Ingate SIParator® as Teleworker Gateway for Mitel MiVoice Connect For Mitel 6900 Series of Phones

Configuration Guide

Version 1.01 of this guide

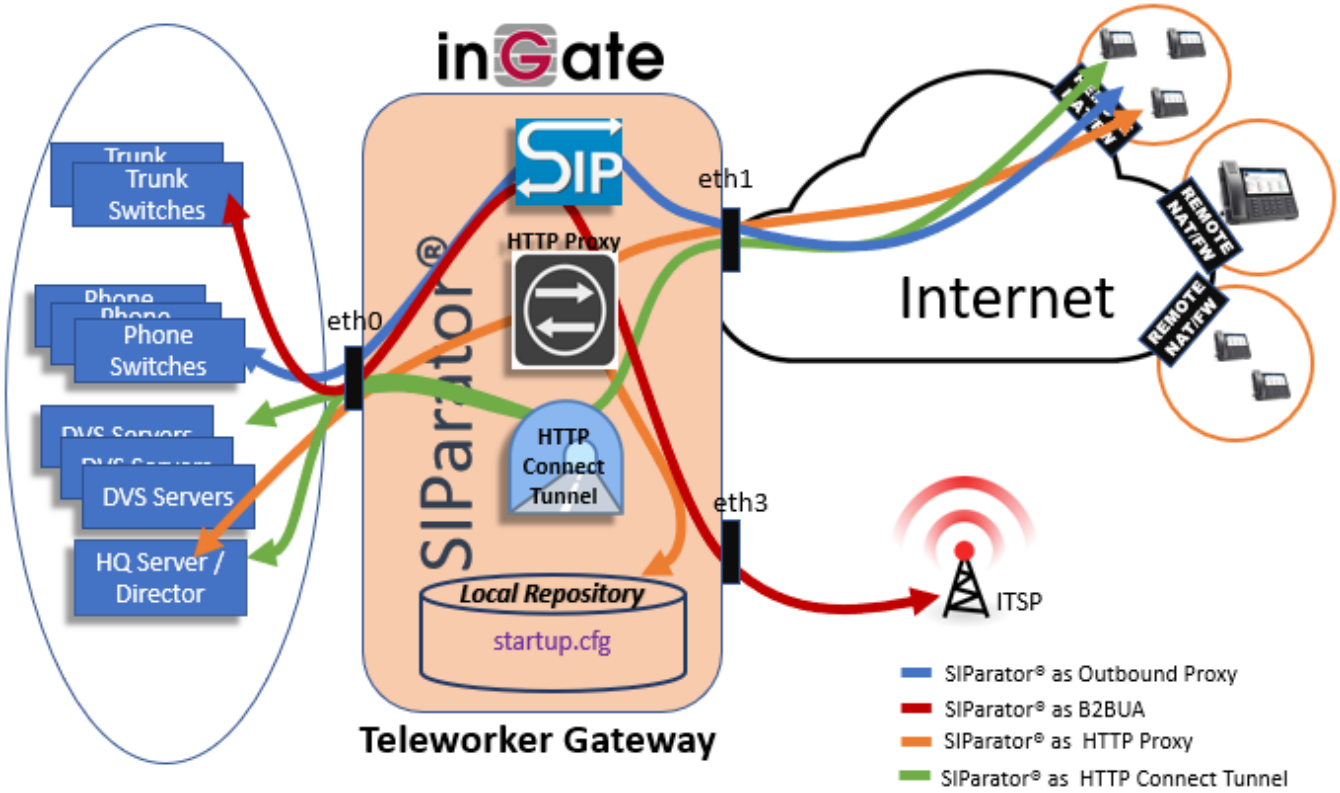
Ingate SIParator® (an SBC/Firewall) version 6.4.1[1] or later
MiVoice Connect 19.3 (Build 22.22.1500.0) or later
Mitel 69xx 6.2.0.1012 or later

[1] Also applies to Ingate's Early Access 6.4.0 SIParator software with patch-6.4.0-mitel-tw-fixes-2.fup

About This Document

This document is a guide on how to configure the Ingate SIParator®, which is an SBC and a Firewall, as a Teleworker Gateway, to allow Mitel Customers and Channel Partners to deploy the MiVoice Connect with Mitel 6900s Phones (the 69xx series of phones) at remote locations (Teleworker scenarios).

This Teleworkers solution for the 6900 series of phones is a joint development between Mitel and Ingate and is based on the architecture explained in section 2.



With this solution, the Teleworkers get the same simple installation procedure, functionality, and behavior as on the company LAN.

Day-1 Remote Installation Support for the Teleworker Gateway

To support deployment, and the by necessity complex Day-1 Installation, including new concepts and the latest certificate technologies, Ingate has agreed with Ernesto Casas, who is known from development of this product and is the main author of this guide, to offer such support from his Florida location through Educronix LLC, under item number IGT-0022-02, ordered through Ingate or directly by Educronix at support@educronix.com and toll free +1 855 866 8854:

IGT-0022-02 Remote Installation Support, per hour (minimum 2h for Mitel Teleworker Gateway), by Educronix (Americas). Additional time beyond the minimum 2 hours is charged afterwards the same hourly rate.

1 Introduction

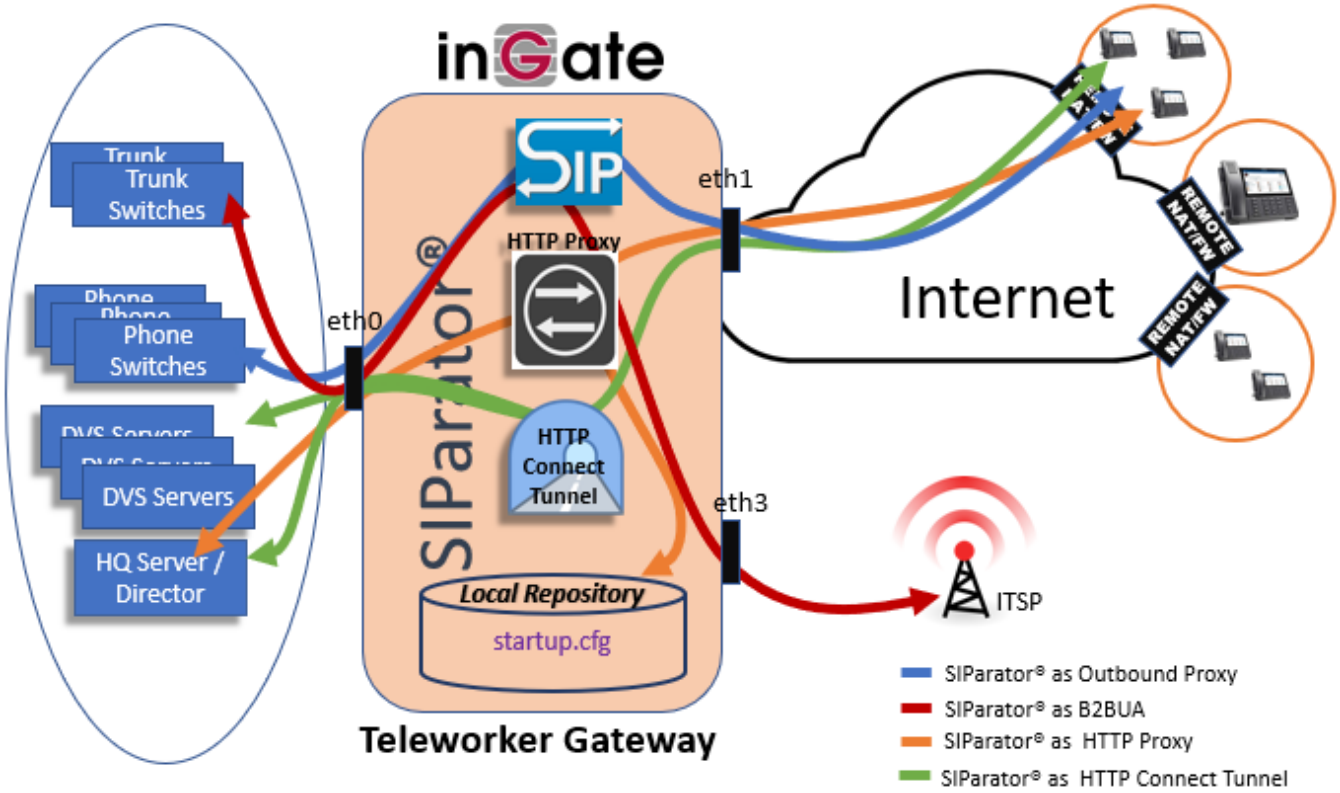
This document describes the steps to configure the Ingate SIParator® (an "E-SBC") as a Teleworker Gateway for the Mitel 6900 Phones to easily (almost automatically) be deployed at remote locations for connection to the Mitel MiVoice Connect (MiVC, previously ShoreTel Shoregear) PBX. All supported Ingate SIParators, including current appliances (most S21, all S22, S42, S52, S82, S95, S97 and S98) as well as the Software SIParator® for VM platforms or cloud can be configured as Teleworker Gateway.

Required Versions and Licenses:
MiVoice Connect (MiVC) PBX (version 19.3 or later).
Mitel 6900 series phones version 6.2.0.1012 or later.
Ingate SIParator® 6.4.1 or later with one ACL license for each remote user (each Teleworker), new MiVC bundles with Teleworker capability, includes the ACL license for the Ingate Teleworker Gateway. Standalone ACL licenses can also be provided.

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

2 Ingate SIParator® as Teleworker Gateway Explained

Teleworkers solution for 6900s series is a joint development between Mitel Networks and Ingate Systems AB, and is based on the following architecture and concepts:



With this solution, the Teleworker gets the same simple installation procedure, functionality and behavior as on the company LAN.

SIParator® architecture includes 4 built in key components for MiVoice Connect Deployments:

1) A full SIP Proxy that will act as outbound proxy for the purpose of all SIP dialogs between Teleworker end points and SIP infrastructure (i.e. Phone Switches).
2) A B2BUA for all SIP traffic with ITSPs for SIP Trunking.
3) An advanced HTTP Proxy that will be used in secure mode (MTLS) for initial parameters needed via a local file maintained in the SIParator® known as "startup.cfg" (contains configuration server address and port to be used for the HTTP Connect tunnel).
4) A HTTP Connect tunnel (MTLS) termination point to build a seamless communication channel between the Teleworker end point and all MiVoice Connect infrastructure sitting or reachable from the SIParator® inside interface (eth0) (i.e. any MiVoice Connect Server, DVS, CAS, etc.).

Initial upgrade from factory loaded MiNET firmware is also included in the solution for best out-of-the-box experience of 6900s phones.

Starting on MiNET firmware version 1.6.0.25 here is the sequence of events happening:

1) When booting up the phone, from the TUI menu, MiVoice Connect is selected.
2) Ingate public FQDN is entered as the configuration server and an MTLS connection is established.
3) The phone requests version.txt file to identify SIP firmware version needed.
4) Firmware is downloaded by the phone via https.
5) The phone saves configuration server information to be used after reboot.
6) After reboot, the phone tries to get hq_ca.crt via http, which will fail in Teleworkers scenario.
7) The phone then initiates an MTLS connection to request startup.cfg file from the SIParator®.

Referring to the previous diagram, all this out-of-the-box sequence happens using HTTP services built into the SIParator® in version 6.4.0 or later.

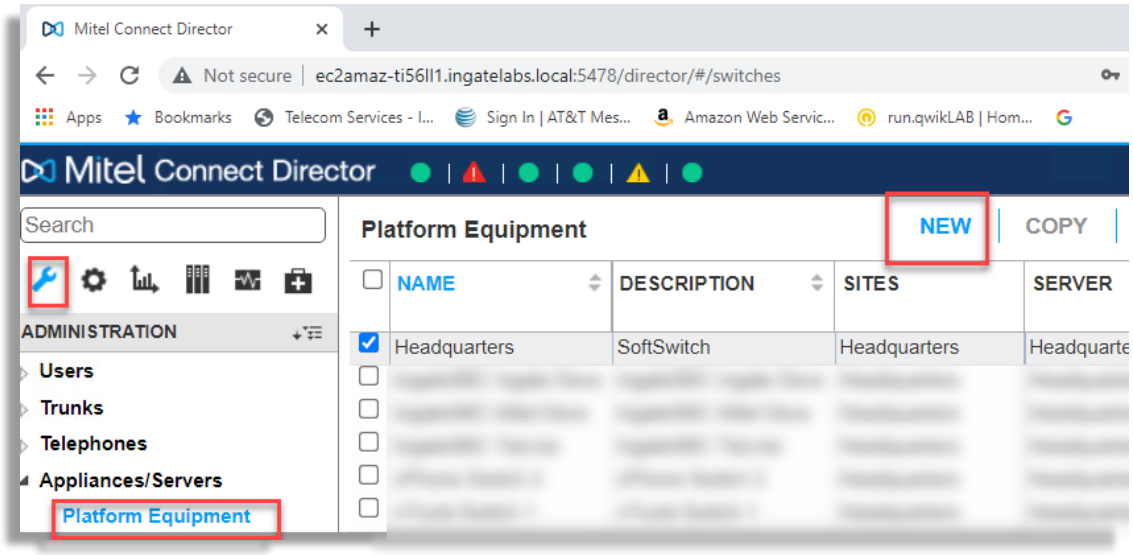
3 MiVoice Connect (MiVC) Configuration

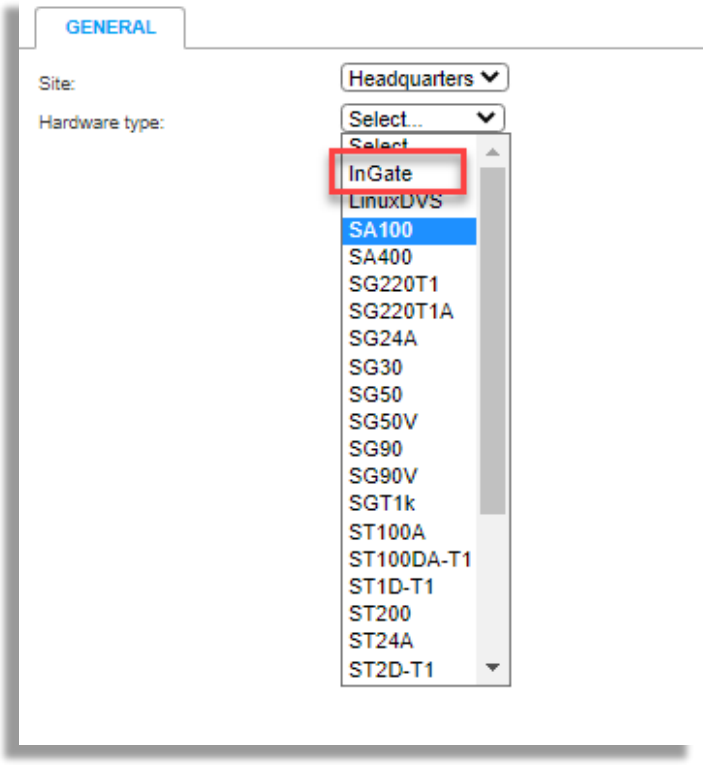
Current Build: 22.22.1500.0

This document doesn't include instructions on how to setup MiVoice Connect, but only the additional elements needed to add Ingate SIParator® as a Teleworker Gateway in the deployment.

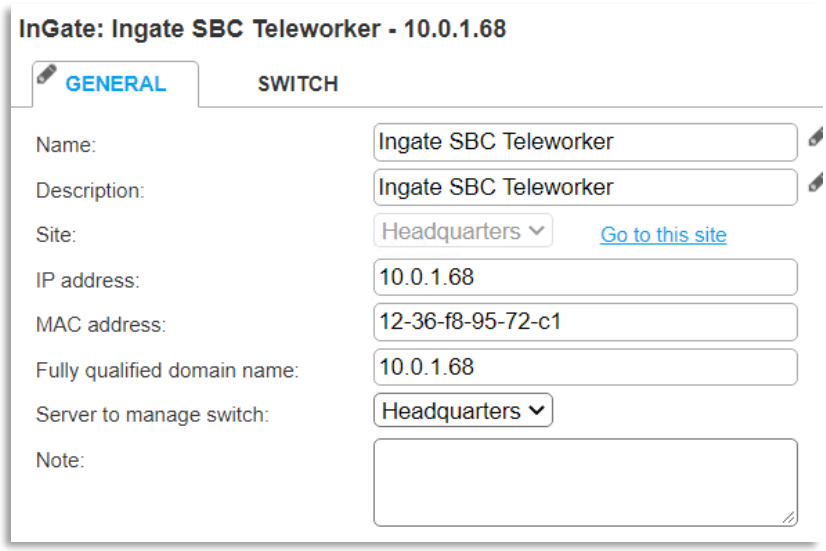
3.1 Add Ingate SIParator® to MiVC Using the PBX "Director"

Using Director Interface in your HQ Server go to Administration under Appliances/Servers → Platform Equipment, add a new appliance (SIParator®)



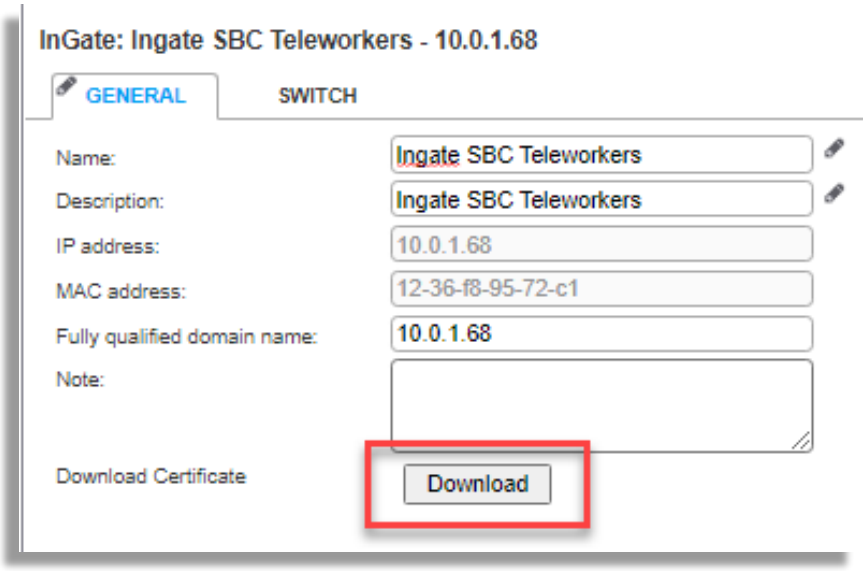


Select Site, in our case it will be "Headquarters" and in Hardware type pull down and select "InGate". Fill in the information including the MAC address and IP address of the internal interface of the Ingate SIParator®.



Press Save and it should show in your MiVoice Connect platform equipment table.

Once saved, you'll notice that a Download button shows up:



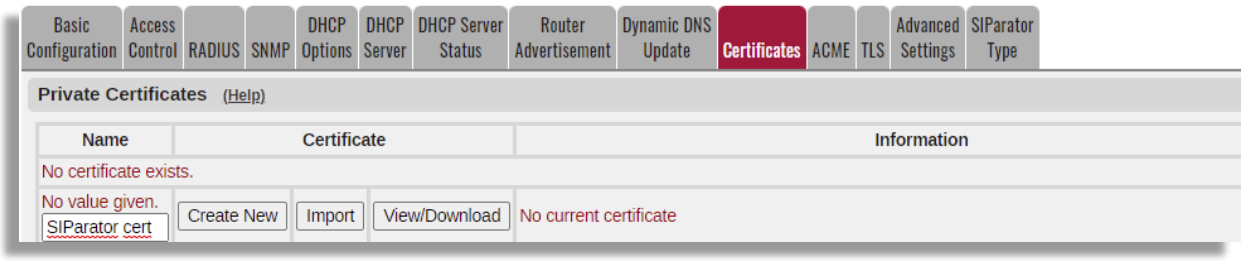
Use this button to download the HQ signed certificate that will be used later for TLS on the inside interface of the SIParator®.

It will show up to easily copy and paste in any ascii editor to saving locally in your computer, or you can also locate the key and certificate files in the indicated folders in the screen.

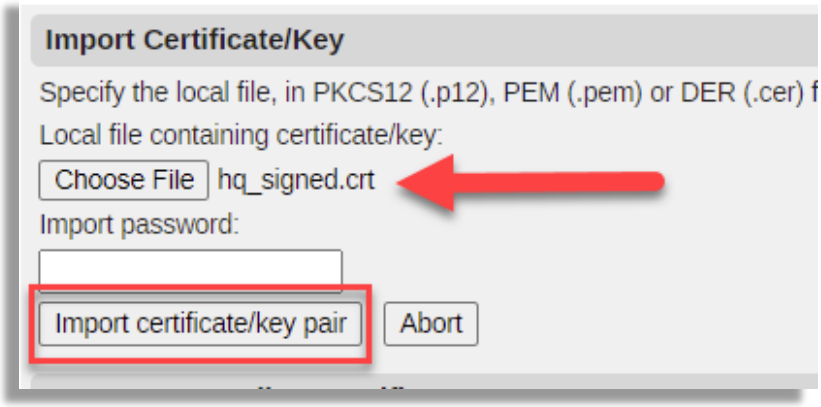
Let's create/save the file as "hq_signed.crt" using copy and paste in Notepad++.

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

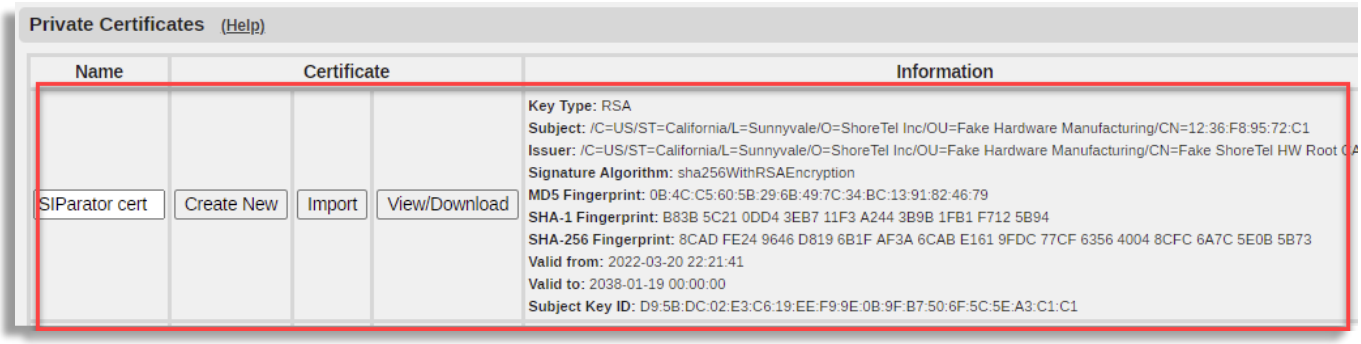
On SIParator® GUI, under Basic Configuration → Certificates, add a new row under Private Certificates:



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.

4 SIParator® Network and Combined Functions Concerns

If the Ingate SIParator® is already in place (typically used for SIP trunking), the Teleworker Gateway functionality can in most, but not all, cases be added. However, for various reasons (frequently commented below), the Teleworker Gateway as a separate function for the Ingate SIParator®, must be regarded as the standard and guaranteed installation.

In a critical live SIParator installation, especially if complex, you should consider whether it is worth to reconfigure the existing SIParator® to also include the Teleworker Gateway functionality, rather than adding an additional SIParator® for the Teleworker Gateway. SIParators® installed for SIP Trunking, with its WAN connection to the real Internet (not the ITSP's private IP pipe), already using TLS over port 5061, cannot also be used as Teleworker Gateway, while SIP Trunking over the real Internet using UDP (or TLS over another port than 5061), can add the Teleworker Gateway without network reconfiguration. Other WAN network connections (typically to an ITSP's private IP pipe - not routable to the real Internet), will require network reconfiguration to be able to add the Teleworker Gateway functionality.

4.1 Required Network Considerations for the Teleworker Gateway

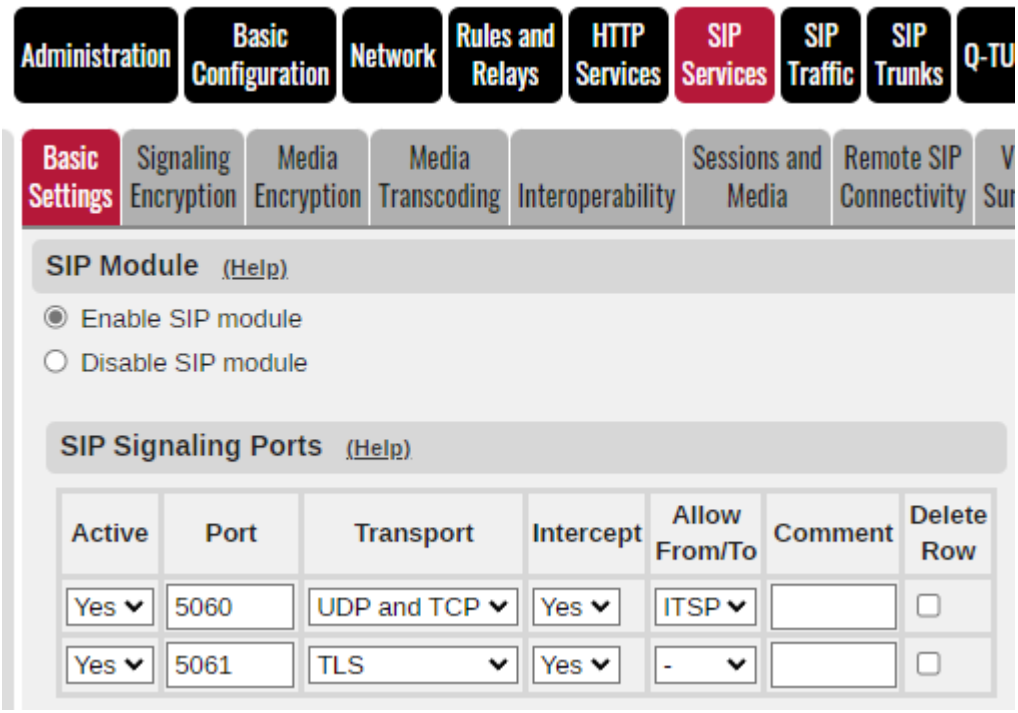
The Teleworker Phones connect **over the Public Internet** to the Public IP address of the SIParator® using MTLS and Let's Encrypt' s self-updating certificates for security. All remote users must be able to use the SIParator's SIP proxy for the Teleworker Gateway functionality, but few others should be able to use the SIParator's SIP proxy.

4.2 Combining Teleworker Gateway with SIP Trunking SIParator®

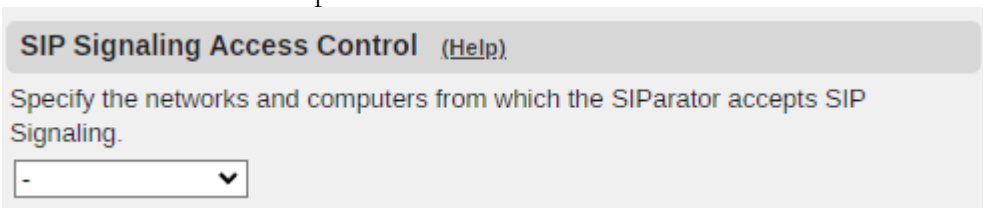
There are thousands of Ingate SIParators used for SIP trunking of PBXs, but the access to the SIParators is most often limited by various means, to avoid misuse of the SIParator's SIP proxy. An existing Ingate SIParator may either be connected and configured to SIP trunk over the Internet or over the ITSP's private network, on private IP addresses for the SIP trunking service, the private IP-pipe here called "SIPtrunkingIPpipe".

4.2.1 Teleworker Gateway with SIP Trunking Over the Public Internet

The SIP Services → Basic Settings sets up the IP addresses allowed for SIP Services. From SIParator® version 6.4.0, you can set up SIP Trunking allowed from/to the ITSP network, as shown at row one of the table in this picture, while allowing TLS at port 5061 for the Teleworker Gateway over the Internet by leaving the "Allow From/To"-column with "-" at row two:



(In previous releases of the SIParator firmware, there was a single setting applying to the whole table, so the two rows could not be separated:



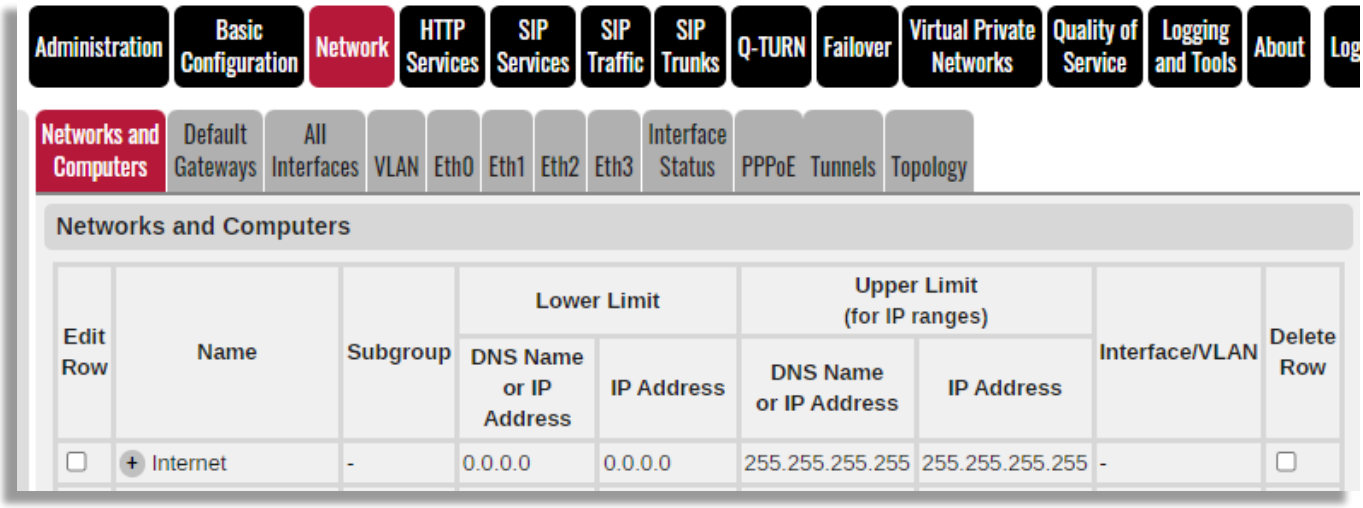
If there were something filling this field in a pre-6.4.0 version of the SIParator, assure that this is entered in row one, representing the SIP trunking service.)

Also notice, that you CANNOT combine both Teleworker Gateway functionality and SIP trunking in the same SIParator®, over the same TLS transport using the same 5061 port. The transport protocol or port has to be different to allow combining in the same SIParator®.

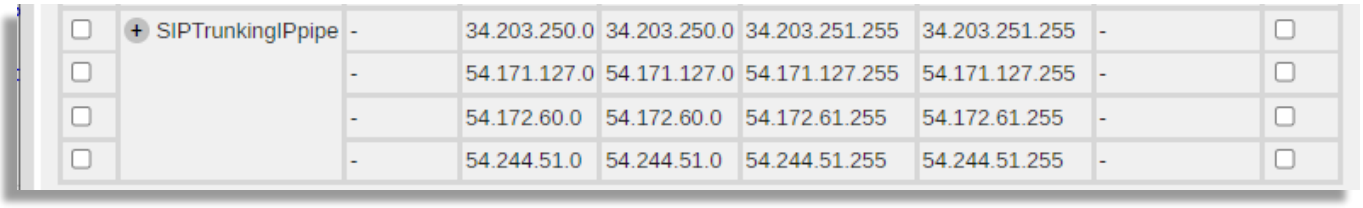
4.2.2 Teleworker Gateway with SIP Trunking on a Private IP Pipe

Since the Teleworker Gateway must be connected to the real Public Internet, the SIP trunking on a private network, cannot be connected to the same Ethernet port 1. Here it is exemplified how the SIP trunking function can be moved over to Ethernet port 3 using the SIParator's "Additional Default Gateway" configuration:

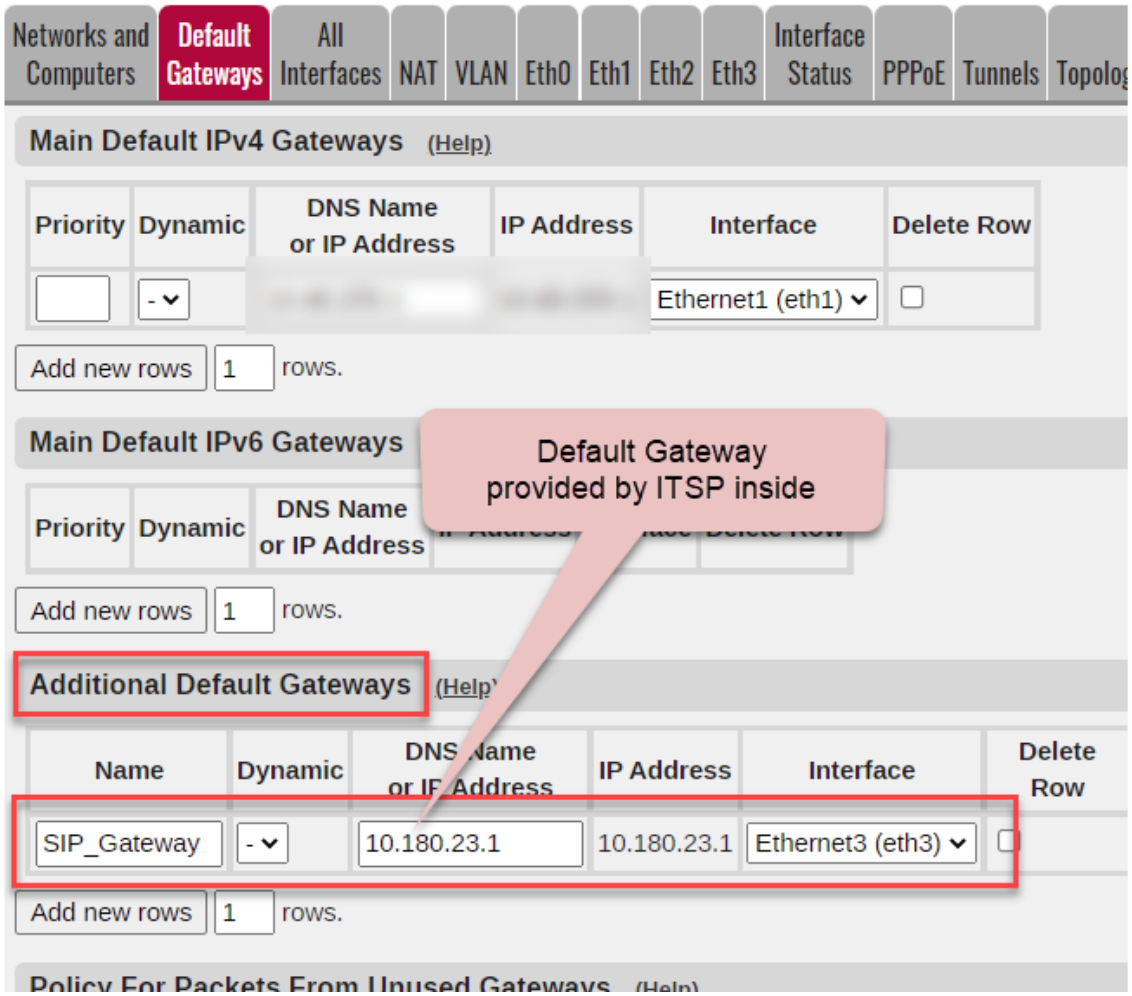
a) Locate the IP addresses that the ITSP uses for its SIP trunking service under Network → Networks and Computers (here "SIPTrunkingIPpipe"):



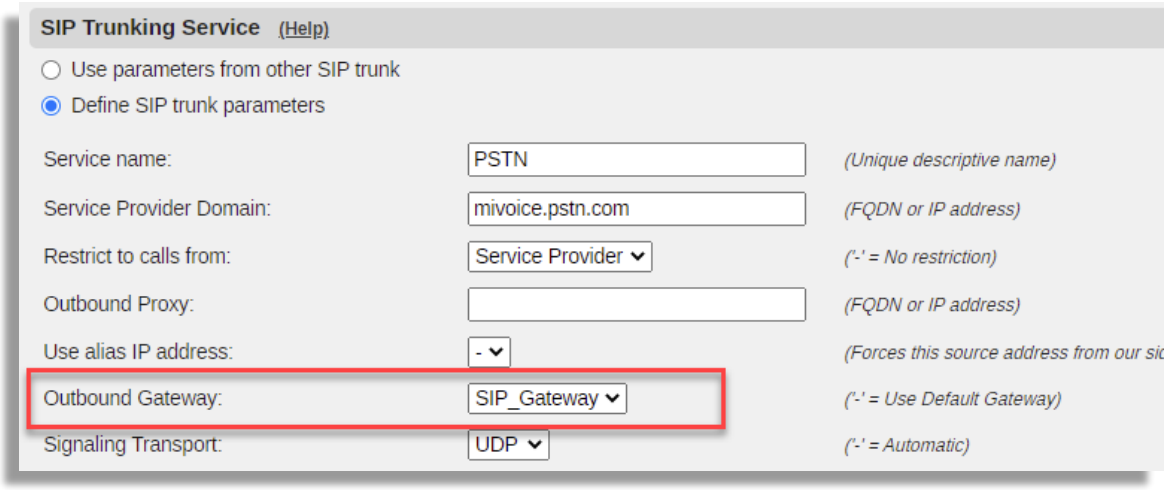
…



b) Under Network → Default Gateways, setup an "Additional Default Gateway" (here "SIP_Gateway") for IP traffic on Ethernet port 3 (eth3):

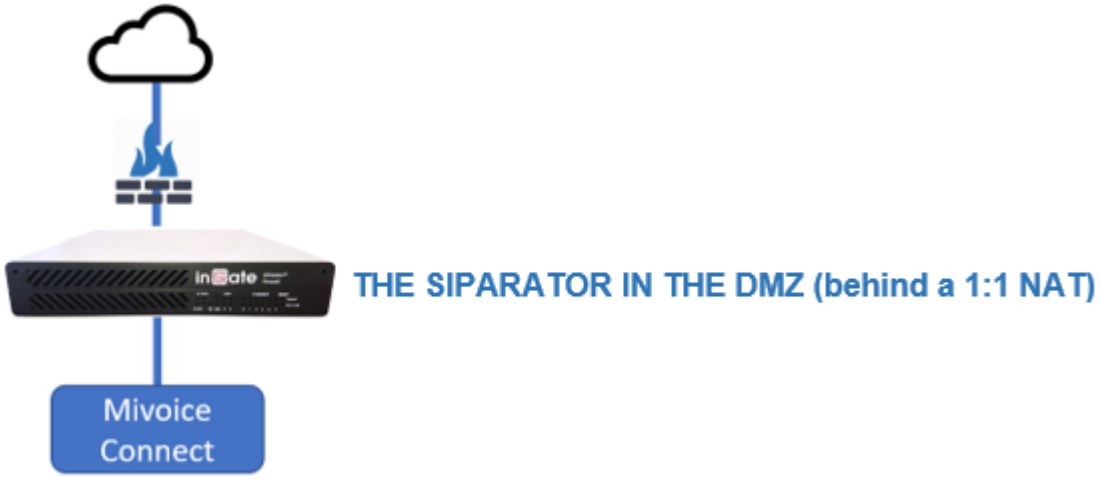


c) Enable that "Additional Default Gateway" (SIP_Gateway) as the "Outbound Gateway" at the SIP Trunks page for the ITSP:

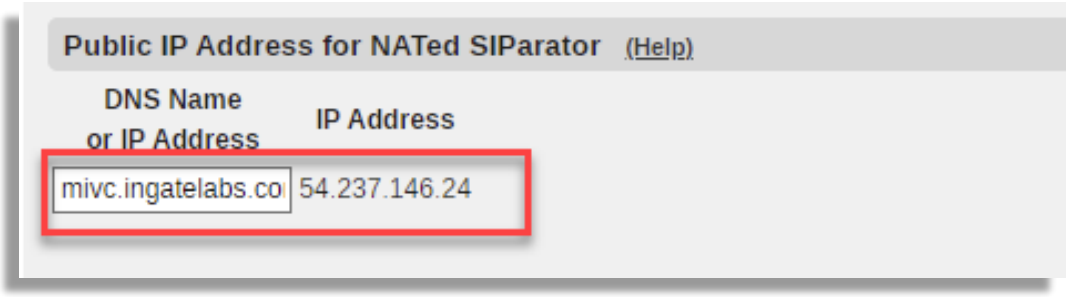


d) Connect Ethernet port 3 to the ITSP's private network and connect Ethernet port 1 to the real Internet for the Teleworker Gateway functionality).

Notice that the SIParator's Internet can be behind a 1:1 NAT or "in the DMZ":



which Public IP address must be configured under SIP Services → Basic Settings:



However, there is NO such function (of being behind a NAT) for the private SIP trunking pipe that must be directly connected to the ITSP's network[2].

NOTE: If you are using an Ingate Software SIParator® (https://www.ingate.com/files/IngateInstallationVirtualMachines.pdf), it may not be possible to add an extra ethernet port (like eth3 recommended above) after already being installed. VMware has shown this restriction, while it has been possible under KVM. Please be aware that changing the EMAC0 address invalidates the Ingate license and you need new licenses to reinstall the Software SIParator® (which can be provided by your Ingate sales channel, if you select to use an already installed Software SIParator® under these circumstances). Take precautions like SIParator backups and VM image backups before doing any change to make sure you have a rollback path in case you need it.

4.2.3 DNS Considerations

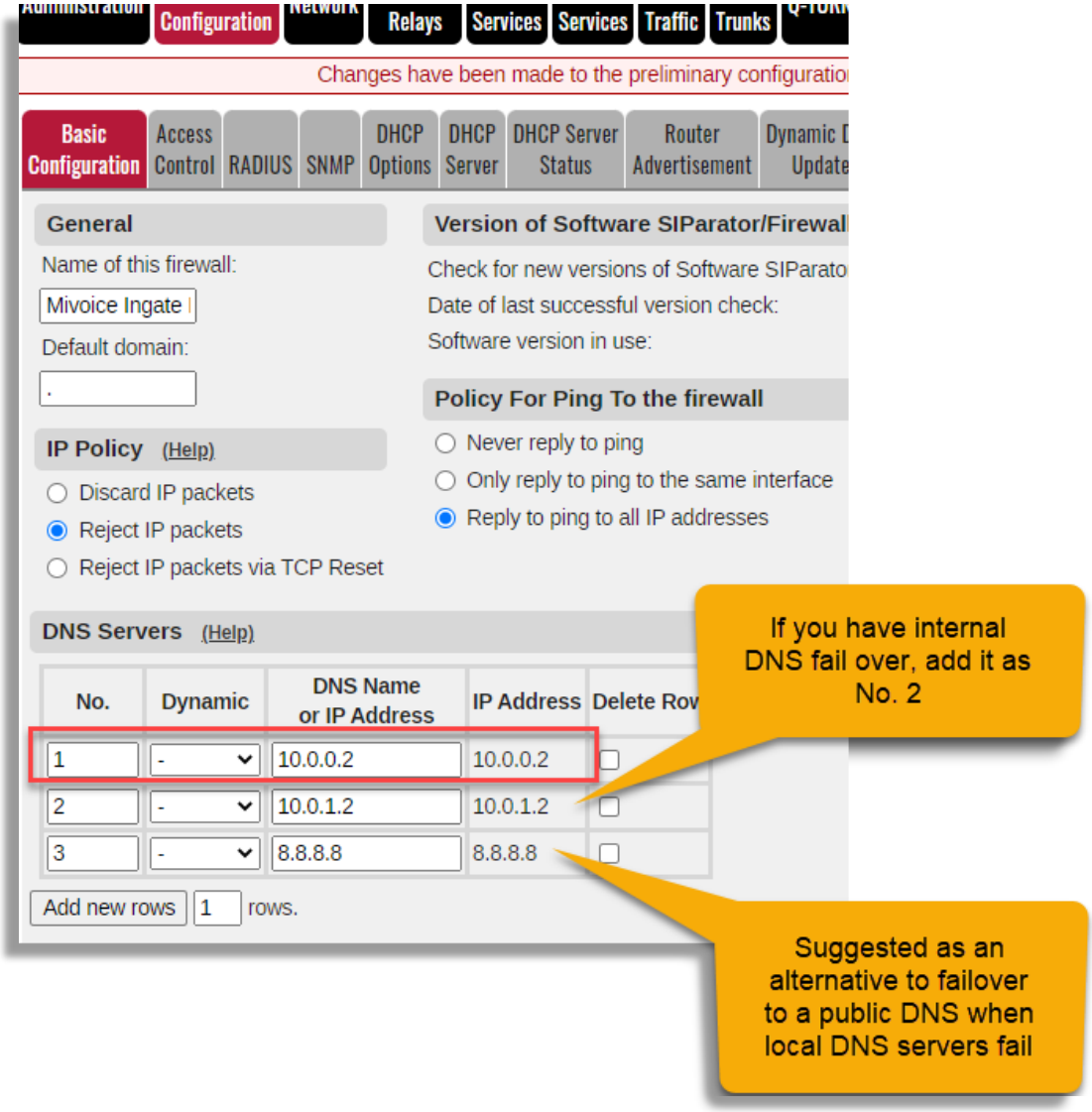
The DNS server(s) that the Ingate SIParator® uses are setup under Basic Configuration → Basic Configuration and are in existing installations usually populated with a commonly known IP such as 8.8.8.8, 8.8.4.4, 4.4.4.4 or similar.

Due to it use of secure MTLS connections using certificates, the Teleworker Gateway functionality of SIParator® requires that the public IP address of the Ingate SIParator® if referred to by an FQDN (Fully Qualified Domain Name), setup and resolved in a public DNS server. If any local addresses to the MiVC

[2] patch-6.2.2-sip-public-ips.fup (intranet/index.php/Fuego_Patches) may imply a possible solution.

servers (or to the inside of the SIParator®) are referred to by an FQDN, those need to be setup and resolved in an internal private (a local) DNS server on the LAN.

It should look like this, assuming in our example the internal private DNS server is at "10.0.0.2":



NOTE: If you use an FQDN rather than an IP address, for the MiVC HQ Server where the "config server" is located, you MUST also specify an FQDN in the startup.cfg file that the Ingate SIParator® hosts, see 8.1 Hosting startup.cfg in the Ingate SIParator®. Mixing FQDN and IP address will cause FAILURE. Such FQDN for the HQ Server must be resolved in a local DNS server.

If no FQDN is used for the any MiVC component you can keep using only a public DNS Server such as 8.8.8.8.

5 SIParator® Basic Network Setup for the Teleworker Gateway

The Teleworker Gateway for the Mitel 6900s phones, is available over the Public Internet using MTLS over port 5061 and gives the phones the same functionality as if connected locally to the MiVC PBX, including automatic phone firmware upgrade, authentication and CAS communication.

The Teleworker Gateway functionality is available in both Firewall and SIParator Mode of the Ingate SIParator®. Typically, SIParator Mode is used, unless you already are or have the intention to use the specific firewall functions (Rules and Relays) of the SIParator®.

Typically, the "Standalone" SIParator Type is used, unless you already are or have the intention to use some other SIParator Type under Basic Configuration → SIParator Type.

5.1 Remote Phone Users Just Select MiVC and FQDN:6586 to Connect from Teleworker Locations

Remote Phones Just Select FQDN:6586[3] to Connect from Teleworker Locations

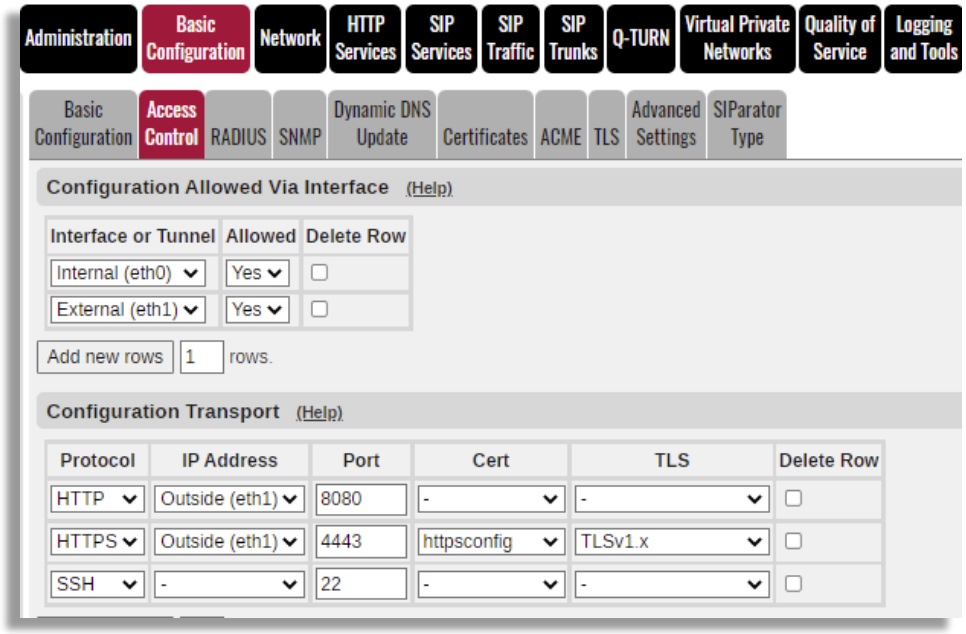
5.2 Initial Port Adjustments on SIParator® Access Control

On this step we will release port 80 and 443 from the default configuration used to access the SIParator's Web GUI. We will use port 8080 for http and 4443 for https. You can decide differently and decide which protocols to use based on your specific needs as far as ports 80 and 443 are not used here.

Port 80 will be used for the ACME protocol to be able to use Let's Encrypt as a certification authority and to obtain auto-renewable certificates from them.

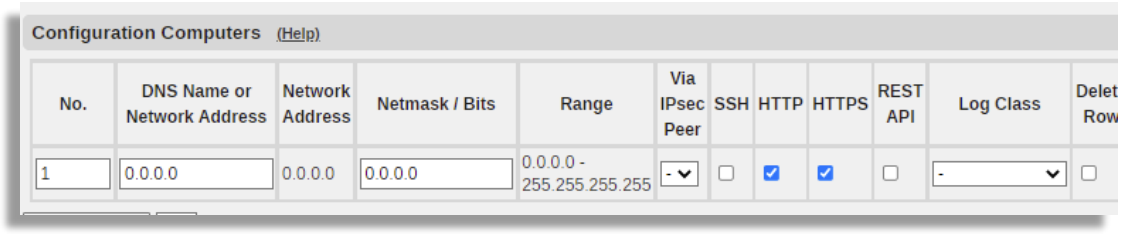
[3] The Mitel local usage is to simply enter the FQDN without any port specification, which selects the TLS standard port 433. However, for a company installing the Teleworker Gateway, that must listen for MTLS connections from its Teleworker's at that particular port, **it would block the company's other usage of port 443** at this FQDN, which typically is the company's Internet connection. Ingate is therefore in this Application Note showing a configuration where the Ingate SIParator is listening to port 6586 from its Teleworkers. To go back to using port 443 and port 444 (which are assigned by IANA for other purposes), simply change port 6586 to 443 and 6587 to 444 as shown in 6.1.1.2 HTTP Services related certificates and 8.2 Local Endpoints.

Port 443 is the default port used by Mitel 6900 series of phones to establish MTLS connections for other than SIP usage, but to free up 443 for other company usage, we instead use port 6586.



NOTE: From this point on make sure to access the Web GUI in the SIParator® to use the appropriate port. Remember that once you apply this change you will lose access to the Web GUI in the current session, and you should have other web instance open with the new port to refresh and save the changes. Otherwise, changes will be unapplied after 30 seconds.

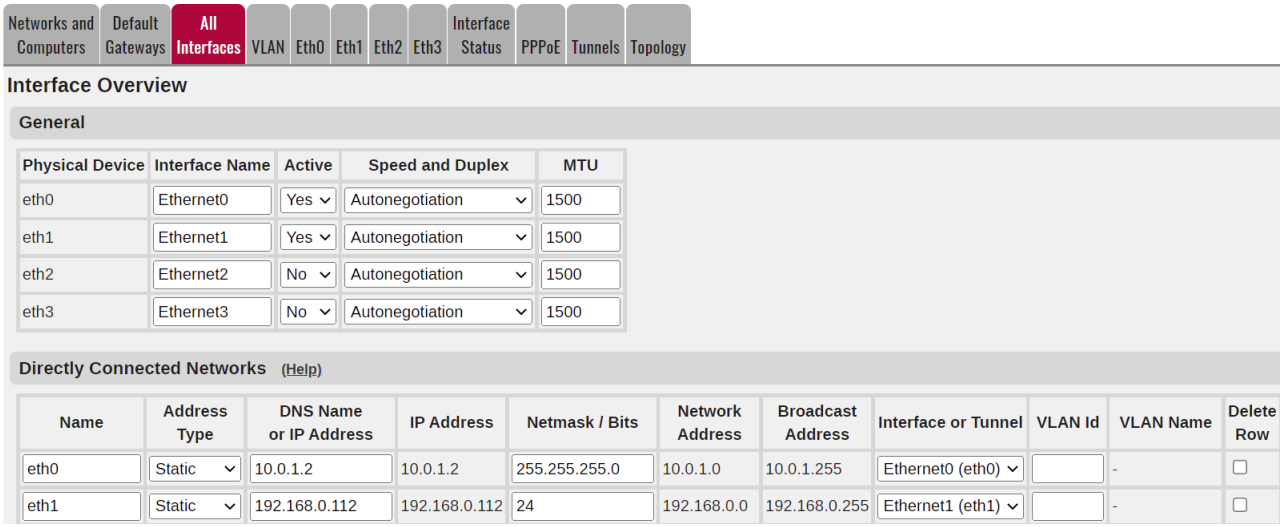
NOTE: If you don't have a certificate created for https, use the instructions in section 6 to create a Let's Encrypt private certificate. You can also add https access later. Make sure that you have enabled the appropriate subnets and IP address to allow access to the SIParator® interface from those networks. Make appropriate adjustments based on your scenario.



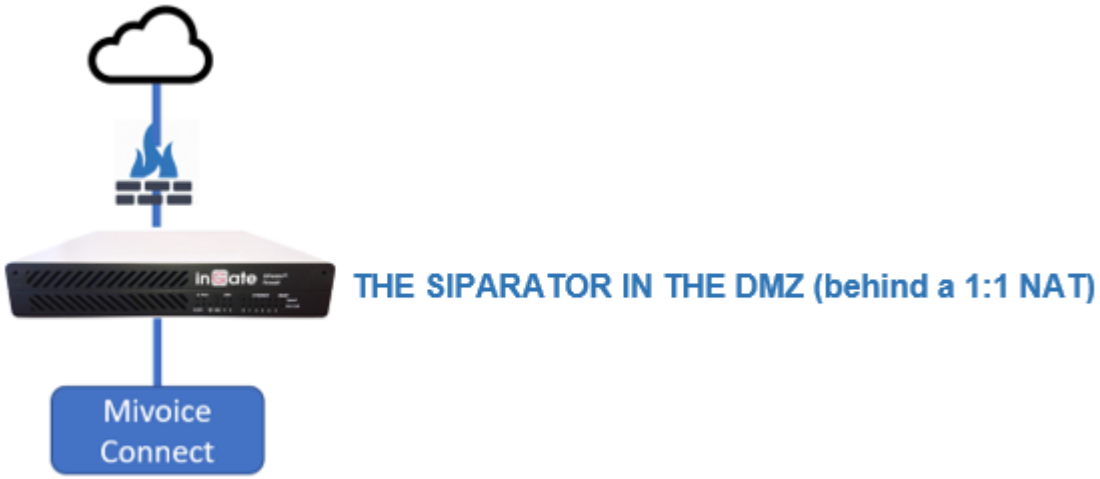
5.3 Network – All Interfaces

There are thousands of SIParators already deployed for SIP trunking, using simple standardized configuration. To comply with the most common usage and terminology the "Inside" of the SIParator®, ethernet port zero (eth0) is named Ethernet0 and connected to the LAN, while the "Outside" of the SIParator®, ethernet port one (eth1) is named Ethernet1 and connected to the LAN.

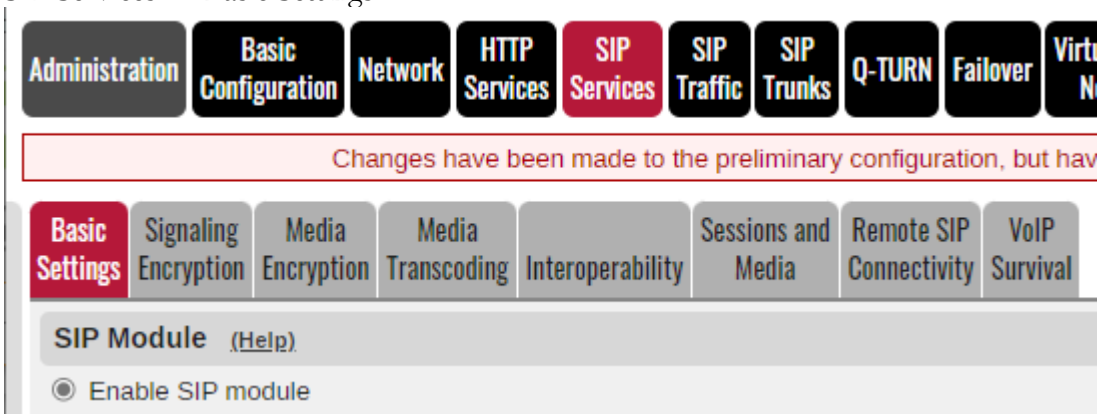
This is set up at Network → All Interfaces:

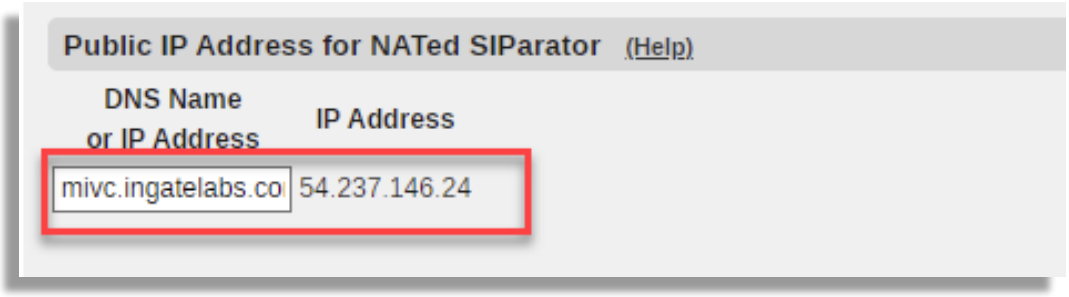


Please notice that the WAN IP address here is Private instead of Public, because the SIParator is behind a 1:1 NAT or "in the DMZ", which simply is "Port Forwarding" – What comes in on the Public IP address is forwarded (without changing ports) to eth1 having the WAN IP address.

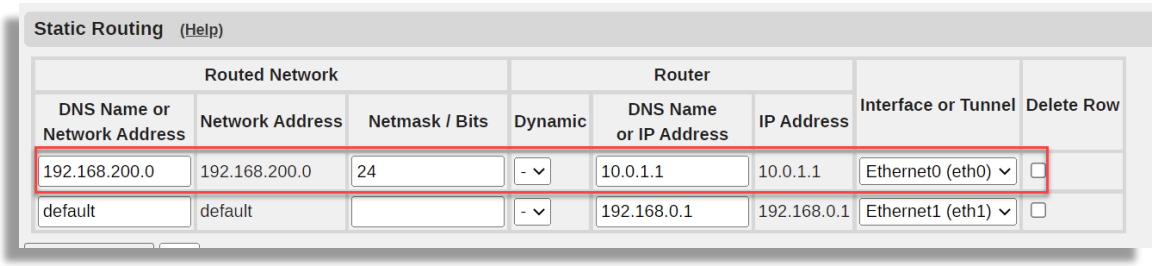


For SIP to work, having the SIParator® in the DMZ, you need to configure the Public IP address under SIP Services → Basic Settings:





Add any static routes in case you need to reach other internal subnets, and define your default gateway (usually to reach the outside or anything else), e.g.:

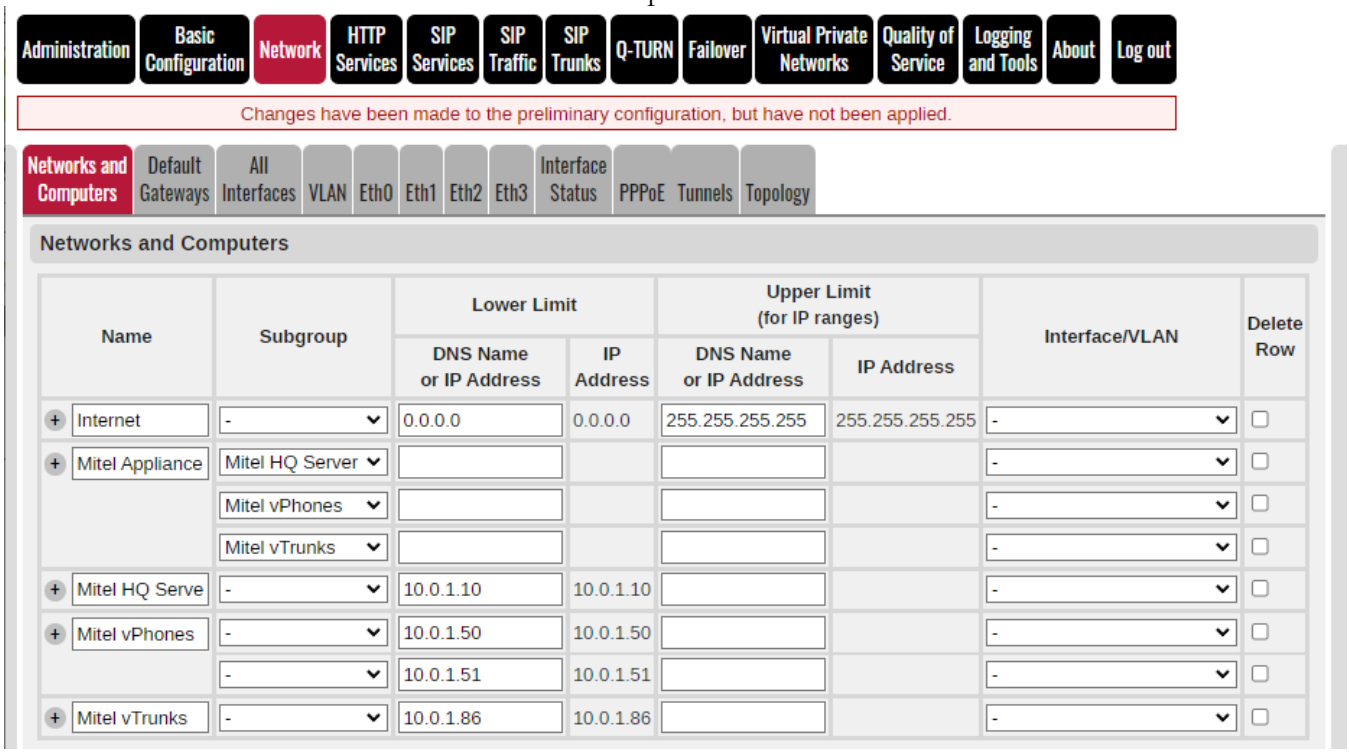


In this example we added a static route to be able to reach some Mitel Devices located in the LAN side but in a subnet that is not directly connected to the SIParator® (i.e. 192.168.0.0/24)

5.4 Networks and Computers

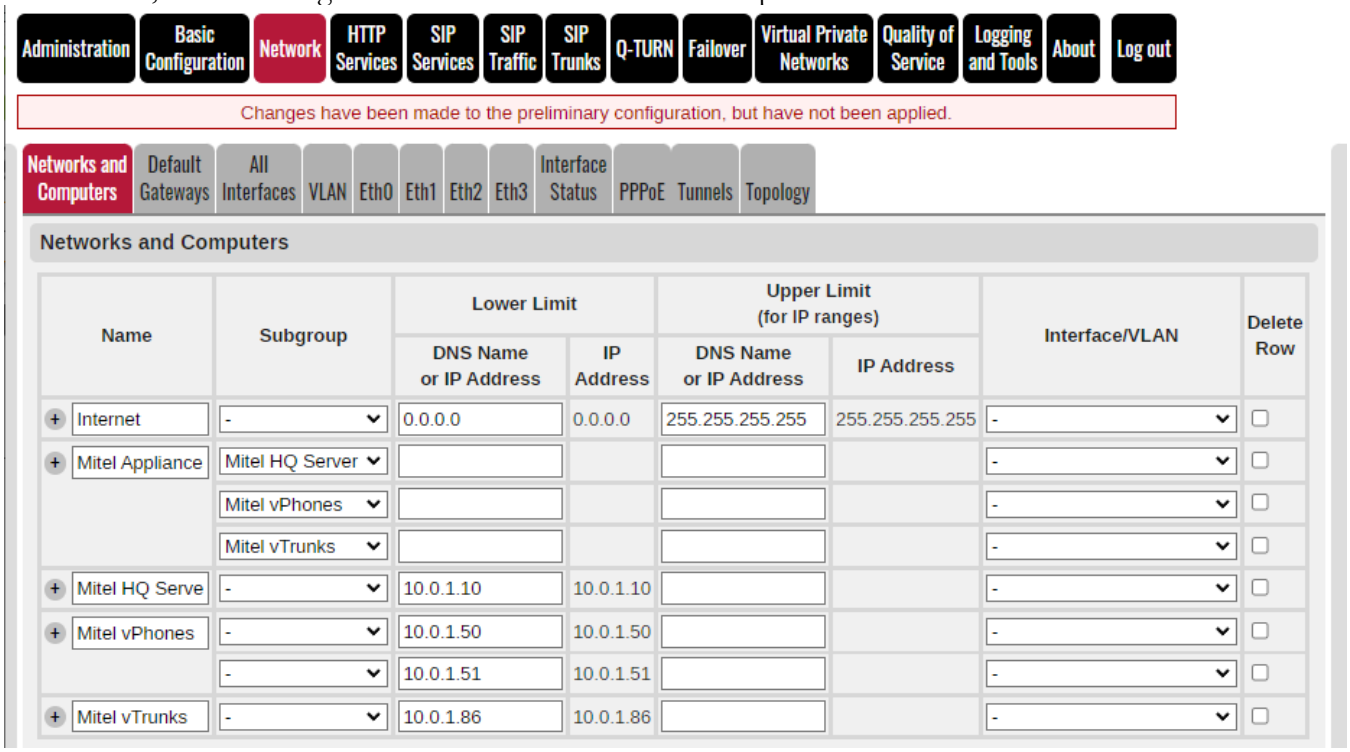
This section shows how to assign names to known IP addresses and group them to make it easier later during remaining configurations.

This is done under Network → Networks and Computers:



We are defining the following names:

- **Mitel Appliance**. All IP ranges where MiVoice Connect appliances are included coming from the Inside.
- **Internet**. Any IP coming from the Outside covering all Internet for any Teleworker.
- Etc., here detailing the IP addresses of all MiVC components:



Existing SIParators already setup for SIP Trunking, typically call their WAN connection "Internet", even if it is not connected to the full Internet, that the Teleworker Gateway must work over. Such "Internet" for existing SIP trunks, typically has to be relocated to another ethernet port (we propose eth3) as described in section 4.2 Combining Teleworker Gateway with SIP Trunking SIParator®. In our example all MiVC appliances are on the same subnet (10.0.1.0/24). If there are other subnets where MiVC appliances can be reached, just add under the same Mitel Appliances by clicking in the "+". Make sure all those additional subnets are reachable via the inside default route or new added static routes.

6 Required Certificates in the Teleworker Gateway

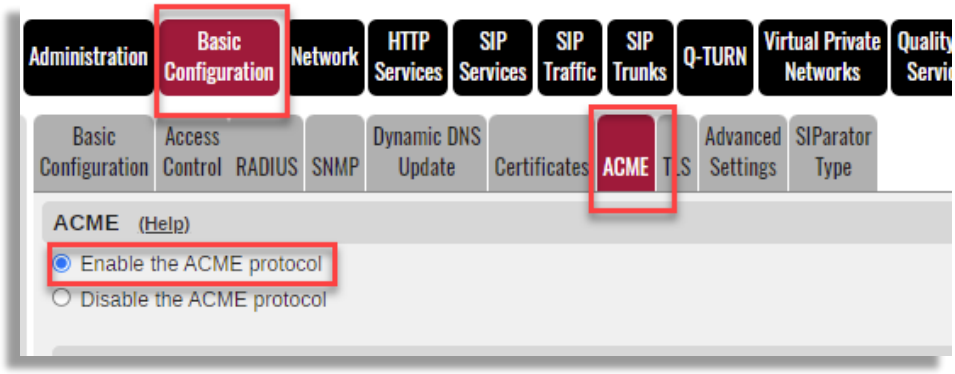
When configuring the MiVC PBX, in section 3.1, a long-time certificate between the SIParator® and MiVC was created in the Director and inserted in SIParator®. There are also certificates needed on the public side (the Internet) between the SIParator and the remote phones. These need to be renewed frequently and the fairly new ACME protocol, is used to automatically update free certificates from Let's Encrypt. Thus, the certificates in the SIParator provide high security and the certificates do not need to be manually updated over time.

6.1 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.

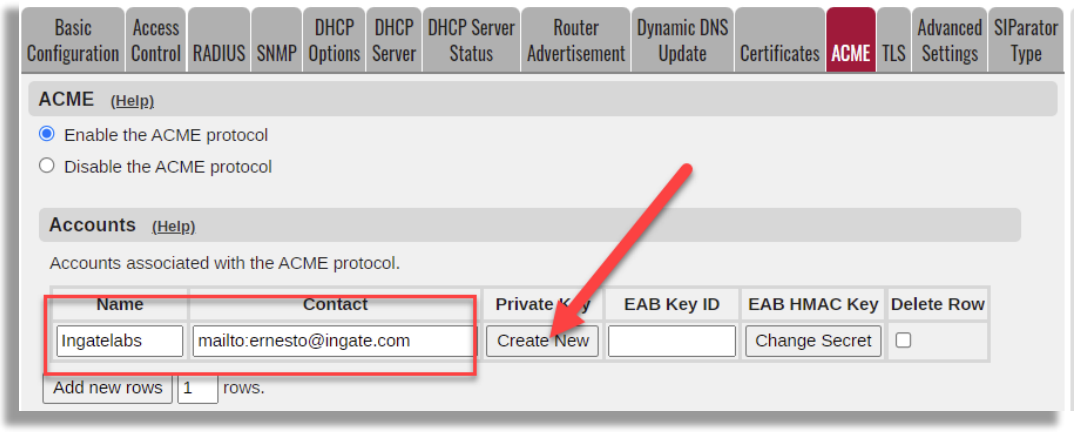
To enable ACME Protocol:



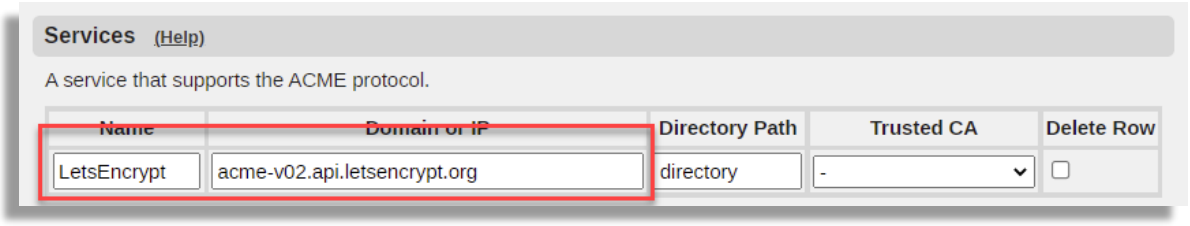
Under Accounts, add a new row, assign a name, fill in the contact information using the following format:

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.

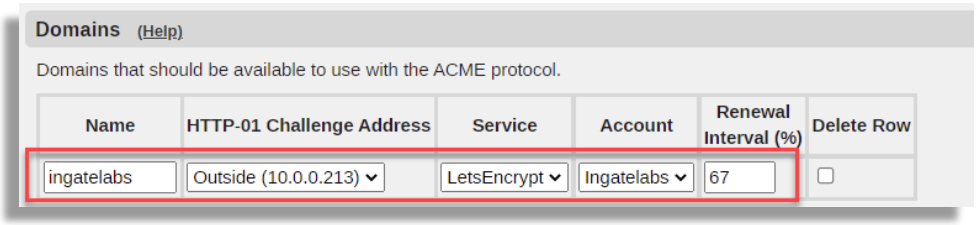


Add a Row under "Services" to point to Let's Encrypt Servers. Assign any name, but use exactly the URL as shown below (acme-v02.api.letsencrypt.org):



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)

6.1.1 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.

6.1.1.1 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).

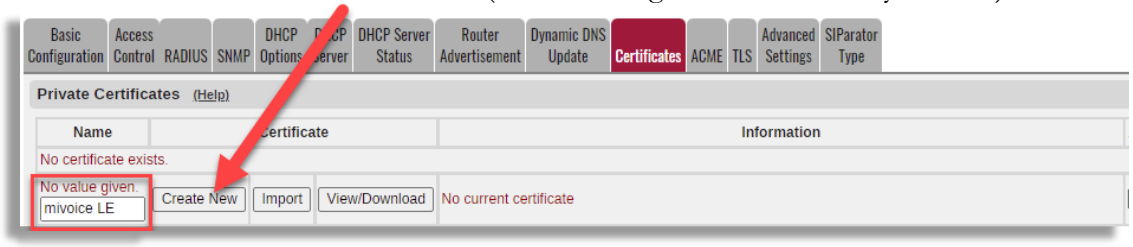
Here we explain how to add Let's Encrypt certificate and then we will explain how to associate both certificates to each interface in the SIP configuration.

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 6.2 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

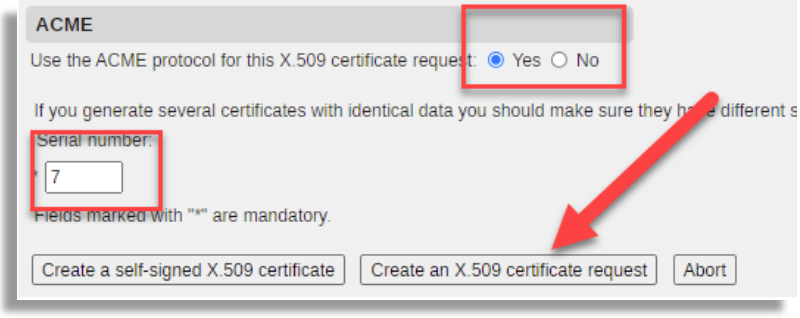
Let's call this certificate "MiVoice LE" (You can assign whatever name you want) and click on Create New



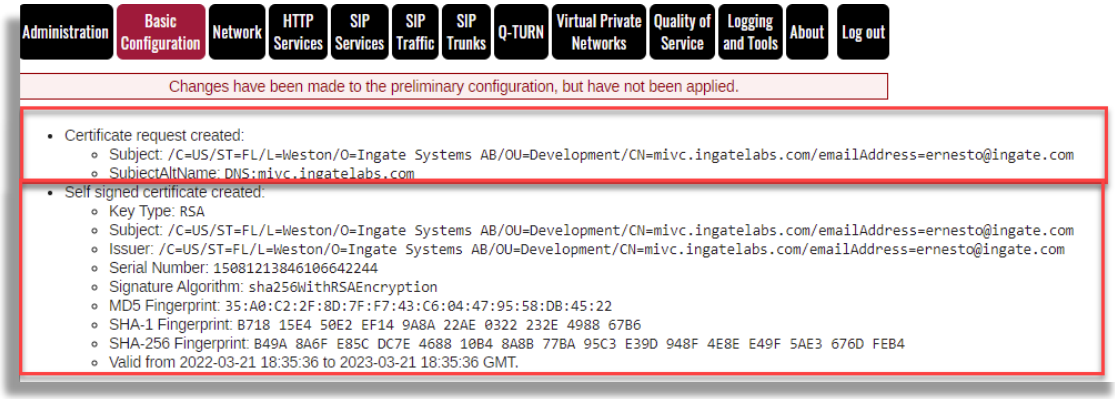
- Fill the information.
  - Expire in days (it doesn't make any difference for Let's Encrypt as they expire every 90 days, but automatically renewed by SIParator®). However, this field is mandatory.
  - Country, Organization, State/Province, Organizational Unit, locality and email. Fill all of them with 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.

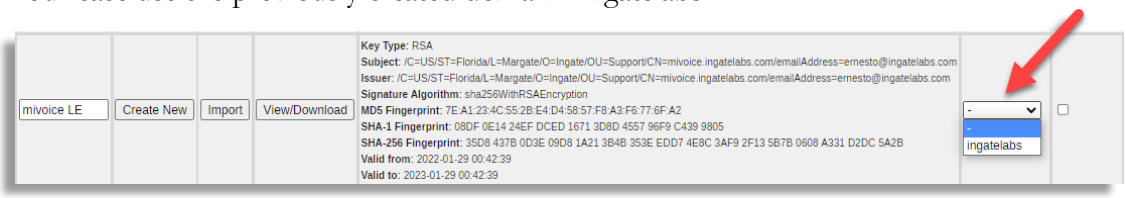


You will see this result screen:

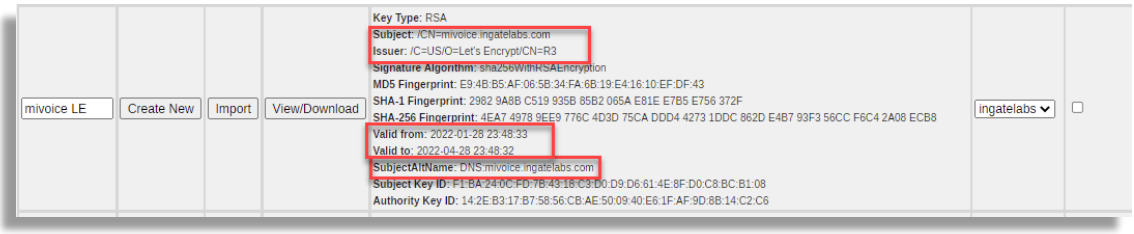


As you can see, a self-signed certificate is generated (it will be used until a signed certificate is received from Let's Encrypt), and also a Signature request is generated to be sent automatically to Let's Encrypt Service.

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.

6.1.1.2 HTTP Services related certificates

For HTTP Services we will need certificates for external connections with the teleworker's phones, including for secure access on port 6586 (443[4]) and HTTP Connect tunneling on port 6587 (444[5]). We will use here the same Let's Encrypt generated certificate used for SIP.

Again, 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 6.2 below.

When proxying https, an internal certificate is needed to connect from port 6586 to the LAN-internal MiVC appliances. In this case the certificate signed by HQ Server is the one to be used, which already was created under section 3 and uploaded to the SIParator®.

More details will be shown in the HTTP Services section later in this document.

[4] Mitel's initial thought to use.
[5] Mitel's initial thought to use.

6.2 Considerations When Using a 3rd Party CA Other Than Let's Encrypt

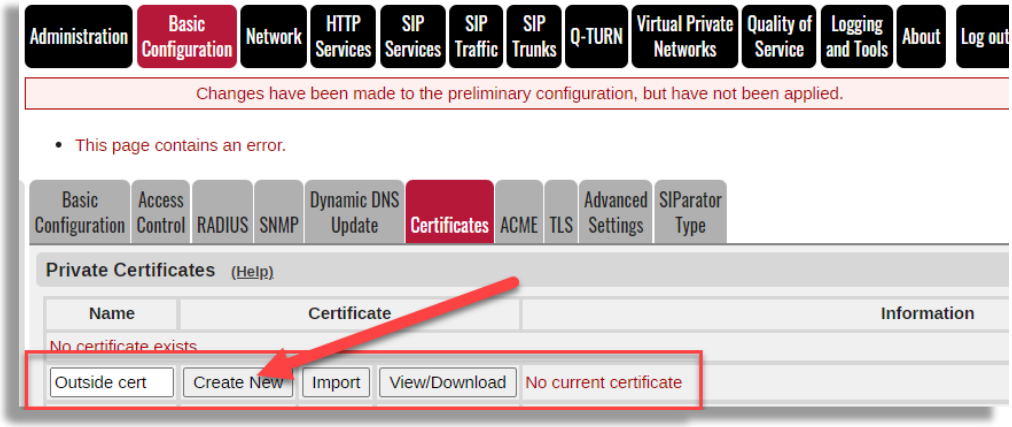
If you select to use a 3rd party CA for the SIParator® external certificates, the ACME protocol is not needed, but you need to specifically add that CA to the SIParator's authorized bundle[6] and there are two possible scenarios to generate the addition to be made:

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

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

6.2.1.1 Step 1: Produce the Request

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

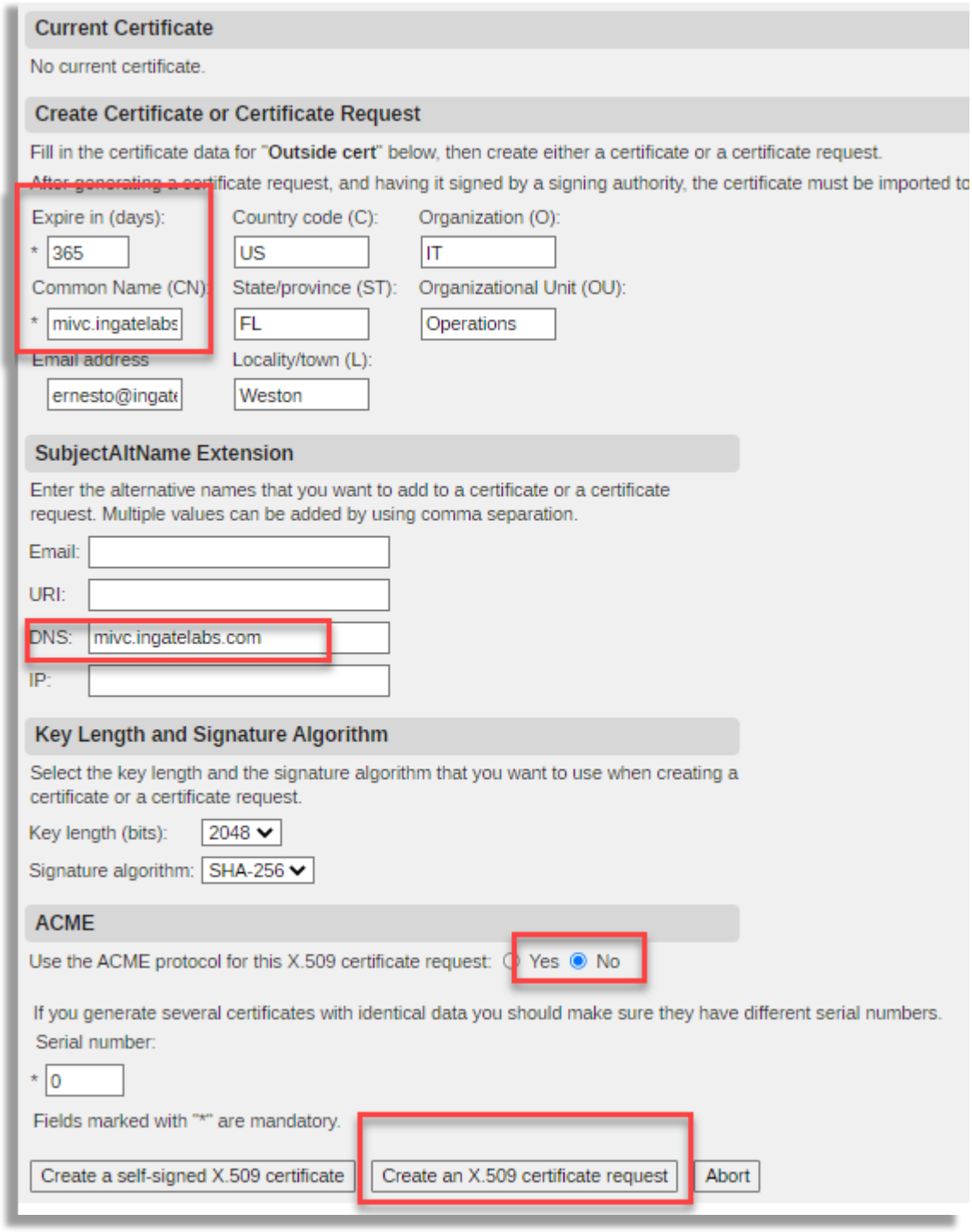


Click on "Create New"

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

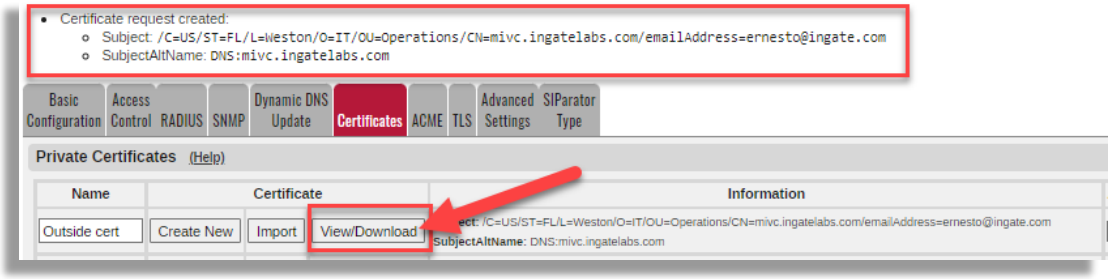
It should look similar to this:

[6] 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.

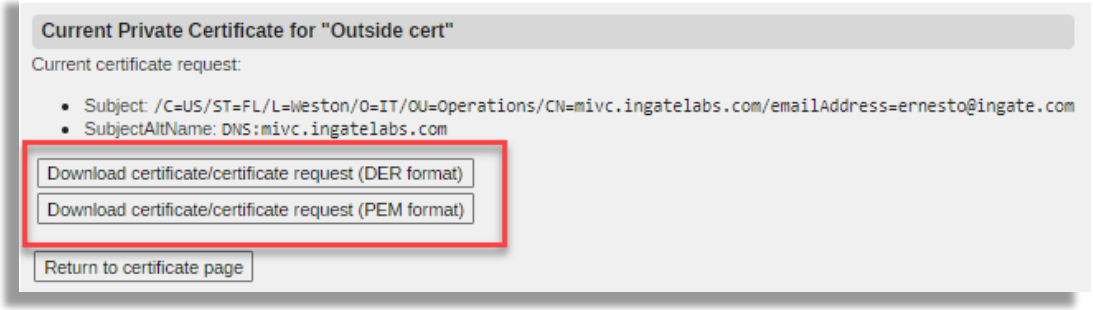


Selecting "Create an X.509 certificate request, and not enabling ACME, will generate a CSR file to be used with the certification authority of your selection (for further signing).

Download then the CSR file:



Click on "View/Download"



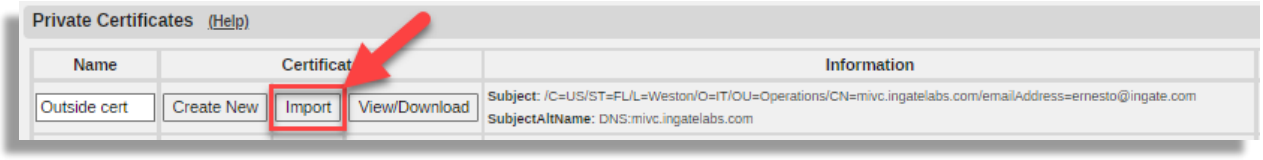
Download the file in any of the 2 formats offerings depending on which one better fits the requirements of the CA you selected to use.

6.2.1.2 Step 2: Load the CA Signed Certificate

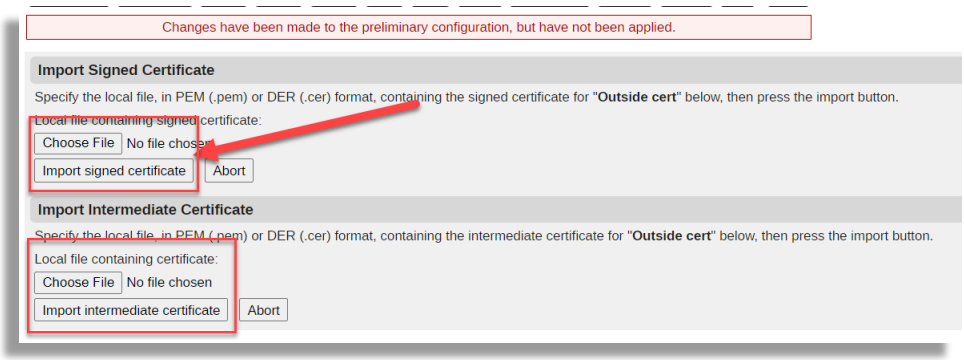
You will receive a set of files from the selected Certification Authority. Those files include one containing the signed certificate.

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.

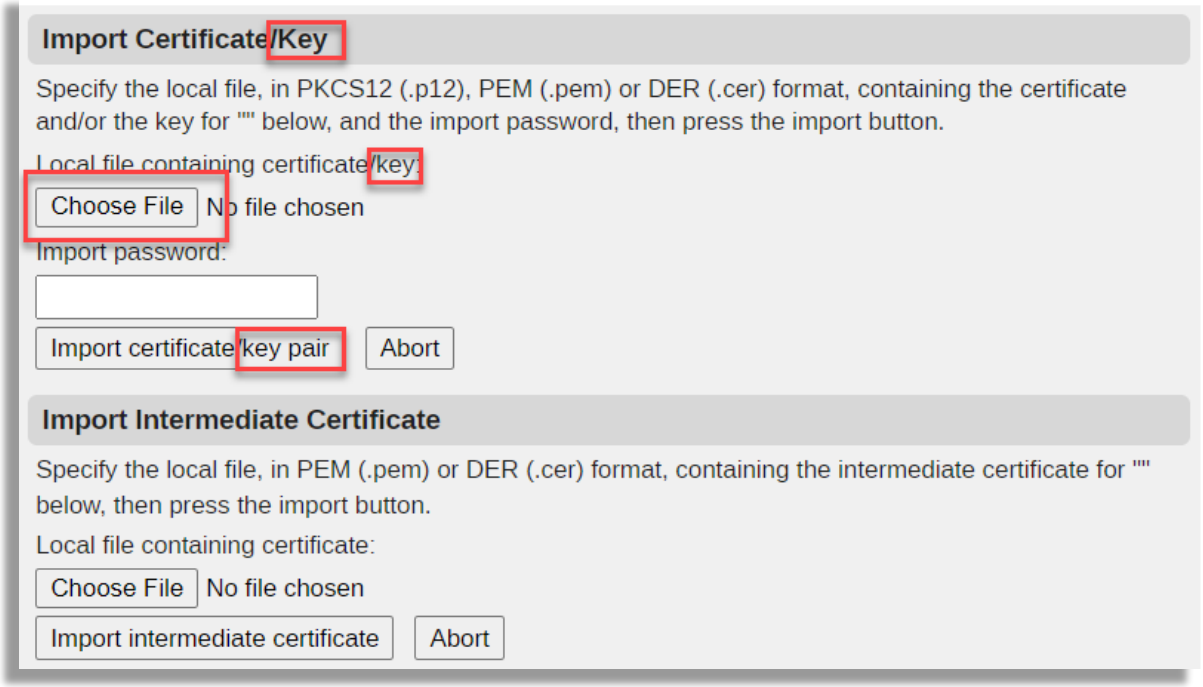


In case you also received a set/bundle of intermediate certificates, they can also be loaded repeating this step, but it is then better to use the options under Import Intermediate Certificates.

6.2.2 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":

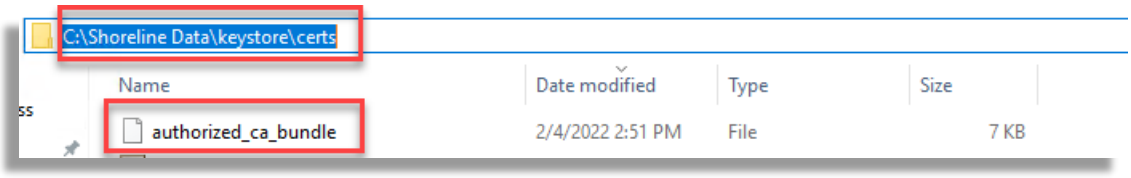


If the file received is protected with a password, make sure you have it and complete in the same screen.

6.3 CA (Certification Authorities) Root Certificates

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:

6.3.1 Add the Mitel Root CA for the Mitel Phones

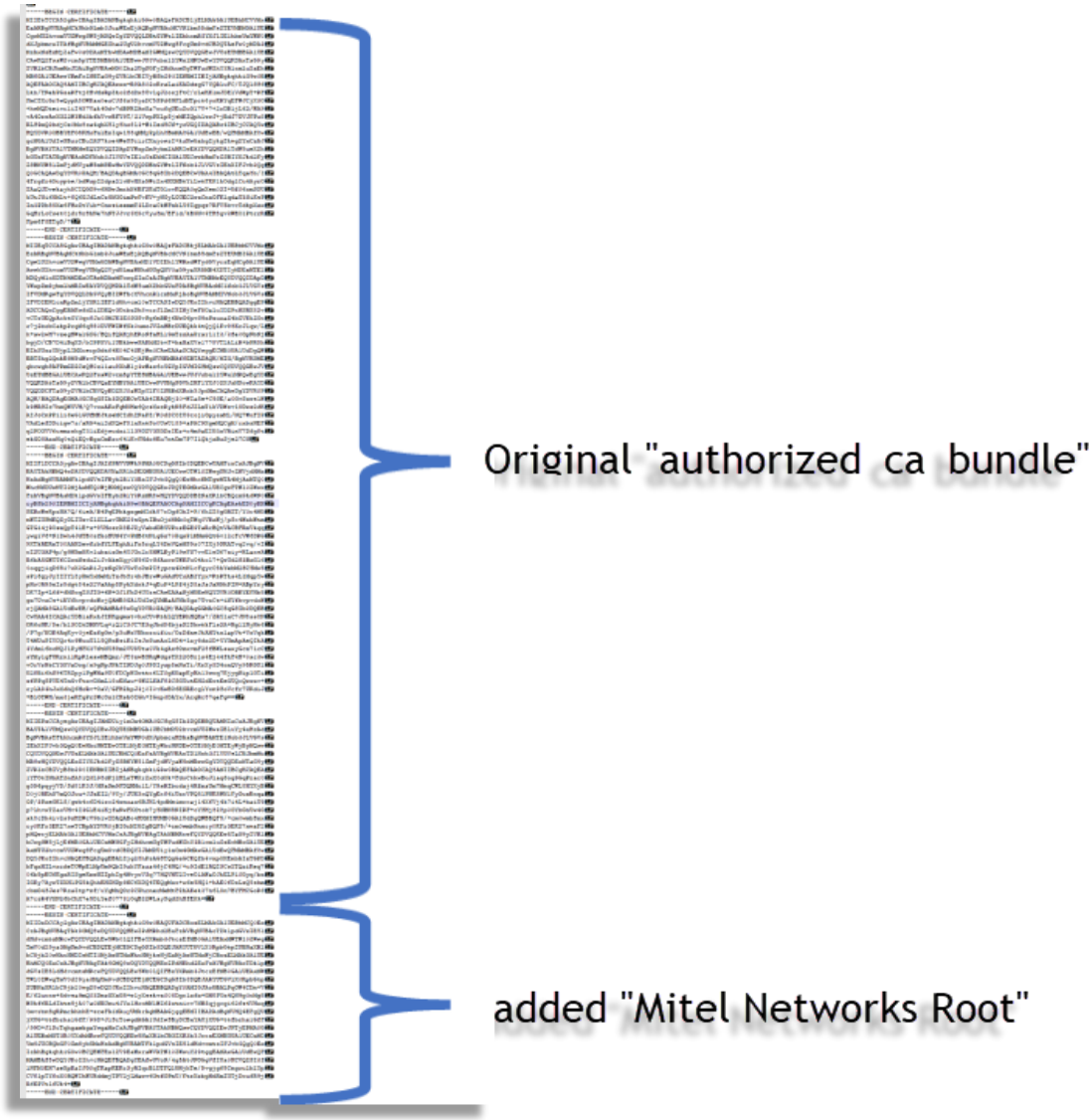
By the time of this document there is one more root CA needed and not included in the bundle downloaded from the HQ Server in the MiVC environment. It refers to the CA needed to recognize certificate built at factory for phone with MiNET firmware loaded.

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:



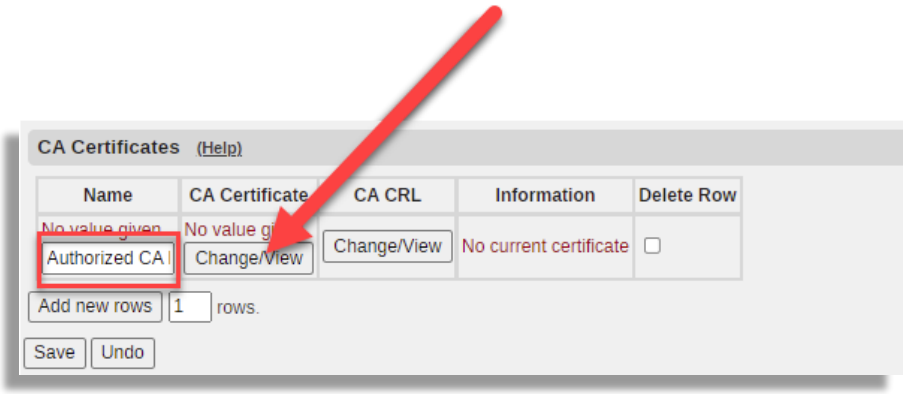
6.3.2 Also Add the CA for the HQ Server, if Using a 3rd Party Certificate for the HQ Server

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®.

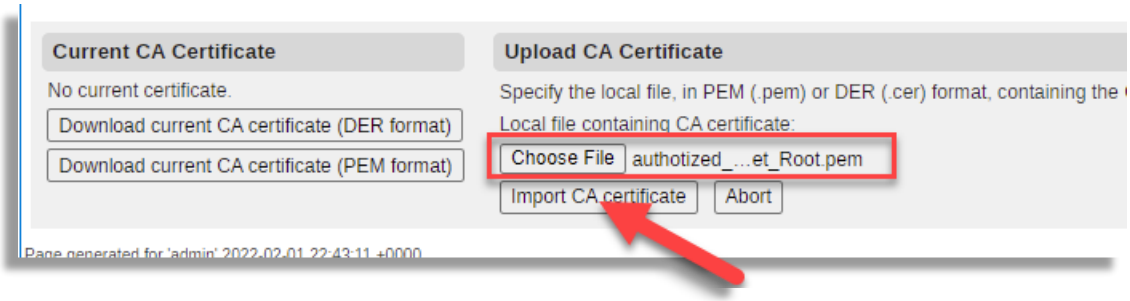
Use the same procedure with an editor as explained in the previous section 6.3.1 to add them before moving to the next step explained in 6.3.3.

6.3.3 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":

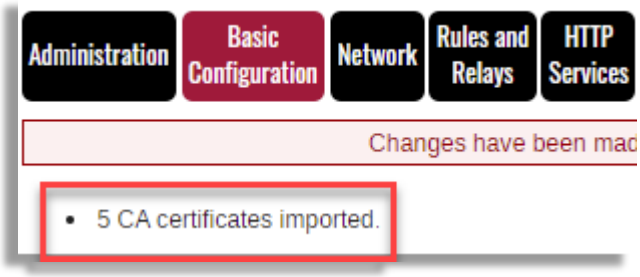


Click on Change/View:

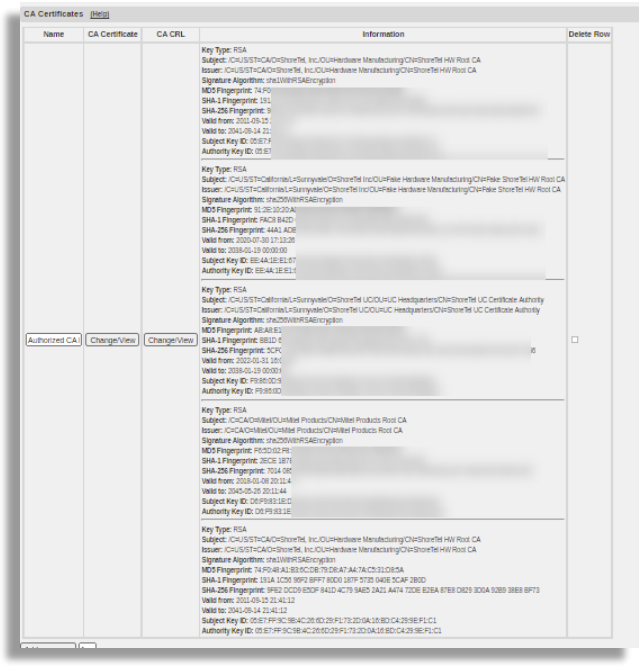


Choose the file and click on Import Certificate.

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.

7 SIParator® SIP Configuration for the Teleworker Gateway

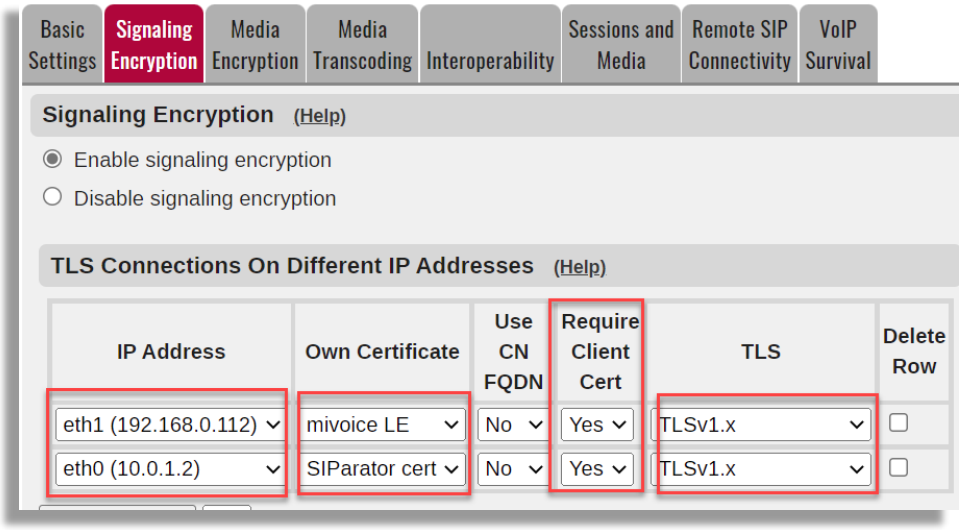
Some configurations required for Teleworker Gateway may interfere when used in a SIParator® already in use (typically for SIP trunking of the MiVC or previous Shoretel Shoregear PBX)[7]. Please notice the concerns and footnotes of this section, as well as the concerns in section 4.

Here we are going to setup the SIP related configuration required for Teleworkers.

7.1 Setup SIP Signaling Encryption (TLS)

We will need TLS encryption for the signaling for the SIP communication going and coming from the inside MiVC PBX as well as from the outside remote phones (the 6900 series phones used by the Teleworkers).

For the inside we will need to associate the certificate we created previously signed by HQ Server (SIParator® cert), and for the outside we will use Let's Encrypt signed certificates.

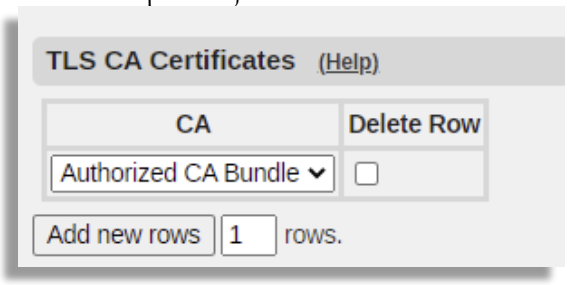


Select Yes on Required Client Cert to enforce Mutual TLS.

Select the appropriate TLS protocol you want. In our example we selected the one that covers all the supported TLS version in the SIParator® (except SSLv3.0 and TLSv1.0)

Add all CA TLS Certificates you want to trust.

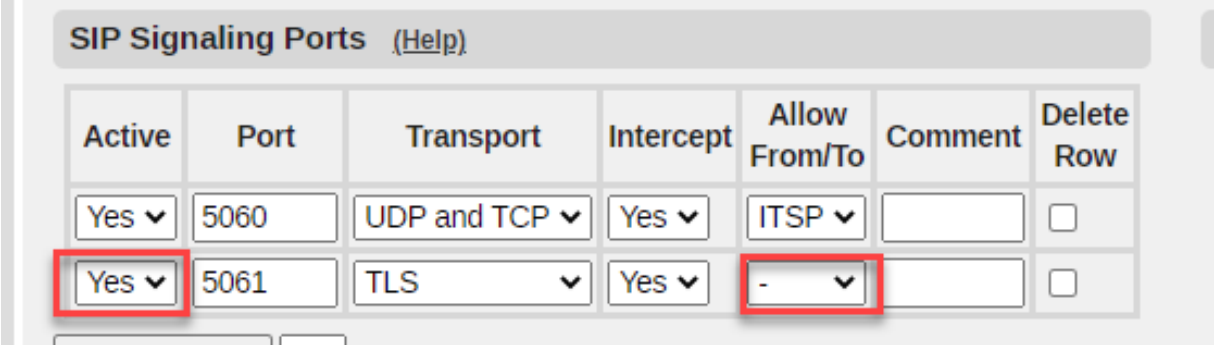
In our example we just added all of them:



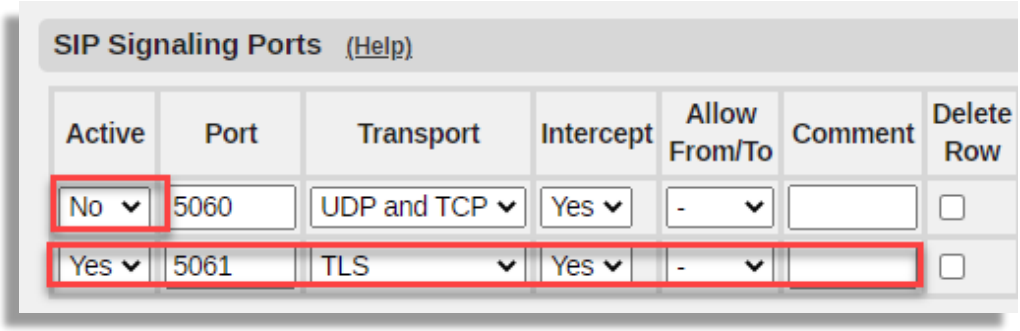
[7] There are typically no conflicts with the SIP configuration of these PBXs in combination with SIP trunking. Conflicts are more prone to occur in the network configuration (see section 4) and often require network reconfiguration of the SIP trunking function, which is detailed in 4.2.1 Teleworker Gateway with SIP Trunking Over the Public Internet and 4.2.2 Teleworker Gateway with SIP Trunking on a Private IP Pipe.

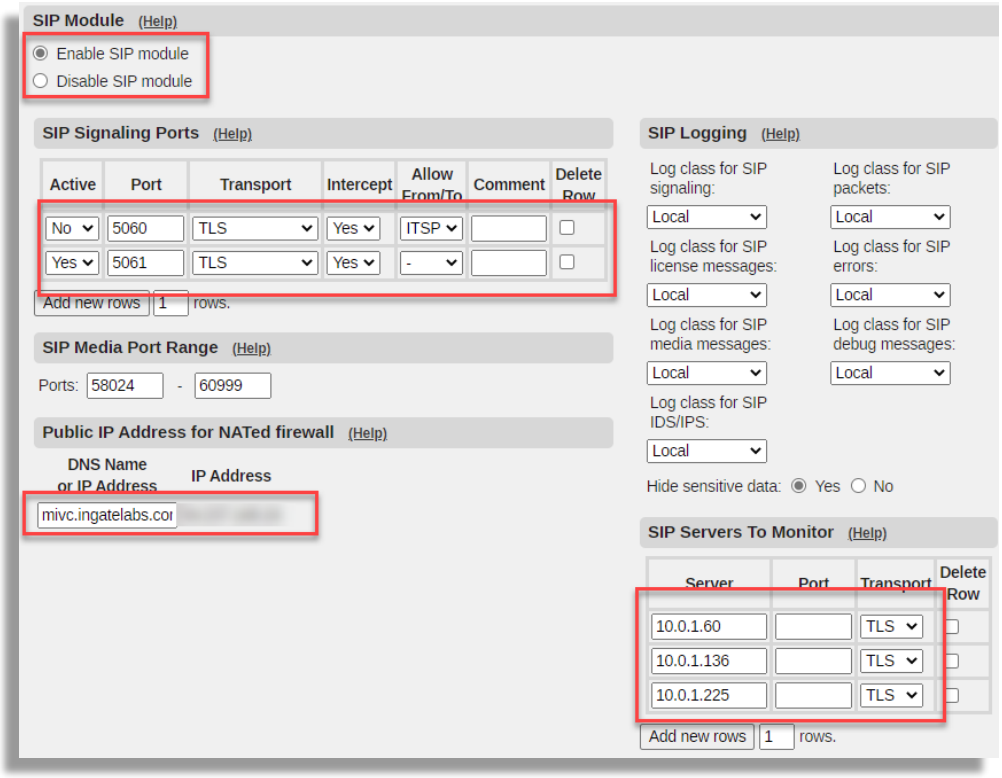
7.2 The Teleworker Gateway Requires MTLS SIP Signaling over the Public Internet

If this installation is an addition of the Teleworker Gateway functionality to a SIParator® already in use, you need to read and understand section 4 SIParator® Network and Combined Functions Concerns and thereafter only make sure that this red marked is setup (and leave the rest):



If, on the other hand, a fresh SIParator® is being installed as Teleworker Gateway, follow the below to make sure the red circled are as shown here:



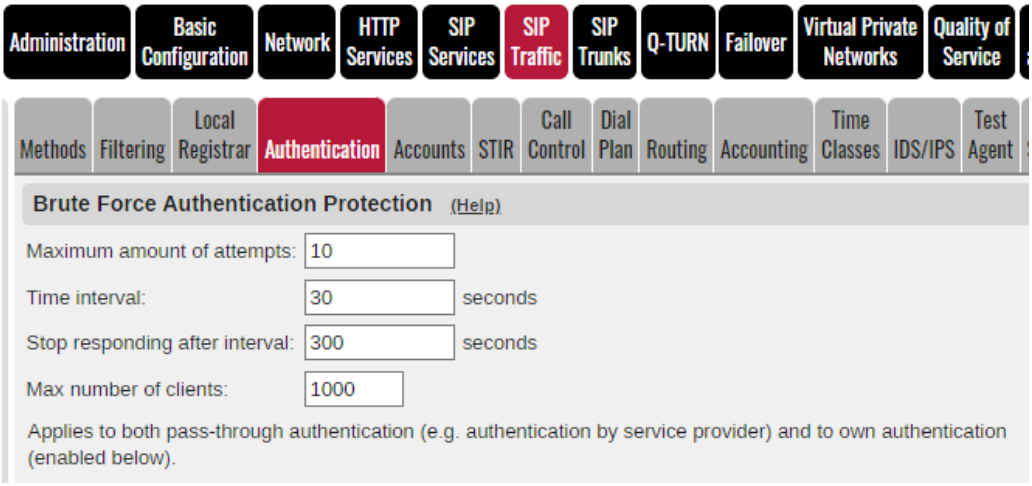


- Enable SIP Module.
- Inactivate port 5060 for TCP and UDP.
- Enable port 5061 for TLS[8] and assure that column "Allow From/To" is unrestricted by "-" (all Internet allowed for Teleworkers). If the Ingate SIParator is in a DMZ behind an existing 1:1 NAT holding the public IP address, enter the public IP or FQDN under SIP Services → Basic Settings in the field for Public IP Address for NATed firewall.
  (In case your SIParator® Type is setup as WAN, you cannot use this field).
- You **may** at the SIP Servers to Monitor, add all the IPs or FQDNs of the known destinations such as Mitel Switches, SIP Servers, and ITSPs. This will allow the SIParator® to monitor those destinations using SIP OPTIONS. In our example we are adding IP addresses of the 3 known Phone Switches.

7.3 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:

[8] In case SIP Trunking also is on port 5061 using TLS, one CANNOT COMBINE the Teleworker Gateway function in the same Ingate SIParator®. (However, most SIP Trunking is over UDP on a private IP pipe from the Trunk provider, not using TLS).



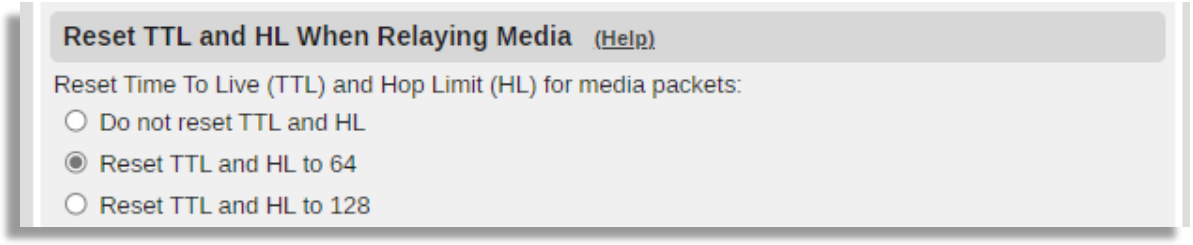
If the Brute Force Authentication is already configured for the Ingate SIParator® where the Teleworker Gateway function is to be added, judge if it is best left as already setup. At very large installations, judge those limits (which is per IP address trying to authenticate) for normal usage.

7.4 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:



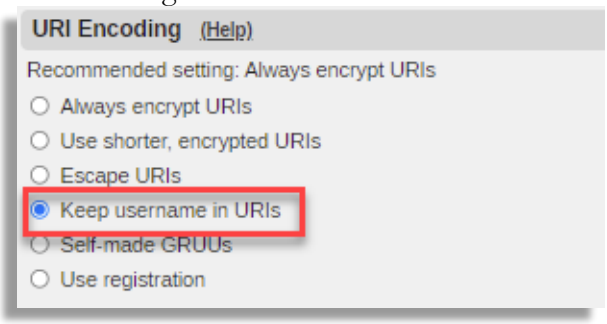
It is recommended that TTL is reset to 64 when the Teleworker Gateway is used with the current version of the 6900s phones. If these phones in a future software release (beyond 6.2.xxx indicated) will increase their TTL to 128, this setting can be set to its default "Do not reset TTL and HL" to restore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

7.5 Interop Parameters to Adjust

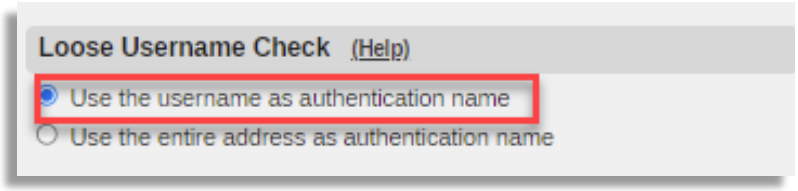
In this section we are showing only the parameters that need to be modified to a different value to the default/recommended setting. If you want to know default/recommended settings, you can review Appendix I.

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

URI Encoding:

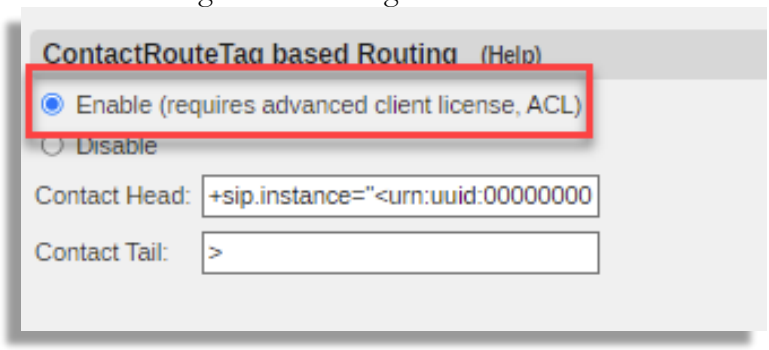


Loose Username Check:



User Matching:

ContactRouteTag based Routing:

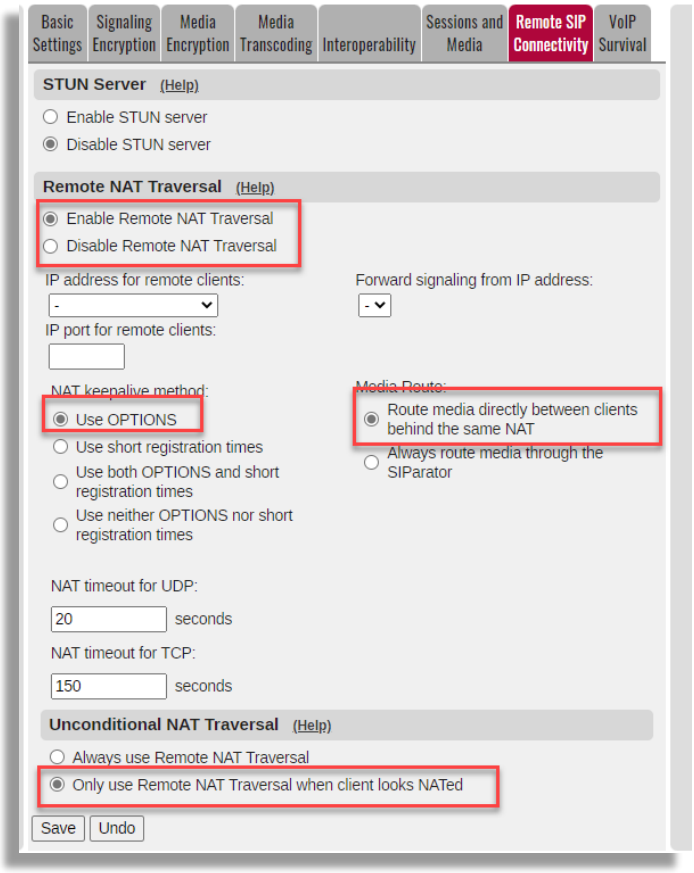


For MiVC, leave the default values as shown on the Contact Head and Tail in this picture.

None of the settings in this section 7.5 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.

7.6 Enable Remote SIP Connectivity

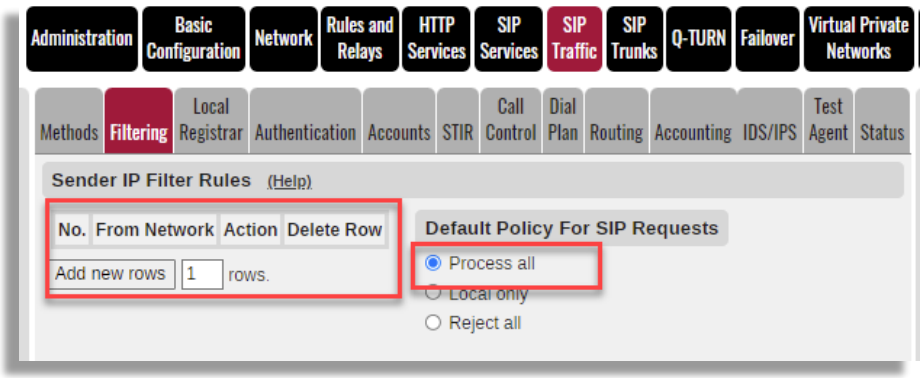
Enable the Remote SIP Connectivity, or Far-End NAT Traversal ("FENT") as it also is called. Change "Media Route:" to "Route media directly between clients behind same NAT (unless some clients are double NATed) and check that the other settings are as shown in the picture below, which are the default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



7.7 Configure SIP Traffic Filtering to be Without Restrictions

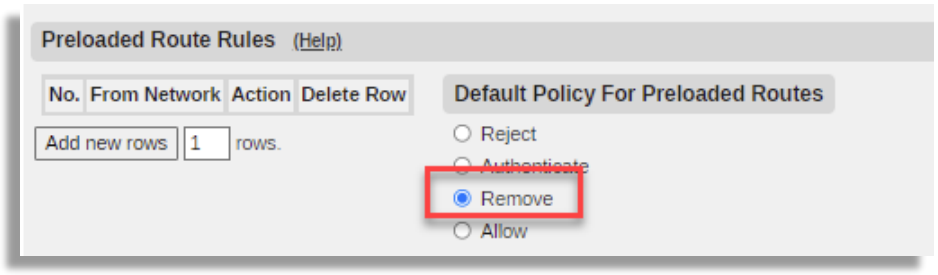
For Teleworkers, where in most cases you have no predictable IPs from where they can connect from, you want to avoid whitelisting of IP address here.[9]

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:

[9] 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.

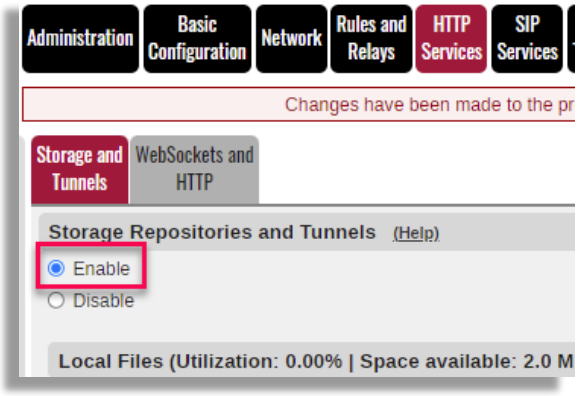

Preloaded Route Rules (Help)
No. From Network Action Delete Row
Add new rows 1 rows.
Default Policy For Preloaded Routes
Reject
Remove
Allow

8 SIParator® HTTP Services Configuration for the Teleworker Gateway

These advanced general HTTP Services are 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.



8.1 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:

8.1.1 Local Files

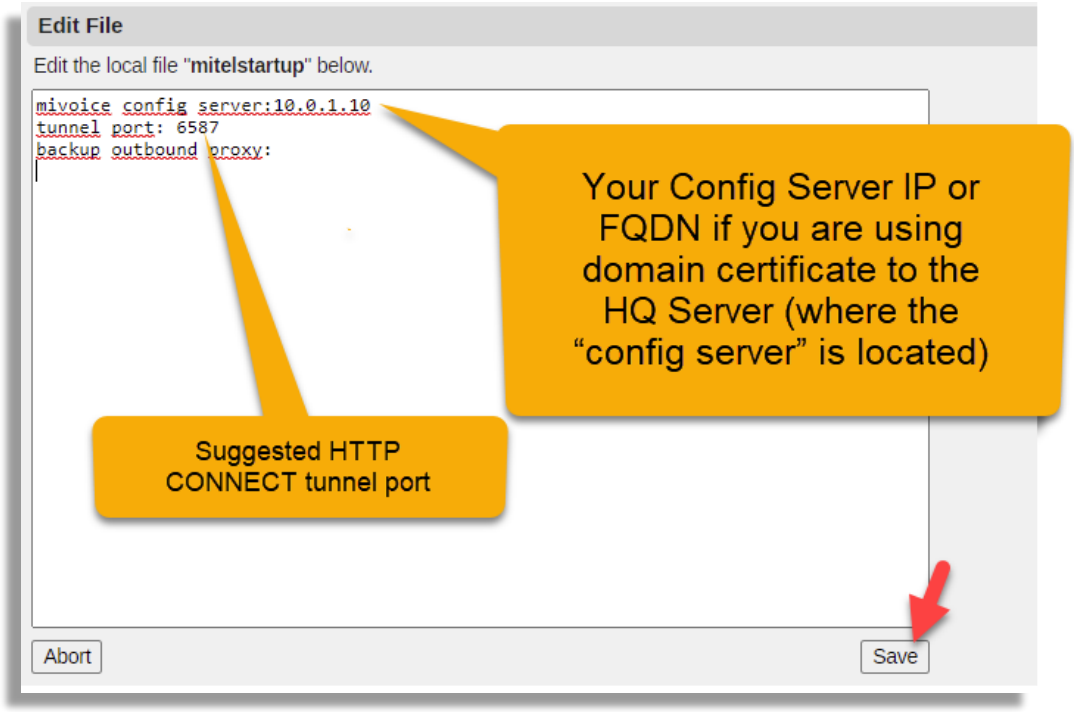
A file hosted locally on the unit. You can edit, upload and download a file. Attach a file entry to one or more Local File Groups. A SHA256 checksum file (with the suffix .sha256) is automatically created for each file entry.

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.

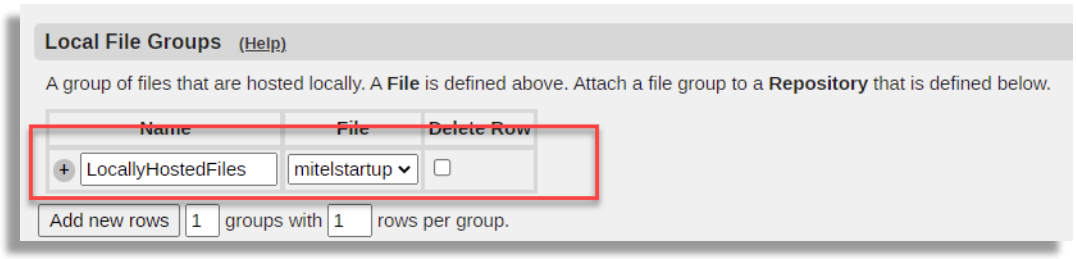
NOTE: For the first line "mivoice config server:", in case you are using a domain certificate (as opposed for a certificate for a fixed IP address) for the HQ Server where the "config server" is located, you MUST

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 4.2.3 DNS Considerations.

8.1.2 Local File Groups

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

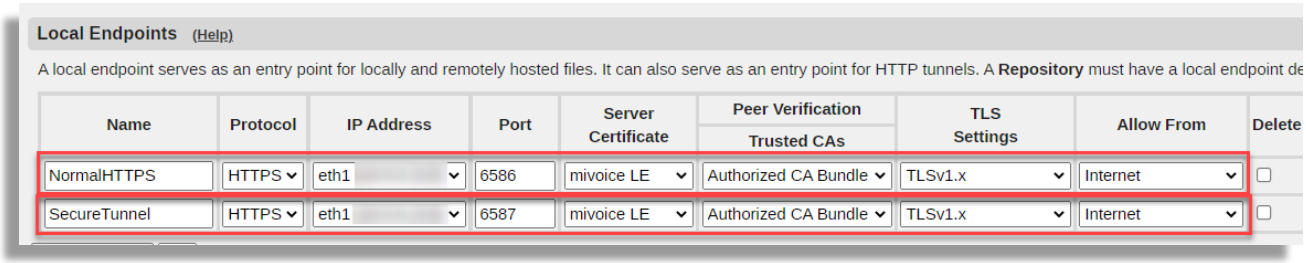
Here you will create a group name to associate to all files that are hosted locally. In our case this group will have only one file, already defined in the previous step.



8.2 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[10] 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.

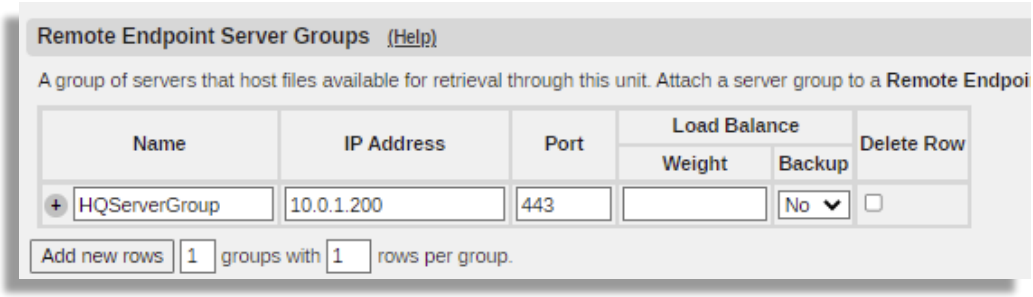
As Teleworkers' IP addresses generally are not predictable, or even in some cases dynamically changing, we will allow access from "Internet"

[10] Configurable in startup.cfg, see 8.1 Hosting startup.cfg

8.3 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.

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.

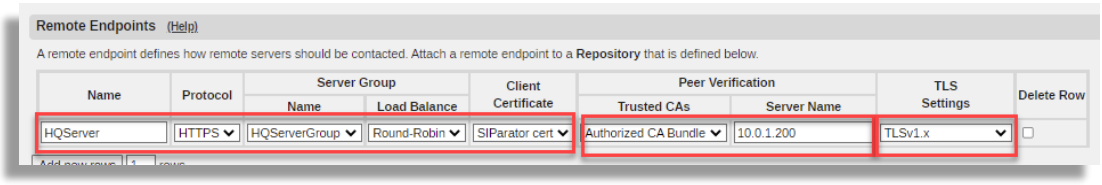


All other internal destinations will be accessible only via http connect tunnels.

8.4 Remote Endpoints

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

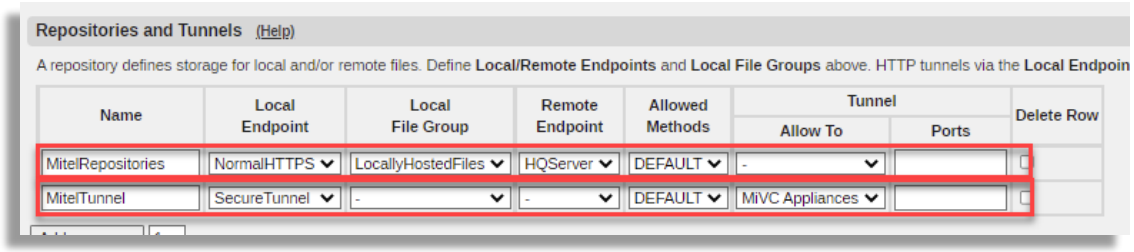
Definition of specific destinations under a group are known as remote endpoints, and we will need to define which protocol will be used and if it is going to be mutual in the case of TLS by completing "Peer Verification". Server Name must match CN on the certificate of the Server connecting to.



NOTE: Make sure the Authorized Bundle includes the MiNET CA certificate and any 3rd Party CA for the HQ Server, as detailed in section 6.

8.5 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.

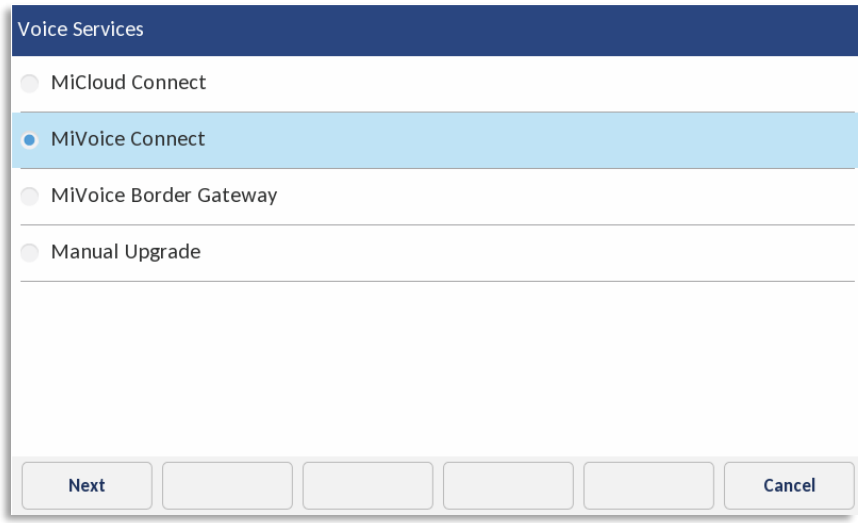
9 Mitel 6900s Phones are Now Ready to be Used Remotely

In this section we will explain how 6900 endpoints are provisioned out-of-the-box.

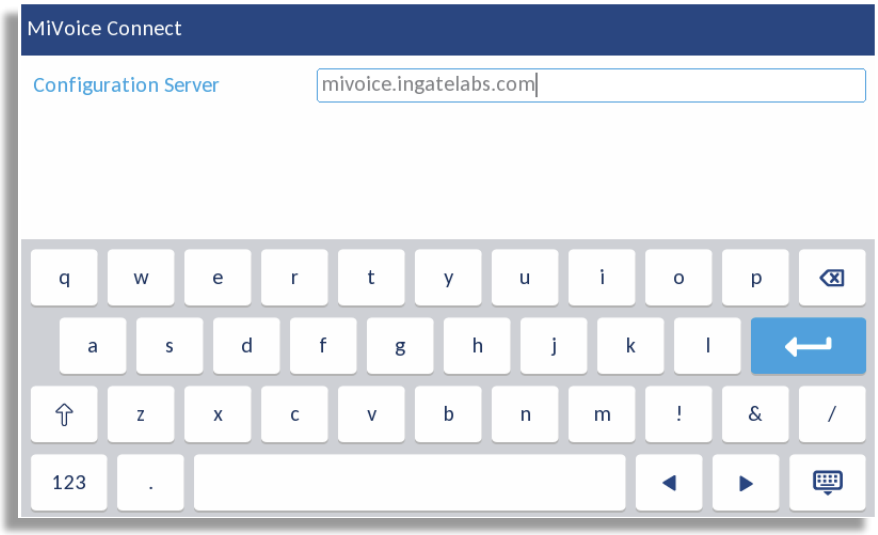
Any new 6900 phone will come from factory with MiNET firmware version 1.6.0.25 or newer. In case you need this version, it can be downloaded from here

9.1 Initial out-of-the-box Boot (MiNET firmware preloaded)

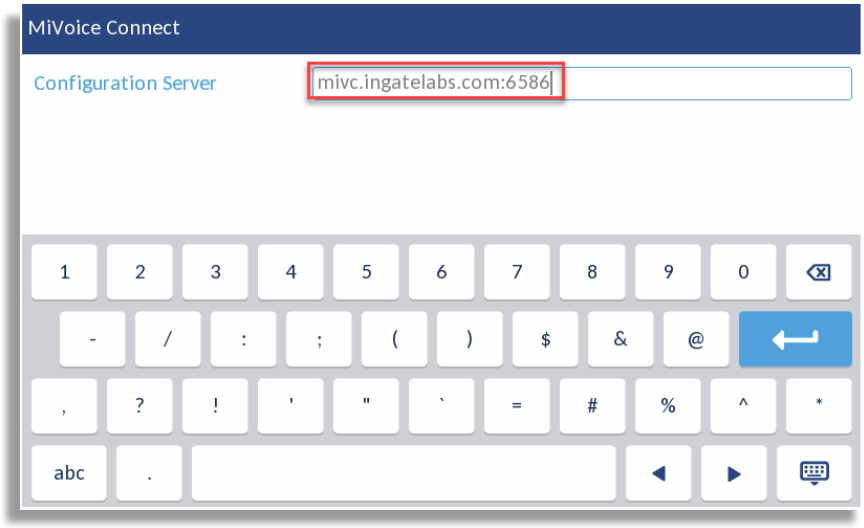
Once the device has booted up, you'll get a provisioning screen like this (using 6940 for illustration):



Select MiVoice Connect and enter SIParator® 's FQDN:



In case you decided to use a port other than 443, you can add it in the TUI like <FQDN>:<port> as far as it is properly configured in the HTTP Services Section.

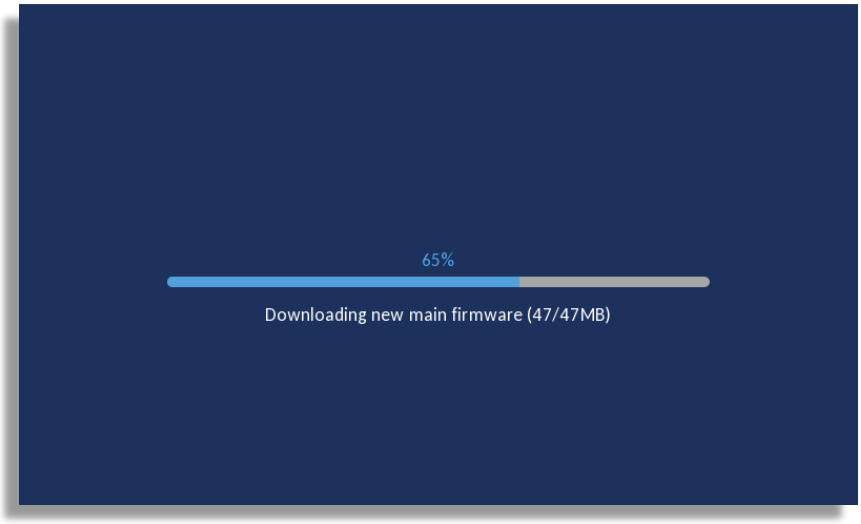


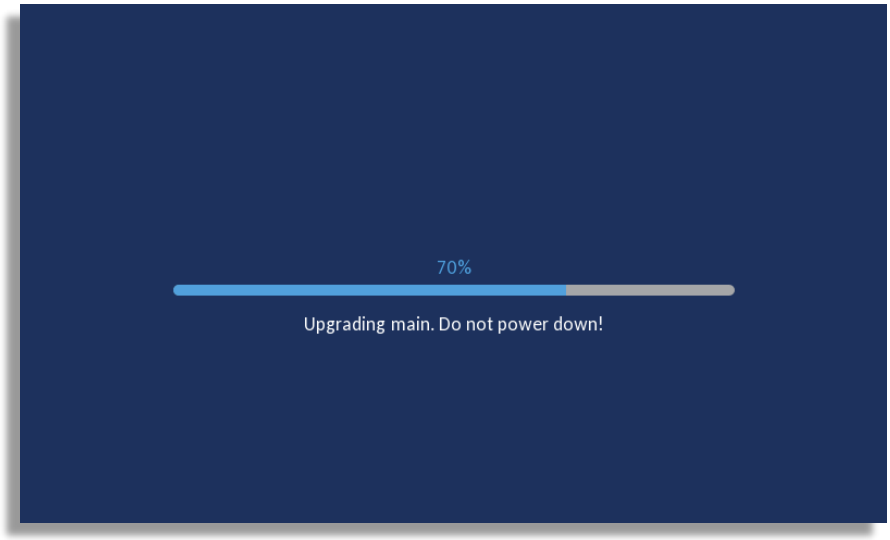
Click Enter and then Save.

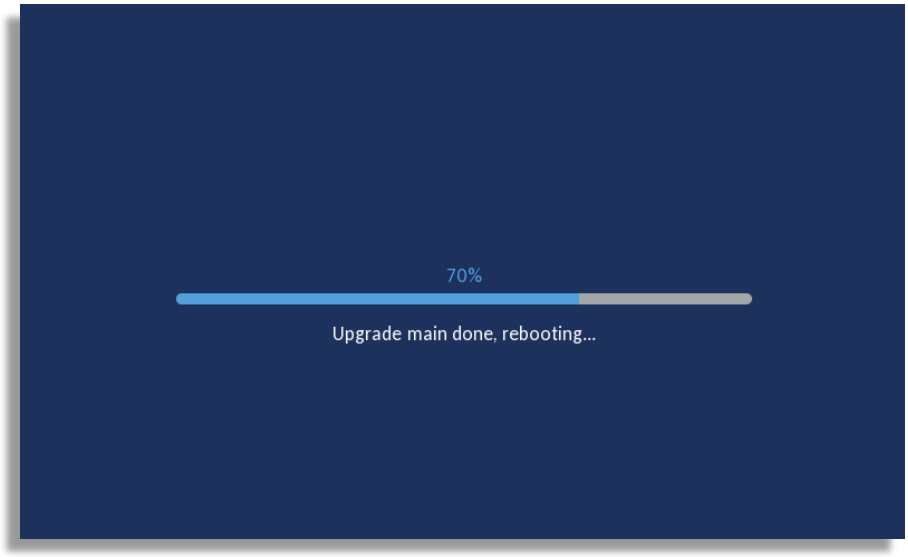
9.2 Version Selection and Update

Once the reboot process begins, the phone will establish MTLS connection with SIParator® to request for version.txt file. SIParator® will obtain and respond back to the Phone with the file obtained from HQ Server.

After identifying the SIP software version needed, it will automatically start downloading it. In our case and based on previously configured data in version.txt, 6.2.0.29 will be loaded in the phone, and rebooted once completed.



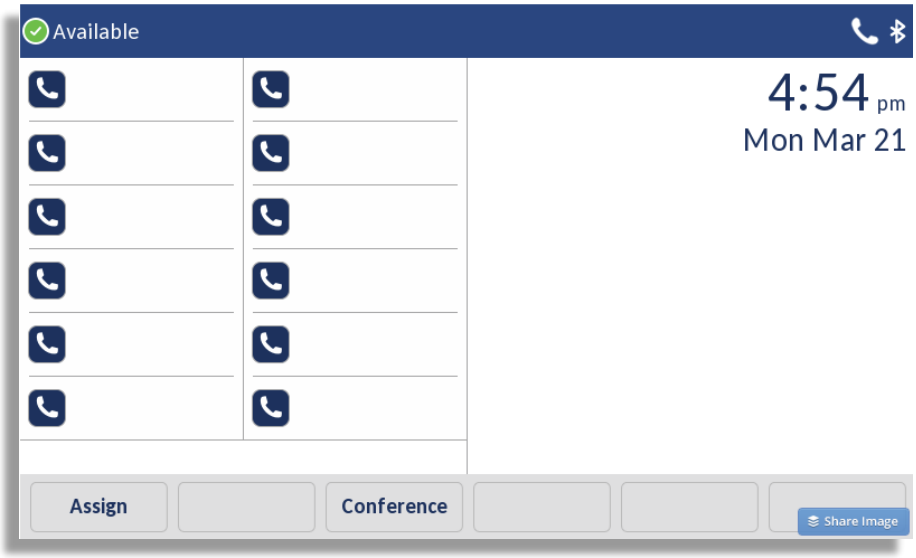




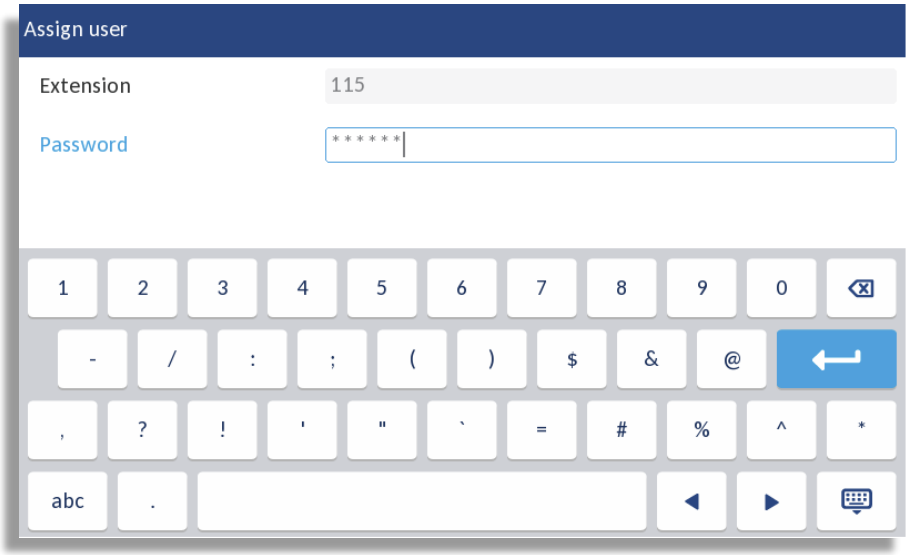
The phones keep a cookie to remember the SIParator® FQDN (Configuration Server for the remote phone)

The phone will then be using the latest SIP Firmware provided by the HQ Server and initiate the initial anonymous initial registration for provisioning.

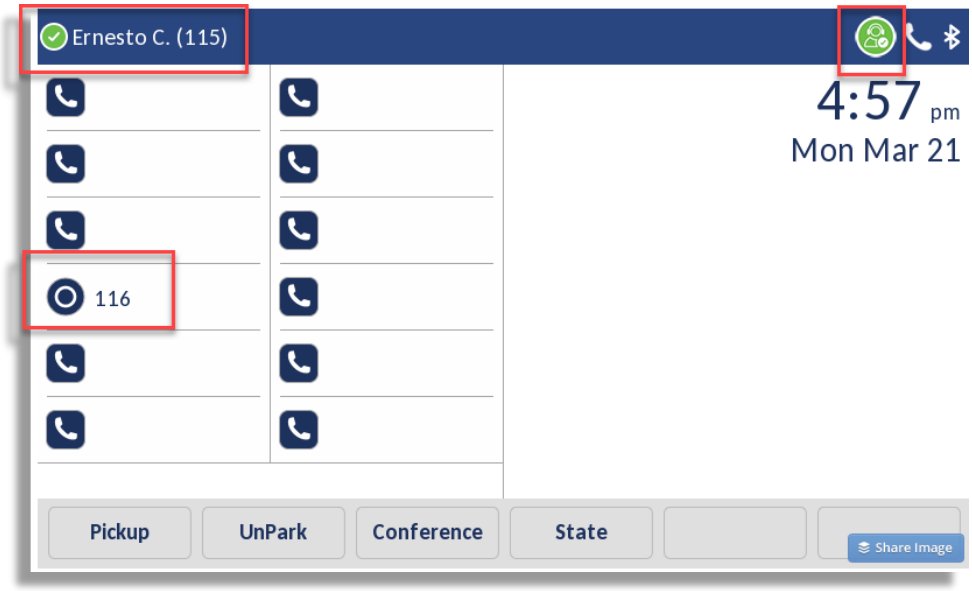
After the process is completed, you'll see the Phone interface like this:



To assign an extension from the TUI, just click on Assign button, introduce extension and password provided by the administrator.



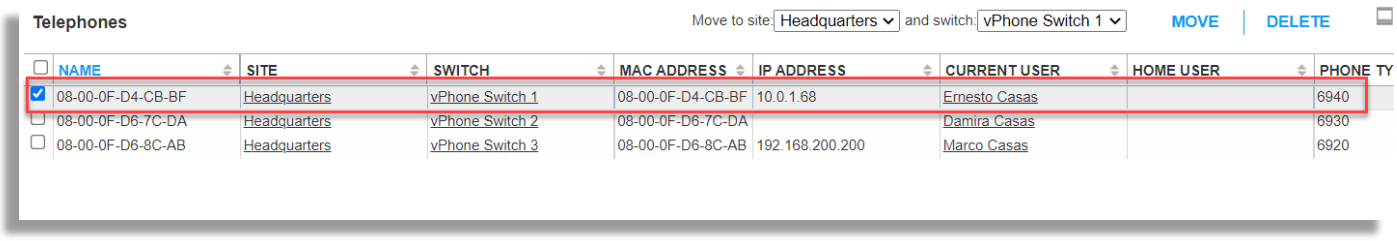
After the assignment is accepted, you'll see the extension assigned in the phone screen, which includes features assigned to the extension such as BLF, Agent status, etc.:



9.3 Loading with New Firmware and Phone Registration

From this point on, the phone will connect to the configuration server and will follow the steps to provision the phone based on what the administration has decided to do. In our case, phones are only registered (anonymous), and extension assignment can be done via TUI for testing purposes and to confirm CAS is working.

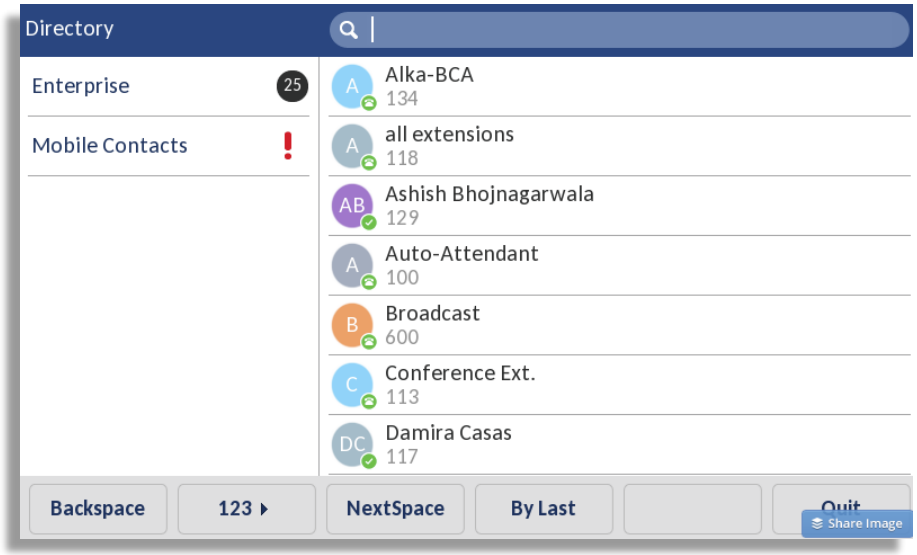
You can confirm that a device is registered in MiVC Director and that the extension is properly assigned.



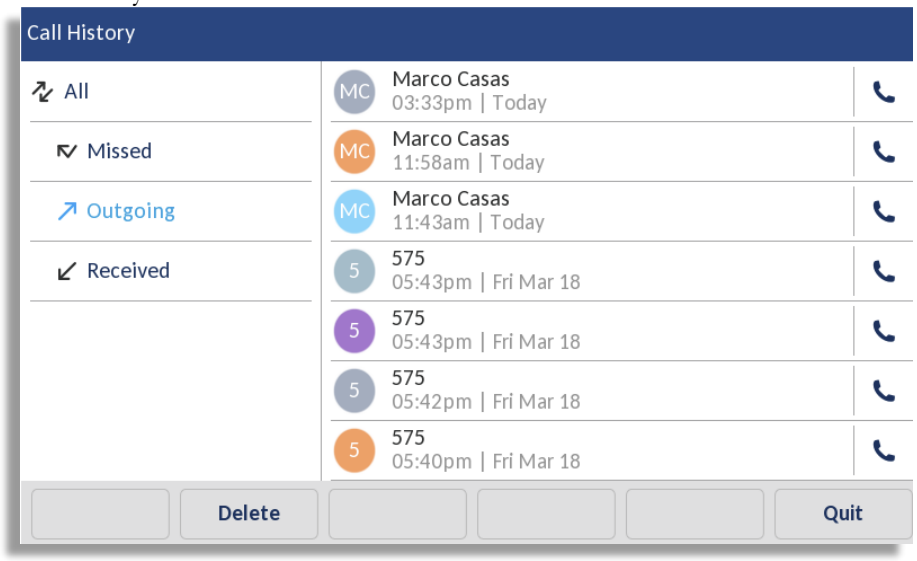
It shows the switch associated to the phone and the IP address matches the internal interface of the SIParator®.

You can test a few CAS based features to confirm everything is good as expected.

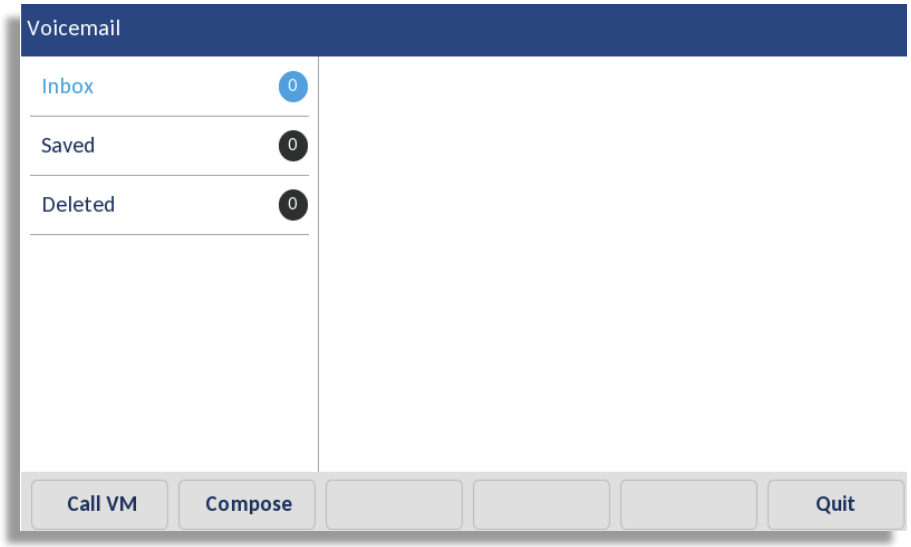
Check company Directory:



Call History:



Voice Mail:



BCA (Bridged Call Appearance)

10 Appendix I

The following list can help to identify "Interoperability" and "Sessions and Media" parameters needed under SIP Services adjusted versus default recommended values specifically needed for Ingate SIParator® Teleworker Gateway deployments.

10.1 SIP Services - Interoperability

Use lr=true:
Default value: "No"

Relaxed Refer-To:
Default value: "No"

Add expires header:
Default value: "Never"

SIP URI encoding:
Default Value: "Always encrypt URIs"
Needed value for Teleworker Gateway: "Keep username in URIs"

Send re-INVITEs all the way directly:
Default value: "Yes"

Loose username check:
Default value: "No"

Match on username and domain:
Default value: "Yes"
Needed value for Teleworker Gateway: "Match only on username"

Force outbound Record-Route:
Default value: "No"

Always force Record-Route:
Default value: "No"

Accept TCP marked as TLS:
Default value: "No"

Allow large UDP packets:
Default value: "No"

Remove headers in 180 responses:
Default value: "No"

Forward CANCEL body:
Default value: "No"

Use CANCEL body in ACK:
Default value: "No"

Use RFC 2543 behavior for Hold SDP:
Default value: “No”

Force RFC 3264 Compliance for Hold SDP:
Default value: “No”

Inhibit hold:
Default value: “Allow hold”

Force "inactive" attribute for "on-hold" SDP:
Default value: “No”

Strip ICE attributes:
Default value: “No”

Add ourselves as ICE Candidate
Default value: “Yes”

Keep User-Agent header:
Default value: “No”

Add codecs to new SDP offer in re-INVITE:
Default value: “No”

Use RTCP attribute:
Default value: “Yes”

Keep To header in forwarded requests:
Default value: “No”

Add Failover header:
Default value: “No”

DNS override when redirecting on 3xx:
Default value: “Yes”

Open port 6891 for file transfer:
Default value: “No”

Allow RFC 2069 authentication:
Default value: “No”

Match Refer-To on Call-ID in Replaces:
Default value: “Yes”

Pretend to support "privacy" option tag in the proxy:
Default value: “No”

Force username in registered Contact:
Default value: “No”

Fix BYE Route set:
Default value: “No”

Fix Bad Route set:
Default value: “No”

Receive PRACK in B2BUA:
Default value: “Yes”

Send PRACK in B2BUA:
Default value: “Yes”

Tear down media state when handling re-INVITEs:
Default value: “No”

Always send B2BUA offer in INVITE:
Default value: “No”

Detect unchanged session version in B2BUA:
Default value: “No”

Disable re-INVITEs:
Default value: “No”

Disable Supported Header in B2BUA:
Default value: “No”

Enable GRUU passthrough:
Default value: “No”

Add Path Header in REGISTER requests:
Default value: “No”

Terminate Transferor on 183:
Default value: “No”

Convert escaped whitespaces:
Default value: “No”

Ignore URI port when using the maddr attribute:
Default value: “No”

Remove SDP from 1xx Provisional Responses:
Default value: “No”

Match also port in Request-URI in Dial Plan:
Default value: “No”

Use session identifier when comparing endpoint SDPs:
Default value: “No”

Update Username Mapping on Refer-To:
Default value: “No”

Accept Late Media Source Change for RSC:
Default value: “No”

Translate Refer-To:
Default value: “Yes”

Convert 5xx Responses to 503:
Default value: “No”

Allow RTP before answer SDP:
Default value: “No”

ContactRouteTag based Routing:
Default value: “No”
Needed value for Teleworker Gateway: “Yes”. Will enable and show:
Contact Head:
Default value: “+sip.instance="<urn:uuid:00000000-0000-1000-8000-“
Contact Tail:
Defaul value: “>”

Remove Via Headers
Default values: “all fields/table empty”

Remove Via Headers for all SIP servers:
Default value: “No”

Translation Exceptions
Except This From Translation
Default value: “table empty”

Force Translation
Always Translate This
Default value: “table empty”

Force Remote TLS Connection Reuse
Default value: “table empty”

Media stream reuse time:
Default value: “0”

Hide our Record-Route header
Default value: “table empty”

Hide our Record-Route header for all SIP servers:
Default value: “No”

Force RTP Packetization Time:

Default value: “blank”

Sequential Register Delay:
Default value: “blank”

Forward 3xx headers
Default value: “table empty”

Contact SIP URI Parameters to keep in REGISTERs
Default value: “table empty”

Add DTMF Payload type:
Default value: “blank”

Add DTMF Payload type for:
Default value: “table empty”

Copy headers from REFER to INVITE in the B2BUA:
Default value: “blank”

10.2 SIP Services - Sessions and Media

Use Media Proxy:
Default value: “No”

Always use the Media Proxy:
Default value: “No”

Limitation of sender of media streams:
Default value: “Lock IP address and port to first sender”
Needed value for Teleworker Gateway: “Allow multiple sender IP addresses and ports”

Support forked media streams:
Default value: “No”

Tear down media streams:
Default value: “No”

Always Relay Media:
Default value: “No”

Reuse port numbers when changing media:
Default value: “No”

Reuse port numbers within same session:
Default value: “Don't reuse port numbers”

Detect codec changes in mid call answers in the B2BUA:
Default value: “Detect only changes to the first payload type listed”
Needed value for Teleworker Gateway: “Detect changes to all payload types (except dynamic)”

Use codec limitation:
Default value: “No”

Play local ringback at call transfer:
Default value: “Never”

Ring tone for Local ringback:
Default value: “US ring tone”

Redirect calls on hold to Music on Hold server:
Default value: “No”

Resolve domain names in the SDP:
Default value: “No”

Session timer (s):
Default value: “14400”

Timeout for SIP over TCP/TLS (s):
Default value: “90”

Allowed amount of concurrent sessions:
Default value: “blank”

Allowed number of senders:
Default value: “10”

Allowed amount of media streams per SIP session:
Default value: ”6”

Timeout for one-way streams (s):
Default value: ”blank”

Timeout for RTP streams (s):
Default value: “blank”

Timeout for RTCP streams (s):
Default value: “blank”

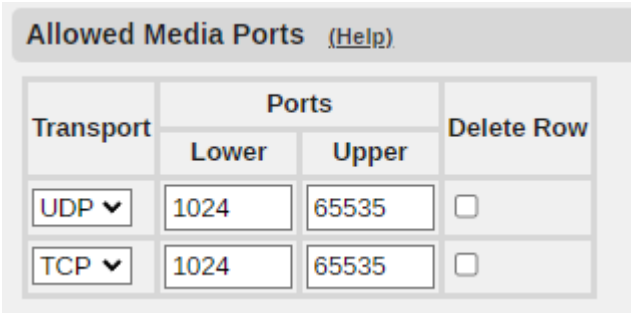
Third Party Call Control Codecs
Default values:

No.	Name	Payload Type	Rate	Channels	Parameters	Delete Row
1	PCMU					☐
2	G729				annexb=yes	☐
3	telephone-ever	96	8000		0-15	☐

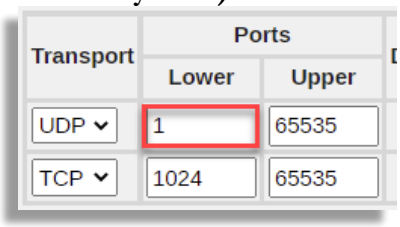
Limitation of RTP Codecs
Default value: “Allow all codecs”

Allowed Media Ports

Default values:



Temporary usage for current MiVC software for Teleworker Gateway has been (but should not be needed anymore):



Strip SDP Lines
Default value: "empty table"

Music on Hold Server
Default value: "leave calls on hold as they are"

Default timeout for INVITE requests (s):
Default value: "180"

Maximum timeout for INVITE requests (s):
Default value: "300"

SIP blacklist interval (s):
Default value: "41"

B2BUA request pending timeout (s):
Default value: "0"

Base retransmission timeout for SIP requests (s):
Default value: "0.5"

Maximum amount of retransmissions for INVITE requests:
Default value: "6"

Maximum amount of retransmissions for non-INVITE requests:
Default value: "10"

Limit Max-Forwards:
Default value: "70"

Maximum SIP packet size (bytes):
Default value: "131072"