MiVoice MX-ONE

Optional Installations

Release 7.1
July 22, 2019

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:

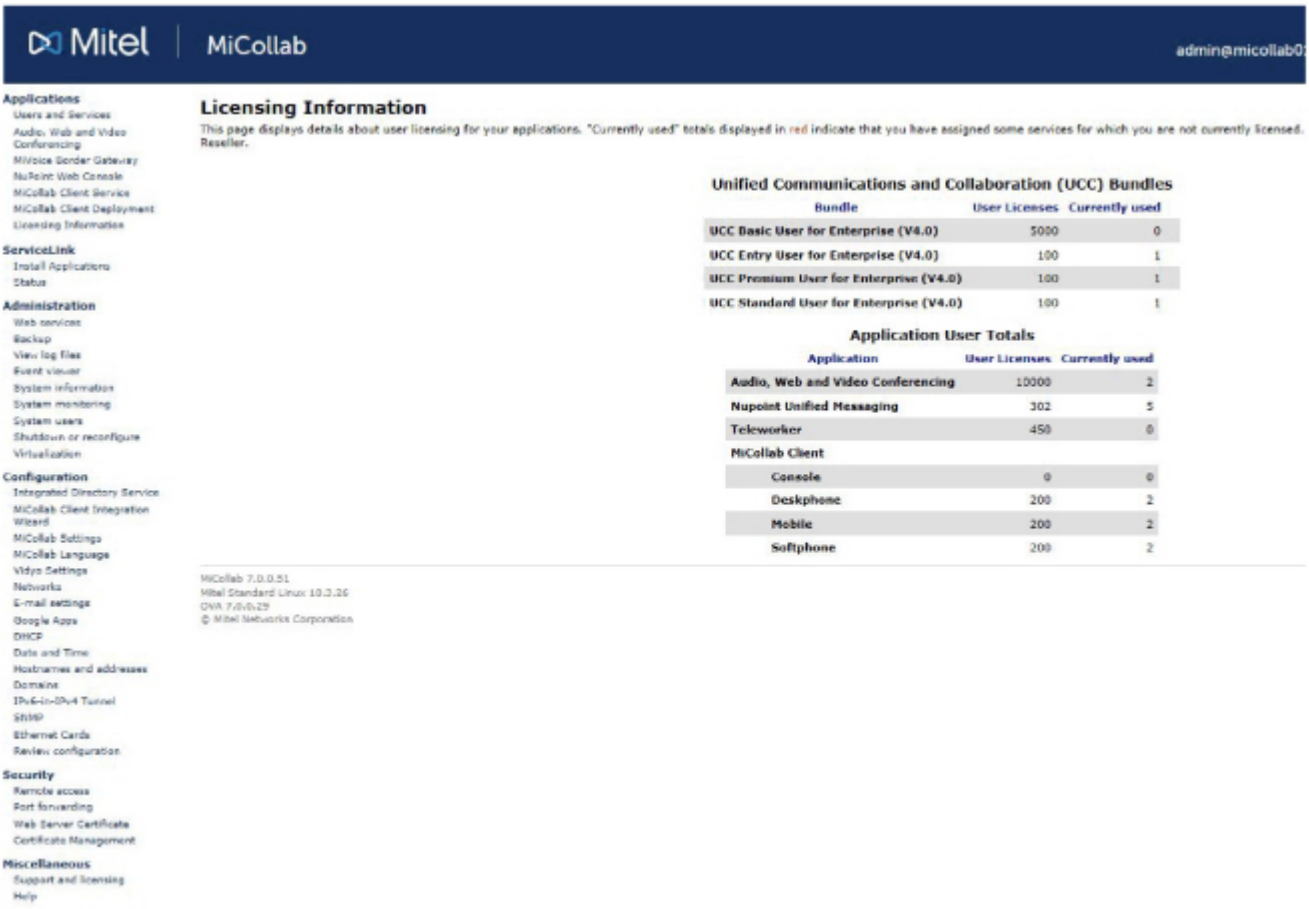
1. Start the virtual machine.
2. Open the console interface.
3. Choose keyboard.
4. Restore from backup - no.

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



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

Customer Product Information of Mitel Performance Analytics, see Product Documentation.

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.

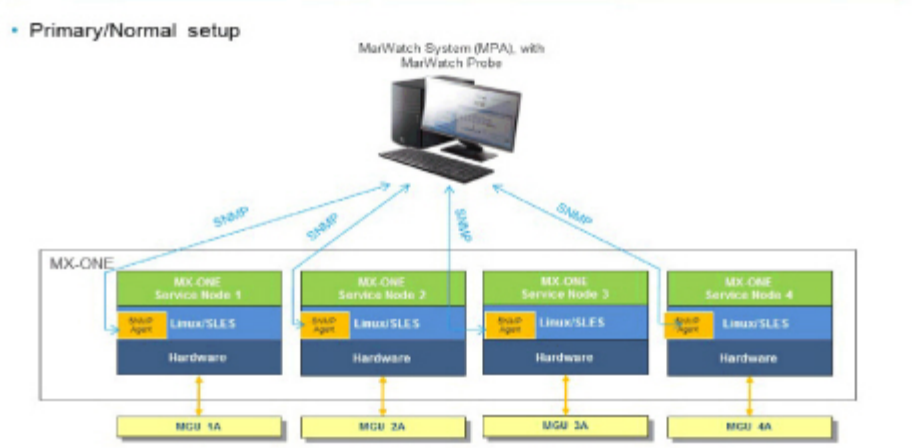
Supported Scenarios

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

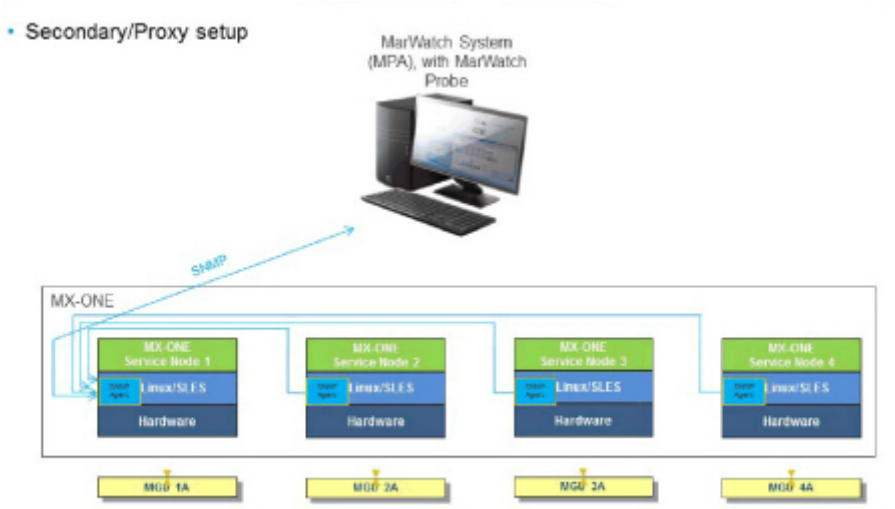


Another possibility is that one Service Node can act as a proxy for several other Service Nodes (and other entities), in which case only the proxy Service Node will be connected to the MPA probe.

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.

Example:(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 MPA’s.

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.

MiVoice Call Recording

Customer Product Information of MiVoice Call Recording, see Product Documentation.

Microsoft Products

This topic discusses the integration of MX-ONE with the Microsoft products described in the following sections:

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

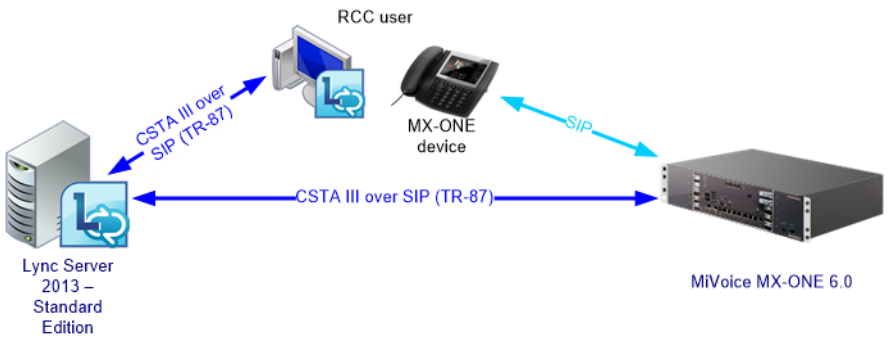
Microsoft Lync Server 2013 offers Remote Call Control (RCC) support that allows users to remotely control phones connected to a call manager, such as MX-ONE. It gives Lync 2013 client users the ability to make or receive calls on their fixed or mobile phone instead of a computer.

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.

Figure 4.1: 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 4.2: 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:

1. CSTA server needs to be initiated
2. CSTA Server needs to be initiated.

CSTA III Setting:

```
csta -- initiate -- lim 1 -- csta-serv 00000010
```

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:

1. Configure a Static Route for Remote Call Control
2. Configure a Trusted Application Entry for Remote Call Control
3. 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 Control Setup, 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 -ApplicationID RCC -TrustedApplicationPoolFqdn 192.168.222.156 -Port 5062 -EnableTcp
To verify the setup use the command:
Get-CsTrustedApplication

Publish the topology

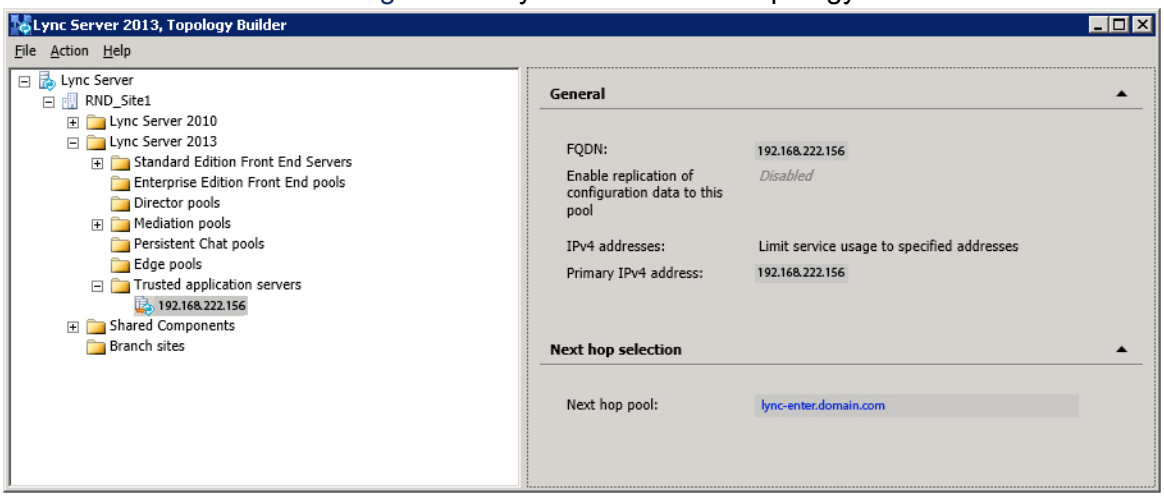
To implement the changes in the Lync , publish the topology
Enable-CsTopology

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.

Figure 4.3: Lync Server 2013 Topology Builder



Enable Lync Users for Remote Call Control

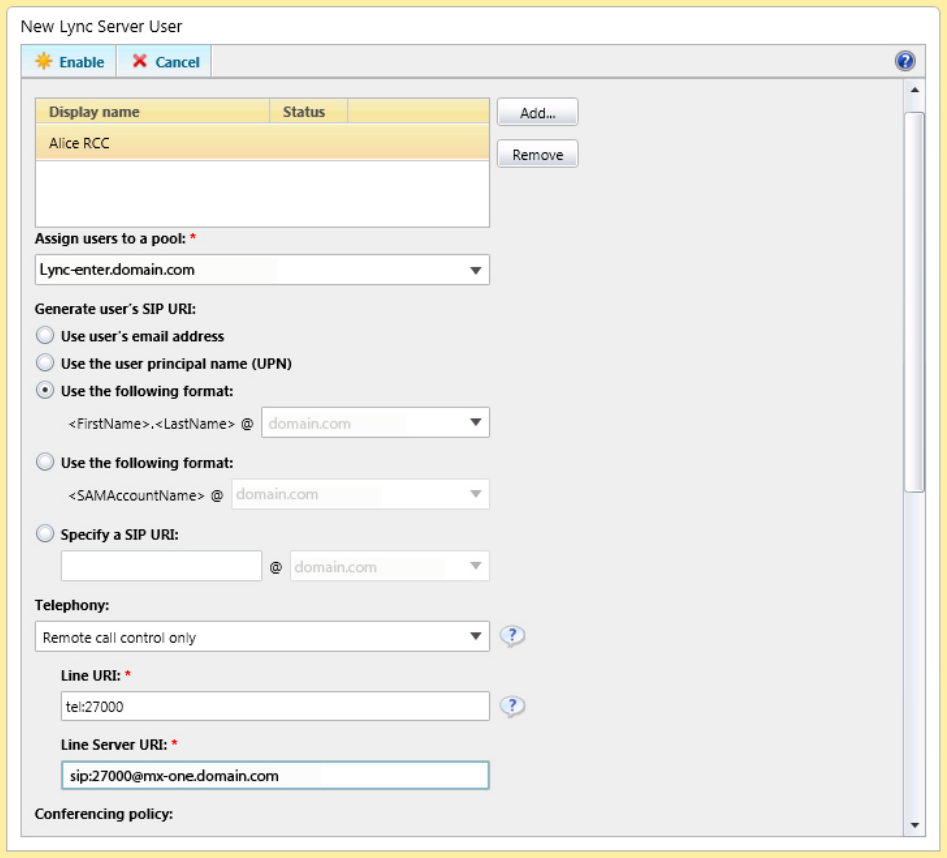
Configure a user for remote call control by using Lync Server Control Panel.

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

Figure 4.4: RCC only new user configuration example



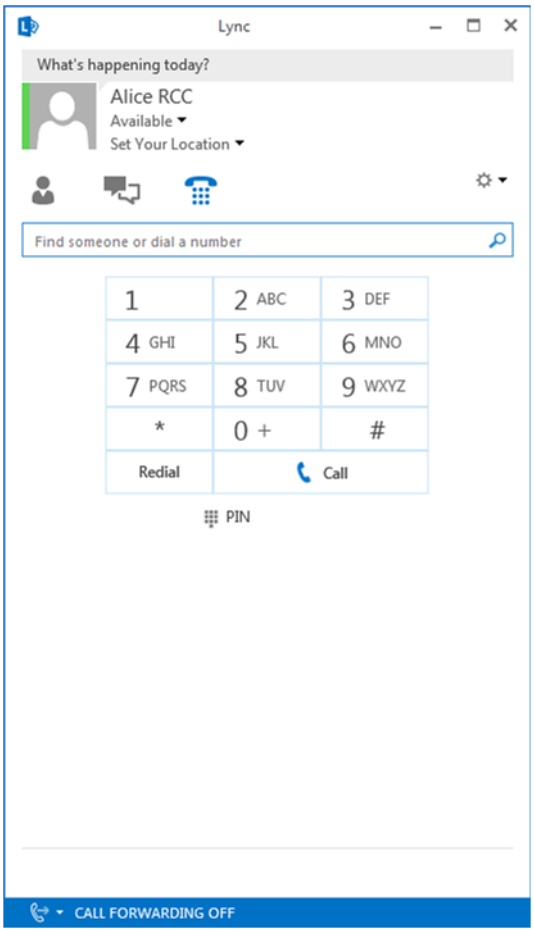
How to Verify the Setup

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

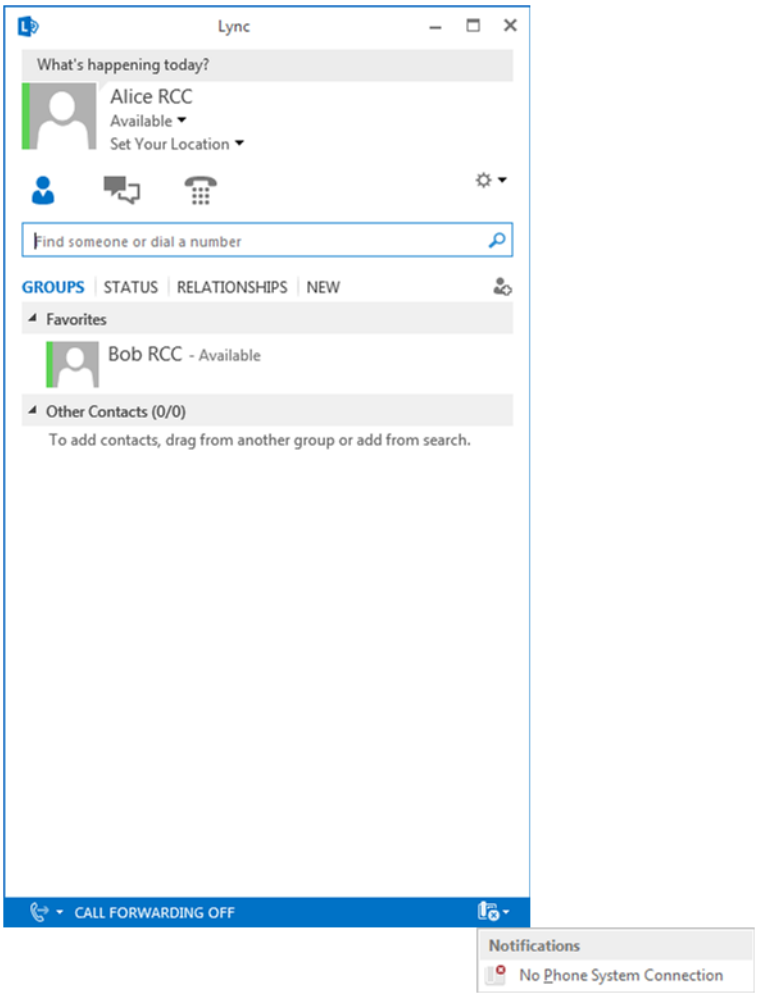
Lync 2013 Client Features

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.

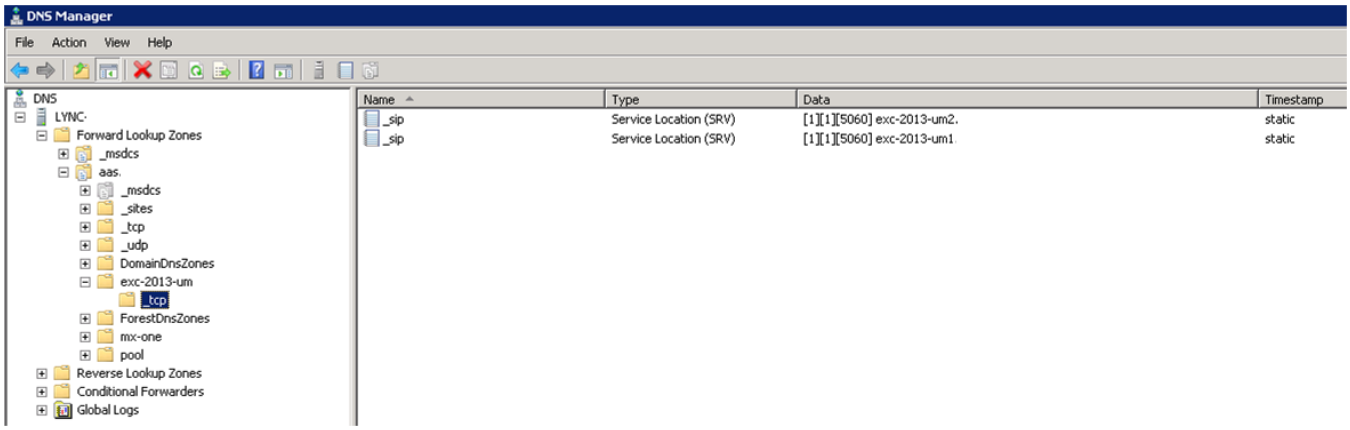
1. Alice.RCC controls the extension 27001, which is a SIP extension in MX-ONE.
2. Bob.RCC controls the extension 27010, which is a SIP extension in MX-ONE.
3. 27000 and 27002 are SIP extensions in MX-ONE.
4. 33350202 and 33350102 are the PSTN phones.

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

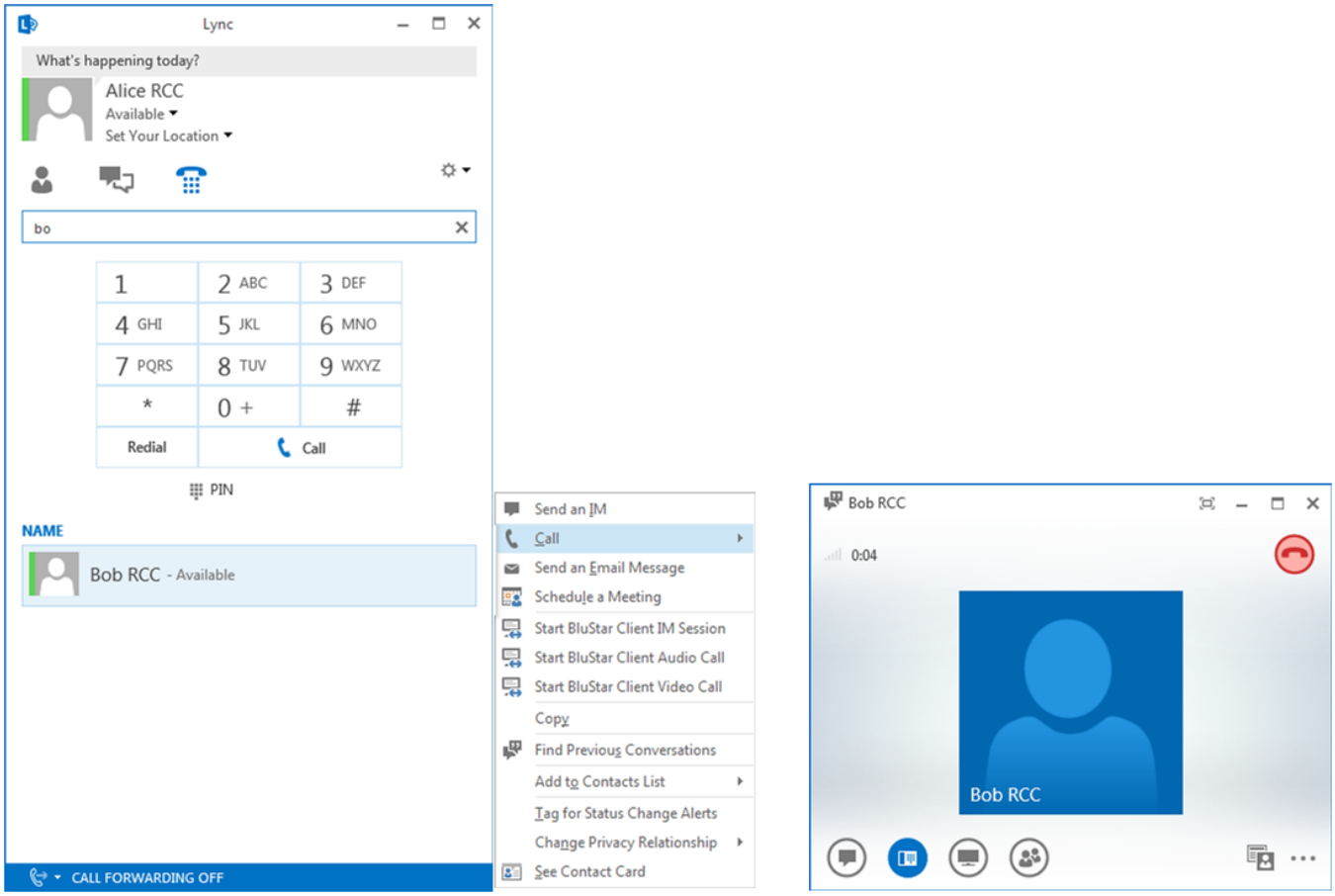
From another extension dial to RCC user, answer it and check if there is speech.



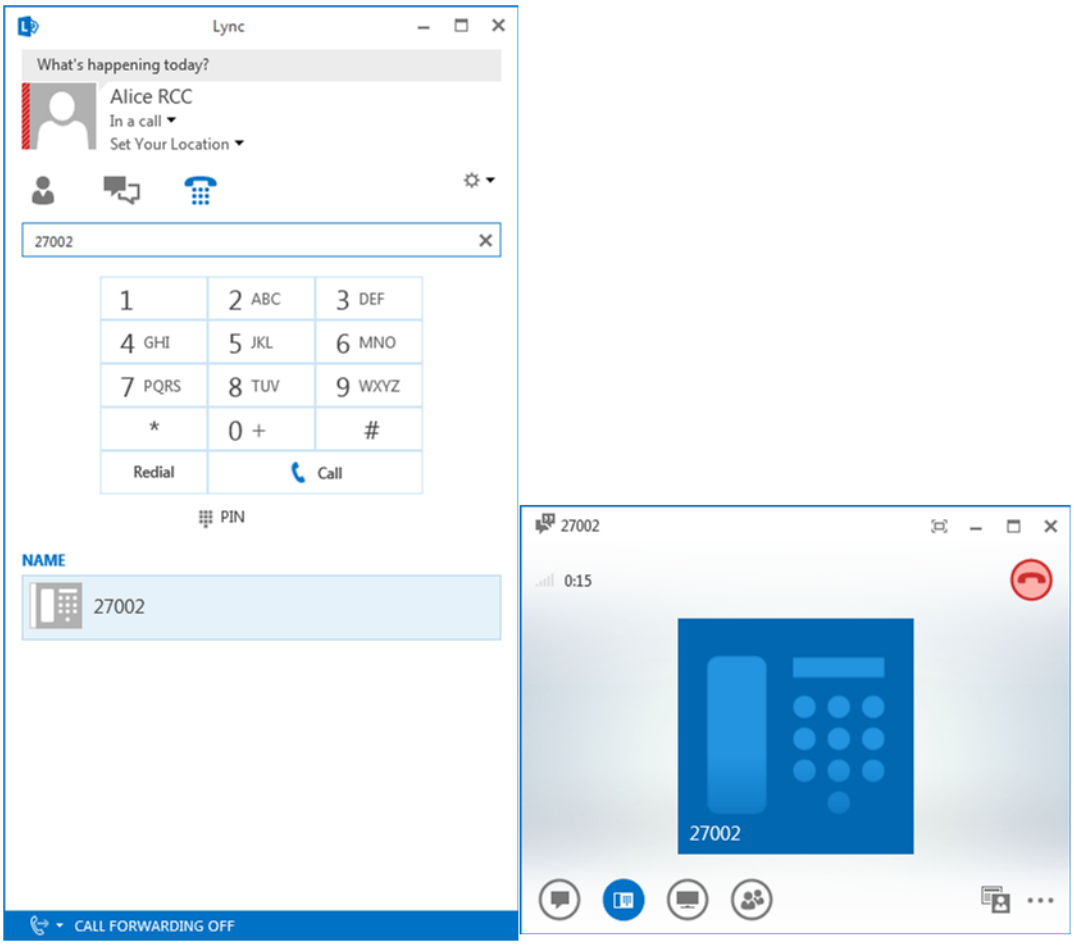
Transfer a Call Between Current Conversations (Monitored Transfer)

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.

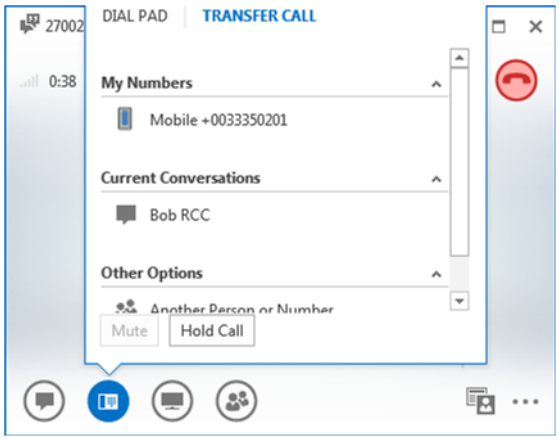
We assume you have answered a call with extension B (27010) from the Lync client (RCC



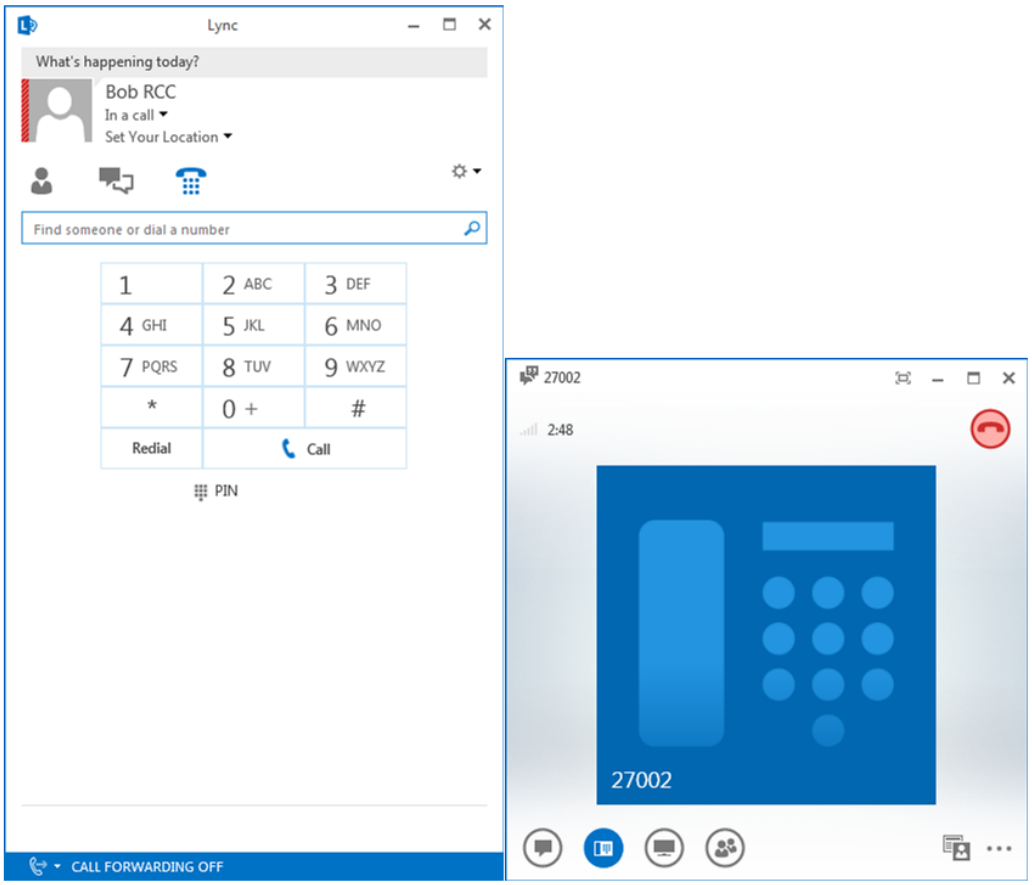
Using the client, put extension B on hold and make a second call to extension C (27002), and wait until the extension C answers.



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.

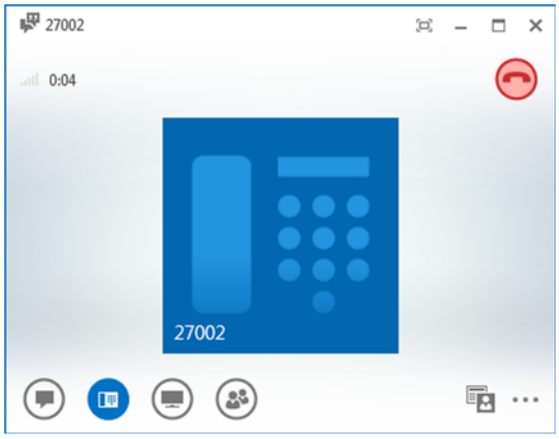


Then, check if the call is correctly transferred.

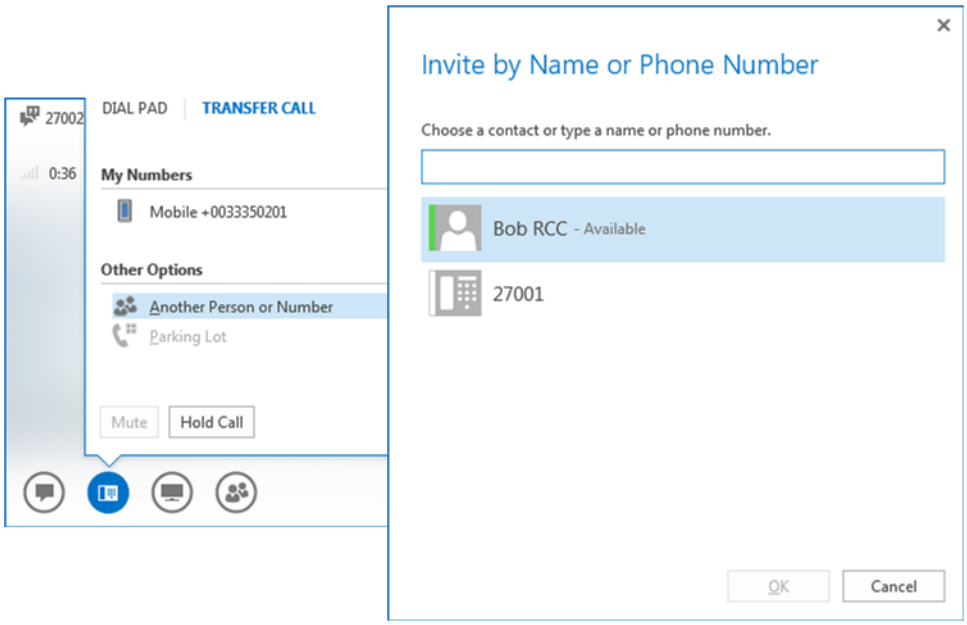
Single Step Transfer

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).

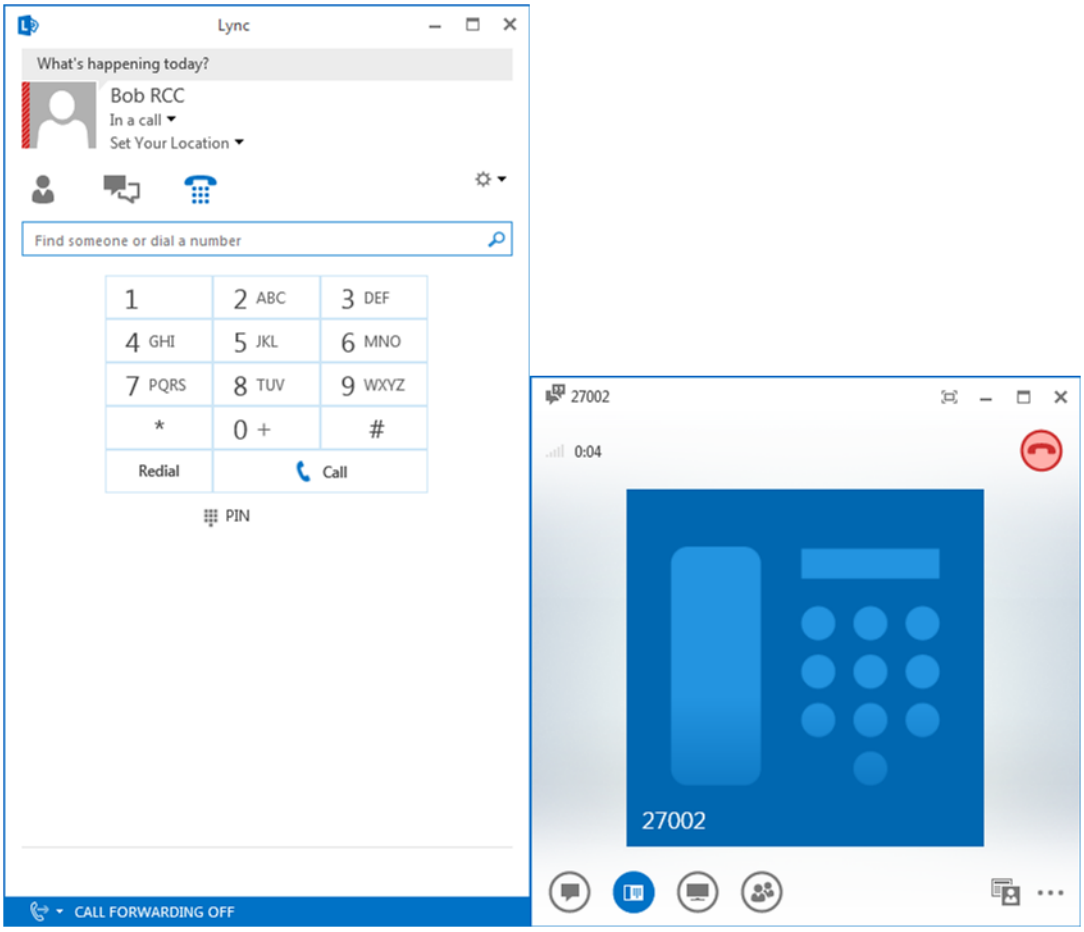
We assume you have answered a call with extension C (27002).



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

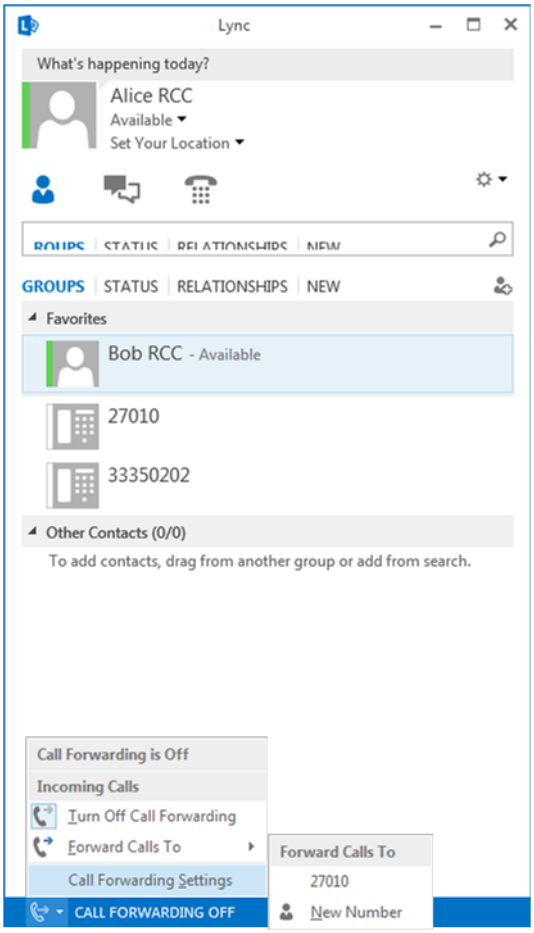


Then, check if the call is correctly transferred.

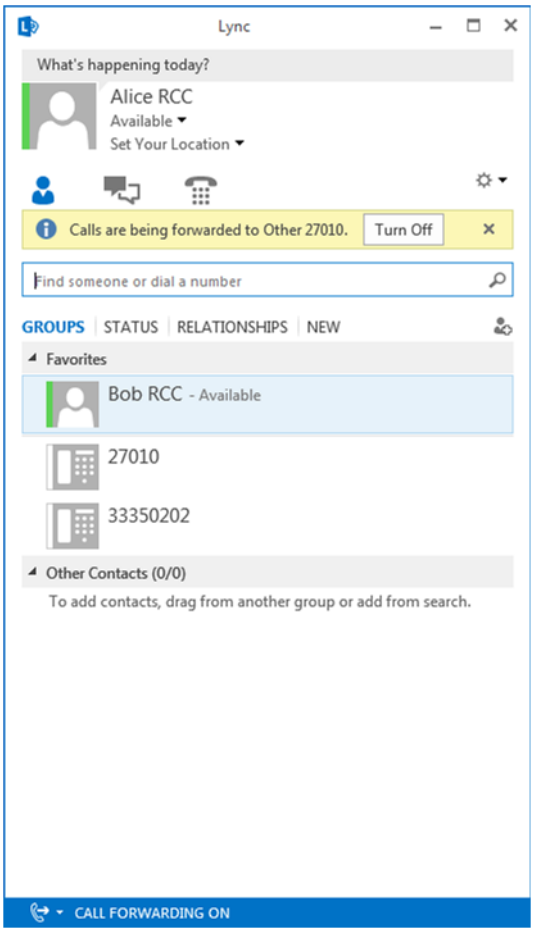


Forward an Incoming Call

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

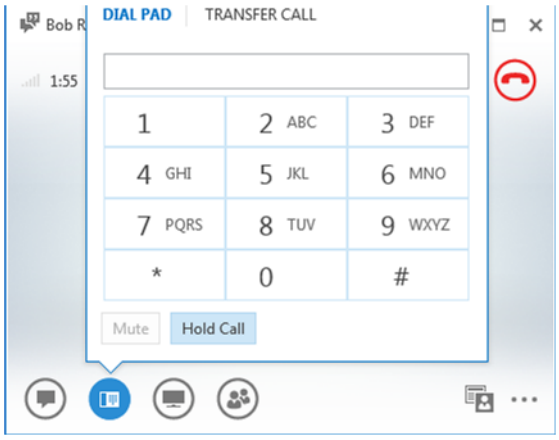


Check if Lync client is showing that the forwarding is on.

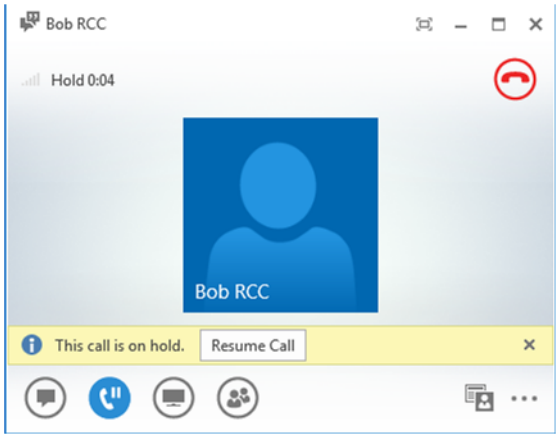


Place Calls on Hold

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

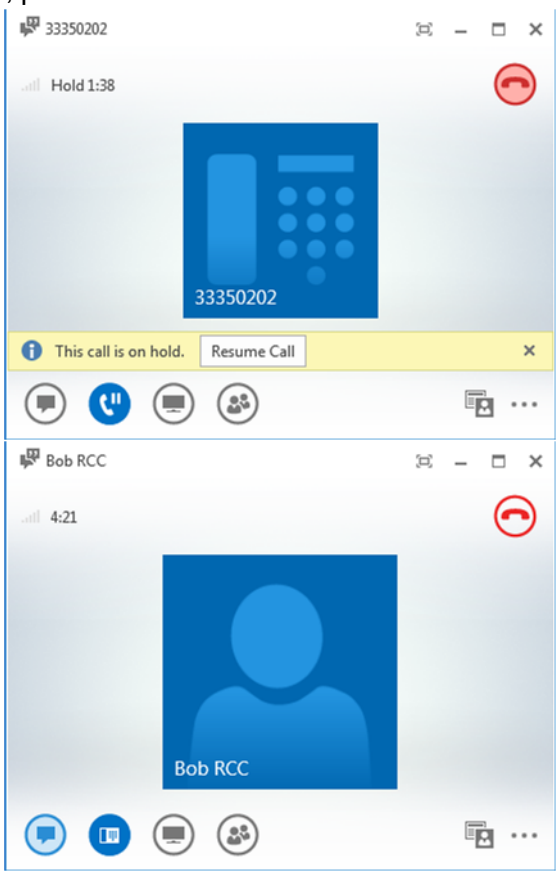


Click on Resume Call to return to the call.

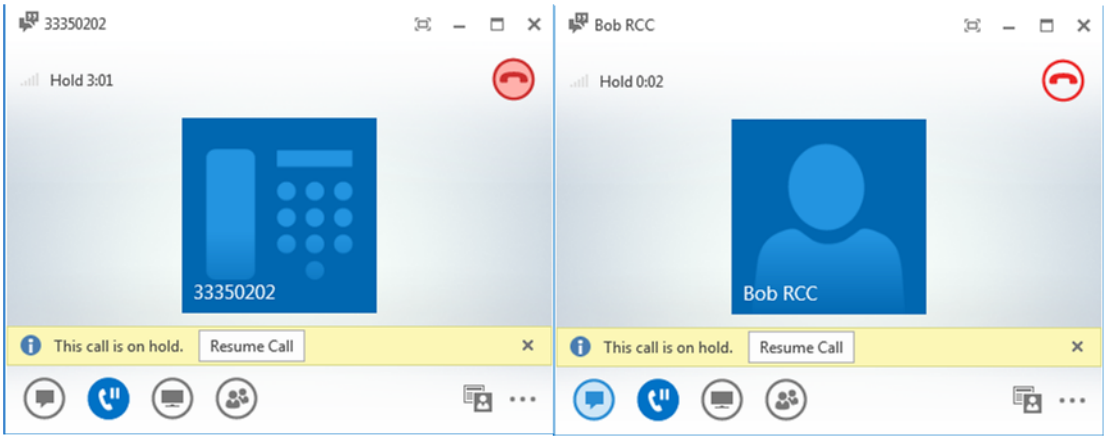


Alternate Between Multiple Concurrent Calls

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

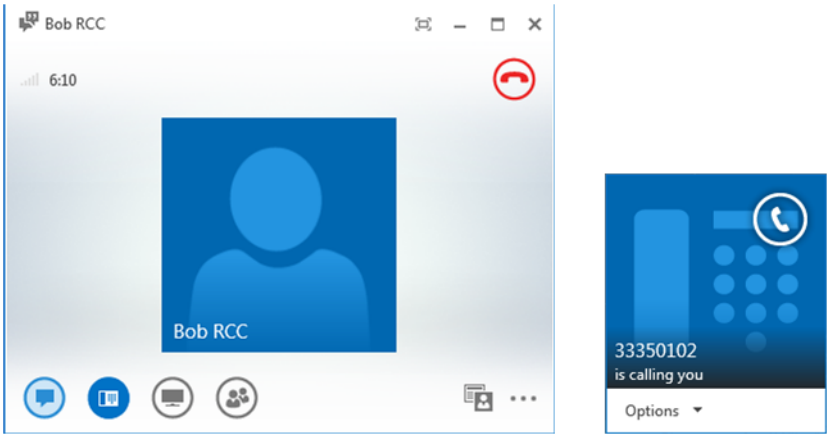


the first one.



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

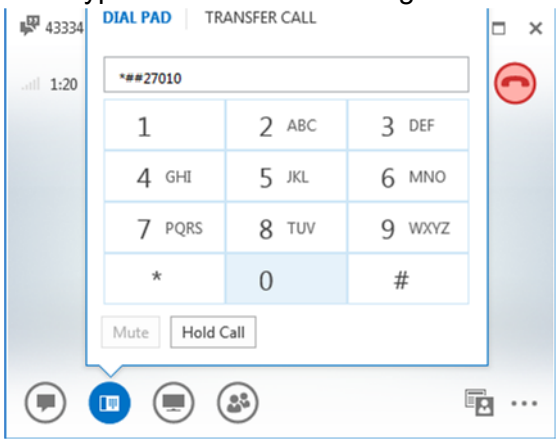
When a second call is alerting, click on Accept Call to answer it.



You can alternate between the calls.

Dial Dual-Tone Multi-Frequency (DTMF) Digits

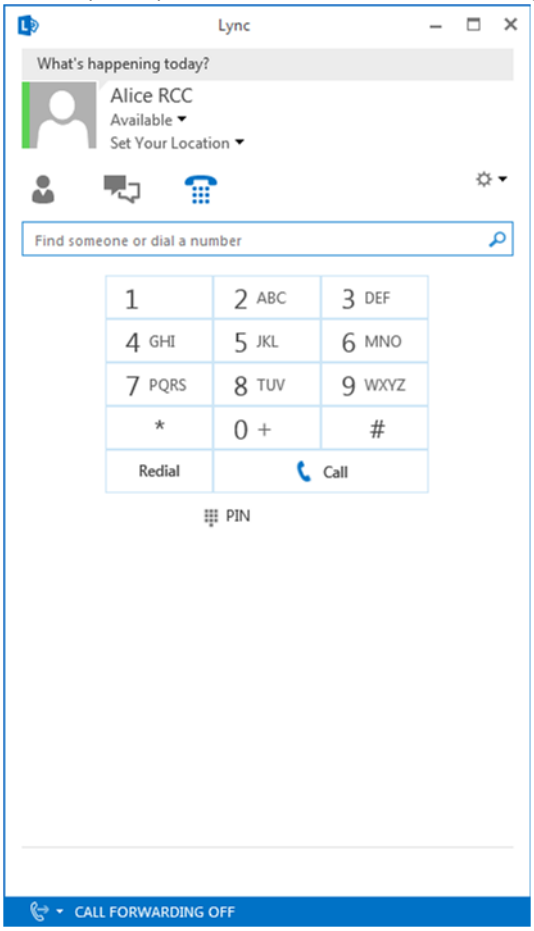
In an established call, click on the keypad and enter DTMF digits.

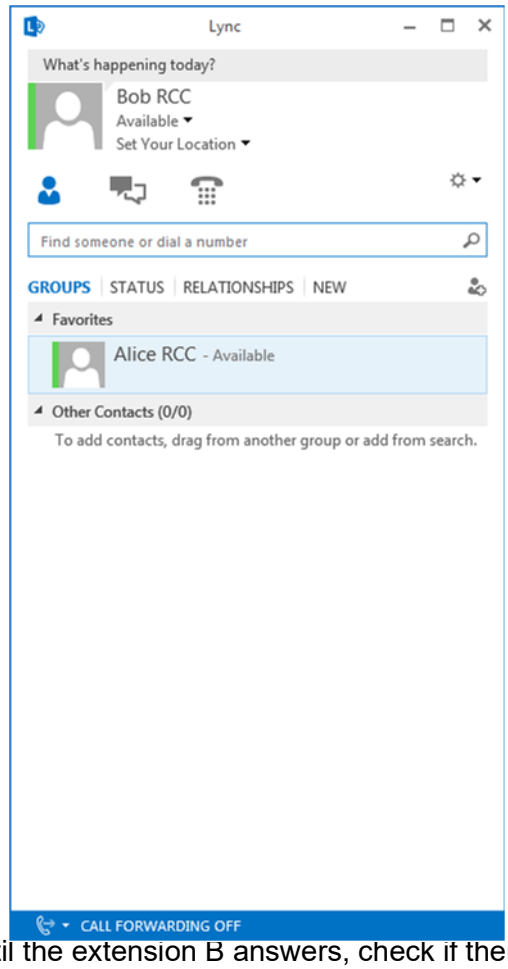


Presence

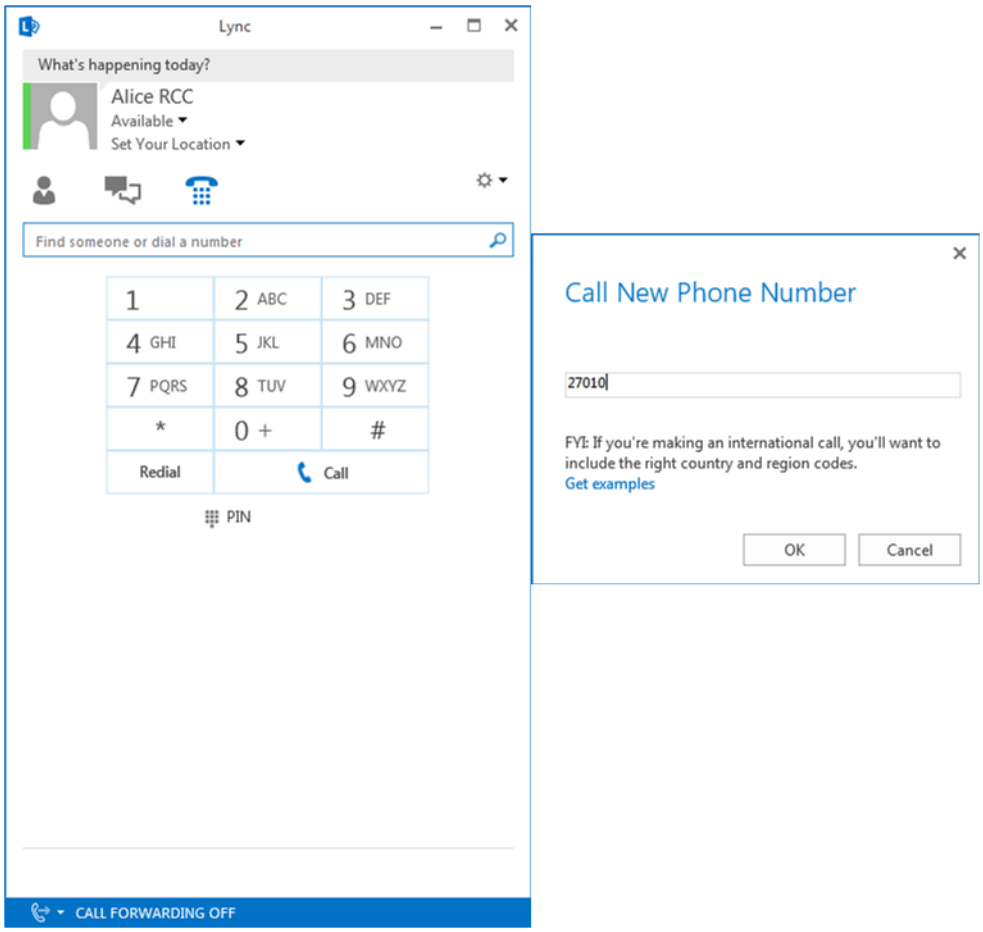
In order to verify presence, establish a call using Lync client (RCC) as below.

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



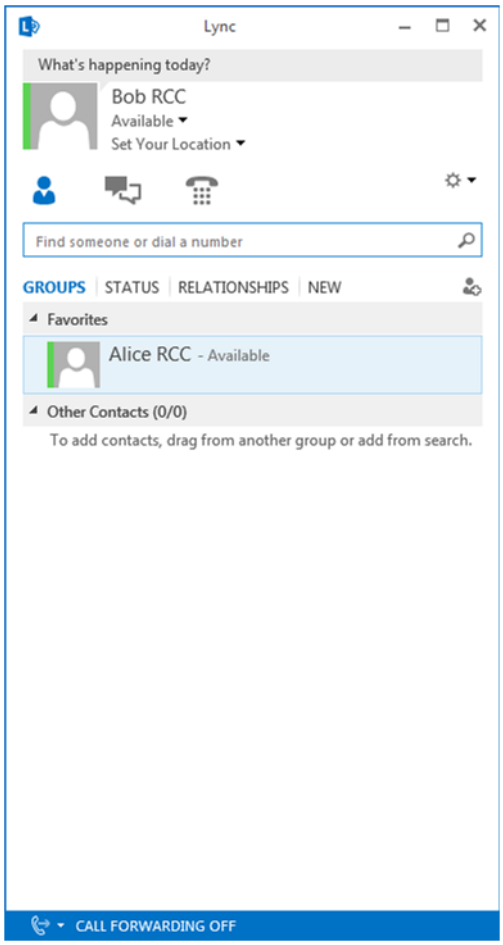


hear the ring back tone, wait until the extension B answers, check if there is speech.



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

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



Limitations

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

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

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

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

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

Good to Know

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

Latest Lync client needs to be installed.

DNS needs to be properly configured.

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

Teleworker Solution

Customer Product Information of MiVoice Border Gateway, see Product Documentation.

General

This document describes how to configure a single standalone MiVoice Border Gateway (MBG) Release 9.2 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)	10.4.13.0	Release 10.4 64 bits is required. Refer to the Hardware Compatibility List for MSL found on Mitel-On-Line.
MX-ONE	6.3	MX-ONE version 6.0 SP2 HF3 was tested in the Kanata lab, so this version, or later, could be used, but 6.3 is recommended.
6900	5.0.0	Release 5.0 SIP extensions
68xxi	4.2.0.181	Release 4.2 Release 4.2 SP1 recommended.
MBG	4.2.0.181	Release 9.2 PR2 and up recommended.

Installation Notes

The principle used here is to configure MBG to have secure communication on the outside towards the home worker terminals and unsecure 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 9.2 on a Standalone Physical Server

1. Install the latest Microsoft SQL (MSL) 10.4 64 bits release software version.
2. Install Release 9.2 via MSL's server-manager Blades panel after syncing with the Mitel Application Management Center (AMC); or,
3. Obtain a copy of the latest MiVoice Border Gateway Rel 9.2 software and burn it onto a CD. After inserting the CD in the CD-ROM/DVD-ROM drive, upgrade via MSL's server-manager Blades panel.

NOTE: Your CD burning software must be capable of burning ISO images.

Installing Release 9.2 in a VMware Environment

Virtual deployment should deploy the latest released MBG 9.2 ova and then upgrade to the latest available blade of that stream.

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 between the Internet and MBG for SIP XML
- TCP port 22222 between MBG and MX-ONE for SIP XML
- TCP port 4431 between the Internet and MBG for Configuration Server Access (Optional)
- TCP port 80 between MBG and the Configuration Server
- UDP port 20000-31000 between the Internet and MBG and between MBG and the LAN for voice
- TCP port 22 between LAN and MBG for secure shell access
- UDP port 53 between MBG and the LAN for DNS resolution to a Corporate DNS server

NOTE: Do not enable TCP port 5060 or UDP port 5060 between the Internet and MBG.

MSL Configuration

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

MBG Configuration

From a new installation of Release 9.2, access the MiVoice Border Gateway User Inter-face from MSL server-manager and perform the following steps:

1. Go to System Configuration > Network Profile.
2. Select Profile and Apply.
3. Go to System Configuration > Settings.
   a. Under SIP options, increase the Set-side registration expiry time to 360 from the default of 240.
   b. Enable SIP support for TCP/TLS and TCP.
   c. Change Codec support to Unrestricted.
   d. 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.
4. Service Configuration > ICPs.
   a. Add your MX-ONE system as type MiVoice MX-ONE with SIP capabilities as UDP, TCP.
   b. Configure MX-ONE support.
   c. Check Link to the ICP and Enable.
   d. Configure the XML listen port as 22223 and check TLS.
   e. Configure the XML destination port as 22222 and uncheck TLS.
   f. Configure the configuration server listen port as 4431 and check TLS.
   g. Configure the configuration server port as 80 and uncheck TLS.
   h. Configure the configuration server address.

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

5. Do not start MBG yet.
6. Setup MBG with mutual TLS for SIP using configuration script.
7. Connect to the system via ssh (ex: using putty) and login as root.
8. 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 --mb-g_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_mx-one_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_mx-one_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.

9. Return to the MiVoice Border Gateway User Interface and click on Dashboard to Start MBG.
10. Confirm that Teleworker 68xx phones have access to the public IP of MBG using the Teleworker Network Analyzer tool.
11. 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.
12. Launch the application and run a connect test against the public IP.

SIP TLS, Aastra MXL MXOne, Voice Traffic (begin) and (end) should return OK.

If any of the above return CLOSED or TIMED OUT, contact your firewall administrator.

Phone Configuration

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

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

Limitations

A list of known limitations shared with the InGate solution.

1. Phones must be staged in the office.
2. Phone firmware must be done in the office as a phone firmware upgrade will remove the certificate loaded.
3. Access to internal configuration server cannot be limited/controlled/blocked from the outside.
4. 68xxi must have access to a NTP server for certificate validation.

5. Corporate directory access must be setup with port forwarding on MSL (server-gateway configuration) or the DMZ firewall.
6. If MX-ONE is setup to like lim1.mysystem.com, the MSL server must point to a Corporate DNS to allow proper DNS resolution.

Here is a list of known limitations with MBG

1. Single dedicated MBG.
2. MBG clustering and backup SIP registrar/proxy in the 68xxi configuration files.
3. Using FQDN instead of IP address in the 68xxi configuration files.

Known Issues

None.

Issues Resolved

Here is a list of issues resolved in 9.2.0.22 in conjunction with 68xx 4.2 SP1 firmware and workaround is not longer required:

1. MN00609195 MBG 9.2: SIP 68xxi/MX-One/SRTP one way audio after “set side” session timer re-invite (decrypt failure).

Conditions: Session timers are configured on TW 68xxi AND greater than 1310 (default in MX-ONE sample is 1800).

Root Cause: 68xxi do NOT increment SDP version but changes SRTP keys in re-invite and MBG falsely detects the SDP as a duplicate.

Workaround: Select a value less than 1200 for session timers in mitel.cfg for TW 68xxi.

2. MN00616730 MBG 9.2: SIP 68xxi/MX-One/SRTP one way audio after “ICP side” session timer re-invite.

Conditions: Session timers are configured on LAN 68xxi AND greater than 1300 AND the codec list is different between LAN and TW set but 1st selection is the same.

Root Cause: Still under investigation.

Workaround #1: Same codec selection list on TW 68xxi as LAN 68xxi (MX-ONE sample has G.722, G711a, G.711u, G.729. Updates are used instead of re-invite.

Workaround #2: Disable session timers in mitel.cfg for LAN 68xxi or reduce the value to 1200 or less.

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-bun
dle.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.

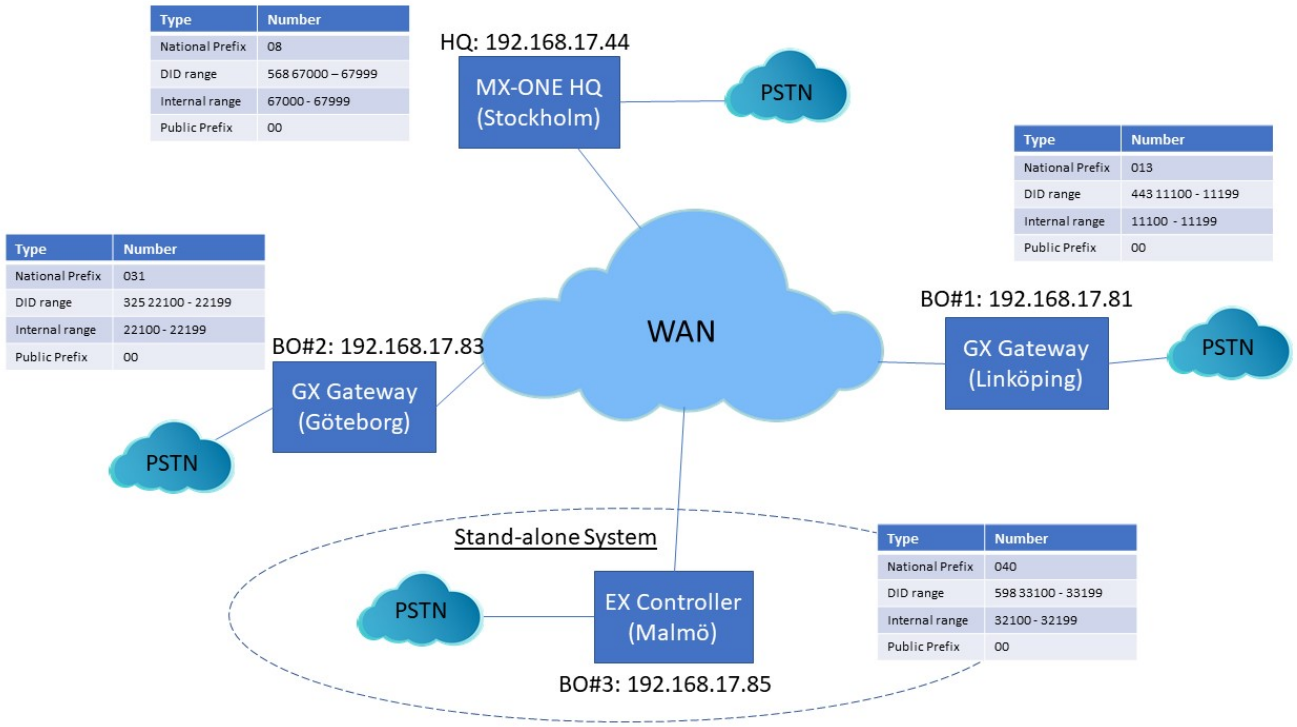
GX and EX Controller

The GX and EX controller installations are explained in this topic.

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 6.1: EX and GX Controller Gateways



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

Prerequisites

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

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

- VDP logon with SCA/SCABR is not working when assigned to a soft key.

- A SIP outbound proxy address must be assigned in the startup.cfg file, that is, the SIP outbound proxy address is the local address of the EX-Controller / GX-Gateway.

Setting up MX-ONE for GX Controller

The number analysis data, extension data, least call routing data, and route data are discussed in this section.

Number Analysis

Number Analysis Data

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

Call Discrimination Data

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

Extension Data

Figure 6.2: Directory Number Profile

Dir Party	Cust Csta	Lim Free	Csp On	Feature Hotline	Lang	Max Hotline	Secretary Num	Max Backup	Security Num	AMC Area	Video	BluStar	Third
Client	Supp		level Second	Line			Cost		Term Exception	Code		Client Mod	SIP
11101	0	1	9		-	-	No	1	Yes	No	No	-	No
00	1		-	-			08101344311101		013				
11102	0	1	9		-	-	No	1	Yes	No	No	-	No
00	1		-	-			08101344311102		013				
11103	0	1	9		-	-	No	1	Yes	No	No	-	No
00	0		-	-			08101344311103		013				
11104	0	1	9		-	-	No	1	Yes	No	No	-	No
00	0		-	-			-		-				
11105	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			08101344311105		013				
11106	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			08101344311106		013				
22101	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			082031325221101		031				
22102	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			082031325221102		031				
22103	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			082031325221103		031				
22104	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			082031325221104		031				
22105	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			082031325221105		031				
22106	0	1	9		-	-	No	4	Yes	No	No	-	No
00	0		-	-			082031325221106		031				
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		-	-			-		-				

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: 11113001100100000000100000300

Cdiv: 111000111010000

Roc: 000001

Npres: 0011000

Offered Time: 0

Forced DisconnectTime: 0

CnnLog: 0

Csp Name: Intrusion

Least Cost Routing Data

Least Cost Destination Data

Table 6.1:

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

END

Least Cost Destination Data

Table 6.2: (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
006	0		N	6	18	Y
007	0		N	6	18	Y
008	0		N	6	18	Y

Table 6.2: (Continued) (Sheet 2 of 2)

Entry	TRC	PRE	CONF	MIN	MAX	ACF
009	0		N	6	18	Y

Least Cost Destination Data

Table 6.3:

Entry	TRC	PRE	ACCT	FRCT	TOLL	CBCS	BTON	TNS	OSA
	5		0	1	111111 111111 111		0		
	5		0	2	111111 111111 111		0		
	5		0	3	111111 111111 111		0		
	4		0	4	111111 111111 111		0		

END

Least Cost Destination Data

Table 6.4:

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

END

Route Data

ROCAP

Route Category Data

Figure 6.3: Route Category Data

```
ROU      CUST SEL            TRM SERV       NODG DIST DISL TRAF     SIG
BCAP
81       7110000000000010 4     3100000001 0    30   128  03151515 0111110000A0
001100
83       7110000000000010 4     3100000001 0    30   128  03151515 0111110000A0
001100
211      7110000000000010 4     3100000001 0    30   128  03151515 0111110000A1
001100
```

RODAP

Route Data

Table 6.5:

ROU	Type	VARC	VARI		VARO	Filter
81	TL66	H'00000000	H'00000000	H'00000000	NO	
83	TL66	H'00000000	H'00000000	H'00000000	NO	
211	TL66	H'00000000	H'00000000	H'00000000	NO	

SIP ROUTE

One SIP route to each branch node is specified.

Route 81 towards BO#1 (Linköping)

route : 81

protocol = tcp

profile = Default

service = PUBLIC

uristring0 = sip:?@192.168.17.81

fromuri0 = sip:?@192.168.17.44

remoteport = 5070

accept = TRUNK_INFO

match = user=trunk

register = NO_REG

Route 83 towards BO#2 (Göteborg)

route : 83

protocol = tcp

profile = Default

service = PUBLIC

uristring0 = sip:?@192.168.17.83

fromuri0 = sip:?@192.168.17.44

remoteport = 5070

accept = TRUNK_INFO

match = user=trunk

register = NO_REG

Route 211 towards BO#3 (Malmö)

route : 211

protocol = udp

profile = MXONE-tieline

service = PRIVATE_SERVICES

uristring0 = sip:?@192.168.17.94;tgrp=BO3

fromuri0 = sip:?@192.168.17.44;tgrp=BO3

accept = ALL

register = SET_BY_PROFILE

trusted = TRUST_BY_PROFILE

NOTE: BO#3 is only reached by SIP trunks as it is an EX controller system running an own instance of MX-ONE.

Setting up the GX Gateway

This section describes how to setup BO#1 (Linköping).

Setting up BO#2 (Göteborg) is similar, only numbering information and own IP-address is changed.

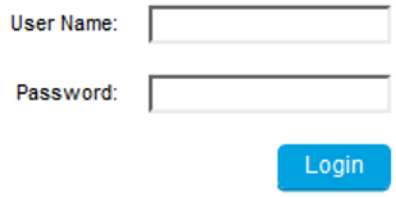
Logon

This section describes how to setup BO#1.

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

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

Figure 6.4: Login page



This section describes how to setup BO#1.

1. Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network)
   – User name/password: public /
   – User name/password: admin/administrator
2. Plug in the analog phone in the FXS port 1 of the EX Controller and dial *#*0 to know the IP address of the EX Controller assigned by using DHCP server.
3. Log into the EX Controller by using the above-mentioned IP address and navigate as described below to configure.

Network Settings

Host

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

Figure 6.5: Host settings - 1

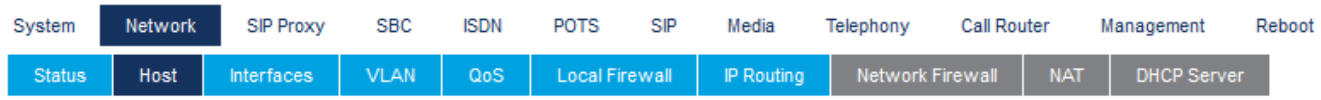
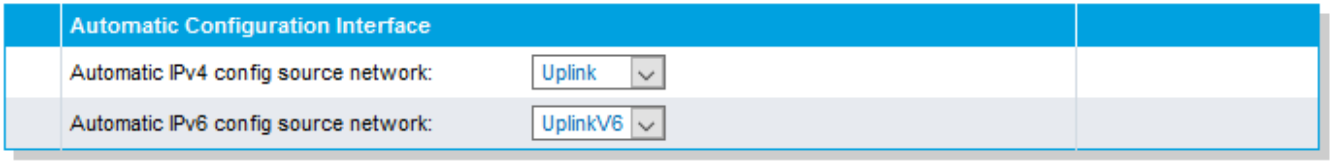
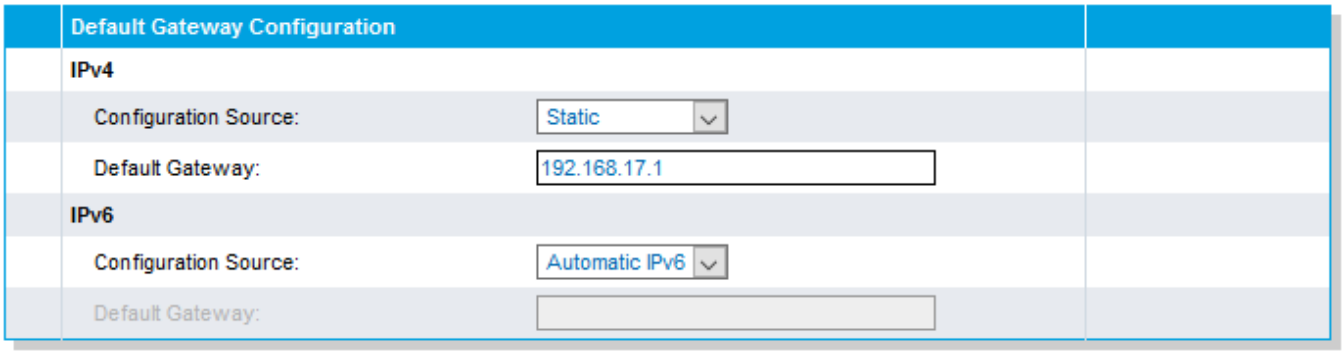


Figure 6.6: Host settings - 2



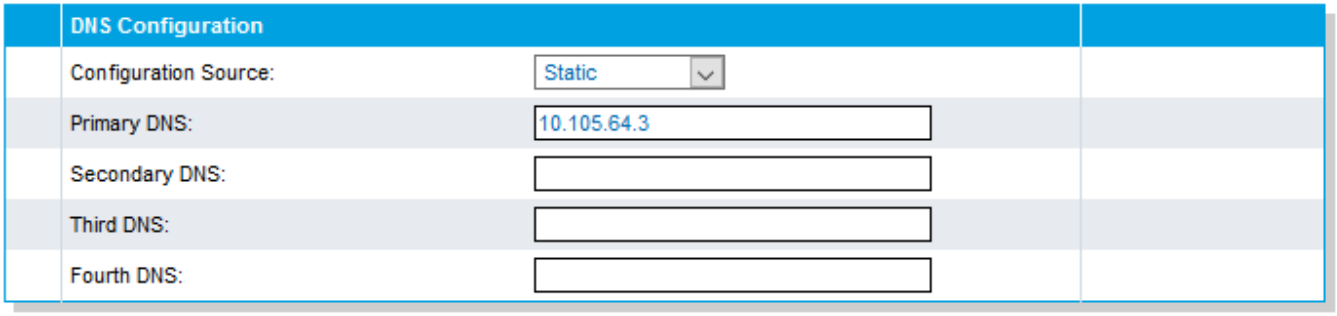
2. Change to **Static IP-address** and enter default Gateway (GW).

Figure 6.7: Changing static IP address



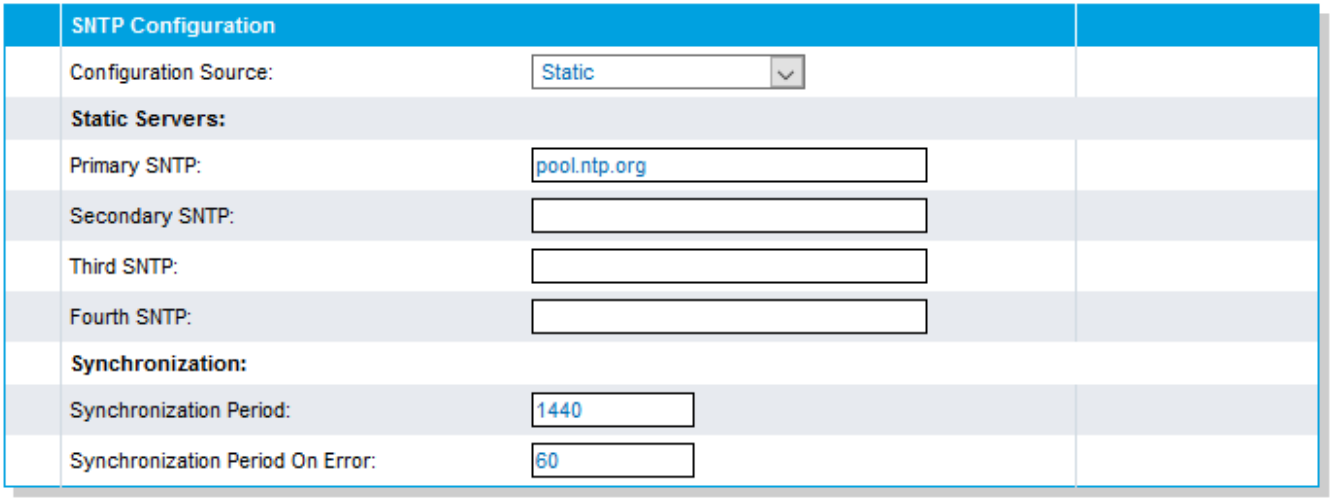
3. Change to static DNS server and enter IP-address or FQDN to DNS server.

Figure 6.8: Changing static DNS server



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

Figure 6.9: Changing to static SNTP server



5. Set the **Static Time Zone**.

Valid options are:

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

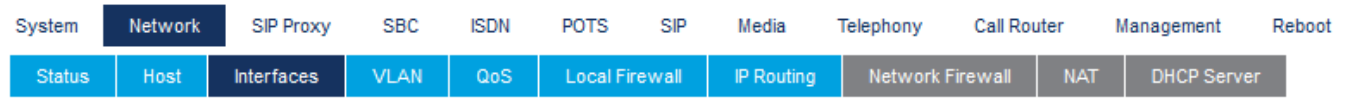
Figure 6.10: Setting static time zone

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

Interfaces

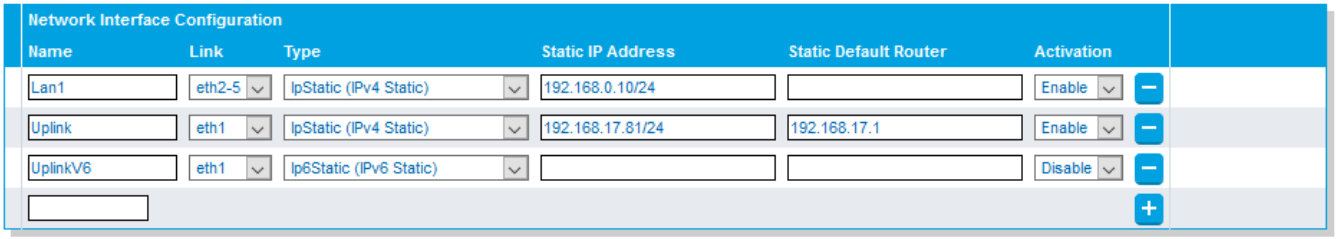
1. Go to **Network** > **Interface**.

Figure 6.11: Interface



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

Figure 6.12: Changing Uplink to IpStatic



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

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

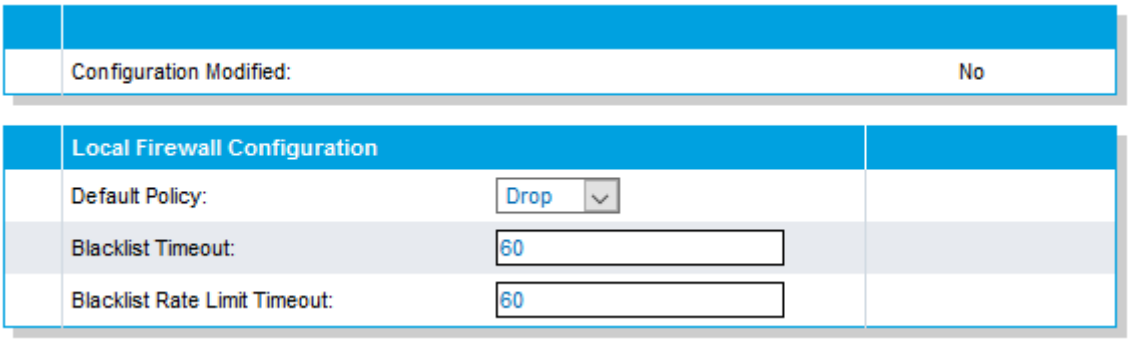
Local Firewalls

1. Go to **Network** > **Local Firewall**.

Figure 6.13: Local firewalls

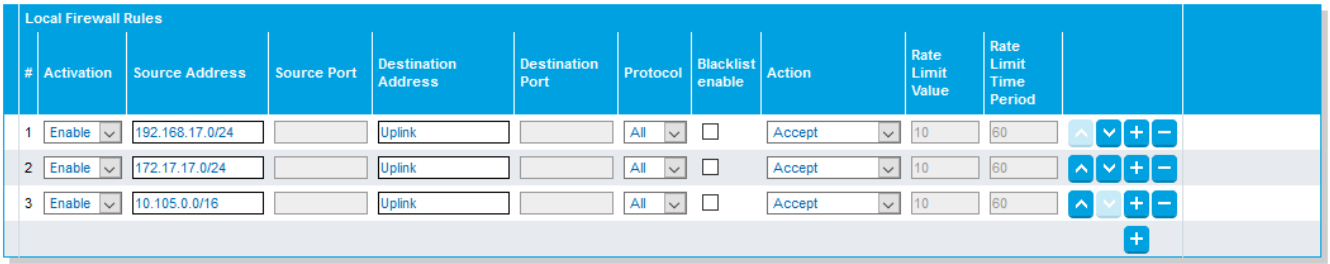
2. If local firewall security is needed change default policy to **Drop**.

Figure 6.14: Changing default policy



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

Figure 6.15: Enter network traffic



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

Session Board Controller (SBC)

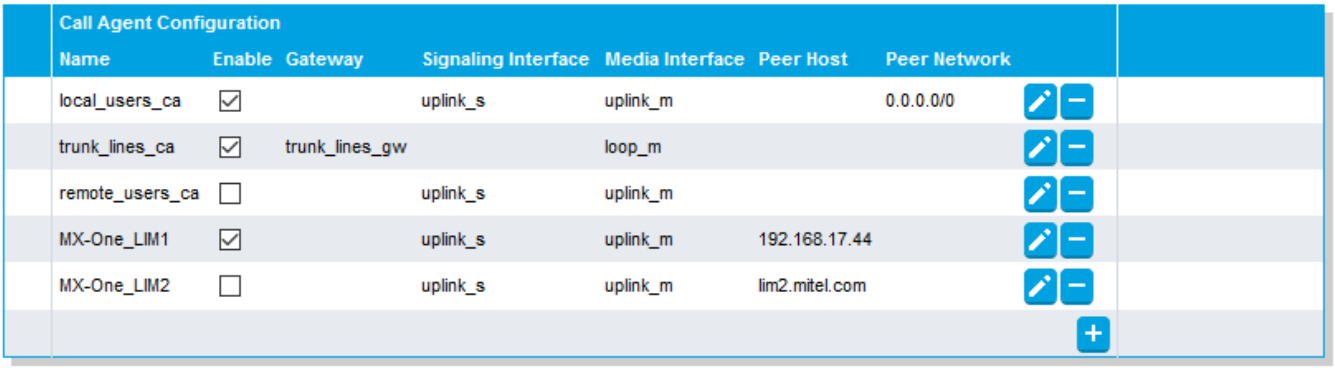
Configuration

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

Figure 6.16: Call agent - 1

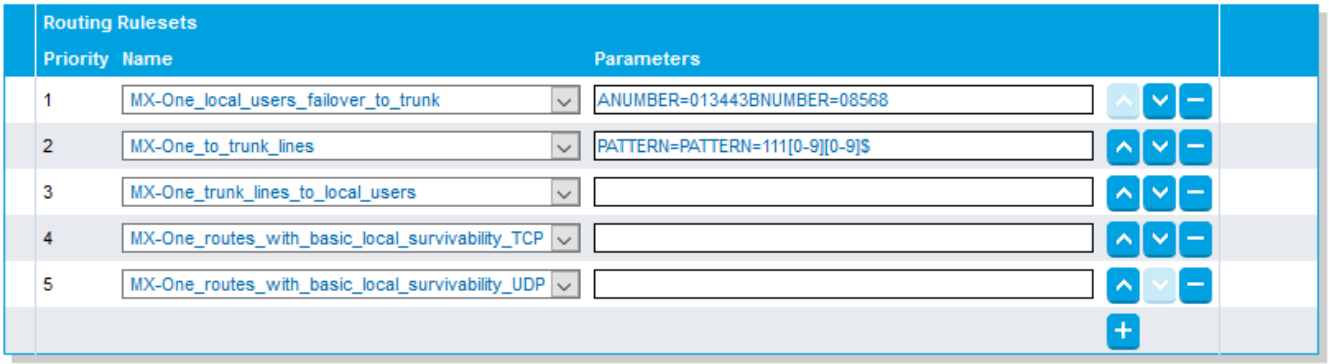
Figure 6.17: Call agent - 2

Figure 6.18: Call agent - 3



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

Figure 6.19: Parameters screen



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

Local_users_ca

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

Figure 6.20: Configure Call Agent screen

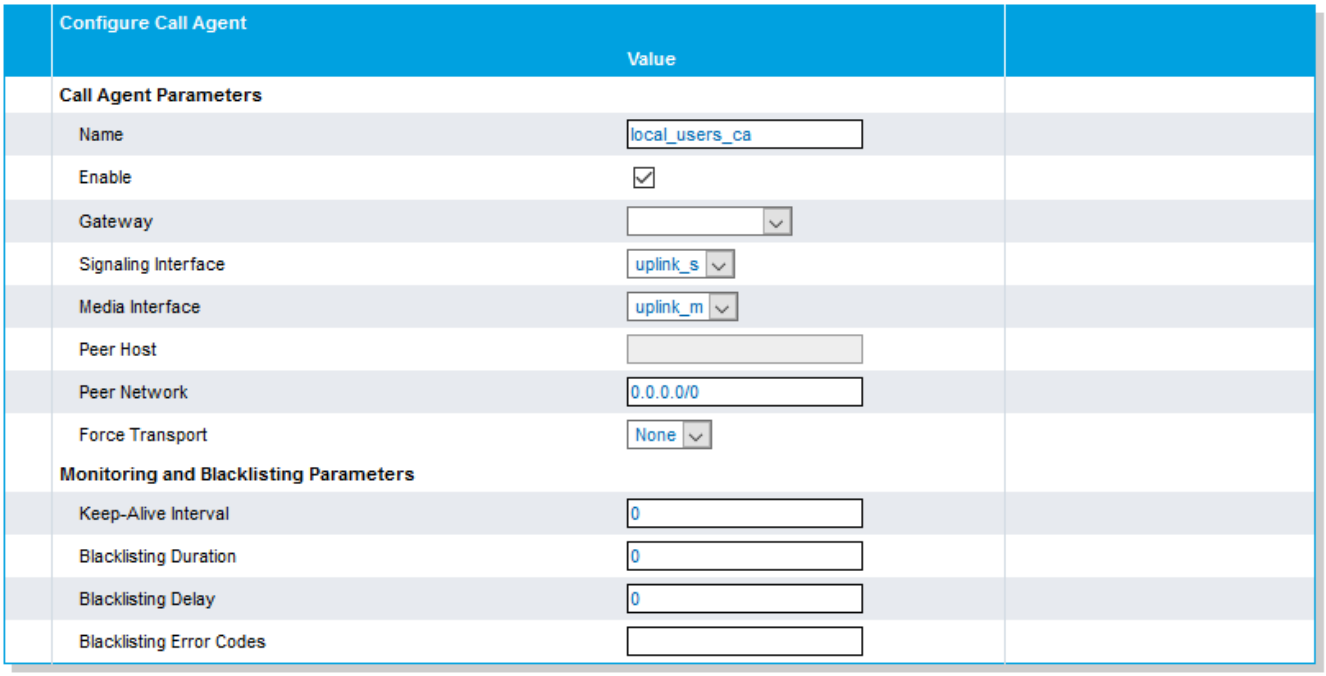
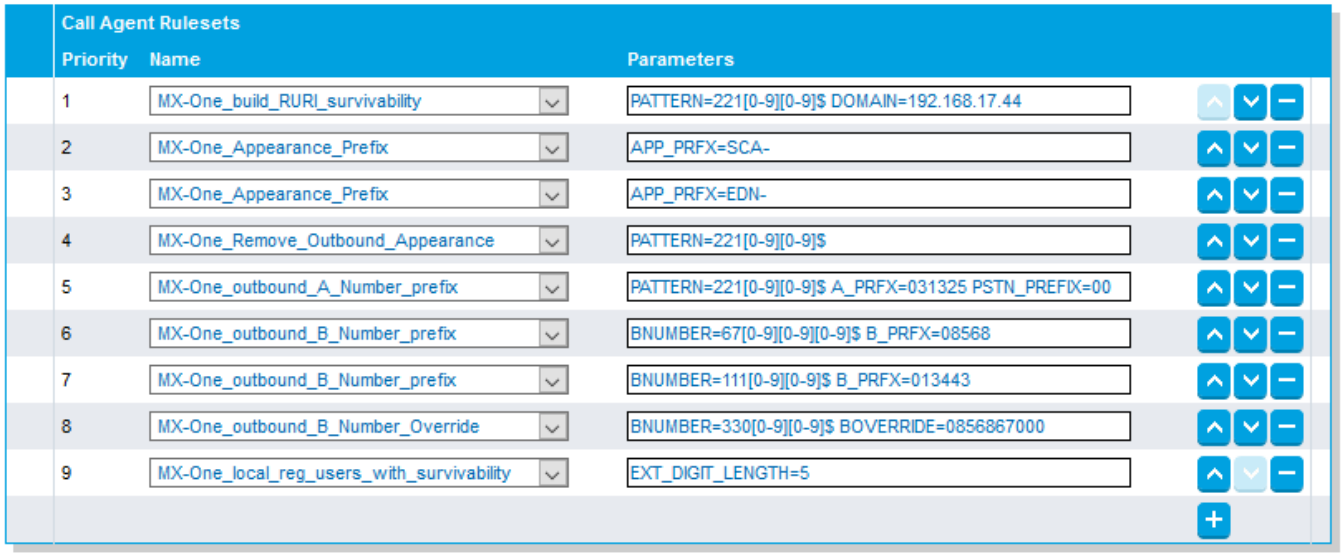


Figure 6.21: Call Agent Rulesets screen



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

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

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

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

DOMAIN=192.168.17.44

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

Ruleset: MX_ONE_Appearance_Prefix (ACTIVE ONLY IN SURVIVAL MODE)

NEW: APP_PREFIX=SCA-

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

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

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

This rule will remove any prefix used for Shared Call Appearance. The pattern for the internal range of numbers, in this example the internal range would be 11100 – 11199

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

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

This defines the local numbers.

A_PRFX=013443

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

PSTN_PREFIX=00

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

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

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

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

Applies to calls to the specific range of extensions,

B_PRFX=08568

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

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

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

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

Applies to calls to the specific range

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE, in this example they will be sent to 0856867000

Ruleset: MX-ONE_local_reg_users_with_survivability

(Builds the registration cache for survivability purpose)

EXT_DIGIT_LENGTH=5

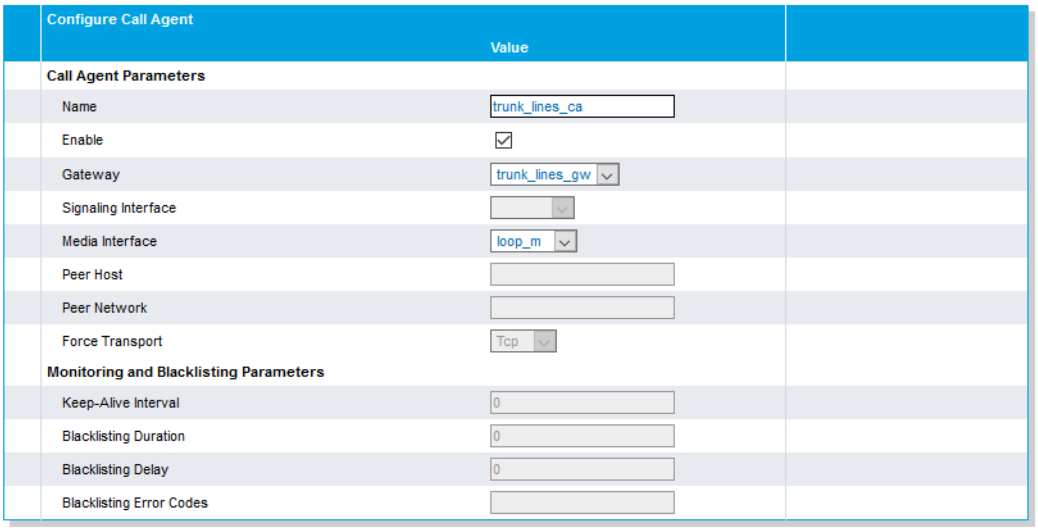
The length of the internal numbers, in this case set to “5”, for numbers like “00001 – 99999”

1. Click **Save** when done.

Trunk _ Lines _ca

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

Figure 6.22: Trunk_Lines_ca



Ruleset: MX-One_remove_prefix

PSTN_PREFIX=00

This is the prefix used to dial out to the PSTN

Ruleset: MX-One_trunk_lines_to_reception_survivability

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

MAIN_EXT=11104

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

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

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

DOMAIN=192.168.17.44

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

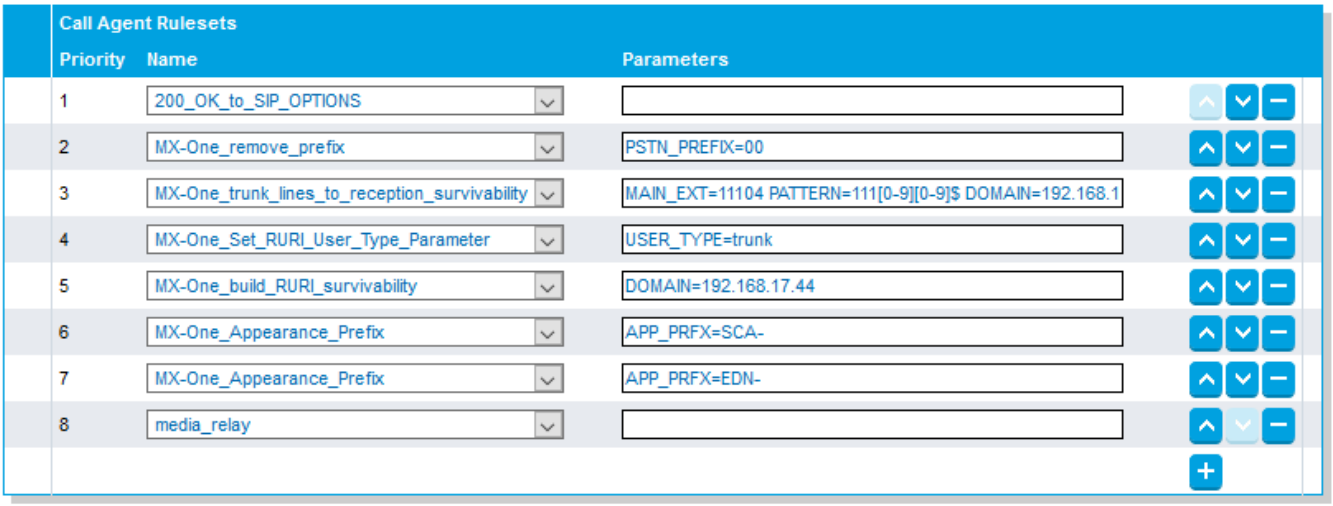
Ruleset: MX-One_Set_RURI_User_Type_Parameter

Set RURI User Type Parameter

USER_TYPE=trunk

a. Click Save when done.

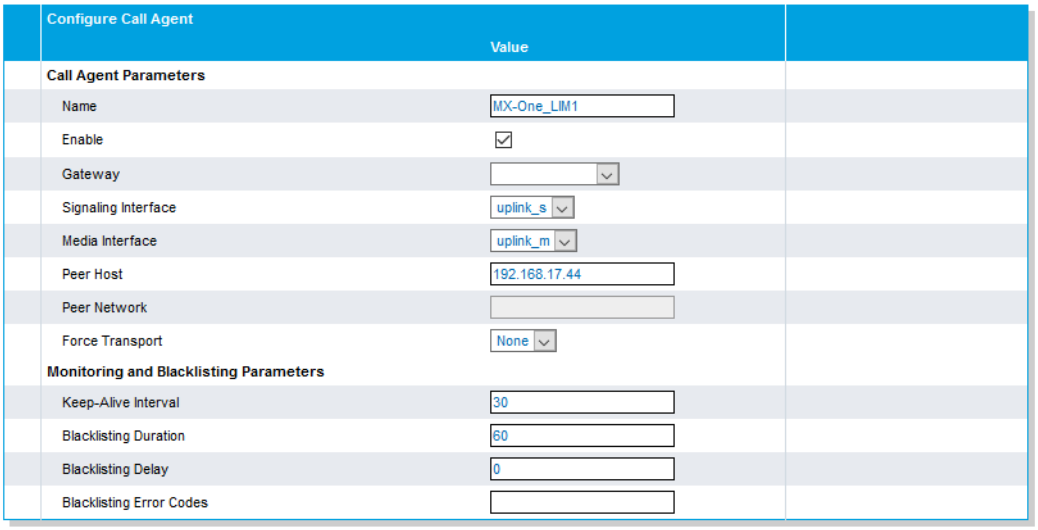
Figure 6.23: Trunk_Lines_ca Parameters



MX-ONE LIM1

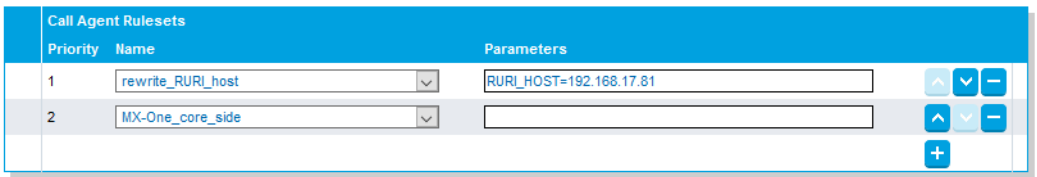
1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 6.24: Peer Host field



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

Figure 6.25: RURI_HOST Parameter



Ruleset: rewrite_RURI_host

Customize RURI host

RURI_HOST= 192.168.17.81. This is the local IP address.

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

MX-ONE Trunk

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

Figure 6.26: MX-ONE Trunk

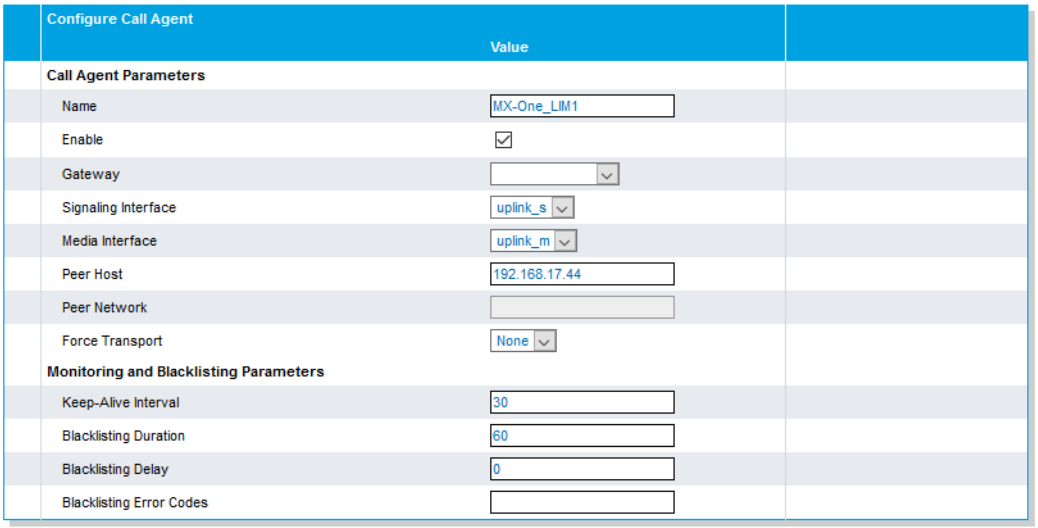
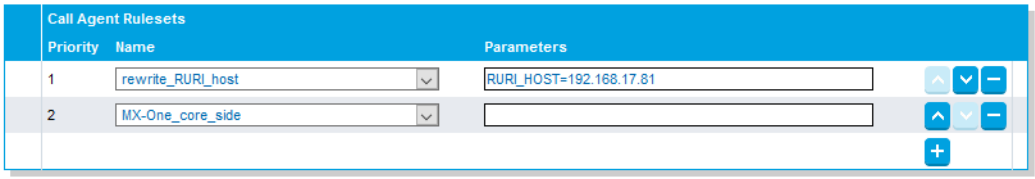


Figure 6.27: MX-ONE_TRUNK Parameters



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

Figure 6.28: Configuration Modified

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

ISDN

Figure 6.29: ISDN tab

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

Primary Rate Interface

Figure 6.30: Primary Rate Interface

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

Figure 6.31: Interface Configuration

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

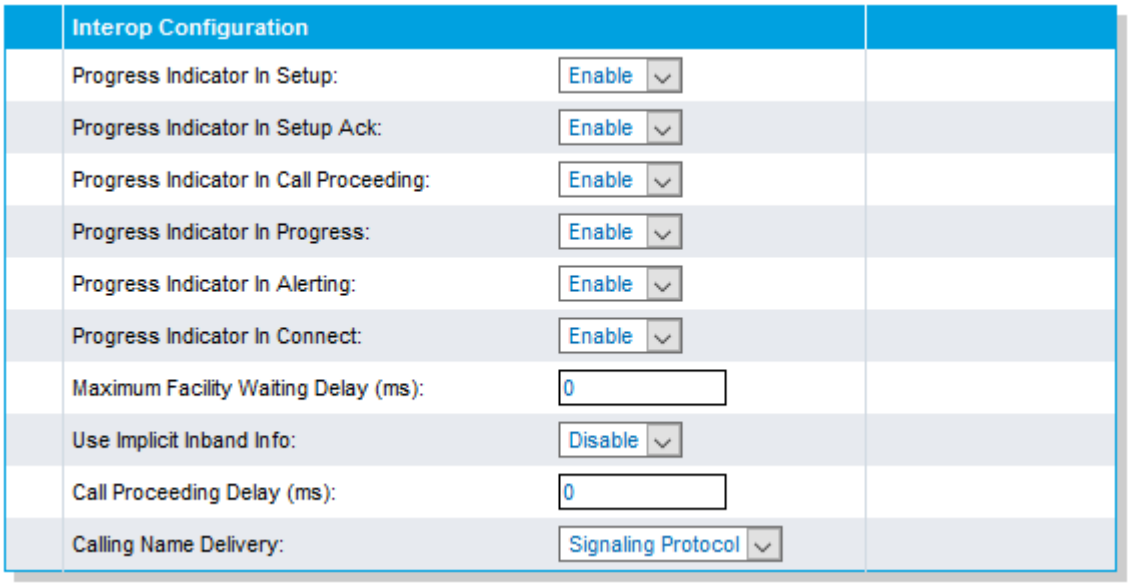
2. Click **Apply** and restart requested service when done.

Interop

Figure 6.32: Interop

1. You can change other parameters dependent on market.

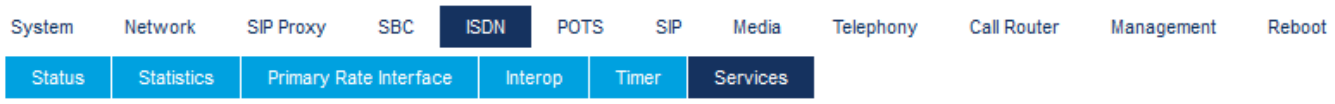
Figure 6.33: Interop Configuration screen



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

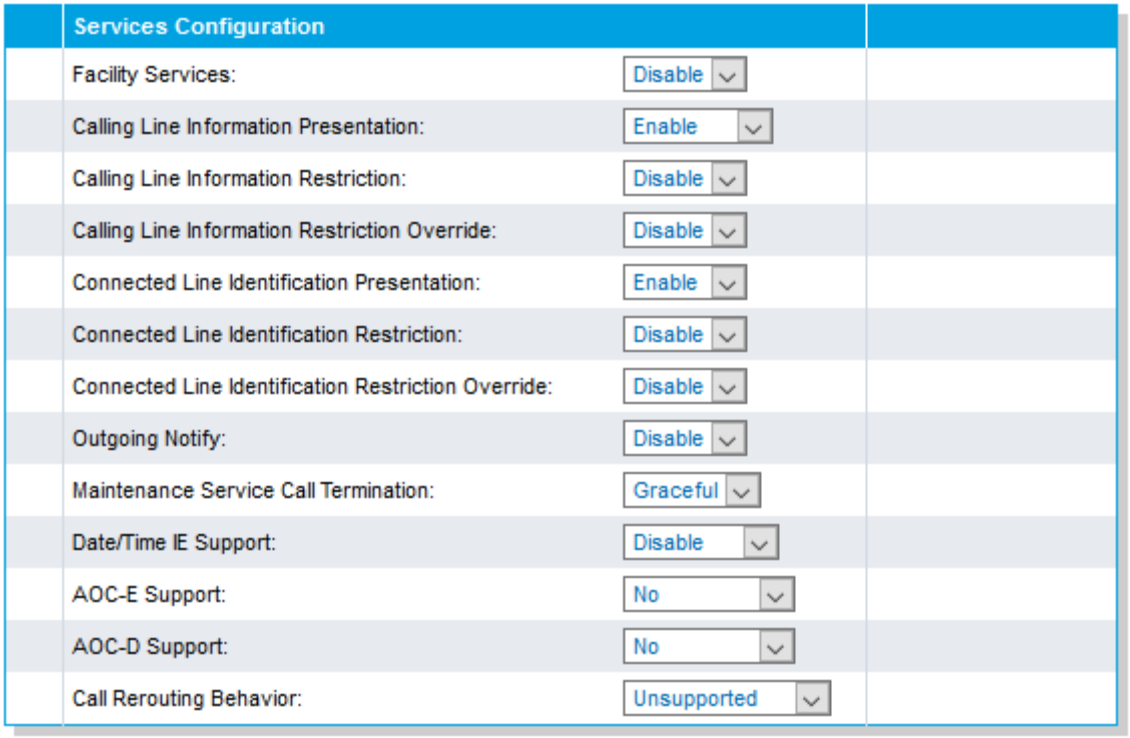
Services

Figure 6.34: Services



1. Change other parameters dependent on market.

Figure 6.35: Services Configuration screen



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

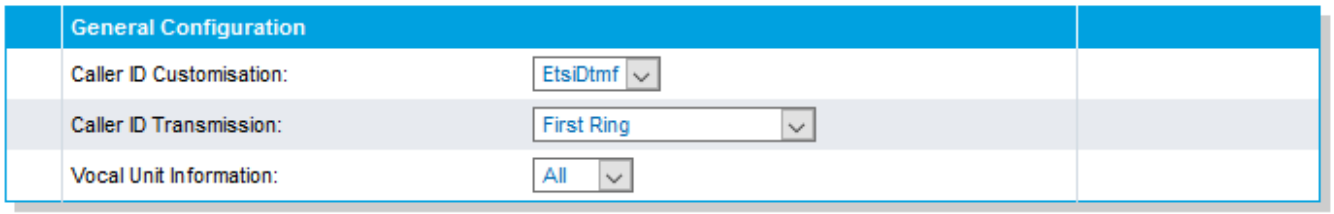
POTS

Config

Figure 6.36: Config

1. Set market specific data for Caller Id handling.

Figure 6.37: General Configuration screen



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

FXS Configuration

Figure 6.38: FXS Configuration

1. Set analog phone specific data according to market.

Figure 6.39: FXS Configuration screen

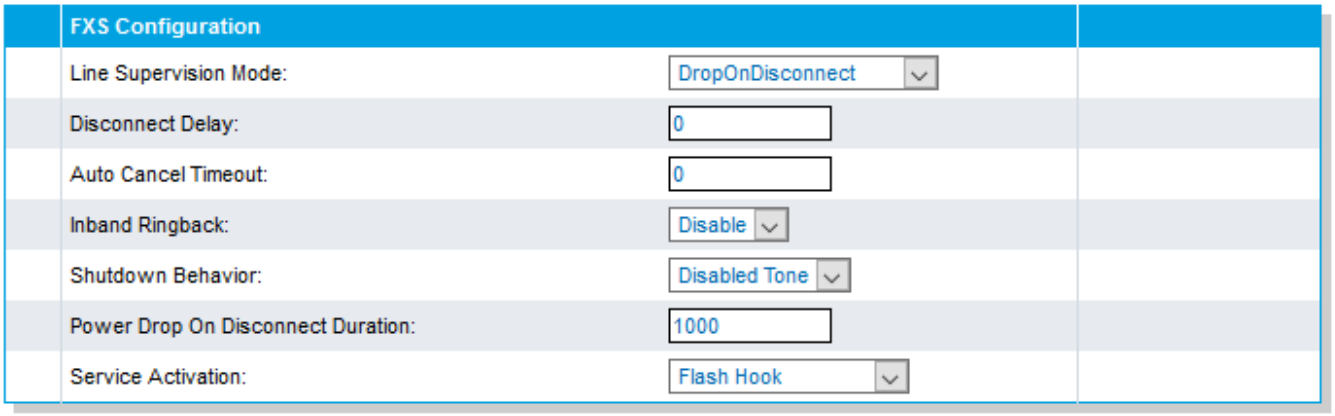
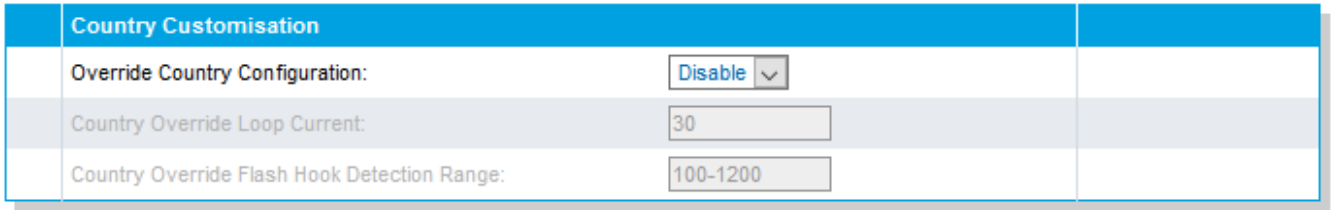


Figure 6.40: Country Customisation screen



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

SIP

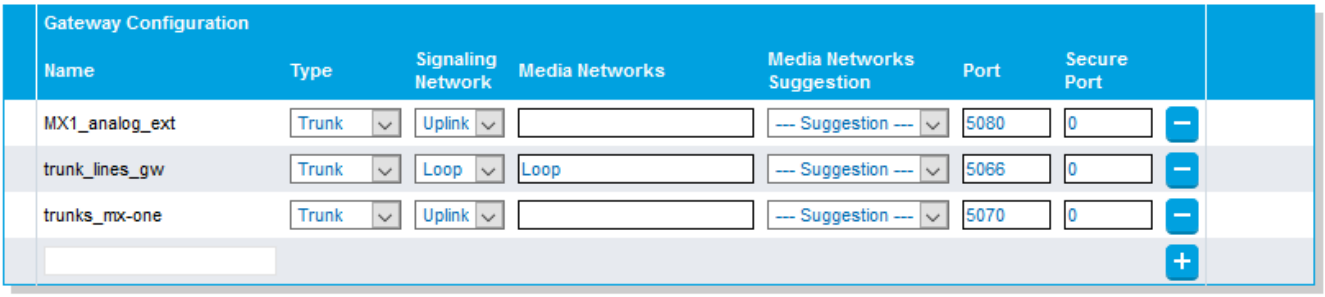
Gateways

Following gateways and port numbers are pre-defined.

Figure 6.41: Gateways

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

Figure 6.42: trunks_mx-one

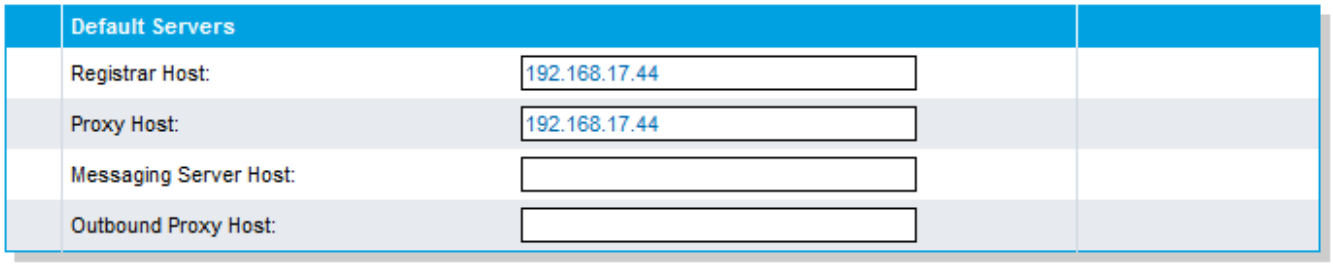


Servers

Figure 6.43: Servers

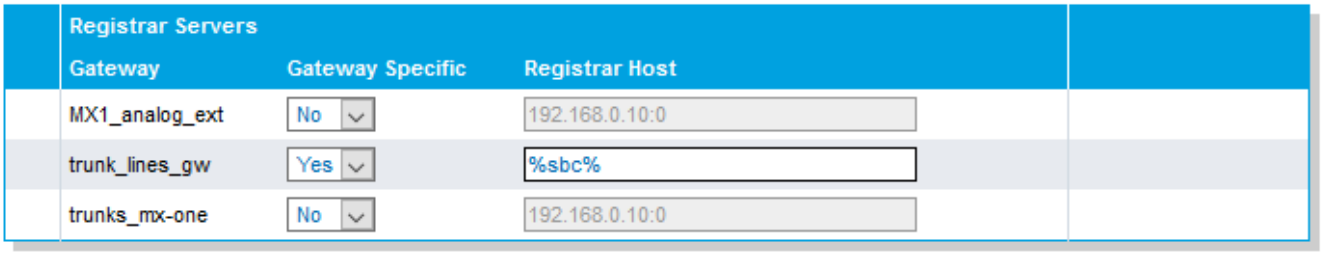
1. Enter IP-address to MX-ONE in both **Registrar Host** and **Proxy Host** fields.

Figure 6.44: Default Servers



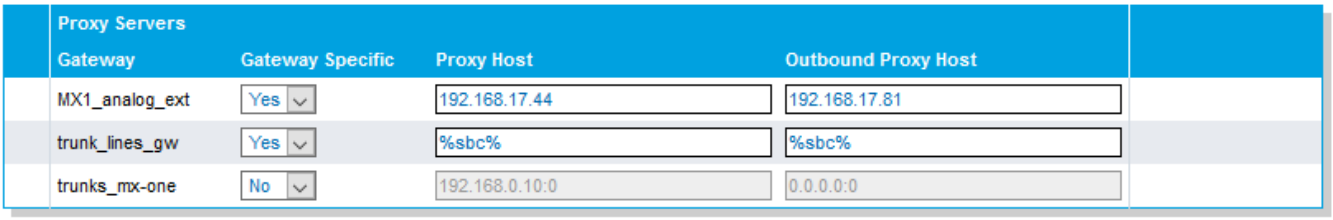
2. Change **trunk_lines_gw** to **Yes** in the drop-down list for **Gateway Specific**.

Figure 6.45: trunk_lines_gw



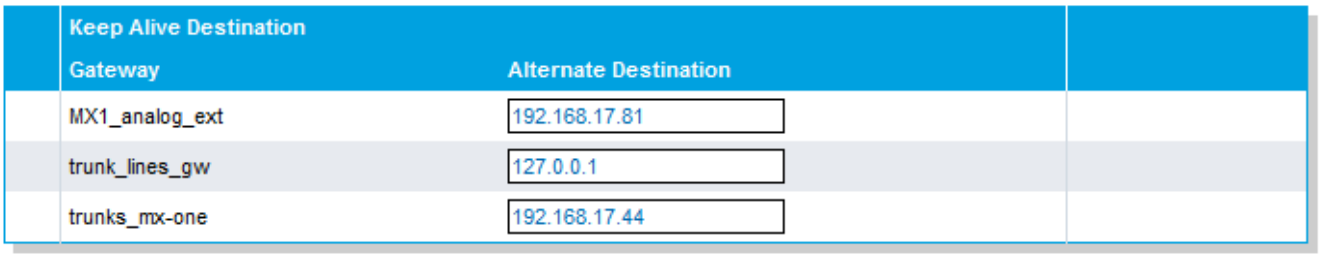
3. Enter IP-address of MX-ONE in the **Proxy Host** field.
4. Enter IP-address of the gateway in the **Outbound Proxy Host** field.

Figure 6.46: Outbound Proxy Host field



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

Figure 6.47: Alternate Destination for trunks_mx-one



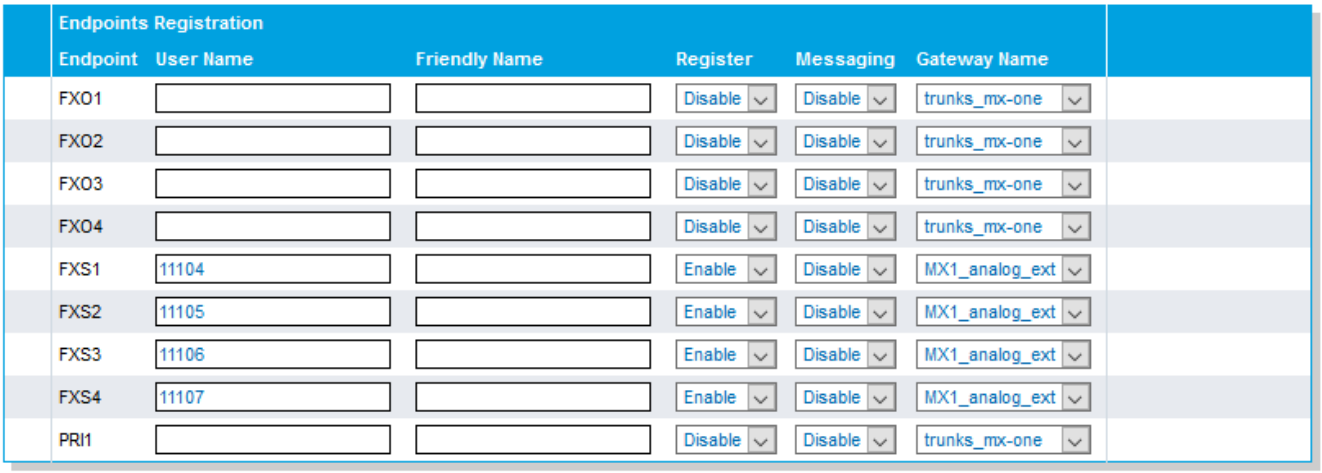
7. Click **Apply** when done and restart service.

Registrations

Figure 6.48: Registrations

1. Enter the extension numbers for the analog extensions.

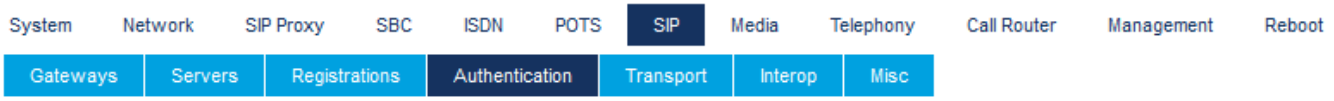
Figure 6.49: Endpoints Registration screen



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

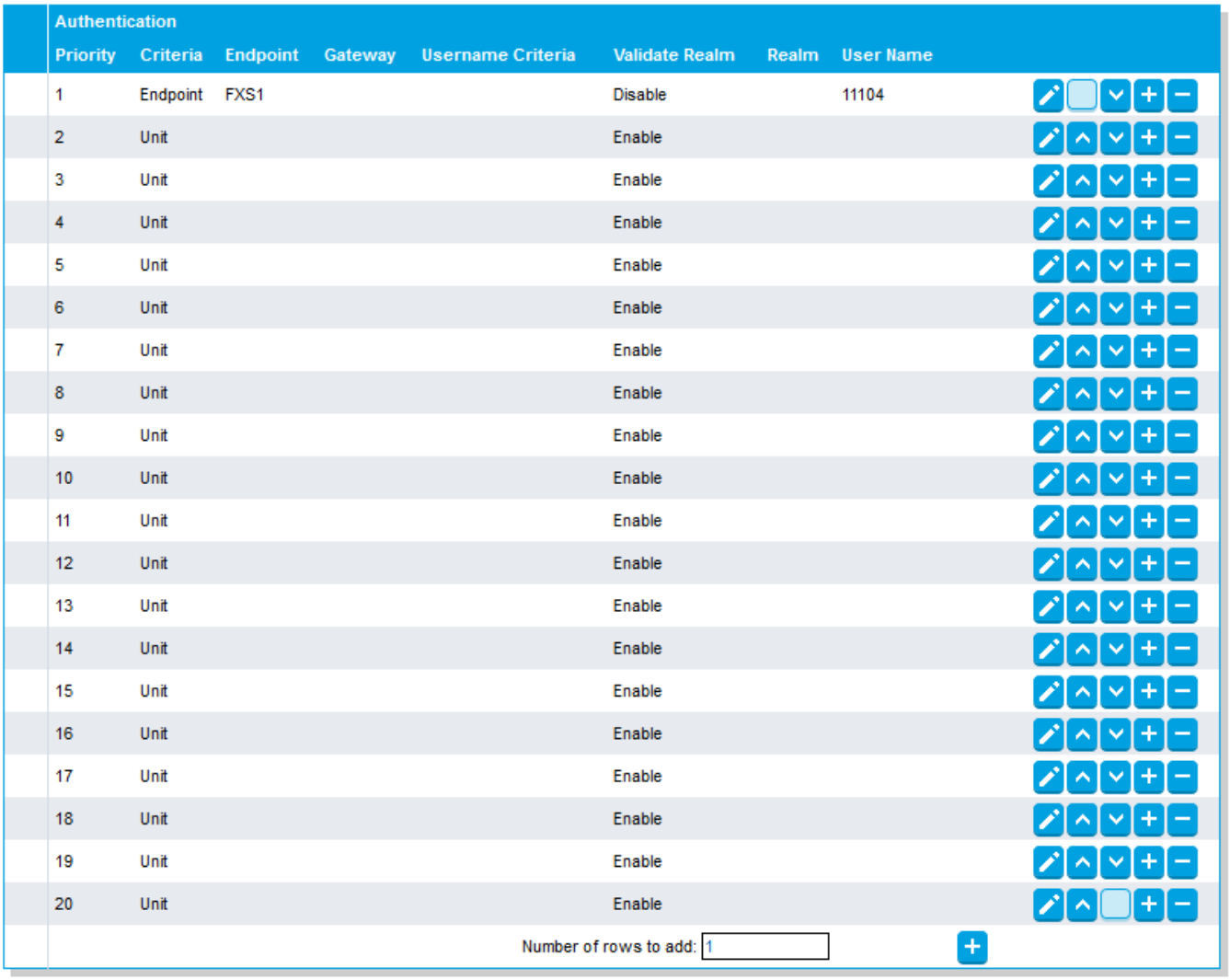
Authentication

Figure 6.50: Authentication



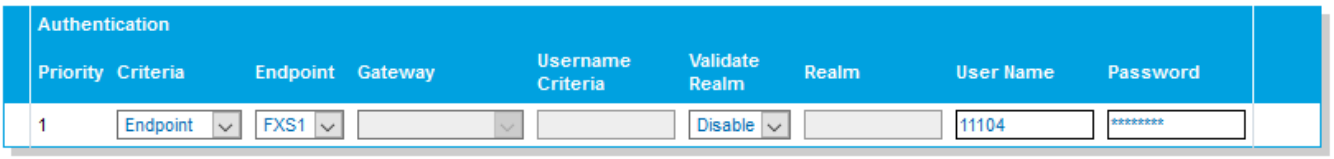
1. If password is required press for any item.

Figure 6.51: Authentication Screen



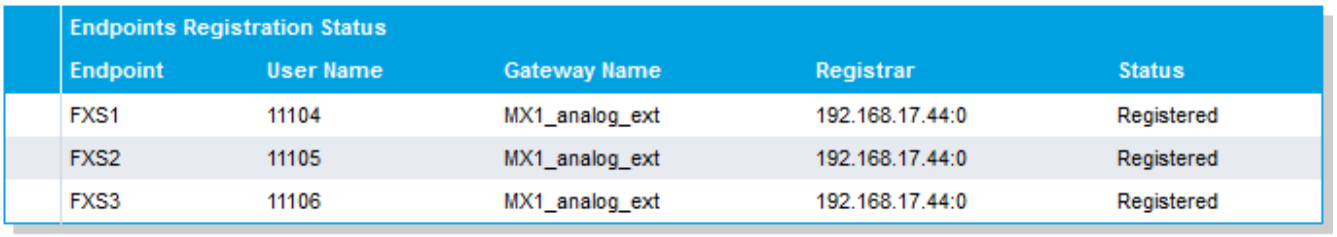
2. Indicate for which Endpoint and Criteria the changes are to apply.
3. Enter the Auth Code, in the **Password** field.
4. In the **Validate Realm** field, select **Disable**.

Figure 6.52: Validate Realm field



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

Figure 6.53: Endpoints Registration Status

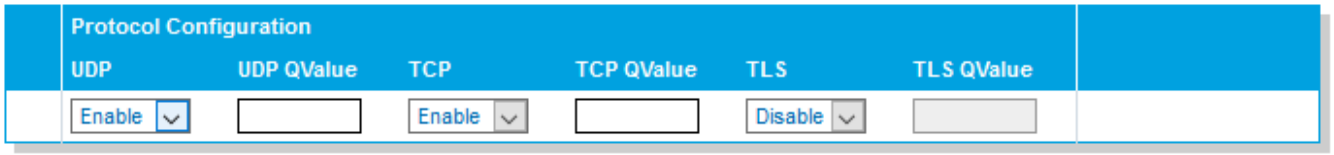


Transport

Figure 6.54: Transport

1. Enable UDP if required.

Figure 6.55: Protocol Configuration screen



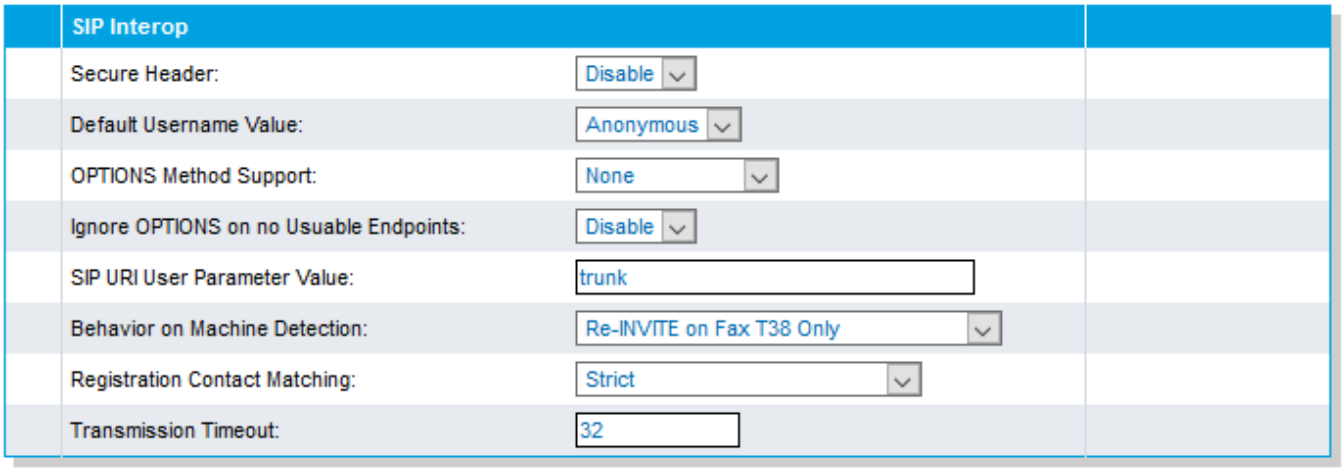
2. Click **Apply** when done and restart service.

Interop

Figure 6.56: Interop

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

Figure 6.57: SIP URI User Parameter Value field



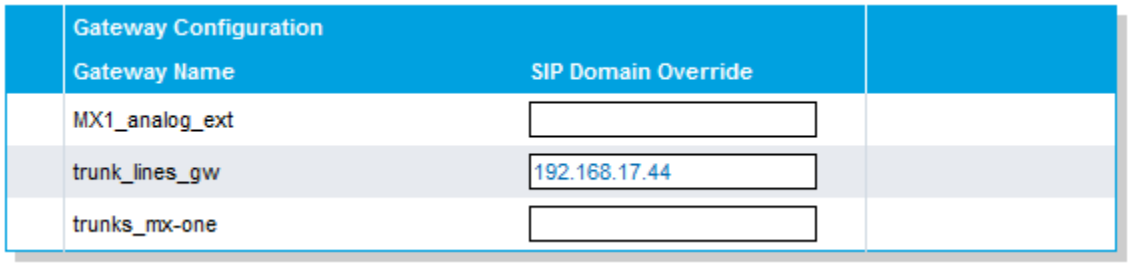
3. Click **Apply** or when done and restart service.

Misc

Figure 6.58: Misc

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

Figure 6.59: Gateway Configuration field



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

Media

Codecs

Figure 6.60: Codecs

1. Change Codecs according to preference.

Figure 6.61: Changing Codecs

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

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

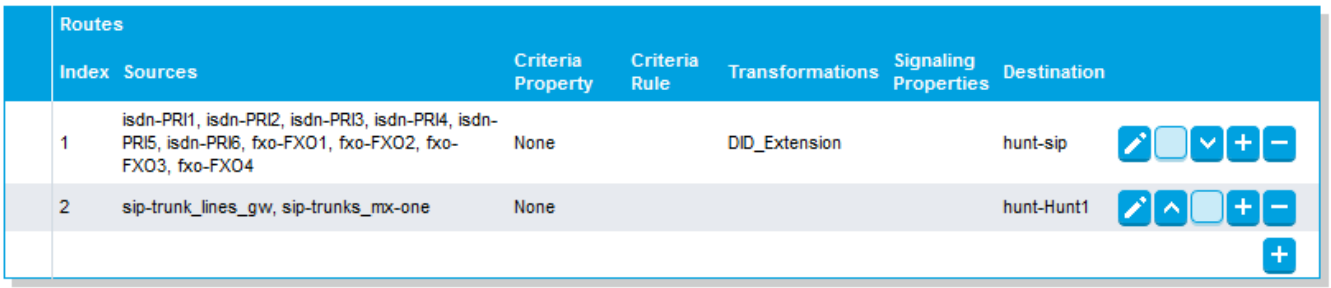
Call Router

Route Config

Figure 6.62: Route Config

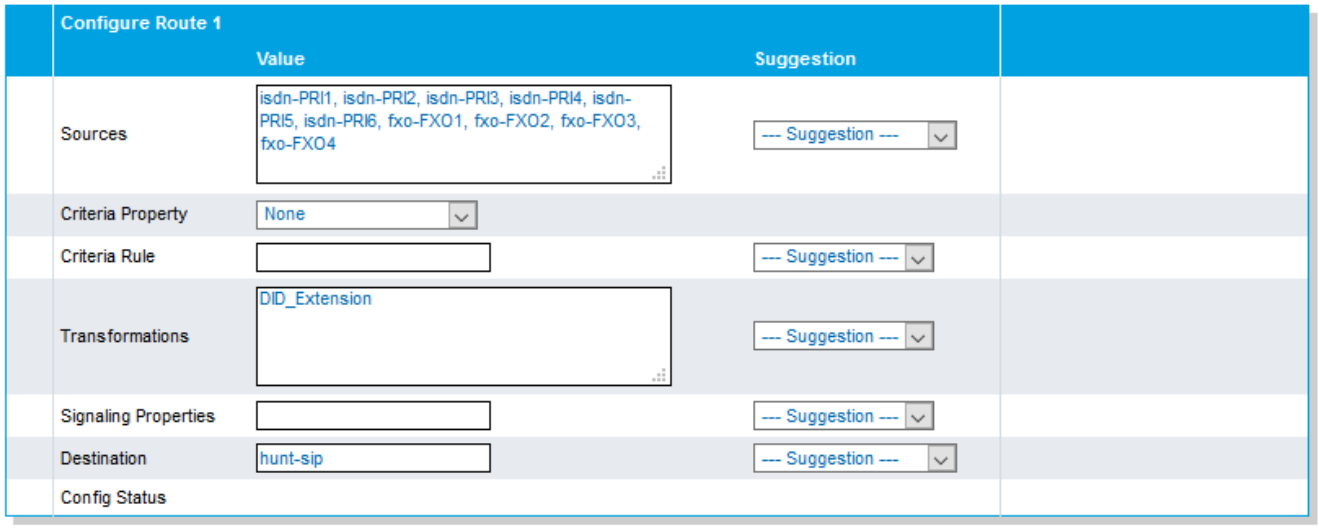
1. Click for index 1. This is used if the received B-number contains a full number. That is, more digits than the pure DID numbers.

Figure 6.63: Routes screen



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

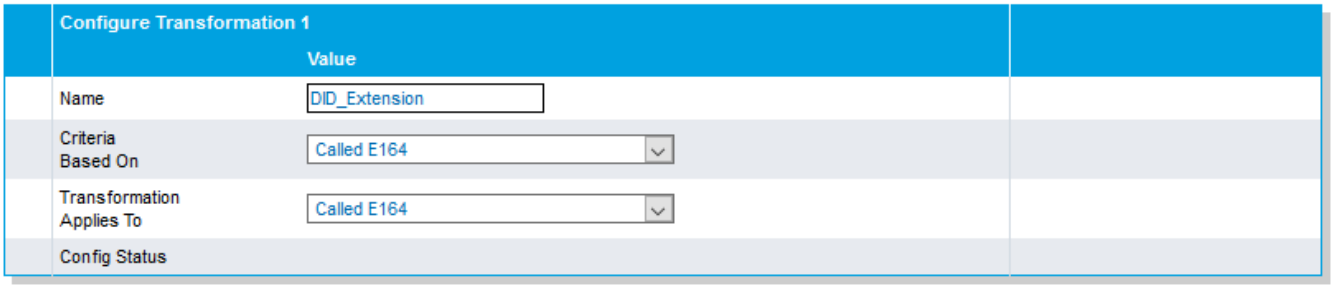
Figure 6.64: Transformations field



3. Click **Save**.
4. Click in the first Call Property Transformation and enter the same name as above.

5. Use **Called E164** for both **Criteria Based On** and **Transformation Applies To** fields.

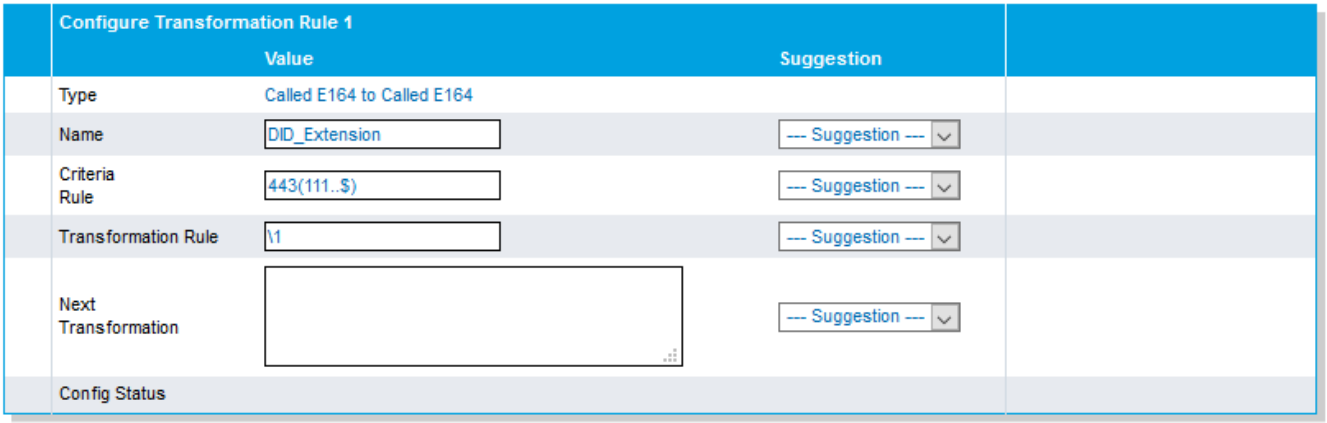
Figure 6.65: Configure Transformation 1 Screen



6. Click **Save** or **Save and Insert Rule**.
7. Click in the second Call Property Transformation and enter the same name as above.

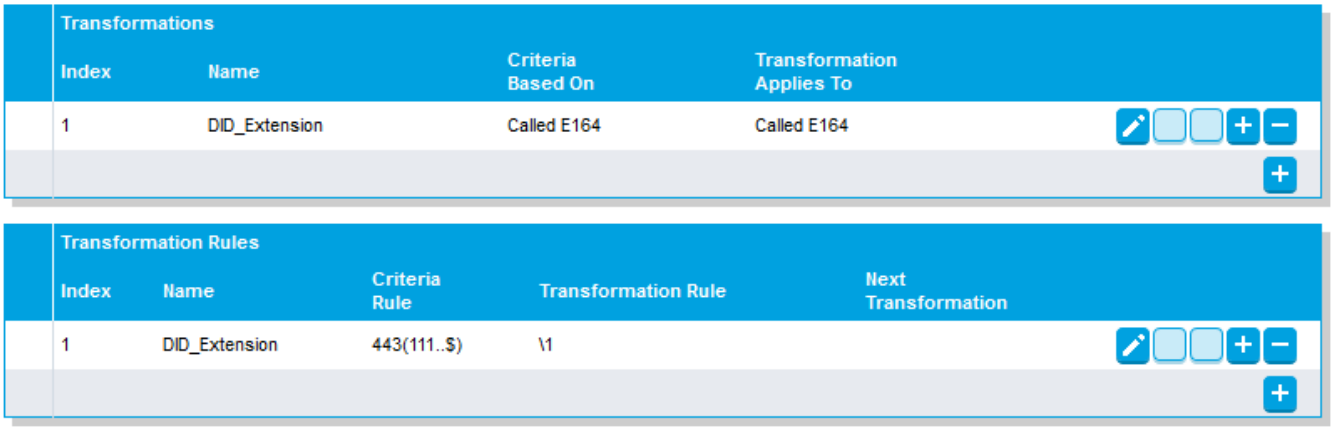
8. The 'Criteria Rule' in this case is 443 (111..)$ and the transformation rule is '\1. This means that if a B-number is received containing 44311104, then the 3 first digits (443) are removed before the call is sent to MX-ONE for further processing. (111..)$ means that the number can only be 5 digits starting with 111.

Figure 6.66: Configure Transformation Rule 1 screen



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

Figure 6.67: Transformations screen



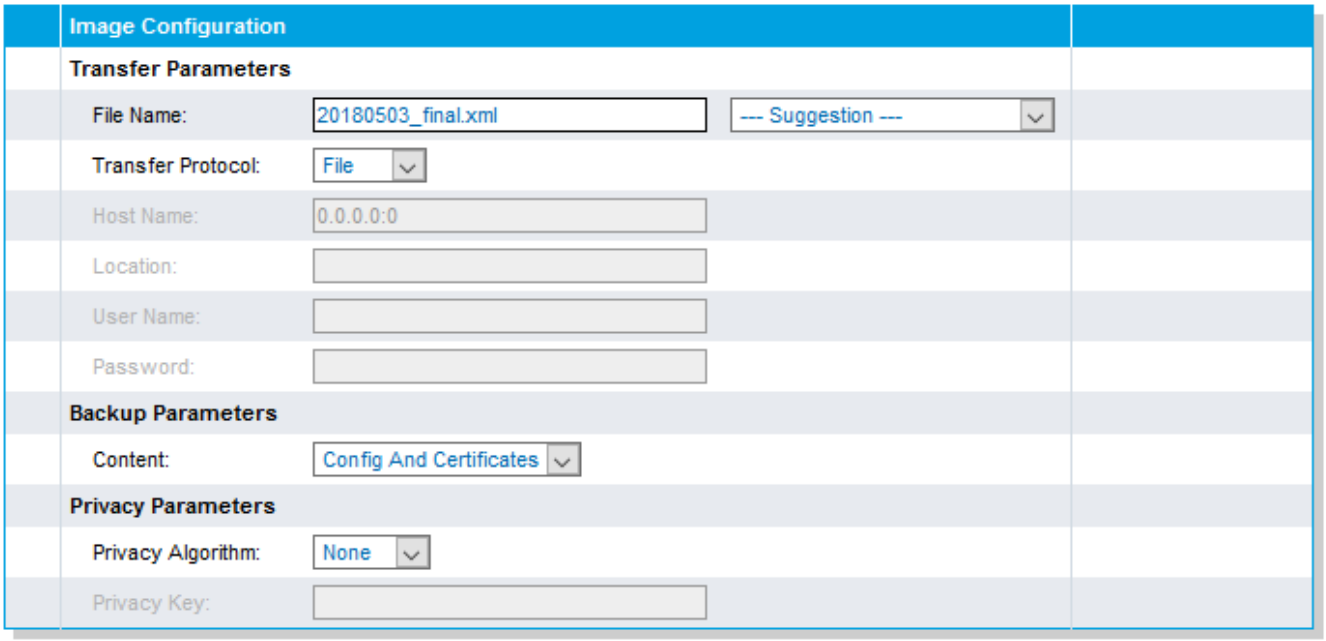
10. Click **Save** if the yellow indication on top of the page is ON.

Management

Backup/Restore

1. Click **Activate .....**

Figure 6.68: Image Configuration screen



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

File

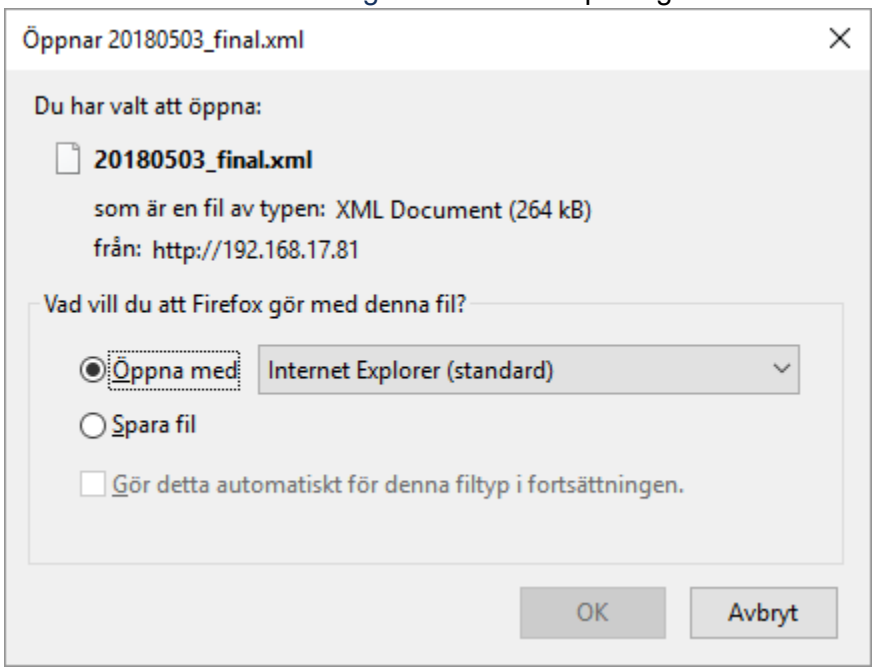
Figure 6.69: Internal files screen

Internal files

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

Find the previously made backup image

Figure 6.70: Backup image



Setting up MX-ONE for an EX Controller

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

Setting up EX Controller

Logon

This section describes how to setup BO#1.

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

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

Figure 6.71: Logon screen

This section describes how to setup BO#1.

1. Factory Reset the EX Controller and plug in the network cable to the ETH1 port on EX Controller (If DHCP is running in the network).
   – User name/password: public /
   – User name/password: admin/administrator
2. Plug in the analog phone in the FXS port 1 of the EX Controller and dial *#*0 to know the IP address of the EX Controller assigned by using DHCP server.
3. Log into the EX Controller by using the above-mentioned IP address and navigate as described below to configure.

Network Settings

Host

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

Figure 6.72: Host screen

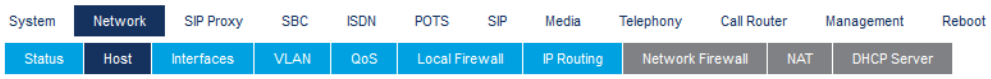
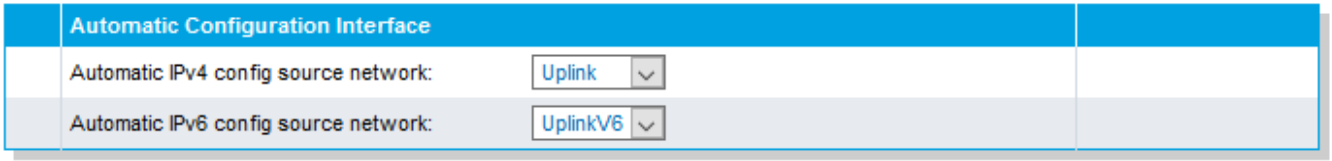
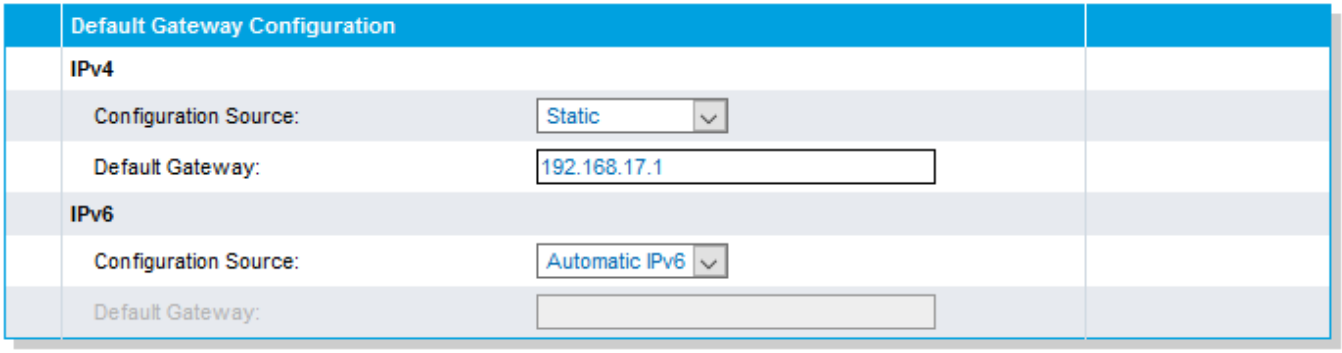


Figure 6.73: Automatic Configuration Interface



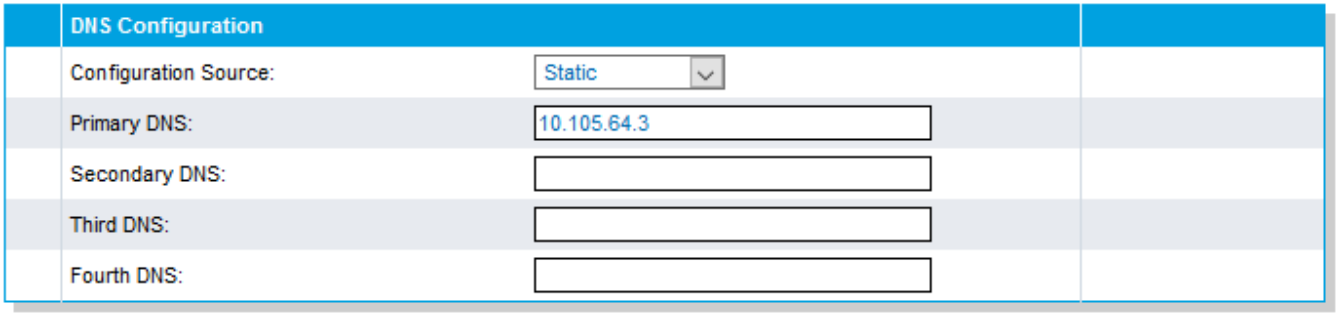
2. Change to Static IP-address and enter default Gateway (GW).

Figure 6.74: Default Gateway Configuration



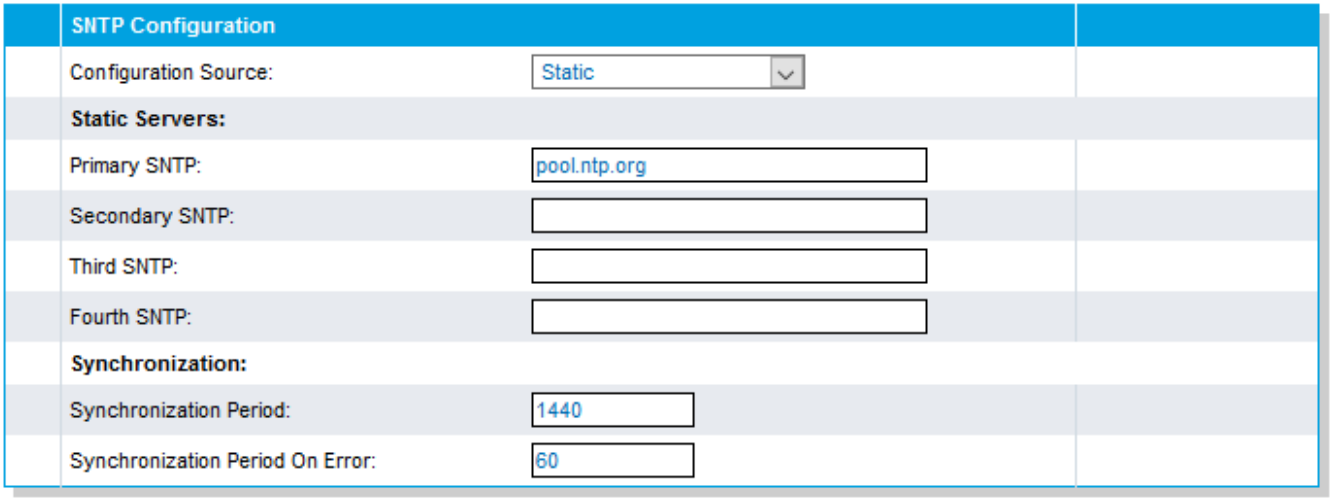
3. Change to static DNS server and enter IP-address or FQDN to DNS server.

Figure 6.75: DNS Configuration screen



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

Figure 6.76: SNTP Configuration



5. Set the Static Time Zone. Valid options are:

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

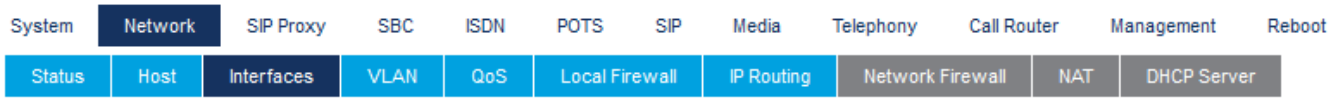
Figure 6.77: Time Configuration screen

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

Interfaces

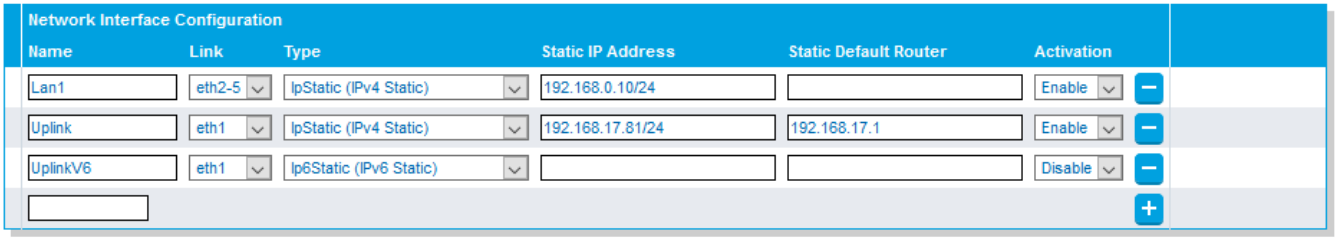
1. Go to **Network** > **Interface**.

Figure 6.78: Interfaces screen



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

Figure 6.79: Network Interface Configuration

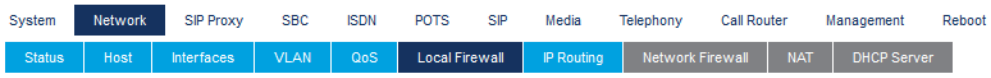


3. Leave all other items as it is and click **Apply** when ready.

Local Firewalls

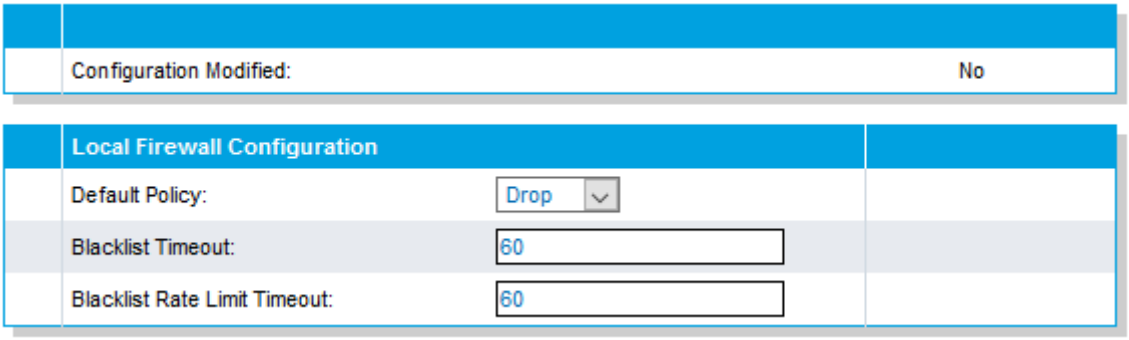
1. Go to **Network** > **Local Firewall**.

Figure 6.80: Local Firewall screen



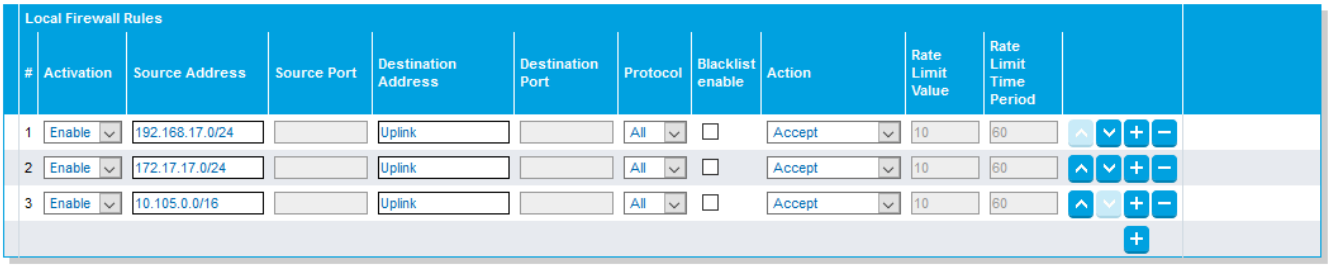
2. If local firewall security is needed, change default policy to **Drop**.

Figure 6.81: Local Firewall Configuration screen



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

Figure 6.82: Local Firewall Rules screen



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

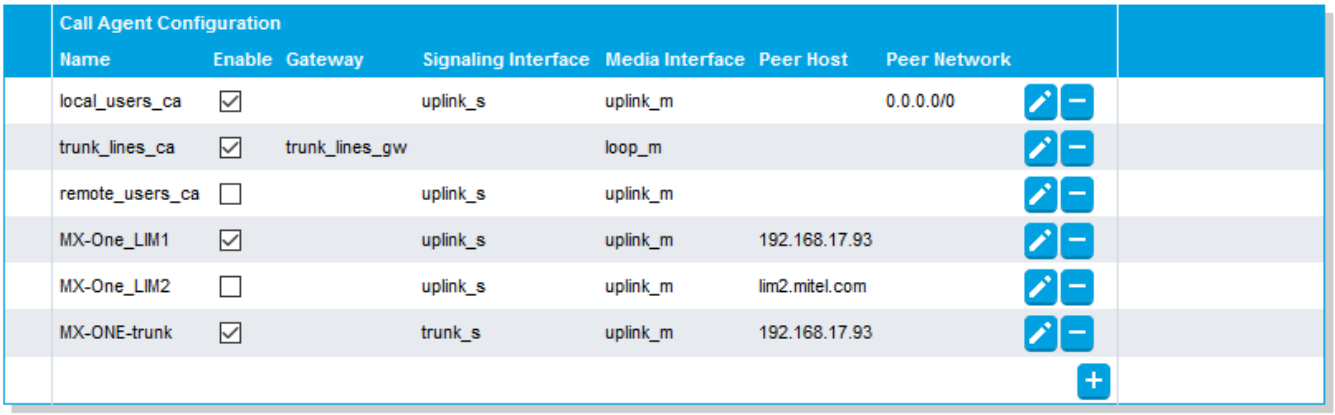
SBC

Configuration

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

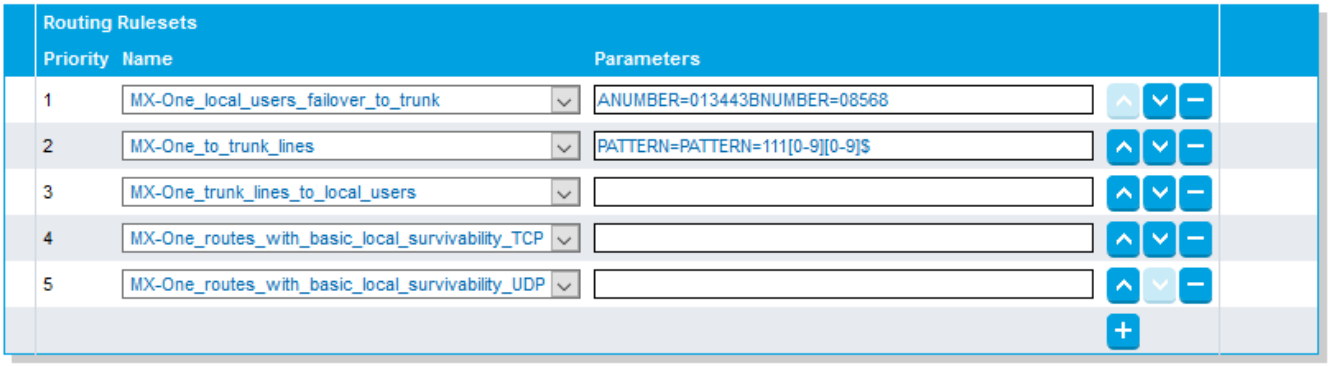
Figure 6.83: SBC Configuration screen

Figure 6.84: Call Agent Configuration screen



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

Figure 6.85: Routing Rulesets screen



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

Local_users_ca

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

Figure 6.86: Configure Call Agent screen

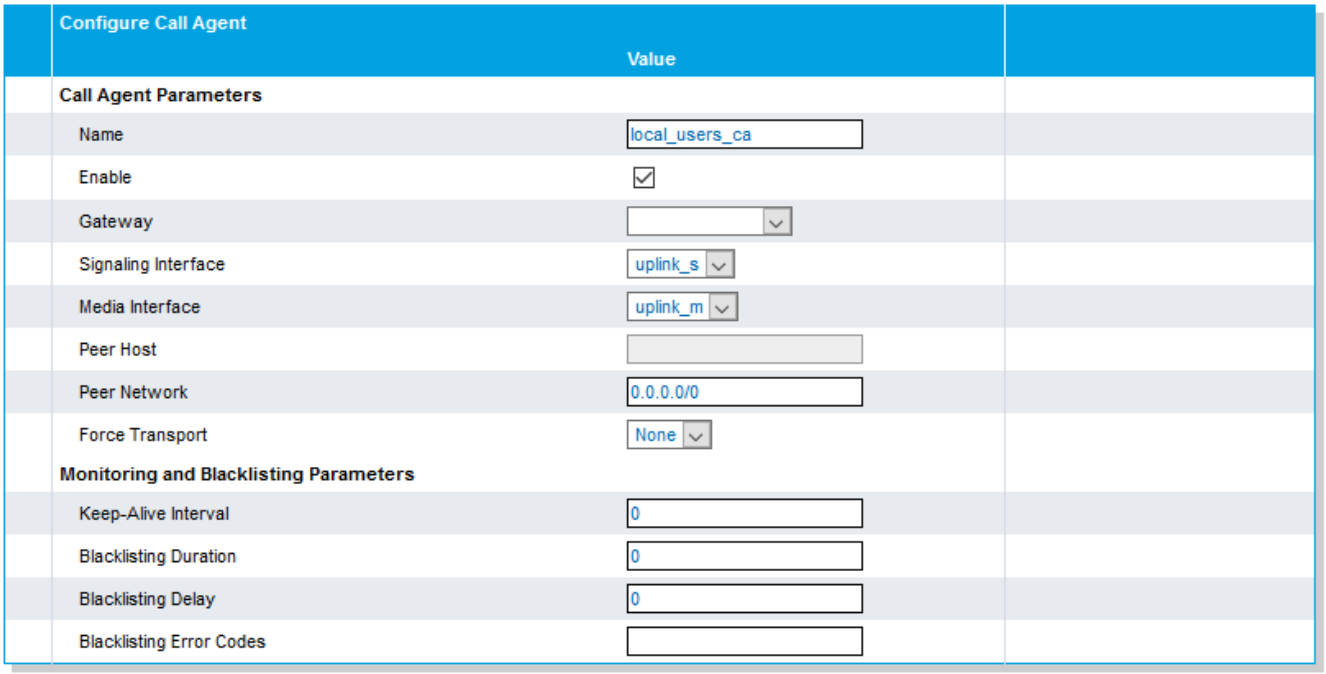
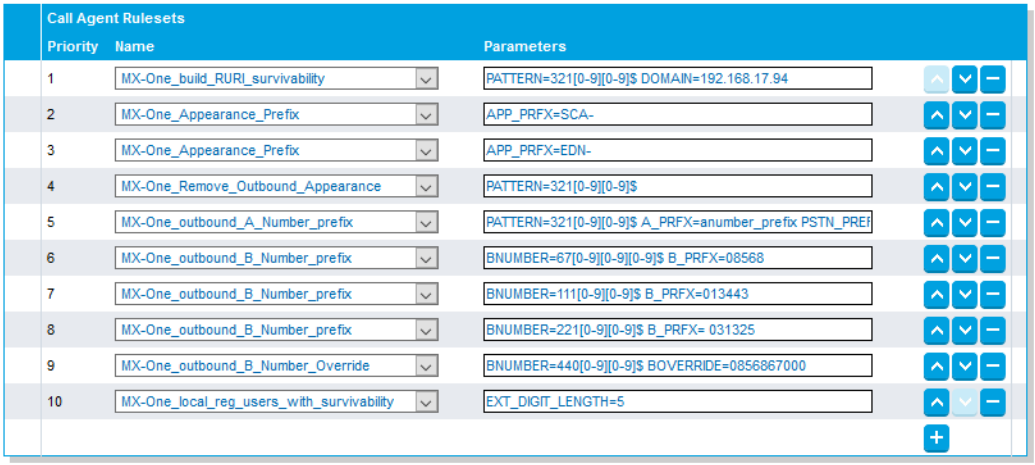


Figure 6.87: Call Agent Rulesets



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

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

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

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

DOMAIN=192.168.17.94

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

Ruleset: MX_One_Appearance_Prefix (ACTIVE ONLY IN SURVIVAL MODE)

NEW: APP_PREFIX=SCA-

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

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

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

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

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

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

This defines the local numbers.

A_PRFX=040598

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

PSTN_PREFIX=00

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

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

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

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

Applies to calls to the specific range of extensions,

B_PRFX=08568

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

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

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

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

Applies to calls to the specific range

BOVERRIDE=0856867000

Calls to extensions like BNUMBER will be sent to BOVERRIDE, in this example they will be sent to 0856867000

Ruleset: MX-One_local_reg_users_with_survivability

(Builds the registration cache for survivability purpose)

EXT_DIGIT_LENGTH=5

The length of the internal numbers, in this case set to "5", for numbers like "00001 – 99999"

1. Click **Save** when done.

Trunk_Lines_ca

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

Figure 6.88: Configure Call Agent screen

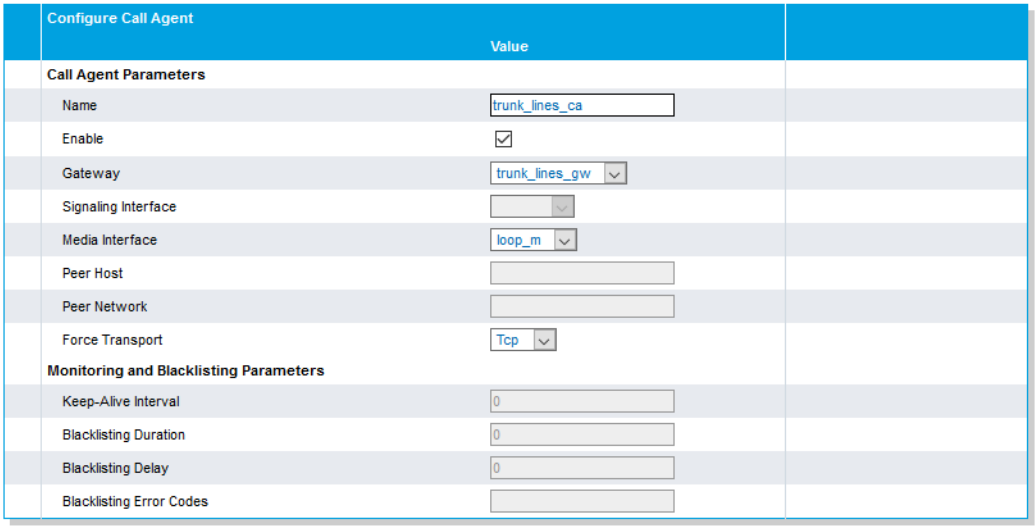
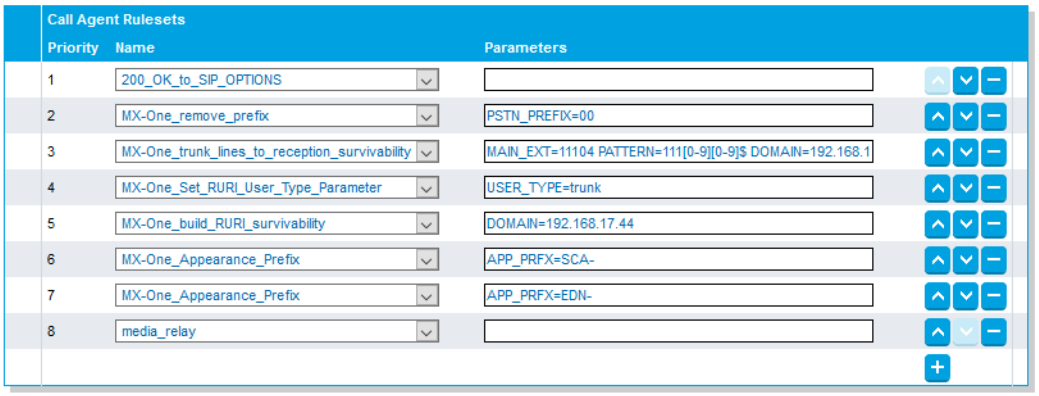


Figure 6.89: Call Agent Rulesets



Ruleset: MX-One_remove_prefix

PSTN_PREFIX=00

This is the prefix used to dial out to the PSTN

Ruleset: MX-One_trunk_lines_to_reception_survivability

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

MAIN_EXT=11104

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

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

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

DOMAIN=192.168.17.94

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

Ruleset: MX-One_Set_RURI_User_Type_Parameter

Set RURI User Type Parameter

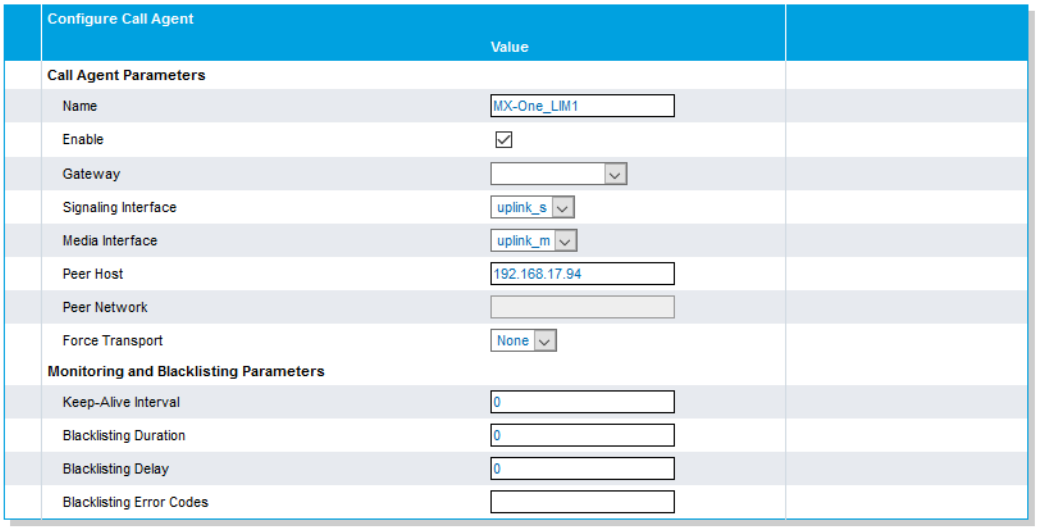
USER_TYPE=trunk

1. Click **Save** when done.

MX-ONE_Lim1

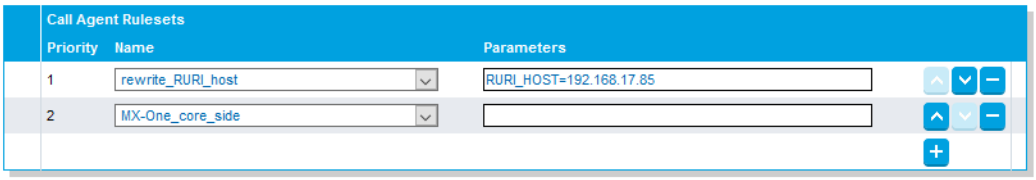
1. Enter the IP-address of the MX-ONE in the **Peer Host** field.

Figure 6.90: Peer Host field



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

Figure 6.91: RURI_HOST parameter



Ruleset: rewrite_RURI_host

Customize RURI host

RURI_HOST= 192.168.17.85. This is the local IP address.

1. Click **Save** when ready.

MX-ONE_TRUNK

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

Figure 6.92: Call Agent Parameters

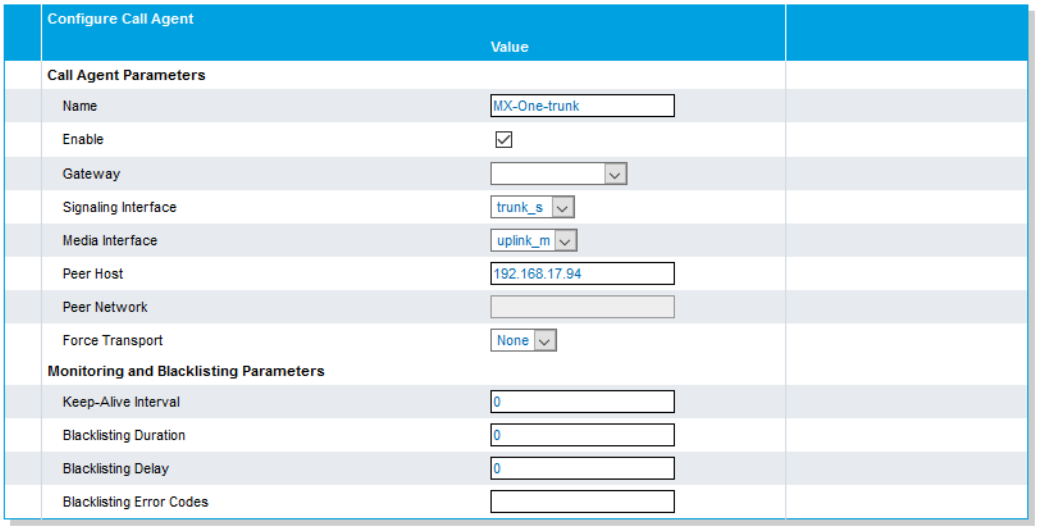
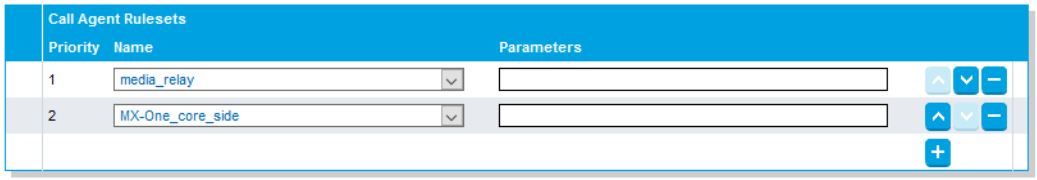


Figure 6.93: Call Agent Rulesets



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

Figure 6.94: Configuration Modified screen

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

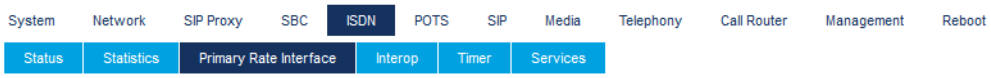
ISDN

Figure 6.95: ISDN Screen

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

Primary Rate Interface

Figure 6.96: Primary Rate Interface screen



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

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

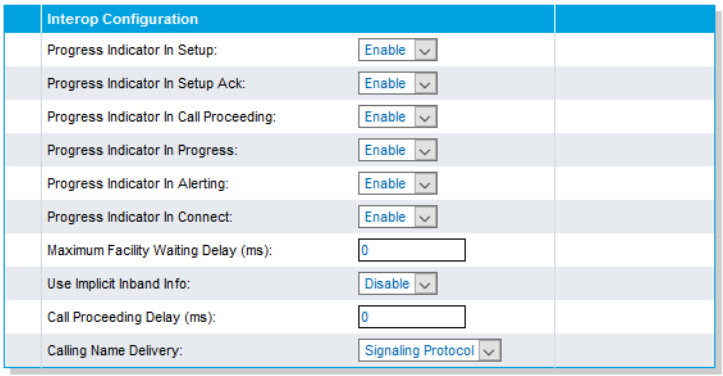
1. Click Apply and restart requested service when done.

Interop

Figure 6.97: Interop screen

1. You can change other parameters dependent on market.

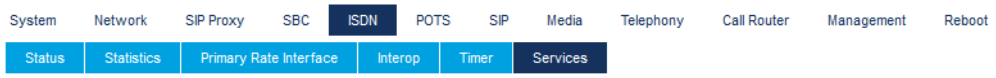
Figure 6.98: Interop Configuration screen



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

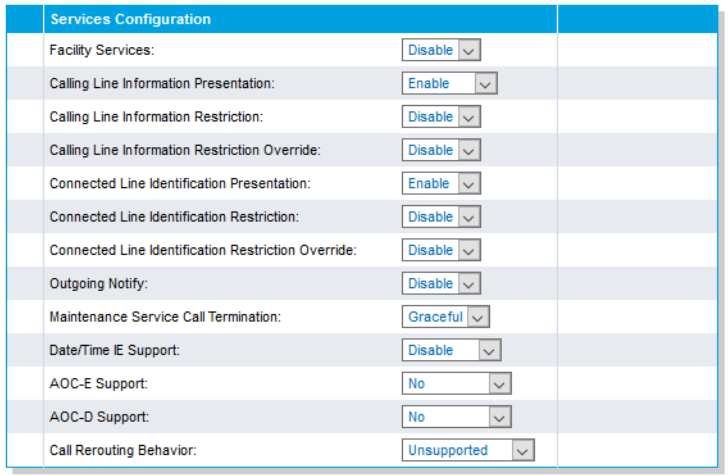
Services

Figure 6.99: ISDN Services screen



1. Change other parameters dependent on market.

Figure 6.100: Services Configuration screen



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

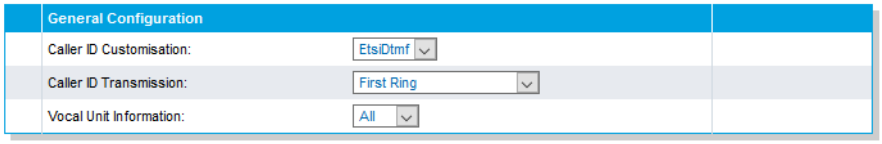
POTS

Config

Figure 6.101: Config screen

1. Set market specific data for Caller Id handling.

Figure 6.102: General Configuration screen



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

FXS Configuration

Figure 6.103: POTS FXS Configuration screen

1. Set analog phone specific data according to market.

Figure 6.104: FXS Configuration screen

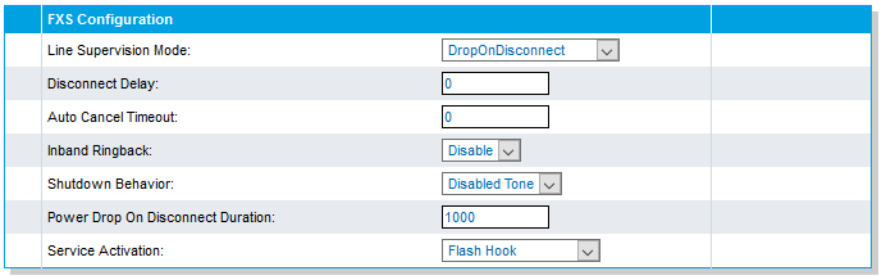
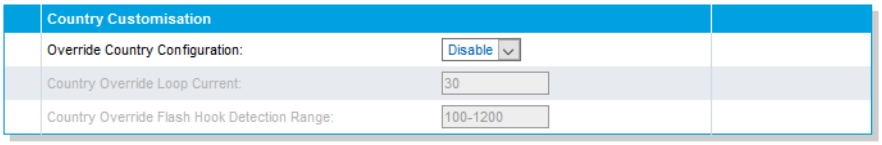


Figure 6.105: Country Customisation screen



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

SIP

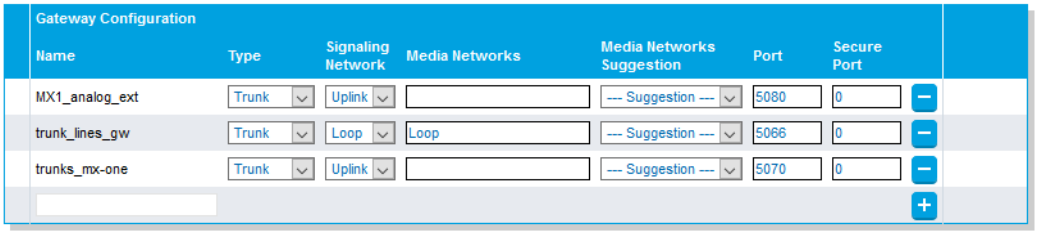
Gateways

Following gateways and port numbers are pre-defined.

Figure 6.106: Gateways screen

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

Figure 6.107: Gateway Configuration screen

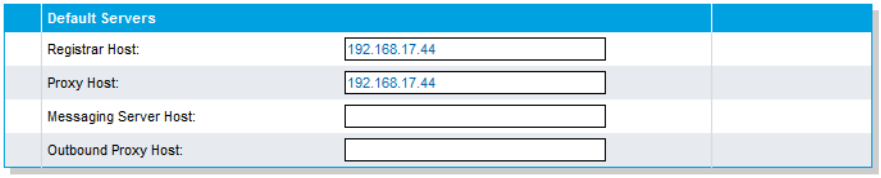


Servers

Figure 6.108: Servers screen

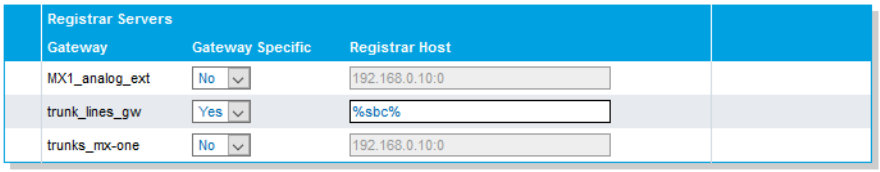
1. Enter IP-address to MX-ONE in both **Registrar Host** and **Proxy Host** fields.

Figure 6.109: Default Servers screen



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

Figure 6.110: Registrar Servers screen

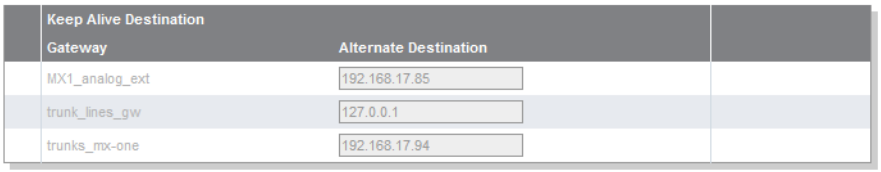


3. Enter IP-address of MX-ONE in the **Proxy Host** field.
4. Enter IP-address of the gateway in the **Outbound Proxy** Host.

Figure 6.111: Proxy Servers screen

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

Figure 6.112: Keep Alive Destination screen



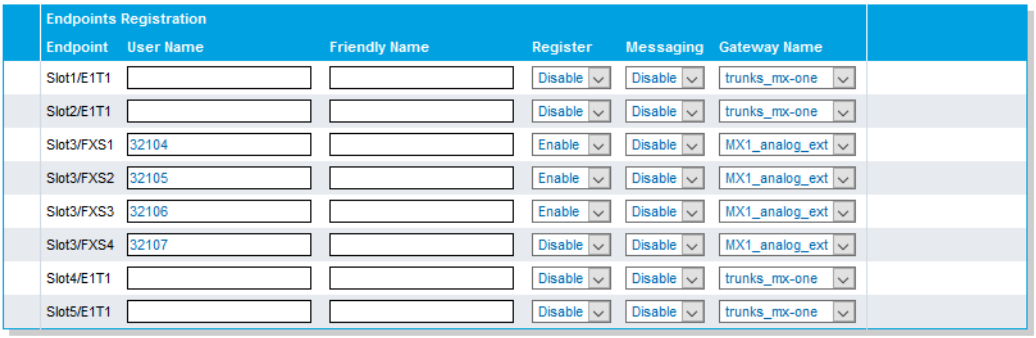
7. Click **Apply** when done and restart service.

Registrations

Figure 6.113: Registrations screen

1. Enter the extension numbers for the analog extensions.

Figure 6.114: Endpoints Registration screen



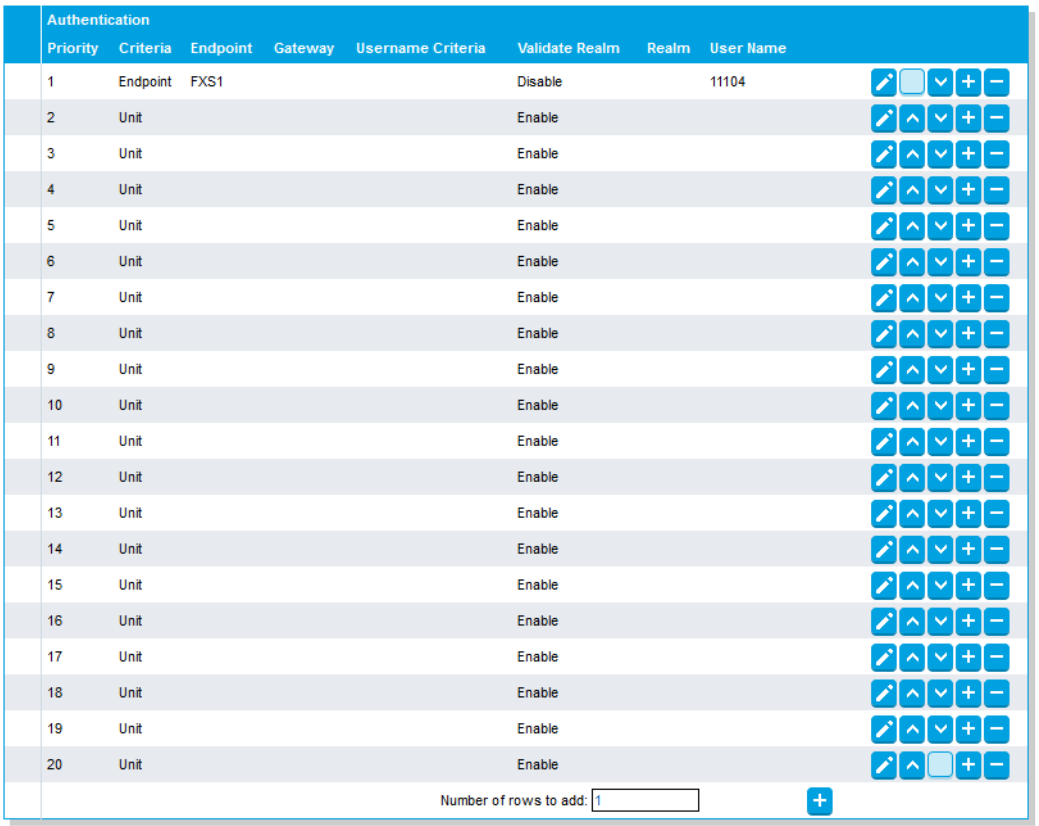
2. Click **Apply** or **Apply and Refresh** when done.

Authentication

Figure 6.115: SIP Authentication screen

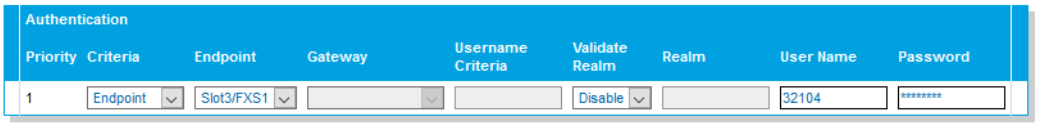
1. If password is required, click for any item.

Figure 6.116: Authentication screen



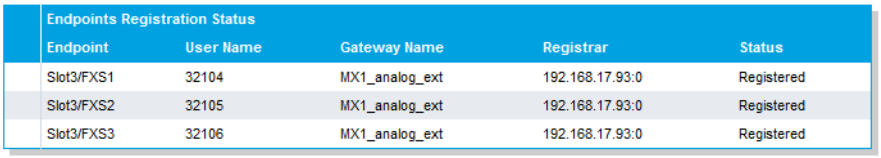
2. Indicate for which Endpoint and Criteria changes are applicable.
3. Enter the Auth Code, in the **Password** field.
4. Disable Validate Realm.

Figure 6.117: Validate Realm screen



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

Figure 6.118: Endpoints Registration screen

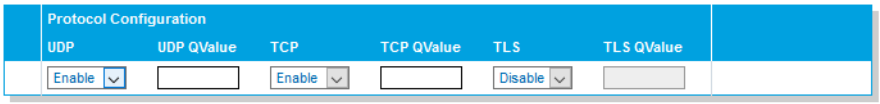


Transport

Figure 6.119: Transport screen

1. Enable UDP if required.

Figure 6.120: Protocol Configuration screen



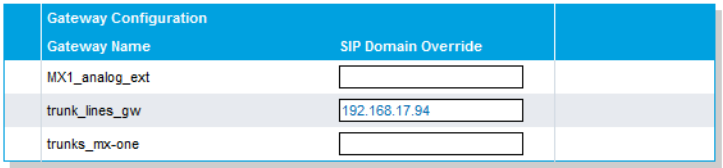
2. Click **Apply** when done and restart service.

Misc

Figure 6.121: Misc screen

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

Figure 6.122: Gateway Configuration screen



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

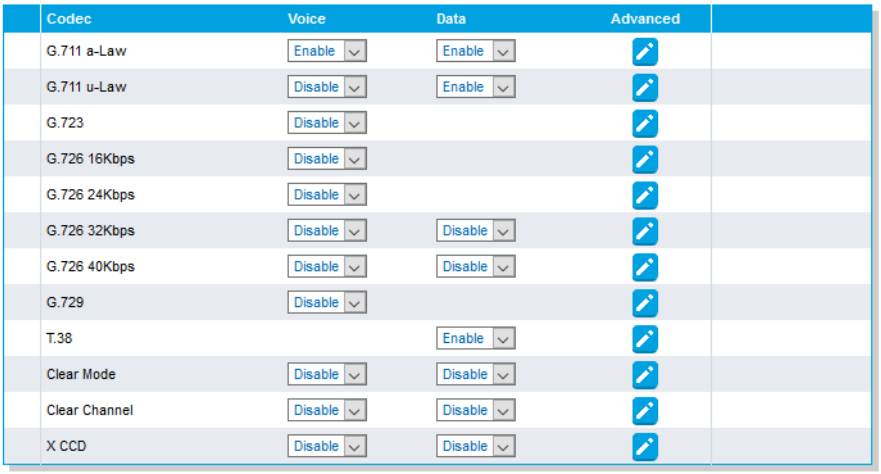
Media

Codecs

Figure 6.123: Codecs screen

1. Change Codecs according to preference.

Figure 6.124: Changing Codecs

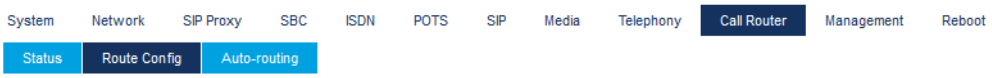


2. Click **Apply** when done and restart service.

Call Router

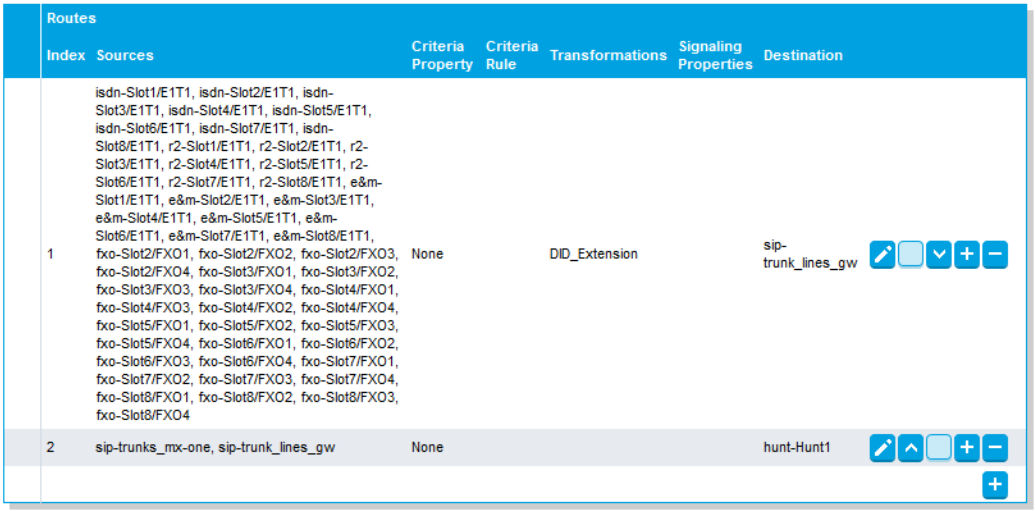
Route Config

Figure 6.125: Route Config screen



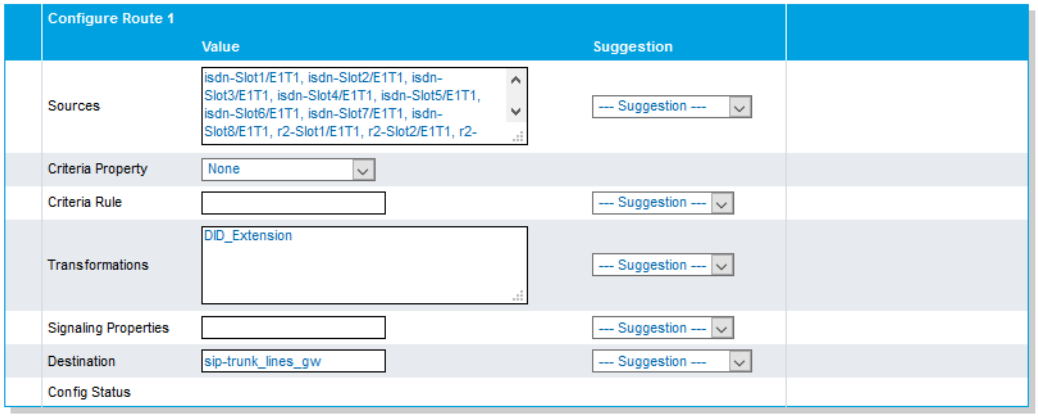
1. Click for index 1. This is used if the received B-number contains a full number. That is, more digits than the pure DID numbers.

Figure 6.126: Routes screen



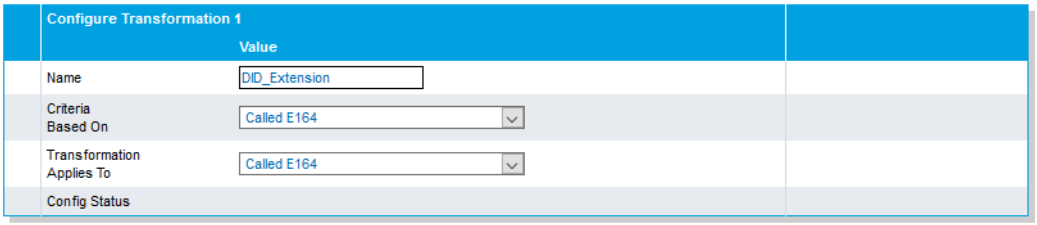
2. In the Transformations field add a name for a transformation rule.

Figure 6.127: Configure Route screen



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

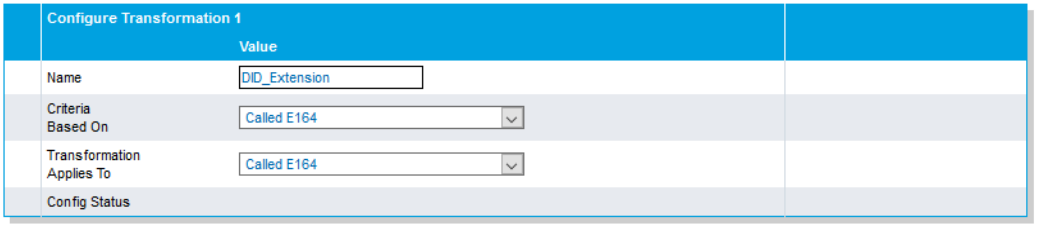
Figure 6.128: Configure Transformation screen



6. Click **Save** or **Save and Insert Rule**.
7. Click in the second Call Property Transformation and enter the same name as above.

8. Use Called E.164 for both **Criteria Based On** and **Transformation Applies To** fields.

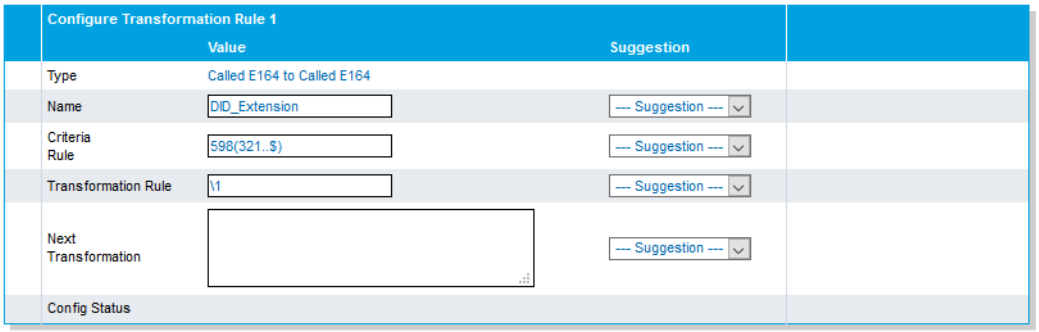
Figure 6.129: Configure Transformation screen 1



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

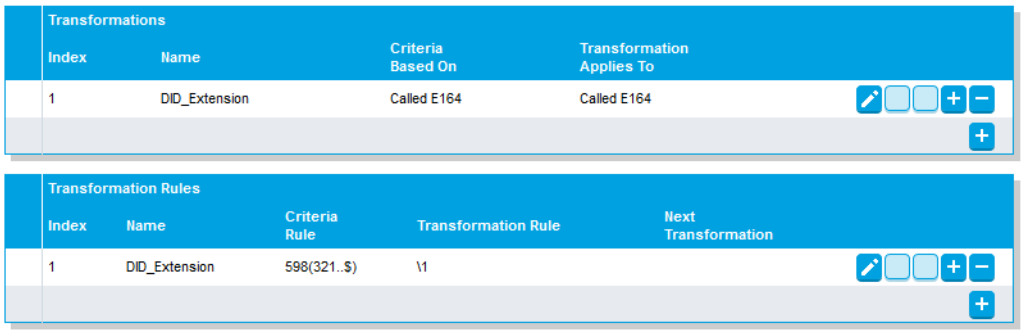
11. The Criteria Rule in this case is 443(111..)$ and the transformation rule is ‘\1.
12. This means that if a B-number is received containing 44311104, then the 3 first digits (443) are removed before the call is sent to MX-ONE for further processing. (111..)$ means that the number can only be 5 digits starting with 111.

Figure 6.130: Configure Transformation Rule 1



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

Figure 6.131: Transformations screen



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

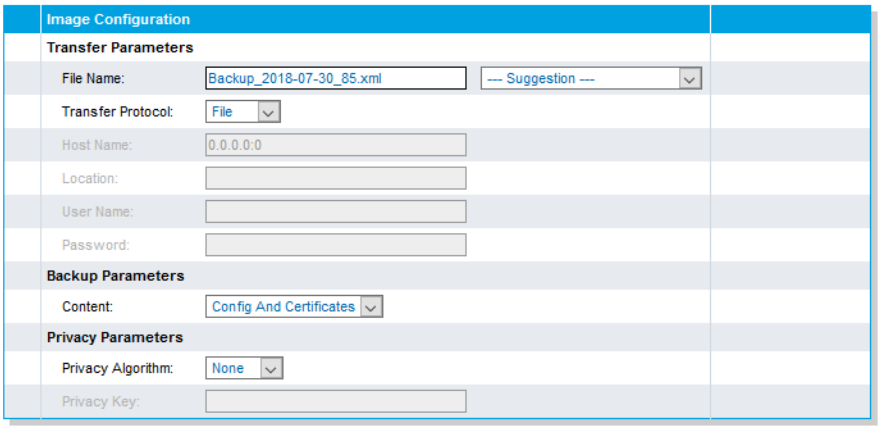
Management

Figure 6.132: Management screen

Backup/Restore

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

Figure 6.133: Image Configuration screen

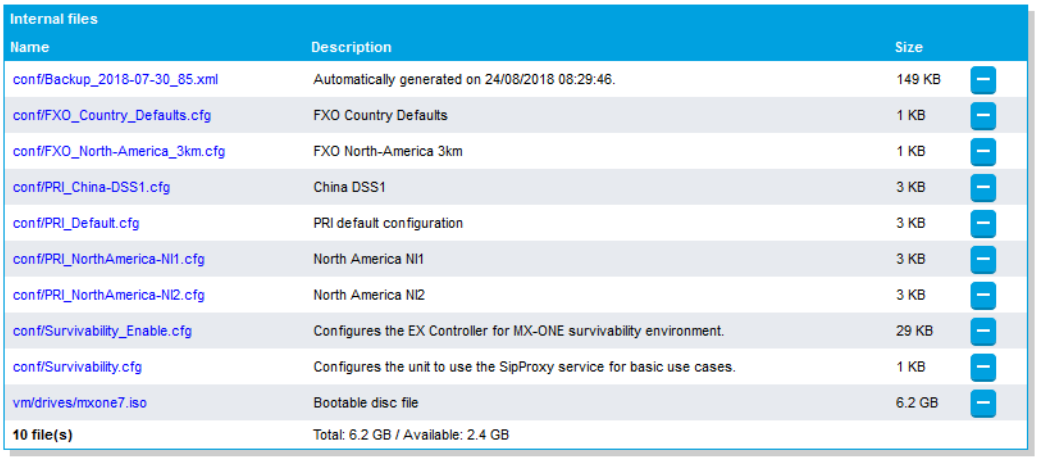


2. Click **Apply and Backup Now**.

File

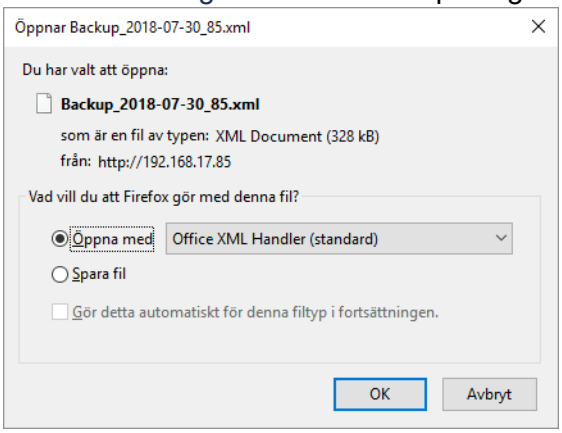
Figure 6.134: File screen

Figure 6.135: Internal files screen



1. Find the previously made backup image.

Figure 6.136: Backup image



2. Download and store on a secure place.

Known Limitations

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

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

MiCollab Advanced Messaging

Customer Product Information of MiCollab Advanced Messaging, see Product Documentation.

Mitel CMG

Customer Product Information of Mitel CMG, see Mitel InfoChannel

Mitel InAttend

Customer Product Information of Mitel InAttend, see Mitel InfoChannel

MiContact Center Enterprise

Customer Product Information of MiContact Center Enterprise, see Product Documentation.

Mitel MC Controller

Customer Product Information of Mitel MC Controller, see Product Documentation.

Mitel
Powering connections

mitel.com

Mitel
Powering connections

mitel.com

Mitel
Powering connections

mitel.com