

MiVoice MX-ONE

Installation and Configuration Guide for GX and EX Controller

Release 7.4 SP1

April 13, 2022



Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

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

®, ™ Trademark of Mitel Networks Corporation
© Copyright 2022, Mitel Networks Corporation
All rights reserved

Contents

Chapter: 1	Introduction	1
Chapter: 2	Prerequisites	2
Chapter: 3	Upgrading Firmware In A GX-Gateway / EX-Controller	3
	Firmware Upgrade	3
	Setup of Communication Server	3
	Firmware Installation	4
	Special Actions for Firmware Upgrade of EX-Controller	4
	Rollback to Previous Firmware	5
Chapter: 4	Setting up Virtual Machine in an EX-Controller	6
	Install and Configure Virtual Machine	6
	Prerequisites	6
	Upload ISO-image to Internal Storage	7
	Create the Virtual Machine	8
Chapter: 5	Setting up MX-ONE for Branch Node Solution	12
	Number Analysis	12
	Extension Data	12
	Common Service Profile 9:	13
	Common Service Profile 11:	13
	Least Cost Routing Data	13
	Route Data	15
	ROCAP	15
	Route Category Data	15
	RODAP	15
	Route Data	15
	RODDP	16
	External Destination Route Data	16
	Number Prefixing	16

Route Number Data	16
SIP ROUTE	17

Chapter: 6

Setting up GX Gateway with ISDN Trunks 19

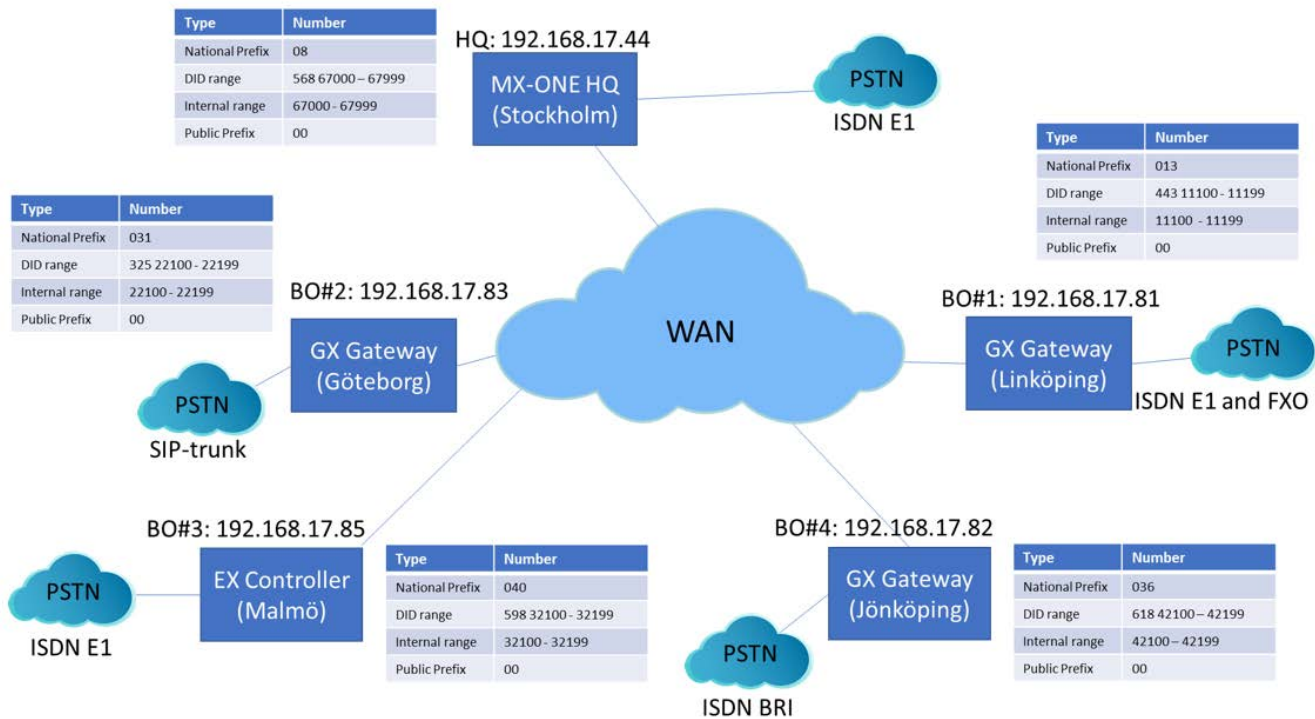
Logon	19
Network Settings	19
Host	19
Interfaces	21
Local Firewalls	21
Session Board Controller (SBC)	22
Configuration	23
Routing Rulesets	23
local_users_ca	25
trunk_lines_ca	28
MX-One_Lim1	29
MX-One_trunk	30
VOIP-trunk2	32
ISDN	33
Primary Rate Interface	33
Settings	33
Interop	34
Services	35
Basic Rate Interface	36
Settings	36
Interop	38
Services	39
POTS	40
Config	40
FXS Configuration	40
FXO Configuration	41
Status	41
FXO Dialing Configuration	43
Services	43
SIP	44
Gateways	44
Servers	45
Registrations	46
Authentication	47
Transport	48
Interop	48
Misc	49
Media	50
Codecs	50
Call Router	51
Route Config	51
Management	54

	Backup/Restore54
	File55
Chapter: 7	Setting up GX-GATEWAY with SIP Trunks	57
	Logon57
	Network Settings57
	Host57
	Interfaces59
	Local Firewalls59
	Session Board Controller (SBC)60
	Configuration60
	Routing Rulesets61
	local_users_ca63
	trunk_lines_ca66
	MX-One_Lim168
	MX-One_trunk68
	VOIP-trunk270
	SIP71
	Gateways71
	Servers72
	Registrations73
	Authentication73
	Transport74
	Misc74
	Media75
	Codecs75
	Call Router76
	Route Config76
	Management79
	Backup/Restore79
	File81
Chapter: 8	Known Limitations	82

Introduction

This document describes a typical scenario for a branch office with survivability and local presence. It contains both the GX and the EX gateways.

Figure 1.1: EX and GX Controller Gateways



Prerequisites

When planning the number series in the branch office following must be considered:

- The extension range must be coherent and matching the local DID number series (if local presence is used).
- MX-ONE SW must be at least version 7.0.
- The firmware level of the EX-Controller and GX-Gateway shall be at least **DGW 42.3.1032-MT** with profile 'S100-MT-D2000-45' for GX-Gateway and 'STNL-MT-D2000-65' for EX-Controller.

Other considerations/restrictions:

- A SIP outbound proxy address must be assigned in the startup.cfg file, that is, the SIP outbound proxy address is the local address of the EX-Controller or GX-Gateway.
- VDP log on with SCA/SCABR and EDN-numbers is not working when assigned to a soft key. A possible workaround can be for each SIP-line specify an outbound proxy and port. For example,
 - sip line3 outbound proxy: <IP-address of gateway>
 - sip line3 outbound proxy port: 5060

This must be repeated for each SIP-line that is allocated for SCA/SCABR or EDN.

- Make sure that sufficient SBC licenses are installed before starting to configure the system.

Upgrading Firmware In A GX-Gateway / EX-Controller

The setting up of MX-ONE is not described in this document since it does not differ from an ordinary MX-ONE set.

Firmware Upgrade

Firmware upgrade can be performed with several options:

Following are the two types of licenses:

- FTP
- TFTP
- HTTP
- HTTPS

Setup of Communication Server

- **FTP**

1. Set an FTP service on the assigned server.
2. Ensure that the FTP server can be reached by the GX Gateway / EX Controller unit.

NOTE: If the file server is located behind a firewall, ensure that the TCP port 21 is open.

- **TFTP**

1. Set a TFTP service on the assigned server.
2. Ensure that the TFTP server can be reached by the GX Gateway / EX Controller unit.

NOTE: If the file server is located behind a firewall, ensure that the TCP port 69 is open.

- **HTTP Server**

1. Set an HTTP service on the assigned server.
2. Ensure that the HTTP server can be reached by the GX Gateway / EX Controller unit.

NOTE: If the file server is located behind a firewall, ensure that the TCP port 80 is open.

- **HTTPS Server**

1. Set an HTTPS service on the assigned server.
2. Ensure that the HTTPS server can be reached by the GX Gateway / EX Controller unit.

NOTE: If the file server is located behind a firewall, ensure that the TCP port 443 is open.

3. Ensure that in the **Management/Certificates** tab, in the Certificate Import Through **Web Browser table**, there is a certificate that authenticates the HTTPS server selected in the Path field, and that Other is selected in the Type field.
4. Set the configuration parameters.

Copy the firmware program (.bin file), to the file server you have chosen to use (FTP, HTTPS, TFTP, or HTTP server).

Firmware Installation

When the communication server is ready with the new version of firmware.

1. Go to **Management > Firmware Upgrade**.

Figure 3.1: Firmware Upgrade



2. Enter the correct protocol and address information where the new firmware is located.

Figure 3.2: Firmware Packs Configuration

Firmware Packs Configuration	
Single File	
Mfp Url:	<input type="text" value="http://192.168.17.8/isoimages/43.1.1264-GX-50.bin"/>
Multiple Files	
Version:	<input type="text"/>
Firmware Pack:	<input type="text" value="Dgw"/>
Transfer Protocol:	<input type="text" value="HTTP"/> ▼
Host Name:	<input type="text" value="0.0.0.0"/>
Location:	<input type="text"/>
Transfer Credentials	
User Name:	<input type="text"/>
Password:	<input type="text"/>

3. Click **Apply & Install Now**.

Special Actions for Firmware Upgrade of EX-Controller

NOTE: If a Virtual Machine (VM) is running on the EX-Controller it is very important to shutdown of the operating system running on the EX-controller before doing any upgrade or reboot. The shutdown method must be the recommended method for the installed OS.

When the EX-Controller is upgraded to new firmware an extra step to finalize the upgrade procedure must take place.

When the new firmware is started a special script file must be executed to setup the SBC and SIP functionality.

1. Go to **Management > Configurations Scripts**.



2. Select the file **Survivability_Enable.cfg** from the drop-down menu.

Figure 3.3: Execute Scripts

Execute Scripts		
Transfer Parameters		
Generic File Name:	<input type="text"/>	--- Suggestion ---
Specific File Name:	<input type="text"/>	--- Suggestion ---
Transfer Protocol:	HTTPS	--- Suggestion ---
Host Name:	0.0.0.0:0	FXO_Country_Defaults.cfg
Location:	<input type="text"/>	Survivability.cfg
User Name:	<input type="text"/>	PRI_China-DSS1.cfg
Password:	<input type="text"/>	Survivability_Enable.cfg
Execution Parameters		
Privacy Key:	<input type="text"/>	PRI_NorthAmerica-NI2.cfg
Allow Repeated Execution:	Enable	PRI_NorthAmerica-NI1.cfg
		PRI_Default.cfg
		FXO_North-America_3km.cfg

- Click **Apply & Execute Now**. Wait until the unit reboots, when the reboot is done the firmware upgrade procedure is finalized. When prompted, select **restart required services**.

Rollback to Previous Firmware

The GX Gateway or EX Controller supports a rollback option to its previous version. If for any reasons, a rollback is needed, select the **Rollback**.

Firmware Packs Installed				
Name	Version	Profile	Bank	
Dgw	43.1.1264	S100-MT-D2000-50	Main - In Use	Factory Reset
Dgw	42.3.1032-MT	S100-MT-D2000-45	Recovery	Rollback

Wait until the unit reboots when the reboot is done and the rollback procedure is finalized.

Setting up Virtual Machine in an EX-Controller

This section only covers the upload of an ISO-image to the EX-Controller.

Install and Configure Virtual Machine

There are two methods to install the SW in a virtual machine:

- Upload an ISO-image to internal file storage.
- Use an ISO-image on a bootable USB stick.

Prerequisites

Before creating and installing a new virtual machine there are a few actions that must be done. If any pre-installed virtual machine exists, that virtual machine must be deleted.

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Information	Services	Hardware	Endpoints	Event Log	Local Log	Packet Capture	Diagnostics	VM			

1. Go to **System > VM**.
2. Click the Plus (+) to create the virtual machine
3. Click **Stop** icon to stop or pause VM if running and click **Delete** icon to delete VM.

Virtual Machine Status											
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State	
exdeploy		12:e7:b0:0c:5d:8e	0	None	e1000	1024	20	qcow2	1	Started	

Virtual Machine Configuration									
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions		
exdeploy	<input type="text"/>	<input type="text" value="12:e7:b0:0c:5d:8e"/>	<input type="text" value="0"/>	<input type="text" value="None"/>	<input type="text" value="e1000"/>	<input type="text" value="Auto"/>	<input type="button" value="Play"/> <input type="button" value="Stop"/> <input type="button" value="Pause"/> <input type="button" value="Reset"/> <input type="button" value="Delete"/>		

Virtual Machine Creation					
Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="raw"/>	<input type="text" value="1"/>	<input type="button" value="+"/>

NOTE: The **exdeploy** VM is only used for MiVoice Business application. It cannot be used with MX-ONE.

Virtual Machines

4. Click the Plus (+) to create the virtual machine.
5. Configure a link as a virtual switch.

6. Go to **Network > Interfaces**.
7. From the **Virtual Switch** selection list, select **Enable** as a link that you wish to enable for the virtual switch.

Ethernet Link Configuration						
Link	MTU	802.1x Authentication	EAP Username	EAP Certificate Validation	Virtual Switch	
eth1	<input type="text" value="1500"/>	<input type="button" value="Disable"/> ▾	<input type="text"/>	<input type="button" value="Trusted And Valid"/> ▾	<input type="button" value="Enable"/> ▾	
eth2-5	<input type="text" value="1500"/>	<input type="button" value="Disable"/> ▾	<input type="text"/>	<input type="button" value="Trusted And Valid"/> ▾	<input type="button" value="Enable"/> ▾	

8. Click **Apply**.

Upload ISO-image to Internal Storage

Figure 4.1: File



1. Go to **Management > File**.
2. Select the **Destination** to **vm/drives/** from the drop-down list.
3. Specify the **URL** where the ISO-images is located.

Figure 4.2: Import File Through URL

Import File Through URL	
Last Import File Result:	None
Import File Parameters <input type="button" value="Import"/>	
Destination:	<input type="text" value="vm/drives/"/> ▾
URL:	<input type="text" value="http://192.168.17.8/isoimages/MX7.0.0.hf2.rc5.iso"/>
Username:	<input type="text"/>
Password:	<input type="text"/>

4. Click **Import** and wait. As the MX-ONE image is quite large (around 6 GB) it will take some time.

Figure 4.3: Last Import File Result

Import File Through URL	
Last Import File Result:	Downloading
Import File Parameters <input type="button" value="Import"/>	
Destination:	<input type="text"/> ▾
URL:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>

5. When the upload is finished, check that the **Last Import File Result** is Success.

Figure 4.4: Import File Success

Import File Through URL	
Last Import File Result:	Success
Import File Parameters Import	
Destination:	<input type="text"/>
URL:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>

- Double check in the internal file storage that file exists.

Figure 4.5: Internal Files

Internal files			
Name	Description	Size	
conf/FXO_Country_Defaults.cfg	FXO Country Defaults	1 KB	—
conf/FXO_North-America_3km.cfg	FXO North-America 3km	1 KB	—
conf/PRI_China-DSS1.cfg	China DSS1	3 KB	—
conf/PRI_Default.cfg	PRI default configuration	3 KB	—
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB	—
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB	—
conf/Survivability_Enable.cfg	Configures the EX Controller for MX-ONE survivability environment.	29 KB	—
conf/Survivability.cfg	Configures the unit to use the SipProxy service for basic use cases.	1 KB	—
vm/drives/MX7.0.0.2.rc5.iso	Bootable disc file	6.3 GB	—
9 file(s)		Total: 6.3 GB / Available: 2.3 GB	

Create the Virtual Machine

Figure 4.6: VM

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Information	Services	Hardware	Endpoints	Event Log	Local Log	Packet Capture	Diagnostic	VM			

- Go to **System > VM**.
- In the Virtual Machine Creation table, fill in the following field details.
 - **Vm Name:** Enter a name for VM, special characters like hyphens (-) are not allowed.
 - **Ram (Mb):** This value shall be 7168 (maximum amount that is available).
 - **Storage (Gb):** Min 100 GB, if less than 100 GB the Linux file structure is not setup properly.
 - **Image Format:** choose **raw** for maximum performance or **qcow2** for space efficiency and flexibility.
 - **No Cores:** This value will be 3.

Figure 4.7: Virtual Machine

Virtual Machine Status											
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State	
Virtual Machine Configuration											
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions				
Virtual Machine Creation											
Vm Name	Ram (Mb)		Storage (Gb)		Image Format		Nb Cores				
mxone7	7168		100		raw		3		+		

NOTE: It is not possible to modify the settings (RAM, name, and so on) once the virtual machine has been created. The only way to change the settings, is to delete the virtual machine and to create it once again.

- Click Plus (+) icon to create the virtual machine. The following message is displayed.

Figure 4.8: Virtual Machine Creation Message

It is not possible to modify the settings (RAM, name, etc.) once the Virtual Machine has been created. The only way to change the settings, is to delete the Virtual Machine and to create it once again.

Click Ok to create the Virtual Machine or Cancel to discard changes.

- Click **OK**. The following screen is displayed after the creation of the Virtual Machine.

Virtual Machines

Figure 4.9: Virtual Machine Status

Virtual Machine Status											
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State	
mxone7		12:b0:c9:0b:ec:8c	0	None	e1000	7168	100	raw	3	Stopped	

Virtual Machine Configuration								
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions	
mxone7		12:b0:c9:0b:ec:8c	0	None	e1000	Manual	<input type="button" value="Play"/> <input type="button" value="Stop"/> <input type="button" value="Reset"/> <input type="button" value="Pause"/> <input type="button" value="Full Screen"/>	




Virtual Machine Creation										
Vm Name	Ram (Mb)		Storage (Gb)		Image Format		Nb Cores			
					raw		1		+	

Using Locally Stored ISO-image

- In the **Iso Name** field, enter the name of the ISO-image stored in the internal file system.

6. In the **Startup** field, select **Auto**.

Figure 4.10: Virtual Machine Configuration

Virtual Machine Configuration								
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions	
mxone7	MX7.0.0.2.rc5.iso	12:9d:0c:0b:ec:8c	0	None	e1000	Auto	     	

7. Click **Start** to start installation from ISO-image. Ensure that the **State** field is changed to **Started**.

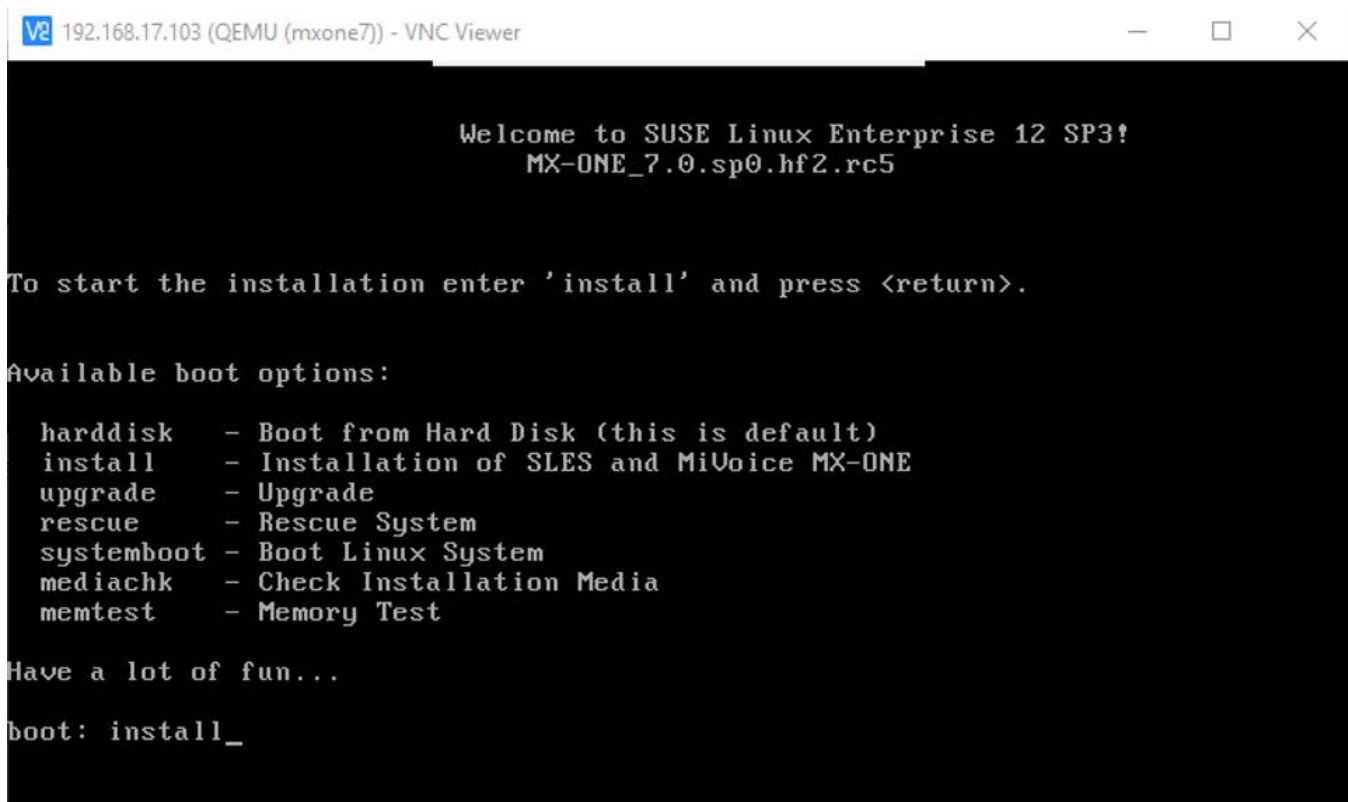
Figure 4.11: Virtual Machine Started Status

Virtual Machine Status										
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State
mxone7	MX7.0.0.2.rc5.iso	12:9d:0c:0b:ec:8c	0	None	e1000	7168	100	qcow2	3	Started

8. Start a VNC-viewer and attach to the **Vnc id** stated in the **Virtual Machine Status** table.

NOTE: UltraVNC Viewer, TightVNC Viewer, and VNC Viewer are presently supported.

9. At the **boot:** prompt, type **Install**. The installation continues as a normal MX-ONE installation. The following screen is displayed.



```

192.168.17.103 (QEMU (mxone7)) - VNC Viewer

Welcome to SUSE Linux Enterprise 12 SP3!
MX-ONE_7.0.sp0.hf2.rc5

To start the installation enter 'install' and press <return>.

Available boot options:

harddisk - Boot from Hard Disk (this is default)
install  - Installation of SLES and MiVoice MX-ONE
upgrade  - Upgrade
rescue   - Rescue System
systemboot - Boot Linux System
mediachk - Check Installation Media
memtest  - Memory Test

Have a lot of fun...

boot: install_

```

Using bootable USB-Stick

10. Ensure that your USB external device contains the Operating System installation media, that is bootable and connected. When downloading, the OS provides architecture choices to choose either AMD64 (64 bit OS) or i386/i686 (32 bit OS). You must choose the architecture for an INTEL processor.
11. Select **All** from the **Usb** field and click **Apply**.

Virtual Machine Configuration								
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions	
mxone7		12:9d:0c:0b:ec:8c	0	All	e1000	Auto		

12. Click Start icon to start the VM. Open the VNC Client located on your computer network that is connected to the unit.

NOTE: UltraVNC Viewer, TightVNC Viewer, and VNC Viewer are presently supported

13. Enter the 'IPAddressOftheUnit':'VNCid', for example - 192.168.0.12:1.

14. From the VNC client, wait for the following message to display *Press F12 for boot menu*. If too late, restart the VM by clicking the **Start** button.

15. Press F12, then select the boot device (in this case 2).

```

iPXE (http://ipxe.org) 00:04.0 CA80 PCI2.10 PnP PMM BFF93860 BFEF3860 CA80

iPXE (http://ipxe.org) 00:05.0 CB80 PCI2.10 PnP PMM BFF93860 BFEF3860 CB80

Press F12 for boot menu.

Select boot device:

1. ata0-0: QEMU HARDDISK ATA-7 Hard-Disk (100 GiBytes)
2. USB MSC Drive Generic USB 2.0 8.07
3. Legacy option rom
4. iPXE (PCI 00:03.0)
5. iPXE (PCI 00:04.0)
6. iPXE (PCI 00:05.0)
  
```

16. At the **boot:** prompt, type **Install**. The installation continues as a normal MX-ONE installation.

Setting up MX-ONE for Branch Node Solution

Number Analysis

Number Analysis Data:

Type of Series	Number Series
Extension Number Series	10000 - 49999 67000 - 67999
External Destination Code	081 – 088
LCR Access Code Number Series	00

Call Discrimination Data:

Type of Series	Number Series
External/Internal Number	CDCAT Customer
Number Analysis Data	-

Extension Data

Figure 5.1: Directory Number Profile

Dir	Cust	Lim	Csp	Feature	Lang	Max	Secretary	Max	Security	AMC	Video	Blu	Star	Third	Party	Csta	Free	On	Hotline	Hotline	Number	Backup	Number	Area
				level		Cost		Term	Exception				Client	Model	SIP	Client	Support	Second	Line	Cost				Code
11100	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08801344311100	013	
11101	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	1	-	-	-	-	-	08801344311101	013	
11102	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	1	-	-	-	-	-	08801344311102	013	
11103	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08801344311103	013	
11104	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08801344311104	013	
22100	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803132522100	031	
22101	0	1	9	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803132522101	031	
22102	0	1	9	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803132522102	031	
22103	0	1	9	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803132522103	031	
22104	0	1	9	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803132522104	031	
32100	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08804059832100	040	
32101	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08804059832101	040	
32102	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08804059832102	040	
32103	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08804059832103	040	
32104	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08804059832104	040	
42100	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803661842100	036	
42101	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803661842101	036	
42102	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803661842102	036	
42103	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803661842103	036	
42104	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	08803661842104	036	
67000	0	1	9	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	-	-	
67512	0	1	11	-	-	No	1	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	-	-	
67820	0	1	11	-	-	No	4	Yes	No	No	No	-	No	No	00	1	-	-	-	-	-	-	-	
67821	0	1	9	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	-	-	
67822	0	1	9	-	-	No	1	Yes	No	No	No	-	No	No	00	1	-	-	-	-	-	-	-	
67823	0	1	10	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	-	-	
67824	0	1	9	-	-	No	4	Yes	No	No	No	-	No	No	00	0	-	-	-	-	-	-	-	

MDSH>

Common Service Profile 9:

Cust: 0
 Traf : 0103151515
 Serv: 111100011001000000000100000300
 Cdiv: 111000111010000
 Roc: 000001
 Npres: 0011000
 Offered Time: 0
 Forced DisconnectTime: 0
 CnnLog: 0
 Csp Name: Standard

Common Service Profile 11:

Cust: 0
 Traf : 0103151515
 Serv: 111130011001000000000100000300
 Cdiv: 111000111010000
 Roc: 000001
 Npres: 0011000
 Offered Time: 0
 Forced DisconnectTime: 0
 CnnLog: 0
 Csp Name: Intrusion

Least Cost Routing Data

ENT Table

Least Cost Destination Data

Table 5.1: External Number Table (Sheet 1 of 2)

Entry	TRC	PRE	Conf
00013443	8		N
00031325	8		N
00036618	7		N
00040598	8		N

Table 5.1: External Number Table (Continued) (Sheet 2 of 2)

Entry	TRC	PRE	Conf
000856867	7		N

NLT Table

Least Cost Destination Data

Table 5.2: Number Length Table

Entry	TRC	PRE	CONF	MIN	MAX	ACF
001	0	-	N	6	18	Y
002	0	-	N	6	18	Y
003	0	-	N	6	18	Y
004	0	-	N	6	18	Y
005	0	-	N	6	18	Y
006	0	-	N	6	18	Y
007	0	-	N	6	18	Y
008	0	-	N	6	18	Y
009	0	-	N	6	18	Y

DNT2 Table

Least Cost Destination Data

Table 5.3: Number Table

Entry	TRC	PRE	ACC T	FRC T	TOLL	CBCS	BTON	TNS	OS A
00013	5	-	0	1	11111111111111	-	0	-	-
00031	5	-	0	2	11111111111111	-	0	-	-
00036	5	-	0	3	11111111111111	-	0	-	-
00040	5	-	0	3	11111111111111	-	0	-	-
0008	4	-	0	4	11111111111111	-	0	-	-

FDT Table

Least Cost Destination Data

Table 5.4: Fictitious Destination Table

FRCT	TZONE	PRE
1	1	081
2	1	082
3	1	083
5	1	085

END

Route Data

ROCAP

Route Category Data

Figure 5.2: Route Category Data

ROU	CUST SEL	TRM SERV	NODG	DIST	DISL	TRAF	SIG	BCAP
81	71100000000000010	4	3100000001	0	30	128	03151515 0111110000A0	001100
82	71100000000000010	4	3100000001	0	30	128	03151515 0111110000A0	001100
83	71100000000000010	4	3100000001	0	30	128	03151515 0111110000A0	001100
85	71100000000000010	4	3100000001	0	30	128	03151515 0111110000A0	001100

RODAP

Route Data

Table 5.5: Route Data

ROU	Type	VARC	VARI	VARO	Filter
1	SL60	H'00000300	H'00000000	H'04410000	NO
81	TL66	H'00000000	H'00000000	H'00000000	NO
82	TL66	H'00000000	H'00000000	H'00000000	NO
83	TL66	H'00000000	H'00000000	H'00000000	NO
85	TL66	H'00000000	H'00000000	H'00000000	NO

RODDP

External Destination Route Data

Table 5.6: External Destination Route Data

DES T	DRN	ROU	CH O	CUS T	ADC	TR C	SR T	NUMAC K	PR E
00	-	1	-	-	12250000000002500 02000000000	0	3	-	-
081	-	81	-	-	12250000000002500 02000000000	0	4	-	-
082	-	82	-	-	12250000000002500 02000000000	0	4	-	-
083	-	83	-	-	12250000000002500 02000000000	0	4	-	-
085	-	85	-	-	12250000000002500 02000000000	0	4	-	-
088	-	1	-	-	12250000000002500 02000000000	0	4	-	-

Number Prefixing

Route Number Data

Table 5.7: Route Data (Sheet 1 of 2)

ROU	PRE	ROUDIR	EXNOPU	EXNOPR	TERAC
1	-	-	1-46 2-08 4-568	-	-
81	-	-	1-46 2-013 4-443	-	-
82	-	-	1-46 2-036 4-418	-	-
83	-	-	1-46 2-031 4-325	-	-

Table 5.7: Route Data (Continued) (Sheet 2 of 2)

ROU	PRE	ROUDIR	EXNOPU	EXNOPR	TERAC
85	-	-	1-46 2-040 4-598	-	-

SIP ROUTE

One SIP route to each branch node is specified.

Route 81 towards BO#1 (Linköping), public access is ISDN.

route : 81

protocol = udp

profile = common-gateway

service = PRIVATE

uristring0 = sip:??@192.168.17.81

fromuri0 = sip:??@192.168.17.44

remoteport = 5070

accept = FROM_DOMAIN

match = 192.168.17.81

register = SET_BY_PROFILE

trusted = TRUST_BY_PROFILE

Route 82 towards BO#4 (Jönköping), public access is ISDN.

route : 82

protocol = udp

profile = common-gateway

service = PRIVATE

uristring0 = sip:??@192.168.17.82

fromuri0 = sip:??@192.168.17.44

remoteport = 5070

accept = FROM_DOMAIN

match = 192.168.17.82

register = SET_BY_PROFILE

trusted = TRUST_BY_PROFILE

Route 83 towards BO#2 (Göteborg), public access is SIP.

```
route : 83
protocol = udp
profile = common-gateway
service = PRIVATE
uristring0 = sip:?@192.168.17.83
fromuri0 = sip:?@192.168.17.44
remoteport = 5090
accept = FROM_DOMAIN
match = 192.168.17.83
register = SET_BY_PROFILE
trusted = TRUST_BY_PROFILE
```

Route 85 towards BO#3 (Malmö), public access is ISDN.

```
route : 85
protocol = udp
profile = common-gateway
service = PRIVATE
uristring0 = sip:?@192.168.17.85
fromuri0 = sip:?@192.168.17.44
remoteport = 5070
accept = FROM_DOMAIN
match = 192.168.17.85
register = SET_BY_PROFILE
trusted = TRUST_BY_PROFILE
```

Setting up GX Gateway with ISDN Trunks

This section describes how to setup the 'Linköping' branch (BO#1) node using ISDN trunk towards PSTN.

NOTE: The setup for the gateway and SBC part for an EX-controller is identical.

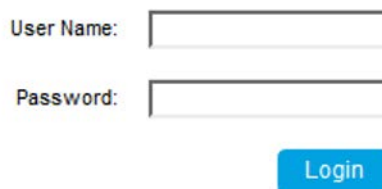
Logon

This section describes how to setup BO#1.

1. Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network).

NOTE: If DHCP is not running into the network then, plug in the network cable to the ETH2 port on EX Controller and use the default IP address of 192.168.0.10 to open the EX Controller Interface.

Figure 6.1: Login page



User Name:

Password:

Login

- User name/password: public /
 - User name/password: admin/administrator
2. Plug in the analog phone in the FXS port 1 of the EX Controller and dial *#*0 to know the IP address of the EX Controller assigned by using DHCP server.
 3. Log into the EX Controller by using the above-mentioned IP address and navigate as described below to configure.

Network Settings

Host

Figure 6.2: Host Settings - 1

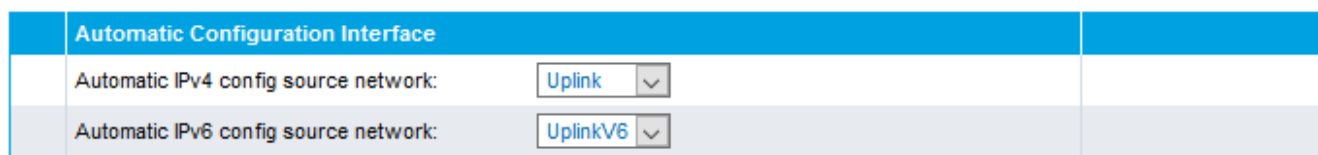


System Network SIP Proxy SBC ISDN POTS SIP Media Telephony Call Router Management Reboot

Status Host Interfaces VLAN QoS Local Firewall IP Routing Network Firewall NAT DHCP Server

1. Select **Network** > **Host** and keep the default configuration interface as mentioned below.

Figure 6.3: Host Settings - 2



Automatic Configuration Interface	
Automatic IPv4 config source network:	Uplink
Automatic IPv6 config source network:	UplinkV6

2. Change to **Static IP-address** and enter default Gateway (GW).

Figure 6.4: Changing Static IP Address

Default Gateway Configuration	
IPv4	
Configuration Source:	Static
Default Gateway:	192.168.17.1
IPv6	
Configuration Source:	Automatic IPv6
Default Gateway:	

3. Change to static DNS server and enter IP-address or FQDN to DNS server.

Figure 6.5: Changing Static DNS Server

DNS Configuration	
Configuration Source:	Static
Primary DNS:	10.105.64.3
Secondary DNS:	
Third DNS:	
Fourth DNS:	

4. Change to static SNTP server, enter time server data.

Figure 6.6: Changing to Static SNTP Server

SNTP Configuration	
Configuration Source:	Static
Static Servers:	
Primary SNTP:	pool.ntp.org
Secondary SNTP:	
Third SNTP:	
Fourth SNTP:	
Synchronization:	
Synchronization Period:	1440
Synchronization Period On Error:	60

5. Set the **Time Zone**.

Valid options are:

- Pacific Time (Canada and US): PST8PDT7,M3.2.0/02:00:00,M11.1.0/02:00:00
- Mountain Time (Canada and US): MST7MDT6,M3.2.0/02:00:00,M11.1.0/02:00:00
- Central Time (Canada and US): CST6CDT5,M3.2.0/02:00:00,M11.1.0/02:00:00
- Eastern Time (Canada and US): EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00

- Atlantic Time (Canada): AST4ADT3,M3.2.0/02:00:00,M11.1.0/02:00:00
- GMT Standard Time: GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
- W. Europe Standard Time: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00
- China Standard Time: CST-8
- Tokyo Standard Time: TST-9
- Central Australia Standard Time: CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
- Australia Eastern Standard Time: AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
- UTC (Coordinated Universal Time): UTC0

Figure 6.7: Setting Static Time Zone

Time Configuration	
Static Time Zone:	WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00

6. Leave all other items as it is and click **Apply** when finished.

Interfaces

Figure 6.8: Interface

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Host	Interfaces	VLAN	QoS	Local Firewall	IP Routing	Network Firewall	NAT	DHCP Server		

1. Go to **Network > Interface**.
2. Change **Uplink** to **IpStatic (IPv4 Static)** and enter the static IP-address and Static Default Gateway.

Figure 6.9: Changing Uplink to IpStatic

Network Interface Configuration						
Name	Link	Type	Static IP Address	Static Default Router	Activation	
Lan1	eth2-5	IpStatic (IPv4 Static)	192.168.0.10/24		Enable	-
Uplink	eth1	IpStatic (IPv4 Static)	192.168.17.81/24	192.168.17.1	Enable	-
UplinkV6	eth1	Ip6Static (IPv6 Static)			Disable	-
						+

3. Leave all other items as it is and click **Apply** when ready.

NOTE: When the IP-address is changed, the connection is lost and a new logon must be done with the new IP-address.

Local Firewalls

Figure 6.10: Local firewalls

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Host	Interfaces	VLAN	QoS	Local Firewall	IP Routing	Network Firewall	NAT	DHCP Server		

1. Go to **Network > Local Firewall**.
2. If local firewall security is needed change default policy to **Drop**.

Figure 6.11: Changing default policy

Configuration Modified:		No
-------------------------	--	----

Local Firewall Configuration	
Default Policy:	Drop ▾
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

3. Enter the networks for which traffic can enter from.

Figure 6.12: Enter network traffic

Local Firewall Rules											
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period	
1	Enable ▾	192.168.17.0/24		Uplink		All ▾	<input type="checkbox"/>	Accept ▾	10	60	⬆ ⬇ ⬆ ⬇
2	Enable ▾	172.17.17.0/24		Uplink		All ▾	<input type="checkbox"/>	Accept ▾	10	60	⬆ ⬇ ⬆ ⬇
3	Enable ▾	10.105.0.0/16		Uplink		All ▾	<input type="checkbox"/>	Accept ▾	10	60	⬆ ⬇ ⬆ ⬇
											+

4. Click **Save** or **Save and Apply** when ready.

Session Board Controller (SBC)

Rulesets define one or several rules used to filter, manipulate or route inbound or outbound requests.

There are 2 types of Rulesets:

- **Call Agent Rulesets:** describe how inbound or outbound requests are handled by a specific Call Agent. These can also implement services or collect data.
- **Routing Rulesets:** used to globally route outbound requests, that is, these apply to all Call Agents.

When a request arrives at a Call Agent from a peer, the inbound rules of the Rulesets associated with the Call Agent are executed. Then, Routing Rulesets are executed until a Call Agent is selected for the destination. Lastly, the outbound rules of the Rulesets associated with the destination Call Agent are executed before sending the request to the peer. Inbound rules of the Ruleset are executed in ascending Ruleset priority order. Outbound rules are executed in descending Ruleset priority order.

Configuration

Figure 6.13: Configuration



1. Go to **SBC > Configuration**. The following Call Agents are present.

Figure 6.14: Configuration Modified



Following Call Agents are present.

Figure 6.15: Call Agent Configuration

Call Agent Configuration								
Name	Enable	Gateway	Signaling Interface	Media Interface	Peer Host	Peer Network		
local_users_ca	<input checked="" type="checkbox"/>		uplink_s	uplink_m		0.0.0.0/0		
trunk_lines_ca	<input checked="" type="checkbox"/>	trunk_lines_gw		loop_m				
remote_users_ca	<input type="checkbox"/>		uplink_s	uplink_m				
MX-One_LIM1	<input checked="" type="checkbox"/>		uplink_s	uplink_m	192.168.17.44			
MX-One_LIM2	<input type="checkbox"/>		uplink_s	uplink_m	lim2.mitel.com			
MX-One-trunk	<input checked="" type="checkbox"/>		trunk_s	uplink_m	lim1.mitel.com			
MX-One-trunk2	<input type="checkbox"/>		trunk_s	uplink_m	lim2.mitel.com			
VoIP-trunk1	<input type="checkbox"/>		uplink_s	uplink_m	voip.provider1			
VoIP-trunk2	<input checked="" type="checkbox"/>		uplink_s	uplink_m	voip.provider2			

Routing Rulesets

Routing Rulesets: are used to globally route outbound requests, that are applied to all Call Agents. Routing Rulesets are executed until a Call Agent is selected for the destination.

Figure 6.16: Routing Rulesets

Routing Rulesets			
Priority	Name	Parameters	
1	MX-One_local_users_failover_to_trunk	A_PRFX=013443 TRUNK_CA=trunk_lines_ca	⬆ ⬇ ⬇
2	MX-One_trunk_lines_to_local_users	TRUNK_CA=trunk_lines_ca	⬆ ⬇ ⬇
3	MX-One_routes_with_basic_local_survivability_TCP		⬆ ⬇ ⬇
4	MX-One_routes_with_basic_local_survivability_UDP		⬆ ⬇ ⬇
5	SIP_trunk_to_MX-One	TRUNK_CA=trunk_lines_ca MX-ONE-TRUNK_CA=MX-One-trunk	⬆ ⬇ ⬇
6	MX-One_to_trunk_lines	MX-ONE-TRUNK_CA=MX-One-trunk TRUNK_CA=trunk_lines_c	⬆ ⬇ ⬇
			+

- **Ruleset MX-One_local_users_failover_to_trunk**

A_PRFX=013443

This is the prefix for the local numbers used on outgoing calls to the PSTN (in this example, you will receive a number block 013443xxxxx from the PSTN provider and add the prefix on outgoing calls, so that the calling party number sent to the PSTN is correct).

TRUNK_CA=trunk_lines_ca

This is the call agent from which the call is coming from.

- **Ruleset SIP_trunk to MX-One**

TRUNK_CA=trunk_lines_ca

This is the call agent from which the call is coming from.

MX-ONE-TRUNK_CA=MX-One-trunk

This is the call agent to which the call will be routed to.

- **Ruleset MX-One_to_trunk_lines**

TRUNK_CA=trunk_lines_ca

This is the call agent from which the call is coming from.

MX-ONE-TRUNK_CA=MX-One-trunk

This is the call agent to which the call will be routed to.

1. Click **Save** and **Apply** when done.
2. Configure each call agent (ca).
3. Click **Modify** to enter specific data for each call agent.

local_users_ca

Figure 6.17: Configure Call Agent screen

Configure Call Agent	
	Value
Call Agent Parameters	
Name	local_users_ca
Enable	<input checked="" type="checkbox"/>
Gateway	<input type="text"/>
Signaling Interface	uplink_s
Media Interface	uplink_m
Peer Host	<input type="text"/>
Peer Network	0.0.0.0/0
Force Transport	None
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	0
Blacklisting Duration	0
Blacklisting Delay	0
Blacklisting Error Codes	<input type="text"/>

Figure 6.18: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	MX-One_build_RURI_survivability	EXT_DIGIT_LENGTH=5 PATTERN=111[0-9][0-9] DOMAIN=192.16	⬆ ⬇ ⬅
2	MX-One_Appearance_Prefix	APP_PRFX=SCA-	⬆ ⬇ ⬅
3	MX-One_Appearance_Prefix	APP_PRFX=EDN-	⬆ ⬇ ⬅
4	MX-One_Remove_Outbound_Appearance	PATTERN=111[0-9][0-9]	⬆ ⬇ ⬅
5	MX-One_outbound_A_Number_prefix	PATTERN=111[0-9][0-9] A_PRFX=013443 PSTN_PREFIX=00	⬆ ⬇ ⬅
6	MX-One_outbound_B_Number_prefix	BNUMBER=67[0-9][0-9] B_PRFX=08568	⬆ ⬇ ⬅
7	MX-One_outbound_B_Number_prefix	BNUMBER=221[0-9][0-9] B_PRFX=031325	⬆ ⬇ ⬅
8	MX-One_outbound_B_Number_prefix	BNUMBER=321[0-9][0-9] B_PRFX=040598	⬆ ⬇ ⬅
9	MX-One_outbound_B_Number_prefix	BNUMBER=421[0-9][0-9] B_PRFX=036618	⬆ ⬇ ⬅
10	MX-One_outbound_B_Number_Override	BNUMBER=^09 BOVERRIDE=0856867000	⬆ ⬇ ⬅
11	MX-One_local_reg_users_with_survivability	EXT_DIGIT_LENGTH=5	⬆ ⬇ ⬅
			+

- Ruleset MX-One_build_RURI survivability (Active only in Survival Mode)

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 11100 - 11199.

PATTERN=111[0-9][0-9]

The pattern for the internal range of numbers would be 11100 - 11199.

Calls to this number range stay always local (would not be sent to the PSTN in survival mode).

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44.

- **Ruleset: MX_One_Appearance_Prefix (Active only in Survival Mode)**

APP_PREFIX=SCA- and APP_PREFIX=EDN-

This is the prefix for the user names connected with shared appearance. In this example, you have two user names: SCA- and EDN-

- **Ruleset: MX-One_Remove_Outbound_Appearance (Active only in Survival Mode)**

PATTERN=111[0-9][0-9]

This rule removes any prefix used for Shared Call Appearance. The pattern for the internal range of numbers would be 11100 - 11199.

- **Ruleset: MX-One_outbound_A_Number_prefix (Active only in Survival Mode)**

PATTERN=111[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 11100 - 11199.

A_PRFX=013443

This is the prefix for the local numbers used on outgoing calls to the PSTN. In this example, add a number block 013443 in front of the number specified in PATTERN-parameter to form a valid calling party number to be sent to the PSTN.

PSTN_PREFIX=00

This parameter specified the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will be truncated.

- **Ruleset: MX-One_outbound_B_Number_prefix (Active only in Survival Mode)**

This ruleset applies to calls to numbers defined in BNUMBER and will add B_PRFX to the called party number.

This ruleset must be repeated for every approved destination (that is, calling the HQ and other branch offices.)

Calling HQ:

BNUMBER=67[0-9][0-9]

Applies to calls to the specific range of extensions. The pattern for the internal range of numbers would be 67000 - 67999.

B_PRFX=08568

This is the prefix for the Called Party Number. In this case, it will be built like: National Prefix (08) + Main part of the HQ's local number: (568).

Calling BO#2:

BNUMBER=221[0-9][0-9]

Applies to calls to the specific range of extensions. The pattern for the internal range of numbers would be 22100 - 22199.

B_PRFX=031325

This is the prefix for the Called Party Number. In this case it will be built like: National Prefix (031) + Main part of the HQ's local number: (325).

Calling BO#3:

BNUMBER=321[0-9][0-9]

Applies to calls to the specific range of extensions. The pattern for the internal range of numbers would be 32100 - 32199.

B_PRFX=040598

This is the prefix for the Called Party Number. In this case it will be built like: National Prefix (040) + Main part of the HQ's local number: (598).

Calling BO#4:

BNUMBER=421[0-9][0-9]

Applies to calls to the specific range of extensions. The pattern for the internal range of numbers would be 42100 - 42199.

B_PRFX=036618

This is the prefix for the Called Party Number. In this case it will be built like: National Prefix (036) + Main part of the HQ's local number: (618).

- **Ruleset: MX-One_outbound_B_Number_Override (Active only in Survival Mode)**

This ruleset applies to calls to numbers defined in BNUMBER and will use the BOVERRIDE as Called Party Number.

One use case could be if a user dials the internal operator (09) while in survivable mode. The dialled number (09) will be replaced with 0856867000 which could be the number to the operator in the HQ.

BNUMBER=09

The internal number to the operator.

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE. In this example, it will be sent to 0856867000.

- **Ruleset: MX-One_local_reg_users_with_survivability**

(Builds the registration cache for survivability purpose).

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 11100 - 11199.

Click **Save** when done.

trunk_lines_ca

Figure 6.19: trunk_lines_ca

Configure Call Agent	
	Value
Call Agent Parameters	
Name	trunk_lines_ca
Enable	<input checked="" type="checkbox"/>
Gateway	trunk_lines_gw
Signaling Interface	
Media Interface	loop_m
Peer Host	
Peer Network	
Force Transport	Tcp
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	0
Blacklisting Duration	0
Blacklisting Delay	0
Blacklisting Error Codes	

Figure 6.20: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	200_OK_to_SIP_OPTIONS		⬆ ⬇ ⬅
2	MX-One_remove_prefix	PSTN_PREFIX=00	⬆ ⬇ ⬅
3	MX-One_trunk_lines_to_reception_survivability	EXT_DIGIT_LENGTH=5 MAIN_EXT=11104 PATTERN=111[0-9][0-	⬆ ⬇ ⬅
4	MX-One_build_RURI_survivability	EXT_DIGIT_LENGTH=5 PATTERN=111[0-9][0-9] DOMAIN=192.16	⬆ ⬇ ⬅
5	MX-One_Appearance_Prefix	APP_PRFX=SCA-	⬆ ⬇ ⬅
6	MX-One_Appearance_Prefix	APP_PRFX=EDN-	⬆ ⬇ ⬅
7	media_relay		⬆ ⬇ ⬅
			+

- Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

This parameter specified the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will truncated.

- Ruleset: MX-One_trunk_lines_to_reception_survivability**

An incoming call in survival mode will be sent to MAIN_EXT destination if not reachable or not available.

MAIN_EXT=11104

This will receive the incoming call in case the original destination is not reachable (not defined or not registered). That is, MAIN_EXT is the default answering position.

PATTERN=321[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 11100 - 11199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44.

- **Ruleset: MX-One_build_RURI_survivability (Active only in Survival Mode)**

Builds the RURI when in survivability mode.

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 11100 - 11199.

PATTERN=111[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 11100 - 11199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44.

- **Ruleset: MX_One_Appearance_Prefix (Active only in Survival Mode)**

APP_PREFIX=SCA- and APP_PREFIX=EDN-

This is the prefix for the user names connected with shared appearance (SCA) and extra directory number (EDN). In this example, you have two user names: "SCA"- and "EDN-"

Click **Save** when done.

MX-One_Lim1

1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 6.21: Configure Call Agent - Peer Host

Configure Call Agent		Value
Call Agent Parameters		
Name	<input type="text" value="MX-One_LIM1"/>	
Enable	<input checked="" type="checkbox"/>	
Gateway	<input type="text" value=""/>	
Signaling Interface	<input type="text" value="uplink_s"/>	
Media Interface	<input type="text" value="uplink_m"/>	
Peer Host	<input type="text" value="192.168.17.44"/>	
Peer Network	<input type="text" value=""/>	
Force Transport	<input type="text" value="None"/>	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	<input type="text" value="30"/>	
Blacklisting Duration	<input type="text" value="60"/>	
Blacklisting Delay	<input type="text" value="0"/>	
Blacklisting Error Codes	<input type="text" value=""/>	

2. Enter the IP-address of the GW in the **RURI_HOST** parameter.

Figure 6.22: RURI_HOST parameter

Call Agent Rulesets			
Priority	Name	Parameters	
1	rewrite_RURI_host	RURI_HOST=192.168.17.81	↑ ↓ -
2	MX-One_core_side		↑ ↓ -
			+

- **Ruleset: rewrite_RURI_host**
RURI_HOST= 192.168.17.81
This is the local IP address of the GX-gateway.
Click **Save** when done.

MX-One_trunk

1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

NOTE: Though the **MX-One-trunk** is not used in this configuration but you must enable it.

Figure 6.23: Call Agent Parameters

Configure Call Agent		Value
Call Agent Parameters		
Name		MX-One-trunk
Enable		<input checked="" type="checkbox"/>
Gateway		
Signaling Interface		trunk_s
Media Interface		uplink_m
Peer Host		192.168.17.44
Peer Network		
Force Transport		None
Monitoring and Blacklisting Parameters		
Keep-Alive Interval		30
Blacklisting Duration		60
Blacklisting Delay		0
Blacklisting Error Codes		

Figure 6.24: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	media_relay		⬆ ⬇ ⬅
2	face_mxone	SOURCE_CA=trunk_lines_ca RURI_HOST=192.168.17.81	⬆ ⬇ ⬅
3	MX-One_remove_prefix	PSTN_PREFIX=00	⬆ ⬇ ⬅
4	MX-One_trunk_lines_to_reception_survivability	EXT_DIGIT_LENGTH=5 MAIN_EXT=11104 PATTERN=111[0-9][0-9]	⬆ ⬇ ⬅
5	MX-One_build_RURI_survivability	EXT_DIGIT_LENGTH=5 PATTERN=111[0-9][0-9] DOMAIN=192.16	⬆ ⬇ ⬅
6	MX-One_core_side		⬆ ⬇ ⬅
			+

- **Ruleset: face_mxone**

SOURCE_CA=trunk_lines_ca

This parameter indicates the call agent from which the call is coming.

RURI_HOST=192.168.17.81

This parameter is used to set a correct value in the FROM DOMAIN in the INVITE message sent to MX-ONE. It will be the local IP-address of the GX-gateway.

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

This parameter specified the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will truncated.

- **Ruleset: MX-One_trunk_lines_to_reception_survivability**

An incoming call in survival mode will be sent to MAIN_EXT destination if not reachable or not available.

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 11100 - 11199.

MAIN_EXT=11104

This extension number (22104) will receive the incoming call in case the original destination is not reachable (not defined or not registered).

PATTERN=111[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 11100 - 11199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44

- **Ruleset: MX-One_build_RURI_survivability**

Builds the RURI when in survivability mode

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 11100 - 11199.

PATTERN=111[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 11100 - 11199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44.

Click **Save** when done

VOIP-trunk2

Figure 6.25: VoIP-trunk2

Configure Call Agent	
	Value
Call Agent Parameters	
Name	VoIP-trunk2
Enable	<input checked="" type="checkbox"/>
Gateway	<input type="text"/>
Signaling Interface	uplink_s
Media Interface	uplink_m
Peer Host	voip.provider2
Peer Network	<input type="text"/>
Force Transport	None
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	0
Blacklisting Duration	0
Blacklisting Delay	0
Blacklisting Error Codes	<input type="text"/>

Figure 6.26: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	topology_hiding_out	<input type="text"/>	⬆ ⬇ ⬅
2	MX-One_remove_prefix	PSTN_PREFIX=00	⬆ ⬇ ⬅
3	face_mxone	SOURCE_CA=trunk_lines_ca RURI_HOST=192.168.17.81	⬆ ⬇ ⬅
			+

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

This parameter specified the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will truncated.

- **Ruleset: face_mxone**

SOURCE_CA=trunk_lines_ca

This parameter indicates the call agent from which the call is coming.

RURI_HOST=192.168.17.81

This parameter is used to set a correct value in the FROM DOMAIN in the INVITE message sent to MX-ONE. It will be the local IP-address of the GX-gateway.

Click **Save** when done.

When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.

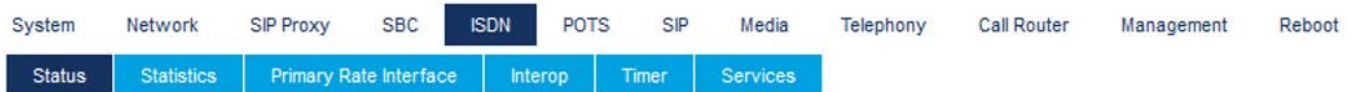


Click **Apply** when ready.

NOTE: Error will be shown in the configuration if the indication is not removed. Double check the changes described above and correct them.

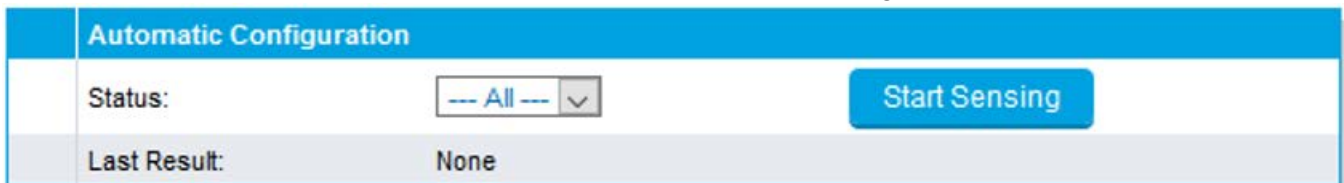
ISDN

Figure 6.27: ISDN



Click **Start Sensing** to start first action if ISDN trunks are used.

Figure 6.28: Automatic Configuration

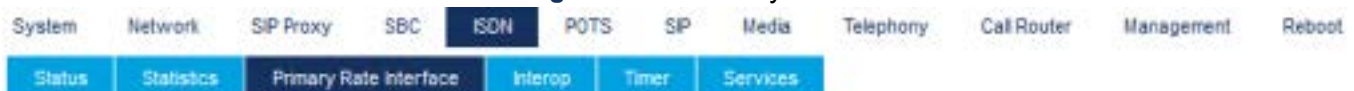


The system automatically detects certain parameters; for example, number of channels.

Primary Rate Interface

Settings

Figure 6.29: Primary Rate Interface



1. Select **ISDN > Primary Rate Interface**.
2. When sensing is done for several markets, specific parameters can be changed.

Figure 6.30: Interface Configuration

Interface Configuration	
Line Type: [Configure]	E1
Endpoint Type:	TE
Clock Mode:	Slave
Port Pinout:	Auto
Monitor Link State:	Enable
Line Coding:	HDB3
Line Framing:	CRC4
Signaling Protocol:	DSS1
Network Location:	User
Preferred Encoding Scheme:	G.711 a-Law
Fallback Encoding Scheme:	G.711 u-Law
Channel Range:	1-30
Channels Reserved for Incoming Calls:	
Channels Reserved for Outgoing Calls:	
Channel Allocation Strategy:	Ascending
Maximum Active Calls:	30
Signal Information Element:	Disable
Inband Tone Generation:	Enable
Inband DTMF Dialing:	Enable
Overlap Dialing:	Disable
Calling Name Max Length:	34
Exclusive B-Channel Selection:	Disable
Sending Complete:	Enable
Send Restart On Startup:	Enable
Link Establishment:	Permanent
Accepted Status Causes:	
Accepted Progress Causes:	1-127
Send Isdn Progress:	Send All
Send Progress Indicator IE:	Send All
Default TON for Calling Party Number IE:	National
Default NPI for Calling Party Number IE:	Isdn Telephony
Default PI for Calling Party Number IE:	Presentation Allowed
Default SI for Calling Party Number IE:	Context Dependent
Default TON for Called Party Number IE:	National
Default NPI for Called Party Number IE:	Isdn Telephony
Notification User Suspended:	Ignore

3. Click **Apply** and restart requested service when done.

Interop

Figure 6.31: Interop

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Statistics	Primary Rate Interface	Interop	Timer	Services						

1. Select **ISDN > Interop**.
2. Change other parameters dependent on market.

Figure 6.32: Interop Configuration

Interop Configuration	
Progress Indicator In Setup:	Enable ▾
Progress Indicator In Setup Ack:	Enable ▾
Progress Indicator In Call Proceeding:	Enable ▾
Progress Indicator In Progress:	Enable ▾
Progress Indicator In Alerting:	Enable ▾
Progress Indicator In Connect:	Enable ▾
Maximum Facility Waiting Delay (ms):	0
Use Implicit Inband Info:	Disable ▾
Call Proceeding Delay (ms):	0
Calling Name Delivery:	Signaling Protocol ▾

3. Click **Apply** and restart requested service when done.

Services

Figure 6.33: ISDN Services

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Statistics	Primary Rate Interface	Interop	Timer	Services						

1. Select **ISDN > Services**.
2. Change other parameters dependent on market.

Figure 6.34: Services Configuration

Services Configuration	
Facility Services:	Disable ▾
Calling Line Information Presentation:	Enable ▾
Calling Line Information Restriction:	Disable ▾
Calling Line Information Restriction Override:	Disable ▾
Connected Line Identification Presentation:	Enable ▾
Connected Line Identification Restriction:	Disable ▾
Connected Line Identification Restriction Override:	Disable ▾
Outgoing Notify:	Disable ▾
Maintenance Service Call Termination:	Graceful ▾
Date/Time IE Support:	Disable ▾
AOC-E Support:	No ▾
AOC-D Support:	No ▾
Call Rerouting Behavior:	Unsupported ▾

3. Click **Apply** and restart requested service when done.

Basic Rate Interface

Settings

Figure 6.35: Settings

System	Network	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Basic Rate Interface	Interop	Timer	Services						

1. Go to **ISDN > Basic Interface Configuration**.
2. When sensing is done several market, specific parameters can be changed.

Figure 6.36: Interface Configuration

Interface Configuration	
Endpoint Type:	TE
Clock Mode:	Auto
Monitor Link State:	Enable
Connection Type:	Point To Point
Signaling Protocol:	DSS1
Network Location:	User
Preferred Encoding Scheme:	G.711 a-Law
Fallback Encoding Scheme:	G.711 a-Law
Channel Allocation Strategy:	Ascending
Maximum Active Calls:	0
Signal Information Element:	Disable
Inband Tone Generation:	Enable
Inband DTMF Dialing:	Enable
Overlap Dialing:	Enable
Calling Name Max Length:	34
Exclusive B-Channel Selection:	Disable
Sending Complete:	Enable
Send Restart On Startup:	Enable
Link Establishment:	Permanent
Hook-Flash Keypad:	
Accepted Status Causes:	
Accepted Progress Causes:	1-127
Send Isdn Progress:	Send All
Send Progress Indicator IE:	Send All
TEI Negotiation:	Power Up
Default TON for Calling Party Number IE:	National
Default NPI for Calling Party Number IE:	Isdn Telephony
Default PI for Calling Party Number IE:	Presentation Allowed
Default SI for Calling Party Number IE:	User Provided Verified And Passed
Default TON for Called Party Number IE:	National
Default NPI for Called Party Number IE:	Isdn Telephony
Notification User Suspended:	Ignore

3. Click **Apply** and restart requested service when done.

Interop

Figure 6.37: Interop



1. Select **ISDN > interop**.

Figure 6.38: Interop Configuration

Interop Configuration	
Progress Indicator In Setup:	<input type="button" value="Enable"/> ▾
Progress Indicator In Setup Ack:	<input type="button" value="Enable"/> ▾
Progress Indicator In Call Proceeding:	<input type="button" value="Enable"/> ▾
Progress Indicator In Progress:	<input type="button" value="Enable"/> ▾
Progress Indicator In Alerting:	<input type="button" value="Enable"/> ▾
Progress Indicator In Connect:	<input type="button" value="Enable"/> ▾
Maximum Facility Waiting Delay (ms):	<input type="text" value="0"/>
Use Implicit Inband Info:	<input type="button" value="Enable"/> ▾
Call Proceeding Delay (ms):	<input type="text" value="0"/>
Calling Name Delivery:	<input type="button" value="Signaling Protocol"/> ▾
Allow TEI Broadcast in Point-to-Point:	<input type="button" value="Enable"/> ▾

2. Click **Apply** and restart requested service when done.

Services

Figure 6.39: Services



- 1. Select **ISDN > Services**.

Figure 6.40: Services Configuration

Services Configuration	
Facility Services:	<div>Disable</div>
Calling Line Information Presentation:	<div>Enable</div>
Calling Line Information Restriction:	<div>Disable</div>
Calling Line Information Restriction Override:	<div>Disable</div>
Connected Line Identification Presentation:	<div>Enable</div>
Connected Line Identification Restriction:	<div>Disable</div>
Connected Line Identification Restriction Override:	<div>Disable</div>
Connected Name Identification Presentation:	<div>Enable</div>
Outgoing Notify:	<div>Disable</div>
Maintenance Service Call Termination:	<div>Graceful</div>
Date/Time IE Support:	<div>Disable</div>
AOC-E Support:	<div>No</div>
AOC-D Support:	<div>No</div>
Call Rerouting Behavior:	<div>Unsupported</div>
Malicious Call Identification (MCID):	<div>Disable</div>
MSN:	<div></div>

- 2. Click **Apply** and restart requested service when done.

POTS

Config

Figure 6.41: Config



1. Select **POTS > Config**.
2. Set market specific data for Caller Id handling.

Figure 6.42: General Configuration

General Configuration	
Caller ID Customisation:	EtsIDtmf ▼
Caller ID Transmission:	First Ring ▼
Vocal Unit Information:	All ▼

3. Click **Apply** when done and restart service.

FXS Configuration

Figure 6.43: FXS Configuration



1. Select **POTS > FXS Configuration**.
2. Set analog phone specific data according to market.

Figure 6.44: FXS Configuration

FXS Configuration	
Line Supervision Mode:	DropOnDisconnect ▼
Disconnect Delay:	0
Auto Cancel Timeout:	0
Inband Ringback:	Disable ▼
Shutdown Behavior:	Disabled Tone ▼
Power Drop On Disconnect Duration:	1000
Service Activation:	Flash Hook ▼

Figure 6.45: Country Customisation

Country Customisation	
Override Country Configuration:	Disable ▾
Country Override Loop Current:	30
Country Override Flash Hook Detection Range:	100-1200

- Click **Apply** when done and restart service.

FXO Configuration

Figure 6.46: FXO Configuration - Status

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Config	FXS Configuration	FXO Configuration								

- Select **POTS > FXO Configuration**.
This section is applicable If analogue trunks are used.
NOTE: Only manual incoming is supported where there is no DID functionality. Only DTMF register signalling is supported for outgoing calls.
- Ensure that all FXO ports are up and idle.

Status

Figure 6.47: Status

Line Status		
ID	Type	State
FXO1	FXO	Idle
FXO2	FXO	Idle
FXO3	FXO	Idle
FXO4	FXO	Idle
FXS1	FXS	Idle
FXS2	FXS	Idle
FXS3	FXS	Idle
FXS4	FXS	Idle

Figure 6.48: FXO Line Status

FXO Line Status	
ID	Link State
FX01	Up
FX02	Up
FX03	Up
FX04	Up

1. Set specific FXO characteristics.

Figure 6.49: FXO Configuration



Select **POTS > FXO Configuration**.

In general, the default values are good but to speed up the answering, change the *Wait Before Answering Delay (ms)* from 8000 ms to 500 ms.

FXO Dialing Configuration

Figure 6.50: FXO Dialing Configuration

FXO Dialing Configuration			
Pre Dial Delay (ms):	<input type="text" value="0"/>		
Dial Tone Detection Mode:	<input type="text" value="CountryTone"/>		
Dial Tone Detection Timeout (ms):	<input type="text" value="3000"/>		

FXO Answering Configuration			
ID	Wait Before Answering Delay (ms)	Answering On Caller Id Detection	Wait For Callee To Answer
FXO1	<input type="text" value="500"/>	<input type="text" value="Enable"/>	<input type="text" value="Enable"/>
FXO2	<input type="text" value="500"/>	<input type="text" value="Enable"/>	<input type="text" value="Enable"/>
FXO3	<input type="text" value="500"/>	<input type="text" value="Enable"/>	<input type="text" value="Enable"/>
FXO4	<input type="text" value="500"/>	<input type="text" value="Enable"/>	<input type="text" value="Enable"/>

FXO Incoming Call Behavior	
ID	Not Allowed Behavior
FXO1	<input type="text" value="Play Congestion Tone"/>
FXO2	<input type="text" value="Play Congestion Tone"/>
FXO3	<input type="text" value="Play Congestion Tone"/>
FXO4	<input type="text" value="Play Congestion Tone"/>

FXO Line Verification	
Link State Verification:	<input type="text" value="Enable"/>
Link State Verification Timeout (ms):	<input type="text" value="1000"/>

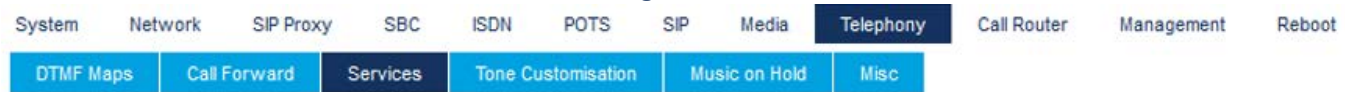
FXO Force End Of Call	
Force End Of Call On Call Failure:	<input type="text" value="Enable"/>
Call Failure Timeout (sec):	<input type="text" value="30"/>
Force End of Call On Silence Detection Mode:	<input type="text" value="Disable"/>
Silence Detection Timeout (sec):	<input type="text" value="300"/>
Force End Of Call On Tone Detection Mode:	<input type="text" value="Country Tone"/>
Tone Detection Custom Frequency:	<input type="text" value="440"/>
Tone Detection Custom Cadence:	<input type="text" value=""/>
Detection Custom Repetition:	<input type="text" value="3"/>

1. Set the answering number for each FXO ports. This number must be a valid extension number, group number or operator number in the central MX-ONE.

Services

1. Select **Telephony > Services** to set a specific market.

Figure 6.51: Services



2. Set the **Automatic Call Target** field.

Select Endpoint:

Services Configuration	Unit Defaults	Endpoint Specific
General Configuration		
Endpoint Specific:		<input type="text" value="No"/>
Hook Flash Processing:	Process Locally	<input type="text" value="Process Locally"/>
Automatic Call		
Endpoint Specific:		<input type="text" value="Yes"/>
Automatic Call Activation:	Disable	<input type="text" value="Enable"/>
Automatic Call Target:		<input type="text" value="44412"/>
Direct IP Address Call		
Direct IP Address Call Activation:	Disable	

3. Set the correct market (Country).

System Network SIP Proxy SBC ISDN POTS SIP Media **Telephony** Call Router Management Reboot

DTMF Maps Call Forward **Services** Tone Customisation Music on Hold Misc

Country
Country Selection <input type="text" value="Sweden1"/>

SIP

Gateways

Figure 6.52: Gateways



Select **SIP > Gateways**.

NOTE: A SIP route must be defined in MX-ONE to handle traffic to and from the **trunks_mx_one** gateway.

Gateway Status						
Name	Signaling Network	Media Networks	Port	Secure Port	State	
MX1_analog_ext	Uplink	Uplink	5080	0	Ready	
trunk_lines_gw	Loop	Loop	5066	0	Network down	
trunks_mx-one	Uplink	Uplink	5070	0	Ready	

Following gateways and port numbers are pre-defined.

Figure 6.53: trunks_mx-one

Gateway Configuration							
Name	Type	Signaling Network	Media Networks	Media Networks Suggestion	Port	Secure Port	
MX1_analog_ext	Trunk	Uplink		--- Suggestion ---	5080	0	-
trunk_lines_gw	Trunk	Loop	Loop	--- Suggestion ---	5066	0	-
trunks_mx-one	Trunk	Uplink		--- Suggestion ---	5070	0	-
							+

Servers

Figure 6.54: Servers

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateways	Servers	Registrations	Authentication	Transport	Interop	Misc					

1. Select **SIP > Servers**.
2. Enter IP-address to MX-ONE in both the **Registrar Host** and **Proxy Host** fields.

Figure 6.55: Default Servers

Default Servers			
Registrar Host:	<input type="text" value="192.168.17.44"/>		
Proxy Host:	<input type="text" value="192.168.17.44"/>		
Messaging Server Host:	<input type="text"/>		
Outbound Proxy Host:	<input type="text"/>		

3. Enter IP-address of MX-ONE in the **Proxy Host** field.
4. Enter IP-address of the gateway in the **Outbound Proxy Host** field.

Figure 6.56: Proxy Servers

Proxy Servers			
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host
MX1_analog_ext	Yes	<input type="text" value="192.168.17.44"/>	<input type="text" value="192.168.17.81"/>
trunk_lines_gw	Yes	<input type="text" value="%sbc%"/>	<input type="text" value="%sbc%"/>
trunks_mx-one	No	<input type="text" value="192.168.0.10:0"/>	<input type="text" value="0.0.0.0:0"/>

5. Change the **Keep Alive Method** to **SIP OPTIONS** and enter **Keep Alive Destination** Gateways.

Figure 6.57: Keep Alive

Keep Alive	
Keep Alive Method:	<div>SIP OPTIONS</div>
Keep Alive Interval (s):	<div>30</div>
Keep Alive Destination:	<div>Alternate Destination</div>

Figure 6.58: Alternate Alive Destination Gateway

Gateway	Alternate Destination
MX1_analog_ext	<div>192.168.17.81</div>
trunk_lines_gw	<div>127.0.0.1</div>
trunks_mx-one	<div>192.168.17.44</div>

6. Click **Apply** when done and restart service.

Registrations

Figure 6.59: Registrations

System Network SIP Proxy SBC ISDN POTS SIP Media Telephony Call Router Management Reboot

Gateways Servers Registrations Authentication Transport Interop Misc

1. Select **SIP > Registrations**.
2. Enter the extension numbers for the analog extensions.

Figure 6.60: Endpoints Registration screen

Endpoints Registration					
Endpoint	User Name	Friendly Name	Register	Messaging	Gateway Name
FXO1			<div>Disable</div>	<div>Disable</div>	<div>trunks_mx-one</div>
FXO2			<div>Disable</div>	<div>Disable</div>	<div>trunks_mx-one</div>
FXO3			<div>Disable</div>	<div>Disable</div>	<div>trunks_mx-one</div>
FXO4			<div>Disable</div>	<div>Disable</div>	<div>trunks_mx-one</div>
FXS1	<div>11104</div>		<div>Enable</div>	<div>Disable</div>	<div>MX1_analog_ext</div>
FXS2	<div>11105</div>		<div>Enable</div>	<div>Disable</div>	<div>MX1_analog_ext</div>
FXS3	<div>11106</div>		<div>Enable</div>	<div>Disable</div>	<div>MX1_analog_ext</div>
FXS4	<div>11107</div>		<div>Enable</div>	<div>Disable</div>	<div>MX1_analog_ext</div>
PRI1			<div>Disable</div>	<div>Disable</div>	<div>trunks_mx-one</div>

3. Click **Apply** or **Apply and Refresh** when done.






































































































Authentication

Figure 6.61: Authentication



1. Select **SIP > Authentication**.

Figure 6.62: Authentication Screen

Authentication									
Priority	Criteria	Endpoint	Gateway	Username	Criteria	Validate	Realm	Realm	User Name
1	Endpoint	FXS1				Disable		11104	    
2	Unit					Enable			    
3	Unit					Enable			    
4	Unit					Enable			    
5	Unit					Enable			    
6	Unit					Enable			    
7	Unit					Enable			    
8	Unit					Enable			    
9	Unit					Enable			    
10	Unit					Enable			    
11	Unit					Enable			    
12	Unit					Enable			    
13	Unit					Enable			    
14	Unit					Enable			    
15	Unit					Enable			    
16	Unit					Enable			    
17	Unit					Enable			    
18	Unit					Enable			    
19	Unit					Enable			    
20	Unit					Enable			    
Number of rows to add: <input type="text" value="1"/>									

2. If password is required click the Image icon for any item that you want to add.
3. Indicate for which **Endpoint** and **Criteria** the changes are to apply.
4. Enter the Auth Code in the **Password** field.
5. In the **Validate Realm** field, select **Disable**.

Figure 6.63: Validate Realm field

Authentication									
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password	
1	Endpoint	FXS1			Disable		11104	*****	

- Click **Apply** or **Apply and Refresh Registration** when done and restart service. The result after *Registration* and *Authentication* should be like as shown in the below screen.

Figure 6.64: Endpoints Registration Status

Endpoints Registration Status				
Endpoint	User Name	Gateway Name	Registrar	Status
FXS1	11104	MX1_analog_ext	192.168.17.44:0	Registered
FXS2	11105	MX1_analog_ext	192.168.17.44:0	Registered
FXS3	11106	MX1_analog_ext	192.168.17.44:0	Registered

Transport

Figure 6.65: Transport

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateways	Servers	Registrations	Authentication	Transport	Interop	Misc					

- Select **SIP > Transport**
- Enable **UDP** or **TCP** dependent on configuration.

Figure 6.66: Protocol Configuration

Protocol Configuration					
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable		Enable		Disable	

- Click **Apply** when done and restart service.

Interop

Figure 6.67: Interop

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateways	Servers	Registrations	Authentication	Transport	Interop	Misc					

- Select **SIP > Interop**.
- Select **trunk** in the **SIP URI User Parameter Value** field.
- This is used in the 'match' parameter for the SIP route in MX-ONE.

Figure 6.68: SIP URI User Parameter Value field

SIP Interop	
Secure Header:	<div>Disable</div>
Default Username Value:	<div>Anonymous</div>
OPTIONS Method Support:	<div>None</div>
Ignore OPTIONS on no Usuable Endpoints:	<div>Disable</div>
SIP URI User Parameter Value:	<div>trunk</div>
Behavior on Machine Detection:	<div>Re-INVITE on Fax T38 Only</div>
Registration Contact Matching:	<div>Strict</div>
Transmission Timeout:	<div>32</div>

4. Click **Apply** or when done and restart service.

Misc

Figure 6.69: Misc

System

Network

SIP Proxy

SBC

ISDN

POTS

SIP

Media

Telephony

Call Router

Management

Reboot

Gateways

Servers

Registrations

Authentication

Transport

Interop

Misc

- 1. Select **SIP > Misc**.
- 2. Enter the IP-address of MX-ONE in the **SIP Domain Override** field for **trunk_lines_gw**.

Figure 6.70: Gateway Configuration field

Gateway Configuration	
Gateway Name	SIP Domain Override
MX1_analog_ext	
trunk_lines_gw	192.168.17.44
trunks_mx-one	

3. Click **Apply** when done and restart service.

Media

Codecs

Figure 6.71: Codecs



1. Select **Media** > **Codecs**.
2. Change **Codecs** according to preference.

Figure 6.72: Codecs

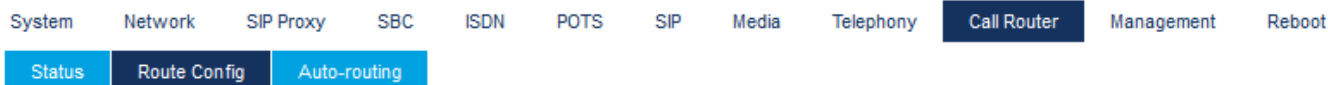
Codec	Voice	Data	Advanced	
G.711 a-Law	<input type="button" value="Enable"/> ▾	<input type="button" value="Enable"/> ▾		
G.711 u-Law	<input type="button" value="Disable"/> ▾	<input type="button" value="Enable"/> ▾		
G.723	<input type="button" value="Disable"/> ▾			
G.726 16Kbps	<input type="button" value="Disable"/> ▾			
G.726 24Kbps	<input type="button" value="Disable"/> ▾			
G.726 32Kbps	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾		
G.726 40Kbps	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾		
G.729	<input type="button" value="Disable"/> ▾			
T.38		<input type="button" value="Enable"/> ▾		
Clear Mode	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾		
Clear Channel	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾		
X CCD	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾		

3. Click **Apply** when done and restart service.

Call Router

Route Config

Figure 6.73: Route Config



1. Select **Call Router > Route Config**.
2. Click for index icon (1). This is used if the received B-number contains a full number, that is, more digits than the pure DID numbers.

Figure 6.74: Routes

Routes						
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination
1	isdn-PRI1, isdn-PRI2, isdn-PRI3, isdn-PRI4, isdn-BRI1, isdn-BRI2, isdn-BRI3, isdn-BRI4, r2-PRI1, r2-PRI2, r2-PRI3, r2-PRI4, e&m-PRI1, e&m-PRI2, e&m-PRI3, e&m-PRI4, fxo-FXO1, fxo-FXO2, fxo-FXO3, fxo-FXO4, fxo-FXO5, fxo-FXO6, fxo-FXO7, fxo-FXO8, fxo-FXO9, fxo-FXO10, fxo-FXO11, fxo-FXO12, fxo-FXO13, fxo-FXO14, fxo-FXO15, fxo-FXO16, fxo-FXO17, fxo-FXO18, fxo-FXO19, fxo-FXO20, fxo-FXO21, fxo-FXO22, fxo-FXO23, fxo-FXO24	None		DID_Extension	local_host	hunt-sip
2	sip-trunks_mx-one, sip-trunk_lines_gw	None			local_host	hunt-Hunt1

3. In the **Transformations** field, add a name for a transformation rule.

Figure 6.75: Configure Route 1

Configure Route 1		
	Value	Suggestion
Sources	isdn-PRI1, isdn-PRI2, isdn-PRI3, isdn-PRI4, isdn-BRI1, isdn-BRI2, isdn-BRI3, isdn-BRI4, r2-PRI1, r2-PRI2, r2-PRI3, r2-PRI4, e&m-PRI1, e&m-PRI2, e&m-PRI3, e&m-PRI4, fxo-FXO1, fxo-FXO2, fxo-FXO3, fxo-FXO4, fxo-FXO5, fxo-FXO6, fxo-FXO7, fxo-FXO8, fxo-FXO9, fxo-FXO10, fxo-FXO11, fxo-FXO12, fxo-FXO13, fxo-FXO14, fxo-FXO15, fxo-FXO16, fxo-FXO17, fxo-FXO18, fxo-FXO19, fxo-FXO20, fxo-FXO21, fxo-FXO22, fxo-FXO23, fxo-FXO24	--- Suggestion ---
Criteria Property	None	
Criteria Rule		--- Suggestion ---
Transformations	DID_Extension	--- Suggestion ---
Signaling Properties	local_host	--- Suggestion ---
Destination	hunt-sip	--- Suggestion ---
Config Status		

4. Click **Save**.
5. Click Plus icon in the first Call Property Transformation and enter the same name as above.
6. Use **Called E164** for both **Criteria Based On** and **Transformation Applies To** fields.

Figure 6.76: Configure Transformation 1

Configure Transformation 1	
	Value
Name	<input type="text" value="DID_Extension"/>
Criteria Based On	<input type="text" value="Called E164"/>
Transformation Applies To	<input type="text" value="Called E164"/>
Config Status	

- Click **Save** or **Save and Insert Rule**.
- Click Plus icon in the second Call Property Transformation, and enter the same name as above.
- The 'Criteria Rule' in this case is 443(111..\$) and the transformation rule is (\1). This means that if a B-number is received containing 44311104, then the 3 first digits (443) are removed before the call is sent to MX-ONE for further processing. (111..\$) means that the number can only be 5 digits starting with 111.

Figure 6.77: Configure Transformation Rule 1 screen

Configure Transformation Rule 1		
	Value	Suggestion
Type	Called E164 to Called E164	
Name	<input type="text" value="DID_Extension"/>	<input type="text" value="--- Suggestion ---"/>
Criteria Rule	<input type="text" value="443(111..\$)"/>	<input type="text" value="--- Suggestion ---"/>
Transformation Rule	<input type="text" value="\1"/>	<input type="text" value="--- Suggestion ---"/>
Next Transformation	<input type="text" value=""/>	<input type="text" value="--- Suggestion ---"/>
Config Status		

- Click **Save** or **Save and Insert Rule**. Now, the 'Call Property Transformations' looks like this as shown below.

Figure 6.78: Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	DID_Extension	Called E164	Called E164	

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	DID_Extension	443(111..\$)	\1	

- Click Plus icon for the Signaling Properties, and enter the data as shown below.

Configure Signaling Property 1		
	Value	Suggestion
Name	<input type="text" value="local_host"/>	
Early Connect	<input type="button" value="Disable"/> ▾	
Early Disconnect	<input type="button" value="Enable"/> ▾	
Destination Host	<input type="text"/>	<input type="button" value="--- Suggestion ---"/> ▾
Allow 180 with SDP	<input type="button" value="Enable"/> ▾	
Allow 183 without SDP	<input type="button" value="Enable"/> ▾	
Privacy	<input type="button" value="Disable"/> ▾	
SIP Header Translation Overrides	<input type="text" value="local_host"/>	<input type="button" value="--- Suggestion ---"/> ▾
Call Property Translation Overrides	<input type="text"/>	<input type="button" value="--- Suggestion ---"/> ▾
Config Status		

12. Click Plus icon for the SIP Header Translation Overrides, and enter the data as shown below.

Configure SIP Header Translation Override 1		
Name	<input type="text" value="local_host"/>	
SIP Header	<input type="button" value="From Header (Host Part)"/> ▾	
Based On	<input type="button" value="Fixed Value"/> ▾	
Fixed Value	<input type="text" value="<local_ip_port>"/>	
Config Status		

13. Click **Save**. Now the Signaling Properties looks like this.

Signaling Properties										
Index	Name	Early Connect	Early Disconnect	Destination Host	Allow 180 with SDP	Allow 183 without SDP	Privacy	SIP Header Translation Overrides	Call Property Translation Overrides	
1	local_host	Disable	Enable		Enable	Enable	Disable	local_host		

SIP Header Translation Overrides				
Index	Name	SIP Header	Based On	Fixed Value
1	local_host	From Header (Host Part)	Fixed Value	<local_ip_port>

Call Property Translation Overrides				
Index	Name	Call Property	Based On	Fixed Value

14. If the yellow indication on top of the page is on, click **Save**.

Management

Backup/Restore

- Click [Activate unsecure script transfers through web browser](#)

Figure 6.79: Image Configuration screen

Image Configuration	
Transfer Parameters	
File Name:	<input type="text" value="20180503_final.xml"/> --- Suggestion ---
Transfer Protocol:	File
Host Name:	<input type="text" value="0.0.0.0:0"/>
Location:	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="password"/>
Backup Parameters	
Content:	Config And Certificates
Privacy Parameters	
Privacy Algorithm:	None
Privacy Key:	<input type="text"/>

- Click **Apply and Backup Now**.

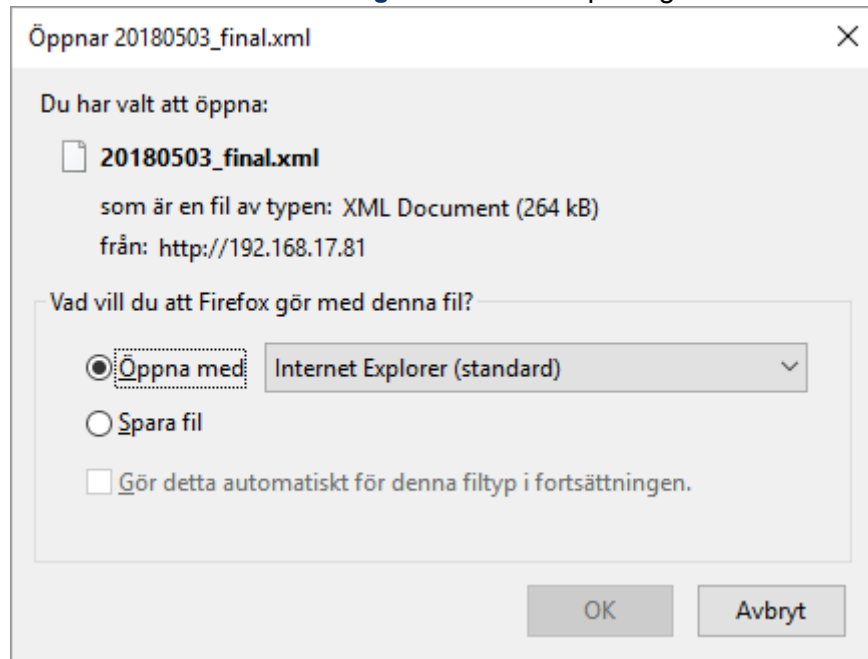
File

Figure 6.80: Internal files screen

Internal files			
Name	Description	Size	
conf/20180503_final.xml	Automatically generated on 03/05/2018 15:50:11.	264 KB	
conf/FXO_Country_Defaults.cfg	FXO Country Defaults	1 KB	
conf/FXO_North-America_3km.cfg	FXO North-America 3km	1 KB	
conf/PRI_China-DSS1.cfg	China DSS1	3 KB	
conf/PRI_Default.cfg	PRI default configuration	3 KB	
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB	
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB	
conf/Survivability.cfg	Configures the unit to use the SipProxy service for basic use cases.	1 KB	
sbc/rulesets/200_OK_to_SIP_OPTIONS.crs	Answer 200 OK to inbound SIP OPTIONS message	1 KB	
sbc/rulesets/MX-One_build_RURI_survivability.crs	Builds the RURI when in survivability mode	6 KB	
sbc/rulesets/MX-One_core_side.crs	Generic ruleset facing MX-One core	5 KB	
sbc/rulesets/MX-One_local_reg_users_with_survivability.crs	local registered users ruleset for MX-One with basic local calling survivability	11 KB	
sbc/rulesets/MX-One_local_users_failover_to_trunk.rrs	Failover route from local_users_ca to trunk_lines_ca	6 KB	
sbc/rulesets/MX-One_outbound_survivability_prefix.crs	ANumber and BNumber prefix	2 KB	
sbc/rulesets/MX-One_remove_prefix.crs	Removes prefix from RURI for outbound calls	1 KB	
sbc/rulesets/MX-One_routes_with_basic_local_survivability_TCP.rrs	MX-One - Basic Routes with Survivability	23 KB	
sbc/rulesets/MX-One_routes_with_basic_local_survivability_UDP.rrs	MX-One - Basic Routes with Survivability	21 KB	
sbc/rulesets/MX-One_to_trunk_lines.rrs	Route from MX-One servers to trunk lines	5 KB	
sbc/rulesets/MX-One_trunk_lines_to_local_users.rrs	Route from trunk_lines_ca to local_users_ca	3 KB	
sbc/rulesets/MX-One_trunk_lines_to_reception_survivability.crs	Forwards trunk calls to reception number in survivability	2 KB	
sbc/rulesets/rewrite_RURI_host.crs	Customize RURI host	1 KB	
21 file(s)	Total: 366 KB / Available: 6 GB		

Find the previously made backup image.

Figure 6.81: Backup image



Setting up GX-GATEWAY with SIP Trunks

This section describes how to setup the 'Göteborg' branch node using SIP trunks towards a SIP provider.

NOTE: The setup for the gateway and SBC part for an EX-controller is identical.

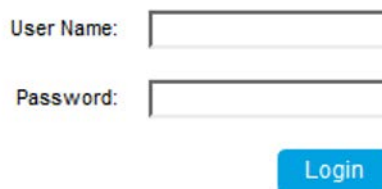
Logon

This section describes how to setup BO#2.

1. Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network).

NOTE: If DHCP is not running into the network then, plug in the network cable to the ETH2 port on EX Controller and use the default IP address of 192.168.0.10 to open the EX Controller Interface.

Figure 7.1: Login page



User Name:

Password:

Login

- User name/password: public /
 - User name/password: admin/administrator
2. Plug in the analog phone in the FXS port 1 of the EX Controller and dial *#*0 to know the IP address of the EX Controller assigned by using DHCP server.
 3. Log into the EX Controller by using the above-mentioned IP address and navigate as described below to configure.

Network Settings

Host

Figure 7.2: Host Settings - 1

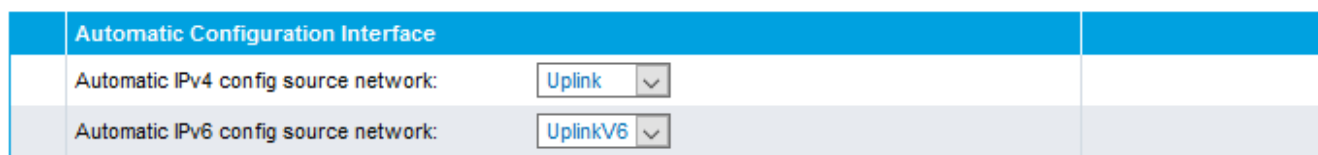


System Network SIP Proxy SBC ISDN POTS SIP Media Telephony Call Router Management Reboot

Status Host Interfaces VLAN QoS Local Firewall IP Routing Network Firewall NAT DHCP Server

1. Select **Network** > **Host**.

Figure 7.3: Host Settings - 2



Automatic Configuration Interface	
Automatic IPv4 config source network:	Uplink
Automatic IPv6 config source network:	UplinkV6

2. Change to **Static IP-address** and enter default Gateway (GW).

Figure 7.4: Changing Static IP Address

Default Gateway Configuration	
IPv4	
Configuration Source:	Static
Default Gateway:	192.168.17.1
IPv6	
Configuration Source:	Automatic IPv6
Default Gateway:	

3. Change to static DNS server and enter IP-address or FQDN to DNS server.

Figure 7.5: Changing Static DNS Server

DNS Configuration	
Configuration Source:	Static
Primary DNS:	10.105.64.3
Secondary DNS:	
Third DNS:	
Fourth DNS:	

4. Change to static SNTP server, enter time server data as required.

Figure 7.6: Changing to Static SNTP Server

SNTP Configuration	
Configuration Source:	Static
Static Servers:	
Primary SNTP:	pool.ntp.org
Secondary SNTP:	
Third SNTP:	
Fourth SNTP:	
Synchronization:	
Synchronization Period:	1440
Synchronization Period On Error:	60

5. Set the **Time Zone**.

Valid options are:

- Pacific Time (Canada and US): PST8PDT7,M3.2.0/02:00:00,M11.1.0/02:00:00
- Mountain Time (Canada and US): MST7MDT6,M3.2.0/02:00:00,M11.1.0/02:00:00
- Central Time (Canada and US): CST6CDT5,M3.2.0/02:00:00,M11.1.0/02:00:00
- Eastern Time (Canada and US): EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00

- Atlantic Time (Canada): AST4ADT3,M3.2.0/02:00:00,M11.1.0/02:00:00
- GMT Standard Time: GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
- W. Europe Standard Time: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00
- China Standard Time: CST-8
- Tokyo Standard Time: TST-9
- Central Australia Standard Time: CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
- Australia Eastern Standard Time: AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
- UTC (Coordinated Universal Time): UTC0

Figure 7.7: Setting Static Time Zone

Time Configuration	
Static Time Zone:	WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00

6. Leave all other items as it is, and click **Apply** when finished.

Interfaces

Figure 7.8: Interface

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Host	Interfaces	VLAN	QoS	Local Firewall	IP Routing	Network Firewall	NAT	DHCP Server		

1. Go to **Network > Interface**.
2. Change **Uplink** to **IpStatic (IPv4 Static)** and enter the static IP-address and Static Default Gateway.

Figure 7.9: Changing Uplink to IpStatic

Network Interface Configuration						
Name	Link	Type	Static IP Address	Static Default Router	Activation	
Lan1	eth2-5	IpStatic (IPv4 Static)	192.168.0.10/24		Enable	-
Uplink	eth1	IpStatic (IPv4 Static)	192.168.17.81/24	192.168.17.1	Enable	-
UplinkV6	eth1	Ip6Static (IPv6 Static)			Disable	-
						+

3. Leave all other items as it is and click **Apply** when ready.

Local Firewalls

Figure 7.10: Local firewalls

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Host	Interfaces	VLAN	QoS	Local Firewall	IP Routing	Network Firewall	NAT	DHCP Server		

1. Go to **Network > Local Firewall**.
2. If local firewall security is needed change default policy to **Drop**.

Figure 7.11: Changing default policy

Configuration Modified:		No
-------------------------	--	----

Local Firewall Configuration	
Default Policy:	Drop
Blacklist Timeout:	60
Blacklist Rate Limit Timeout:	60

- Enter the networks for which traffic can enter from.

Figure 7.12: Enter network traffic

Local Firewall Rules											
#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period	
1	Enable	192.168.17.0/24		Uplink		All	<input type="checkbox"/>	Accept	10	60	⬆ ⬇ ⬆ ⬇
2	Enable	172.17.17.0/24		Uplink		All	<input type="checkbox"/>	Accept	10	60	⬆ ⬇ ⬆ ⬇
3	Enable	10.105.0.0/16		Uplink		All	<input type="checkbox"/>	Accept	10	60	⬆ ⬇ ⬆ ⬇
											+

- Click **Save** or **Save and Apply** when ready.

Session Board Controller (SBC)

Rulesets define one or several rules used to filter, manipulate or route inbound or outbound requests.

There are 2 types of Rulesets:

- **Call Agent Rulesets:** describe how inbound or outbound requests are handled by a specific Call Agent. These can also implement services or collect data.
- **Routing Rulesets:** used to globally route outbound requests, that is, these apply to all Call Agents.

When a request arrives at a Call Agent from a peer, the inbound rules of the Rulesets associated with the Call Agent are executed. Then, Routing Rulesets are executed until a Call Agent is selected for the destination. Lastly, the outbound rules of the Rulesets associated with the destination Call Agent are executed before sending the request to the peer. Inbound rules of the Ruleset are executed in ascending Ruleset priority order. Outbound rules are executed in descending Ruleset priority order.

Configuration

- Go to **SBC > Configuration**. The following Call Agents are present.

Figure 7.13: Configuration




















System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Configuration	Rulesets	Live Calls	Running Config	Events	Registration					

Figure 7.14: Configuration Modified

Configuration Modified:	no
-------------------------	----

Following Call Agents are present.




















Figure 7.15: Call Agent Configuration

Call Agent Configuration								
Name	Enable	Gateway	Signaling Interface	Media Interface	Peer Host	Peer Network		
local_users_ca	<input checked="" type="checkbox"/>		uplink_s	uplink_m		0.0.0.0/0	 	
trunk_lines_ca	<input checked="" type="checkbox"/>	trunk_lines_gw		loop_m			 	
remote_users_ca	<input type="checkbox"/>		uplink_s	uplink_m			 	
MX-One_LIM1	<input checked="" type="checkbox"/>		uplink_s	uplink_m	192.168.17.44		 	
MX-One_LIM2	<input type="checkbox"/>		uplink_s	uplink_m	lim2.mitel.com		 	
MX-One-trunk	<input checked="" type="checkbox"/>		trunk_s	uplink_m	lim1.mitel.com		 	
MX-One-trunk2	<input type="checkbox"/>		trunk_s	uplink_m	lim2.mitel.com		 	
VoIP-trunk1	<input type="checkbox"/>		uplink_s	uplink_m	voip.provider1		 	
VoIP-trunk2	<input checked="" type="checkbox"/>		uplink_s	uplink_m	voip.provider2		 	
								

Routing Rulesets

Routing Rulesets: are used to globally route outbound requests, that are applied to all Call Agents. Routing Rulesets are executed until a Call Agent is selected for the destination.

Figure 7.16: Routing Rulesets

Routing Rulesets					
Priority	Name	Parameters			
1	MX-One_local_users_failover_to_trunk	A_PRFX=013443 TRUNK_CA=trunk_lines_ca	  		
2	MX-One_trunk_lines_to_local_users	TRUNK_CA=trunk_lines_ca	  		
3	MX-One_routes_with_basic_local_survivability_TCP		  		
4	MX-One_routes_with_basic_local_survivability_UDP		  		
5	SIP_trunk_to_MX-One	TRUNK_CA=trunk_lines_ca MX-ONE-TRUNK_CA=MX-One-trunk	  		
6	MX-One_to_trunk_lines	MX-ONE-TRUNK_CA=MX-One-trunk TRUNK_CA=trunk_lines_c	  		
					

- **Ruleset MX-One_local_users_failover_to_trunk**

A_PRFX=031325

This is the prefix for the local numbers used on outgoing calls to the PSTN (in this example, you will receive a number block 031325xxxxx from the PSTN provider and add the prefix on outgoing calls, so that the calling party number sent to the PSTN is correct).

TRUNK_CA=VoIP-trunk2

This is the call agent from which the call is coming from.

- **Ruleset MX-One_trunk_lines_to_local_users**

TRUNK_CA=VoIP-trunk2

This is the call agent from which the call is coming.

- **Ruleset SIP_trunk to_MX-One**

TRUNK_CA=VoIP-trunk2

This is the call agent from which the call is coming.

MX-ONE-TRUNK=MX-One-trunk_CA

This is the call agent to which the call will be routed to.

Ruleset MX-One_to_trunk_lines

TRUNK_CA=VoIP-trunk2

This is the call agent from which the call is coming.

TRUNK2_CA=VoIP-trunk2 (Not used at the moment, this is a placeholder for future use).

This is the call agent from which the call is coming.

MX-ONE-TRUNK_CA=MX-One-trunk_CA

This is the call agent to which the call will be routed to.

1. Click **Save** and **Apply** when done.
2. Configure each call agent (ca).
3. Click **Modify** to enter specific data for each call agent.

local_users_ca

Figure 7.17: Configure Call Agent screen

Configure Call Agent		Value
Call Agent Parameters		
Name	<input type="text" value="local_users_ca"/>	
Enable	<input checked="" type="checkbox"/>	
Gateway	<input type="text" value=""/>	
Signaling Interface	<input type="text" value="uplink_s"/>	
Media Interface	<input type="text" value="uplink_m"/>	
Peer Host	<input type="text" value=""/>	
Peer Network	<input type="text" value="0.0.0.0/0"/>	
Force Transport	<input type="text" value="None"/>	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	<input type="text" value="0"/>	
Blacklisting Duration	<input type="text" value="0"/>	
Blacklisting Delay	<input type="text" value="0"/>	
Blacklisting Error Codes	<input type="text" value=""/>	

Figure 7.18: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	<input type="text" value="MX-One_build_RURI_survivability"/>	<input type="text" value="EXT_DIGIT_LENGTH=5 PATTERN=111[0-9][0-9] DOMAIN=192.16"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
2	<input type="text" value="MX-One_Appearance_Prefix"/>	<input type="text" value="APP_PRFX=SCA-"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
3	<input type="text" value="MX-One_Appearance_Prefix"/>	<input type="text" value="APP_PRFX=EDN-"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
4	<input type="text" value="MX-One_Remove_Outbound_Appearance"/>	<input type="text" value="PATTERN=111[0-9][0-9]"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
5	<input type="text" value="MX-One_outbound_A_Number_prefix"/>	<input type="text" value="PATTERN=111[0-9][0-9] A_PRFX=013443 PSTN_PREFIX=00"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
6	<input type="text" value="MX-One_outbound_B_Number_prefix"/>	<input type="text" value="BNUMBER=67[0-9][0-9][0-9] B_PRFX=08568"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
7	<input type="text" value="MX-One_outbound_B_Number_prefix"/>	<input type="text" value="BNUMBER=221[0-9][0-9] B_PRFX=031325"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
8	<input type="text" value="MX-One_outbound_B_Number_prefix"/>	<input type="text" value="BNUMBER=321[0-9][0-9] B_PRFX=040598"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
9	<input type="text" value="MX-One_outbound_B_Number_prefix"/>	<input type="text" value="BNUMBER=421[0-9][0-9] B_PRFX=036618"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
10	<input type="text" value="MX-One_outbound_B_Number_Override"/>	<input type="text" value="BNUMBER=^09 BOVERRIDE=0856867000"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
11	<input type="text" value="MX-One_local_reg_users_with_survivability"/>	<input type="text" value="EXT_DIGIT_LENGTH=5"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
			<input data-cs="3" data-kind="parent" type="button" value="+"/>

- **Ruleset MX-One_build_RURI survivability (Active only in Survival Mode)**

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 22100 - 22199.

PATTERN=221[0-9][0-9]

The pattern for the internal range of numbers would be 22100 - 22199.

Calls to this number range stay always local (would not be sent to the PSTN in survival mode).

DOMAIN=192.168.17.44

The IP-address of the MX-ONE in this case 192.168.17.44.

- **Ruleset: MX_One_Appearance_Prefix (Active only in Survival Mode)**

APP_PREFIX=SCA- and APP_PREFIX=EDN-

This is the prefix for the usernames connected with shared appearance and extra directory number (EDN). In this example, you have two user names: SCA- and EDN-

- **Ruleset: MX-One_Remove_Outbound_Appearance (Active only in Survival Mode)**

PATTERN=221[0-9][0-9]

This defines the local numbers, in this example the internal range would be 22100 - 22199.

A_PRFX=031325

This is the prefix for the local numbers used on outgoing calls to the PSTN. In this example, you can add a number block 031325 in front of the number specified in PATTERN-parameter to form a valid calling party number to be sent to the PSTN.

PSTN_PREFIX=00

This parameter specifies the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will be truncated.

- **Ruleset: MX-One_outbound_B_Number_prefix (Active only in Survival Mode)**

This ruleset applies to calls to numbers defined in BNUMBER and will add B_PRFX to the called party number.

This ruleset must be repeated for every approved destination (that is, calling the HQ and other branch offices).

Calling HQ:

BNUMBER=67[0-9][0-9][0-9]

Applies to calls to the specific range of extensions. The pattern for the internal range of numbers would be 67000 - 67999.

B_PRFX=08568

This is the prefix for the Called Party Number. In this case, it will be built like: National Prefix (08) + Main part of the HQ's local number: (568).

Calling BO#1:

BNUMBER=111[0-9][0-9]

Applies to calls to the specific range of extensions. The pattern for the internal range of numbers would be 11100 - 11199.

B_PRFX=013443

This is the prefix for the Called Party Number. In this case it will be built like: National Prefix (013) + Main part of the HQ's local number: (443).

Calling BO#3:

BNUMBER=321[0-9][0-9] Applies to calls to the specific range of extensions. The pattern for the internal range of numbers, in this example the internal range would be 32100 - 32199.

B_PRFX=040598

This is the prefix for the Called Party Number. In this case it will be built like: National Prefix (040) + Main part of the HQ's local number: (598).

Calling BO#4:

BNUMBER=421[0-9][0-9]

Applies to calls to the specific range of extensions. The pattern for the internal range of numbers, in this example the internal range would be 42100 - 42199.

B_PRFX=036618

This is the prefix for the Called Party Number. In this case it will be built like: National Prefix (036) + Main part of the HQ's local number: (618).

- **Ruleset: MX-One_outbound_B_Number_Override (Active only in Survival Mode)**

This ruleset applies to calls to numbers defined in BNUMBER and will use the BOVERRIDE as Called Party Number.

One use case could be if a user dials the internal operator (09) while in survivable mode. The dialled number (09) will be replaced with 0856867000 which could be the number to the operator in the HQ.

BNUMBER=09

The internal number to the operator.

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE. In this example, it will be sent to 0856867000.

- **Ruleset: MX-One_local_reg_users_with_survivability**

(Builds the registration cache for survivability purpose).

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 22100 - 22199.

Click **Save** when done.

trunk_lines_ca

Figure 7.19: trunk_lines_ca

Configure Call Agent	
	Value
Call Agent Parameters	
Name	trunk_lines_ca
Enable	<input checked="" type="checkbox"/>
Gateway	trunk_lines_gw
Signaling Interface	
Media Interface	loop_m
Peer Host	
Peer Network	
Force Transport	Tcp
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	0
Blacklisting Duration	0
Blacklisting Delay	0
Blacklisting Error Codes	

Figure 7.20: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	200_OK_to_SIP_OPTIONS		⬆ ⬇ ⬅
2	MX-One_remove_prefix	PSTN_PREFIX=00	⬆ ⬇ ⬅
3	MX-One_trunk_lines_to_reception_survivability	EXT_DIGIT_LENGTH=5 MAIN_EXT=11104 PATTERN=111[0-9][0-	⬆ ⬇ ⬅
4	MX-One_build_RURI_survivability	EXT_DIGIT_LENGTH=5 PATTERN=111[0-9][0-9] DOMAIN=192.16	⬆ ⬇ ⬅
5	MX-One_Appearance_Prefix	APP_PRFX=SCA-	⬆ ⬇ ⬅
6	MX-One_Appearance_Prefix	APP_PRFX=EDN-	⬆ ⬇ ⬅
7	media_relay		⬆ ⬇ ⬅
			+

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

This parameter specified the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will be truncated.

- **Ruleset: MX-One_trunk_lines_to_reception_survivability**

An incoming call in survival mode will be sent to MAIN_EXT destination if not reachable or not available.

EXT_DIGIT_LENGTH=5

The length of the internal numbers, in this case set to 5, for numbers like 11100 - 11199.

MAIN_EXT=22104

This is the extension number (22104) and the call will be routed to when an incoming call's destination is not reachable (not defined or not registered). Where, MAIN_EXT is the default answering position.

PATTERN=221[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 22100 - 22199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44.

- **Ruleset: MX-One_build_RURI_survivability (Active only in Survival Mode)**

Builds the RURI when in survivability mode.

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 22100 - 22199.

PATTERN=221[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 22100 - 22199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44.

- **Ruleset: MX_One_Appearance_Prefix (Active only in Survival Mode)**

APP_PREFIX=SCA- and APP_PREFIX=EDN-

This is the prefix for the user names connected with shared appearance (SCA) and extra directory number (EDN). In this example, you have two user names: "SCA"- and "EDN-"

Click **Save** when done.

MX-One_Lim1

1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 7.21: Configure Call Agent - Peer Host

Configure Call Agent		Value
Call Agent Parameters		
Name	<input type="text" value="MX-One_LIM1"/>	
Enable	<input checked="" type="checkbox"/>	
Gateway	<input type="text" value=""/>	
Signaling Interface	<input type="text" value="uplink_s"/>	
Media Interface	<input type="text" value="uplink_m"/>	
Peer Host	<input type="text" value="192.168.17.44"/>	
Peer Network	<input type="text" value=""/>	
Force Transport	<input type="text" value="None"/>	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	<input type="text" value="30"/>	
Blacklisting Duration	<input type="text" value="60"/>	
Blacklisting Delay	<input type="text" value="0"/>	
Blacklisting Error Codes	<input type="text" value=""/>	

2. Enter the IP-address of the GW in the **RURI_HOST** parameter.

Figure 7.22: RURI_HOST parameter

Call Agent Rulesets			
Priority	Name	Parameters	
1	<input type="text" value="rewrite_RURI_host"/>	<input type="text" value="RURI_HOST=192.168.17.83"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
2	<input type="text" value="MX-One_core_side"/>	<input type="text" value=""/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
			<input type="button" value="+"/> <input type="button" value="−"/>

- **Ruleset: rewrite_RURI_host**
RURI_HOST= 192.168.17.83
This is the local IP address of the GX-gateway.
Click **Save** when done.

MX-One_trunk

1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

NOTE: Though the **MX-One-trunk** is not used in this configuration but you must enable it.

Figure 7.23: Call Agent Parameters

Configure Call Agent		Value
Call Agent Parameters		
Name	<input type="text" value="MX-One-trunk"/>	
Enable	<input checked="" type="checkbox"/>	
Gateway	<input type="text" value=""/>	
Signaling Interface	<input type="text" value="trunk_s"/>	
Media Interface	<input type="text" value="uplink_m"/>	
Peer Host	<input type="text" value="192.168.17.44"/>	
Peer Network	<input type="text" value=""/>	
Force Transport	<input type="text" value="None"/>	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	<input type="text" value="30"/>	
Blacklisting Duration	<input type="text" value="60"/>	
Blacklisting Delay	<input type="text" value="0"/>	
Blacklisting Error Codes	<input type="text" value=""/>	

Figure 7.24: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	<input type="text" value="media_relay"/>	<input type="text" value=""/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
2	<input type="text" value="face_mxone"/>	<input type="text" value="SOURCE_CA=trunk_lines_ca RURI_HOST=192.168.17.81"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
3	<input type="text" value="MX-One_remove_prefix"/>	<input type="text" value="PSTN_PREFIX=00"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
4	<input type="text" value="MX-One_trunk_lines_to_reception_survivability"/>	<input type="text" value="EXT_DIGIT_LENGTH=5 MAIN_EXT=11104 PATTERN=111[0-9][0-9]"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
5	<input type="text" value="MX-One_build_RURI_survivability"/>	<input type="text" value="EXT_DIGIT_LENGTH=5 PATTERN=111[0-9][0-9] DOMAIN=192.16"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
6	<input type="text" value="MX-One_core_side"/>	<input type="text" value=""/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="−"/>
			<input type="button" value="+"/>

- **Ruleset: face_mxone**

SOURCE_CA=VoIP-trunk2

This parameter indicates the call agent from which the call is coming from.

RURI_HOST=192.168.17.83

This parameter is used to set a correct value in the FROM DOMAIN in the INVITE message sent to MX-ONE. It shall be the local IP-address of the GX-gateway.

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

This parameter specified the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will be truncated.

- **Ruleset: MX-One_trunk_lines_to_reception_survivability**

An incoming call in survival mode will be sent to MAIN_EXT destination if not reachable or not available.

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 22100 - 22199.

MAIN_EXT=22104

This extension number (22104) will receive the incoming call in case the original destination is not reachable (not defined or not registered).

PATTERN=221[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 22100 - 22199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44

- **Ruleset: MX-One_build_RURI_survivability**

Builds the RURI when in survivability mode

EXT_DIGIT_LENGTH=5

The length of the internal numbers is set to 5, for numbers like 22100 - 22199.

PATTERN=221[0-9][0-9]

This defines the local numbers. The pattern for the internal range of numbers would be 22100 - 22199.

DOMAIN=192.168.17.44

The IP-address of the headquarter (the main PBX) is 192.168.17.44.

Click **Save** when done.

VOIP-trunk2

Configure Call Agent		Value
Call Agent Parameters		
Name	<input type="text" value="VoIP-trunk2"/>	
Enable	<input checked="" type="checkbox"/>	
Gateway	<input type="text" value=""/>	
Signaling Interface	<input type="text" value="uplink_s"/>	
Media Interface	<input type="text" value="uplink_m"/>	
Peer Host	<input type="text" value="192.168.17.54"/>	
Peer Network	<input type="text" value=""/>	
Force Transport	<input type="text" value="None"/>	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	<input type="text" value="0"/>	
Blacklisting Duration	<input type="text" value="0"/>	
Blacklisting Delay	<input type="text" value="0"/>	
Blacklisting Error Codes	<input type="text" value=""/>	

VoIP-trunk2

Figure 7.25: Call Agent Rulesets

Call Agent Rulesets			
Priority	Name	Parameters	
1	topology_hiding_out		⬆ ⬇ ⬅
2	MX-One_remove_prefix	PSTN_PREFIX=00	⬆ ⬇ ⬅
3	face_mxone	SOURCE_CA=VoIP-trunk2 RURI_HOST=192.168.17.83	⬆ ⬇ ⬅
			⬆

• Ruleset: MX-One_remove_prefix

PSTN_PREFIX=00

This parameter specified the prefix to break out to the PSTN. When a user dials this number (in survivable mode) it will truncated.

• Ruleset: face_mxone

SOURCE_CA=VoIP-trunk2

This parameter indicates the call agent from which the call is coming.

RURI_HOST=192.168.17.81

This parameter is used to set a correct value in the FROM DOMAIN in the INVITE message sent to MX-ONE. It will be the local IP-address of the GX-gateway.

Click **Save** when done.

When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.



Click **Apply** when ready.

NOTE: Error will be shown in the configuration if the indication is not removed. Double check the changes described above and correct them.

SIP

Gateways

Figure 7.26: Gateways



Following gateways are predefined and port numbers.

NOTE: The SIP route must be defined in MX-ONE to handle traffic to and from the **trunks_mx-one** gateway.

Figure 7.27: Gateway Configuration

Gateway Configuration							
Name	Type	Signaling Network	Media Networks	Media Networks Suggestion	Port	Secure Port	
MX1_analog_ext	Trunk	Uplink		--- Suggestion ---	5080	0	—
trunk_lines_gw	Trunk	Loop	Loop	--- Suggestion ---	5066	0	—
trunks_mx-one	Trunk	Uplink		--- Suggestion ---	5070	0	—
							+

Servers

Figure 7.28: Servers

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateways	Servers	Registrations	Authentication	Transport	Interop	Misc					

1. Select **SIP > Servers**.
2. Enter IP-address to MX-ONE in both the **Registrar Host** and **Proxy Host** fields.

Figure 7.29: Default Servers

Default Servers	
Registrar Host:	192.168.17.94
Proxy Host:	192.168.17.94
Messaging Server Host:	
Outbound Proxy Host:	

3. Enter IP-address of MX-ONE in the **Proxy Host** field.
4. Enter IP-address of the gateway in the **Outbound Proxy Host** field.

Figure 7.30: Proxy Servers

Proxy Servers			
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host
MX1_analog_ext	Yes	192.168.17.94	192.168.17.85
trunk_lines_gw	Yes	192.168.17.94	%sbc%
trunks_mx-one	No	192.168.0.10:0	0.0.0.0:0

5. Click **Apply** when done and restart service.

Registrations

Figure 7.31: Registrations



1. Select **SIP > Registrations**.
2. Enter the extension numbers for the analog extensions.

Figure 7.32: Endpoints Registration screen

Endpoints Registration						
Endpoint	User Name	Friendly Name	Register	Messaging	Gateway Name	
Slot1/E1T1	<input type="text"/>	<input type="text"/>	Disable ▾	Disable ▾	trunks_mx-one ▾	
Slot2/E1T1	<input type="text"/>	<input type="text"/>	Disable ▾	Disable ▾	trunks_mx-one ▾	
Slot3/FXS1	<input type="text" value="32104"/>	<input type="text"/>	Enable ▾	Disable ▾	MX1_analog_ext ▾	
Slot3/FXS2	<input type="text" value="32105"/>	<input type="text"/>	Enable ▾	Disable ▾	MX1_analog_ext ▾	
Slot3/FXS3	<input type="text" value="32106"/>	<input type="text"/>	Enable ▾	Disable ▾	MX1_analog_ext ▾	
Slot3/FXS4	<input type="text" value="32107"/>	<input type="text"/>	Disable ▾	Disable ▾	MX1_analog_ext ▾	
Slot4/E1T1	<input type="text"/>	<input type="text"/>	Disable ▾	Disable ▾	trunks_mx-one ▾	
Slot5/E1T1	<input type="text"/>	<input type="text"/>	Disable ▾	Disable ▾	trunks_mx-one ▾	

3. Click **Apply** or **Apply and Refresh** when done.

Authentication

Figure 7.33: Authentication



1. Select **SIP > Authentication**.

Figure 7.34: Authentication Screen

Endpoints Registration Status				
Endpoint	User Name	Gateway Name	Registrar	Status
Slot3/FXS1	32104	MX1_analog_ext	192.168.17.93:0	Registered
Slot3/FXS2	32105	MX1_analog_ext	192.168.17.93:0	Registered
Slot3/FXS3	32106	MX1_analog_ext	192.168.17.93:0	Registered

2. If password is required click the Modify icon for any item that you want to add.
3. Indicate for which **Endpoint** and **Criteria** the changes are to be applied.
4. Enter the Auth Code in the **Password** field.
5. In the **Validate Realm** field, select **Disable**.

Figure 7.35: Validate Realm field

Authentication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password
1	Endpoint	Slot3/FXS1			Disable		32104	*****

6. Click **Apply** or **Apply and Refresh Registration** when done, restart service. The result after *Registration* and *Authentication* should be like as shown in the below screen.

Figure 7.36: Endpoints Registration Status

Endpoints Registration Status					
Endpoint	User Name	Gateway Name	Registrar	Status	
FXS1	11104	MX1_analog_ext	192.168.17.44:0	Registered	
FXS2	11105	MX1_analog_ext	192.168.17.44:0	Registered	
FXS3	11106	MX1_analog_ext	192.168.17.44:0	Registered	

Transport

Figure 7.37: Transport

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateways	Servers	Registrations	Authentication	Transport	Interop	Misc					

1. Select **SIP > Transport**
2. Enable **UDP** or **TCP** dependent on configuration.

Figure 7.38: Protocol Configuration

Protocol Configuration					
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable		Enable		Disable	

NOTE: Only 1 transport mechanism can be **Enabled** if both enabled survivability will not work.

3. Click **Apply** when done and restart service.

Misc

Figure 7.39: Misc

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateways	Servers	Registrations	Authentication	Transport	Interop	Misc					

1. Select **SIP > Misc**.
2. Enter the IP-address of MX-ONE in the **SIP Domain Override** field for **trunk_lines_gw**.

Figure 7.40: Gateway Configuration field

Gateway Configuration		
Gateway Name	SIP Domain Override	
MX1_analog_ext	<input type="text"/>	
trunk_lines_gw	<input type="text" value="192.168.17.44"/>	
trunks_mx-one	<input type="text"/>	

- Click **Apply** when done and restart service.

Media












Codecs

Figure 7.41: Codecs

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Codecs	Security	RTP Statistics	Misc								

- Select **Media > Codecs**.
- Change **Codecs** according to preference.

Figure 7.42: Codecs

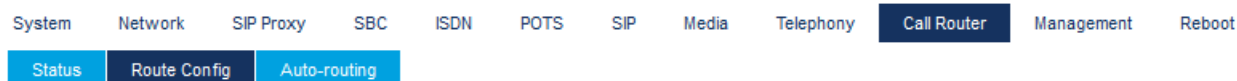
Codec	Voice	Data	Advanced
G.711 a-Law	<input type="button" value="Enable"/> ▾	<input type="button" value="Enable"/> ▾	
G.711 u-Law	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	
G.723	<input type="button" value="Disable"/> ▾		
G.726 16Kbps	<input type="button" value="Disable"/> ▾		
G.726 24Kbps	<input type="button" value="Disable"/> ▾		
G.726 32Kbps	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	
G.726 40Kbps	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	
G.729	<input type="button" value="Enable"/> ▾		
T.38		<input type="button" value="Enable"/> ▾	
Clear Mode	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	
Clear Channel	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	
X CCD	<input type="button" value="Disable"/> ▾	<input type="button" value="Disable"/> ▾	

- Click **Apply** when done and restart service.

Call Router









Route Config

Figure 7.43: Route Config screen



1. Click Modify icon for index 1. This is used if the received B-number contains a full number. That is, more digits than the pure DID numbers.

Figure 7.44: Routes

Routes						
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination
1	isdn-Slot1/E1T1, isdn-Slot2/E1T1, isdn-Slot3/E1T1, isdn-Slot4/E1T1, isdn-Slot5/E1T1, isdn-Slot6/E1T1, isdn-Slot7/E1T1, isdn-Slot8/E1T1, r2-Slot1/E1T1, r2-Slot2/E1T1, r2-Slot3/E1T1, r2-Slot4/E1T1, r2-Slot5/E1T1, r2-Slot6/E1T1, r2-Slot7/E1T1, r2-Slot8/E1T1, e&m-Slot1/E1T1, e&m-Slot2/E1T1, e&m-Slot3/E1T1, e&m-Slot4/E1T1, e&m-Slot5/E1T1, e&m-Slot6/E1T1, e&m-Slot7/E1T1, e&m-Slot8/E1T1, fxo-Slot2/FXO1, fxo-Slot2/FXO2, fxo-Slot2/FXO3, fxo-Slot2/FXO4, fxo-Slot3/FXO1, fxo-Slot3/FXO2, fxo-Slot3/FXO3, fxo-Slot3/FXO4, fxo-Slot4/FXO1, fxo-Slot4/FXO3, fxo-Slot4/FXO2, fxo-Slot4/FXO4, fxo-Slot5/FXO1, fxo-Slot5/FXO2, fxo-Slot5/FXO3, fxo-Slot5/FXO4, fxo-Slot6/FXO1, fxo-Slot6/FXO2, fxo-Slot6/FXO3, fxo-Slot6/FXO4, fxo-Slot7/FXO1, fxo-Slot7/FXO2, fxo-Slot7/FXO3, fxo-Slot7/FXO4, fxo-Slot8/FXO1, fxo-Slot8/FXO2, fxo-Slot8/FXO3, fxo-Slot8/FXO4	None		DID_Extension		sip-trunk_lines_gw    
2	sip-trunks_mx-one, sip-trunk_lines_gw	None				hunt-Hunt1    

2. In the Transformations field, add a name for a transformation rule.

Figure 7.45: Configure Route

Configure Route 1		
	Value	Suggestion
Sources	isdn-Slot1/E1T1, isdn-Slot2/E1T1, isdn-Slot3/E1T1, isdn-Slot4/E1T1, isdn-Slot5/E1T1, isdn-Slot6/E1T1, isdn-Slot7/E1T1, isdn-Slot8/E1T1, r2-Slot1/E1T1, r2-Slot2/E1T1, r2-	--- Suggestion ---
Criteria Property	None	
Criteria Rule		--- Suggestion ---
Transformations	DID_Extension	--- Suggestion ---
Signaling Properties		--- Suggestion ---
Destination	sip-trunk_lines_gw	--- Suggestion ---
Config Status		

3. Click **Save**.
4. Click Plus icon in the first Call Property Transformation and enter the same name as above.
5. Use Called E164 for both **Criteria Based On** and **Transformation Applies To** fields.

Figure 7.46: Configure Transformation

Configure Transformation 1	
	Value
Name	<input type="text" value="DID_Extension"/>
Criteria Based On	<input type="text" value="Called E164"/>
Transformation Applies To	<input type="text" value="Called E164"/>
Config Status	






6. Click Plus icon in the second Call Property Transformation, and enter the same name as above.
7. The Criteria Rule in this case is 443(111..)\$ and the transformation rule is \1.
8. This means that if a B-number is received containing 59832104, then the 3 first digits (443) are removed before the call is sent to MX-ONE for further processing. (111..)\$ means that the number can only be 5 digits starting with 111.






Figure 7.47: Configure Transformation Rule 1

Configure Transformation Rule 1		
	Value	Suggestion
Type	Called E164 to Called E164	
Name	<input type="text" value="DID_Extension"/>	<input type="text" value="--- Suggestion ---"/>
Criteria Rule	<input type="text" value="598(321..\$)"/>	<input type="text" value="--- Suggestion ---"/>
Transformation Rule	<input type="text" value="\1"/>	<input type="text" value="--- Suggestion ---"/>
Next Transformation	<input type="text" value=""/>	<input type="text" value="--- Suggestion ---"/>
Config Status		

9. Click **Save** or **Save and Insert Rule**. Now, the Call Property Transformations looks like this as shown below.

Figure 7.48: Transformations

Transformations				
Index	Name	Criteria Based On	Transformation Applies To	
1	DID_Extension	Called E164	Called E164	   
				

Transformation Rules				
Index	Name	Criteria Rule	Transformation Rule	Next Transformation
1	DID_Extension	598(321..\$)	\1	
				   
				

10. Click Plus icon for the Signalling Properties, and enter the data shown below.

Figure 7.49: Configure Signaling Property 1

Configure Signaling Property 1		
	Value	Suggestion
Name	<input type="text" value="local_host"/>	
Early Connect	<input type="button" value="Disable"/> ▾	
Early Disconnect	<input type="button" value="Enable"/> ▾	
Destination Host	<input type="text"/>	<input type="button" value="--- Suggestion ---"/> ▾
Allow 180 with SDP	<input type="button" value="Enable"/> ▾	
Allow 183 without SDP	<input type="button" value="Enable"/> ▾	
Privacy	<input type="button" value="Disable"/> ▾	
SIP Header Translation Overrides	<input type="text" value="local_host"/>	<input type="button" value="--- Suggestion ---"/> ▾
Call Property Translation Overrides	<input type="text"/>	<input type="button" value="--- Suggestion ---"/> ▾
Config Status		

11. Click Plus icon for the **SIP Header Translation Overrides**, and enter the following data as shown below.

Figure 7.50: Configure SIP Header Translation Override 1

Configure SIP Header Translation Override 1	
Name	<input type="text" value="local_host"/>
SIP Header	<input type="button" value="From Header (Host Part)"/> ▾
Based On	<input type="button" value="Fixed Value"/> ▾
Fixed Value	<input type="text" value="<local_ip_port>"/>
Config Status	

12. Click **Save** Now the Signalling Properties looks like this as shown below.

Signaling Properties										
Index	Name	Early Connect	Early Disconnect	Destination Host	Allow 180 with SDP	Allow 183 without SDP	Privacy	SIP Header Translation Overrides	Call Property Translation Overrides	
1	local_host	Disable	Enable		Enable	Enable	Disable	local_host		

SIP Header Translation Overrides				
Index	Name	SIP Header	Based On	Fixed Value
1	local_host	From Header (Host Part)	Fixed Value	<local_ip_port>

Call Property Translation Overrides				
Index	Name	Call Property	Based On	Fixed Value

13. Click **Save** if the yellow indication on top of the page is on.

Management

Backup/Restore

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Configuration Scripts	Backup / Restore	Firmware Upgrade	Certificates	SNMP	CWMP	Access Control	File	Misc			

1. Select **Management** > **Backup/Restore**.
2. Click the [Activate unsecure script transfers through web browser](#) link.

Figure 7.51: Image Configuration

Image Configuration	
Transfer Parameters	
File Name:	<input type="text" value="Backup_2018-07-30_85.xml"/> <input type="button" value="--- Suggestion ---"/>
Transfer Protocol:	<input type="text" value="File"/>
Host Name:	<input type="text" value="0.0.0.0:0"/>
Location:	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Backup Parameters	
Content:	<input type="text" value="Config And Certificates"/>
Privacy Parameters	
Privacy Algorithm:	<input type="text" value="None"/>
Privacy Key:	<input type="text"/>

3. Click **Apply and Backup Now**.

File

Figure 7.52: File screen



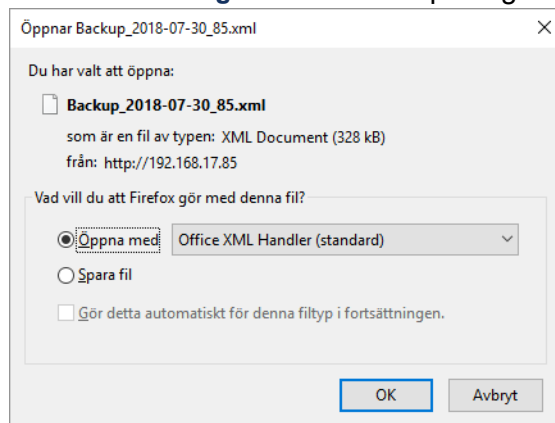
1. Select **Management > File**.

Figure 7.53: Internal files

Internal files			
Name	Description	Size	
conf/Backup_2018-07-30_85.xml	Automatically generated on 24/08/2018 08:29:46.	149 KB	—
conf/FXO_Country_Defaults.cfg	FXO Country Defaults	1 KB	—
conf/FXO_North-America_3km.cfg	FXO North-America 3km	1 KB	—
conf/PRI_China-DSS1.cfg	China DSS1	3 KB	—
conf/PRI_Default.cfg	PRI default configuration	3 KB	—
conf/PRI_NorthAmerica-NI1.cfg	North America NI1	3 KB	—
conf/PRI_NorthAmerica-NI2.cfg	North America NI2	3 KB	—
conf/Survivability_Enable.cfg	Configures the EX Controller for MX-ONE survivability environment.	29 KB	—
conf/Survivability.cfg	Configures the unit to use the SipProxy service for basic use cases.	1 KB	—
vm/drives/mxone7.iso	Bootable disc file	6.2 GB	—
10 file(s)		Total: 6.2 GB / Available: 2.4 GB	

1. Find the previously made backup image.

Figure 7.54: Backup image



2. Download and store on a secure place.

Known Limitations

Below are some known limitations when using the EX-Controller or GX-Gateway:

- When MX-ONE is installed as a virtual machine in the EX-Controller, Provisioning Manager is not allowed to be installed.
- When EX-Controller is used in a multi-server configuration the EX-controller can never be the master server.
- Maximum 5 servers can exist in a multi-server configuration, where at least one of the servers is an EX-controller.
- When deploying a MX-ONE as a virtual machine, the maximum amount of RAM is 7168 Mbytes.

