MiVoice MX-ONE Optional Installations Release 7.3 SP1 February 19, 2021



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: <u>http://www.mitel.com/trademarks</u>.

> ®,™ Trademark of Mitel Networks Corporation
> © Copyright 2021, Mitel Networks Corporation All rights reserved

Contents

Chapter:	1	MiCollab Integration1MiCollab Example Introduction1Prerequisites1OVA Deployment Installation1Configuration of MiCollab2Menu: Service Link3Menu: Configuration3Menu: Security4Menu: Administration4Menu Application4Option: Users and Service4Option: MiCollab Client Service5Option: NuPoint Web Console5Option: NuPoint Web Console6Test Access to AWV and NuPoint8
Chapter:	2	Introduction9Brief Description of Mitel Performance Analytics9Supported Scenarios9
Chapter:	3	Prerequisites
Chapter:	4	Mitel Performance Analytics SNMP integration with MiVoice MX-ONE 12 How to integrate with MiVoice MX-ONE
Chapter:	5	Co-existence with Similar Tools
Chapter:	6	References
Chapter:	7	Introduction

	General
Chapter: 8	Integration Description
	Direct SID 15
	Direct SIP
	Direct SIP Signaling Overview
	MiVOICE MX-ONE Requirements
	Skype for Business Server 2019
	Main Components
	Licenses
Chapter: 9	Installation and Configuration
	Installation
	MiVoice MX-ONE Installation
	Microsoft Infrastructure 18
	Configuration
	Direct SIP Setup
	MiVoice MX-ONE Direct SIP Setup - TCP
	Skype for Business Server 2019 Configuration TCP
	Define PSTN Gateway in the Skype for Business Server 2019 Topology
	Builder
	Define a Dial Plan
	Define Voice Policy
	Define Trunk Configuration
	Conclusion 28
	Direct SIP with Security and Media Bypass Setup
	MiVoice MX-ONE Direct SIP with Security and Media Bypass Setup 28
	Import the Certificate to MX-ONE Service Node
	Lync Configuration with Security and Media Bypass Setup
	Define Dial Plan and Voice Policy
	Define Trunk Configuration
	Load Balancing and Failover Setup
	Load Balancing
	Failover
	DNS Setup
	MX-ONE Direct SIP with Load Balancing and Failover Setup - TCP 38
	Lync Configuration with Load Balancing and Failover Setup – TCP 39
	MX-ONE Direct SIP with Load Balancing and Failover Setup - TLS 39
	Import the Certificate to MX-ONE Service Node
	Lync Configuration with Load Balancing and Failover Setup – TLS 40
Chanter: 10	Integration Notes 40
Simpler 10	

Chapter:	11	References
Chapter:	12	Revision History
Chapter:	13	Introduction
Chapter:	14	Prerequisites
Chapter:	15	Setting up MX-ONE for GX Controller
		Number Analysis
		Extension Data
		Common Service Profile 9:
		Common Service Profile 11:
		Least Cost Routing Data
		Route Data
		ROCAP
		Route Category Data 47
		RODAP
		Route Data
		SIP ROUTE
Chanter:	16	Setting up the GX Gateway
chapter.	10	Logon
		Logon
		Hoct 40
		Local FileWalls
		Configuration 52
		Primary Rate Interface 60
		Interon 63
		Services 64
		POTS 65
		Config 65
		EVS Configuration 65
		Gateways
		Sarvars
		Registrations 60
		Authentication
		Interop

	Misc
	Media
	Codecs
	Call Router
	Route Config
	Management
	Backup/Restore
	File
Chapter: 17	Setting up MX-ONE for an EX Controller
Chapter: 18	Setting up EX Controller
	Logon
	Network Settings
	Host
	Interfaces
	Local Firewalls
	SBC
	Configuration
	Local_users_ca82
	ISDN
	Primary Rate Interface
	Interop
	Services
	POIS
	EVS Configuration
	Gateways 93
	Servers 94
	Registrations 95
	Authentication
	Transport
	Misc
	Media
	Codecs
	Call Router
	Route Config
	Management
	Backup/Restore
	File
Chapter: 19	Configure TLS on an EX/GX Controller
-	Prerequisites
	Creating TLS Certificate with SAN

		Connecting CA to the MX-ONE Server
		Verifying the CA File
		Generating the Unit Certificate with SAN
		Copying the Files on PC
		Configuring the EX/GX for TLS
		Login to the EX/GX Controller
		Installing Unit Certificates
		Configuring the Secure SIP ports
		Setting the TLS version. Cipher Suite, and Certificate Validation Level 108
		Enabling TLS on the SBC Service
		Enabling TLS between SIP Gateways and SBC 110
		Enabling SRTP on FX/GX Controller
		Enabling Certificate Validation 111
Chanter:	20	Known Limitations 111
chapter.	20	
Chantor	21	Introduction 112
Chapter.	21	
		Scope
Chapter:	22	Solution Description
		Mil/oico MX-ONE 114
		Mirror contraction Contracti
Chapter:	23	Requirements and Setup
		MIVOICE MX-ONE Requirements
		Microsoft Lync Server 2013 Requirements
		Integration Setup - TCP
		MiVoice MX-ONE Setup - TCP
		Microsoft Lync Server 2013 Setup – TCP
		Enable Lync Users for Remote Call Control
Chapter:	24	How to Verify the Setup
		Lvnc 2013 Client Features
		Make an Outgoing Call Using the Lync 2013 Client
		Answer an Incoming Call
		Transfer a Call Between Current Conversations (Monitored Transfer), 122
		Single Sten Transfer 124
		Forward an Incoming Call 126
		Place Calls on Hold 127
		Alternate Between Multiple Concurrent Calls 128
		Answer a Second Call While Already in a Call (call waiting) 128
		Dial Dual-Tone Multi-Frequency (DTME) Digits 120
		Dresence
		Tresence

Chapter: 25	Limitations
Chapter: 26	Good to Know
Chapter: 27	Revision History
Chapter: 28	General
Chapter: 29	Application Requirements
Chapter: 30	Installation Notes
	Licensing135Installing Release 11.0 on a Standalone Physical Server135Installing Release 11.0 in a VMware Environment135Firewall Configuration135MSL Configuration136MBG Configuration136Phone Configuration139Limitations139Known Issues140Upgrade Notes140Appendix - Config Script141

MiCollab Integration

This topic discusses the MiCollab integration with MX-ONE. For information on the MiCollab integration with MX-ONE see MiCollab Platform Integration Guide.

MiCollab Example Introduction

This document contains an example of basic installation and configuration of the MiCollab application server for integration with MiVoice MX-ONE.

Prerequisites

- Configure MX-ONE for MiCollab integration (see MX-ONE integration chapter in MiCollab Customer Documentation).
 - Configure PBX group and members in MX-ONE to be used for AWV.
 - Configure SIP trunk in MX-ONE using profile NuPoint (remember to use remote port=5058).
 - Configure csta link in MX-ONE.
- · Used numbers and IP address in the examples:
 - Attendant number in MX-ONE: 09
 - MX-ONE IP address: 192.168.222.100
 - Internal number serie:4xxxx
 - Internal number length: 5 digits
 - NuPoint: Access number: 6001
 - Lines to NuPoint VoiceMail: 15
 - Lines for NuPoint MWI: 1
 - Lines for outgoing calls from NuPoint: 4
 - AWV Access number: 8003
 - Number of ports AWV: 3
 - SIP Port Extension numbers for AWV: 8004,8005,8006

OVA Deployment Installation

Do as follows:

Deploy the MiCollab .ova file:

- 1. Start the virtual machine.
- 2. Open the console interface.
- 3. Choose keyboard.
- 4. Restore from backup no.

CHAPTER 1

- 5. Set Administrator's password (this is the same for both root and admin user).
- 6. Select Timezone (e.g. CET).
- 7. Enter primary domain (e.g. mydomian.com).
- 8. Enter system name (e.g. micollab).
- 9. Select only eth0 just now no WAN should be enabled.
- **10.** Type the IP address of the server.
- 11. Type the netmask.
- 12. Do not configure IPv6.
- 13. Do not configure eth1.
- 14. Do not configure another local network adapter.
- 15. Type the default gateway for the server.
- 16. Type the IP address of the corporate DNS .
- 17. Select the corporate DNS for DNS resolution.
- **18.** Wait for the configuration to be activated.
- 19. Enter ARID and IP address (Important use correct address) of the FMC and then select PBX type.
- 20. Login through the console interface as admin.
- 21. Select 9. Manage Trusted Networks.
- 22. Select 2. Add IPv4 trusted network.(e.g the internal corporate ip network segments).
- 23. Enter the subnetmask.
- 24. Enter the router to use for the trusted network normally the same router as for the server.
- 25. Select Next, then Back to the menu.
- 26. Login to https://<fqdn>/server-manager with admin and password configured during installation.

Configuration of MiCollab

In the main window and from the left menu you administrate the configuration of the MiCollab, see below.Complete all configurations before start using PM to deploy users.

Figure 1.1: Main window

Adde: Wite and Wates Concerning Adde: Wite and Wates Concerning Adde: Wite and Wates Concerning Machability Observiol Machability			adn
Ancess Unified Communications and Collaboration MCGlab Chee Deployment Bundle User License MCGlab Chee Deployments UCC Basic User for Enterprise (V4.0) 1 Total Applications UCC Basic User for Enterprise (V4.0) 1 Data Applications UCC Pennium Date for Enterprise (V4.0) 1 Use Instructions UCC Standed User for Enterprise (V4.0) 1 Value Statistics UCC Standed User for Enterprise (V4.0) 1 Value Statistics UCC Standed User for Enterprise (V4.0) 1 Value Statistics Applications (V4.0) 1 Statistics Applications (V4.0) 1 Statistics Application User License Statistics Application User License Statistics Audio, Web and Video Conferencing 1000 Statistics Nucleib Clent Censele 20 Statistics Statistics Statistics 20 Models Statistics Models Clent 20 20 Models Statistics Statistics 20 Models Statistics </th <th>services for which you (</th> <th>ned some services for which yo</th> <th>u are not</th>	services for which you (ned some services for which yo	u are not
Notifies	tion (UCC) Bundle	laboration (UCC) Bund	lles
Utaging Information UCC Dasic User for Enterprise (V4.0) 54 Ential Applications UCC Draw User for Enterprise (V4.0) 54 Status UCC Draw User for Enterprise (V4.0) 54 Status UCC Draw User for Enterprise (V4.0) 54 Status UCC Draw User for Enterprise (V4.0) 54 Web status UCC Draw User for Enterprise (V4.0) 54 Web status UCC Standard User for Enterprise (V4.0) 54 Web status UCC Standard User for Enterprise (V4.0) 54 Web status Status Status Status 55 Web status Vec Standard User for Enterprise (V4.0) 54 54 55 Status Status Status Status 55 <	enses Currently used	User Licenses Currently us	ed
circle.lk UCC Entry User for Enterprise (V4.0) 1 bindiary Station UCC Entry User for Enterprise (V4.0) 1 bindiary Station UCC Standard User for Enterprise (V4.0) 1 bindiary Station UCC Standard User for Enterprise (V4.0) 1 bindiary Station UCC Standard User for Enterprise (V4.0) 1 bindiary Station UCC Standard User for Enterprise (V4.0) 1 bindiary Station Application UCC Entry User Totals Veriag Bins Application User License System instruments Nupoint Unified Messaging 1000 System instruments Nupoint Unified Messaging 0 System instruments Nupoint Unified Messaging 0 System instruments Censols 200 System instruments Censols 200 System instruments Nupoint Unified Messaging 200 Notable Cleart Viser Totals 200 200 Notable Statis System <t< td=""><td>5000 0</td><td>5000</td><td>0</td></t<>	5000 0	5000	0
Intel Application IDEC Production Use of Prior (vis.0) IDEC Production User (vis.0) IDEC Production User (vis.0) IDEC Production User Prior (vis.0) IDEC Production User Pris (vis.0) IDEC Production User Pr	100	100	1
interest of the second	100	100	1
Interestation Interpret (vie.or) 1 Reckap Application User Totals Reckap Application User Totals Kenck log files Application User Totals Event vie.or Application User Totals System methodses Nupoint Unified Nessaging 30 System methodses Nupoint Unified Nessaging 30 Intraduction recentions Teleworker 45 Nicolab Cleent Censole 30 Intraduction Service Deskpheme 20 Nicolab Scient Program Meblie 20 Nicolab Scient Program Meblie 20 Nicolab Scient Program Meblie 20 Nicolab Scient Program Nocolab Scient Program 20 Nicolab Scient Program Nocolab Program 20 Nicolab Scient Program Nocolab Program 20 Nicolab Scient Program Nocolab Program 20 Nicolab Sc	140	100	
International Sector Application User Total Sector State Values Application User Total Sector Value Information Audio, Web and Video Conferencing 0.000 System reshing Resolution Officiation User Total Sector Resolution Officiation User Sector Resolution User Sector R	100	100	4
tion in final set of the set of t	s	r Totals	
hand stokeer hysise include hysise include hysise hysise include hysis	uses Currently used	Iser Licenses Currently use	d
Spatien miniguration Aution, wice and valeo Contenencing 1000 Spatem making Nupoint Unified Messaging 30 Spatem making Teleworker 45 Autobal Line Console 20 Autobal Line Console 20 Autobal Line Console 20 Michals Cline 20 30 Michals Cline 20 30 Michals Cline 20 30 Michals Cline 20 30 Michals Contenence 20 30	0000 0	10000	
ystam uses Ruppint Unified Messaging 20 hidds-in or recordigues fectorate (Records or recordigues) fectorate (Records or recordigues) 66 hidds-in or recordigues Micollab Client 62 62 hidds-in or recordigues Ceased 7 62 hidds-in or recordigues Ceased 7 62 hidds-in or recordigues Records or recordigues 6 62	2	10000	-
statu data Teleworker 45 Musican or reactigue Micollab Client 45 Hastadion Cassile 20 Stoppate Directory Service Deskphene 20 Collab Stoppa Mobile 20 Collab Stoppa Mobile 20 Collab Stoppa Softphone 20	302 5	302	5
Micellab Client Micellab Client figuration Console 20 Callab Client Insertion Deskphene 20 Callab Client Insertion Booling and the set of the	450 0	450	0
Generation representation calls binetary Service Calls binetary Serv			
inguration contexts tervice contexts of the set of the			
Deskphene Deskphene 26 Calla Citett Integration card Mobile 26 Calla Statiuty Softphone 26 Calla Statiuty Softphone 26 Calla Statiuty Softphone 26 Calla Statiuty Softphone 26 Softphone 26 Softphone 26 Softphone Milel Standard Linux 10.0.26 Softphone 26 Softphone CMA 7/M-0.25 Softphone 26 Softphone CP Softphone 26 Softphone CMA 7/M-0.25 Softphone 26 Softphone Softphone 26 Softphone 26 Softphone Calla Statiuty Softphone 26 Softphone 26 Softphone Calla Statiuty Softphone 26 Softphone 26 Softphone Calla Statiuty Softphone Softphone 26 Softphone 26 Softphone Softphone Softphone Softphone Softphone <td< td=""><td>0 0</td><td>0</td><td>0</td></td<>	0 0	0	0
Iteral Mobile 20 Colls Language Softphone 20 dps Settings Micellab 7.0.0.51 20 Mobile Mobile 20 Mobile	200 2	200	2
Collab Language Soliphone 20 dys Settings Micellab 7.0.0.51 20 chart and settings Wicellab 7.0.0.51 20 chart and settings Wicellab 7.0.0.51 20 collab Language © Micellabe 7.0.0.51 20 collab Language © Micellabe 7.0.0.51 20 collab Language © Micellabe 7.0.0.52 20 collab Language © Micellaberarise Componition 20 HCP standames and addresses 20 collaberarise Componition 20 20 homed Cards Soliphone 20 weise configuration 20 20 ablandure Certificate 20 20 de forward Certificate 20 20	200 2	200	2
Codes unguige Inclusion	200 2	200	2
McDibs 7.0.0.51 Working McDibs 7.0.0.51 Working Monitor Linex 10.0.36 mail sections mail sections MCP © Monitor Linex MCP sections MCP sections MCP sections MCP sections MCP sections MCP sections MCP sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP Sections MCP MCP MCP MCP MCP MCP MCP MCP			
Mail Standard Linux: 10.3.06 Mail Standard Linux: 10.3.06 Orgin Argan Orgin Argan Orgin Argan Mittel Mesuarks Comporation HCP ats and Time outrums and addwases outrums and addwases outrums and addwases beine/Det Tunnel hargen hargen hargen wrise configuration arrity wrise configuration arrity wrise configuration arrity arrite arces wrise configuration arrity arches			
CP Control Prince CP			
ICS te and Time addresses testine adjusted testine			
te and Time abrames and addeese barnine u6-in-Dive Tussel bir bir bir bir bir bir testa and testa addeese testa ad			
aburnes and addresses mains ScientDe4 Tunnel SD Semet Cards view configuration artigr mote scores ft forwarding à Genere Cardinate etilane Annapement etilaneous			
mains 6-1-cPU-R Tunnel pp wmet Cards fear.configuration withy note access f forwarding b Berver Cartificate Biorean Cartificate Biorean Sangarrent			
se-in-DV4 Tunnel 500 smatt Cards view configuration artify mode access at Sonver Cardinate discret Cardinate discret Cardinate cellaneOus			
top hemotic configuration unitive antive this forward contraction de donver contracte reflicute Management collaneous			
vervet Cards verve configuration artity motos access 4 forwarding 16 Jenver Cartificate effante Management effante Outs			
www.configuration writy wrote ecose writor wrote scores writors because wrote configuration wrote configurate wrotecase wrotec			
unity mote access f forwarding b Barver Cartificate tificate Management reliancous			
rity moto access forwarding i Barver Cettificate Richte Namporrent Rianeous			
Incle scolais t forwarding t forward t			
et Sonarding ab Server Cantificate diffester Management cellaneous			
ib Server Certificate tificise Management effancous			
reflexes Management cellaneous			
rellaneous			
LODAR and Townsing			
Artip			

Menu: Service Link

- Select Service Link and then Status.
- If you have not entered your ARID (Service account id) during the initial installation then enter it now together with the ip.address of the FMC.

NOTE: If you have not selected the PBX during the initial installation, go to ServiceLink/Install Applications/Install Applications - select the PBX type and Next.

Menu: Configuration

- Select and start the MiCollab Client Integration Wizard.
- Select MiCollab Language Settings and set the System Language and Other NuPoint UM Prompt.
- Select E-mail settings. If required, configure settings for outbound SMTP server and userid.

Menu: Security

 Select Remote Access. If required, change Secure Shell Settings to allow SSH access for later diagnostics.

Menu: Administration

• Select System Users. For the account micollab api. select Reset password and enter a new password. You will require this user account and password when configuring the MiCollab subsystem in PM.

Menu Application

Menu application options are discussed in this section.

Option: Users and Service

Select User and Services and then configure following options:

- Option: Network Element
 - a. Select Add.
 - **b.** Type =MiVoice MX-ONE
 - c. System Name= <my Mxone>
 - d. IP Address = 192.168.222.100
 - e. Call Forward Destination Number = 6001
- Option: User templates
 - Select Add.

Create customer roles templates from available default templates. It's done by selecting wanted default template, creating a copy of it and save with a new name. Edit the created customer templates for Entry, Premium, Standard and Standard - Mobile.

- Entry
 - Select TUI Passcode. TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more). TUI Passcode = Use this value = 4-10 digits (if extension length is less than 4 digits).
 - Attendant Extension: 09
 - Message Waiting #1 = DTMF to PBX
- Premium
 - Password = Use this value = "Strong Password"
 - Select TUI Passcode
 - TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more)
 - TUI Passcode = Use this value = 4-10 digits (if extension is less than 4 digits)
 - Attendant Extension: 09
 - Message Waiting #1 = DTMF to PBX
- Standard

- Password = Use this value = Enter a strong Password
- Select TUI Passcode
- TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more)
- TUI Passcode = Use this value = 4-10 digits (if extension is less than 4 digits)
- Attendant Extension: 09
- Message Waiting #1 = DTMF to PBX
- Standard Mobile
 - Password = Use this value = Enter a strong Password
 - Select TUI Passcode
 - TUI Passcode = Same as Primary Phone Extension (can only be used if extension length is 4 digits or more)
 - TUI Passcode = Use this value = 4-10 digits (if extension is less than 4 digits)
 - Attendant Extension: 09
 - Message Waiting #1 = DTMF to PBX

Option: MiCollab Client Service

Select MiCollab Client Services and then Configure MiCollab Client Services. Configure following options.

PBX Nodes.

- Select the PBX Node and configure.
- Set length: 5 (internal number length in the MiVoice MX-ONE).

Enterprise

- Select Enterprise and then Default Account Settings.
- Select appropriate Country from the drop-down list

Option: Audio, Web and Video Conferencing

Select Audi, WEB and VIDEO conferencing and configure following options.

Configure SIP Server

- Select Add and configure, MX-ONE SIP Server Configuration. Extension first: 8004 Extension last: 8006
- SIP password: 8003 (if authorization code is set to 8003 in MX-ONE for the extensions 8004-8006)
- SIP Domain: mydomain.com (domain of MX-ONE)
- IP Address: 192.168.222.100
- SIP Port: 5060

Web Conferencing Settings

- Select and configure Web Conference Name.
- · Web conferencing Name: micollab.mydomain.com

System Options

Select and configure System Options:

- Platform MiVoice MX-ONE
- Dial -in phone number 1: 8003 (Internal number to AVW)
- Dial in Phone Number 1 Label: internal
- Dial-in Phone number 2: 8468003 (corporate number to AWV)
- Dial- in Phone number 2 Label: corporate
- Dial -in number 3 +4684428003 (Public number to AWV)
- Dial- In Phone number 3 Label: Public
- Webserver admin E-mail system.admin@mydomain.com
- Generate Alert E-mail system admin@mydomain.com
- · Prompt for Access Code first: Enable checkbox
- Allow HD Video Resolutions: Enable checkbox
- Prompt to extend conference 5 minutes prior to its end time: Enable checkbox

Option: NuPoint Web Console

Select and NuPoint Web Console and configure following options

Offline Configuration

Select Offline configuration/Edit Offline configuration and Duplicate Active Configuration - yes

Then select and configure following items:

- 1. Network Elements/Add
 - a. Type = SIP GATEWAY
 - **b.** Name = Mxone
 - **c.** IP Address = 192.168.222.100
 - d. Number of Ports = 20
- 2. Dialers (Pagers) (for Request playback call feature in UCA client) and select:
 - a. Add a "dialer"
 - b. Number: Select Next Available
 - c. Enter a name Dialer
 - d. Acces code: T
 - e. Hold Time : 20
 - f. Add
- 3. Line Groups/Add
 - a. Add a line group for Voicemail connection:
 - Line Group Number = 1
 - Name = VoiceMail
 - Application = NuPoint Voice
 - User Interface = NuPoint Voice
 - Lines/Add
 - Line Triplet next Available

- Number of lines = 15
- PBX = MX-ONE
- Mapping = 1 (0 must not be used, see Online help "add at Line Group)
- "Save"
- Pilot Number = 6001
- Dialling Plan
- · Length of extensions starting with...
- 4 = 5 digits
- Voicemail
- System Attendent's extension = 09
- Save
- **b.** Add a line group for Message Waiting indication:
- Line Group Number = 2
- Name = MWI
- Application = DTMF to PBX Dialler
- User Interface = NuPoint Voice
- Lines/Add
- Line Triplet next Available
- Number of lines = 1
- PBX = MX-ONE
- Mapping = 16
- Add
- Pilot number = 6001
- DTMF to PBX Dialler/DTMF to PBX Dialer
- Pre-DN On Dial String = 1
- Pre-DN Off Dial String = 0
- Save
- c. Add a line group for Outgoing calls from NuPoint:
- Line Group Number = 3
- Name = Outgoing Dialler
- Application = Outbound (Pager) Dialer
- User Interface = NuPoint Voice
- Lines/Add
- Line Triplet next Available
- Number of lines = 4
- PBX = MX-ONE
- Mapping = 17
- Add
- Pilot number = 6001
- Save
- Dialling Plan
- Length of extensions starting with...

- 4 = 5 digits
- Select the Dialer(Pagers) created in step b) by selecting the checkbox
- Save
- 4. Select Commit Changes and Exit and then Activate.

Active Configuration/Line Groups

- Select Active Configuration/Line groups and then Edit line group for Voicemail (Linegroup 1)
- Check that Prompt Language 1 is set to default (Do not change this).

Class of service Feature COS/14. MAS

- · Select Class of Service/Feature COS and then Edit FCOS number 14 (MAS)
- Enable checkbox for:
 - 051 Do not switch language for outside callers
 - 218 Passcode NOT needed on direct calls
 - 263 Store Caller Line Id as a phone or mailbox number
 - 264 Play outside caller user interface (with FCOS bit 280)
 - 280 Enable CLI Outside caller interface (with FCOS bit 264)

Test Access to AWV and NuPoint

- Call Voice Mail (access number 6001). Get Welcome message.
- Call to AWV (access number 8003). Get prompt to enter conference code.

Mitel Performance Analytics SNMP integration with MiVoice MX-ONE

Introduction

Brief Description of Mitel Performance Analytics

The Mitel Performance Analytics (MPA 2.1, former MarWatch) monitoring system provides fault and performance management for multiple enterprise VoIP systems and associated network infrastructure, both LAN and WAN. MPA supports monitoring and remote access, both for private networks, such as enterprise LANs and MPLS VPNs, and for public network or Internet-reachable devices, such as access routers.

MPA can monitor any SNMP device regarding alarms and general status.

MPA is a product from Martello Technologies.

Supported Scenarios

For an MX-ONE system with a single Service Node, the MPA shall of course be connected to that Service Node.

The MPA can be connected in a couple of different ways to a multi-server MX-ONE system.

The primary multi-server scenario is that each Service Node server is connected to a MPA probe.

Figure 2.1: Primary scenario, direct connection to all MX-ONE servers in a 4-server MiVoice MX-ONE system



Another possibility is that one Service Node can act as a proxy for several other Service Nodes (and other entities), in which case only the proxy Service Node will be connected to the MPA probe.

The second scenario is not recommended, since it has certain resiliency problems, due to the fact that the monitoring function will be fully dependent on the proxy, so if the proxy goes down, the status of the other nodes will not be reported.

You can also have a mix of the primary and secondary scenarios.



Figure 2.2: Secondary scenario, connection by proxy, connection only to one MX-ONE Service Node

Prerequisites

MPA consists of a number of web services running on either a cloud-hosted computing platform or on-premises computing platform. There are several components to MPA. The remote 'Probe' installed in non-Internet accessible networks maintains databases of status and events, and provides a web portal with access security. Additionally, MPA has a Remote Access Service that provides a secure "cross-connect" for remote access to the customer network.

MPA 2.1 or later version shall be used.

The MiVoice MX-ONE system(s) shall be up and running on Linux (SLES), either on a cloud-hosted computing platform or on-premises computing platform. Appropriate MIB shall be active.

Mitel Performance Analytics SNMP integration with MiVoice MX-ONE

How to integrate with MiVoice MX-ONE

Do as follows:

- 1. As root open the file /etc/snmp/snmpd.conf.
- 2. Set the correct syslocation and syscontact to reflect where the server is located and who manages it.
- 3. Update the rocommunity setting to allow the Martello Marprobe to perform snmp-queries towards the MX-ONE.
- 4. Update the trapsink setting to point towards the Martello Marprobe. This should be done in all MX-ONE servers that the Martello MPA system should monitor.
- 5. After saving the changes you need to restart the snmpd daemon for the changes to take effect.

(The Martello MPA probe has been assigned IP-address 192.168.157.128. To limit the access the "rocommunity" setting can be set to only allow access from a certain subnet or even a single IP-address).

Useful information

- Please see /usr/share/doc/packages/net-snmp/EXAMPLE.conffor a more complete example and snmpd.conf(5).
- Writing is disabled by default for security reasons. If you would like to enable it, uncomment the rwcommunity line and change the community name to something nominally secure (keeping in mind that this is transmitted in clear text).

NOTE: do not use '< > in strings for syslocation or syscontact.

NOTE: If you define the following here you will not be able to change them with:

snmpset syslocation (Optional) Server Room on Floor 7.

syscontact Sysadmin (mxone-adminstrator@example.com).

They include all MIBs and can use considerable resources. See snmpd.conf(5) for information on setting up groups and limiting MIBs.

rocommunity public 127.0.0.1

rocommunity public 192.168.157.0/24

rwcommunity mysecret 127.0.0.1

MX-ONE alarm traps use the agentx protocol:

master agentx

AgentXSocket tcp:localhost:705

MX-ONE alarm traps can trigger snmptrapd to sent mail and textmessages rapcommunity:

Default trap sink community to use trapcommunity private

trap2sink: A SNMPv2c trap receiver

trap2sink 192.168.157.128

Co-existence with Similar Tools

There are other tools for fault and performance management, for example the Manager System Performance application, that can also be connected to the MiVoice MX-ONE system, as long as different IP addresses are used compared to MPAs.

However, there should be no need to have several such tools, so that is not recommended.

References

For further reading regarding MPA and its features and configuration options, please see MPA System Guide, Release 2.1 or later.

Integration of MiVoice MX-ONE and Skype for Business Server 2019, Quick Setup Guide

Introduction

The MiVoice MX-ONE communication system is based on an open software and hardware environment that uses standard servers with a Linux SUSE operating system. This open standards approach enables Mitel to offer our customers the choice of integrating MiVoice MX-ONE latest Microsoft UC products. We have worked with Microsoft to ensure that this possibility is workable.

MiVoice MX-ONE 5.0 is the first communications system (IP-PBX) to be fully Unified Communications Open Interoperability Program (UCOIP) qualified with Skype for Business Server 2019. The integration of MX-ONE with Microsoft products is a complete Direct SIP Integration, including security and media bypass, enabling customers to have both MX-ONE 5.0/6.x and Microsoft Lync 2019 co-exist in the same infrastructure and thereby derive the benefits from the best of both worlds. MX-ONE integrates with Microsoft UC solutions directly via a SIP connection to reduce the overall cost and complexity of the combined solution.

Refer to Microsoft's TechNet site for "Infrastructure Qualified for Microsoft Lync" for more information about the Microsoft Unified Communications Open Interoperability Program. http://technet.micro-soft.com/en-us/lync/gg131938

General

Integration of MiVoice MX-ONE with Skype for Business Server 2019 is supported as a complementary solution providing end-user services, such as instant messaging and conferencing.

Microsoft Partner Program has certified the integration between MX-ONE communications system running the MX-ONE Service Node software 5.0 SP4 and Skype for Business Server 2019 through a Direct SIP connection. Also, later versions of MX-ONE can be integrated with Skype for Business Server 2019.

Scope

This guide describes the basic integration between MiVoice MX-ONE and Skype for Business Server 2019. The following sections describe the solution integration that has been certified through the Microsoft Partner Program and covers only the Direct SIP Integration. For more information about how this integra-

tion is set up and functions, refer to the relevant CPI documentation for MX-ONE, or go to the Microsoft UC product websites.

We recommend that you check the latest products documentation.

Integration Description

The integration of MiVoice MX-ONE and Skype for Business Server 2019 described in this guide is achieved via a Direct SIP that is specified by Microsoft. It means that a SIP trunk is used to connect MX-ONE and Skype for Business Server 2019 (Mediation Server). The SIP trunk connection between the systems can be deployed with or without encryption. MX-ONE supports TLS for signaling and SRTP for media encryption when connected with Mediation Server.



This guide covers only the components that are required in the integration between MX-ONE 5.0 SP4 or a later version, and Skype for Business Server 2019 via Direct SIP to offer the functionality required by the Microsoft UC Open Interoperability Program for enterprise telephony services and infrastructure.

At least the following Skype for Business Server 2019 components are required to support this integration:

- Server Infrastructure
 - Microsoft infrastructure (Domain Controller, Active Directory, DNS and so on)
 - Skype for Business Server 2019 Standard or Enterprise Edition
 - Microsoft Mediation Server
- Client
 - Microsoft Lync 2019

Direct SIP

In Direct SIP Integration, referred to as Enterprise Voice by Microsoft Lync 2019, users will have dedicated phone numbers that differ from those used in the MX-ONE.



This enables the Microsoft Lync 2019 client to make and receive external calls through a PC. The calls are routed from the Skype for Business Server 2019 by the SIP trunk to the MX-ONE and further to the PSTN and vice-versa. MX-ONE and Skype for Business Server 2019 will behave as networked PBXs, as typically is the case with all external trunks in the MX-ONE.

Direct SIP Signaling Overview

MiVoice MX-ONE supports SIP/TCP or SIP/TLS as the SIP transport mechanism when connected with Mediation Server.

The MX-ONE ports used for such connections are:

- SIP/TCP: 5060
- SIP/TLS: 5061

In addition to this, MX-ONE also supports media encryption (SRTP) when connected with Microsoft Lync 2019 Server when TLS is used. The media encryption is done between MX-ONE media gateway unit (MGU) and Microsoft Mediation Server or between MX-ONE media gateway unit (MGU) and Microsoft Lync client when Media Bypass is configured in Microsoft Lync 2019 Server.

Direct SIP Supported Features

During the certification process, the following Microsoft Lync features were validated with MX-ONE Service Node software 5.0 SP4.

- Basic Call services between MX-ONE and Lync end-points over SIP trunks:
 - Anonymous user calls
 - Caller ID on both ends
 - Decline call
 - Call forwarding and simultaneously ring feature
 - Inbound and outbound calls
- Media bypass (also known as direct media between MX-ONE and Microsoft Lync clients). Encryption (TLS and SRTP) is required for this functionality.
 - Inbound call from MX-ONE user device to Microsoft Lync client
 - Outbound call from Microsoft Lync client to MX-ONE user device
 - Outbound call: Call Forward All (CFA) to another Microsoft Lync client

- Outbound call from Microsoft Lync to another Lync user; with bypass enabled and CFA enabled
- Outbound call: PBX CFB (Call Forward on Busy) to another Microsoft Lync user
- Outbound call from Microsoft Lync to another Lync user; with bypass enabled and CFB enabled
 Conference
- Failover (to secondary Mediation Server Lync gateway)
- Security (support for TLS/SRTP encryption)

Prerequisites

For proper integration between MiVoice MX-ONE and Skype for Business Server using Direct SIP, there are some prerequisites on both sides that must be fulfilled.

MiVOICE MX-ONE Requirements

On the MiVoice MX-ONE side, at least one MX-ONE Service Node and one Media Gateway are required to interwork with Skype for Business Server 2019.

Main Components

At least, the following MX-ONE components are required:

- MX-ONE communications system
 - MX-ONE Service Node
 - 5.0 SP4 or a later version
- Supported media gateways with the latest firmware compatible with 5.0 SP4, or a later version, which can be:
 - MX-ONE Classic 7U 19-inch chassis, MGU board, or
 - MX-ONE Lite 3U 19-inch chassis, using MGU board
 - MX-ONE Slim 1U 19-inch chassis, using MGU board
- Terminals
 - All current MX-ONE terminal types are supported with this integration: SIP, H.323, analog, digital, DECT, and mobile extension

Licenses

The MX-ONE licenses needed for this integration are:

- SIP trunk licenses-note that the quantity of licenses depend on how the system is deployed).
- Encryption licenses are required if encryption (TLS/SRTP) is used.

Always check with your Mitel partner that your system has the required licenses, before beginning the integration deployment.

Skype for Business Server 2019

A Microsoft environment needs to be in place in the customer site. Note that Microsoft Lync is not part of the MX-ONE offering. It is important that expertise of Microsoft-competent engineers are available for

installation and integration according to the MX-ONE configuration guidelines for the interface between the systems.

Main Components

The main Microsoft components that are required to interconnect with MiVoice MX-ONE are Skype for Business Server 2019, Mediation Server, and Lync clients. The Lync requirements are described in the Microsoft Lync Serve documentation. See the chapter References at the end of this guide. **NOTE:** In Mitel's lab validation, a single Skype for Business Server Standard Edition with a co-located Mediation Server was used. For testing load balancing and failover, two stand-alone Mediation

Servers were added to the topology.

Licenses

Microsoft licenses needed for this integration are described as they are beyond the scope of this guide.

Contact Microsoft or a qualified Microsoft partner to obtain the proper license requirements for each component of the Skype for Business Server solution.

Installation and Configuration

Installation

MiVoice MX-ONE Installation

Ensure that MX-ONE Service Node software 5.0 SP4 or a later version is installed in the customer environment. The system installation is not covered in this guide and must be performed by a qualified Mitel certified partner before the start of the integration work begins.

For Mitel MX-ONE installation, check the appropriate CPI documentation.

Microsoft Infrastructure

Ensure that Microsoft infrastructure and Skype for Business Server are installed in the customer environment by a qualified engineer.

For Microsoft infrastructure and Skype for Business Server requirements, check the appropriate Microsoft documentation.

Configuration

The following information was used in Mitel's laboratory setup during the validation of the solution. The setup may change depending of the customer specific needs.

NOTE: Fully Qualified Domain Name (FQDN) needs to be properly specified in the Domain Name System (DNS).

- MX-ONE 5.0 SP4 (or a later version)
 - Domain: lab.moon.galaxy Note that MX-ONE is part of a sub-domain
 - IP address: 192.168.222.10

FQDN: mx-one-lync.lab.moon.galaxy

- Microsoft Domain Controller, Active Directory, Certification Authority, and DNS Server
 - Domain: moon.galaxy
 - IP address: 192.168.222.2

FQDN: lync-infra.moon.galaxy

- Skype for Business Server Standard Edition and Mediation pool
 - Domain: moon.galaxy
 - IP address: 192.168.222.3

FQDN: lync-2019-se.moon.galaxy

NOTE: Mitel recommends that complex scenarios be validated in the partner labs before customer deployment.

Direct SIP Setup

A SIP trunk must be configured in MX-ONE and the access code for this route (a trunk towards Skype for business).

MX-ONE uses ports TCP 5060 and TLS 5061 to be interconnected with Skype for Business Server 2019. **NOTE:** MX-ONE 5.0 SP4 (or a later version) works with predefined SIP profiles for certain SIP service providers. if used, the profile file will help you in configuring the right data for the type selected. Each profile file may contain a number of profiles. The profile will preconfigure settings such as "-register", "-trusted", and so on according to the requirements of telephony provider.

MX-ONE 5.0 SP4 (or a later version) has predefined SIP trunk profiles to be used with Microsoft Lync 2019. One of the following trunk profiles needs to be selected during the MX-ONE SIP trunk configuration.

- Lync_TCP TCP is used as transport protocol; the listening port is 5068.
- Lync_TLS_SRTP. TCP is used as transport protocol; the listening port is 5067. SRTP is used to encrypt the media; it uses RTP/SAVP.

The following setup uses Lync_TCP where TCP is the transport protocol. In this case, the remote port is expected to be listening on port 5068.

To ensure a good interoperability between MiVoice MX-ONE and Skype for Business Server 2019, the SIP trunk profiles defined to Lync are "Forced Gateway", at this guarantees the same behavior for all types of calls passing through MX-ONE and towards Skype for Business Server 2019.

MiVoice MX-ONE Direct SIP Setup - TCP

The following figure shows the Direct SIP Configuration used in this guide.



The following setup needs to be done in MX-ONE for configuring Direct SIP. Note that only SIP Route definitions are shown.

1. Use the following command to view more details regarding the SIP Profile Lync_TCP:

sip_route -print -profile Lync_TCP

2. Define SIP Route category:

ROCAI:ROU=99,SEL=711000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=001100;

3. Define SIP Route data:

```
RODAI:ROU=99,TYPE=TL66,VARC=0000000,VARI=0000000,VARO=0000000;
```

4. Define SIP trunk data specific:

sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;

5. Verify your configuration:

sip_route -print -route 99 -short

6. Define the SIP Route equipment initiate; for example:

ROEQI:ROU=99,TRU=1-1&&1-30;

7. Define external destination SIP Route data:

```
RODDI:ROU=99,DEST=99,ADC=000500000000250000001010000,SRT=3;
```

Skype for Business Server 2019 Configuration -- TCP

To finalize the configuration between MX-ONE and Skype for Business Server 2019, do the following:

1. Enable TCP port for the Mediation pool (disabled by default).

-	Edit Properties	x
General Next hop PSTN gateway	General FQDN: * meds.moon.galaxy 	~
	Associations Associate Edge pool (for media components) • New Note: To view or change the federation route, use the site property page. Next hop selection Next hop pool: ajantaskype.mxonebglman.com VWSKYPE	=
	Mediation Server PSTN gateway ▲ Listening ports: * TLS: 5067 - 5068 - 5068 ✓ Enable TCP port The following trunks are associated with this Mediation Server. Click Make Default to mark a trunk as default. A default trunk is required only when your topology contains Office Communications Server 2007 R2. Image: Content of the server of th	~
Help	OK Cance	el

Define PSTN Gateway in the Skype for Business Server 2019 Topology Builder

- 1. Open Skype for Business Server 2019, Topology Builder, and define a PSTN gateway to be used between Lync and MX-ONE.
- 2. To define the PSTN gateway, expand Shared Components, right-click **PSTN gateways**option.

⊿		Shared Components		
	\triangleright	SQL Server stores		
	\triangleright	🚞 File stores		
	⊿	🚞 PSTN gateways		
		🐻 mxone-ne	New IP/PSTN Ga	ateway
		🐻 mxone.m	Topology	Define a new IP/PSTN gateway.
	⊿ 📮 Trunks			
		🥸 mxone-nc	Help	

3. Click New IP/PSTN Gateway. The dialog box opens the Gateway FQDN or IP Address. Specify the MX-ONE IP Address or FQDN and click Next.

-

	Define New IP/PSTN Gateway	X				
5	Define the PSTN Gateway FQDN					
Define th F <u>Q</u> DN: *	Define the fully qualified domain name (FQDN) for the PSTN gateway.					
mx-one	e-lync.lab.moon.galaxy					
Help	<u>B</u> ack <u>N</u> ext Cancel					

4. Define the IP address: in this example, the default is retained. Click **Next**.

Define New IP/PSTN Gateway	X
Define the IP address	
Enable IPv4	
Use all configured IP addresses.	
○ Limit service usage to selected IP addresses.	
PSTN <u>I</u> P address:	
O Enable IPv <u>6</u>	
<u>U</u> se all configured IP addresses.	
○ Limit service usage to selected IP addresses.	
PSTN <u>I</u> P address:	
Help Back Next Cance	el

- 5. Define the root trunk:
 - Trunk name: FQDN (MX-ONE FQDN)
 - Listening port for IP/PSTN gateway: 5060 (MX-ONE SIP TCP port)
 - SIP Transport Protocol: TCP
 - Associated Mediation Server: lync-2019-se.moon.galaxy
 - Associated Mediation Server port: 5068 (default)
- 6. Click Next.
- 7. Publish the Topology.

▲ PSTNL cateways		
-	New IP/PSTN Gateway	
5	Topology	New
⊿ 🛄 Tru	Help	Open
4) Inax	ne nouce.mxoncogman.com	Download Current Topology
	Meh Anns Servers	Save A Copy
Video gateways		Publish
SIP Vid	eo trunks	Insta Publish topology to the Central Management store.
🚞 Branch site	25	Remove Deployment

Define a Dial Plan

The **Dial Plan** configuration is required to allow Microsoft Lync users to dial to MX-ONE terminals and PSTN.

To define it, execute the following:

- 1. Open the Skype for Business Server Control Panel.
- 2. Click Voice Routing and choose Dial Plan.
- Define Normalization rules that fits your organization needs. A rule for Lync users to dial to MX- ONE terminals and another to dial to PSTN (ensure that MX-ONE is connected to PSTN) are required. If needed, contact Microsoft for the appropriate setup for your requirement.

	Skype for Business Server 2015 Control Panel	_ _ X
Osers	Create voice mution test care information	,
Topology	create voice routing text case information	
IM and Presence		
Persistent Chat	J OK X Cancel	
Voice Routing		
Voice Features	MXONE-10.211.62.15	
Response Groups	Description:	
Conferencing	MXONE-10.211.62.15	
Clients	Build a Normalization Rule	
Federation and	Fill in the fields that you want to use, or create the rule manually by clicking Edit.	
External Access	Starting digits:	
Monitoring and Archiving	4	
Security	Length:	
Natwork	Exactly 🔻 4	
Configuration	Digits to remove:	
	0	
	Digits to add:	
	Pattern to match: *	
	^(4\d(3))\$	
	Translation rule: *	
	\$1	
	Edit Reset	
		>

Figure 3.1: New Normalization Rule, five digits example

4. Commit the changes.

Define Voice Policy

A voice policy is required to enable Microsoft Lync users to dial out via the Direct SIP connection using MX-ONE. Lync client users need to be assigned for this policy.

To Create the Voice Policy, do the following:

- 1. Click Voice Routing and choose Voice Policy.
- 2. Click **New** and choose the type of policy that is applicable for your company setup, site policy or user policy.
- 3. Enter a Name and a Description for the voice policy.

	Skype for Business Server 2015 Control Panel	
IM and Presence Persistent Chat Voice Routing	Edit Voice Policy - Global	
Voice Features	Scope: Global Name: *	
Response Groups	Global	
Conferencing	Description:	
Clients	Global	
Federation and External Access	 ^ Calling Features ✓ Enable call forwarding ✓ Enable detection 	✓ Enable team call ✓ Enable PSTN reroute
and Archiving	Enable call transfer	Enable bandwidth policy override
Security	Enable call park	Enable malicious call tracing
Network Configuration	C Enable simultaneous ringing of phones	Enable busy options
	🔶 New 🔛 Select 🥖 Show details Remove 👚 🐣	
	PSTN usage record Associated routes	
	MXONE-10.211.62.15 towards-MXONE-10.211.62.15	
	MXONE-10.211.62.18 MXONE-10.211.62.18	
	Call forwarding and simultaneous ringing PSTN usages:	
	Route using the call PSTN usages	

- 4. Associate a new PSTN for the policy and click New.
- 5. Enter a Name and a Description for the New PSTN Usage Record

Skype for Business Server 2015 Control Panel		
Home	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING	
Topology	Create voice routing test case information	
IM and Presence Persistent Chat	Edit Voice Policy > New PSTN Usage Record	
Voice Routing		
Voice Features	Name:	
Response Groups	Associated Routes	
Conferencing	🗢 New 👫 Select_ 🖉 Show details_ Remove	
Clients	Name Pattern to match	
Federation and External Access		

- 6. Click New to associate a route with this PSTN usage record.
- 7. Enter a Name and a Description for the new Route.
- 8. Associate the MX-ONE gateway that you created earlier with the new **Route**. To do this, click **Add in Associated Gateways**.

	Skype for Business Server 201	5 Control Panel	>
IM and Presence Persistent Chat	Edit Voice Policy IP New PSTN Usage Record IP New Voi V New Your X Cancel	e Route	
Voice Routing	Scope:		
Voice Features	Name: *		
Response Groups	Route to MX-ONE		
Conferencing	Description:		
Clients			
Federation and	Build a Pattern to Match		
External Access	Add the starting digits that you want this route to handle, the expression manually by clicking Edit.	or create	
Monitoring	Starting digits for numbers that you want to allow:		
and Archiving	Type a valid number and then click Add.	Add	
Security		Frantian	
Network		(hearing and a line of the lin	
Configuration		Remove	
	Match this nattern: *		
	Edit Reset		
	Suppress caller ID		
	Alternate caller ID:		

- 9. In Select Gateway, select the MX-ONE gateway created previously.
- 10. Click **OK** for all the queries to retain the configurations made.
- **11.** Commit all changes.

elect Trunk		0	23
	Q		
Service	Site		
PstnGateway:mxone-node2.mxonebglman.com	VWSKYPE		
PstnGateway:mxone.mxonebglman.com	VWSKYPE		
	OK	Cancel	

Define Trunk Configuration

To assign the MX-ONE gateway to a site or pool trunk, follow these steps:

- 1. Click Voice Routing and then click Trunk Configuration.
- 2. Click **New** and choose the type of trunk that is applicable for your company setup, site trunk, or pool trunk.

	Skype for Business Server 2015 Control Panel	
Skype for Business	: Server	Administrator Sign out 6.0.9319.259 Privacy statement
Home Users Topology IM and Presence Persistent Chat	DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING Create voice routing test case information Edit Trunk Configuration - Global	×
Voice Routing Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network Configuration	Scope: Global Name: Global Description: Global Maximum early dialogs supported: 20 Encryption support level: Required Refer support: Enable sending refer to the gateway Centralized media processing Enable forward cal history Enable forward or Absorder timer Associated PSTN Usages Select. Remove Select. S	

3. Select the Encryption support level. In this case, it is Not supported.

Encryption support level:		
Not supported	•	
Required		
Optional		
Not supported		

4. Commit all changes to complete the setup.

Conclusion

Now the setup is complete, assign users to the Policy created previously and test the integration by making calls between the systems.

See the topic Enable users for Enterprise Voice in Skype for business Server at the following link: http://technet.microsoft.com/en-us/library/gg413011.aspx

Direct SIP with Security and Media Bypass Setup

The following figure shows the Direct SIP with security and Media Bypass configuration used in this guide.



MiVoice MX-ONE Direct SIP with Security and Media Bypass Setup

The following setup needs to be done in MX-ONE in order to configure Direct SIP with security (encryption). Note that only Route definitions are shown.

NOTE: MX-ONE FQDN needs to be properly defined in the DNS Server.

When using security, the appropriate certificate must be installed in MX-ONE in addition to the encryption licenses. Check Certificate Management on MX-ONE CPI documentation for more details regarding certificates.

NOTE: TLS/SRTP security is required for Media bypass functionality. It means that the proper encryptions licenses must be loaded in the MX-ONE system.

- 1. Use the following command to view more details regarding the SIP Profile Lync_TLS_SRTP: sip_route -print -profile Lync_TLS_SRTP
- 2. Define SIP Route category:

```
ROCAI:ROU=98,SEL=711000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=001100;
```

3. Define SIP Route data:

RODA I:ROU=98,TYPE=TL66,VARC=0000000,VARI=00000000, VARO=00000000;
4. Define SIP trunk data specific:

sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;

5. Verify your configuration:

sip_route -print -route 98 -short

- 6. Define the SIP Route equipment initiate: ROEQI:ROU=98,TRU=1-1;
- 7. Define external destination SIP Route data:

RODDI:ROU=98,DEST=98,ADC=000500000000250000001010000,SRT=3;

Import the Certificate to MX-ONE Service Node

Import the server certificate mx-one-certificate.pfx to MX-ONE Service Node.

- 1. Install the certificate in the MX-ONE Service Node 1.
- 2. Run the mxone_certificate as root and press Enter button. The following screen appears.

MX-ONE Maintenance Utility
If an enterprise CA or standalone root CA is to be used select 'certificate' to create the CSR and import later the signed certificate. Use also this option if TLS networking shall be used and a CSR shall be signed on another MX-ONE server.
If neither an enterprise CA nor standalone root CA is to be used select 'auto' or 'root' plus 'server' to create needed certificates.
The auto option will create and install a certificate with default settings and activate TLS in all servers in the MX-ONE system.
Choose option for certificate. (-) certificate root Manage Certificate root Manage Root Certificate server Manage Server Certificate mxone-tls Manage TLS in MX-ONE mxone-secLevel Manage Security level in MX-ONE
100%
< <mark>0</mark> K > < Help > < Exit >

3. Select certificate and click OK. The following screen appears.



4. Select import and click OK. The following screen appears.

MX-ONE Maintenance Utility Import of signed certificate. The CA can issue a certificate in different formats, e.g. x509 PEM, PKCS#7 or PKCS#12. There can be one or more files received from the CA. When importing a PKCS#12 file the password must be stored in a file named password.txt in the same directory as the PKCS#12 file. A PKCS#12 file contains the private key, server certificate, intermediate CA and root CA. For other formats than PKCS#12, the password file and private key file created at CSR creation will be used (both files are expected to be in a sub-directory under /etc/opt/eri sn/certs/pending) unless the private key exists in the file to be imported. A PKCS#7 file is expected to contain certificate, intermediate CA and root CA in that order. If a x509 PEM file contains several certificates, this tool expects the order to be certificate, intermediate CA and root CA. This tool expects the intermediate CA and root CA to be in the same file (i.e. the server certificate can be in a separate file). A x509 PEM file might contain the private key as well. < <mark>0</mark>K >

5. Click **OK**. The following screen appears to select a file or directory where the signed certificate is stored.

Directories	Files	
lagagagagagagagagagagagagagagagagagagag		
	adadadadadadada Tagagggggggggggggggggggg	44444444444
n <mark>e</mark> X	x lesshst	
v cassandra	y mdsh history	
x dbus	x rnd	
X (DUD)	x vininfo	
x kbd	x7.0 Subbankar D LAB CPE Ver2 x 2-1 lic	
x ssh	xcall ncan	
whin	vsin route	
vinst-svs	x	
A number of a	,	
x	, x	
×	x	
x	, x	
x	x	
x	X	
x	x	
x	×	
x	X	
x	x	
x	x	
magaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa		
100000000000000000000000000000000000000	aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	pepepepee
x/root/		
magaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa		
	OK > <cancel></cancel>	

6. Specify the path where the **forMXONE.pfx** certificate is stored as shown in the following screen.

Directories	Files
199999999999999999999999999999999999999	
X.	x.rnd
x	x.s.PGSQL.5432
x.ICE-unix	x.s.PGSQL.5432.lock
x.Test-unix	xartemisJLHandler 35b2s4
x.X11-unix	xxartemisJLHandler 4UIAMF
x.XIM-unix	xartemisJLHandler V6OKFK
x.com ibm tools attach	xartemisJLHandler XhjYL4
x.font-unix	xartemisJLHandler nnv74j
xSLES12SP3 updates 20181126	xartemisJLHandler sToC50
xYaST2-03472-NikCs6	xaxis2-tmp-1696558935556050315.tmp.lck
xaxis2-tmp-1696558935556050315.tmp	xaxis2-tmp-1966729109227965252.tmp.lck
xaxis2-tmp-1966729189227965252.tmp	xaxis2-tmp-863070690944369777.tmp.lck
xaxis2-tmp-863070690944369777.tmp	xerimca trace startup.conf
x <mark>hsperfdata mxone db d</mark>	xerioma trace startup.conf
xhsperfdata_root	xerisupv_trace_startup.conf
xjna89375289	xx for MXONE.pfx
xmxone	xliblz4-java5532951713714107759.so
xss19804	xliblz4-java7618868143503649692.so
xsystemd-private-28c36a71dfee4b84b08d37f335a324f6-ntpd	.se xliblz4-java7914401218714933630.so
xsystemd-private-449d37501b0f41a49c1876ac809acb79-ntpd	.se xliblz4-java997645639968539253.so
maaaaaa gaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	1qqjmqqqqqq 👘 qqqqqqqqqqqqqqqqqqqqqqqqqqqqq
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq	400000000000000000000000000000000000000
m qaqaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa	
เดสสนสสนสสสสสสนสสนสสนสสนสสนสสนสสนสสนสสนสส	184864444444444444444444444444444444444
	<cancel></cancel>

7. Click **OK** to store the imported certificate. Next, you install the certificate that you have imported and click **OK**.

M	X-ONE Maintenance Utility
Choose option for c	ertificate
	Currents (CCP) (Countificates (Cirminal Democrat)
request	Create CSR (Certificate Signing Request)
c onfig-to-csr	Create CSR from configuration file
import	Import Signed Certificate
install	Install Imported Certificate
uninstall	Uninstall Certificate
	View Installed Contificate(s) Summany
Summary	view installed certificate(s) Summary
v iew-installed	View Installed Certificate
v iew-imported	View Imported Certificate
view	View Certificate
< <mark>O</mark> K	> < Help > < Back >



- Enable the TLS in MX-ONE > Manage TLS in MX-ONE -> Configure MX-ONE to use TLS. Refer to the 132/154 31-ANF 901 14 document for more detail.
- 9. Enable Media Encryption in the route:

media_encryption_enable -type route media_encryption_enable -type extension media_encryption_enable -type intermgw media_encryption_print

Lync Configuration with Security and Media Bypass Setup

You must do the following to finalize the configuration between Mitel MX-ONE and Skype for Business Server 2019 the following needs to be done:

Define PSTN Gateway in the Skype for Business Server 2019 Topology Builder

1. Open the Skype for Business Server 2019, Topology Builder, and define a PSTN gateway be used between Lync and MX-ONE.



- 2. To define the PSTN gateway, expand Shared Components and right-click the PSTN gateway.
- 3. Click New IP/PSTN Gateway. The Define the PSTN Gateway FQDN dialog box appears.

6	Define New IP/PSTN Gateway	×
5	Define the PSTN Gateway FQDN	
Define th F <u>Q</u> DN: *	he fully qualified domain name (FQDN) for the PSTN gateway.	
mx-one	e-lync.lab.moon.galaxy	
Help	<u>B</u> ack <u>N</u> ext Cancel	

- 4. Enter the FQDN or the IP address: specify the MX-ONE IP Address or FQDN and click Next.
- 5. Define the IP address: in this example, the default is retained. Click Next.

4	Define New IP/PSTN Gateway	X
5	Define the IP address	
© Ena © ○	ble IPv4 Use all configured IP addresses. Limit service usage to selected IP addresses. PSTN IP address:	
) Ena () ()	ble IPv <u>6</u> Use all configured IP addresses. Limit service usage to selected IP addresses. PSTN IP address:	
Hel	<u>B</u> ack <u>N</u> ext Cancel	

6. Define the root trunk:

- Trunk name: FQDN (MX-ONE FQDN)
- Listening port for IP/PSTN gateway: 5061 (MX-ONE SIP TCP port)
- SIP Transport Protocol: TCP
- Associated Mediation Server: lync-2019-se.moon.galaxy
- Associated Mediation Server port: 5067 (default)
- 7. Click Next.

Define New IP/PSTN Gateway	X
Define the root trunk	
Irunk name: *	
mx-one-lync.lab.moon.galaxy	
Listening port for IP/PSTN gateway: *	
5067	
SIP Transport Protocol:	
TLS	•
Associated Mediation Server:	
ajantaskype.mxonebgIman.com VWSKYPE	-
Associated Mediation Server port: *	
5067	
Help <u>B</u> ack <u>F</u> inish Cance	el

8. Publish the **Topology**

	nateways	
	New IP/PSTN Gateway	
	Topology •	New
⊿ 🛄 Tru	Help	Open
		Download Current Topology
	Web Apps Servers	Save A Copy
Video	gateways	Publish
SIP Vid	deo trunks	Insta Publish topology to the Central Management store.
🚞 Branch sit	es	Remove Deployment

Define Dial Plan and Voice Policy

Define the Dial Plan and the Voice Policy as explained previously in this section.

Define Trunk Configuration

To assign the MX-ONE gateway to a site or a pool trunk, and follow these steps:

- 1. Click Voice Routing, and then click Trunk Configuration.
- 2. Click **New** and choose the type of trunk that is applicable for your company setup, site trunk, or pool trunk.
- 3. Select Enable media bypass.

N	Skype for Business Server 2015 Control Panel	
Topology	Create voice routing test case information	^
IM and Presence		
Persistent Chat	Edit Dial Plan Edit Normalization Rule - MXONE-10.211.62.15	
Voice Routing	Manage Cancel	
Voice Features	MXONE-10.211.62.15	
Response Groups	Description:	
Conferencing	MXONE-10.211.62.15	
Clients	Build a Normalization Rule	
Federation and External Access	Fill in the fields that you want to use, or create the rule manually by clicking Edit.	
Monitoring and Archiving	Starting digits:	
Security	Length:	
Network	Exactly • 4	
Configuration	Digits to remove:	
	Digits to add:	
	Translation rule: *	
	\$1	
	Edit Reset 🥐	× .
		>

4. Keep the default Encryption support level, which in this case is **Required**.

Now that the setup is concluded, assign users with the policy created previously and test the integration making calls between the systems.

Load Balancing and Failover Setup

Load Balancing

Mitel MX-ONE 5.0 and later versions support load balancing setup when connected with more than one Mediation Server. In such scenario, the Microsoft DNS Load Balancing functionality can be used.

MX-ONE 5.0 and later versions support DNS SRV and multiple A-record query where a list with multiple entries can be used. When properly configured, MX-ONE will attempt to send an INVITE to the entries in the list until the call is successful. No answer or 503 Service Unavailable from one entry will trigger MX-ONE to try the next entry.

For more details, see MX-ONE SIP Route command description in CPI or sip_route –help, parameter remote port.

Failover

The failover feature also uses the Microsoft DNS Load Balancing functionality. When integrating MX-ONE and Mediation Server, the same configuration is valid for both failover and load balancing.

In a scenario, where two Mediation servers are used and if one of the servers is unavailable, then the first call will be attempted to set up to the first server, but it will be redirected after a few seconds and answered; and all subsequent calls will be redirected and answered in the second Mediation Server.

The reason it takes some seconds before getting an answer from the second server, is that after the INVITE is sent to the first server, the system waits four seconds for an answer, and if no answer is received, the host is grey-listed for 32 seconds and an INVITE is sent to the second server after this.

For additional details, see the MX-ONE SIP Route command description in CPI or sip_route – help, parameter remote port.

The following is a description of the setup that was verified in Mitel's lab.



For this scenario, two standalone Mediation servers are used. In the MX-ONE side, only one MX-ONE Service Node is used, and it is configured with the Mediation Pool entry.

DNS Setup

Microsoft DNS needs to be configured to support Round Robin as described in the TechNet article "Configure DNS for Load Balancing". Follow the link and see the item "To enable round robin for Windows Server".

http://technet.microsoft.com/en-us/library/gg398251.aspx

The following figure shows the setup when Round Robin option is enabled.

LINC 2013-101 P	roperties				? >
Debug Logging Interfaces	Event Logging Forwarders	I Trus	t Anchors Advanced	Monito	ring Security Root Hints
Server version n	umber:				
Server options:)))				
Disable recur	sion (also disable laries	es forwar	ders)		
□Fail on load if ▼Enable round	bad zone data robin				
✓Enable netma ✓Secure cach	ask ordering e against pollutio	n			
Name checking:		Multiby	ite (UTF8)		•
Load zone data	on startup:	From A	ctive Direct	ory and	registry 💌
Enable autor	matic scavenginj	g of stale	records		
Scavenging	period:	0	C	lays	7
				<u>R</u> esel	t to Default
	ОК	Cancel	AP	ply	Help

DNS Multiple A record setup - Mediation Servers

To set up DNS Host (A) records for the two Mediation servers, the following must be configured. In the DNS Manager Tool, create the entries as shown in the following table.

NOTE: For more information about creating the DNS Host A records, refer to http://technet.micro-soft.com/en-us/library/gg398593.

FQDN	ТҮРЕ	IP ADDRESS
med.moon.galaxy	Host (A)	192.168.222.7
med.moon.galaxy	Host (A)	192.168.222.8

To test your configuration, use the command ping to check the setup.

📾 Administrator: C:\Windows\system32\cmd.exe	_ 🗆 >
C:\Users\Administrator.AAS>ping meds	-
Pinging meds. Reply from .7: bytes=32 time=35ms TIL=128 Reply from .7: bytes=32 time=21ms TIL=128 Reply from .7: bytes=32 time(ins TIL=128 Reply from .7: bytes=32 time(ins TIL=128 Reply from .7: bytes=32 time(ins TIL=128	
Ping statistics for the second of the second secon	
C:\Users\Administrator.AAS>ping meds	
Pinging meds 81 with 32 bytes of data: Reply from .8: bytes=32 time=Ims TTL=128	
Ping statistics for the second second .8: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms	
C:\Users\Administrator.AAS>ping meds	
Pinging meds. Reply from .8: bytes=32 time=1ns TIL=128 Reply from .8: bytes=32 time=1ns TIL=128 Reply from .8: bytes=32 time=1ns TIL=128 Reply from .8: bytes=32 time=1ns TIL=128	
Ping statistics for the second 1 .8: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approxinate round trip times in milli-seconds: Minimum = 1ms, Maximum = 1ms, Average = 1ms	
C:\Users\Administrator.AAS>ping meds	
Pinging meds	
Ping statistics for the second of the second of the second of the second of the second secon	
C:\Users\Administrator.AAS>	

MX-ONE Direct SIP with Load Balancing and Failover Setup - TCP

The following setup needs to be done in MX-ONE for configuring Direct SIP with load balancing and failover setup. Note that only Route definitions are shown.

NOTE: MX-ONE FQDN needs to be properly defined in the DNS Server.

- 1. Use the following command to view more details regarding the Profile Lync_TCP: sip route -print -profile Lync TCP
- 2. Define SIP Route category:

RO-

CAI:ROU=97,SEL=711000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4,SERV=3100 0000 01,BCAP=00110;

3. Define SIP Route data:

RODAI:ROU=97,TYPE=TL66,VARC=0000000,VARI=00000000, VARO=00000000;

4. Define SIP trunk data specific:

sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;

5. Verify the configuration:

sip_route -print -route 97 -short

6. Define the SIP Route equipment initiate:

ROEQI:ROU=97,TRU=1-1;

7. Define external destination SIP Route data:

RODDI:ROU=97,DEST=97,ADC=000500000000250000001010000,SRT=3;

Lync Configuration with Load Balancing and Failover Setup – TCP

Define a Mediation poll in the Skype for Business Server 2019 Topology Builder.

In the test validation, a Mediation poll named meds.moon.galaxy was created with two standalone Mediation servers.

Mediation Pool FQDN=meds.moon.galaxy Mediation Server 1 FQDN= med-1.moon.galaxy Mediation Server 2 FQDN= med-2.moon.galaxy

KLync Server 2013, Topology Builder			
<u>File Action H</u> elp			
Lync Server RND_Site1	General		•
Lync Server 2010 Lync Server 2013 De Lync Server 2013 De Candard Edition Front End Servers De Settember 26 Han Servers	FQDN:	meds.moon.galaxy	
Director pools	Associations		
🖃 🧰 Mediation pools	Edge pool (for media):	Not associated	
ag lync-2013-se1. ag lync-2013-se2. □ Fr meds.mon.galaxy	Note: To view the federation	n route, use the site property page.	
med2.moon.galaxy	Next hop selection		<u> </u>
□ Persistent Chat pools □ Edge pools □ Trusted application servers □ □ Shared Components	Next hop pool:	lync-2013-se2.: (RND_Sit	<u>e1)</u>
	Mediation Server PSTN gat	eway	<u> </u>
	TLS listening port:	5067 - 5067 5068 - 5068	
Branch sites	Trunke:	5000 - 5000	[]
	Hunka.	Default Trunk	Gateway Site
	•		

To set up the PSTN gateways, refer the Skype for Business Server 2019 configuration - TCP.

Execute calls between MX-ONE and Microsoft Lync and check that the calls are distributed between the systems.

MX-ONE Direct SIP with Load Balancing and Failover Setup - TLS

The following setup needs to be done in MX-ONE in order to configure Direct SIP with load balancing and failover setup, please note that only Route definitions are showed.

NOTE: MX-ONE FQDN needs to be properly defined in the DNS Server.

- 1. Use the following command to check more details regarding SIP Profile Lync_TLS sip_route -print -profile Lync_TLS
- 2. Define SIP Route category:

```
ROCAI:ROU=96,SEL=711000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=00110;
```

3. Define SIP Route data:

RODAI: ROU=96,TYPE=TL66,VARC=0000000,VARI=00000000, VARO=00000000;

4. Define SIP trunk data specific:

sip_route -set -route 1 -profile Lync_TLS_SRTP -uristring0 "sip:+?@skype.skypebusiness.com" -remoteport 5067 -accept REMOTE_IP -match "mxoneskype.skypebusiness.com,10.211.62.165,skype.skypebusiness.com,10.211.62.175" -codecs PCMA,PCMU -protocol tls -service PRIVATE;

5. Verify your configuration:

sip_route -print -route 96 -short

6. Define the SIP Route equipment initiate:

ROEQI:ROU=96,TRU=1-1;

7. Define external destination SIP Route data:

RODDI: ROU=96,DEST=96,ADC=000500000000250000001010000,SRT=3;

Import the Certificate to MX-ONE Service Node

Import the server certificate mx-one-certificate.pfx to MX-ONE Service Node. On the access Server, for example, MX-ONE Service Node 1 runs the following command:

- 1. Install the certificate in the MX-ONE Service Node 1: mxone_certificate, and select the certificate mx-one-certificate.pfx
- 2. Enable Media Encryption in the route: media_encryption_enable -type route

Lync Configuration with Load Balancing and Failover Setup – TLS

Define a Mediation poll in the Skype for Business Server 2019 Topology Builder.

In the test validation, a Mediation poll named meds.moon.galaxy was created with two standalone Mediation servers.

Mediation Pool FQDN=meds.moon.galaxy Mediation Server 1 FQDN= med-1.moon.galaxy Mediation Server 2 FQDN= med-2.moon.galaxy

To set up the PSTN gateways, refer the Lync configuration with security and Media Bypass setup section.

Execute calls between MX-ONE and Microsoft Lync and check that the calls are distributed between the systems.

Integration Notes

The latest software and firmware versions of MX-ONE components must be used.

NOTE: Mitel recommends that complex scenarios shall be validated in the partner labs before to customer deployment.

References

Always check the latest documentation. The links below are the ones available for reference. Mitel CPI Documentation – Mitel MX-ONE 5.0 SP4 or a later version.

Skype for Business Server Deploying Enterprise Voice

Enable Users for Enterprise Voice

Revision History

DOCUMENT VERSION	COMMENTT	DATE
А	First release	2015-11-19
В	Minor corrections	2014-03-28
С	Updated with Mitel template	2015-06-08
D	Updated in 4.2.3.7, cert_install_local replaced by mxone_certificate. MX-ONE version information also corrected.	2015-10-27
D3	Spelling correction	2017-04-05
D4	2013 old screens replaced with 2015 screens	2019-04-24
D5	Server 2015 is changed to server 2019	2019-09-10

Installation and Configuration Guide for GX and EX Controller

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 4.1: EX and GX Controller Gateways

NOTE: The EX gateway can only be used as a stand-alone system.

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 7.2.
- The firmware level of the EX-Controller and GX-Gateway shall be at least DGW 44.2.1669.

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 / GX-Gateway.

Setting up MX-ONE for GX Controller

Number Analysis

Number Analysis Data

Type of Series	Number Series
Extension Number Series	10000 - 31999 33200 - 49999 67000 - 67999
External Destination Code	068 081 – 088 321 331 81 - 88
LCR Access Code	00

Call Discrimination Data

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

Extension Data

Figure 4.2: Directory Number Profile

Dir Party	Cust Csta	Lin Fr	i Ca	sp Featu On H	ure lotli	Lan ne	ig Max Hotline	Secretar Num Bao	y Max ckup No	Security um	AMC Area	Vide	o BluStar	Third
Client	Supr		Seco	level nd Line			Cost	t:	⊺em	Exception	n Code		Client Mod	SIP
11101 00	0	1	9	-		-	121	No 08101344	1 431110	Yes 1 013	No	No	а.	No
11102 00	0 1	1	9	-		•	-	No 08101344	1 43 1 110	Yes 2 013	No	No		No
11103 00	0 0	1	9	-		•	-	No 08101344	1 431110	Yes 3 013	No	No	-	No
11104 00	0 0	1	9	-	-	•	•	No -	1.	Yes	No	No	70	No
11105 00	0 0	1	9	-		•		No 08101344	4 431110	Yes 5 013	No	No	•	No
11106 00	0 0	1	9	-		-	-	No 0810 1 344	4 4 311 10	Yes 6 013	No	No	•	No
22101 00	0	1	9	_		·	-	No 08203132	4 252211	Yes 01 031	No	No	•	No
22102 00	0 0	1	9	_		•		No 0820313	4 252211	Yes 02 031	No	No		No
22103 00	0 0	1	9	_		•	-	No 0820313	4 252211	Yes 03 031	No	No		No
22104 00	0 0	1	9			-		No 0820313	4 252211	Yes 04 031	No	No	-	Na
22105 00	0	1	9			-		No 0820313	4 252211	Yes 05 031	No	No		No
22106 00	0 0	1	9	-		-		No 0820313	4 252211	Yes 06 031	No	No		No
67820 00	0 1	1	11			•		Na -	4	Yes	No	No		Na
67821 00	0 0	1	9			2		No -	4	Yes	No	No	÷	No
67822 00	0	1	9			5	2	No	1	Yes	No	No	ē.	Na

MDSH>

Common Service Profile 9:

Cust: 0 Traf : 0103151515 Serv: 1111000110000000000000000000 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: 11113001100100000000100000300 Cdiv: 111000111010000 Roc: 000001 Npres: 0011000 Offered Time: 0 Forced DisconnectTime: 0 CnnLog: 0 Csp Name: Intrusion

Least Cost Routing Data

Least Cost Destination Data

 Table 4.1: External Number Table

Entry	TRC	PRE	Conf
00013443111	8		Ν
00031325	8		Ν
00040598	8		Ν
00084226	7		Ν
000856867	7		Ν

END

Least Cost Destination Data

 Table 4.2: Number Length Table (Sheet 1 of 2)

Entry	TRC	PRE	CONF	MIN	MAX	ACF
001	0		Ν	6	18	Υ
002	0		Ν	6	18	Υ
003	0		Ν	6	18	Y
004	0		Ν	6	18	Y
005	0		Ν	6	18	Y
006	0		Ν	6	18	Y

Table 4.2: Number Length Table (Continued) (Sheet 2 of 2)

Entry	TRC	PRE	CONF	MIN	МАХ	ACF
007	0		Ν	6	18	Y
008	0		Ν	6	18	Y
009	0		Ν	6	18	Y

Least Cost Destination Data

Table 4.3: Number Table

Entry	TRC	PRE	ACCT	FRCT	TOLL	CBCS	BTON	TNS	OSA
	5		0	1	1111111 1111111 1		0		
	5		0	2	1111111 1111111 1		0		
	5		0	3	1111111 1111111 1		0		
	4		0	4	1111111 1111111 1		0		

END

Least Cost Destination Data

Table 4.4: Fictitious Destination Table

FRCT	TZONE	PRE
1	1	081
2	1	083
3	1	085
4	1	088

END

Route Data

ROCAP

Route Category Data

	Figure 4.3: Route Category Data										
ROU BCAP	CUST SEL	TRM	SERV	NODG	DIST	DISL	TRAF	SIG			
81 001100	7110000000000010	4	31000000	1 0	30	128	03151515	0111110000A0			
83 001100	7110000000000010	4	31000000	01 0	30	128	03151515	0111110000A0			
211 001100	711000000000000000000000000000000000000	4	310000000	01 0	30	128	03151515	0111110000A1			

RODAP

Route Data

Table 4.5: Route Data

ROU	Туре	VARC	VARI		VARO	Filter
81	TL66	H'00000000	H'0000000 0	H'00000000	NO	
83	TL66	H'00000000	H'0000000 0	H'00000000	NO	
211	TL66	H'00000000	H'0000000 0	H'00000000	NO	

SIP ROUTE

One SIP route to each branch node is specified.

Route 81 towards BO#1 (Linköping) route : 81 protocol = tcp profile = Default service = PUBLIC uristring0 = sip:?@192.168.17.81

fromuri0 = sip:?@192.168.17.44

```
remoteport = 5070
accept = TRUNK INFO
match = user=trunk
register = NO REG
Route 83 towards BO#2 (Göteborg)
route:83
protocol = tcp
profile = Default
service = PUBLIC
uristring0 = sip:?@192.168.17.83
fromuri0 = sip:?@192.168.17.44
remoteport = 5070
accept = TRUNK_INFO
match = user=trunk
register = NO_REG
Route 211 towards BO#3 (Malmö)
route : 211
protocol = udp
profile = MXONE-tieline
service = PRIVATE SERVICES
uristring0 = sip:?@192.168.17.94;tgrp=BO3
fromuri0 = sip:?@192.168.17.44;tgrp=BO3
accept = ALL
register = SET_BY_PROFILE
trusted = TRUST BY PROFILE
NOTE: BO#3 is only reached by SIP trunks as it is an EX controller system running an own instance of
MX-ONE.
```

Setting up the GX Gateway

This section describes how to setup BO#1 (Linköping). Setting up BO#2 (Göteborg) is similar, only numbering information and own IP-address is changed.

Logon

This section describes how to setup BO#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 4.4: l	_ogin page
User Name:		
Password:		
		Login

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)
 - 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

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

	Figure 4.5: Host settings - 1												
Sys	tem	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Rou	uter	Management	Reboot
s	tatus	Host	Interfaces	VLAN	QoS	Local Fir	ewall	IP Routing	Network	Firewall	NAT	DHCP Server	
	Figure 4.6: Host settings - 2												
	Auto	matic Con	figuration In	terface									
	Auton	natic IPv4 c	onfig source r	network:		Uplink 🔹	~						
	Auton	natic IPv6 c	onfig source r	network:		UplinkV6	~						
2	han	no to St	atic IP ad	draee o	nd onte	or dofou	lt Cat	oway (C)	۸/)				

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

Figure 4.7: 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 4.8: 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 4.9: 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 Static 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 4.10: Setting static time zone

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

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

Interfaces

1. Go to Network > Interface.

	Figure 4.11: Interface												
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Ro	uter	Management	Reboot	
Status	Host	Interfaces	VLAN	QoS	Local Fi	rewall	IP Routing	Network	Firewall	NAT	DHCP Server		

2. Change Uplink to IpStatic (IPv4 Static) and enter the static IP-address and Static Default Gateway.

Figure 4.12: Changing Uplink to IpStatic

Network Interface C	onfiguration	1				
Name	Link	Туре	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

1. Go to Network > Local Firewall.

	Figure 4.13: Local firewalls												
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Rou	ıter	Management	Reboot	
Status	Host	Interfaces	VLAN	QoS	Local Fir	ewall	IP Routing	Network Fi	irewall	NAT	DHCP Server		

2. If local firewall security is needed change default policy to Drop.

Figure 4.14: 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 4.15: Enter network traffic

Lo	ocal 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 🗸		Accept 🗸	10	60		
2	Enable 🗸	172.17.17.0/24		Uplink		All 🗸		Accept 🗸	10	60	<u>∧∨+−</u>	
3	Enable 🗸	10.105.0.0/16		Uplink		All 🗸		Accept 🗸	10	60		
											•	

4. Click Save or Save and Apply when ready.

Session Board Controller (SBC)

Configuration

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

	Figure 4.16: Call agent - 1											
System	Network SI	IP Proxy S	BC ISDN	POTS SIP	Media	Telephony	Call Router	Management	Reboot			
Status	Configuration	Rulesets	Live Calls	Running Config	Events	Registration						
(Configuration N		no									

Figure 4.18: Call agent - 3

Call Agent Config	guration	1						
Name	Enable	Gateway	Signaling Interface	Media Interface	Peer Host	Peer Network		
local_users_ca	\checkmark		uplink_s	uplink_m		0.0.0.0/0		
trunk_lines_ca	\checkmark	trunk_lines_gw		loop_m				
remote_users_ca			uplink_s	uplink_m			2-	
MX-One_LIM1			uplink_s	uplink_m	192.168.17.44			
MX-One_LIM2			uplink_s	uplink_m	lim2.mitel.com		2-	
							+	

- 2. Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers in when the GW is in survivable mode, that is, the call is routed to PSTN and thus needs to be prefixed.
- **3.** Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 111[0-9][0-9]\$ means that the allowed number range in this branch is 11100 11199.

Figure 4.19: Parameters screen

Routing	Rulesets				
Priority	Name		Parameters		
1	MX-One_local_users_failover_to_trunk	/	ANUMBER=013443BNUMBER=08568		
2	MX-One_to_trunk_lines	/	PATTERN=PATTERN=111[0-9][0-9]\$		
3	MX-One_trunk_lines_to_local_users	/			
4	MX-One_routes_with_basic_local_survivability_TCP	/			
5	MX-One_routes_with_basic_local_survivability_UDP	/		\land \checkmark \square	
				•	

- 4. Configure each call agent (ca).
- 5. Click to enter specific data for each call agent.

Local_users_ca

- Enter the IP-address of MX-ONE to the DOMAIN variable.
- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 111[0-9][0-9]\$ means that the allowed number range in this branch is 11100 11199.
- Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers in when the GW is in survivable mode, that is, the call is routed to PSTN and thus needs to be prefixed.

Ì

Figure 4.20: Configure Call Agent screen

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	local_users_ca	
Enable	\checkmark	
Gateway		
Signaling Interface	uplink_s 🗸	
Media Interface	uplink_m 🗸	
Peer Host		
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		

Figure 4.21: Call Agent Rulesets screen

Call Age	nt Rulesets						
Priority	Name	Parameters					
1	MX-One_build_RURI_survivability ~	PATTERN=221[0-9][0-9]\$ DOMAIN=192.168.17.44					
2	MX-One_Appearance_Prefix	APP_PRFX=SCA-					
3	MX-One_Appearance_Prefix v	APP_PRFX=EDN-					
4	MX-One_Remove_Outbound_Appearance	PATTERN=221[0-9][0-9]\$					
5	MX-One_outbound_A_Number_prefix v	PATTERN=221[0-9][0-9]\$ A_PRFX=031325 PSTN_PREFIX=00					
6	MX-One_outbound_B_Number_prefix	BNUMBER=67[0-9][0-9][0-9]\$ B_PRFX=08568					
7	MX-One_outbound_B_Number_prefix v	BNUMBER=111[0-9][0-9]\$ B_PRFX=013443					
8	MX-One_outbound_B_Number_Override	BNUMBER=330[0-9][0-9]\$ BOVERRIDE=0856867000					
9	MX-One_local_reg_users_with_survivability 🗸	EXT_DIGIT_LENGTH=5					
			•				

Ruleset MX-ONE_build_RURI survivability (ACTIVE ONLY IN SURVIVAL MODE)

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

The pattern for the internal range of numbers, in this example the internal range would be 11100 – 11199 Calls to this number range stay always local (do not send to the PSTN in survival mode) DOMAIN=192.168.17.44

The IP of the headquarter (the main PBX), in this case 192.168.17.44

Ruleset: MX_ONE_Appearance_Prefix (ACTIVE ONLY IN SURVIVAL MODE)

NEW: APP_PREFIX=SCA-

This is the prefix for the usernames connected with shared appearance. In this example we have two: "SCA-" and "EDN-"

Ruleset: MX-ONE_Remove_Outbound_Appearance (ACTIVE ONLY IN SURVIVAL MODE)

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

This rule will remove any prefix used for Shared Call Appearance. The pattern for the internal range of numbers, in this example the internal range 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.

A_PRFX=013443

This is the prefix for the local numbers used on outgoing calls to the PSTN (in this example we received 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)

PSTN_PREFIX=00

Dial this prefix to break out to the PSTN. Here we have configured the "00" (not to be mixed up with the "00" for international calls!)

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.

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

Applies to calls to the specific range of extensions,

B_PRFX=08568

This is the prefix for the Called Party Number. In this case it was build like: National Prefix (08) + Main part of the HQ's local number: (568), in case somebody dials an extension in the HQ

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.

BNUMBER=330[0-9][0-9]\$

Applies to calls to the specific range

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE, in this example they 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, in this case set to "5", for numbers like "00001 – 99999"

1. Click **Save** when done.

Trunk _ Lines _ca

- Enter the IP-address of MX-ONE to the DOMAIN variable (in two places).
- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 111[0-9][0-9]\$ means that the allowed number range in this branch is 11100 11199.
- Insert a main extension number in MAIN_EXT parameter, this is could be the local answering position when dialling a vacant number, and so on.
- Enter the PSTN_PREFIX and STRIPNDIGTS, this is used to remove the public access code when dialling PSTN calls in survivable mode.

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	trunk_lines_ca	
Enable	\checkmark	
Gateway	trunk_lines_gw 🗸	
Signaling Interface	\sim	
Media Interface	loop_m 🗸	
Peer Host		
Peer Network		
Force Transport	Тср 🗸	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	0	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		

Figure 4.22: Trunk_Lines_ca

Figure 4.23: Trunk_Lines_ca Parameters

Call Ager	nt 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 🗸	MAIN_EXT=11104 PATTERN=111[0-9][0-9]\$ DOMAIN=192.168.1	
4	MX-One_Set_RURI_User_Type_Parameter	USER_TYPE=trunk	
5	MX-One_build_RURI_survivability	DOMAIN=192.168.17.44	
6	MX-One_Appearance_Prefix	APP_PRFX=SCA-	
7	MX-One_Appearance_Prefix 🗸	APP_PRFX=EDN-	
8	media_relay 🗸		
			+

Ruleset: MX-One_remove_prefix

PSTN_PREFIX=00

This is the prefix used to dial out to the PSTN

Ruleset: MX-One_trunk_lines_to_reception_survivability

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

MAIN_EXT=11104

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

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

The pattern for the internal range of numbers, in this example the internal range would be 11100 - 11199

DOMAIN=192.168.17.44

The IP of the headquarter (the main PBX), in this case 192.168.17.44

Ruleset: MX-One_Set_RURI_User_Type_Parameter

Set RURI User Type Parameter

USER_TYPE=trunk

1. Click Save when done.

MX-ONE_Lim1

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

Figure 4.24: Peer Host field

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	MX-One_LIM1	
Enable	\checkmark	
Gateway	~	
Signaling Interface	uplink_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		

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

Figure 4.25: RURI_HOST Parameter

Call Age	nt Rulesets		
Priority	Name	Parameters	
1	rewrite_RURI_host v	RURI_HOST=192.168.17.81	
2	MX-One_core_side		
			•

Ruleset: rewrite_RURI_host

Customize RURI host

RURI_HOST= 192.168.17.81. This is the local IP address.

- 3. When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.
- 4. Click **Save** when ready.

MX-ONE_TRUNK

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

Figure 4.26: MX-ONE Trunk

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	MX-One_LIM1	
Enable		
Gateway	~	
Signaling Interface	uplink_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 4.27: MX-ONE_TRUNK Parameters

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

- 2. When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.
- 3. Click **Save** when ready.

Figure 4.28: Configuration Modified



- 4. If the indication is not removed there are some error in the configuration.
- 5. Double check changes described above and correct them.

ISDN

						Figure	4.29: ISD	N tab			
System	Network	SIP Proxy	SBC	ISDN	POT	s sip	Media	Telephony	Call Router	Management	Reboot
Status	Statistics	Primary Ra	ate Interface	Inte	erop	Timer	Services				

If ISDN trunks are used, press **Start Sensing**. The system automatically detects certain parameters, for example, number of channels.

Primary Rate Interface

Figure 4.30: Primary Rate Interface											
System	Network	SIP Proxy	SBC	ISDN	POT	s sip	Media	Telephony	Call Router	Management	Reboot
Status	Statistics	Primary Ra	ate Interface	Int	erop	Timer	Services				

1. When sensing is done for several markets, specific parameters can be changed.

Figure 4.31: 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 V	
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 🗸	

2. Click Apply and restart requested service when done.

Interop

		Figure 4.32: Interop									
System	Network	SIP Proxy	SBC	ISDN	POT	'S SIP	Media	Telephony	Call Router	Management	Reboot
Status	Statistics	Primary Ra	ate Interface	: In	terop	Timer	Services				

1. You can change other parameters dependent on market.

Figure 4.33: Interop Configuration screen

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 🗸	

2. Click Apply and restart requested service when done.

Services

		Figure 4.34: Services									
System	Network	SIP Proxy	SBC	ISDN	POTS	s sip	Media	Telephony	Call Router	Management	Reboot
Status	Statistics	Primary Ra	ate Interface	Inte	erop	Timer	Services				

1. Change other parameters dependent on market.

Figure 4.35: Services Configuration screen

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 🗸	

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

Config

			Figure 4.36: Config									
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot	
Status	Config	FXS Configu	ration	FXO Cont	FXO Configuration							

1. Set market specific data for Caller Id handling.

Figure 4.37: General Configuration screen

General Configuration		
Caller ID Customisation:	EtsiDtmf 🗸	
Caller ID Transmission:	First Ring 🗸	
Vocal Unit Information:	All 🗸	

2. Click Apply when done and restart service.

FXS Configuration

Figure 4.38: FXS Configuration

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Config	FXS Configu	ration	FXO Cont	figuration						

1. Set analog phone specific data according to market.

Figure 4.39: FXS Configuration screen

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 4.40: Country Customisation screen

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

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

SIP

Gateways

Following gateways and port numbers are pre-defined.

							Figure 4.	41: Gate	ways			
System	Net	twork	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateway	s	Servers	Regi	strations	Authentio	cation	Transport	Interop	Misc			

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

Figure 4.42:	trunks	mx-one
--------------	--------	--------

Gateway Configuration							
Name	Туре	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	• -	
trunks_mx-one	Trunk 🗸	Uplink 🗸		Suggestion 🗸	5070	0 -	
						•	

Servers

							Figure 4	.43: Serv	ers			
System	Network	SIF	P Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateway	's Se	rvers	Regist	rations	Authentio	cation	Transport	Interop	Misc			

1. Enter IP-address to MX-ONE in both **Registrar Host** and **Proxy Host** fields.

Figure 4.44: Default Servers

Default Servers		
Registrar Host:	192.168.17.44	
Proxy Host:	192.168.17.44	
Messaging Server Host:		
Outbound Proxy Host:		

2. Change trunk_lines_gw to Yes in the drop-down list for Gateway Specific.

Figure 4.45: trunk_lines_gw

Registrar Servers			
Gateway	Gateway Specific	Registrar Host	
MX1_analog_ext	No 🗸	192.168.0.10:0	
trunk_lines_gw	Yes 🗸	%sbc%	
trunks_mx-one	No 🗸	192.168.0.10:0	

- 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 4.46: Outbound Proxy Host field

Proxy Servers	Proxy Servers									
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host							
MX1_analog_ext	Yes 🗸	192.168.17.44	192.168.17.81							
trunk_lines_gw	Yes 🗸	%sbc%	%sbc%							
trunks_mx-one	No 🗸	192.168.0.10:0	0.0.0.0:0							

- 5. Enter the IP-address of the gateway as Alternate Destination for MX1_analog_ext.
- 6. Enter the IP-address of MX-ONE as Alternate Destination for trunks_mx-one.

Figure 4.47: Alternate Destination for trunks_mx-one

Keep Alive Destination		
Gateway	Alternate Destination	
MX1_analog_ext	192.168.17.81	
trunk_lines_gw	127.0.0.1	
trunks_mx-one	192.168.17.44	

7. Click Apply when done and restart service.

Registrations

							Fi	gure 4.48	8: Regis	trat	tions			
System	Net	work	SIP	Proxy	SBC	ISDN	POTS	SIP	Media	Те	elephony	Call Router	Management	Reboot
Gateway	/S	Server	s	Registra	ations	Authenti	cation	Transport	Intero	р	Misc			

1. Enter the extension numbers for the analog extensions.

Figure 4.49: Endpoints Registration screen

Endpoint	Endpoints Registration										
Endpoint	t User Name	Friendly Name	Register	Messaging	Gateway Name						
FX01			Disable 🗸	Disable 🗸	trunks_mx-one 🧹						
FX02			Disable 🗸	Disable 🗸	trunks_mx-one 🗸						
FX03			Disable 🗸	Disable 🗸	trunks_mx-one 🗸						
FXO4			Disable 🗸	Disable 🗸	trunks_mx-one 🗸						
FXS1	11104		Enable 🗸	Disable 🗸	MX1_analog_ext 🗸						
FXS2	11105		Enable 🗸	Disable 🗸	MX1_analog_ext 🗸						
FXS3	11106		Enable 🗸	Disable 🗸	MX1_analog_ext 🗸						
FXS4	11107		Enable 🧹	Disable 🗸	MX1_analog_ext 🗸						
PRI1			Disable 🗸	Disable 🗸	trunks_mx-one 🗸						

2. Click Apply or Apply and Refresh when done.

Authentication

					Fig	gure 4.50	: Authen	tication			
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateway	ys Serve	ers Regist	rations	Authenti	cation	Transport	Interop	Misc			

1

1. If password is required press for any item.

Authenti	cation							
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	
1	Endpoint	FXS1			Disable		11104	1#2
2	Unit				Enable			188
3	Unit				Enable)#C
4	Unit				Enable			
5	Unit				Enable			188
6	Unit				Enable			
7	Unit				Enable)#C
8	Unit				Enable			
9	Unit				Enable			1÷8
10	Unit				Enable			
11	Unit				Enable)÷=
12	Unit				Enable			188
13	Unit				Enable			188
14	Unit				Enable)#8
15	Unit				Enable)#C
16	Unit				Enable			
17	Unit				Enable)#2
18	Unit				Enable)#8
19	Unit				Enable			
20	Unit				Enable			+-
				Number of	rows to add: 1		+	

Figure 4.51: Authentication Screen

- 2. Indicate for which Endpoint and Criteria the changes are to apply.
- 3. Enter the Auth Code, in the **Password** field.
- 4. In the Validate Realm field, select Disable.

Figure 4.52: Validate Realm field

Authent	ication								
Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password	
1	Endpoint 🗸	FXS1 🗸	\sim		Disable 🗸		11104	*******	

5. Click **Apply** or **Apply and Refresh Registration** when done and restart service. The result after 'Registration' and 'Authentication' should be like as follows:

Figure 4.53:	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 4.54: Transport								54 : Transport				
Syster	m Ne	etwork	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gat	eways	Server	s Reg	istrations	Authenti	cation	Transport	Interop	Misc			

1. Enable UDP if required.

Figure 4.55: Protocol Configuration screen

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

2. Click Apply when done and restart service.

Interop

							Figure	4.56: Inte	erop			
System	Net	work	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateway	ys	Servers	Registr	ations	Authentic	ation	Transport	Interop	Misc			

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

Figure 4.57: SIP URI User Parameter Value field

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

3. Click Apply or when done and restart service.

Misc

							Figure	4.58: Mis	SC			
System	Ne	twork	SIP Prox	ky SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gatewa	ays	Server	s Re	egistrations	Authenti	cation	Transport	Interop	Misc			

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

Figure 4.59: Gateway Configuration field

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

2. Click Apply when done and restart service.

Media

Codecs

					F	igure	4.60 : Co	decs			
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Codecs	Security	RTP Statis	stics	Misc							

1. Change Codecs according to preference.

	Figure	4.61:	Changing	Codecs
--	--------	-------	----------	--------

Codec	Voice	Data	Advanced	
G.711 a-Law	Enable 🗸	Enable 🗸		
G.711 u-Law	Disable 🗸	Enable 🗸		
G.723	Disable 🗸			
G.726 16Kbps	Disable 🗸			
G.726 24Kbps	Disable 🗸			
G.726 32Kbps	Disable 🗸	Disable 🗸		
G.726 40Kbps	Disable 🗸	Disable 🗸		
G.729	Disable 🗸			
Т.38		Enable 🗸		
Clear Mode	Disable 🗸	Disable 🗸		
Clear Channel	Disable 🗸	Disable 🗸		
X CCD	Disable 🗸	Disable 🗸		

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

Call Router

Route Config

	Figure 4.62: Route Config										
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Route Cont	ig Auto-r	outing								
Clarad			County								

1. Click for index 1. This is used if the received B-number contains a full number. That is, more digits P

than the pure DID numbers.

Figure	4.63:	Routes	screen
--------	-------	--------	--------

Route	s						
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	isdn-PRI1, isdn-PRI2, isdn-PRI3, isdn-PRI4, isdn- PRI5, isdn-PRI6, fxo-FX01, fxo-FX02, fxo- FX03, fxo-FX04	None		DID_Extension		hunt-sip	
2	sip-trunk_lines_gw, sip-trunks_mx-one	None				hunt-Hunt1	
							E

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

Figure 4.64: Transformations field

Configure Route 1			
	Value	Suggestion	
Sources	isdn-PRI1, isdn-PRI2, isdn-PRI3, isdn-PRI4, isdn- PRI5, isdn-PRI6, fxo-FXO1, fxo-FXO2, fxo-FXO3, fxo-FXO4	Suggestion 🗸	
Criteria Property	None		
Criteria Rule		Suggestion 🗸	
Transformations	DID_Extension	Suggestion 🗸	
Signaling Properties		Suggestion 🗸	
Destination	hunt-sip	Suggestion 🗸	
Config Status			

÷

- 3. Click Save.
- 4. Click 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 4.65: Configure Transformation 1 Screen

Configure Transformation	1	
	Value	
Name	DID_Extension	
Criteria Based On	Called E164	
Transformation Applies To	Called E164	
Config Status		

- 6. Click Save or Save and Insert Rule.
- 7. Click in the second Call Property Transformation and enter the same name as above.
- 8. 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 4.66: Configure Transformation Rule 1 screen

Configure Transform	ation Rule 1		
	Value	Suggestion	
Туре	Called E164 to Called E164		
Name	DID_Extension	Suggestion 🗸	
Criteria Rule	443(111\$)	Suggestion 🗸	
Transformation Rule	\1	Suggestion 🗸	
Next Transformation		Suggestion 🗸	
Config Status			

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

Figure 4.67: Transformations screen

Name	Criteria Based On	Transformation Applies To	
DID_Extension	Called E164	Called E164	
			•
	DID_Extension	DID_Extension Called E164	DID_Extension Called E164 Called E164

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

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

Management

Backup/Restore

1. Click Activate

Figure 4.68: Image Configuration screen

Image Configuration			
Transfer Parameters			
File Name:	20180503_final.xml	Suggestion 🗸	
Transfer Protocol:	File 🗸		
Host Name:	0.0.0.0:0		
Location:			
User Name:			
Password:			
Backup Parameters			
Content:	Config And Certificates 🗸		
Privacy Parameters			
Privacy Algorithm:	None 🗸		
Privacy Key:			

2. Click Apply and Backup Now.

File

Figure 4.69: Internal files screen

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

Find the previously made backup image

Figure 4.7	0: Backup	o image
------------	-----------	---------

Öppnar 20180503_final	.xml	×			
Du har valt att öppna:					
20180503_fina	l.xml				
som är en fil av	typen: XML Document (264 kB)				
från: http://192	.168.17.81				
Vad vill du att Firefox gör med denna fil?					
Oppna med Internet Explorer (standard) ∨					
○ Spara fil					
<u>G</u> ör detta automatiskt för denna filtyp i fortsättningen.					
	OK Avbryt				

Setting up MX-ONE for an EX Controller

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

Setting up EX Controller

Logon

This section describes how to setup BO#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	4.71:	Logon	screen
--------	-------	-------	--------

User Name:	
Password:	
	Login

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).
 - 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

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

 Figure 4.72: Host screen

 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

Figure 4.73: Automatic Configuration Interface

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 4.74: Default Gateway Configuration

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 4.75: DNS Configuration screen

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

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

Figure 4.76: SNTP Configuration

SNTP	Configuration		
Config	uration Source:	Static	
Static	Servers:		
Primary	y SNTP:	pool.ntp.org	
Secon	dary SNTP:		
Third S	SNTP:		
Fourth	SNTP:		
Synch	ironization:		
Synch	ronization Period:	1440	
Synch	ronization Period On Error:	60	

- 5. Set the Static 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 4.77: Time Configuration screen

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

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

Interfaces

1. Go to Network > Interface.

	Figure 4.78: Interfaces screen											
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Ro	uter I	Management	Reboot
Status	Host	Interfaces	VLAN	QoS	Local Fi	rewall	IP Routing	Network	Firewall	NAT	DHCP Server	

2. Change Uplink to IpStatic (IPv4 Static) and enter the static IP-address and Static Default Gateway.

Figure 4.79: Network Interface Configuration

Network Interface Configuration								
Name	Link	Туре	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

1. Go to Network > Local Firewall.

	Figure 4.80: Local Firewall screen											
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Ro	uter	Management	Reboot
Status	Host	Interfaces	VLAN	QoS	Local Fi	rewall	IP Routing	Network	Firewall	NAT	DHCP Server	

2. If local firewall security is needed, change default policy to Drop.

Figure 4.81: Local Firewall Configuration screen

	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 4.82: Local Firewall Rules screen

#	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 🗸		Accept 🗸	10	60		
2	Enable 🗸	172.17.17.0/24		Uplink		All 🗸		Accept 🗸	10	60	<u>∧∨+−</u>	
3	Enable 🗸	10.105.0.0/16		Uplink		All 🗸		Accept 🗸	10	60		
											+	

4. Click Save or Save and Apply when ready.

SBC

Configuration

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

Figure 4.83: SBC Configuration scree	en
--------------------------------------	----

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

Figure 4.84: Call Agent Configuration screen

Call Agent Confi	guratior						
Name	Enable	Gateway	Signaling Interface	Media Interface	Peer Host	Peer Network	
local_users_ca	\checkmark		uplink_s	uplink_m		0.0.0/0	
trunk_lines_ca	\checkmark	trunk_lines_gw		loop_m			
remote_users_ca			uplink_s	uplink_m			2-
MX-One_LIM1	\checkmark		uplink_s	uplink_m	192.168.17.93		
MX-One_LIM2			uplink_s	uplink_m	lim2.mitel.com		2-
MX-ONE-trunk	\checkmark		trunk_s	uplink_m	192.168.17.93		
							+

- 2. Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers when the GW is in survivable mode. That is, the call is routed to PSTN and thus needs to be prefixed.
- **3.** Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 321[0-9][0-9]\$ means that the allowed number range in this branch is 32100 32199.

Figure 4.85: Routing Rulesets screen

Routing Rulesets							
Priority	Name		Parameters				
1	MX-One_local_users_failover_to_trunk	~	ANUMBER=013443BNUMBER=08568				
2	MX-One_to_trunk_lines	~	PATTERN=PATTERN=111[0-9][0-9]\$				
3	MX-One_trunk_lines_to_local_users	~		<u>^</u>			
4	MX-One_routes_with_basic_local_survivability_TCP	~					
5	MX-One_routes_with_basic_local_survivability_UDP	~		\land \checkmark \square			
				•			

- 4. Configure each call agent (ca).
- 5. Click to enter specific data for each call agent.

Local_users_ca

- Enter the IP-address of MX-ONE to the DOMAIN variable.
- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 321[0-9][0-9]\$ means that the allowed number range in this branch is 32100 32199.
- Insert A-Number prefix and B-number prefix. These numbers are to be added in front of the numbers when the GW is in survivable mode. That is, the call is routed to PSTN and thus needs to be prefixed.

Ì

Figure 4.86: Configure Call Agent screen

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	local_users_ca	
Enable	\square	
Gateway		
Signaling Interface	uplink_s 🗸	
Media Interface	uplink_m 🗸	
Peer Host		
Peer Network	0.0.0/0	
Force Transport	None 🗸	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	0	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		

Figure 4.87: Call Agent Rulesets

	Call Ager	nt Rulesets		
	Priority	Name	Parameters	
	1	MX-One_build_RURI_survivability ~	PATTERN=321[0-9][0-9]\$ DOMAIN=192.168.17.94	
	2	MX-One_Appearance_Prefix	APP_PRFX=SCA-	
	3	MX-One_Appearance_Prefix 🗸	APP_PRFX=EDN-	
	4	MX-One_Remove_Outbound_Appearance	PATTERN=321[0-9][0-9]\$	
	5	MX-One_outbound_A_Number_prefix 🗸	PATTERN=321[0-9][0-9]\$ A_PRFX=anumber_prefix PSTN_PREf	
	6	MX-One_outbound_B_Number_prefix v	BNUMBER=67[0-9][0-9][0-9]\$ B_PRFX=08568	
	7	MX-One_outbound_B_Number_prefix v	BNUMBER=111[0-9][0-9]\$ B_PRFX=013443	
3	8	MX-One_outbound_B_Number_prefix	BNUMBER=221[0-9][0-9]\$ B_PRFX= 031325	
1	9	MX-One_outbound_B_Number_Override	BNUMBER=440[0-9][0-9]\$ BOVERRIDE=0856867000	
	10	MX-One_local_reg_users_with_survivability 🗸	EXT_DIGIT_LENGTH=5	
				+

Ruleset MX-One_build_RURI survivability (ACTIVE ONLY IN SURVIVAL MODE)

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

The pattern for the internal range of numbers, in this example the internal range would be 11100 - 11199

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

DOMAIN=192.168.17.94

The IP-address of the MX-ONE instance running on the VM, in this case 192.168.17.94

Ruleset: MX_One_Appearance_Prefix (ACTIVE ONLY IN SURVIVAL MODE)

NEW: APP_PREFIX=SCA-

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

Ruleset: MX-One_Remove_Outbound_Appearance (ACTIVE ONLY IN SURVIVAL MODE)

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

This rule removes any prefix used for Shared Call Appearance. The pattern for the internal range of numbers, in this example the internal range would be 32100 – 32199

Ruleset: MX-One_outbound_A_Number_prefix (ACTIVE ONLY IN SURVIVAL MODE)

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

This defines the local numbers.

A_PRFX=040598

This is the prefix for the local numbers used on outgoing calls to the PSTN (in this example, received 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)

PSTN_PREFIX=00

Dial this prefix to break out to the PSTN. Here, you need to configure the "00" (not to be mixed up with the "00" for international calls!)

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.

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

Applies to calls to the specific range of extensions,

B_PRFX=08568

This is the prefix for the Called Party Number. In this case, it was build like: National Prefix (08) + Main part of the HQ's local number: (568), in case somebody dials an extension in the HQ.

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.

BNUMBER=440[0-9][0-9]\$

Applies to calls to the specific range

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE, in this example they 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, in this case set to "5", for numbers like "00001 – 99999"

1. Click Save when done.

Trunk_Lines_ca

• Enter the IP-address of MX-ONE to the DOMAIN variable (in two places).

- Enter the number range that is allowed in the branch in the PATTERN parameter. For example, 321[0-9][0-9]\$ means that the allowed number range in this branch is 32100 32199.
- Insert a main extension number in MAIN_EXT parameter, this is could be the local answering position when dialling a vacant number, and so on.
- Enter the PSTN_PREFIX and STRIPNDIGTS, this is used to remove the public access code when dialling PSTN calls in survivable mode.

Figure 4.88: Configure Call Agent screen

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	trunk_lines_ca	
Enable	\square	
Gateway	trunk_lines_gw 🗸	
Signaling Interface	\sim	
Media Interface	loop_m 🗸	
Peer Host		
Peer Network		
Force Transport	Тср 🗸	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	0	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		

Figure 4.89: Call Agent Rulesets

Call Age	gent Rulesets										
Priority	Name	Parameters									
1	200_OK_to_SIP_OPTIONS V										
2	MX-One_remove_prefix V	PSTN_PREFIX=00									
3	MX-One_trunk_lines_to_reception_survivability 🗸	MAIN_EXT=11104 PATTERN=111[0-9][0-9]\$ DOMAIN=192.168.1									
4	MX-One_Set_RURI_User_Type_Parameter V	USER_TYPE=trunk									
5	MX-One_build_RURI_survivability ~	DOMAIN=192.168.17.44									
6	MX-One_Appearance_Prefix V	APP_PRFX=SCA-									
7	MX-One_Appearance_Prefix ~	APP_PRFX=EDN-									
8	media_relay 🗸										
			+								

Ruleset: MX-One_remove_prefix

PSTN_PREFIX=00

This is the prefix used to dial out to the PSTN

Ruleset: MX-One_trunk_lines_to_reception_survivability

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

MAIN_EXT=11104

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

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

The pattern for the internal range of numbers, in this example the internal range would be 32100 – 32199

DOMAIN=192.168.17.94

The IP of the headquarter (the main PBX), in this case 192.168.17.94

Ruleset: MX-One_Set_RURI_User_Type_Parameter

Set RURI User Type Parameter

USER_TYPE=trunk

1. Click Save when done.

MX-ONE_Lim1

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

Figure	4.90:	Peer	Host	field
--------	-------	------	------	-------

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	MX-One_LIM1	
Enable	\square	
Gateway	~	
Signaling Interface	uplink_s 🗸	
Media Interface	uplink_m 🗸	
Peer Host	192.168.17.94	
Peer Network		
Force Transport	None 🗸	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	0	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		

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

Figure 4.91: RURI_HOST parameter

Call Agent Rulesets									
Priority	Name	Parameters							
1	rewrite_RURI_host 🗸	RURI_HOST=192.168.17.85							
2	MX-One_core_side								
			F						

Ruleset: rewrite_RURI_host

Customize RURI host

RURI_HOST= 192.168.17.85. This is the local IP address.

1. Click Save when ready.

MX-ONE_TRUNK

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

-	•	
Configure Call Agent		
	Value	
Call Agent Parameters		
Name	MX-One-trunk	
Enable	\checkmark	
Gateway	~	
Signaling Interface	trunk_s 🗸	
Media Interface	uplink_m 🗸	
Peer Host	192.168.17.94	
Peer Network		
Force Transport	None 🗸	
Monitoring and Blacklisting Parameters		
Keep-Alive Interval	0	
Blacklisting Duration	0	
Blacklisting Delay	0	
Blacklisting Error Codes		

Figure 4.92: Call Agent Parameters

Figure 4.93: Call Agent Rulesets

Call Age	nt Rulesets		
Priority	Name	Parameters	
1	media_relay 🗸		
2	MX-One_core_side 🗸		
			+

- 2. When all the changes for call agents are done, a yellow field is shown indicating that configuration has been modified.
- 3. Click Save when ready.

Figure 4.94: Configuration Modified screen



- 4. If the indication is not removed there are some error in the configuration.
- 5. Double check changes described above and correct them.

ISDN



If ISDN trunks are used the first action to do is to click **Start Sensing**. The system automatically detects certain parameters, for example, number of channels.

Primary Rate Interface



1. When sensing is done for several markets, specific parameters can be changed.

Interface Configuration		
Line Type: [Configure]	E1	
Endpoint Type:		
Clock Mode:	Slave V	
Port Pinout:	Auto 🗸	
Monitor Link State:	Enable 🗸	
Line Coding:	HDB3 🗸	
Line Framing:	CRC4 🗸	
Signaling Protocol:	DSS1 V	
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 🗸	

1. Click Apply and restart requested service when done.

Interop

Figure 4.97: Interop screen											
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Statistics	Primary Ra	ate Interfac	e Inte	erop T	ïmer	Services				

1. You can change other parameters dependent on market.

Figure 4.98: Interop Configuration screen

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 🗸	

2. Click Apply and restart requested service when done.

Services



1. Change other parameters dependent on market.

Figure 4.100: Services Configuration screen

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 🗸	

2. Click Apply and restart requested service when done.

POTS

Config

Figure 4.101: Config screen											
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Config	FXS Configu	ration	FXO Con	figuration						

1. Set market specific data for Caller Id handling.

Figure 4.102: General Configuration screen

General Configuration		
Caller ID Customisation:	EtsiDtmf 🗸	
Caller ID Transmission:	First Ring 🗸	
Vocal Unit Information:	All	

2. Click Apply when done and restart service.

FXS Configuration

Figure 4.103: POTS FXS Configuration screen

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

1. Set analog phone specific data according to market.

Figure 4.104: FXS Configuration screen

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 4.105: Country Customisation screen

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

2. Click Apply when done and restart service.

SIP

Gateways

Following gateways and port numbers are pre-defined.



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

Figure 4.107: Gateway Configuration screen

Gateway Configuration							
Name	Туре	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	•	
trunks_mx-one	Trunk 🗸	Uplink 🗸		Suggestion 🗸	5070	0 📃	
						•	

Servers

Figure 4.108: Servers screen												
System	Network	SIF	Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateway	s Serve	ers	Registr	ations	Authentic	ation	Transport	Interop	Misc			

1. Enter IP-address to MX-ONE in both **Registrar Host** and **Proxy Host** fields.

Figure 4.109: Default Servers screen

Default Servers		
Registrar Host:	192.168.17.44	
Proxy Host:	192.168.17.44	
Messaging Server Host:		
Outbound Proxy Host:		

2. Change trunk_lines_gw to Yes in the drop-down list for Gateway Specific.

Figure 4.110: Registrar Servers screen

Registrar Servers			
Gateway	Gateway Specific	Registrar Host	
MX1_analog_ext	No 🗸	192.168.0.10:0	
trunk_lines_gw	Yes 🗸	%sbc%	
trunks_mx-one	No 🗸	192.168.0.10:0	

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

Figure 4.111: Proxy Servers screen

Proxy Servers			
Gateway	Gateway Specific	Proxy Host	Outbound Proxy Host
MX1_analog_ext	Yes 🗸	192.168.17.44	192.168.17.81
trunk_lines_gw	Yes 🗸	%sbc%	%sbc%
trunks_mx-one	No 🗸	192.168.0.10:0	0.0.0.0:0

- 5. Enter the IP-address of the gateway as Alternate Destination for MX1_analog_ext.
- 6. Enter the IP-address of MX-ONE as **Alternate Destination** for **trunks_mx-one**.

Figure 4.112: Keep Alive Destination screen

Keep Alive Destination		
Gateway	Alternate Destination	
MX1_analog_ext	192.168.17.85	
trunk_lines_gw	127.0.0.1	
trunks_mx-one	192.168.17.94	

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

Registrations

Figure 4.113: Registrations screen												
System	Network	SI	P Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gateway	/s Se	rvers	Regist	ations	Authentio	ation	Transport	Interop	Misc			

1. Enter the extension numbers for the analog extensions.

Figure 4.114: Endpoints Registration screen

Endpoints	Registration					
Endpoint	User Name	Friendly Name	Register	Messaging	Gateway Name	
Slot1/E1T1			Disable 🗸	Disable 🗸	trunks_mx-one 🗸	
Slot2/E1T1			Disable 🗸	Disable 🗸	trunks_mx-one 🗸	
Slot3/FXS1	32104		Enable 🗸	Disable 🗸	MX1_analog_ext 🗸	
Slot3/FXS2	32105		Enable 🗸	Disable 🗸	MX1_analog_ext 🗸	
Slot3/FXS3	32106		Enable 🗸	Disable 🗸	MX1_analog_ext 🗸	
Slot3/FXS4	32107		Disable 🗸	Disable 🗸	MX1_analog_ext 🗸	
Slot4/E1T1			Disable 🗸	Disable 🗸	trunks_mx-one 🗸	
Slot5/E1T1			Disable 🗸	Disable 🗸	trunks_mx-one 🗸	

2. Click Apply or Apply and Refresh when done.

Authentication





Ì

1. If password is required, click for any item.

				Figure 4.1	16: Authen	ticatio	on screen	
Authenti	cation							
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 o	f rows to add: 1			

- 2. Indicate for which Endpoint and Criteria changes are applicable.
- 3. Enter the Auth Code, in the **Password** field.
- 4. Disable Validate Realm.

Figure 4.117: Validate Realm screen

	Authent	ication								
	Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name	Password	
Γ	1	Endpoint 🗸	Slot3/FXS1 🗸	~		Disable 🗸		32104	******	

5. Click **Apply** or **Apply and Refresh Registration** when done and restart service. The result after 'Registration' and 'Authentication' should be like as follows.

Figure 4.1 ⁴	18:	Endpoints	Registration	screen
U				

Endpoints Reg	istration 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

Transport

					F	igure	4.119:	Trans	port s	creen		
S	system	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
	Gateway	s Serve	rs Regist	rations	Authenti	cation	Transport	Interop	Misc			

1. Enable UDP if required.

Figure 4.120: Protocol Configuration screen

Protocol Conf	iguration					
UDP	UDP QValue	тср	TCP QValue	TLS	TLS QValue	
Enable 🗸		Enable 🗸		Disable 🗸		

2. Click Apply when done and restart service.

Misc

Figure 4.121: Misc screen

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Gatewa	vs Serv	ers Reais	trations	Authenti	cation	Transport	Interop	Misc			

1. Enter the IP-address of MX-ONE in the SIP Domain Override filed for trunk_lines_gw.

Figure 4.122: Gateway Configuration screen

Gat	eway Configuration		
Gat	eway Name	SIP Domain Override	
MX	1_analog_ext		
trur	ik_lines_gw	192.168.17.94	
trur	iks_mx-one		

2. Click Apply when done and restart service.

Media

Codecs

				F	igure	4.12	3: Coo	decs scr	reen		
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Codecs	Security	RTP Statis	tics	Misc							

1. Change Codecs according to preference.

	Figure	Figure 4.124: Changing Codecs							
Codec	Voice	Data	Advanced						
G.711 a-Law	Enable 🗸	Enable 🗸							
G.711 u-Law	Disable 🗸	Enable 🗸							
G.723	Disable 🗸								
G.726 16Kbps	Disable 🗸								
G.726 24Kbps	Disable 🗸								
G.726 32Kbps	Disable 🗸	Disable 🗸							
G.726 40Kbps	Disable 🗸	Disable 🗸							
G.729	Disable 🗸								
T.38		Enable 🗸							
Clear Mode	Disable 🗸	Disable 🗸							
Clear Channel	Disable 🗸	Disable 🗸							
X CCD	Disable 🗸	Disable 🗸							

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

Call Router

Route Config

				Fig	ure 4.	125:	Route	Config	screen		
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Route Cor	ifig Auto-	routing								

Figure 4.126: Routes screen

1. Click for index 1. This is used if the received B-number contains a full number. That is, more digits

than the pure DID numbers.

Routes	5						
Index	Sources	Criteria Property	Criteria Rule	Transformations	Signaling Properties	Destination	
1	isdn-Slot1/E1T1, isdn-Slot2/E1T1, isdn- Slot3/E1T1, isdn-Slot2/E1T1, isdn-Slot5/E1T1, isdn-Slot3/E1T1, isdn-Slot7/E1T1, isdn- Slot8/E1T1, isdn-Slot7/E1T1, isdn- Slot8/E1T1, izd-Slot7/E1T1, izd- Slot8/E1T1, iz2-Slot7/E1T1, r2- Slot8/E1T1, r2-Slot7/E1T1, r2- Slot8/E1T1, r2-Slot7/E1T1, e&m- Slot1/E1T1, e&m-Slot5/E1T1, e&m- Slot8/E1T1, e&m-Slot5/E1T1, e&m- Slot6/E1T1, e&m-Slot8/E1T1, e&m- Slot6/EX03, fxo-Slot6/FX02, fxo-Slot4/FX03, fxo-Slot5/FX01, fxo-Slot6/FX02, fxo-Slot6/FX03, fxo-Slot5/FX01, fxo-Slot6/FX04, fxo-Slot7/FX04, fxo-Slot7/FX01, fxo-Slot8/FX02, fxo-Slot7/FX04, fxo-Slot7/FX01, fxo-Slot8/FX02, fxo-Slot8/FX03, fxo-Slot8/FX01, fxo-Slot8/FX02, fxo-Slot8/FX03, fxo-Slot8/FX01, fxo-Slot8/FX02, fxo-Slot8/FX03, fxo-Slot8/FX01, fxo-Slot8/FX02, fxo-Slot8/FX03, fxo-Slot8/FX04	None		DID_Extension		sip- trunk_lines_gw	
2	sip-trunks_mx-one, sip-trunk_lines_gw	None				hunt-Hunt1	
							F

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

Figure 4.127: Configure Route screen

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 V	
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 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.

Configure Transformation	1	
	Value	
Name	DID_Extension	
Criteria Based On	Called E164	
Transformation Applies To	Called E164	
Config Status		

+

- 6. Click Save or Save and Insert Rule.
- 7. Click in the second Call Property Transformation and enter the same name as above.
- 8. Use Called E.164 for both Criteria Based On and Transformation Applies To fields.

Figure 4.129: Configure Transformation screen 1

Configure Transformation	1	
	Value	
Name	DID_Extension	
Criteria Based On	Called E164	
Transformation Applies To	Called E164	
Config Status		

- 9. Click Save or Save and Insert Rule.
- **10.** Click in the second Call Property Transformation, and enter the same name as above.



12. 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 4.130: Configure Transformation Rule 1

Configure Transform	ure Transformation Rule 1			
	Value	Suggestion		
Туре	Called E164 to Called E164			
Name	DID_Extension	Suggestion 🗸		
Criteria Rule	598(321\$)	Suggestion 🗸		
Transformation Rule	\1	Suggestion 🗸		
Next Transformation	,ii	Suggestion v		
Config Status				

13. Click Save or Save and Insert Rule. Now, the 'Call Property Transformations' looks like this as shown below.
Figure 4.131: Transformations screen



14. Click Save if the yellow indication on top of the page is ON.

Management

Figure 4.132: Management screen													
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Teleph	ony Ca	I Router	Manage	ment	Reboot
Configu	ration Scripts	Backup / R	estore	Firmware	Upgrade	Certif	īcates	SNMP	CWMP	Access	s Control	File	Misc

Backup/Restore

1. Click the Activate unsecure script transfers through web browser link.

Figure 4.133: Image Configuration screen

Image Configuration			
Transfer Parameters			
File Name:	Backup_2018-07-30_85.xml	Suggestion 🗸	
Transfer Protocol:	File 🗸		
Host Name:	0.0.0:0		
Location:			
User Name:			
Password:			
Backup Parameters			
Content:	Config And Certificates 🗸		
Privacy Parameters			
Privacy Algorithm:	None 🗸		
Privacy Key:			

2. Click Apply and Backup Now.

File

	Figure 4.134: File screen												
System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Teleph	ony Ca	ll Router	Manage	ment	Reboot
Configu	ration Scripts	Backup / R	estore	Firmware	e Upgrade	Certi	ficates	SNMP	CWMP	Acces	s Control	File	Misc

Figure 4.135: Internal files screen

Internal files			
Name	Description	Size	
conf/Backup_2018-07-30_85.xml	Automatically generated on 24/08/2018 08:29:46.	149 KB	8
conf/FXO_Country_Defaults.cfg	FXO Country Defaults	1 KB	
conf/FXO_North-America_3km.cfg	FXO North-America 3km	1 KB	8
conf/PRI_China-DSS1.cfg	China DSS1	3 KB	
conf/PRI_Default.cfg	PRI default configuration	3 KB	8
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	8
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 4.136: Backup imag	е
Öppnar Backup_2018-	07-30_85.xml	×
Du har valt att öppna	:	
Backup_2018-	07-30_85.xml	
som är en fil av från: http://192	typen: XML Document (328 kB) .168.17.85	
Vad vill du att Firefox	k gör med denna fil?	
Oppna med	Office XML Handler (standard) \sim	
◯ <u>S</u> para fil		
<u>G</u> ör detta auto	omatiskt för denna filtyp i fortsättningen.	
	OK Avbryt	

2. Download and store on a secure place.

Configure TLS on an EX/GX Controller

This section describes how to configure TLS on an EX/GX controller with a typical scenario for a branch office with survivability and local presence. TLS ensures secure communication between the MX-ONE system and the EX and GX controller.

Prerequisites

Before you configure the TLS on the controller, ensure that the following requirements are met:

• The EX/GX controller setup is complete without TLS before you configure TLS on the controller. See the previous chapters in this document for the setup information.

CHAPTER 4

- The EX/GX controller setup is fully loaded and the virtual machine on which MX-ONE has been setup is switched on.
- The FXS extensions are registered. You can view the registration status in the path SIP > Registrations.
- The FXS extensions need to be in the SBC registration cache. You can view in the path SBC > Registration.
- The TLS certificate authority is generated and is available in the path /etc/opt/eri sn/certs/root with:
 - Certificate authority file: /etc/opt/eri_sn/certs/root/CA.pem
 - Private key: /etc/opt/eri_sn/certs/root/private_key.pem

Creating TLS Certificate with SAN

This section describes how to create a TLS certificate with Subject Alternative Name (SAN). SAN extension of the certificate specifies additional host names so that more than one host can use the same copy of a single certificate. This is required because the traffic between FXS ports and the SBC uses the loopback 127.0.0.1 address.

Connecting CA to the MX-ONE Server

To connect Certificate Authority (CA) to the MX-ONE server:

- 1. Log into the SSH client, such as Putty.
- 2. Connect to the MX-ONE server using the administrator credentials:

Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection 	Basic options for your PuTT Specify the destination you want to co Host Name (or IP address) 10.211.162.41 Connection type: Raw Telnet Rlogin Load, save or delete a stored session Saved Sessions	Y session onnect to Port 22 SSH © Serial
Colours ⊡ · Connection ··· Data ··· Proxy ··· Telnet ··· Rlogin ⊡ · SSH ··· Serial	Close window on exit:	Load Save Delete
About Help	Only Only	on clean exit

MX-ONE Server - SSH

Verifying the CA File

Using the command line, verify that the certificate authority file is valid and contains the required Issuer:

openssl x509 -in /etc/opt/eri_sn/certs/root/CA.pem -text| grep Issuer Issuer: CN=MXOneEnterpriseCA, C=SG, O=Root Certificate, OU=MX-ONE/emailAddress=root@EXLIMIPV4V6.mxonebglman.com

Generating the Unit Certificate with SAN

For the TLS to be enabled on different interfaces you must generate a unit certificate with SAN. For example:

- Uplink: 10.211.162.127
- LAN1: 192.168.0.10 (default IP)
- Loopback: 127.0.0.1 (IP to connect FXS and PSTN ports to the internal SBC)

The certificate must be generated on the MX-ONE server using the following procedure:

1. Create a directory for the unit certificates.

```
mkdir -p /etc/opt/eri_sn/certs/units
cd /etc/opt/eri sn/certs/units
```

 Create a configuration file for the uplink (10.211.162.127.cnf) to provide SAN options. Replace the uplink IP (10.211.162.127) with the IP address of the EX and GX controller.

```
cat << EOF > 10.211.162.127.cnf
[req]
distinguished name = req distinguished name
req extensions = v3 req
prompt = no
[req distinguished name]
CN = 10.211.162.127
[v3 req]
basicConstraints = CA:false
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt names
[alt names]
DNS.1 = 192.168.0.10
DNS.2 = 127.0.0.1
DNS.3 = 10.211.162.127
IP.1 = 192.168.0.10
IP.2 = 127.0.0.1
IP.3 = 10.211.162.127
EOF
```

 Generate a Private Key for the EX and GX controller unit. The first command will generate a key with password, the second one will convert the key so it requires no password (required by the following steps):

```
openssl genrsa -aes256 -out 10.211.162.127.key.protected 2048
openssl rsa -in 10.211.162.127.key.protected -out 10.211.162.127.key
```

4. Generate a CSR for the Unit.

```
openssl req -new -key 10.211.162.127.key -out 10.211.162.127.csr -sha256 -config 10.211.162.127.cnf
```

5. Verify the CSR:

```
openssl req -text -noout -verify -in 10.211.162.127.csr
```

6. Sign the CSR and generate a new certificate:

```
openssl x509 -req -sha256 -days 3652 -in 10.211.162.127.csr -CA
../root/CA.pem -CAkey ../root/private_key.pem -CAserial ../root/CA.srl
-CAcreateserial -out 10.211.162.127.crt -extfile 10.211.162.127.cnf
-extensions v3_req
```

7. Verify the uplink certificate (10.211.162.127.crt):

```
openssl x509 -in 10.211.162.127.crt -text
```

8. Create the uplink .pem file.

cat 10.211.162.127.crt 10.211.162.127.key > 10.211.162.127.pem

 Generate a Private Key for the EX and GX controller unit. The first command will generate a key with password, the second one will convert the key so it requires no password (required by the following steps):

```
openssl genrsa -aes256 -out 10.211.162.127.key.protected 2048
openssl rsa -in 10.211.162.127.key.protected -out 10.211.162.127.key
```

10. Generate a CSR for the Unit.

```
openssl req -new -key 10.211.162.127.key -out 10.211.162.127.csr -sha256 -config 10.211.162.127.cnf
```

11. Verify the CSR:

```
openssl req -text -noout -verify -in 10.211.162.127.csr
```

12. Sign the CSR and generate a new certificate:

```
openssl x509 -req -sha256 -days 3652 -in 10.211.162.127.csr -CA
../root/CA.pem -CAkey ../root/private_key.pem -CAserial ../root/CA.srl
-CAcreateserial -out 10.211.162.127.crt -extfile 10.211.162.127.cnf
-extensions v3_req
```

13. Verify the uplink certificate (10.211.162.127.crt):

openssl x509 -in 10.211.162.127.crt -text

14. Create the uplink .pem file.

cat 10.211.162.127.crt 10.211.162.127.key > 10.211.162.127.pem

Copying the Files on PC

Using a file transfer software, copy the following files from the MX-ONE to your PC:

- Unit Certificate: /etc/opt/eri_sn/certs/units/10.211.162.127.pem
- Root Certificate: /etc/opt/eri_sn/certs/root/CA.pem

Configuring the EX/GX for TLS

The procedures described in this section shows how to configure TLS in an EX/GX controller to establish a secure connection with MX-ONE system.

Login to the EX/GX Controller

Open a Web browser, log in to the EX/GX controller by using the default IP address or the previously configured uplink IP address. You can either log in as a public user (with no password) or an administrator using default credentials.

Installing Unit Certificates

1. In the EX/GX controller user interface, navigate to Management > Certificates.

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telepho	ony Call	Router	Manager	ment
Configura	ation Scripts	Backup / Re	estore	Firmware	Certific	ates	Virtuo	SNMP	CWMP	Access	Control	File

Certificates

Certificate transfer through web browser is disabled because of unsecure HTTP access.

Activate unsecure certificate transfer through web browser

- 2. Under Certificate Import Through Web browser.
 - a. Choose Host and click Choose.
 - b. Select the appropriate file (.pem file) on your PC and then click Import.

Certificate Import Through Web Browser											
Туре	Path										
Host 🔻	Choose File 10.211.162.127.pem	Import									

- 3. Under Certificate Import Through Web browser.
 - a. Choose Other and click Choose.
 - b. Select the appropriate file (.pem file) on your PC and then click Import.



4. Verify that the certificates have been installed:

Some changes require to restart a service to apply new configuration. Please click this link to access the services table or just restart required services

Certificates

Host Certificates											
File Name	Issued To	Issued By		Valid F	rom		Valid To		Usage	•	
10.211.162.127.pem	10.211.162.127	MXOneEnte	rpriseCA	2019-0	8-09 14:40:	22	2029-08-	08 14:40:	22 TIsClie	ent, TIsServer	6
Other Certificates											
File Name	Issued To		Issued By	/		Vali	d From	Valid	To Us	age (CA
CAmx.pem	MXOneEnterpris	seCA	MXOneEr	nterpriseC,	A	2019 14:5	9-08-07 58:23	2020-0 14:58:	08-06 23	1	/es 🗧
Cert_MxDefault001.der	Media5 Corpora Primary CA	tion - Mediatrix	Media5 Co Primary C	orporation A	- Mediatrix	2019 15:0	5-03-06)6:40	2065-0 15:06:	03-06 Tis 40 Tis	Client, Server	/es 🗧
Host Certificate Assoc	iations										
File Name	SIP	Web EAP	Conf	Fpu	File	Cert	Nim	SBC	CWMP		
10.211.162.127.pem					-			1			

5. Restart required services and log in to the EX/GX controller user interface again.

Configuring the Secure SIP ports

By default, the EX/GX controllers only listen to the non-secure SIP ports.

1. Navigate to **SIP > Gateways** in the EX/GX controller interface.

Gateway Configuration							
Name	Туре	Signaling Network	Media Networks	Media Networks Suggestion	Port	Secure Port	
MX1_analog_ext	Trunk T	Uplink T		Suggestion V	5080	<u>5081</u> _	
trunk_lines_gw	Trunk T	Loop 🔻	Loop	Suggestion V	5066	5067	
trunks_mx-one	Trunk T	Uplink T		Suggestion V	5070	5071 -	
						•	

- 2. For each SIP Gateway, add a secure port (Port +1).
- 3. Click Apply and restart the services.

Setting the TLS version, Cipher Suite, and Certificate Validation Level

For SIP gateways on the EX/GX to communicate with the SBC service, configure the TLS version to 1.2 and the Cipher Suite to CS3.

NOTE: It is recommended to disable the certificate validation until the setup is complete.

- 1. Navigate to Management > Configuration Scripts and click Execute.
- 2. Select Activate unsecure script transfers and execution through web browser.
- 3. In Execute inline script, copy and paste the following:

Apply

SipEp.TransportTlsVersion=TLSv1_2 SipEp.TransportTlsCipherSuite=CS3 SipEp.InteropTlsCertificateValidation=NoValidation Sbc.CertificateValidation=NoValidation Scm.RestartRequiredServices	
Execute Inline Script SipEp.TransportTlsVersion=TLSv1_2 SipEp.TransportTlsCipherSuite=CS3	
StpEp.InteropTisCertificateValidation=NoValidation Sbc.CertificateValidation=NoValidation Scm.RestartRequiredServices	(Clear Script)

4. Click Execute. It takes approximately 30 seconds for the services to restart.

Enabling TLS on the SBC Service

To enable TLS on SBC:

1. Navigate to SBC > Configuration.

System	Network	SIP Proxy	SBC	ISDN	POTS	SIP	Media	Telephony	Call Router	Management	Reboot
Status	Configuratio	on Rulese	ets L	ive Calls	Running (Config	Events	Registration			

- Configuration
- 2. In Call Agent Configuration, edit trunk_lines_ca by clicking on the Edit icon next to it.

Call Agent Configura	Call Agent Configuration							
Name En	able Gateway	Signaling Interface	Media Interface Peer Host	Peer Network				
local_users_ca 🕑)	uplink_s	uplink_m	0.0.0.0/0				
trunk_lines_ca 🕑	trunk_lines_gw		loop_m					

3. Set Force Transport as **TIs** and click **Save**.

Configure Call Agent

Configure Call Agent		
	Value	
Call Agent Parameters		
Name	trunk_lines_ca	
Enable		
Gateway	trunk_lines_gw V	
Signaling Interface	Ŧ	
Media Interface	loop_m ▼	
Peer Host		
Peer Network		
Force Transport		

4. Repeat the above steps for local_users_ca and MX-ONE_LIM1 call agents.

5. In Signaling Interface Configuration, edit loop_sand uplink_sand set Allowed Transports to TIsOnly and TIs Mode to Both and click Apply.

Signaling Interface Configuration							
Name	Network	Port	Secure Port	Allowed Transports	TIs Mode	Public Address	
loop_s	Loop 🔻	0	0	TIsOnly T	Both T		
lan1_s	Lan1 🔻	0	0	All 🔻	Client v		
uplink_s	Uplink T	0	0	TIsOnly T	Both T		
trunk_s	Uplink v	5090	5092	All 🔻	Client T	_	
						E	

- 6. Restart the required services. It takes about 30 seconds for the SBC service to restart.
- 7. Clear cache registration by navigating to **SBC > Registration**.

Enabling TLS between SIP Gateways and SBC

To enable TLS between SIP Gateways and SBC:

1. Navigate to SIP > Transport.

System	Network	SIP Proxy SB	C ISDN	POTS	SIP	Media	Telephon	y Call Router	Man
Gateways	Servers	Registrations	Authentica	ation T	Fransport	Interop	Misc		

Transport

General Configu	uration				
Add SIP Transpo	ort in Registration	:	Enable T		
Add SIP Transpo	ort in Contact Hea	ider:	Enable T		
Persistent Base	Port:		16000		
Failback Interval	:		15		
TLS Certificate T	rust Level:		Locally Trusted	•	
TCP Connect Tir	meout:		127		
Protocol Config	juration				
UDP	UDP QValue	ТСР	TCP QValue	TLS	TLS QValue
Disable V		Enable V		Enable T	

Apply

- 2. Configure the general configuration details as shown in the above figure and click Apply.
- 3. Restart the required services. It takes about 30 seconds for the service to restart.
- 4. Navigate to SIP > Registrations.
- 5. Validate if endpoints are registered the agent MX1_analog_ext.

6. Navigate to SBC > Registration, validate all endpoints are registered using TLS.

AoR	Contact-URI
sip:32100@10.211.162.41	sip:32100@10.211.162.127:16000;transport=tls
sip:32101@10.211.162.41	sip:32101@10.211.162.127:16000;transport=tls
sip:32102@10.211.162.41	sip:32102@10.211.162.127:16000;transport=tls
sip:32103@10.211.162.41	sip:32103@10.211.162.127:16000;transport=tls

7. Test a call between endpoints. For example 32100 to 32101.

Enabling SRTP on EX/GX Controller

To enable SRTP on the EX/GX controller:

- 1. Navigate to Media > Security.
- 2. Under Select Endpoint, choose Secure.
- 3. Select Mode as, Secure.
- 4. Select Key Management Protocol as, SDES.
- 5. Select Encryption as, AES_CM_128.
- 6. Select **Yes** for the T.38 setting.

Enabling Certificate Validation

After the EX/GX controller with TLS setup is complete, you can enable certificate validation:

- Navigate to Management > Configuration Scripts > Execute and select Activate unsecure script transfers and execution through web browser.
- 2. In Execute Inline Script, copy and paste the following:

```
SipEp.InteropTlsCertificateValidation=HostName
bc.CertificateValidation=HostName
Sbc.ResetRegistrationCache
Scm.RestartRequiredServices
```

- 3. Click Execute.
- 4. Navigate SIP > Registrations.
- 5. Validate that the endpoints are registered to call agent MX1_analog_ext.

Known Limitations

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

CHAPTER 4

- When MX-ONE is installed as a virtual machine in the EX-Controller, Provisioning Manger 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.

Integration of MiVoice MX-ONE with Microsoft[®] Lync Server™ 2013 – Remote Call Control

Introduction

MiVoice MX-ONE, a complete IP-based communications system, has evolved from a voice centric system into a true multimedia communication system that can route and provide services to media sessions like video, instant messaging etc. It is the core component of the MX-ONE solution, which provides the necessary applications to offer true mobility and Unified Communications and Collaboration (UCC). MX-ONE (TS) is based on an open software and hardware environment, using standard servers with a LINUX SUSE operating system. MX-ONE Service Node focuses on enhanced SIP implementations to target our strategy regarding openness, cloud computing and video support. An example of MX-ONE openness is the fact that it can interwork with third party UC products using standards-based protocols, such as SIP and CSTA III (XML).

As part of this standards-based approach and in order to offer our customers a choice, we have worked together with Microsoft to ensure that MX-ONE can be integrated with the latest Microsoft Unified Communications products. MX-ONE is fully certified by the Microsoft Partner Program since Version 4.1 with Lync Server 2010 (Direct SIP integration) as well as MX-ONE 5.0 SP3 HF2 with Lync 2013 (Direct SIP integration) in order to ensure that customers have seamless experiences with setup, support, and use of MX-ONE with Microsoft Unified Communications software.

In MX-ONE 5.0 SP1, TR-87 support for CSTA III (Computer Supported Telecommunications Applications Version 3) was added to allow a third party application to control an MX-ONE device via CSTA and SIP messages. This service can be used, for example, to connect MX-ONE and Microsoft Lync Server via a function called Remote Call Control.

Mitel has performed an internal integration validation between MX-ONE 6.0 and Lync Server 2013 via Remote Call Control, where several tests were executed to assure the compatibility between the products.

Scope

The intent of this guide is to describe the setup tasks to integrate MiVoice MX-ONE and Microsoft Lync Server 2013 for Remote Call Control.

For more details regarding components of this integration, we refer to the relevant MX-ONE CPI documentation or, please, go to the Microsoft Lync Server 2013 product website.

Ē

Note! Always check the latest products documentation.

Solution Description

Integration of MX-ONE 6.0 with Microsoft Lync Server 2013 for Remote Call Control as a complementary solution, provides users enabled for remote call control to use Lync 2013 client to control calls on their MX-ONE phones.

MiVoice MX-ONE

MiVoice MX-ONE has a built-in CSTA III server that is an interface that other applications can use to remotely control a phone. Examples of operations that can be performed with CSTA Phase III are: make call, answer call, dial a number and terminate a call.

MX-ONE 6.0 supports CSTA method that is based on European Computer Manufacturers Association (ECMA) Technical Report-87 (TR-87), called Using CSTA for SIP Phone User Agents (uaCSTA). MX-ONE implements a subset of the capabilities and methods proposed in TR-87 specification.

In TR-87 (Using CSTA for SIP Phone User Agents (uaCSTA)):

SIP is used to establish a CSTA application session

CSTA service request and response messages are transported over SIP

CSTA monitor is started and CSTA events are transported over SIP

Microsoft Lync Server 2013

Microsoft Lync Server 2013 offers Remote Call Control (RCC) support that allows users to remotely control phones connected to a call manager, such as MX-ONE. It gives Lync 2013 client users the ability to make or receive calls on their fixed or mobile phone instead of a computer.

Integration

CSTA III (XML) is required to provide the integration between MX-ONE and Lync Server for Remote Call Control as shown in the figure below.

The telephony feature commands are sent from the Lync 2013 client through the Microsoft Lync Server 2013 to the internal MX-ONE CSTA server as CSTA III messages over SIP, so called user agent CSTA (uaCSTA). The internal MX-ONE CSTA server analyzes the requests and maps them to the corresponding CSTA commands towards MX-ONE, which will then carry out the requests.



Figure 1 - Integration via Remote Call Control (RCC) between MX-ONE and Lync Server 2013

With Microsoft Lync Server 2013 integration, it is possible from Lync 2013 client (Remote Call Control Only) to manage calls and talk using any fixed and remote extensions within the MX-ONE.

The features that a Lync 2013 client can manage when integrate with MX-ONE using RCC are:

Make an outgoing call

Answer an incoming call

Transfer a call to another user (monitored transfer with current conversations)

Single step transfer

Forward an incoming call to an internal number (internal and private network extensions)

Forward an incoming call to an external number

Redirect an incoming call

Place calls on hold

Alternate (toggle) between multiple concurrent calls

Answer a second call while already in a call.

Dial dual-tone multi-frequency (DTMF) digits

Requirements and Setup

MX-ONE and Microsoft Lync needs to be configured in different sip domains. Mitel recommendation is that MX-ONE is a sub-domain of the Lync domain.

For example, Lync runs on the domain: domain.com and MX-ONE runs on the domain: mx-one.domain.com.

MIVOICE MX-ONE Requirements

Software and licenses required for Microsoft Remote Call Control integration:

MiVoice MX-ONE Service Node 6.0 or later

MX-ONE licenses for:

CSTA III



Note! Multi terminal extensions cannot be monitored via CSTA and therefore it does not work in the Remote Call Control scenario.

Microsoft Lync Server 2013 Requirements

The Microsoft infrastructure (AD, DNS, CA, etc) needs to be in place, including all licenses required.

This guide does not cover the Lync Server 2013 installation. Our recommendation is that the Microsoft infrastructure shall be installed by a trained Microsoft engineer.

Before to start Microsoft Lync Server 2013 for RCC setup, read the following document:

Microsoft Lync Server 2013, Deploying Remote Call Control

http://technet.microsoft.com/en-us/library/gg558664.aspx

ľ

Note! This Microsoft documentation is used in conjunction with this guide.

MX-ONE was validated with Microsoft Lync 2013 Remote Call Control with only one Lync Front End server.

Microsoft Lync 2013 requires load balancer when more than one Front End is used. Please note that this setup was not validated with MX-ONE.



Note! The latest Lync Client (Lync 2013 update: April 2014) needs to be installed in the end user computers, please see that article below.

http://support.microsoft.com/kb/2880474

Integration Setup - TCP

The setup used in this guide is based on the following scenario:

One Microsoft Lync Server - Standard Edition connected with one MiVoice MX-ONE 6.0.



Figure 2 - Integration setup



Note! Mitel recommends that complex scenarios shall be validated in the partner labs prior to customer deployment.

MiVoice MX-ONE Setup - TCP

The following shall be configured:

CSTA server needs to be initiated

Creating CSTA Server

CSTA III Setting:

csta--initiate--lim1 --csta-serv00000010

For more about CSTA III, see MX-ONE CPI documentation.

Microsoft Lync Server 2013 Setup – TCP

The following setup is based in the Microsoft Lync Server 2013 documentation, Deploying Remote Call Control, for more about commands syntaxes check:

http://technet.microsoft.com/en-us/library/gg558664.aspx

The following shall be configured:

Configure a Static Route for Remote Call Control

Configure a Trusted Application Entry for Remote Call Control

Configure Static Route for Remote Call Control

The following commands shall be executed in the Lync Server Management Shell to configure Remote Call Control.

Route for Remote Call ControlSetup, port 5060 (TCP):

\$TCPRoute= New-CsStaticRoute-TCPRoute-Destination 192.168.222.156 -Port 5062 -MatchUrimx-one.domain.com

Set-CsStaticRoutingConfiguration-Route @{Add=\$TCPRoute} -Identity Global

To verify the setup use the command:

Get-CsStaticRoutingConfiguration

Configure a Trusted Application Pool Entry for Remote Call Control

To create a Trusted Application Pool use the command:

New-CsTrustedApplicationpool-Identity 192.168.222.156 -Registrar lync-enter.domain.com –Site 1 –TreatAsAuthenticated\$True –ThrottleAsServer\$True

To verify the setup use the command:

Get-CsTrustedApplicationpool

Configure a Trusted Application Entry for Remote Call Control

To setup the trusted application use the command::

New-CsTrustedApplication-ApplicationIDRCC -TrustedApplicationPoolFqdn192.168.222.156 -Port 5062 -EnableTcp

To verify the setup use the command:

Get-CsTrustedApplication

Publish the topology

To implement the changes in the Lync, publish the topology

Enable-CsTopology

Define a SIP/CSTA Gateway IP Address

In this example TCP is used, then the SIP/CSTA gateway IP address needs to be defined. Follow the instruction in the session "Define a SIP/CSTA Gateway IP Address" from Microsoft documentation: http://technet.microsoft.com/en-us/library/gg602125.aspx.

When the setup is done, the Topology Builder screen should be similar to figure below.

Kunc Server 2013, Topology Builder		
<u>F</u> ile <u>A</u> ction <u>H</u> elp		
Lync Server Modeling Constraints Lync Server 2010 Lync Server 2013 Lync Server 2013 Lync Server 2013 Director pools Mediation pools Persistent Chat pools Ledge pools Director pools Dire	General FQDN: Enable replication of configuration data to this pool IPv4 addresses: Primary IPv4 address:	▲ 192.168.222.156 Disabled Limit service usage to specified addresses 192.168.222.156
 □ Tractac projection Servers □ 192.168.222.156 □ Shared Components □ Branch sites 	Next hop selection	▲

Figure 3 - Lync Server 2013 Topology Builder

Enable Lync Users for Remote Call Control

Configure a user for remote call control by using Lync Server Control Panel.

Under Telephony, select Remote Call Control Only. Please, note that the option "Remote Call Control" is not supported by MX-ONE.

The following needs to be configured under Line URI and Line Server URI.

Enable Lync Users for Remote Call Control:

Line URI:tel:phonenumber, exampletel:27000

Line Server URI:sip:tel@MatchUri, for example: sip:27000@mx-one.domain.com

* Enable × Cancel			
Display name	Status	Add	
Alice RCC			
		Remove	
Assign users to a pool: *			
Lync-enter.domain.com		T	
Generate user's SIP URI:			
Use user's email address			
Use the user principal name (UP)	PN)		
Use the following format:			
<firstname>.<lastname> @</lastname></firstname>	domain.com	▼	
Use the following format:			
<samaccountname> @ doma</samaccountname>	in.com	v	
Specify a SIP URI:			
	@ domain.com	v	
Telephony:			
Remote call control only		▼ ?	
Line URI: *			
tel:27000		?	
Line Server URI: *			
sip:27000@mx-one.domain.com	n		
Conferencing policy:			

Figure 4 - RCC only new user configuration example

How to Verify the Setup

After completing the setup, the integration can be verified in the following way:

Lync 2013 Client Features

Using a Lync 2013 client sign-in a RCC user.

If the configuration was done properly the user will be signed in without any error, see the figure below.

٩		Lync		-		×				
What's ha	What's happening today?									
2	Alice RCC Available ▼ Set Your Location ▼									
	🎍 👦 😭									
Find some	Find someone or dial a number									
	1	2 ABC	3 DEF							
	4 GHI	5 JKL	6 MNO							
	7 pqrs	8 TUV	9 wxyz							
	*	0 +	#							
	Redial	L C	Call							
	1	II PIN								
🕼 🕶 CALI	FORWARDING	DFF								

If there is small icon in the lower right side of the Lync 2013 client, showing a phone with an error, check the setup, because the CSTA monitoring could not be established.

	Lync	- 0	×
What's h	appening today?		
0	Alice RCC Available ▼ Set Your Location ▼		
2	N	¢	÷ •
Find som	one or dial a number		٩
GROUPS	STATUS RELATIONSHIPS NEV	v	*
2	Bob RCC - Available		
▲ Other C	ontacts (0/0)		
🕼 + CAL	L FORWARDING OFF	Û	ō-
			Notifications
			No Phone System Conne

Use the MiVoice MX-ONE command "csta -p --lim all --devices" to check the devices that are monitored.

In the use cases below two Lync clients were used and three MX-ONE extensions.

- 1. Alice.RCC controls the extension 27001, which is a SIP extension in MX-ONE.
- 2. Bob.RCC controls the extension 27010, which is a SIP extension in MX-ONE.
- 3. 27000 and 27002 are SIP extensions in MX-ONE.
- 4. 33350202 and 33350102 are the PSTN phones.

Make an Outgoing Call Using the Lync 2013 Client

From extension A use the Lync client (RCC) to dial extension B, pick up your handset as soon as you hear the ring back tone, wait the extension B answer, check if there is speech.

Answer an Incoming Call

From another extension dial to RCC user, answer it and check if there is speech.



Transfer a Call Between Current Conversations (Monitored Transfer)

In this scenario A (Alice.RCC - extension 27001) calls B (Bob.RCC - extension 27010), A puts B on hold and then calls extension C (27002). After C answers, A transfers the call between B and C.

We assume you have answered a call with extension B (27010) from the Lync client (RCC



Using the client, put extension B on hold and make a second call to extension C (27002), and wait until the extension C answers.

D		Lync		>]	
What's	happening today	?				
	Alice RCC In a call ▼ Set Your Loca	ition 🔻				
	P	2		☆ •		
27002				×		
	1	2 ABC	3 DEF			
	4 сні	5 JKL	6 мио			
	7 PQRS	8 TUV	9 wxyz			
	*	0 +	#			
	Redial	د ا	Call			
	1	III PIN			27002	≍ - □
NAME					.atf 0:15	e
	27002					
					27002	
(⇒• c	ALL FORWARDING	OFF			ه 🗉	

Once speech is established, initiate the transfer of extension B (Bob RCC) using the Current Conversations option as shown below.

27002	DIAL PAD TRANSFER CALL		n x
ant 0:38	My Numbers	*	$oldsymbol{eta}$
	Mobile +0033350201		
	Current Conversations	^	
	Bob RCC		
	Other Options	^	
	Mute Hold Call	¥	
	•	Ē	E

Then, check if the call is correctly transferred.

D		Lync		-	□ ×				
What's h	appening today?								
0	Bob RCC In a call ▼ Set Your Locat	ion 🔻							
*	P				☆ -				
Find some	eone or dial a nu	mber			Q				
	1	2 ABC	3 DEF						
	4 GHI	5 жі	6 ммо						
	7 pqrs	8 TUV	9 wxvz			27002		2	- 🗆 ×
	*	0 +	#			2:48			
	Redial	د ا	Call						\cup
		₩ PIN					27002		
€ CAL	L FORWARDING	OFF						22	••••

Then, check if the call is correctly transferred.

Single Step Transfer

In this scenario A (Alice.RCC - extension 27001) is talking with C (extension 27002), A transfer C directly to extension B (Bob.RCC - extension 27010).

We assume you have answered a call with extension C (27002).



A does single-step transfer from extension C (27002) to B (Bob.RCC - extension 27010).

			×
		Invite by Name or Phone Number	
27002	DIAL PAD TRANSFER CALL	Choose a contact or type a name or phone number.	
	My Numbers		
	Mobile +0033350201	Bob RCC - Available	
	Other Options		
	Another Person or Number	27001	
	C ^{III} <u>P</u> arking Lot		
	Mute Hold Call		
		<u>OK</u> Cancel	

Then, check if the call is correctly transferred.



Forward an Incoming Call

Select a predefined or a new number (internal, network extension or external) and click ok.

•	Lyr	nc			_		j	×
What's ha	ppening today?							
0	Alice RCC Available - Set Your Location	•						
2	t						¢	•
ROHPS	STATIS RELATIO	исні	IDC	NEW			ş	C
GROUPS	STATUS RELATIO	NSHI	IPS	NEW			ł	ò
▲ Favorite	s							
	Bob RCC - Availa	ble						
	27010							
]	33350202							
▲ Other Co	ontacts (0/0)							
To add	contacts, drag from	anot	her g	roup or add fror	n sea	arch.		
Call Forw	arding is Off							
Incoming	Calls							
C Ium	Off Call Forwarding							
C Eorw	ard Calls To	+	For	ward Calls To				
Call F	orwarding <u>S</u> ettings			27010				
🕼 👻 CALI	L FORWARDING OFF		4	<u>N</u> ew Number				

Check if Lync client is showing that the forwarding is on.



Place Calls on Hold

When in speech, press the hold button to hold a call.

🔛 Bob R	DIAL PAD TRANSFER CALL							
atl 1:55				\bigcirc				
	1	2 ABC	3 DEF					
	4 сні	5 JKL	6 ммо					
	7 pqrs	8 TUV	9 wxyz					
	*	0	#					
	Mute Hold C	Call						

Click on Resume Call to return to the call.



Alternate Between Multiple Concurrent Calls

When connected with two calls, press the hold button to hold a call and click on Resume Call to return to



the first one.



Answer a Second Call While Already in a Call (call waiting)

When a second call is alerting, click on Accept Call to answer it.



You can alternate between the calls.

Dial Dual-Tone Multi-Frequency (DTMF) Digits

In an established call, click on the keypad and enter DTMF digits.



Presence

In order to verify presence, establish a call using Lync client (RCC) as below.

From extension A use the Lync client (RCC) to dial extension B, pick up your handset as soon as you

		Lync		×			
What's ha	ppening today?						
	Available •						
Set Your Location -							
2	t	•		\$ -			
Find some	one or dial a nu	mber		۵			
1110 30110							
	1	2 ABC	3 DEF				
	4 GHI	5 JKL	6 MNO				
	7 PQRS	8 TUV	9 wxyz				
	*	0 +	#				
	Redial	٠ ر	Call				
		•	Cull				
		PIN					
🕼 + CALI	FORWARDING	OFF					
		Lync	-	n x			
What's	happening toda	v?					
	Bob RCC						
	Available 🔻						
	Set Your Loc	ation •					
.				-Q: •			
Find so	meone or dial a r	number		Q			
CROUPS			NEW				
4 Eavori	tec	LATIONSHIPS	INEW	60			
- Tavon	Alico PCC	Ausilabla					
Alice RCC - Available							
✓ Other	Contacts (0/0)						
✓ Other To ad	Contacts (0/0) d contacts, drag	ı from another g	roup or add fror	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	I from another g	roup or add froi	n search.			
 Other To ad 	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
 Other To ad 	Contacts (0/0) d contacts, drag	from another g	roup or add froi	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	, from another g	roup or add fror	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
 Other To ad 	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
 Other To ad 	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
 Other To ad 	Contacts (0/0) d contacts, drag	from another g	roup or add fror	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	from another g	roup or add fron	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	i from another g	roup or add fron	n search.			
▲ Other To ad	Contacts (0/0) d contacts, drag	, from another g	roup or add fron	n search.			
Other To ad	Contacts (0/0) d contacts, drag	from another g	roup or add fron	n search.			

hear the ring back tone, wait until the extension B answers, check if there is speech.

:	Available - Set Your Locat	ion -		⇔ -	
Find som	neone or dial a nu	mber		٩	×
	1	2 ABC	3 DEF		Call New Phone Number
	4 сні	5 JKL	6 MNO	_	
	7 PQRS	8 TUV	9 wxyz		27010
	*	0 +	#		FYI: If you're making an international call, you'll want to
	Redial	C	Call		include the right country and region codes. Get examples
	1	II PIN		-	OK Cancel

From another Lync client, for example Bob, RCC that is monitoring Alice RCC, check if the presence status is now "In a Call".

D		Lync			-		×
What's hap	pening to	oday?					
	Bob RC In a call ▼ Set Your I	C ocation 🔻					
2 "	-,					¢	•
Find someo	ne or dial	a number					ρ
GROUPS S	TATUS	RELATIONS	HIPS	VEW			•
▲ Favorites							
	Alice RC	CC - In a call					
▲ Other Con	ntacts (0/	D)					
🕞 🔻 CALL F	FORWARD	DING OFF					

Disconnect the call from extension A (Alice RCC) and check if the Alice RCC presence status goes to Available in the Bob RCC.



Limitations

The integration supports Lync 2013 clients configured with "Remote Call Control only" option. The option "Remote Call Control" is not supported.

The secure transport mechanism using TLS is not supported in MX-ONE 6.x.

The features listed below are not supported in this integration, when initiated by the Lync client:

Do not disturb (it is not supported by Lync client)



Note! Although these features may not be possible from the client, they may be invoked directly on the terminal instead.

Good to Know

MX-ONE and Lync Server cannot be part of the same domain.

Latest Lync client needs to be installed.

DNS needs to be properly configured.

Conference can be invoked via Lync client using MX-ONE procedure (normally dialing 3). However, the Lync client will merge all other screens with the first one and that will be presented until the last member disconnects.

Revision History

Document Version	Comment	Date
Rev. A	First release	2014-05-09
Rev. B	Rebranding	2015-05-10
Rev. B1	Some further rebranding corrections done.	2016-03-17
Rev. B2	Minor changes done.	2016-10-10

MiVoice Border Gateway MBG -Installation Instructions

General

This document describes how to configure a single standalone MiVoice Border Gateway (MBG) Release 11.0 server to support Mitel 6900/6800 SIP Terminals as Tele-worker devices for MX-ONE.

This document complements MX-ONE document "Mitel 6700i and 6800i SIP Terminals for MX-ONE" and provides instructions how to setup MBG as an Ingate replacement. The principle used here is to configure MBG to have secure communication on the outside towards the home worker terminals and unsecured communication on the inside towards MX-ONE. The proposed solution has the same limitations as the existing Ingate deployment.

Instructions in this document are specific to the above configuration and must NOT be used in any other deployments. For example, MiCollab 7.1 with MBG and MiCollab clients with MX-ONE.

Application Requirements

You must meet the minimum software level requirements for each application listed below so that the applications function correctly with this Release.

Application	Recommended Software Level	Comments
Mitel Standard Linux (MSL)	11.0	Refer to the <i>MBG Installation</i> <i>and Maintenance Guide 11.0</i> located in the Doc Center on the MiAccess Portal.
MX-ONE	7.3	-
6900	5.1 SP5	Release 5.1 SIP extensions
68xxi	5.1 SP5	Release 5.1 SP5
MBG	11.0	-

Installation Notes

The principle used here is to configure MBG to have secure communication on the outside towards the home worker terminals and insecure communication on the inside towards MX-ONE.

Licensing

The only licensing required is a MiVoice Border Gateway base kit (physical or virtual) and Teleworker licenses (1 per 68xxi device + a few floater licenses).

Installing Release 11.0 on a Standalone Physical Server

For installation of MBG on a standalone physical server, refer to the *MBG Installation and Maintenance Guide 11.0.*

Installing Release 11.0 in a VMware Environment

For installation of MBG on a standalone physical server, refer to the *MBG Installation and Maintenance Guide 11.0*.

Firewall Configuration

If MBG is deployed in a demilitarized zone, the following ports need to be opened (above ports needed for communication with the AMC).

- TCP port 5061 between the Internet and MBG for SIP TLS
- TCP port 5060 between MBG and MX-ONE
- TCP port 22223 (for classic XML logon) or 22226 (for native VDP logon) between the Internet and MBG for SIP XML
- TCP port 22222 (for classic XML logon) or 22225 (for native VDP logon) between MBG and MX-ONE for SIP XML
- TCP port 4431 between the Internet and MBG for Configuration Server Access (Optional)
- TCP port 80 between MBG and the Configuration Server
- UDP port 20000-31000 between the Internet and MBG and between MBG and the LAN for voice
- TCP port 22 between LAN and MBG for secure shell access
- UDP port 53 between MBG and the LAN for DNS resolution to a Corporate DNS server NOTE: Do not enable TCP port 5060 or UDP port 5060 between the Internet and MBG.

MSL Configuration

- 1. Configure your MSL server to use a Corporate DNS server that can resolve any FQDN associated with MX-ONE.
- 2. Configure your MSL server to allow Remote Access for secure shell from a local network. This access will be needed to run a special setup script.
- 3. Navigate to Remote Access under MSL Server Manager.
- 4. Select "Allow access only from trusted and remote management networks" to setup secure shell access.
- 5. Select "Yes" for administrative command line access over secure shell.
- 6. Select "Yes" to allow secure shell access using standard passwords.

MBG Configuration

From a new installation of Release 11.0, access the MiVoice Border Gateway User Interface from MSL server-manager and perform the following steps:

- 1. Go to System Configuration > Network Profile.
 - a. Select Profile and Apply.
- **2.** Go to System Configuration > Settings.
 - a. Enable SIP support for TCP/TLS and TCP.
 - b. Change Codec support to Unrestricted.
 - c. Change Set-side RTP security to Require (to enforce SRTP between the phone and MBG). NOTE: Optionally, you can disable support for all protocols under Minet Support.
- 3. Service Configuration > ICPs
 - a. Add your MX-ONE system as type MiVoice MX-ONE with SIP capabilities as UDP, TCP.
 - **b.** Configure MX-ONE support.
 - c. Check Link to the ICP and Enable.
 - d. Configure the XML listen port as 22223 (for classic XML logon) or 22226 (for native VDP logon) and check TLS.
 - e. Configure the XML destination port as 22222 (for classic XML logon) or 22225 (for native VDP logon) and uncheck TLS.
 - f. Configure the configuration server listen port as 4431 and check TLS.
 - g. Configure the configuration server port as 80 and uncheck TLS.
 - h. Configure the configuration server address.

NOTE: Only provide access to the configuration server if ALL the files in all the directories are encrypted with anacrypt. If not, enter a bogus IP address to not expose the internal configuration server to the Internet. The InGate solution has the same exposure.

- i. Click Save.
- 4. Do not start MBG yet.
- 5. Setup MBG with mutual TLS for SIP using configuration script.
- 6. Connect to the system via ssh (ex: using putty) and login as root.
- 7. Run the configuration script specifying the MBG Public IP address (i.e the address the Teleworker 68xx phones will connect to) and the MBG local or LAN IP address.

Optionally, you can use the script to modify an existing mitel.cfg or use MBG as a TFTP server for the phones. To view all options available, run the configuration script without arguments. [root@mysystem ~]# /usr/sbin/configure 68xx mbg support.sh Example #1: MBG Public IP is 1.1.1.1 and MBG local IP is 192.168.100.10 [root@mysystem ~]# /usr/sbin/configure 68xx mbg support.sh --mbg wan ip ip ad-dress --mbg lan ip ip address --generate certificate [root@mysystem ~]#/usr/sbin/configure 68xx mbg support.sh --mbg wan ip 1.1.1.1 --mbg lan ip 192.168.100.10 --generate certificate mbg wan ip=1.1.1.1 mbg lan ip=192.168.100.10 configure tftp=false generate certificate=true force=false creating /root/aastra tftp, output files will be placed there. configuring mbg certificate with ip address: 1.1.1.1 Generating a 2048 bit RSA private key ++++++ writing new private key to '/root/aastra tftp/mbg mxone key pem' writing RSA key details: InsertCertificateIntoChain Subject: /CN=1.1.1.1 Issuer: /CN=1.1.1.1 ReorderCertificateChain:: client certificate found: Subject: /CN=1.1.1.1 Issuer : /CN=1.1.1.1 ReorderCertificateChain:: root CA certificate found: Subject: /CN=1.1.1.1

lssuer : /CN=1.1.1.1

VerifyCertificateChain:: m_vrCerts.size()=1 rc=1

certificate and key files for set are /root/aastra_tftp/mbg_mxone_cert.pem and /root/aastra_tftp/mbg_mxone_key.pem done.

Example #2:MBG Public IP is 1.1.1.1, MBG local IP is 192.168.100.10, modify an existing mitel.cfg (transferred to /root

[root@mysystem ~]#/usr/sbin/configure 68xx mbg support.sh --mbg wan ip 1.1.1.1 --mbg lan ip 192.168.100.10 --generate certificate --modify cfg template mitel.cfg --ntp server pool.ntp.org --time zone name SE-Stockholm mbg wan ip=1.1.1.1 mbg lan ip=192.168.100.10 configure tftp=true generate certificate=true force=false will configure tftp directory /root/aastra tftp to serve up config files creating /root/aastra tftp, output files will be placed there. configuring mbg certificate with ip address: 1.1.1.1 Generating a 2048 bit RSA private kev++++++ writing new private key to '/root/aastra tftp/mbg mxone key.pem' ____ writing RSA key details: InsertCertificateIntoChain Subject: /CN=1.1.1.1 Issuer : /CN=1.1.1.1 ReorderCertificateChain:: client certificate found: Subject: /CN=1.1.1.1 Issuer : /CN=1.1.1.1 ReorderCertificateChain:: root CA certificate found: Subject: /CN=1.1.1.1 Issuer : /CN=1.1.1.1 VerifyCertificateChain:: m vrCerts.size()=1 rc=1 certificate and key files for set are /root/aastra tftp/mbg mxone cert.pem and /root/mitel tftp/mbg mxone key.pem creating mitel.cfg from template, configured with MBG's CN ip sip proxy ip sip proxy port sip registrar ip sip registrar port sip outbound proxy sip outbound proxy port tftp server sips trusted certificates sips root and intermediate certificates sips local certificate sips private key https validate certificates https user certificates time server disabled time server

time zone name sip transport protocol found URL's pointing to 22222, switching to https and port 22223 appending fixed URLs to config file done.

- 8. Return to the MiVoice Border Gateway User Interface and click on Dashboard to Start MBG
- **9.** Confirm that Teleworker 68xx phones have access to the public IP of MBG using the Teleworker Network Analyzer tool.
- **10.** Download the tool from Administration File Transfer and install it on a Windows machine that has network connectivity to the public IP of your system.
- **11.** Launch the application and run a connect test against the public IP.

SIP TLS, Aastra MXL MX-ONE, Voice Traffic (begin) and (end) should return OK. If any of the above return CLOSED or TIMED OUT, contact your firewall administrator.

Phone Configuration

- 1. Phone must be staged in the office.
- 2. Using WinSCP, copy the /root/aastra_tftp/mbg_mxone_cert.pem and /root/aastra_tftp/mbg_mxone_key.pem to a special folder (ex: athome) on your configuration server.
- 3. Append the settings listed in "Appendix mitel.cfg Settings" to your mitel.cfg file or used the modified mitel.cfg also available under /root/aastra_tftp.

If needed, update all other files (ex: <model.cfg>) to use https/22223 instead of http/22222.

Limitations

A list of known limitations shared with the InGate solution.

- 1. Phones must be staged in the office.
- 2. Phone firmware must be done in the office as a phone firmware upgrade will remove the certificate loaded.
- 3. Access to internal configuration server cannot be limited/controlled/blocked from the outside.
- 4. 68xxi must have access to a NTP server for certificate validation.
- 5. Corporate directory access must be setup with port forwarding on MSL (server-gateway configuration) or the DMZ firewall.
- 6. If MX-ONE is setup to like lim1.mysystem.com, the MSL server must point to a Corporate DNS to allow proper DNS resolution.

Here is a list of known limitations with MBG

- a. Single dedicated MBG.
- b. MBG clustering and backup SIP registrar/proxy in the 68xxi configuration files.
- c. Using FQDN instead of IP address in the 68xxi configuration files.

- 7. Music On Idle is not supported.
- 8. MiCollab Meetings Center application which is accessed through the meetings softkey is not supported.

Known Issues

None.

Upgrade Notes

Trials sites that have deployed based on earlier versions of this document, need to run the following command on their system to ensure that all required files are part of a backup.

[root@mysystem ~]# db tug setprop config backuplist /etc/tug/tug.ini.certifi-cates.ini,/etc/tug/tugcerts.ini,/etc/tug/ca-bundle.crt,/etc/tug/mbg_mxone.ini

Appendix - Config Script

Usage: /usr/sbin/configure_68xx_mbg_support.sh --mbg_wan_ip ip_address --mbg_lan_ip ip_address [--tftp] [--generate_certificate] [--force] [--modify_cfg_tem-plate aastra_cfg_file_template] [--ntp_server fqdn/ip] [--time_zone_name aastra_name_string]

--mbg_wan_ip - MBG public address

sets connect to this address and MBG certificate will contain this

--mbg_lan_ip - MBG private address

used for SIP udp and tcp communications with ICP

(udp and tcp are disabled on MBG's public address)

--tftp - configure this MBG to supply configuration files via tftp

--generate_certificate - create a certificate using the value supplied for 'mbg_wan_ip'

--force - override 'certificate already exists' check

--modify_cfg_template - If set, specified file will be modified.
Cfg settings dealing with certs/sip will be adjusted
--ntp_server - If set, specified fqdn will be used for ntp settings.
otherwise 'pool.ntp.org' will be used.
--time_zone_name - If set, specified time zone string will be used for ntp settings.
otherwise 'SE-Stockholm' will be used.

Appendix - mitel.cfg Settings

#-----# MiVoice Border Gateway (MBG) Teleworker features
SIP TLS and SRTP between the phone and MBG
HTTPS used for XML
#------

MBG is the SIP proxy and registrar sip proxy ip:MBGIP sip proxy port:5061 sip registrar ip:MBGIP sip registrar port:5061 sip outbound proxy:MBGIP sip outbound proxy port:5061 #5061 or 0(which will attempt SRV and as fall back send to 5061 due to TLS)

Persistent SIP TLS (requires 'sip outbound proxy')
sips persistent tls:1
sip outbound support:1
sip transport protocol:4 #4-TLS

Certificates/keys for sip-tls sips trusted certificates: mbg_mxone_cert.pem sips root and intermediate certificates: mbg_mxone_cert.pem sips local certificate: mbg_mxone_cert.pem sips private key: mbg_mxone_key.pem https validate certificates: 1 https user certificates: mbg_mxone_cert.pem # Voice Encryption (SRTP) sip srtp mode:2

OPTIONAL – Use MBG's TFTP server #tftp server:MBGIP

#NTP server must be accessible from the home network time server disabled: 0 Time server1:<NTP server>

Action URI must use HTTPS to port 22223
action uri startup:https://\$\$PROXYURL\$\$:22223/Startup?user=\$\$SIPUSERNAME\$\$
services script: https://\$\$PROXYURL\$\$:22223/Services?user=\$\$SIPUSER-NAME\$\$&voicemailnr=
#------

NOTE: Similar changes may be required to <model>.cfg or <mac>.cfg files.



© Copyright 2021, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation, including itself and subsidiaries and authorized entities. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.