A MITEL
PRODUCT
GUIDE

MiContact Center Enterprise

Configure MBG for WEBRTC - Operating Instructions

Release 9.6
Document Version 1.0

October 2022

Mitel
Powering connections

Notices

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

Trademarks

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

®,™ Trademark of Mitel Networks Corporation

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:

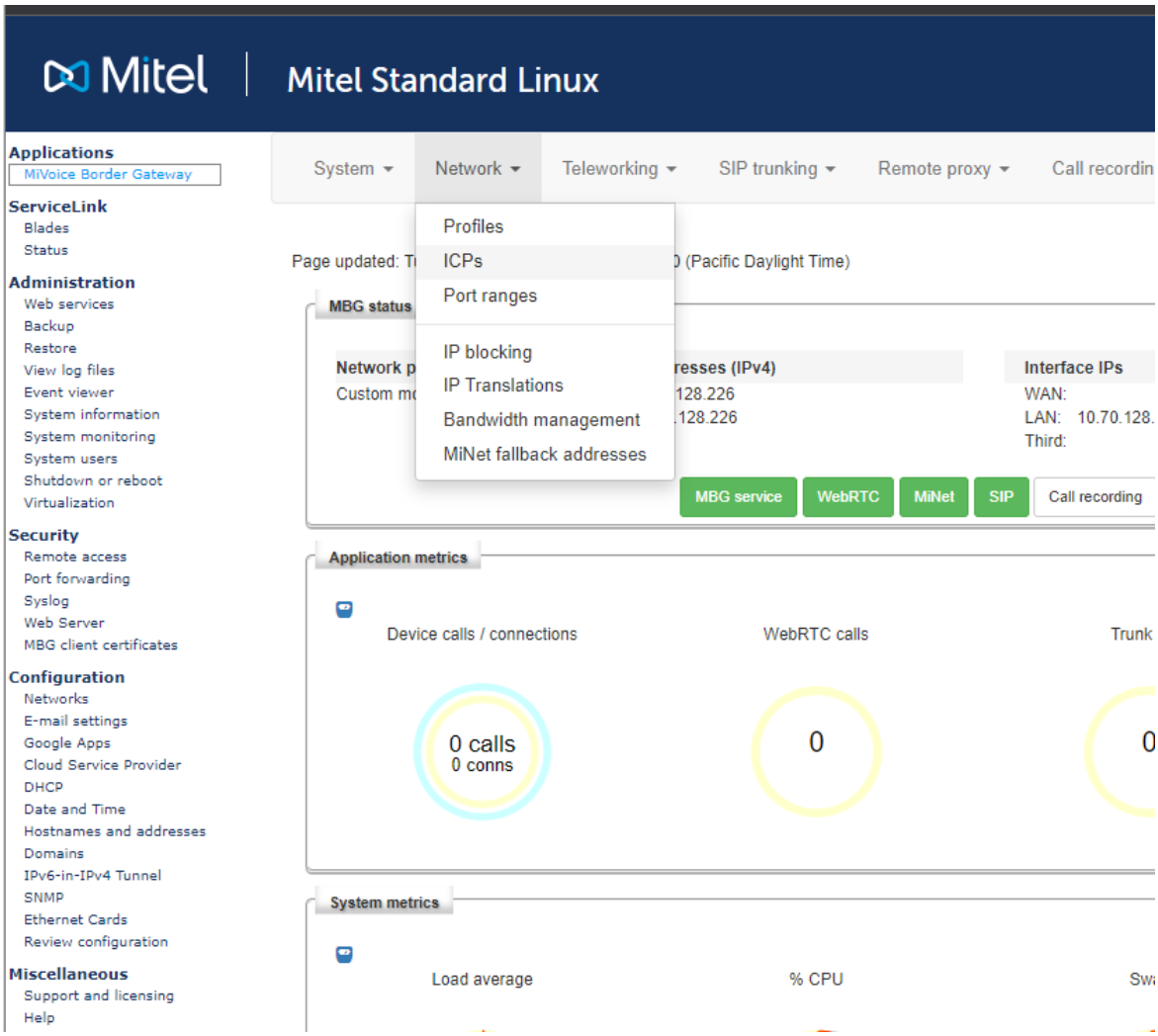
- MBG server
  Note: In this release, the MBG used by the MiCC Enterprise WebRTC Web Agents cannot be shared with MX-ONE Teleworkers or MiCollab users. A dedicated MBG will be needed. Also note that the WebRTC Pro feature of the MBG cannot not be used by MiCC-E Web Agents, so recording via MBG's SRC 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

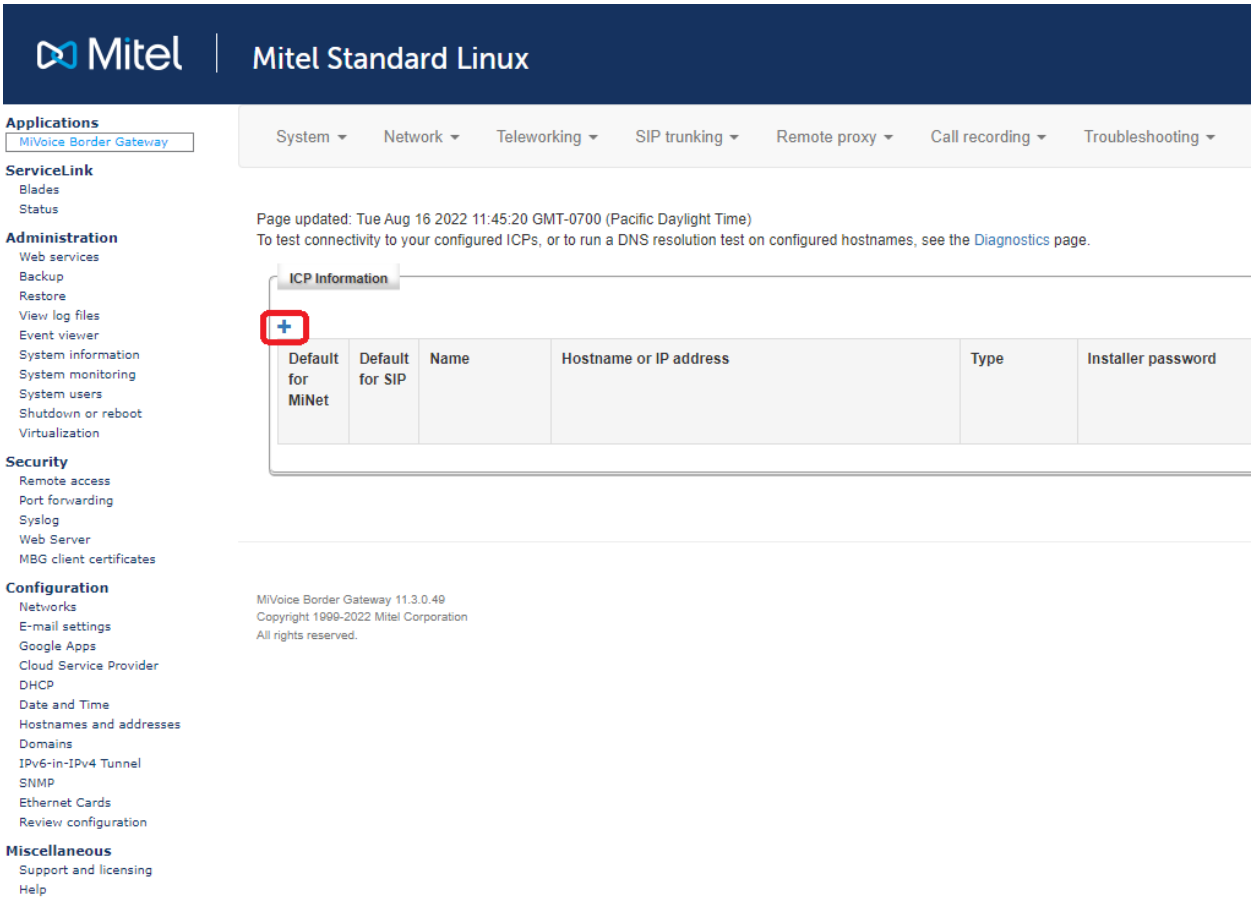
- Optionally: Test Client / MBG inbuilt test client

MBG SERVER CONFIGURATION

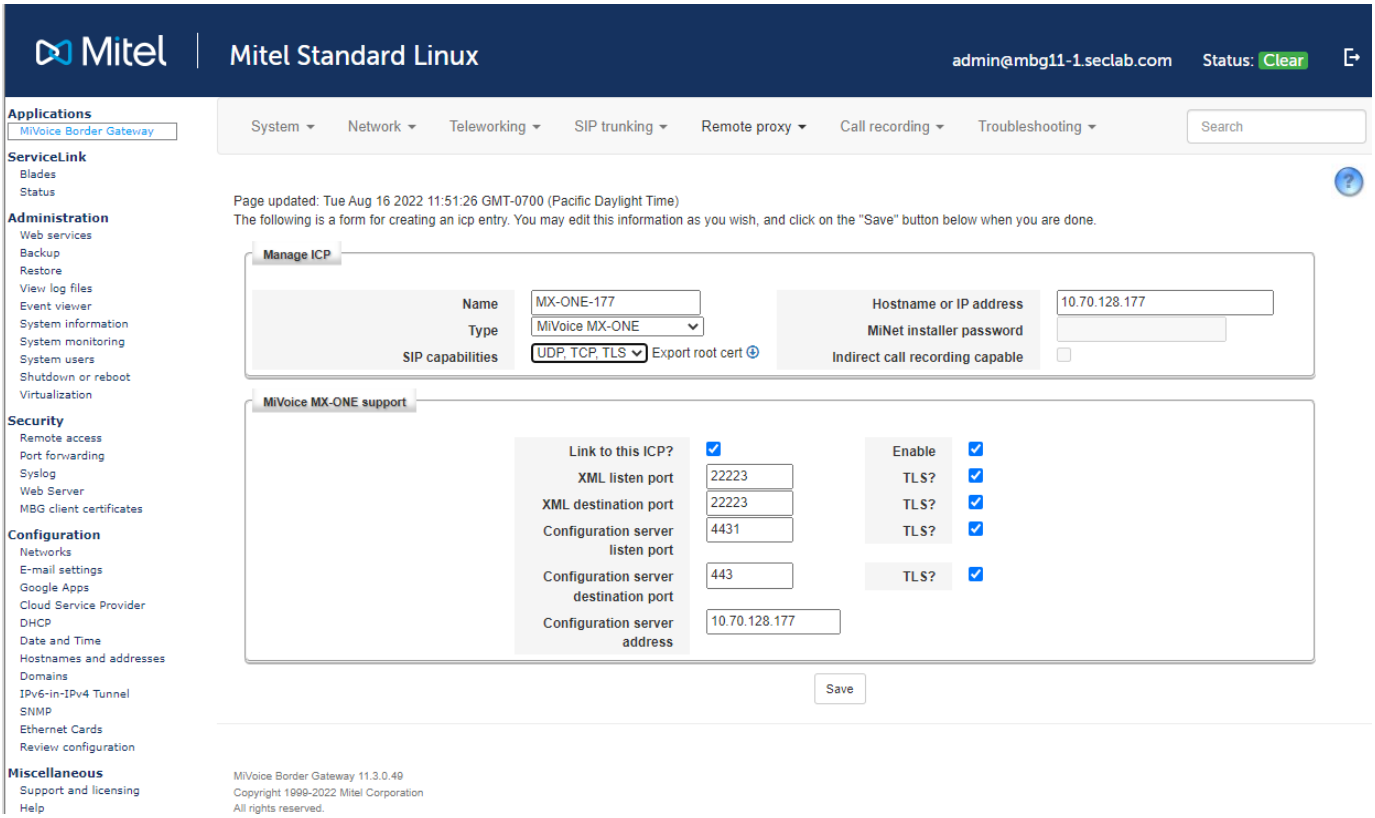
1. The very first thing we need to do is to create an ICP. From the top menu, select “Network->ICPs”.



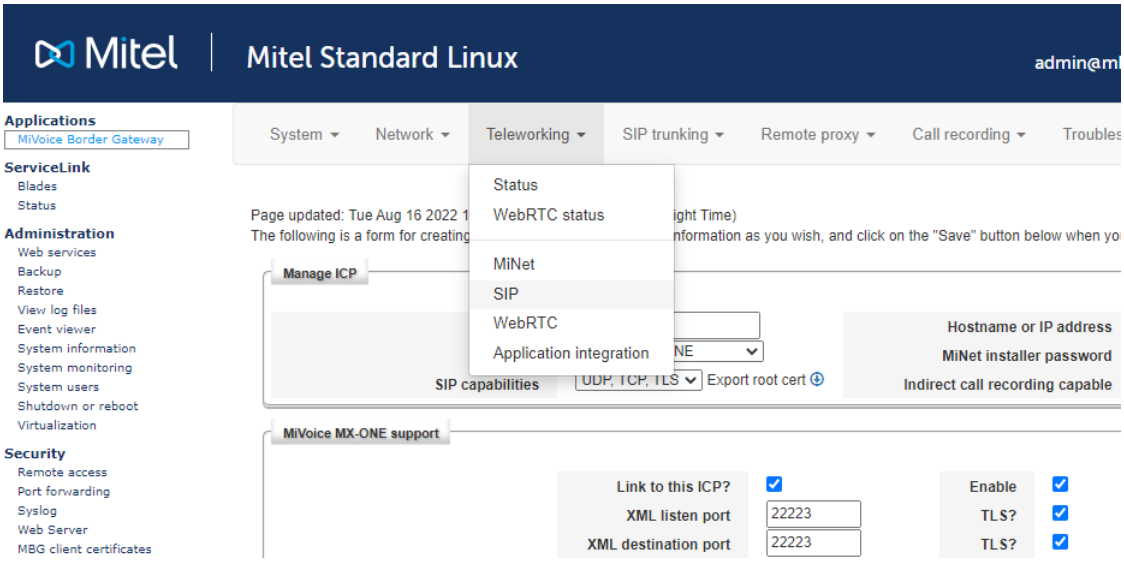
2. On the ICPs page, click the “+” icon to add a new ICP.



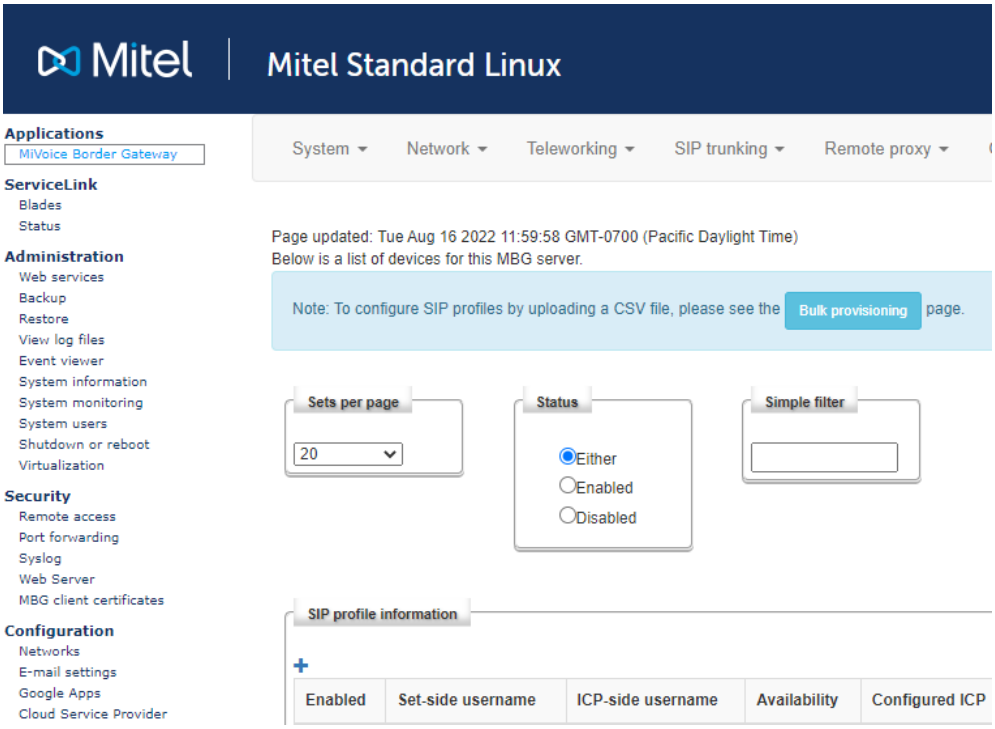
3. On “Manage ICP” page, enter a name which can be anything you want. For the “Type” field, select “MiVoice MX_ONE”. For the “SIP capabilities” field, select “UDP, TCP, TLS”. For the “Hostname or IP address” field, enter the MXONE IP address. Click the “Save” button.



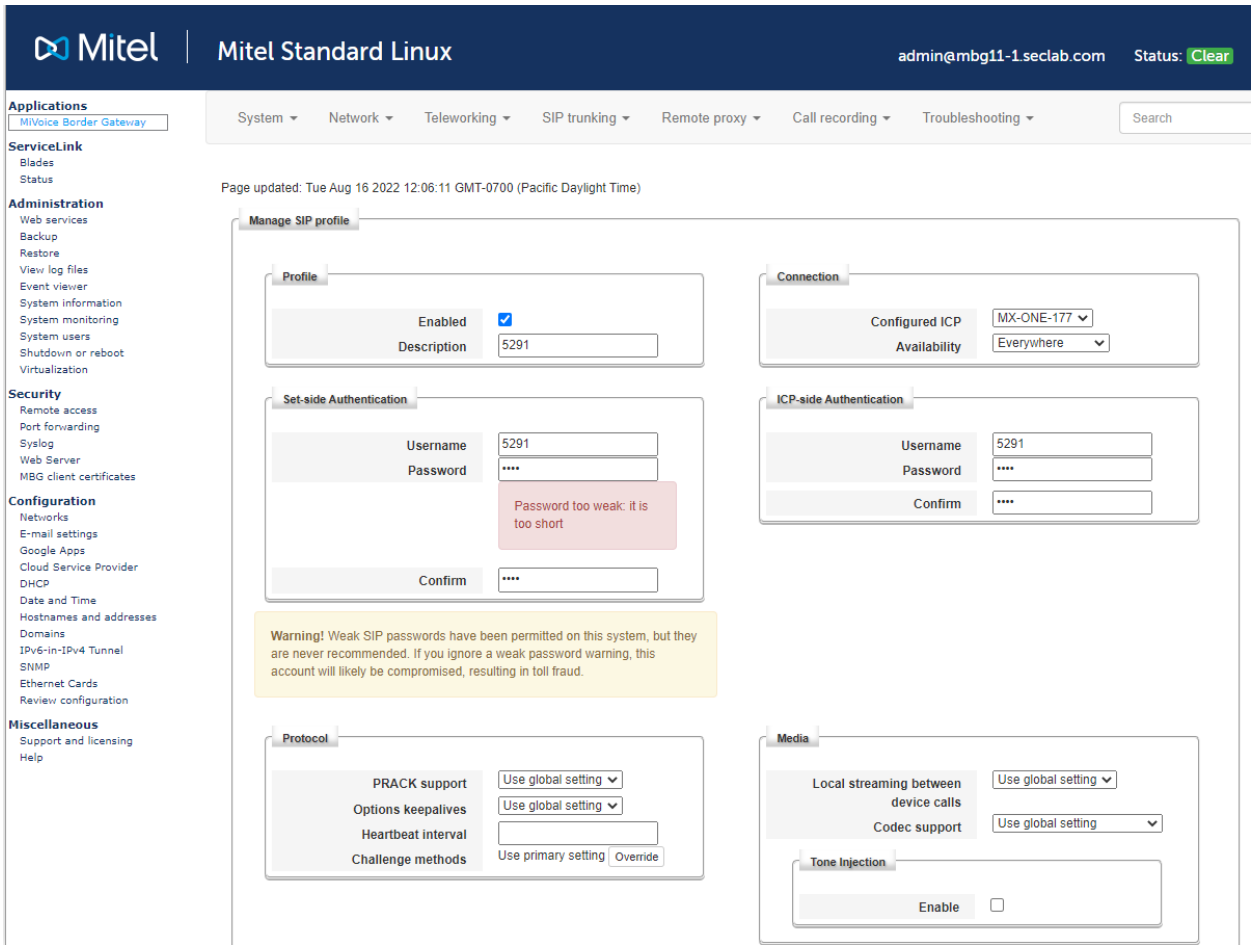
4. Now we need to add a SIP teleworker user that will be making WebRTC calls. We have to program this user in MBG and in MXONE. From the top menu, select “Teleworking->SIP”.



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

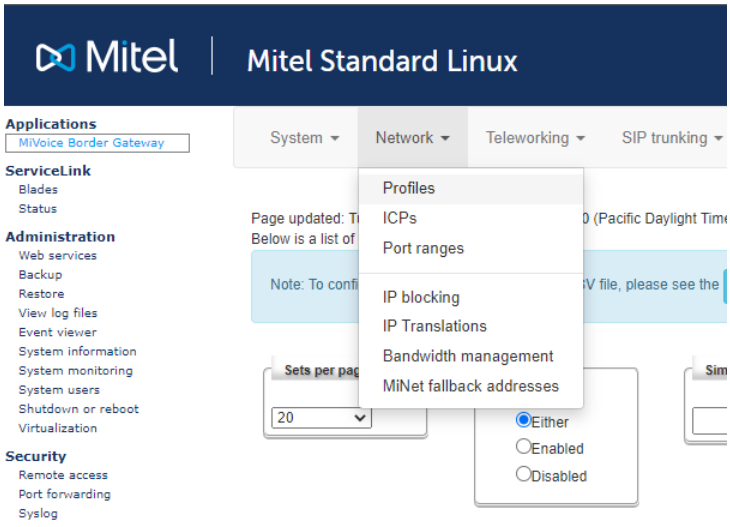


6. In the “Manage SIP profile” page, check the “Enable” checkbox. For both “Set-side username” and “Icp-side username” fields, use the extension we plan to use as the UC Endpoint user in MXONE. For the “Configured ICP” dropdown, select the MXONE we just created at step 3 above. For both set-side and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

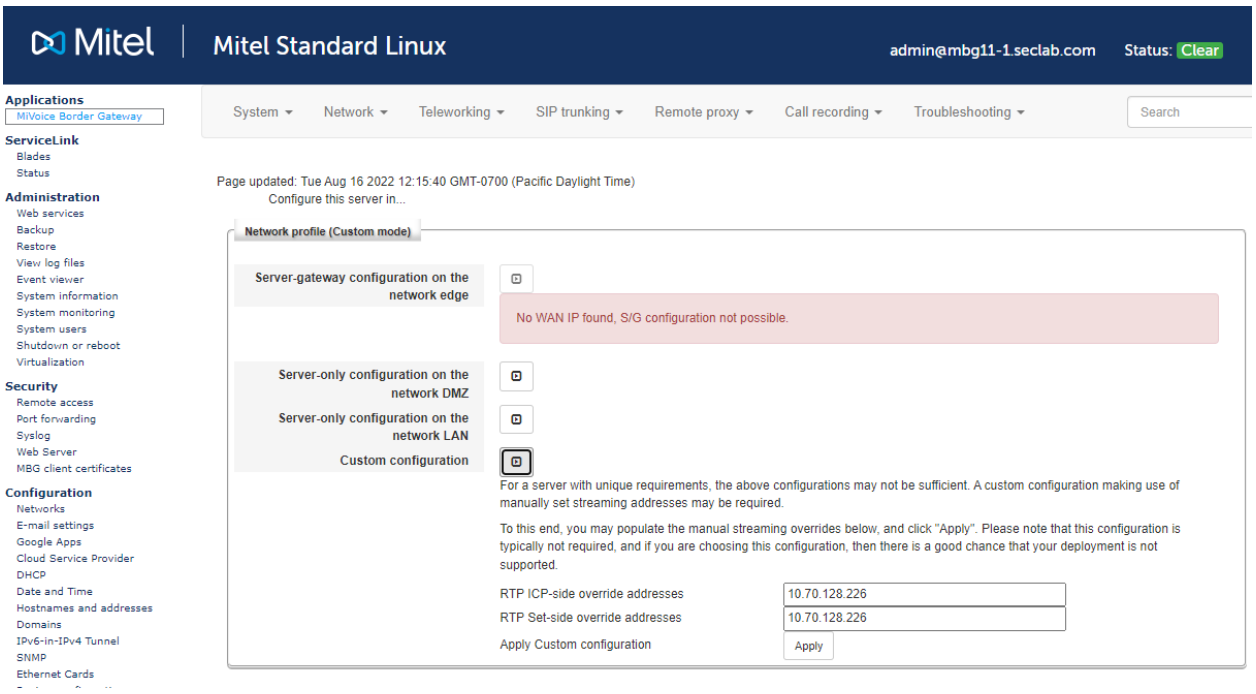


MBG may not allow you to add weak passwords, in that case go to System → Settings → Find “Permit weak SIP passwords“ in the very bottom of the page and enable the checkbox.

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

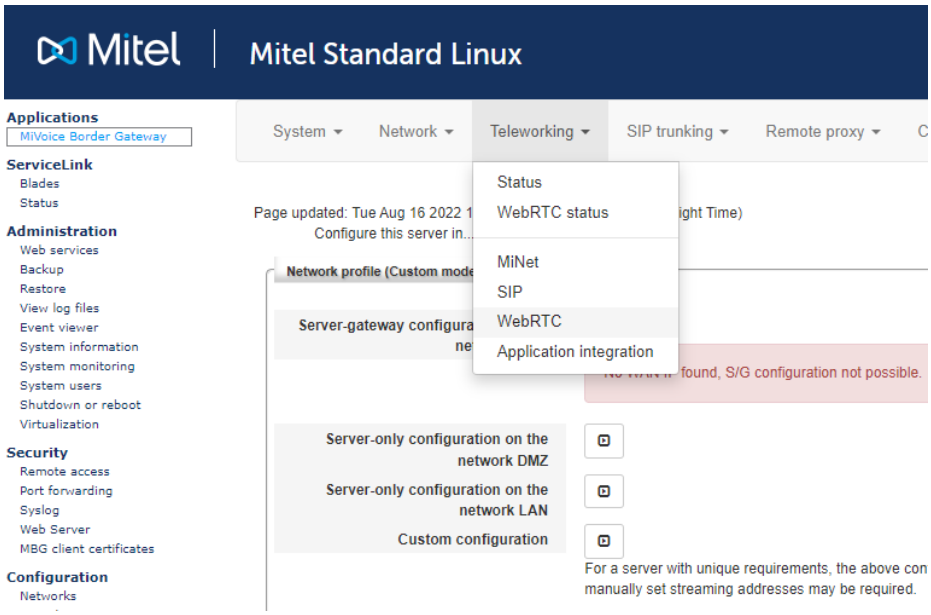


8. In “Network profile” page, click on the right-arrow on the right of “Custom Configuration”, enter the MBG IP address for both “RTP ICP-side override addresses“ and “RTP Set-side override addresses“ and click the “Apply” button.



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.

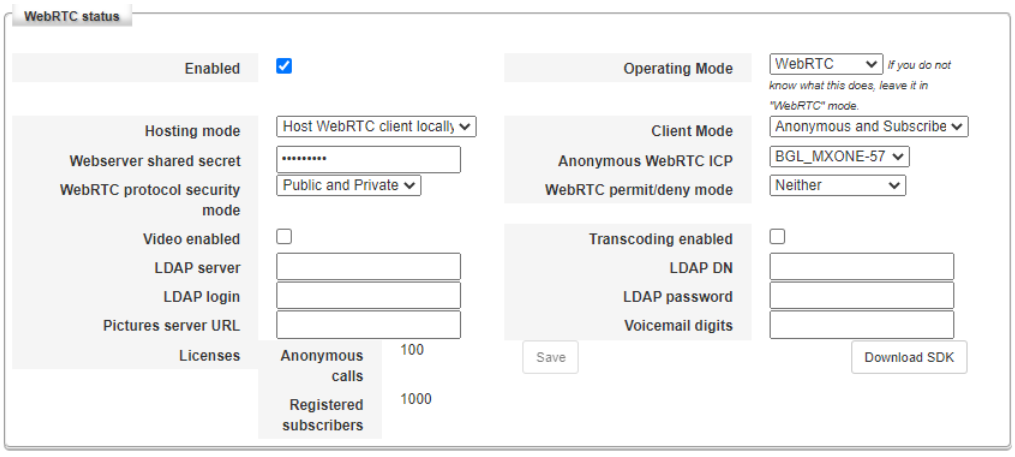
    c. For the “WebRTC protocol security mode” field, just select “Public and Private”.

    d. “Video enabled” should be unchecked.

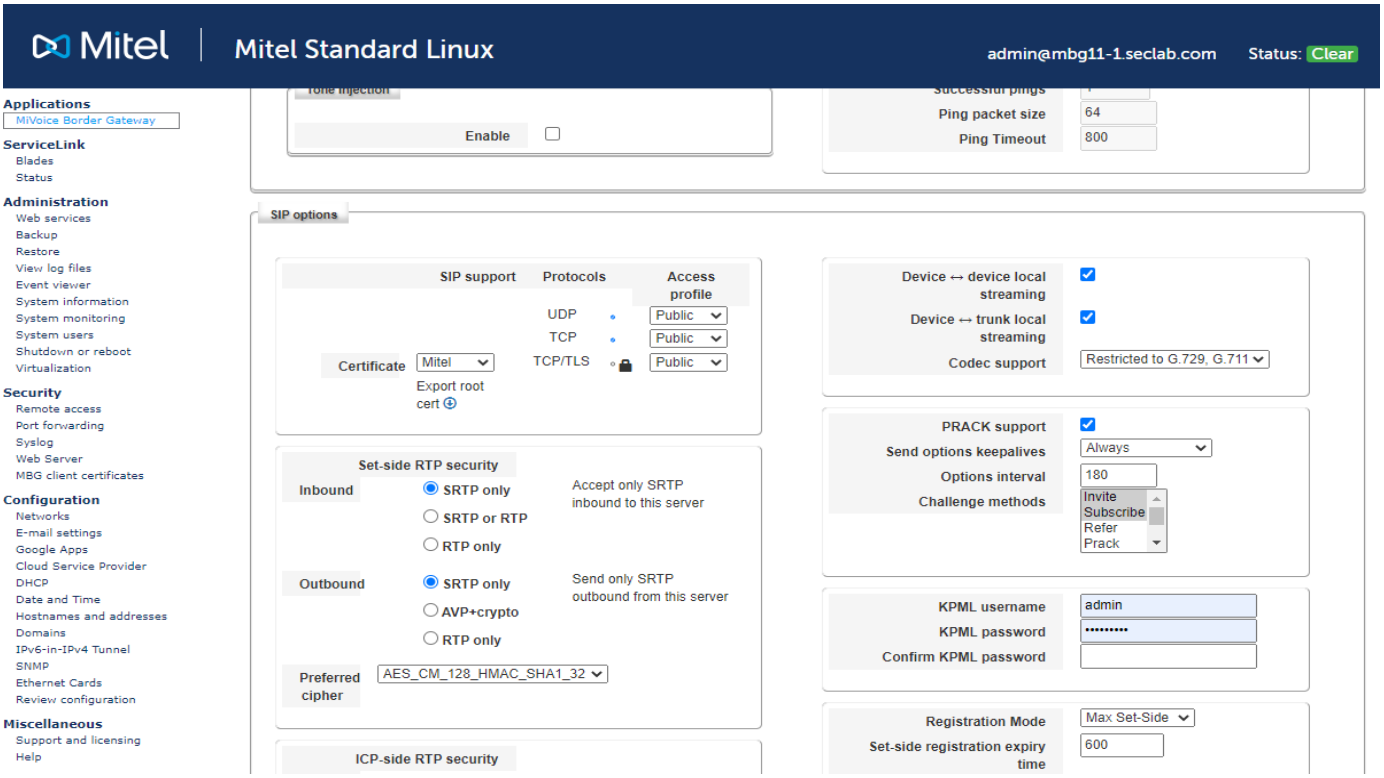
    e. For the “Mode” field, select “Anonymous and Subscriber”.

    f. Anonymous WebRTC ICP - Select the Configured ICP name

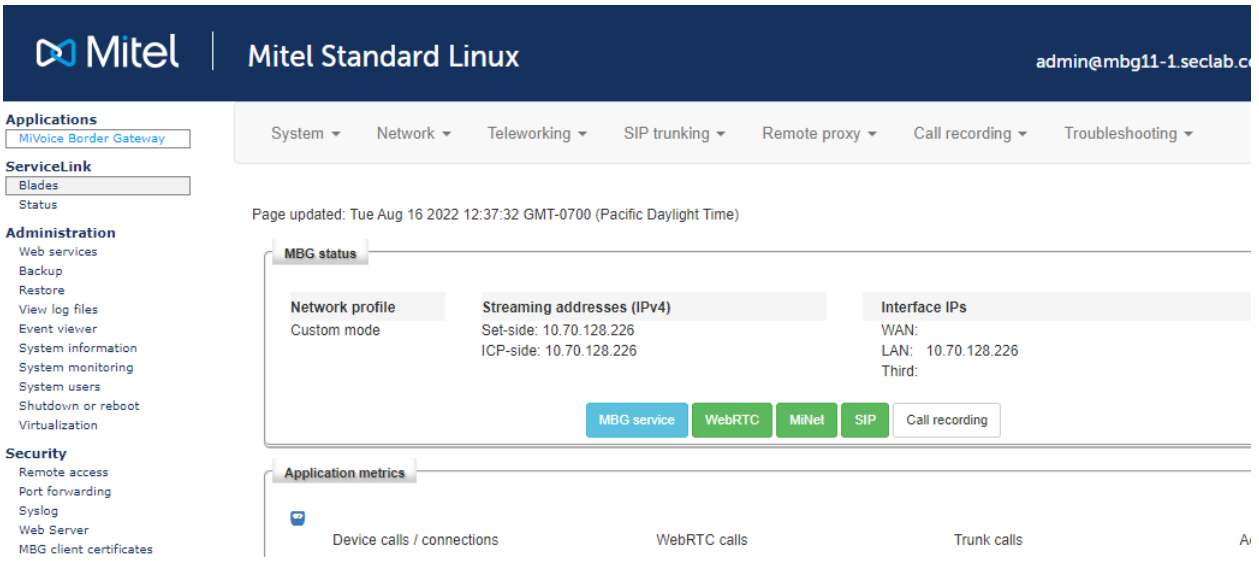
    g. WebRTC whitelist/blacklist mode - choose “neither“



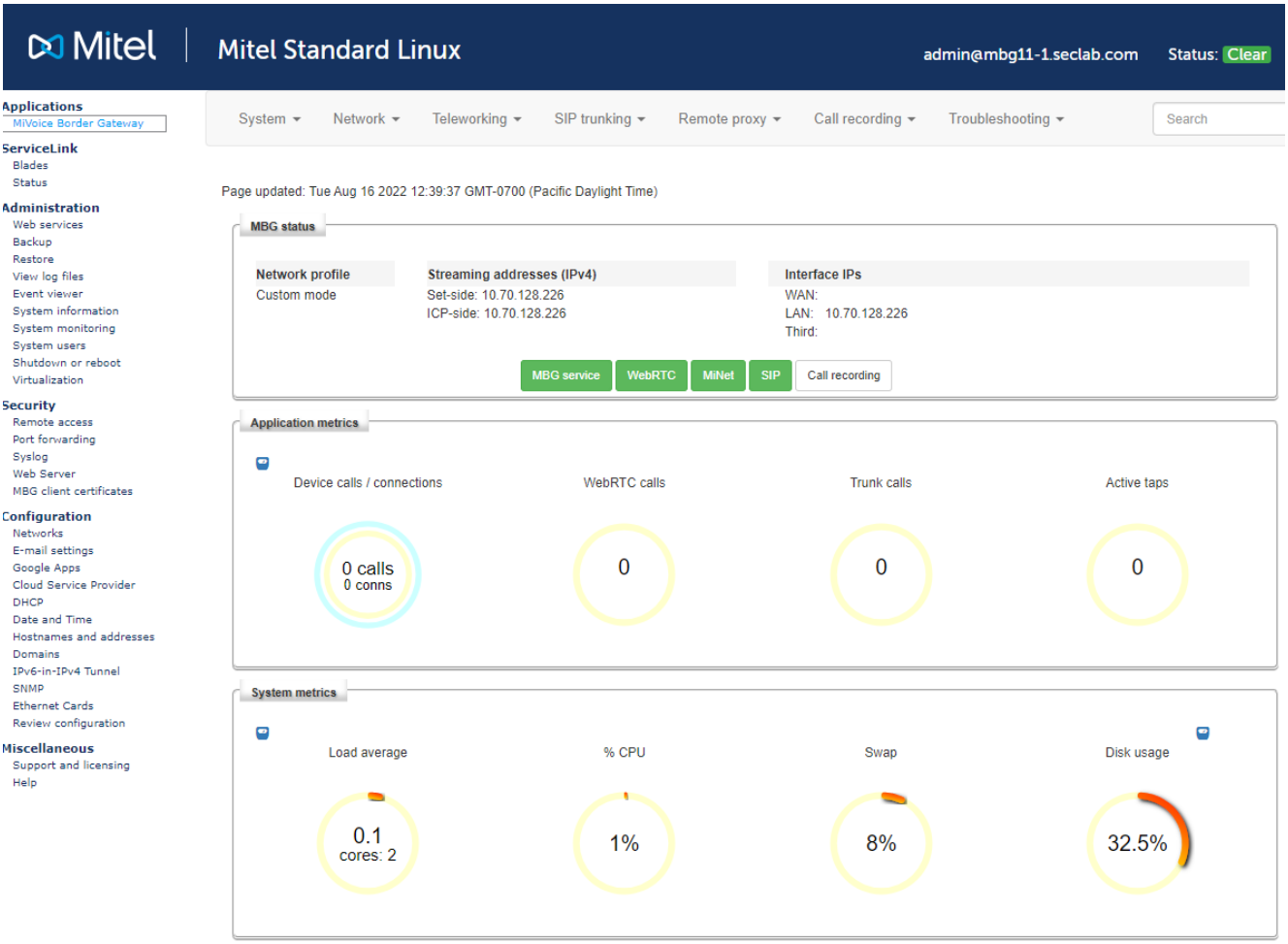
12. Now we need to enable SIP option. From the top menu, select “System->Settings”, in the “SIP options” section, enable UDP, TCP and TCP/TLC protocols.



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



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



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>`

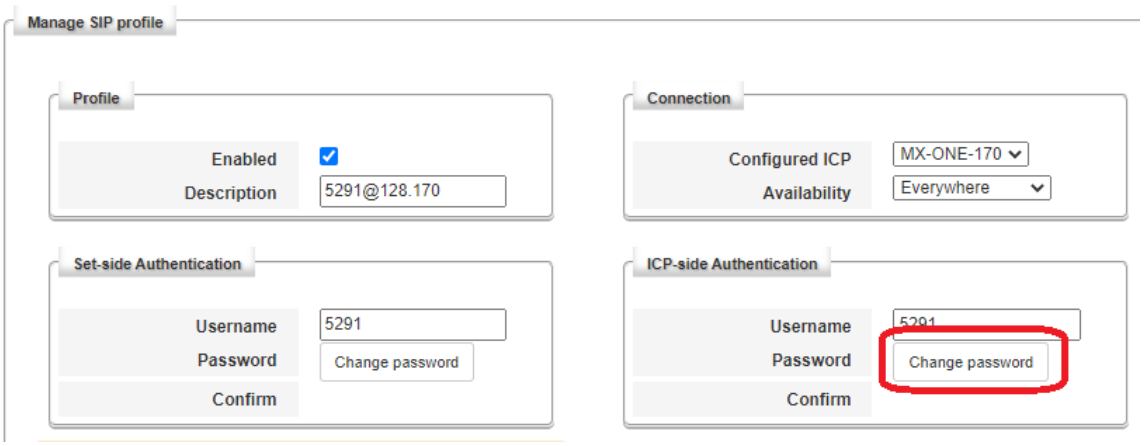
Example:

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

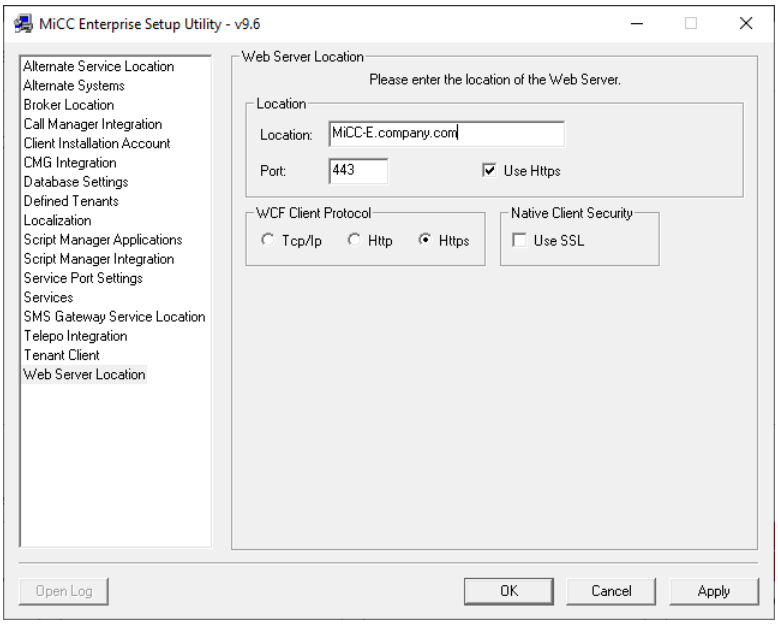
```
customer dir  auth code                                cil code CSP restr new customer
======== ==== ==================================== ======== === ===== ============
       0 5291 md5a1:3417465e46c5d2b3fb78d0e8489bb278       5291  0     -
```

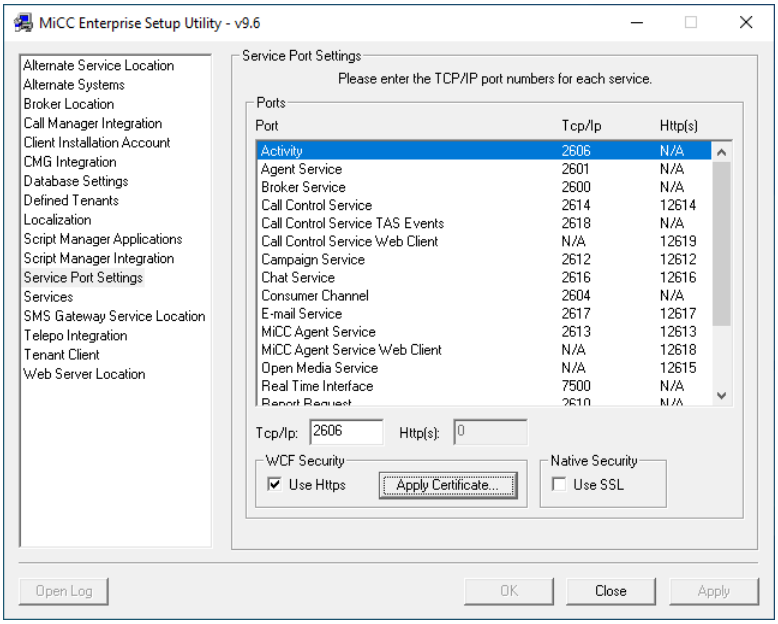
Copy the highlighted part to the clipboard and open the MBG Configuration tool. Navigate to Mitel Border Gateway->Teleworker->SIP and click to edit the extension. Click on Change Password buttons for the ICP-side Authentication and paste in the encrypted password that was copied from MX-ONE. Don't forget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



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.





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

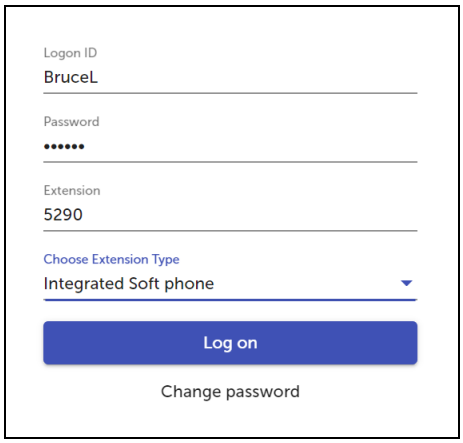
1. DNS
   Each client device needs to be able to reach the MBG server, so if the MBG is reached by server name or FQDN the DNS must be able to resolve them. If not, entries will have to be added to the clients HOSTS file. Same things would apply for the resolving the MiCC-E server name.
2. Certificates
   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

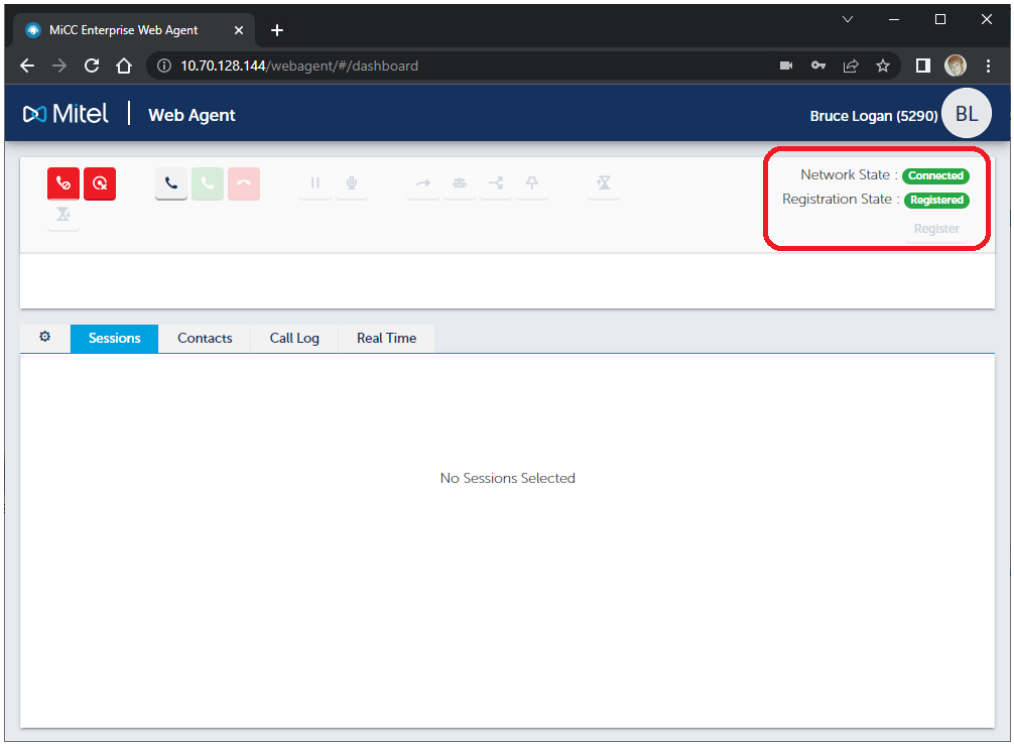
The configuration can be validated in two ways.

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:



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:



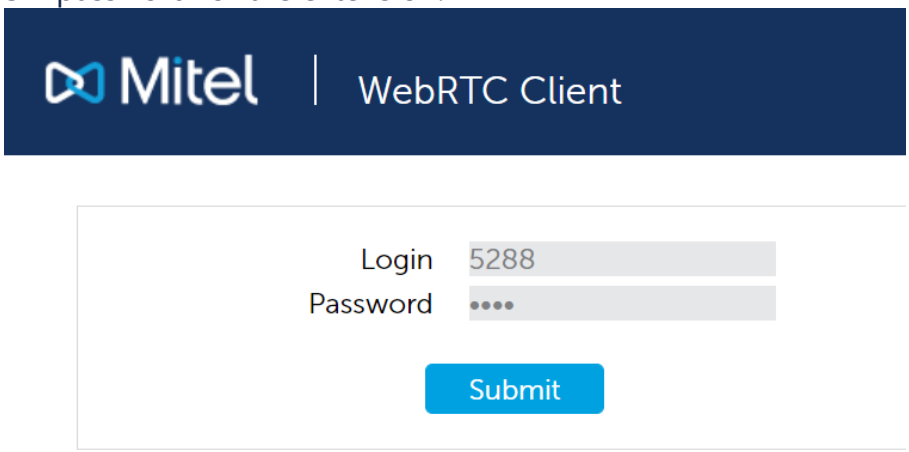
If not, then click F12 to enter Console mode in Chrome to troubleshoot connectivity and Registration issues.

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.



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.