MiVoice MX-ONE

Optional Installations

Release 7.3 SP2

June 8, 2021

Mitel®

Notice

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

Trademarks

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

Contents

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:

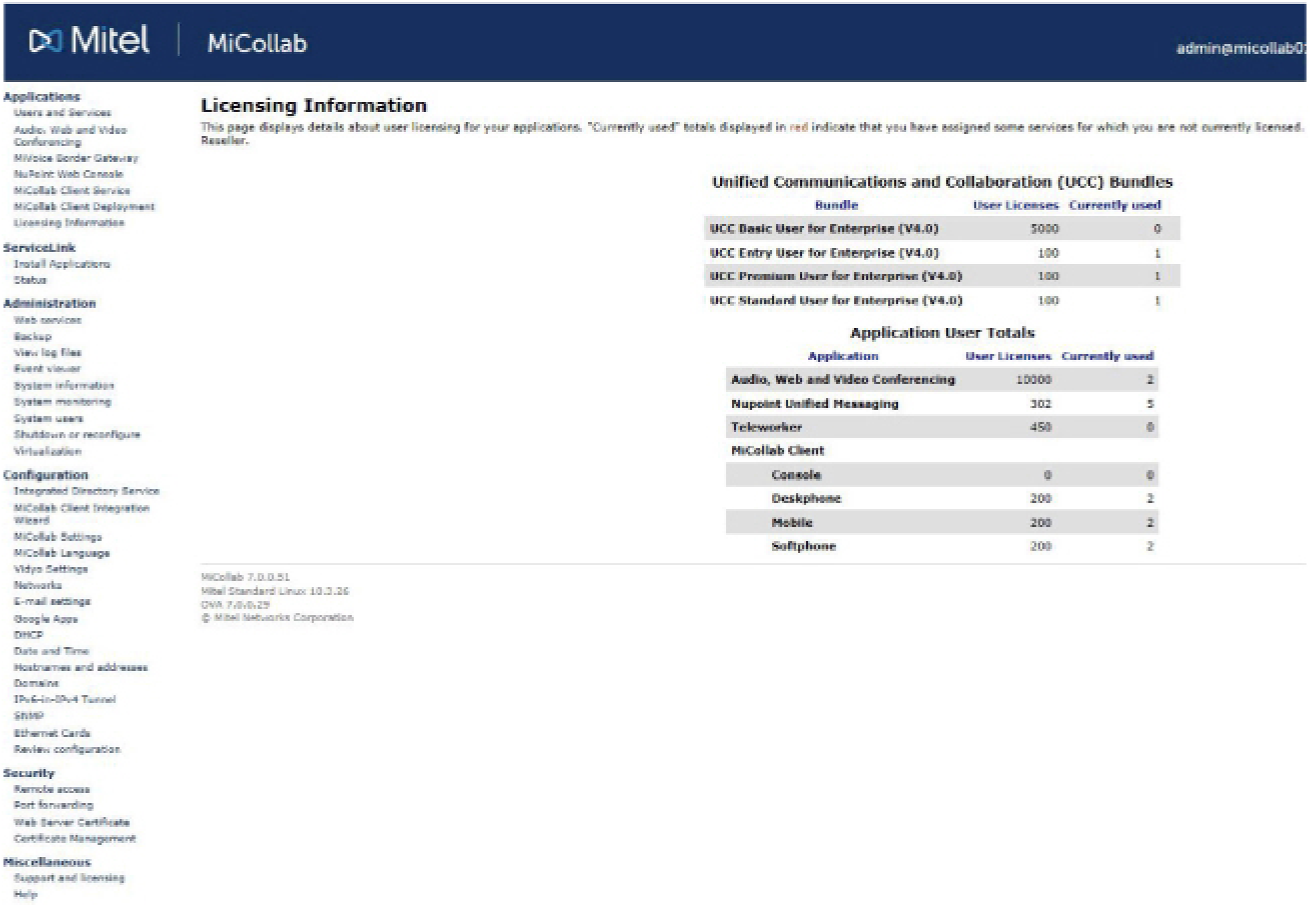
1. Start the virtual machine.
2. Open the console interface.
3. Choose keyboard.
4. Restore from backup - no.

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



Licensing Information

This page displays details about user licensing for your applications. "Currently used" totals displayed in red indicate that you have assigned some services for which you are not currently licensed. Reseller.

Unified Communications and Collaboration (UCC) Bundles

Bundle	User Licenses	Currently used
UCC Basic User for Enterprise (V4.0)	5000	0
UCC Entry User for Enterprise (V4.0)	100	1
UCC Premium User for Enterprise (V4.0)	100	1
UCC Standard User for Enterprise (V4.0)	100	1

Application User Totals

Application	User Licenses	Currently used
Audio, Web and Video Conferencing	10000	2
Nupoint Unified Messaging	302	5
Teleworker	450	0
MiCollab Client		
Console	0	0
Deskphone	200	2
Mobile	200	2
Softphone	200	2

MiCollab 7.0.0.51
Mitel Standard Linux 10.3.26
OVA 7.0.0.29
© Mitel Networks Corporation

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.

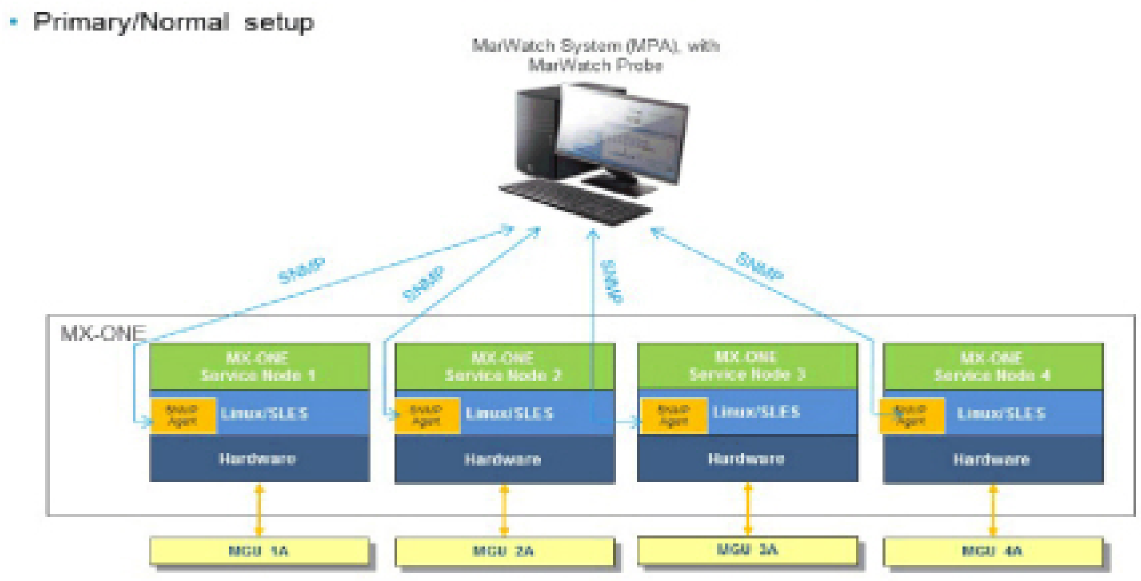
Supported Scenarios

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

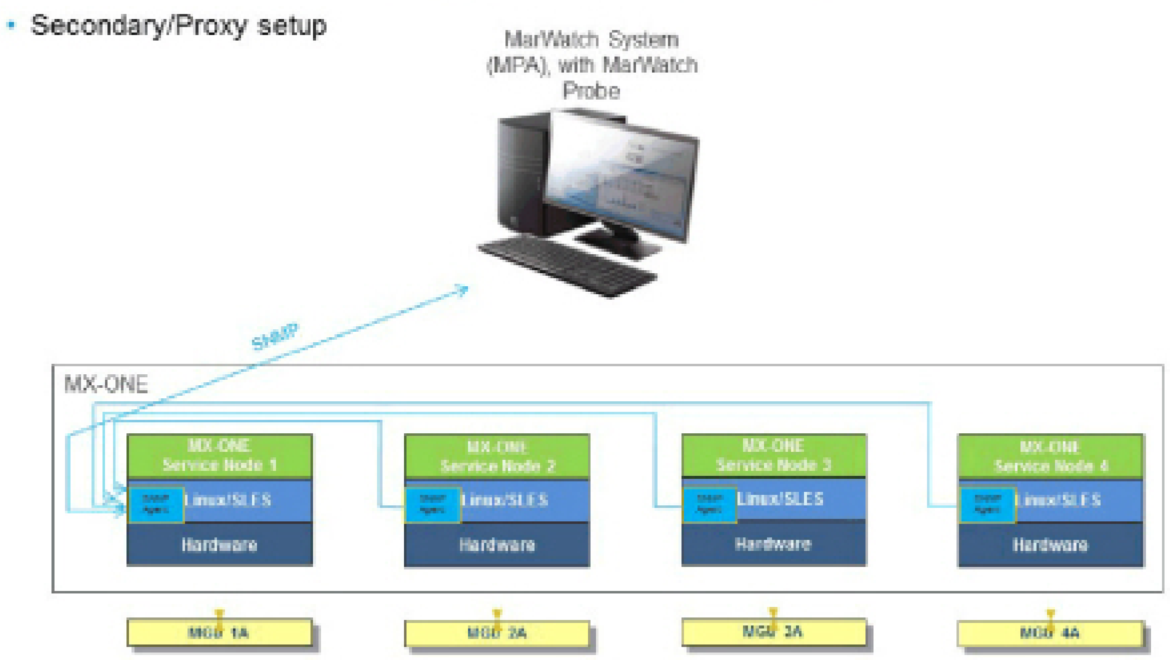


Another possibility is that one Service Node can act as a proxy for several other Service Nodes (and other entities), in which case only the proxy Service Node will be connected to the MPA probe.

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.microsoft.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.

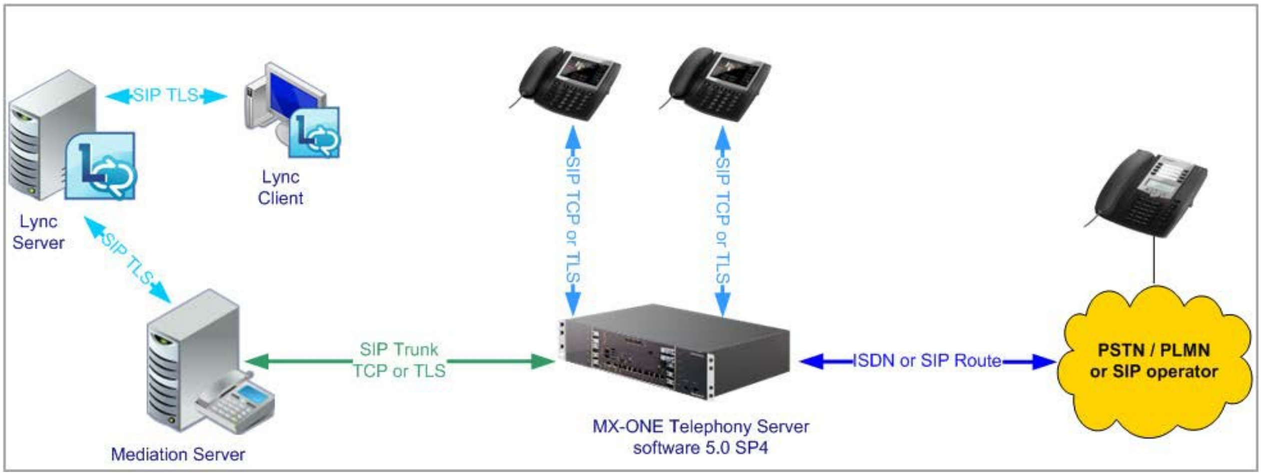
Scope

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 integration 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.



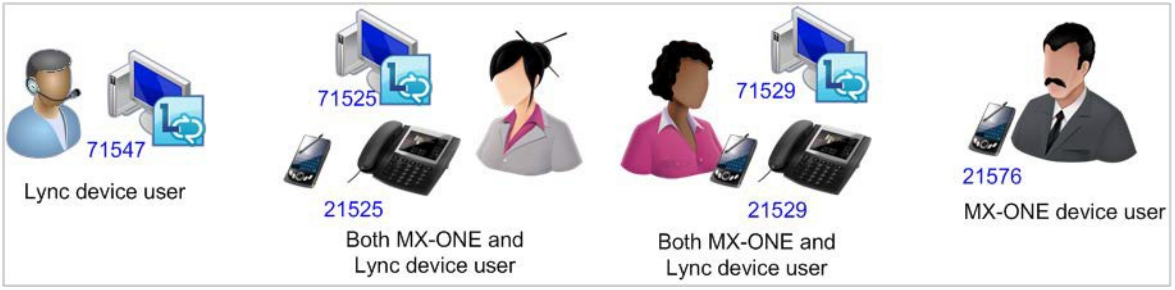
This guide covers only the components that are required in the integration between MX-ONE 5.0 SP4 or a later version, and Skype for Business Server 2019 via Direct SIP to offer the functionality required by the Microsoft UC Open Interoperability Program for enterprise telephony services and infrastructure.

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.


71547
Lync device user
71525
21525
Both MX-ONE and Lync device user
71529
21529
Both MX-ONE and Lync device user
21576
MX-ONE device user

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

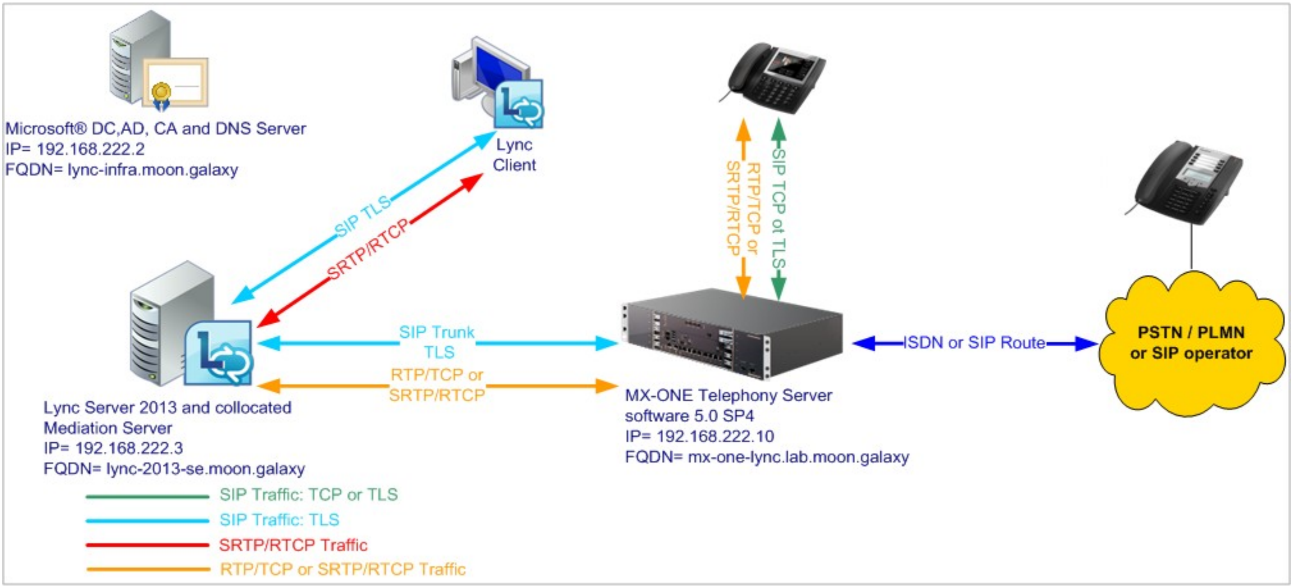
  TCP is used as transport protocol; the listening port is 5068.
- Lync_TLS_SRTP. TCP is used as transport protocol; the listening port is 5067. SRTP is used to encrypt the media; it uses RTP/SAVP.

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=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=001100;

3. Define SIP Route data:

   RODAI:ROU=99,TYPE=TL66,VARC=00000000,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 99 –short

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

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

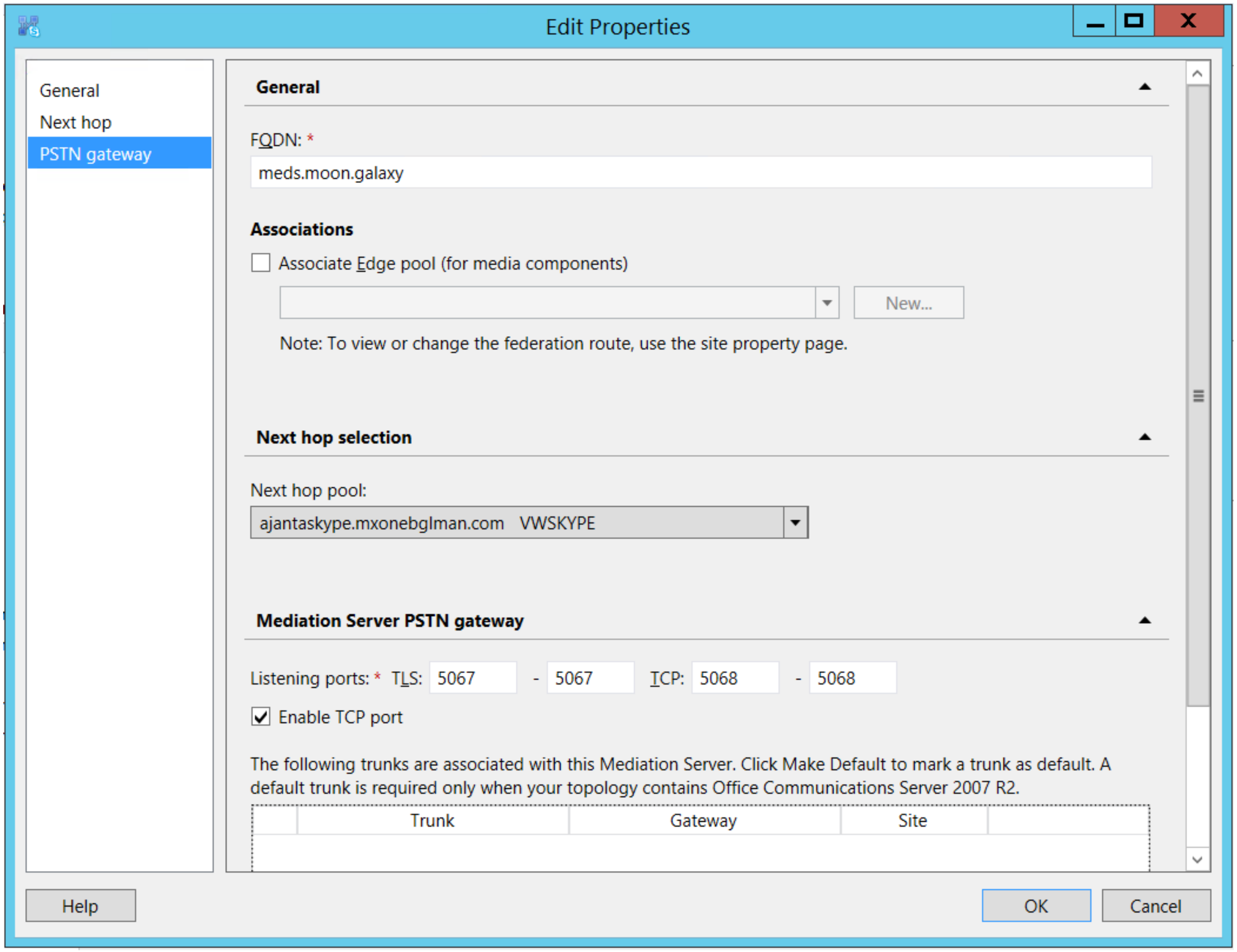
7. Define external destination SIP Route data:

   RODDI:ROU=99,DEST=99,ADC=0005000000000250000001010000,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).



General

FQDN: * meds.moon.galaxy

Associations

☐ Associate Edge pool (for media components)

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 - 5067 TCP: 5068 - 5068

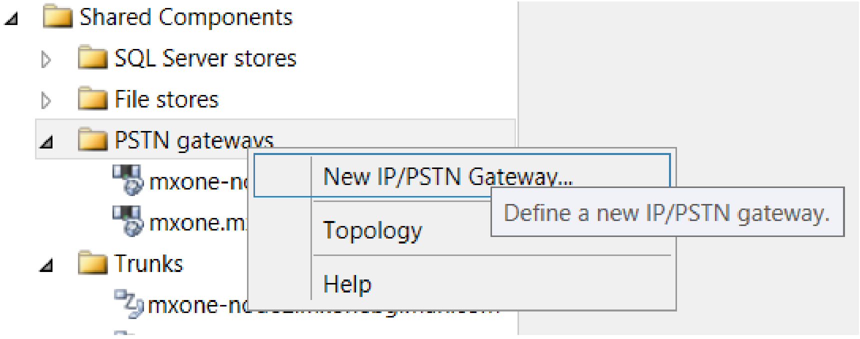
☑ Enable TCP port

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.

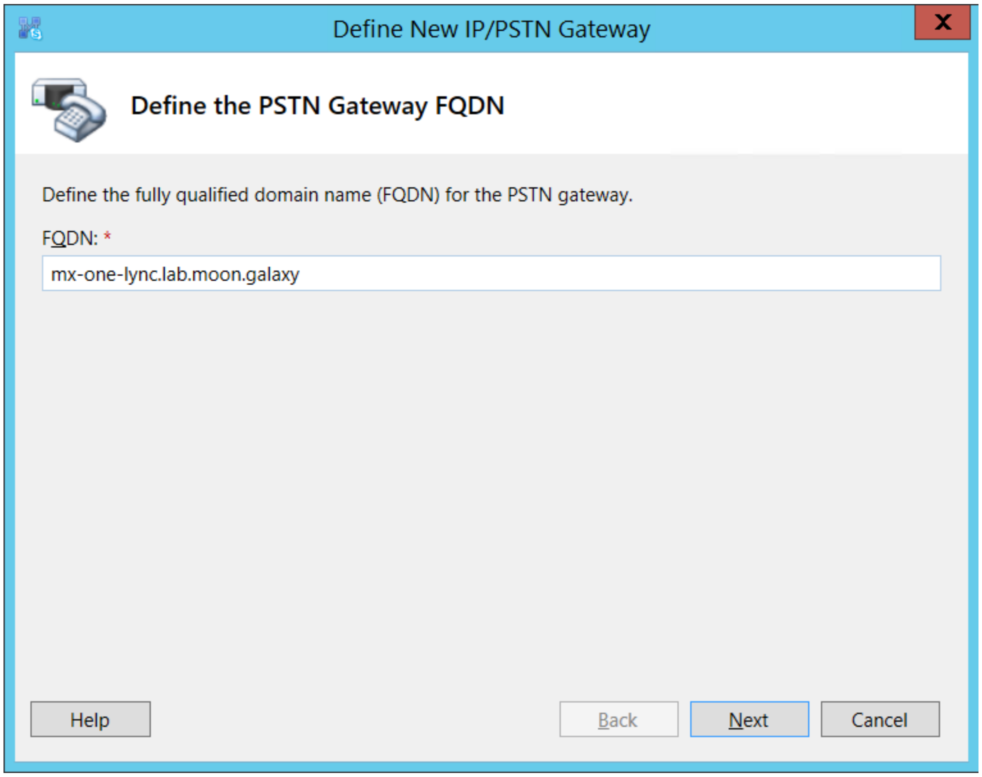
	Trunk	Gateway	Site	

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.



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

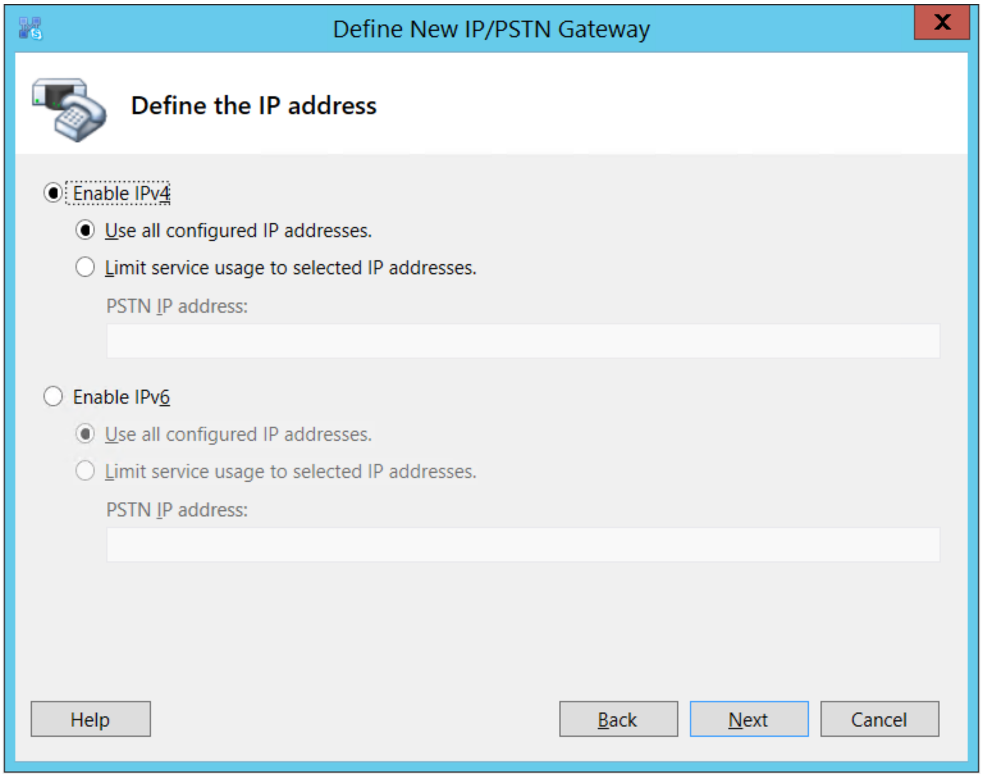
Define the PSTN Gateway FQDN

Define the fully qualified domain name (FQDN) for the PSTN gateway.

FQDN: *

mx-one-lync.lab.moon.galaxy

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



Define New IP/PSTN Gateway

Define the IP address

● Enable IPv4

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

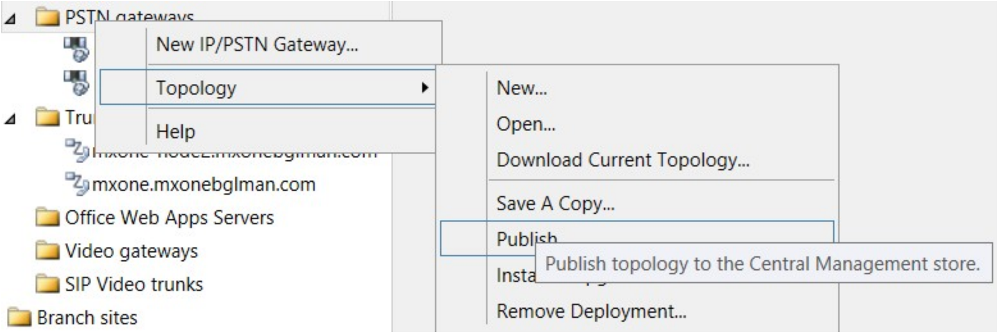
○ Enable IPv6

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

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**.



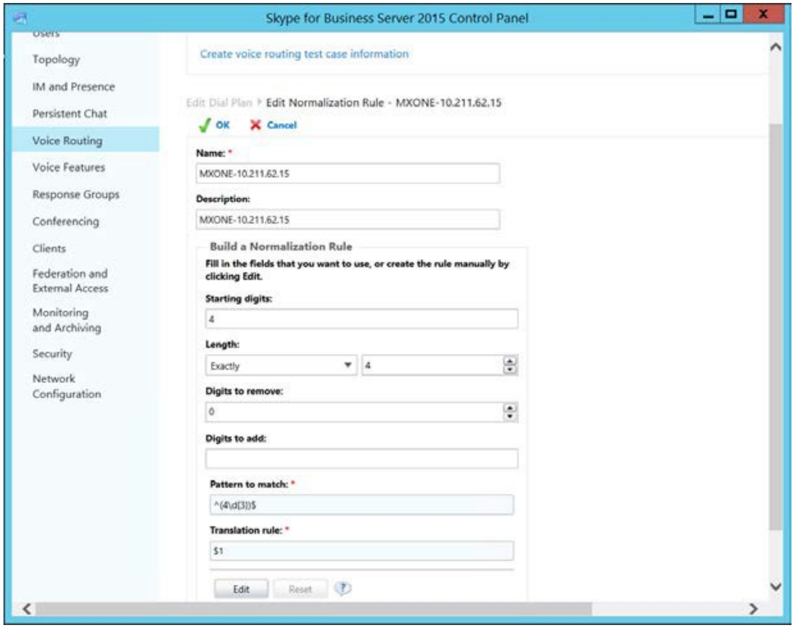
Define a Dial Plan

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**.
3. 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.

Figure 3.1: New Normalization Rule, five digits example



Edit Normalization Rule - MXONE-10.211.62.15

Name: * MXONE-10.211.62.15

Description: MXONE-10.211.62.15

Build a Normalization Rule

Fill in the fields that you want to use, or create the rule manually by clicking Edit.

Starting digits: 4

Length: Exactly 4

Digits to remove: 0

Digits to add:

Pattern to match: * ^(4\d{3})$

Translation rule: * $1

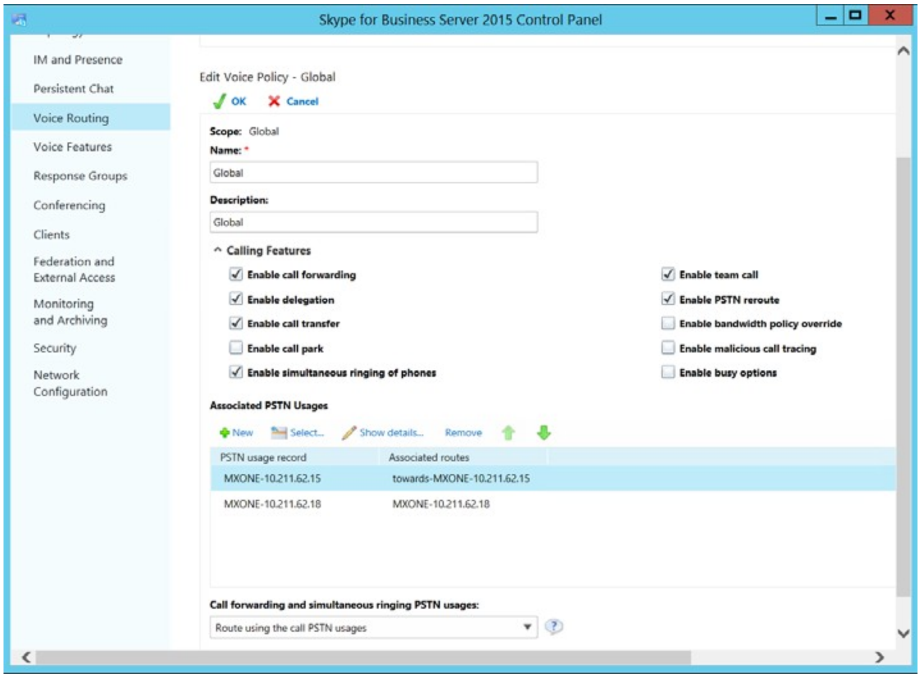
4. Commit the changes.

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.



Edit Voice Policy - Global

Scope: Global

Name: *

Global

Description:

Global

Calling Features

☑ Enable call forwarding

☑ Enable delegation

☑ Enable call transfer

□ Enable call park

☑ Enable simultaneous ringing of phones

☑ Enable team call

☑ Enable PSTN reroute

□ Enable bandwidth policy override

□ Enable malicious call tracing

□ Enable busy options

Associated PSTN Usages

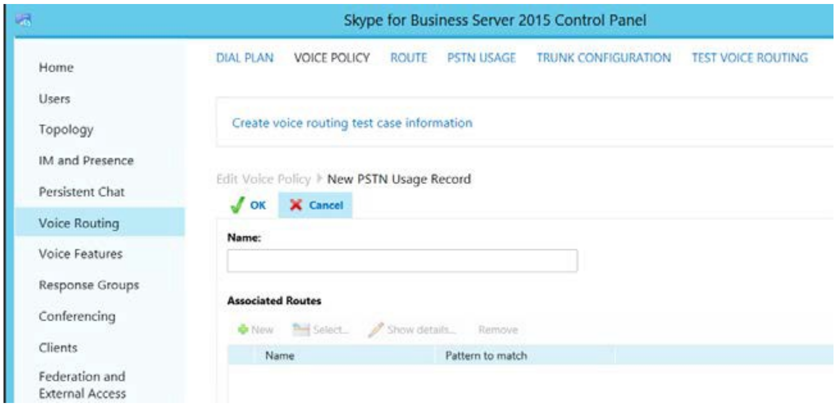
PSTN usage record	Associated routes
MXONE-10.211.62.15	towards-MXONE-10.211.62.15
MXONE-10.211.62.18	MXONE-10.211.62.18

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**



Edit Voice Policy ▸ New PSTN Usage Record

Name:

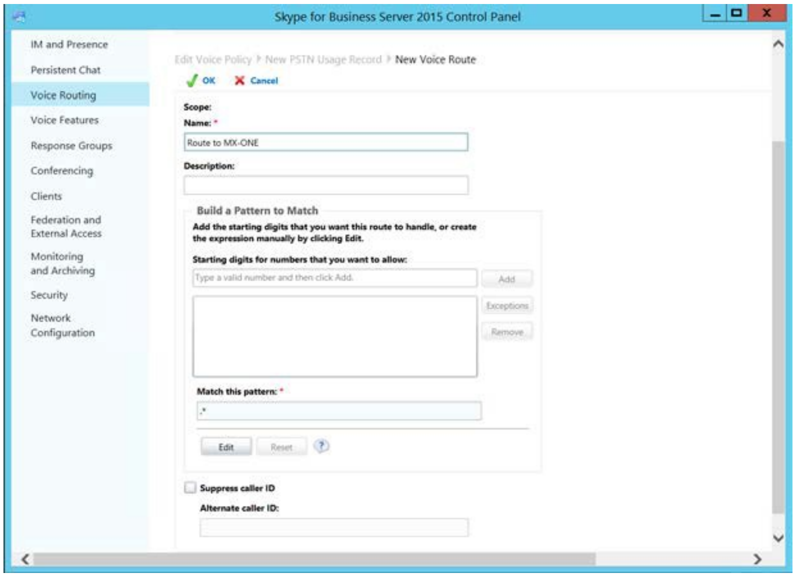
Associated Routes

Name	Pattern to match

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**.



Scope:

Name: * Route to MX-ONE

Description:

Build a Pattern to Match

Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.

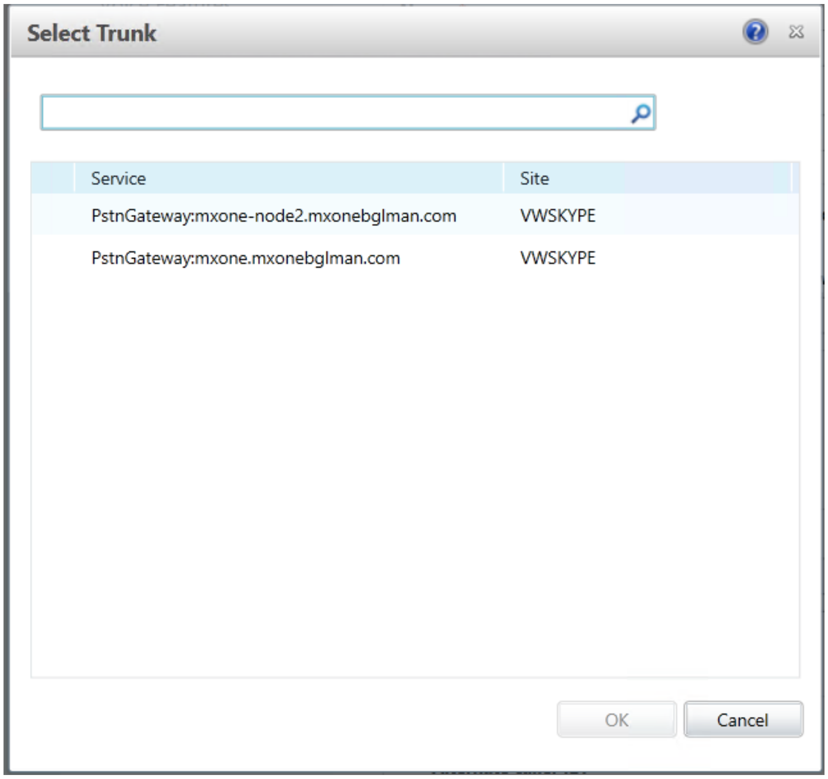
Starting digits for numbers that you want to allow: Type a valid number and then click Add.

Match this pattern: * .*

□ 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.

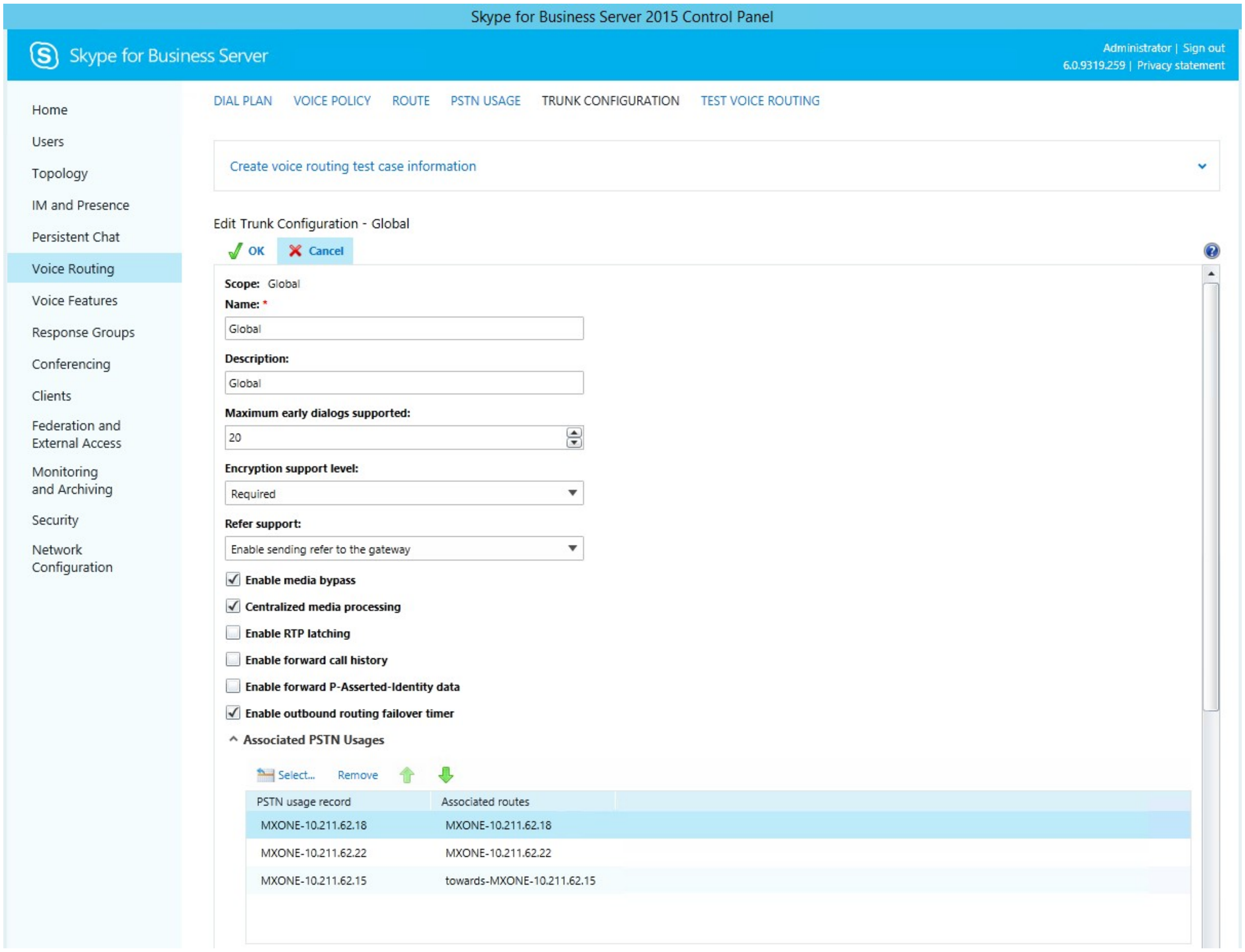


Service	Site
PstnGateway:mxone-node2.mxonebglman.com	VWSKYPE
PstnGateway:mxone.mxonebglman.com	VWSKYPE

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.



Edit Trunk Configuration - Global

Scope: Global

Name: * Global

Description: Global

Maximum early dialogs supported: 20

Encryption support level: Required

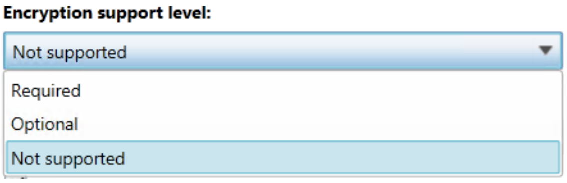
Refer support: Enable sending refer to the gateway

☑ Enable media bypass
☑ Centralized media processing
☐ Enable RTP latching
☐ Enable forward call history
☐ Enable forward P-Asserted-Identity data
☑ Enable outbound routing failover timer

Associated PSTN Usages

PSTN usage record	Associated routes
MXONE-10.211.62.18	MXONE-10.211.62.18
MXONE-10.211.62.22	MXONE-10.211.62.22
MXONE-10.211.62.15	towards-MXONE-10.211.62.15

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



Encryption support level: Not supported

4. Commit all changes to complete the setup.

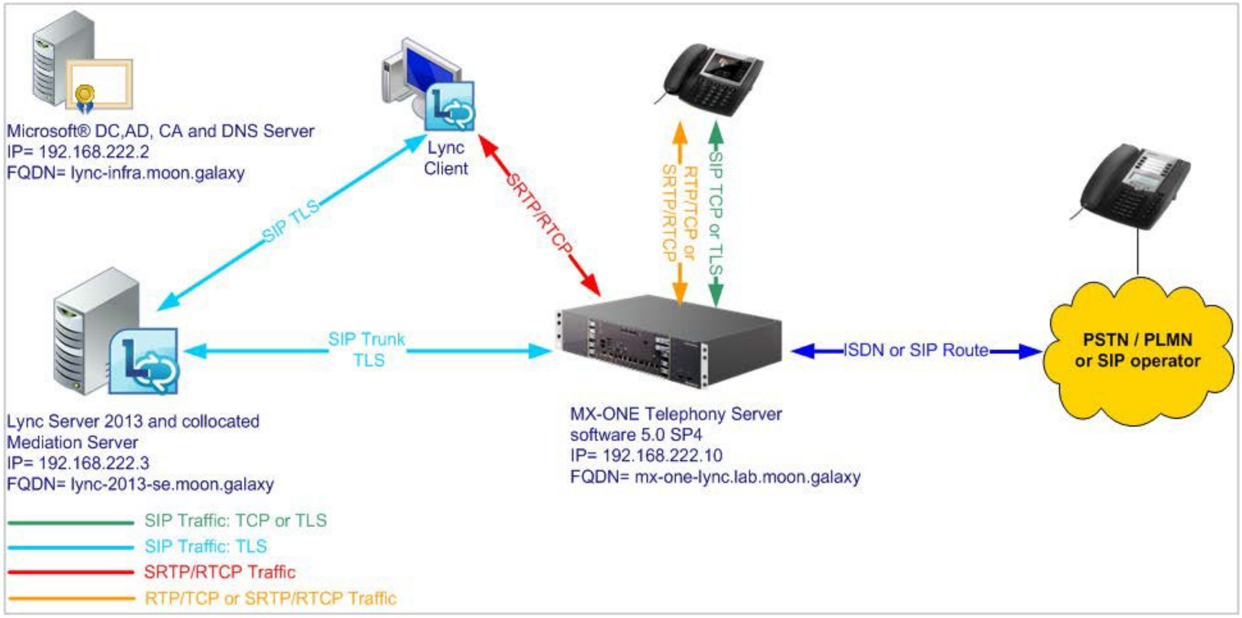
Conclusion

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=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=001100;
3. Define SIP Route data:

   RODA I:ROU=98,TYPE=TL66,VARC=00000000,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:

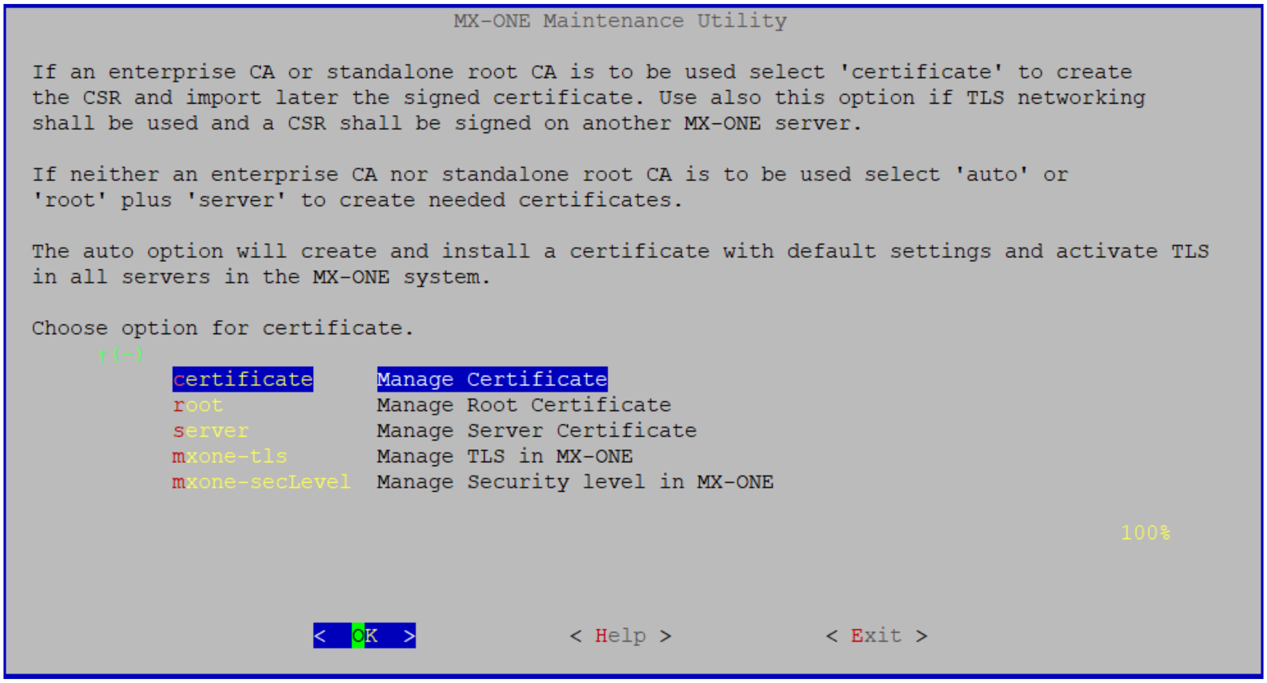
   sip_route -print –route 98 -short
6. Define the SIP Route equipment initiate: ROEQI:ROU=98,TRU=1-1;
7. Define external destination SIP Route data:

   RODDI:ROU=98,DEST=98,ADC=0005000000000250000001010000,SRT=3;

Import the Certificate to MX-ONE Service Node

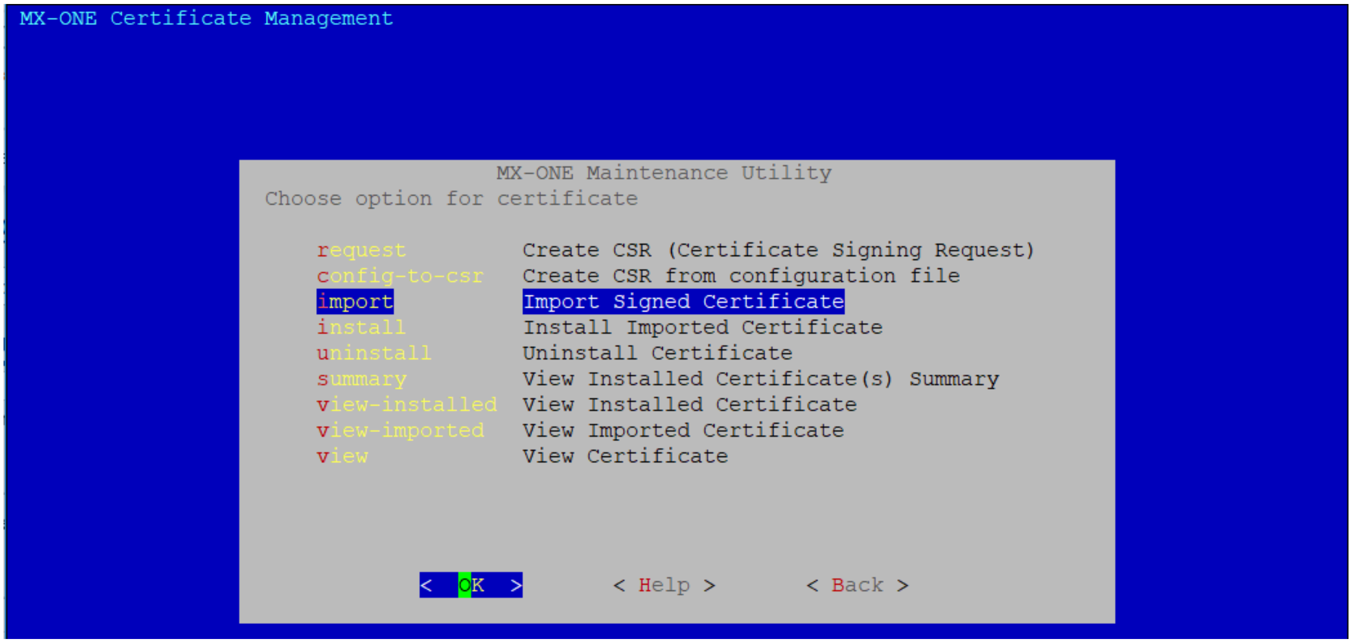
Import the server certificate mx-one-certificate.pfx to MX-ONE Service Node.

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.



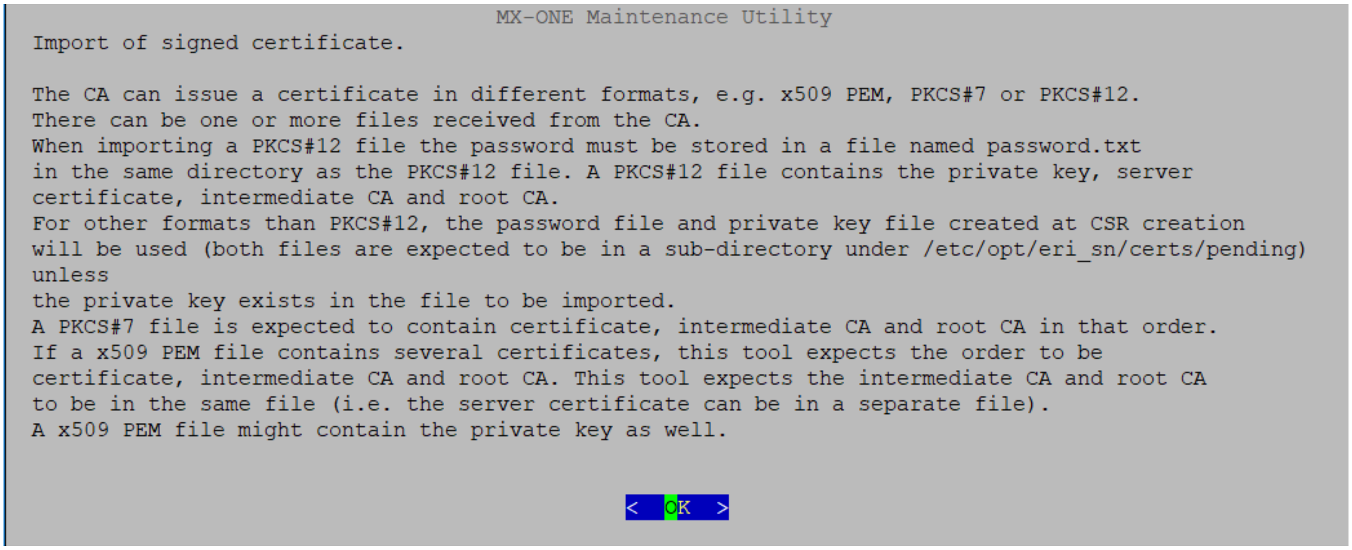
```
                              MX-ONE Maintenance Utility

  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     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%


                       <  OK  >            < Help >            < Exit >
```

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



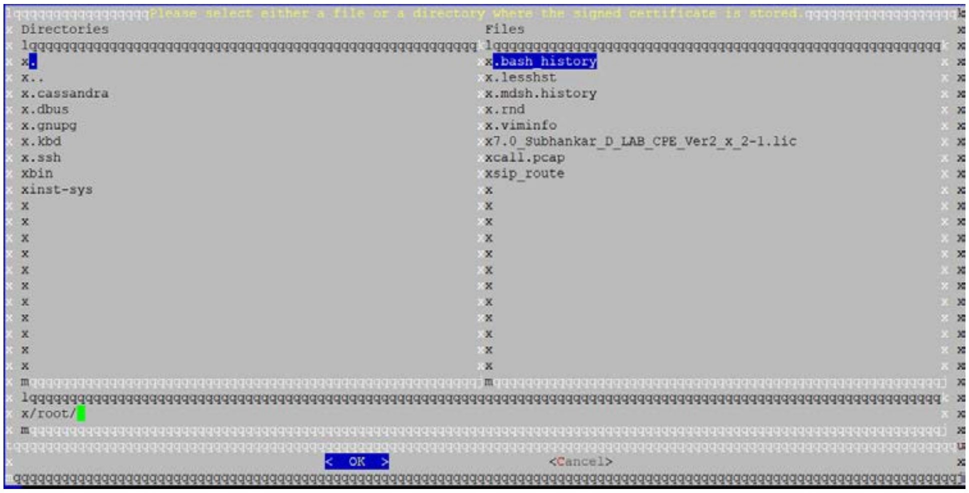
```
MX-ONE Certificate Management

                    MX-ONE Maintenance Utility
  Choose option for certificate

      request           Create CSR (Certificate Signing Request)
      config-to-csr     Create CSR from configuration file
      import            Import Signed Certificate
      install           Install Imported Certificate
      uninstall         Uninstall Certificate
      summary           View Installed Certificate(s) Summary
      view-installed    View Installed Certificate
      view-imported     View Imported Certificate
      view              View Certificate

              <  OK  >        < Help >        < Back >
```

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



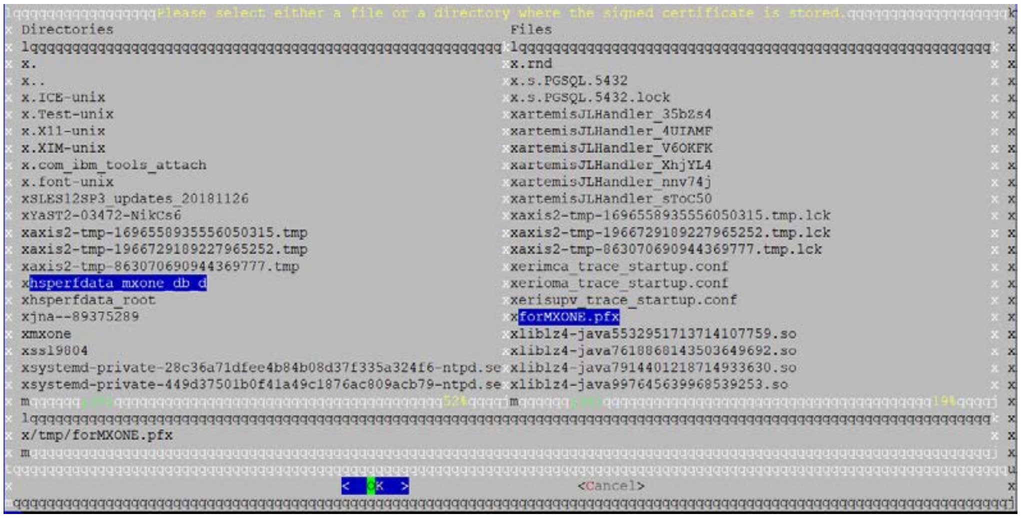
```
                                MX-ONE Maintenance Utility
 Import of signed certificate.

 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.

                                      <  OK  >
```

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



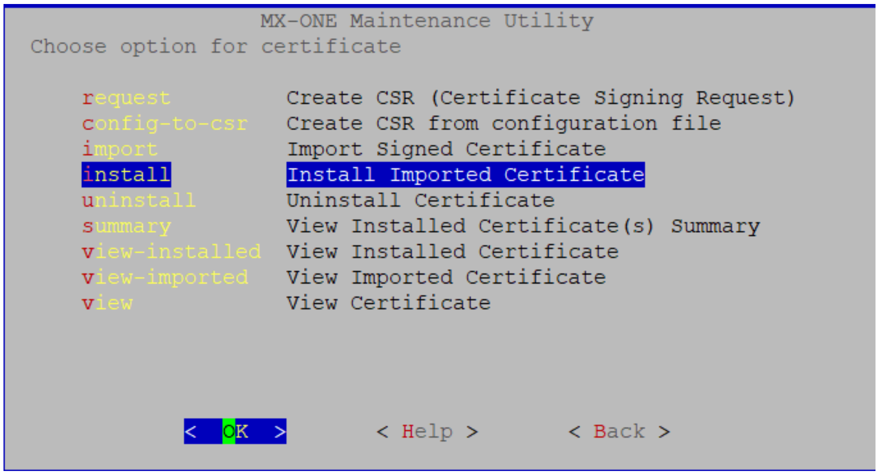
```
Please select either a file or a directory where the signed certificate is stored.
 Directories                                             Files
 x.                                                      x.bash_history
 x..                                                     x.lesshst
 x.cassandra                                             x.mdsh.history
 x.dbus                                                  x.rnd
 x.gnupg                                                 x.viminfo
 x.kbd                                                   x7.0_Subhankar_D_LAB_CPE_Ver2_x_2-1.lic
 x.ssh                                                   xcall.pcap
 xbin                                                    xsip_route
 xinst-sys
 x/root/
                              < OK >                     <Cancel>
```

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

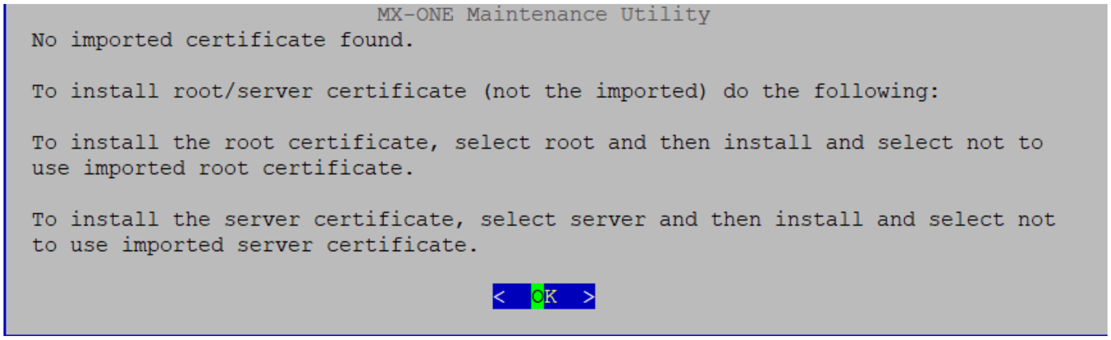


```
Please select either a file or a directory where the signed certificate is stored.
 Directories                                             Files
 x.                                                      x.rnd
 x..                                                     x.s.PGSQL.5432
 x.ICE-unix                                              x.s.PGSQL.5432.lock
 x.Test-unix                                             xartemisJLHandler_35bZs4
 x.X11-unix                                              xartemisJLHandler_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-1966729189227965252.tmp.lck
 xaxis2-tmp-1966729189227965252.tmp                      xaxis2-tmp-8630706909443697777.tmp.lck
 xaxis2-tmp-8630706909443697777.tmp                      xerimca_trace_startup.conf
 xhsperfdata_mxone_db_d                                  xerioma_trace_startup.conf
 xhsperfdata_root                                        xerisupv_trace_startup.conf
 xjna--89375289                                          xforMXONE.pfx
 xmxone                                                  xliblz4-java5532951713714107759.so
 xss19804                                                xliblz4-java7618868143503649692.so
 xsystemd-private-28c36a71dfee4b84b08d37f335a324f6-ntpd.se xliblz4-java7914401218714933630.so
 xsystemd-private-449d37501b0f41a49c1876ac809acb79-ntpd.se xliblz4-java9976456399685392 53.so
 x/tmp/forMXONE.pfx
                              < OK >                     <Cancel>
```

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



```
                 MX-ONE Maintenance Utility
  Choose option for certificate

      request         Create CSR (Certificate Signing Request)
      config-to-csr   Create CSR from configuration file
      import          Import Signed Certificate
      install         Install Imported Certificate
      uninstall       Uninstall Certificate
      summary         View Installed Certificate(s) Summary
      view-installed  View Installed Certificate
      view-imported   View Imported Certificate
      view            View Certificate

              < OK >       < Help >       < Back >
```



```
                    MX-ONE Maintenance Utility
No imported certificate found.

To install root/server certificate (not the imported) do the following:

To install the root certificate, select root and then install and select not to
use imported root certificate.

To install the server certificate, select server and then install and select not
to use imported server certificate.

                          <  OK  >
```

8. 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:

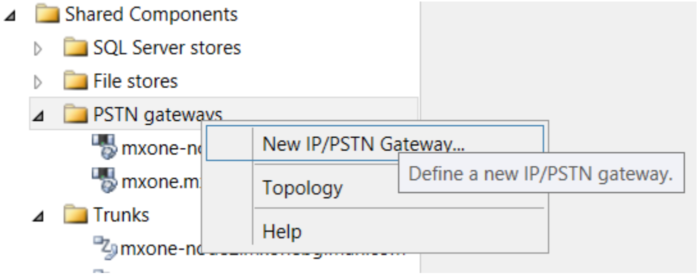
   media_encryption_enable -type route
   media_encryption_enable -type extension
   media_encryption_enable -type intermgw
   media_encryption_print

Lync Configuration with Security and Media Bypass Setup

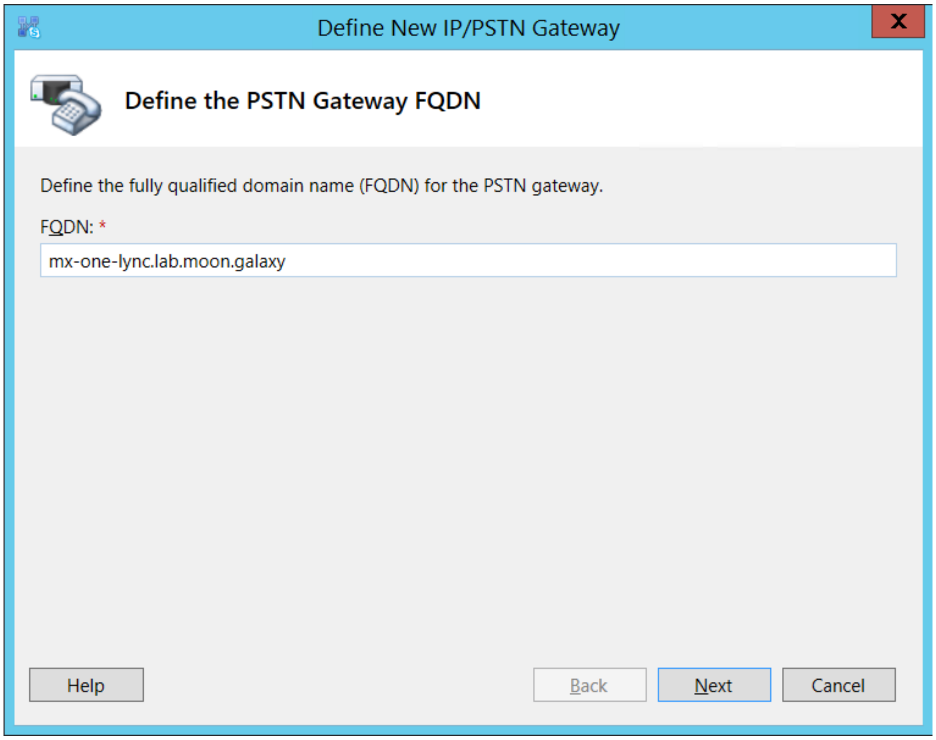
You must do the following to finalize the configuration between Mitel MX-ONE and Skype for Business Server 2019 the following needs to be done:

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.



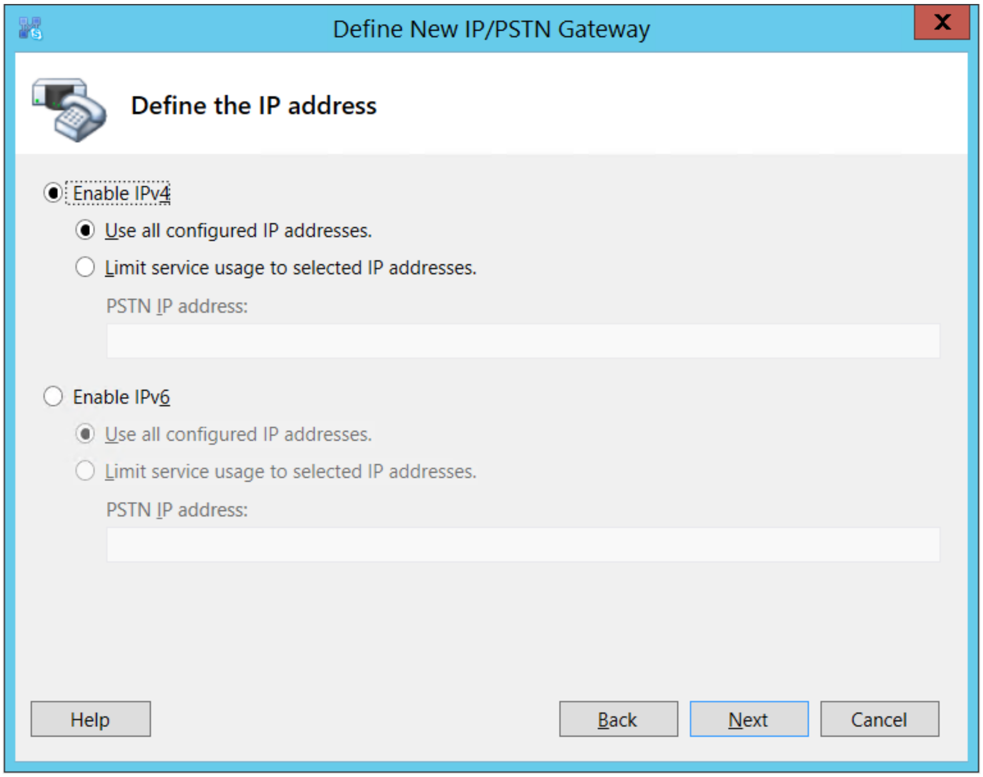
Define New IP/PSTN Gateway

Define the PSTN Gateway FQDN

Define the fully qualified domain name (FQDN) for the PSTN gateway.

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

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**.



Define New IP/PSTN Gateway

Define the IP address

● Enable IPv4

● Use all configured IP addresses.

○ Limit service usage to selected IP addresses.

PSTN IP address:

○ Enable IPv6

● Use all configured IP addresses.

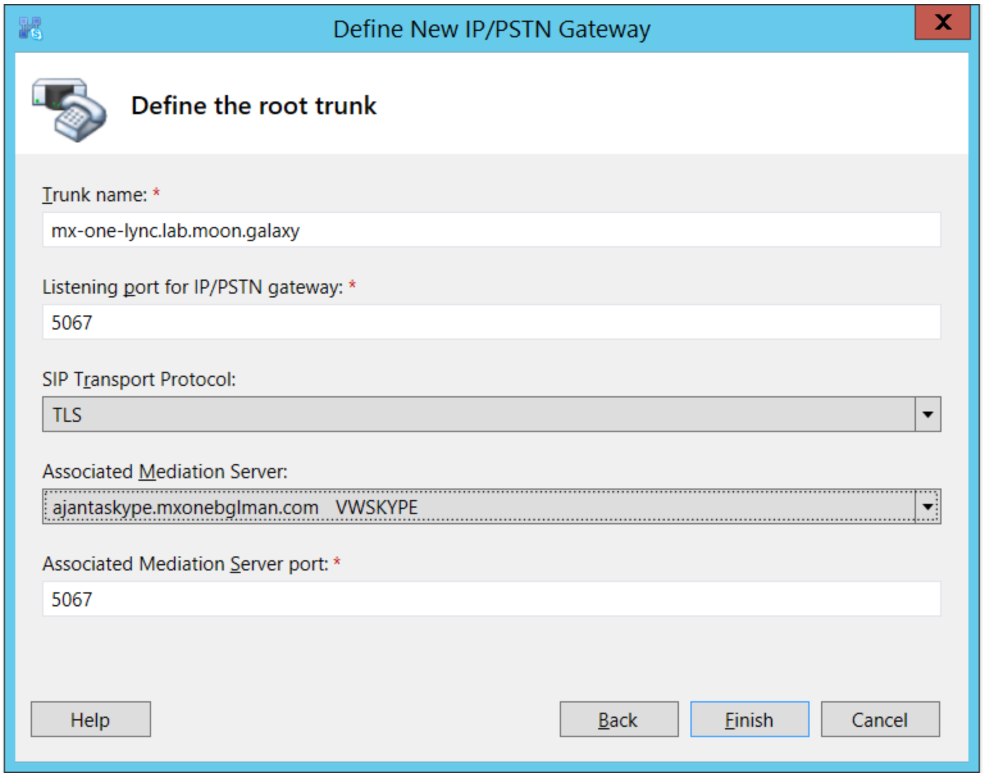
○ Limit service usage to selected IP addresses.

PSTN IP address:

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

Define the root trunk

Trunk name: *
mx-one-lync.lab.moon.galaxy

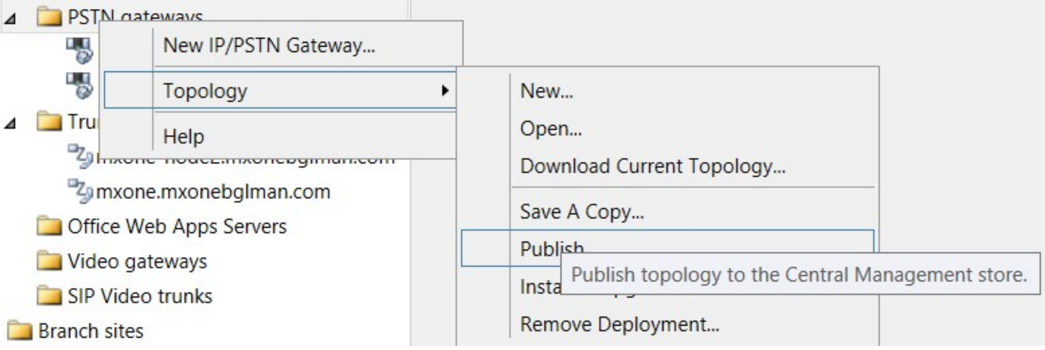
Listening port for IP/PSTN gateway: *
5067

SIP Transport Protocol:
TLS

Associated Mediation Server:
ajantaskype.mxonebglman.com VWSKYPE

Associated Mediation Server port: *
5067

8. Publish the **Topology**



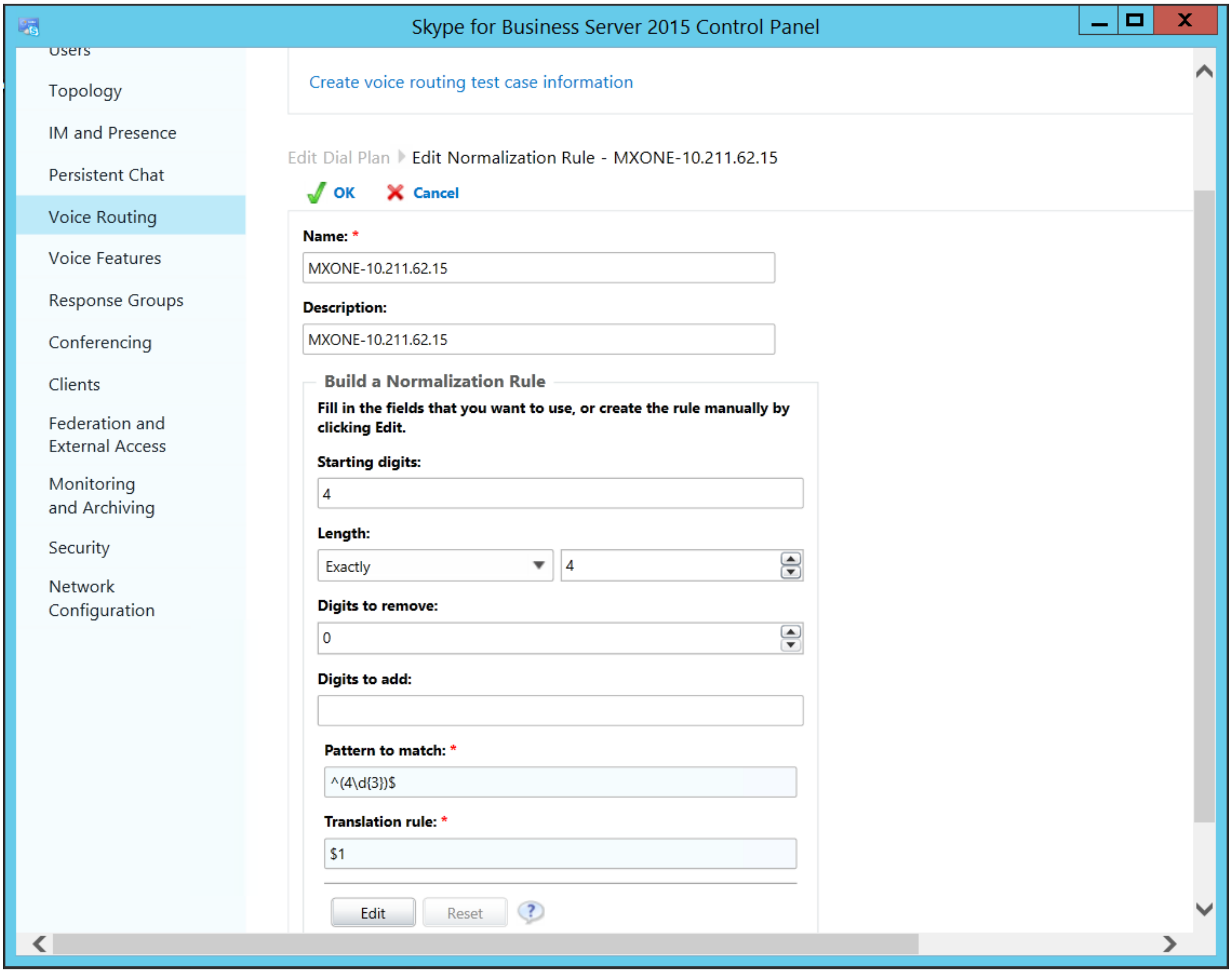
Define Dial Plan and Voice Policy

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**.



Edit Normalization Rule - MXONE-10.211.62.15

Name: * MXONE-10.211.62.15

Description: MXONE-10.211.62.15

Build a Normalization Rule

Fill in the fields that you want to use, or create the rule manually by clicking Edit.

Starting digits: 4

Length: Exactly 4

Digits to remove: 0

Digits to add:

Pattern to match: * ^(4\d{3})$

Translation rule: * $1

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

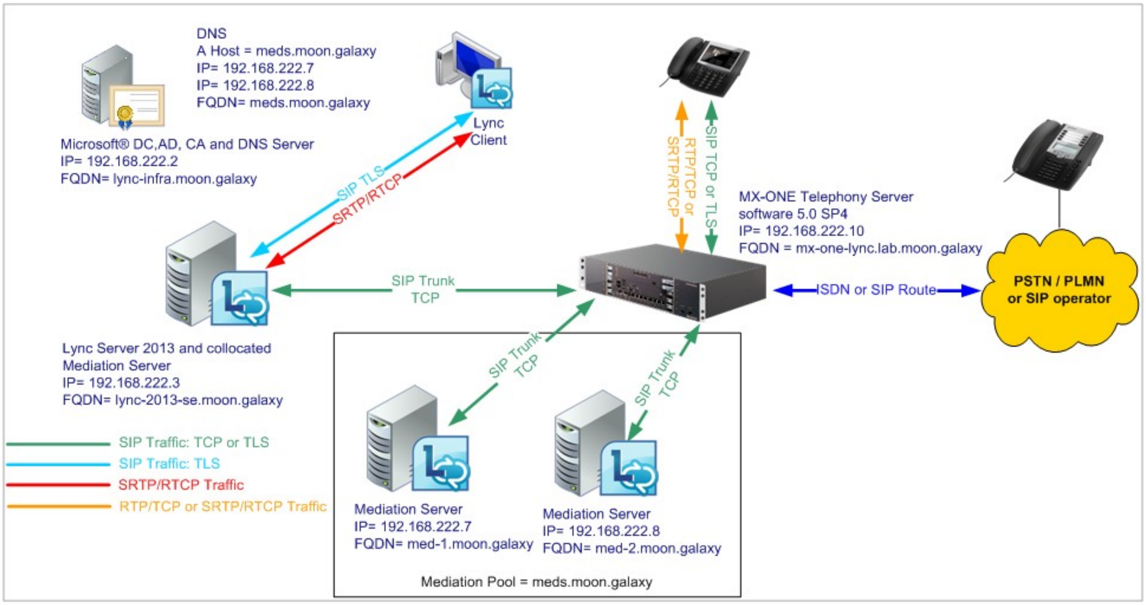
The failover feature also uses the Microsoft DNS Load Balancing functionality. When integrating MX-ONE and Mediation Server, the same configuration is valid for both failover and load balancing.

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.



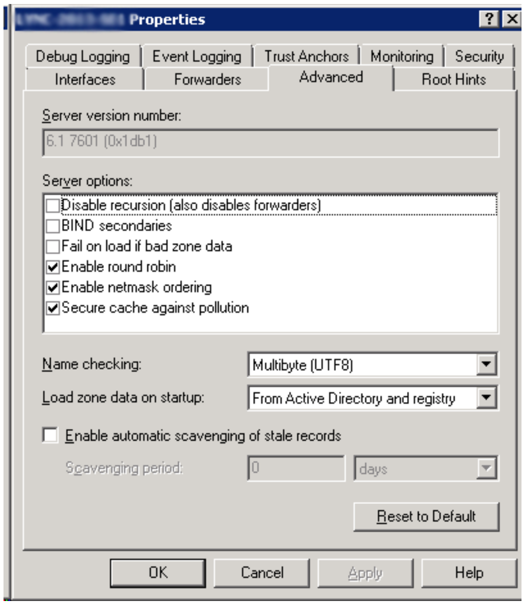
For this scenario, two standalone Mediation servers are used. In the MX-ONE side, only one MX-ONE Service Node is used, and it is configured with the Mediation Pool entry.

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.



Server version number: 6.1 7601 (0x1db1)

Server options:

- ☐ Disable recursion (also disables forwarders)
- ☐ BIND secondaries
- ☐ Fail on load if bad zone data
- ☑ Enable round robin
- ☑ Enable netmask ordering
- ☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

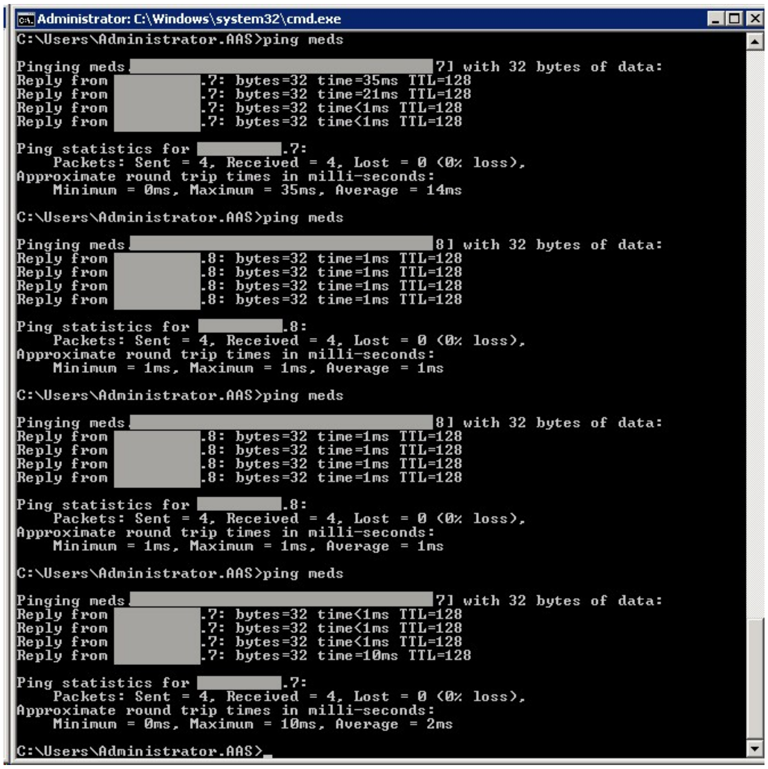
DNS Multiple A record setup – Mediation Servers

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.microsoft.com/en-us/library/gg398593.

FQDN	TYPE	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.



```
C:\Users\Administrator.AAS>ping meds

Pinging meds.[redacted]7] with 32 bytes of data:
Reply from [redacted].7: bytes=32 time=35ms TTL=128
Reply from .7: bytes=32 time=21ms TTL=128
Reply from .7: bytes=32 time<1ms TTL=128
Reply from .7: bytes=32 time<1ms TTL=128

Ping statistics for [redacted].7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 35ms, Average = 14ms

C:\Users\Administrator.AAS>ping meds

Pinging meds.[redacted]8] with 32 bytes of data:
Reply from [redacted].8: bytes=32 time=1ms TTL=128
Reply from .8: bytes=32 time=1ms TTL=128
Reply from .8: bytes=32 time=1ms TTL=128
Reply from .8: bytes=32 time=1ms TTL=128

Ping statistics for [redacted].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.[redacted]8] with 32 bytes of data:
Reply from [redacted].8: bytes=32 time=1ms TTL=128
Reply from .8: bytes=32 time=1ms TTL=128
Reply from .8: bytes=32 time=1ms TTL=128
Reply from .8: bytes=32 time=1ms TTL=128

Ping statistics for [redacted].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.[redacted]7] with 32 bytes of data:
Reply from [redacted].7: bytes=32 time<1ms TTL=128
Reply from .7: bytes=32 time<1ms TTL=128
Reply from .7: bytes=32 time<1ms TTL=128
Reply from .7: bytes=32 time=10ms TTL=128

Ping statistics for [redacted].7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

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=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4,SERV=31000000 01,BCAP=00110;
3. Define SIP Route data:

   RODAI:ROU=97,TYPE=TL66,VARC=00000000,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:

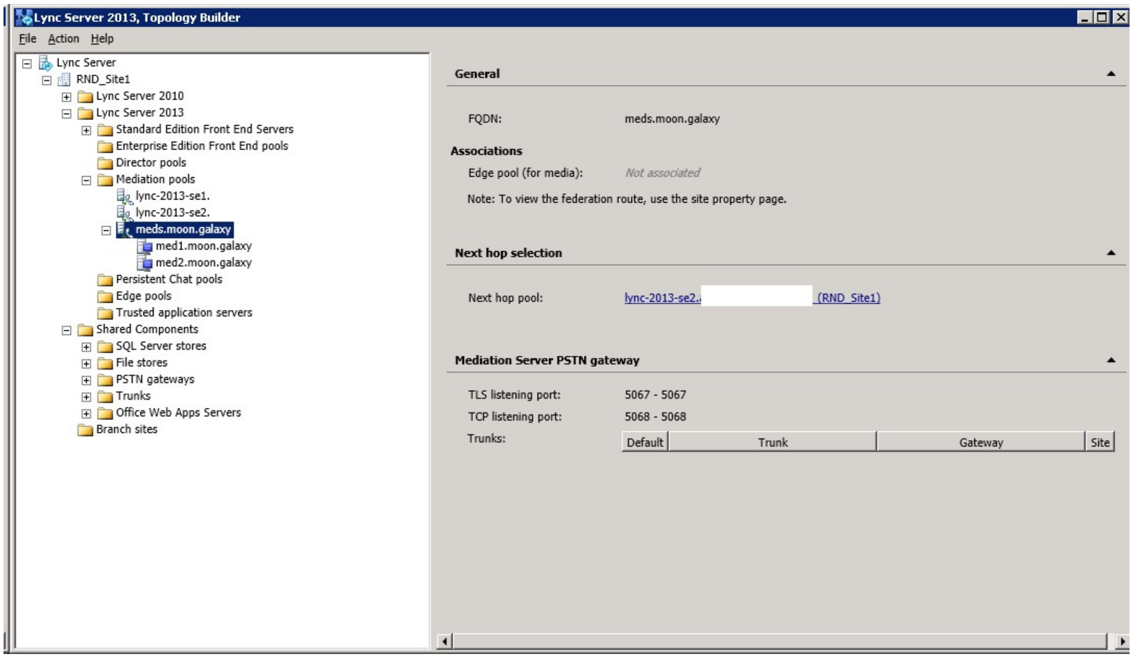
RODDI:ROU=97,DEST=97,ADC=0005000000000250000001010000,SRT=3;

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



- Lync Server
  - RND_Site1
    - Lync Server 2010
    - Lync Server 2013
      - Standard Edition Front End Servers
      - Enterprise Edition Front End pools
      - Director pools
      - Mediation pools
        - lync-2013-se1.
        - lync-2013-se2.
        - meds.moon.galaxy
          - med1.moon.galaxy
          - med2.moon.galaxy
      - Persistent Chat pools
      - Edge pools
      - Trusted application servers
    - Shared Components
      - SQL Server stores
      - File stores
      - PSTN gateways
      - Trunks
      - Office Web Apps Servers
    - Branch sites

General

FQDN: meds.moon.galaxy

Associations

Edge pool (for media): *Not associated*

Note: To view the federation route, use the site property page.

Next hop selection

Next hop pool: lync-2013-se2.[redacted] (RND_Site1)

Mediation Server PSTN gateway

TLS listening port: 5067 - 5067

TCP listening port: 5068 - 5068

Trunks:

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=7110000000000010,SIG=0111110000A0,TRAF=03151515,TRM=4, SERV=3100000001,BCAP=00110;
3. Define SIP Route data:

   RODAI: ROU=96,TYPE=TL66,VARC=00000000,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=0005000000000250000001010000,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

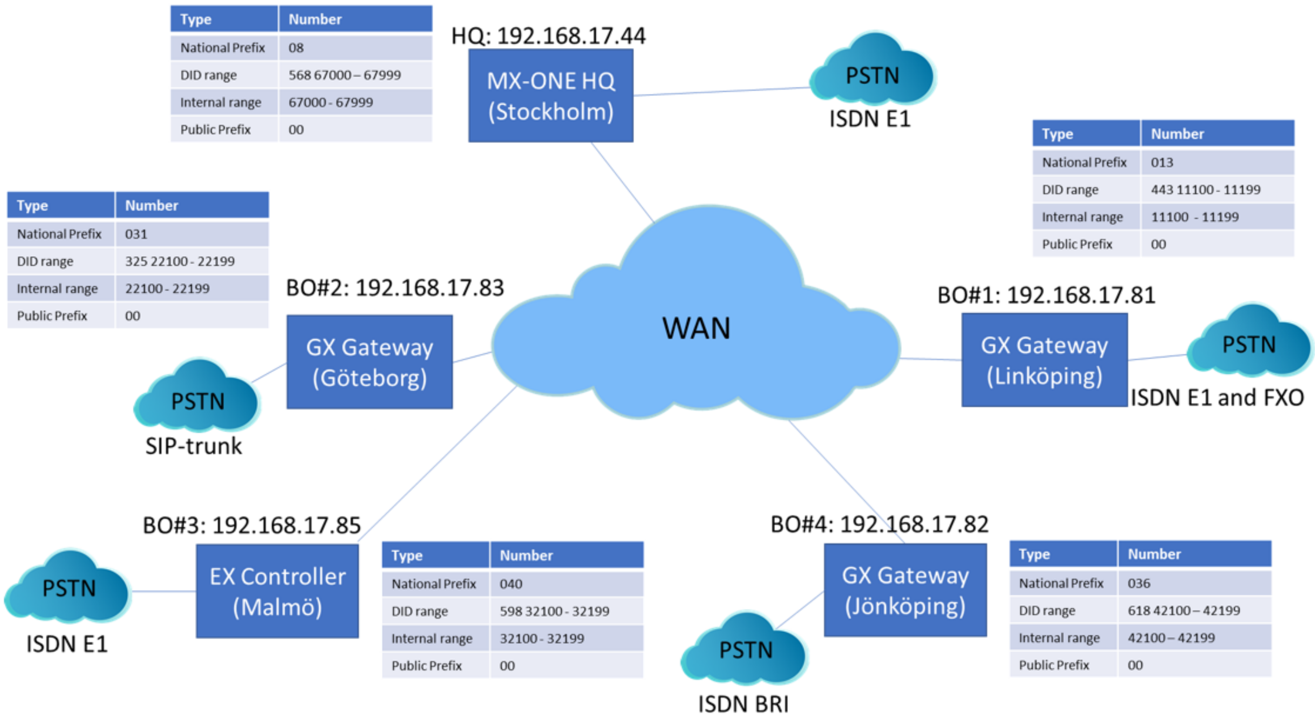
DOCUMENT VERSION	COMMENTT	DATE
A	First release	2015-11-19
B	Minor corrections	2014-03-28
C	Updated with Mitel template	2015-06-08
D	Updated in 4.2.3.7, cert_install_local replaced by mxone_certificate. MX-ONE version information also corrected.	2015-10-27
D3	Spelling correction	2017-04-05
D4	2013 old 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



Type	Number
National Prefix	08
DID range	568 67000 – 67999
Internal range	67000 - 67999
Public Prefix	00

Type	Number
National Prefix	013
DID range	443 11100 - 11199
Internal range	11100 - 11199
Public Prefix	00

Type	Number
National Prefix	031
DID range	325 22100 - 22199
Internal range	22100 - 22199
Public Prefix	00

Type	Number
National Prefix	040
DID range	598 32100 - 32199
Internal range	32100 - 32199
Public Prefix	00

Type	Number
National Prefix	036
DID range	618 42100 – 42199
Internal range	42100 – 42199
Public Prefix	00

Prerequisites

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

- The extension range must be coherent and matching the local DID number series (if local presence is used).
- MX-ONE SW must be at least version 7.0.

- The firmware level of the EX-Controller and GX-Gateway shall be at least **DGW 42.3.1032-MT** with profile 'S100-MT-D2000-45' for GX-Gateway and 'STNL-MT-D2000-65' for EX-Controller.

Other considerations/restrictions:

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

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

Upgrading Firmware In A GX-Gateway / EX-Controller

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

Firmware Upgrade

Firmware upgrade can be performed with several options:

Following are the two types of licenses:

- FTP
- TFTP
- HTTP
- HTTPS

Setup of Communication Server

- **FTP**

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

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

- **TFTP**

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

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

- **HTTP Server**

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

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

- **HTTPS Server**

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

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

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

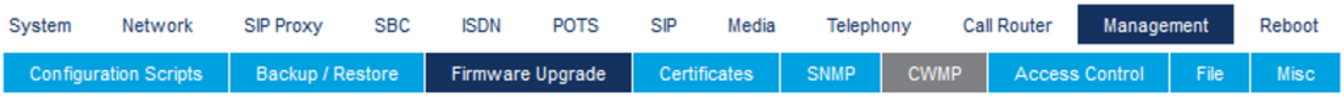
Copy the firmware program (.bin file), to the file server you have chosen to use (FTP, HTTPS, TFTP, or HTTP server).

Firmware Installation

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

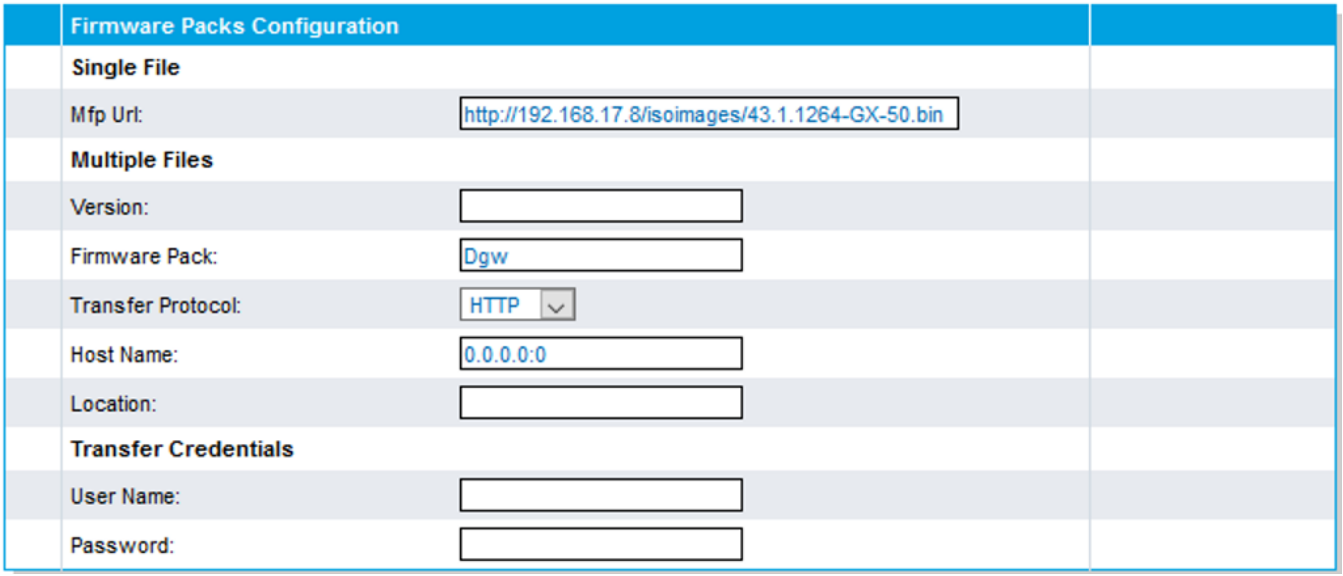
1. Go to **Management** > **Firmware Upgrade**.

Figure 4.2: Firmware Upgrade



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

Figure 4.3: Firmware Packs Configuration



Firmware Packs Configuration	
Single File	
Mfp Url:	http://192.168.17.8/isoimages/43.1.1264-GX-50.bin
Multiple Files	
Version:	
Firmware Pack:	Dgw
Transfer Protocol:	HTTP
Host Name:	0.0.0.0:0
Location:	
Transfer Credentials	
User Name:	
Password:	

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

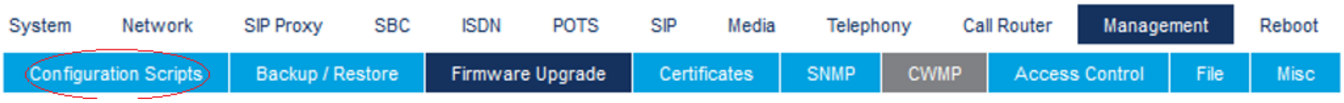
Special Actions for Firmware Upgrade of EX-Controller

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

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

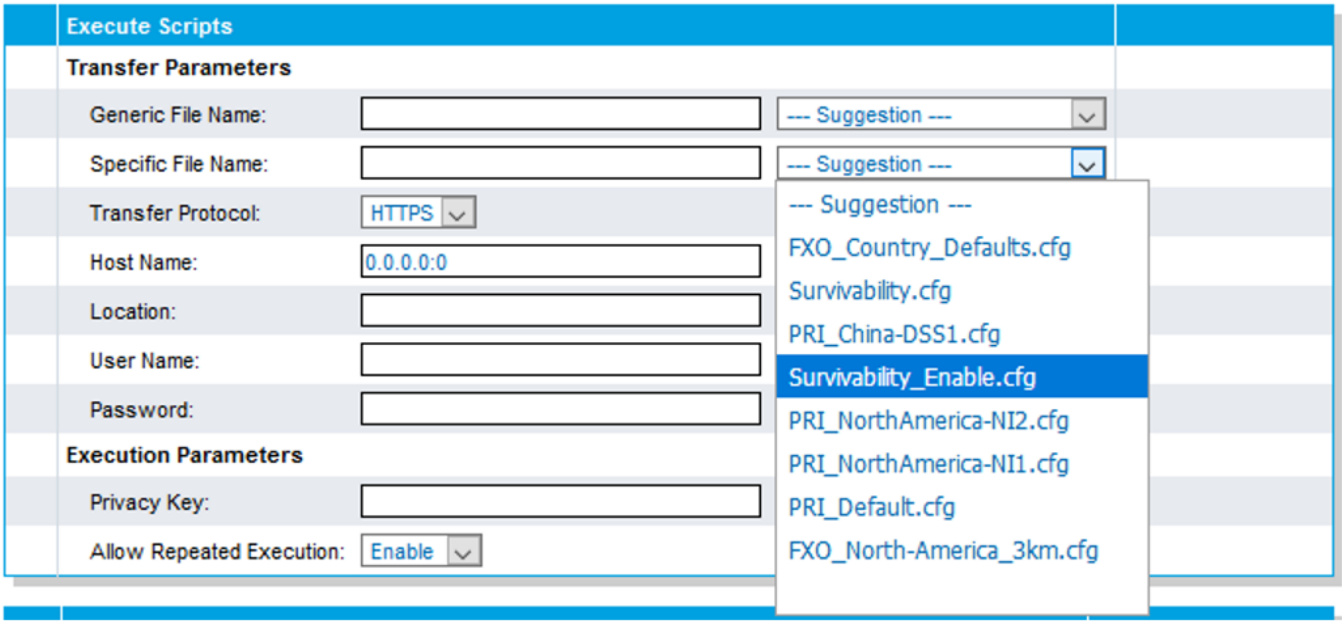
When the new firmware is started a special script file must be executed to setup the SBC and SIP functionality.

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



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

Figure 4.4: Execute Scripts



Execute Scripts

Transfer Parameters

Generic File Name:		--- Suggestion ---
Specific File Name:		--- Suggestion ---
Transfer Protocol:	HTTPS	
Host Name:	0.0.0.0:0	
Location:		
User Name:		
Password:		

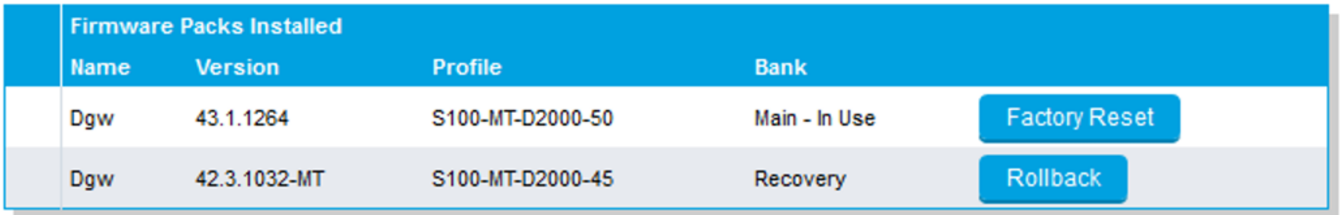
Execution Parameters

Privacy Key:	
Allow Repeated Execution:	Enable

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

Rollback to Previous Firmware

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



Firmware Packs Installed

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

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

Setting up Virtual Machine in an EX-Controller

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

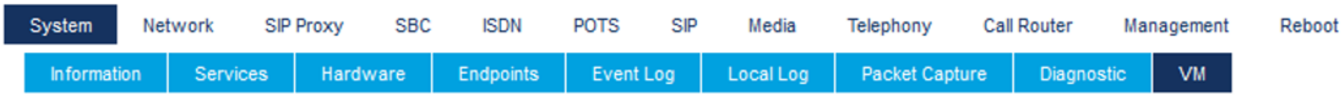
Install and Configure Virtual Machine

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

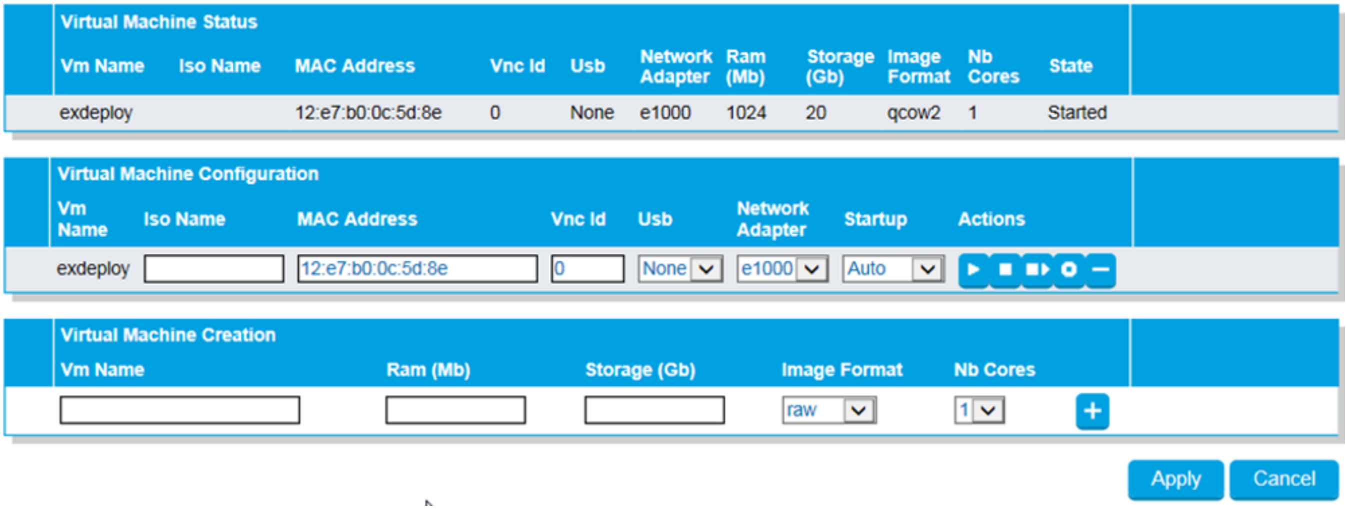
- Upload an ISO-image to internal file storage.
- Use an ISO-image on a bootable USB stick.

Prerequisites

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



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



Virtual Machine Status

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

Virtual Machine Configuration

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
exdeploy		12:e7:b0:0c:5d:8e	0	None	e1000	Auto	▶ ■ ■▶ ● −

Virtual Machine Creation

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

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

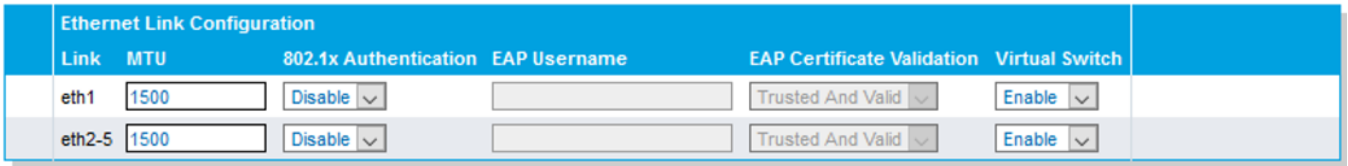
Virtual Machines

4. Click the Plus (+) to create the virtual machine.

5. Configure a link as a virtual switch.

6. Go to **Network** > **Interfaces**.

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



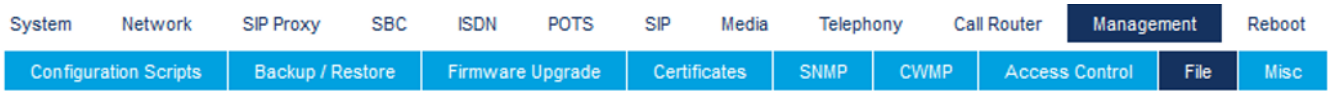
Ethernet Link Configuration

Link	MTU	802.1x Authentication	EAP Username	EAP Certificate Validation	Virtual Switch
eth1	1500	Disable		Trusted And Valid	Enable
eth2-5	1500	Disable		Trusted And Valid	Enable

8. Click **Apply**.

Upload ISO-image to Internal Storage

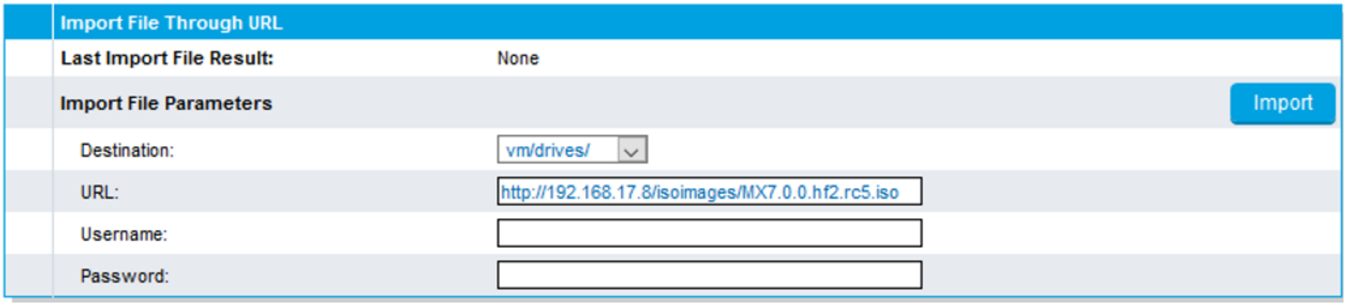
Figure 4.5: File



1. Go to **Management** > **File**.
2. Select the **Destination** to **vm/drives/** from the drop-down list.

3. Specify the **URL** where the ISO-images is located.

Figure 4.6: Import File Through URL



Import File Through URL

Last Import File Result: None

Import File Parameters

Destination: vm/drives/

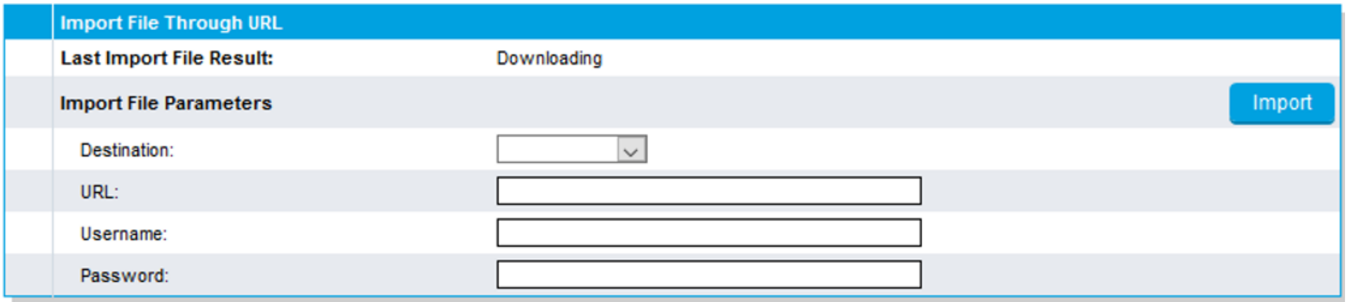
URL: http://192.168.17.8/isoimages/MX7.0.0.hf2.rc5.iso

Username:

Password:

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

Figure 4.7: Last Import File Result



Import File Through URL

Last Import File Result: Downloading

Import File Parameters

Destination:

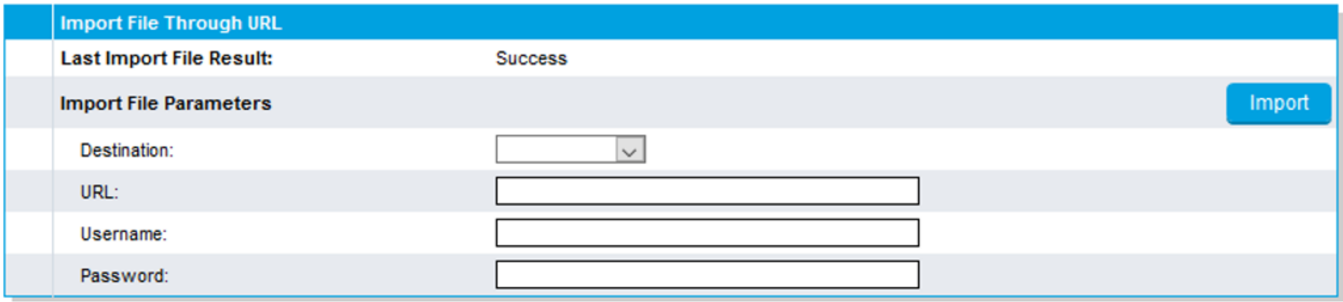
URL:

Username:

Password:

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

Figure 4.8: Import File Success



Import File Through URL

Last Import File Result: Success

Import File Parameters

Destination:

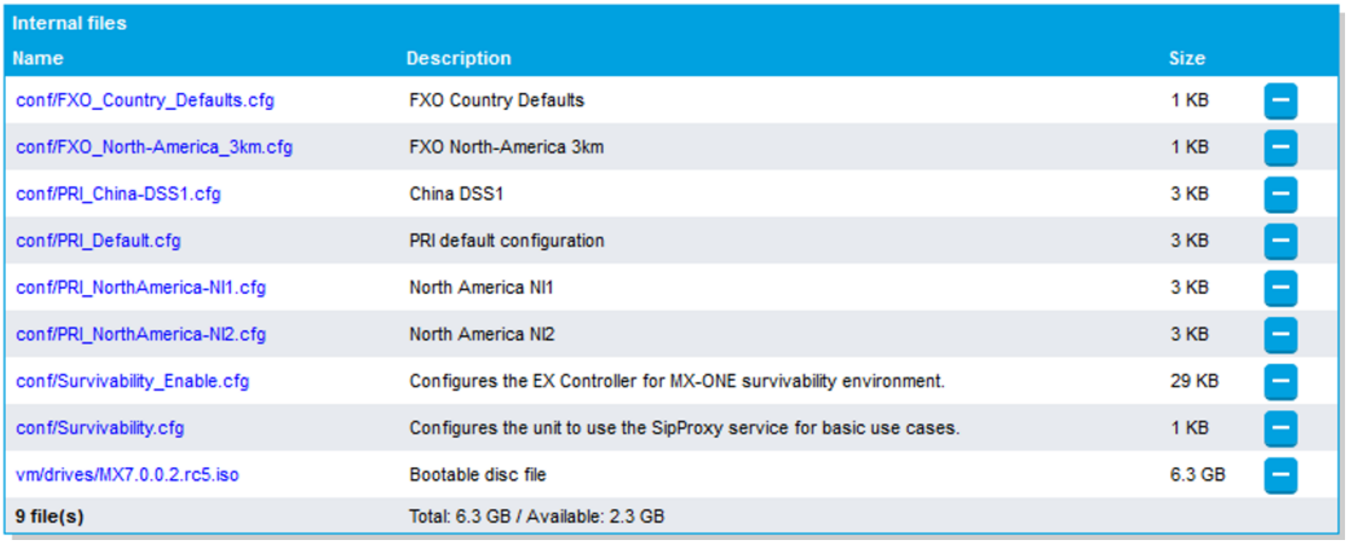
URL:

Username:

Password:

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

Figure 4.9: Internal Files

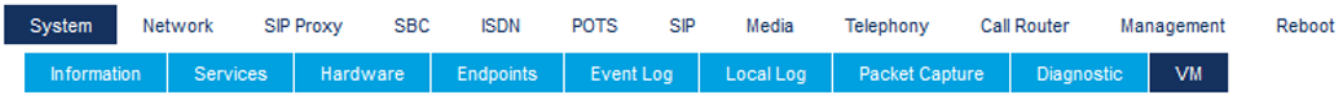


Internal files

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

Create the Virtual Machine

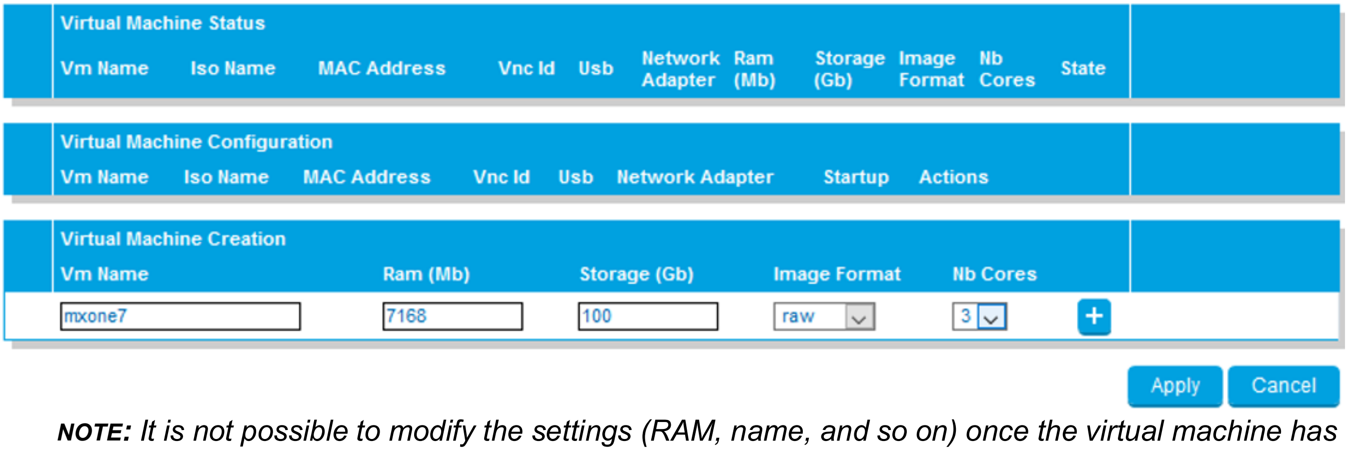
Figure 4.10: VM



1. Go to **System** > **VM**.
2. In the Virtual Machine Creation table, fill in the following field details.

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

Figure 4.11: Virtual Machine



Virtual Machine Status

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State

Virtual Machine Configuration

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions

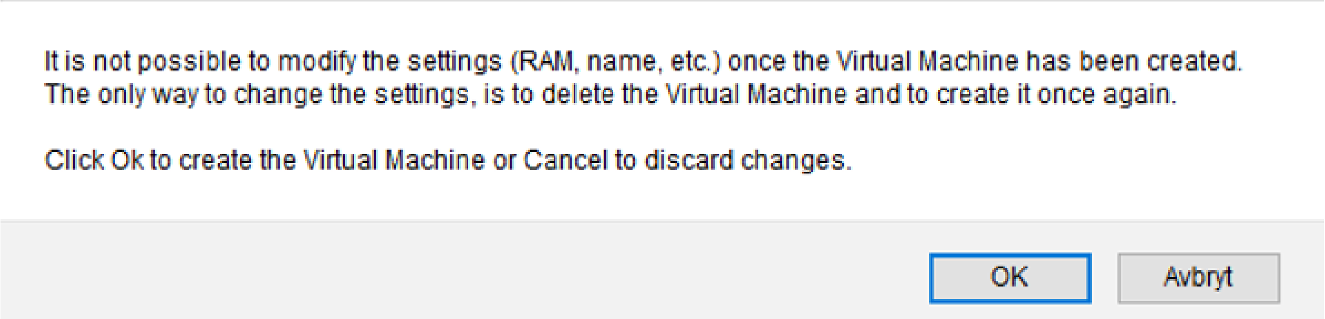
Virtual Machine Creation

Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	
mxone7	7168	100	raw	3	+

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

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

Figure 4.12: Virtual Machine Creation Message



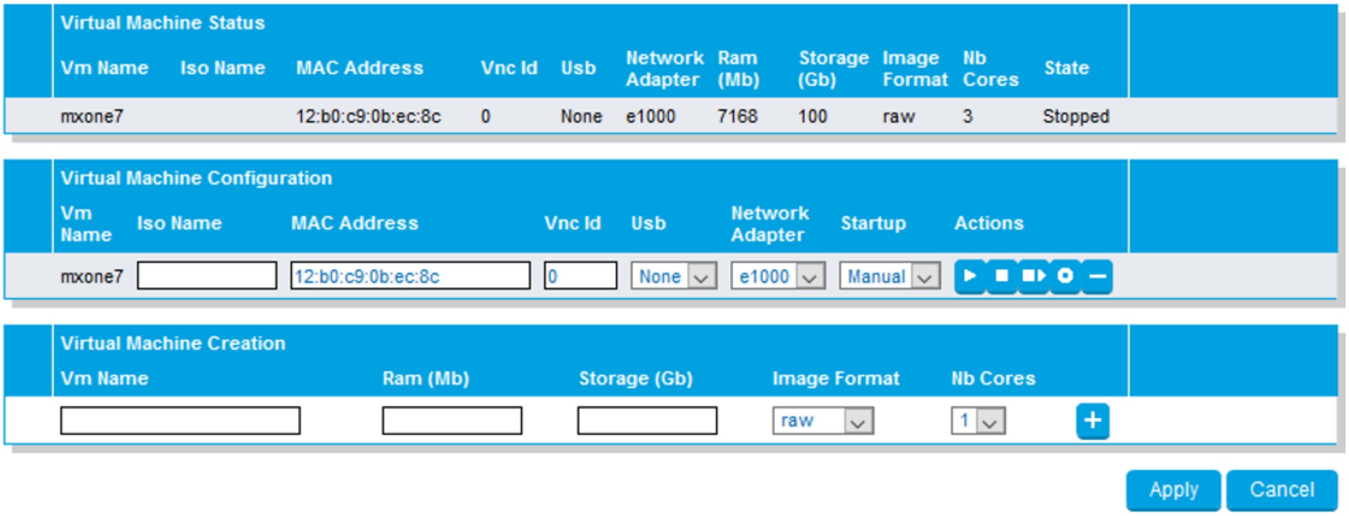
It is not possible to modify the settings (RAM, name, etc.) once the Virtual Machine has been created.
The only way to change the settings, is to delete the Virtual Machine and to create it once again.

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

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

Virtual Machines

Figure 4.13: Virtual Machine Status



Virtual Machine Status

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

Virtual Machine Configuration

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
mxone7		12:b0:c9:0b:ec:8c	0	None	e1000	Manual	▶ ■ ■▶ ● —

Virtual Machine Creation

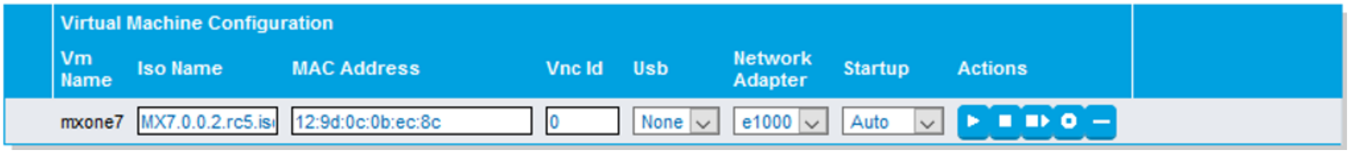
Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	
			raw	1	+

Using Locally Stored ISO-image

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

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

Figure 4.14: Virtual Machine Configuration

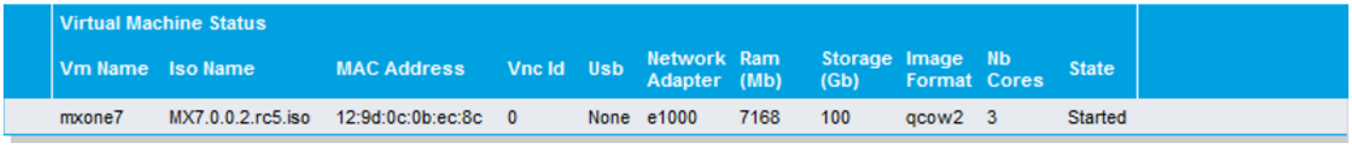


Virtual Machine Configuration

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
mxone7	MX7.0.0.2.rc5.is	12:9d:0c:0b:ec:8c	0	None	e1000	Auto	▶ ■ ■▶ ● —

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

Figure 4.15: Virtual Machine Started Status



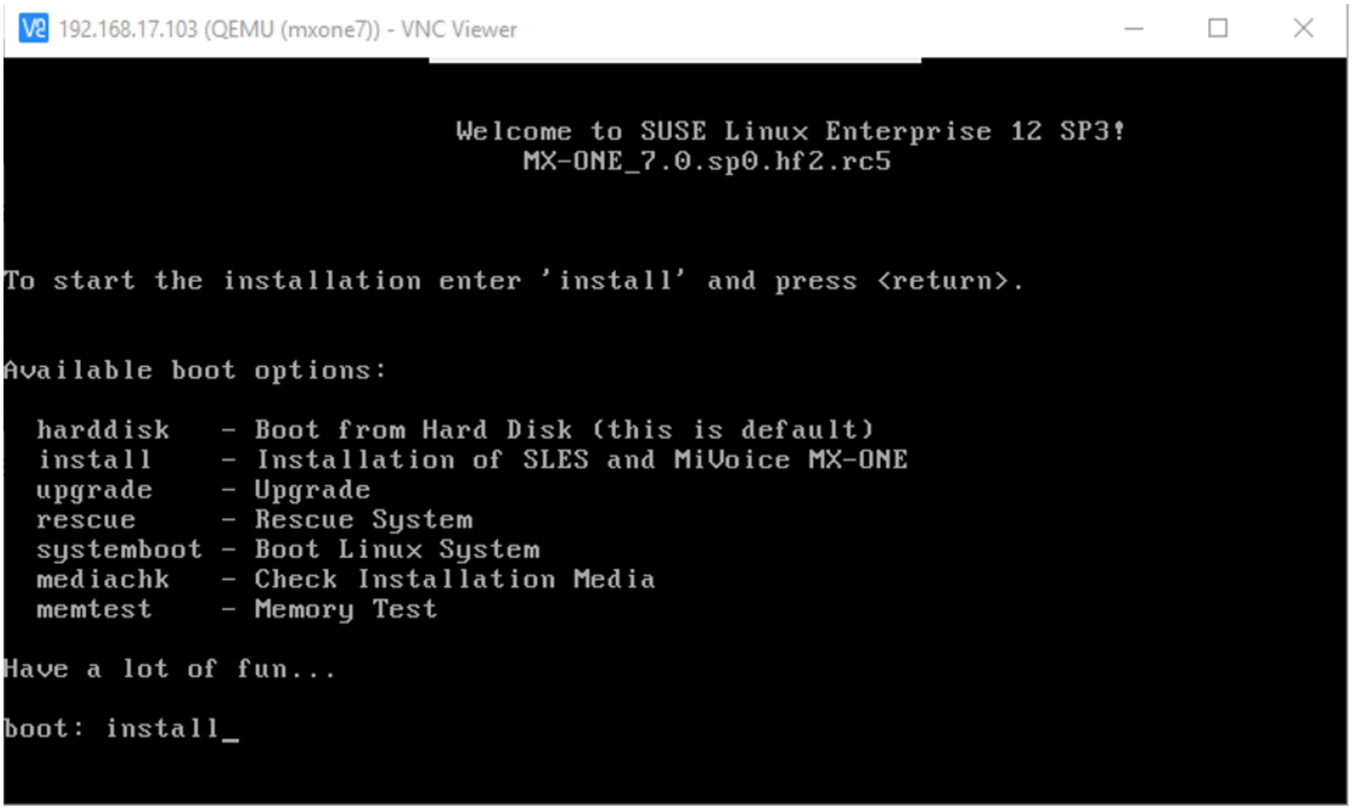
Virtual Machine Status

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

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

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

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

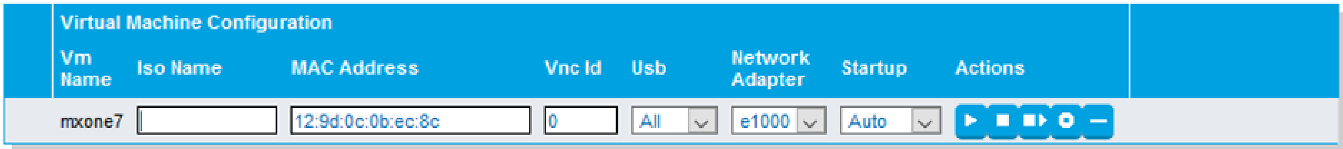


```
                         Welcome to SUSE Linux Enterprise 12 SP3!
                             MX-ONE_7.0.sp0.hf2.rc5


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


Available boot options:

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

Have a lot of fun...

boot: install_
```

Using bootable USB-Stick

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

11. Select **All** from the **Usb** field and click **Apply**.


Virtual Machine Configuration

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
mxone7		12:9d:0c:0b:ec:8c	0	All	e1000	Auto	▶ ■ ■▶ ● —

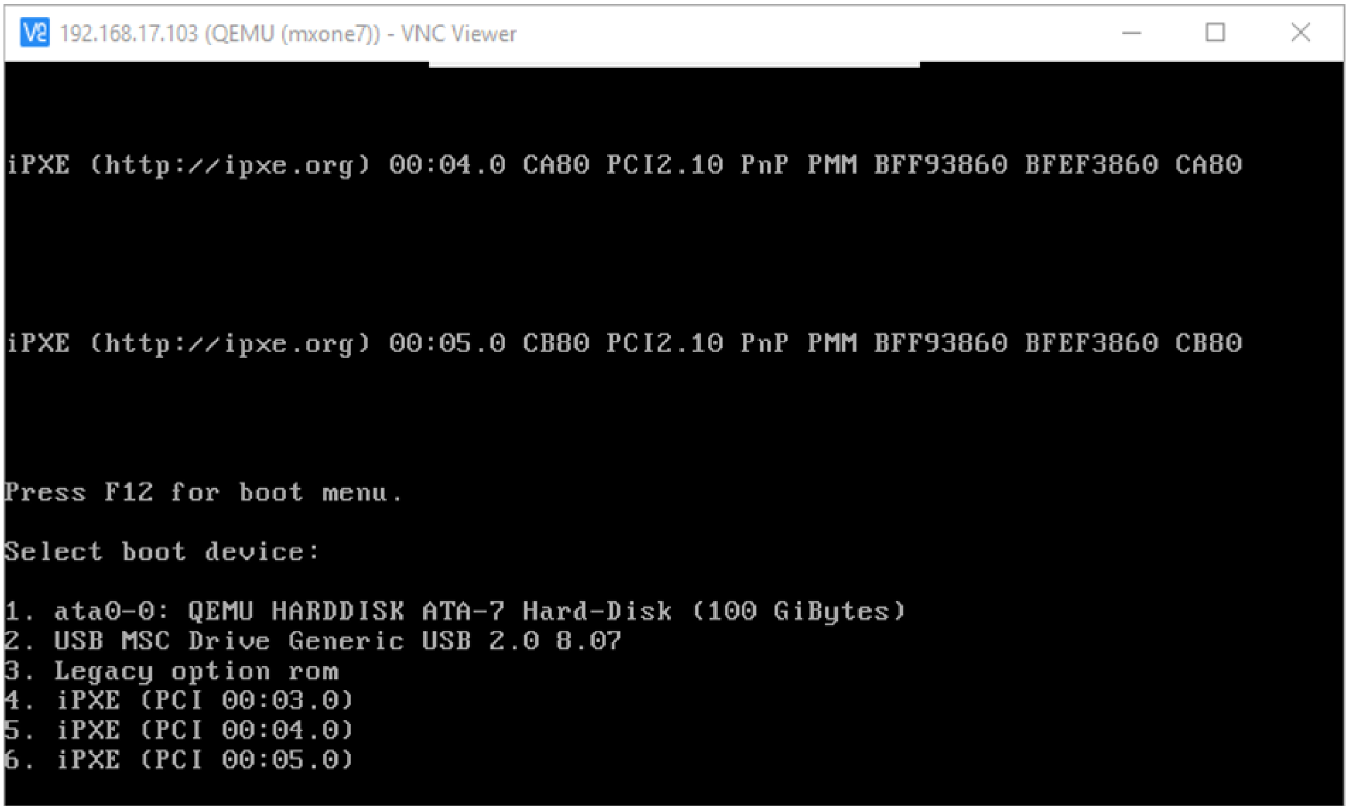
12. Click Start icon to start the VM. Open the VNC Client located on your computer network that is connected to the unit.

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

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

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

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



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


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


Press F12 for boot menu.

Select boot device:

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

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

Setting up MX-ONE for Branch Node Solution

Number Analysis

Number Analysis Data:

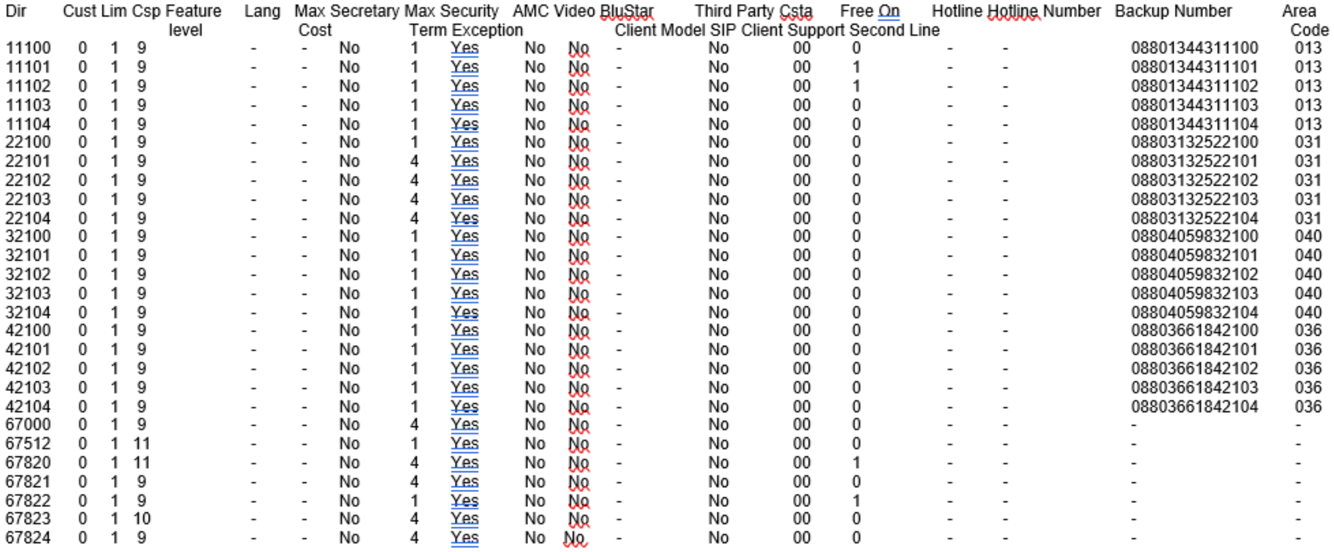
Type of Series	Number Series
Extension Number Series	10000 - 49999 67000 - 67999
External Destination Code	081 – 088
LCR Access Code Number Series	00

Call Discrimination Data:

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

Extension Data

Figure 4.16: Directory Number Profile



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

MDSH>

Common Service Profile 9:

Cust: 0

Traf : 0103151515

Serv: 11110001100100000000100000300

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: 1111300110010000000000100000300

Cdiv: 111000111010000

Roc: 000001

Npres: 0011000

Offered Time: 0

Forced DisconnectTime: 0

CnnLog: 0

Csp Name: Intrusion

Least Cost Routing Data

ENT Table

Least Cost Destination Data

Table 4.1: External Number Table

Entry	TRC	PRE	Conf
00013443	8		N
00031325	8		N
00036618	7		N
00040598	8		N
000856867	7		N

NLT Table

Least Cost Destination Data

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

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

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

Entry	TRC	PRE	CONF	MIN	MAX	ACF
006	0	-	N	6	18	Y
007	0	-	N	6	18	Y
008	0	-	N	6	18	Y
009	0	-	N	6	18	Y

DNT2 Table

Least Cost Destination Data

Table 4.3: Number Table

Entry	TRC	PRE	ACCT	FRCT	TOLL	CBCS	BTON	TNS	OSA
00013	5	-	0	1	111111111111111	-	0	-	-
00031	5	-	0	2	111111111111111	-	0	-	-
00036	5	-	0	3	111111111111111	-	0	-	-
00040	5	-	0	3	111111111111111	-	0	-	-
0008	4	-	0	4	111111111111111	-	0	-	-

FDT Table

Least Cost Destination Data

Table 4.4: Fictitious Destination Table

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

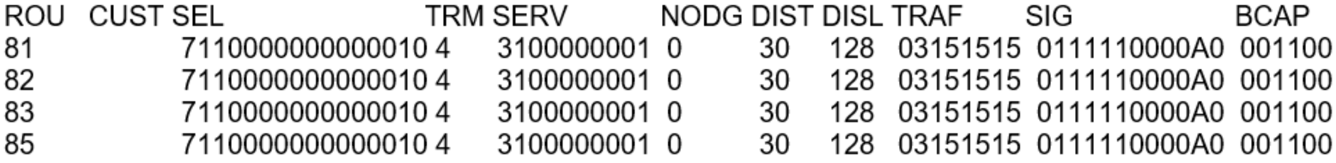
END

Route Data

ROCAP

Route Category Data

Figure 4.17: Route Category Data



```
ROU   CUST SEL                      TRM SERV          NODG DIST DISL TRAF        SIG                BCAP
81              7110000000000010 4    3100000001  0        30    128  03151515  0111110000A0  001100
82              7110000000000010 4    3100000001  0        30    128  03151515  0111110000A0  001100
83              7110000000000010 4    3100000001  0        30    128  03151515  0111110000A0  001100
85              7110000000000010 4    3100000001  0        30    128  03151515  0111110000A0  001100
```

RODAP

Route Data

Table 4.5: Route Data

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

RODDP

External Destination Route Data

Table 4.6: External Destination Route Data (Sheet 1 of 2)

DEST	DRN	ROU	CHO	CUST	ADC	TRC	SRT	NUMACK	PRE
00	-	1	-	-	1225000000000250002000000000	0	3	-	-
081	-	81	-	-	1225000000000250002000000000	0	4	-	-
082	-	82	-	-	1225000000000250002000000000	0	4	-	-

Table 4.6: External Destination Route Data (Continued) (Sheet 2 of 2)

DEST	DRN	ROU	CHO	CUST	ADC	TRC	SRT	NUMACK	PRE
083	-	83	-	-	1225000000000250002000000000	0	4	-	-
085	-	85	-	-	1225000000000250002000000000	0	4	-	-
088	-	1	-	-	1225000000000250002000000000	0	4	-	-

Number Prefixing

Route Number Data

Table 4.7: Route Data

ROU	PRE	ROUDIR	EXNOPU	EXNOPR	TERAC
1	-	-	1-46 2-08 4-568	-	-
81	-	-	1-46 2-013 4-443	-	-
82	-	-	1-46 2-036 4-418	-	-
83	-	-	1-46 2-031 4-325	-	-
85	-	-	1-46 2-040 4-598	-	-

SIP ROUTE

One SIP route to each branch node is specified.

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

route : 81

protocol = udp

profile = common-gateway

```
service = PRIVATE
uristring0 = sip:?@192.168.17.81
fromuri0 = sip:?@192.168.17.44
remoteport = 5070
accept = FROM_DOMAIN
match = 192.168.17.81
register = SET_BY_PROFILE
trusted = TRUST_BY_PROFILE
```

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

```
route : 82
protocol = udp
profile = common-gateway
service = PRIVATE
uristring0 = sip:?@192.168.17.82
fromuri0 = sip:?@192.168.17.44
remoteport = 5070
accept = FROM_DOMAIN
match = 192.168.17.82
register = SET_BY_PROFILE
trusted = TRUST_BY_PROFILE
```

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

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

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

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

Setting up GX Gateway with ISDN Trunks

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

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

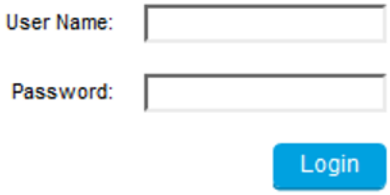
Logon

This section describes how to setup BO#1.

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

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

Figure 4.18: Login page



- User name/password: public /
- User name/password: admin/administrator

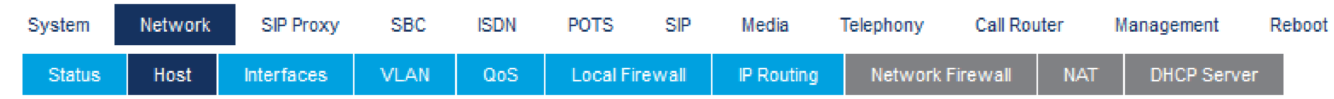
2. Plug in the analog phone in the FXS port 1 of the EX Controller and dial *#*0 to know the IP address of the EX Controller assigned by using DHCP server.

3. Log into the EX Controller by using the above-mentioned IP address and navigate as described below to configure.

Network Settings

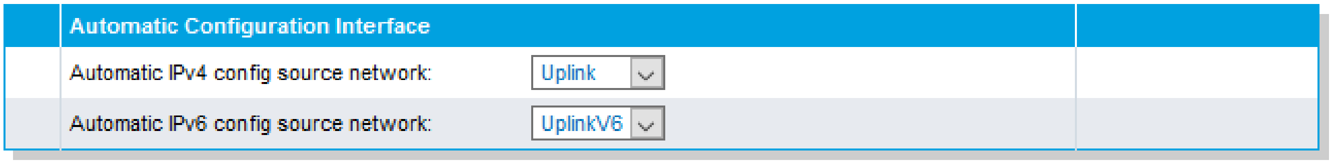
Host

Figure 4.19: Host Settings - 1



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

Figure 4.20: Host Settings - 2

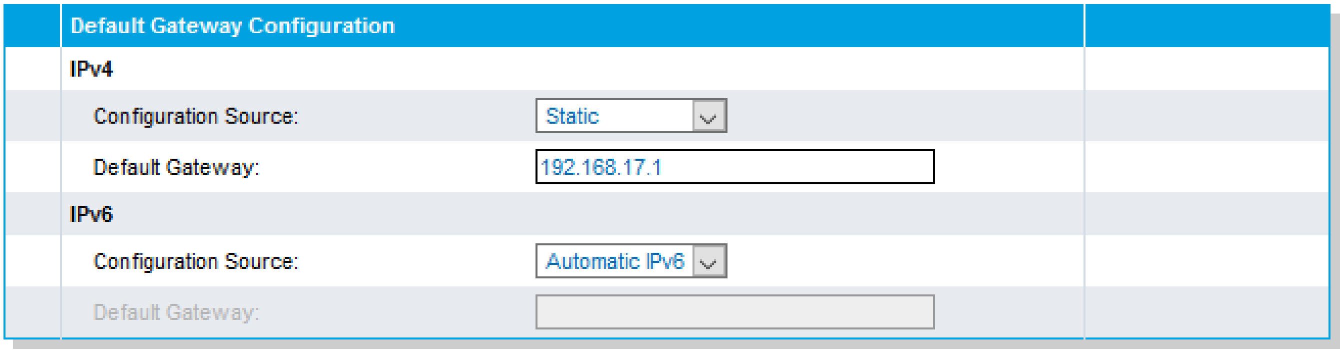


Automatic Configuration Interface

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

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

Figure 4.21: Changing Static IP Address

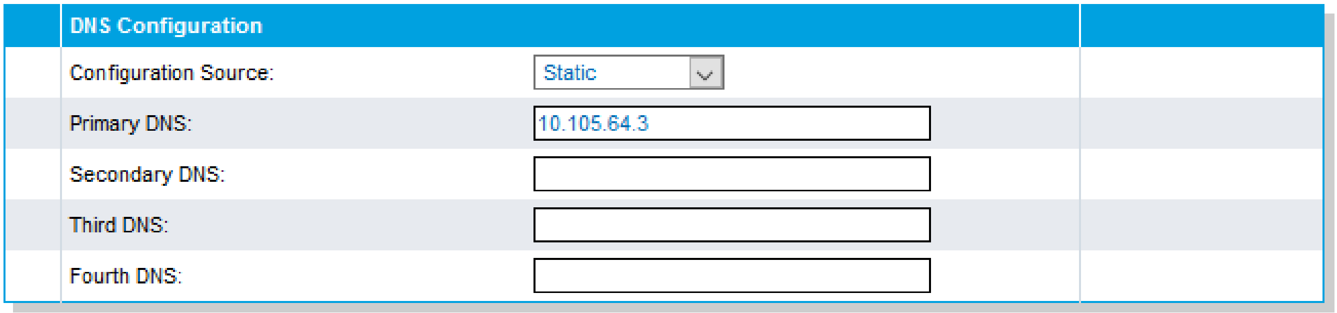


Default Gateway Configuration

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 4.22: Changing Static DNS Server

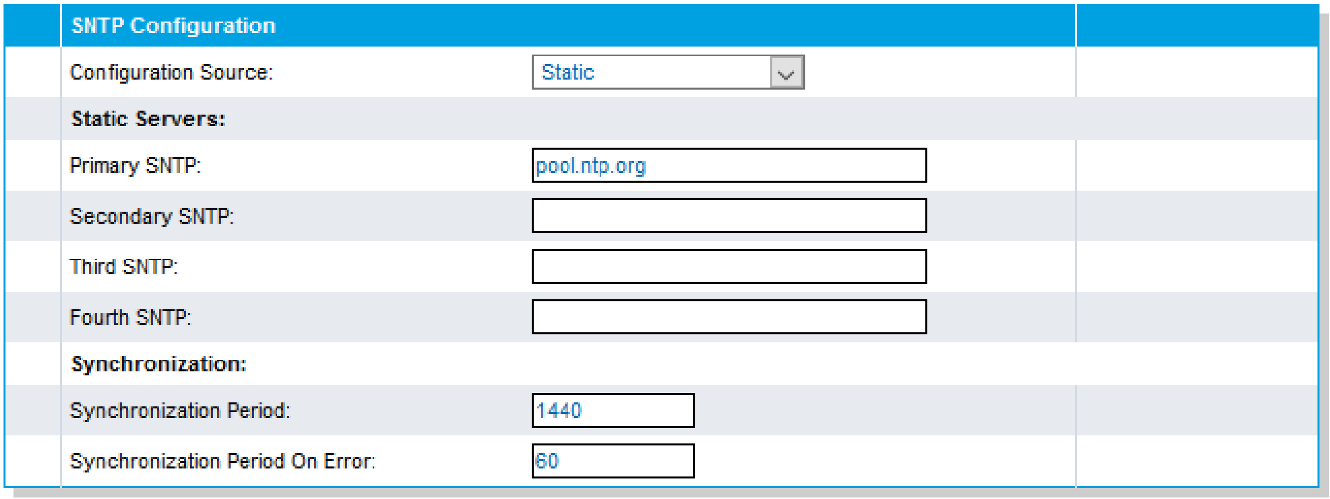


DNS Configuration

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 4.23: Changing to Static SNTP Server



SNTP Configuration

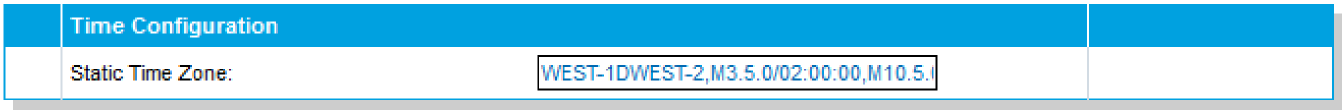
Configuration Source:	Static
Static Servers:	
Primary SNTP:	pool.ntp.org
Secondary SNTP:	
Third SNTP:	
Fourth SNTP:	
Synchronization:	
Synchronization Period:	1440
Synchronization Period On Error:	60

5. Set the **Time Zone**.

   Valid options are:

   - Pacific Time (Canada and US): PST8PDT7,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Mountain Time (Canada and US): MST7MDT6,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Central Time (Canada and US): CST6CDT5,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Eastern Time (Canada and US): EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Atlantic Time (Canada): AST4ADT3,M3.2.0/02:00:00,M11.1.0/02:00:00
   - GMT Standard Time: GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
   - W. Europe Standard Time: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00
   - China Standard Time: CST-8
   - Tokyo Standard Time: TST-9
   - Central Australia Standard Time: CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
   - Australia Eastern Standard Time: AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
   - UTC (Coordinated Universal Time): UTC0

Figure 4.24: Setting Static Time Zone



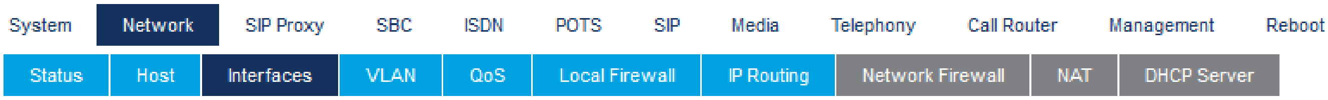
Time Configuration

Static Time Zone:	WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.(

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

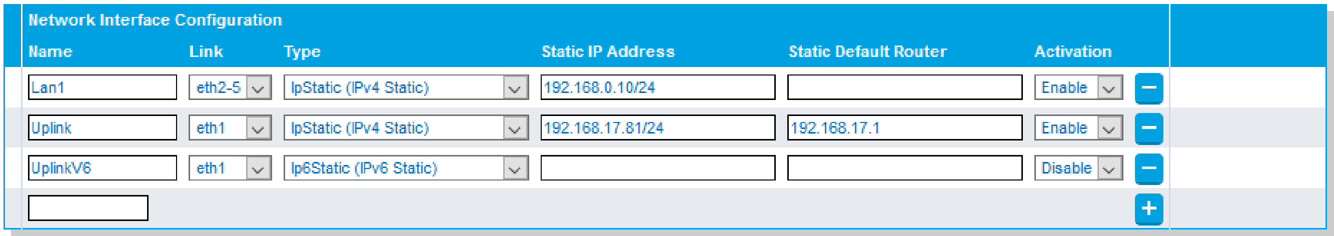
Interfaces

Figure 4.25: Interface



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

Figure 4.26: Changing Uplink to IpStatic



Network Interface Configuration

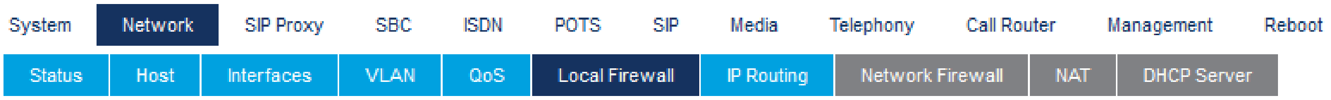
Name	Link	Type	Static IP Address	Static Default Router	Activation
Lan1	eth2-5	IpStatic (IPv4 Static)	192.168.0.10/24		Enable
Uplink	eth1	IpStatic (IPv4 Static)	192.168.17.81/24	192.168.17.1	Enable
UplinkV6	eth1	Ip6Static (IPv6 Static)			Disable

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

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

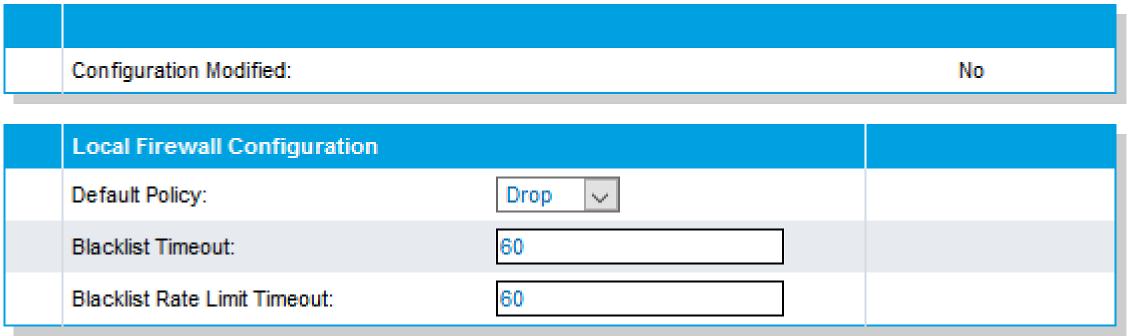
Local Firewalls

Figure 4.27: Local firewalls



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

Figure 4.28: Changing default policy



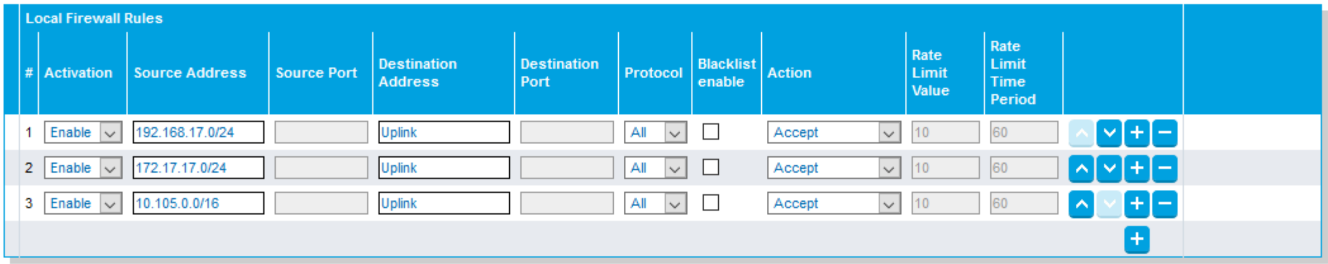
Configuration Modified:	No

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 4.29: Enter network traffic



Local Firewall Rules

#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period
1	Enable	192.168.17.0/24		Uplink		All	☐	Accept	10	60
2	Enable	172.17.17.0/24		Uplink		All	☐	Accept	10	60
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)

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

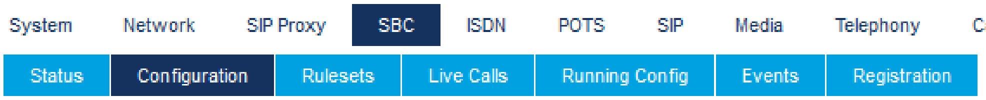
There are 2 types of Rulesets:

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

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

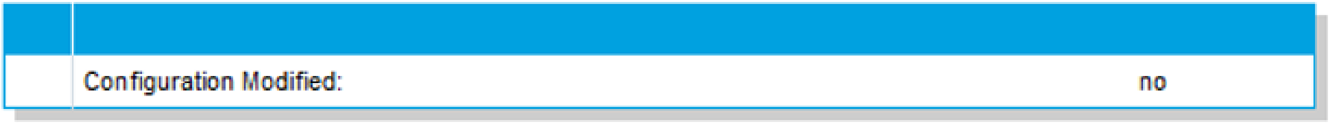
Configuration

Figure 4.30: Configuration



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

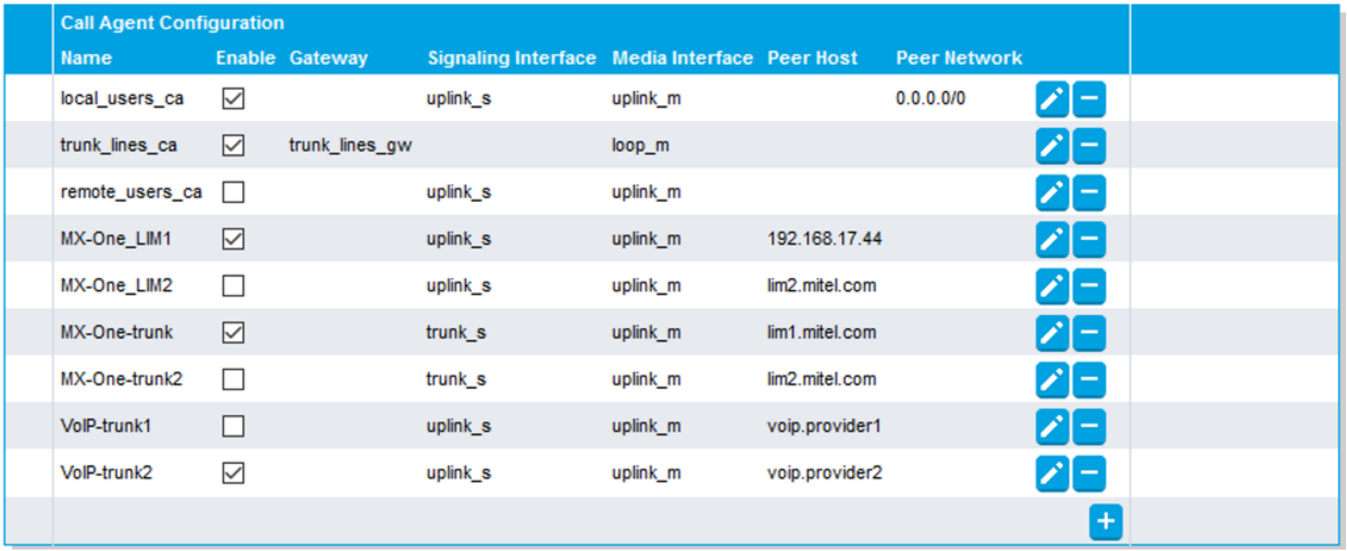
Figure 4.31: Configuration Modified



Configuration Modified: no

Following Call Agents are present.

Figure 4.32: Call Agent Configuration



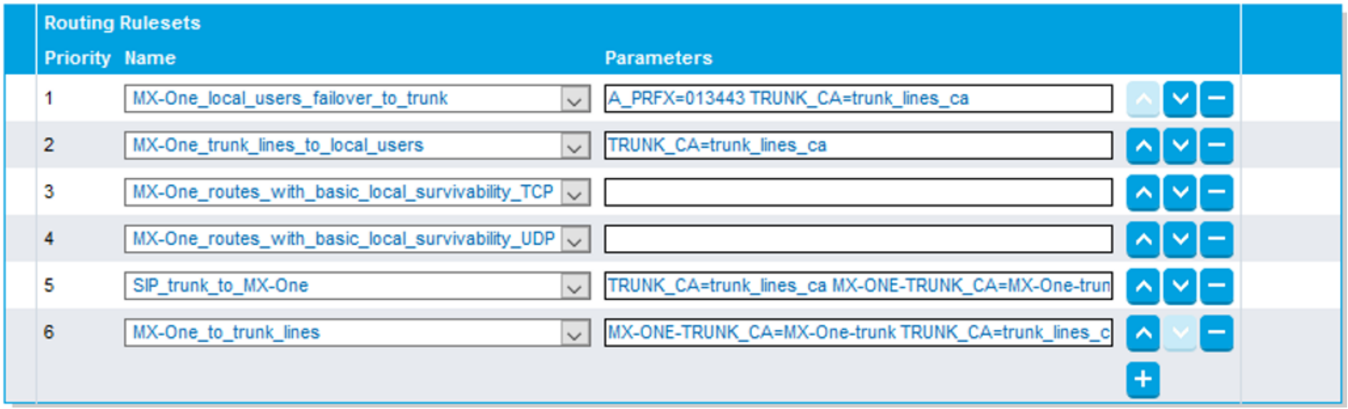
Call Agent Configuration

Name	Enable	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		
remote_users_ca	☐		uplink_s	uplink_m		
MX-One_LIM1	☑		uplink_s	uplink_m	192.168.17.44	
MX-One_LIM2	☐		uplink_s	uplink_m	lim2.mitel.com	
MX-One-trunk	☑		trunk_s	uplink_m	lim1.mitel.com	
MX-One-trunk2	☐		trunk_s	uplink_m	lim2.mitel.com	
VoIP-trunk1	☐		uplink_s	uplink_m	voip.provider1	
VoIP-trunk2	☑		uplink_s	uplink_m	voip.provider2	

Routing Rulesets

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

Figure 4.33: Routing Rulesets



Routing Rulesets

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

- **Ruleset MX-One_local_users_failover_to_trunk**

A_PRFX=013443

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

TRUNK_CA=trunk_lines_ca

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

- **Ruleset SIP_trunk to_MX-One**

TRUNK_CA=trunk_lines_ca

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

MX-ONE-TRUNK=MX-One-trunk

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

- **Ruleset MX-One_to_trunk_lines**

TRUNK_CA=trunk_lines_ca

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

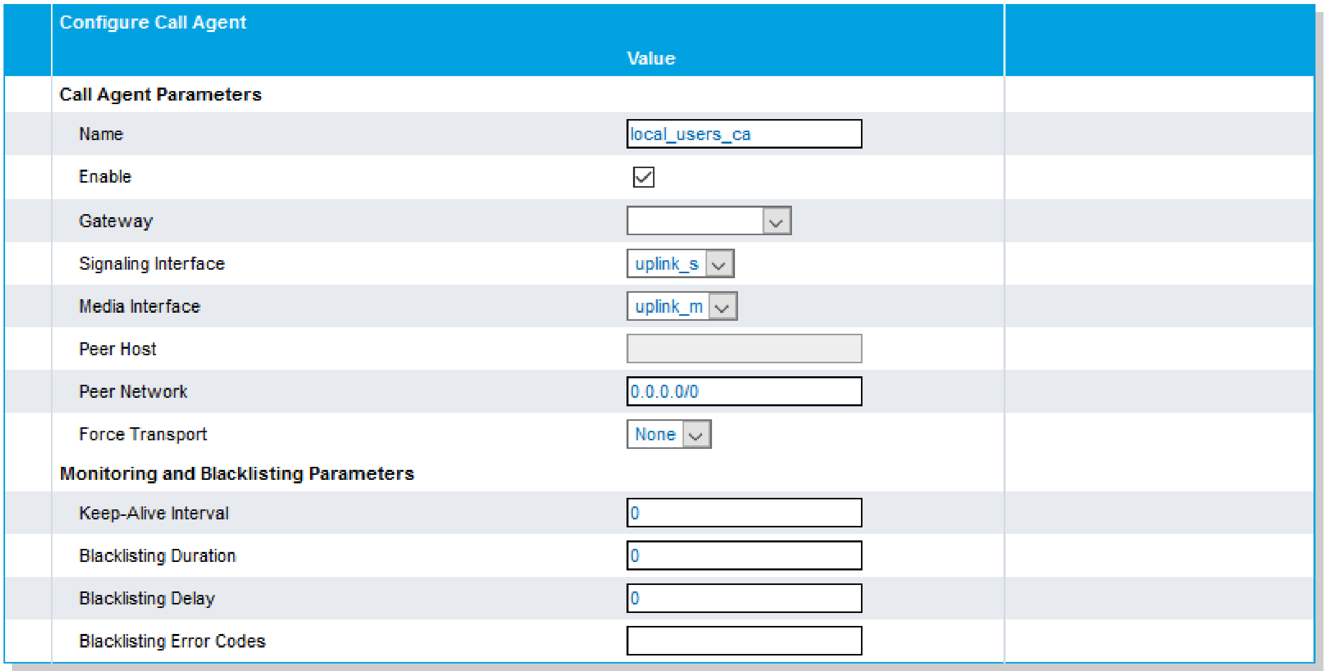
MX-ONE-TRUNK=MX-One-trunk

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

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

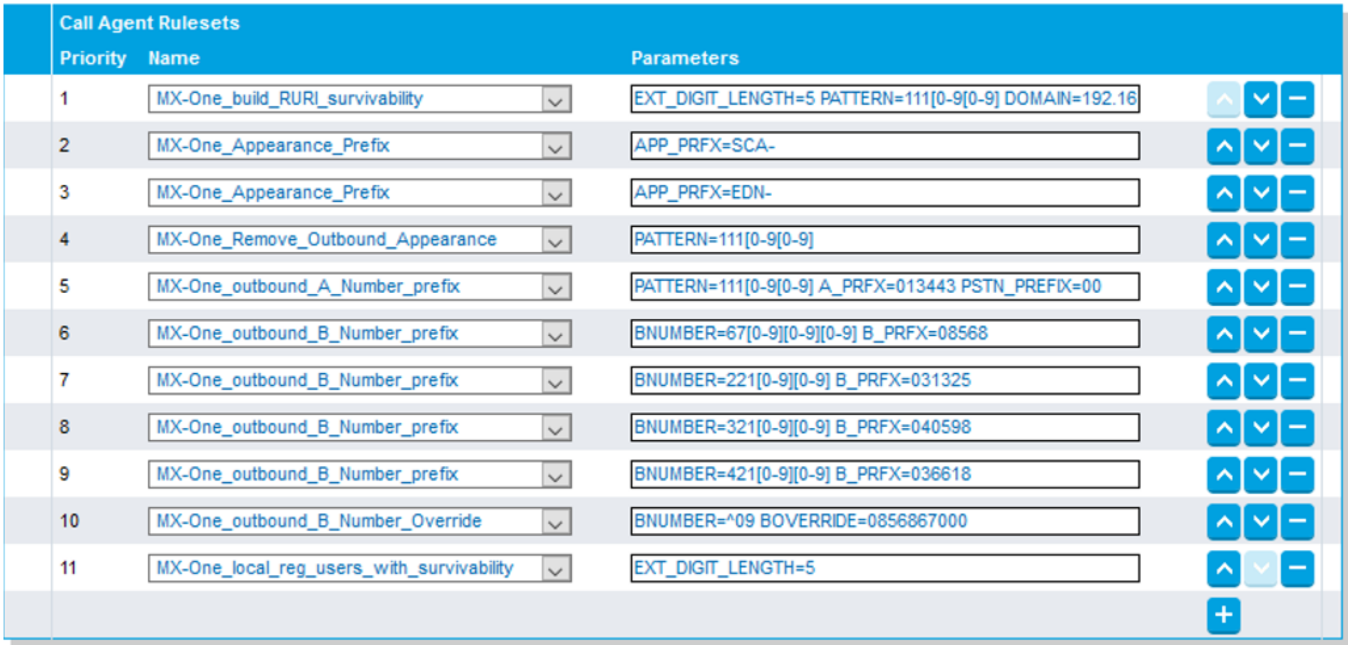
local_users_ca

Figure 4.34: Configure Call Agent screen



Configure Call Agent	Value
Call Agent Parameters	
Name	local_users_ca
Enable	☑
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 4.35: Call Agent Rulesets



Call Agent Rulesets

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

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

EXT_DIGIT_LENGTH=5

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

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

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

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

DOMAIN=192.168.17.44

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

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

APP_PREFIX=SCA- and APP_PREFIX=EDN-

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

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

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

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

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

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

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

A_PRFX=013443

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

PSTN_PREFIX=00

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

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

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

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

Calling HQ:

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

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

B_PRFX=08568

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

Calling BO#2:

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

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

B_PRFX=031325

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

Calling BO#3:

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

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

B_PRFX=040598

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

Calling BO#4:

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

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

B_PRFX=036618

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

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

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

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

BNUMBER=09

The internal number to the operator.

BOVERRIDE=0856867000

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

- **Ruleset: MX-One_local_reg_users_with_survivability**

(Builds the registration cache for survivability purpose).

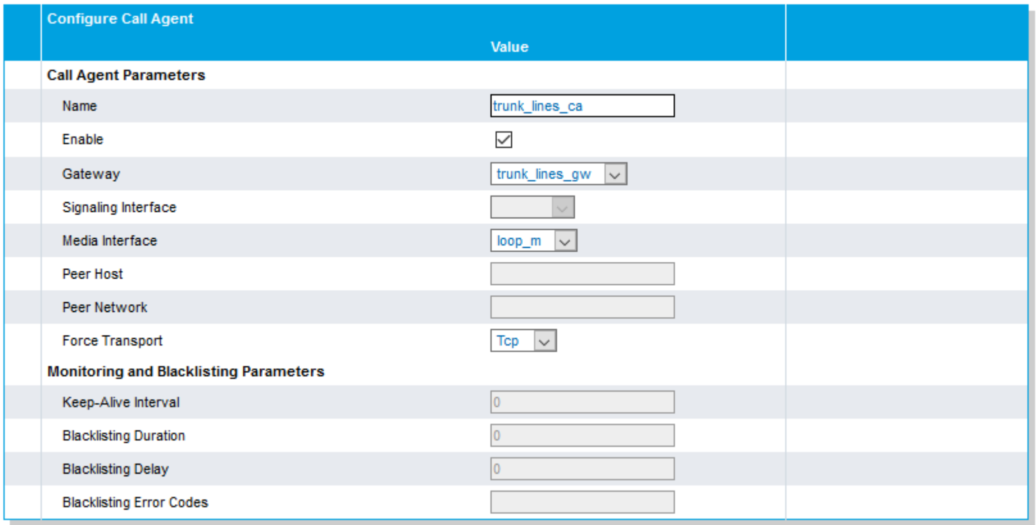
EXT_DIGIT_LENGTH=5

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

Click **Save** when done.

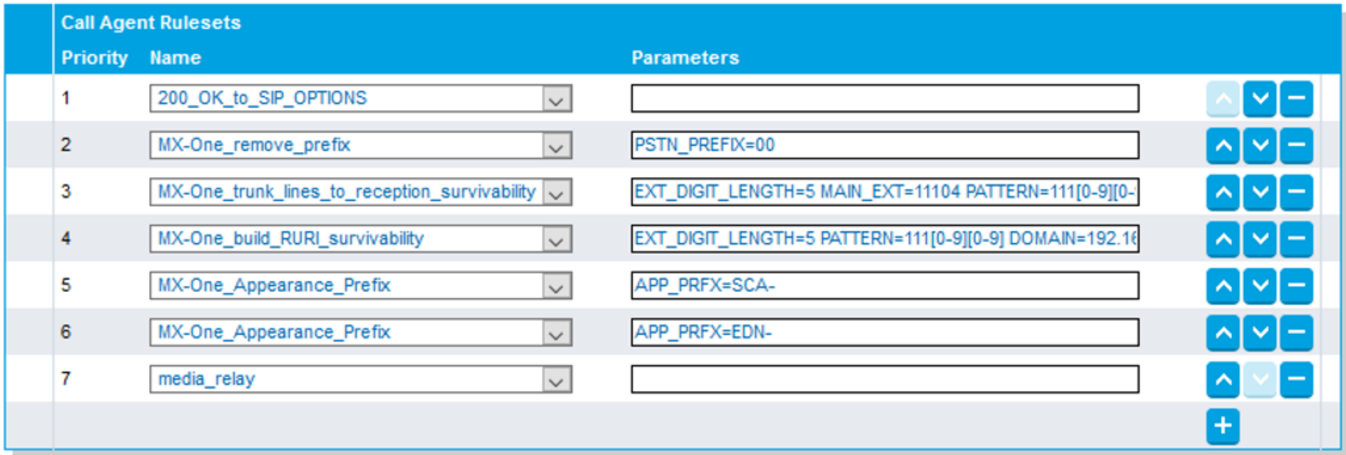
trunk_lines_ca

Figure 4.36: trunk_lines_ca



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

Figure 4.37: Call Agent Rulesets



Call Agent Rulesets

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

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

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

- **Ruleset: MX-One_trunk_lines_to_reception_survivability**

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

MAIN_EXT=11104

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

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

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

DOMAIN=192.168.17.44

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

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

Builds the RURI when in survivability mode.

EXT_DIGIT_LENGTH=5

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

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

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

DOMAIN=192.168.17.44

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

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

APP_PREFIX=SCA- and APP_PREFIX=EDN-

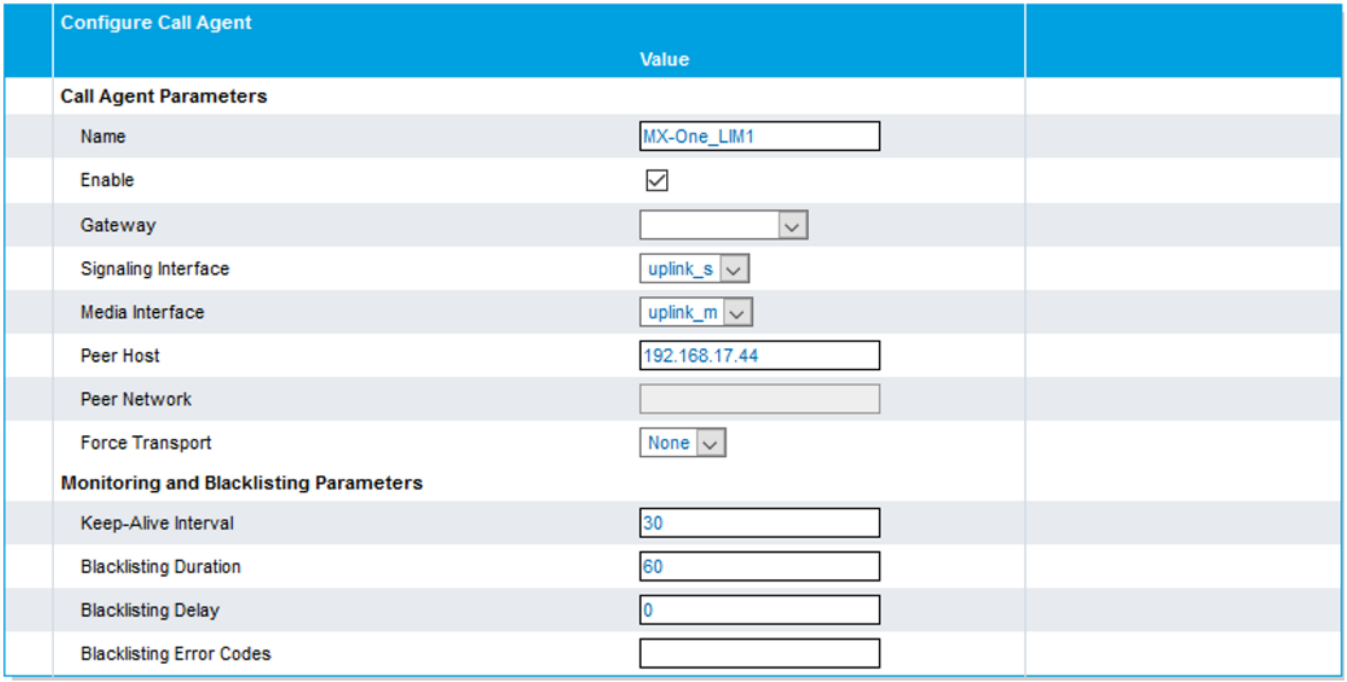
This is the prefix for the user names connected with shared appearance (SCA) and extra directory number (EDN). In this example, you have two user names: "SCA"- and "EDN-"

Click **Save** when done.

MX-One_Lim1

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

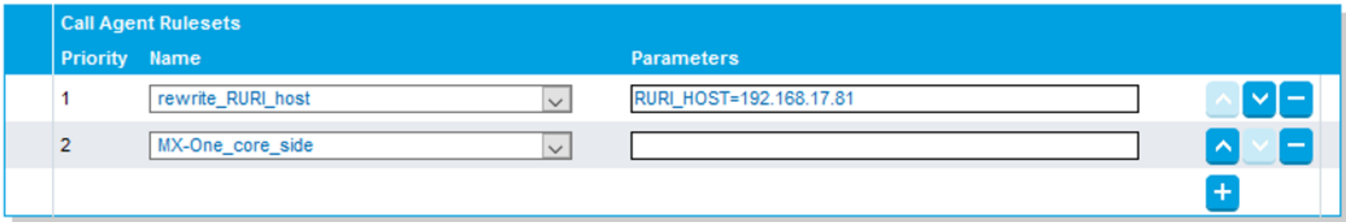
Figure 4.38: Configure Call Agent - Peer Host



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	

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

Figure 4.39: RURI_HOST parameter



Call Agent Rulesets

Priority	Name	Parameters
1	rewrite_RURI_host	RURI_HOST=192.168.17.81
2	MX-One_core_side	

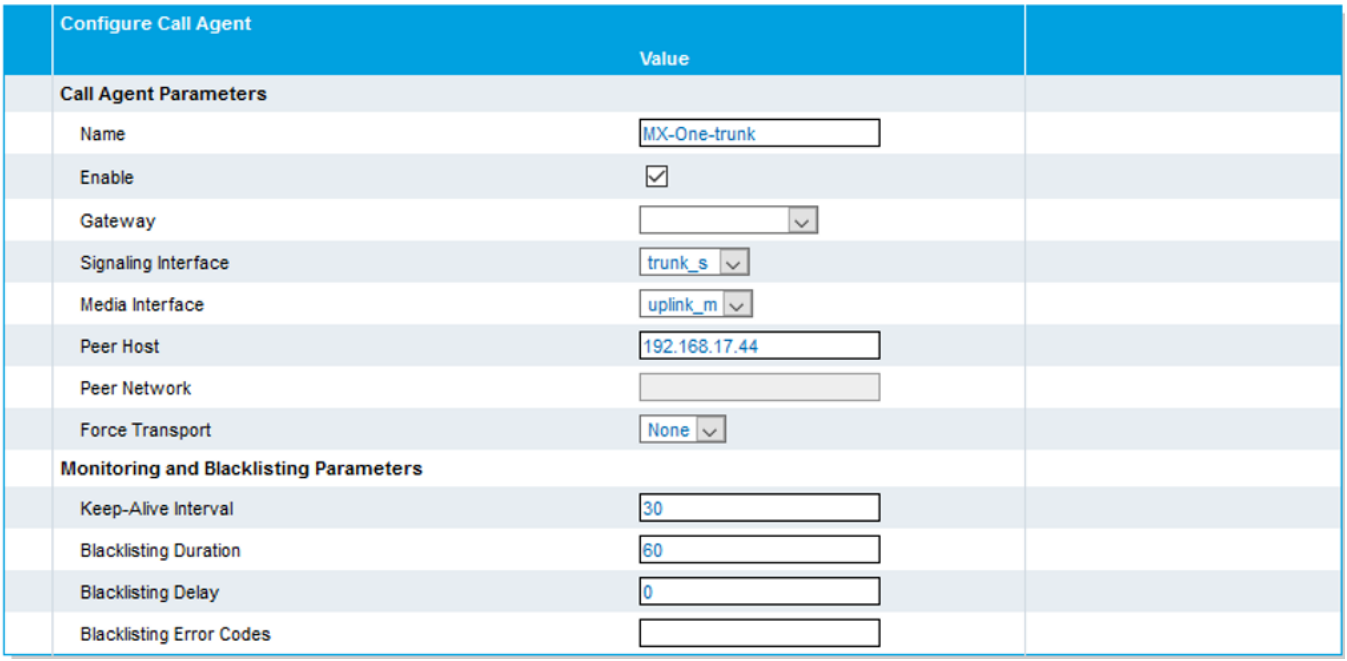
- **Ruleset: rewrite_RURI_host**
  RURI_HOST= 192.168.17.81
  This is the local IP address of the GX-gateway.
  Click **Save** when done.

MX-One_trunk

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

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

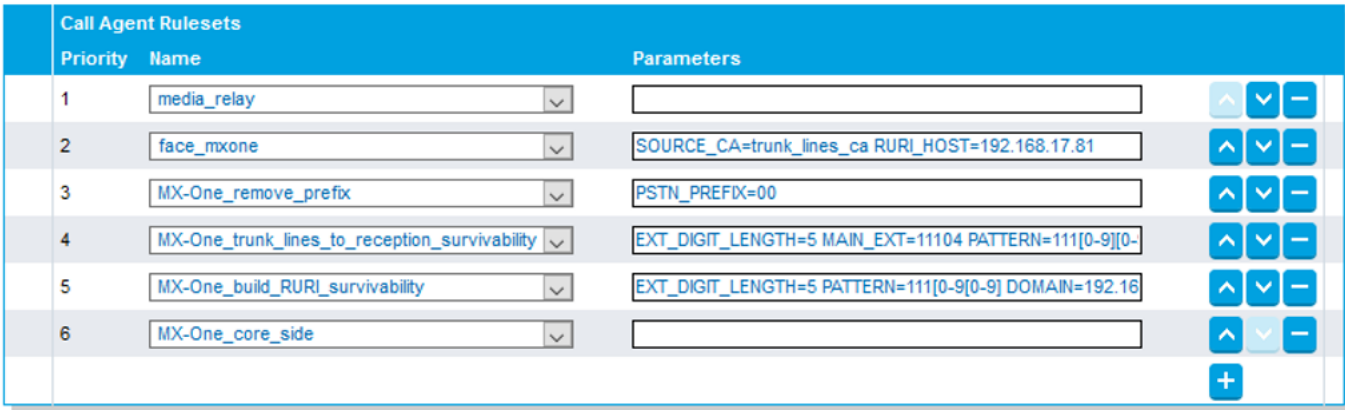
Figure 4.40: Call Agent Parameters



Configure Call Agent

	Value
Call Agent Parameters	
Name	MX-One-trunk
Enable	☑
Gateway	
Signaling Interface	trunk_s
Media Interface	uplink_m
Peer Host	192.168.17.44
Peer Network	
Force Transport	None
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	30
Blacklisting Duration	60
Blacklisting Delay	0
Blacklisting Error Codes	

Figure 4.41: Call Agent Rulesets



Call Agent Rulesets

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

- **Ruleset: face_mxone**

SOURCE_CA=trunk_lines_ca

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

RURI_HOST=192.168.17.81

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

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

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

- **Ruleset: MX-One_trunk_lines_to_reception_survivability**

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

EXT_DIGIT_LENGTH=5

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

MAIN_EXT=11104

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

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

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

DOMAIN=192.168.17.44

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

- **Ruleset: MX-One_build_RURI_survivability**

Builds the RURI when in survivability mode

EXT_DIGIT_LENGTH=5

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

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

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

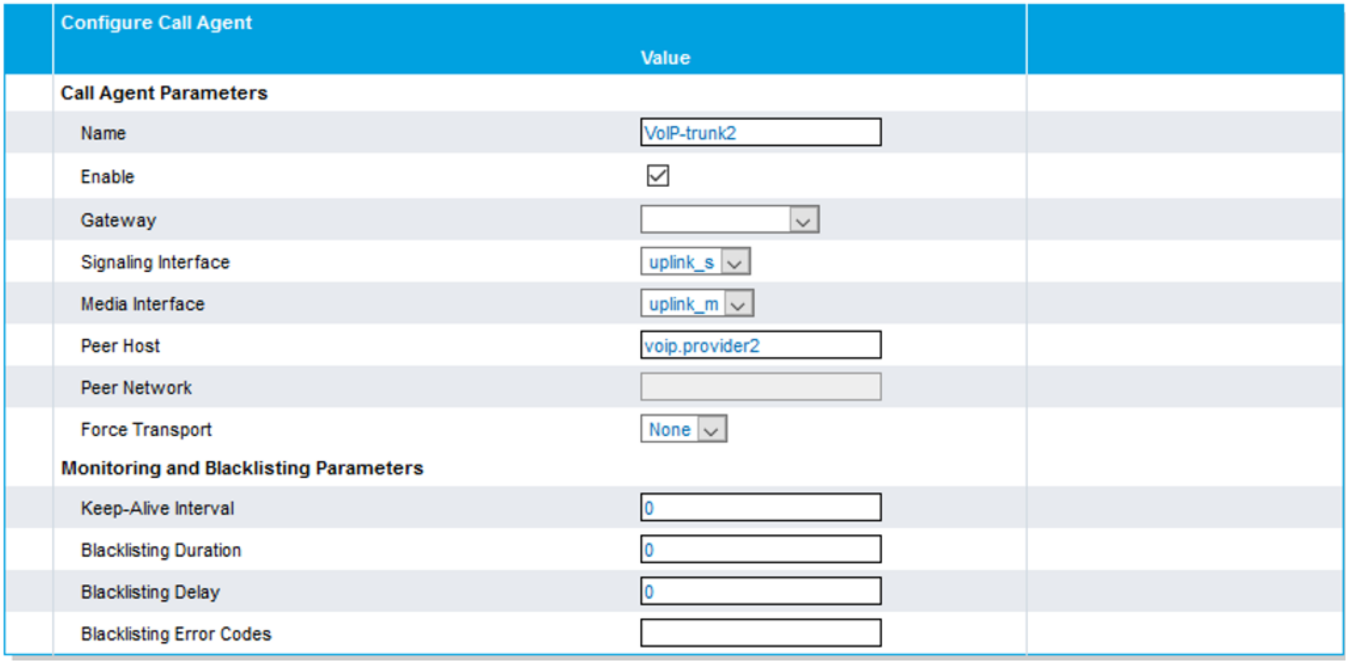
DOMAIN=192.168.17.44

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

Click **Save** when done

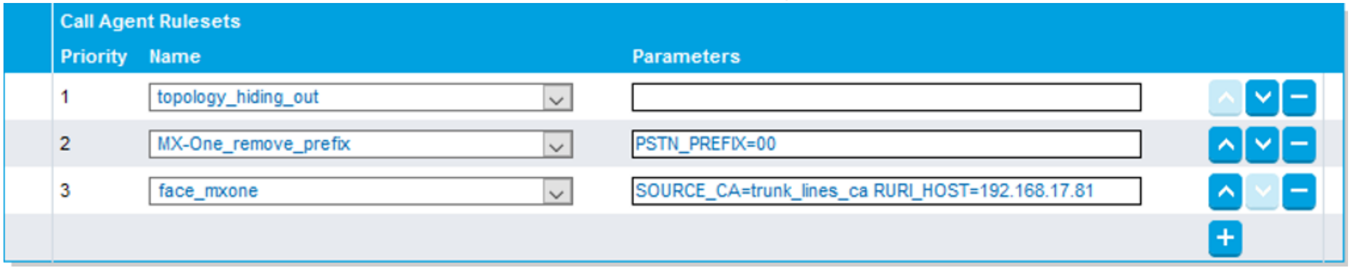
VOIP-trunk2

Figure 4.42: VoIP-trunk2



Configure Call Agent	Value
Call Agent Parameters	
Name	VoIP-trunk2
Enable	☑
Gateway	
Signaling Interface	uplink_s
Media Interface	uplink_m
Peer Host	voip.provider2
Peer Network	
Force Transport	None
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	0
Blacklisting Duration	0
Blacklisting Delay	0
Blacklisting Error Codes	

Figure 4.43: Call Agent Rulesets



Priority	Name	Parameters
1	topology_hiding_out	
2	MX-One_remove_prefix	PSTN_PREFIX=00
3	face_mxone	SOURCE_CA=trunk_lines_ca RURI_HOST=192.168.17.81

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

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

- **Ruleset: face_mxone**

SOURCE_CA=trunk_lines_ca

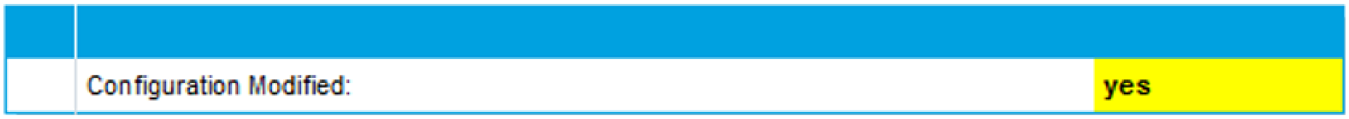
This parameter indicates the call agent from which the call is coming.

RURI_HOST=192.168.17.81

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

Click **Save** when done.

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



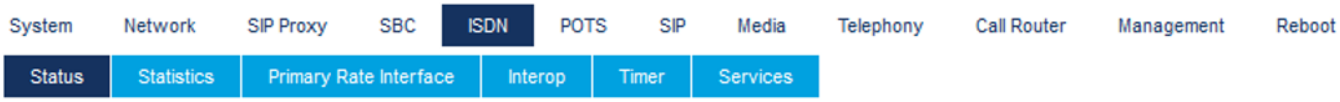
Configuration Modified: yes

Click **Apply** when ready.

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

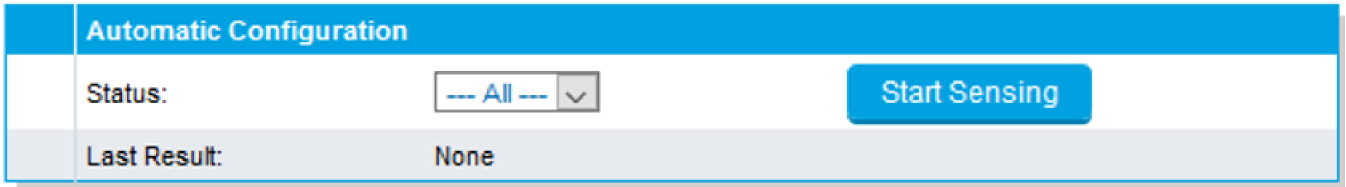
ISDN

Figure 4.44: ISDN



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

Figure 4.45: Automatic Configuration



Status: --- All ---

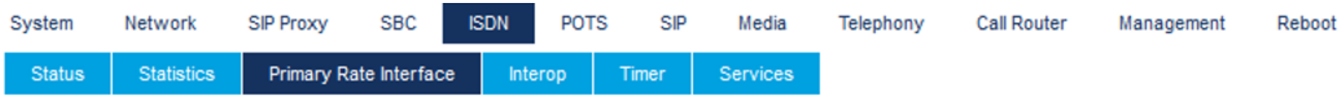
Last Result: None

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

Primary Rate Interface

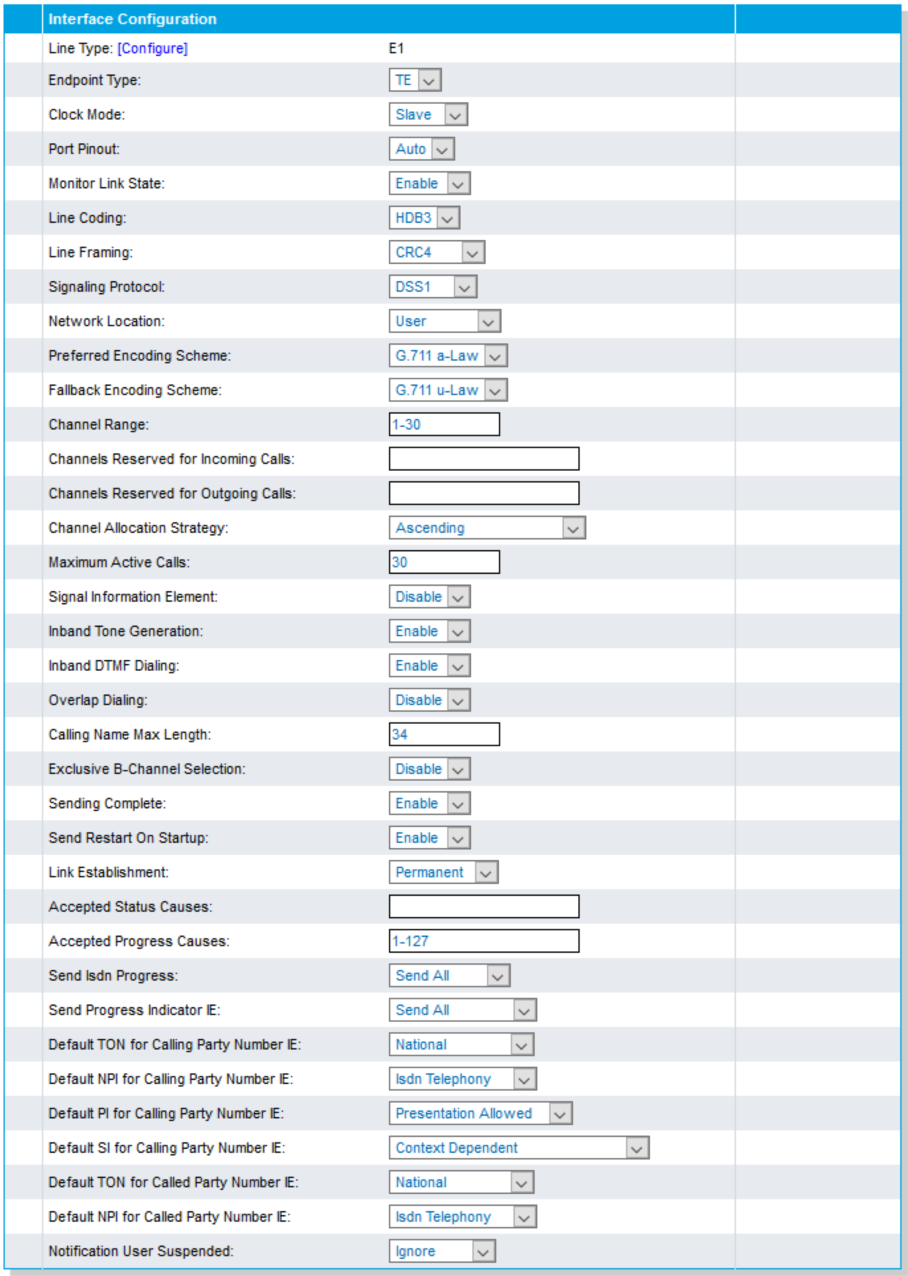
Settings

Figure 4.46: Primary Rate Interface



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

Figure 4.47: Interface Configuration

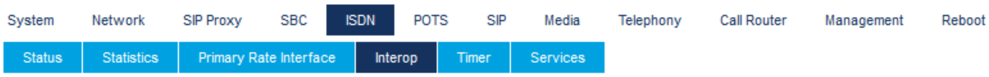


Interface Configuration	
Line Type: [Configure]	E1
Endpoint Type:	TE
Clock Mode:	Slave
Port Pinout:	Auto
Monitor Link State:	Enable
Line Coding:	HDB3
Line Framing:	CRC4
Signaling Protocol:	DSS1
Network Location:	User
Preferred Encoding Scheme:	G.711 a-Law
Fallback Encoding Scheme:	G.711 u-Law
Channel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

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

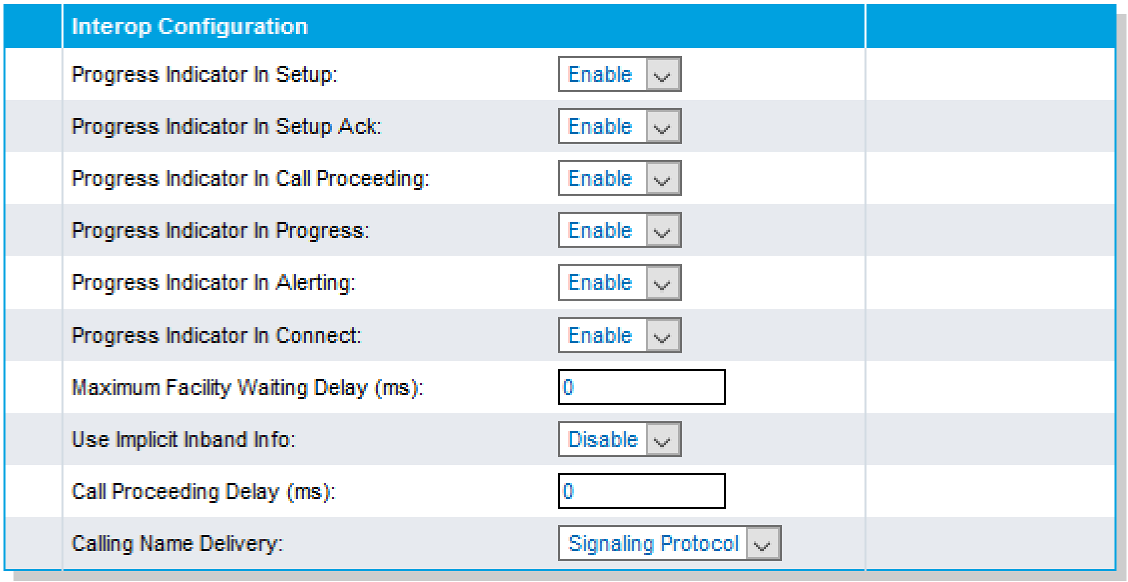
Interop

Figure 4.48: Interop



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

Figure 4.49: Interop Configuration



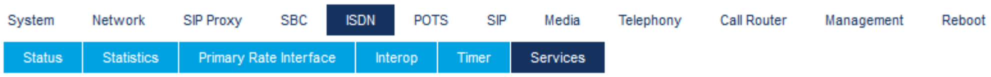
Interop Configuration

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

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

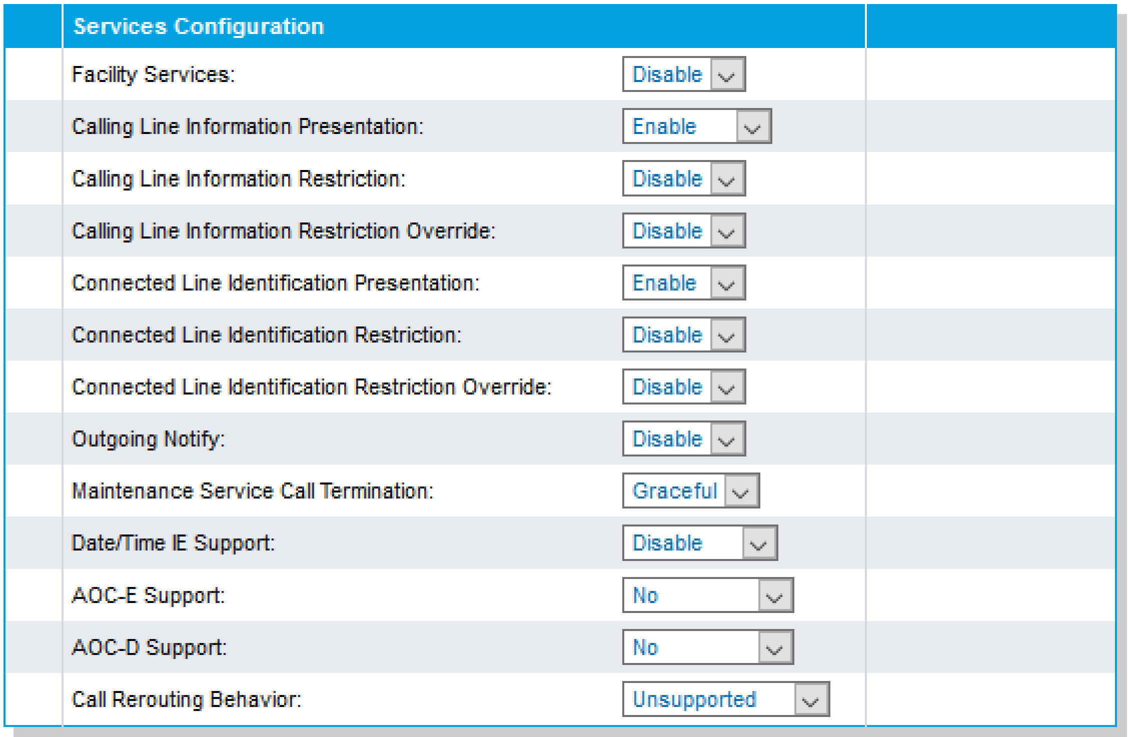
Services

Figure 4.50: ISDN Services



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

Figure 4.51: Services Configuration



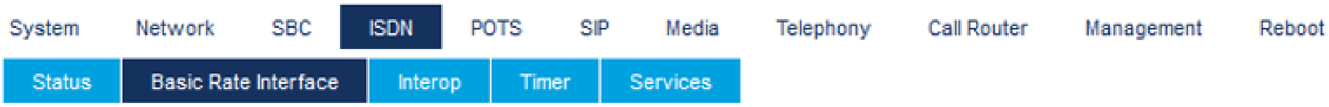
Services Configuration	
Facility Services:	Disable
Calling Line Information Presentation:	Enable
Calling Line Information Restriction:	Disable
Calling Line Information Restriction Override:	Disable
Connected Line Identification Presentation:	Enable
Connected Line Identification Restriction:	Disable
Connected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

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

Basic Rate Interface

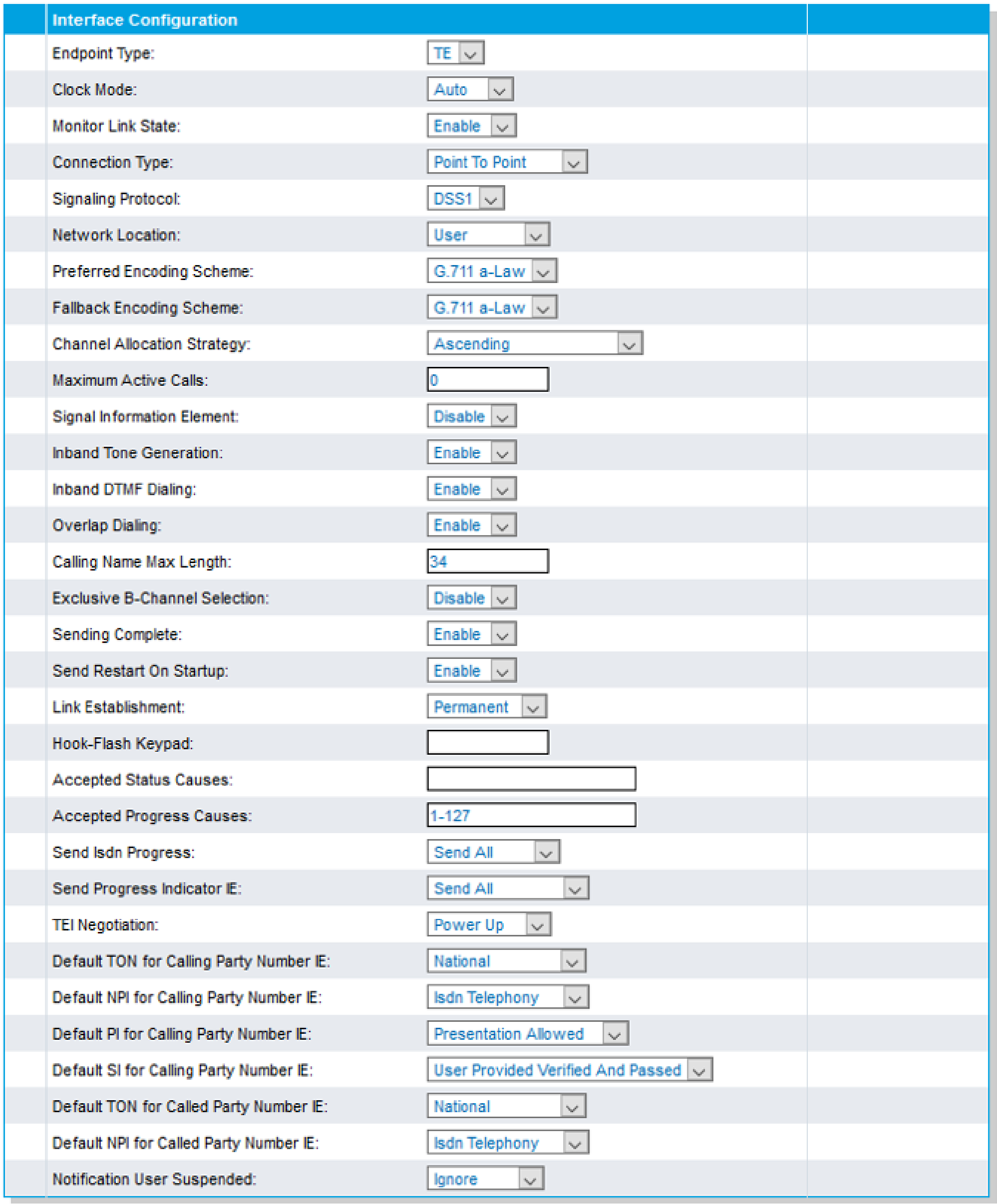
Settings

Figure 4.52: Settings



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

Figure 4.53: Interface Configuration



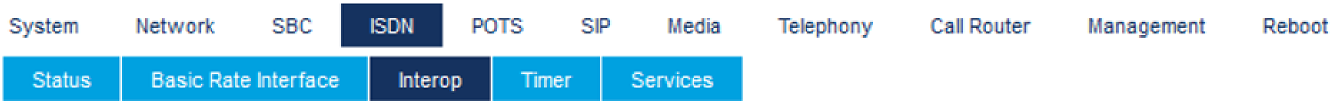
Interface Configuration

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

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

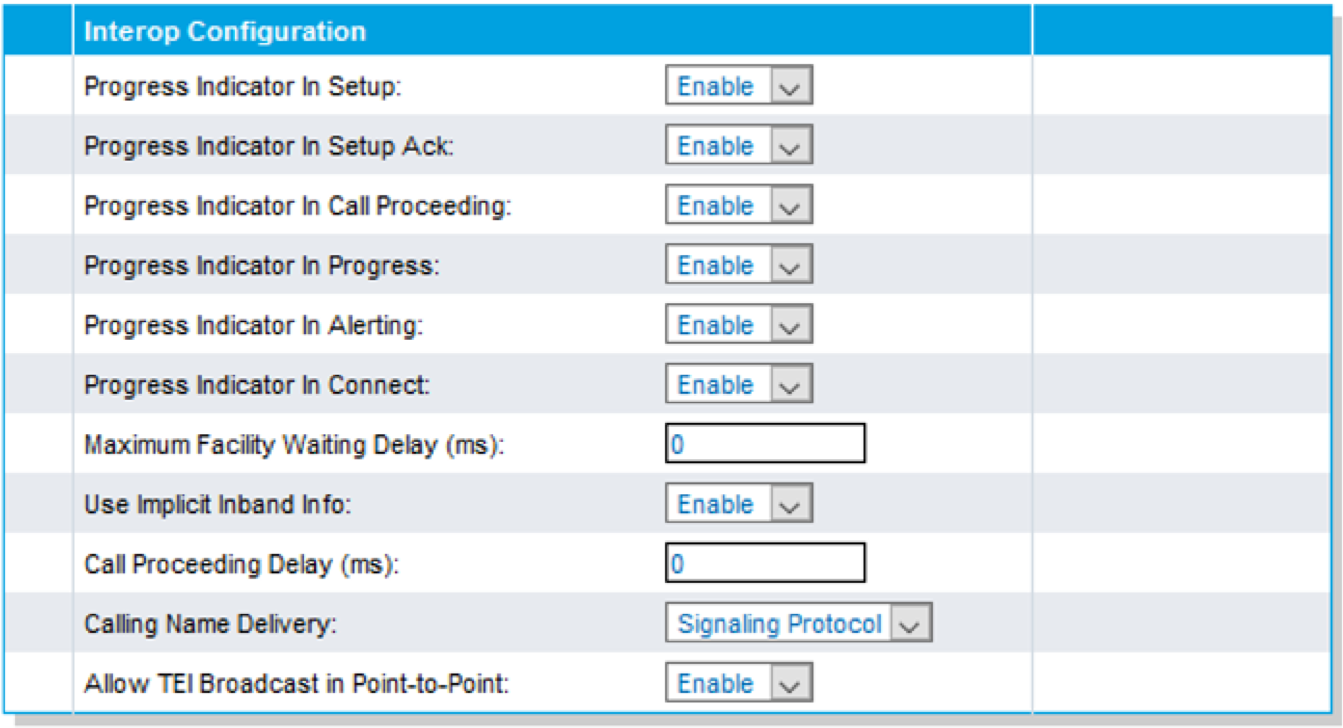
Interop

Figure 4.54: Interop



1. Select **ISDN** > **interop**.

Figure 4.55: Interop Configuration

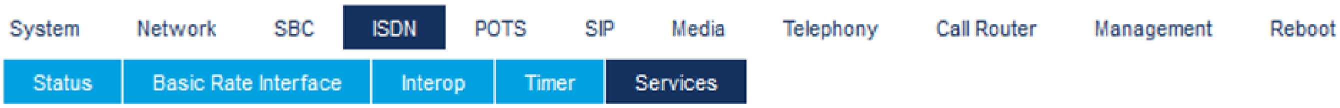


Interop Configuration	
Progress Indicator In Setup:	Enable
Progress Indicator In Setup Ack:	Enable
Progress Indicator In Call Proceeding:	Enable
Progress Indicator In Progress:	Enable
Progress Indicator In Alerting:	Enable
Progress Indicator In Connect:	Enable
Maximum Facility Waiting Delay (ms):	0
Use Implicit Inband Info:	Enable
Call Proceeding Delay (ms):	0
Calling Name Delivery:	Signaling Protocol
Allow TEI Broadcast in Point-to-Point:	Enable

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

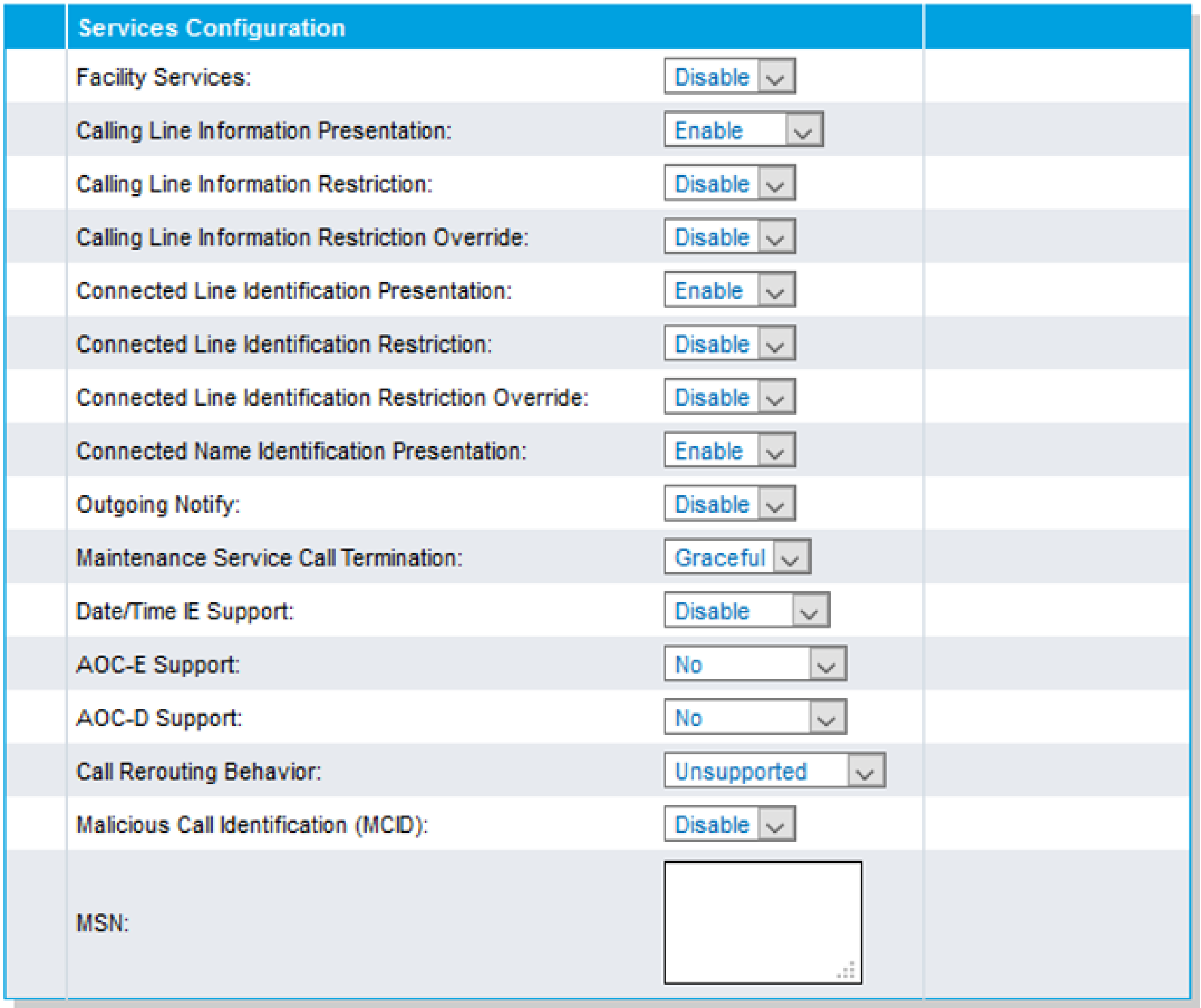
Services

Figure 4.56: Services



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

Figure 4.57: Services Configuration



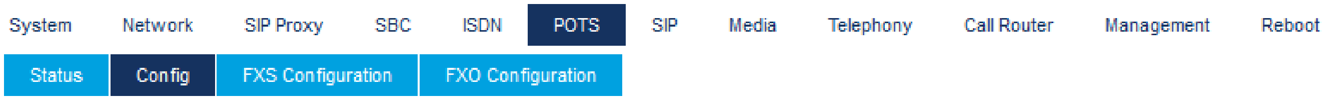
Services Configuration	
Facility Services:	Disable
Calling Line Information Presentation:	Enable
Calling Line Information Restriction:	Disable
Calling Line Information Restriction Override:	Disable
Connected Line Identification Presentation:	Enable
Connected Line Identification Restriction:	Disable
Connected Line Identification Restriction Override:	Disable
Connected Name Identification Presentation:	Enable
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
Malicious Call Identification (MCID):	Disable
MSN:	

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

POTS

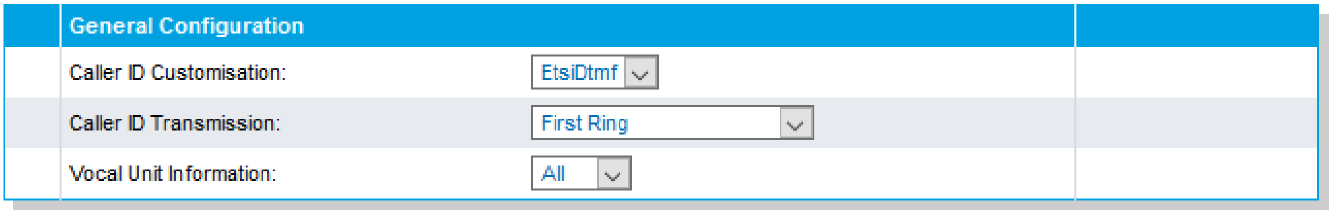
Config

Figure 4.58: Config



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

Figure 4.59: General Configuration



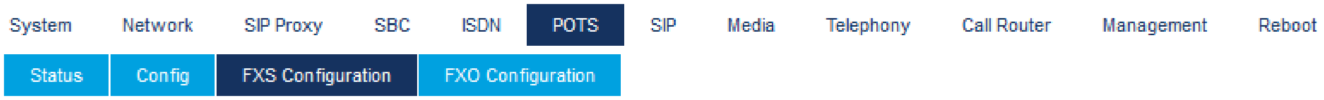
General Configuration

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

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

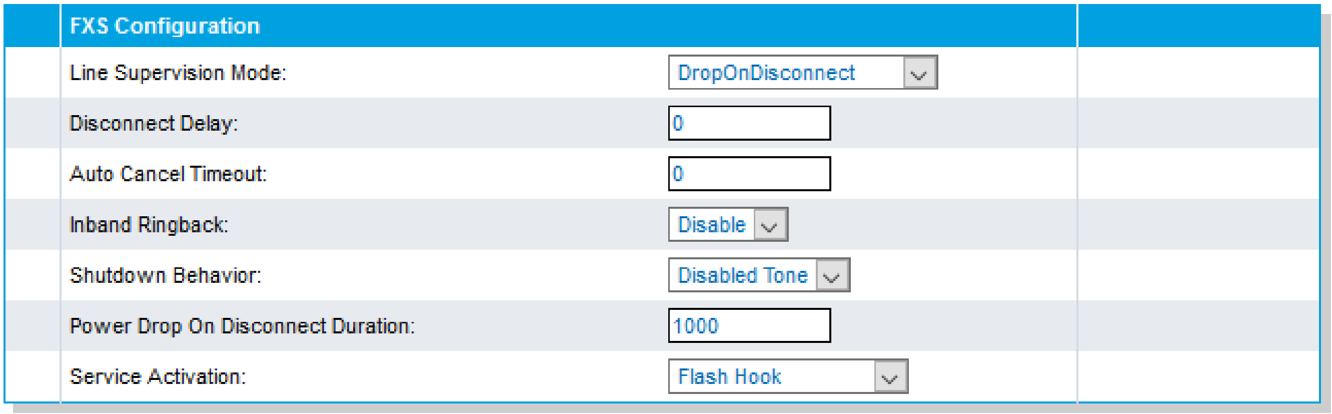
FXS Configuration

Figure 4.60: FXS Configuration



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

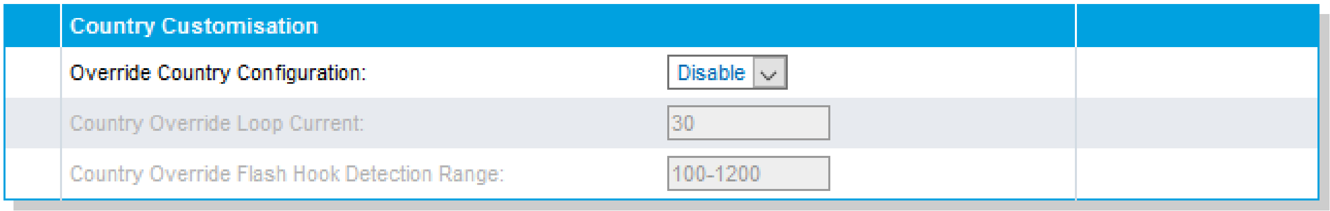
Figure 4.61: FXS Configuration



FXS Configuration

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

Figure 4.62: Country Customisation

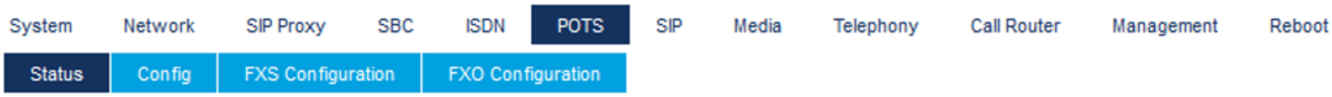


Country Customisation	
Override Country Configuration:	Disable
Country Override Loop Current:	30
Country Override Flash Hook Detection Range:	100-1200

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

FXO Configuration

Figure 4.63: FXO Configuration - Status



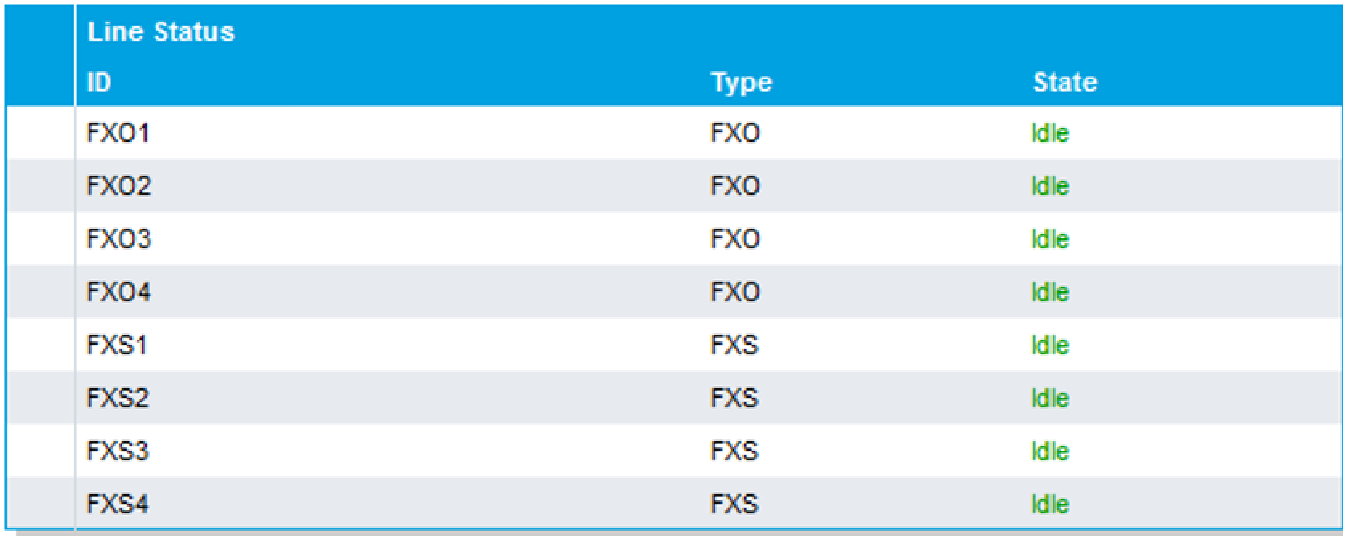
1. Select **POTS** > **FXO Configuration**.
This section is applicable If analogue trunks are used.

> **NOTE:** Only manual incoming is supported where there is no DID functionality. Only DTMF register signalling is supported for outgoing calls.

2. Ensure that all FXO ports are up and idle.

Status

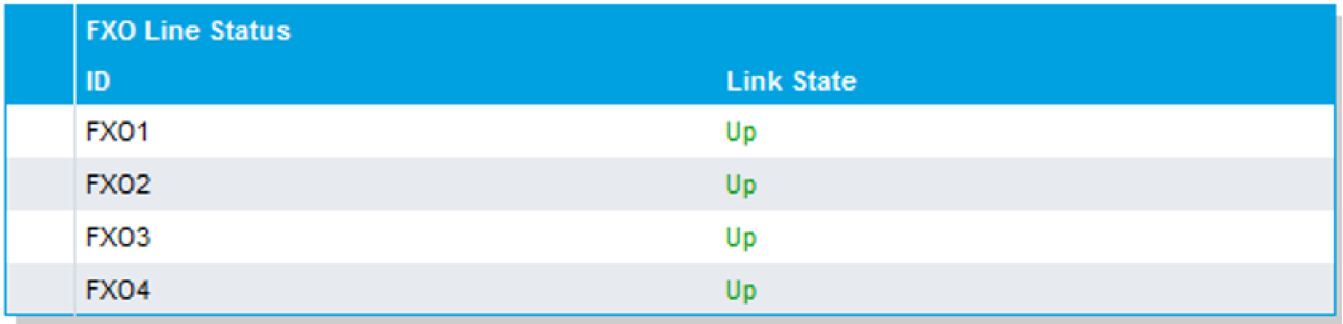
Figure 4.64: Status



Line Status

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

Figure 4.65: FXO Line Status

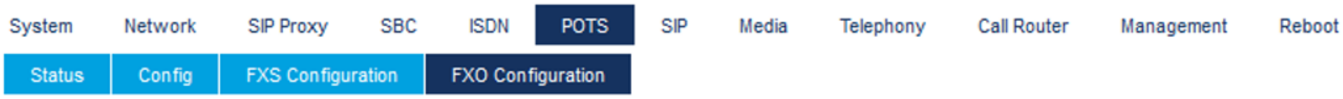


FXO Line Status

ID	Link State
FXO1	Up
FXO2	Up
FXO3	Up
FXO4	Up

1. Set specific FXO characteristics.

Figure 4.66: FXO Configuration

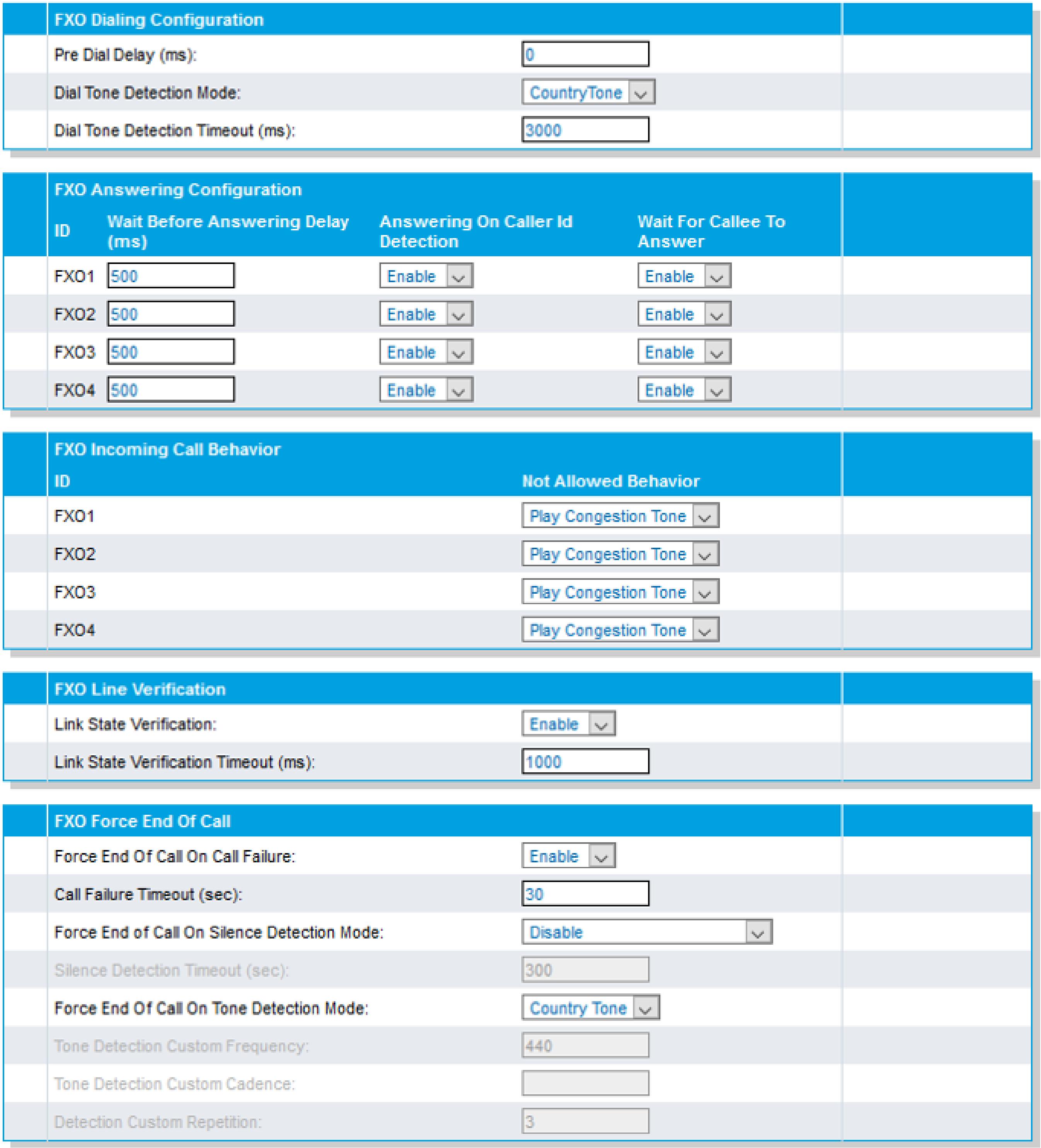


Select **POTS** > **FXO Configuration**.

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

FXO Dialing Configuration

Figure 4.67: FXO Dialing Configuration



FXO Dialing Configuration

Pre Dial Delay (ms):	0
Dial Tone Detection Mode:	CountryTone
Dial Tone Detection Timeout (ms):	3000

FXO Answering Configuration

ID	Wait Before Answering Delay (ms)	Answering On Caller Id Detection	Wait For Callee To Answer
FXO1	500	Enable	Enable
FXO2	500	Enable	Enable
FXO3	500	Enable	Enable
FXO4	500	Enable	Enable

FXO Incoming Call Behavior

ID	Not Allowed Behavior
FXO1	Play Congestion Tone
FXO2	Play Congestion Tone
FXO3	Play Congestion Tone
FXO4	Play Congestion Tone

FXO Line Verification

Link State Verification:	Enable
Link State Verification Timeout (ms):	1000

FXO Force End Of Call

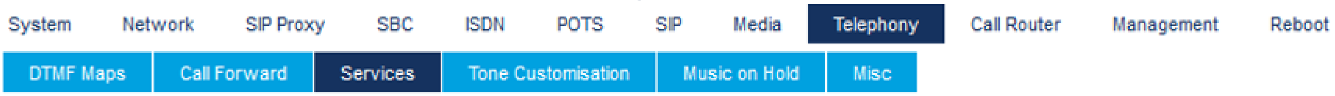
Force End Of Call On Call Failure:	Enable
Call Failure Timeout (sec):	30
Force End of Call On Silence Detection Mode:	Disable
Silence Detection Timeout (sec):	300
Force End Of Call On Tone Detection Mode:	Country Tone
Tone Detection Custom Frequency:	440
Tone Detection Custom Cadence:	
Detection Custom Repetition:	3

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

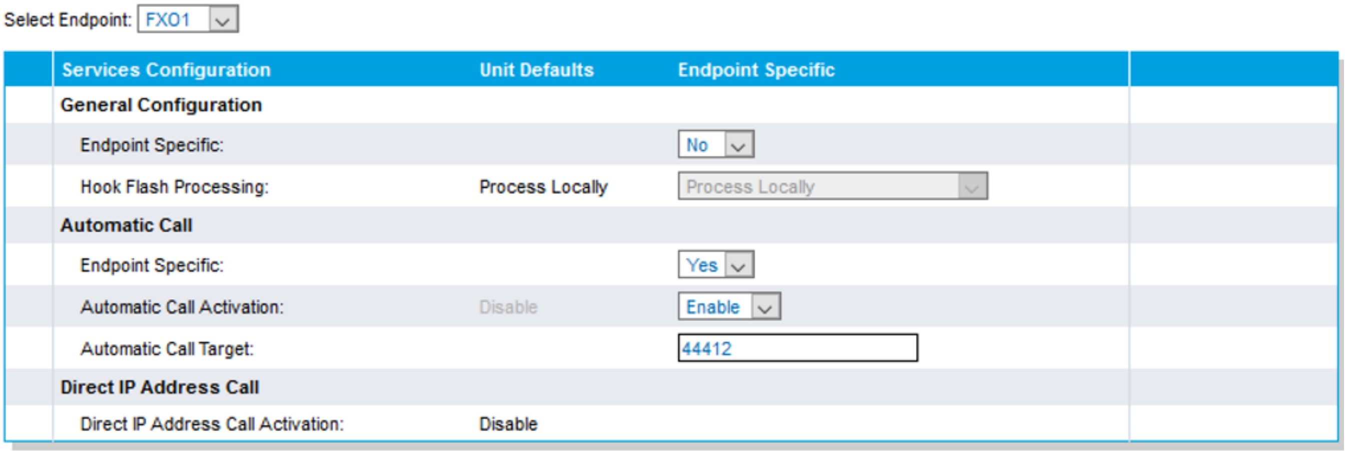
Services

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

Figure 4.68: Services



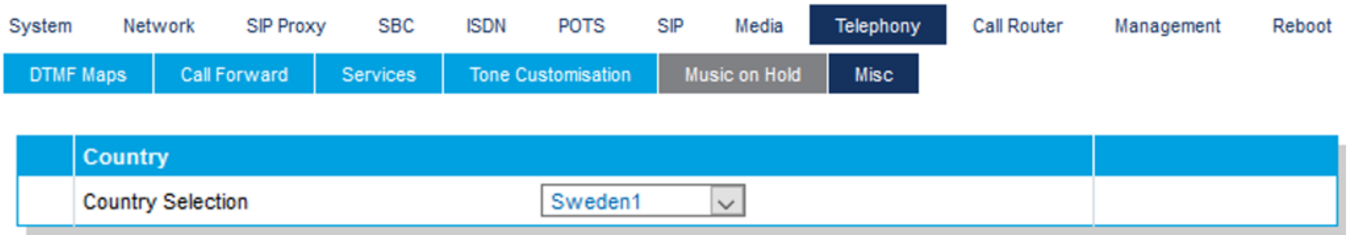
2. Set the **Automatic Call Target** field.



Select Endpoint: FXO1

Services Configuration	Unit Defaults	Endpoint Specific
General Configuration		
Endpoint Specific:		No
Hook Flash Processing:	Process Locally	Process Locally
Automatic Call		
Endpoint Specific:		Yes
Automatic Call Activation:	Disable	Enable
Automatic Call Target:		44412
Direct IP Address Call		
Direct IP Address Call Activation:	Disable	

3. Set the correct market (Country).

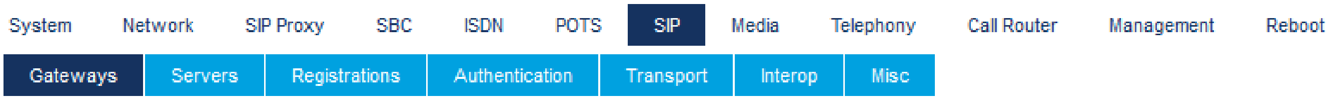


Country	
Country Selection	Sweden1

SIP

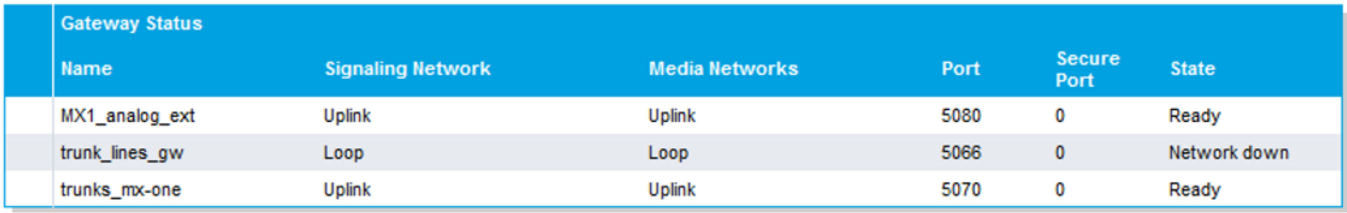
Gateways

Figure 4.69: Gateways



Select **SIP** > **Gateways**.

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

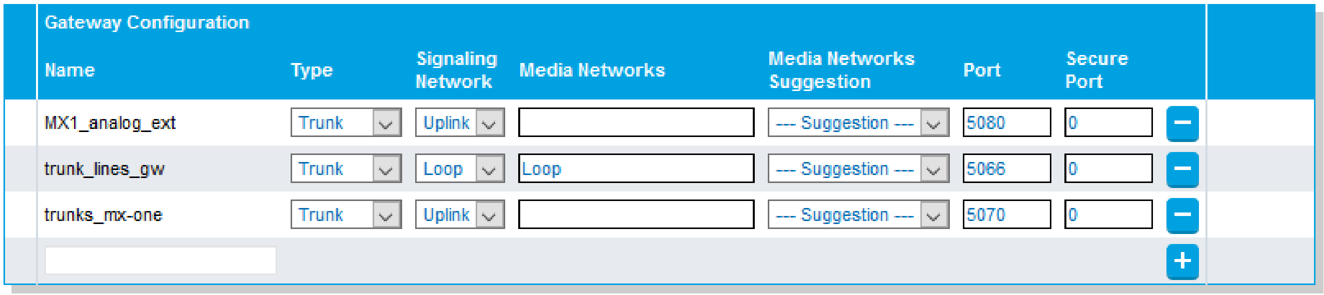


Gateway Status

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

Following gateways and port numbers are pre-defined.

Figure 4.70: trunks_mx-one

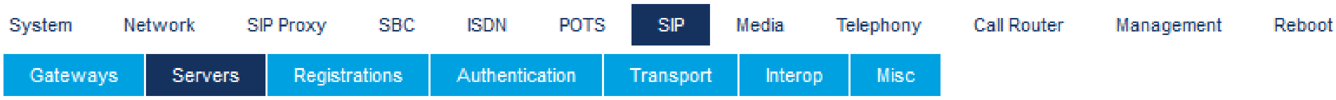


Gateway Configuration

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

Servers

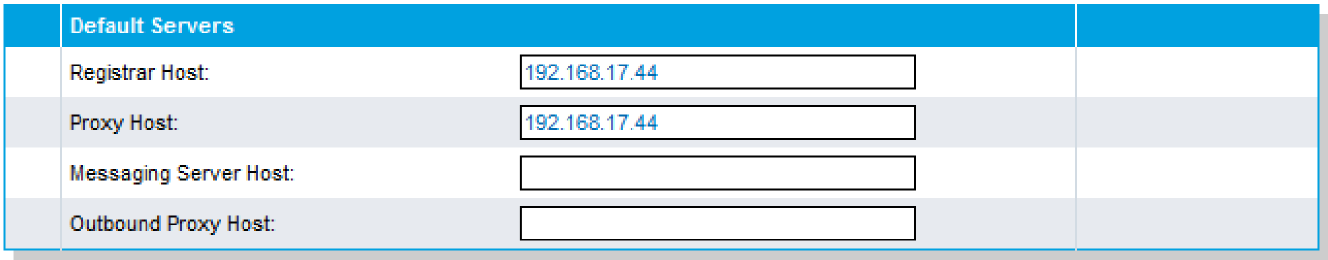
Figure 4.71: Servers



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

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

Figure 4.72: Default Servers

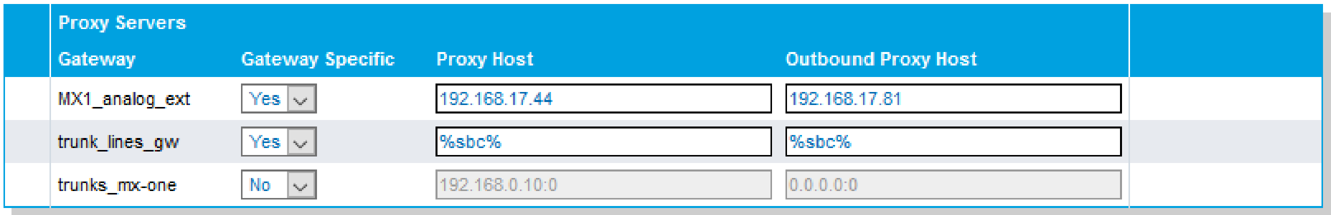


Default Servers

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

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

Figure 4.73: Proxy Servers

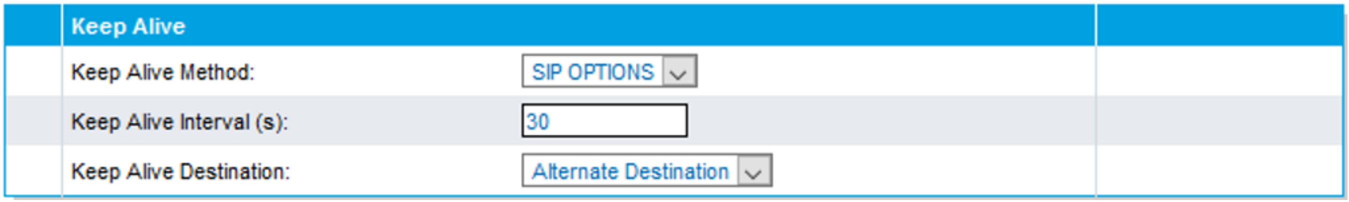


Proxy Servers

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

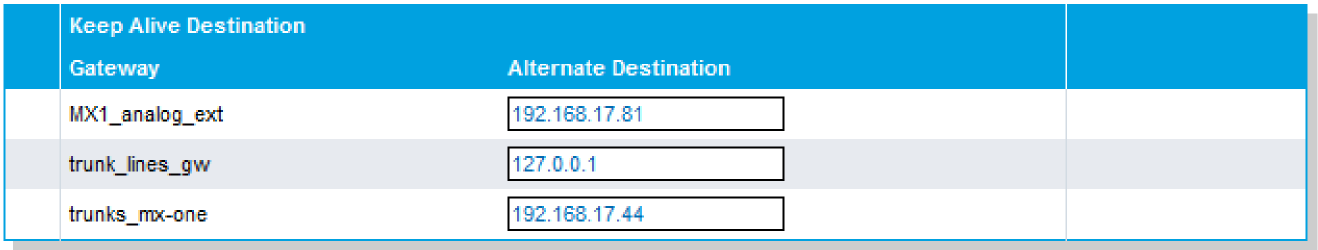
5. Change the **Keep Alive Method** to **SIP OPTIONS** and enter **Keep Alive Destination** Gateways.

Figure 4.74: Keep Alive



Keep Alive	
Keep Alive Method:	SIP OPTIONS
Keep Alive Interval (s):	30
Keep Alive Destination:	Alternate Destination

Figure 4.75: Alternate Alive Destination Gateway



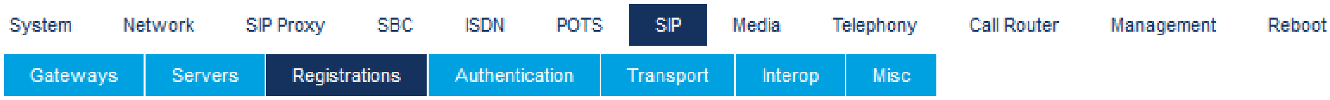
Keep Alive Destination

Gateway	Alternate Destination
MX1_analog_ext	192.168.17.81
trunk_lines_gw	127.0.0.1
trunks_mx-one	192.168.17.44

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

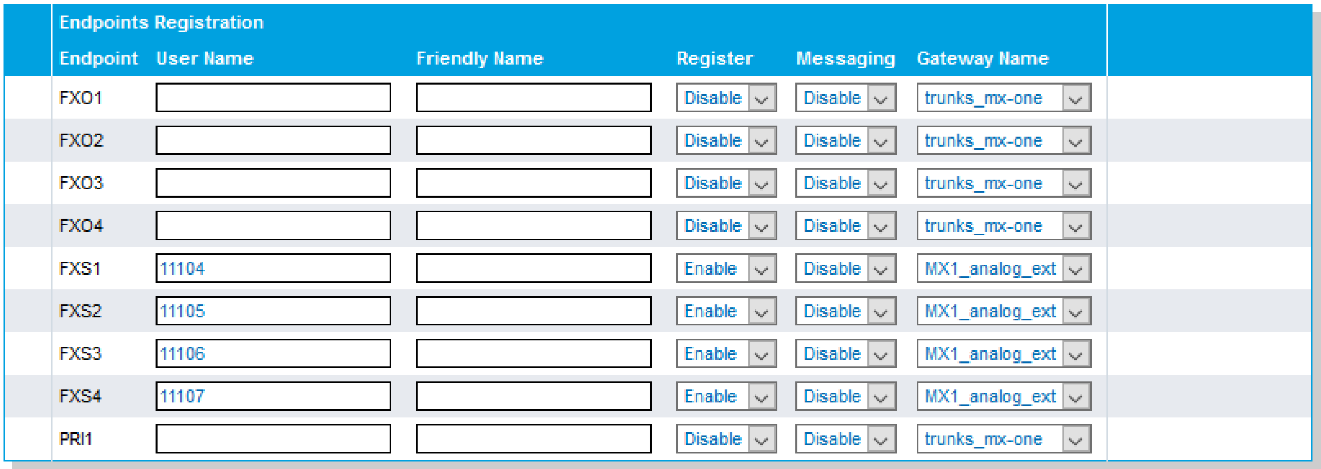
Registrations

Figure 4.76: Registrations



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

Figure 4.77: Endpoints Registration screen



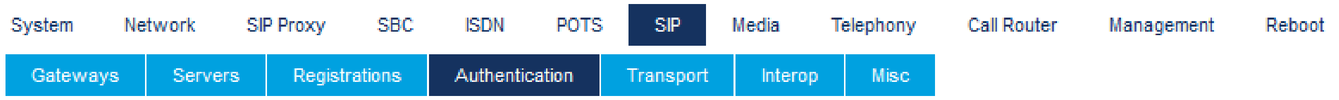
Endpoints Registration

Endpoint	User Name	Friendly Name	Register	Messaging	Gateway Name
FXO1			Disable	Disable	trunks_mx-one
FXO2			Disable	Disable	trunks_mx-one
FXO3			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

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

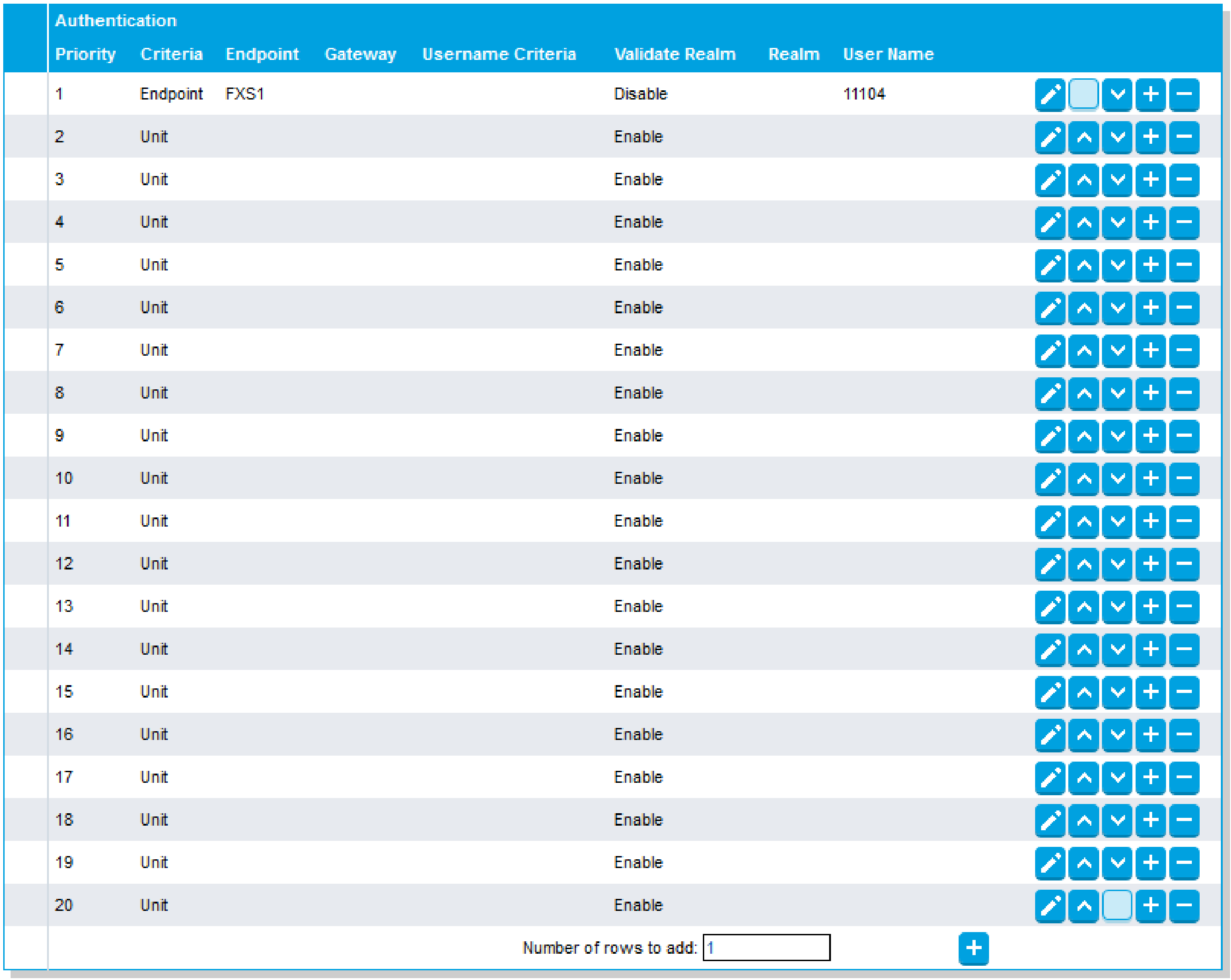
Authentication

Figure 4.78: Authentication



1. Select **SIP** > **Authentication**.

Figure 4.79: Authentication Screen



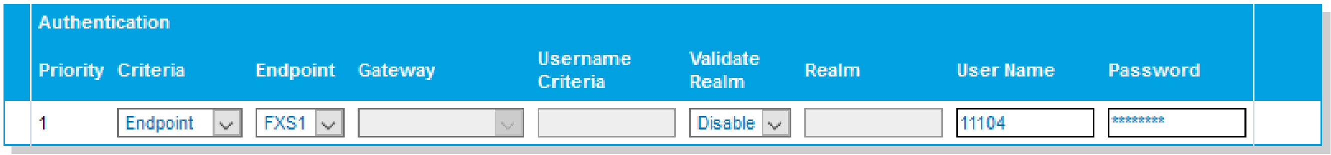
Authentication

Priority	Criteria	Endpoint	Gateway	Username Criteria	Validate Realm	Realm	User Name
1	Endpoint	FXS1			Disable		11104
2	Unit				Enable		
3	Unit				Enable		
4	Unit				Enable		
5	Unit				Enable		
6	Unit				Enable		
7	Unit				Enable		
8	Unit				Enable		
9	Unit				Enable		
10	Unit				Enable		
11	Unit				Enable		
12	Unit				Enable		
13	Unit				Enable		
14	Unit				Enable		
15	Unit				Enable		
16	Unit				Enable		
17	Unit				Enable		
18	Unit				Enable		
19	Unit				Enable		
20	Unit				Enable		

Number of rows to add: 1

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

Figure 4.80: Validate Realm field

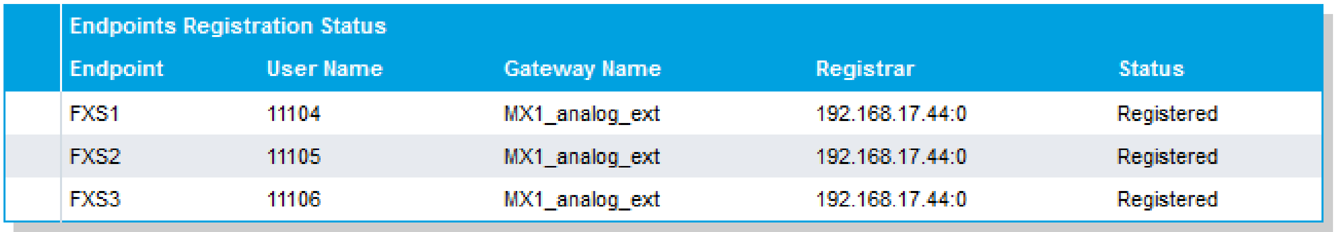


Authentication

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

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

Figure 4.81: Endpoints Registration Status

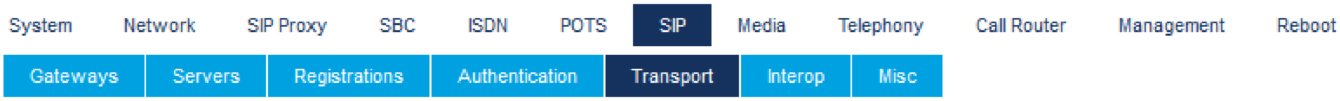


Endpoints Registration Status

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

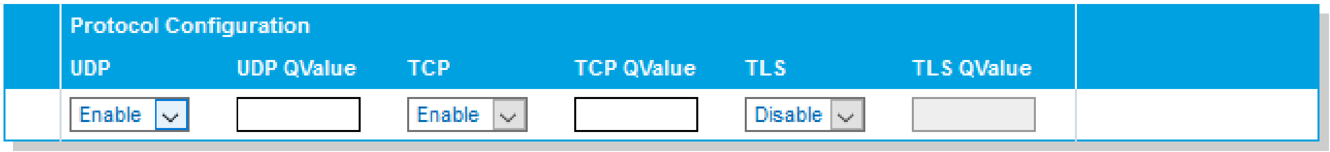
Transport

Figure 4.82: Transport



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

Figure 4.83: Protocol Configuration



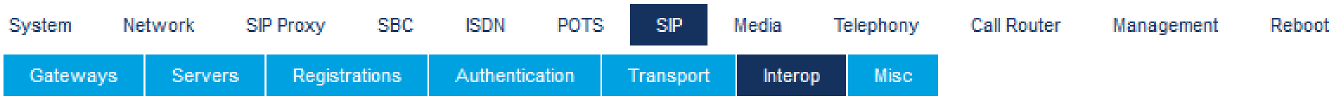
Protocol Configuration

UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable		Enable		Disable	

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

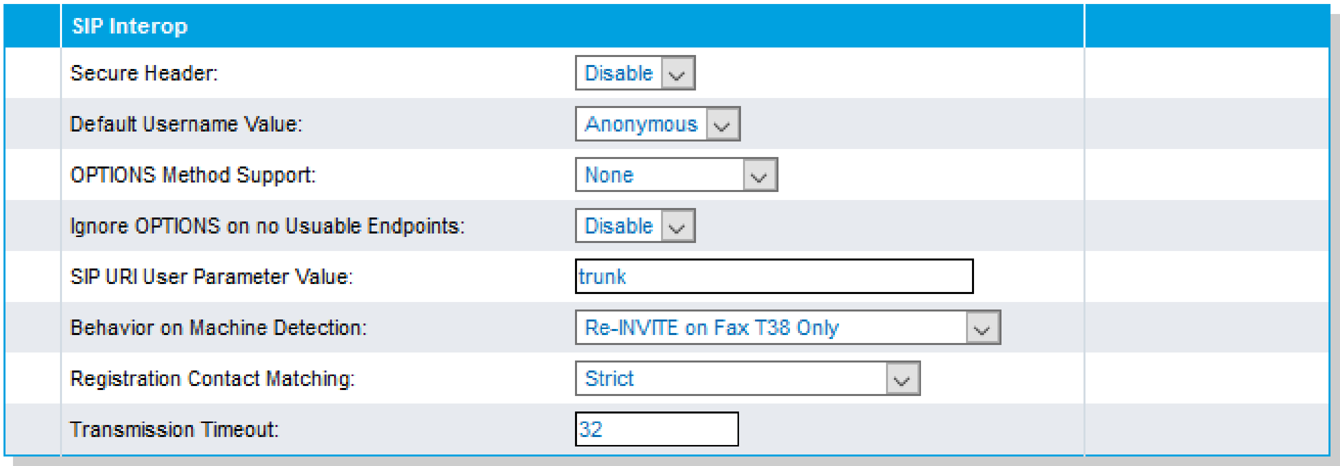
Interop

Figure 4.84: Interop



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

Figure 4.85: SIP URI User Parameter Value field

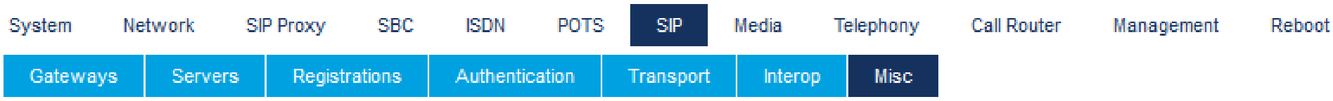


SIP Interop	
Secure Header:	Disable
Default Username Value:	Anonymous
OPTIONS Method Support:	None
Ignore OPTIONS on no Usuable Endpoints:	Disable
SIP URI User Parameter Value:	trunk
Behavior on Machine Detection:	Re-INVITE on Fax T38 Only
Registration Contact Matching:	Strict
Transmission Timeout:	32

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

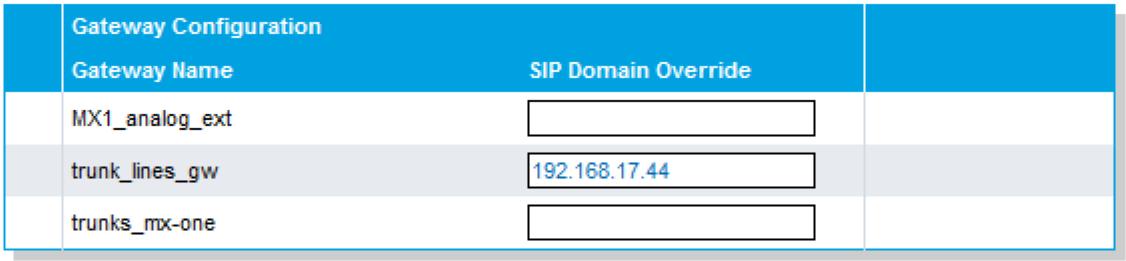
Misc

Figure 4.86: Misc



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

Figure 4.87: Gateway Configuration field



Gateway Configuration

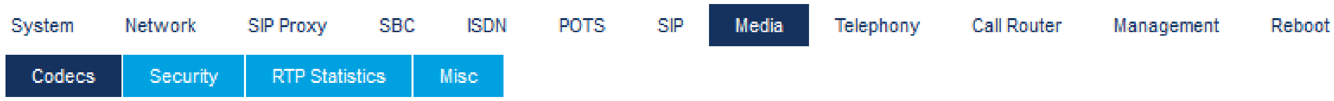
Gateway Name	SIP Domain Override
MX1_analog_ext	
trunk_lines_gw	192.168.17.44
trunks_mx-one	

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

Media

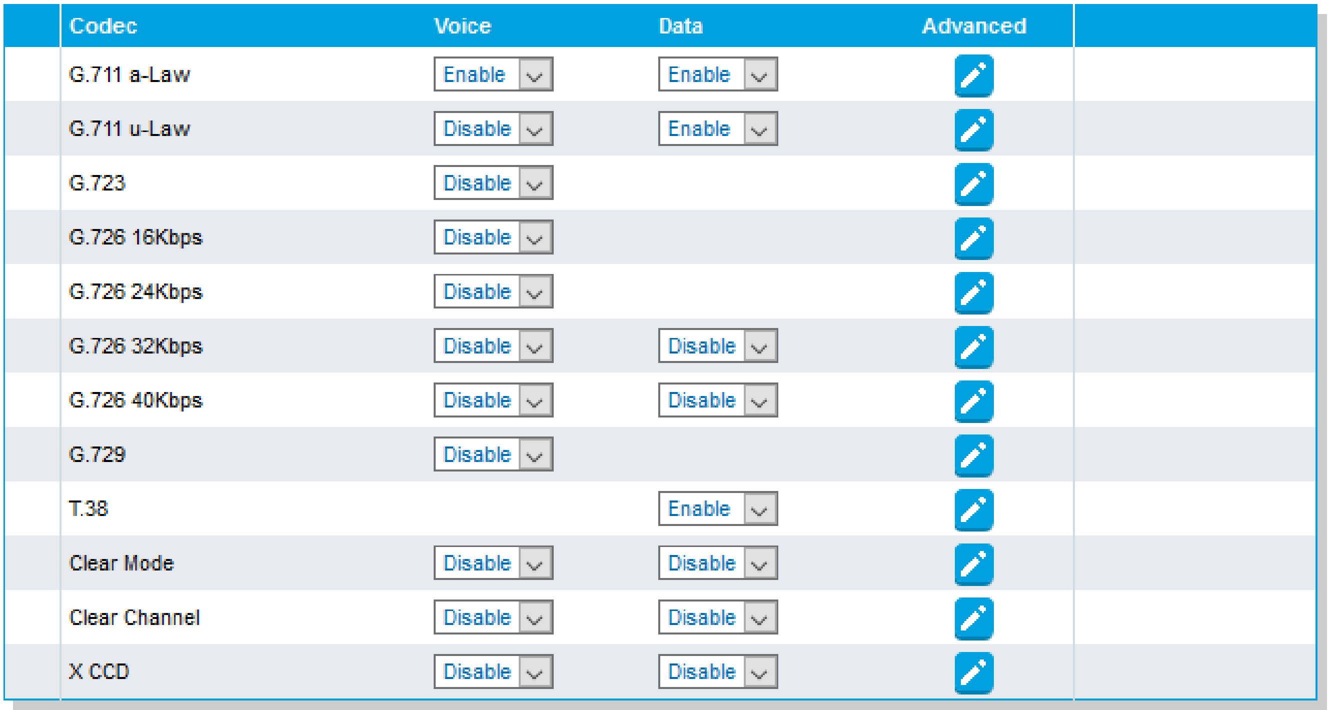
Codecs

Figure 4.88: Codecs



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

Figure 4.89: Codecs



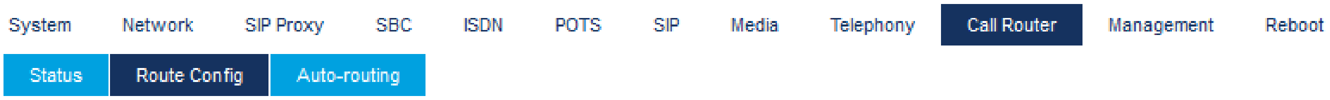
	Codec	Voice	Data	Advanced	
	G.711 a-Law	Enable	Enable	✎	
	G.711 u-Law	Disable	Enable	✎	
	G.723	Disable		✎	
	G.726 16Kbps	Disable		✎	
	G.726 24Kbps	Disable		✎	
	G.726 32Kbps	Disable	Disable	✎	
	G.726 40Kbps	Disable	Disable	✎	
	G.729	Disable		✎	
	T.38		Enable	✎	
	Clear Mode	Disable	Disable	✎	
	Clear Channel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

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

Call Router

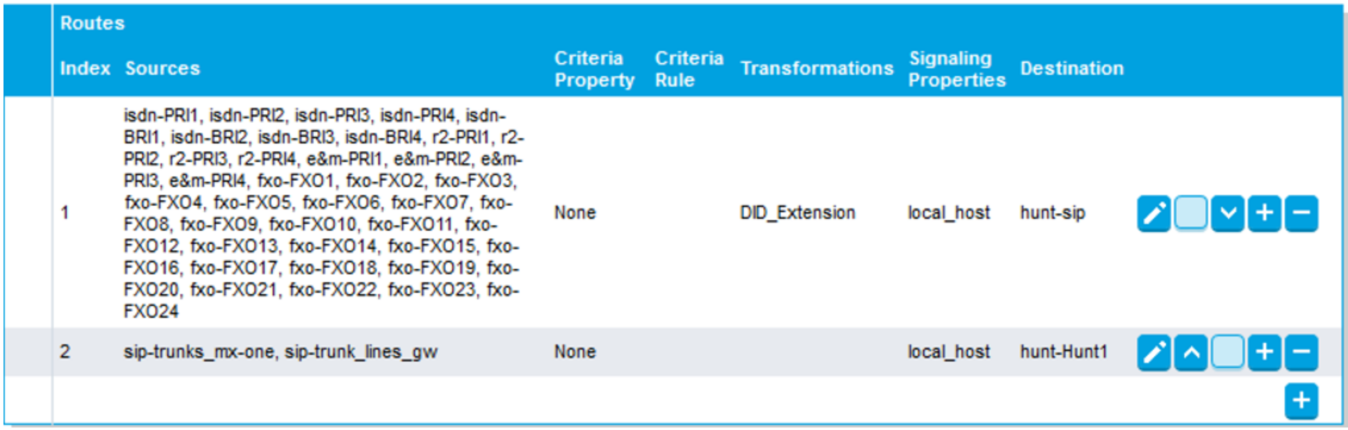
Route Config

Figure 4.90: Route Config



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

Figure 4.91: Routes

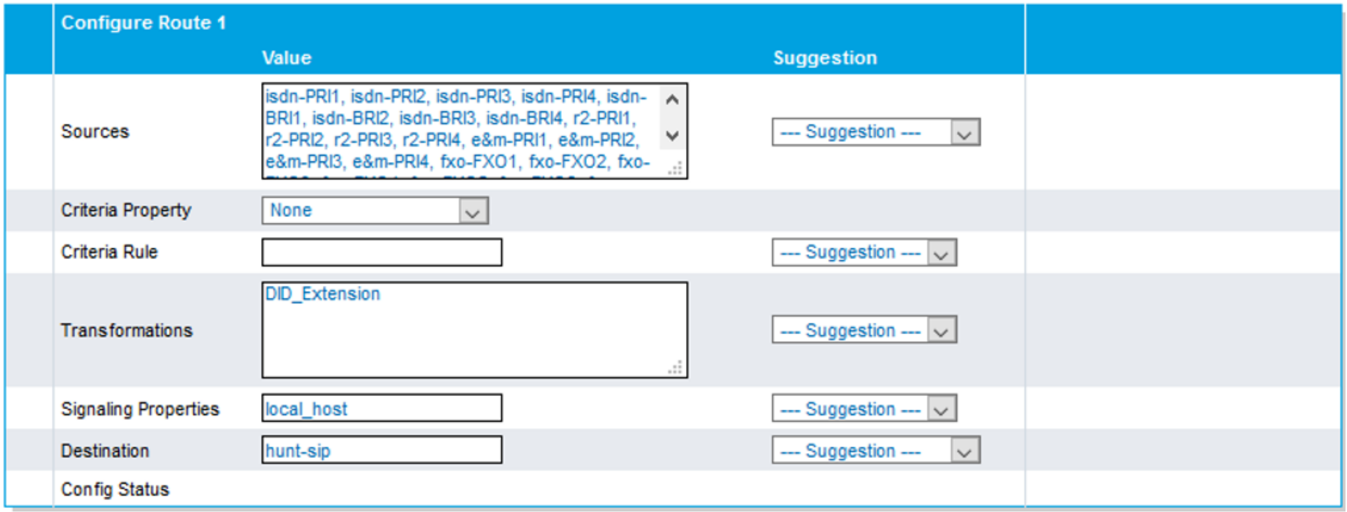


Routes

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

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

Figure 4.92: Configure Route 1

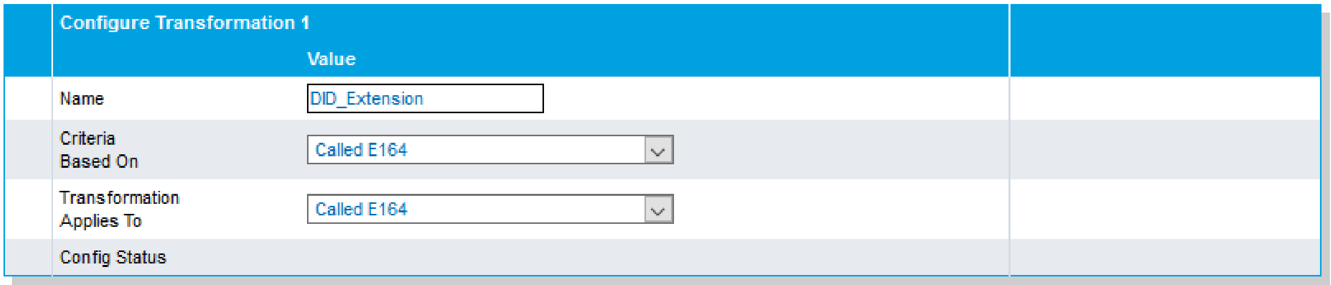


Configure Route 1

	Value	Suggestion
Sources	isdn-PRI1, isdn-PRI2, isdn-PRI3, isdn-PRI4, isdn-BRI1, isdn-BRI2, isdn-BRI3, isdn-BRI4, r2-PRI1, r2-PRI2, r2-PRI3, r2-PRI4, e&m-PRI1, e&m-PRI2, e&m-PRI3, e&m-PRI4, fxo-FXO1, fxo-FXO2, fxo-	--- Suggestion ---
Criteria Property	None	
Criteria Rule		--- Suggestion ---
Transformations	DID_Extension	--- Suggestion ---
Signaling Properties	local_host	--- Suggestion ---
Destination	hunt-sip	--- Suggestion ---
Config Status		

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

Figure 4.93: Configure Transformation 1



Configure Transformation 1

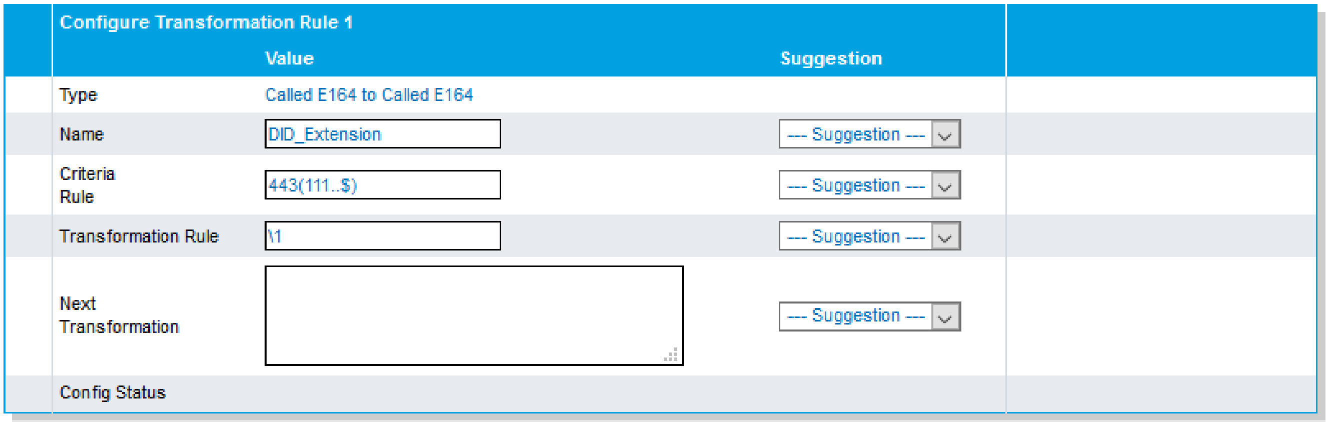
	Value
Name	DID_Extension
Criteria Based On	Called E164
Transformation Applies To	Called E164
Config Status	

7. Click **Save** or **Save and Insert Rule**.

8. Click Plus icon in the second Call Property Transformation, and enter the same name as above.

9. 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 4.94: Configure Transformation Rule 1 screen

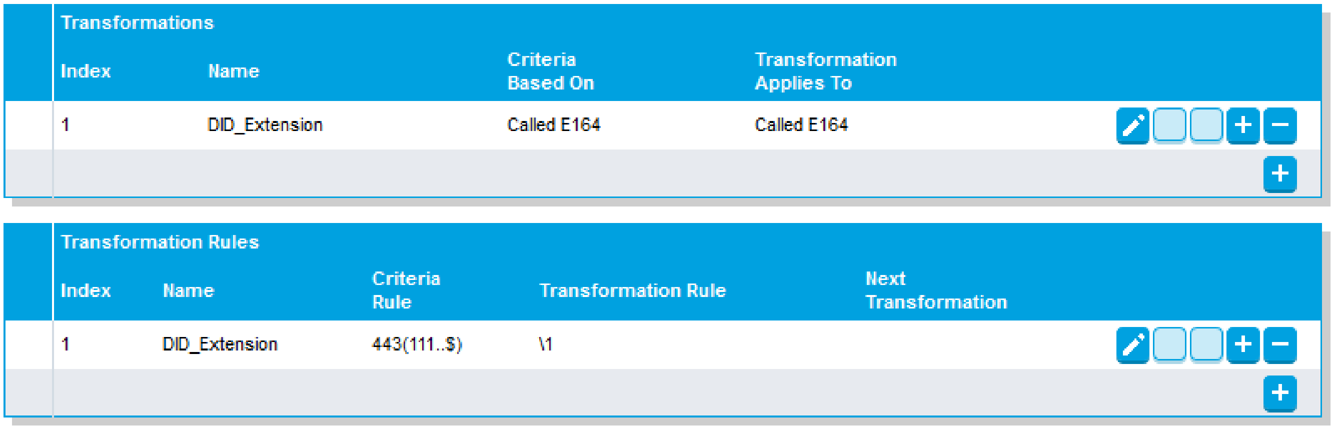


Configure Transformation Rule 1

	Value	Suggestion
Type	Called E164 to Called E164	
Name	DID_Extension	--- Suggestion ---
Criteria Rule	443(111..$)	--- Suggestion ---
Transformation Rule	\1	--- Suggestion ---
Next Transformation		--- Suggestion ---
Config Status		

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

Figure 4.95: Transformations



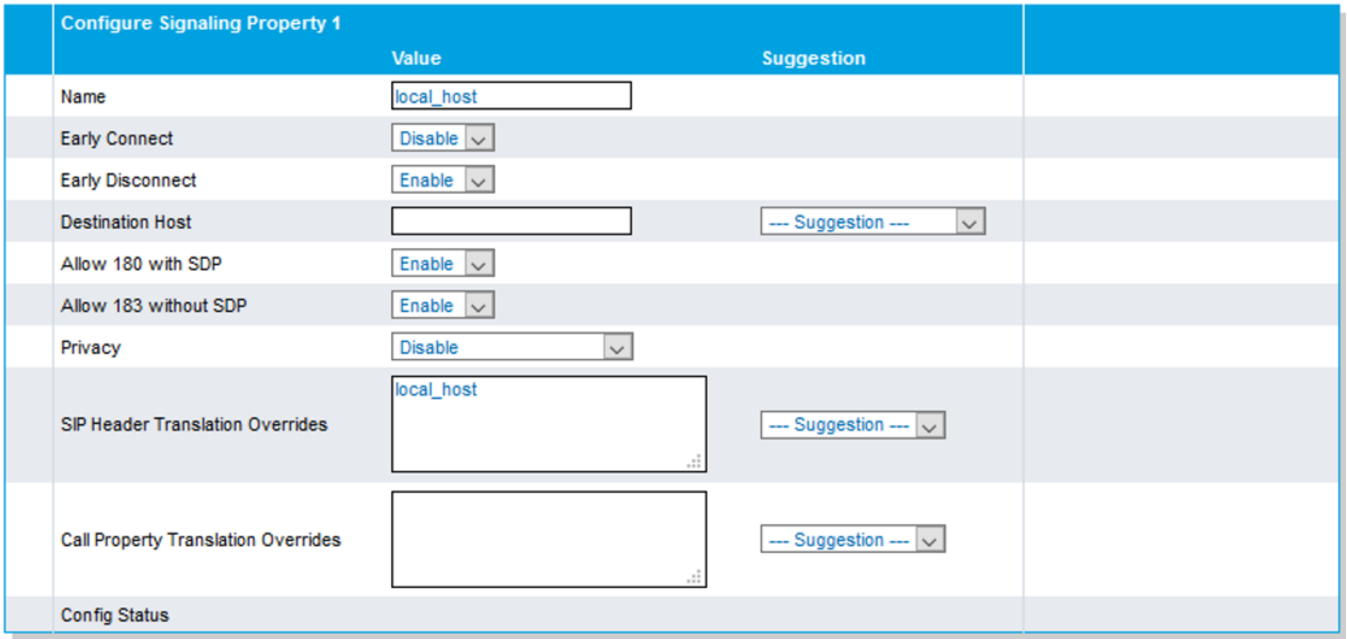
Transformations

Index	Name	Criteria Based On	Transformation Applies To	
1	DID_Extension	Called E164	Called E164	✎ + −
				+

Transformation Rules

Index	Name	Criteria Rule	Transformation Rule	Next Transformation	
1	DID_Extension	443(111..$)	\1		✎ + −
					+

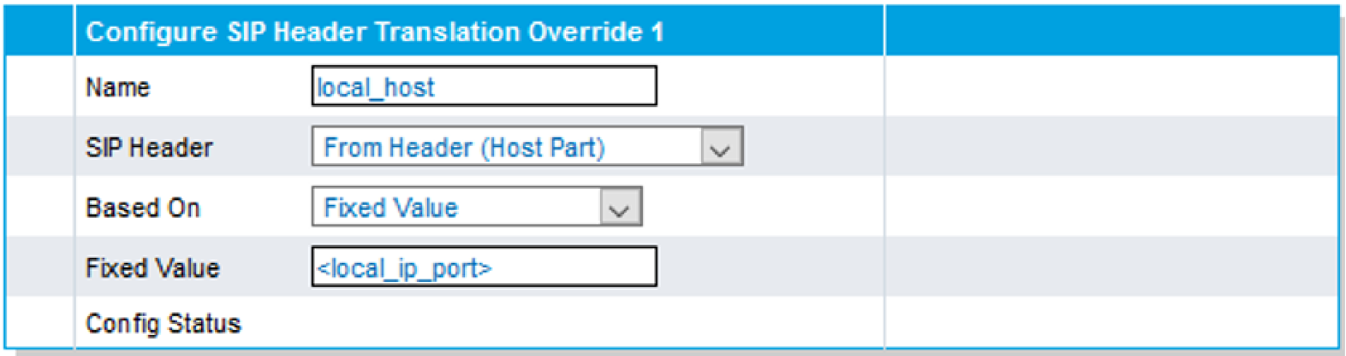
11. Click Plus icon for the Signaling Properties, and enter the data as shown below.



Configure Signaling Property 1

	Value	Suggestion
Name	local_host	
Early Connect	Disable	
Early Disconnect	Enable	
Destination Host		--- Suggestion ---
Allow 180 with SDP	Enable	
Allow 183 without SDP	Enable	
Privacy	Disable	
SIP Header Translation Overrides	local_host	--- Suggestion ---
Call Property Translation Overrides		--- Suggestion ---
Config Status		

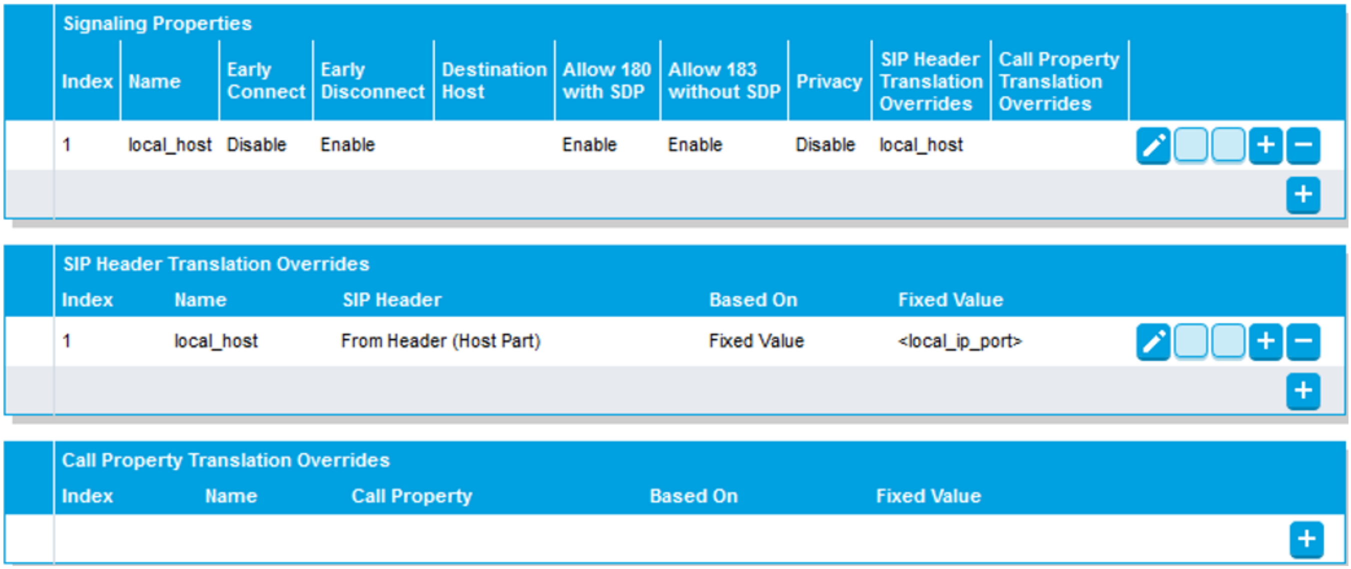
12. Click Plus icon for the SIP Header Translation Overrides, and enter the data as shown below.



Configure SIP Header Translation Override 1

Name	local_host
SIP Header	From Header (Host Part)
Based On	Fixed Value
Fixed Value	<local_ip_port>
Config Status	

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



Signaling Properties

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

SIP Header Translation Overrides

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

Call Property Translation Overrides

Index	Name	Call Property	Based On	Fixed Value

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

Management

Backup/Restore

1. Click **Activate unsecure script transfers through web browser**

Figure 4.96: Image Configuration screen

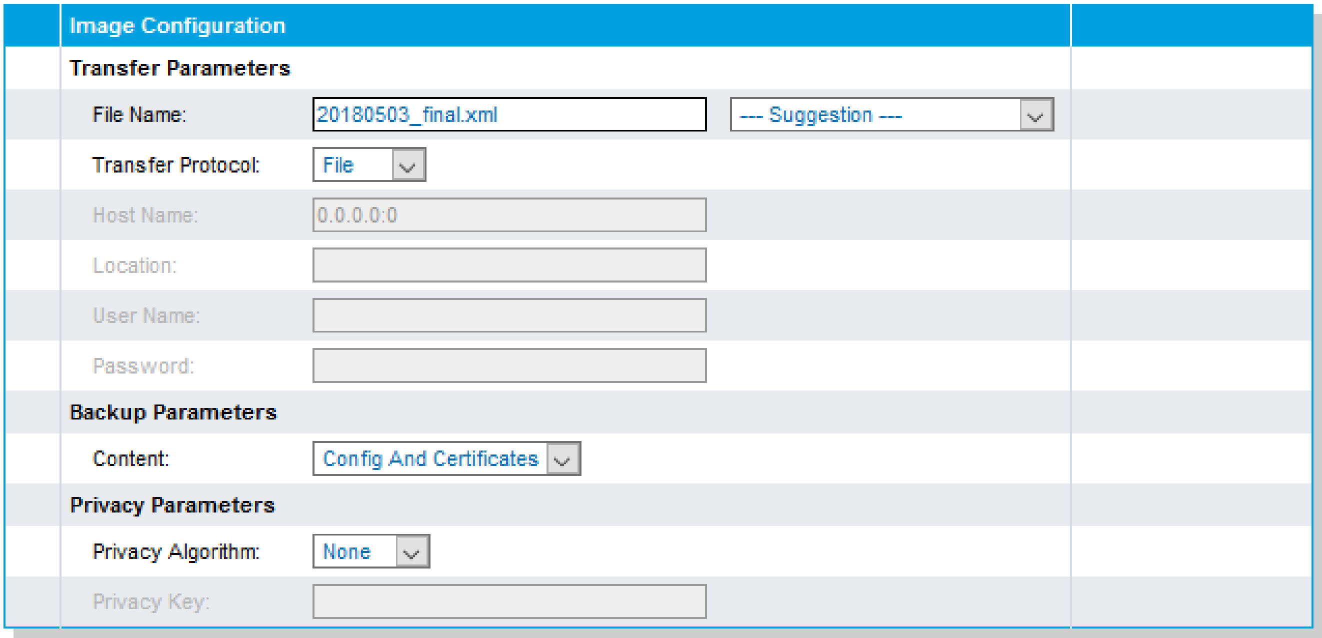


Image Configuration

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

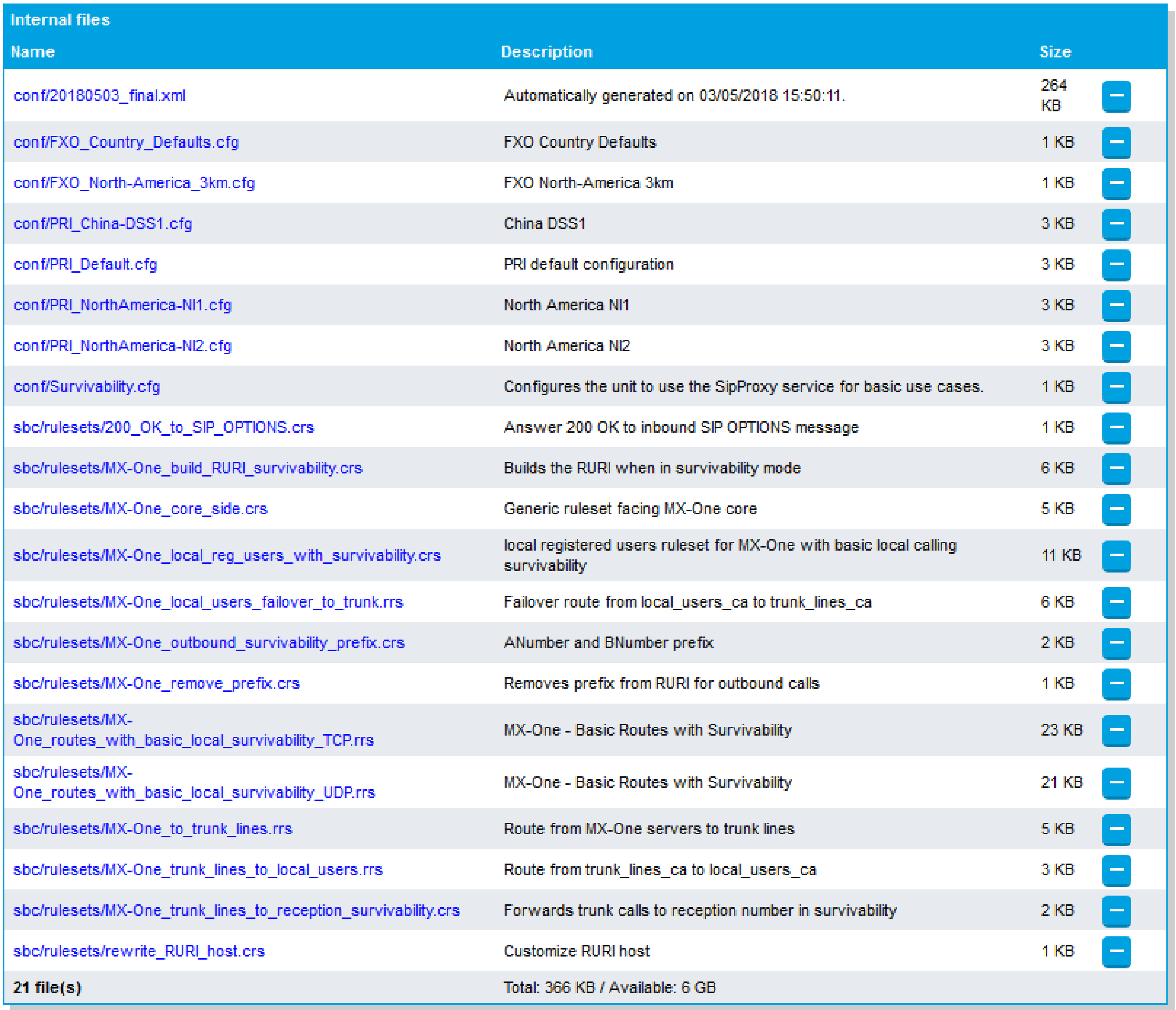
Privacy Parameters

Privacy Algorithm:	None
Privacy Key:	

2. Click **Apply and Backup Now**.

File

Figure 4.97: Internal files screen

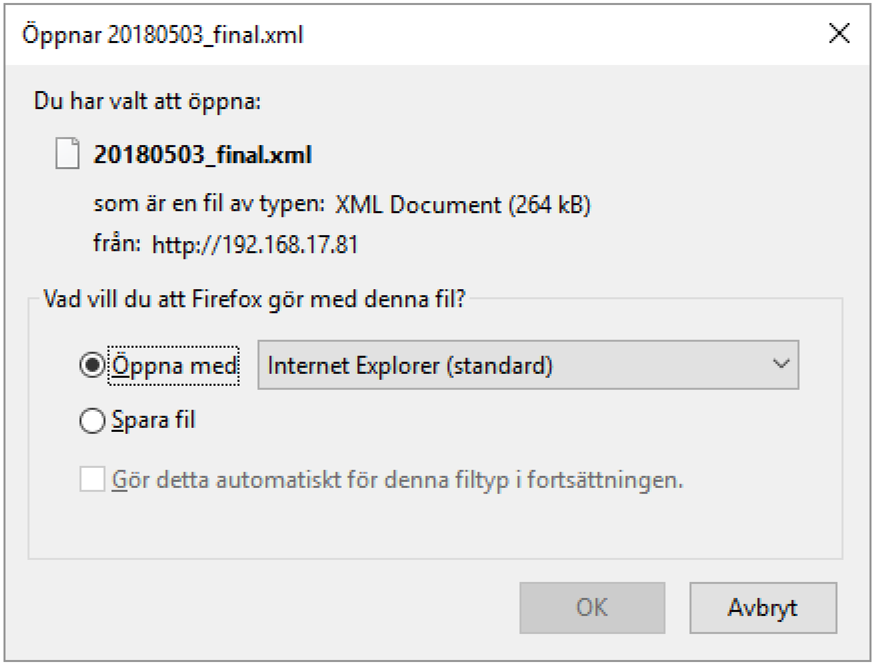


Internal files

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

Find the previously made backup image.

Figure 4.98: Backup image



Öppnar 20180503_final.xml

Du har valt att öppna:

20180503_final.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?

● Öppna med Internet Explorer (standard)

○ Spara fil

□ Gör detta automatiskt för denna filtyp i fortsättningen.

Setting up GX-GATEWAY with SIP Trunks

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

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

Logon

This section describes how to setup BO#2.

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

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

Figure 4.99: Login page

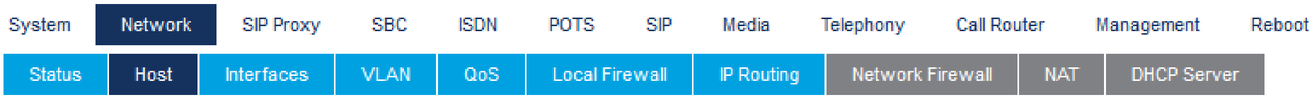
- User name/password: public /
- User name/password: admin/administrator

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

Network Settings

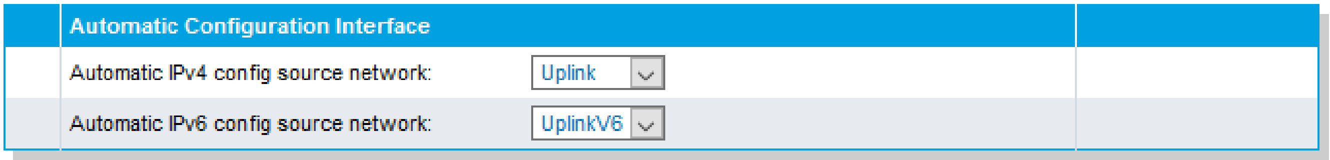
Host

Figure 4.100: Host Settings - 1



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

Figure 4.101: Host Settings - 2

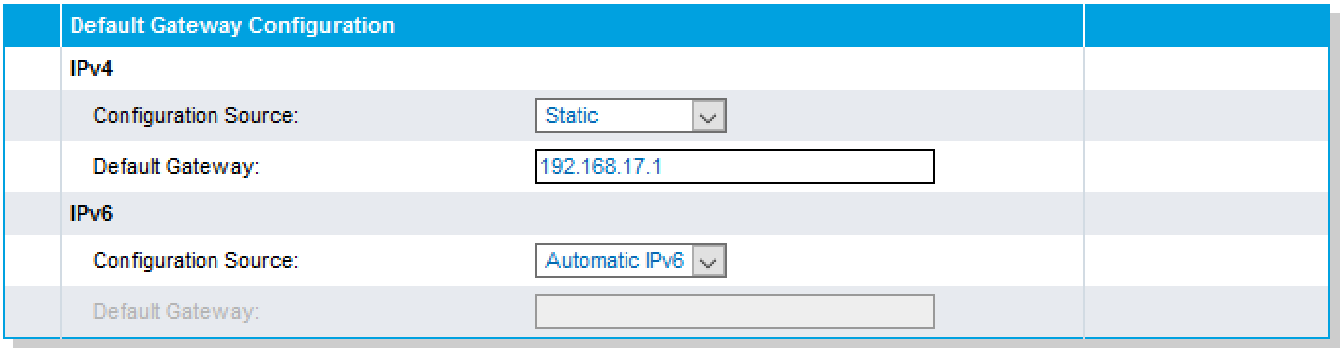


Automatic Configuration Interface

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

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

Figure 4.102: Changing Static IP Address

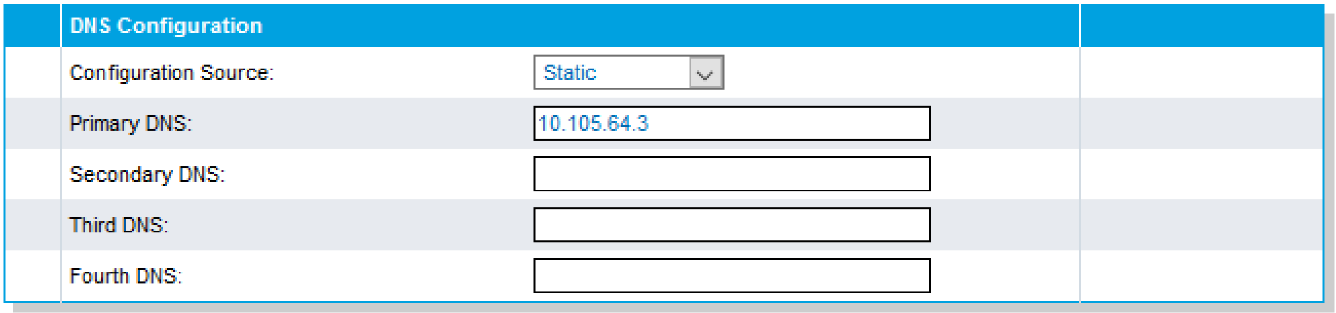


Default Gateway Configuration

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 4.103: Changing Static DNS Server

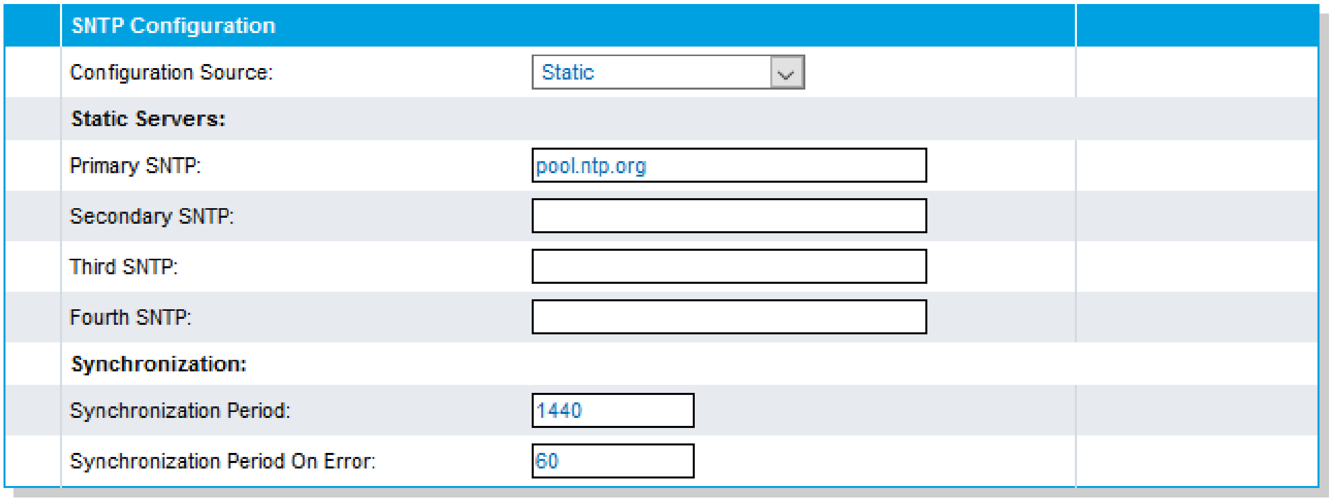


DNS Configuration

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

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

Figure 4.104: Changing to Static SNTP Server



SNTP Configuration

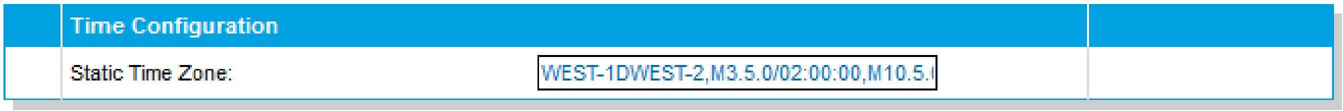
Configuration Source:	Static
Static Servers:	
Primary SNTP:	pool.ntp.org
Secondary SNTP:	
Third SNTP:	
Fourth SNTP:	
Synchronization:	
Synchronization Period:	1440
Synchronization Period On Error:	60

5. Set the **Time Zone**.

   Valid options are:

   - Pacific Time (Canada and US): PST8PDT7,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Mountain Time (Canada and US): MST7MDT6,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Central Time (Canada and US): CST6CDT5,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Eastern Time (Canada and US): EST5EDT4,M3.2.0/02:00:00,M11.1.0/02:00:00
   - Atlantic Time (Canada): AST4ADT3,M3.2.0/02:00:00,M11.1.0/02:00:00
   - GMT Standard Time: GMT0DMT-1,M3.5.0/01:00:00,M10.5.0/02:00:00
   - W. Europe Standard Time: WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00
   - China Standard Time: CST-8
   - Tokyo Standard Time: TST-9
   - Central Australia Standard Time: CAUST-9:30DCAUST-10:30,M10.5.0/02:00:00,M3.5.0/02:00:00
   - Australia Eastern Standard Time: AUSEST-10AUSDST-11,M10.5.0/02:00:00,M3.5.0/02:00:00
   - UTC (Coordinated Universal Time): UTC0

Figure 4.105: Setting Static Time Zone



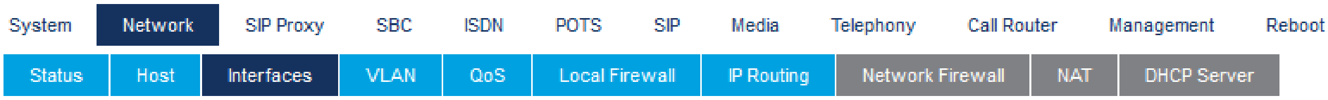
Time Configuration

Static Time Zone:	WEST-1DWEST-2,M3.5.0/02:00:00,M10.5.(

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

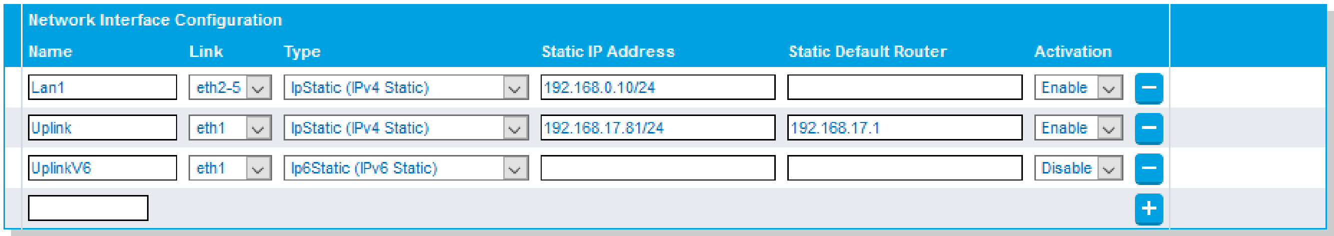
Interfaces

Figure 4.106: Interface



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

Figure 4.107: Changing Uplink to IpStatic



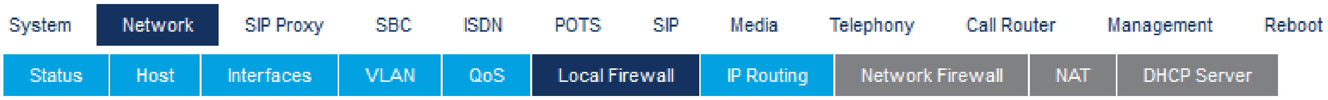
Network Interface Configuration

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

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

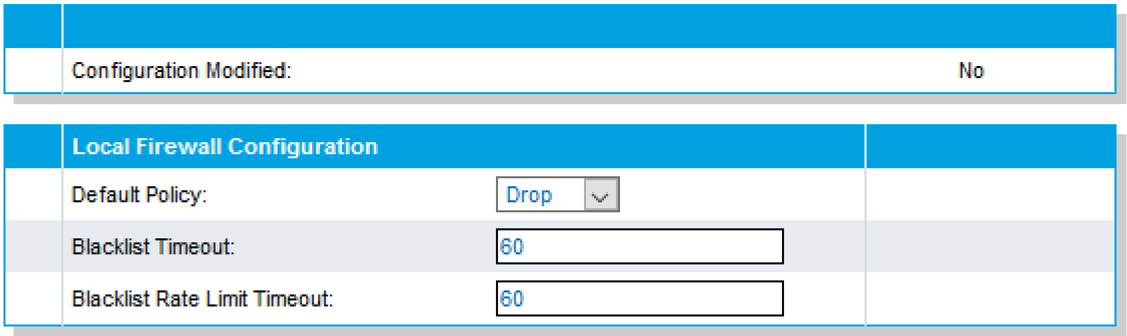
Local Firewalls

Figure 4.108: Local firewalls



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

Figure 4.109: Changing default policy



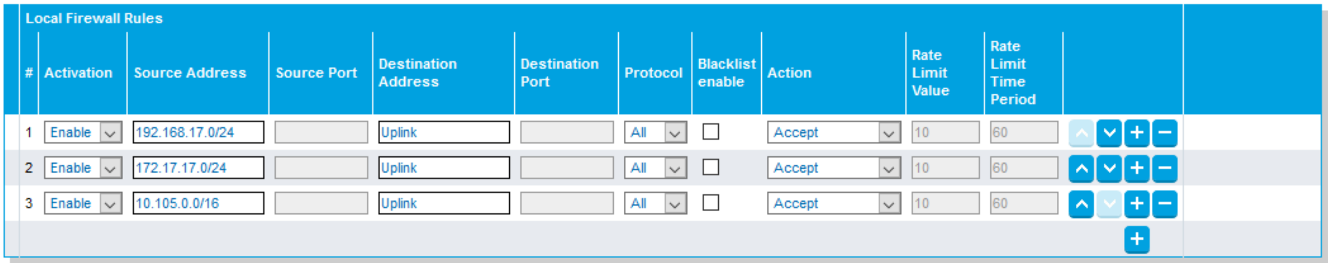
Configuration Modified:	No

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 4.110: Enter network traffic



Local Firewall Rules

#	Activation	Source Address	Source Port	Destination Address	Destination Port	Protocol	Blacklist enable	Action	Rate Limit Value	Rate Limit Time Period
1	Enable	192.168.17.0/24		Uplink		All	☐	Accept	10	60
2	Enable	172.17.17.0/24		Uplink		All	☐	Accept	10	60
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)

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

There are 2 types of Rulesets:

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

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

Configuration

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

Figure 4.111: Configuration

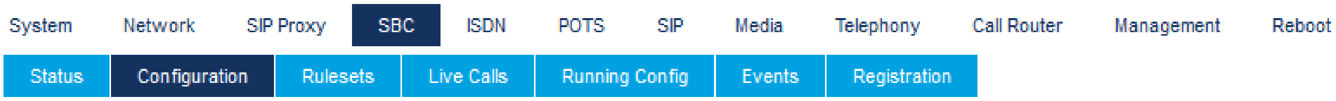
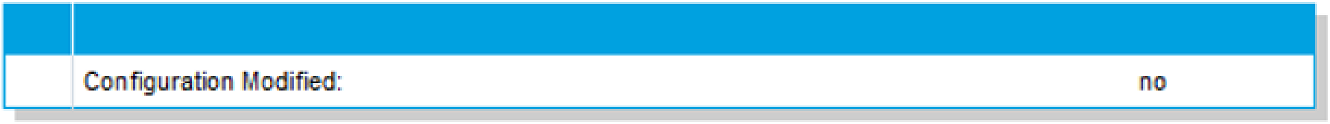


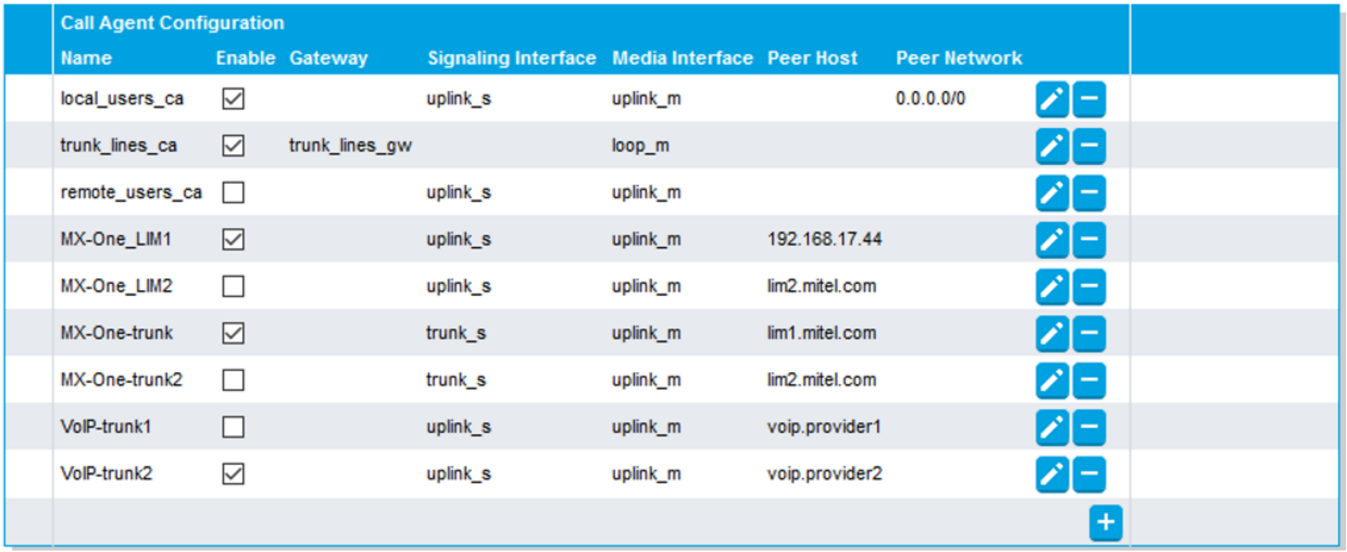
Figure 4.112: Configuration Modified



Configuration Modified: no

Following Call Agents are present.

Figure 4.113: Call Agent Configuration



Call Agent Configuration

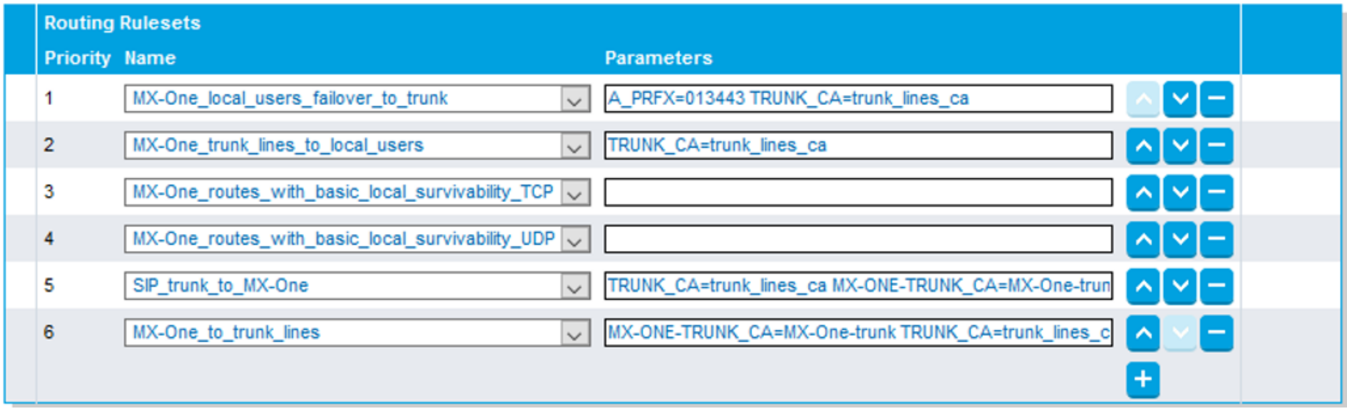
Name	Enable	Gateway	Signaling Interface	Media Interface	Peer Host	Peer Network
local_users_ca	☑		uplink_s	uplink_m		0.0.0.0/0
trunk_lines_ca	☑	trunk_lines_gw		loop_m		
remote_users_ca	□		uplink_s	uplink_m		
MX-One_LIM1	☑		uplink_s	uplink_m	192.168.17.44	
MX-One_LIM2	□		uplink_s	uplink_m	lim2.mitel.com	
MX-One-trunk	☑		trunk_s	uplink_m	lim1.mitel.com	
MX-One-trunk2	□		trunk_s	uplink_m	lim2.mitel.com	
VoIP-trunk1	□		uplink_s	uplink_m	voip.provider1	
VoIP-trunk2	☑		uplink_s	uplink_m	voip.provider2	

Routing Rulesets

Routing Rulesets: are used to globally route outbound requests, that are applied to all Call Agents.

Routing Rulesets are executed until a Call Agent is selected for the destination.

Figure 4.114: Routing Rulesets



Routing Rulesets

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

- **Ruleset MX-One_local_users_failover_to_trunk**

A_PRFX=031325

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

TRUNK_CA=VoIP-trunk2

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

- **Ruleset MX-One_trunk_lines_to_local_users**

TRUNK_CA=VoIP-trunk2

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

- **Ruleset SIP_trunk to_MX-One**

TRUNK_CA=VoIP-trunk2

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

MX-ONE-TRUNK=MX-One-trunk

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

Ruleset MX-One_to_trunk_lines

TRUNK_CA=VoIP-trunk2

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

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

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

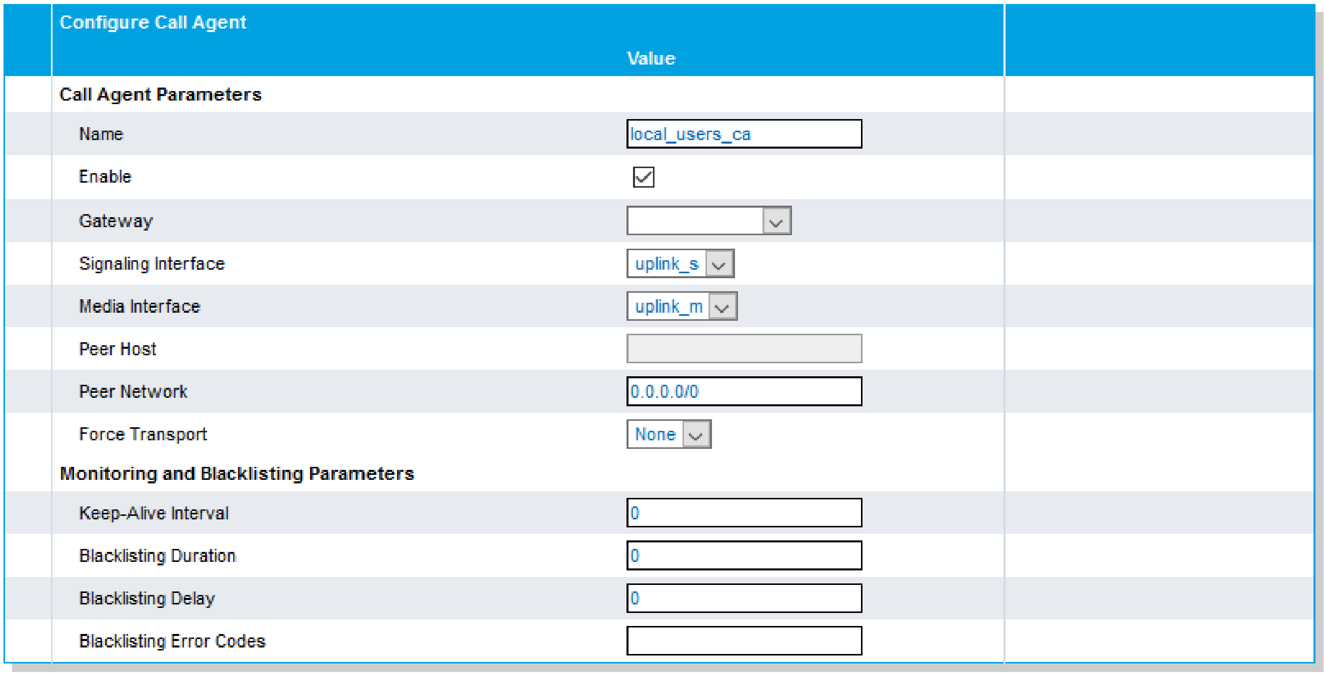
MX-ONE-TRUNK_CA=MX-One-trunk

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

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

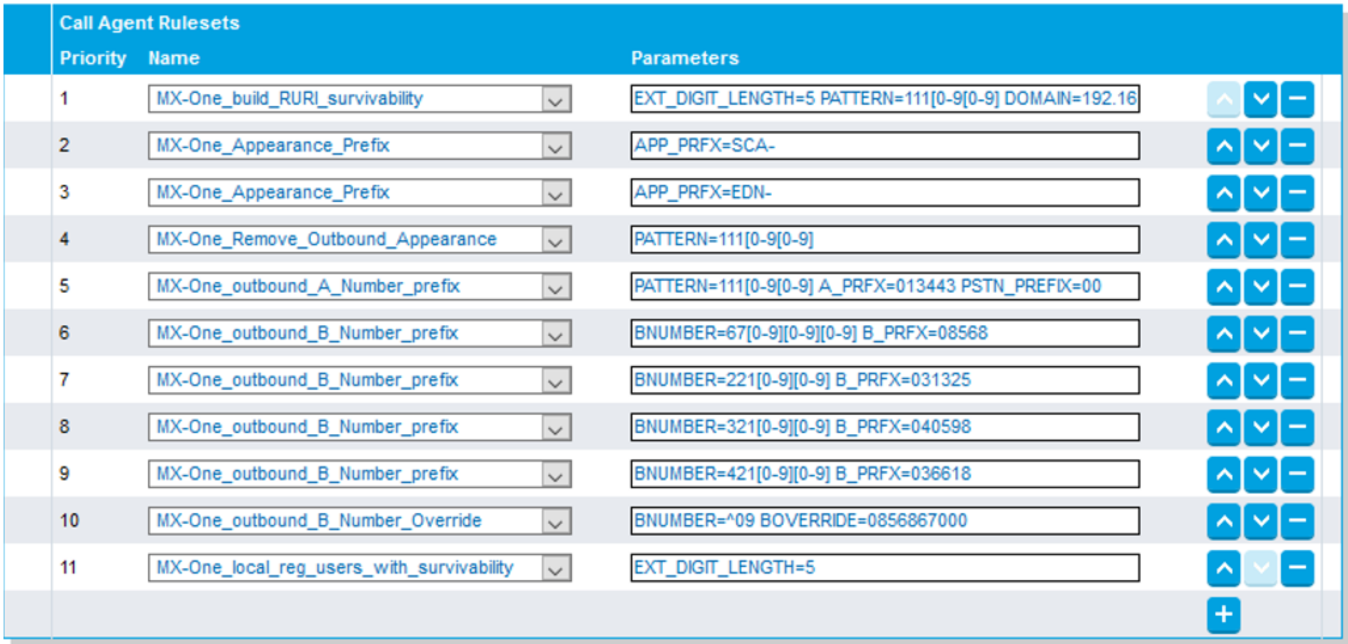
local_users_ca

Figure 4.115: Configure Call Agent screen



Configure Call Agent	Value
Call Agent Parameters	
Name	local_users_ca
Enable	☑
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 4.116: Call Agent Rulesets



Call Agent Rulesets

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

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

EXT_DIGIT_LENGTH=5

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

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

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

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

DOMAIN=192.168.17.44

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

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

APP_PREFIX=SCA- and APP_PREFIX=EDN-

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

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

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

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

A_PRFX=031325

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

PSTN_PREFIX=00

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

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

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

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

Calling HQ:

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

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

B_PRFX=08568

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

Calling BO#1:

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

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

B_PRFX=013443

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

Calling BO#3:

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

B_PRFX=040598

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

Calling BO#4:

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

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

B_PRFX=036618

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

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

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

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

BNUMBER=09

The internal number to the operator.

BOVERRIDE=0856867000

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

- **Ruleset: MX-One_local_reg_users_with_survivability**

(Builds the registration cache for survivability purpose).

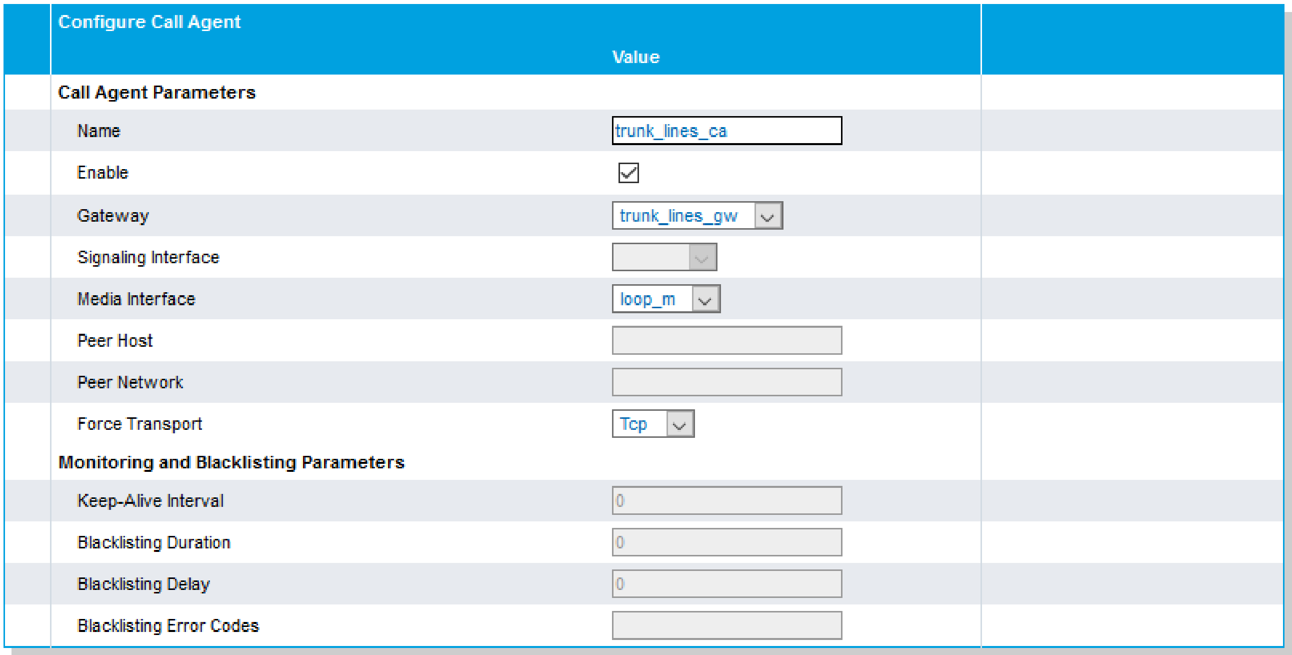
EXT_DIGIT_LENGTH=5

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

Click **Save** when done.

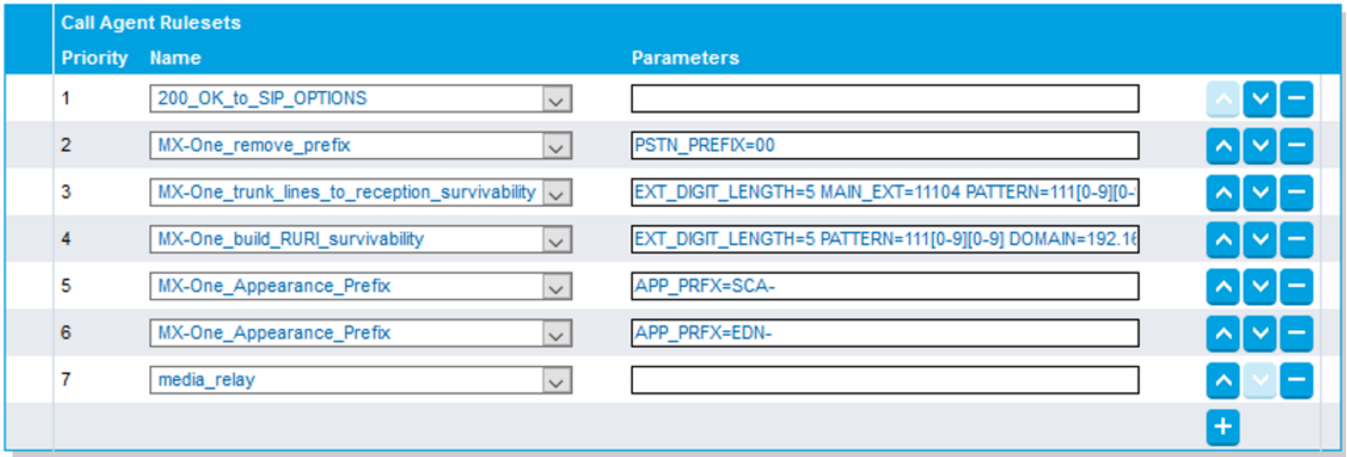
trunk_lines_ca

Figure 4.117: trunk_lines_ca



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

Figure 4.118: Call Agent Rulesets



Call Agent Rulesets

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

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

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

- **Ruleset: MX-One_trunk_lines_to_reception_survivability**

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

EXT_DIGIT_LENGTH=5

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

MAIN_EXT=22104

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

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

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

DOMAIN=192.168.17.44

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

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

Builds the RURI when in survivability mode.

EXT_DIGIT_LENGTH=5

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

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

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

DOMAIN=192.168.17.44

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

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

APP_PREFIX=SCA- and APP_PREFIX=EDN-

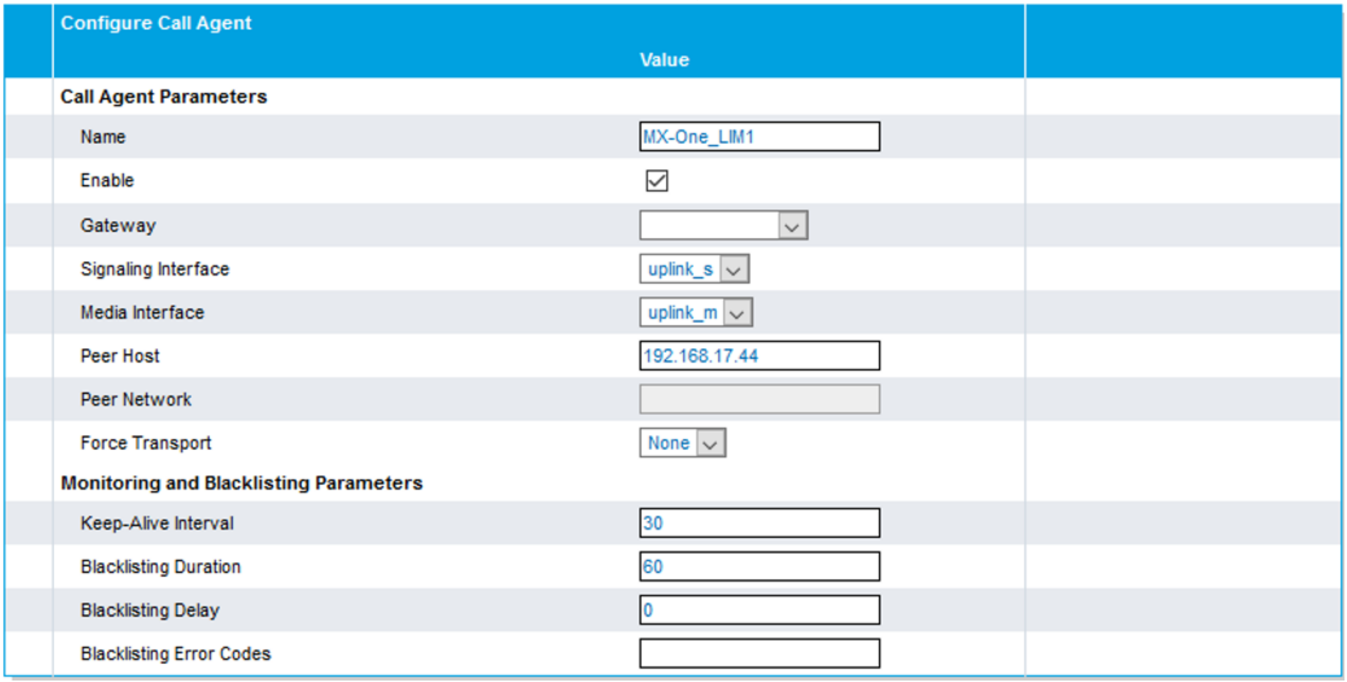
This is the prefix for the user names connected with shared appearance (SCA) and extra directory number (EDN). In this example, you have two user names: "SCA"- and "EDN-"

Click **Save** when done.

MX-One_Lim1

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

Figure 4.119: Configure Call Agent - Peer Host

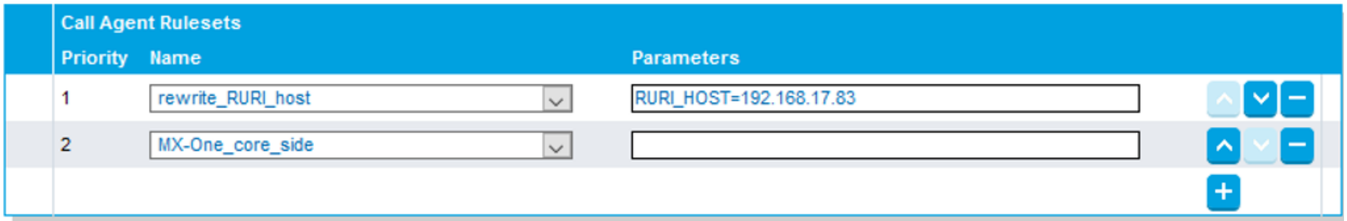


Configure Call Agent

	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	

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

Figure 4.120: RURI_HOST parameter



Call Agent Rulesets

Priority	Name	Parameters
1	rewrite_RURI_host	RURI_HOST=192.168.17.83
2	MX-One_core_side	

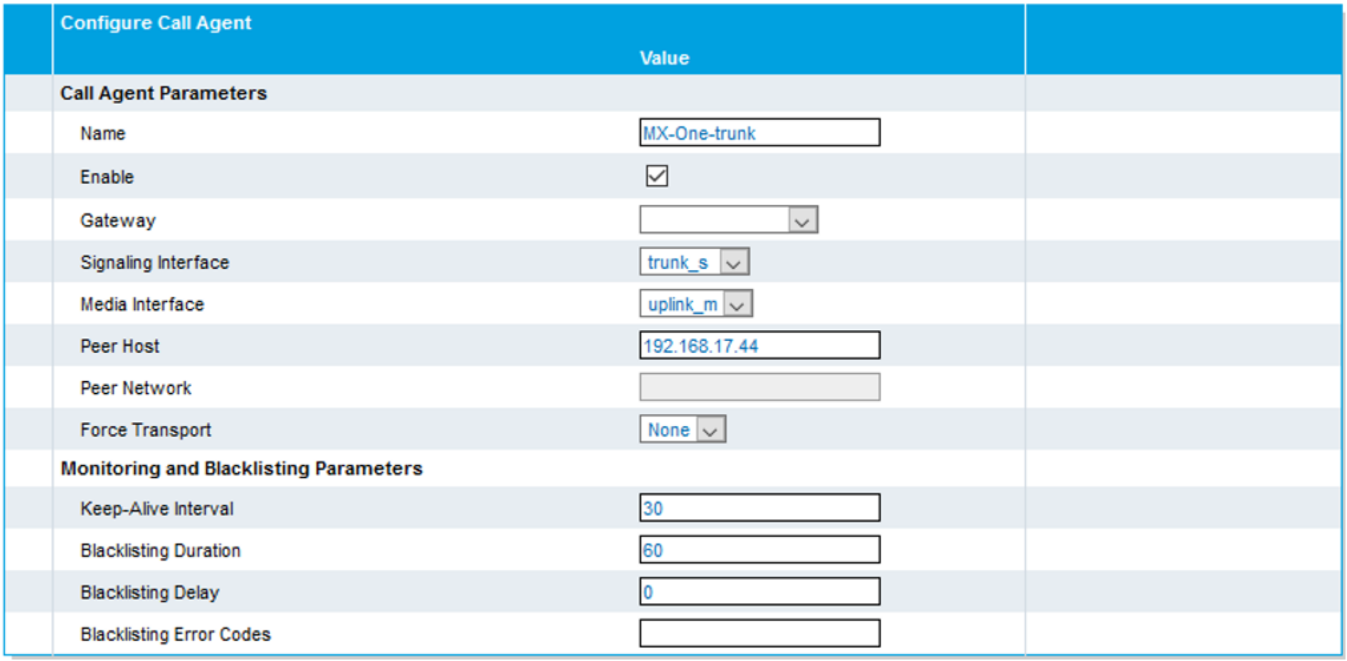
- **Ruleset: rewrite_RURI_host**
  RURI_HOST= 192.168.17.83
  This is the local IP address of the GX-gateway.
  Click **Save** when done.

MX-One_trunk

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

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

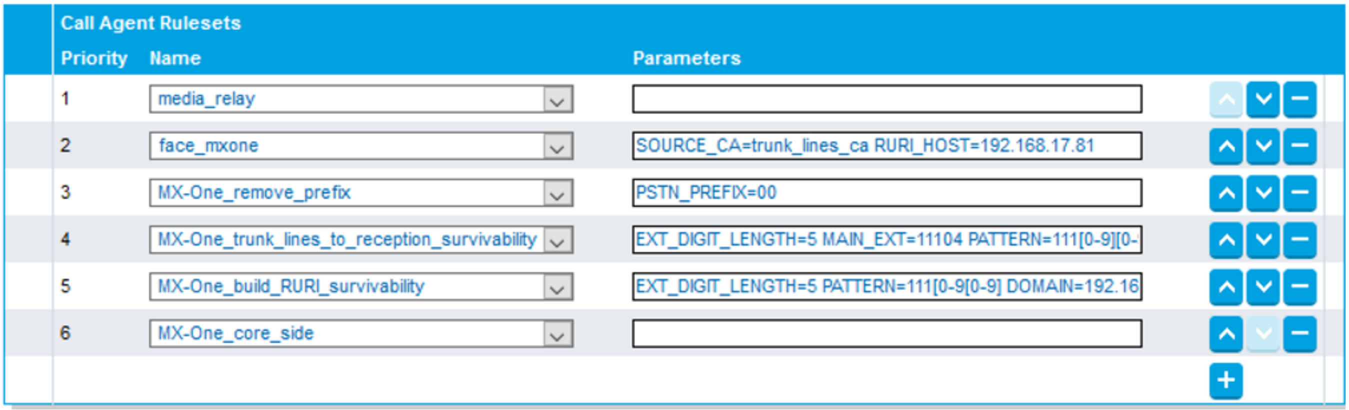
Figure 4.121: Call Agent Parameters



Configure Call Agent

	Value
Call Agent Parameters	
Name	MX-One-trunk
Enable	☑
Gateway	
Signaling Interface	trunk_s
Media Interface	uplink_m
Peer Host	192.168.17.44
Peer Network	
Force Transport	None
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	30
Blacklisting Duration	60
Blacklisting Delay	0
Blacklisting Error Codes	

Figure 4.122: Call Agent Rulesets



Call Agent Rulesets

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

- **Ruleset: face_mxone**

SOURCE_CA=VoIP-trunk2

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

RURI_HOST=192.168.17.83

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

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

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

- **Ruleset: MX-One_trunk_lines_to_reception_survivability**

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

EXT_DIGIT_LENGTH=5

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

MAIN_EXT=22104

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

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

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

DOMAIN=192.168.17.44

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

- **Ruleset: MX-One_build_RURI_survivability**

Builds the RURI when in survivability mode

EXT_DIGIT_LENGTH=5

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

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

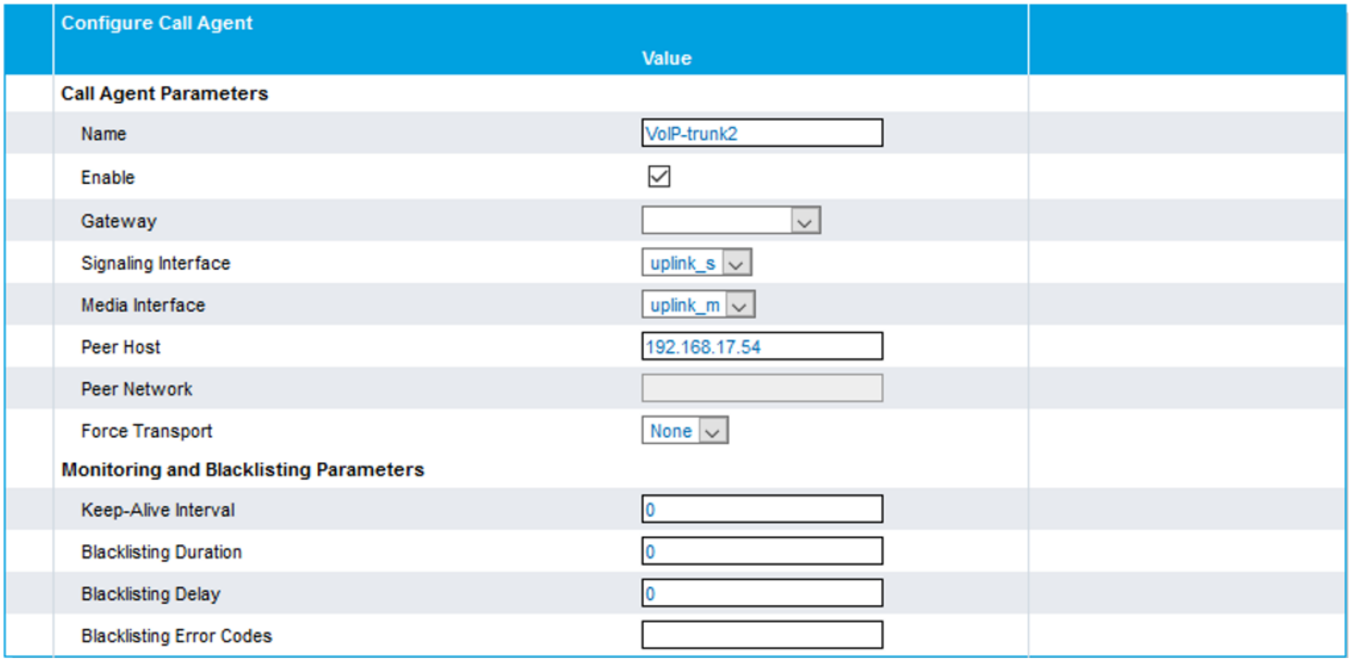
This defines the local numbers. The pattern for the internal range of numbers would be 22100 - 22199.

DOMAIN=192.168.17.44

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

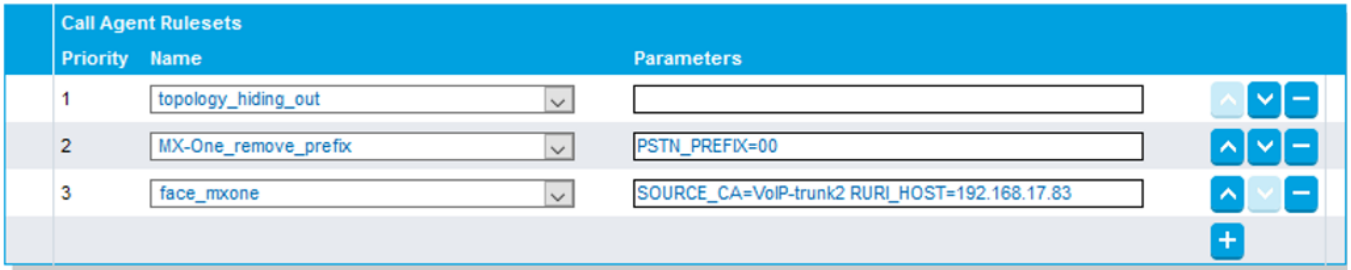
Click **Save** when done.

VOIP-trunk2



Configure Call Agent	Value
Call Agent Parameters	
Name	VoIP-trunk2
Enable	☑
Gateway	
Signaling Interface	uplink_s
Media Interface	uplink_m
Peer Host	192.168.17.54
Peer Network	
Force Transport	None
Monitoring and Blacklisting Parameters	
Keep-Alive Interval	0
Blacklisting Duration	0
Blacklisting Delay	0
Blacklisting Error Codes	

Figure 4.123: Call Agent Rulesets



Call Agent Rulesets

Priority	Name	Parameters
1	topology_hiding_out	
2	MX-One_remove_prefix	PSTN_PREFIX=00
3	face_mxone	SOURCE_CA=VoIP-trunk2 RURI_HOST=192.168.17.83

- **Ruleset: MX-One_remove_prefix**

PSTN_PREFIX=00

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

- **Ruleset: face_mxone**

SOURCE_CA=VoIP-trunk2

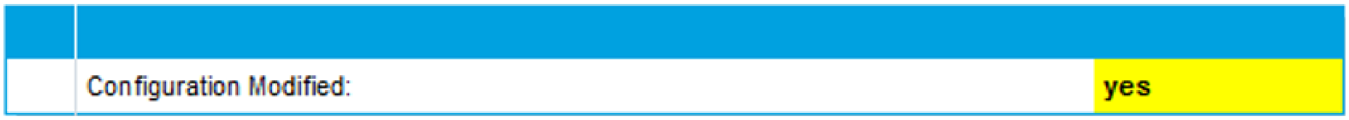
This parameter indicates the call agent from which the call is coming.

RURI_HOST=192.168.17.81

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

Click **Save** when done.

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



Configuration Modified: yes

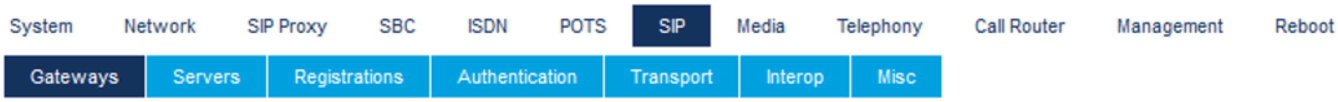
Click **Apply** when ready.

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

SIP

Gateways

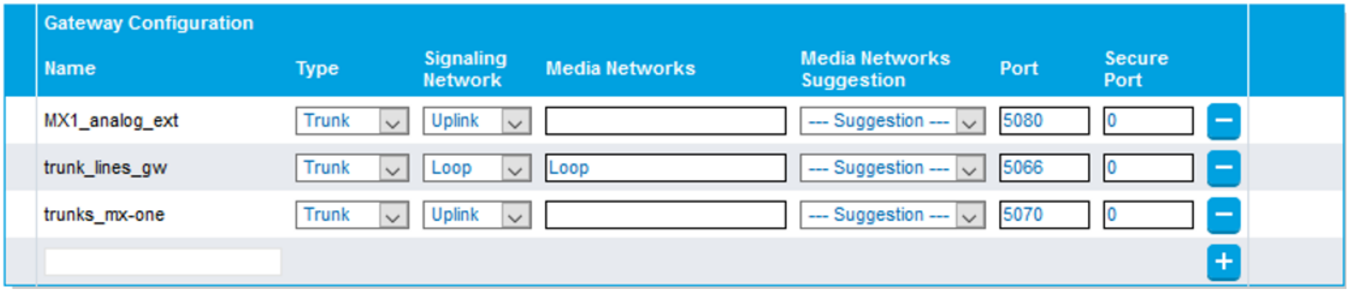
Figure 4.124: Gateways



Following gateways are predefined and port numbers.

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

Figure 4.125: Gateway Configuration

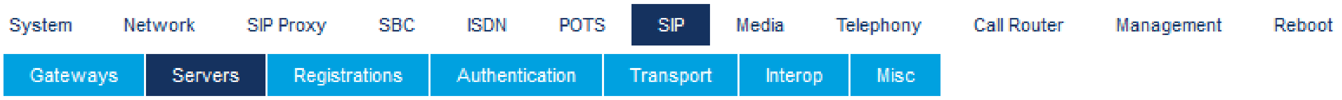


Gateway Configuration

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

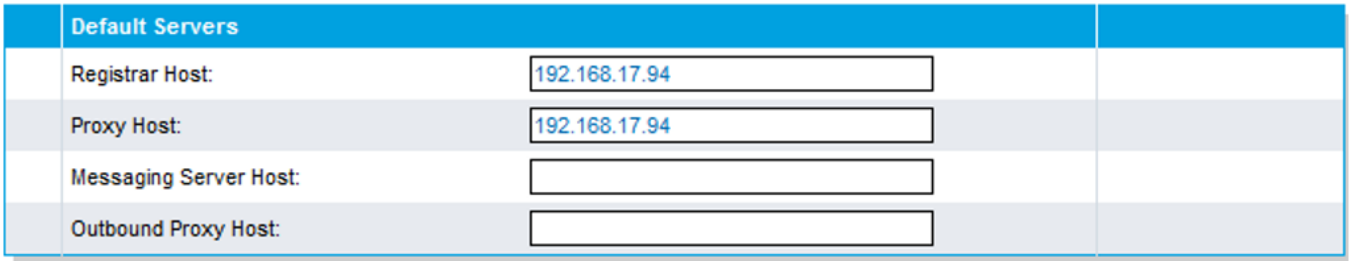
Servers

Figure 4.126: Servers



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

Figure 4.127: Default Servers

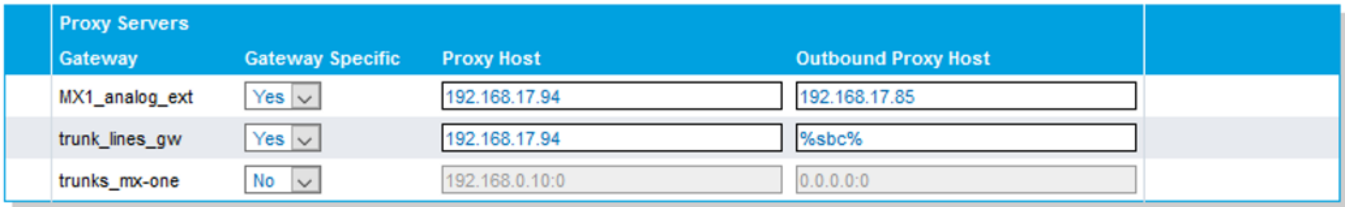


Default Servers

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

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

Figure 4.128: Proxy Servers



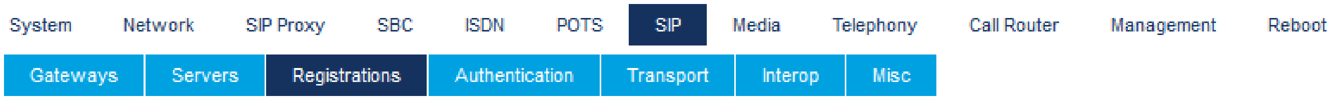
Proxy Servers

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

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

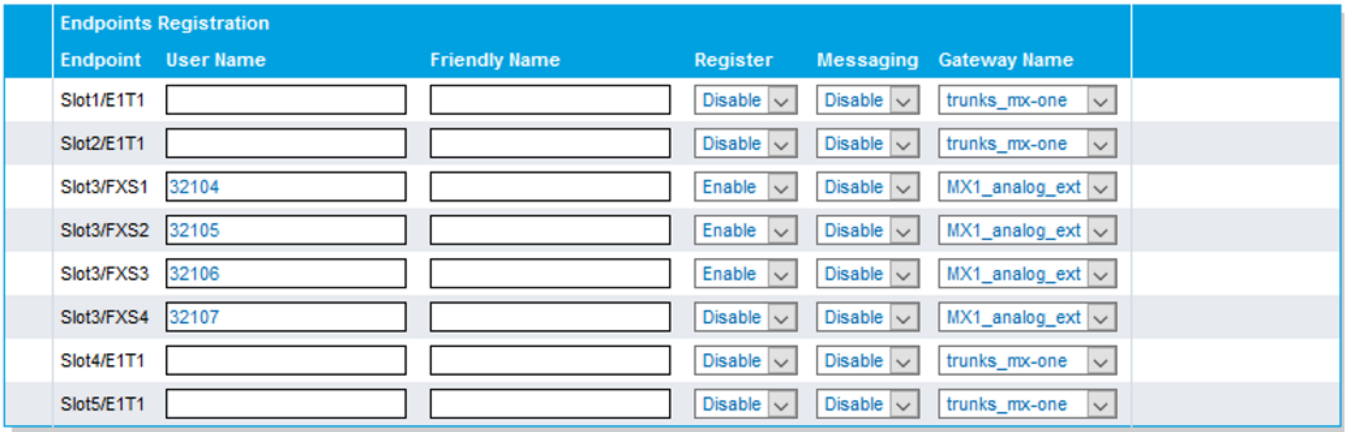
Registrations

Figure 4.129: Registrations



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

Figure 4.130: Endpoints Registration screen



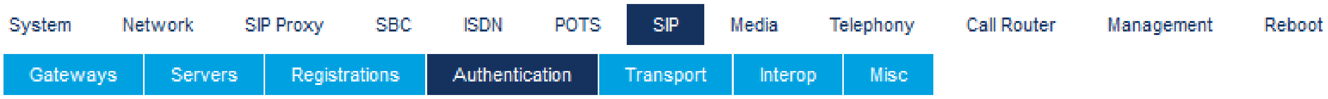
Endpoints Registration

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

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

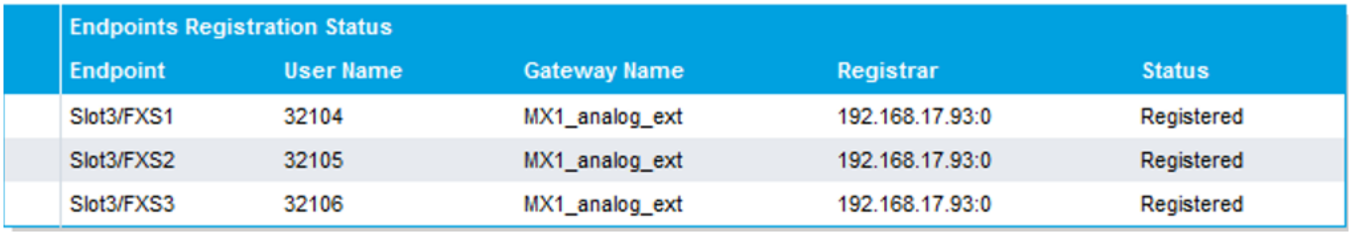
Authentication

Figure 4.131: Authentication



1. Select **SIP** > **Authentication**.

Figure 4.132: Authentication Screen

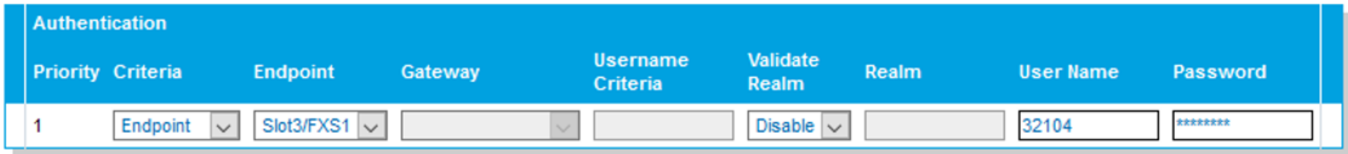


Endpoints Registration Status

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

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

Figure 4.133: Validate Realm field

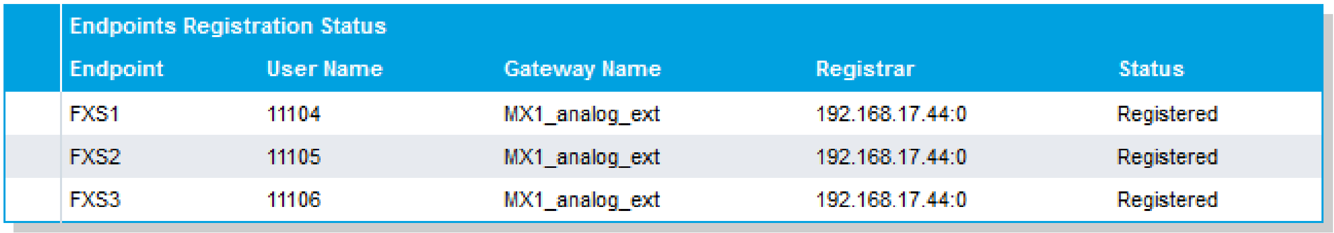


Authentication

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

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

Figure 4.134: Endpoints Registration Status

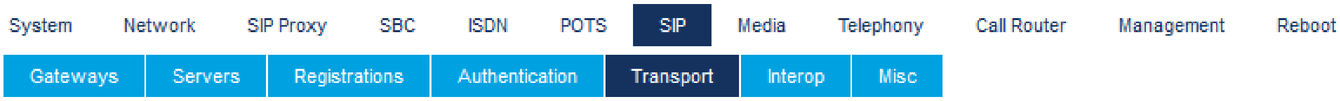


Endpoints Registration Status

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

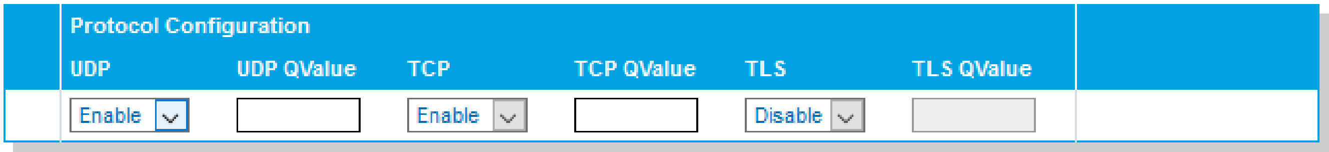
Transport

Figure 4.135: Transport



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

Figure 4.136: Protocol Configuration



Protocol Configuration

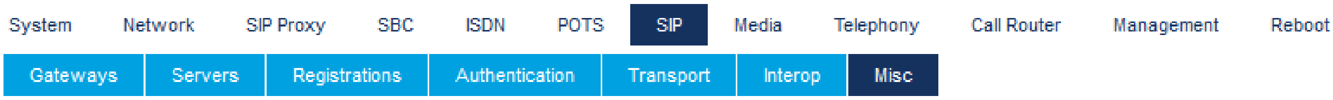
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable		Enable		Disable	

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

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

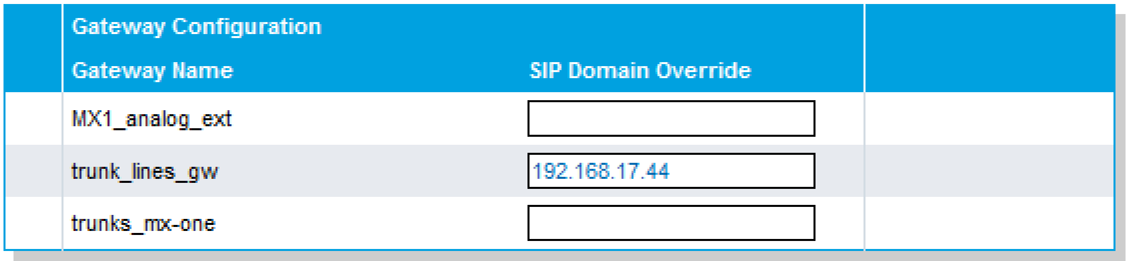
Misc

Figure 4.137: Misc



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

Figure 4.138: Gateway Configuration field



Gateway Configuration

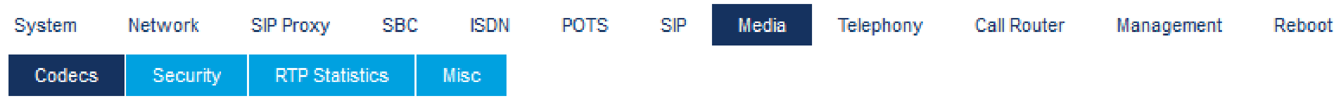
Gateway Name	SIP Domain Override
MX1_analog_ext	
trunk_lines_gw	192.168.17.44
trunks_mx-one	

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

Media

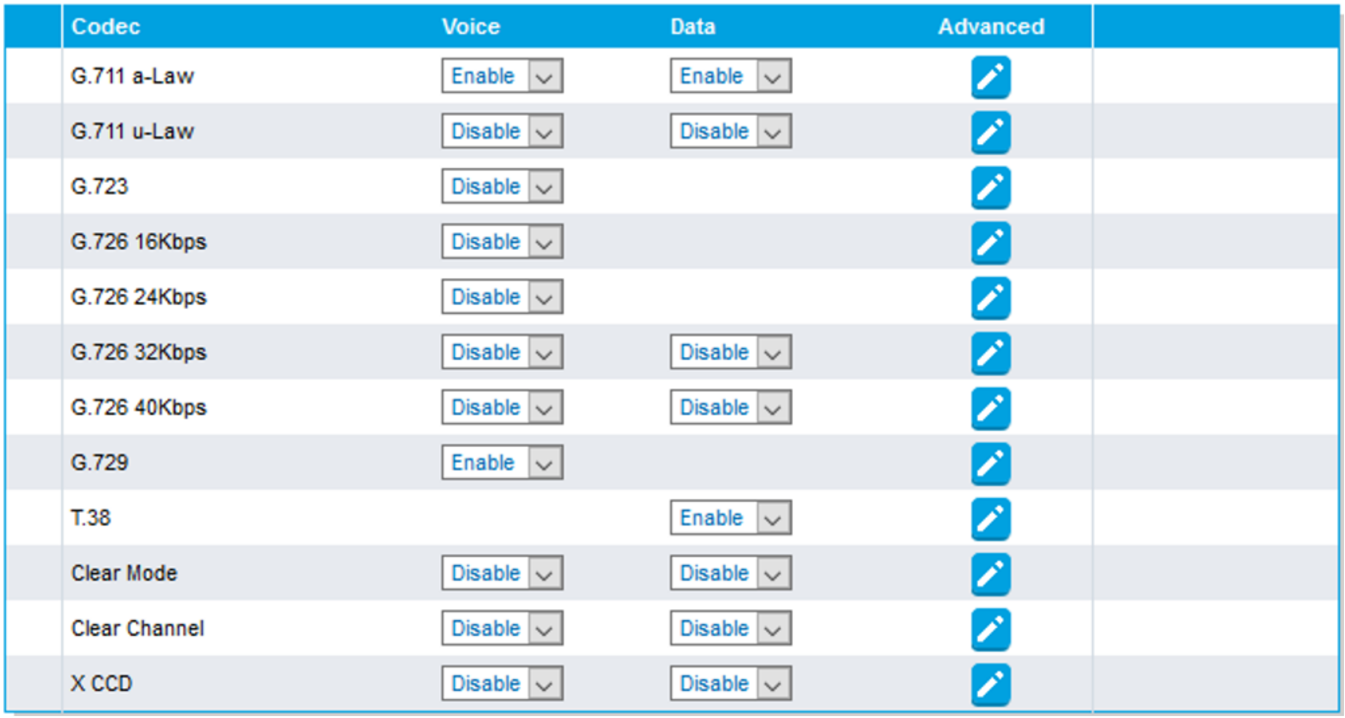
Codecs

Figure 4.139: Codecs



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

Figure 4.140: Codecs



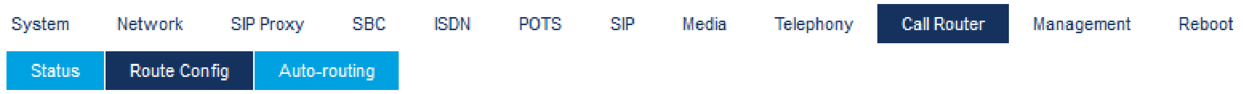
Codec	Voice	Data	Advanced
G.711 a-Law	Enable	Enable	✎
G.711 u-Law	Disable	Disable	✎
G.723	Disable		✎
G.726 16Kbps	Disable		✎
G.726 24Kbps	Disable		✎
G.726 32Kbps	Disable	Disable	✎
G.726 40Kbps	Disable	Disable	✎
G.729	Enable		✎
T.38		Enable	✎
Clear Mode	Disable	Disable	✎
Clear Channel	Disable	Disable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

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

Call Router

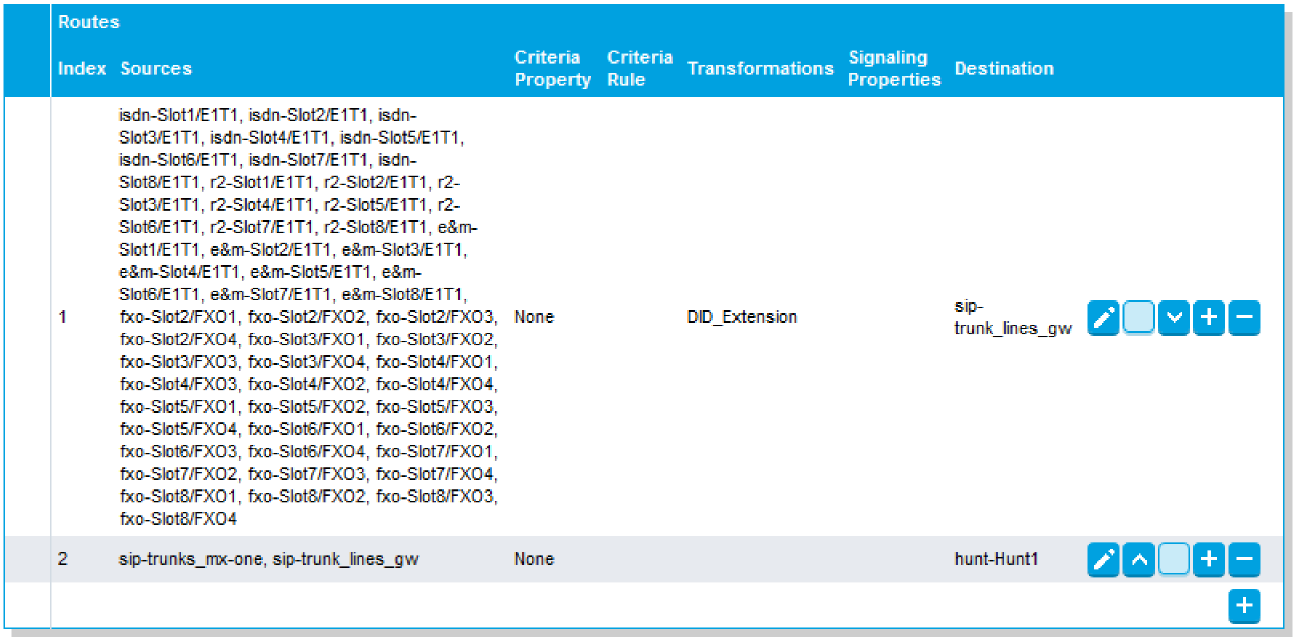
Route Config

Figure 4.141: Route Config screen



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

Figure 4.142: Routes

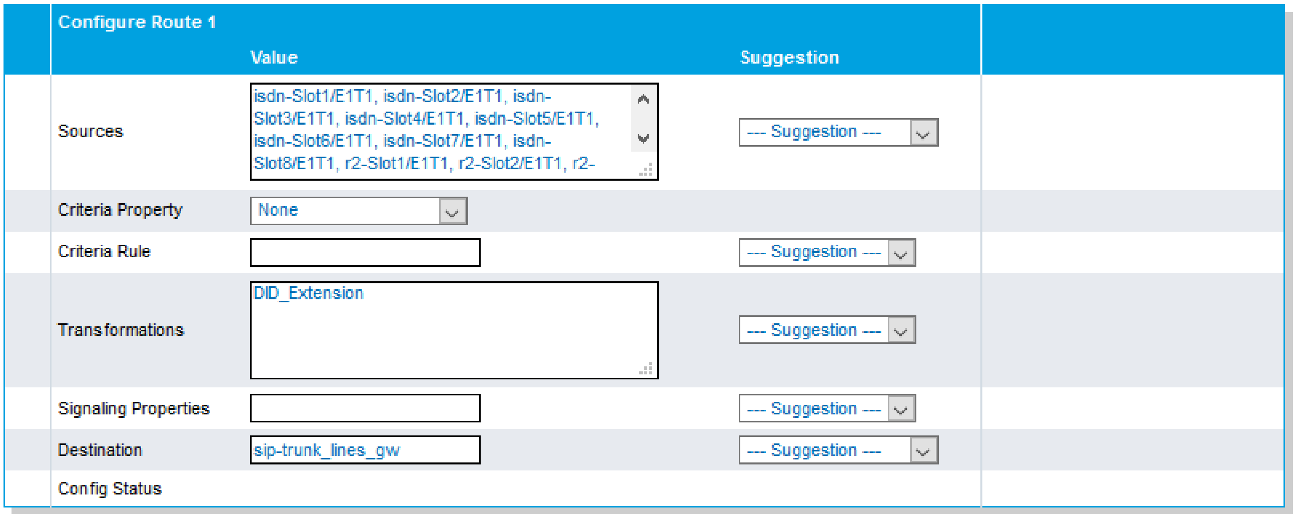


Routes

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

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

Figure 4.143: Configure Route

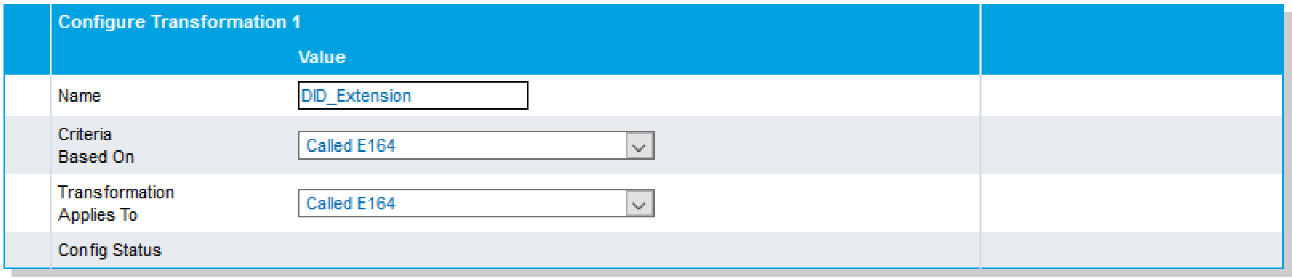


Configure Route 1

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

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

Figure 4.144: Configure Transformation

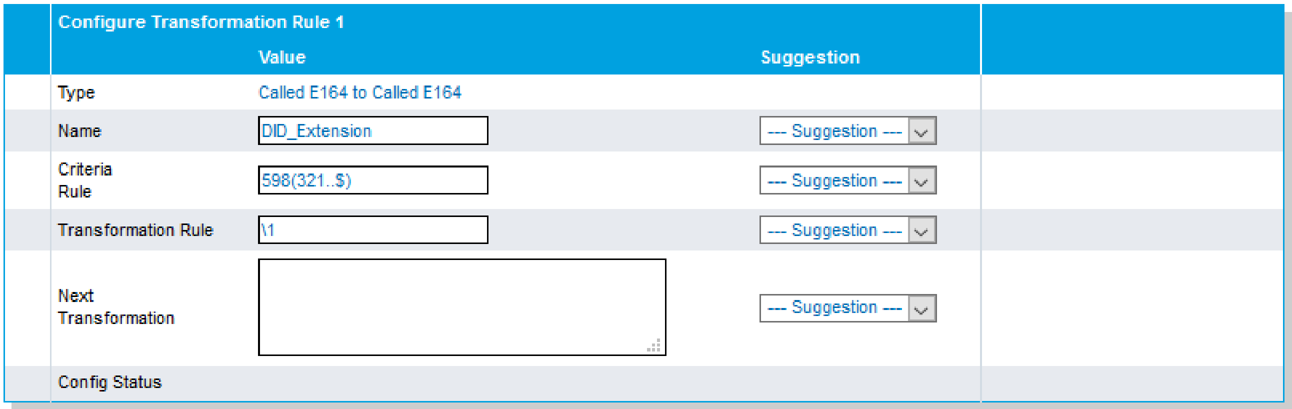


Configure Transformation 1

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

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

Figure 4.145: Configure Transformation Rule 1

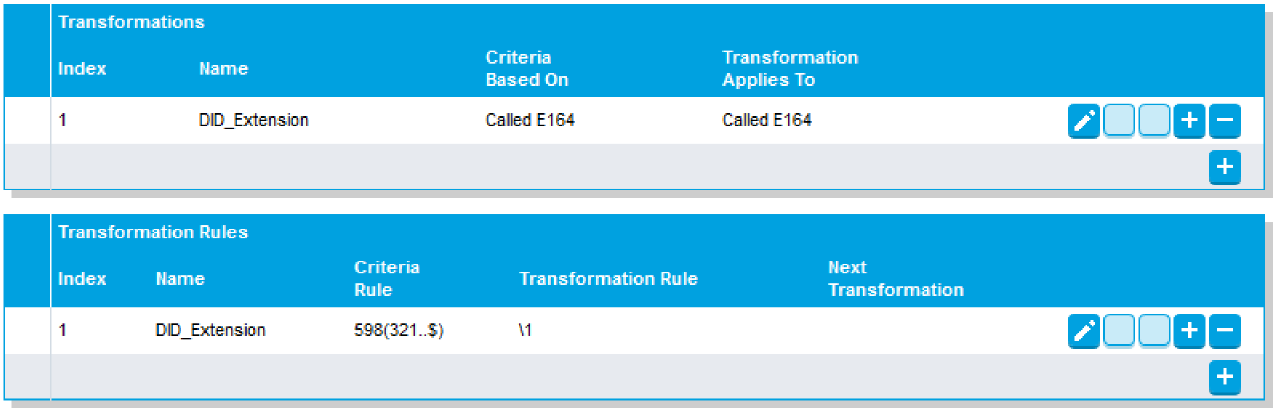


Configure Transformation Rule 1

	Value	Suggestion
Type	Called E164 to Called E164	
Name	DID_Extension	--- Suggestion ---
Criteria Rule	598(321..$)	--- Suggestion ---
Transformation Rule	\1	--- Suggestion ---
Next Transformation		--- Suggestion ---
Config Status		

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

Figure 4.146: Transformations



Transformations

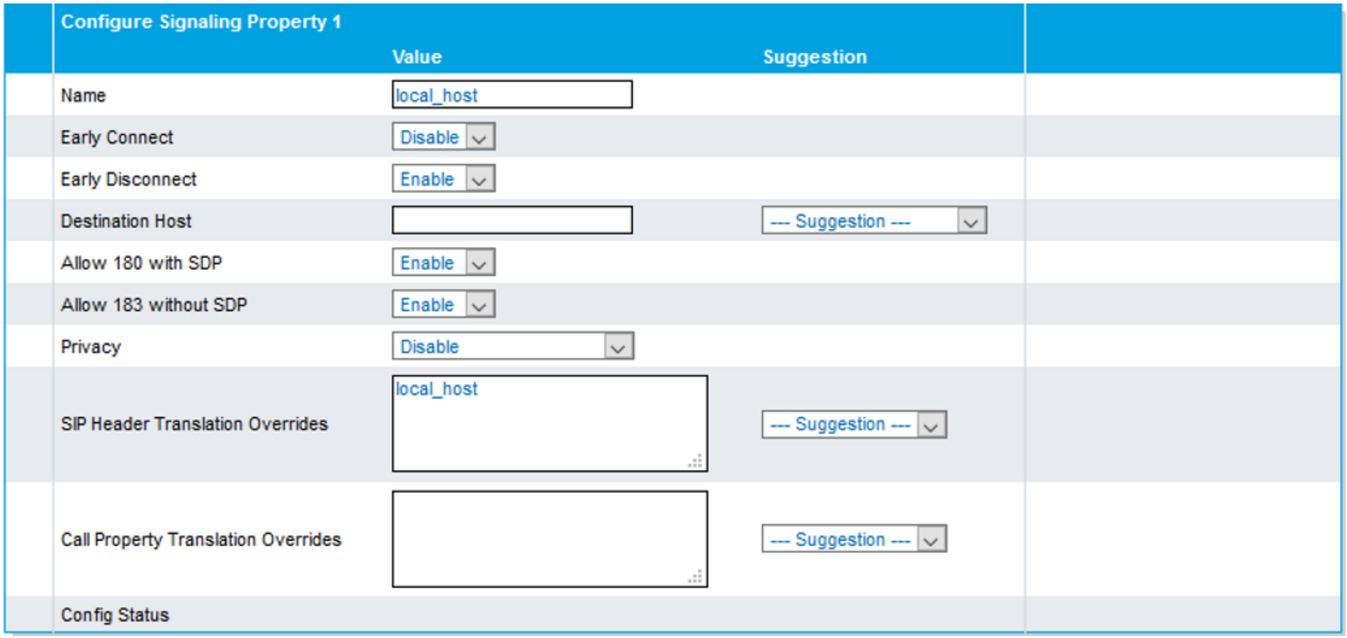
Index	Name	Criteria Based On	Transformation Applies To	
1	DID_Extension	Called E164	Called E164	✎ ☐ ☐ + −
				+

Transformation Rules

Index	Name	Criteria Rule	Transformation Rule	Next Transformation	
1	DID_Extension	598(321..$)	\1		✎ ☐ ☐ + −
					+

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

Figure 4.147: Configure Signaling Property 1

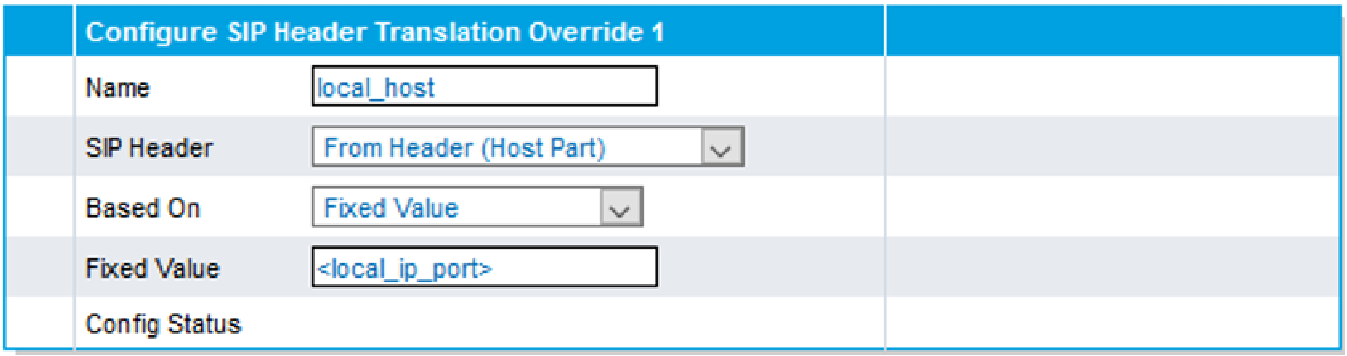


Configure Signaling Property 1

	Value	Suggestion
Name	local_host	
Early Connect	Disable	
Early Disconnect	Enable	
Destination Host		--- Suggestion ---
Allow 180 with SDP	Enable	
Allow 183 without SDP	Enable	
Privacy	Disable	
SIP Header Translation Overrides	local_host	--- Suggestion ---
Call Property Translation Overrides		--- Suggestion ---
Config Status		

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

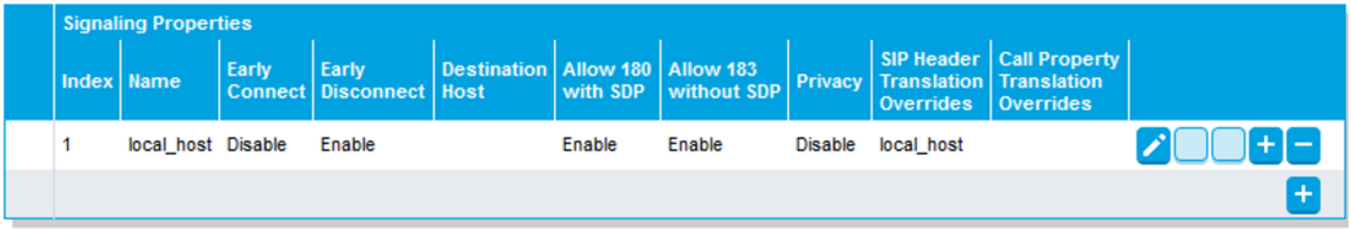
Figure 4.148: Configure SIP Header Translation Override 1



Configure SIP Header Translation Override 1

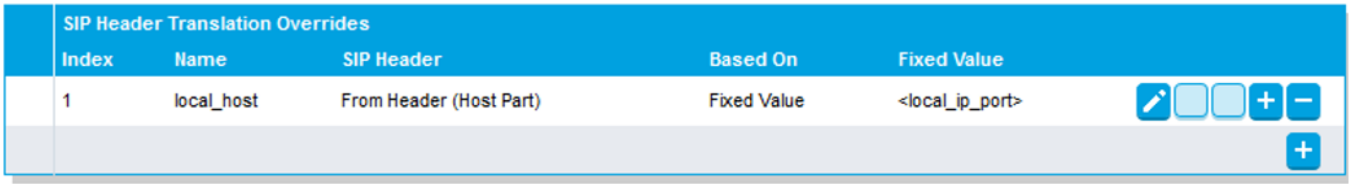
Name	local_host
SIP Header	From Header (Host Part)
Based On	Fixed Value
Fixed Value	<local_ip_port>
Config Status	

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



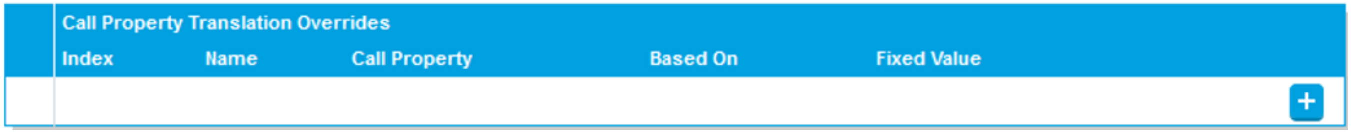
Signaling Properties

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



SIP Header Translation Overrides

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



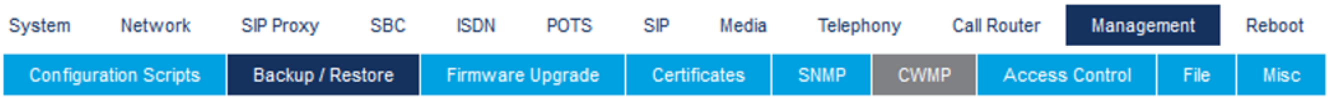
Call Property Translation Overrides

Index	Name	Call Property	Based On	Fixed Value

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

Management

Backup/Restore



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

Figure 4.149: Image Configuration

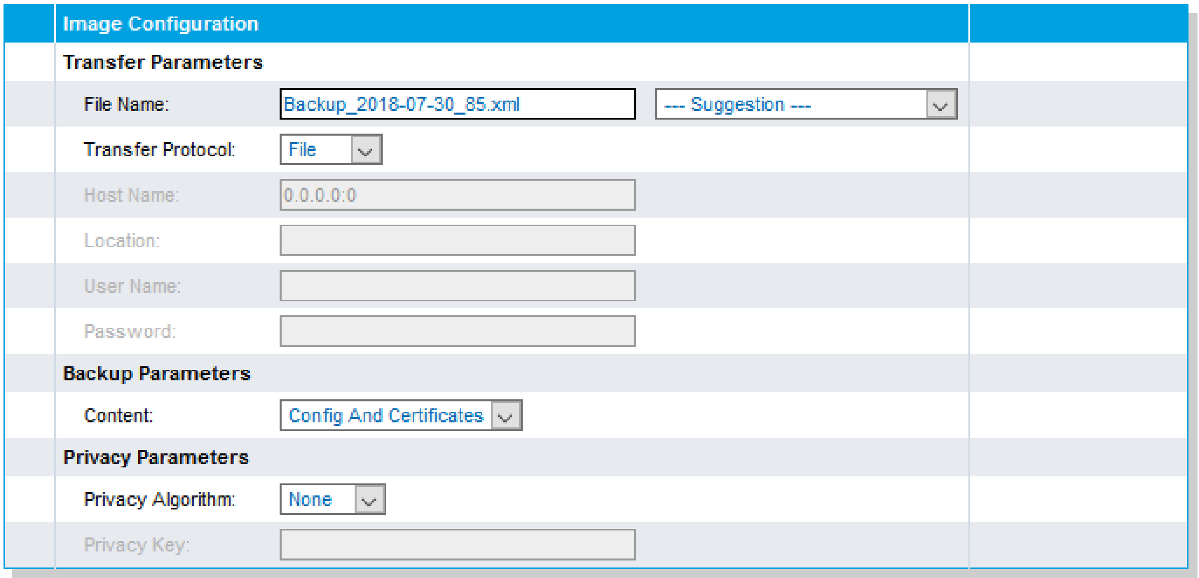


Image Configuration

Transfer Parameters

File Name:	Backup_2018-07-30_85.xml	--- Suggestion ---
Transfer Protocol:	File	
Host Name:	0.0.0.0:0	
Location:		
User Name:		
Password:		

Backup Parameters

Content:	Config And Certificates

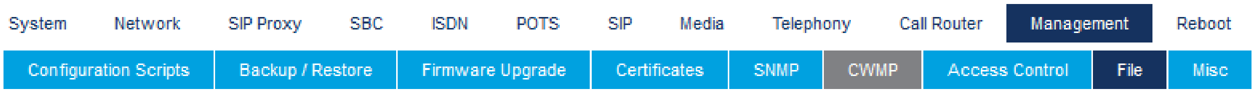
Privacy Parameters

Privacy Algorithm:	None
Privacy Key:	

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

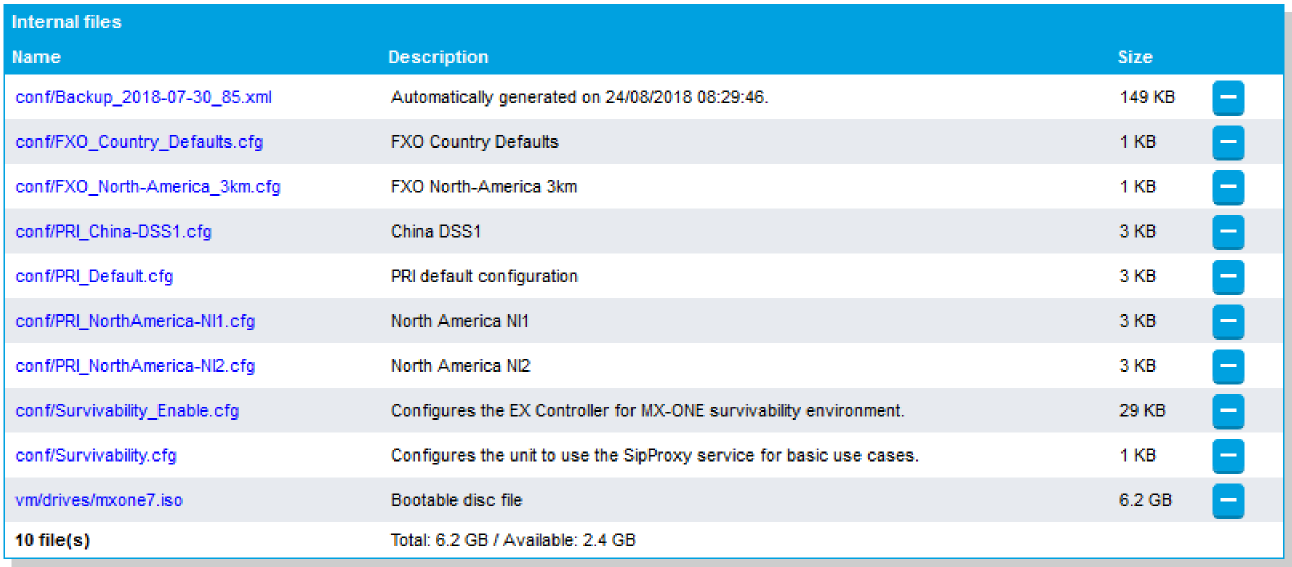
File

Figure 4.150: File screen



1. Select **Management** > **File**.

Figure 4.151: Internal files

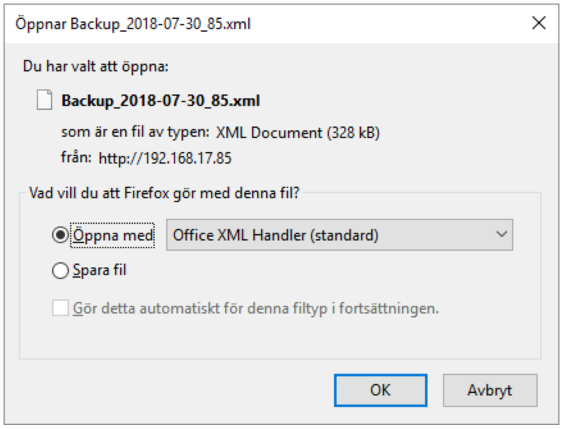


Internal files

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

1. Find the previously made backup image.

Figure 4.152: Backup image



Öppnar Backup_2018-07-30_85.xml

Du har valt att öppna:

Backup_2018-07-30_85.xml

som är en fil av typen: XML Document (328 kB)
från: http://192.168.17.85

Vad vill du att Firefox gör med denna fil?

● Öppna med Office XML Handler (standard)

○ Spara fil

□ Gör detta automatiskt för denna filtyp i fortsättningen.

2. Download and store on a secure place.

Known Limitations

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

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

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.

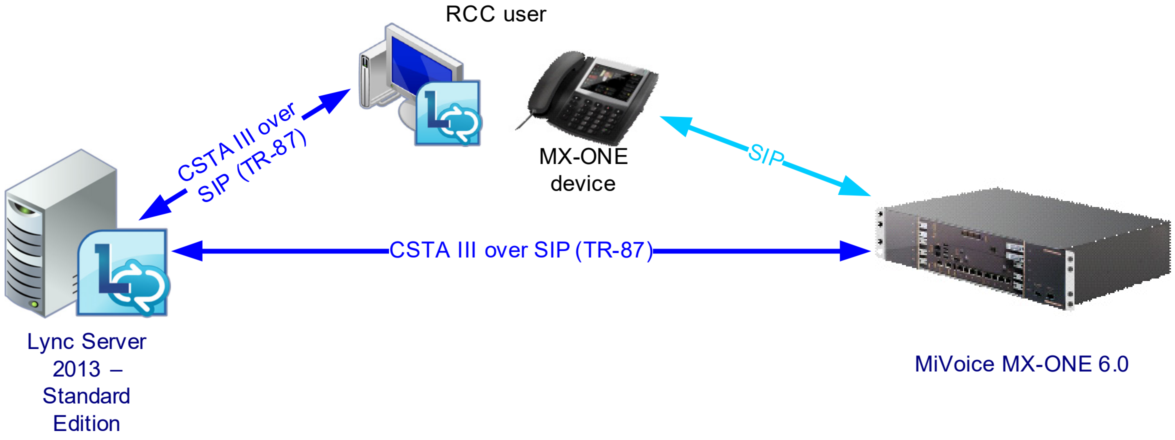

RCC user
MX-ONE device
CSTA III over SIP (TR-87)
SIP
CSTA III over SIP (TR-87)
Lync Server 2013 – Standard Edition
MiVoice MX-ONE 6.0

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

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.

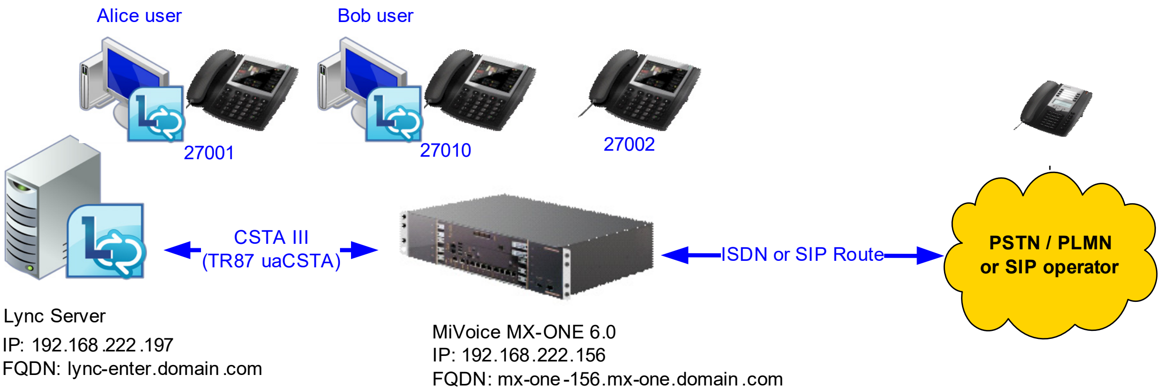


Figure 2 - Integration setup

📝	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

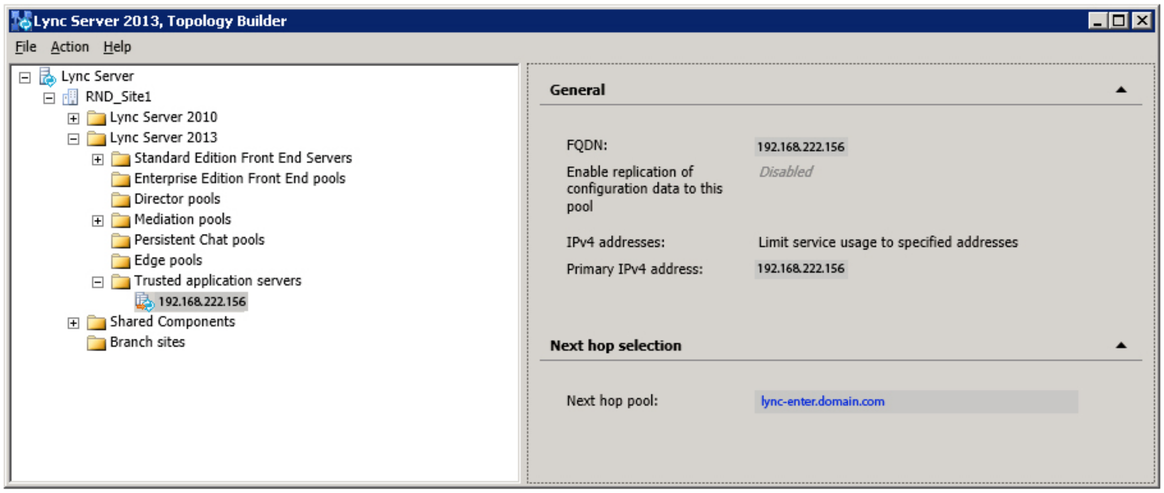
Publish the topology

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.



```
⊟ Lync Server
  ⊟ RND_Site1
    ⊞ Lync Server 2010
    ⊟ Lync Server 2013
      ⊞ Standard Edition Front End Servers
        Enterprise Edition Front End pools
        Director pools
      ⊞ Mediation pools
        Persistent Chat pools
        Edge pools
      ⊟ Trusted application servers
          192.168.222.156
    ⊞ Shared Components
      Branch sites
```

General

FQDN: 192.168.222.156

Enable replication of configuration data to this pool: *Disabled*

IPv4 addresses: Limit service usage to specified addresses

Primary IPv4 address: 192.168.222.156

Next hop selection

Next hop pool: lync-enter.domain.com

Figure 3 - Lync Server 2013 Topology Builder

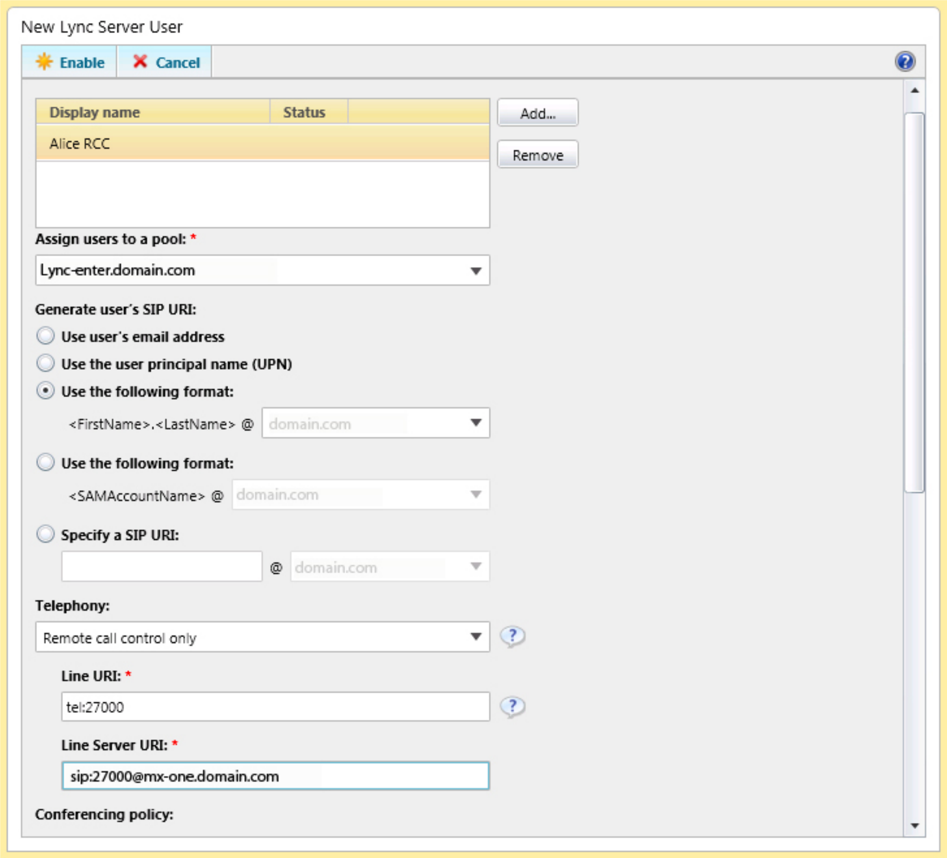
Enable Lync Users for Remote Call Control

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



Display name	Status
Alice RCC	

Assign users to a pool: *

Lync-enter.domain.com

Generate user's SIP URI:

○ Use user's email address

○ Use the user principal name (UPN)

● Use the following format:

<FirstName>.<LastName> @ domain.com

○ Use the following format:

<SAMAccountName> @ domain.com

○ Specify a SIP URI:

@ domain.com

Telephony:

Remote call control only

Line URI: *

tel:27000

Line Server URI: *

sip:27000@mx-one.domain.com

Conferencing policy:

Figure 4 - RCC only new user configuration example

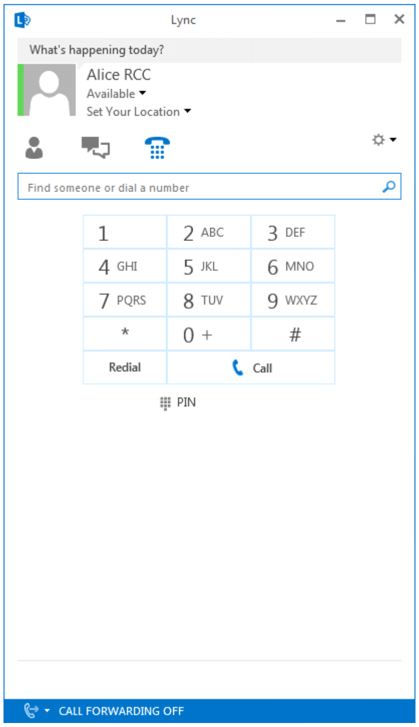
How to Verify the Setup

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

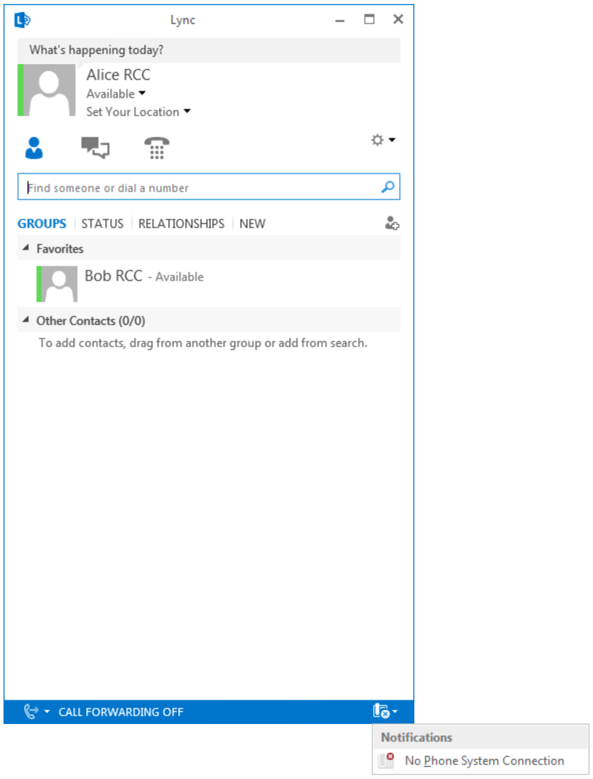
Lync 2013 Client Features

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.



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.



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.

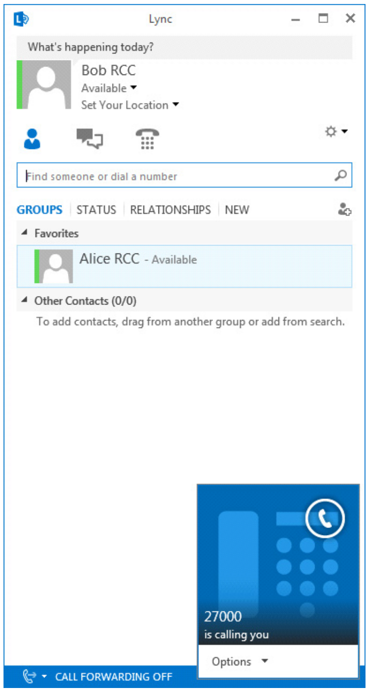
1. Alice.RCC controls the extension 27001, which is a SIP extension in MX-ONE.
2. Bob.RCC controls the extension 27010, which is a SIP extension in MX-ONE.
3. 27000 and 27002 are SIP extensions in MX-ONE.
4. 33350202 and 33350102 are the PSTN phones.

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

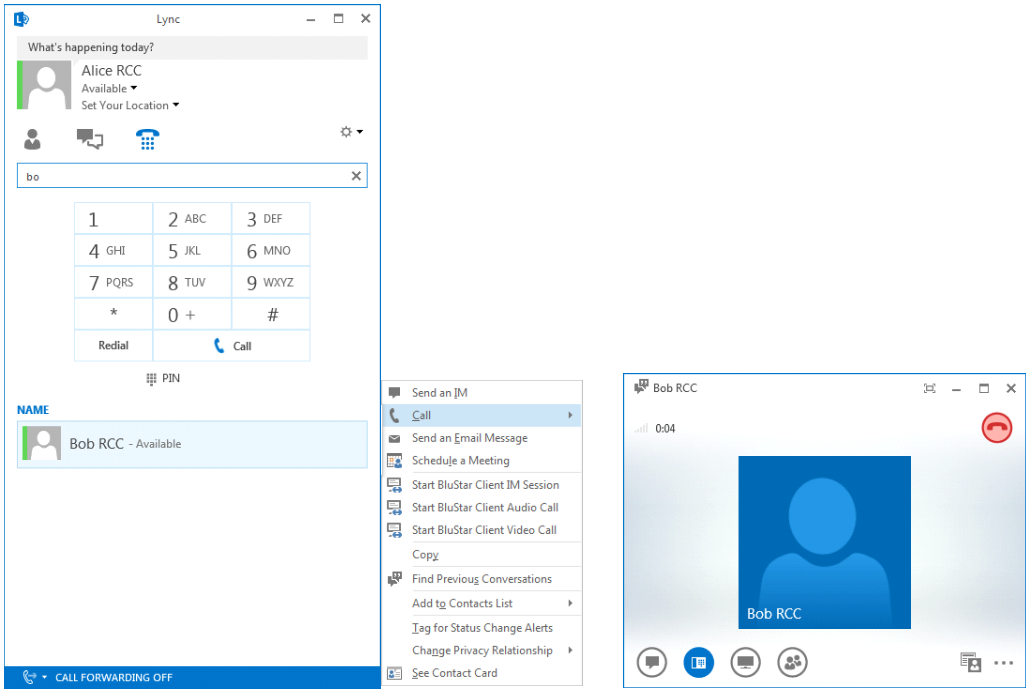
From another extension dial to RCC user, answer it and check if there is speech.



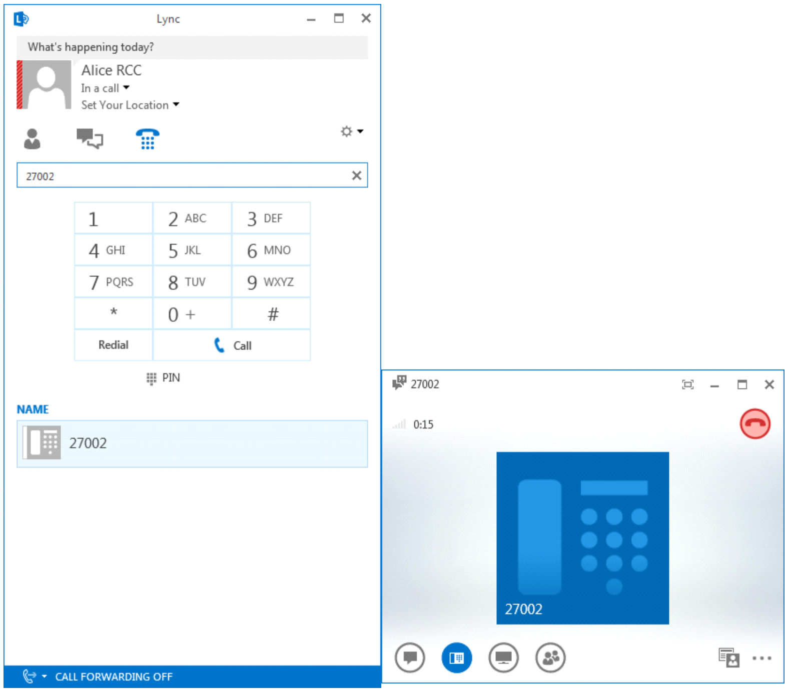
Transfer a Call Between Current Conversations (Monitored Transfer)

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.

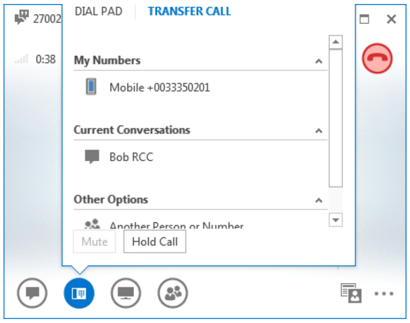
We assume you have answered a call with extension B (27010) from the Lync client (RCC



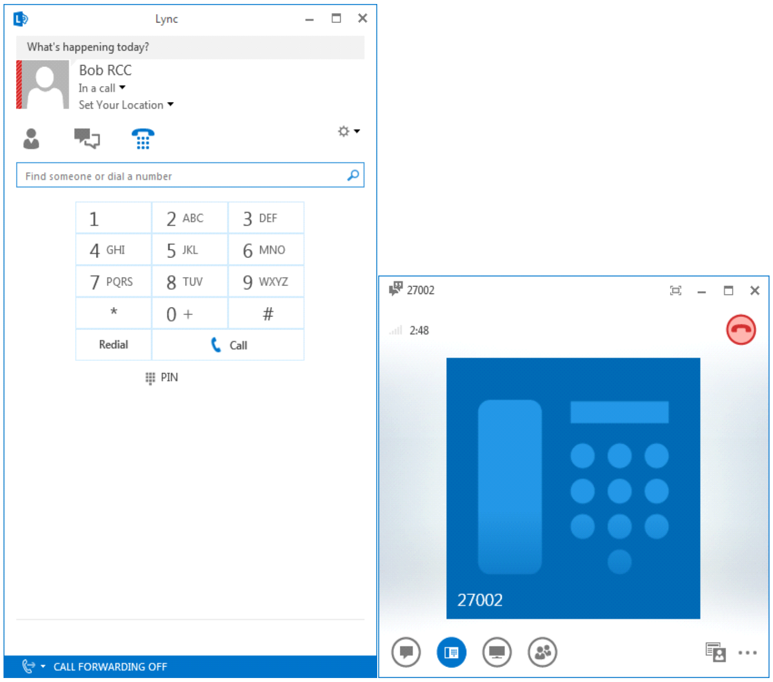
Using the client, put extension B on hold and make a second call to extension C (27002), and wait until the extension C answers.



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



Then, check if the call is correctly transferred.

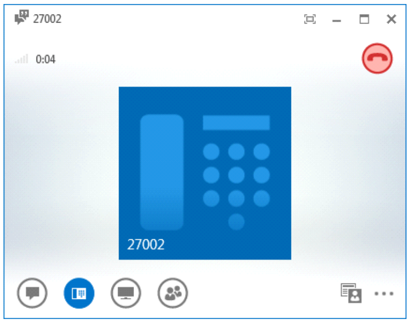


Then, check if the call is correctly transferred.

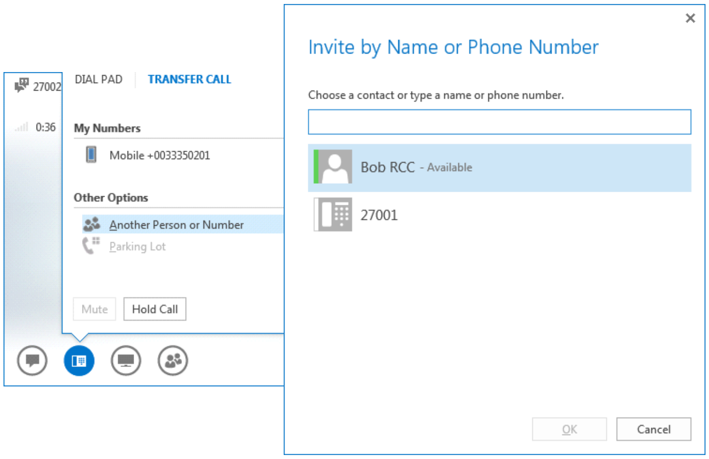
Single Step Transfer

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).

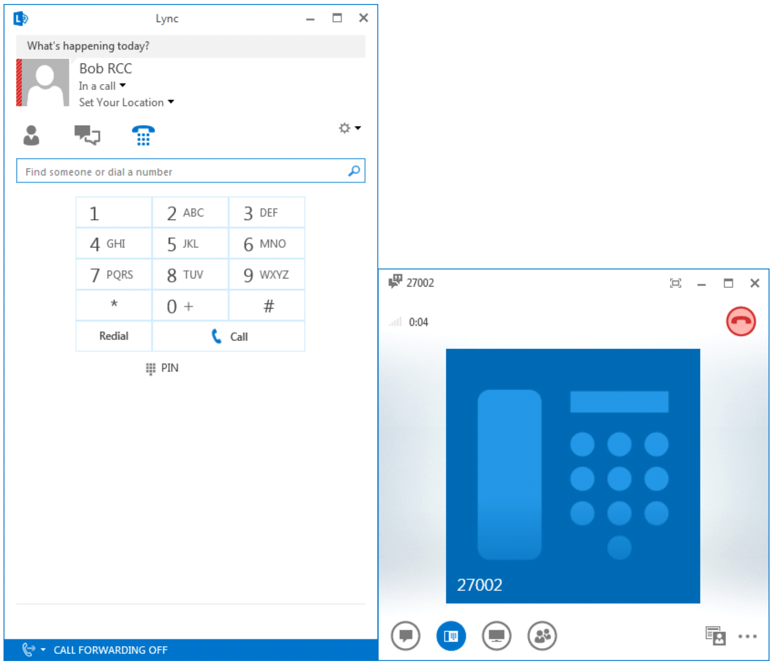
We assume you have answered a call with extension C (27002).



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

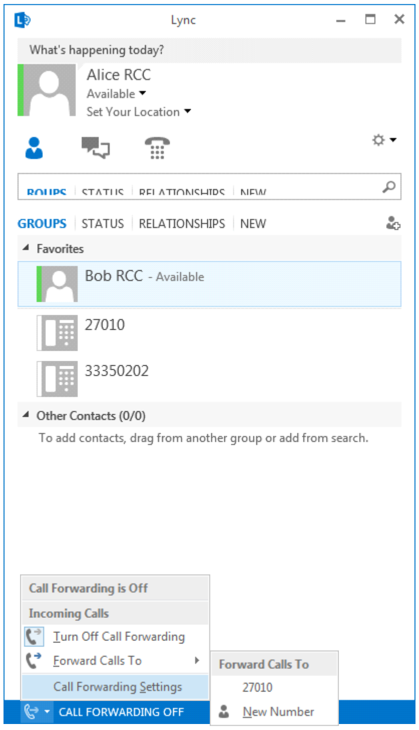


Then, check if the call is correctly transferred.

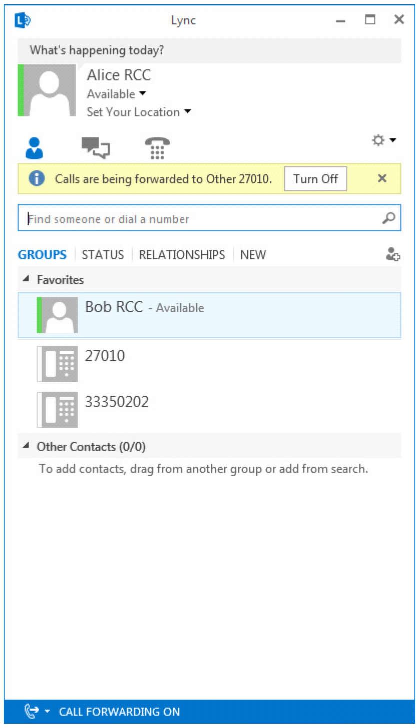


Forward an Incoming Call

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



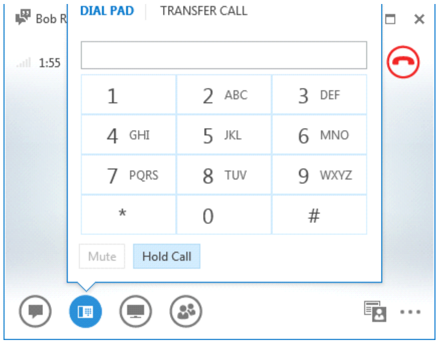
Check if Lync client is showing that the forwarding is on.



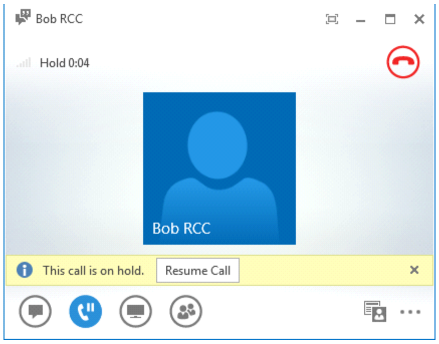
Calls are being forwarded to Other 27010.

Place Calls on Hold

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



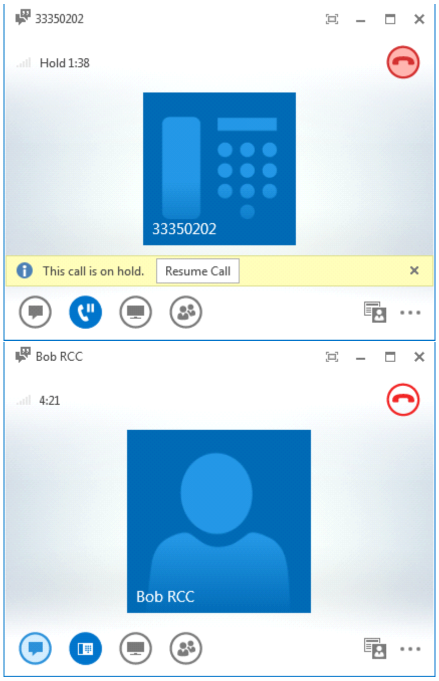
Click on Resume Call to return to the call.



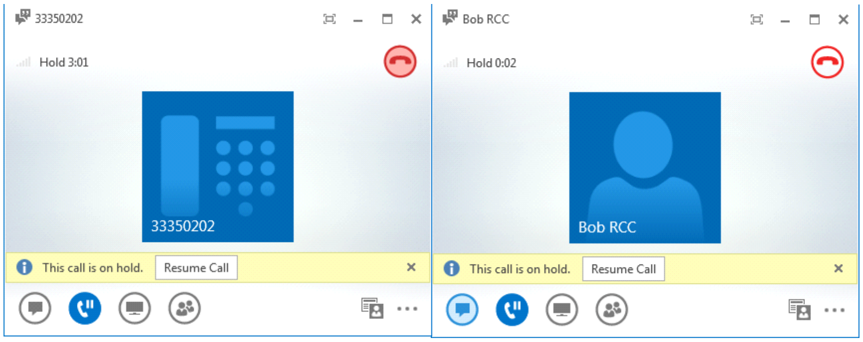
This call is on hold.

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.



This call is on hold.

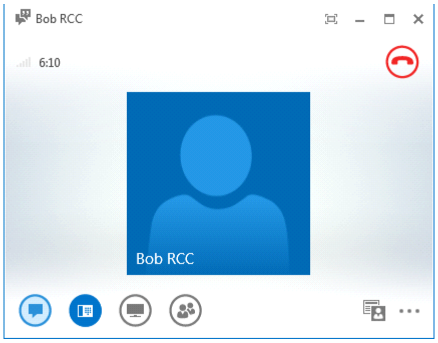


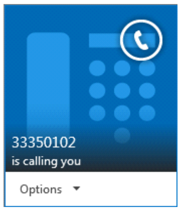
This call is on hold.

This call is on hold.

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

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

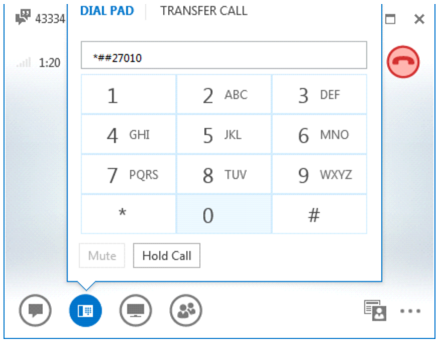




You can alternate between the calls.

Dial Dual-Tone Multi-Frequency (DTMF) Digits

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

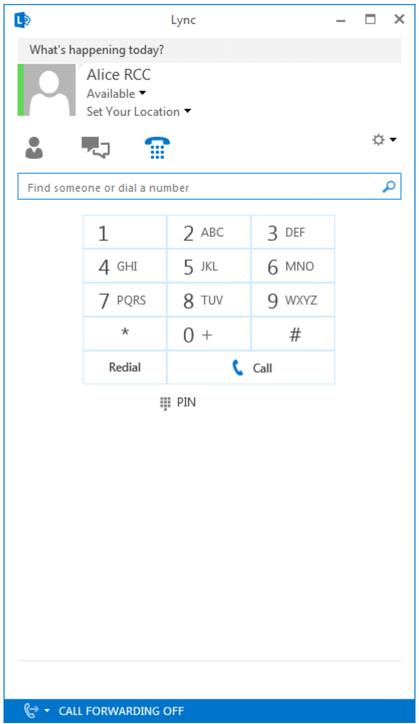


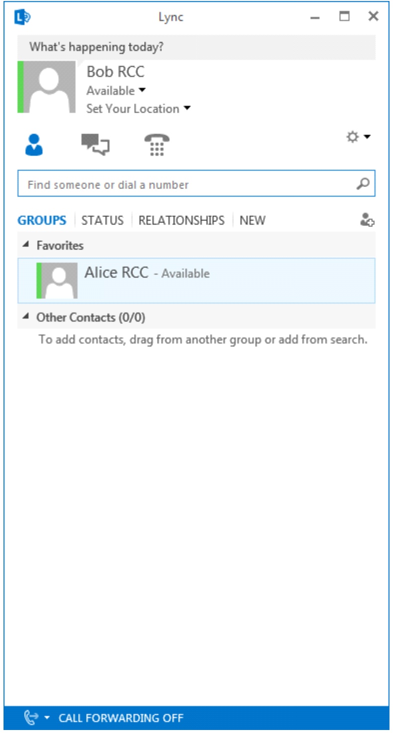
*##27010

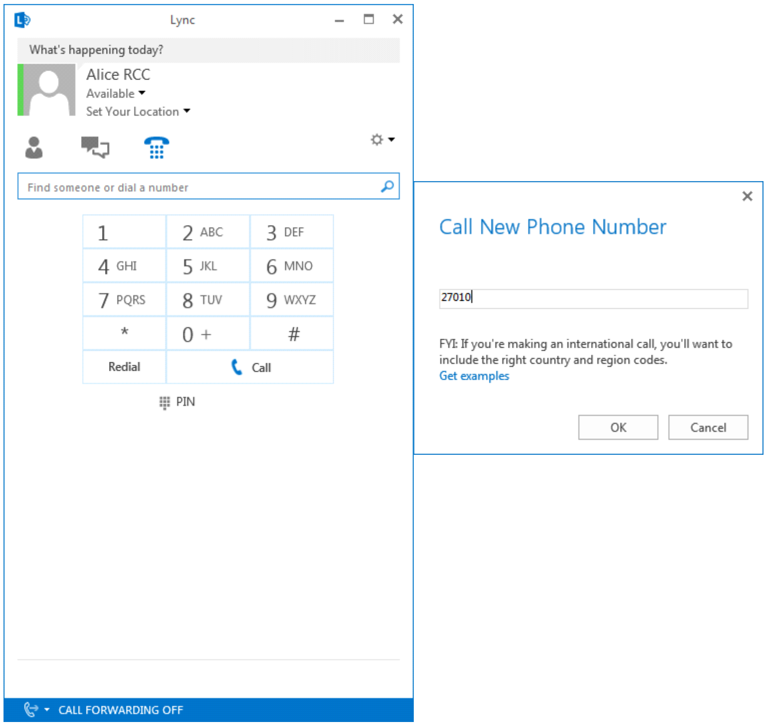
Presence

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





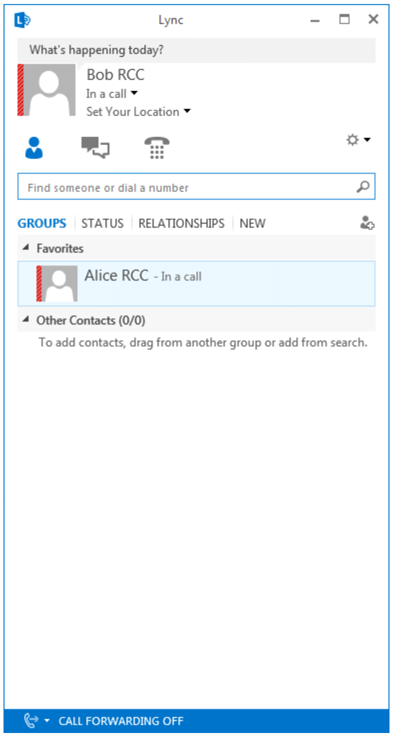


Call New Phone Number

27010

FYI: If you're making an international call, you'll want to include the right country and region codes.

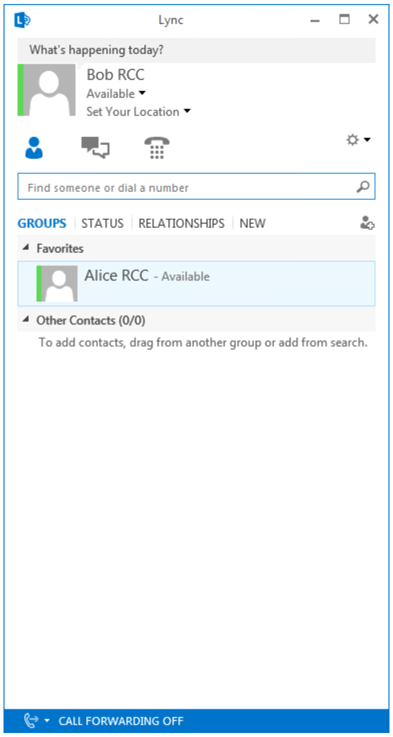
From another Lync client, for example Bob, RCC that is monitoring Alice RCC, check if the presence status is now “In a Call”.



Alice RCC - In a call

To add contacts, drag from another group or add from search.

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



To add contacts, drag from another group or add from search.

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 *MBG Installation and Maintenance Guide 11.0* 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 between the Internet and MBG for SIP XML
- TCP port 22222 for classic XML logon between MBG and MX-ONE for SIP XML
- TCP port 22226 for native VDP logon between the Internet and MBG for Configuration Server Access
- TCP port 22225 for native VDP logon between MBG and the Configuration Server (MX-ONE)

- 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. Classic XML logon:
      i. Configure the XML listen port as 22223 and check TLS.
      ii. Configure the XML destination port as 22222 and uncheck TLS.
   e. Native VDP logon:
      i. Configure the configuration server listen port as 22226 and check TLS.
      ii. Configure the configuration server port as 22225 and uncheck TLS.
   f. Configure the configuration server address (the address to MX-ONE).
   g. 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
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/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 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
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/22222 for classic XML logon or https/22226 instead of http/22225 for native VDP logon.

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

```
[root@ ~]# /usr/sbin/configure_68xx_mbg_support.sh
mbg_wan_ip=
mbg_lan_ip=
configure_tftp=false
generate_certificate=false
force=false
----------
--mbg_lan_ip parameter must be specified
----------
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.

Mitel

Powering connections

mitel.com