tagged member of VLAN A. Values range from 0 to 7.
- **VLAN Table**: This table specifies the VLAN ID and inclusion status of the two phone circuits (one circuit in the ZIP 2x1, ZIP 2P, and ZIP w+) for VLAN A through VLAN H.
- **VLAN ID column**: Enter the VLAN ID for the specified VLAN in this data entry box.

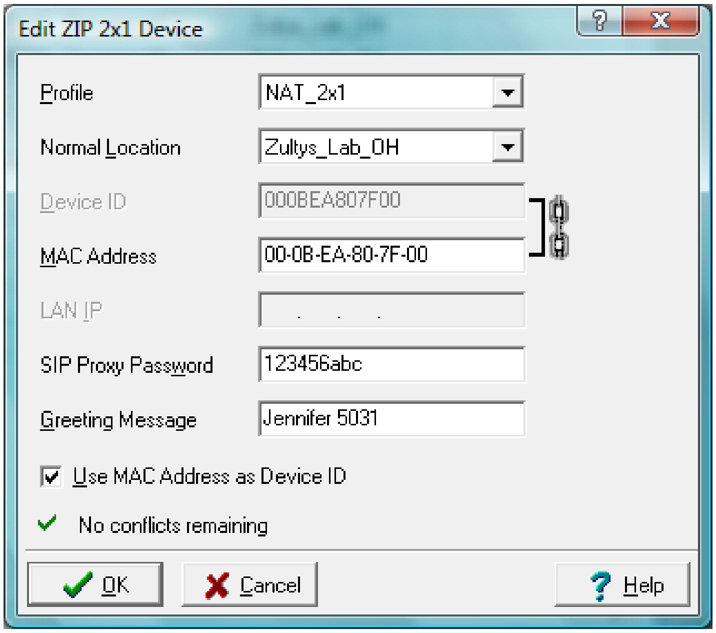
- **VLAN Tagging columns**: Enter the inclusion status of the specified circuit for the VLAN in this data entry box.

25.2.7 NAT Specific Notes

When using the ZIP2xN phone as a NAT phone you are required to use a SIP Proxy Password, and this must be set up in the Profile and manually set in the phone as it is not part of the configuration file for security reasons.

25.2.7.1 Setting SIP Proxy Password in the MX-E

In the device manager, edit the device and enter in a SIP Proxy Password



Edit ZIP 2x1 Device

Profile: NAT_2x1

Normal Location: Zultys_Lab_OH

Device ID: 000BEA807F00

MAC Address: 00-0B-EA-80-7F-00

LAN IP: . . .

SIP Proxy Password: 123456abc

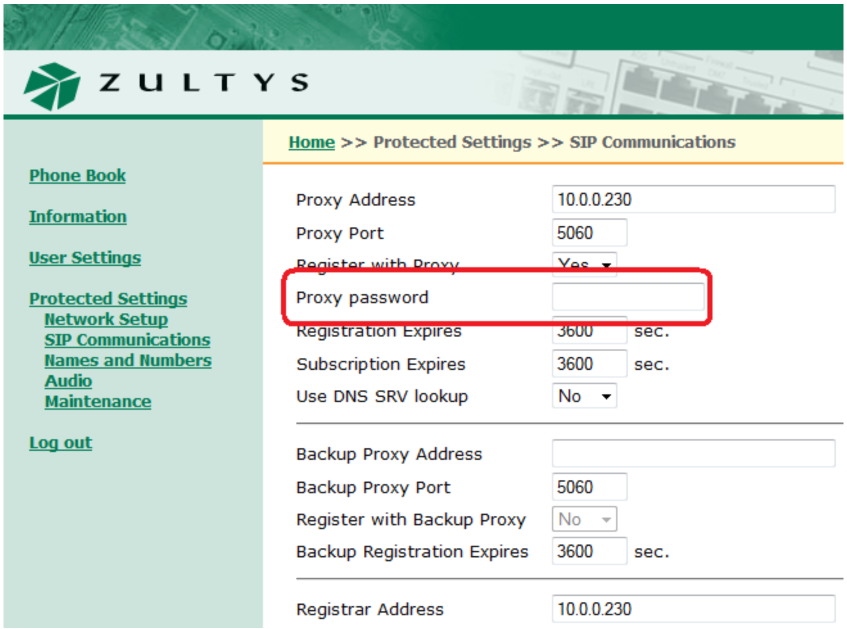
Greeting Message: Jennifer 5031

☑ Use MAC Address as Device ID

✓ No conflicts remaining

25.2.7.2 Setting the SIP Proxy Password in the ZIP2xN

From the web interface of the ZIP2xN, click on Protected Settings in the navigation menu then choose SIP Communications and enter the password in the Proxy Password Field. This will require a reboot of the ZIP2xN.



Home >> Protected Settings >> SIP Communications

Proxy Address	10.0.0.230	
Proxy Port	5060	
Register with Proxy	Yes	
Proxy password		
Registration Expires	3600	sec.
Subscription Expires	3600	sec.
Use DNS SRV lookup	No	
Backup Proxy Address		
Backup Proxy Port	5060	
Register with Backup Proxy	No	
Backup Registration Expires	3600	sec.
Registrar Address	10.0.0.230	

26. Adding Users

The process of adding users requires three steps: Adding the users, adding their devices, and matching the user with their phone (Assignment). Along the way, there are two methods of adding users: one at a time, or importing a list of users.

The process of adding users requires three steps:

- Adding the users and their profiles
- Adding their devices and their profiles
- Assignment (matching the user with their phone)
- Along the way, there are two methods of adding users:
  - one at a time
  - importing a list of users

26.2 Adding a user to the System:

User can be added to a system in two ways. You can add a user one at a time, or you can import them from a CSV file.

26.2.1 Creating Profiles:

There are four types of Profiles. User profiles are used to determine the privileges that the group of users assigned to the profile will have. Administrator Profiles, which are used to create various levels of Administrators that may or may not have access to various function. Paging Group Profiles which are used to map various paging zones (configured in the services window) to people that will receive the pages. And Recording Profiles which are used to configure the Call recording values of the group. After the profiles are created, users will be assigned to the various profiles.

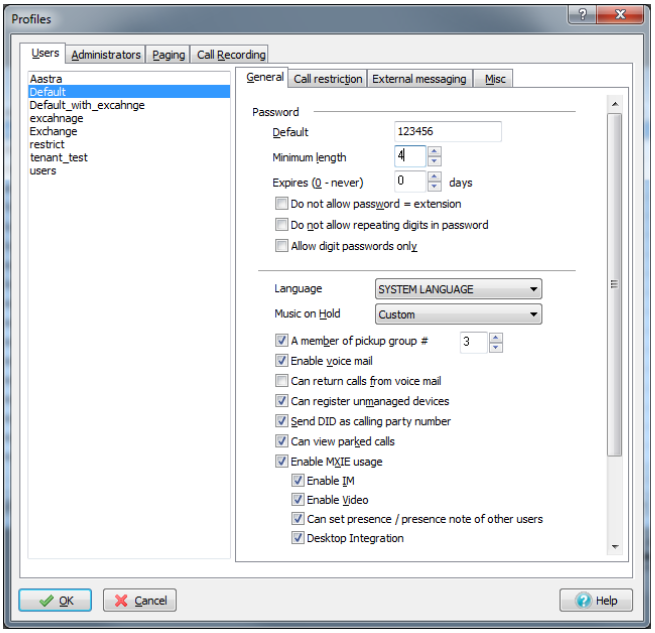
26.2.1.1 Modifying the Default Profile

The MX-E comes with one profile – this profile is called "Default".

- From the Configure → Users window, click on the Profile button on the bottom of the screen.
- Click on the Default Profile:

This allows you to review or modify the "default" settings.

***Note**: Enabling MXIE requires a MXIE license for each member of this Group. Several other options require licenses such as CRM Integration, Exchange Integration, Desktop Integration and others. You will be notified if you are missing or exceed the number of licenses.*



Aastra
Default
Default_with_excahnge
excahnage
Exchange
restrict
tenant_test
users

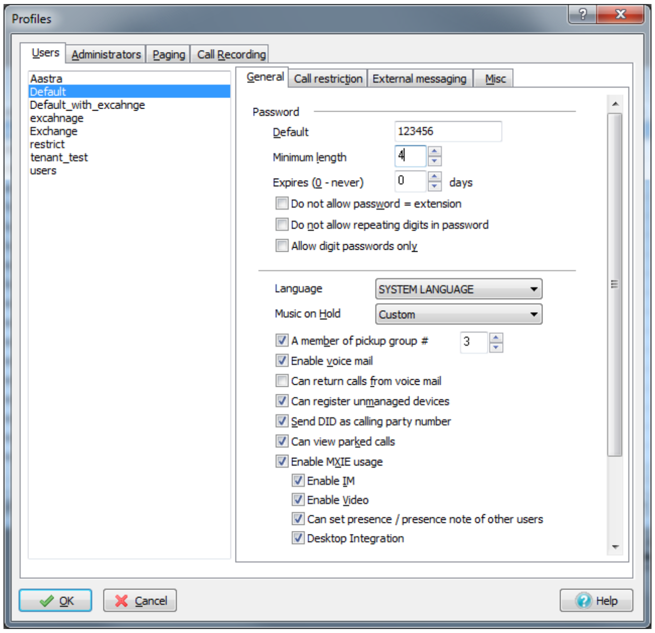
Password
Default 123456
Minimum length 4
Expires (0 - never) 0 days
□ Do not allow password = extension
□ Do not allow repeating digits in password
□ Allow digit passwords only

Language SYSTEM LANGUAGE
Music on Hold Custom
☑ A member of pickup group # 3
☑ Enable voice mail
□ Can return calls from voice mail
☑ Can register unmanaged devices
☑ Send DID as calling party number
☑ Can view parked calls
☑ Enable MXIE usage
☑ Enable IM
☑ Enable Video
☑ Can set presence / presence note of other users
☑ Desktop Integration

26.2.1.2 Creating a user profile

A User Profile is used to enable or disable various functions for users assigned to that group. Among the functions that are controlled by a profile are Password, Membership in a Pickup Group, Voicemail, On-Demand Call Recording, ability to register unmanaged devices, and if you want your DID number sent as your Calling Party Number.

- From the "Configure" → "Users" window click on the "Profiles" button
- Right click in the white box and select "New"
- Enter a Name for this new user profile
- Set the default password
- Set any options
- Then click "OK" and "Apply".



Aastra
Default
Default_with_excahnge
excahnage
Exchange
restrict
tenant_test
users

Password

Default 123456

Minimum length 4

Expires (0 - never) 0 days

□ Do not allow password = extension

□ Do not allow repeating digits in password

□ Allow digit passwords only

Language SYSTEM LANGUAGE

Music on Hold Custom

☑ A member of pickup group # 3

☑ Enable voice mail

□ Can return calls from voice mail

☑ Can register unmanaged devices

☑ Send DID as calling party number

☑ Can view parked calls

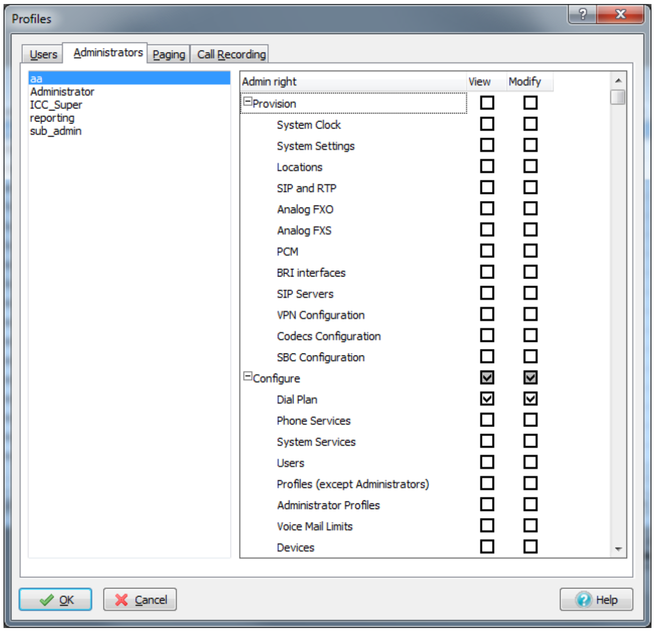
☑ Enable MXIE usage

- ☑ Enable IM
- ☑ Enable Video
- ☑ Can set presence / presence note of other users
- ☑ Desktop Integration

26.2.1.3 Creating an Administrator Profile

The MX-E allows you to create a wide range of Administrator Profiles. These profiles, once assigned to a user, will allow a user access to specific administrative functions while denying them access to other functions. An example of the function would be to create a profile for HR where they could add users, devices, assign users to devices, while denying them access critical system settings that may cause the system to restart.

1. From the “Configure” → “Users” window click on the “Profiles” button
2. Click on the Administrators Tab
3. Either right-click and select New or press the Insert key on the keyboard.
4. Create a new profile name
5. Assign properties to the newly created profile:
6. Click on OK



aa
Administrator
ICC_Super
reporting
sub_admin

Admin right	View	Modify
⊟Provision	□	□
System Clock	□	□
System Settings	□	□
Locations	□	□
SIP and RTP	□	□
Analog FXO	□	□
Analog FXS	□	□
PCM	□	□
BRI interfaces	□	□
SIP Servers	□	□
VPN Configuration	□	□
Codecs Configuration	□	□
SBC Configuration	□	□
⊟Configure	☑	☑
Dial Plan	☑	☑
Phone Services	□	□
System Services	□	□
Users	□	□
Profiles (except Administrators)	□	□
Administrator Profiles	□	□
Voice Mail Limits	□	□
Devices	□	□

26.2.1.4 Creating Paging Profiles

Paging profiles allow the user to send and receive pages sent to one or more paging zones. Before creating a paging profile a paging group must be created in Configure → Phone Services → Paging Groups.

From the “Configure” → “Users” window click on the “Profiles” button, Click on the Paging Tab. Either right-click and select New or press the Insert key on the keyboard.

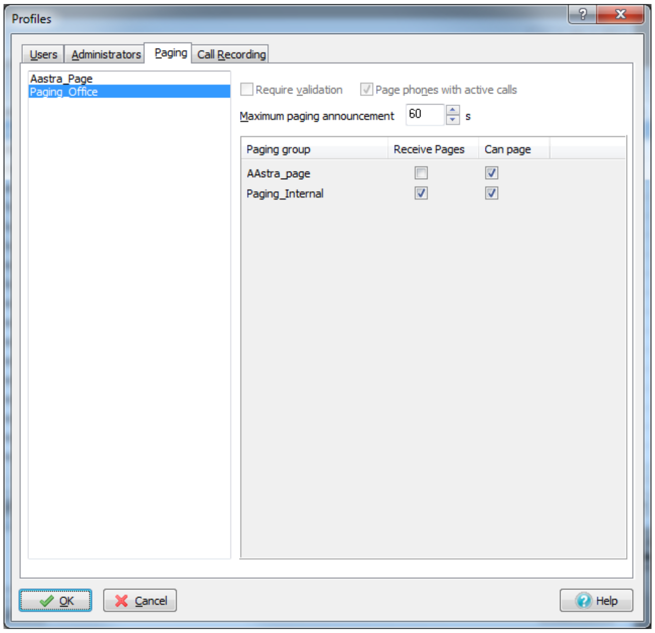
The parameters on the upper right side of the panel configure paging rights for the users that are assigned to this profile. Data entry boxes display parameter settings for the highlighted profile in the Profile List.

- Require Validation: When this parameter is enabled, the MX-E requires that users assigned to this profile enter their extension and password before being allowed to page. This feature is not supported at this time.
- Page phones with active calls: When enabled, pages initiated by users assigned to this profile are sent to all users in the paging group, including those that are on an active call. This feature is not supported at this time at a global level, but can be implemented at a device level.
- Maximum paging announcement: This parameter determines the duration of the longest page that can be sent by users assigned to this profile. Valid parameter settings range from 0 to 999 seconds; 10 seconds is the default value.

26.2.1.5 Paging Group Table

This table determines the paging group membership for users assigned to this active profile.

- Paging Group column lists each Paging Group defined in the Configure → Phone Services → Page Groups window.
- Member assigns paging group membership to the users to which this profile is applied. Each user can be assigned to more than one paging group.
- Can Page authorizes users assigned to this profile to page the selected paging groups. A user does not need to be a member of a paging group to have authorization to page the group.



Aastra_Page
Paging_Office

☐ Require validation ☑ Page phones with active calls

Maximum paging announcement 60 s

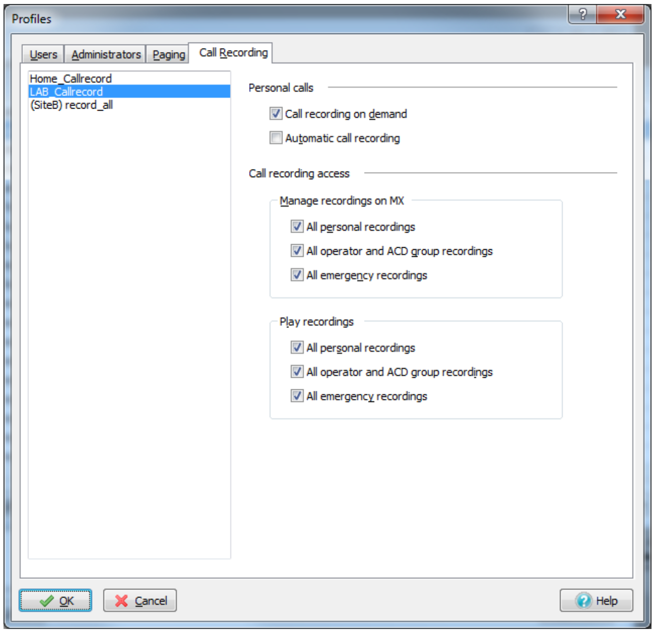
Paging group	Receive Pages	Can page
AAstra_page	☐	☑
Paging_Internal	☑	☑

26.2.1.6 Creating Call Recording Profiles

Call Recording profiles allow the user have their calls automatically recorded, or manually select which calls are recorded using the “record” button in MXIE during an active call. Call Recording Profiles also provide access restriction to the recorded calls.

- Creating an Call Recording Profile:
  - From the Profiles window, select the Call Recording Tab.
  - Right-Click and select new
  - Name the profile
  - Configure the Following Settings:
    - Personal Calls
      - Call Recording on demand: all calls will have the option to be recorded, if the user click the “record” icon in MXIE (Call Recording License is required)
      - Automatic call recording: all calls made from the user’s role will be recorded (Call Recording License is required)
    - Call Recording Access:

- Manage recordings: These options permit users assigned to this profile to remove phone recordings from the call recording database.
    - Personal: Select this option to manage calls involving system users within their user roles.
    - Group: Select this option to manage calls involving ACD groups, Operator groups, hunt groups, and Inbound Call centers.
    - Emergency: Select this option to manage all emergency calls.
- Play recordings: These options permit users assigned to this profile to listen to any phone recording in the call recording database.
    - Personal: Select this option for access to calls involving system users within their user roles.
    - Group: Select this option for access to calls involving ACD groups, Operator groups, hunt groups, and Inbound Call centers.
    - Emergency: Select this option for access to emergency calls.



Personal calls

☑ Call recording on demand

☐ Automatic call recording

Call recording access

Manage recordings on MX

☑ All personal recordings

☑ All operator and ACD group recordings

☑ All emergency recordings

Play recordings

☑ All personal recordings

☑ All operator and ACD group recordings

☑ All emergency recordings

26.2.2 Adding a Single User

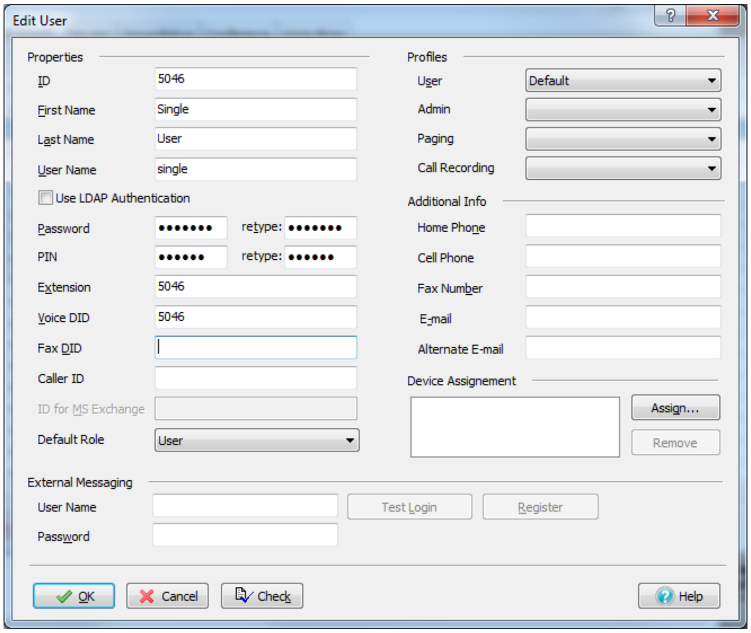
- In the MX-E Administrator click on "Configure" and select "Users".
- When the "Users" window opens right click in it and select "New User" or press the Insert key
- For "ID" use a unique identifier (name or extension number is recommended)
- For "User Name" Your First Name and Last Name using any format example: **First_Name.Last_Name**
- "First Name" is the users First name
- "Last Name" is the users Last name
- Use LDAP Authentication: Enables this user to use only LDAP authentication, that is the MX-E will not be used for login authentication, but an external LDAP server
- Password: password used when logging into MXIE, MX-E Administrator or other CSTA applications (E.G. Zultys Mobile, SalesForce, Outlook Communicator)
- Pin: Numeric only password word when logging into Voicemail from a phone, or Call Group login via a button.
- Extension is the extension number assigned to this user
- Voice DID: is the DID assigned to this user
- Fax DID: is the fax DID assigned to this user

  ***Note**: there is a relationship between seeing the DID fields on this screen and the settings found on the "Outside" tab of the Dial Plan.*
- ID for MS Exchange: this is the ID assigned by the exchange administrator for that user

  Note – this cannot have an @ symbol for MSEC V 1. Version 2.2x of MSEC supports the @ symbol
- Caller ID: is the Caller ID this user will present to the PSTN when making a call
- Home Phone: OPTIONAL, Enter a 7 to 10 digit home phone
- Cell Phone – OPTIONAL, Enter a cell phone number
- Fax Number – OPTIONAL, Enter A fax number
- Email – OPTIONAL, enter an email address
- Alternate Email – OPTIONAL, Enter a backup email address

- Under “Profiles” Select a User Profile to be assigned to this user
- Under Admin: Select an Administrator Profile to be assigned to this user
- Under Paging: Select a Paging Profile to be assigned to this user
- Under Call Recording Select a Call Recording Profile to be assigned to this user
- Device assignment window also allows you to assign a device to this user directly from the user screen.
- Click on the “OK” and “Apply” buttons to commit these changes – See **Error! Reference source not found.**

**Note: Voice Mail is automatically set up by the “User Profile” field*



Edit User

Properties

ID 5046
First Name Single
Last Name User
User Name single
☐ Use LDAP Authentication
Password ••••••• retype: •••••••
PIN •••••• retype: ••••••
Extension 5046
Voice DID 5046
Fax DID
Caller ID
ID for MS Exchange
Default Role User

Profiles

User Default
Admin
Paging
Call Recording

Additional Info

Home Phone
Cell Phone
Fax Number
E-mail
Alternate E-mail

Device Assignement

External Messaging

User Name
Password

26.3 Importing a Group of Users from a CSV file:

Importing a list of users allows you to bring all of the users in a company into the system in a single step. It offers a fast alternative to adding a user one at a time. There are three steps that involved in importing a list of users. First, you must create the list, second, you must map the fields from the list into the MX-E Database, and finally you must import the users.

26.3.1 Import Users

The Import Directory window is the tool for copying data file records into user accounts. Each imported data record either creates a new user account or updates an existing account in the User List. After the import operation is complete, you can save the results by pressing the Apply button in the User List. See Importing User Data for the step by step import procedure.

The Import Directory window is accessed by pressing the Import button from the Users window.

Import From

- Data Type: Specifies the input file type. Only CSV files are supported at this time.
- File Type: Selects the source file for the imported data records. Either type the file name (including path) in the edit box or click the Browse icon (right of the edit box) to select a file from your directory.

Data Sample

This table displays a sample of the data from the import file; it allows you to verify that the file information is consistent and compatible with User List records. Fields within the table are not editable.

The top line (gray) lists the field names for the data records. The next two lines list the first two data records from the import file.

MX-E User Properties

This table defines the mapping between user account property fields and data record fields. This table comprises two columns:

- Property: each cell in this column corresponds to a User List property, as defined in the Columns (Users) window. See User Account Structure.
- Source: each cell specifies the data file field that will be mapped to the MX-E user property. You can type data directly into these cells (such as a default password) or drag and drop fields from the Source Fields table.

Source Fields

This table lists the import file data fields. These names are also listed in the grey bar of the Data Sample table.

To map an import field to an MX-E user property:

1. Move the mouse cursor to the desired field.
2. Click and hold the left mouse button.
3. While holding the button, move the mouse cursor into the cell that is adjacent to the desired property. The cursor should appear as an arrow originating from a page that points to the cell.
4. Release the left button to display the source field in the cell.

Button Bar

Close button exits the Import Directory window and returns to the Users window. Imported data will appear in the User List but will not be saved to the database until you press the Apply button in the Users window..

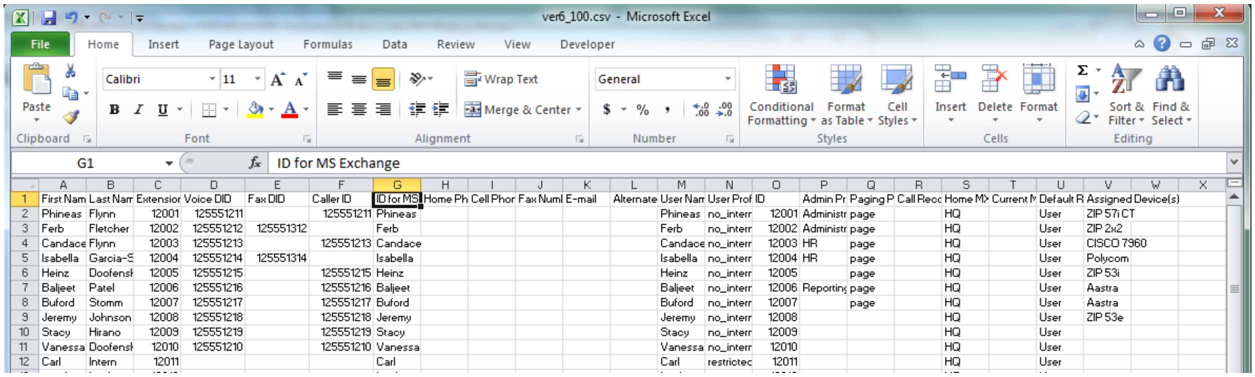
Load Map button imports a Property-to-Source map from a file that was previously saved with the Save Map button. Pressing Load Map accesses an MS file open dialog window, from where you specify the name and location of the map file. See Map Files.

Save Map button stores the Property-to-Source map defined in the User Properties table into a data file. Pressing this button opens a MS file open dialog window, from where you can specify the storage location of the new map file.

Import Data button initiates the import operation defined in the window.

26.3.2 Creating a List:

In Excel create a list with the following information:



G1 ID for MS Exchange

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	First Nam	Last Nam	Extensior	Voice DID	Fax DID	Caller ID	ID for MS	Home Ph	Cell Phor	Fax Numl	E-mail	Alternate	User Nam	User Prof	ID	Admin Pr	Paging P	Call Recc	Home M>	Current M	Default R	Assigned Device(s)
2	Phineas	Flynn	12001	125551211		125551211	Phineas						Phineas	no_interr	12001	Administr	page		HQ		User	ZIP 57i CT
3	Ferb	Fletcher	12002	125551212	125551312		Ferb						Ferb	no_interr	12002	Administr	page		HQ		User	ZIP 2x2
4	Candace	Flynn	12003	125551213		125551213	Candace						Candace	no_interr	12003	HR	page		HQ		User	CISCO 7960
5	Isabella	Garcia-S	12004	125551214	125551314		Isabella						Isabella	no_interr	12004	HR	page		HQ		User	Polycom
6	Heinz	Doofensł	12005	125551215		125551215	Heinz						Heinz	no_interr	12005		page		HQ		User	ZIP 53i
7	Baljeet	Patel	12006	125551216		125551216	Baljeet						Baljeet	no_interr	12006	Reportinç	page		HQ		User	Aastra
8	Buford	Stomm	12007	125551217		125551217	Buford						Buford	no_interr	12007		page		HQ		User	Aastra
9	Jeremy	Johnson	12008	125551218		125551218	Jeremy						Jeremy	no_interr	12008				HQ		User	ZIP 53e
10	Stacy	Hirano	12009	125551219		125551219	Stacy						Stacy	no_interr	12009				HQ		User	
11	Vanessa	Doofensł	12010	125551210		125551210	Vanessa						Vanessa	no_interr	12010				HQ		User	
12	Carl	Intern	12011				Carl						Carl	restrictec	12011				HQ		User	

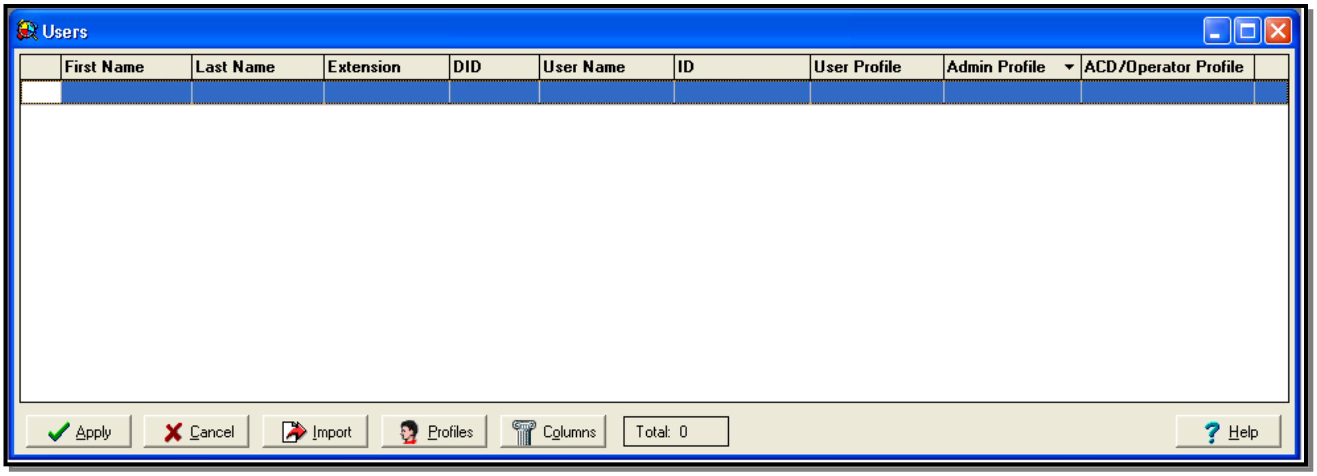
If you do not have Excel, create a file using a text editor. Separate each value with a comma. Save the file with a “CSV” Suffix.

Other values can also be added to the CSV file. These include User Profile, Admin Profile, . . .

If the User, Administrator, Call Recording or Paging Profile do not exist, you will be prompted to allow the MX-E to automatically create these profiles and assign to the user, or to simply use the default profile.

26.3.3 Importing a List of Users:

1. From Configure menu select Users
2. The Users window appears.



First Name	Last Name	Extension	DID	User Name	ID	User Profile	Admin Profile	ACD/Operator Profile

Total: 0

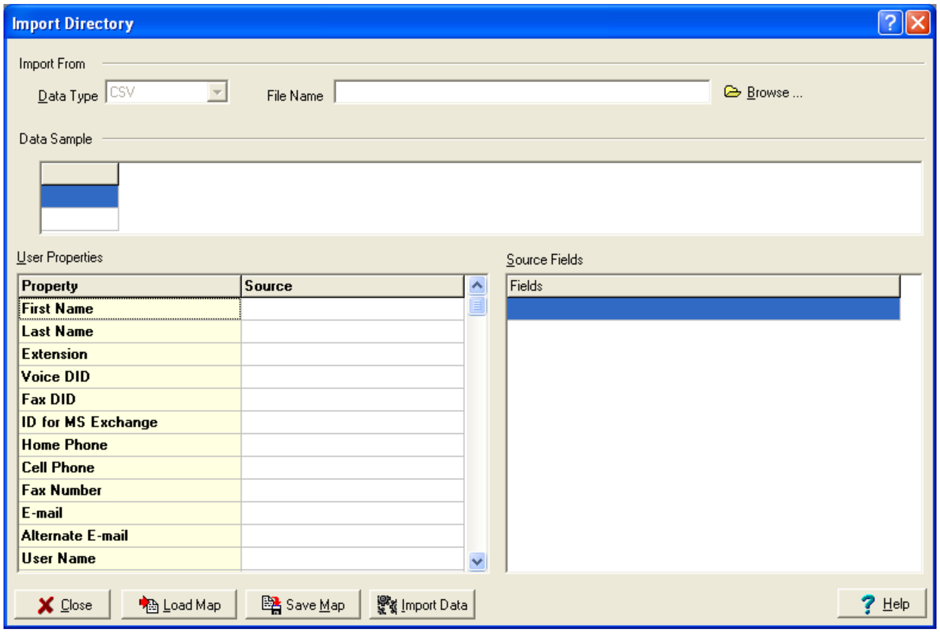
3. Blank user list indicates that no users are provisioned in the database
4. Click on the “Import” button

Importing records from a data file is a fast, efficient, and accurate method of creating and modifying user accounts. The Import Directory window contains all necessary resources to import a data file to the User List.

The following procedure for importing data records into a user account describes the steps required to create new user accounts and to modify existing accounts.

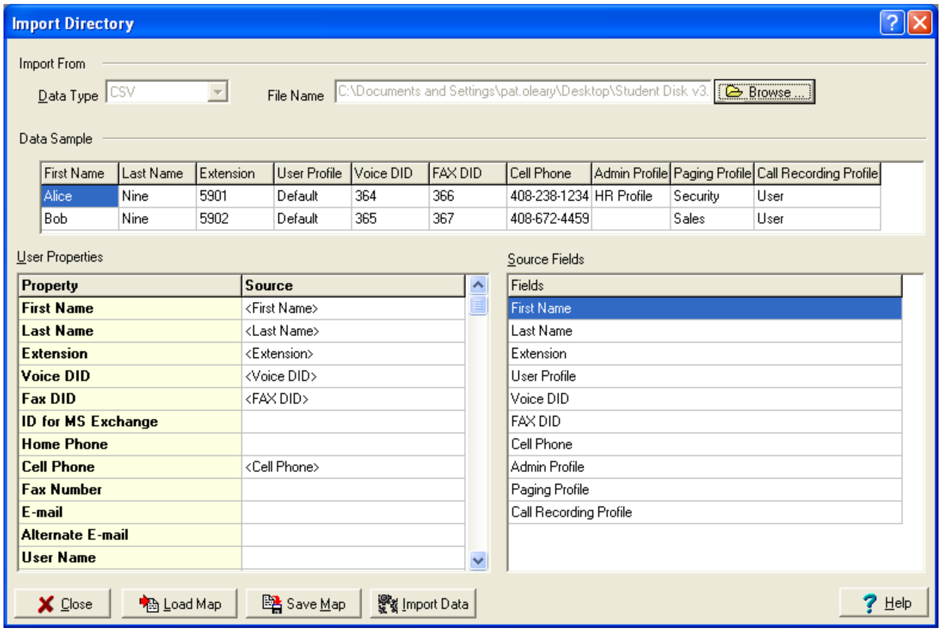
Import Procedure

1. Open the Import Directory Window, by pressing the Import button in the Users window.



Property	Source
First Name	
Last Name	
Extension	
Voice DID	
Fax DID	
ID for MS Exchange	
Home Phone	
Cell Phone	
Fax Number	
E-mail	
Alternate E-mail	
User Name	

2. Select the data file type. The MX-E only supports the import of CSV files at this time.
3. Select the data file. Enter the path and file name of the import file in the data entry box or press the Browse icon to select a file from your system directory.
4. Verify the file structure of the data file, as displayed in the Data Sample table. Table contents for the sample records should be consistent with the table headings.



Import Directory

Import From

Data Type: CSV

File Name: C:\Documents and Settings\pat.oleary\Desktop\Student Disk v3.

Data Sample

First Name	Last Name	Extension	User Profile	Voice DID	FAX DID	Cell Phone	Admin Profile	Paging Profile	Call Recording Profile
Alice	Nine	5901	Default	364	366	408-238-1234	HR Profile	Security	User
Bob	Nine	5902	Default	365	367	408-672-4459		Sales	User

User Properties

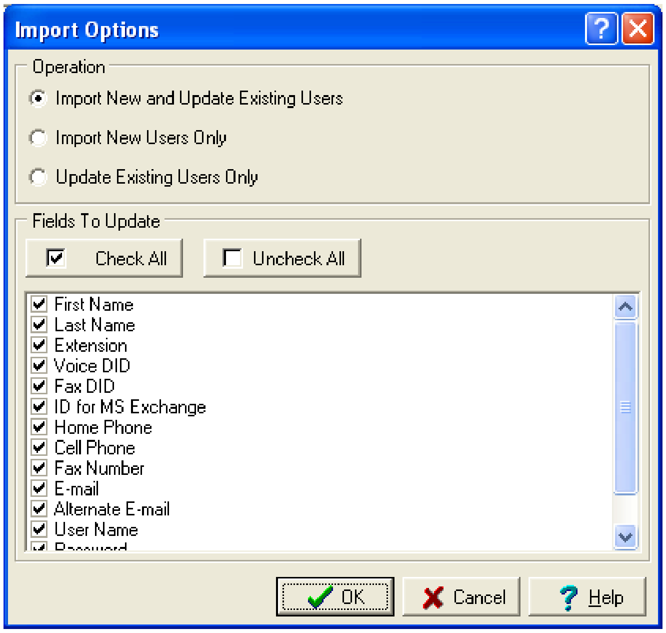
Property	Source
First Name	<First Name>
Last Name	<Last Name>
Extension	<Extension>
Voice DID	<Voice DID>
Fax DID	<FAX DID>
ID for MS Exchange	
Home Phone	
Cell Phone	<Cell Phone>
Fax Number	
E-mail	
Alternate E-mail	
User Name	

Source Fields

Fields
First Name
Last Name
Extension
User Profile
Voice DID
FAX DID
Cell Phone
Admin Profile
Paging Profile
Call Recording Profile

5. Define Account Property fields. The source column of the MX-E User Properties table defines the mapping of data file field into user accounts after the import operation is complete. There are four options for entering data into the Source column:
    a. Drag and drop fields from the Source Fields table into the desired source column cells in the Users Properties table. You can enter multiple field names into any individual source field.
    b. Enter data directly into source column cells. This method is useful for entering the same password into all user accounts. Source file fields entered in this fashion should be surrounded by brackets, such as <Last Name>.
    c. Enter data and source file fields into the MX-E User Properties table. This method is useful when creating a user name from a user's first and last name separated by a period.
    d. Press the Load Map button to access a data file that automatically fills the source fields with preconfigured field names. This option is available if you have previously used the Save Map key to store a Property field to Source field map. The Load Map option is valuable if you periodically import an updated version of the same file. See Map Files for instructions on creating a map file.

6. Press Import Data button to open the Import options window. If the Source column for the User ID field is blank, the UI will not process the request. Otherwise the UI opens the Import Options window.
7. Choose the Desired Operation (Import Options window) from among the following options:
    a. import new users
    b. update existing users
    c. import new users and update existing users
        i. The MX-E interprets a data record as a new user account if it fills the ID field with an entry that is not duplicated by the ID field of an existing user account. If the import operation is set to only process new user accounts, all data records that would only update existing accounts are disregarded.
8. Choose update fields (Import Options window) by placing tick marks in the desired checkboxes. This option is valid only if the import operation is updating existing users.



Import Options

Operation

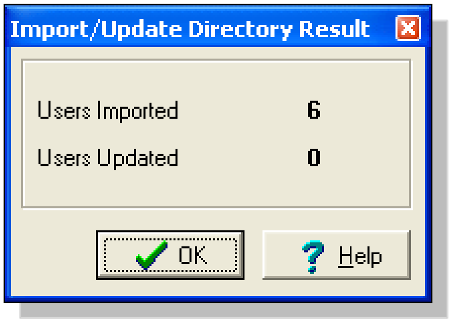
● Import New and Update Existing Users
○ Import New Users Only
○ Update Existing Users Only

Fields To Update

☑ First Name
☑ Last Name
☑ Extension
☑ Voice DID
☑ Fax DID
☑ ID for MS Exchange
☑ Home Phone
☑ Cell Phone
☑ Fax Number
☑ E-mail
☑ Alternate E-mail
☑ User Name
☑ Password

9. Press OK button to close Import Options window and initiate the import operation.
    a. Observe import results from Import / Update Directory Results. Close dialog box.

10. Press the Close button to exit the Import Directory window.
11. Resolve Conflicts in User List. If the Apply button is inactive (all gray), the User List contain user accounts that either have errors or have conflicts with other accounts. Edit each user account that displays the error icon in the extreme left column.
12. If the import operation was successful, Press Apply (User List) to save results. If the import operation improperly edited existing accounts or created excessive account errors, Press Cancel to restore the User List to its pre-import state.

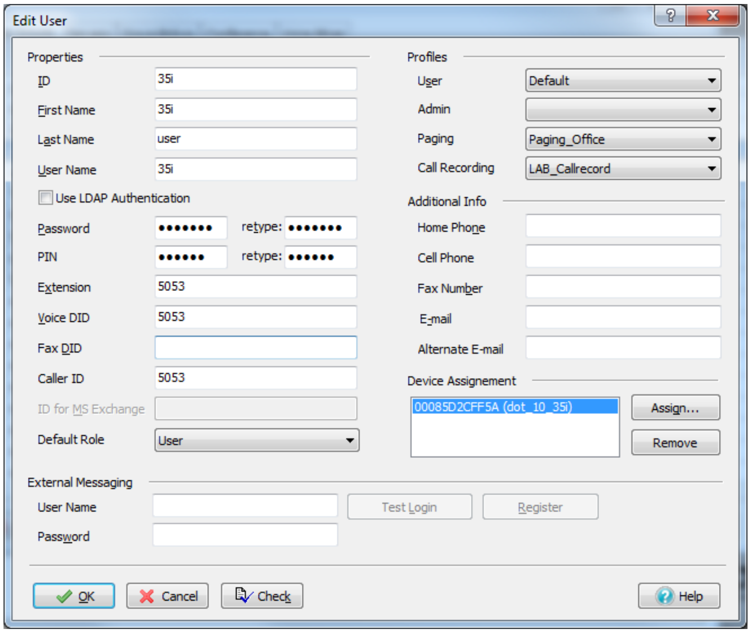

Import/Update Directory Result

Users Imported	6
Users Updated	0

26.3.4 Changing a User's information or profile:

You may change a single user's information by right clicking a user and choosing "Edit User" or select a number of users that need to be modified with the same information by selecting all the users you wish to modify, right click and choose "Edit Users" from the list of options.

1. Right click on the User(s) that you want to change
2. Change the information to match the needs of your users and click OK
3. Repeat this process for all users.



Edit User

Properties

ID	35i
First Name	35i
Last Name	user
User Name	35i

□ Use LDAP Authentication

Password	•••••••	retype:	•••••••
PIN	••••••	retype:	••••••

Extension	5053
Voice DID	5053
Fax DID	
Caller ID	5053
ID for MS Exchange	
Default Role	User

Profiles

User	Default
Admin	
Paging	Paging_Office
Call Recording	LAB_Callrecord

Additional Info

Home Phone	
Cell Phone	
Fax Number	
E-mail	
Alternate E-mail	

Device Assignement

00085D2CFF5A (dot_10_35i)

External Messaging

User Name	
Password	

4. Apply your changes by clicking Apply

27. Assigning Users to Devices

Once you have configured users and devices, you now assign the devices to users. You can assign only managed devices. If you have chosen to not manage any devices, you do not need to access this window.

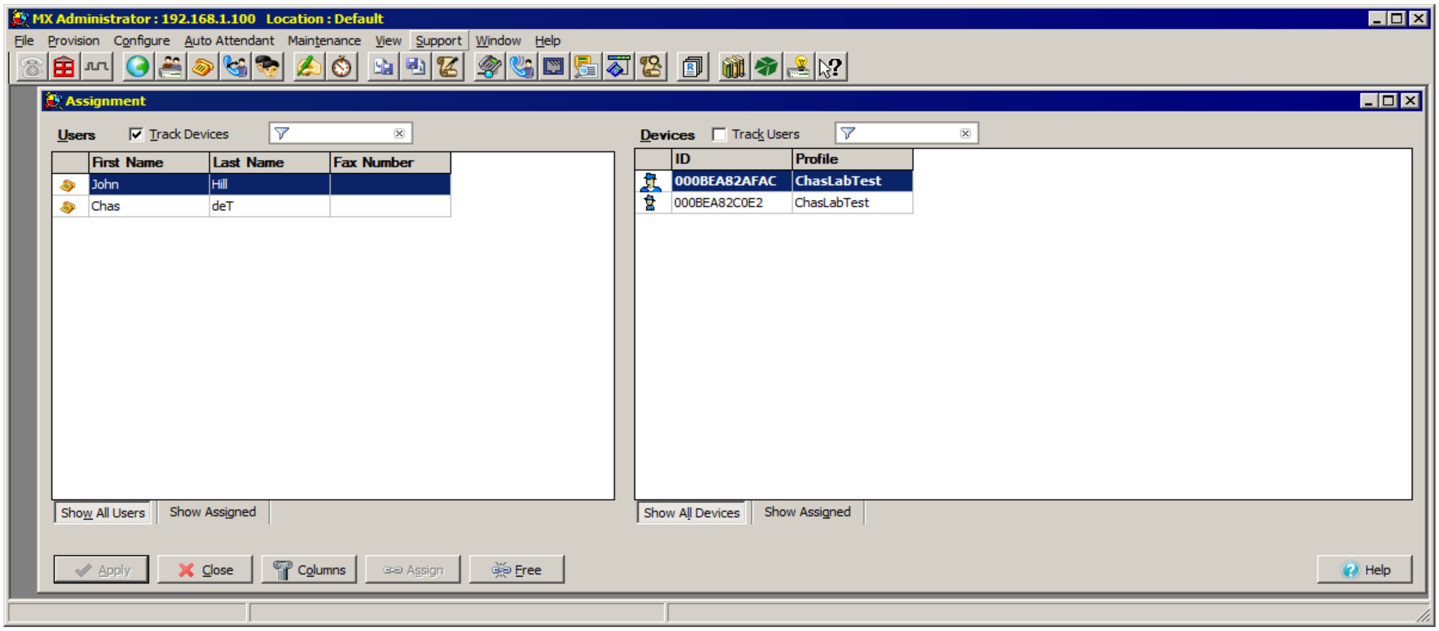
25.1 Assignment Window

The Assignment window configures and displays the relationship between Managed Devices and User Accounts. Specific tasks that you can perform from this window include:

- assigning managed devices to user accounts
- detecting assignments between managed device and user accounts
- displaying unassigned managed devices and user accounts

Each user account may be assigned to one or more managed device; conversely, each managed device may be assigned to multiple users.

You access the Assignment window by selecting Configure | Assignment from the main menu.



First Name	Last Name	Fax Number
John	Hill	
Chas	deT	

ID	Profile
000BEA82AFAC	ChasLabTest
000BEA82C0E2	ChasLabTest

25.2 Users Table

The Assignment window displays a User's Table on the left side of the window. You can select the parameters that the Users Table displays by pressing the ***Columns*** button. When the Users Table is in assignment detection mode, the top line in the table (listed in boldtype) displays the user that is assigned to the highlighted device in the Devices Table. Select the *Track Users* option located above the Devices Table to place the Users Table in assignment detection mode.

Assignment window features that are displayed in the Users table include:

- The ***Track Devices*** checkbox, located above the list of Users, places the Devices table in assignment detection mode. When in this mode, the name of each device assigned to the highlighted user is displayed at the top of the Devices table in bold text.

- The ***Assignment*** column is located on the left side of the table. Cells in this column display a phone icon for each user that is assigned to a managed device.
- The ***Filter*** buttons, located below the Users table, determine which users are displayed by the table.

  select **Show All Users** to display all users

  select **Show Assigned** to display those users that have one or more devices assigned to them

  select **Show Free** to display those users that have no devices assigned to them. This option is available only if the *Track Devices* and *Track User* checkboxes are not selected.

25.3 Devices Panel

The Assignment window displays a Devices table on the right side of the window. Devices table contents are configured in the Managed Devices Window.

You can select the parameters that the Devices Table displays by pressing the ***Columns*** button.

When the Devices Table is in assignment detection mode, the top line in the table (listed in boldtype) displays the device that is assigned to the highlighted user in the Users Table. Select the *Track Devices* option located above the Users Table to place the Devices Table in assignment detection mode.

Assignment window features that are displayed in the Devices table include:

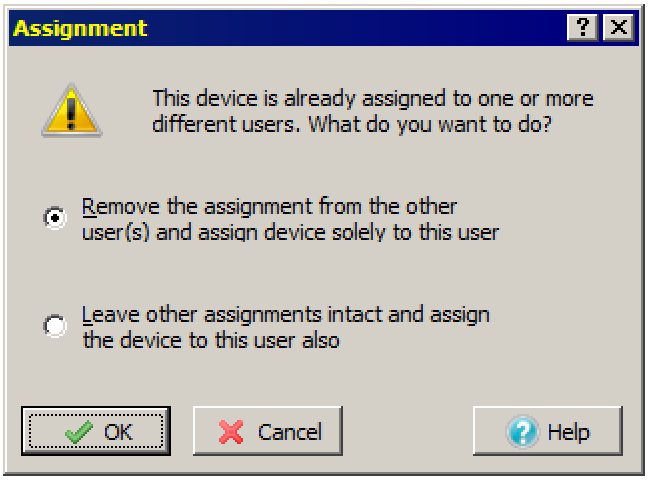
- The ***Track Users*** checkbox places the Users table in assignment detection mode. When in this mode, the name of each user to which the highlighted device is assigned is displayed at the top of the Users table in bold text.
- The ***Assignment*** column is on the left side of the table. Cells in this column display an agent icon for each device that is assigned to a user.
- The ***Filter*** buttons, located below the Devices table, determine which devices are displayed by the table.

  select **Show All Devices** to display all devices select **Show Assigned** to display those devices that are assigned to one or more users

select **Show Free** to display those devices that are not assigned to any users. This option is available only if the *Track Devices* and *Track User* checkboxes are not selected.

25.4 Assigning Devices to Users

To assign a device to a user, select a user and a device and click on **Assign**. Icons are displayed in the assignment columns of both tables to indicate the new assignment. You will normally link most devices with a single user. However, there are cases when you want to assign a device to multiple users. Therefore, if you select a device that is already assigned to a user, and click on **Assign**, the program opens the window to ask you if you want to:


Assignment

This device is already assigned to one or more different users. What do you want to do?

● Remove the assignment from the other user(s) and assign device solely to this user

○ Leave other assignments intact and assign the device to this user also

- add this user to the users already linked to this device
- remove the linkage from the other users and keep this user only linked to the device

Cancelling the assignment request maintains the device assignments in their current state.

25.5 Disconnecting a User from a Device

To remove an assignment between a user and a device, select the user and the device and click on Free. If the user has no other devices assigned to him or her, the program removes the icon from the assignment column of the Users Table. If the device is now not assigned to any user, the program shows agent icon from the assignment column of the Devices Table.

When you delete a user or a device, the MX-E removes the association between the user and the device.

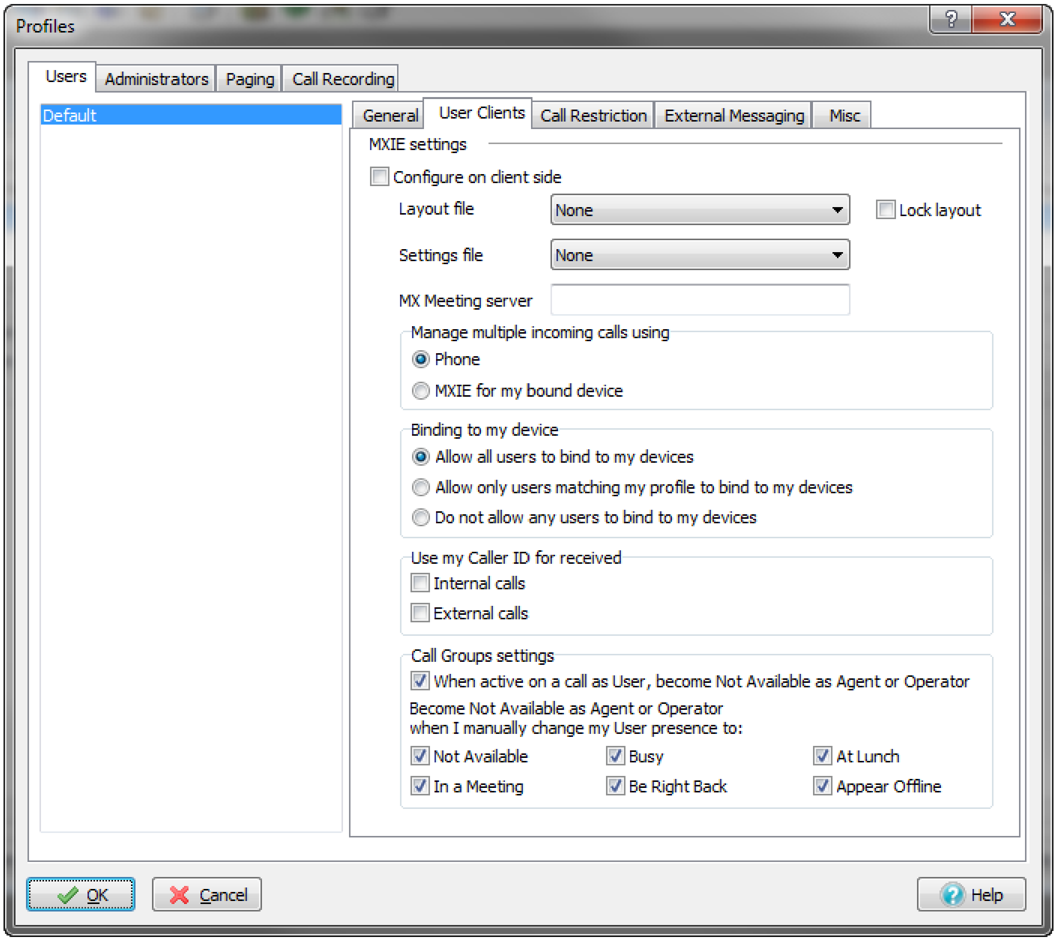
28. Centralized MXIE Settings

System administrators have the ability to push MXIE settings to all users on the MX-E system without the need to configure MXIE individually for each user.

MXIE settings are assigned per user profile.

In MX-E Administrator navigate to *Configure* -> *Users* and select the *Profiles* button.

In the *Profiles* window, select a profile to edit from the list in the left-hand column and open the *Client Settings* tab.



MXIE settings

□ Configure on client side

Layout file: None □ Lock layout

Settings file: None

MX Meeting server:

Manage multiple incoming calls using

● Phone

○ MXIE for my bound device

Binding to my device

● Allow all users to bind to my devices

○ Allow only users matching my profile to bind to my devices

○ Do not allow any users to bind to my devices

Use my Caller ID for received

□ Internal calls

□ External calls

Call Groups settings

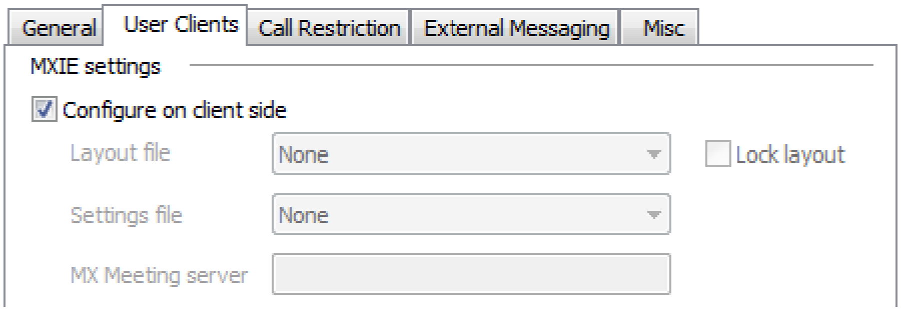
☑ When active on a call as User, become Not Available as Agent or Operator

Become Not Available as Agent or Operator
when I manually change my User presence to:

☑ Not Available ☑ Busy ☑ At Lunch

☑ In a Meeting ☑ Be Right Back ☑ Appear Offline

By default, the *Configure on Client Side* checkbox is enabled. This setting means that all MXIE configurations need to be done individually from user’s MXIE client.



MXIE settings

☑ Configure on client side

Layout file: None □ Lock layout

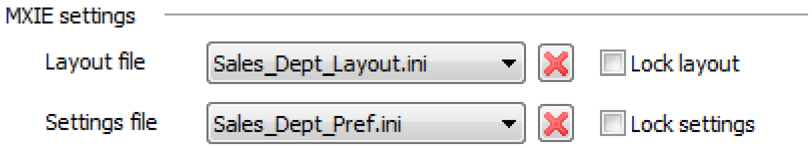
Settings file: None

MX Meeting server:

If the *Configure on Client Side* checkbox is disabled, all of the settings in this tab will be enforced for all users that are assigned to this profile.

Note that all settings in this tab, excluding the MXIE layout and setting file, apply to other clients besides MXIE, for example Zultys Outlook Communicator and Zultys Salesforce Communicator.

You may specify a MXIE layout configuration file or a general preference ‘Settings’ configuration file for all users with this profile. See Section 28.1. If either of these two fields is left blank, the Users will need to configure them individually from their MXIE client. Previously saved ini files may be deleted by clicking the red X.

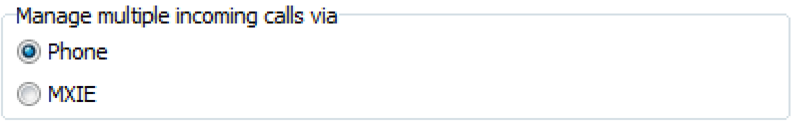


MXIE settings

Layout file: Sales_Dept_Layout.ini ☒ □ Lock layout

Settings file: Sales_Dept_Pref.ini ☒ □ Lock settings

Select whether to manage multiple incoming calls via the user’s bound phone or MXIE. The user will not be able to change this configuration from MXIE.

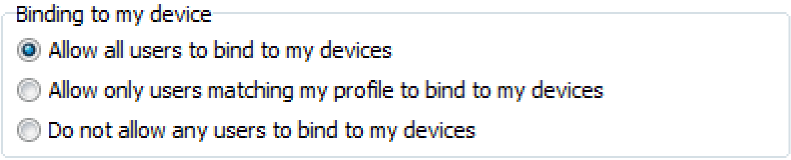


Manage multiple incoming calls via

● Phone

○ MXIE

Select whether other users can bind to a device that is assigned to a user with this User Profile. The user will not be able to change this configuration from MXIE.



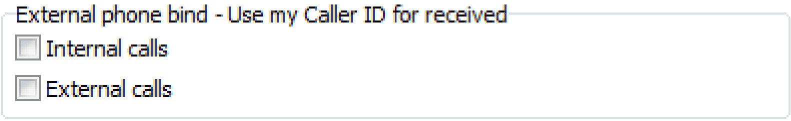
Binding to my device

● Allow all users to bind to my devices

○ Allow only users matching my profile to bind to my devices

○ Do not allow any users to bind to my devices

Select whether the user’s Caller ID is used when passing a received call to an external phone bound to MXIE. The user will not be able to change this configuration from MXIE.

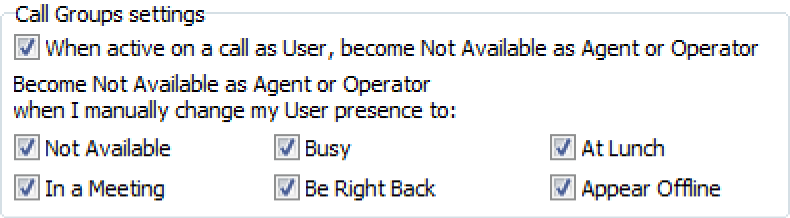


External phone bind - Use my Caller ID for received

□ Internal calls

□ External calls

For users that are members of Call Groups, you can choose how changes to their User presence affect their Agent Status.



Call Groups settings

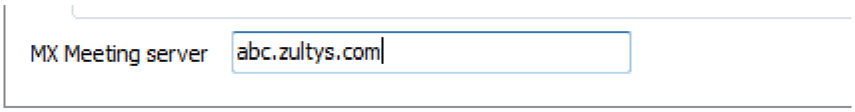
☑ When active on a call as User, become Not Available as Agent or Operator

Become Not Available as Agent or Operator
when I manually change my User presence to:

☑ Not Available ☑ Busy ☑ At Lunch
☑ In a Meeting ☑ Be Right Back ☑ Appear Offline

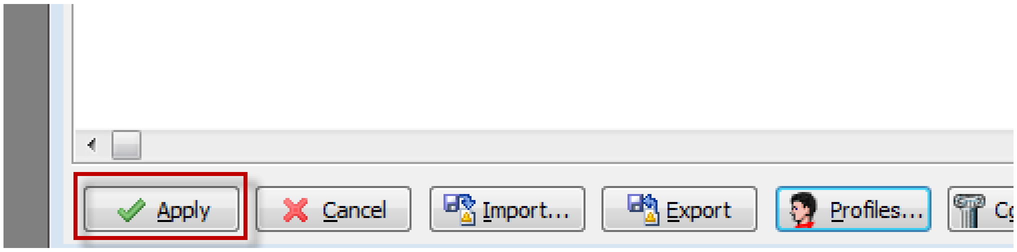
To choose how changes to Agent Status affect the User Presence and wrap up time, see Section 28.2.

Where an MXmeeting appliance is deployed, enter the address of the appliance under *MX-E Meeting server*. This setting is available regardless of whether *Configure on client side* option is enabled or disabled.



MX Meeting server: abc.zultys.com

Click *OK* to close the *Profile* window then click the *Apply* button in the *User* window to push the changes to all users.



Changes will take effect immediately. Users do not need to restart MXIE.

28.1 Exporting MXIE Layout and Preferences

The MXIE Screen Layout and Preference Settings may be defined centrally on per User Profile basis. This is achieved by exporting the Layout and/or Preference Settings from a suitably configured MXIE instance running in Admin Mode and then selecting the relevant ini file from within the *User Profile* in MX-E Administrator.

28.1.1 MXIE Admin Mode

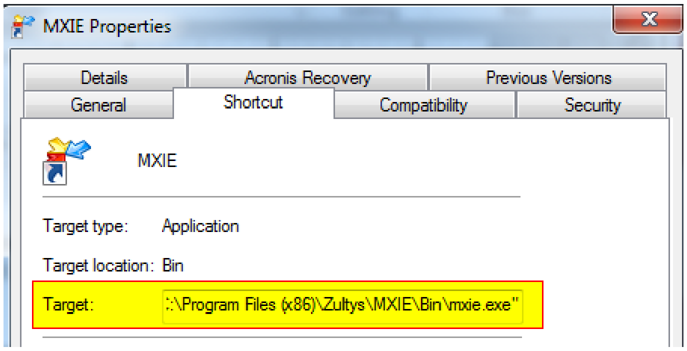
To create a configuration file, MXIE must be launched in Admin Mode.

28.1.1.1 Opening MXIE Admin Mode on Microsoft Windows

1. Select *Start* -> *All Programs* -> *Zultys MX-E*, then right-click on *MXIE* and select *Copy*.

2. Paste the copied shortcut to a desired location and rename it, for example: “MXIE – Admin”.

3. Right-click the new shortcut and select *Properties*, select the Shortcut tab.



Target type: Application

Target location: Bin

Target: :\Program Files (x86)\Zultys\MXIE\Bin\mxie.exe"

4. Type the *admin* command line parameter at the end of the target field.

```
"C:\Program Files\Zultys\MXIE\Bin\MXIE.exe" admin
```

5. Click *OK* to save changes and launch the shortcut.

28.1.1.2 Opening MXIE Admin Mode on Apple Mac OSX

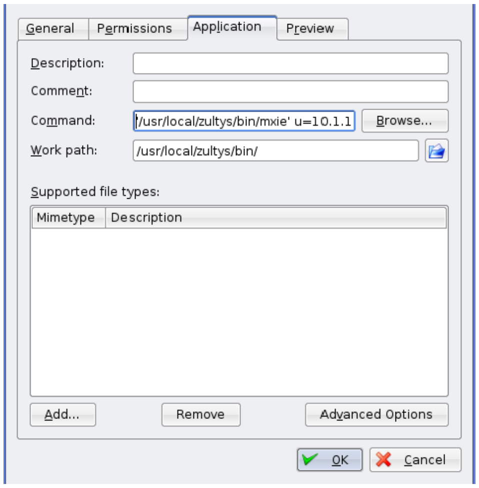
1. Enter the desired parameters from the OSX command line. To launch MXIE from a terminal application, open the terminal, and enter in the following

```
$ cd /Applications/Zultys/MXIE.app/Contents/MacOS

$ ./MXie admin
```

28.1.1.3 Opening MXIE Admin Mode on Linux

1. Select *Start Menu* -> *K Menu* -> *Copy* -> *Add to Desktop*.

2. Right-click and select *Link* -> *Properties*. A screen similar to the screenshot below will appear.



Command: '/usr/local/zultys/bin/mxie' u=10.1.1

Work path: /usr/local/zultys/bin/

3. Enter the following in the Command field:

```
'/usr/local/zultys/bin/MXie' admin
```

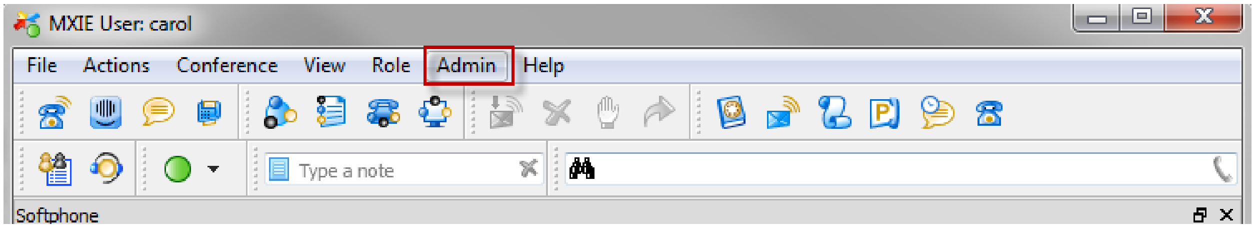
4. Click *OK* to save changes and launch the shortcut.

28.1.1.4 Exporting Layout or Preference Settings File

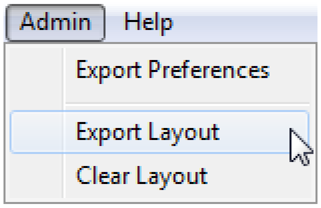
Launch MXIE using the Admin Mode shortcut created above.

1. Type the credentials for the user under which you wish to export settings and login.

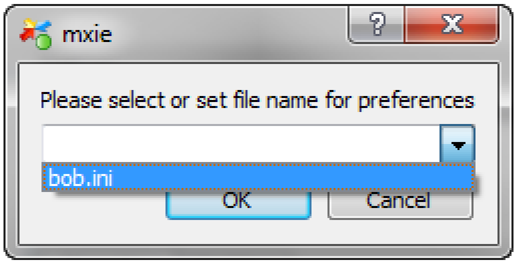
2. MXIE opens. The Admin option will be available.



3. Customize the User Preferences and MXIE layout for this user as necessary.
4. When finished, open the Admin menu option and select *Export Layout* or *Export Preferences*.



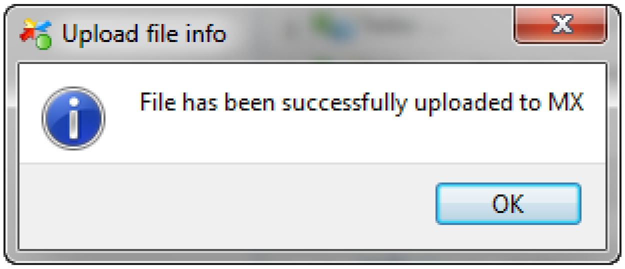
5. Type a name for a new file or select an existing file to overwrite then click *OK*.



Please select or set file name for preferences

bob.ini

6. A popup will notify you that a new file was successfully saved on the MX-E.

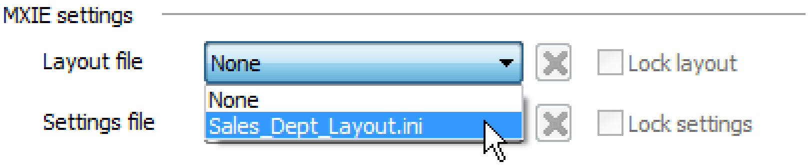


File has been successfully uploaded to MX

28.1.1.5 Configuring Centralized MXIE layout

After you have created a configuration file for MXIE layout in Admin Mode of MXIE, you can use this file to duplicate the same layout for all users with a specific profile.

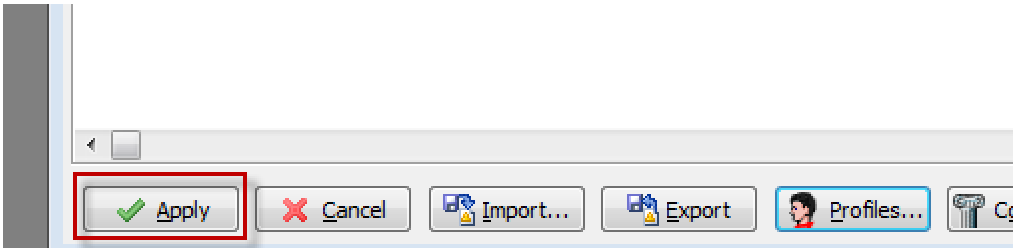
In the *Client Settings* tab of the User Profile, select a Layout File from the drop-down list.



Layout file: None
Settings file:
□ Lock layout
□ Lock settings

You can enable the *Lock Layout* checkbox to prevent users from customizing their MXIE screen layout.

Click *OK* to close the *Profile* window then click the *Apply* button in the *User* window to push the changes to all users.

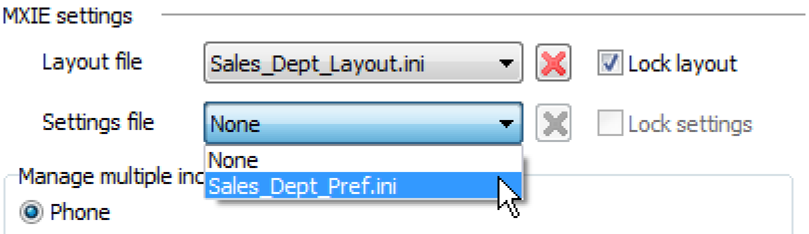


Changes will take effect immediately. Users do not need to restart MXIE.

26.1.1.6 Configuring Centralized MXIE Preferences

After you have created a configuration file for MXIE Preferences in Admin Mode of MXIE, you can use this file to duplicate the same preferences for all users with a specific profile.

In the *User Clients* tab of the User Profile, select a Setting file from the drop-down list.

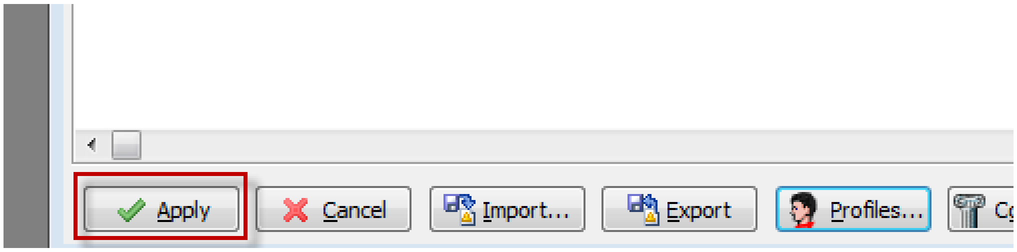

MXIE settings

Layout file: Sales_Dept_Layout.ini ☑ Lock layout

Settings file: None □ Lock settings

You can enable the *Lock Settings* checkbox to prevent users from customizing their MXIE preferences.

Click *OK* to close the *Profile* window then click the *Apply* button in the *User* window to push the changes to all users.



Changes will take effect immediately. Users do not need to restart MXIE.

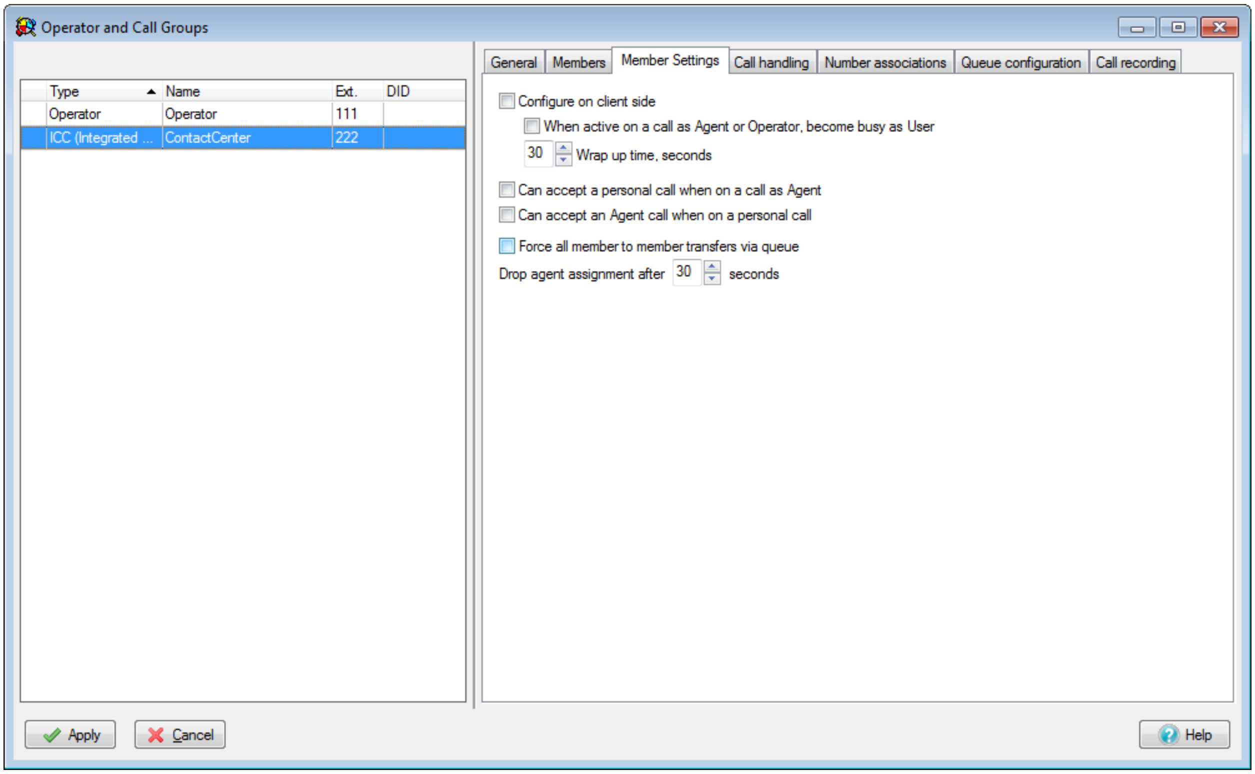
Note that the following are not included in the configuration file for MXIE Preferences.

Setting	Comment
Audio Drivers	Must be configured individually for each user in MXIE.
Softphone -> Audio Parameters	Must be configured individually for each user in MXIE.
Call Groups and Operators	Agent's status settings and wrap up times are configured in the User Profile or Call Groups window in MX-E Administrator. See Sections 28 and 28.2. Popup notification and Call Management settings are included in the centralized MXIE Preference .ini file.
Supervisor	Must be configured individually for each user in MXIE.
Device Access Policy	Configured in the User Profile in MX-E Administrator, see Section 28.

Setting	Comment
MXmeeting	Configured in the User Profile in MX-E Administrator, see Section 28.
Call Handling	Configured in the User Profile in MX-E Administrator, see Section 28.3.

28.2 Centralized Agent Settings

To set how changes to Agent Status affect the User Status and wrap up time and other group-specific configurations, navigate to *Configure -> Operator and Call Groups*. Select a Call Group to edit from the list in the left-hand column and open the *Member Settings* tab.



Type	Name	Ext.	DID
Operator	Operator	111	
ICC (Integrated ...	ContactCenter	222	

□ Configure on client side

□ When active on a call as Agent or Operator, become busy as User

30 Wrap up time, seconds

□ Can accept a personal call when on a call as Agent

□ Can accept an Agent call when on a personal call

□ Force all member to member transfers via queue

Drop agent assignment after 30 seconds

By default, the *Configure on client side* checkbox is enabled. This setting means that wrap up time and *When Active on a Call as Agent or Operator, become* *busy as User* option need to be configured individually from each user's MXIE client.

From this tab, you can choose whether agents can accept personal calls while on an active agent call, as well as whether they can accept agent calls while on an active personal call. With Release 9.0, this setting is now available for all types of Call Groups.

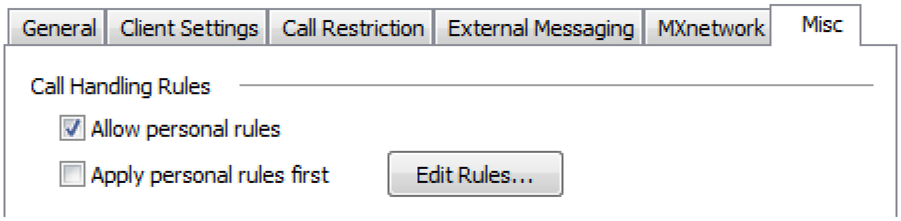
Settings for how changes to User's status affect their Agent Status are located in the User Profile. See Section 28.

When *Force all member to member transfers via queue* option is enabled, all calls transferred between users who are members of the same Call Group will be considered Agent Transfers. These transferred calls will be placed into Call Group's queue with highest priority for a particular Agent. If this Agent fails to answer the call in a timely fashion, after the time period specified in the *Drop Agent Assignment* setting expires, this call will be sent to the next available agent. The same timeout period also applies to parked Call Group calls.

When finished, click *Apply* to push the changes to all users.

28.3 Centralized Call Handling Rules

To configure centralized Call Handling Rules, in the User Profile navigate to the *Misc* tab.



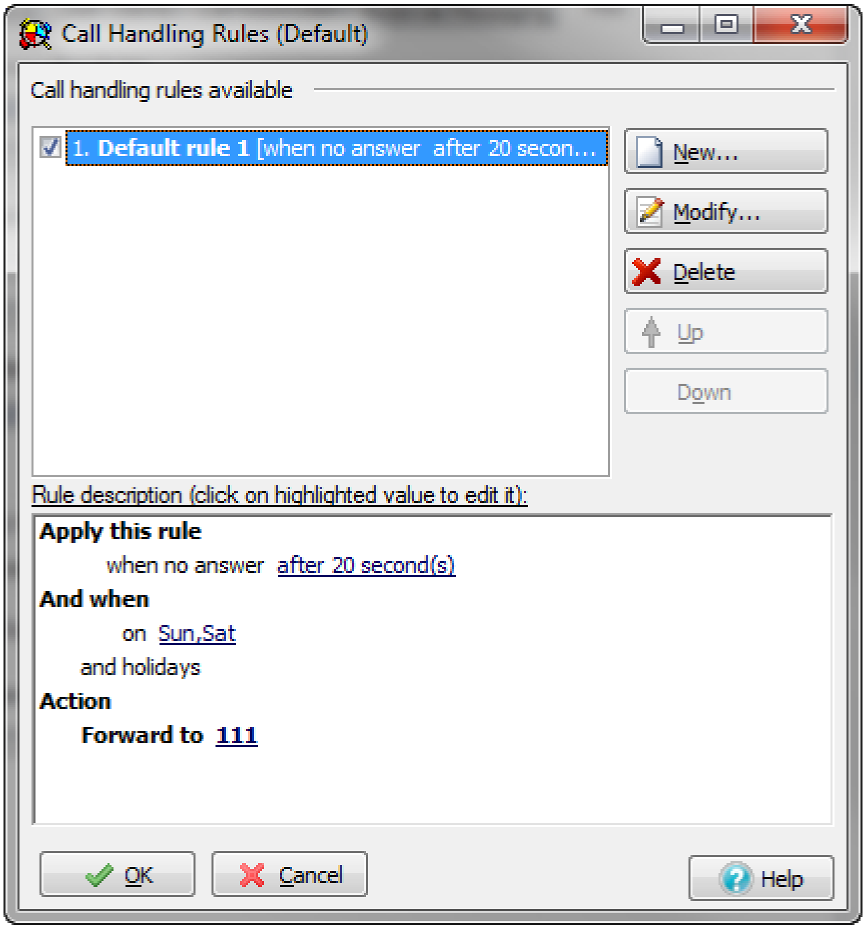
Call Handling Rules

☑ Allow personal rules

□ Apply personal rules first

The *Allow personal rules* option allows users to configure their own Call Handling Rules in addition to the ones configured for their User Profile. If this option is enabled, you can choose whether centralized or personal Call Handling Rules will take precedence with *Apply personal rules first* option, effectively this option determines whether personal rules appear before or after rules defined in the Profile.

To create new Call Handling Rules or edit existing ones, click the *Edit Rules* button.



Call Handling Rules (Default)

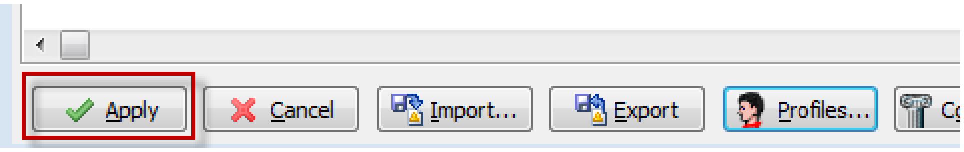
Call handling rules available

☑ 1. **Default rule 1** [when no answer after 20 secon…

Rule description (click on highlighted value to edit it):

Apply this rule
when no answer after 20 second(s)
And when
on Sun,Sat
and holidays
Action
Forward to 111

When finished, click *OK* to save the new Call Handling Rules then click the *Apply* button in the *User* window to push the changes to all users.



Changes will take effect immediately. Users do not need to restart MXIE.

29. Adding Operators, Hunt Groups, ACD and Inbound call Centers

Overview: Groups provide a special function for users of the MX-E. They allow one phone number (Either extension and / or DID) to be assigned to multiple users. Each group can support up to four tiers of skills based routing, which allows the calls to be routed to the highest priority agent in the group. In cases where there are multiple agents of the same priority, incoming calls can be setup to be routed between agents using one of three patterns: Ring All, Longest Idle, or Least Busy. In most cases, the agent would have to be logged into the group using MXIE for calls to be routed to the agent. The exception to this is the Hunt Group which is always logged in and calls will be routed to the agent's phone even if they are not logged into the system.

29.1 Adding Operators, Hunt Groups, ACD and Inbound Call Center Groups

- Click on Configure | Operators and Call Groups
- Right click in the left panel and select "Add" or press the Insert key on your computer.

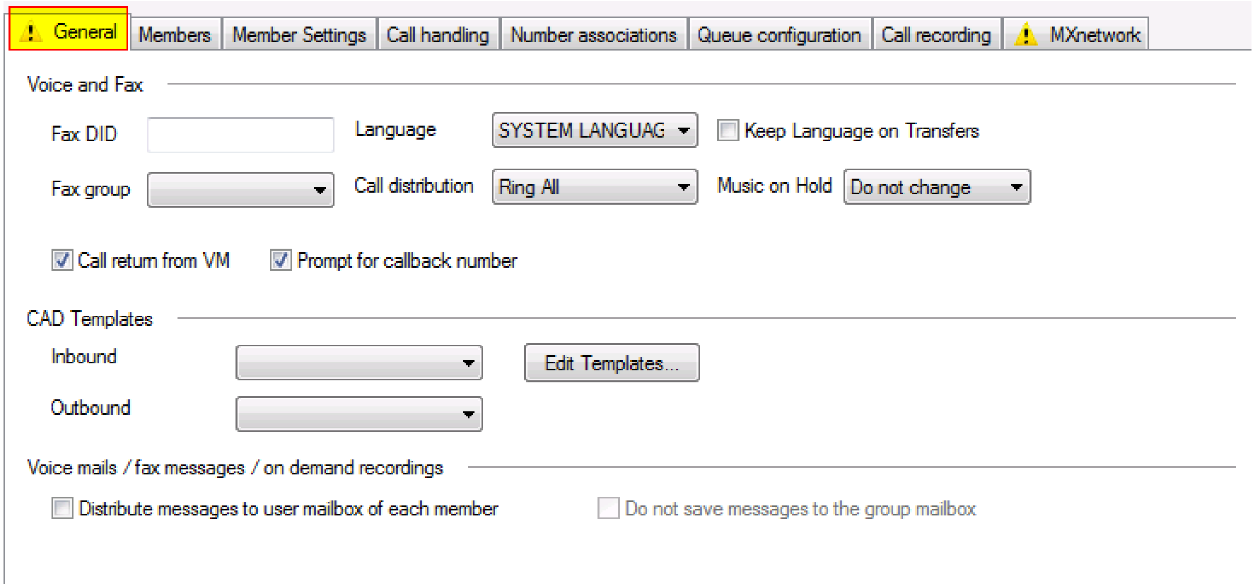
29.2 Adding a Call Group:

- Select Call Group Type
- Enter a name
- Assign the group a valid extension number
- Assign the group a valid DID (optional)
- Other configurable parameters:
    - Voice and FAX
        - Fax DID
        - Fax Group
        - Language
        - Call Distribution
            - Least Busy - The agent who was on the phone for shortest time (time from all calls summed together) gets the next call
            - Ring All – rings all agents of the same priority
            - Longest Idle – implements the "longest idle" algorithm or the agent who was not on a call for the longest time will get the next call

        - Music on Hold
        - Can Return Calls from Voice Mail
        - Prompt caller for Callback Number
    - CAD Templates
        - Inbound
        - Outbound
    - Voice mails / Fax messages / on demand settings
        - Distribute messages to user mailbox of each member
        - Do not save messages to the group mailbox

29.2.1 Creating a Call Group:

1. Double click on the “Type” field and select **Call Group Type**
    1. **Operator**
    2. **ACD**
    3. **Hunt**
    4. **ICC (Inbound Call Center)**
2. Double click on the “Name” field and enter name
3. Double click on the “Extension” field and enter a valid extension
4. Set “Call Distribution”, “Call Return from VM” and “Prompt for callback number” shown below



Voice and Fax

Fax DID

Language: SYSTEM LANGUAG

□ Keep Language on Transfers

Fax group

Call distribution: Ring All

Music on Hold: Do not change

☑ Call return from VM

☑ Prompt for callback number

CAD Templates

Inbound

Outbound

Voice mails / fax messages / on demand recordings

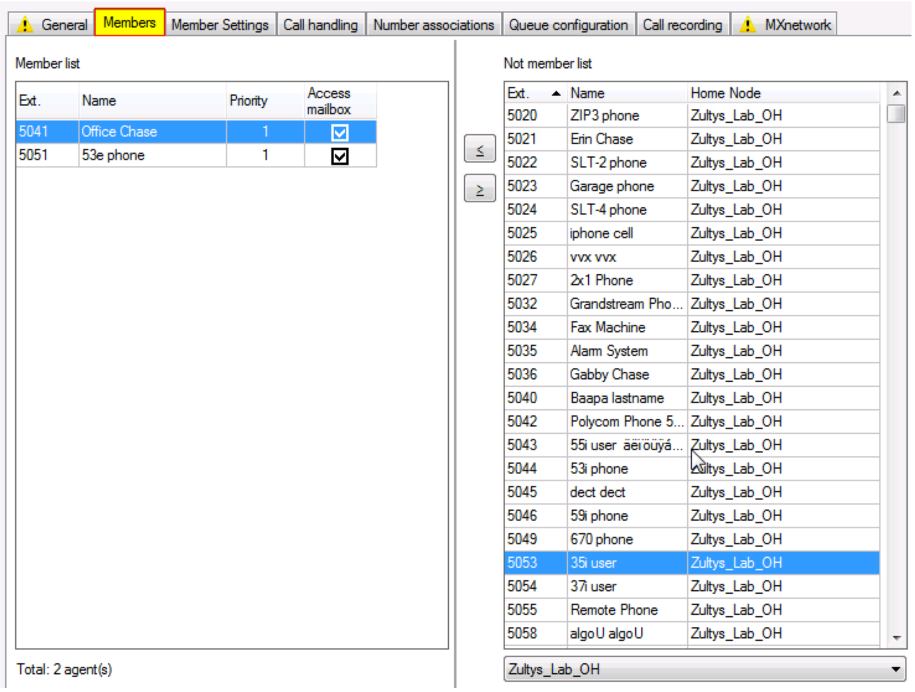
□ Distribute messages to user mailbox of each member

□ Do not save messages to the group mailbox

Figure 1: Configuring the General Tab for Operator Groups

29.2.2 Adding Members to a Call Group:

5. From the Configuration Pull-down menu, select Operators and Call Groups
6. From the Call Group Configuration Screen, Click on the Call Group, then click on the Members Tab
7. Select users from the “Not a Member” list and Click on Add
   - If the MX-E is part of a MXnetwork there is an option to filter to particular nodes
8. Repeat this process to add other users to the “Members List” as shown below
9. Setting Priority to 3 – this means that the user will receive fewer calls then Priority 1
10. Setting Priority to 1 – this means that calls will always be routed to this user first.
11. Select which users to have access to the group’s voicemail by placing a checkmark in the Access mailbox. See below



Member list

Ext.	Name	Priority	Access mailbox
5041	Office Chase	1	☑
5051	53e phone	1	☑

Total: 2 agent(s)

Not member list

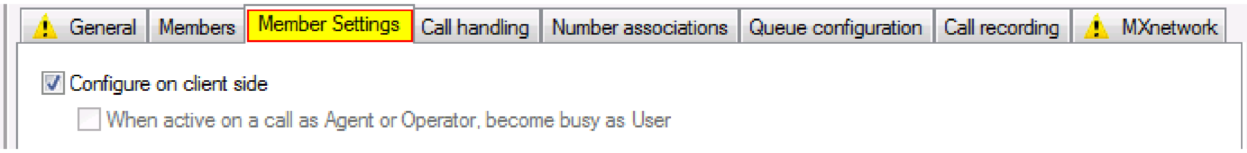
Ext.	Name	Home Node
5020	ZIP3 phone	Zultys_Lab_OH
5021	Erin Chase	Zultys_Lab_OH
5022	SLT-2 phone	Zultys_Lab_OH
5023	Garage phone	Zultys_Lab_OH
5024	SLT-4 phone	Zultys_Lab_OH
5025	iphone cell	Zultys_Lab_OH
5026	vvx vvx	Zultys_Lab_OH
5027	2x1 Phone	Zultys_Lab_OH
5032	Grandstream Pho...	Zultys_Lab_OH
5034	Fax Machine	Zultys_Lab_OH
5035	Alarm System	Zultys_Lab_OH
5036	Gabby Chase	Zultys_Lab_OH
5040	Baapa lastname	Zultys_Lab_OH
5042	Polycom Phone 5...	Zultys_Lab_OH
5043	55i user äëïöüýá...	Zultys_Lab_OH
5044	53i phone	Zultys_Lab_OH
5045	dect dect	Zultys_Lab_OH
5046	59i phone	Zultys_Lab_OH
5049	670 phone	Zultys_Lab_OH
5053	35i user	Zultys_Lab_OH
5054	37i user	Zultys_Lab_OH
5055	Remote Phone	Zultys_Lab_OH
5058	algoU algoU	Zultys_Lab_OH

Zultys_Lab_OH

Figure 2: Adding members to a Call Group

29.2.3 Configuring Member Settings for a Call Group:

Configure if the Agent is allowed to changes these settings from their MXIE client or if they are set via the MX-E and are not allowed to be modified by the Agent in MXIE.



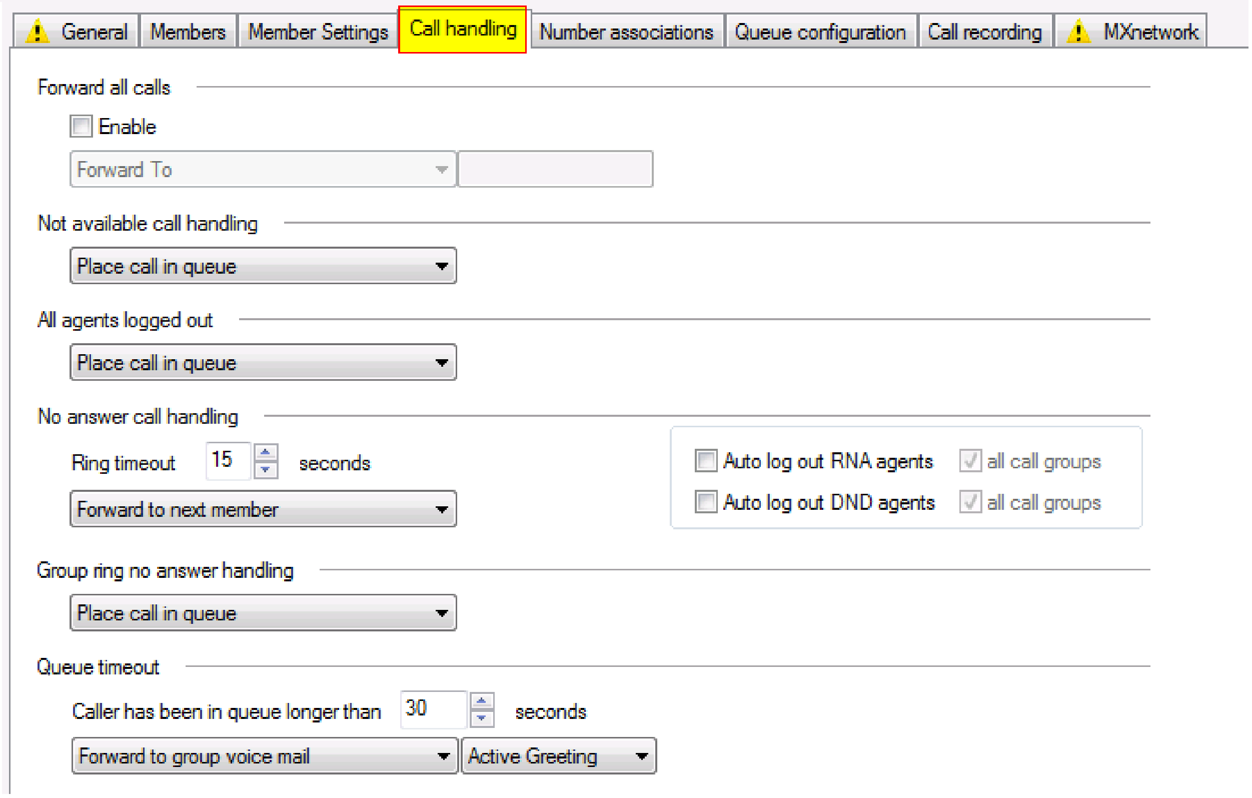
☑ Configure on client side

□ When active on a call as Agent or Operator, become busy as User

29.2.4 Configuring Call Handling for a Call Group:

Overview: Call Handling options allow you to configure how you want calls handled when an agent is not available to take a call.

- From the Configuration Pull-down menu, select Operators and Call Groups
- From the Call Group Configuration Screen, Click on the Call Group, then click on the Call Handling Tab
- Configure the following options: (See Below)
    - **Forward All Calls**: If enabled, all calls can either be sent to another extension or to the group voicemail box.
    - **No Answer Call Handling**: These options describe what action should be taken if a call is not answered by a specific agent within a configurable amount of time. Normally, the default action, Forward to Next Member, is the preferred action.
    - **Not available call handling** describes what to do when an agent is not available to answer the call. The default action, Place call in queue, allows the caller to be placed in queue and the call would be routed to the first agent that becomes available.
    - The **Group RNA** (Ring No Answer) handling option defines what actions should be taken if everyone in the group is busy. Here, the default action, Place call in queue, is the preferred action.
    - The All Agents logged out option allows you configure the action for when all agents are logged out of the group.
    - The last option, Queue timeout allows you to configure what to do if the call is not answered within a configurable amount of time.



Forward all calls

□ Enable

Forward To

Not available call handling

Place call in queue

All agents logged out

Place call in queue

No answer call handling

Ring timeout 15 seconds

Forward to next member

□ Auto log out RNA agents ☑ all call groups

□ Auto log out DND agents ☑ all call groups

Group ring no answer handling

Place call in queue

Queue timeout

Caller has been in queue longer than 30 seconds

Forward to group voice mail | Active Greeting

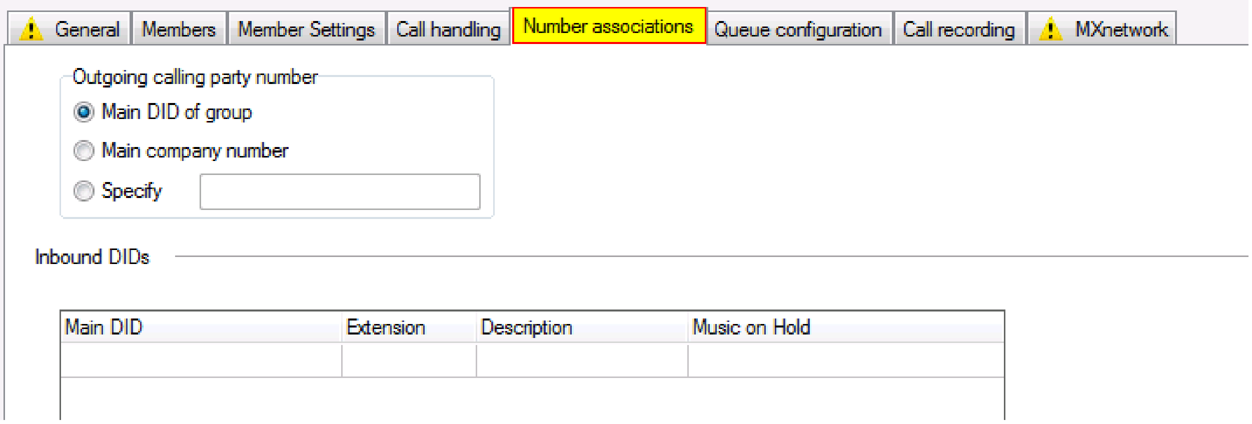
Figure 3: Configuring Call handling options for a Call Group

29.2.5 Configuring Number Associations

Overview: Number Associations allow one group to receive calls made to a variety of phone numbers. Each sub-group can be configured for a Main DID, an Extension, and a Description of the group. When a call comes into the sub-group the call rings in on the main group's MXIE interface with the addition of a description of the called number.

- From the Configuration Pull-down menu, select Operators and Call Groups
- From the Call Group Configuration Screen, Click on the Call Group, then click on the Number Associations Tab
- Configure the following options:
  - Outgoing calling party number: Defines the caller ID for outbound calls made from the group.
    - Main DID of the group – then number of the main group

        - Main company number – the main number configured under Provision | System Settings | Company Information screen
        - Specify – Some other number
    - Inbound DIDs: Defines the Main DID, Extension, Description, and Music On Hold Play List of the sub-group(s)



Outgoing calling party number

● Main DID of group

○ Main company number

○ Specify

Inbound DIDs

Main DID	Extension	Description	Music on Hold

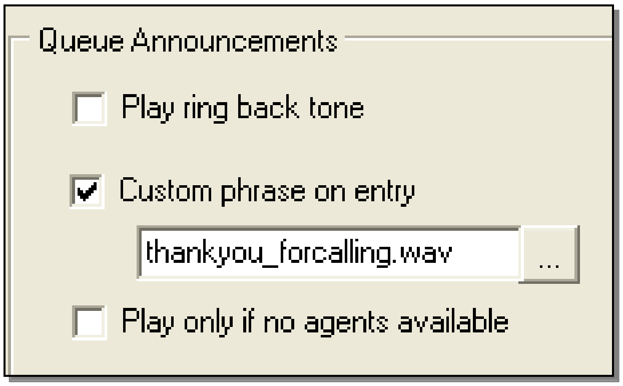
Figure 4: Adding Number Associations

29.2.6 Call Group Queue Announcements:

When a caller is placed in queue, the Queue Announcements are used to configure which messages the caller will hear while they are in queue. The first section deals with what the caller will hear when they enter the queue and the second section defines which messages will be played and how often they will be played while the caller is in queue.

- **Play ring back tone**: Plays a ring back signal once when the caller is connected to the queue.
- **Custom Phrase on entry** – allows you to play a greeting message (Only Available for Inbound Call Center)
    - Three choices:
        - Local Files – any 8KHz, 8 Bit, Mono CCITT U-Law “wav” file on your local system
        - System Prompts – Select from a list of system provided prompts
        - Text to speech – allows you to create a script and convert it from text to speech.

- **Play only when no agent is available** – If selected, greeting messages are only played when no agent is available.
- **Position in Queue** – informs the caller how many people are ahead of them in the queue
- **Expected Wait Time** – describes how long they should expect to be in queue
- **Note**: This value is reset based on the "Real-Time Group and Agent statistics reset configuration" found at the bottom of the "General" Tab of the Inbound Call Center configuration window.



Queue Announcements

□ Play ring back tone

☑ Custom phrase on entry

thankyou_forcalling.wav

□ Play only if no agents available

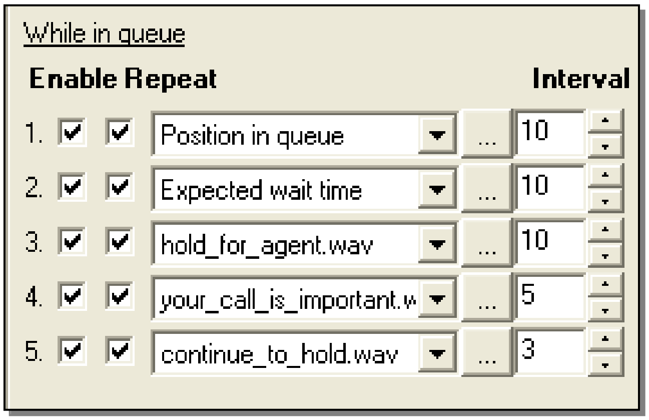
29.2.6.1 While in the Queue:

This section describes how the call will be treated while the caller is in the queue. Which messages will be played, will they repeat, and how often will they be played. You can play up to five messages and decide if they are to repeat.

- Click on both Enable and Repeat for the first outgoing message:
  - Select Position in Queue from the pull-down menu
  - Set the repeat time to 10 seconds – this will play this message 10 seconds after the last message.
- Click on both Enable and Repeat for the second outgoing message:
  - Select Expected Wait Time from the pull-down menu
  - Set the repeat time to 10 seconds – this will play this message 10 seconds after the last message.
- Click on both Enable and Repeat for the third outgoing message:

  - Select the system prompt “Hold_For_Agent.wav” by clicking on the files button ... and select system prompts
  - Select a repeat period of 5 seconds. This message will play 5 seconds after the previous greeting.
- Click on both Enable and Repeat for the fourth outgoing message:
  - Select the system prompt “Your_Call_Is_Important.wav” by clicking on the files button ... and select system prompts
  - Select a repeat period of 5 seconds. This message will play 5 seconds after the previous greeting.
- Click on both Enable and Repeat for the fifth outgoing message:
  - Select the system prompt “Continue_To_Hold.wav” by clicking on the files button ... and select system prompts
  - Select a repeat period of 5 seconds for this file. This message will play 5 seconds after the previous message.

***Note**: If the caller is still in queue, the caller will next hear the first message. In our case, that is the position in queue message and it will play 10 seconds after the Continue_To_Hold message.*



While in queue

	Enable	Repeat			Interval
1.	☑	☑	Position in queue	...	10
2.	☑	☑	Expected wait time	...	10
3.	☑	☑	hold_for_agent.wav	...	10
4.	☑	☑	your_call_is_important.w	...	5
5.	☑	☑	continue_to_hold.wav	...	3

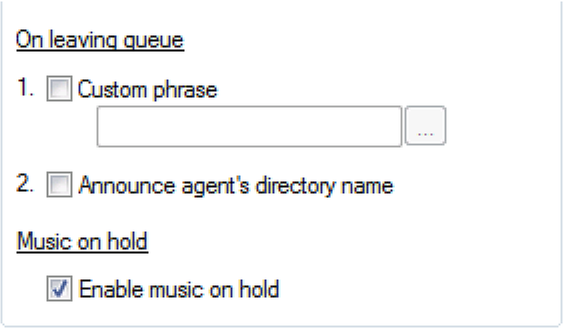
29.2.6.2 On Leaving Queue:

Overview: The last section of the while in Queue Announcements field describes how the system will respond when the call is answered.

- **Custom Phrase** – Allows you to select a wave file to be played when the call is answered.
  - Select the System Prompt “transfer_to.wav”
- **Announce Agent’s Directory Name** – Enable this feature

29.2.6.3 Enable Music on Hold – will play music while the caller is on hold.

- Enable this feature if required.



On leaving queue

1. □ Custom phrase

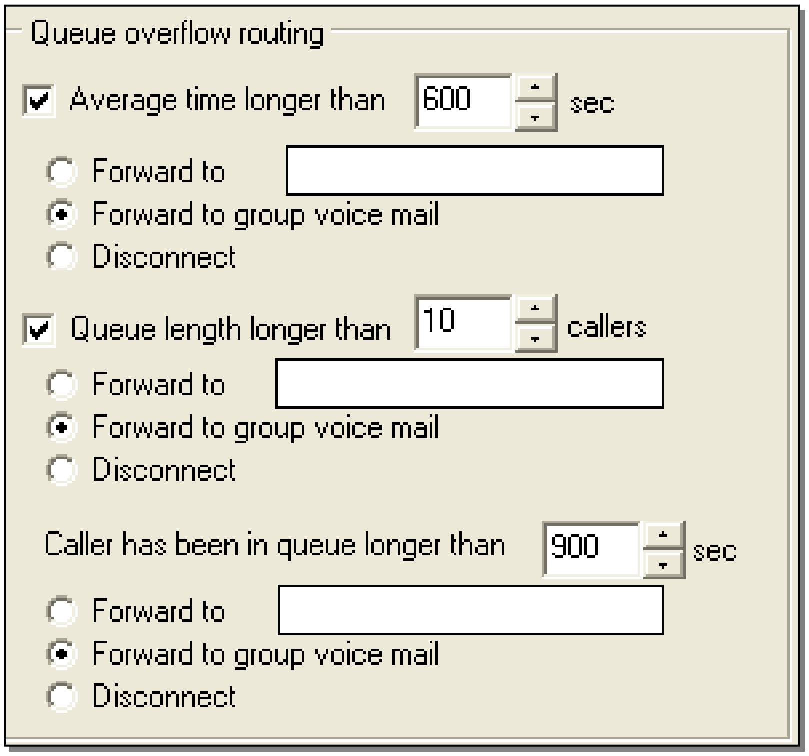
2. □ Announce agent's directory name

Music on hold

☑ Enable music on hold

29.2.6.4 Configuring Inbound Call Center Queue Overflow Routing:

Overview: Queue Overflow Routing allows the system to set some general rules when too many callers hit the ICC group at the same time. Among the configurable values are: Average Time, Queue Length, and Caller has been on hold to long. In each case, the choices are the same: Forward to another number, Forward to Group Voice Mail, or Play Busy Tone and Disconnect. This option is for ICC call groups only.



Queue overflow routing

☑ Average time longer than 600 sec

○ Forward to
● Forward to group voice mail
○ Disconnect

☑ Queue length longer than 10 callers

○ Forward to
● Forward to group voice mail
○ Disconnect

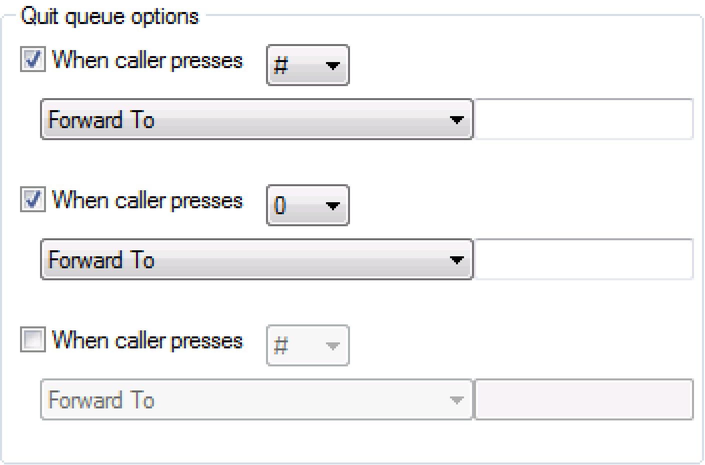
Caller has been in queue longer than 900 sec

○ Forward to
● Forward to group voice mail
○ Disconnect

29.2.6.5 Configuring Quit Queue Options:

Overview: This section is used to configure the MX-E to respond to specific input from the caller while they are in queue. The specific inputs that can be used to exit the queue are pound / hash (#) and any number from zero to nine (0, 1, 2…9) and the actions that can be taken are either Forward to Group Voice Mail or Forward To a specific extension. Up to 3 different options may be configured.

- When Caller Presses # -- choose forward to voicemail or to another extension/phone number
- When Caller Presses 0 -- choose forward to voicemail or to another extension/phone number
- When finished, click Apply to save your changes.
- See below for details



Quit queue options

☑ When caller presses #
Forward To

☑ When caller presses 0
Forward To

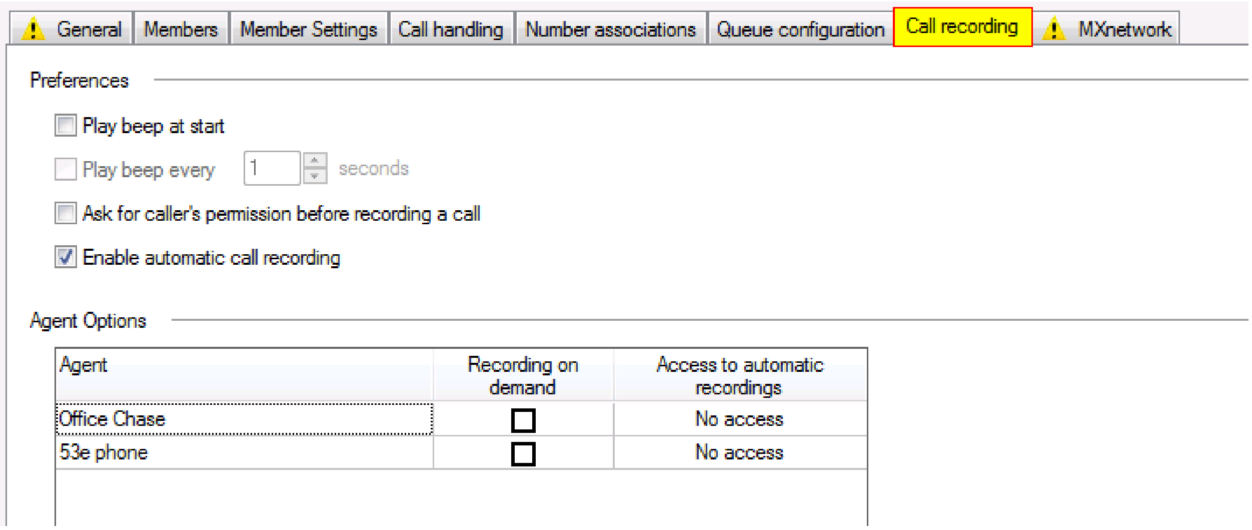
☐ When caller presses #
Forward To

Figure 5: Configuring Queue Configuration

29.2.7 Configuring Call Recording for a Call Center:

- From the Call Group menu, click on the call recording Tab
- From the Preferences menu:
  - **Play beep at start** – plays a beep at the start of recordings
  - **Play beep every XX seconds** – configures the frequency of the call recording beep.

  - **Ask the caller's permission before recording** – prompts the caller for permission to record
  - **Enable automatic call recording** – automatically records all calls
- Agent Options: These options allow the administrator to configure Record on Demand and Access to Automatic recordings options. See below for details.



Preferences

☐ Play beep at start

☐ Play beep every 1 seconds

☐ Ask for caller's permission before recording a call

☑ Enable automatic call recording

Agent Options

Agent	Recording on demand	Access to automatic recordings
Office Chase	☐	No access
53e phone	☐	No access

Figure 6: Configuring call recording options on a Call Group

29.2.8 MXnetwork options

MXnetwork tab allows the configuration of MXnetwork features when the MX-E is part of an MXnetwork.

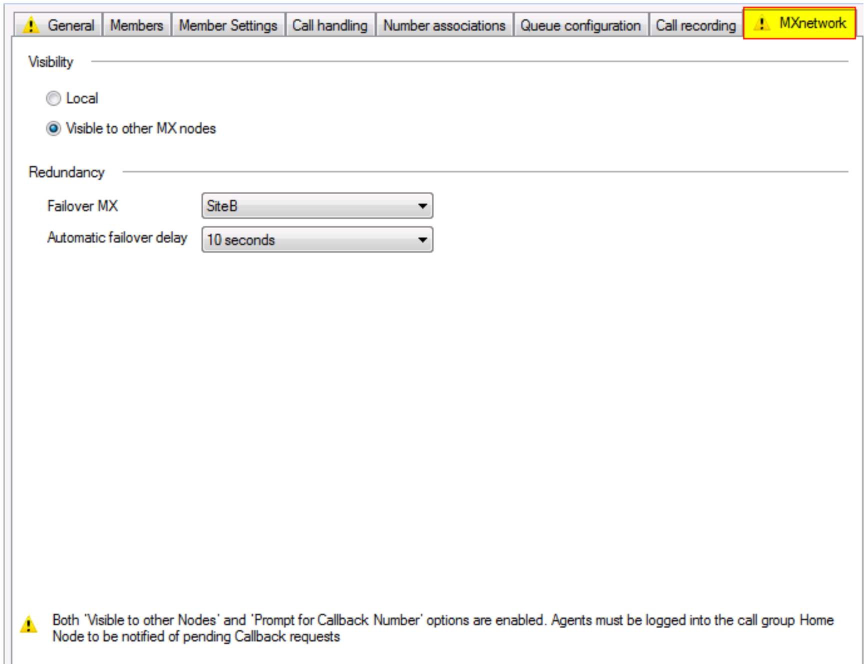
Visibility

- **Local**: the Call Group is only visible to agents logged into this node, only agents logged into this node are able to be a member of the call group
- **Visible to other MX-E nodes**: The call group is visible on all nodes of the MXnetwork, and agents may login to this call group while logged into their home node.

Redundancy

This feature requires MXnetwork and MXnetwork failover licensing

- **Failover MX-E**: Define the MX-E the call group functionality will failover to in the event this MX-E fails.
- **Automatic failover delay**: delay time before the call group fails over.



Visibility

○ Local

● Visible to other MX nodes

Redundancy

Failover MX: SiteB

Automatic failover delay: 10 seconds

Both 'Visible to other Nodes' and 'Prompt for Callback Number' options are enabled. Agents must be logged into the call group Home Node to be notified of pending Callback requests

30. Configuring Dial Plan:

The Dial Plan is used to decide how calls are routed by the MX-E. There are several tabs that are used to configure the routing of calls, how calls will be distributed, and if any restrictions have been configured.

30.2 Configuring Call Routing:

The Call Routing screen is used to describe for a specific dialed number, how the call will be routed by the MX-E. This screen has four significant fields: Pattern, Interface, Transformation, and Restriction. As you configure the Call Routing, you will add a line that will be used to define a specific pattern. Then you will select the Destination – or which interface the call will be routed to. Next, you will configure the Transformation field to describe how a dialed number will be modified before it will be sent over interface. Lastly, you will be asked if the calls on a specific interface may be restricted. As you build your dial plan, you will add multiple patterns for the dialed number. Each dialed number will be compared to the first pattern. If it doesn’t match the first pattern it will be compared to the second number. The call will continue this process until it finds a pattern that matches the dialed number. As such**, the specific order of the individual patterns is very important**. Therefore, items should be organized from most specific (first) to least specific (last).

30.2.1 Source Options

- **Internal:** Covers any call originated on this MX-E, another MX-E node in MXnetwork, internal SIP servers, Tie Lines
- **This MX-E**: Covers calls that originate on this MX-E
- **External**: This covers all external trunks (PSTN / ISDN / External SIP server / ITSP)
- **Location XXX**: Calls from the location specified
- **MX-E Node XXX**: Calls from the MX-E Node specified
- **FXO XXX**: The call originated from the FXO Group
- **PCM XXX**: The call originated from the PCM Group
- **ITSP XXX**: The call originated from the ITSP Service provider

- **SIP XXX**: The call originated from the SIP provider
- **Location XXX**: The call originated from the Location Specified
- **AA xxx**: The call originated from the Auto Attendant Specified

30.2.2 Destination Options

- **Blocked**: The call is rejected with no option to bypass
- **Extensions**: Covers User extensions and System Services including those shared across MXnetwork
- **FXO XXX**: The call is routed out the FXO Group
- **PCM XXX**: The call is routed out the PCM Group
- **ITSP XXX**: The call is routed out the ITSP Service provider
- **SIP XXX**: The call is routed out the SIP provider
- **Location XXX**: The call is routed out the Location Specified
- **This MX-E DID's**: Available only when Source = External. When selected the Transformation will be checked against DID numbers provisioned on this MX-E.
- **AA xxx**: The call is routed to the Auto Attendant Specified
- **MX-E Node XXX**: Calls is routed to the MX-E Node specified
- **Transform and Continue**: The transformation is applied to the dialed number, and the call continues to move down the dial plan looking for a new match

Note: Trunk Groups are automatically added to the destination drop down after they are created and applied. Please create all trunk groups before modifying the Dial Plan.

30.2.3 Pattern vs Route

- **Pattern**: This is what the caller dials and is matched against in the dial plan to be routed.
- **Route**: This is how the call is routed once a match is found. You can have multiple routes for a single pattern.

30.2.4 Call Routing Pattern Variables:

- In your MX-E Administrator click on “Configure” and then select “Dial Plan”
- Click on the “Routing” tab

- **Source**: Can limit application of rule to calls made from a specific location, SIP servers etc. Normally set to “Internal”
- **Pattern Variables**:
  - X or x – Any digit.
  - + (plus sign) used for international dialing
  - [or] – Square brackets. Surround a range of numbers.
  - - – A dash – used to separate a range of numbers.
    - 5-6 – when used with square brackets EG [5-6], indicate a range of numbers.
  - 0,1,2,3,4,5,6,7,8,9,0 – Specific Digits.
  - @ – A wild card – meaning “or more”. For example: XXXXXXX@ means seven or more digits.
- **Destination**: A pull-down menu that is used to select the physical or logical Interface that would be used to carry the call.
- **Transformation Patterns**:
  - X or x – Any digit. The corresponding digit in “Pattern” field is sent as is
  - 0,1,2,3,4,5,6,7,8,9,0 – Specific Digits – used to insert digits in the transformation field
  - D or d – used to delete digits in the Transformation field
  - + (plus sign) used for international dialing
  - * or # -- used to insert digits in the transformation field
- **Restricted**: Indicates if a specific pattern may be restricted. Once a check mark is placed in the restricted field it will show up in the user profile → call restriction tab.

30.2.5 Configuring Basic Call Routing:

Dial plan entries are added by right clicking and choosing “New Pattern” from the dropdown.

The Routing table specifies rules for routing calls that are dialed by users of your MX-E system and of other MX-E systems located within your MXnetwork. Each row lists one dialing rule or an alternate route for an existing dialing rule. Rules are listed in order of precedence; if a phone number matches the pattern of two different rules, the dialing plan will use the rule with the lowest precedence number.

30.2.5.1 Field Definitions

Each dialing rule comprises the following parameters, as listed in the table:

·Rule Status (first blank column heading): An icon in this column indicates that the rule has a configuration problem:

- There are two symbols that you may see while viewing the dial plan.
  - The ⛔ denotes a serious problem with the dial plan and you will not be able to click apply until the problem is resolved. The simplest way to resolve problems is the click on the line where you see the symbol and the system will tell you what the problem is. The most common problem that you will find is an inconsistency between the pattern and the transformation.
  - The ⚠ is a cautionary statement – it is used draw your attention to the line and you must decide if there is a problem. The most common problem that you will find is if one pattern is completely hidden by another one. This occurs when items in the dial plan are not arranged from specific to general. You can also see a caution saying that one pattern is partially overlapped by another. Most times this is not a problem.
- ·Precedence (second blank column heading): Dialing rules are evaluated based on precedence. Dialed numbers are evaluated first against the rule with the smallest precedence number, then against rules with successively higher precedence numbers until a match is found between the dialed number and a rule.

When a rule has multiple destinations and transformations, MX-E attempts to place the call through the route defined by the destination that appears on the row that defines the rule. If it is unable to access that route, it will attempt to use the destination-transformation on the next row.

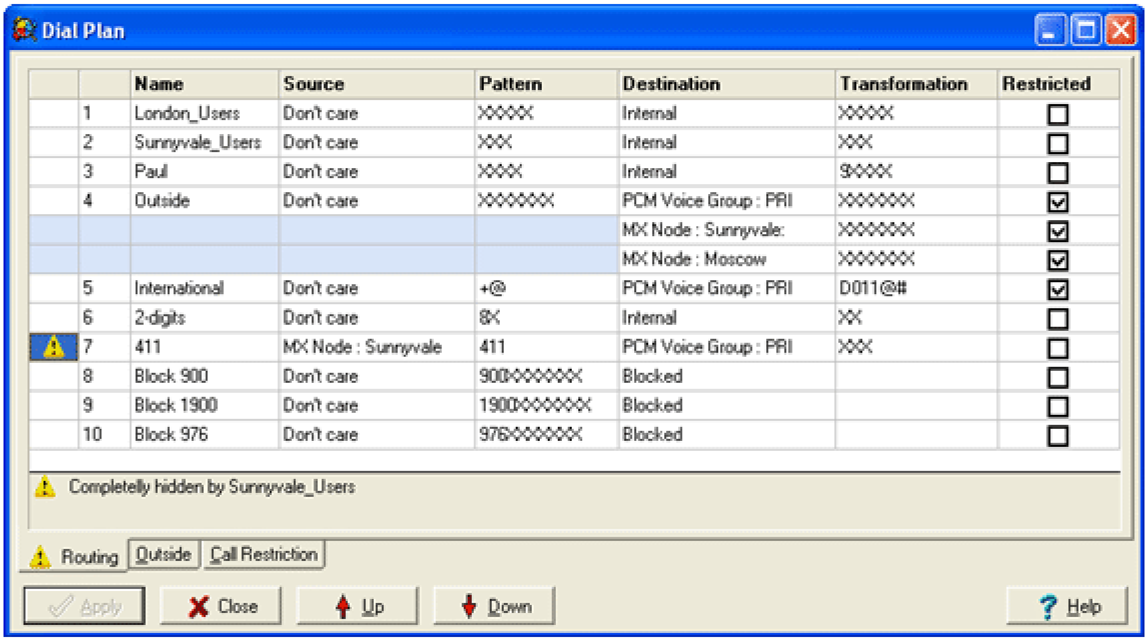
To change the precedence of a dialing rule or alternate destination-transformation, use the Up and Down buttons located at the bottom of the panel.

- Name: This is the alphanumeric name of the rule. The MX-E refers to dialing rules in other panels by this name. You can have spaces in the name and define rules with duplicate names within a dial plan.
- Source: This column indicates the users for which the rule is valid:
- Pattern: This column lists the filter pattern that the MX-E compares to a dialed number. If the dialed number matches the pattern, the number is transformed and routed as defined by the rule. A dialed number is evaluated against the patterns of different rules until the MX-E finds a match. If a number does not match any rule pattern, the call is discarded.
- You cannot specify any entity defined by the Services panel (voice mail server, bind server, park server, page server, or any auto attendant) or by the Operators and ACD Groups window (ACD groups, Inbound Call Center groups, hunt groups, or operator groups).
- Destination: The destination defines the route that the MX-E uses to transmit the call filtered by the dialing pattern. Destination setting options include each available transmission option including:
- Transformation: When a dialed number matches a rule pattern, this field defines the transformation algorithm that converts the dialed number into the digits required to contact the destination entity.
- Restricted: Placing a checkmark in this box restricts access to phone numbers covered by the dialing rule. Access restrictions can prevent specified users from making a call or require an account code before completing the call. Call Restrictions describes the process of implementing MX-E call restrictions.

30.2.5.2 Creating a Dialing Rule

A dialing rule requires the following parameters: Name, Source, Pattern, Destination, and Transformation. In addition to the required parameters, you can define alternate destinations and transformations for each dialing rule and configure selected rules for call restrictions and account codes.

Each row table that lists a name, source, and pattern defines a dialing rule. Dialing rules that have more than one destination-transformation setting lists the additional settings immediately after the row that defines the rule; these rows do not list a name, source, or pattern setting.



		Name	Source	Pattern	Destination	Transformation	Restricted
	1	London_Users	Don't care	XXXXX	Internal	XXXXX	□
	2	Sunnyvale_Users	Don't care	XXX	Internal	XXX	□
	3	Paul	Don't care	XXXX	Internal	9XXXX	□
	4	Outside	Don't care	XXXXXXX	PCM Voice Group : PRI	XXXXXXX	☑
					MX Node : Sunnyvale:	XXXXXXX	☑
					MX Node : Moscow	XXXXXXX	☑
	5	International	Don't care	+@	PCM Voice Group : PRI	D011@#	☑
	6	2-digits	Don't care	8X	Internal	XX	□
⚠	7	411	MX Node : Sunnyvale	411	PCM Voice Group : PRI	XXX	□
	8	Block 900	Don't care	900XXXXXXX	Blocked		□
	9	Block 1900	Don't care	1900XXXXXXX	Blocked		□
	10	Block 976	Don't care	976XXXXXXX	Blocked		□

⚠ Completelly hidden by Sunnyvale_Users

The routing plan above configures a dial plan with the following attributes:

- ·The dial plan defines ten dialing rules.
- ·Dialing rule #4 provides two alternate destination-transformation settings in addition to the PCM Voice Group: PRI destination.
- ·The dial plan warns that rule #7 is completely hidden by rule #2 (Sunnyvale_Users).

Rules and alternate routes are created and deleted by right-clicking the mouse while the cursor points in the table. Table contents are always sorted by rule precedence defined in the second column. You can change the precedence of a rule by pressing the Up and Down button at the bottom of the panel or by right clicking the mouse and selecting Up or Down.

30.2.5.3 Dialing Rule Conflicts

Dialing rule conflicts result when a phone number is specified by more than one dial rule. For example in the screenshot in section 30.2.5.2, the number 411 is covered by dial rule #2 (pattern = xxx) and dial rule #7 (pattern = 411). When a user enters 411 under this dial rule, the call is routed as configured by rule #2; dial rule #7 is never used because of the conflict.

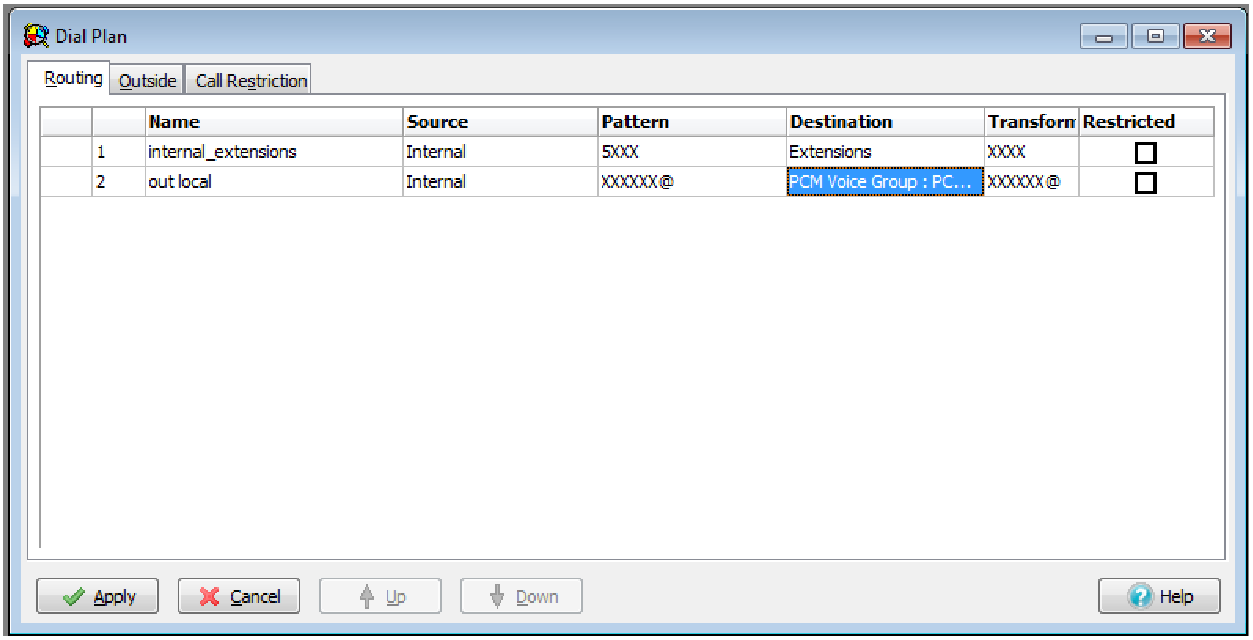
The MX-E reports three types of conflicts:

- B is overlapped by A indicates that some of the numbers defined by rule B are covered by a portion of the numbers defined by a preceding rule. In this case, all numbers covered by both rules will be resolved using the preceding rule (or rule A).
- B is completely hidden by A indicates that all numbers defined by rule B are covered by a portion of the numbers defined by a preceding rule. In this case, all numbers covered by rule B will be resolved using the preceding rule.
- B is partially hidden by A indicates that a portion of the numbers defined by rule B are covered by all of the numbers defined by a preceding rule. In this case, all rules covered by both rules will be resolved using the preceding rule.

30.2.5.4 Keyboard Manipulation

To access the data in the table, type the Tab key until an element in the table is selected. Type the Insert or Delete keys to add a new rule or delete an existing rule, respectively. Press Enter to edit the data and Enter again when you have finished editing the data. Use the arrow keys, Home, End, PgUp, and PgDn to move among the cells of the table. Use Control-Up arrow and Control-Down arrow to change the sequence of the rules.

Important: Routing panel changes do not take effect until you press the Apply button. If you press the Cancel button before pressing Apply, all pending changes to Dial Plan panels are disregarded. Pressing the Apply button saves all pending changes to every Dial Plan panel.



	Name	Source	Pattern	Destination	Transform	Restricted
1	internal_extensions	Internal	5XXX	Extensions	XXXX	□
2	out local	Internal	XXXXXX@	PCM Voice Group : PC...	XXXXXX@	□

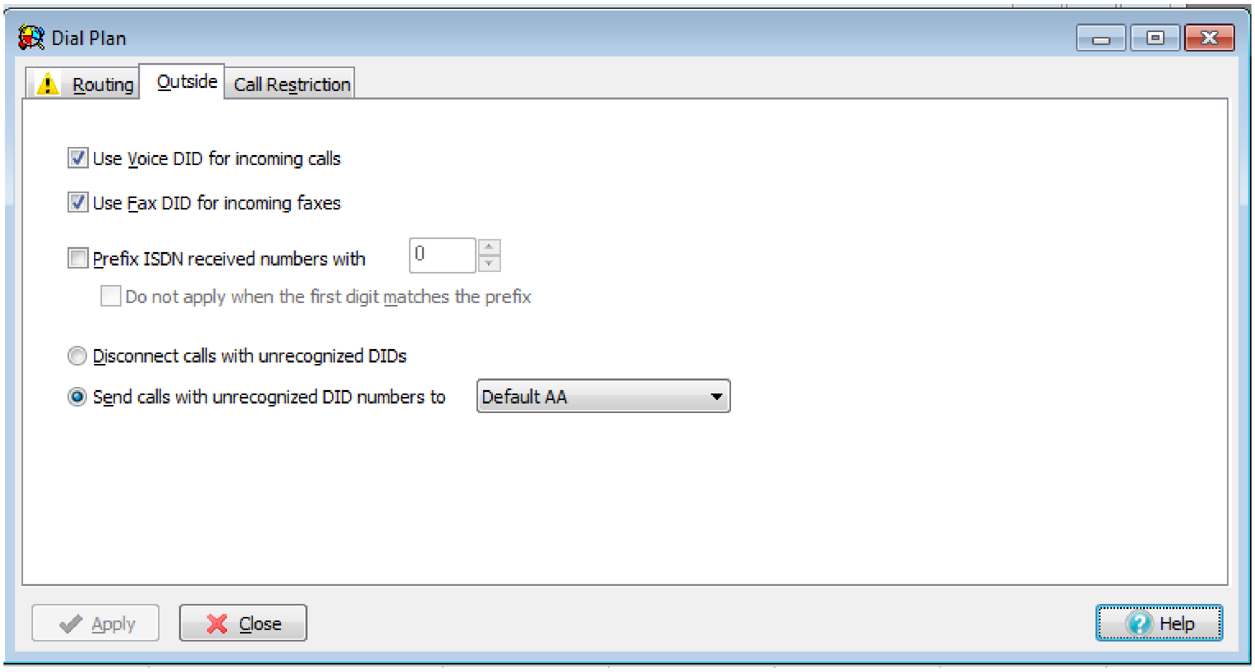
30.3 Configuring Dial plan: Outside:

- Use Voice DID for Incoming Calls
    - Enabling this option allows users that have Voice DID numbers to receive calls directly from the party calling their DID number without operator or auto attendant intervention. Selecting this option adds the Voice DID column to the User list.
    - Do not check this box if you are using ISDN subaddressing.
- Use Fax DID for Incoming Calls
    - Enabling this option allows users that have Fax DID numbers to receive Fax transmissions from callers that are external to the MX-E. Selecting this option adds the Fax DID column to the User list. Faxes sent to an MX-E user are stored in voice mail and received through MXIE.
    - Do not check this box if you are using ISDN subaddressing.
- Prefix ISDN Received Calls With
    - This option is typically used for calls received by the MX-E from an ISDN circuit (such as a tie line) and routed to another ISDN circuit (normally a PSTN line). Select this option to append the specified digit to the beginning of the ISDN number. You can choose not to

        append the digit if the first digit of the received number matches the digit.

- Send calls with Unrecognized DID Numbers
    - This option specifies a method of handling incoming calls with DID numbers that are not defined in the MX-E User List. This situation may arise where an MX-E is daisy chained between the PSTN and a legacy PBX that supports DID. In this case, the MX-E should send the call directly to the tie line that connects to the legacy system.
- Disconnect Calls with unrecognized DIDs to discard calls to DID numbers that are not assigned to a user or a group.
- Send calls with unrecognized DID numbers to route calls to DID numbers that are not assigned to a user or group.
    - Default Attendant
        - The term Default Attendant refers to a uniform call routing method. The Default Attendant routes calls in the following manner.
        - 1.Calls are sent to the Default Auto Attendant if that entity is on duty.
        - 2.Calls not handled by the Default Auto Attendant are sent to the Default Operator, if that entity is on duty. If the default operator is not configured, the call is lost.
        - 3.Calls not handled by a configured Default Operator are sent to voice mail.
    - Any Trunk defined in the MX-E

Important: Outside panel changes do not take effect until you press the Apply button. If you press the Cancel button before pressing Apply, all pending changes to Dial Plan panels are disregarded. Pressing the Apply button saves all pending changes to every Dial Plan panel.



Dial Plan

☑ Use Voice DID for incoming calls

☑ Use Fax DID for incoming faxes

□ Prefix ISDN received numbers with 0

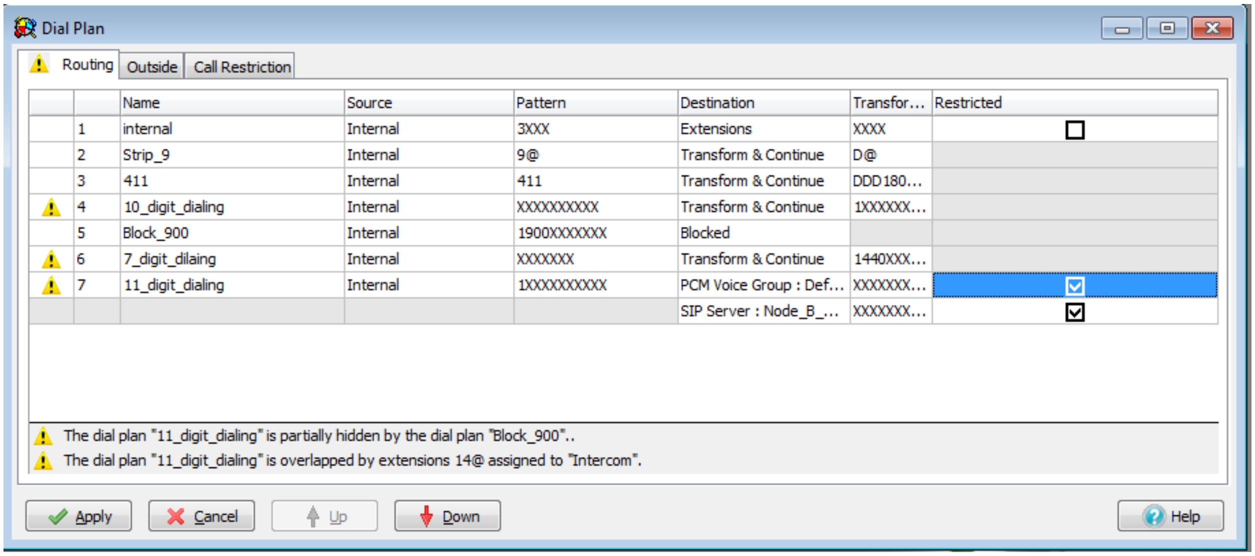
□ Do not apply when the first digit matches the prefix

○ Disconnect calls with unrecognized DIDs

● Send calls with unrecognized DID numbers to Default AA

31. Understanding Call Restrictions on the MX-E:

Call restrictions indicate whether or not a call over a particular trunk interface may be restricted. Once configured, user profiles are created that can either Restrict, Block or allow calls over a particular trunk interface. There are three steps to call restrictions: First in the “Dial Plan” – “Routing” window, clicking on the “Restricted” check-box. The second step requires that you define the restriction from the “Call Restriction” tab. And the third step requires that you define which user profiles are affected by the restrictions.



		Name	Source	Pattern	Destination	Transfor…	Restricted
	1	internal	Internal	3XXX	Extensions	XXXX	□
	2	Strip_9	Internal	9@	Transform & Continue	D@	
	3	411	Internal	411	Transform & Continue	DDD180…	
⚠	4	10_digit_dialing	Internal	XXXXXXXXXX	Transform & Continue	1XXXXXX…	
	5	Block_900	Internal	1900XXXXXXX	Blocked		
⚠	6	7_digit_dilaing	Internal	XXXXXXX	Transform & Continue	1440XXX…	
⚠	7	11_digit_dialing	Internal	1XXXXXXXXXX	PCM Voice Group : Def…	XXXXXXX…	☑
					SIP Server : Node_B_…	XXXXXXX…	☑

⚠ The dial plan "11_digit_dialing" is partially hidden by the dial plan "Block_900"..

⚠ The dial plan "11_digit_dialing" is overlapped by extensions 14@ assigned to "Intercom".

31.2 Adding Restrictions to Call Routing

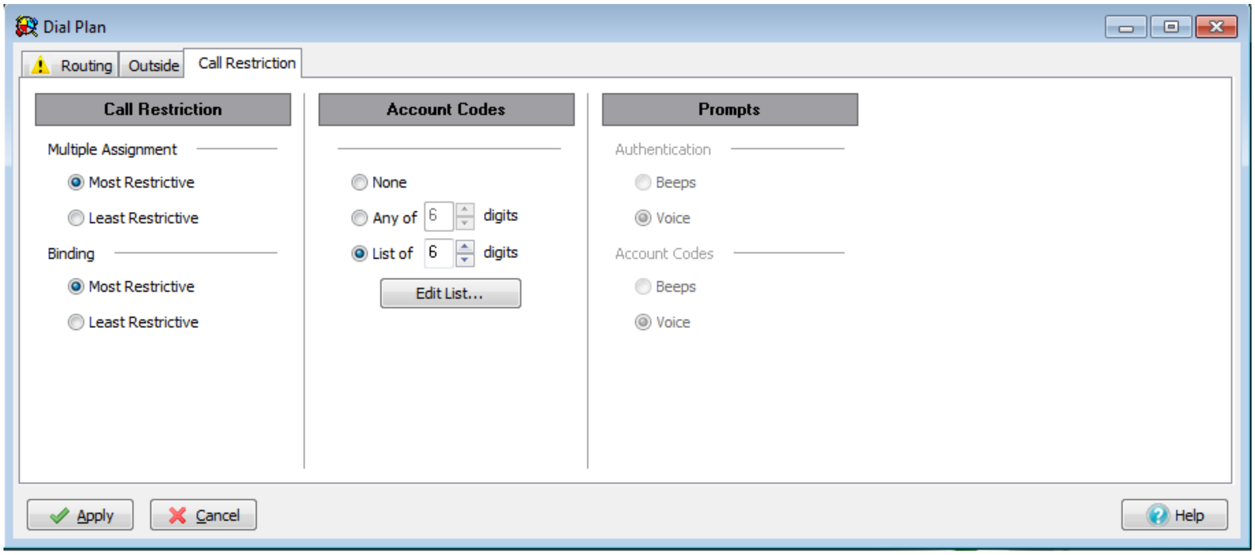
1. From the Configure pull-down menu, select Dial Plan.
2. Put a check in the restricted column on any interface that you would like to restrict calls on.

31.3 Defining Call Restrictions:

1. From the Dial Plan window, Click on the “Call Restriction” tab
2. There are three areas in the Call Restriction window, two of which offer configurable areas:
    - **Call Restrictions**:
        - *Multiple Assignment*: If a Phone is assigned to multiple people
            - Most Restrictive – Phone permission is set to the higher restriction level. When a user tries to make a call, they will be prompted to enter their extension and password. If their account does not allow the call to be routed, the user will get an error message.
            - Least Restrictive – Permissions are set to the lowest permission level.
        - *Binding*: If multiple people bind to a specific phone (Via MXIE):

- Most Restrictive – Phone permission is set to the higher restriction level. When a user tries to make a call, they will be prompted to enter their extension and password. If their account does not allow the call to be routed, the user will get an error message.
- Least Restrictive – Permissions are set to the lowest permission level.

- **Account Codes**: You can require that the user enter a code that represents a specific project. The length of the codes can be controlled by the administrator. Further, you can allow the user to enter any account code or specify which account codes are allowed.
- **Prompts**: This section is currently not available for any configuration options.



Call Restriction

Multiple Assignment
● Most Restrictive
○ Least Restrictive

Binding
● Most Restrictive
○ Least Restrictive

Account Codes

○ None
○ Any of 6 digits
● List of 6 digits
Edit List...

Prompts

Authentication
○ Beeps
● Voice

Account Codes
○ Beeps
● Voice

31.4 Applying Call Restrictions to User Groups

31.4.1 Defining User Profile Call Restriction options

The Policy section of the Call Restriction panel specifies the authentication policy that the MX-E enforces for all users to whom the profile is assigned. The MX-E defines three authentication policies: Phone, Phone and User, and User.

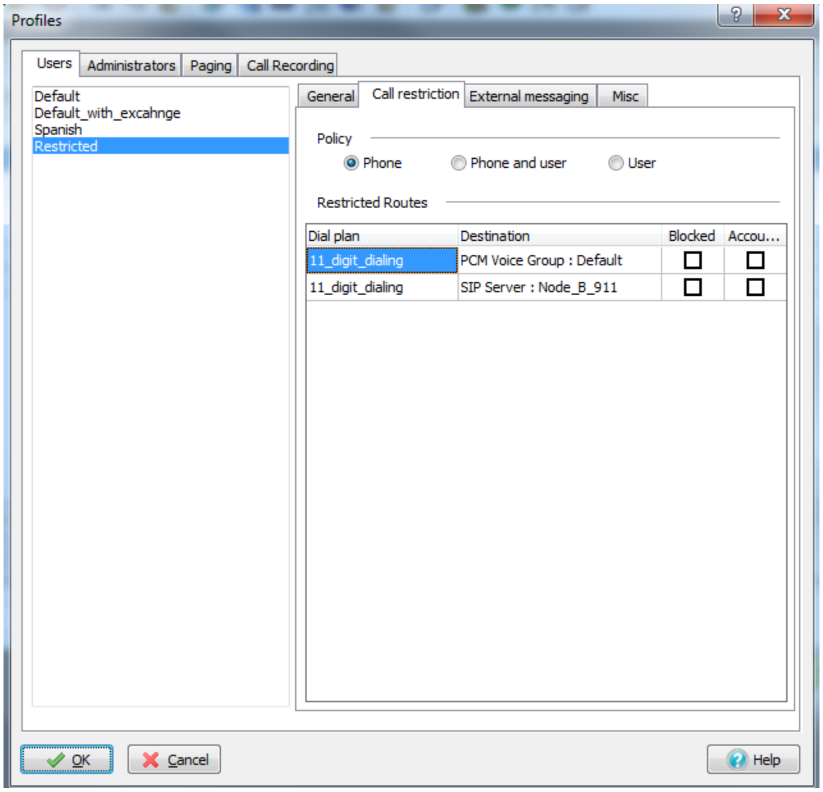
Phone: This policy uses the access authorization of the phone to determine which calls are sent. When you dial a number that is blocked by the phone's access authorization, the phone will not make the call regardless of the user’s access authorization. This is the most restrictive restriction policy.

Phone and User: This policy uses the access authorization of the phone and the user to determine which calls are sent. When you dial a number that is blocked by the phone’s access authorization, the phone will ask you to authenticate the call. If your user access authentication permits you to dial that number, the phone will complete the call. This allows a user to complete a call from a phone that is assigned to another user that does not have sufficient access to complete your call. If you place a call from MXIE, your MXIE credentials are assumed.

User: This policy uses the access authorization of the user to determine which calls are sent. When you dial a number on a phone with the User policy, it asks you to authenticate the call. If your user access authentication permits you to dial that number, the phone will complete the call. If you place a call from MXIE, your MXIE credentials are assumed.

31.4.2 Creating a User Profile with Restrictions

- From the Configure, User menu, select the Profiles button.
- Create new Profiles by right clicking in the profile name area, and selecting “new”
- Highlight the new user profile and click on the “Call Restriction tab, apply the required restriction options
- Click on OK to return to the User screen



Profiles

Default
Default_with_excahnge
Spanish
Restricted

Policy

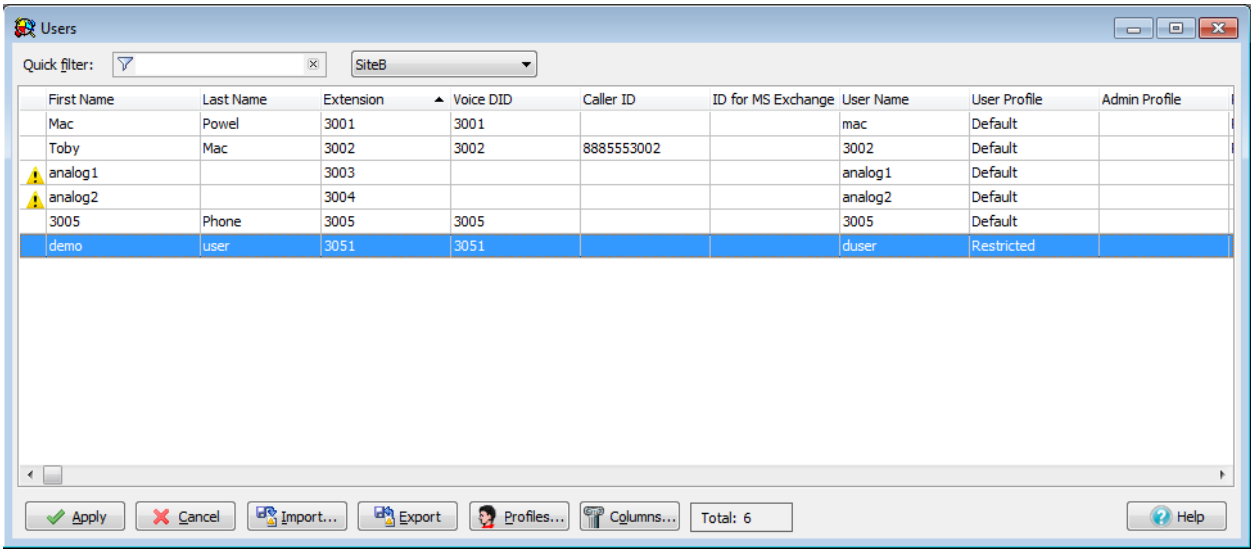
● Phone ○ Phone and user ○ User

Restricted Routes

Dial plan	Destination	Blocked	Accou...
11_digit_dialing	PCM Voice Group : Default	□	□
11_digit_dialing	SIP Server : Node_B_911	□	□

31.4.3 Assigning Users to Profiles that are restricted:

1. Modify user account and assign the proper profile, by either double clicking on the account, or right clicking once and selecting edit user. You may also assign a user profile to multiple users by selecting multiple users and right clicking then selecting edit users
2. Click on Apply to write your changes to the MX-E.



Users

Quick filter: SiteB

First Name	Last Name	Extension	Voice DID	Caller ID	ID for MS Exchange	User Name	User Profile	Admin Profile
Mac	Powel	3001	3001			mac	Default	
Toby	Mac	3002	3002	8885553002		3002	Default	
⚠ analog1		3003				analog1	Default	
⚠ analog2		3004				analog2	Default	
3005	Phone	3005	3005			3005	Default	
demo	user	3051	3051			duser	Restricted	

Total: 6

32. Creating an Automated attendant script

Auto attendants allow calls to be directed to an “IVR”. Then based on the caller’s actions, the call can be routed to a specific user, ACD group, or function. When creating an automated attendant, you need to first plan which ACD/ICC/Operator/Hunt Groups and extensions need to be called from within the Auto Attendant. Then decide which functions (i.e.: Dial by name, Transfer to an internal number, transfer to attendant, etc.) need to be called. Next, create a diagram that details which numbers or functions will be called, who will be at each extension, and what number needs to be dialed. The first step in configuring an Auto Attendant is to create a script. The script has three elements: the narrative section, the actions, and the properties. After an Auto Attendant script is created, it must be scheduled before it will function.

32.2 Creating an Auto Attendant:

The Auto Attendant panel configures extensions and DIDs for the MX-E automated attendants, to access this panel, select the Auto Attendants tab from Configure → Phone Services → Auto Attendants window.

Each row defines an auto attendant. Each column with a row configures an auto attendant parameter:

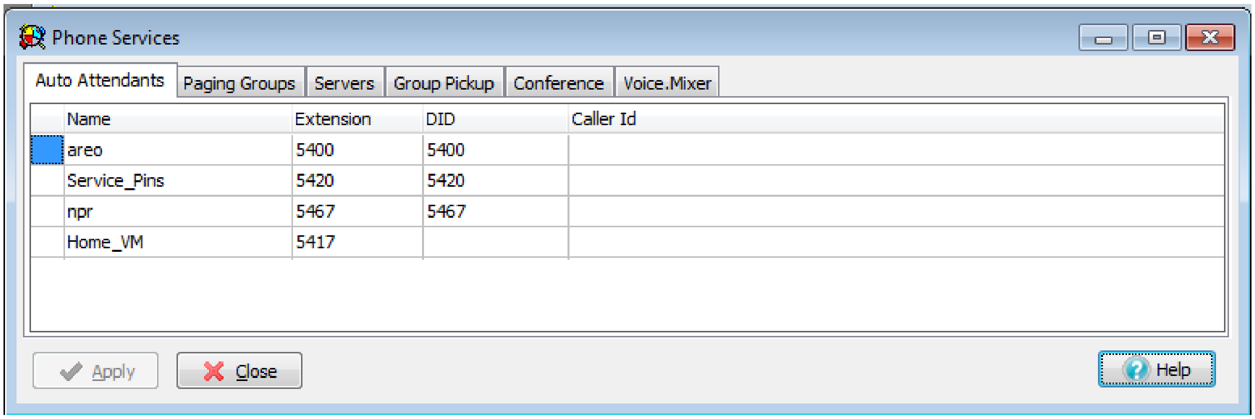
- Name: The name is an alphanumeric label that identifies the auto attendant. This name is used by other user interface windows, such as the Script Selection window.
- Extensions: This parameter specifies the extension number that contacts the auto attendant.
- DID: This parameter specifies the direct phone number that reaches the auto attendant. This column appears only when DID is enabled in the Dial Plan: Outside panel.

To add an auto attendant to your system, right click the mouse while pointing in the Auto Attendant table and select New.

To edit an auto attendant’s extension or DID, highlight the desired Auto Attendant in the panel, right click the mouse while pointing in the Auto Attendant table and select Edit.

Auto Attendant panel changes do not take effect until you press the Apply button. If you press the Cancel button before pressing Apply, all pending changes to Phone Services panels are disregarded. Pressing the Apply button saves all pending changes to every Phone Services panel.

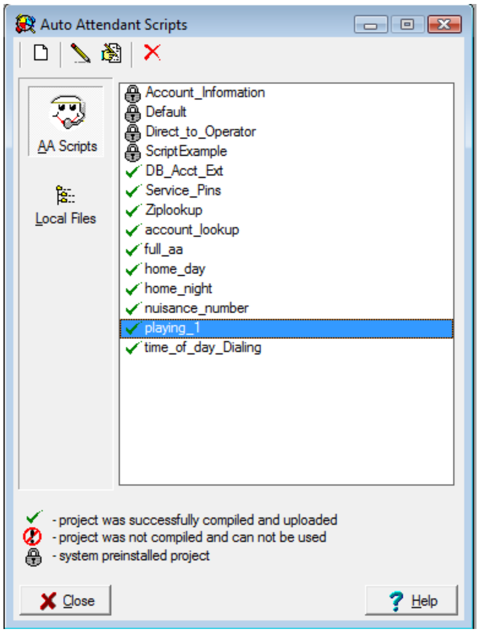
There can only be one AA with no DID assigned to it. This is the AA that will be used when no match is found for incoming DID's or no DID is presented to the MX-E



Name	Extension	DID	Caller Id
areo	5400	5400	
Service_Pins	5420	5420	
npr	5467	5467	
Home_VM	5417		

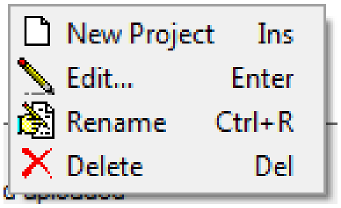
32.3 Creating the Script:

From Auto Attendant → Scripts you can create, edit or remove existing auto attendants. To edit a script either 2x click on the script or right mouse click and choose Edit. To create a new script click on the new button or right mouse click and choose New Project

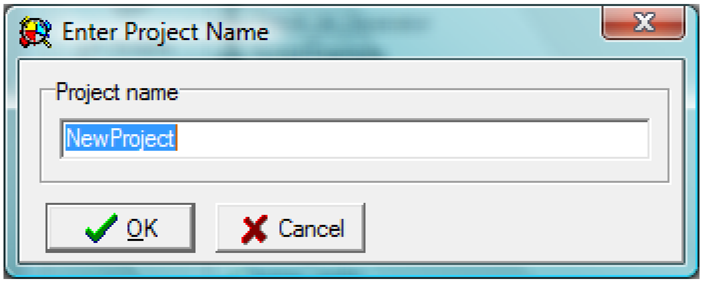


Account_Information
Default
Direct_to_Operator
ScriptExample
DB_Acct_Ext
Service_Pins
Ziplookup
account_lookup
full_aa
home_day
home_night
nuisance_number
playing_1
time_of_day_Dialing

✓ - project was successfully compiled and uploaded
- project was not compiled and can not be used
- system preinstalled project



Once you choose New Project you will be asked to give it a name.



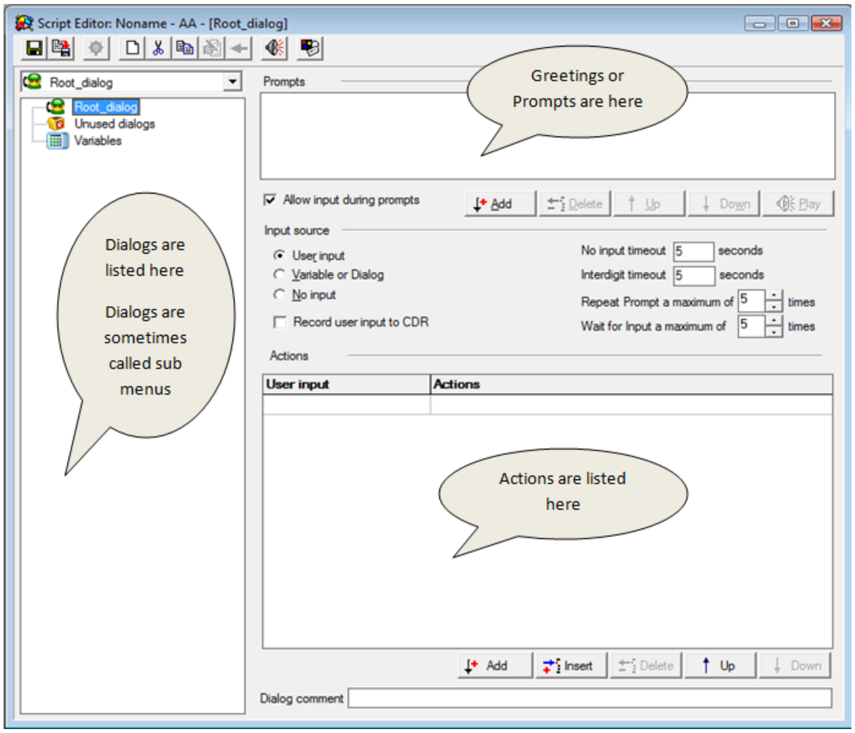
Project name: NewProject

Click OK, after providing a name for the script.

32.3.1 The Auto Attendant Screen

The Auto Attendant Screen is broken into 3 basic parts

- Prompts or Greetings
- Actions
- Dialogs



☑ Allow input during prompts

Input source

● User input
○ Variable or Dialog
○ No input
□ Record user input to CDR

No input timeout 5 seconds
Interdigit timeout 5 seconds
Repeat Prompt a maximum of 5 times
Wait for Input a maximum of 5 times

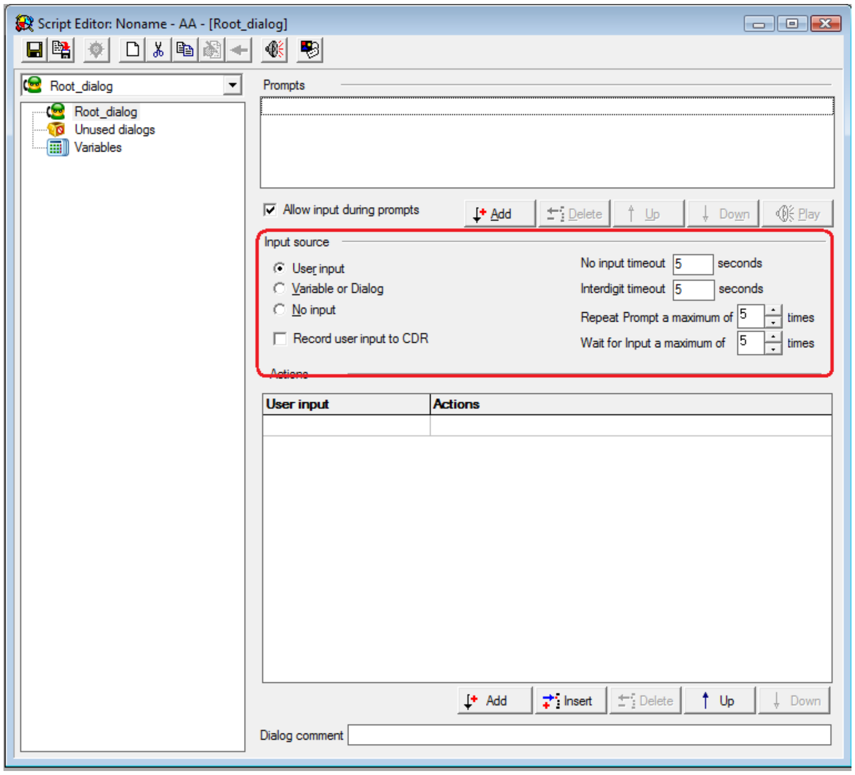
User input	Actions

This center section defines if and where the inputs will come from

- User input via DTMF
- A Variable
- Info collected and stored from other dialogs, or data sources
- No Input at all

Record the input into the CDR table.

This is helpful if looking to see how often a particular option is used, or running reports on how the scripts are being used



☑ Allow input during prompts

Input source

● User input
○ Variable or Dialog
○ No input
□ Record user input to CDR

No input timeout 5 seconds
Interdigit timeout 5 seconds
Repeat Prompt a maximum of 5 times
Wait for Input a maximum of 5 times

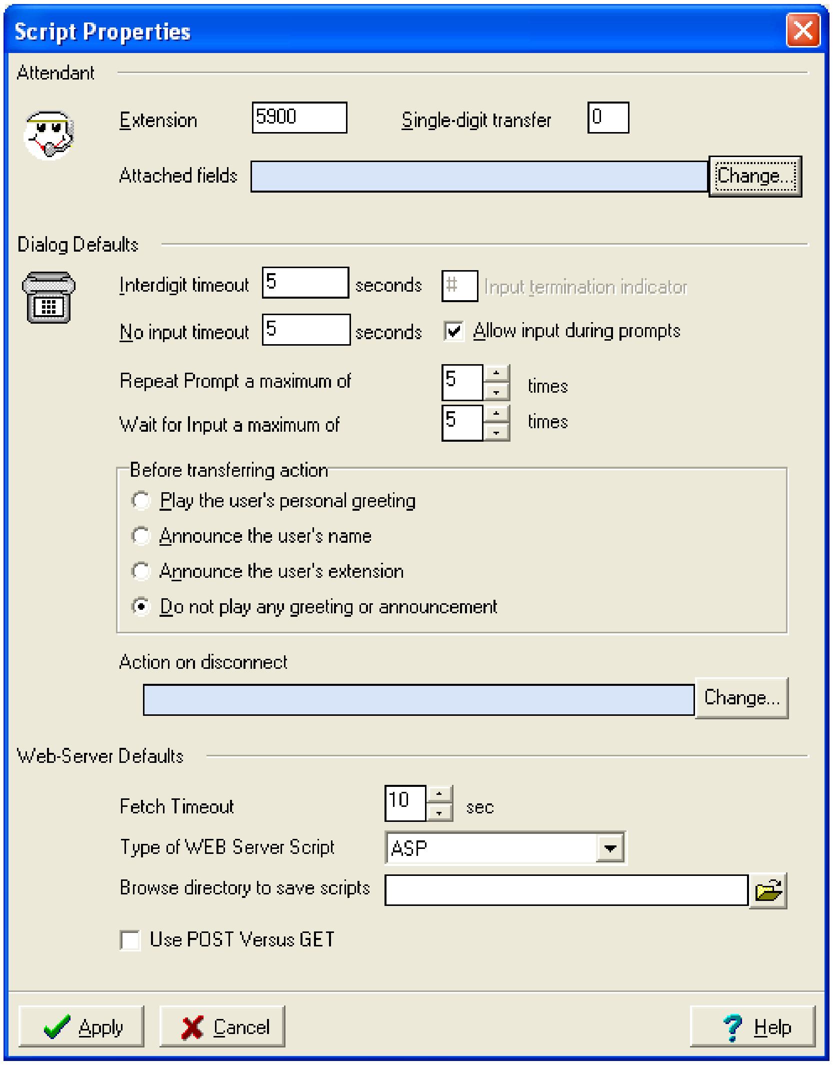
User input	Actions

Dialog comment

32.4 Script Properties:

1. In the “Script Editor” click on the “Script Properties” icon
2. Set the “Single Digit Transfer” to **0**

3. Set the “Attendant Extension” to extension number of the operator group then click OK.



Script Properties

Attendant

Extension: 5900 Single-digit transfer: 0

Attached fields:

Dialog Defaults

Interdigit timeout: 5 seconds □ # Input termination indicator

No input timeout: 5 seconds ☑ Allow input during prompts

Repeat Prompt a maximum of 5 times

Wait for Input a maximum of 5 times

Before transferring action
- ○ Play the user's personal greeting
- ○ Announce the user's name
- ○ Announce the user's extension
- ● Do not play any greeting or announcement

Action on disconnect:

Web-Server Defaults

Fetch Timeout: 10 sec

Type of WEB Server Script: ASP

Browse directory to save scripts:

□ Use POST Versus GET

32.5 Actions

Actions in a script do basic functions such as transferring a call or playing a message, however scripts may also transfer to other scripts allowing for very complex structures to be created. This allows individual departments to have and control their scripts while maintaining call routing between different departmental scripts.

For each of the inputs you can choose one of the following actions

- Goto

- Transfer
- Transfer to Attendant
- Transfer to VM
- Dial by Name
- Disconnect
- Web Server Request
- Assign to Variable
- Change Language
- Fax on Demand
- Repeat Prompt
- Wait for Input

32.5.1 Adding User Input Options

User inputs define the valid responses to a prompt. When a prompt presents a set of options to a caller, it provides the numbers which, when pressed, triggers specified actions. Valid user inputs include:

- **Digits and symbols**: This input is any combination of digits plus the * and # symbol. Single symbol input typically branches to other options, whereas multiple symbol input usually refers to a user extension. The '?' symbol can be used as a wild card, which is useful for branching to multiple extensions.
- **No input**: This condition is the case where the caller does not respond to the prompt within a specified time.
- **No match**: This condition is the case where the caller responds to the prompt, but the prompt does not match one of the other defined inputs.

32.5.2 Adding Actions

Right mouse click in the actions panel and choose add action. This will introduce a new line, and then click on the ellipse button to choose an action from the list presented.

- **Go to**
    - The Go to Action panel is the Action Editor panel that implements a Go to Action. The Go to Action panel displays a data entry box that specifies the dialog that will receive control of the script.

- **Transfer**
  - The Transfer Action panel is the Action Editor panel that implements a Transfer Action. Transfer actions transfer the caller to the extension or phone number specified in the Destination section. The extension or phone number is may be listed directly, derived from a previously executed dialog, or passed as a variable from a web script. This action also offers routing and message options if the transfer is not successful.
  - Prompt Options
  - In addition to the greeting prompt that is available for all types of actions, you can also choose a prompt that will be played if the system is unable to transfer the caller. Select the On failure tab and press the Add button to select a WAV file.
  - Before transferring
    - This field allows you to choose an audio introduction that is played before the caller is transferred. The default setting for this option is configured in the Script Properties window.
  - Destination
    - This field selects the destination to where the caller is transferred.
    - Extension or phone# routes the caller to the specified user.
    - Variable or dialog routes the user on the basis of the value of the specified script variable or input passed from a previously executed dialog.
  - Call Attached Fields
    - This field specifies the name and value of Call Attached variables assigned to the call before it is transferred to the specified destination. Press the Change button to access the Attached Fields panel for selecting these variables.
  - When ACD Queue Priority is selected, the call corresponding field determines the initial queue position when the call is routed to its destination.
    - Call 'Priority Values' of 0 to 5 only impact the priority of a call within its queue (unchanged from previous firmware

releases). Call 'Priority Values' of 6 to 10 impact the priority of a call across all queues that an agent is logged into allowing for a customer to configure a VIP queue where the waiting calls take precedence over all other call groups even when there are calls in other queues that have been waiting longer.

- On Failure
    - This field determines the script behavior if the MX-E is unable to perform the transfer.
    - Go to transfers the caller to the dialog that is specified in the accompanying entry box.
    - Disconnect terminates the call.
    - Transfer to Attendant sends the caller to the extension specified in the Script Properties window.

- **Transfer to Attendant**
    - The Transfer to Attendant Action panel is the Action Editor panel that implements a Transfer to Attendant Action. Transfer to Attendant actions transfer the caller to the attendant extension designated by the Script Properties panel.
    - Call Attached Fields: This field specifies the name and value of Call Attached variables assigned to the call before it is transferred to the specified destination. Press the Change button to access the Attached Fields panel for selecting these variables.
- **Leave Voicemail**
    - The Leave Voicemail Action panel is the Action Editor panel that implements a Transfer to VM Action. Transfer to VM actions transfer the caller to a specified user’s voice mail recorder.
    - Panel parameters specify the user that will receive the voice message.
    - Destination
        - This field selects the destination to where the caller is transferred.
        - Extension or phone# routes the caller to the specified user.

        - Variable or dialog routes the caller based on the value of the specified script variable or the input passed from a previously executed dialog.
    - On Failure
        - This field determines the script behavior if the MX-E is unable to perform the transfer.
        - Go to transfers the caller to the dialog that is specified in the accompanying entry box.
        - Disconnect terminates the call.
        - Transfer to Attendant sends the caller to the extension specified in the Script Properties window.
- **Dial By Name**
    - The Dial by Name Action panel is the Action Editor panel that implements a Dial by Name Action. Dial by Name actions transfer the call to the user that is requested by the caller.
    - Prompt Options
        - In addition to the greeting prompt that is available for all types of actions, you can also choose a prompt that will be played when the transfer takes place if the user name cannot be found or if the system is unable to transfer the caller. Select the appropriate tab and press the add button to select a WAV file.
    - Name Lookup
        - This option determines the method of searching for the user.
        - When Search by first name is selected, the auto attendant prompts the caller to enter the first three letters of the user’s first name.
        - When Search by last name is selected, the auto attendant prompts the caller to enter the first three letters of the user’s last name.
        - When Ask caller is selected, the auto attendant asks the caller to choose between a first name search and a last name search.
    - Number of times a caller can begin new search

        - This option determines the number of unsuccessful searches that the system will perform. After performing these searches, the system will either go to another dialog, disconnect the call, or call the attendant defined on the Script Properties window.
    - Before transferring
        - This option allows you to choose an audio introduction that is played before the caller is transferred. This introduction is played after the On Transfer prompt (selected at the top of this window). The default setting for this option is configured in the Script Properties window.
        - Speak the Names of People Found by the Search
        - If this option is selected, the auto attendant plays the names of users that meet the search criteria and have configured their recorded name when setting up their mail box. The auto attendant plays these recorded names after a successful search and before the On Transfer prompt.
    - On Failure to Transfer
        - This field determines the script behavior if the auto attendant is unable to perform the transfer.
        - Go to transfers the caller to the dialog that is specified in the accompanying entry box.
        - Disconnect terminates the call.
        - Transfer to Attendant sends the caller to the extension specified in the Script Properties window.
        - Note: If the end users Name/Extension is not recorded their extension will not be included.
- **Disconnect**
    - The Disconnect Action panel is the Action Editor panel that implements a Disconnect Action. Disconnect actions terminates calls that are connected to the auto attendant. The only

configurable component on the Disconnect Action panel is the message prompt selection list at the top of the panel.

- **Web Server Request**
    - The Web Server Request Action panel is the Action Editor panel that implements a Web Server Request Action. Web Server Request actions executes a web script located on a specified web server. Parameter values are passed from the web script to the AA script for use in the dialog.
    - Web Server Request requires an IVR license
    - Request Panel
        - The Request panel, specifies the web server that executes the web script and the parameter values that the action passes to the web script.
        - Request panel parameters include:
            - URL: The URL data field lists the name and location of the web script.
            - Script Parameter Table: This list identifies the parameters passed by the MX-E to the web script. Each row corresponds to one web script parameter. Table fields include:
            - Script Parameter: This column lists the names of the parameters that are passed to the web script. These names must match the parameter names defined in the web script.
            - Variable: When this field is marked, the value of the Variable Name or Value field is a variable. When this field is not marked, the value of the Variable Name or Value is a constant value that is passed directly to the web script.
            - Variable Name or Value: This field specifies the value of the parameter passed to the web script.

  - Fetch Timeout: This field specifies the period that the dialog waits for a response from the web script. The action transfers to the dialog specified for failure conditions if a response from the web script is not received.
  - Use Post Method: When this field is selected, the MX-E encrypts the variable values that are sent to the web server.
- Response Panel
  - Script parameter: This column lists the names of web script parameters. The value of these parameters are passed from the web script to the AA dialog action. These names must match the parameter names defined in the web script.
  - Variable name: This column lists the AA action variable to which the web script parameter is passed.
- Script Panel
  - The Script panel, displays the parameter values passed from the web script to the AA dialog action, provides a tool for creating a web script file template, which can be edited to create the web script.
  - Script Type: This parameter specifies the scripting language used for creating the template.
  - Save generated script as: This parameter specifies the name and network location where the MX-E stores the template. Press the browse button to view your file structure and enter a location through a point and click operation with the mouse.
- After Execution Go To parameter specifies the next dialog that the script executes if the web script runs successfully and all response parameter settings are valid.
- On Failure Go To parameter specifies the next dialog that the script executes if the web script does not run successfully or if all response parameter settings are not valid.

- Assign Variable
    - The Assign to Variable Action panel is the Action Editor panel that implements a Assign to Variable Action. Assign by Variable actions assign values to Auto Attendant script variables, which are then passed to the web script or used in the AA script.
    - Assign Variable requires an IVR license, and is not part of the basic course
    - Assign to Variable specifies the name of the variable, as defined by the Variable Definition Table. A drop down menu lists the available variable names.
    - Variable specifies the type of value that is assigned to the variable by this action. When this field is marked, the value of the Variable Name or Value field is a system variable or a value passed by a previously executed dialog. When this field is not marked, the value of the Variable Name or Value is a constant value that is passed directly to the web script.
    - Variable Name or Value specifies the new value of the variable.
    - The Go To field specifies the dialog that receives control of the script after the variables settings are changed.
    - The On failure field specifies the dialog that receives control of the script if the variable settings cannot be changed.
- Change Language
    - The Change Language Action panel is the Action Editor panel that implements a Change Language Action. Change Language actions specify the language spoken by the auto attendant. The set of available languages depend on the Language Packs previously installed on your system .
    - Change Language action panel parameters include:
    - Language: This field specifies the language that is spoken by the auto attendant after this action is executed.
    - then Go to: This field specifies the dialog that receives control of the script after the language setting is changed.
- Fax On Demand

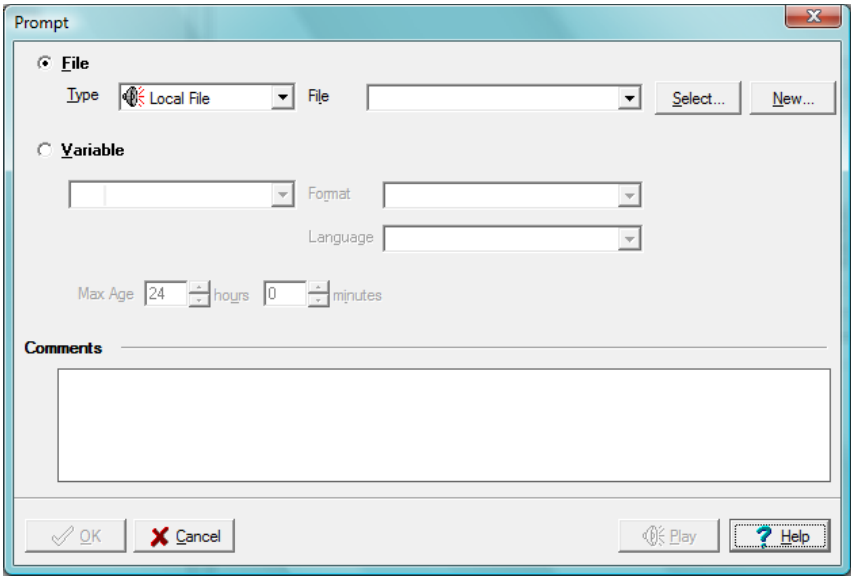
  - The Fax on Demand Action panel is the Action Editor panel that implements a Fax on Demand Action. Fax on Demand sends a specified graphics file as a fax transmission to one or more listed extensions, phone numbers, or addresses
  - FOD requires an IVR License, and is not part of the basic course
  - Fax File Location
    - You can designate any tif file accessible to your MX-E as a fax. This section of the panel specifies the location of the tif file sent by this action:
    - URL routes the caller to the specified user.
    - Variable routes the caller based on the value of the specified script variable or the input passed from a previously executed dialog.
  - Fetch Timeout field specifies the period that the dialog waits for the specified destination to make the tif file available. The action transfers to the dialog specified for the failure condition if the tif file is not available within this period.
  - Send to
    - This table lists the recipients of the fax. Each line in the table specifies the phone number or address of one recipient. Table parameters include:
    - Variable specifies the type of value that specifies the phone number or IP address. When this field is marked, the recipient destination value is a variable. When this field is not marked, the recipient destination value is fixed.
    - Value specifies the recipient destination.
  - After Execution Go To
    - This parameter specifies the next dialog that the script executes if the action successfully sends the fax message.
  - On Failure Go To
    - This parameter specifies the next dialog that the script is unable to send the fax because the tif file did not become available before expire of the Fetch Timeout.

- **Repeat Prompt**

  - The Repeat Prompt Action panel is the Action Editor panel that implements a Repeat Prompt Action. Repeat Prompt actions repeat the dialog prompt and wait for caller input. The only configurable component on the Repeat Prompt action panel is the message prompt selection list at the top of the panel.
  - Repeat prompt can also be used as “Play a prompt”
- **Wait for Input**
  - The Wait for Input Action panel is the Action Editor panel that implements a Wait for Input Action. Wait for Input actions wait a specified period for further caller input. The only configurable component on the Repeat Prompt action panel is the message prompt selection list at the top of the panel.

32.6 Adding the Prompt:

Either Right click in the “Prompts” area and select “Add”, or click on the Add button



Prompt

● File

Type: Local File

○ Variable

Max Age 24 hours 0 minutes

Prompts

- File prompts are specified by selecting a File Prompt Type in the Type data entry field and the specific file in the File field.
  - Local files and Text to Speech files can be specified through a drop down menu or by pressing the Select button located to the right of

the file field. You can also create new Local or Text to Speech files by pressing the New button.

  - System prompts are specified by accessing the drop down menu on the file field.

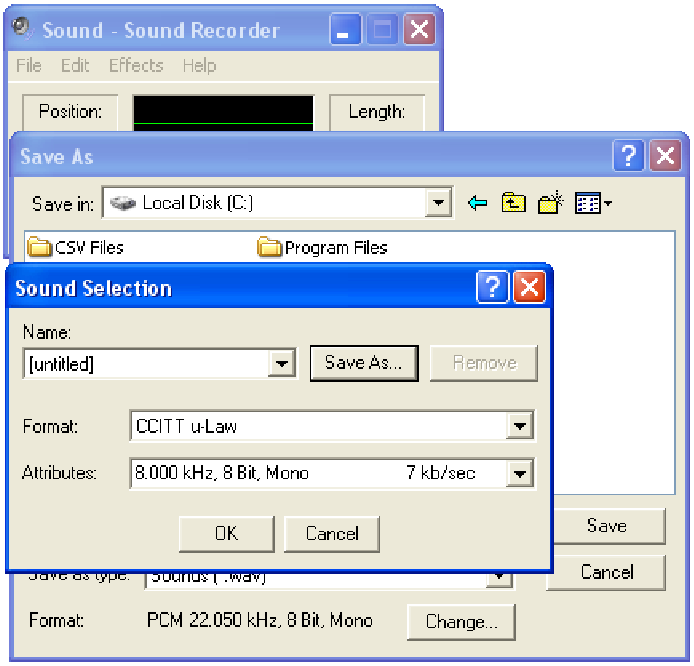
- Internet prompts are specified by entering a URL in the file field. If the internet file has been placed into the MX-E internal memory within the time specified by the Max Age parameter, that file will be used as the prompt; otherwise, the MX-E will download the specified file from the internet.
- Variable prompts are specified by selecting the variable in the data field directly below the Variable radio button. After selecting the variable, you can determine how the variable contents will be spoken by selecting a Format; available formats depend on the selected variable. Examples of format include "AS_INTEGER" (variable is spoken as an integer number), "AS_DATE" (variable is spoken as a calendar date), or "AS_SPELLING" (each letter of the variable text is spoken). If REAL_TIME_TTS is selected, you must enter a language in the Language field; this specifies the language in which the text will be spoken.

32.6.1 Creating the Prompt – Option 1:

32.6.1.1 Using Sound Recorder to create a local file:

System prompts, Music on Hold and voice mail messages are standard 8 bit wav files. You can use any program you wish to record WAV files for upload to the MX-E as long as it can save the file in the following format "CCITT u-Law 8.000 kHz, 8 Bit". The Microsoft Sound Recorder that is included with all versions of Windows prior to Windows® Vista® can save files in this format.

1. Click on the Start Button on your desktop
2. Select "All programs" then select "Accessories" then Launch "Sound Recorder"
3. Record the message
4. Then in Sound Recorder click on "File" and select "Save As"
5. Set the location to your desktop and set the file name to **Main**
6. Click on the "Change" button and change the format to **CCITT u-Law**
7. Set the attributes field to **8.000 kHz, 8 bit, Mono**.

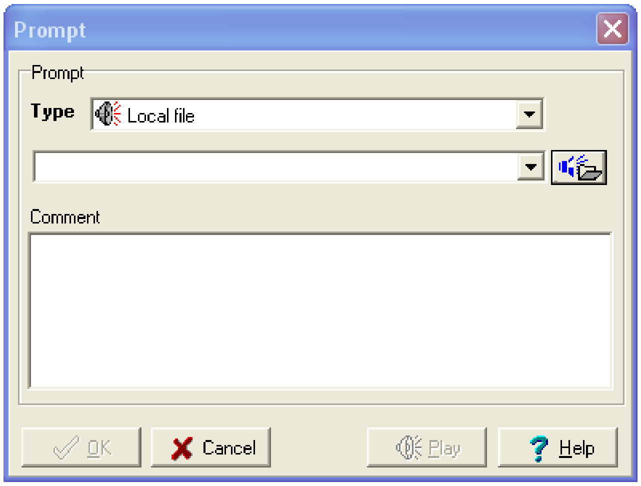


8. Click on “OK” then “Save”

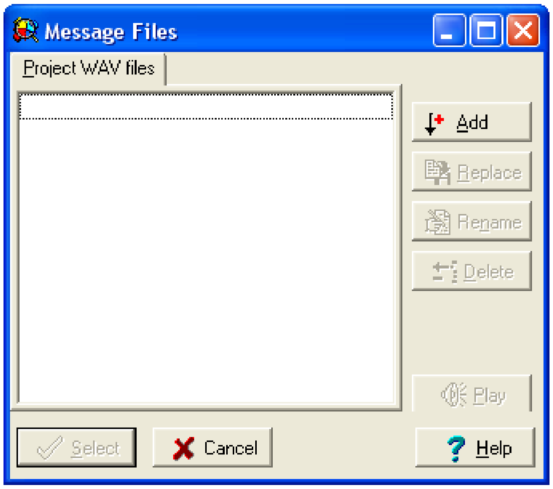
Note: *Files saved at too high or too low a volume will have poor playback quality.*

32.6.1.2 Selecting a local Wave File:

1. When the “Prompt” window opens set the “Type” field to **Local file**.
2. Click on the “Message Files” icon New... in the “Prompt” window.
3. In the “Message Files” window click on the “Add” button.



Type: Local file



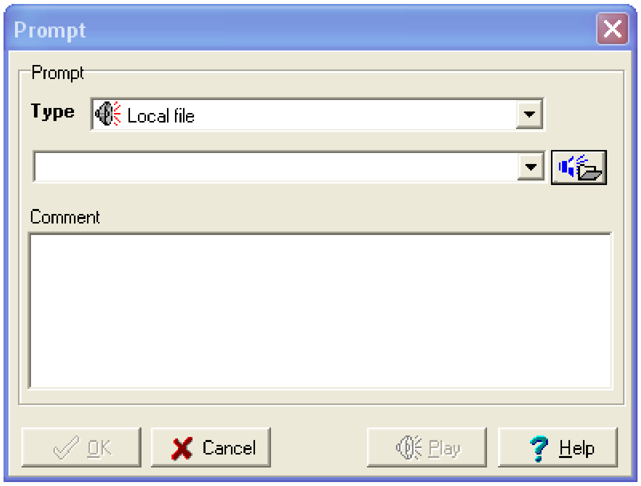
4. Select the file from your computer and click “Open”
5. Click “Select” then click “OK”

32.6.2 Record Message in your voicemail and upload – Option 2:

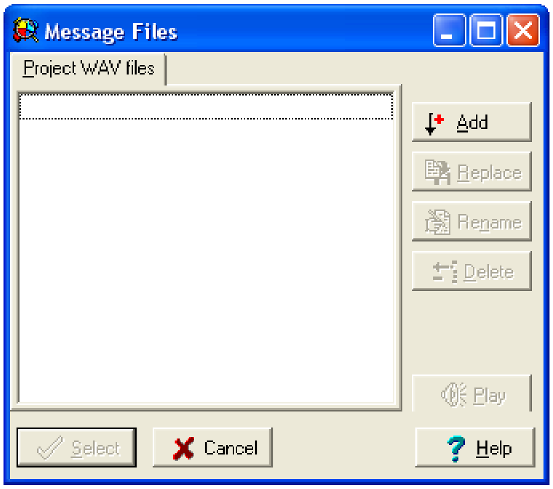
1. Leave a message in a voicemail
2. Download the message via MXIE to your desktop

32.6.2.1 Selecting a local Wave File:

1. When the “Prompt” window opens set the “Type” field to **Local file**.
2. Click on the “Message Files” icon New... in the “Prompt” window



Type: Local file

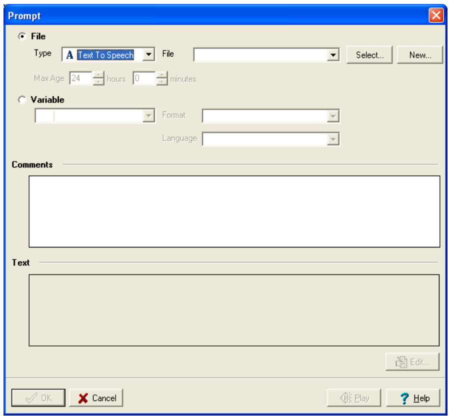


3. In the “Message Files” window click on the “Add” button.
4. Select file from computer and click “Open”

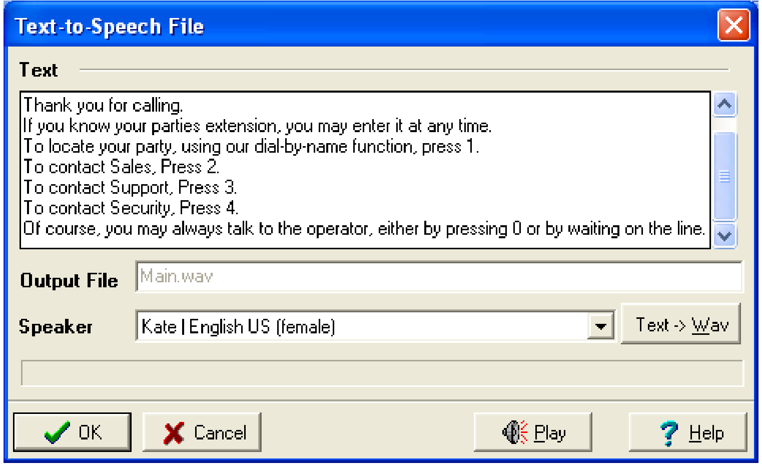
5. Click “Select” then click “OK”

32.6.3 Text to Speech– Option 3:

1. From the Prompt menu, select Text to Speech
2. Click on **New**
3. Change the name for the output file.
4. Enter the script that you want to generate
5. When you are done, click on the **Text** -> **Wav** button
6. Optional – Click on **Play** to listen to your output file
7. When you are satisfied, click on **OK** to return to the previous menu



● File
Type: Text To Speech
Max Age 24 hours 0 minutes
○ Variable



Text:
Thank you for calling.
If you know your parties extension, you may enter it at any time.
To locate your party, using our dial-by-name function, press 1.
To contact Sales, Press 2.
To contact Support, Press 3.
To contact Security, Press 4.
Of course, you may always talk to the operator, either by pressing 0 or by waiting on the line.

Output File: Main.wav

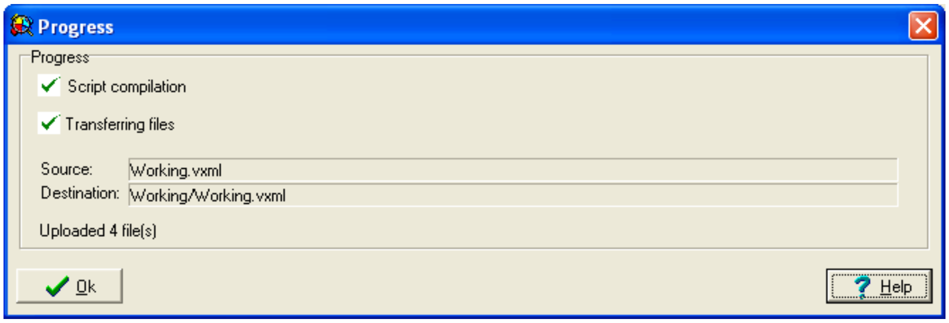
Speaker: Kate | English US (female)

32.7 Saving the Script:

32.7.1 Saving and Uploading the Script:

1. In the “Script Editor” click on the “Save” icon 💾

2. Your script should compile and show you a message indication it compiled successfully
3. Click "OK" then close the "Script Editor"



Progress

Progress

✓ Script compilation

✓ Transferring files

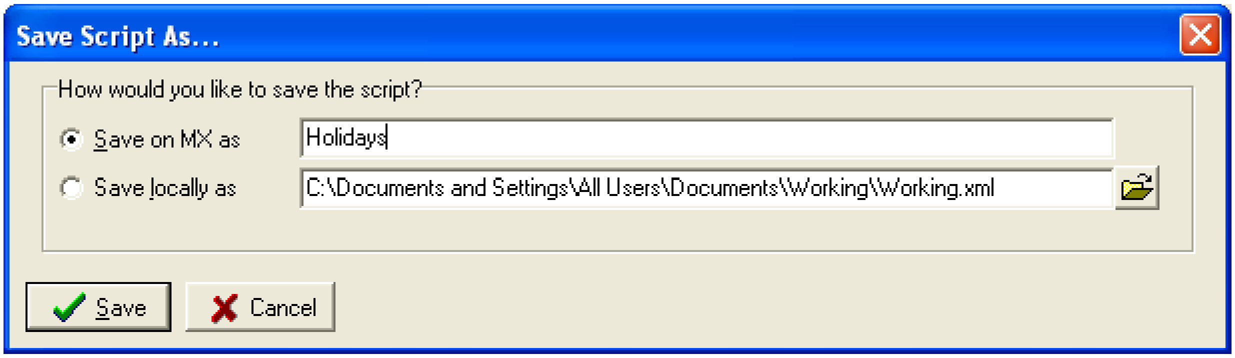
Source: Working.vxml

Destination: Working/Working.vxml

Uploaded 4 file(s)

32.7.2 Saving a script with a new name:

1. In the "Script Editor" click on the "Save As" icon
2. Put a check in the Save As function and Change the Name of the script to Holidays.



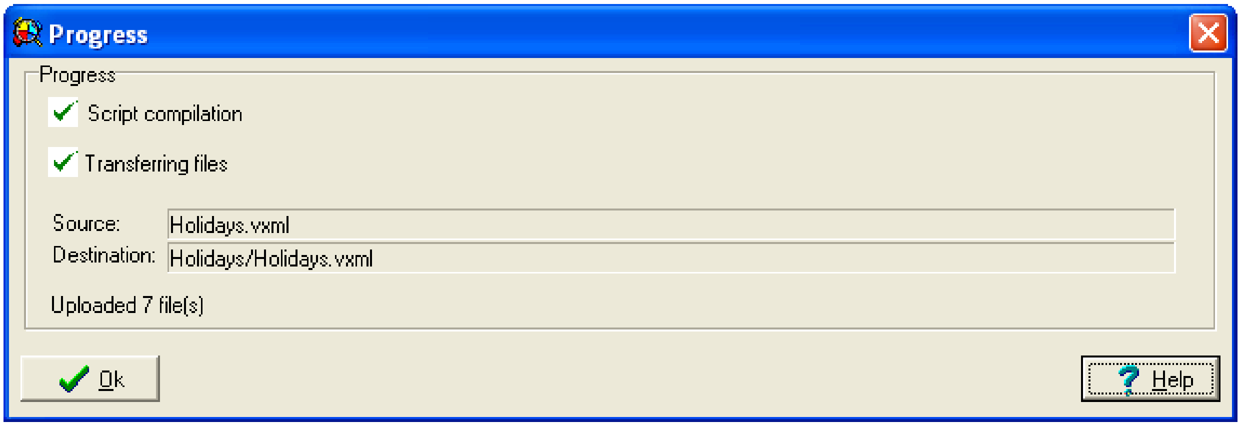
Save Script As...

How would you like to save the script?

● Save on MX as: Holidays

○ Save locally as: C:\Documents and Settings\All Users\Documents\Working\Working.xml

3. The files will be uploaded using the new filename.
4. After the script has been renamed, it can be modified to create a new script.



Progress

Progress

✓ Script compilation

✓ Transferring files

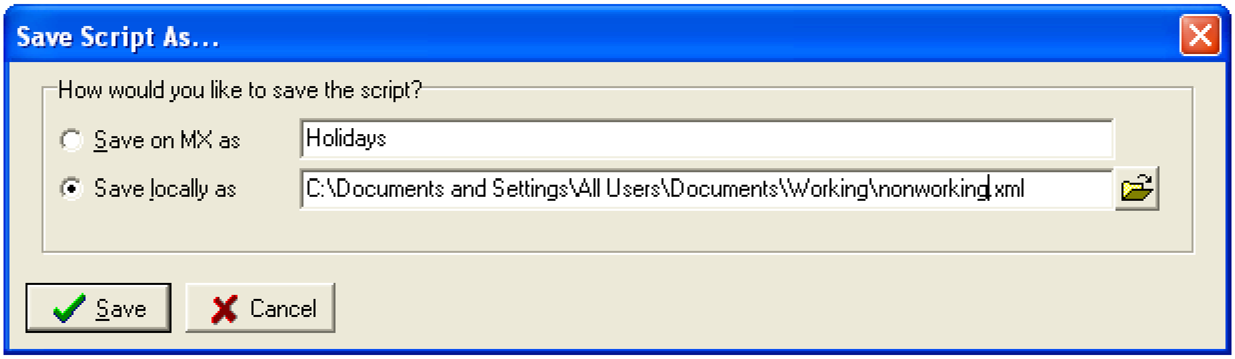
Source: Holidays.vxml

Destination: Holidays/Holidays.vxml

Uploaded 7 file(s)

32.7.3 Saving the Script to the local computer:

1. In the "Script Editor" click on the "Save As" icon
2. Put a mark in the Save Locally as button and change the name to Main
3. Click on Save to save the file to the local computer



Save Script As...

How would you like to save the script?

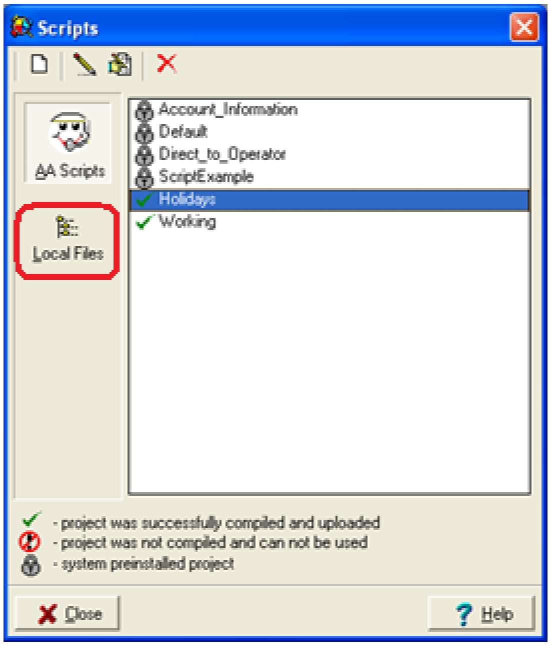
○ Save on MX as: Holidays

● Save locally as: C:\Documents and Settings\All Users\Documents\Working\nonworking.xml

NOTE!	When saving a script, insure that the full absolute path is entered.

32.7.4 Uploading a Local File:

1. From the Auto Attendant Pull Down menu, select Scripts:
2. Click on the Local Files button.



✓ - project was successfully compiled and uploaded
- project was not compiled and can not be used
- system preinstalled project

3. Browse to the Location where the files are stored
4. Select the desired file and click on Open
5. Save and upload the file:

   – In the "Script Editor" click on the "Save" icon 💾

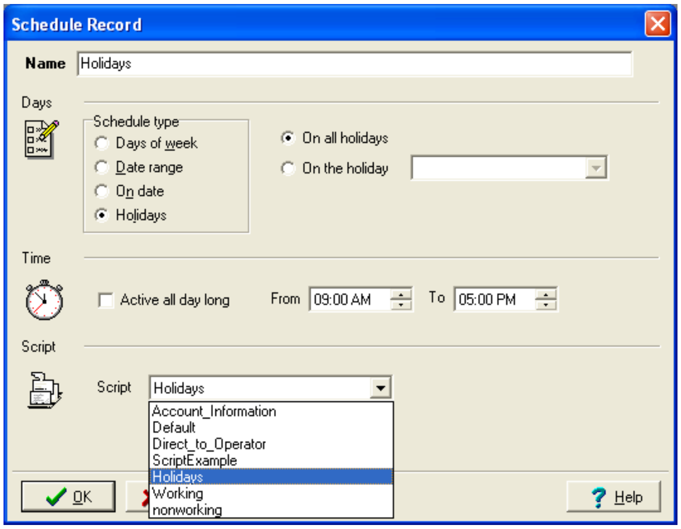
32.8 Scheduling Auto-Attendant:

The final step is to schedule the auto-attendant and assign scripts based on date and time. Schedules are set within the Auto Attendant →Schedule window. All the auto-attendants that have been defined with the Phone Services window are listed on the left side of the schedule window. You can assign scripts by highlighting the auto-attendant of choice on the left and adding schedules on the right. Much like the dial plan, the MX-E looks at auto-attendant schedules from top to bottom. You can define different times of the day and days of the week, as well as holidays, and assign different scripts for each.

NOTE: Failure to assign a schedule will result in the call being dropped by the MX-E when sent to the auto attendant.

32.8.1 Scheduling a Script to run on Holidays:

1. From the "Auto Attendant" menu select "Schedule"
2. Click on New
3. Provide a name for the schedule
4. In the Days Field, Select Holidays
    - Choose a particular holiday, or all holidays
    - Holidays are programed under Configure → Holidays
5. Select a time for this schedule to run on the holiday
6. Click on OK



Schedule Record

Name: Holidays

Days

Schedule type
○ Days of week
○ Date range
○ On date
● Holidays

● On all holidays
○ On the holiday

Time

□ Active all day long From 09:00 AM To 05:00 PM

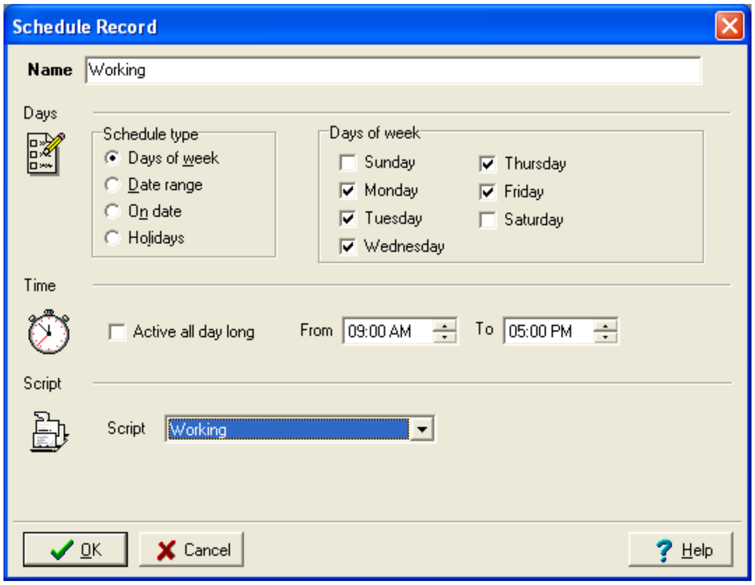
Script

Script: Holidays

32.8.2 Scheduling a Script to run During Working Hours:

1. From the "Auto Attendant" menu select "Schedule"

2. Click on New
3. Provide a name for the schedule
4. In the Days Field, Select Days this schedule should run
5. In the Time Field, Select the time that this schedule should be enabled
6. In the Scripts Field, Select correct script you wish to run on the programed days and hours
7. Click on OK



Schedule Record

Name Working

Days

Schedule type
- ● Days of week
- ○ Date range
- ○ On date
- ○ Holidays

Days of week
- □ Sunday
- ☑ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday
- □ Saturday

Time

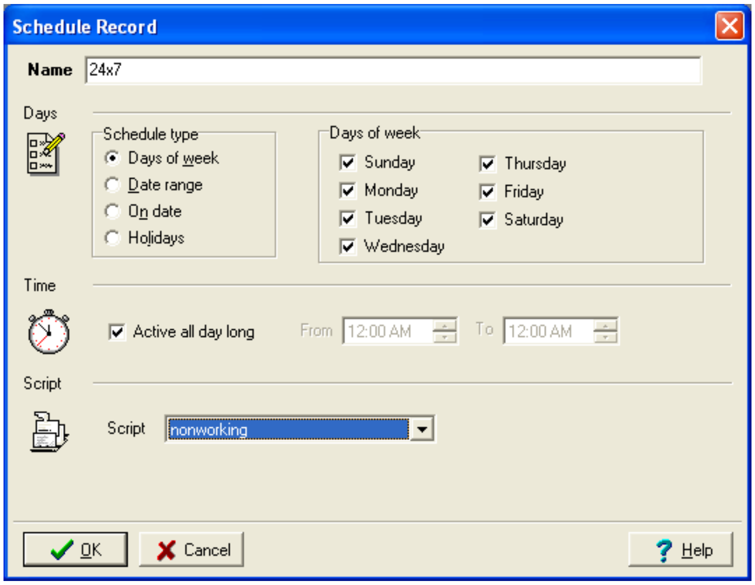
□ Active all day long From 09:00 AM To 05:00 PM

Script

Script Working

32.8.3 Scheduling a Script to run During Non-Working Hours:

1. From the “Auto Attendant” menu select “Schedule”
2. Click on New
3. Provide a name for this schedule
4. In the Days Field, Select all days of the week (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday)
5. In the Time Field, check Active all day
6. In the Scripts Field, Select correct script you wish to run on the programed days and hours
7. Click on OK



Schedule Record

Name 24x7

Days

Schedule type
● Days of week
○ Date range
○ On date
○ Holidays

Days of week
☑ Sunday
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday

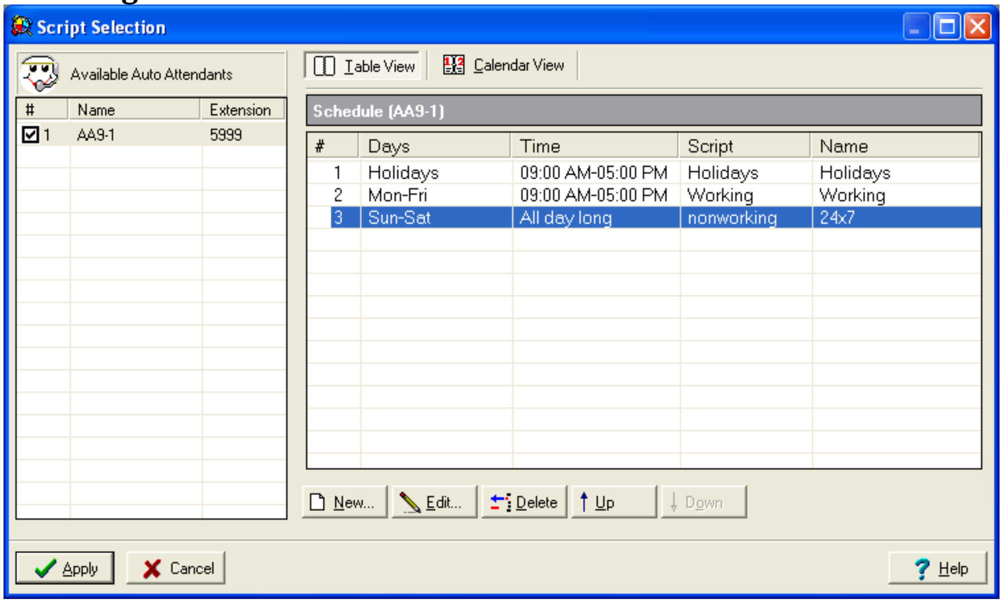
Time

☑ Active all day long From 12:00 AM To 12:00 AM

Script

Script nonworking

32.8.4 Viewing the Finished Schedule:

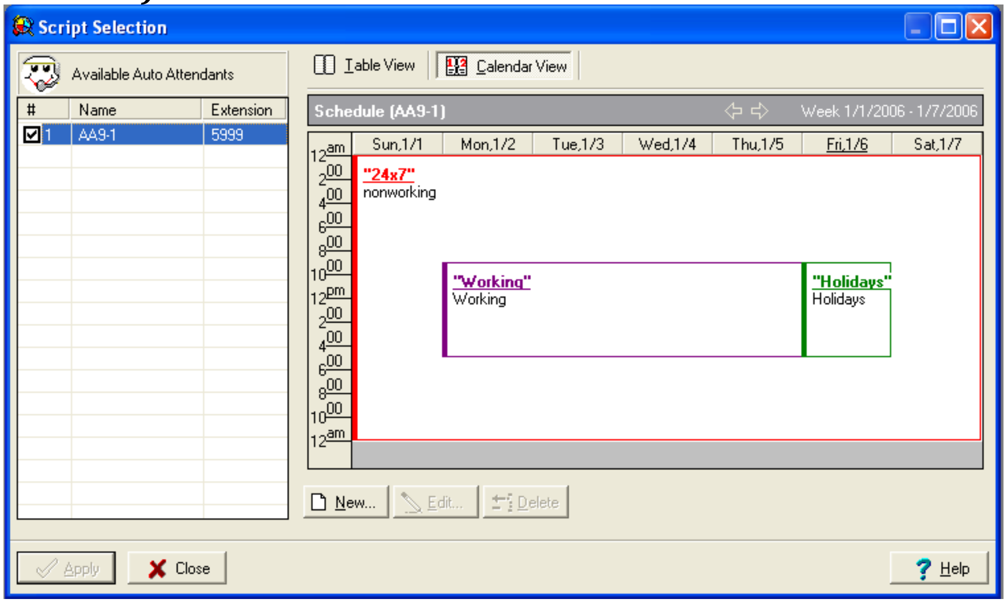


#	Name	Extension
☑ 1	AA9-1	5999

Schedule (AA9-1)

#	Days	Time	Script	Name
1	Holidays	09:00 AM-05:00 PM	Holidays	Holidays
2	Mon-Fri	09:00 AM-05:00 PM	Working	Working
3	Sun-Sat	All day long	nonworking	24x7

32.8.4.1 *Viewing the Schedule from the Calendar View: (Error! Reference source not found.)*



#	Name	Extension
☑ 1	AA9-1	5999

Notice how you can set different scripts to run for the same extension/DID according to the time of day, name of the day or even on holidays. Scripts are evaluated from the top down.

33. Digital Certificates

33.2 Digital Security Certificates

Zultys Mobile Communicator™, Outlook Communicator, and SalesForce Integration use a Transport Layer Security (TLS) secured connection between the mobile device and your MX-E. A digital security certificate is required to enable a connection to the MX-E. A security certificate is a digital document assuring users that their transmission is encrypted, secure and connected to the right server, and it also informs the company that the callers are who they claim to be.

If that certificate has been signed and approved by an independent certification authority (CA) then the Zultys mobile client software accepts the two endpoints as legitimate and proceeds with the connection.

Alternatively, the digital security certificate can be self-signed by the company and is not validated by a third-party certification authority. In essence, a self-signed certificate conveys the message, "You can trust me", but forces the user to acknowledge and accept that trust whenever connecting to the PBX.*

* Optionally, you can e-mail to the user a copy of the certificate and have the user install it on his/her mobile phone. In so doing, the mobile phone will confirm the MX-E server's identity eliminating this step for the user. Please refer to your mobile devices product documentation for further details of how to store a self-signed certificate.

Of the two types of certificates, the third-party certificate from a certificate authority is preferred.

Section 33.3 describes how to generate a security key

Section 33.4 describes how to generate and install a self-signed certificate

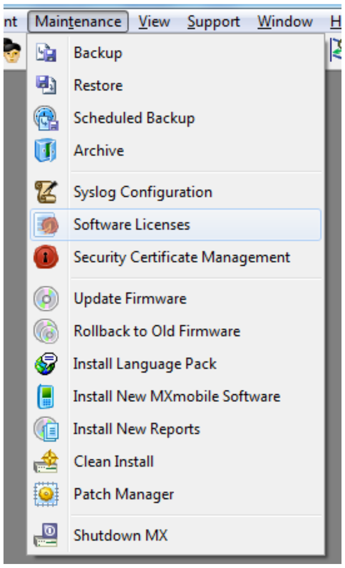
Section 33.5 describes how to generate a request for a certificate from a certificate authority

Section 33.6 describes how to install a certificate received from a certificate authority.

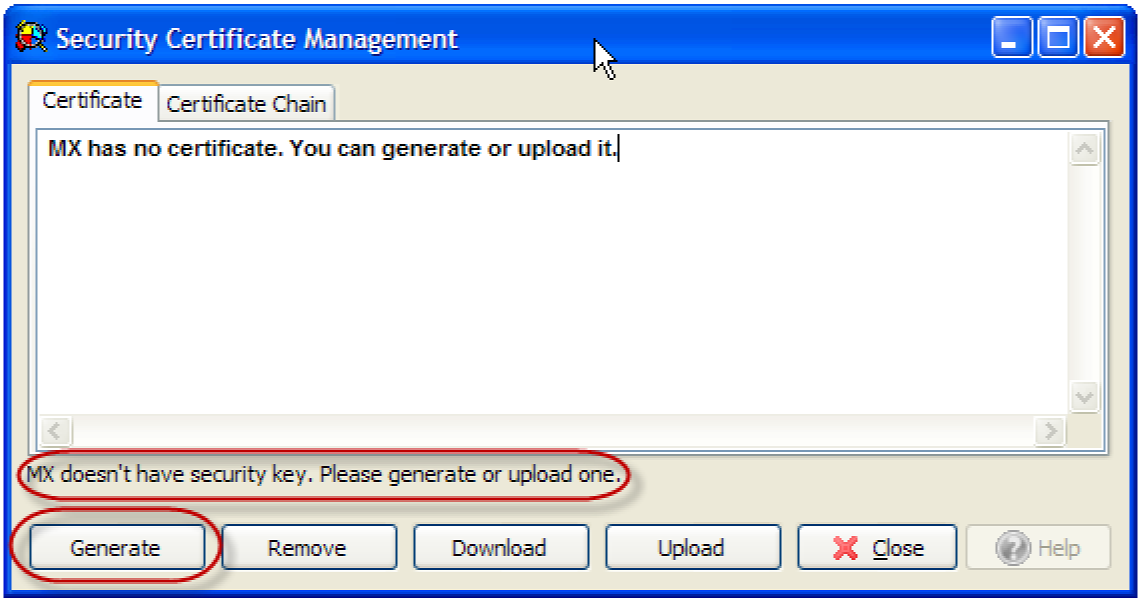
33.3 Generating a Security Key

Generating a security Key is a precursor to generating any one of the certificate types.

1. Maintenance -> Security Certificate Management

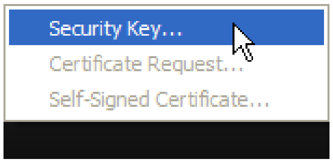


2. Generate -> Security Key
   Click on *Generate*, and select *Security Key* from the dropdown list

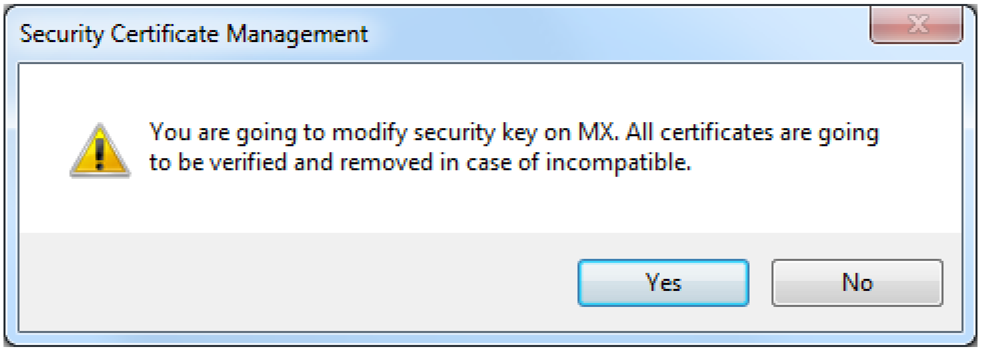


MX has no certificate. You can generate or upload it.

MX doesn't have security key. Please generate or upload one.



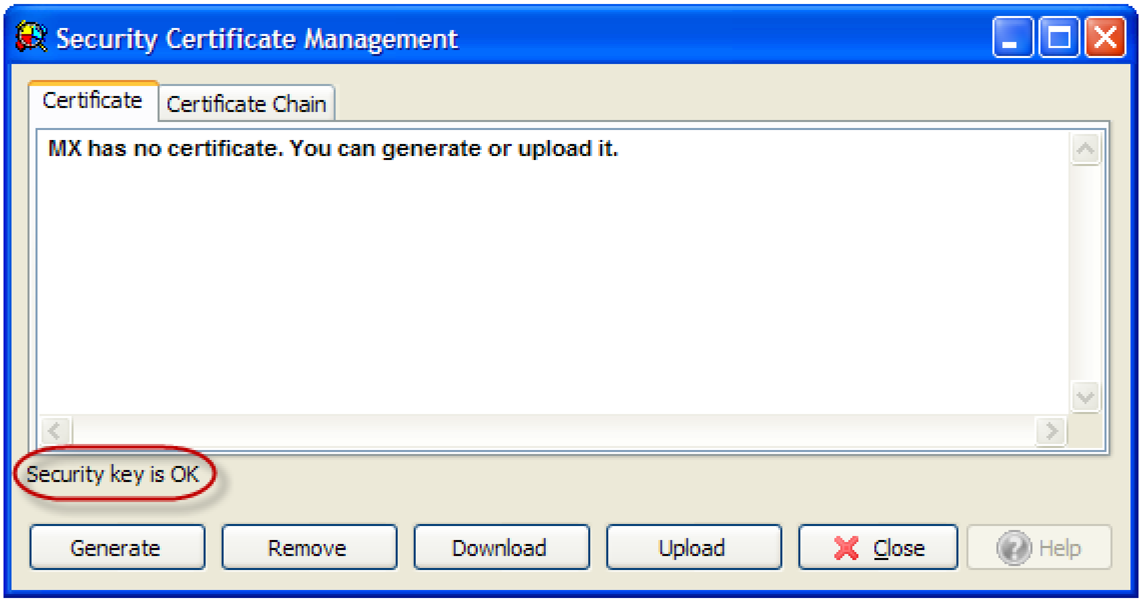
3. Click OK to the following popup message



You are going to modify security key on MX. All certificates are going to be verified and removed in case of incompatible.

4. Verify Security Key is successfully installed

Once the Key is generated, the screen will update to reflect this information

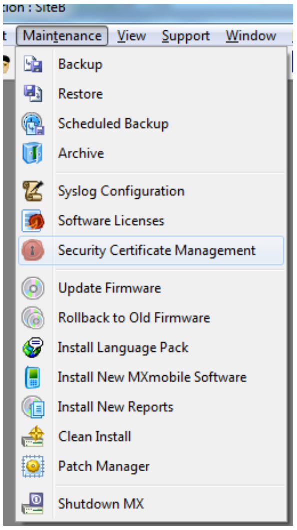


MX has no certificate. You can generate or upload it.

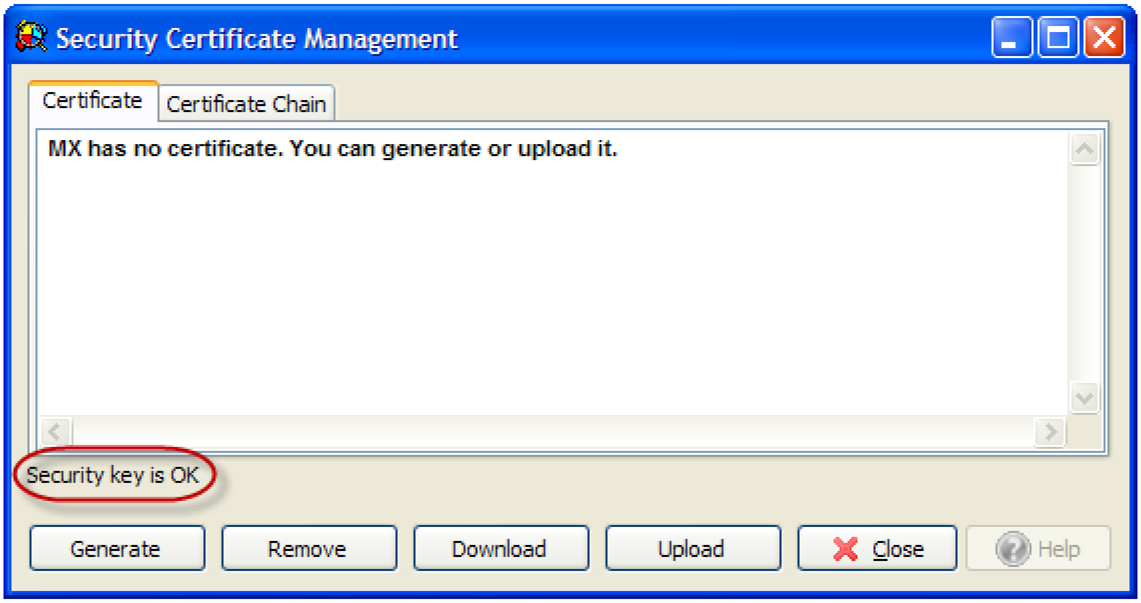
Security key is OK

33.4 Generate and Install a Self-Signed Certificate

1. Maintenance -> Security Certificate Management



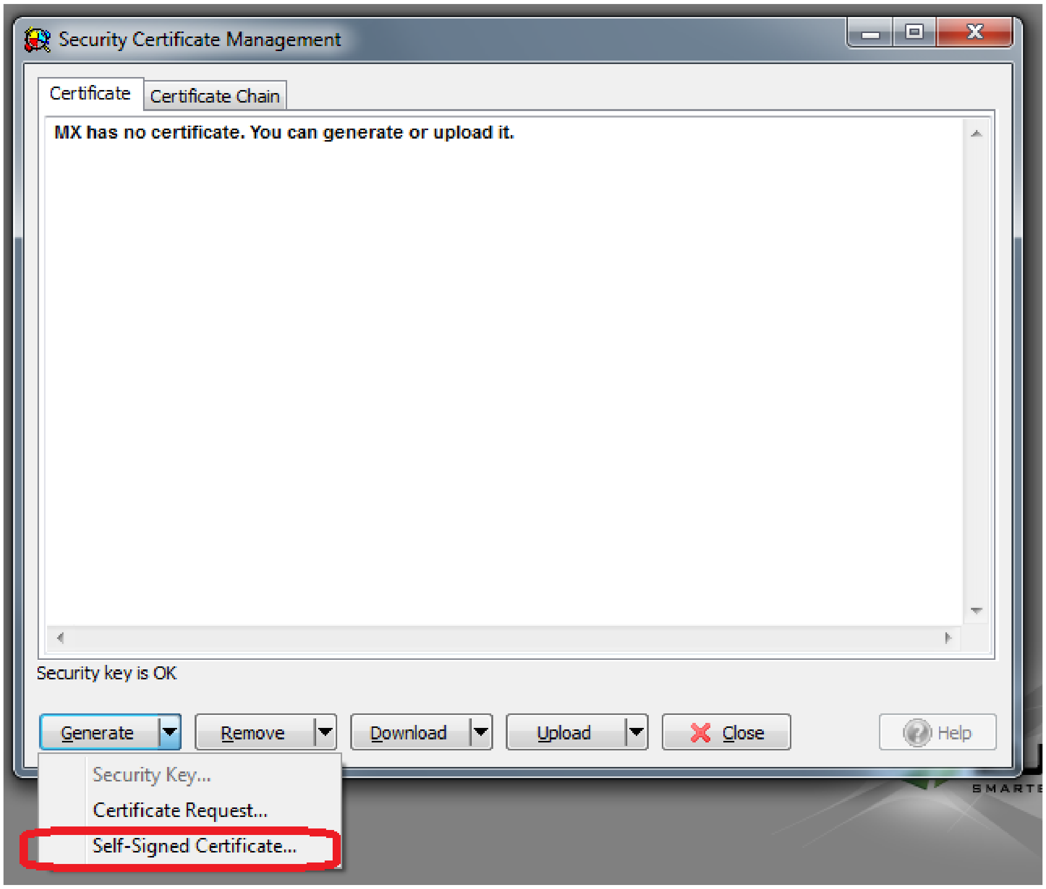
2. Generate Certificate



MX has no certificate. You can generate or upload it.

Security key is OK

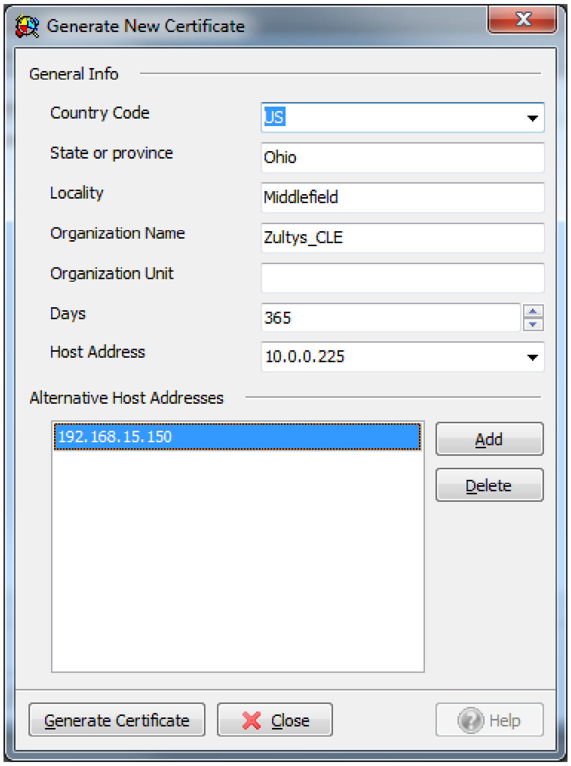
3. Generate -> Generate Self-Signed Certificate



MX has no certificate. You can generate or upload it.

Security key is OK

4. Complete form information



Generate New Certificate

General Info

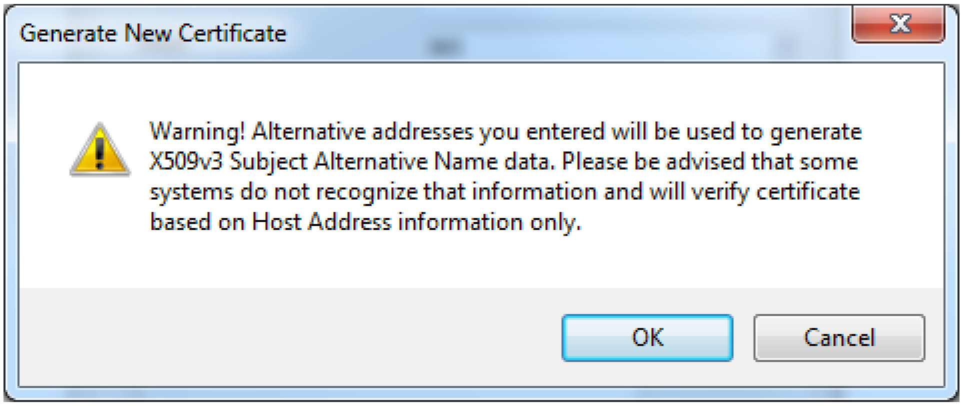
Country Code	US
State or province	Ohio
Locality	Middlefield
Organization Name	Zultys_CLE
Organization Unit	
Days	365
Host Address	10.0.0.225

Alternative Host Addresses

192.168.15.150

5. Click *Generate Certificate*

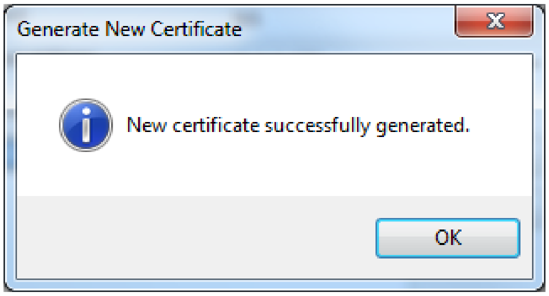
6. Click *OK* to the warning popup up message



Generate New Certificate

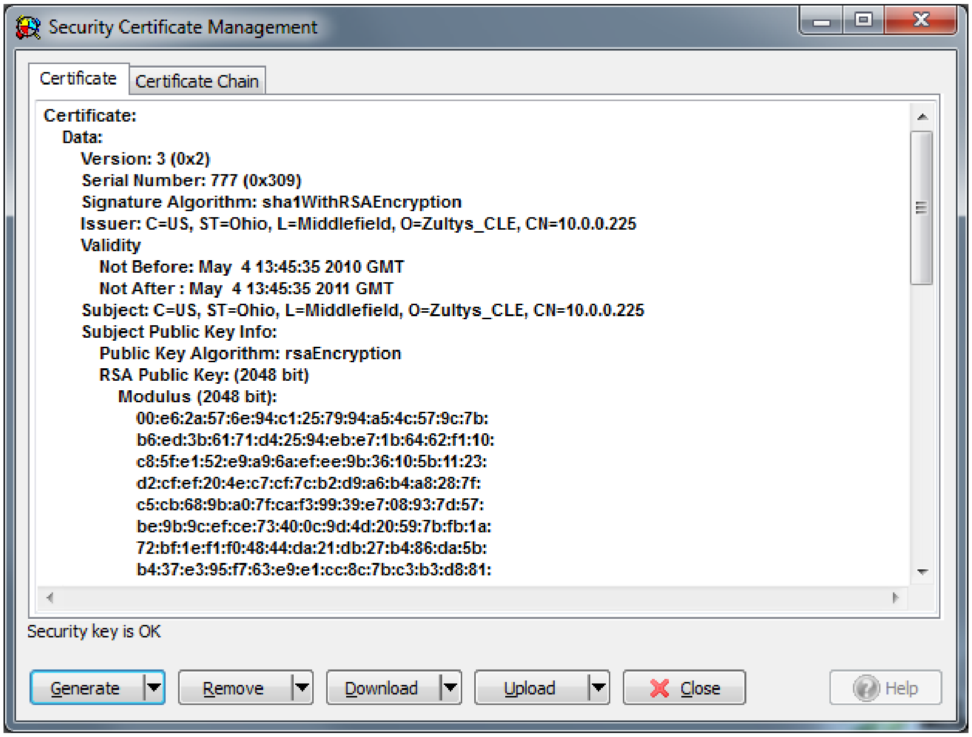
Warning! Alternative addresses you entered will be used to generate X509v3 Subject Alternative Name data. Please be advised that some systems do not recognize that information and will verify certificate based on Host Address information only.

7. Click OK to the confirmation popup message



New certificate successfully generated.

8. Click Close

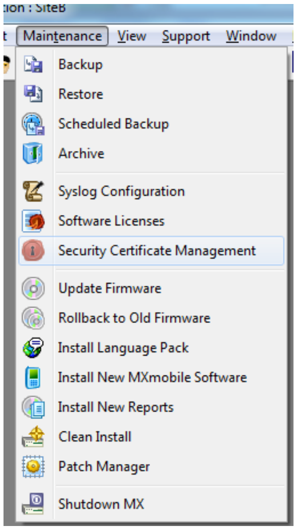


```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 777 (0x309)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=Ohio, L=Middlefield, O=Zultys_CLE, CN=10.0.0.225
    Validity
      Not Before: May  4 13:45:35 2010 GMT
      Not After : May  4 13:45:35 2011 GMT
    Subject: C=US, ST=Ohio, L=Middlefield, O=Zultys_CLE, CN=10.0.0.225
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:e6:2a:57:6e:94:c1:25:79:94:a5:4c:57:9c:7b:
          b6:ed:3b:61:71:d4:25:94:eb:e7:1b:64:62:f1:10:
          c8:5f:e1:52:e9:a9:6a:ef:ee:9b:36:10:5b:11:23:
          d2:cf:ef:20:4e:c7:cf:7c:b2:d9:a6:b4:a8:28:7f:
          c5:cb:68:9b:a0:7f:ca:f3:99:39:e7:08:93:7d:57:
          be:9b:9c:ef:ce:73:40:0c:9d:4d:20:59:7b:fb:1a:
          72:bf:1e:f1:f0:48:44:da:21:db:27:b4:86:da:5b:
          b4:37:e3:95:f7:63:e9:e1:cc:8c:7b:c3:b3:d8:81:
```

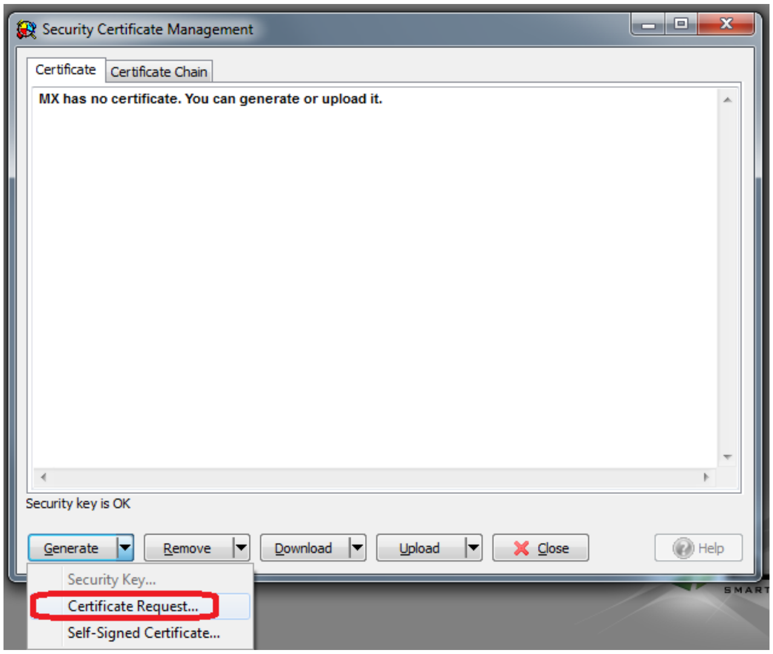
Security key is OK

33.5 Generate a Request for a Certificate from a Certificate Authority

1. Maintenance -> Security Certificate Management



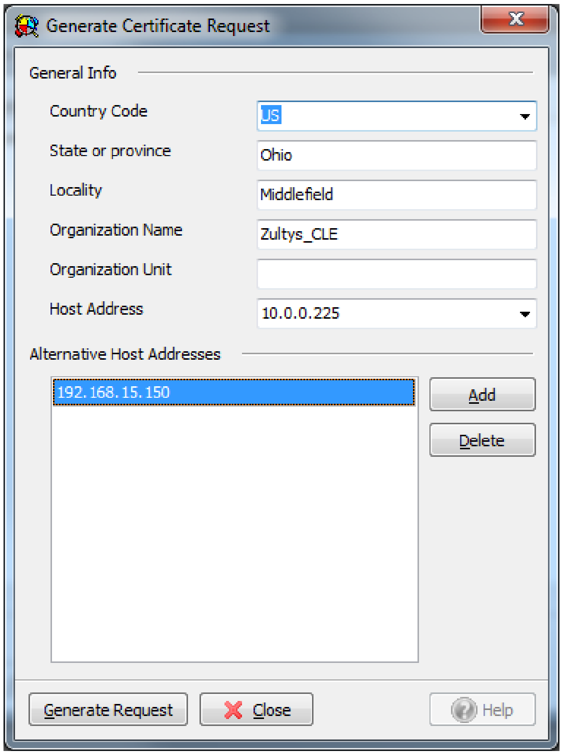
2. Generate a *Certificate Request*



MX has no certificate. You can generate or upload it.

Security key is OK

3. Complete form



Generate Certificate Request

General Info

Country Code: US

State or province: Ohio

Locality: Middlefield

Organization Name: Zultys_CLE

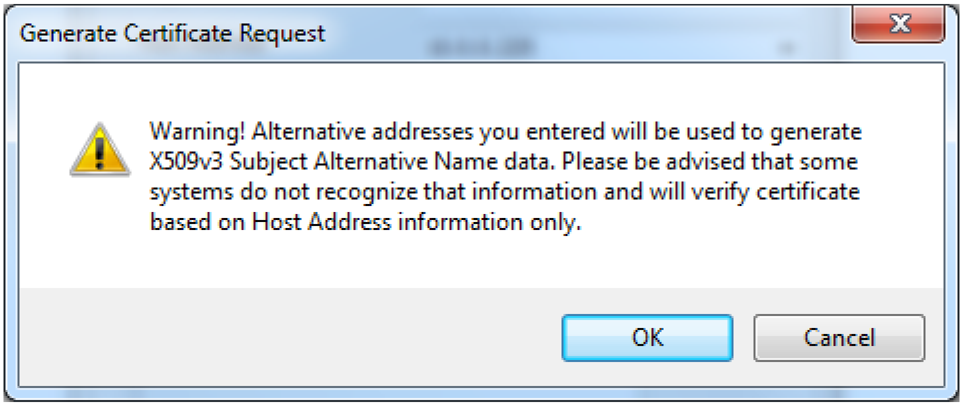
Organization Unit:

Host Address: 10.0.0.225

Alternative Host Addresses

192.168.15.150

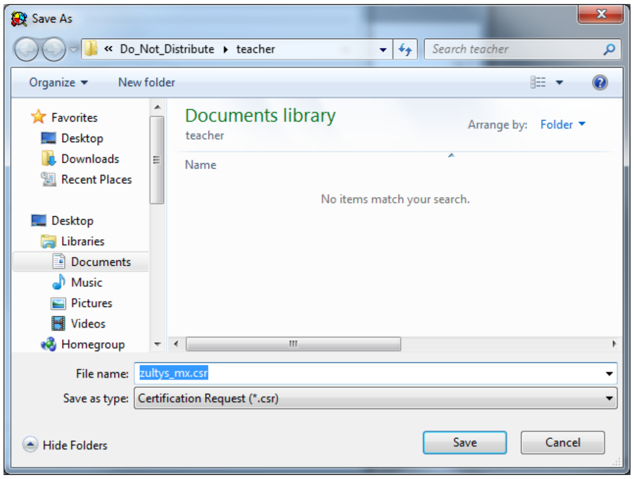
4. Click on *Generate Request*
5. Click ok to the warning popup



Generate Certificate Request

Warning! Alternative addresses you entered will be used to generate X509v3 Subject Alternative Name data. Please be advised that some systems do not recognize that information and will verify certificate based on Host Address information only.

6. Save generated Certificate Request



No items match your search.

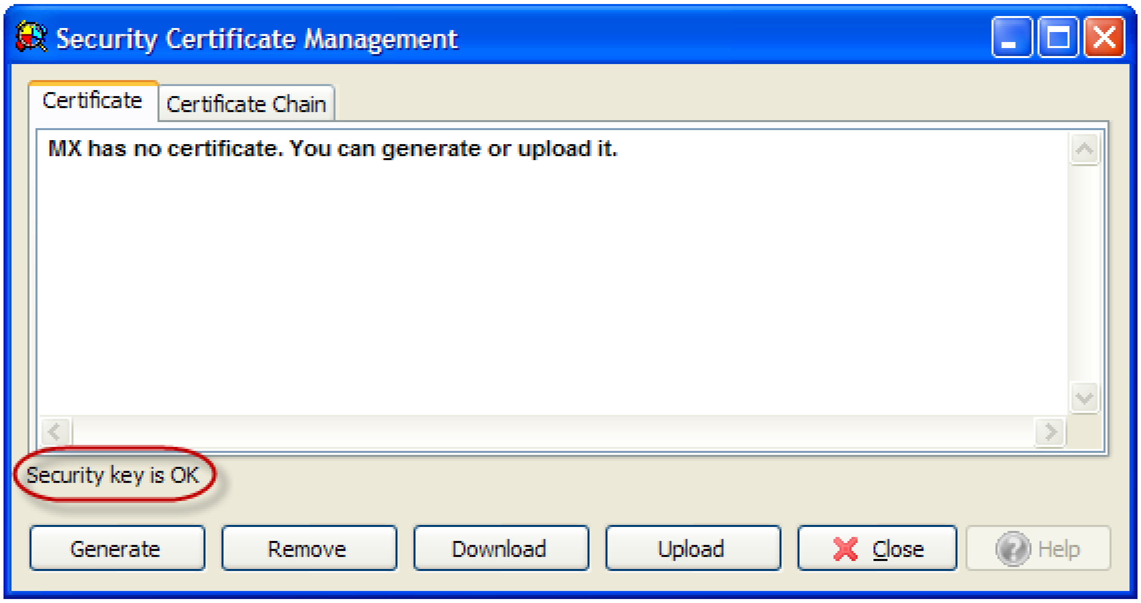
File name: zultys_mx.csr

Save as type: Certification Request (*.csr)

7. Purchase online a certificate from a Certificate Authority. When requested, upload the above CSR file.
8. The certificate authority will download your certificate.

33.6 Install a Certificate from a Certificate Authority

1. Maintenance –> Security Certificate Management



MX has no certificate. You can generate or upload it.

Security key is OK

33.6.1 Upload -> Certificate

1. Navigate to certificate file location and select
2. Certificate will display. Check that data shown is correct.

3. If required, upload a certificate chain

33.6.2 Upload -> Certificate Chain

1. Navigate to certificate file location and select
2. Mobile phone connectivity now is enabled.

34. Security

While Zultys provides high level security protection for the MX-E system against an outside attack, it is still essential to protect the MX-E with a strong administrative password and take other preventive measures against unauthorized access to the system. This section discusses ways in which the channel partner can safeguard an MX-E against unauthorized access for the purposes of toll fraud or unauthorized calls.

34.1 Password Strength

The following exert from wikipedia.org discusses password strength and provides a few useful suggestions for securing the passwords on the MX-E system. Original article can be found at http://en.wikipedia.org/wiki/Password_strength

> Password strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity, and unpredictability.
>
> Using strong passwords lowers overall risk of a security breach, but strong passwords do not replace the need for other effective security controls. The effectiveness of a password of a given strength is strongly determined by the design and implementation of the authentication system software, particularly how frequently password guesses can be tested by an attacker and how securely information on user passwords is stored and transmitted. Risks are also posed by several means of breaching computer security which are unrelated to password strength.

As with any security measure, passwords vary in effectiveness (i.e., strength); some are weaker than others. For example, the difference in weakness between a dictionary word and a word with obfuscation (i.e., letters in the password are substituted by, say, numbers— a common approach) may cost a password cracking device a few more seconds- this adds little strength. The examples below illustrate various ways weak passwords might be constructed, all of which are based on simple patterns which result in extremely low entropy, allowing them to be tested automatically at high speeds:

- Default passwords (as supplied by the system vendor and meant to be changed at installation time): password, default, admin, guest, etc. Lists of default passwords are widely available on the internet.
- Dictionary words: chameleon, RedSox, sandbags, bunnyhop!, IntenseCrabtree, etc., including words in non-English dictionaries.
- Words with numbers appended: password1, deer2000, john1234, etc., can be easily tested automatically with little lost time.
- Words with simple obfuscation: p@ssw0rd, l33th4x0r, g0ldf1sh, etc., can be tested automatically with little additional effort. For example a domain administrator password compromised in the DigiNotar attack was reportedly Pr0d@dm1n.
- Doubled words: crabcrab, stopstop, treetree, passpass, etc.
- Common sequences from a keyboard row: qwerty, 12345, asdfgh, fred, etc.
- Numeric sequences based on well-known numbers such as 911 (9-1-1, 9/11), 314159... (pi), or 27182... (e), etc.
- Identifiers: jsmith123, 1/1/1970, 555-1234, "your username", etc.
- Anything personally related to an individual: license plate number, Social Security number, current or past telephone number, student ID, address, birthday, sports team, relative's or pet's names/nicknames/birthdays/initials, etc., can easily be tested automatically after a simple investigation of person's details.

There are many other ways a password can be weak, corresponding to the strengths of various attack schemes; the core principle is that a password should have high entropy (usually taken to be equivalent to randomness) and not be readily derivable by any "clever" pattern, nor should passwords be mixed with information identifying the user. On-line services often provide a restore password function that a hacker can figure out and by doing so bypass a password. Choosing hard to guess restore password questions can further secure the password.

34.2 MX-E Administrator Password

All MX-E systems ship with the default ‘administrator’ user for the MX-E Administrator already programmed on the system. If an unauthorized individual gains access to this user’s password, they will gain full control of the system.

34.2.1 Default Password

Zultys strongly recommends changing the default administrator password immediately after initial deployment of the MX-E system. Try to use a strong alpha numeric password that contains both upper and lower case letters.

34.2.2 Multiple Logins

Zultys recommends creating a separate login and password for each person accessing the MX-E Administrator. This allows you to easily track and identify who is logging into MX-E Administrator and making changes. In the event that one of the users’ login and password are compromised, you can easily remove their administrative privileges.

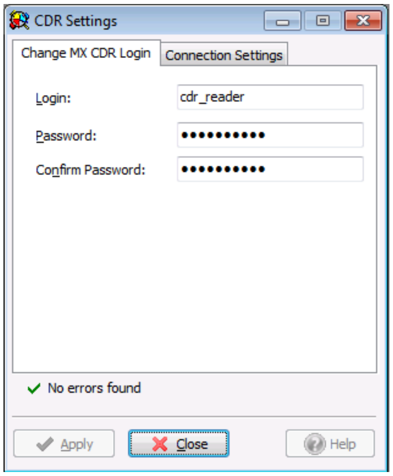
34.2.3 Assign proper rights

Zultys recommends limiting the administrative rights of users who require access to MX-E Administrator. Disable the user’s ability to edit all sections of MX-E Administrator that do not pertain to their responsibilities. This prevents users from “accidently” or “maliciously” making unnecessary changes to the system.

34.3 CDR Password

Zultys recommends changing the password for the CDR Database. To change the password, navigate to *File* -> *CDR Settings* and click on the *Change MX-E*

CDR Login tab to change both the login and the password for accessing the database.



Login: cdr_reader

Password: ••••••••••

Confirm Password: ••••••••••

✓ No errors found

34.4User Passwords

Administrators should stress the importance of a “strong” password to all the users on the MX-E system. While an average user may not see the importance of securing their login credentials, exploited user passwords constitute the majority of security issues facing administrators of the MX-E system.

34.4.1 MXIE

The password used to log into MXIE can also be used to log into other MX-E Administrator as long as the user in question has administrative privileges. MXIE password is also used to log into Zultys Mobile Communicator, Zultys Salesforce Communicator, Zultys Outlook Communicator and Zultys Flex Communicator.

Zultys recommends using a strong alpha numeric password that contains both upper and lower case letters. It is inadvisable to set a user’s password to be identical to their PIN number.

34.4.2 PIN

The PIN number is used to check the user’s voicemail box from a phone or log into a call group via a phone’s preprogrammed login button. The users PIN number with their User ID are used to register softphone. Depending on configuration, a compromised PIN number can be used to access other sensitive services. For more details see Section 34.9.

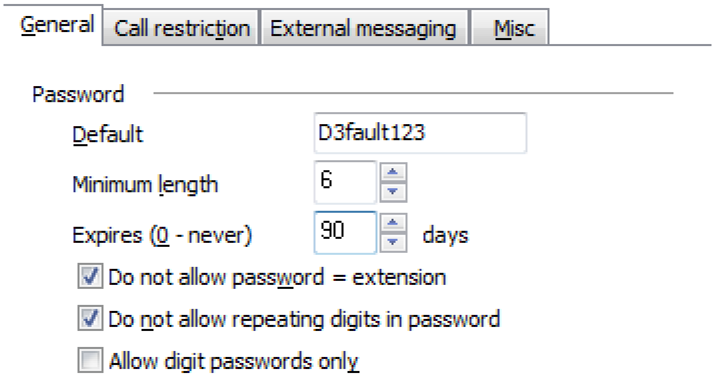
Zultys recommends using 6 digit-long PIN numbers to increase the security of users' PINs. MXIE user passwords should never be the same as the users PIN number.

34.4.3 Password Policies

Administrators can set a strict password policy for all users on the MX-E system. The policies are configured per user profile.

In MX-E Administrator, navigate to *Configure -> Users* and select the *Profile.* Zultys recommends implementing the following password policy for all user profiles.

- Set minimum password length to 6 characters
    - 8 to 10 character-long passwords are preferred
- Set the password to expire every 90 days
- Enable the *Do Not Allowing Password = Extension* option
- Enable the *Do Not Allow Repeating Digits in Password* option
- Disable the *Allow Digit Passwords Only* option



Password

Default: D3fault123

Minimum length: 6

Expires (0 - never): 90 days

☑ Do not allow password = extension

☑ Do not allow repeating digits in password

☐ Allow digit passwords only

Password policies should be implemented in ALL profiles. When you create a new profile, copy the default profile with the password policies already in place.

It is important to note that Password Policies only apply to passwords only, not PIN numbers.

Password Policies will not have any effect if LDAP integration is enabled. Do not configure these settings if you are using LDAP.

34.4.4 LDAP Integration

To simplify management of user passwords, including MXIE passwords, Zultys recommends implementing LDAP authentication. LDAP integration uses your Windows Active Directory, or LDAP server, to authenticate all user logins. In this scenario users only need to login once to access all of their secured accounts. However, there is a risk that if the LDAP server is unavailable, users will not be able to log into MXIE.

Note that LDAP authentication manages only user passwords and not PIN numbers. It is the user's responsibility to manage and update their PIN numbers regularly.

If LDAP authentication is used, you do not need to set the password policies in user profiles as seen in Section 34.4.3. In particular, do not set the password for a user to expire in MX-E Administrator.

34.5 Call Handling Rules, Find Me Follow Me and Call Forwards

Zultys Technical Support has encountered instances where Call Handling Rules, Find Me Follow me, and Call Forwarding functions has been implemented by unauthorized individuals to initiate toll fraud or make unauthorized calls. In the event there is a possibility of a security breach, Zultys recommends that the system administrator first investigates the call handling rules that are currently configured on the MX-E system.

Call Handling Rules, Find Me Follow me, and Call Forwarding functions can be implemented on the MX-E side (server side) or on the user's device (client side), both should be investigated separately.

Upon request, Zultys Technical Support may be able to assist administrators of a compromised system by putting together a report on all call handling rules configured on the MX-E system.

Review both the call handling rules set up on the MX-E system in either MXIE, MX-E Administrator or via DTMF Controls and the device-level call handling rules set up via the web interface.

34.5.1 Device Level Forwarding

Call forwarding can be implemented on the device level. If a remote phone is compromised, in most cases the unauthorized individual sets up call forwarding from the web interface of the device in question. If you suspect that a device has been compromise, you should investigate at the device level.

34.6 MX-E Security Options

This section details some suggested Security settings for the MX-E system.

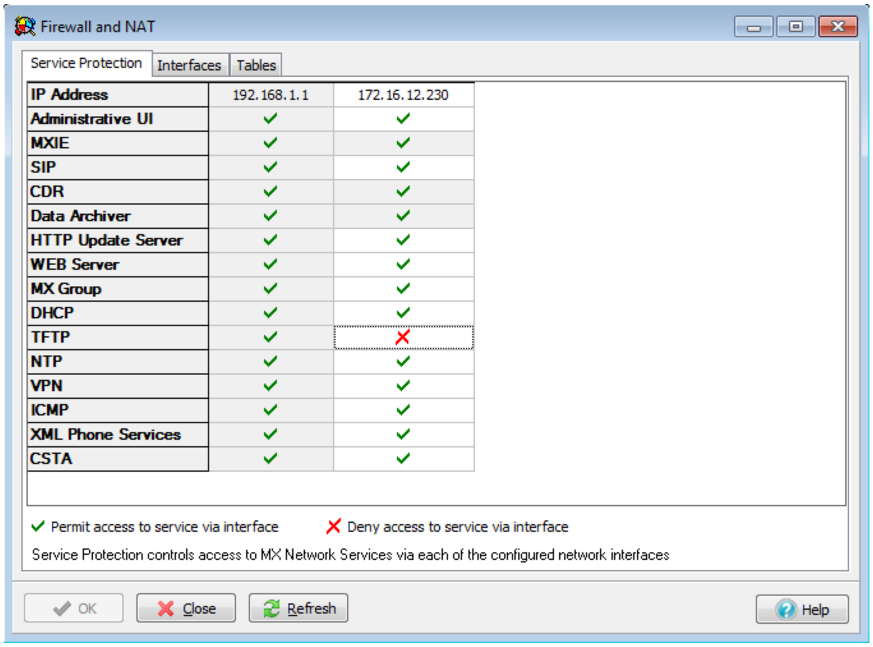
34.6.1 Disable TFTP for public access

Zultys highly recommends disabling public access to the TFTP server, unless it is required for use with remote devices.

It is important to remember the MX-E TFTP Directory by design is READ ONLY. It is impossible to change this, as a result unauthorized changes to the files in the TFTP Directory can be made by simply uploading a new file to the TFTP Directory.

If there are little to no changes required for the remote devices on the system, it is recommended to disable TFTP for public access, for more information see Section 34.11.3.

TFTP can be disabled via MX-E Administrator. Navigate to *Provision -> Firewall and NAT* and open the *Service Protection* tab. To disable public access, click on the box in the TFTP row corresponding to the public address of the MX-E. If you are using SBC or port forwarding options, this will need to be done on the firewall/router that is providing the NAT services.



IP Address	192.168.1.1	172.16.12.230
Administrative UI	✓	✓
MXIE	✓	✓
SIP	✓	✓
CDR	✓	✓
Data Archiver	✓	✓
HTTP Update Server	✓	✓
WEB Server	✓	✓
MX Group	✓	✓
DHCP	✓	✓
TFTP	✓	✗
NTP	✓	✓
VPN	✓	✓
ICMP	✓	✓
XML Phone Services	✓	✓
CSTA	✓	✓

✓ Permit access to service via interface ✗ Deny access to service via interface

Service Protection controls access to MX Network Services via each of the configured network interfaces

34.6.2 Disable/Limit SIP Access

You may be able to disable or limit SIP access from the public address of the MX-E to strengthen the security of the system. This setting is accessed from the *Service Protection* tab in MX-E Administrator in *Provision -> Firewall and NAT*.

Because SIP access is required for some day-to-day operation, only disable it in the following situations:

- If the system has no remote devices and is not using SIP trunks, disable SIP on the public IP address.
- If the system is only using SIP trunks, with no remote devices, place the MX-E behind a firewall, and limit SIP access to only the IP addresses used by the SIP carrier.
- If the system is using static IP addresses for remote devices, for example if the remote devices are deployed at another office location, then place the MX-E behind a firewall, and limit SIP access to only the IP addresses used by the office in question.

34.6.3 Properly Define Networks in SBC

Make sure that when defining the networks used by the SBC, you define the exact network address.

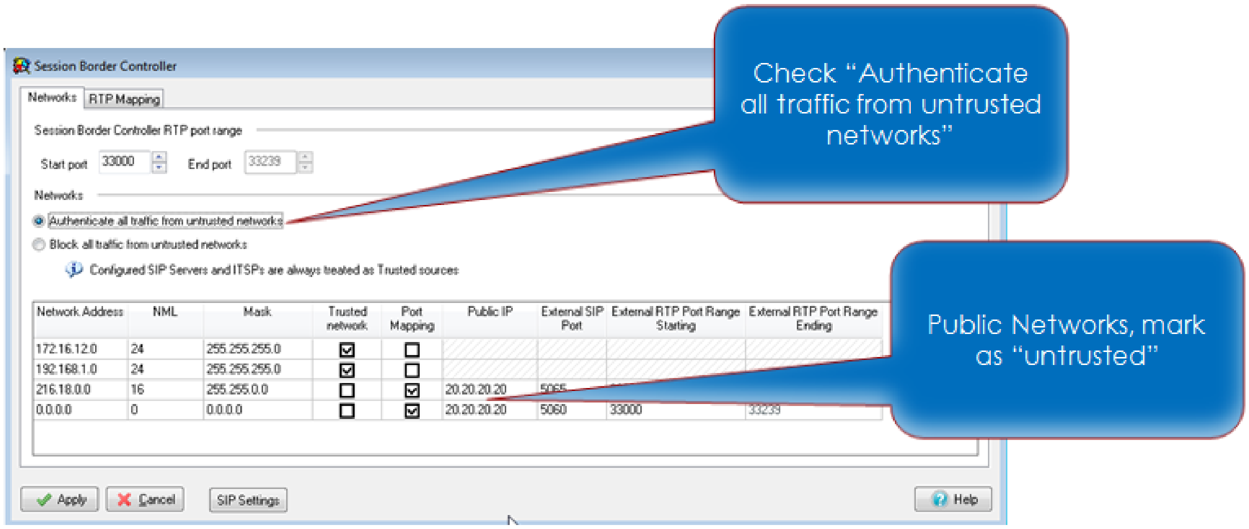
For example: if the network used by your MX-E system is 192.168.1.0/24 and you have several other networks which have inbound traffic from the internet but do not require SIP services from the MX-E. In this example, you should define the network in SBC as 192.168.1.0/24. Do not use the default address of 192.168.0.0/16.

34.6.3.1 Define Trusted and Untrusted Networks

For MX-E Release versions 7.0 and later, Zultys recommends defining Trusted and Untrusted Networks in SBC settings. If SIP requests (REGISTER, INVITE, or SUBSCRIBE) arrive from an untrusted network they will require forced authorization. This behavior is not applied to defined ITSP/SIP servers. It is assumed that all configured ITSP/SIP servers are always trusted (even if ITSP has an address that belongs to an untrusted network). Networks defined as Trusted do not require any authentication. Incorrectly defining your trusted networks can lead to the ability to override the requirement to authenticate.

34.6.3.2 Set the option to require authentication from untrusted networks

By default the option to require authentication of untrusted networks is NOT enabled. Zultys recommends enabling this option in SBC. As indicated below SIP servers and ITSPs are excluded from this requirement.



Session Border Controller

Session Border Controller RTP port range

Start port 33000 End port 33239

Networks

● Authenticate all traffic from untrusted networks
○ Block all traffic from untrusted networks

Configured SIP Servers and ITSPs are always treated as Trusted sources

Network Address	NML	Mask	Trusted network	Port Mapping	Public IP	External SIP Port	External RTP Port Range Starting	External RTP Port Range Ending
172.16.12.0	24	255.255.255.0	☑	☐				
192.168.1.0	24	255.255.255.0	☑	☐				
216.18.0.0	16	255.255.0.0	☐	☑	20.20.20.20	5065		
0.0.0.0	0	0.0.0.0	☐	☑	20.20.20.20	5060	33000	33239

Check "Authenticate all traffic from untrusted networks"

Public Networks, mark as "untrusted"

Every time a new network is added to the table in SBC window, it is marked as trusted by default. If a network is not listed in SBC, it's considered untrusted.

So, if the MX-E receives a request from an IP address which does not match any networks listed in SBC, the request will be either authorized or ignored.

In the *Networks* section of the SBC window, select whether requests from untrusted networks are ignored or authenticated.

Authenticate all traffic from untrusted networks: If this option is selected, all requests that come from untrusted or unlisted networks will be always authorized even if the password for the user or device is not set.

Block all traffic from untrusted networks: If this option is selected, then the MX-E system will ignore all requests from untrusted networks. Exceptions to this rule are requests from ITSP/SIP Servers and requests from IP addresses to which requests were generated during previous SIP sessions (for example: some transfer scenarios require additional requests from clients which are not necessary to authorize).

34.6.4 RTP Traffic

RTP Traffic is not encrypted. Zultys recommends having the devices on a separate VLAN from the data traffic in situations when the RTP Security is a concern. For remote devices, Zultys recommends using hardware VPN to encrypt the tunnel in which the RTP travels.

34.6.5 SIP Registration / Digest Authentication

SIP registration with authentication is required. All passwords are encrypted using the SIP standards. The HTTP digest authentication scheme is documented in RFC2617 and extended in RFC 3310

34.7 Auto Attendant Options

Consider disabling the ability to dial a pattern of ??? (3 digit extensions) for transfers in “From Root Dialog” settings. This setting could become an issue if your dial plan also allows 3 digit dialing to the carrier for “411”.

Likewise, consider disabling the No Match option transfers in “From Root Dialog” settings.

34.8 Conference Server and Voice Mixer

An unauthorized individual may be able to exploit the conference server and voice mixer ports and set up unauthorized conferences. One way to prevent this is to set the voice mixer and conference ports to be controlled by auto attendant during off work hours, since majority of "hacking" cases happen during the night.

Zultys recommends disabling the ability to link toll free calls to the conference server for unmanaged/repeating conferences or the voice mixer to minimize the risk of unauthorized conferences accruing toll free charges.

34.8.1 Voice Mixer

Note that exposed voice mixer ports or extensions could be exploited. Voice Mixer ports do not have any security on them, as no password or PIN is required to join the conference like the conference bridge.

34.8.2 Conference Server

There is also a possibility that a Repeating Conferences can be exploited by someone who has knowledge of the PIN or access code to join the conference. Be mindful when distributing this information.

34.9 User Rights

When setting up user rights, it is recommended to carefully review the rights assigned to each user, and make sure that they are given access only to the features necessary for their job requirements. If you are providing "Higher Risk" permissions to a user, make sure the customer fully understands the risks.

The following user rights are considered "Higher Risk" and should be limited to users who absolutely must have access to them.

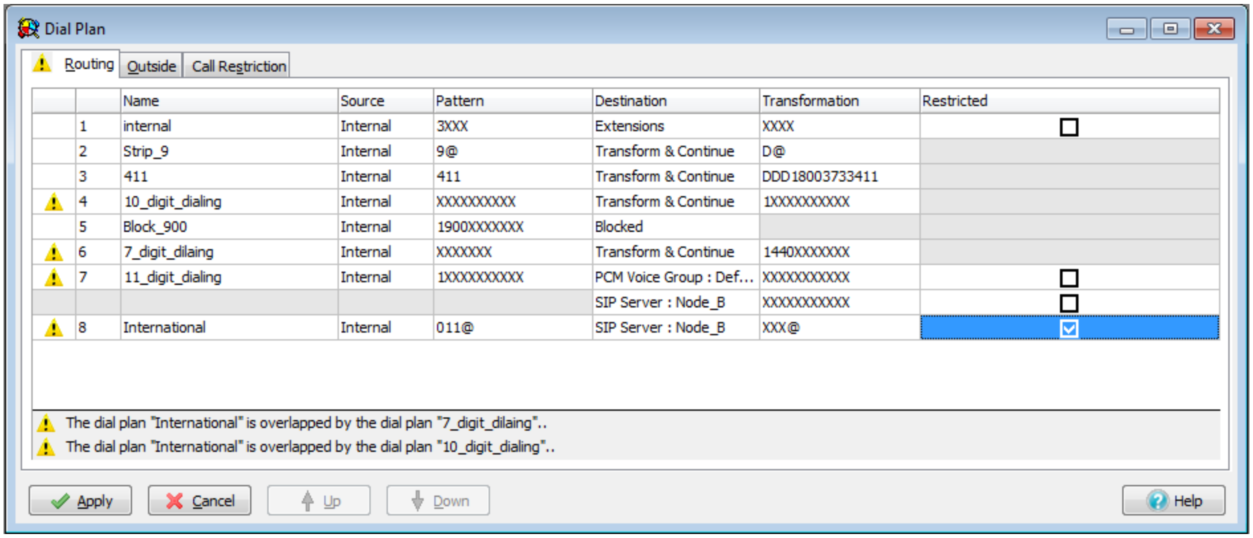
- "Can return calls from voicemail"
    - This is a permission that allows a user to log into their voicemail box, and make calls from it. All rights and permissions this user has will be used when making the call.
- Access to the MX-E Administrator to make changes
- DTMF Controls -> Call Forwarding Control

    - Allows the user to set up a call handling rule to forward all calls to a number of their choosing from Voice Mail.
- “Can Register Softphone”
    - This is used to enable MXIE Softphone, Zultys Mobile Communicator for iPhone/Android with softphone.
    - This feature allows MXIE Username and PIN to be used to register a softphone or an unauthorized device.
- Call restrictions that are “open”
    - The user has little to no call restrictions in place for 900, international calls, 411, and operator assisted calls. Be mindful of allowing users to make calls that can accrue large phone charges.
- “Bind to external number”
    - This feature could be exploited. In a situation where MXIE login is compromised and bound to a PSTN number, the hacker can make unauthorized calls.

34.10 Dial Plan

When setting up the dial plan, Zultys recommends that you apply restrictions or block numbers that can be “expensive” such as 900/976, international numbers, as well as 411.

- International calls
    - At minimum, apply an MX-E account code that is forced and verified.
    - Or block the call completely if international calls are not required.
- 900 Numbers
    - At minimum, apply an MX-E account code that is forced and verified.
    - Or block the call completely if 900 calls are not required.
- Make sure all options are covered for patterns that you are restricting
    - Options to dial as 9+ number.
    - Options to dial as just 10 digit number.
    - Options to dial as 11 digit number.



		Name	Source	Pattern	Destination	Transformation	Restricted
	1	internal	Internal	3XXX	Extensions	XXXX	□
	2	Strip_9	Internal	9@	Transform & Continue	D@	
	3	411	Internal	411	Transform & Continue	DDD18003733411	
⚠	4	10_digit_dialing	Internal	XXXXXXXXXX	Transform & Continue	1XXXXXXXXXX	
	5	Block_900	Internal	1900XXXXXXX	Blocked		
⚠	6	7_digit_dilaing	Internal	XXXXXXX	Transform & Continue	1440XXXXXXX	
⚠	7	11_digit_dialing	Internal	1XXXXXXXXXX	PCM Voice Group : Def...	XXXXXXXXXXX	□
					SIP Server : Node_B	XXXXXXXXXXX	□
⚠	8	International	Internal	011@	SIP Server : Node_B	XXX@	☑

⚠ The dial plan "International" is overlapped by the dial plan "7_digit_dilaing"..
⚠ The dial plan "International" is overlapped by the dial plan "10_digit_dialing"..

34.11 Device Security

Zultys recommends securing devices, to stop or block unauthorized devices from registering to the MX-E system. Most importantly when using remote devices, make sure they are using “strong” passwords for both the User and Administrator access to the device.

34.11.1 Registering a device as extension number or user name

Zultys discourages allowing devices to be registered as a user’s MXIE Username or as a user’s extension number and MXIE Password. By default this option is disabled.

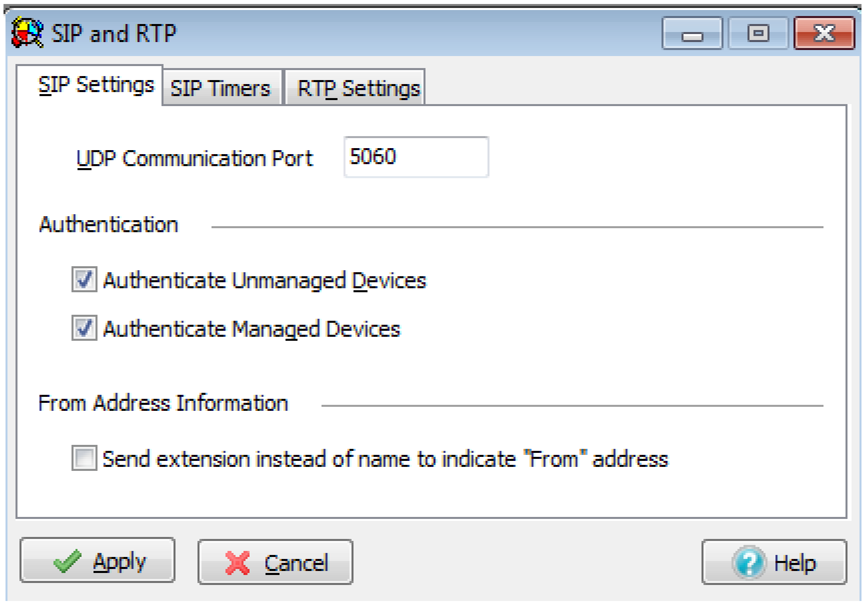
34.11.2 Require SIP Proxy password for ALL devices

External devices by design are required to have a SIP Proxy password, but it is recommended to also apply this restriction to internal devices as well. To enable this option, in MX-E Administrator navigate to *Provision* -> *SIP and RTP* -> *SIP Settings* and select “Authenticate Manage Devices” option. This will require internal devices to be challenged when registering to provide the SIP Proxy Password. Be default this option is disabled, and internal devices are not challenged. There are two options for MX-E authentication of Trusted Networks:

Authenticate Unmanaged Devices: Unmanaged devices can be registered with an MX-E only if the registered address is a valid MX-E user ID or a valid MX-E extension number. Selecting this option requires that the user provide a correct password when registering the device.

Authenticate Managed Devices: Selecting this option requires the user to provide a correct password when registering the device.

The above settings have no effect for “untrusted” or “external” requests.



UDP Communication Port: 5060

Authentication

☑ Authenticate Unmanaged Devices

☑ Authenticate Managed Devices

From Address Information

□ Send extension instead of name to indicate "From" address

34.11.3 Strong SIP Proxy Password

While it is possible for an unauthorized individual to user ‘brute force’ hacking to compromise a device, to do so they would need break both the device’s MAC address and the password. By using a “strong” password it is possible to make the “hacker’s” job much harder and therefore discouraging them from attempting to compromise the device.

As a side note, the MX-E has built-in ability to “block” or not respond to this type of hacking, which will serve as your first line of defense in the event of a ‘brute force’ hacking attempt.

34.11.4 Device Default Passwords

Devices that are “naked” on the internet—that is directly assigned a public IP address—should always have their default administrator and user passwords changed. The manufacturer’s default passwords are public knowledge and sometimes even “blank” making it easier to hack the device unless the password is changed. With a call forward enabled on the device, all they hacker has to do is dial the extension number from the auto attendant, and the call is forwarded by the device to the number of the "hackers" choosing, assuming the dial plan permits it.

Some devices allow calls to be placed from the web UI of the device, but on some phone models these calls cannot be transferred afterwards. This is another reason to change the default user and admin passwords.

34.11.5 Should a device be compromised

Should a device become compromised, Zultys recommends resetting the device to its factory default, so that it returns to the configuration setup by the MX-E Administrator. This will remove all configuration options added by the hacker.

Zultys also recommends changing the device registration name and all SIP proxy passwords. Also change all device user and administrator passwords.

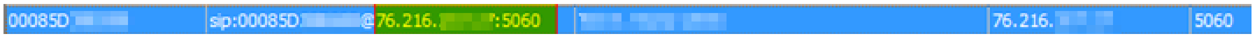
For a ZIP5 device, you can review the "Local configuration" file from the device itself to see what was changed from the MX-E configuration settings. Hackers can implement all kinds of different options to control the phones which include:

- XML call setup and control
- XML Configuration options
- Call forwarding rules
- Change in user or administrator passwords

34.11.6 Devices "Naked" on the internet

SIP devices should never be fully exposed on the internet (save for testing), since they are susceptible to SIP attacks. You can identify a "Naked" device can by reviewing the device status in the MX-E Administrator. Navigate to *Configure* -> *Devices*. If a public address for the device is displayed in the "Contact Field" for that device, it may be exposed. Some ALG functions will show the public address in the contact field but not expose the device.

Below is an example of a device "Naked" on the internet



00085D[redacted]	sip:00085D[redacted]@76.216.[redacted]:5060	[redacted]	76.216.[redacted]	5060

35. MX-E Redundancy

When discussing MX-E Redundancy, it is important to understand the terminology used in this manual and in general for MX-E Redundancy. This includes:

- **Primary Node**: A Primary or Master Node is the node that contains all of the data including but not limited to the Database, Dial Plan and Licensing. It may also be referred to as Master Node. The Primary Node is the first system configured in Redundancy. The Primary Node provides the configuration settings, network settings, system IP address, user list, managed device list, dial plan, PSTN circuitry, and all other parameter settings for the Redundancy.

  Redundant Node: A Redundant Node is the node that is a mirror image of the Primary Node. In the event of the Primary Node failing, the Redundant Node will assume this position and functionality. It may also be referred to as Standby Node. When routed through an XRS12 switch, the PCM circuits on the Redundant Node can replace the PCM circuits of a failed Primary Node. If the option slot circuits on the Redundant Node are configured identically to the Primary Node, then the Redundant Node circuits can be utilized a well.
- **Master State**: This mode specifies the operational status of the MX-E master node.
- **Redundancy State** - This mode specifies the operational status of the MX-E Redundant/Standby node.
- **Switchover** - The Redundant Node has replaced the Primary Node or a Redundant Node.

MX-E Redundancy requires that a redundant license, part number 90-15350, is installed on the Primary Node.

All license management, for all nodes is done via the MX Administrator using the Main IP Address of the MX-E Redundancy.

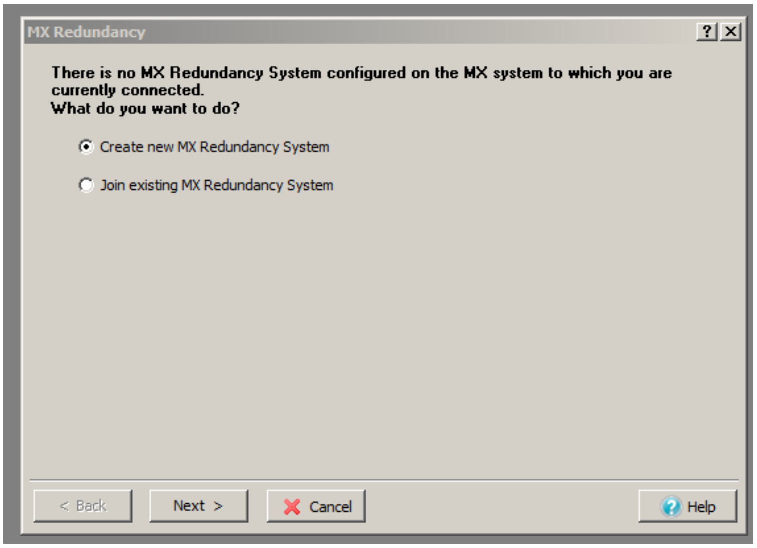
MX-E Redundancy has several requirements that need to be followed in order to be properly set up and function. Not following these recommendations will make the system ineligible for support of any kind from Zultys technical support.

- All nodes must be on the same LAN.
    - No VPN connections between nodes.
    - Same subnet.
    - Same location.
    - Same power source.
    - Same switch.
    - It is recommended to have dedicated Switch for the Redundancy.
- The Primary and Redundant nodes must have an unused and unique IP address.
- The Primary IP address of the MX-E Redundancy cannot be the same as the Primary Node or Redundant node IP address.
- All networking devices must support Gratuitous ARP (GARP).
- All nodes must be properly licensed.
- The Primary/Redundant nodes must be in bridging mode (utilize Ethernet connector 1 on both nodes)   .
- The Primary/Redundant nodes must be running the same version of MX software.
- FXO circuits must be deployed on the Primary Node only.

There are two (2) main steps to creating the Redundancy, create the new redundant Master and then join the Standby system to the Redundancy.

Master System:

- MX Administrator\File\MX Redundancy
- Click Create



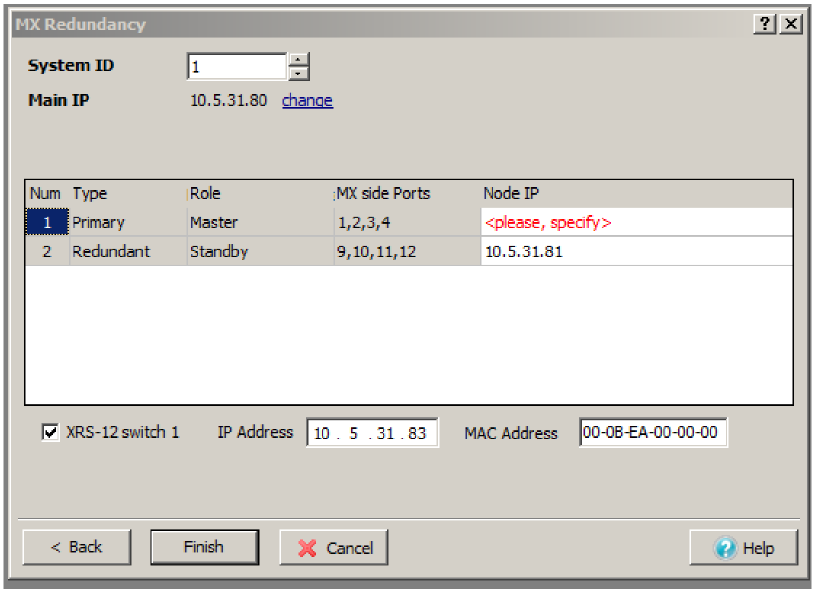
MX Redundancy

There is no MX Redundancy System configured on the MX system to which you are currently connected.
What do you want to do?

● Create new MX Redundancy System

○ Join existing MX Redundancy System

- Enter the desired system ID (make a note as you will need this information for the Standby system)
- Enter the desired Main IP (must be unique)
- Enter the Primary node IP (must be unique and cannot be the Main IP address)
- Enter the Redundant Node IP (must be unique)
- Select if an XRS-12 is used. If so, enter the IP address and MAC address of the XRS-12 unit
- Click Finish



MX Redundancy

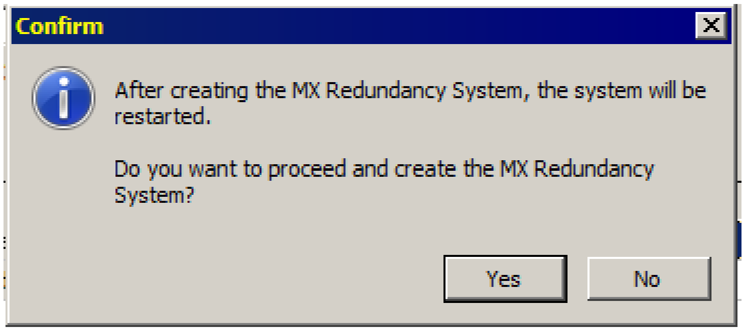
System ID 1

Main IP 10.5.31.80 change

Num	Type	Role	MX side Ports	Node IP
1	Primary	Master	1,2,3,4	<please, specify>
2	Redundant	Standby	9,10,11,12	10.5.31.81

☑ XRS-12 switch 1 IP Address 10 . 5 . 31 . 83 MAC Address 00-0B-EA-00-00-00

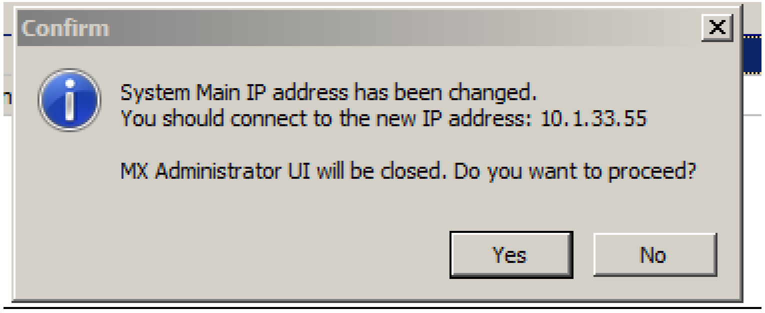
- Click yes at the Confirm windows:



Confirm

After creating the MX Redundancy System, the system will be restarted.

Do you want to proceed and create the MX Redundancy System?

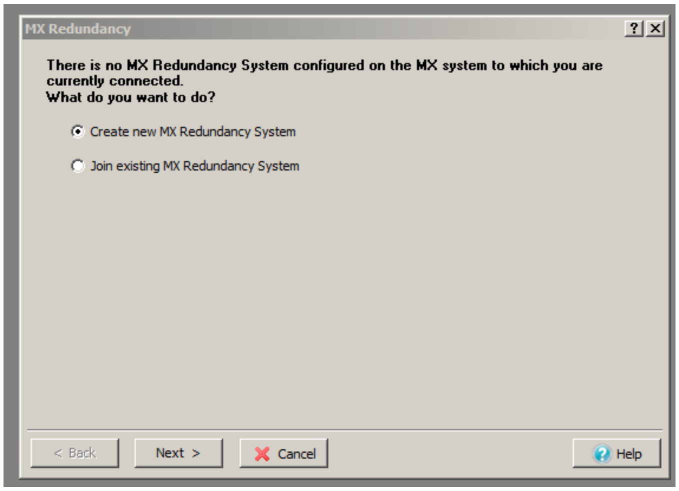


Confirm

System Main IP address has been changed.
You should connect to the new IP address: 10.1.33.55

MX Administrator UI will be closed. Do you want to proceed?

- Once the Redundancy has been created and the Primary system is back online, access the MX Administrator of the desired MX-E to be the Standby system.
- MX Administrator\File\MX Redundancy
- Click Join


MX Redundancy

There is no MX Redundancy System configured on the MX system to which you are currently connected.
What do you want to do?

● Create new MX Redundancy System

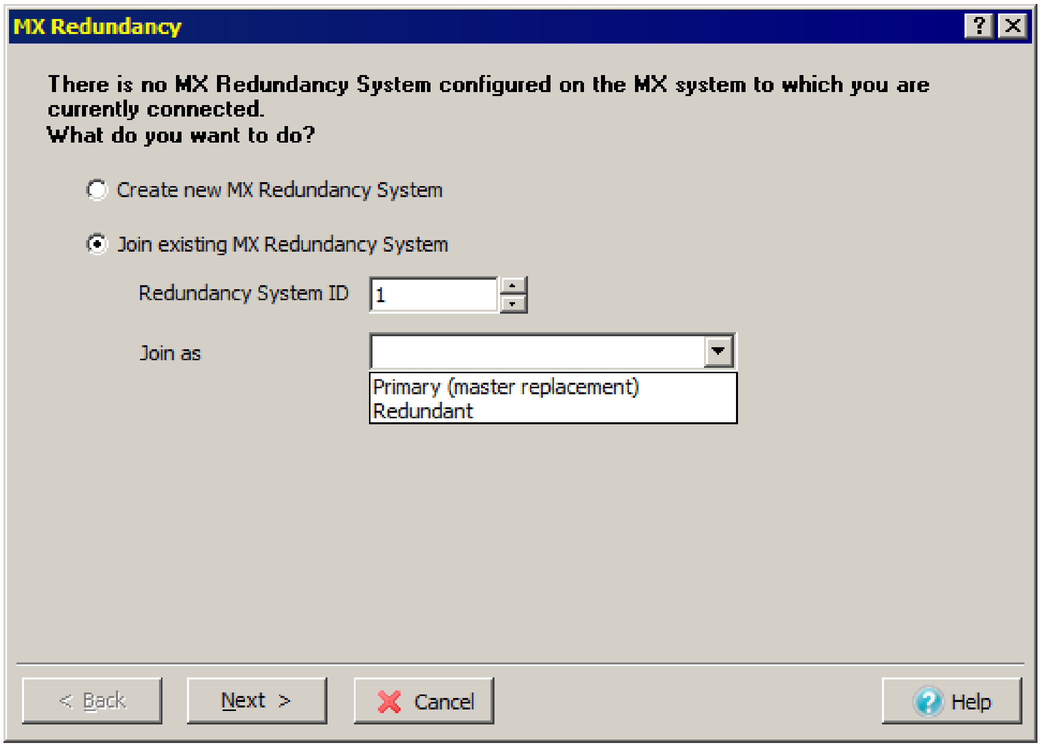
○ Join existing MX Redundancy System

- Select Join existing MX Redundancy System

- Enter the Redundancy System ID

- Select the Join as drop down and select Redundant

- Click Next



MX Redundancy

There is no MX Redundancy System configured on the MX system to which you are currently connected.
What do you want to do?

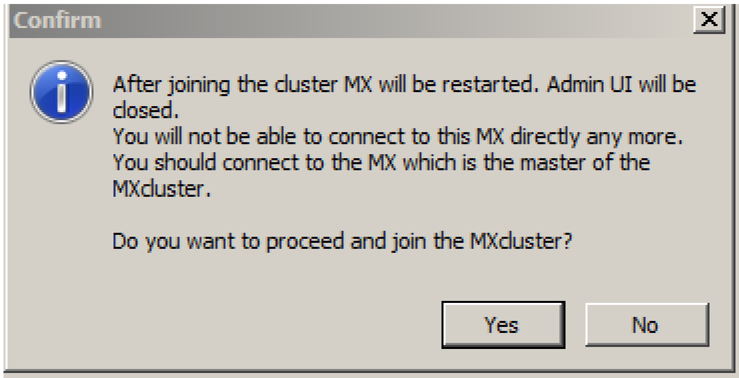
○ Create new MX Redundancy System

● Join existing MX Redundancy System

Redundancy System ID: 1

Join as:
Primary (master replacement)
Redundant

- Click Yes to confirm.



Confirm

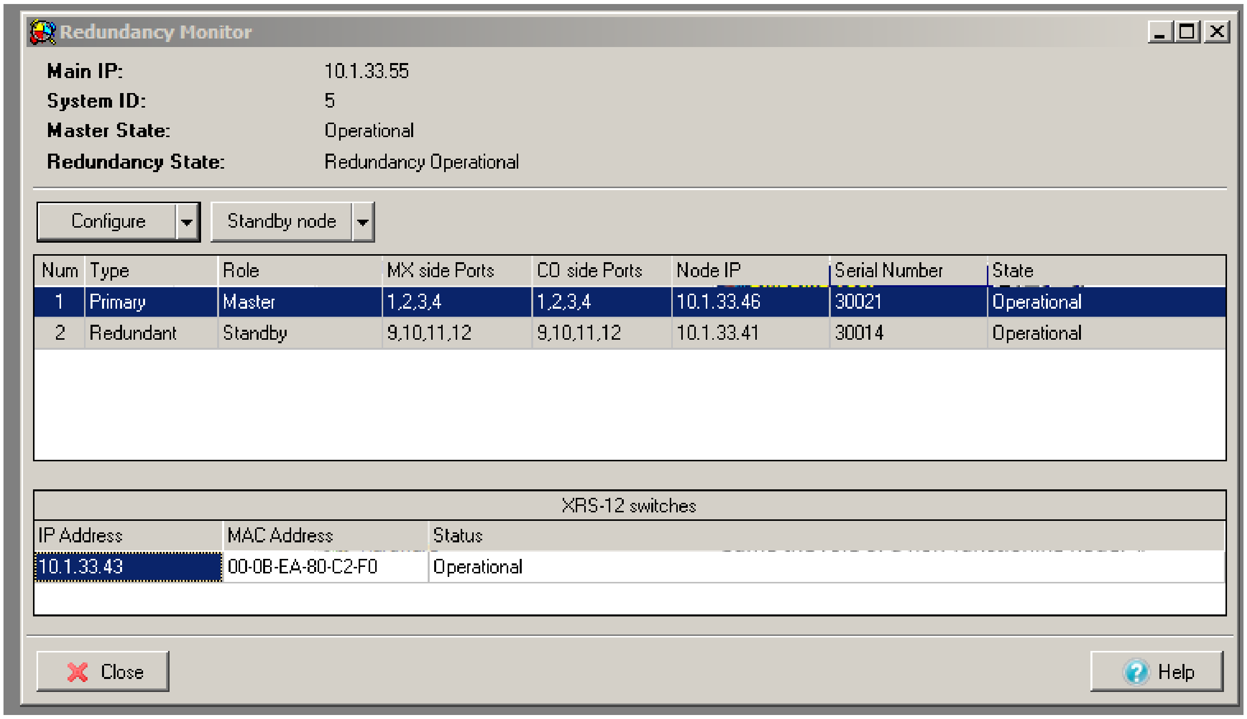
After joining the cluster MX will be restarted. Admin UI will be closed.
You will not be able to connect to this MX directly any more.
You should connect to the MX which is the master of the MXcluster.

Do you want to proceed and join the MXcluster?

Redundancy Monitor

The Redundancy Monitor window displays the Primary/Redundant Nodes and their status. You can perform controlled switchovers and switchbacks, monitor the redundancy status, observe the Redundant configuration, and disband the Redundancy from the Monitor.

To access this window, select *File/MX Redundancy* from the main menu.



Main IP: 10.1.33.55
System ID: 5
Master State: Operational
Redundancy State: Redundancy Operational

Num	Type	Role	MX side Ports	CO side Ports	Node IP	Serial Number	State
1	Primary	Master	1,2,3,4	1,2,3,4	10.1.33.46	30021	Operational
2	Redundant	Standby	9,10,11,12	9,10,11,12	10.1.33.41	30014	Operational

XRS-12 switches

IP Address	MAC Address	Status
10.1.33.43	00-0B-EA-80-C2-F0	Operational

Status Parameters

The top section of the Redundancy Monitor identifies and provides status information about it.

System ID: This parameter indicates the identification number of the Redundancy. Member nodes must use this number when joining a redundancy.

Master State: This mode specifies the operational status of the MX-E master node.

Redundancy State – This mode specifies the operational status of the MX-E Redundant/Standby node.

- **Switched Standby** – This setting indicates the Redundant Node has assumed the role of a Master or Member node. The replaced node assumes the standby role. If the Standby Node is operational, it can protect against the failure of the Redundant Node. A switchback operation must be performed to restore full redundancy protection to the redundancy.
- **Redundancy Operational** – This setting indicates that the Redundant Node is operational, the redundancy is in Normal mode, and the redundancy is protected against the failure of the Primary or Redundant Nodes.
- **No Redundancy License** – This setting indicates that the current system, although configured for redundancy, cannot provide redundancy protection because a valid redundancy license does not exist on the Primary or Redundant Nodes.
- **Master Selection Required** – This setting indicates that, after a Master Node switchback, the Primary and Redundant Nodes have each attempted to operate as the Master Node. Full redundancy protection is not provided in this state. To select one of the nodes as the permanent master, press the *Master selection* button at the bottom of the panel.

Redundancy Node table

The Redundancy Node table lists the attributes of each MX-E system. Each row represents one MX-E system. The rows are ordered by the role of the system. The top row is always the Master Node. In a redundant system, the bottom row is always the Standby Node.

Type: This column identifies the MX-E systems as the Primary or Redundant Node.

Role: This column indicates the function of the MX system. The Master Node is always at the top of the list. The Standby Node, if operational, provides redundancy protection to the Primary. In Normal mode, the Standby Node is the

Redundant Node. In Switchover mode, the Standby Node is the system that was replaced.

MX side Ports: Routing telephony circuits from each node through an XRS12 Metallic Switch to the PSTN protects the redundancy's access to these circuits if a redundant system fails. This parameter specifies the set of XRS12-MX ports to which the MX system's telephony circuits are connected.

CO side Ports: This parameter specifies the XRS-CO ports to which the node's telephony circuits are routed. These ports typically connect to the PSTN. Normally, the CO side port numbers are identical to the MX side Port numbers for Master and Member nodes unless the redundancy is in switch over mode.

Node IP: This parameter indicates the Main IP address of the redundancy.

Serial Number: This parameter indicates the IP address of the MX system.

State: This parameter indicates the operational status of the MX system. The following state values are listed in order of functionality:

- **Operational** – This status indicates that the MX system is operating normally.
- **Initializing** – This status indicates that the MX system booted up properly and is now initializing.
- **Upgrading** – This status indicates that the MX system is upgrading its software.
- **Booting** – This status indicates that the MX system is booting up.
- **Waiting for node** – This status indicates that Redundancy was unable to locate the MX system at the provided IP address.
- **Failed** – This status indicates that the MX system is not functioning properly or was unable to boot up or initialize.

XRS-12 Switch table

The Metallic Switch table, when displayed by the Redundancy Monitor, lists the XRS12 switches that support the redundancy specified by the monitor. Each XRS12 switch must reside on the same subnet as the redundancy.

IP Address: This parameter indicates the IP address of the XRS12 switch.

MAC Address: This parameter indicates the MAC address of the XRS12 switch.

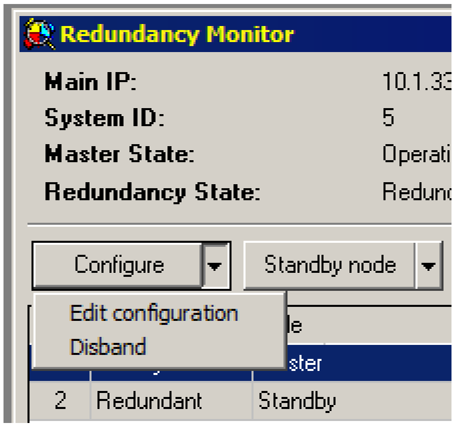
Status: This parameter indicates the operational status of the XRS12 switch. The status variable is set to one of the following values:

- **Operational** – This status indicates that the switch is operating normally.
- **Upgrading** – This status indicates that the switch is upgrading its software. Although PSTN redundancy is disabled until the upgrade is completed, PSTN service is not disrupted.
- **Unknown** – This status indicates that the redundancy is unable to locate the XRS12 switch at the configured address.

Click *Configure* button to edit the parameters of the XRS12 switches in the redundancy. This is required when replacing a switch or changing the IP address. Changing the XRS12 IP addresses will cause the redundancy to reboot the XRS12, but the systems within the redundancy do not reboot.

Editing the Redundancy Monitor

Operations that can be performed from the Redundancy Monitor include editing, disbanding, switchovers, switchbacks, and shutting down the Standby node, and selecting a Master Node. To edit the Redundancy configuration, click the *Configure* button and Edit configuration



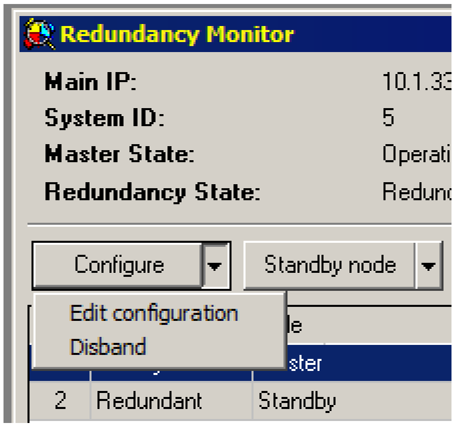
Main IP: 10.1.33
System ID: 5
Master State: Operati
Redundancy State: Redund

		le
		ster
2	Redundant	Standby

Disbanding the Redundancy

This operation removes the Redundant relationship between the nodes and places each in standalone mode. The Primary Node retains the data as configured for the entire redundancy. The Redundant Node retains the data that was stored within their MX system prior to the creation of the Redundancy. The Redundant Node is cleared of its configuration and data.

- To disband, press the Disband button from the list of options provided by the *Configure* button.



Redundancy Monitor

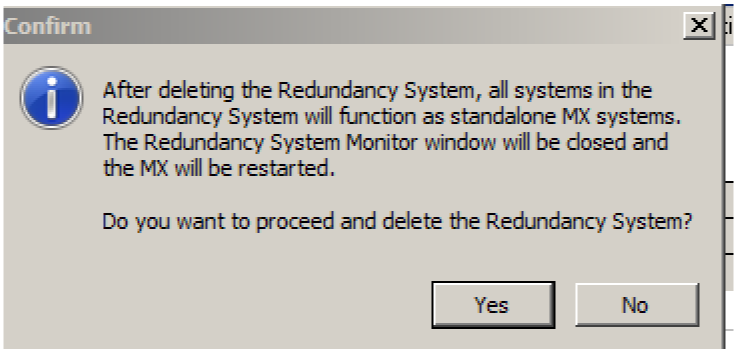
Main IP: 10.1.33

System ID: 5

Master State: Operati

Redundancy State: Redunc

- Confirm the procedure at the warning message:



Confirm

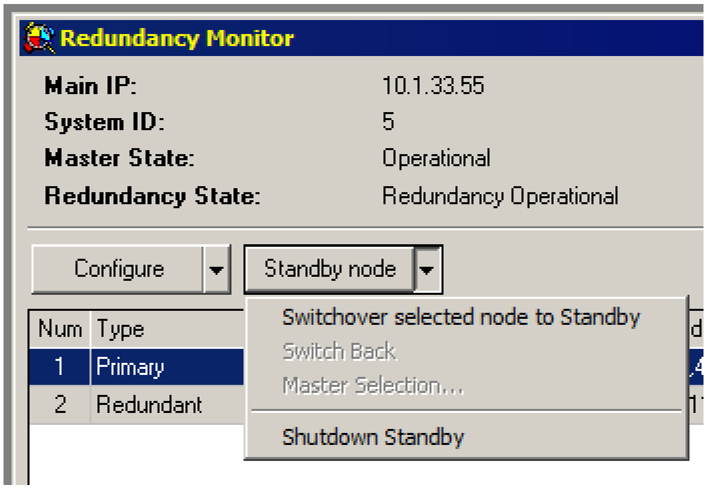
After deleting the Redundancy System, all systems in the Redundancy System will function as standalone MX systems. The Redundancy System Monitor window will be closed and the MX will be restarted.

Do you want to proceed and delete the Redundancy System?

Switch Over

The switch over operation replaces the specified Primary Node with the Redundant Node. A switchover is automatically performed if the Primary Node fails.

To perform a controlled switchover, select the Primary Node in the table, right click the mouse and select *SwitchOver to standby,* or select *SwitchOver selected* *node to Standby* from the *Standby node* button. You can only perform a switchover if the Redundancy State is Redundancy Operational.



Redundancy Monitor

Main IP: 10.1.33.55
System ID: 5
Master State: Operational
Redundancy State: Redundancy Operational

Num	Type
1	Primary
2	Redundant

Switch Back

The switch back operation is performed when the redundancy is in the switched over state to re-establish redundancy. The node that was replaced by the Redundant Node must be operational in order to perform the switch back.

To perform a switchback, click the *Switch Back* link from the *Standby node* button . If the button is inactive, the redundancy is not in Switchover mode or the switched MX system is not functional as a redundancy node.

Shutdown Standby

The *Standby node* button allows for shutting down the MX-E system operating as the Standby role. When you restart the system, the system attempts to rejoin the Redundancy.

Master System Selection

If the Primary and Redundant Nodes simultaneously attempt to act as the Master Node, Redundancy automatically assigns one mode as the Active Master and the other to Passive Standby status. In this state, the Standby Node is not mirroring the Master Node, which disables redundancy. The *Master Selection* button is visible only when the Redundancy State is Master Selection Required. Click this button to select a permanent Master Node and restore redundancy.

1:1 Redundancy

A single XRS12 switch is required to protect four PCM circuits from the Primary Node. If you are using redundant with PCM circuits, Zultys recommends using an XRS12. The XRS12 is a physical relay switch used to switch over the PCM circuits. There is no GUI or configuration on the XRS12. Configuration for XRS12 is transferred from the MX system to the device on boot up. When the XRS12 is booted, it will get an IP address via DHCP, and use option 66 to download its configuration file. DHCP with option 66 is a requirement for installing an XRS12. Once the XRS12 has received its configuration file, it will use its static IP address. It is required that the MAC address of the XRS12 is programmed in the MX and set correctly.

Redundancy protection for the PCM circuits in your redundancy requires an XRS12 switch. The following sections specify the recommended XRS12 connection configurations. Each XRS12 switch must reside on the same subnet as the redundancy.

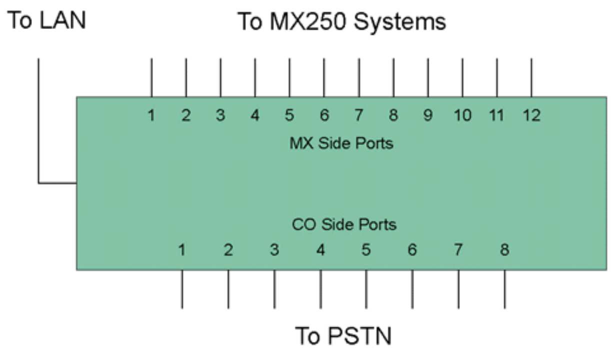
Integrating with XRS12

1.6.1 XRS12 Ethernet

The XRS12 is a metallic switch that connects the MX-E PCM circuits from the Redundancy to the PSTN. If the primary system fails, the XRS12 replaces the PSTN circuits from that Node with the PSTN circuits from the Redundant Node. The XRS12 switch is not a mandatory redundant of a redundancy if PSTN circuit redundancy is not required.

The XRS12 comprises 13 input ports and 8 output ports

- 12 input ports receive T1 signals from the MX250 system
- 1 input port receives a control signal from the LAN
- 8 output ports sends T1 signals to the Central Office



The PCM circuits from the Primary and Redundant Nodes connect to MX Side Ports 1-8. During normal redundancy operation, these input ports connect directly to the eight CO Side Ports. PCM circuits from the Redundant Node connect to MX Side Ports 9-12

These ports do not connect to the CO Side Ports unless the Primary Node or one of the Redundant Nodes fails. In this case, the XRS12 switches the input ports from the Redundant Node to replace the PCM signals from the failed system.

10/100Base-T

The XRS12 has one 10/100Base-T Ethernet circuit that connects the XRS12 to your LAN. The XRS12 receives switching commands from the MX250 and communicates the operational status of the internal switch over the Ethernet circuit. The circuit does not supply Power over Ethernet.

PSTN Circuits

The XRS12 has 20 RJ45 connectors that transport telephony signals between MX-E systems and the PSTN. Each connector supports a PRI transmission.

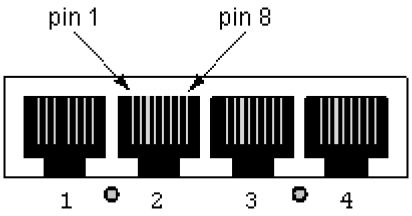
- MX Ports: MX 1 through MX 12 connects to a MX250 PCM circuits.
- CO Ports: CO1 through CO8 connect to a PSTN facility compatible with MX port circuits.

PCM RJ45 Pin Assignments

The image below shows the pin assignment and placement of the RJ45 connectors when transmitting PCM data. All connectors have the same PCM pin assignment.

Pin Description of a PCM RJ45 Connector

1	*Received Data, ring*	*XRS12*	Facility
2	*Received Data, tip*	*XRS12*	Facility
3	*Not connected*		
4	*Transmitted Data, ring*	*MX250*	XRS12
5	*Transmitted Data, tip*	*MX250*	XRS12
6	*Not connected*		
7	*Not connected*		
8	*Not connected*		

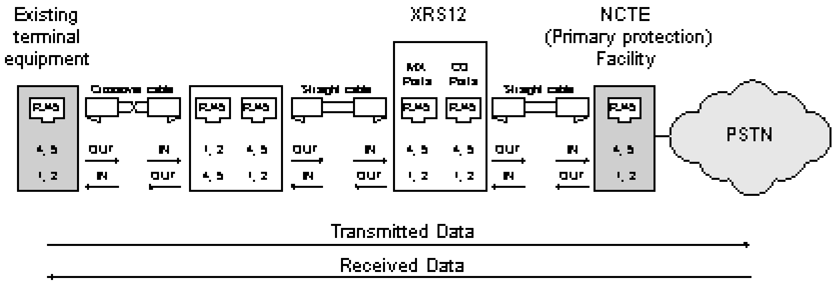


Use a PCM crossover cable when connecting two XRS12 ports to create a feedback loop for PCM transmissions. Verify that pins 3, 6, 7, and 8 on each cable end are not connected to any pin on either end of the cable.

It is not recommended to use a CTA5 cable for the PSTN connections as it will create circuit errors. You must use a proper PCM cable.

The image below displays PCM circuit connections and pinouts typically used for terminal and network equipment. Use a straight PSTN cable to connect the XRS12 to MX-E systems and to existing terminal systems (such as a PBX). Refer to device documentation to confirm pin assignments.

<u>Wiring PCM Circuits to the Network or Other Equipment</u>



Connecting the XRS12 to an MX-E Redundancy

Configuring an XRS12

There is no configuration that is done on the XRS12 itself, all configuration is done in the Redundancy configuration wizard on the MX-E. The XRS12 relies on DHCP with option 66 referencing the MX-E for the XRS12 to download its configuration. The MX-E creates a configuration file on the Primary Node for the XRS12 to download.

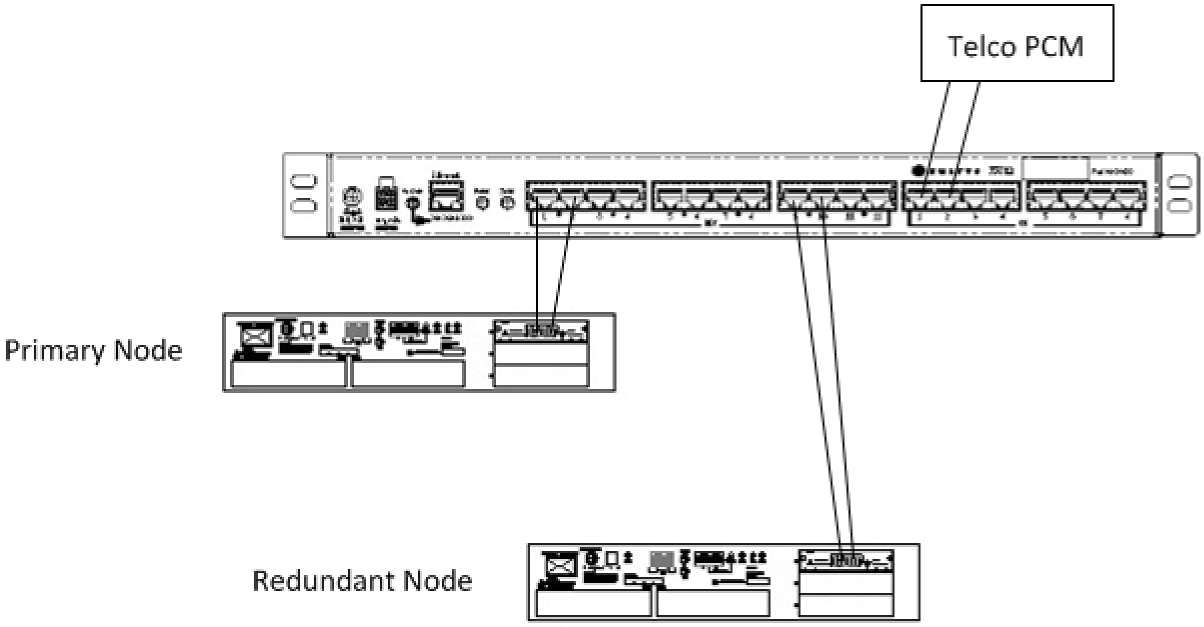
XRS12 used in a 1:1 Redundant Redundancy

The image below displays the connection of two MX-E systems to an XRS12 switch in a 1:1 Redundancy. PCM cards must be placed in each MX-E and connecting cables must be routed as below. Straight cables are required to connect the XRS12 to the MX-E systems.

If an Redundancy node fails, the Redundancy performs a switchover. The Redundant Node functions in place of the failed node and the XRS12 switches Redundant Node's PCM circuits to replace circuits from the failed node. Port LEDs for failed node ports turn off, while Redundant Node's LEDs turn green.

- Primary Node PCM Circuit 1 connects to XRS12 Port 1
- Primary Node PCM Circuit 2 connects to XRS12 Port 2
- Redundant Node PCM Circuit 1 Connects to XRS12 Port 9
- Redundant Node PCM Circuit 2 Connects to XRS12 Port 10
- Telco PCM Circuit 1 Connects to XRS12 Telco Circuit 1
- Telco PCM Circuit 2 Connects to XRS12 Telco Circuit 2

XRS12 in a 1:1 Redundant Redundancy Configuration



36. Regulatory Approvals

33.1 EMC

U.S.A.:

FCC Class A Notice

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Modifications: Any modifications made to this device that are not approved by Oracle may void the authority granted to the user by the FCC to operate this equipment.

Canada:

ICES-003 Class A Notice - Avis NMB-003, Class A

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia/ New Zealand

AS/NZS CISPR 22:2009 + A1 :2010 for Information Technology Equipment.

CE

EN 55024:2010

EN 300 386 V1.6.1 (20112-04)

EN 55022:2010/AC :2011

EN 61000-3-3:2008

36.2 SAFETY

UL 60950-1, 2nd Edition, 2011-12-19 (Information Technology Equipment - Safety - Part 1)

CSA C22.2 No. 60950-1-07, 2nd Edition, 2011-12 (Information Technology Equipment - Safety - Part 1)

IEC 60950-1(ed.2)

IEC 60950-1(ed.2);am1

CB CERTIFICATE # US-23669-UL

36.3 TELECOM

U.S.A.

FCC 47 CFR, Part 68

TIA-968-B - August 2009,

TIA-968-B-1 (Addendum to TIA-968-B), August 2012

TIA-1096

37. SRTP

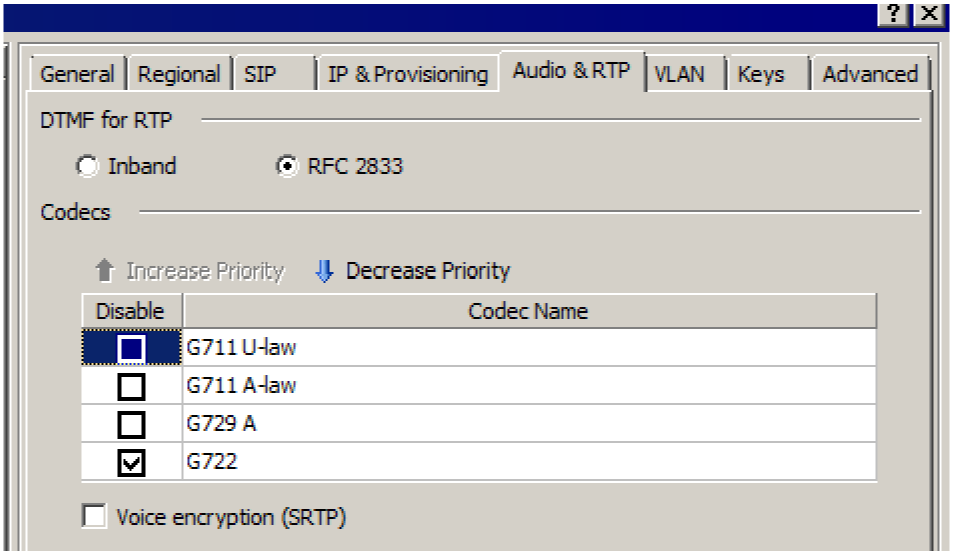
The **Secure Real-time Transport Protocol** (or **SRTP**) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity. SRTP provides an extra layer of security for real time voice/fax traffic.

SRTP in MX Release 13.0.2 allows ZIP3/Polycom, MXIE/ZAC softphone phone to phone calls to be encrypted for additional security. In addition, Codec profiles that utilize SRTP can be created for external SRTP traffic.

Administration

MX Administrator Configure\Devices\Profiles

- Select a ZIP 3 or Polycom profile
- Go to the Audio & RTP tab
- Check the Voice Encryption (SRTP) item



DTMF for RTP

○ Inband ● RFC 2833

Codecs

Disable	Codec Name
□	G711 U-law
□	G711 A-law
□	G729 A
☑	G722

☐ Voice encryption (SRTP)

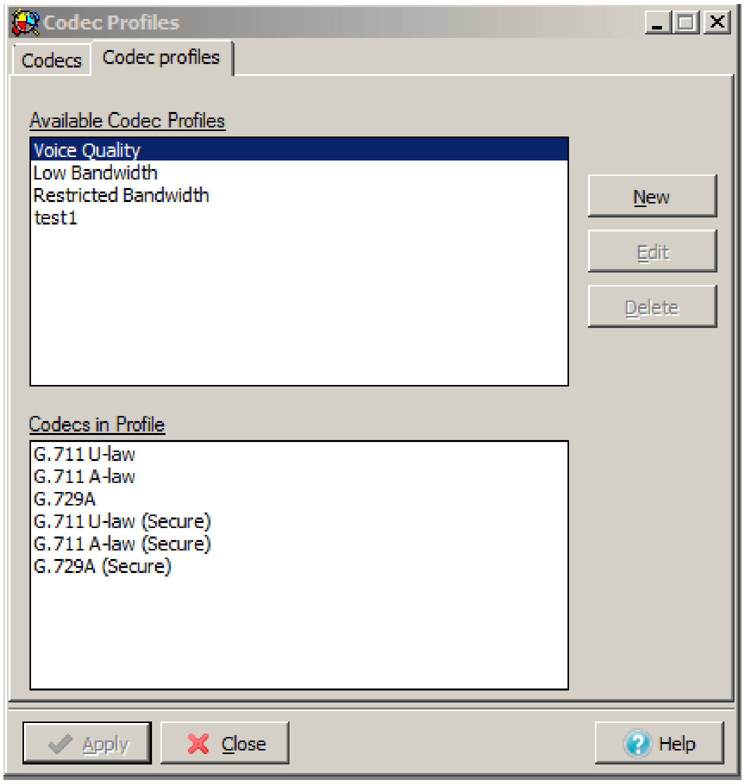
- Click OK then Apply

MX Administrator\Provision\Codecs\Codec Profiles

Secure Codec profiles can be setup in the Codec Profile area.

You can create secure codec profiles for:

- G.711 U-law
- G.711 A-law
- G.729A



Available Codec Profiles: Voice Quality, Low Bandwidth, Restricted Bandwidth, test1

Codecs in Profile:
G.711 U-law
G.711 A-law
G.729A
G.711 U-law (Secure)
G.711 A-law (Secure)
G.729A (Secure)

Note: Zultys has not performed any certifications with ITSPs or other external sources utilizing SRTP codecs.

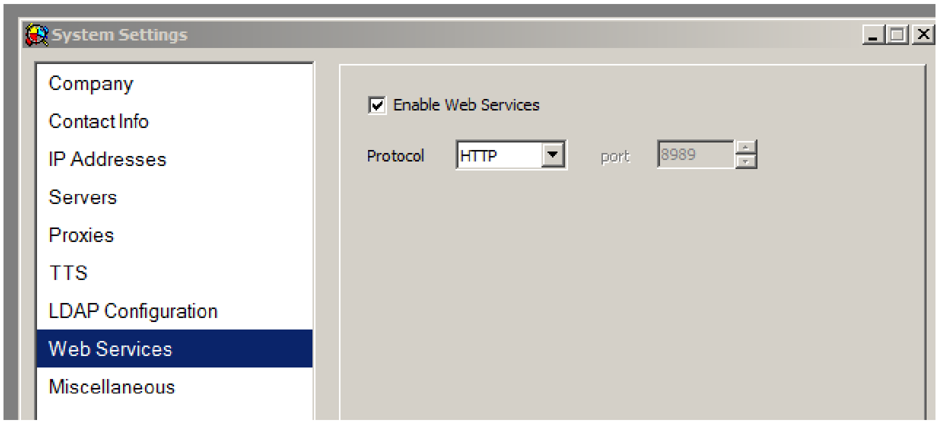
38. Web Based User Portal

This feature allows a user to access via a web browser a portal to perform viewing/administration functions of certain user features. These features are address book, call handling rules, and voicemail notification rules.

MX Administrator

Provision\System Settings\Web Services

Check the “Enable Web Services” item and click Apply.



☑ Enable Web Services

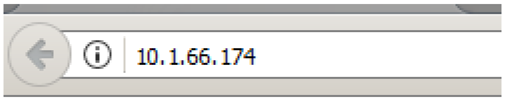
Protocol: HTTP

port: 8989

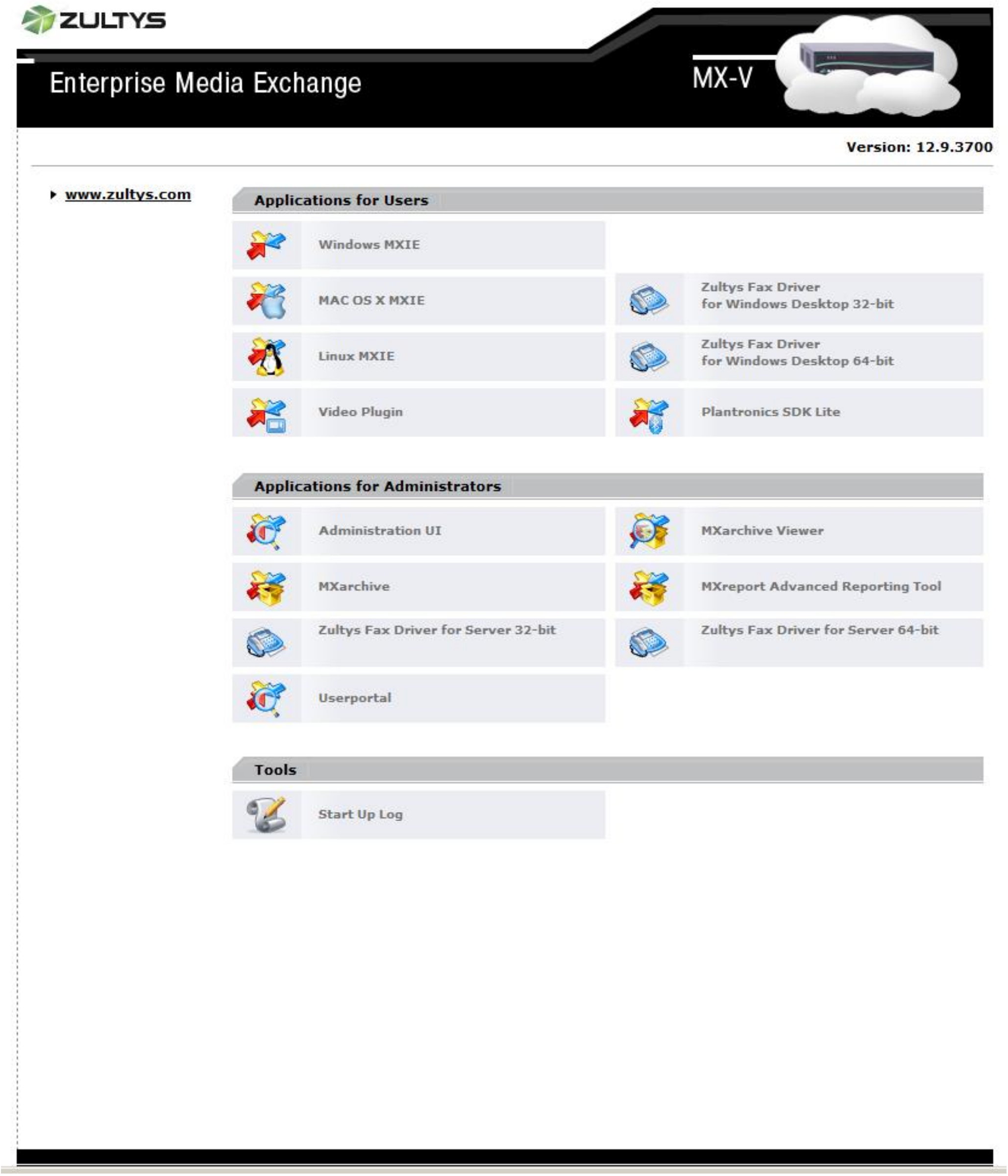
- Make sure that Port 443 is accessible!
- Insure there is a security certificate installed for HTTPS.

Login to User Portal

- From a browser, type the domain name or IP address of the MX system in the URL bar:
- You will reach the MX system landing page.



10.1.66.174



ZULTYS

Enterprise Media Exchange

MX-V

Version: 12.9.3700

▸ www.zultys.com

Applications for Users

Windows MXIE	
MAC OS X MXIE	Zultys Fax Driver for Windows Desktop 32-bit
Linux MXIE	Zultys Fax Driver for Windows Desktop 64-bit
Video Plugin	Plantronics SDK Lite

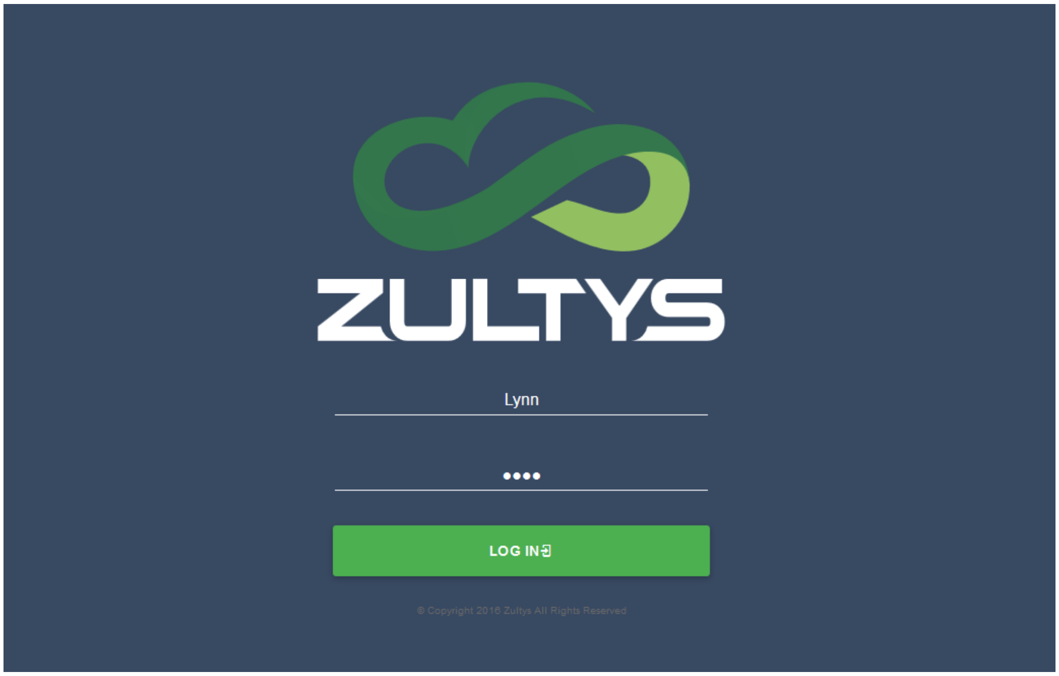
Applications for Administrators

Administration UI	MXarchive Viewer
MXarchive	MXreport Advanced Reporting Tool
Zultys Fax Driver for Server 32-bit	Zultys Fax Driver for Server 64-bit
Userportal	

Tools

Start Up Log

- Select the Userportal option on the page
- Enter the user login information:
- Username/password
- Click LOG IN

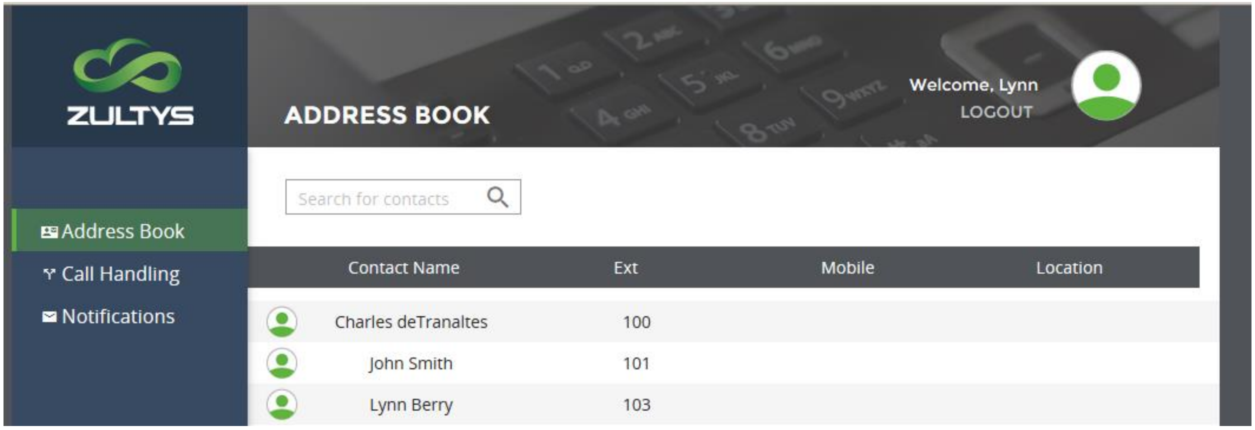


Lynn

••••

© Copyright 2016 Zultys All Rights Reserved

After a successful login with the user name and password, the main user portal is presented:



Contact Name	Ext	Mobile	Location
Charles deTranaltes	100		
John Smith	101		
Lynn Berry	103		

- To Logout of the portal, click the LOGOUT button.

Address Book

This allows users to view the contacts in the system. The user can view contact name, Extension, Mobile phone, and location.

They can also utilize the search function to search for a particular contact.

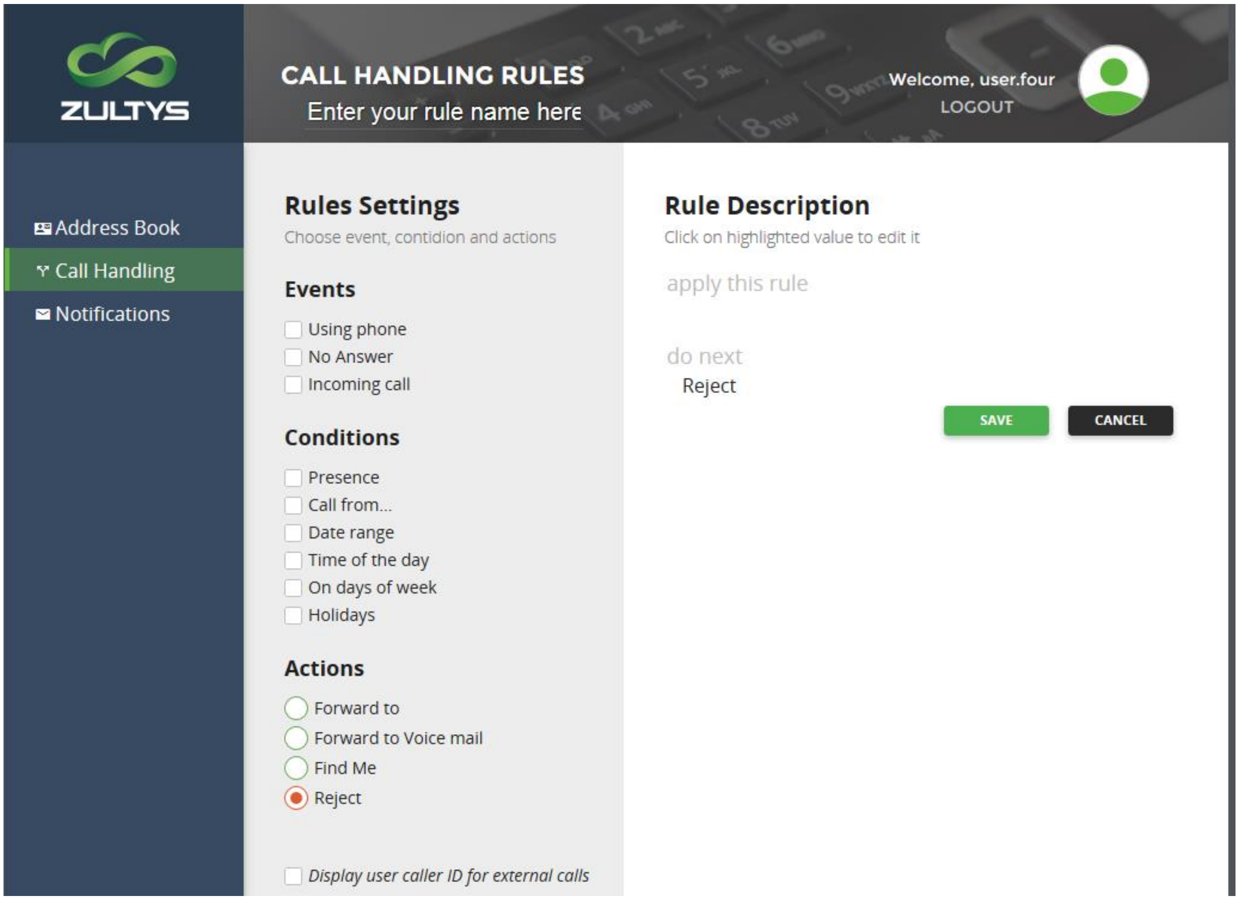
Call Handling Rules (CHR)

This area allows a user to create, modify, or delete their call handling rules (CHR).

Create:

To create a new call handling rule:

Click the + icon.



Rules Settings

Choose event, contidion and actions

Events

□ Using phone
□ No Answer
□ Incoming call

Conditions

□ Presence
□ Call from...
□ Date range
□ Time of the day
□ On days of week
□ Holidays

Actions

○ Forward to
○ Forward to Voice mail
○ Find Me
● Reject

□ *Display user caller ID for external calls*

Rule Description

Click on highlighted value to edit it

apply this rule

do next

Reject

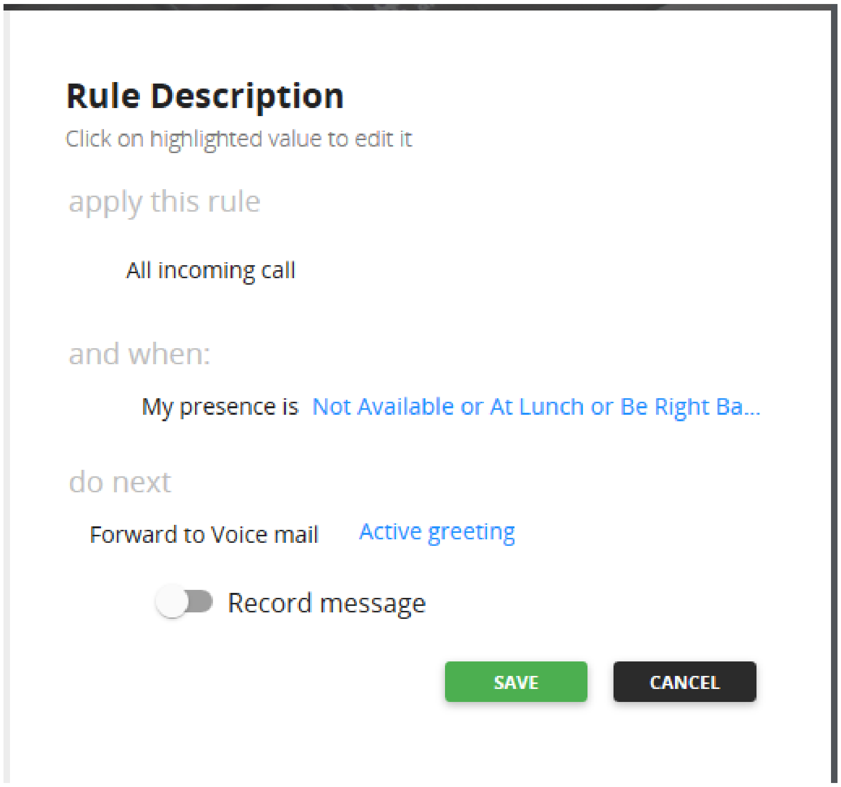
Enter the rule name at the top of the screen. You must delete the existing text first.

Check the desired Event(s) that apply to the rule. Note that if you select Incoming call, that is the only selection allowed. You may combine the Using phone and No Answer events.

As you enter Events, the Rule Description area will update. Depending on the selection, additional information may need to be added in this area. Information will be highlighted in this area when input is required.

Check the desired Conditions for the rule. As you enter Conditions, the Rule Description area will update. Depending on the selection, additional information may need to be added in this area. Information will be highlighted in this area when input is required.

Check the desired Actions for the rule. As you enter Actions, the Rule Description area will update. Depending on the selection, additional information may need to be added in this area. Information will be highlighted in this area when input is required.



Rule Description

Click on highlighted value to edit it

apply this rule

All incoming call

and when:

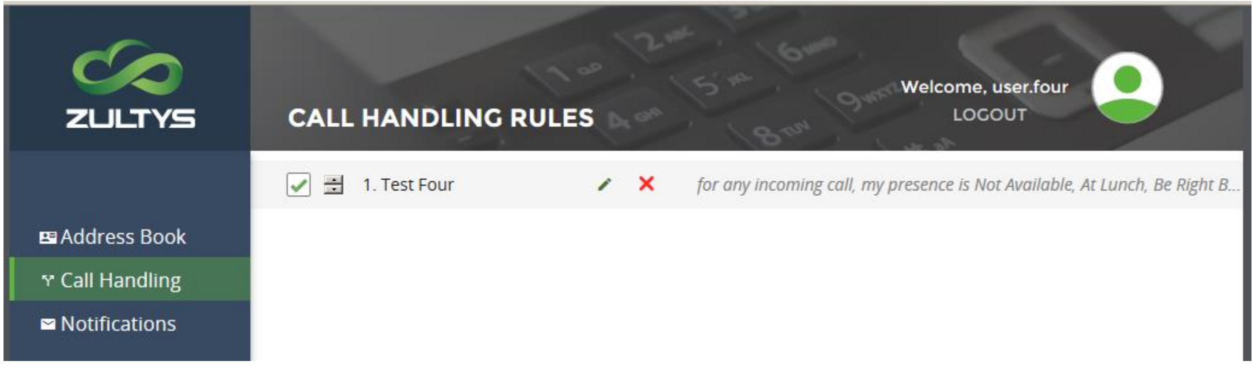
My presence is Not Available or At Lunch or Be Right Ba...

do next

Forward to Voice mail Active greeting

Record message

- Click Save when you are finished creating the rule.
- The new rule will now appear in the list of Call Handling Rules.



☑ 1. Test Four — for any incoming call, my presence is Not Available, At Lunch, Be Right B...

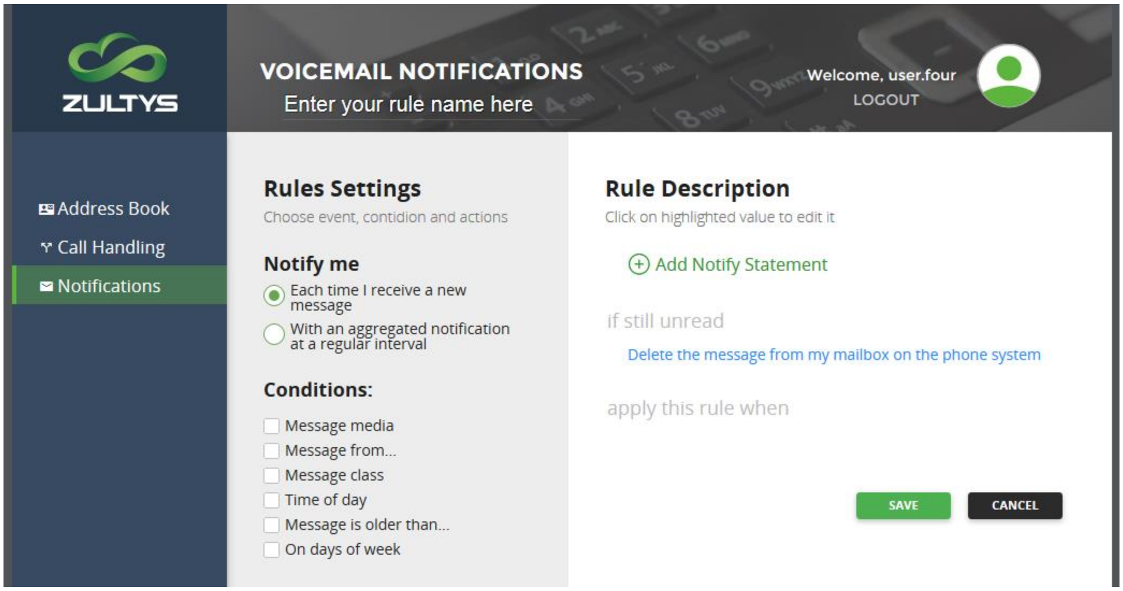
You may double-click or select the edit icon to modify the rule. You may delete the rule by clicking the delete icon.

Voicemail Notifications

This area allows a user to create, modify, or delete their Voicemail Notification rules.

- Create:
- To create a new Voicemail Notification rule:

Click the + icon.



VOICEMAIL NOTIFICATIONS
Enter your rule name here

Welcome, user.four
LOGOUT

Address Book
Call Handling
Notifications

Rules Settings
Choose event, contidion and actions

Notify me
● Each time I receive a new message
○ With an aggregated notification at a regular interval

Conditions:
□ Message media
□ Message from...
□ Message class
□ Time of day
□ Message is older than...
□ On days of week

Rule Description
Click on highlighted value to edit it

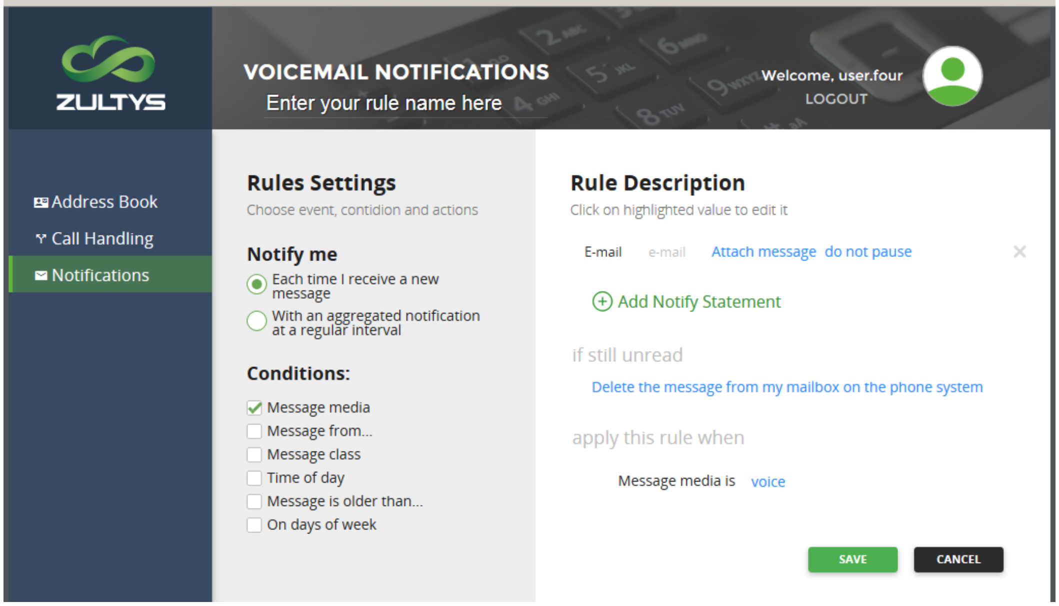
⊕ Add Notify Statement

if still unread
Delete the message from my mailbox on the phone system

apply this rule when

SAVE CANCEL

- Enter the rule name at the top of the screen. You must delete the existing text first.
- Check the desired Notify me conditions that apply to the rule.
  As you enter information, the Rule Description area will update. Depending on the selection, additional information may need to be added in this area. Information will be highlighted in this area when input is required.
- Check the desired Conditions for the rule. As you enter Conditions, the Rule Description area will update. Depending on the selection, additional information may need to be added in this area. Information will be highlighted in this area when input is required.



VOICEMAIL NOTIFICATIONS
Enter your rule name here

Rules Settings
Choose event, contidion and actions

Notify me
● Each time I receive a new message
○ With an aggregated notification at a regular interval

Conditions:
☑ Message media
□ Message from...
□ Message class
□ Time of day
□ Message is older than...
□ On days of week

Rule Description
Click on highlighted value to edit it

E-mail e-mail Attach message do not pause ×

⊕ Add Notify Statement

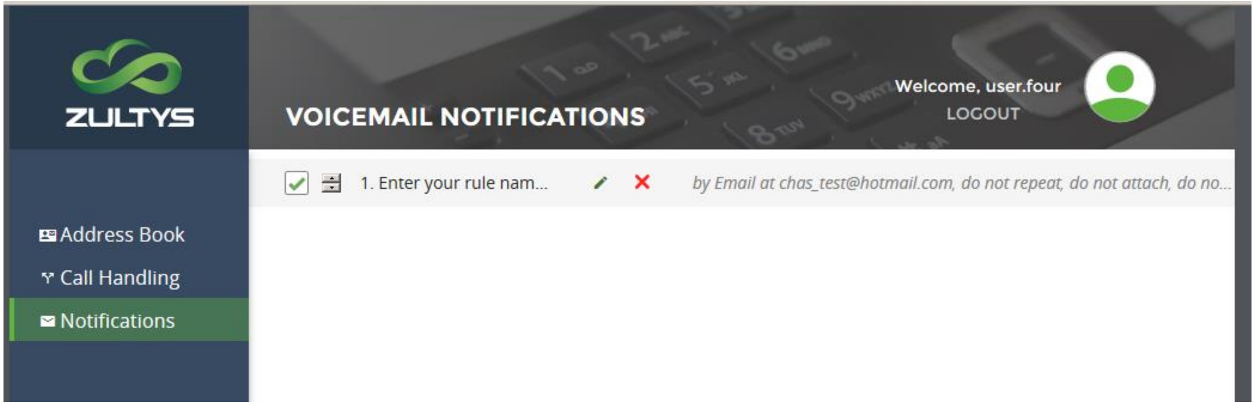
if still unread
Delete the message from my mailbox on the phone system

apply this rule when
Message media is voice

SAVE CANCEL

- Click Save

The new rule will now appear in the list of Voicemail Notifications rules.



VOICEMAIL NOTIFICATIONS

☑ 1. Enter your rule nam... *by Email at chas_test@hotmail.com, do not repeat, do not attach, do no...*

You may double-click or select the edit icon to modify the rule. You may delete the rule by clicking the delete icon.

39. Return Customer Routing

This feature provides two methods for callers who have previously called an ICC group to have special routing treatment applied upon a returning call.

Last Agent Assigned

This option will allow a caller reaching the ICC group to be routed to the last agent they spoke with. If caller with matching callerID/DID returns within the specified timeframe, MX will try to route the caller to the last assigned agent for that caller.

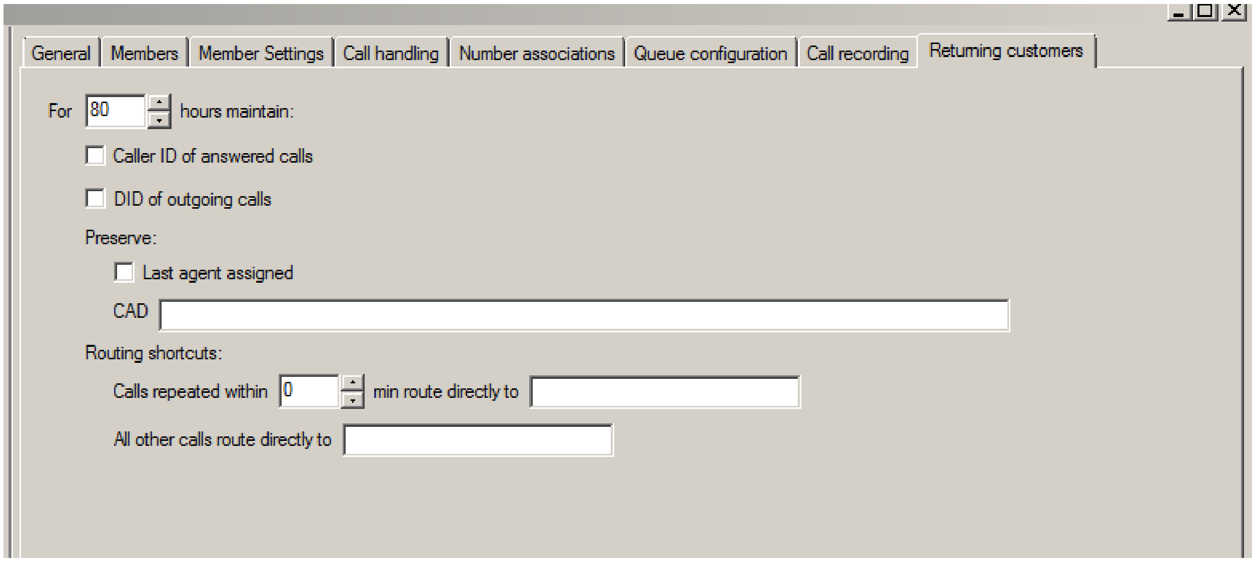
Routing shortcuts

The MX will analyze callerID information and apply a routing shortcut to a programmed destination if the caller has called back within the specified timeframe. This applies after the caller has initially reached the group and the MX has captured CallerID/DID information. Please note that this will allow a returning caller to bypass system routing via dial plan. Destinations can be AA scripts, call group extensions, extensions. *Please note that this routing decision takes place prior to the dial plan processing of the incoming call.*

MX Administration

MX Administrator\Configure\Operator and Call Groups\ICC type

Select the Returning customers tab



For 80 hours maintain:

☐ Caller ID of answered calls

☐ DID of outgoing calls

Preserve:

☐ Last agent assigned

CAD

Routing shortcuts:

Calls repeated within 0 min route directly to

All other calls route directly to

- Enter the desired storage time for the MX to maintain callerID and DID numbers. Values are from 1 to 80.

- Select if the MX is to maintain callerID and/or DID numbers

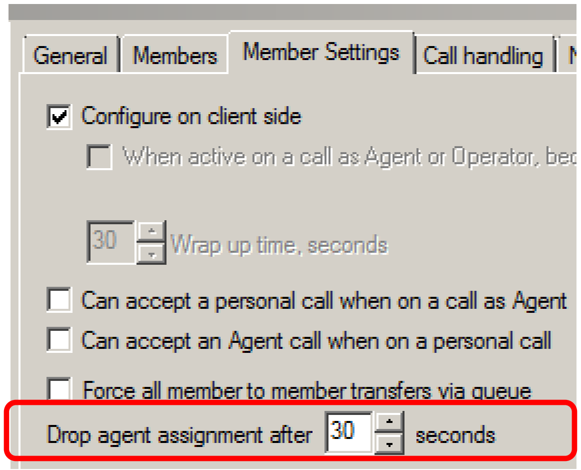
- Select if the MX is to maintain the last agent assigned to the caller.

- Enter any CAD values to be associated with the call.

Conditions

- If last agent is logged out, returning caller will be routed to the next available agent, their call has highest queue priority.

- If last agent is busy, caller will wait for that agent for the length of the Drop Agent Assignment in the Member Settings tab. On expiration, caller is routed to next available agent and the call has the highest priority.



☑ Configure on client side

□ When active on a call as Agent or Operator, bec

30 Wrap up time, seconds

□ Can accept a personal call when on a call as Agent

□ Can accept an Agent call when on a personal call

□ Force all member to member transfers via queue

Drop agent assignment after 30 seconds

40. Unmanaged Device Password

This feature provides a mechanism for the MX to generate SIP authentication passwords for unmanaged devices. This reduces vulnerability due to the usage of weak PINs that are utilized by many users.

Note: Zultys strongly recommends the regeneration of unmanaged device passwords to provide unauthorized access due to weak passwords.

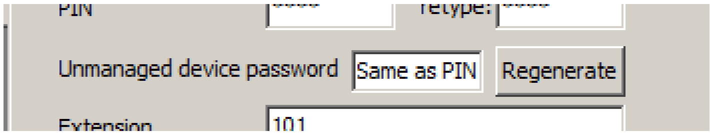
MX Administration

MX Administrator\Configure\Users

Single User:

Select the desired user from the user list.

Click the Regenerate button for Unmanaged device password.

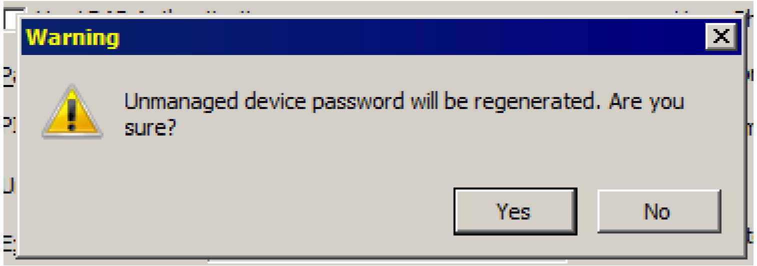


PIN ••••• retype: •••••

Unmanaged device password Same as PIN

Extension 101

Click Yes at the Warning dialog:



Warning

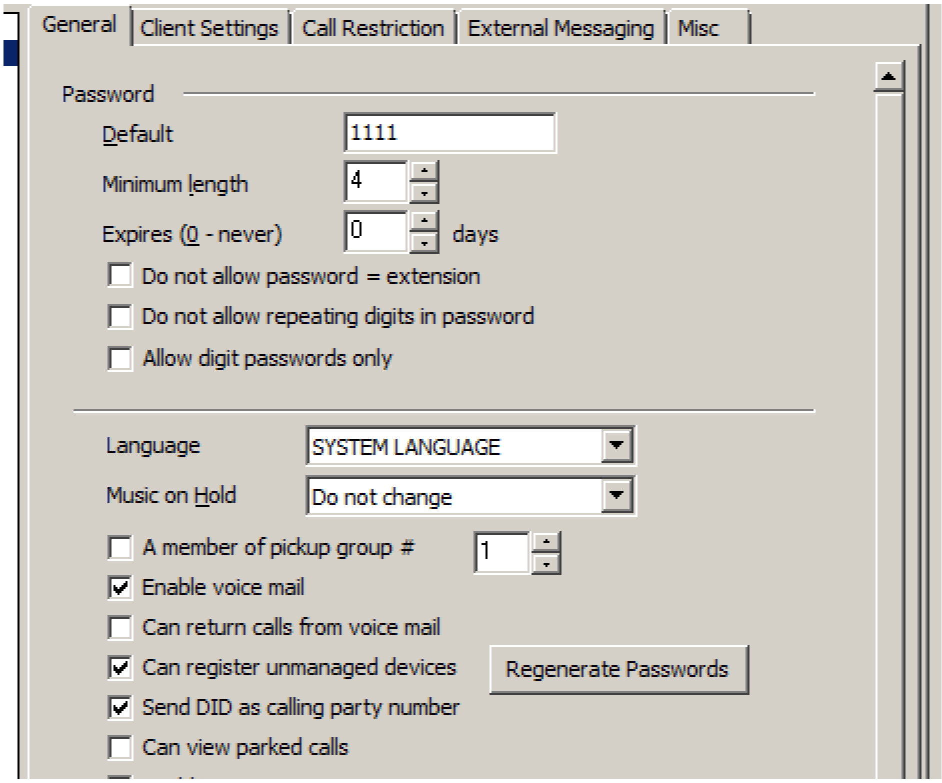
Unmanaged device password will be regenerated. Are you sure?

Make note of the new password.

User Profile:

Select the desired Profile from the user list.

In the General tab, click the Regenerate Passwords button next to “Can register unmanaged devices”.



Password

Default 1111

Minimum length 4

Expires (0 - never) 0 days

□ Do not allow password = extension

□ Do not allow repeating digits in password

□ Allow digit passwords only

Language SYSTEM LANGUAGE

Music on Hold Do not change

□ A member of pickup group # 1

☑ Enable voice mail

□ Can return calls from voice mail

☑ Can register unmanaged devices

☑ Send DID as calling party number

□ Can view parked calls

Conditions

- The MX will generate a Syslog event when an unmanaged device utilizing a weak password is registered.

  "Unmanaged device registered with weak password:", " DeviceID = %s, UserAgent = %s."
- Examples of weak passwords:

  – using user name, extension or login name is reducing the password bit length.

  – Passwords with characters in sequence, 12345.