A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise

Configure MBG for WEBRTC - Operating Instructions

Release 9.6 SP1
Document Version 2.0

June 2023

Mitel
Powering connections

Notices

Trademarks

INTRODUCTION

The Web Agent application contains WebRTC components so that it can be used as a WebRTC powered soft phone for voice calls. This requires that a Mitel Border Gateway (MBG) to be configured as a WebRTC Gateway connected to the MX-ONE call manager. It is highly recommended that the technician configuring the MBG system is trained and certified on that product.

To have the WebRTC calls to work you need access to:

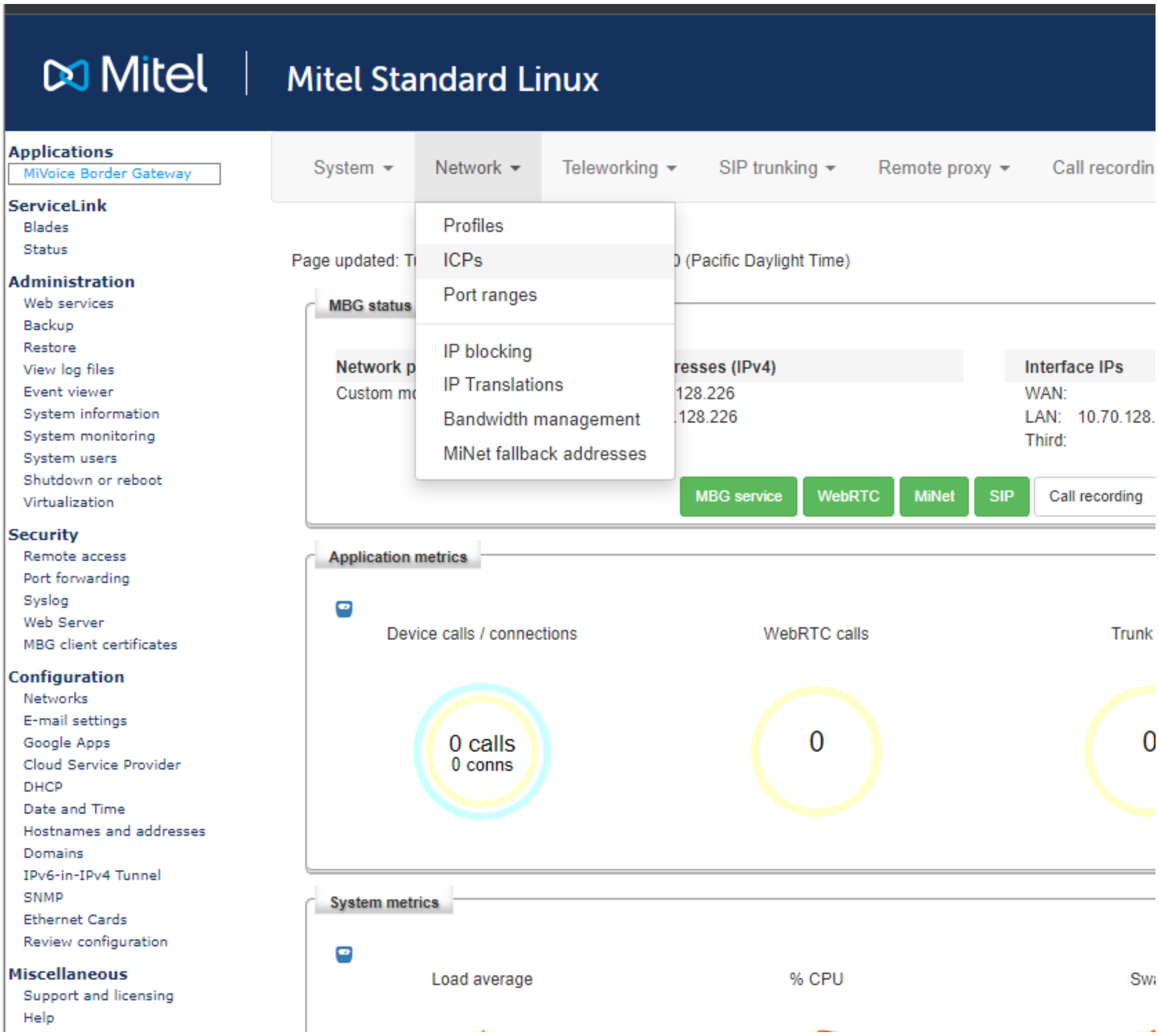
- MBG server
  Note: In this release, the MBG used by the MiCC Enterprise WebRTC Web Agents cannot be configured to use the WebRTC Pro feature, so recording via MBG's SRC ports cannot be done. This will be supported in a future release of MBG. In the meantime, in order to be able to record WebRTC Web Agents it is recommended that the TAS based recording feature is used together with Mitel Interaction Recorder (MIR).

- MXONE Server

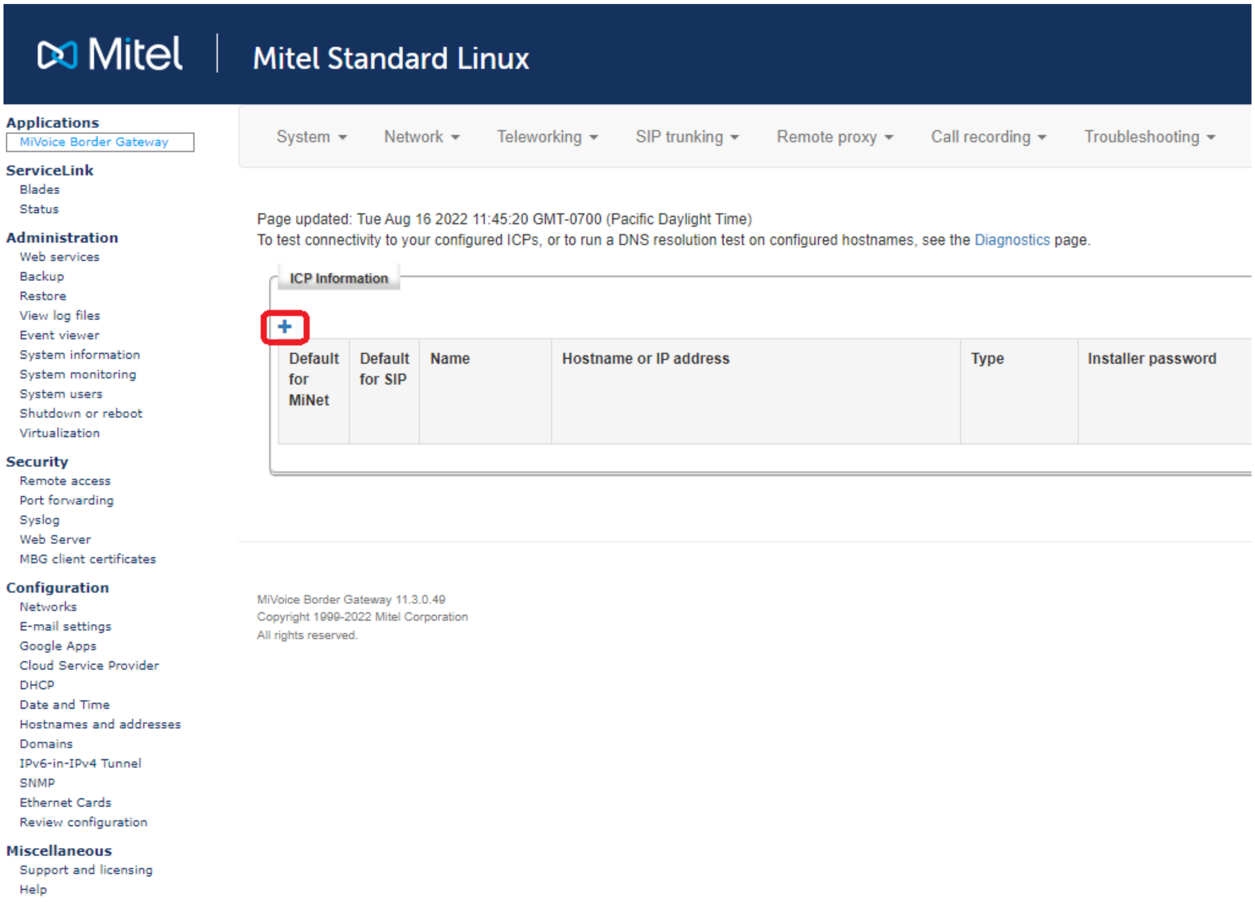
- Optionally: Test Client / MBG inbuilt test client

MBG SERVER CONFIGURATION

1. The very first thing we need to do is to create an ICP. From the top menu, select “Network->ICPs”.



2. On the ICPs page, click the “+” icon to add a new ICP.

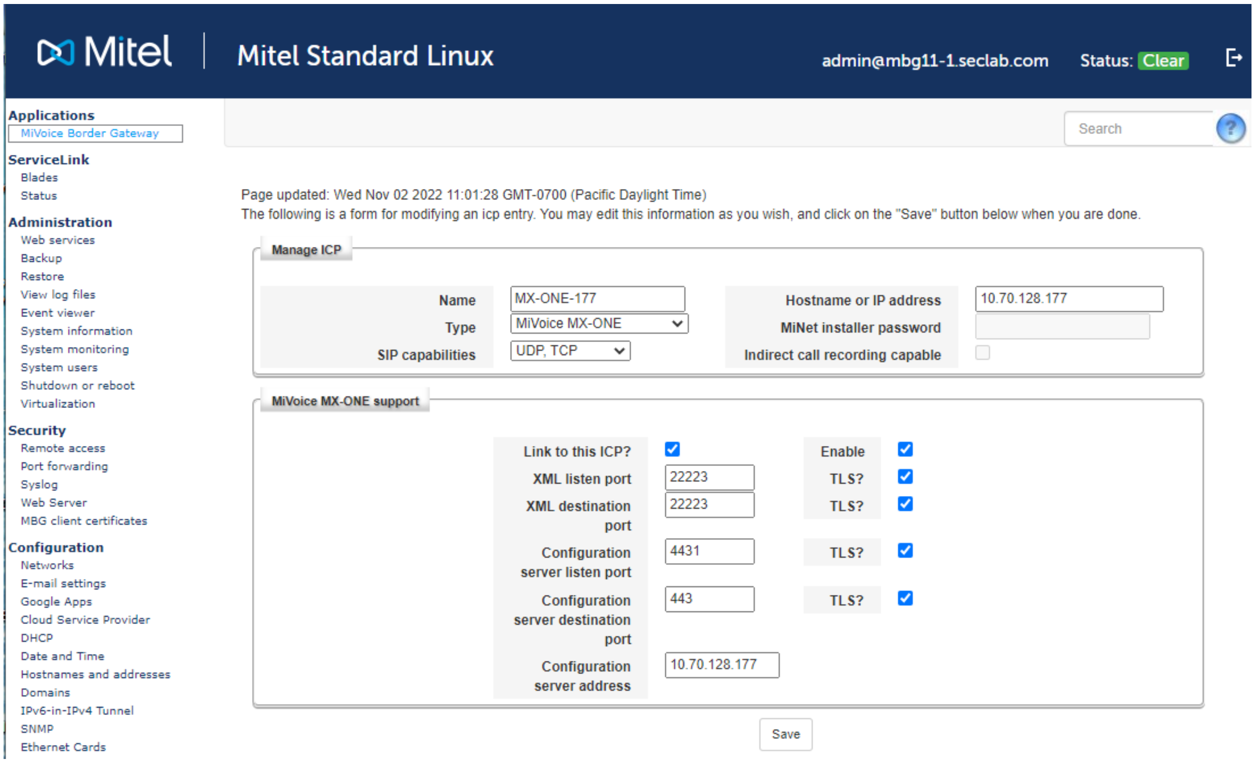


Page updated: Tue Aug 16 2022 11:45:20 GMT-0700 (Pacific Daylight Time)
To test connectivity to your configured ICPs, or to run a DNS resolution test on configured hostnames, see the Diagnostics page.

Default for MiNet	Default for SIP	Name	Hostname or IP address	Type	Installer password

MiVoice Border Gateway 11.3.0.49
Copyright 1999-2022 Mitel Corporation
All rights reserved.

3. On “Manage ICP” page, enter a name which can be anything you want. For the “Type” field, select “MiVoice MX_ONE”. For the “SIP capabilities” field, select “UDP, TCP, TLS”. For the “Hostname or IP address” field, enter the MXONE IP address. Click the “Save” button.



Page updated: Wed Nov 02 2022 11:01:28 GMT-0700 (Pacific Daylight Time)
The following is a form for modifying an icp entry. You may edit this information as you wish, and click on the "Save" button below when you are done.

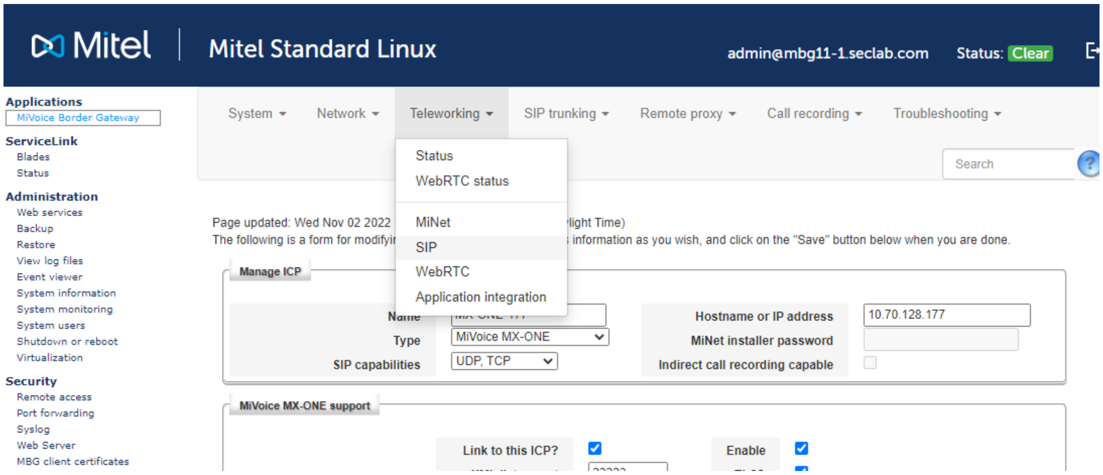
Manage ICP

Name	MX-ONE-177	Hostname or IP address	10.70.128.177
Type	MiVoice MX-ONE	MiNet installer password	
SIP capabilities	UDP, TCP	Indirect call recording capable	□

MiVoice MX-ONE support

Link to this ICP?	☑	Enable	☑
XML listen port	22223	TLS?	☑
XML destination port	22223	TLS?	☑
Configuration server listen port	4431	TLS?	☑
Configuration server destination port	443	TLS?	☑
Configuration server address	10.70.128.177		

4. Now we need to add a SIP teleworker user that will be making WebRTC calls. We have to program this user in MBG and in MXONE. From the top menu, select “Teleworking->SIP”.



Page updated: Wed Nov 02 2022 ...light Time)
The following is a form for modifyi... information as you wish, and click on the "Save" button below when you are done.

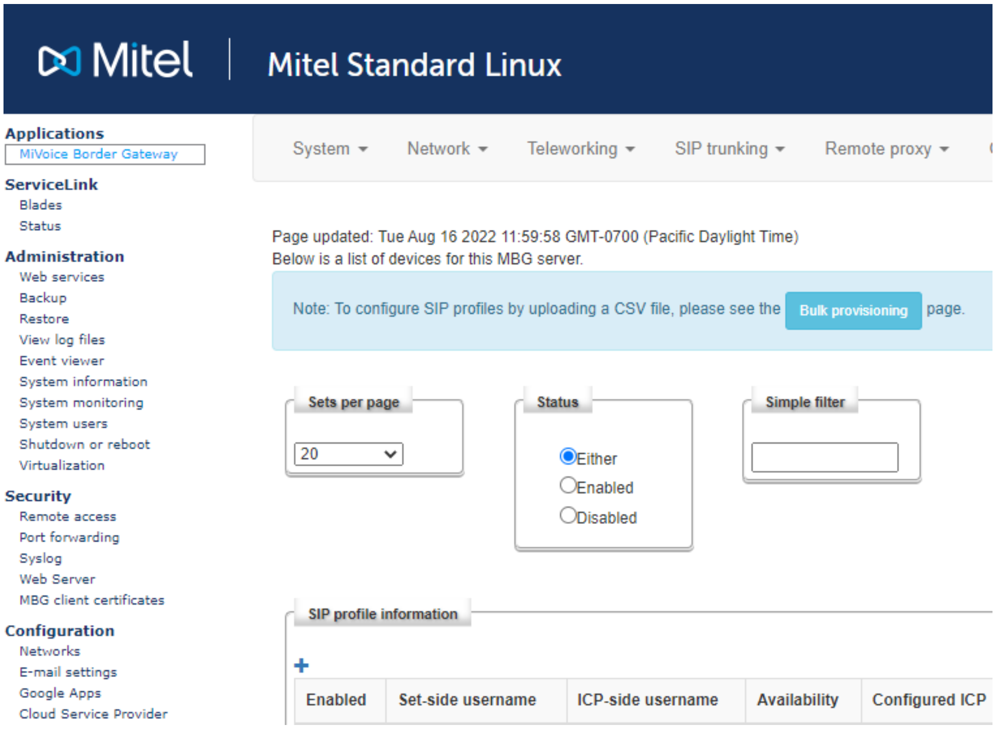
Manage ICP

Name	MX-ONE-177	Hostname or IP address	10.70.128.177
Type	MiVoice MX-ONE	MiNet installer password	
SIP capabilities	UDP, TCP	Indirect call recording capable	□

MiVoice MX-ONE support

Link to this ICP?	☑	Enable	☑

5. In the “SIP profile information” section, click on the “+” icon to add a new teleworking user.



Page updated: Tue Aug 16 2022 11:59:58 GMT-0700 (Pacific Daylight Time)
Below is a list of devices for this MBG server.

Note: To configure SIP profiles by uploading a CSV file, please see the Bulk provisioning page.

Sets per page: 20

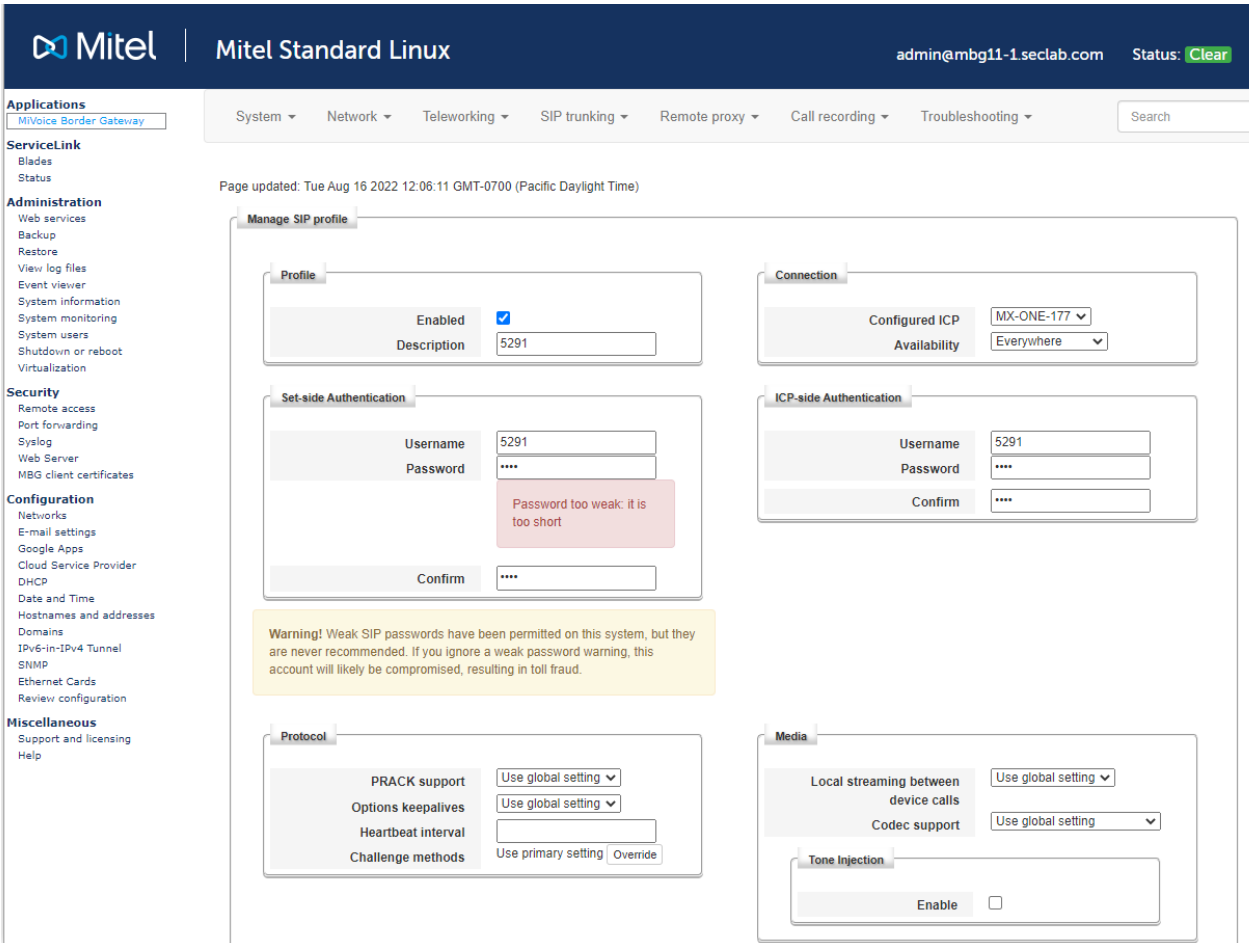
Status: ● Either ○ Enabled ○ Disabled

Simple filter:

SIP profile information

Enabled	Set-side username	ICP-side username	Availability	Configured ICP

6. In the “Manage SIP profile” page, check the “Enable” checkbox. For both “Set-side username” and “Icp-side username” fields, use the extension we plan to use as the UC Endpoint user in MXONE. For the “Configured ICP” dropdown, select the MXONE we just created at step 3 above. For both set-side and icp-side passwords, use the SIP password same as the extension number. Click the “Save” button.



Page updated: Tue Aug 16 2022 12:06:11 GMT-0700 (Pacific Daylight Time)

Manage SIP profile

Profile

Enabled ☑

Description 5291

Connection

Configured ICP MX-ONE-177

Availability Everywhere

Set-side Authentication

Username 5291

Password ••••

Password too weak: it is too short

Confirm ••••

ICP-side Authentication

Username 5291

Password ••••

Confirm ••••

Warning! Weak SIP passwords have been permitted on this system, but they are never recommended. If you ignore a weak password warning, this account will likely be compromised, resulting in toll fraud.

Protocol

PRACK support Use global setting

Options keepalives Use global setting

Heartbeat interval

Challenge methods Use primary setting Override

Media

Local streaming between device calls Use global setting

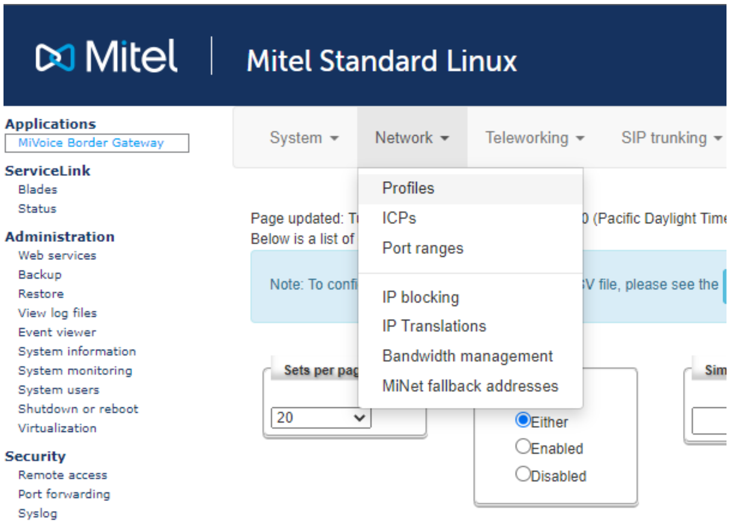
Codec support Use global setting

Tone Injection

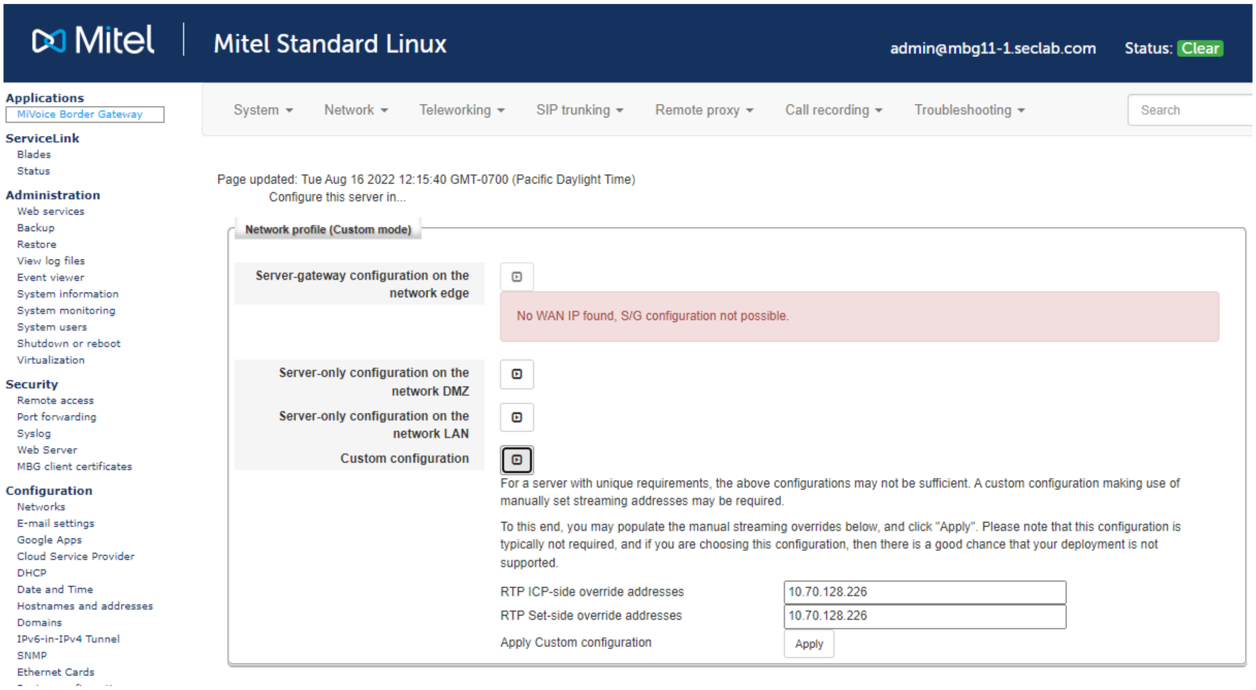
Enable □

MBG may not allow you to add weak passwords, in that case go to System → Settings → Find “Permit weak SIP passwords“ in the very bottom of the page and enable the checkbox.

7. We now need to create a Network profile before we can configure WebRTC. From the top menu, select "Network->Profiles".



8. In "Network profile" page, click on the right-arrow on the right of "Custom Configuration", enter the MBG IP address for both "RTP ICP-side override addresses" and "RTP Set-side override addresses" and click the "Apply" button.



Page updated: Tue Aug 16 2022 12:15:40 GMT-0700 (Pacific Daylight Time)
Configure this server in...

Network profile (Custom mode)

Server-gateway configuration on the network edge ⊡

No WAN IP found, S/G configuration not possible.

Server-only configuration on the network DMZ ⊡

Server-only configuration on the network LAN ⊡

Custom configuration ⊡

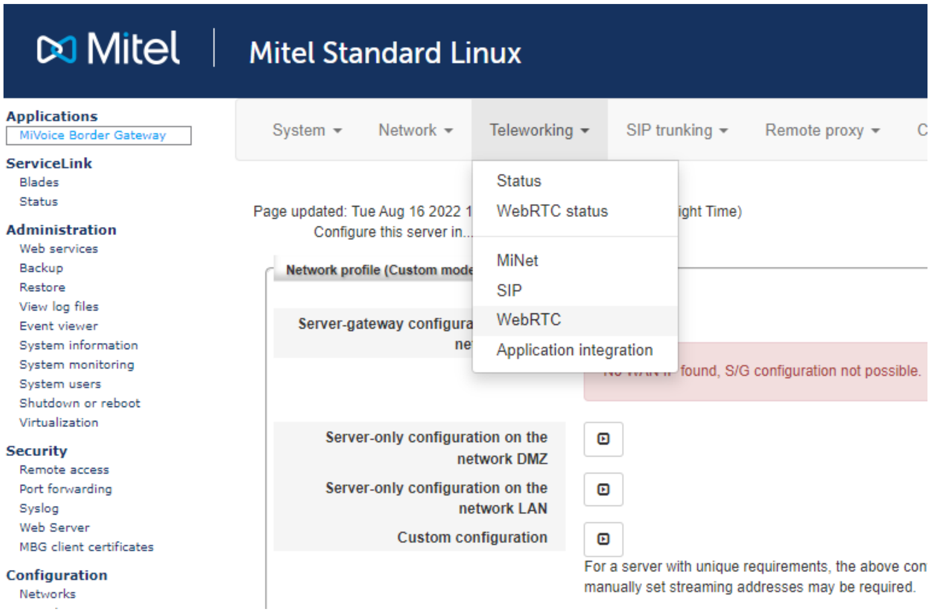
For a server with unique requirements, the above configurations may not be sufficient. A custom configuration making use of manually set streaming addresses may be required.

To this end, you may populate the manual streaming overrides below, and click "Apply". Please note that this configuration is typically not required, and if you are choosing this configuration, then there is a good chance that your deployment is not supported.

RTP ICP-side override addresses	10.70.128.226
RTP Set-side override addresses	10.70.128.226
Apply Custom configuration	Apply

9. If the network profile is created successfully, you will see "Custom mode" beside the "Network profile" label.

10. Now we need to configure WebRTC, from the top menu, select “Teleworking->WebRTC”.



11. In “WebRTC” page, click the “Enabled” checkbox.

a. For the “Hosting mode” dropdown, select “Host WebRTC client locally”.

b. For “Webserver shared secret” field, just enter something, it is not used but something must be entered.

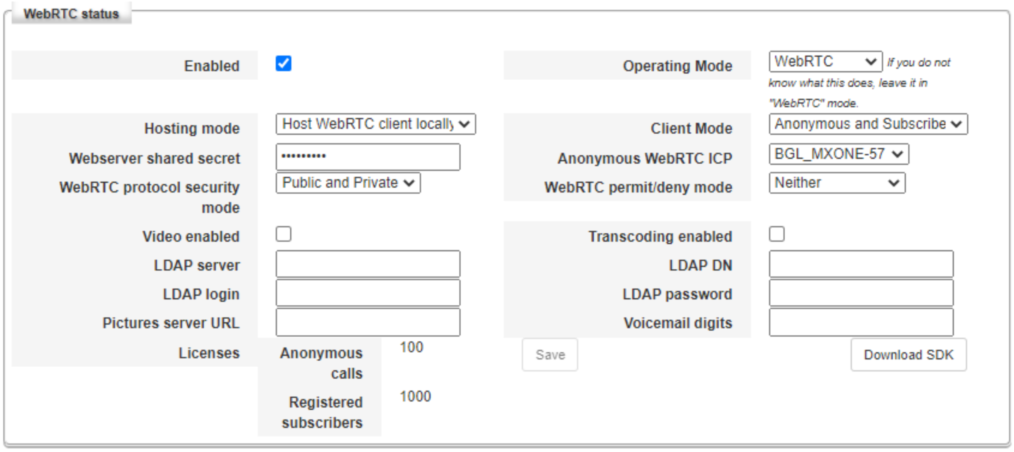
c. For the “WebRTC protocol security mode” field, just select “Public and Private”.

d. “Video enabled” should be unchecked.

e. For the “Mode” field, select “Anonymous and Subscriber”.

f. Anonymous WebRTC ICP - Select the Configured ICP name

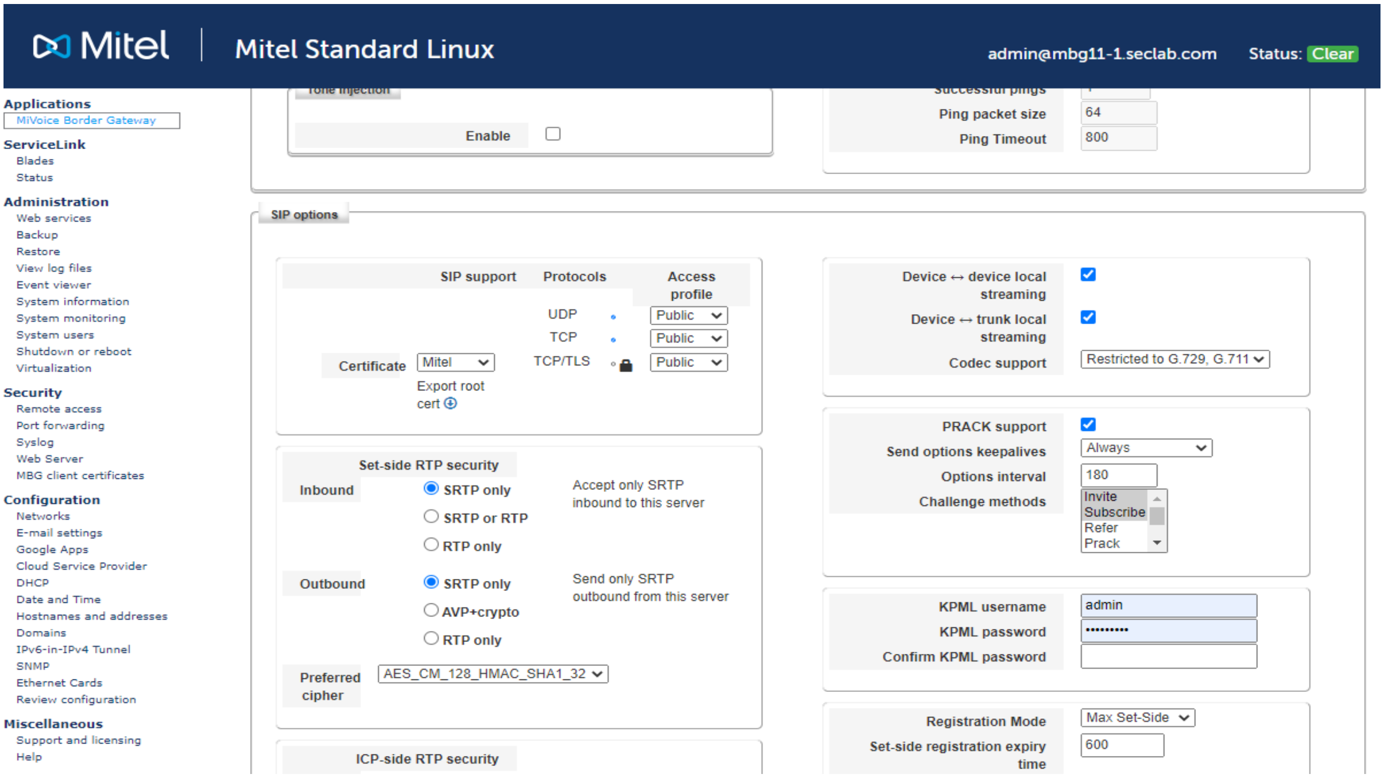
g. WebRTC whitelist/blacklist mode - choose “neither“



WebRTC status

Enabled	☑	Operating Mode	WebRTC ▾ *If you do not know what this does, leave it in "WebRTC" mode.*
Hosting mode	Host WebRTC client locally ▾	Client Mode	Anonymous and Subscribe ▾
Webserver shared secret	•••••••••	Anonymous WebRTC ICP	BGL_MXONE-57 ▾
WebRTC protocol security mode	Public and Private ▾	WebRTC permit/deny mode	Neither ▾
Video enabled	☐	Transcoding enabled	☐
LDAP server		LDAP DN	
LDAP login		LDAP password	
Pictures server URL		Voicemail digits	
Licenses	Anonymous calls 100 Registered subscribers 1000	Save	Download SDK

12. Now we need to enable SIP option. From the top menu, select “System->Settings”, in the “SIP options” section, enable UDP, TCP and TCP/TLC protocols.



Tone injection
Enable □

Successful pings
Ping packet size 64
Ping Timeout 800

SIP options

SIP support	Protocols		Access profile
	UDP	●	Public
	TCP	●	Public
Certificate Mitel Export root cert	TCP/TLS	●	Public

Set-side RTP security
Inbound ● SRTP only ○ SRTP or RTP ○ RTP only — Accept only SRTP inbound to this server
Outbound ● SRTP only ○ AVP+crypto ○ RTP only — Send only SRTP outbound from this server
Preferred cipher AES_CM_128_HMAC_SHA1_32

ICP-side RTP security

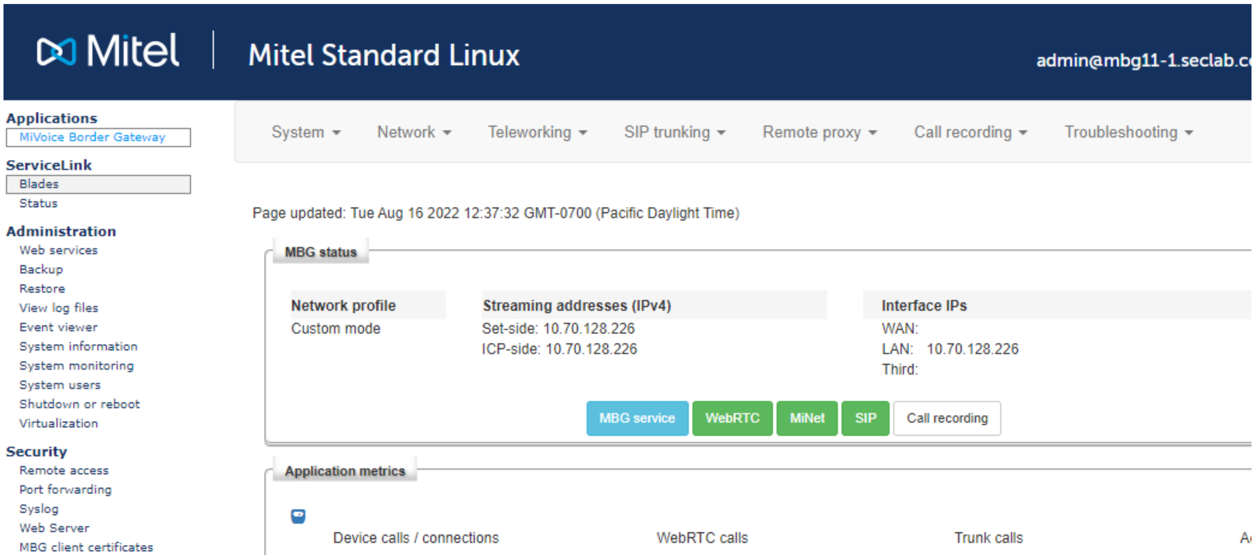
Device ↔ device local streaming ☑
Device ↔ trunk local streaming ☑
Codec support Restricted to G.729, G.711

PRACK support ☑
Send options keepalives Always
Options interval 180
Challenge methods Invite, Subscribe, Refer, Prack

KPML username admin
KPML password •••••••••
Confirm KPML password

Registration Mode Max Set-Side
Set-side registration expiry time 600

13. Now we need to start MBG service. From the top menu, select “System->Dashboard” and click on the “MBG service” button.



Page updated: Tue Aug 16 2022 12:37:32 GMT-0700 (Pacific Daylight Time)

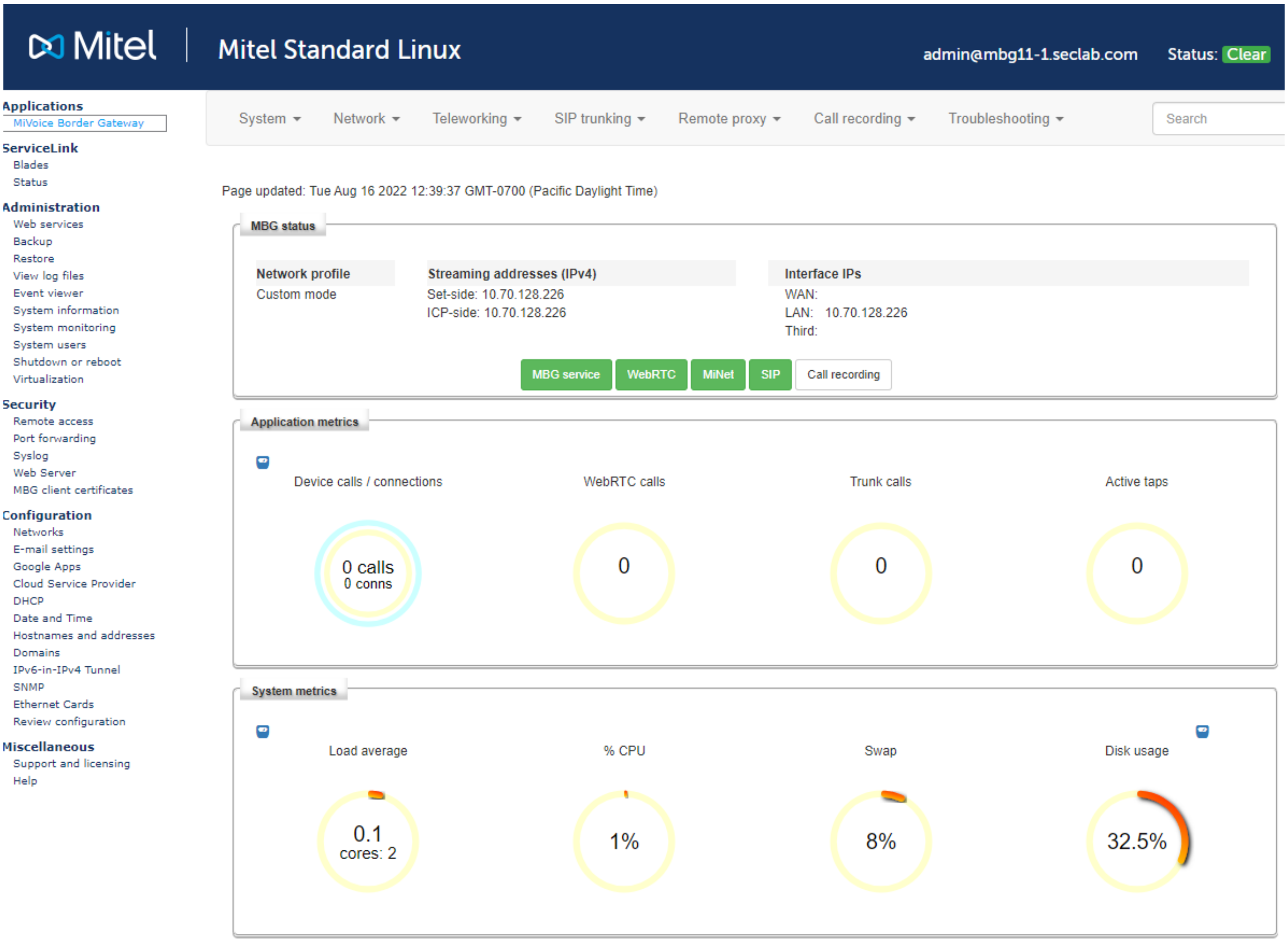
MBG status

Network profile	Streaming addresses (IPv4)	Interface IPs
Custom mode	Set-side: 10.70.128.226 ICP-side: 10.70.128.226	WAN: LAN: 10.70.128.226 Third:

Application metrics

Device calls / connections — WebRTC calls — Trunk calls — A

14. The MBG service should now turn green, and we can continue with MX-ONE configuration.



Page updated: Tue Aug 16 2022 12:39:37 GMT-0700 (Pacific Daylight Time)

MBG status

Network profile	Streaming addresses (IPv4)	Interface IPs
Custom mode	Set-side: 10.70.128.226 ICP-side: 10.70.128.226	WAN: LAN: 10.70.128.226 Third:

Application metrics

Device calls / connections	WebRTC calls	Trunk calls	Active taps
0 calls 0 conns	0	0	0

System metrics

Load average	% CPU	Swap	Disk usage
0.1 cores: 2	1%	8%	32.5%

MX-ONE CONFIGURATION

SIP EXTENSION PASSWORD

For the Registration of any extension to on MBG → WebRTC Gateway the MBG does not accept Register of users without challenging SIP password.

Which means SIP Passwords must be added for extensions on MX-ONE side with MD5 Authentication (and replace the ICP Side Passwords into the corresponding SIP users in MBG).

On MX-ONE side set the passwords for the extensions by the below commands:

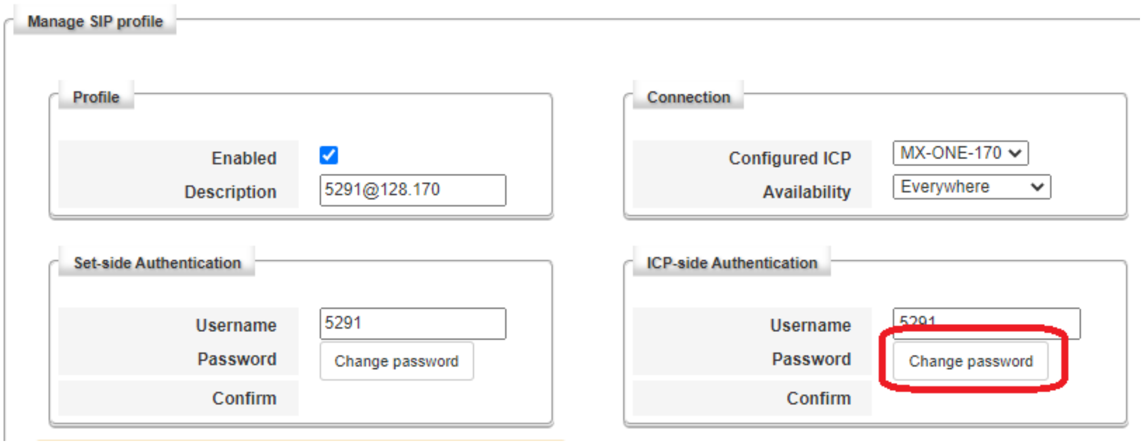
1. `auth_code -i --dir <extension> --auth-code <extension> --csp 0 --cil <extension>`
2. `auth_code --encrypt -d <extension> --hash-type md5a1`
3. `auth_code -p -dir <extension>`

Example:

```
auth_code -i --dir 5291 --auth-code 5291 --csp 0 --cil 5291
auth_code --encrypt --dir 5291 --hash-type md5a1
auth_code -p --dir 5291
```

```
customer dir  auth code                              cil code CSP restr new customer
======== ==== ====================================== ======== === ===== ============
       0 5291 md5a1:3417465e46c5d2b3fb78d0e8489bb278       5291  0     -
```

Copy the highlighted part to the clipboard and open the MBG Configuration tool. Navigate to Mitel Border Gateway->Teleworker->SIP and click to edit the extension. Click on Change Password buttons for the ICP-side Authentication and paste in the encrypted password that was copied from MX-ONE. Don't forget to click Save at the bottom of the page.



Profile

Enabled ☑

Description 5291@128.170

Connection

Configured ICP MX-ONE-170

Availability Everywhere

Set-side Authentication

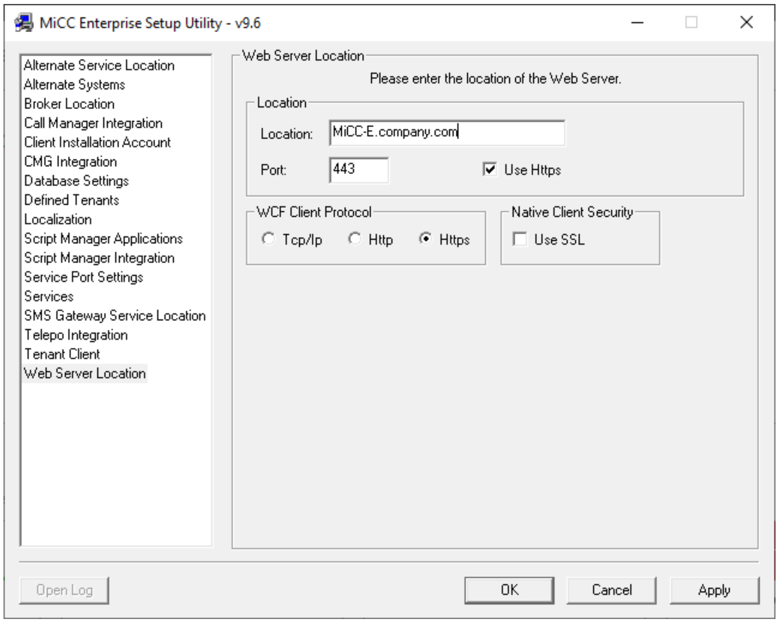
Username 5291

ICP-side Authentication

Username 5291

CONFIGURE THE MICC ENTERPRISE SERVER

The MiCC Enterprise system needs to be configured to use HTTPS in order for WebRTC to work well. This is configured using the MiCC Enterprise Setup Utility.



Web Server Location

Please enter the location of the Web Server.

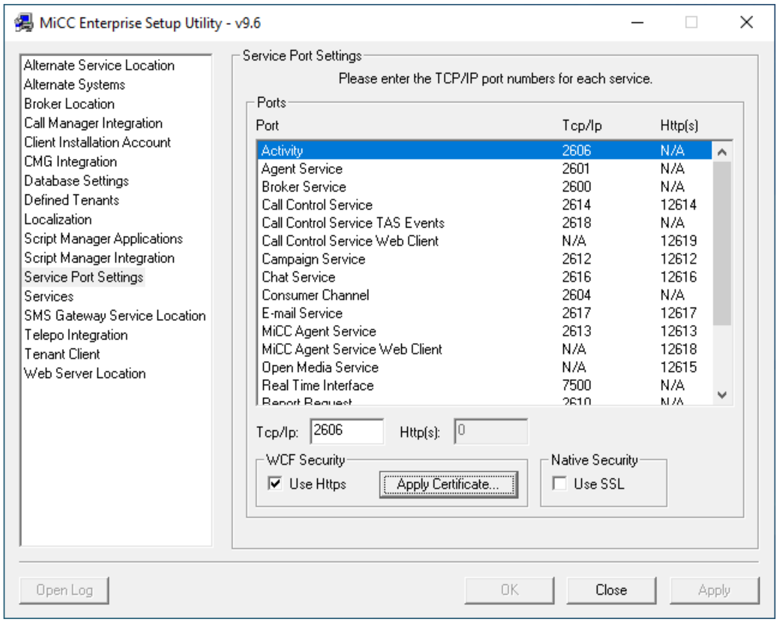
Location

Location: MiCC-E.company.com

Port: 443 ☑ Use Https

WCF Client Protocol: ○ Tcp/Ip ○ Http ● Https

Native Client Security: □ Use SSL



Service Port Settings

Please enter the TCP/IP port numbers for each service.

Ports

Port	Tcp/Ip	Http(s)
Activity	2606	N/A
Agent Service	2601	N/A
Broker Service	2600	N/A
Call Control Service	2614	12614
Call Control Service TAS Events	2618	N/A
Call Control Service Web Client	N/A	12619
Campaign Service	2612	12612
Chat Service	2616	12616
Consumer Channel	2604	N/A
E-mail Service	2617	12617
MiCC Agent Service	2613	12613
MiCC Agent Service Web Client	N/A	12618
Open Media Service	N/A	12615
Real Time Interface	7500	N/A
Report Request	2610	N/A

Tcp/Ip: 2606 Http(s): 0

WCF Security: ☑ Use Https

Native Security: □ Use SSL

The location of the MBG server needs to be configured on the MiCC-E server. Open the config.json file located in the <MiCC-E install location>\Services\Web\WebAgent\assets folder in a text editor and change the "*webSocketServerURL*" entry in the "*webRTCConfig*" section to pointy to the location of the MBG server.
Example:

```
"webRTCConfig": {

                    "userAgent": "Mitel-UC-Endpoint",

                    "webSocketServerURL": "wss://vm-mbg11-1.seclab.com:5063",

                    "domain": "192.168.0.1"

          }
```

Leave the "*domain*" entry as is.

CONFIGURE THE WEB AGENT CLIENT

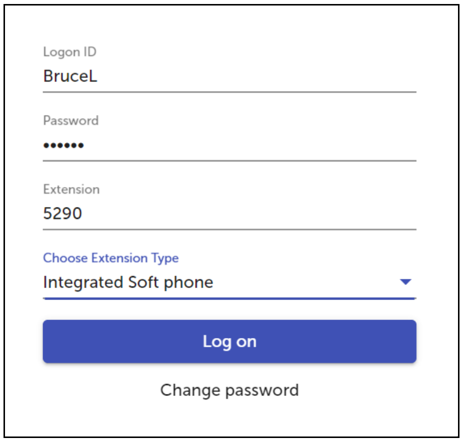
1. DNS
   Each client device needs to be able to reach the MBG server, so if the MBG is reached by server name or FQDN the DNS must be able to resolve them. If not, entries will have to be added to the clients HOSTS file. Same things would apply for the resolving the MiCC-E server name.
2. Certificates
   a. Login into MBG server, Go to Security → Web Server menu
   b. Under "Web Server Certificate" tab, find "Download the current web server certificate" and click on Perform button, it will download the certificate
   c. Use the Certificate Manager in Windows to install the certificate into the "Trusted Root Certification Authorities".

VALIDATE THE CONFIGURATION

The configuration can be validated in two ways.

1. Using Web Agent
   If the MiCC Enterprise system is already in place and is configured, then the MBG setup can be validated using Web Agent. Start Web Agent in a Chrome browser by loading:
   http://<MiCC Enterprise Server>/WebAgent
   or in case of a multi-tenanted system loading:
   http://<MiCC Enterprise Server>/WebAgent/#/login/<Tenant Name>

   The Web Agent logon dialog will be presented:



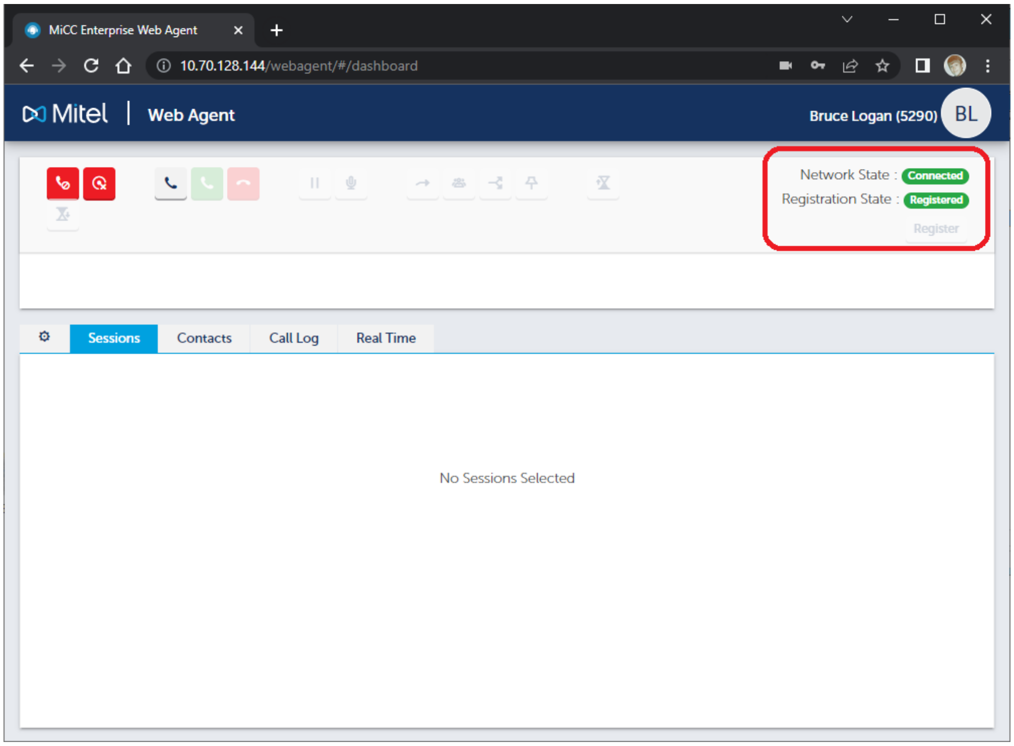
Logon ID
BruceL

Password
••••••

Extension
5290

Choose Extension Type
Integrated Soft phone

Enter the SIP extension number that has been configured in MX-ONE and MBG and select *Integrated Soft Phone*. If all goes well then Web Agent will load, and Network State and Registration State should be shown as green:



10.70.128.144/webagent/#/dashboard

Bruce Logan (5290)

Network State : Connected
Registration State : Registered

No Sessions Selected

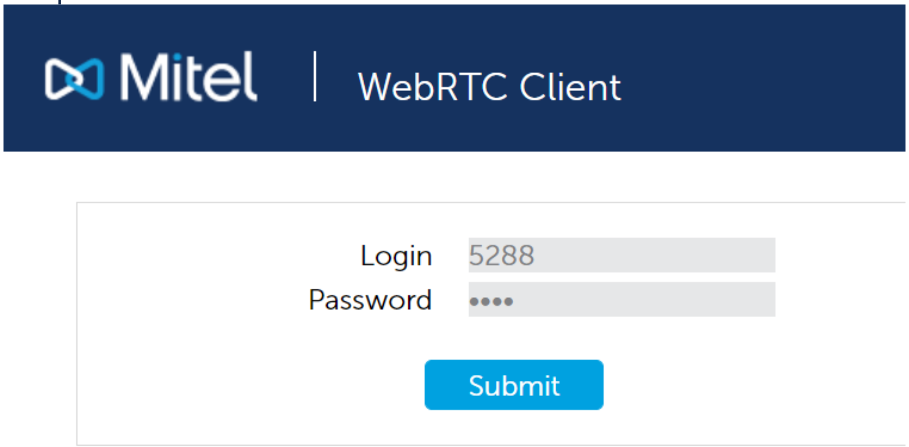
If not, then click F12 to enter Console mode in Chrome to troubleshoot connectivity and Registration issues.

2. Using MBG inbuilt app
To use the MBG built-in test app, from the top menu of the MBG server manager, select "Teleworking->WebRTC", and click the "?" icon. This will bring up the help page.

As per the help page, there are two different ways to launch the client app. One is Anonymous call mode (c://<MBG-FQDN>/webrtc/call.php?to=<CalledNumber | SipUri>) and the other is the Subscriber call mode (https://<MBG-FQDN>/webrtc/index.php) Subscriber call mode will be used in this example.

Note that you might have to add the <MBG-FQDN> in your computer's hosts file (c:\Windows\System32\drivers\etc\hosts) if it is not in your corporate DNS.

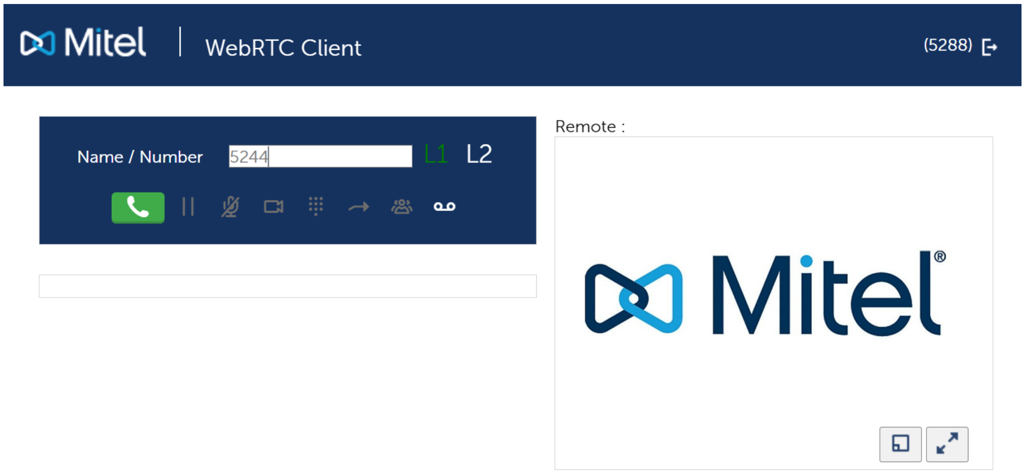
When you enter the URL in your browser, you will be prompted to enter Login/Password. The Login is the extension number and the password is the SIP password for the extension.



Login 5288
Password ••••

Note that the password needs to be the MD5 hashed password as entered above for the SIP user.

If correct credential is entered, you will see this and you can make WebRTC call by enter a number in the “Name/Number” field.



Name / Number 5244