Ingate SIParator® for SIP Trunking and extending the Mitel MiVoice Connect using Ingate's Native Mitel ShoreSIP Emulation (NMSE)

Configuration Guide

Version 1.00 of this guide

Ingate SIParator® (an SBC/Firewall) version 7.1.1 or later
Requires the NMSE and CCS Ingate licenses, but requires
no Mitel vTrunk license nor any Mitel SIP Trunk licenses
(Mitel has stopped selling extended licenses for the MiVoice Connect)

About This Document

This document is a guide on how to configure the Mitel MiVoice Connect (MiVC) and the **new Ingate SIParator® feature, the Native Mitel ShoreSIP Emulation (NMSE), for SIP trunking of Mitel MiVoice Connect PBX (formerly Shoretel PBX**), introduced in software release 7.1.1, without requiring special Mitel equipment or licenses for SIP trunking.

Since the NMSE implementation in the Ingate SIParator® allows the SIParator to reach MiVC clients, e.g. by their extension numbers, the MiVC can both be SIP trunked to the PSTN, replacing the "old copper network" connection, as well as tie trunked to other PBX systems, local or remote, on-premise or in the cloud.

Further, the SIParator's ability to act as a SIP registrar (under the SRU license), you can extend the MiVC PBX with more capacity and new functionality using equipment following the SIP standard, e.g. SIP telephones or soft clients. Examples of this is shown and exemplified in this guide and more examples of usage are in the plans.

In this document we have left five "good to have" appendices, previously written for the Configuration Guide for Ingate as Teleworker Gateway for Mitel MiVoice Connect and Mitel 6900 phones.

Day-1 Remote Installation Support for SIP trunking the MiVC

Remote Installation Support is available from three sources at different item numbers:

IGT-0022-03 Remote Installation Support by CTD (North America)
support@ingate.com toll free: +1-866-809-0002 NA did: +1-864-551-4216
Sales and ordering: Computer Telephony Distribution (CTD) ingate@ctdconnect.com
(866) 533-3331 (toll free), (864 527-9600 (local)

IGT-0022-02 Remote Installation Support by Educronix (Latin America, also in Spanish)
Educronix LCC also does special projects and Ingate training from a Florida location. Order through Ingate or directly by Educronix at support@educronix.com and toll free: +1 855 866 8854

IGT-0022-01 Remote Installation Support by Ingate (Rest of the World)
support@ingate.com +46-8 600 7766

Remote Installation Support, per hour (minimum 2h for Mitel SIP Trunking). Additional time beyond the minimum 2 hours is charged afterwards the same hourly rate.

Contents

1 Introduction

This document describes the steps to configure the Ingate SIParator® (an "E-SBC" often used for connecting PBXs to SIP trunks) and the Mitel MiVoice Connect (formerly ShoreTel PBX) using

Ingate's Native Mitel ShoreSIP Emulation (NMSE) for SIP trunking, was introduced in version 7.1.1 of the SIParator® software. All supported Ingate SIParators, including current appliances (most S21, all S22, S42, S52, S82, S95, S97 and S98) as well as the Software SIParator® for virtual x86 machines and cloud platforms, can be configured using NMSE for SIP trunking of the MiVoice Connect (MiVC).

Required Versions and Licenses:
MiVoice Connect (MiVC) PBX (Formerly ShoreTel)[1]
Ingate SIParator® 7.1.1 or later with one NMSE and one CCS license for each concurrent SIP trunk session

A fair knowledge of MiVC Connect, as well as the Ingate SIParator®, is required to be able to follow this document.

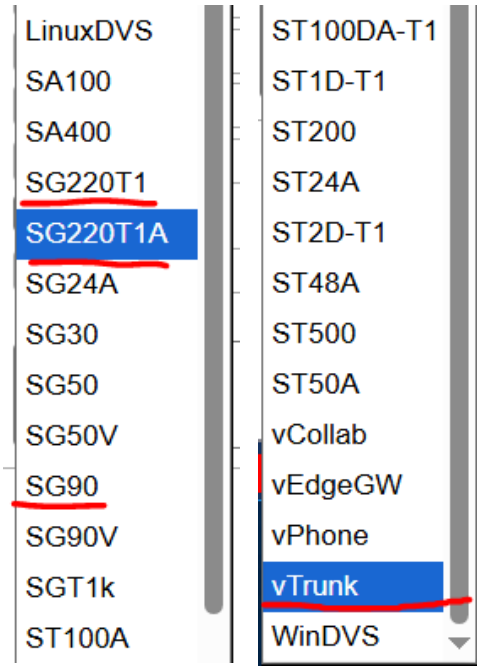
The MiVoice Connect Platform Documentation is available at
https://www.mitel.com/document-center/business-phone-systems%3Amivoice-connect%3Amivoice-connect-platform

The Ingate SIParator® Documentation is available at
https://www.ingate.com/Documentation.php

[1] Tested on MiVoice Connect 20.0 HF1 (Build: 23.30.4100.0) but believed to be backwards compatible. Contact Ingate support for any problem.

2 Ingate SIParator® Using Native Mitel ShoreSIP Emulation (NMSE) Explained

The MiVoice Connect PBX (MiVC, formerly Shoretel) consist of several appliances or servers connected to local LAN, where the red-underlined can be used to hold the other together in a SIP trunk group that, (most often) via an Ingate SIParator® (an enterprise SBC and Firewall), to connect the MiVC hardware or software devices on the Mitel LAN, to an outside SIP world that may be an ITSP's SIP trunk, over the Internet or on a private IP pipe.



Ingate's Native Mitel ShoreSIP Emulation (NMSE), makes the SIP trunking functionality of the red-underlined hardware or software (Mitel's vTrunk) components obsolete. The NMSE license enables the Mitel-specific protocols required for SIP trunking and connects directly to the local Mitel LAN.

Ingate has selected to emulate the SIP trunking functionality of the SG220T1A, being a since-long available and (hopefully) stable product requiring no Mitel licenses at all. We have not yet seen any capacity limitations of our emulation.

The SIP trunking functionality you get, is equivalent to Mitel's vTrunk plus the Ingate SIParator, for connecting to "anything using SIP", including ITSP trunking to the PSTN and privately tie-trunking to other SIP PBX services (locally or over the Internet), se chapter **5 Connecting Your MiVC to PSTN SIP Trunk Providers and Other SIP PBXs (tie trunking).**

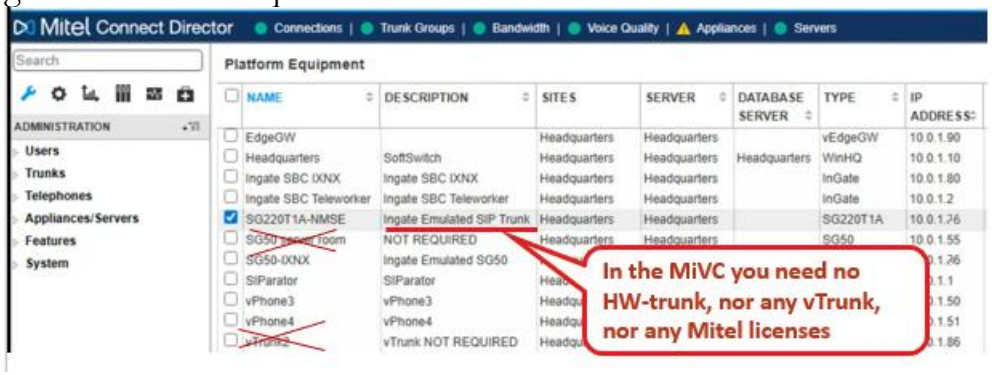
The requirement for the NMSE implementation became urgent when Mitel towards the end of 2025 announced:

> MiVoice Connect End of Extended License Sales fast approaching
>
> - Partners who wish to purchase Ingate SIParator products may continue to do so directly from Ingate:
>   - Partners in the US and Canada should contact Ingate's US distributor: Computer Telephony Distributing (CTD)
>   www.ctdconnect.com
>   (866) 533-3331 (toll free)
>   (864) 527-9600 (local)
>   - Partners in other countries should contact Ingate directly via email to sales@ingate.com

Email CTD at: ingate@ctdconnect.com

The Native Mitel ShoreSIP Emulation (NMSE) is straight forward to install and to use. In short, it is an ordinary SIP trunking installation (the NMSE license cost is approximately half of the Mitel SIP trunking cost) that you enable at the Ingate SIParator's SIP Trunk configuration page:

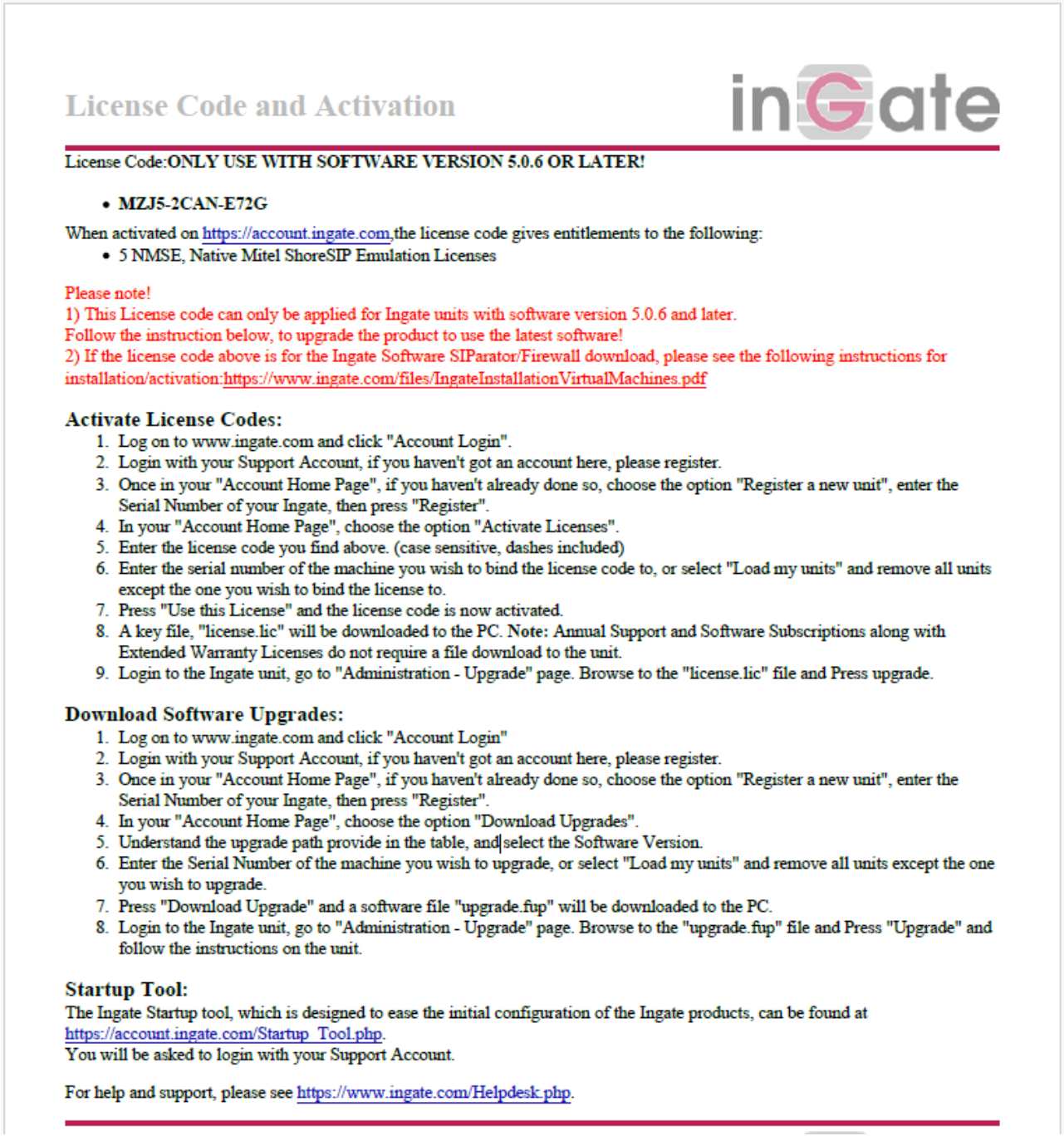
The NMSE license is per concurrent session. There are no additional Mitel SIP trunking gear or licenses required:



You simply set up your current MiVC PBX to reach the PSTN via the Ingate SIParator® NMSE-emulated SG220T1A.

3 Configuration of the Ingate SIParator® for SIP Trunking of the MiVC, using the Native Mitel ShoreSIP Emulation (NMSE)

After activation of the NMSE license on an existing SIParator® installation:



License Code and Activation

License Code:**ONLY USE WITH SOFTWARE VERSION 5.0.6 OR LATER!**

- **MZJ5-2CAN-E72G**

When activated on https://account.ingate.com,the license code gives entitlements to the following:

- 5 NMSE, Native Mitel ShoreSIP Emulation Licenses

Please note!
1) This License code can only be applied for Ingate units with software version 5.0.6 and later.
Follow the instruction below, to upgrade the product to use the latest software!
2) If the license code above is for the Ingate Software SIParator/Firewall download, please see the following instructions for installation/activation:https://www.ingate.com/files/IngateInstallationVirtualMachines.pdf

Activate License Codes:

1. Log on to www.ingate.com and click "Account Login".
2. Login with your Support Account, if you haven't got an account here, please register.
3. Once in your "Account Home Page", if you haven't already done so, choose the option "Register a new unit", enter the Serial Number of your Ingate, then press "Register".
4. In your "Account Home Page", choose the option "Activate Licenses".
5. Enter the license code you find above. (case sensitive, dashes included)
6. Enter the serial number of the machine you wish to bind the license code to, or select "Load my units" and remove all units except the one you wish to bind the license to.
7. Press "Use this License" and the license code is now activated.
8. A key file, "license.lic" will be downloaded to the PC. **Note:** Annual Support and Software Subscriptions along with Extended Warranty Licenses do not require a file download to the unit.
9. Login to the Ingate unit, go to "Administration - Upgrade" page. Browse to the "license.lic" file and Press upgrade.

Download Software Upgrades:

1. Log on to www.ingate.com and click "Account Login"
2. Login with your Support Account, if you haven't got an account here, please register.
3. Once in your "Account Home Page", if you haven't already done so, choose the option "Register a new unit", enter the Serial Number of your Ingate, then press "Register".
4. In your "Account Home Page", choose the option "Download Upgrades".
5. Understand the upgrade path provide in the table, and select the Software Version.
6. Enter the Serial Number of the machine you wish to upgrade, or select "Load my units" and remove all units except the one you wish to upgrade.
7. Press "Download Upgrade" and a software file "upgrade.fup" will be downloaded to the PC.
8. Login to the Ingate unit, go to "Administration - Upgrade" page. Browse to the "upgrade.fup" file and Press "Upgrade" and follow the instructions on the unit.

Startup Tool:

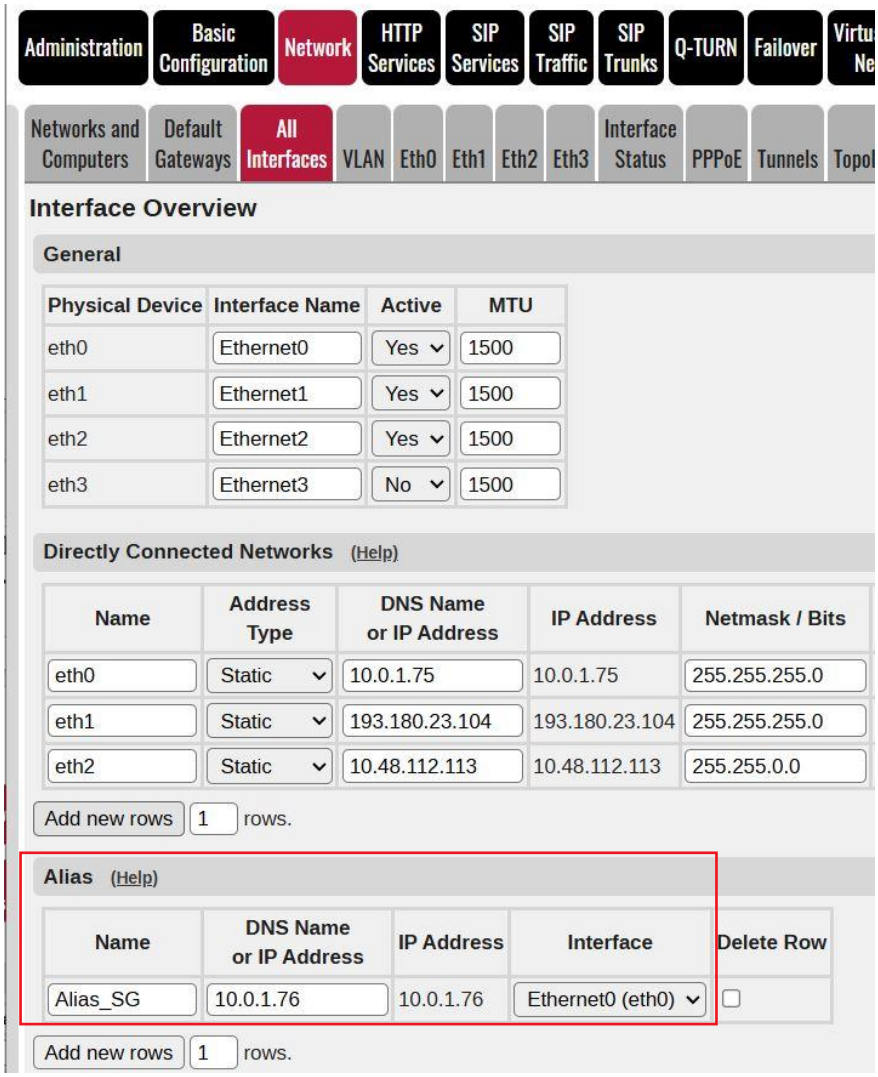
The Ingate Startup tool, which is designed to ease the initial configuration of the Ingate products, can be found at https://account.ingate.com/Startup_Tool.php.
You will be asked to login with your Support Account.

For help and support, please see https://www.ingate.com/Helpdesk.php.

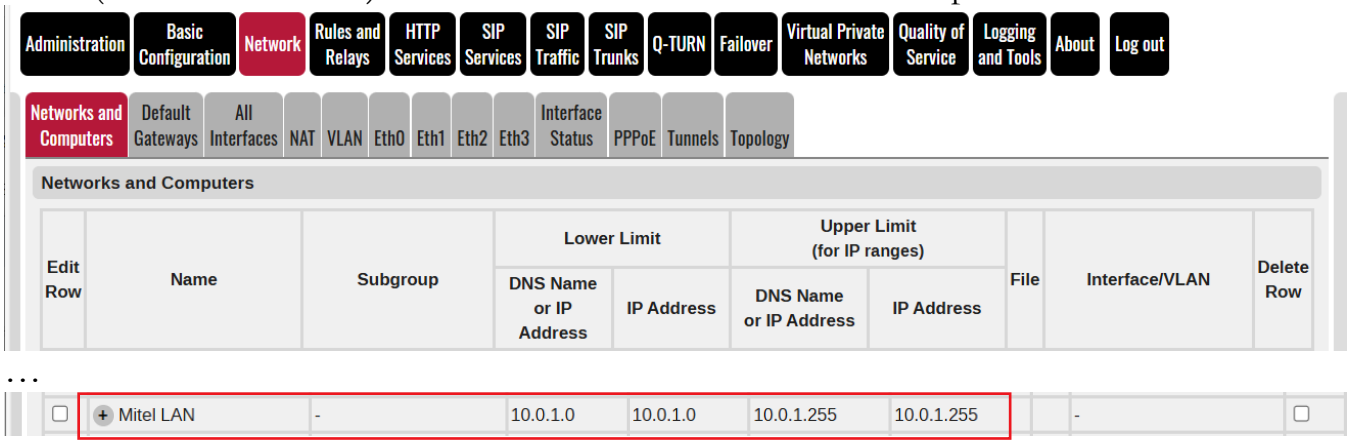
or after a new SIParator® installation, e.g. by using the Startup Tool as outlined at the bottom of above "License Code and Activation" printout, you need to do the following additional configuration.

3.1 Network Setup

At the **Network>All Interfaces** GUI page, you need to define an alias address (here "Alias_SG"), that should be a free (not already used) IP address of the local LAN that the MiVoice Connect is installed on.



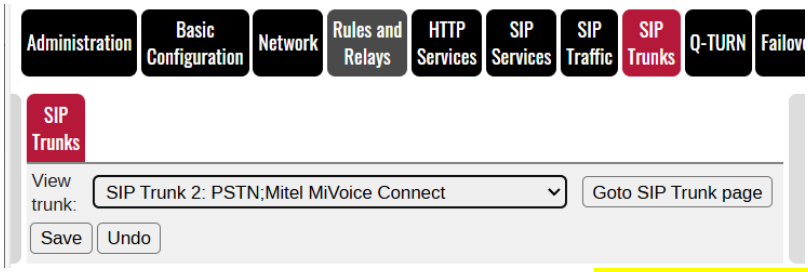
and at the **Network>Network and Computers** GUI page, you need to have a network name (here "Mitel LAN") that includes all MiVoice Connect components.



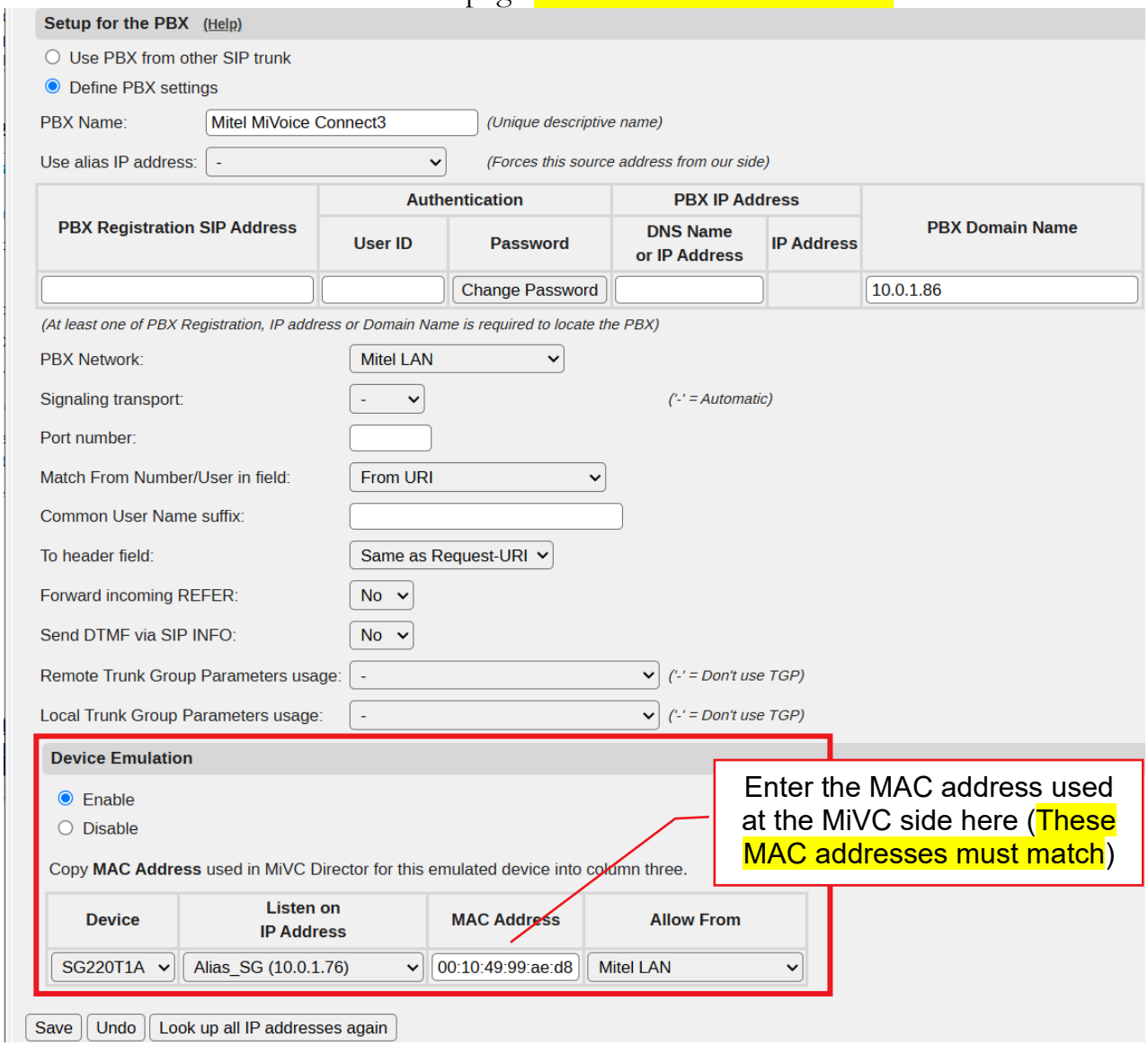
…

3.2 Enable the Native Mitel ShoreSIP Emulation (NMSE) at a SIP Trunk GUI Page

Go to the SIP trunk page to be used (typically SIP Trunk 1), where you have activated the NMSE licenses:



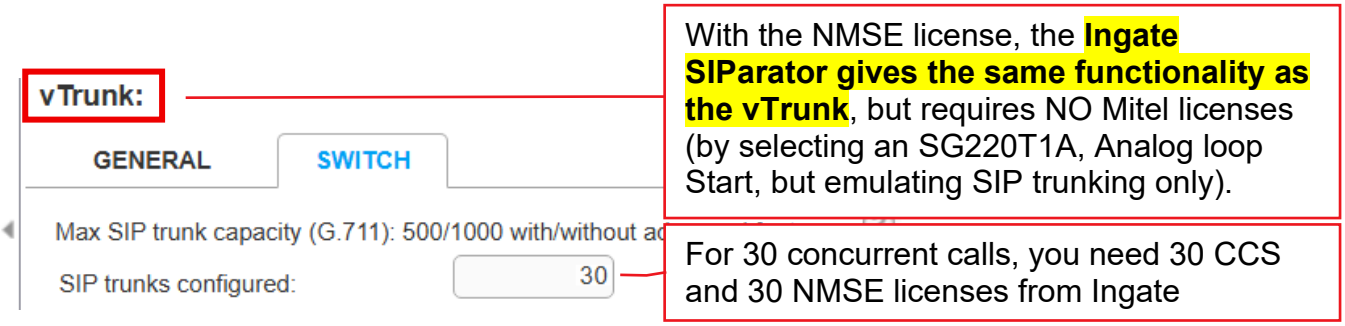
and at the bottom of the SIP trunk page enable "Device Emulation":



select the Device SG220T1A, the Alias IP defined above, the MAC address you setup in the Director of the MiVC (the three first hex digits are pre-defined by Mitel and select e.g. 1a:2b:3c for the last three hex digits (must be unique on the Mitel LAN). The MAC address MUST BE THE SAME as used at the MiVC side (seen in the MiVC Director). (You must only enable the SG220T1A emulation at one of a SIParator's SIP Trunk pages, but you may use it towards several ITSP PSTN trunks and several other PBX tie trunks.)

4 Configure the MiVC to Use Ingate's NMSE-Emulated SG220T1A to get vTrunk Functionality

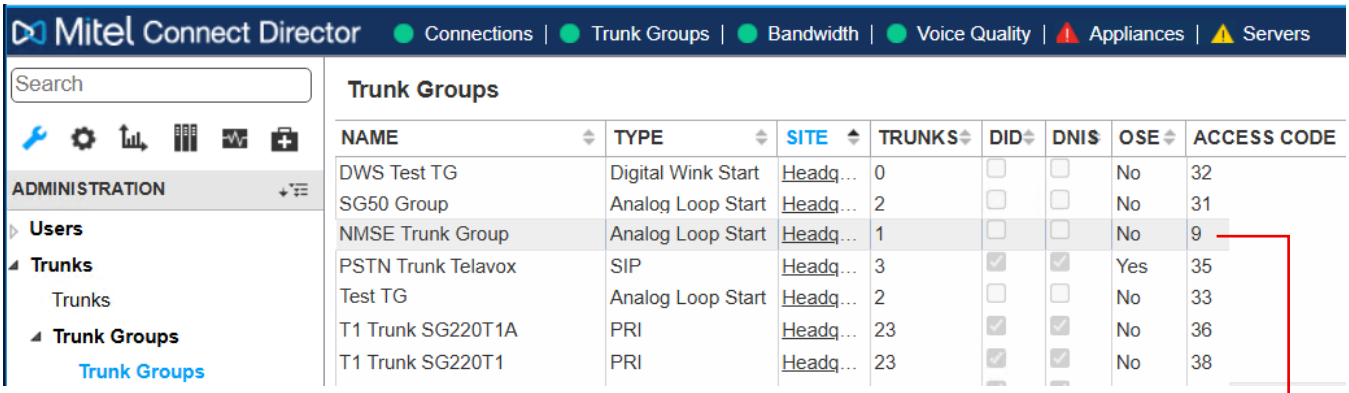
The Ingate SIParator with software 7.1.1 or higher will – with the NMSE license and the below yellow highlighted configuration – give the functionality of the Mitel MiVC vTrunk (only for comparison, no vTrunk needs to be present):



To setup the MiVC to use an Ingate SIParator® NMSE (Native Mitel ShoreSIP Emulation) trunk, you first setup the **Trunk Groups**, then the **Platform Equipment** and then the **Trunk**.

4.1 Select an ACCESS CODE (a dialing prefix[2]) on the Trunk Groups page for using the Ingate NMSE Trunk Interface in the MiVC Director

At the Mitel Connect Director>ADMINISTRATION>**Trunk Groups** page:

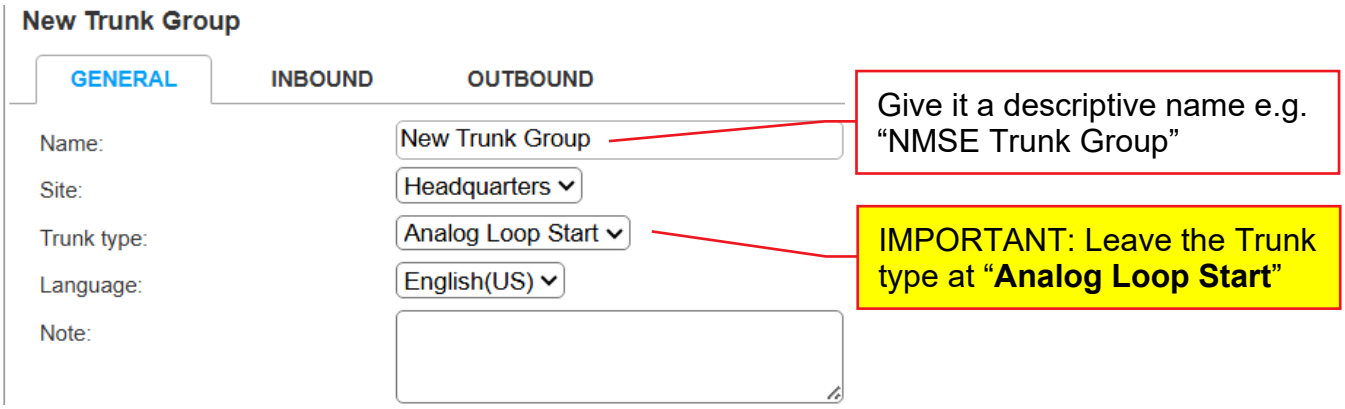


To create this new row press the **NEW** button at the top to the right

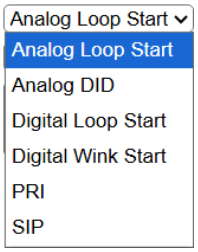
[2] If you already have a traditional PSTN connection for your MiVC, e.g. using dialing prefix (or access code) 9 to reach out of your company and want to continue to use 9 for the new SIP connection, it is recommended that you replace 9 with another available access code (if needed, you can expand the access code range at Director>ADMINISTRATION>System>Dialing Plan>**Dial Plan**), e.g. with 39, and setup the new Ingate SIParator® NMSE SIP trunking using dialing prefix 9.

and in the lower part of that page these three tabs will appear.

At the **GENERAL** tab:

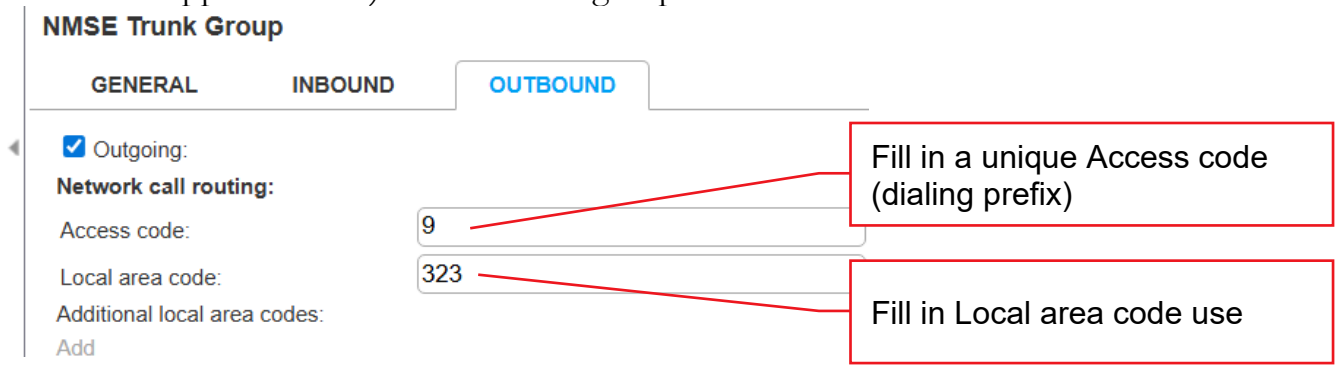


(If SIP would be selected, Mitel SIP trunk session licenses would be required. **The Ingate SIParator NMSE Emulation will do SIP**, and nothing else, anyway.)



leave the **INBOUND** tab at its default:

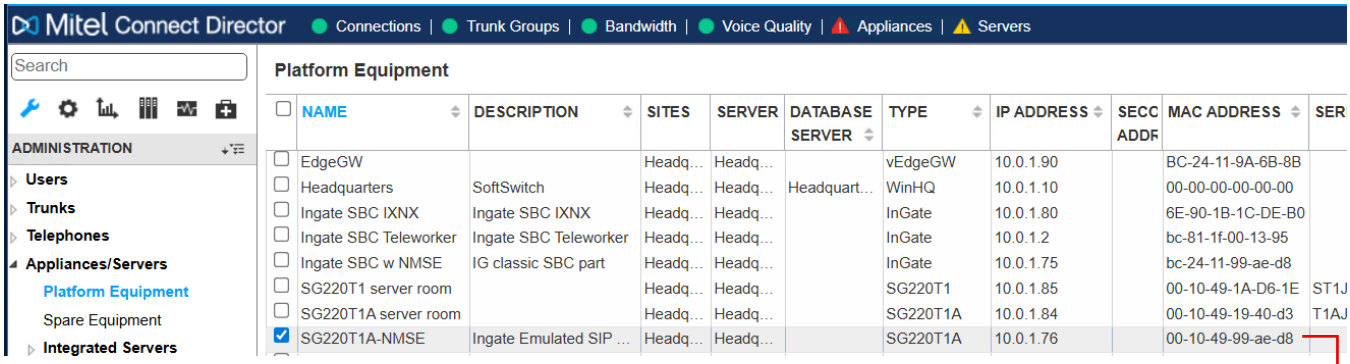
at the **OUTBOUND** tab, select the prefix and the local area code (at the locality the phone clients are supposed to be) for this trunk group.



Then press the **SAVE** button to the right 

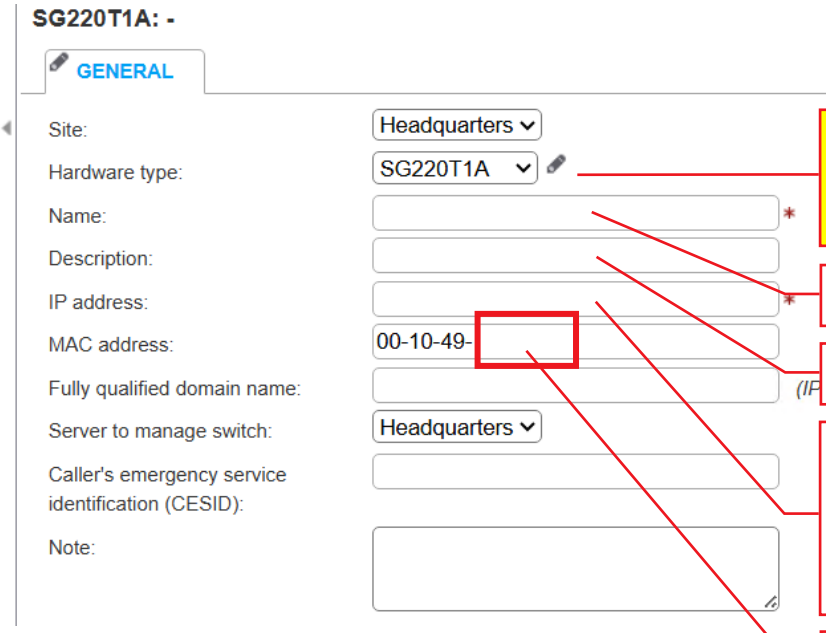
4.2 Setup a new Platform Equipment – The Ingate SIParator® emulated SG220T1A

At the Mitel Connect Director>ADMINISTRATION>**Platform Equipment** page:



To create this new row press the **NEW** button at the top to the right

and in the lower part of that page this **GENERAL** tab will appear:



Select Hardware type **SG220T1A** and these fields will show up:

Fill in a Name

Fill in a Description

Fill in the alias IP address defined in the Ingate SIParator

Alias_SG	10.0.1.76

as defined in 3.1 Network Setup

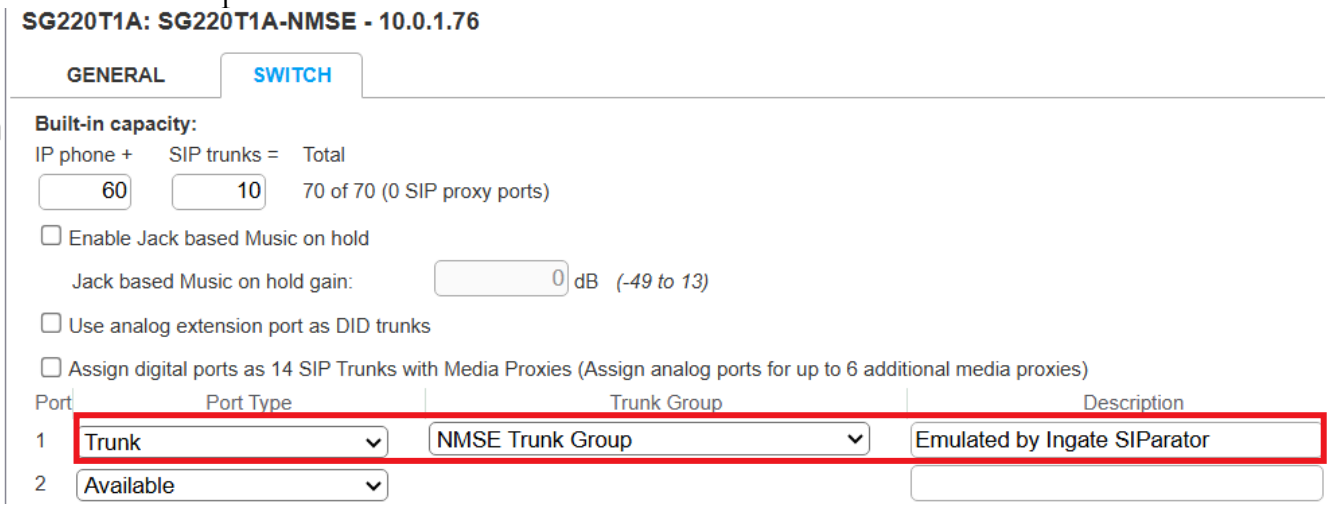
Mitel provides these three first hex digits of the MAC address and you should add the last three hex digits – any unique hex digits (e.g. a1-b2-c3) will be ok, BUT THE FULL MAC ADDRESS MUST BE THE SAME AS USED IN THE Ingate SIParator.

Fill in the above and press the **SAVE** button to the right

We should then have got this and can proceed to the **SWITCH** tab.

Check that this MAC address is the same as used on the Ingate side (see section 3.2 above)!

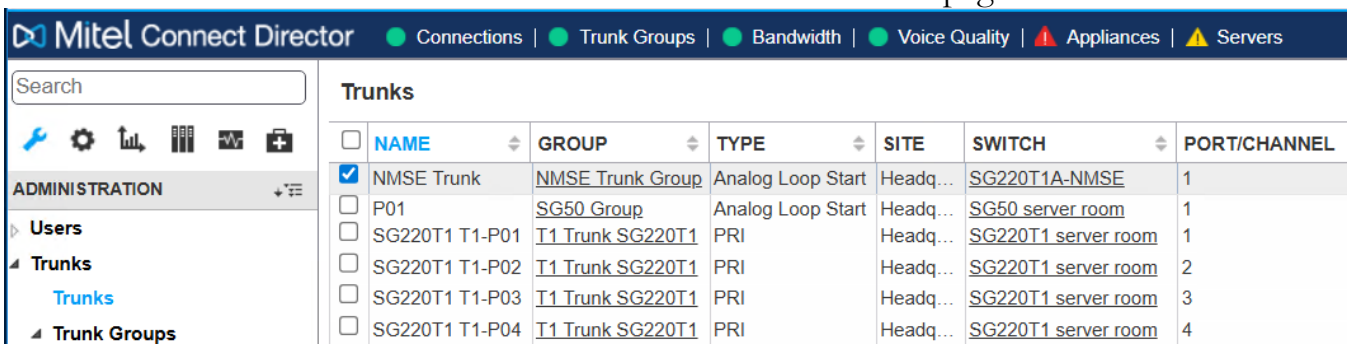
At the **SWITCH** tab at the bottom **Platform Equipment** page, select the red-framed and provide a Description:



Then press the **SAVE** button to the right 

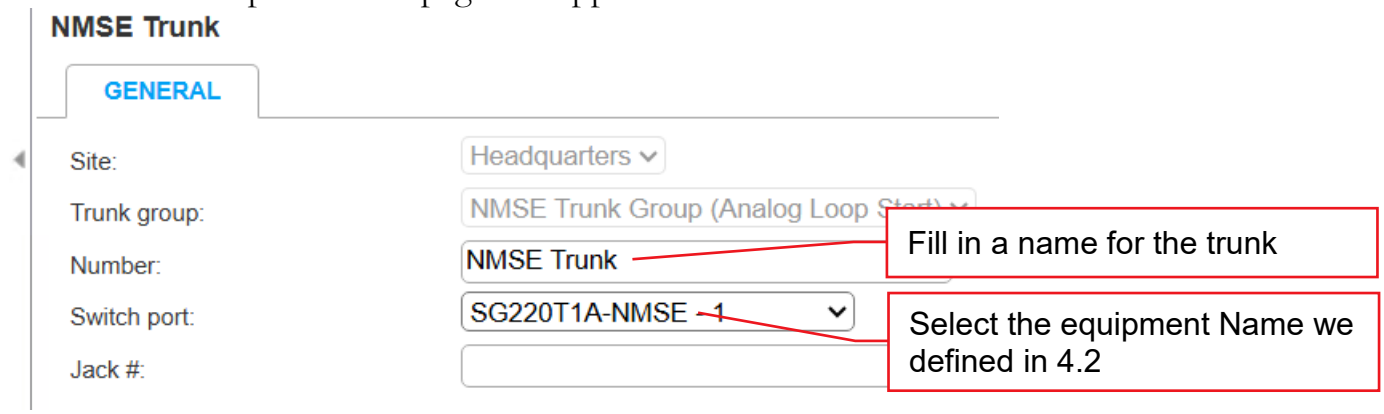
4.3 Create a Trunk for Ingate NMSE Trunk Group in the MiVC Director

At the Mitel Connect Director>ADMINISTRATION>**Trunks** page:



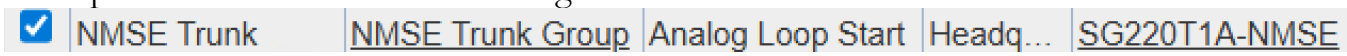
Create a new trunk by pressing the **NEW** button at the top to the right

and in the lower part of that page will appear:



Then press the **SAVE** button to the right

and the



row at the upper half of this Director GUI page will appear.

5 Connecting Your MiVC to PSTN SIP Trunk Providers and Other SIP PBXs (tie trunking)

The Ingate SIParator®/Firewall is often referred to as the "Swiss Army Knife" for real-time communication, meaning SIP routing, SIP interoperability as well as enterprise and SIP firewalling, specially through its flexible SIP Dial Plan and multiple SIP Trunks configuration possibilities. For each set of concurrent call licenses (CCS licenses) you buy, you get the option to apply these new CCS licenses to an existing or new SIP Trunk GUI page that will allow integration with another SIP environment.

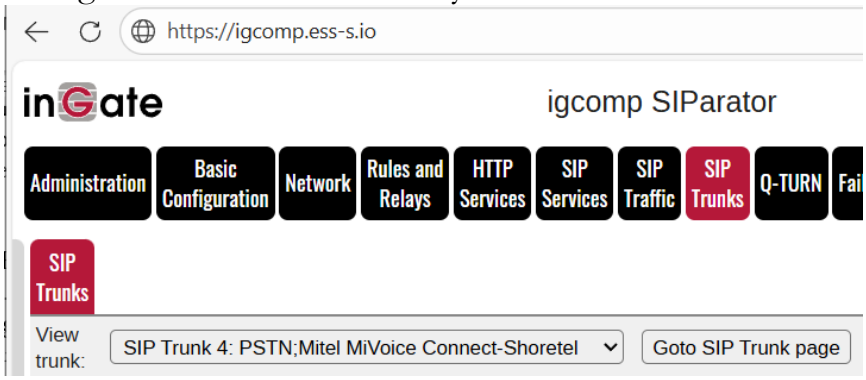
These capabilities have existed in the Ingate SIParator® (often called just SBC or E-SBC) for over a decade, but in the highly popular MiVoice Connect/ShoreTel PBX environment – where the Ingate SIParator® has been an OEM component since 2008(!) – the Ingate SIParator has mostly been used for "plain SIP trunking", i.e. connecting the PBX to the Public Switched Telephone Network (the PSTN) over an IP network rather than over the old "copper network".

Now, with the Native Mitel ShoreSIP Emulation (NMSE) introduced in software release 7.1.1, we expect the MiVC – many still being connected or "trunked" to the PSTN over copper lines – to move over to a SIP IP connection to the PSTN, but ALSO to use SIParator® for **"tie trunking".**

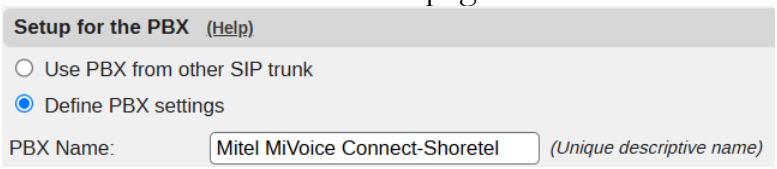
This section is written to provide an understanding and overview, to exemplify setup and to point out relevant information the new **tie trunking for migrating to whatever is to come, on-premise or in the cloud**, to improve the total enterprise PBX experience.

There are two useful guides that will be referenced:
How To SIP Trunking Using the SIP Trunk Page, and
How To use Generic Header Manipulation
and there are extensive help texts (Help) in the SIParator GUI (in addition to the reference manual Ingate Reference Guide), to detail how to configure and use for:
Connecting Your MiVC to PSTN SIP Trunk Providers, as well as
Connecting Your MiVC to Other SIP PBXs (tie trunking)

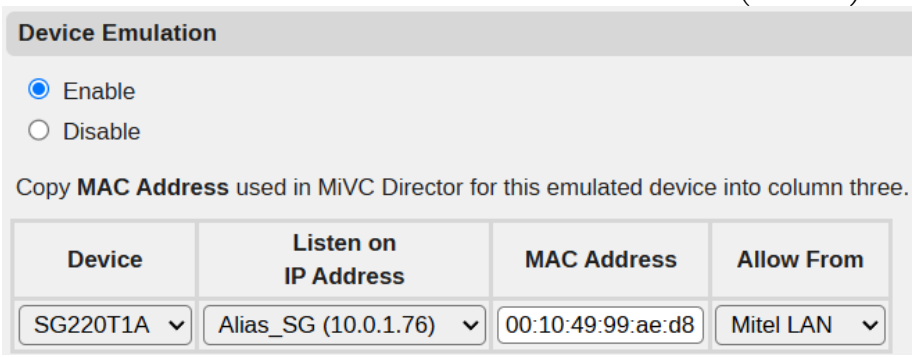
In these examples, assume the company Igcomp has a SIParator @igcomp.ess-s.io, with its configuration GUI reachable by a web browser at:



and in the previous sections, we setup at the Mitel MiVoice Connect–Shoretel PBX at the bottom of SIP Trunk 4 GUI page:



and enabled the Mitel Native ShoreSIP Emulation (NMSE) under "Device Emulation":



Before going into how tie trunking to another IG-LAN is done, let's rehearse how the SIParator's Dial Plan and SIP Trunk typically are setup (e.g. by the startup tool, SUT TG), by these three cuts from How To SIP Trunking Using the SIP Trunk Page:

There is one Dial Plan that can trap outgoing calls meant for a certain SIP Trunk (that there may be many of):

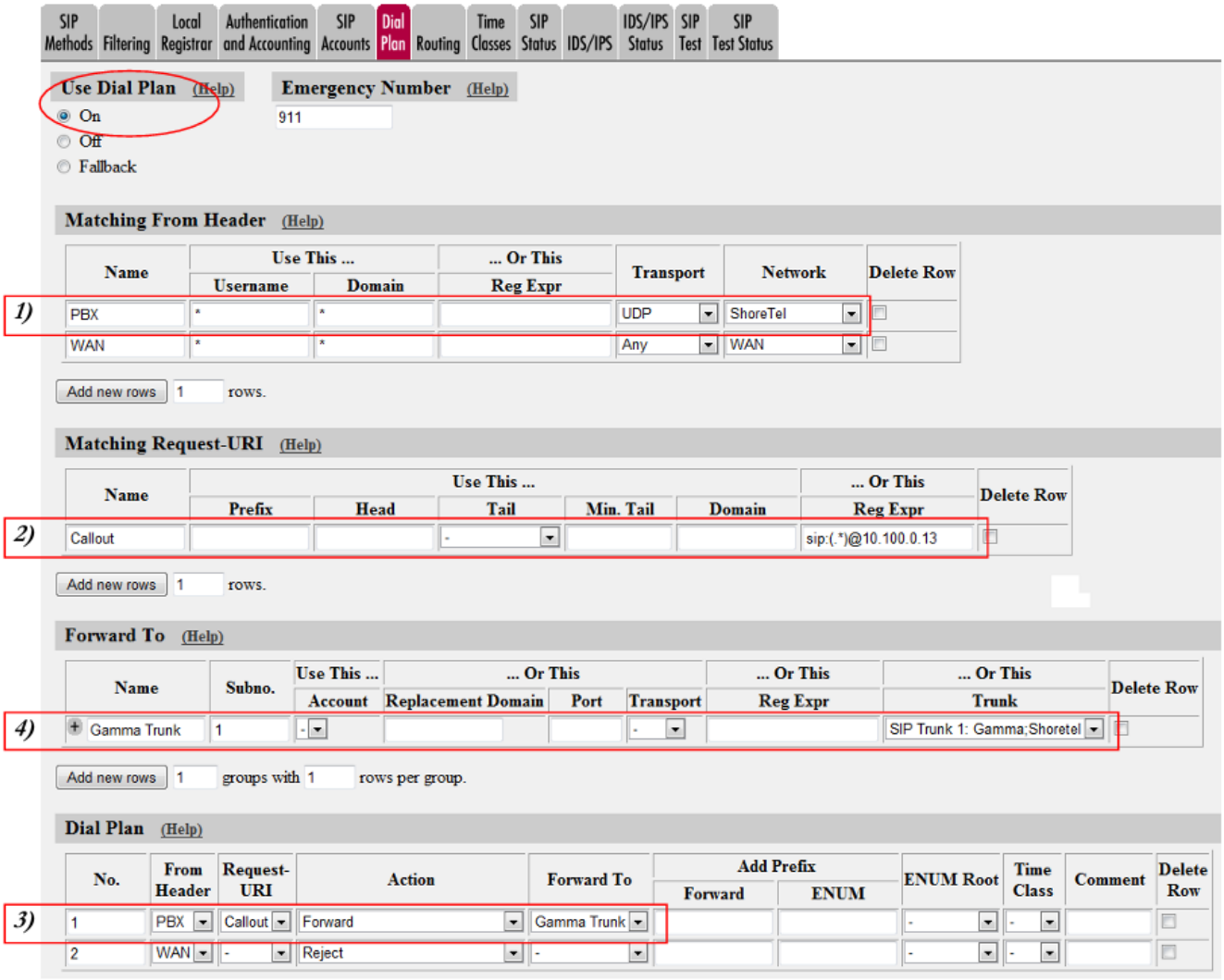
2 Setting up SIP Trunking

This section describes the functioning and set-up of the SIP Trunk page in the Ingate.
Please remember that these settings, as well as most of the other ones in this description, usually are done by the Startup Tool TG and that this description is provided for reference.

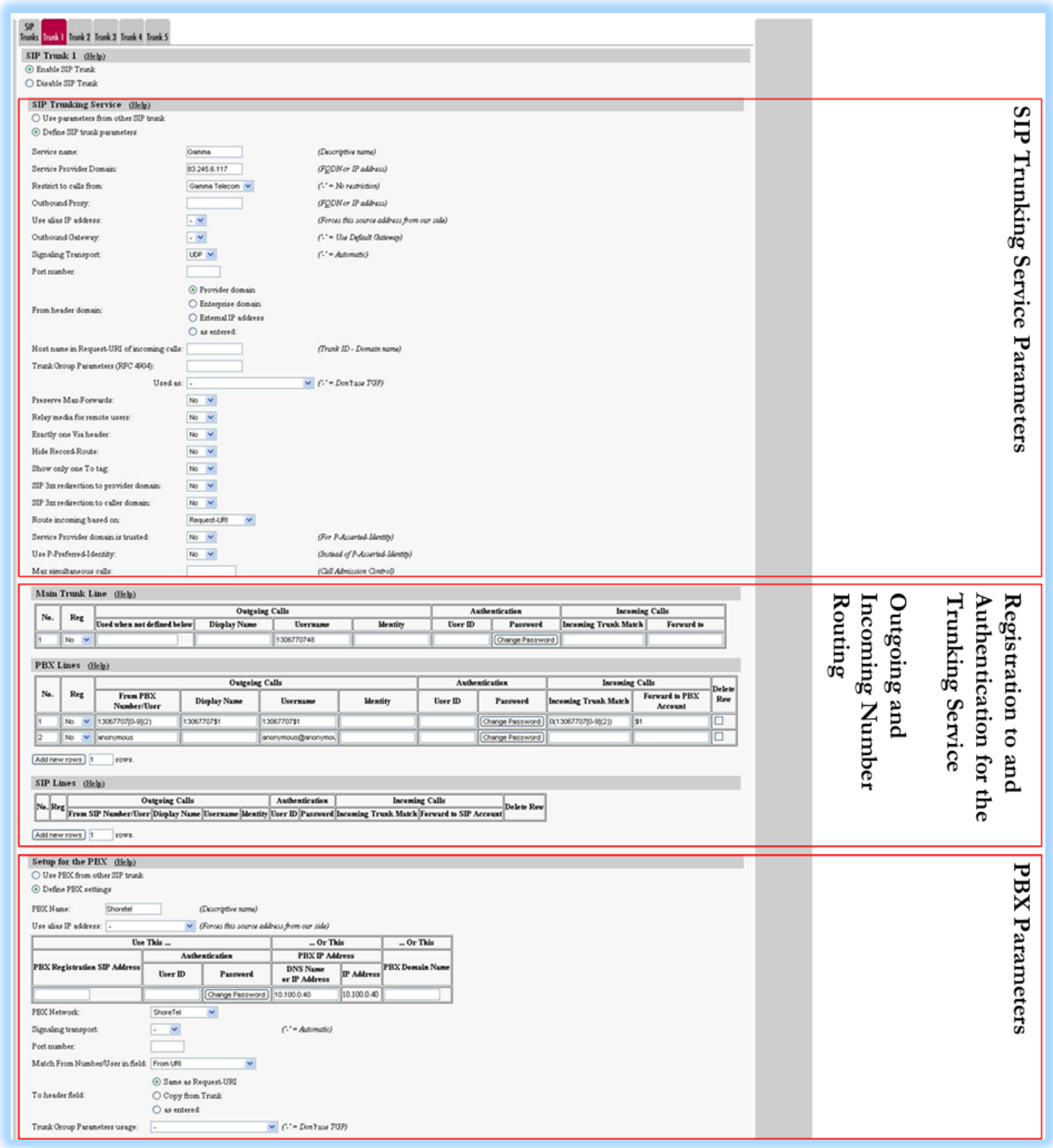
2.1 Defining Outgoing Call Handling in the Dial Plan

Outgoing calls are processed through the Dial Plan, which must be ***On***. At a minimum, the fields exemplified below must be entered. The actual Dial Plan table is searched line by line from the top for a match from the PBX of the dialed number where after it is forwarded to the SIP Trunk page.

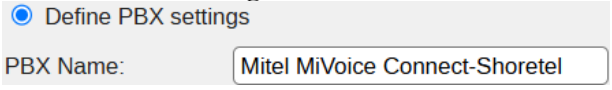
1) Calls from the PBX connected to network "ShoreTel"
2) …with a any dialed number send sent to this unit (regular expression (.*)@10.100.0.13)
3) …will be forward for further processing to "Gamma Trunk"
4) …which is defined on SIP Trunk page 1



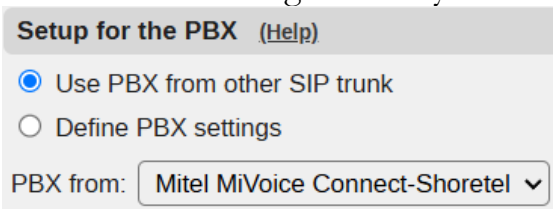
At ***4)*** in above cut, you see a **Forward To** SIP Trunk 1: Gamma;Shoretel in this cut:



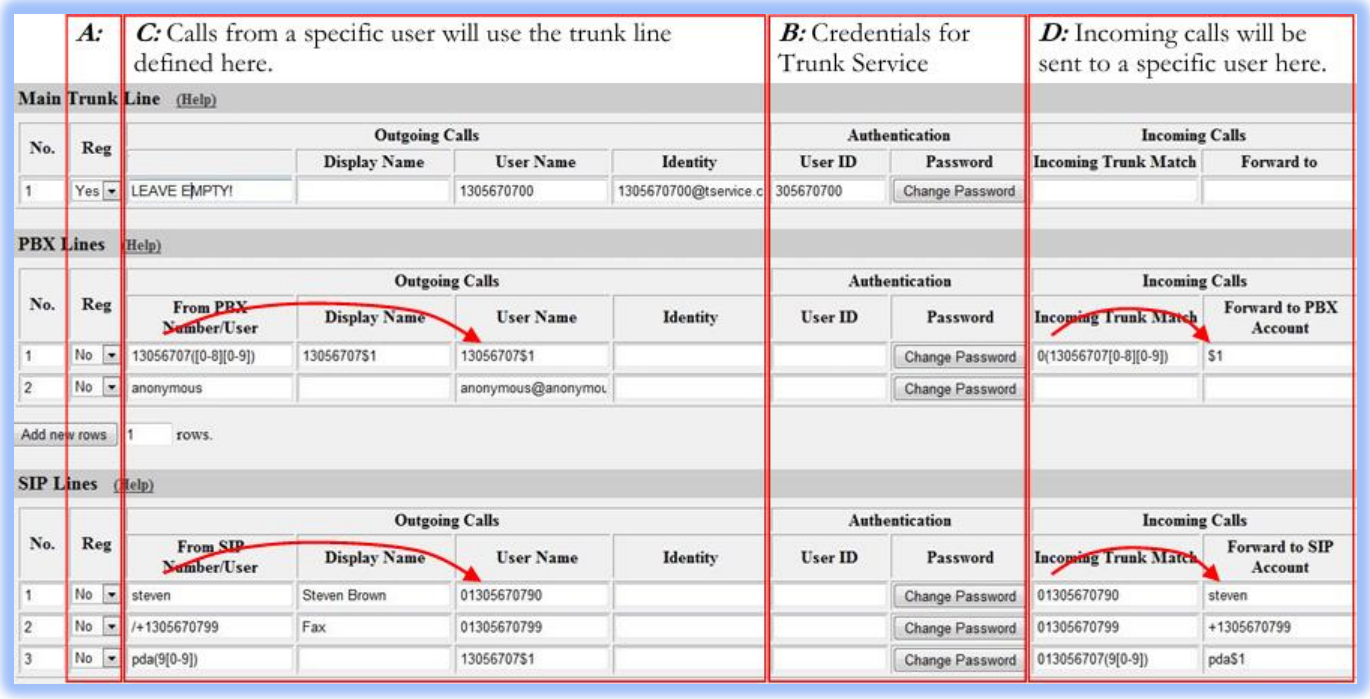
Each SIP Trunk has its own configuration GUI page, where the top portion is the configuration towards the remote end (e.g. a SIP trunking provider that we have defined at SIP Trunk 4 or another PBX environment that we will exemplify tie trunking to at SIP Trunk 2).

The bottom portion is the configuration towards the local PBX, that we at SIP Trunk 4, setup towards:  with its NMSE emulation

and at bottom portion of SIP Trunk 2 and we will re-use the same Mitel MiVoice Connect-Shoretel PBX configuration by:



In the middle portion of each SIP Trunk GUI page, we have:



and understand that outgoing calls are forwarded by the Dial Plan to red-framed column C:, while incoming on a certain SIP Trunk, goes directly to red-framed column D: for a match and forwarding.

In these rows of SIP forwarding, you can use both numbers and SIP names, regular expressions and generic header manipulation to do everything needed, both simple setup and complex fixes to various SIP environments.

Under **PBX lines** you see some usage of regular expressions, and the simplest is (.*) which matches and stores any amount of characters in $1. In section 3.2 of How To use Generic Header Manipulation, you find the full notation for regular expressions, where one example of usage is:

Incoming Trunk Match	Forward to
\+1306(7707[0-9]{2})	0$1
\+1306(7707[0-9]{2})	0$1;user=phone

With the above understanding of SIP routing, let's see how to setup Igacomp's SIParator®:

where the top of SIP Trunk 4 GUI page, handle the connection to the PSTN, which configuration can be as easy as this (although the SIParator® has extensive possibilities to handle any trunk):

Service name:	PSTN	*(Unique descriptive name)*
Service Provider Domain:	80.81.82.83	*(FQDN or IP address)*
Restrict to calls from:	Telavox_Trunks	*('-' = No restriction)*
Outbound Proxy:		*(FQDN or IP address)*
Use alias IP address:	-	*(Forces this source address from our side)*
Outbound Gateway:	-	*('-' = Use Default Gateway)*
Signaling Transport:	UDP	*('-' = Automatic)*
Port number:		
From header domain:	Provider domain	

and at the top of SIP Trunk 2 SIP Trunk 2: IG-LAN;Mitel MiVoice Connect-Shoretel, we handle the connection to the IG-LAN environment, where there is another PBX that we want to integrate with, to allow communication with the same Mitel MiVoice Connect-Shoretel PBX (at the NMSE interface) using extension numbers instead of DID, thus NOT going over PSTN. Notice that the NMSE interface can handle both DID and extension numbers at the same time, which was not possible going through a Mitel vTrunk (or SG device, where a MiVC configured trunk either is for the PSTN or for a tie trunk):

Service name:	IG-LAN	*(Unique descriptive name)*
Service Provider Domain:	10.48.255.1	*(FQDN or IP address)*
Restrict to calls from:	Ingate tie-trunk	*('-' = No restriction)*
Outbound Proxy:		*(FQDN or IP address)*
Use alias IP address:	-	*(Forces this source address from our side)*
Outbound Gateway:	-	*('-' = Use Default Gateway)*
Signaling Transport:	TCP	*('-' = Automatic)*
Port number:		
From header domain:	Provider domain	
Host name in Request-URI of incoming calls:	10.48.112.112	*(Trunk ID - Domain name)*

where the last line is an additional ethernet port configured to connect to IG-LAN, setup at the **Network>All Interfaces** GUI page:

IG_LAN	Static	10.48.112.112	10.48.112.112	16	10.48.0.0	10.48.255.255	Ethernet

The SIP Trunk to the PSTN (typically setup by the startup tool, SUT TG), here at SIP Trunk 4 SIP Trunk 4: PSTN;Mitel MiVoice Connect-Shoretel (where a PBX like the MiVC handles the SIP addressing to and from the PSTN trunk itself, the SIParator typically just forwards the numbers), thus the middle portion the SIP Trunk GUI page may look like:

Main Trunk Line (Help)

No.	Reg	Outgoing Calls				Authentication		Incoming Calls	
			Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
1	No			$(user.name)			Change Password	(.*)	$1

PBX Lines (Help)

No.	Reg	Outgoing Calls				Authentication		Incoming Calls	
		From PBX Number/User	Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to PBX Account
2	No	anonymous		anonymous@anonym			Change Password		
3	No	(.*)		$1			Change Password	(.*)	$1

But at SIP Trunk 2 SIP Trunk 2: IG-LAN;Mitel MiVoice Connect-Shoretel, it is set up to forward any incoming call, **starting with 1 followed by two digits**, to the MiVC PBX at IP address 10.0.1.76 (which is the NMSE interface):

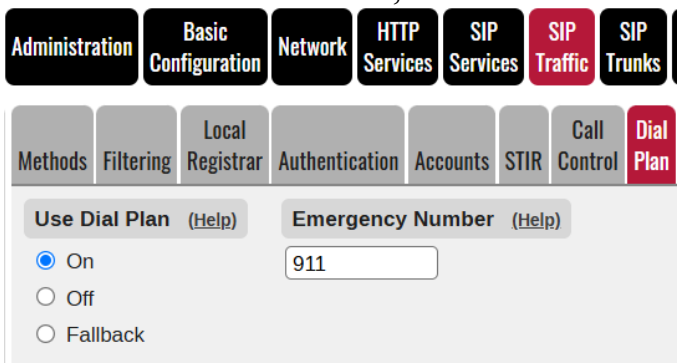
Main Trunk Line (Help)

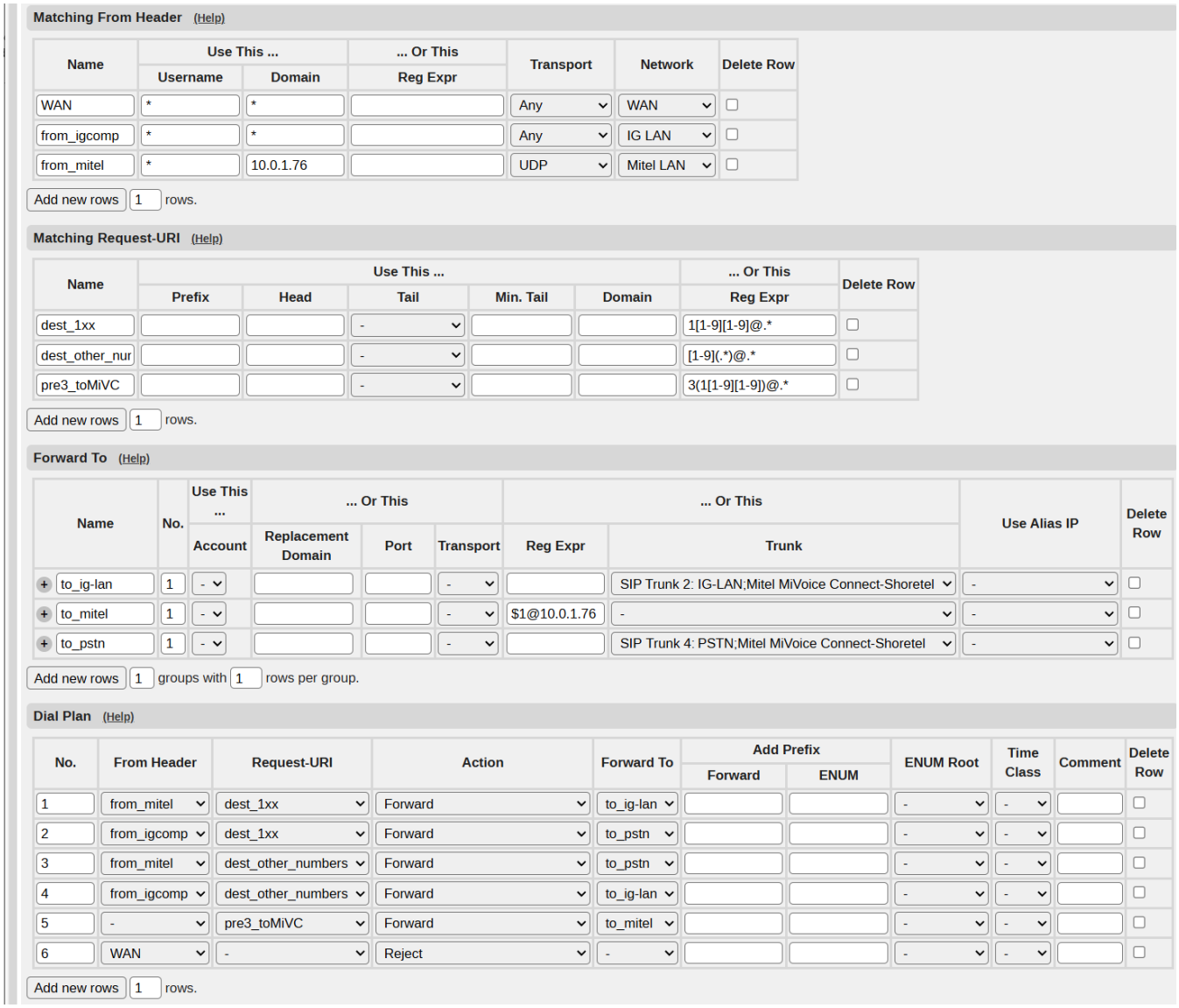
No.	Reg	Outgoing Calls				Authentication		Incoming Calls	
			Display Name	User Name	Identity	User ID	Password	Incoming Trunk Match	Forward to
1	No			$(from.user)			Change Password	(1[0-9][0-9])	$1@10.0.1.76

This is done by the regular expression (1[0-9][0-9]) that evaluates to $1@10.0.1.76.

That NMSE emulation at SIP Trunk 4, will also be used for SIP Trunk 2 that instead if connecting to the PSTN, now connects to the IG-LAN PBX environment SIP Trunk 2: IG-LAN;Mitel MiVoice Connect-Shoretel which applies for INCOMING CALLS.

For OUTGOING CALLS, the Dial Plan in the SIParator® is used



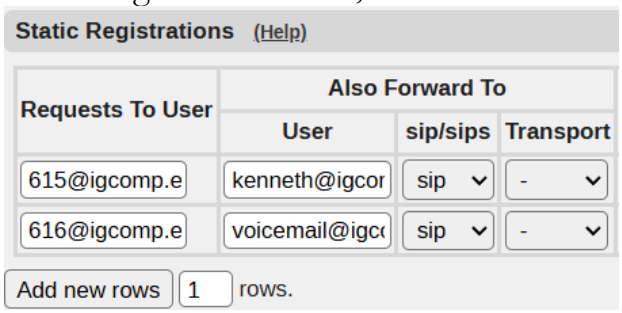


and this setup should make the MiVoice Connect-Shoretel PBX using three-digit extension numbers starting with 1, reachable from the IX-LAN environment, by using prefix 3.

6 Extending Your Mitel MiVoice Connect (MiVC) with more SIP Equipment and Clients by using the Ingate SIParator® Registrar

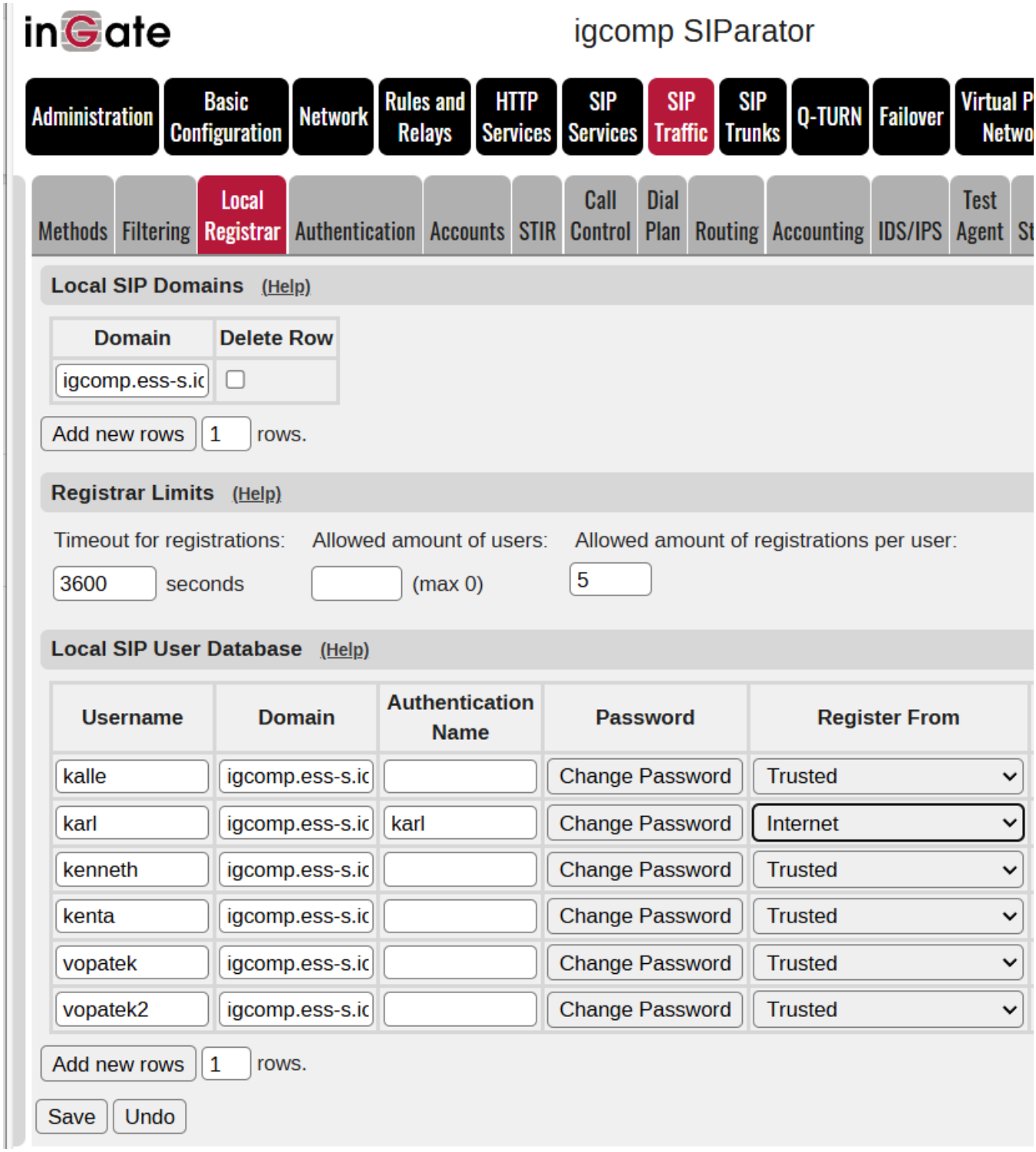
The above tie trunking, explained above in 5 Connecting Your MiVC to PSTN SIP Trunk Providers and Other SIP PBXs (tie trunking), can be used to integrate your MiVC PBX with persons and functionality in the SIParator® itself.

In the Ingate SIParator®, under **SIP Traffic>Routing**. You can define "static registrations":



and if buying SRU licences – SIP Registrar User Licenses – you can use the "User Routing" found in the SIParator® under **SIP Traffic>Routing**, that can be setup for persons or for special SIP equipment or purposes:

The actual SIP registrar in the SIParator® is found under **SIP Traffic>Local Registrar** and on next page you see an example with six users configured:



This is just one example-setup of the registrar in Igacomp's SIParator®.

The setup in previous chapter allows these clients to directly reach use both the PSTN trunk and the tie trunk to the Mitel MiVoice Connect-Shortel.

7 APPENDIX 1: Configuring ACME for Using Automatically Updated Certificates, e. g. Free Let's Encrypt Certificates

Release 6.4.X of the Ingate SIParator® / Firewall SBC added Support for Automated Deployment of X.509 Certificates Using the ACME Protocol. This appendix is mainly imported from the Configuration Guide for Ingate as Teleworker Gateway for Mitel MiVoice Connect and Mitel 6900 phones.

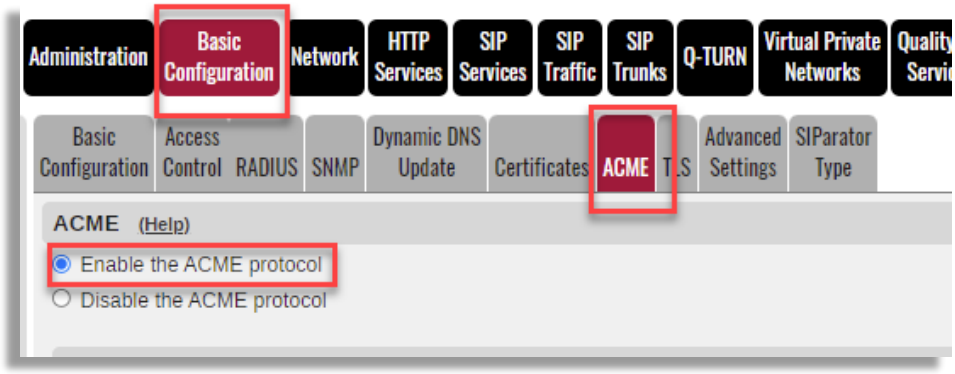
Whenever certificates are required on the public side (the Internet) it is recommended to use automatically frequently updated certificates, such as the free Let's Encrypt certificates The ACME protocol is used to automatically update such certificates. Thus, the certificates in the SIParator provide high security and the certificates do not need to be manually updated over time.

7.1 Enable the ACME Protocol to Allow Self-updating Certificates

(e.g., Let's Encrypt self-updating free certificates)

SIParator® 6.4 added full support to create and manage Let's Encrypt certificates using ACME protocol.

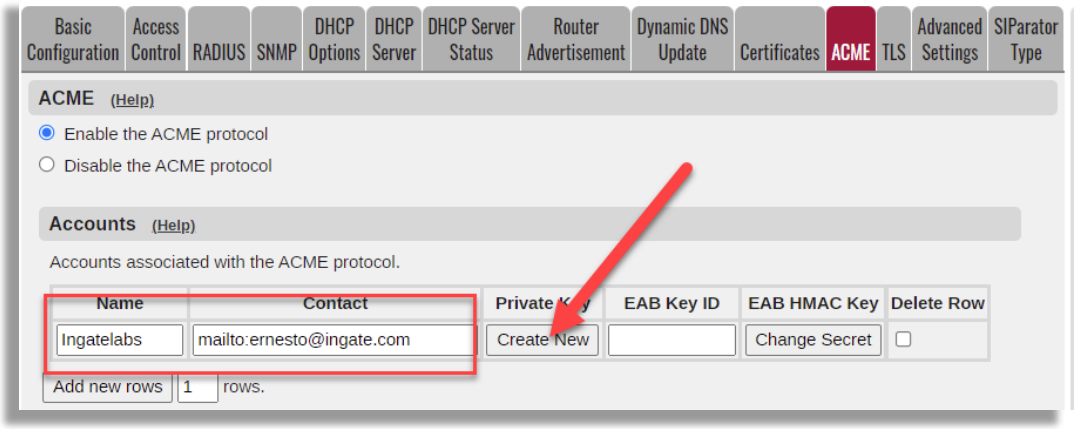
To enable ACME Protocol:



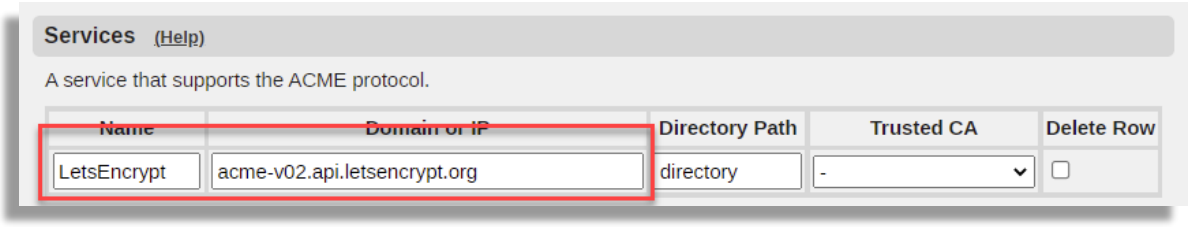
Under Accounts, add a new row, assign a name, fill in the contact information using the following format:

mailto:youremail@yourcompany.com **(i.e.** mailto:ernesto@ingate.com**)**

Once you have completed the contact information click on the "Create New" under Private Key. That will trigger the process to create an account for further use.

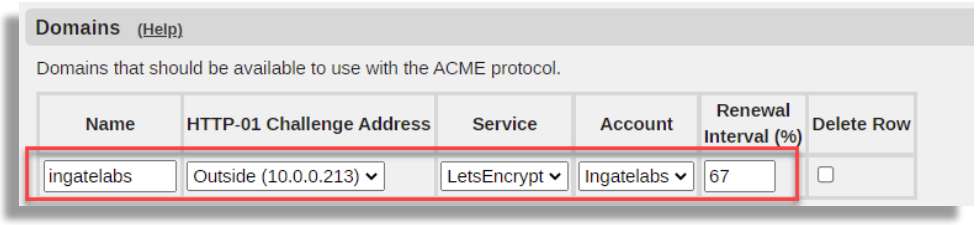


Add a Row under "Services" to point to Let's Encrypt Servers. Assign any name, but use exactly the URL as shown below (acme-v02.api.letsencrypt.org):



Directory Path must point to "directory"

Add a domain row. Here you will associate, via a name, which interface that will be used to connect to Let's Encrypt Servers and receive challenges (In our case the outside interface), which service and Account that will be used for this named domain.



Leave renewal interval at default value of 67%. This controls when the renewal process will be triggered for each Let's Encrypt managed certificate (every 60-90 days).

In this section we will add the private and CA Certificates needed to properly configure the Teleworker Gateway solution.

Just to refresh, private certificates are those the ingate will use to identify itself, while CA Certificates are the ones used by the SIParator® to validate signage of those certificates presented to it, to make sure those certificates can be trusted.

How are certificates used in SIParator® when deploying Teleworkers?

Two main areas of attention must be clear when deciding certificates needed, first all related to SIP signaling, and secondly the ones needed for other secure services mainly based on secure http happening during most of the advanced functionalities on the phones (Provisioning, phone maintenance, phone configuration, operation, CAS based Services among others)

7.1.1 Create Certificates Between the SIParator® and the Remote Phones

Here will be shown how to create the certificates needed for the SIP signaling as well as for the HTTP services.

7.1.1.1 SIP signaling related certificates

Interface eth0 (Inside) will have a certificate signed by HQ Server as explained in Create an HQ signed certificate to be used in the SIParator® internal interface for TLS.

Interface eth1 (Outside) will have a certificate signed by a trusted authority. SIParator® supports integration with Let's Encrypt using ACME protocol and that will make life easier at no additional cost (no need for purchasing signed certificates).

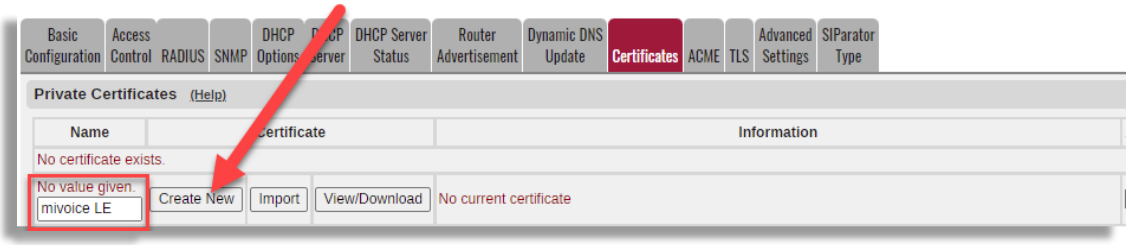
Here we explain how to add Let's Encrypt certificate and then we will explain how to associate both certificates to each interface in the SIP configuration.

NOTE: If you decide to use another 3rd party CA for this Outside certificate, you must assure that the certificate provider is authorized by the Ingate SIParator®, see considerations in section 8 below.

You must have ACME already configured and enabled as explained in Enable ACME protocol (Let's Encrypt) to manage SIParator® external certificate.

- Go to Basic Configuration → Certificates
- Add a new row to Private certificates

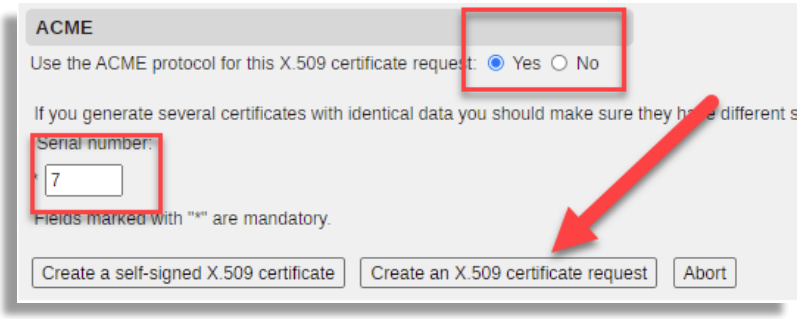
Let's call this certificate "MiVoice LE" (You can assign whatever name you want) and click on Create New



- Fill the information.
  - Expire in days (it doesn't make any difference for Let's Encrypt as they expire every 90 days, but automatically renewed by SIParator®). However, this field is mandatory.
  - Country, Organization, State/Province, Organizational Unit, locality and email. Fill all of them with appropriate information. It is just informational.
  - Common Name (CN) this one must match the FQDN of the SIParator® resolving the public IP. In our case it will be "mivc.ingatelabs.com".

- Let's Encrypt requires Subject Alternate Names extension to be included and DNS must match also the same FQDN mentioned above.

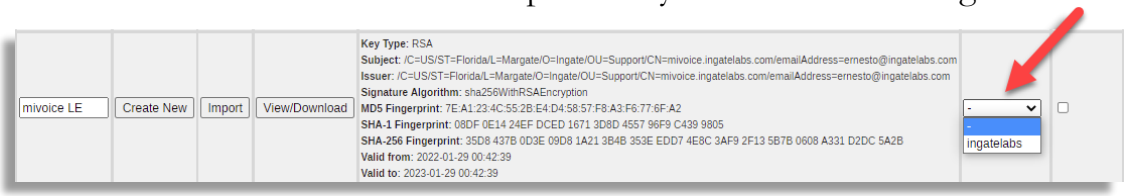
- Leave Key Length and Signature Algorithm on default values
- Enable ACME in the ACME section, assign a serial number if you want and click on create an X.509 certificate request.
- Serial Number is automatically generated, but you can assign any serial you want.



You will see this result screen:

As you can see, a self-signed certificate is generated (it will be used until a signed certificate is received from Let's Encrypt), and also a Signature request is generated to be sent automatically to Let's Encrypt Service.

To make sure the request is sent we need to associate such certificate to one of the ACME created domains. In our case use the previously created domain "ingatelabs"



Save and apply the changes and after a few minutes you will see the certificate already signed.

You can confirm it was signed by Let's Encrypt, has a duration of 90 days, and Domains are properly setup and validated.

8 APPENDIX 2: Using Ordinary (NOT Self-Upgrading Using ACME) Third-Party CA Certificates

This appendix is mainly imported from the Configuration Guide for Ingate as Teleworker Gateway for Mitel MiVoice Connect and Mitel 6900 phones.

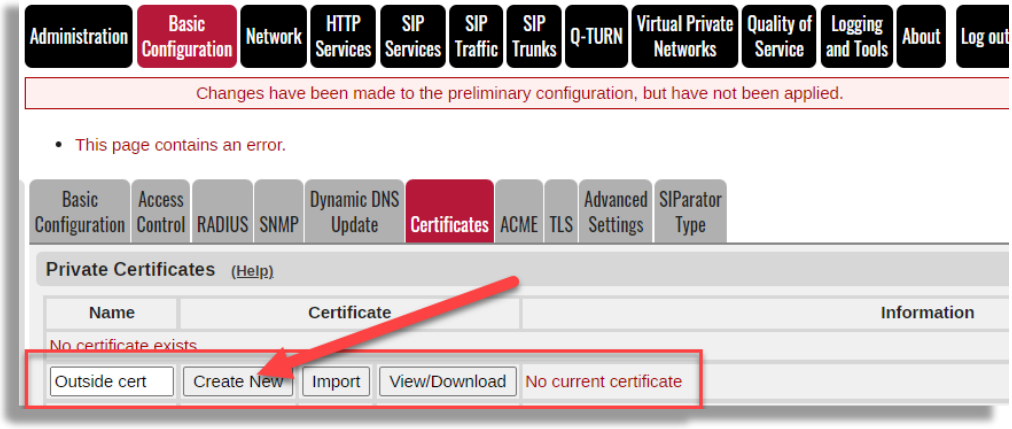
If you select to use a 3rd party CA for the SIParator® external certificates, the ACME protocol is not needed, but you need to specifically add that CA to the SIParator's authorized bundle[3] and there are two possible scenarios to generate the addition to be made:

8.1 Generating CSR (Certificate Signature Request) in the SIParator®

This is a 2 step procedure. First you need to create a signature request in the SIParator®.

8.1.1 Step 1: Produce the Request

Create a new Private Certificate row, and in this example, we will call it "Outside cert".

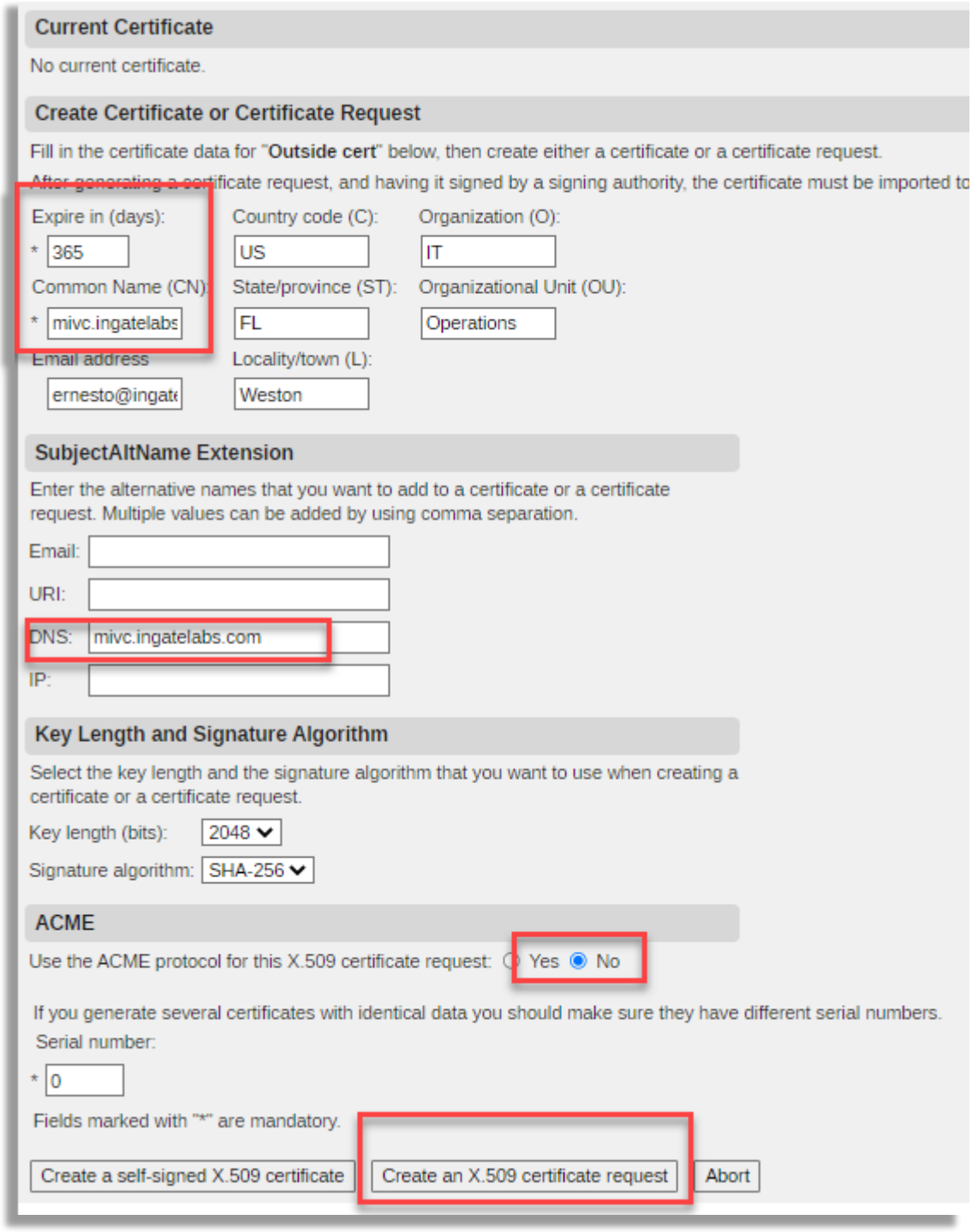


Click on "Create New"

Let's assume we are using mivc.ingatelabs.com FQDN to resolve on SIParator's external public IP

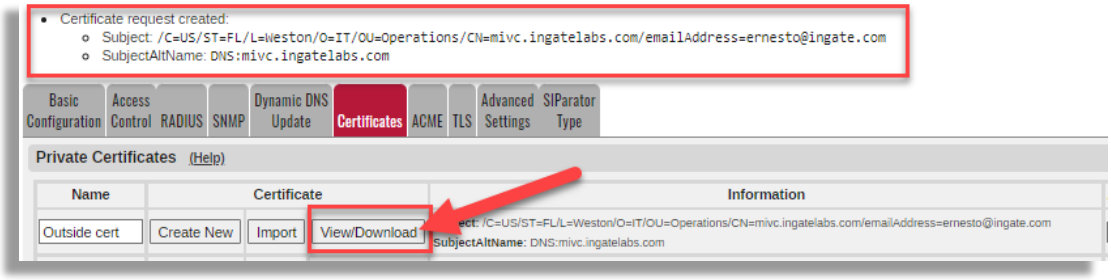
It should look similar to this:

[3] Any 3rd party you choose to use must also be trusted by the Mitel 6900 phones, which probably is the case since most of the known Public Certification Authorities already are included in the MiVC environment. Addition of Private Certification Authorities is not supported by Mitel.

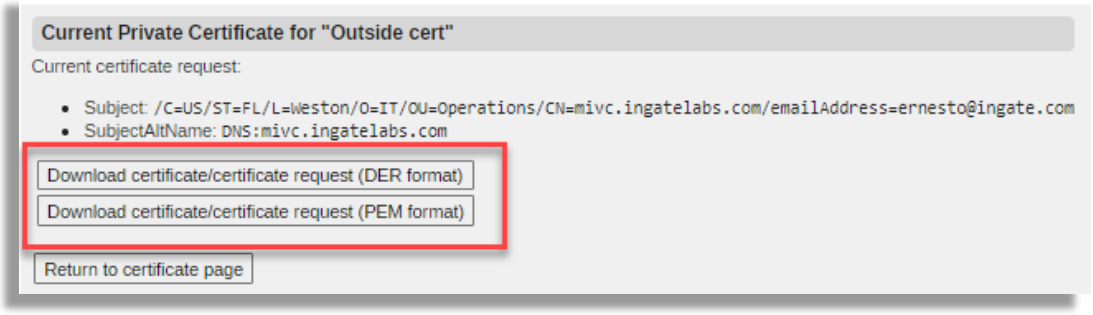


Selecting "Create an X.509 certificate request, and not enabling ACME, will generate a CSR file to be used with the certification authority of your selection (for further signing).

Download then the CSR file:



Click on "View/Download"



8.1.2 Download the file in any of the 2 formats offerings depending on which one better fits the requirements of the CA you selected to use.

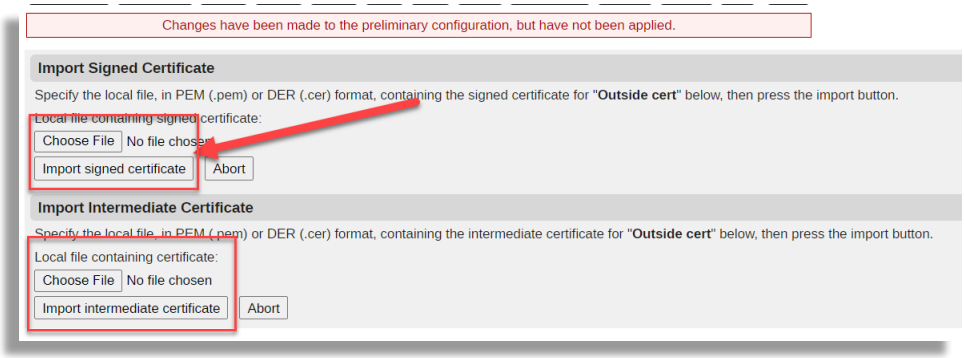
8.1.3 Step 2: Load the CA Signed Certificate

You will receive a set of files from the selected Certification Authority. Those files include one containing the signed certificate.

As the SIParator was the one generating the CSR, private key is already known, so only a signed certificate is needed.

Load the signed certificate using the "Import" button in the certificate request you created.

Then select and load the file in next screen.

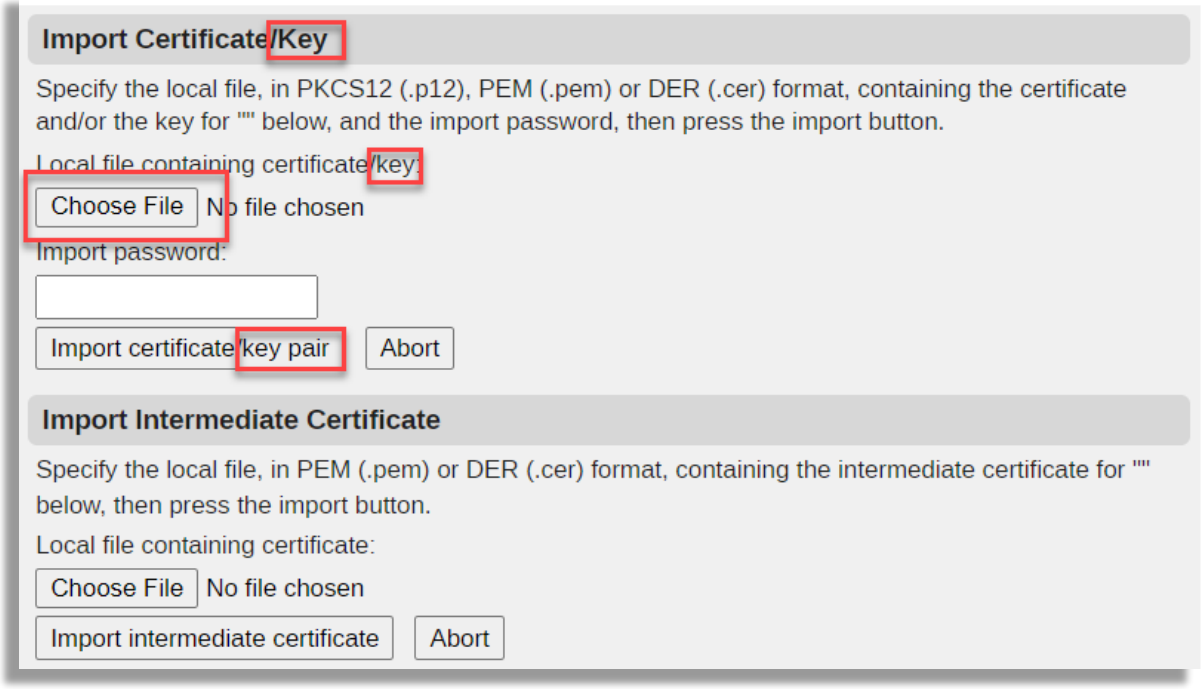


In case you also received a set/bundle of intermediate certificates, they can also be loaded repeating this step, but it is then better to use the options under Import Intermediate Certificates.

8.1.4 Not Using the SIParator® to Generate the CSR

In case the SIParator was not used to create the CSR, you will need to just create a new row in the Private Certificates section and import the file provided by the CA, but now the file that includes the Certificate and Private Key.

Note the same screen (under Basic Configuration → Certificates, after adding new row and clicking "Import") is used to import the certificate and private key in this scenario. It specifically shows "Import Certificate/Key":

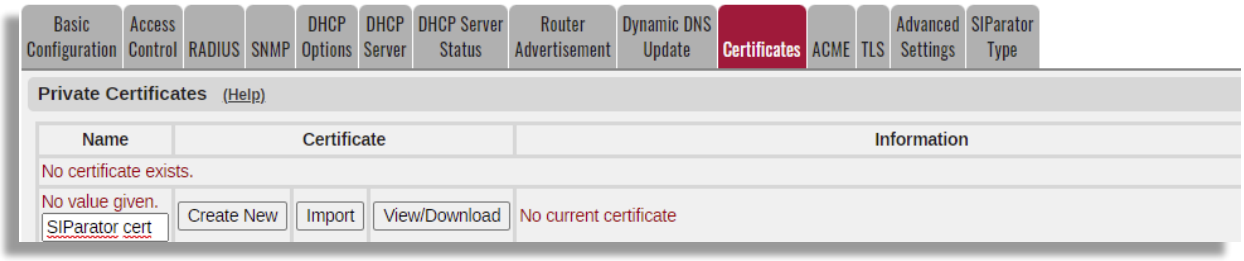


If the file received is protected with a password, make sure you have it and complete in the same screen.

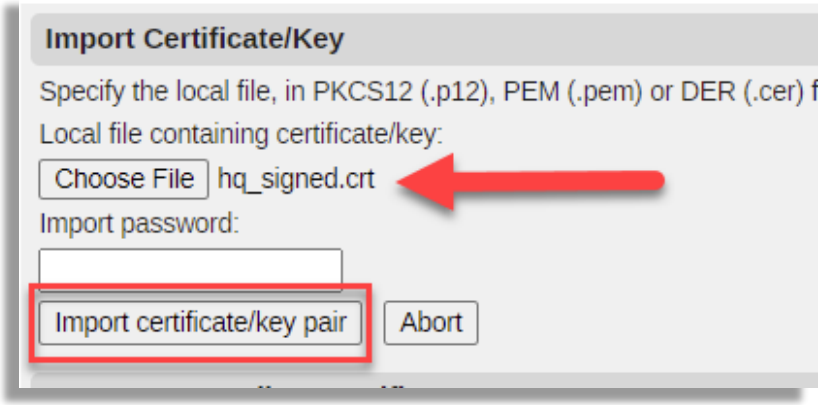
ERR*** ---FROM ELSEWHERE
Once saved, you'll notice that a Download button shows up:

8.2 Load HQ signed certificate in SIParator® for further assignment to Inside interface for TLS

On SIParator® GUI, under Basic Configuration → Certificates, add a new row under Private Certificates:



Select Import button and point to the previously saved "hq_signed.crt" file:



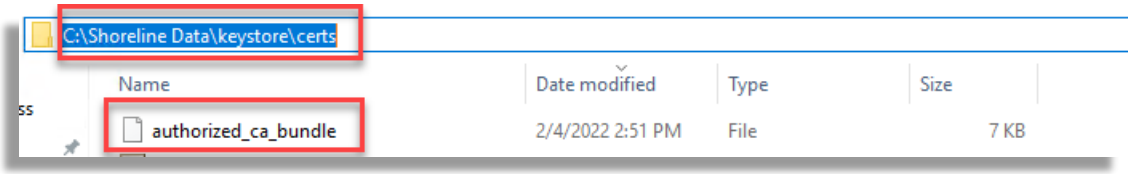
You will see that the Certificate was loaded as expected:

Save and apply the changes.

9 APPENDIX 3: CA (Certification Authorities) Root Certificates

This appendix is mainly imported from the Configuration Guide for Ingate as Teleworker Gateway for Mitel MiVoice Connect and Mitel 6900 phones.

If not already available in the SIParator® in an existing installation, you always need to upload the CA certificates and CRLs used for authenticating peers using X.509 certificates, including SIP peers using the TLS transport protocol. For the specific needs of the Teleworker Gateway functionality of the SIParator®, we need to use the bundle built inside HQ Server under →Shoreline Data/keystore/certs, named "authorized_ca_bundle" to start with.



Save it in your local PC and assign ".pem" extension. Thereafter, you most likely need to add one or both of below authorized CA's before loading the authorized_ca_bundle in the SIParator:

9.1.1 Add the Mitel Root CA for the Mitel Phones

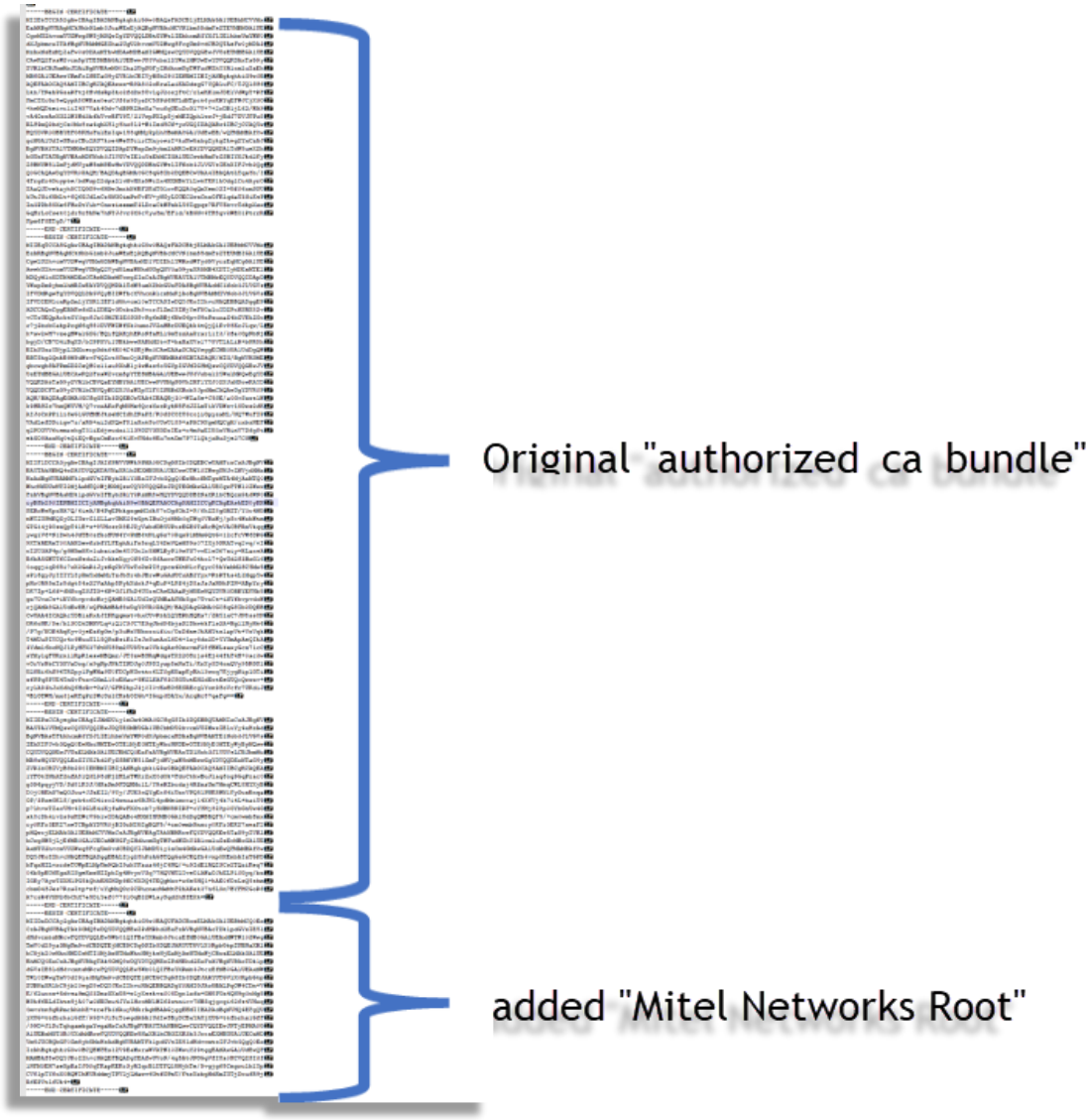
By the time of this document there is one more root CA needed and not included in the bundle downloaded from the HQ Server in the MiVC environment. It refers to the CA needed to recognize certificate built at factory for phone with MiNET firmware loaded.

Using an editor, add "Mitel Networks Root CA" currently missing from the HQ Server bundle and used as the Trusted CA for the certificate built in 6900s with out-of-the-box MiNET firmware.

This root certificate can be obtained from here: Mitel Networks Root CA or here initially .

Copy the content of this last certificate and paste it at the end of the already created authorized_ca_bundle.pem. Save the new file as, let's say, "authorized CA bundle plus Minet.pem".

In MiVC release 19.3 the new merged bundle file must contain 5 certificates and will look similar to this:



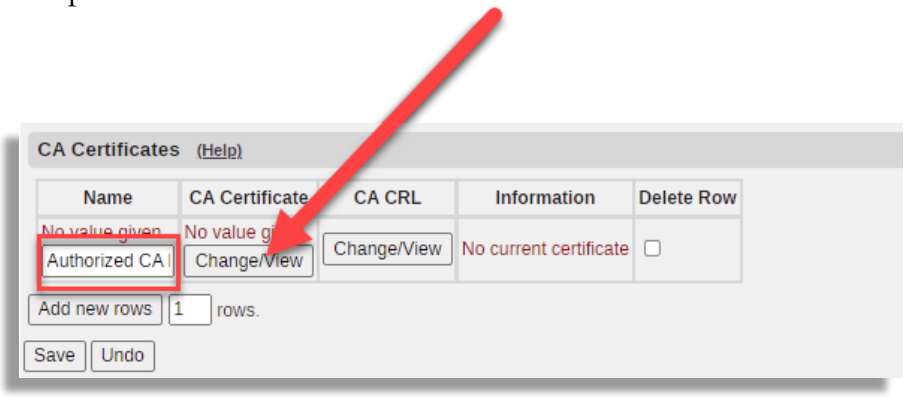
9.1.2 Also Add the CA for the HQ Server, if Using a 3rd Party Certificate for the HQ Server

When using 3rd party CA, you should have available CA root certificates as well as any intermediate certificate needed. You must use the same procedure to also append those certificates in "PEM" format at the end of the bundle you are creating to load in the SIParator®.

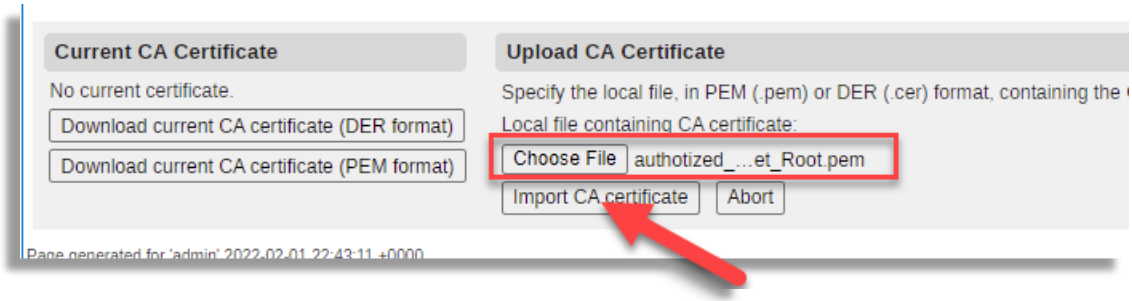
Use the same procedure with an editor as explained in the previous section 9.1.1 to add them before moving to the next step explained in 9.1.3.

9.1.3 Load the Created Bundle into the SIParator®

Load the new merged bundle in CA Certificates in the SIParator®. Name assigned in this example "Authorized CA Bundle":

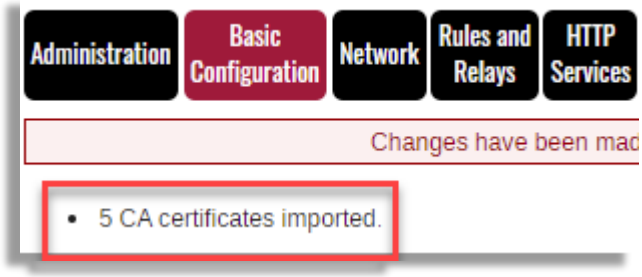


Click on Change/View:

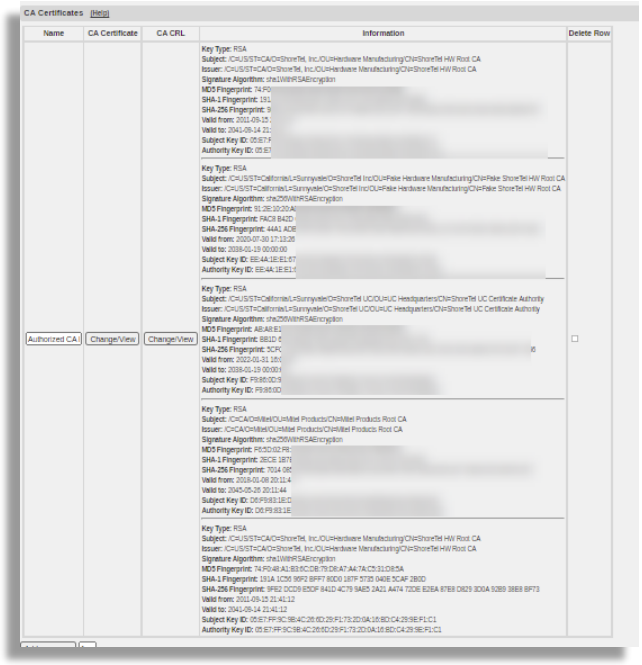


Choose the file and click on Import Certificate.

You should get this result:



and:



NOTE: If you also added 3rd party CA Certificates and Intermediates, the total number of imported certificates should show 6 or more.

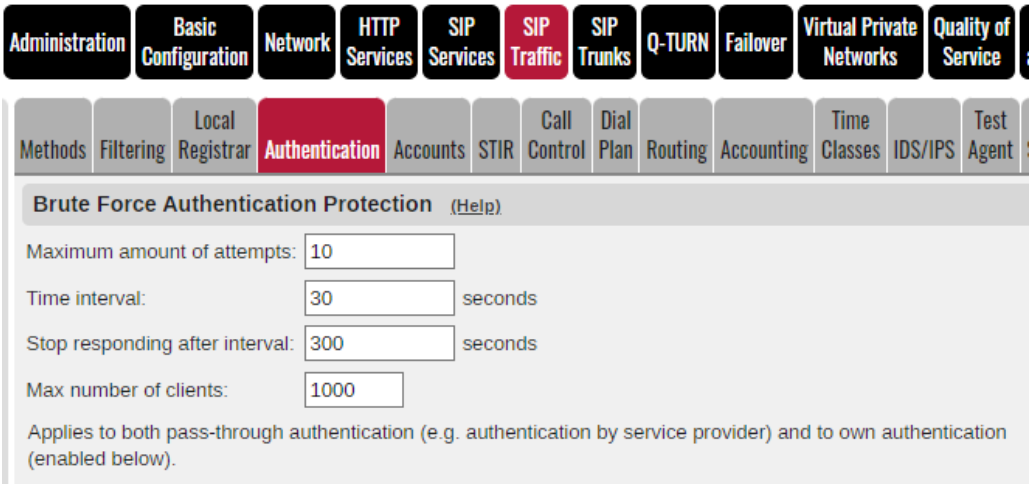
At this point you are ready with certificates.

10 APPENDIX 4: Useful Features in The SIParator

This appendix is mainly imported from the Configuration Guide for Ingate as Teleworker Gateway for Mitel MiVoice Connect and Mitel 6900 phones.

10.1 Add SIP Brute Force Authentication Protection

Since the Teleworker Gateway has to listen to SIP communication on standard 5061 port for TLS from the public Internet, it is advisable to protect from malice authentication attempts. The following configuration under SIP Traffic → Authentication is suggested:



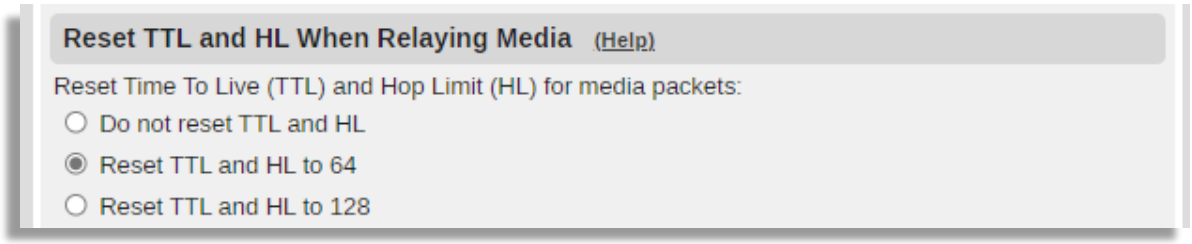
If the Brute Force Authentication is already configured for the Ingate SIParator® where the Teleworker Gateway function is to be added, judge if it is best left as already setup. At very large installations, judge those limits (which is per IP address trying to authenticate) for normal usage.

10.2 Assure that TTL for Media Packets is Enough for Remote Users

One way audio or no audio has occurred because the TTL (counting down for each router hop) has reached zero in complex, long distant scenarios, so the media packets don't reach their destination. This is most likely to happen when one Teleworker phone is calling another Teleworker phone behind another remote NAT, where the media packets have to go via the Teleworker Gateway (instead of directly between the phones).

This has happened with the current version of the 6900s phones (6.2.0.xxx), setting TTL to 64 (verses 128 that would eliminate this unreliability).

In the 6.4.0 version of the SIParator®, a new setting has therefore been introduced under SIP Services → Session and Media:



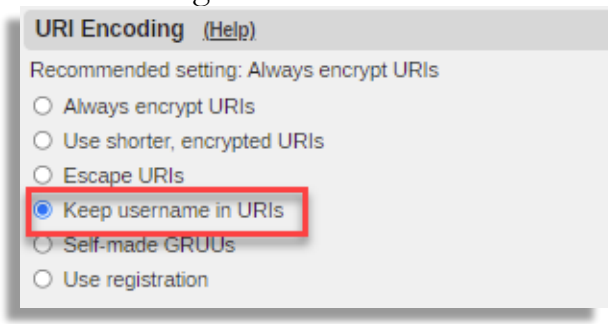
It is recommended that TTL is reset to 64 when the Teleworker Gateway is used with the current version of the 6900s phones. If these phones in a future software release (beyond 6.2.xxx indicated) will increase their TTL to 128, this setting can be set to its default "Do not reset TTL and HL" to restore loop control of media.

10.3 Interop Parameters to Adjust

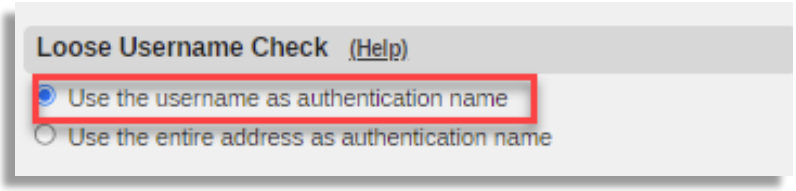
In this section we are showing only the parameters that need to be modified to a different value to the default/recommended setting. If you want to know default/recommended settings, you can review Appendix I.

Adjust or confirm the following parameters under SIP Services → Interoperability:

URI Encoding:

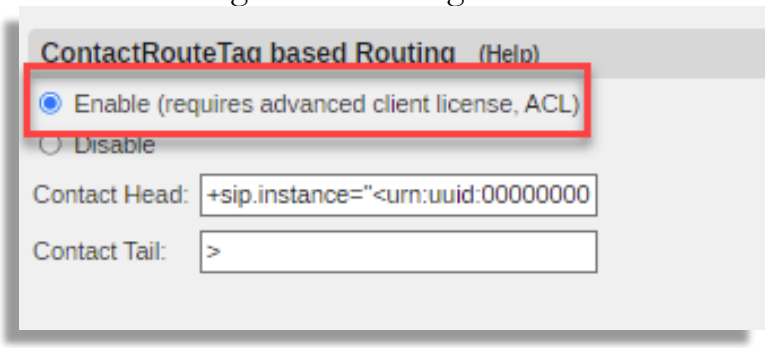


Loose Username Check:



User Matching:

ContactRouteTag based Routing:

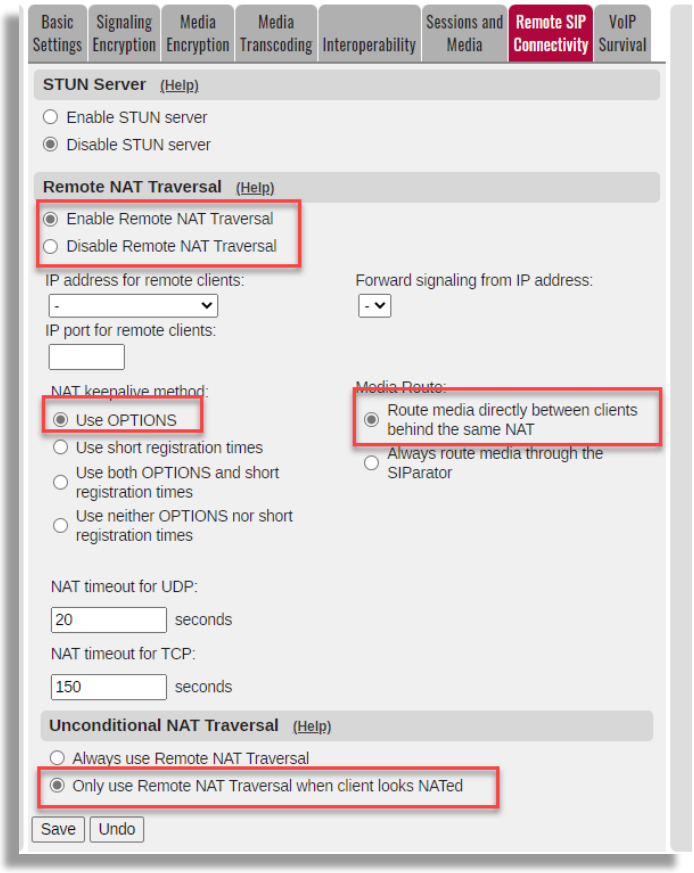


For MiVC, leave the default values as shown on the Contact Head and Tail in this picture.

None of the settings in this section 10.3 should interfere with an Ingate SIParators® configured for ordinary SIP trunking of MiVC. For further details regarding specific adjustments and typical default/recommended values see Appendix I.

10.4 Enable Remote SIP Connectivity

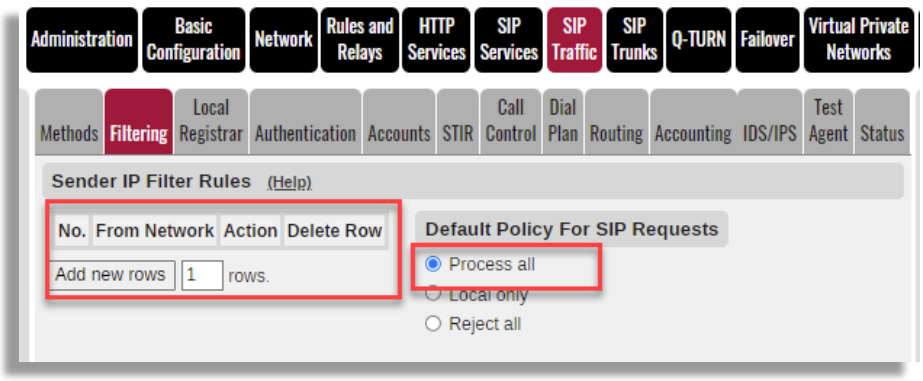
Enable the Remote SIP Connectivity, or Far-End NAT Traversal ("FENT") as it also is called. Change "Media Route:" to "Route media directly between clients behind same NAT (unless some clients are double NATed) and check that the other settings are as shown in the picture below, which are the default values.



10.5 Configure SIP Traffic Filtering to be Without Restrictions

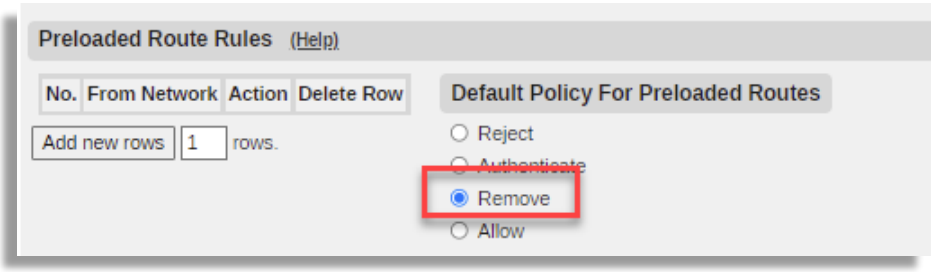
For Teleworkers, where in most cases you have no predictable IPs from where they can connect from, you want to avoid whitelisting of IP address here.[4]

The "Default Policy for SIP Requests" should be left at its default "Process all".



Under the same SIP Traffic → Filtering, we are removing preloaded routes, rather than rejecting them as the default setting is:

[4] If there are other settings already configured here, in an Ingate SIParator® already in use, you need to understand the reason for those and consider whether your intended usage of the Teleworker Gateway can be added to the existing SIParator® or if an additional SIParator for the Teleworker Gateway function must be added.


Preloaded Route Rules (Help)
No.
From Network
Action
Delete Row
Add new rows
1
rows.
Default Policy For Preloaded Routes
Reject
Remove
Allow

11 APPENDIX 5: SIParator® HTTP Services Configuration Exemplified

This appendix is mainly imported from the Configuration Guide for Ingate as Teleworker Gateway for Mitel MiVoice Connect and Mitel 6900 phones.

Release 6.4.X of the Ingate SIParator® / Firewall SBC introduced highly useful additional functionality called HTTP Services. Release 7.1.1 added security rate limiting to the HTTP services, see the reference guide. This functionality comes with the ACL license.

Advanced Client License (ACL) - A New Ingate Per User or Per Seat License
This license makes SIPoWS (SIP over WebSocket, RFC 7118) available for implementing third party WebRTC browser clients, typically using JsSIP, and also adds the advanced and flexible HTTP Services described below, which are much more than ordinary HTTP Reverse Proxy functions.

HTTP Support for File Repositories, Load Balancing and CONNECT Tunnels
A repository defines storage for local and/or remote files available for download via HTTP. Requests to remote HTTP servers can be load-balanced using different schemes and algorithms. HTTP CONNECT tunnels to the Ingate SIParator are firewalled to specific servers (typically on an enterprise LAN).

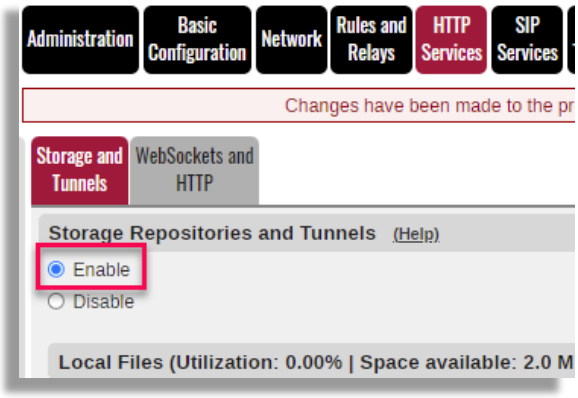
These functions are used by a major PBX vendor for supporting Teleworkers (SIP phone users behind remote NAT/firewalls over the Internet) over MTLS connections with every additional TCP based feature, automatic configuration, and upgrades as if the PBX vendor's phone appliances were connected on the enterprise LAN.

Splitter for Single Port (typically port 443) Usage of HTTP and Any WebSocket Traffic
The configuration of this WebSocket splitter allows selection of various WebSocket protocols to be handled locally and/or remotely. Plain HTTP/HTTPS traffic using the same port is also handled separately.

These advanced general HTTP Services were developed and introduced for the 6.4.0 version of the SIParator® for the required tunneling for the Teleworker Gateway and for other purposes. The HTTP Services are available under the ACL license, both in SIParator and in Firewall mode. There should not be any conflict in using the HTTP Services for the Teleworker Gateway in a SIParator® already in use (typically for SIP trunking of the MiVC or previous Shoretel Shoregear PBX).

This is one of the most important sections of configuration for Mitel 6900 series of phones when used by Teleworkers. Here we will control all advanced services besides the SIP communication. In this section we will enable the "HTTP Connect" tunneling that is able to handle all TCP communication transparently, as well as secure access to MiVC private infrastructure.

First, we will enable HTTP Services, Storage Repositories and Tunnels.



11.1 Hosting startup.cfg in the Ingate SIParator®

The Mitel defined file startup.cfg is requested by the teleworker phone at the initial connection to the SIParator®. Follow these steps to host the file in the Ingate SIParator:

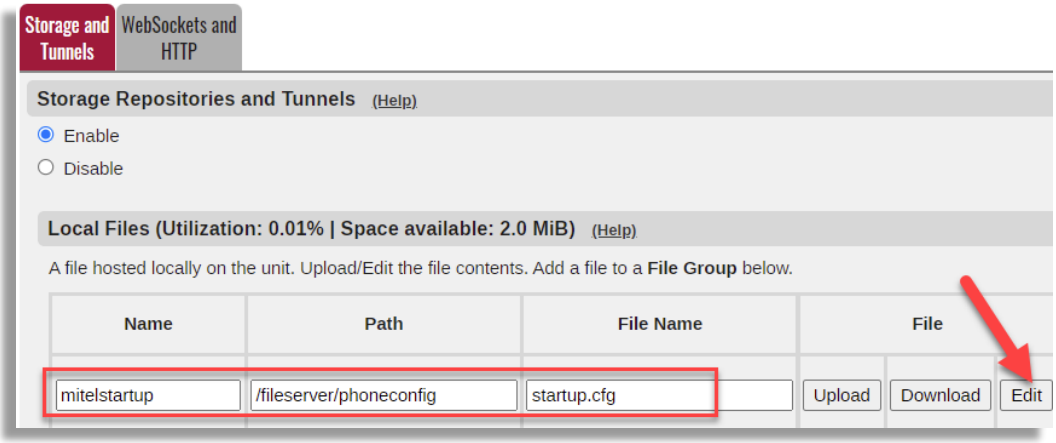
11.1.1 Local Files

A file hosted locally on the unit. You can edit, upload and download a file. Attach a file entry to one or more Local File Groups. A SHA256 checksum file (with the suffix .sha256) is automatically created for each file entry.

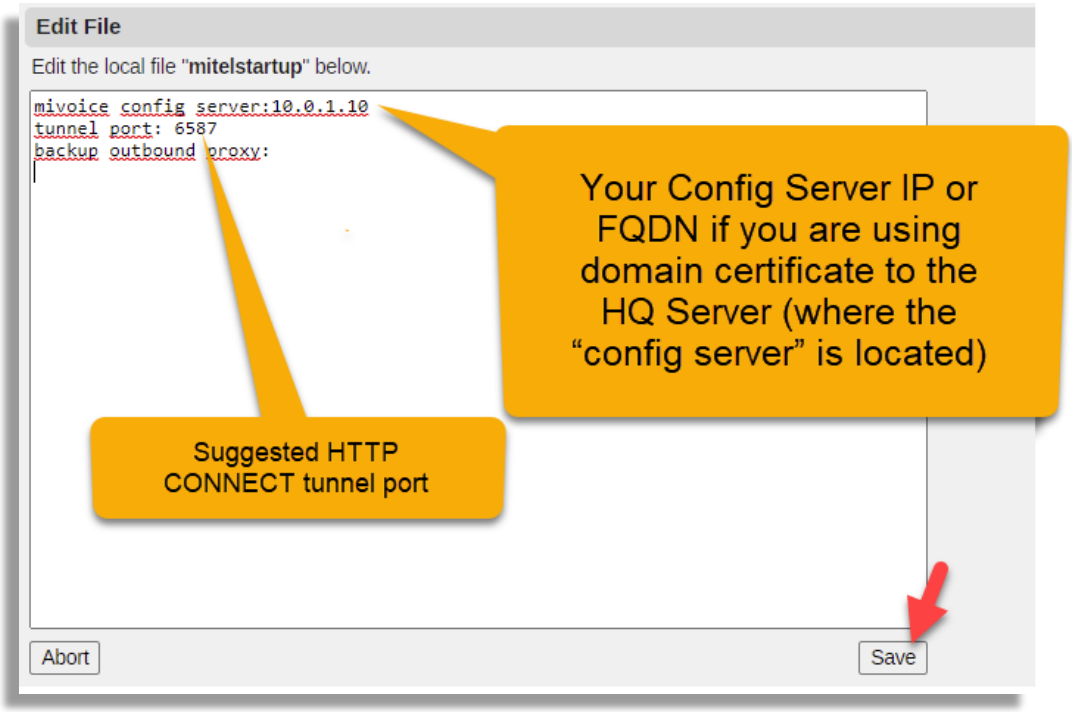
Add a row to Local files to define a locally hosted/cached file.

Let's give it the name of "mitelstartup"

Define the path and the file name it should be found.



Click Edit to type in the file content. You can also upload or download.



Anything after a "#" is just a comment until end of that line.
Three lines following this format are needed:

mivoice config server: <HQ Server ip address/FQDN> [,<secondary IP address/FQDN>[,<….>]]
tunnel port: <port used for HTTP CONNECT tunnel> #use 6587
backup outbound proxy: <leave blank by now – for future use>

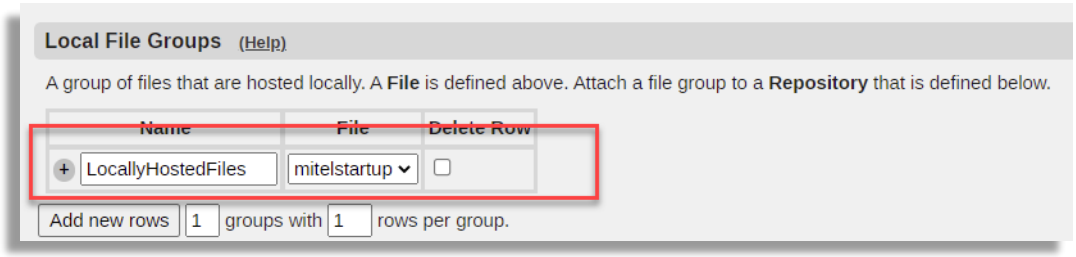
You can use any port number for the HTTP CONNECT tunnel, as far as it is a free and available port from the outside of the MiVC LAN. Ingate recommends ports 6586 (setup elsewhere) for addressing the public side of the Ingate SIParator itself and 6587 for the HTTP CONNECT tunnel, while Mitel's standard is 443 and 444 that are more likely to be occupied for the customer's other usage.

NOTE: For the first line "mivoice config server:", in case you are using a domain certificate (as opposed for a certificate for a fixed IP address) for the HQ Server where the "config server" is located, you MUST specify an FQDN that resolves to the HQ Server private IP in the MiVC environment, rather than its IP address. Mixing FQDN and IP address will cause FAILURE. Also notice that an FQDN for the HQ Server must be resolved in a local DNS server, see section **Error! Reference source not found. Error! Reference source not found.**.

11.1.2 Local File Groups

A group of files that are hosted locally. Attach a file group to a Repositories and/or Tunnels entry.

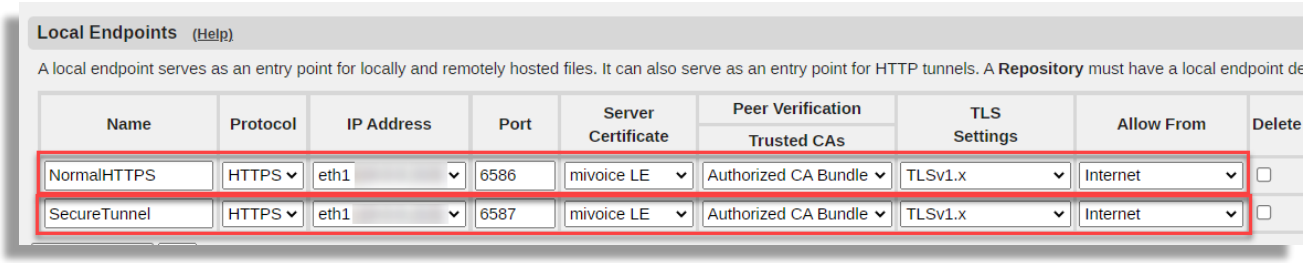
Here you will create a group name to associate to all files that are hosted locally. In our case this group will have only one file, already defined in the previous step.



11.2 Local Endpoints

A local endpoint serves as an entry point for locally and remotely hosted files. It can also serve as an entry point for HTTP connect tunnels. A Repository must have a local endpoint defined.

Here we will define external ports enabled for certain services (Local Endpoints):



For Teleworkers, only 3 ports are needed, port 5061 for SIP, port 6586 for HTTPS and port 6587[5] for the HTTP Connect tunnels (Mitel's standard is port 443 and 444 instead of 6586 and 6587).

In both cases the protocol to select is https and both are going to use the Let's Encrypt previously generated certificate. In both cases for MTLS, peer verification will be used by selecting the Bundle we created before ("Authorized CA Bundle").

TLS Setting must be any option that includes TLSv1.2. In our case TLSv1.x as we already set it up before.

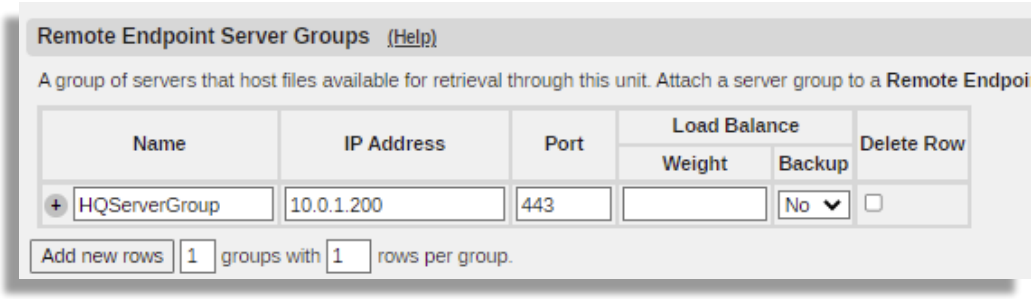
As Teleworkers' IP addresses generally are not predictable, or even in some cases dynamically changing, we will allow access from "Internet"

11.3 Remote Endpoints Server Groups

A group of servers that host files available for retrieval through this unit. Attach a server group to a Remote Endpoint that is defined below. This typically is the Server to reach to obtain version.txt file and latest SIP firmware when the phone has MiNET preloaded firmware.

[5] Configurable in startup.cfg, see 11.1 Hosting startup.cfg

Here we will need to define remote endpoints groups (in this case remote means in the internal network side), destinations we want to enable to be reached. In our case, the only one we want to reach will be our HQ server (10.0.1.200) on port 443.

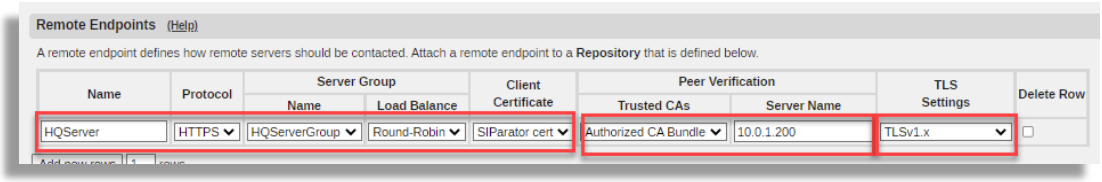


All other internal destinations will be accessible only via http connect tunnels.

11.4 Remote Endpoints

A remote endpoint defines how remote servers should be contacted. Attach a remote endpoint to a Repository that is defined below.

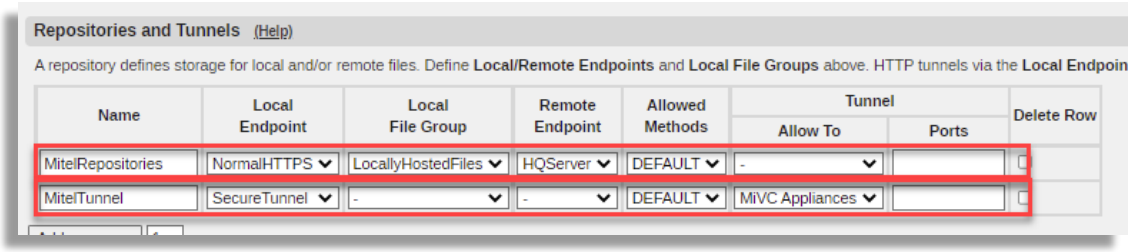
Definition of specific destinations under a group are known as remote endpoints, and we will need to define which protocol will be used and if it is going to be mutual in the case of TLS by completing "Peer Verification". Server Name must match CN on the certificate of the Server connecting to.



NOTE: Make sure the Authorized Bundle includes the MiNET CA certificate and any 3rd Party CA for the HQ Server, as detailed in section 0.

11.5 Repositories and Tunnels

Here we will define repositories to obtain files or tunnels to connect to devices:



To define repositories, “Tunnel - Allow To” must be selected to show “-“.

For the locally hosted files to reach (here only startup.cfg), the appropriate Local File Group must be selected and the HQServer is selected under Remote Endpoints.

Notice we selected DEFAULT Allowed Methods as predefined in the configuration.

Here we created two types of access as mentioned at the beginning of this section, one to be able to reach content via secure MTLS connections and the second to any appliance under Mite Appliances via an HTTPS CONNECT Tunnel terminated at the SIParator® and no restriction to ports.