# Administering IP Office 11.0 High Availability and Avaya Session Border Controller for Enterprise 7.2.2 to support Remote Workers


## Abstract

This document provides step-by-step instructions about how to configure IP Office 11.0 (IPO) and Avaya Session Border Controller for Enterprise 7.2.2 (SBCE) to support different soft clients locally and remotely. It does not substitute the Installation or Administration Guides but collects all steps needed for a working solution. The goal is to register Avaya Communicator for Windows, Avaya Communicator for iPad, Avaya One-X Mobile Preferred (Android and IOS) and Equinox in VoIP mode using signaling and media encryption, and to have Presence and Instant Messaging on them.



Issue 1.0

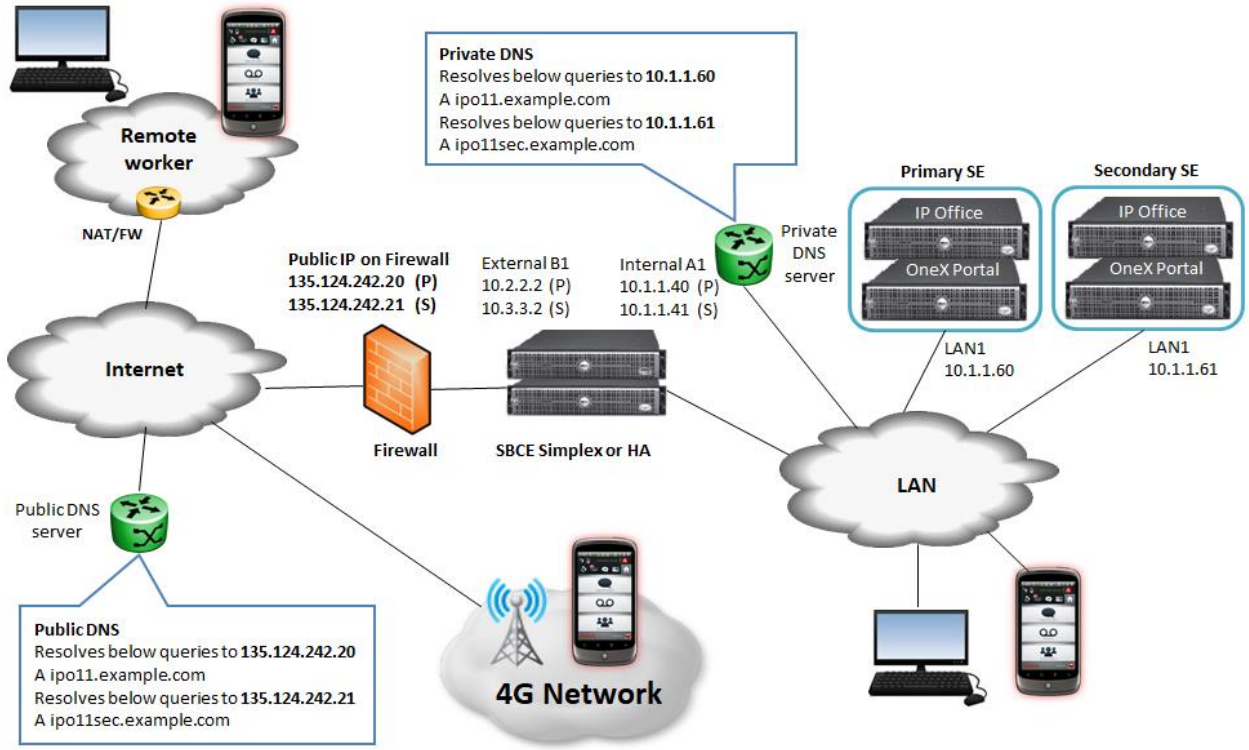
17 May 2018

AVAYA

## Contents

## Overview

A typical deployment can be the following:




Soft clients want to register to IPO directly when they are in the office using Wifi, and want to register through the SBCE when they are on mobile network or on Wifi at a remote site. To achieve this, Split DNS is needed, which resolves the same FQDNs to the internal IP of IP Office or the public IP of SBCE depending on where the clients are. In the reference configuration IP Office Server Edition will be used where the One-X Portal and IP Office components are on the same Virtual Machine, so have the same IP address.

The IP Office / One-X Portal Resiliency setup requires two IP Office Server Edition, one will act as a Primary Server, the other as Secondary. The IP Office resiliency supports Alternate Registration of SIP endpoints, which means only one of the servers can accept registrations at the same time. When the primary server goes down, secondary will take over the control and will start accepting registrations.

NOTE: IP Office Resiliency protects only against server outage, but not against network issues between the client and the server. In other words, if the link between the client and the primary server goes down while the server itself is up and can still communicate with secondary server, the client will NOT be able to register either to primary or secondary. The client can register to secondary only if the primary server itself goes down.

In the IP Office high availability setup the SBCE can be just considered as “part of the link” between the client and the IP Office. Practically we do two identical and independent configuration on SBCE mapping a dedicated external/internal IP pair to Primary IP Office SE, and another dedicated external/internal pair to Secondary IP Office SE. In this sense it does not matter if the SBCE itself is Simplex or HA, or even two independent boxes (one dedicated for Primary IPO, other dedicated to Secondary IPO), the logic of the configuration will be the same in all those scenarios.

NOTE: Communicator for iPad does not support resiliency. The other clients can support resiliency including both voip and presence.

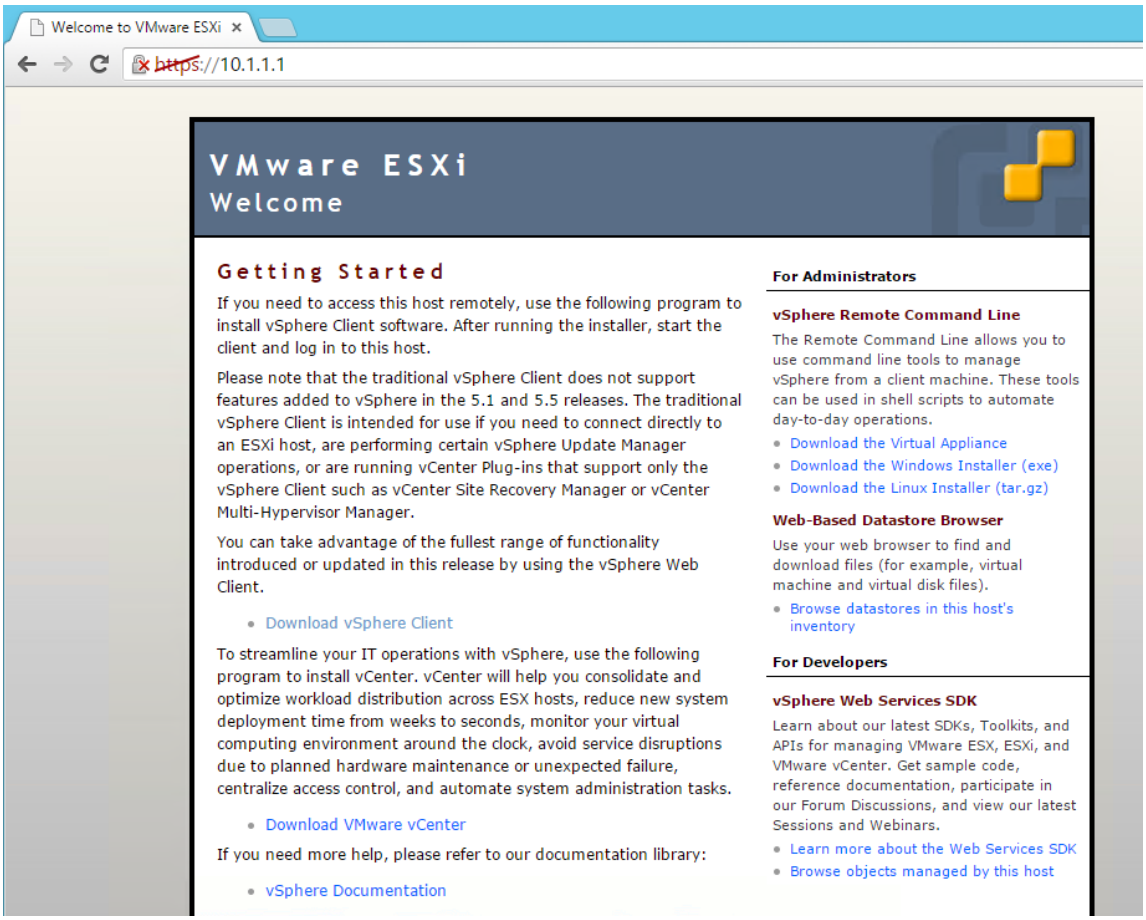
## Prerequisites

### VMware

VMware ESXi deployment is out of the scope of this document. The assumption is that VMware environment or Avaya Virtualization Platform (AVP) has already been deployed.

### vSphere Client

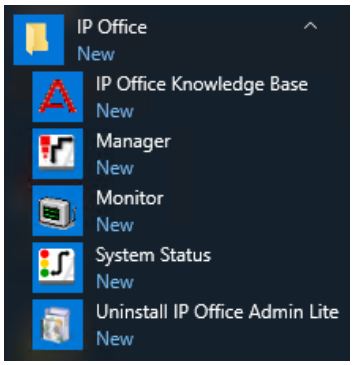
1. Open a browser to **https://<IP of VMware ESXi host>**




2. Click on **Download vSphere Client**
3. Run the downloaded exe file and follow the installation wizard

### IP Office Administration Tools

1. Download latest **IPOAdminLite_XXX.exe** from **plds.avaya.com**
2. Run the file on your PC and follow the wizard
3. After completing installation, Start Menu will have the following new entries:




## Firewall configuration

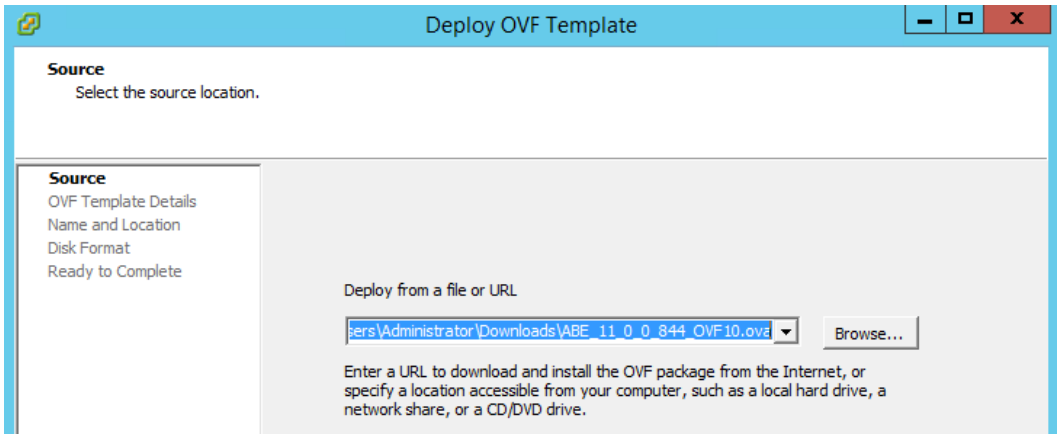
1. Allow Layer 3 NAT only, disable all SIP aware functionality, ALG, etc.
2. Forward the following ports to the B1 interface of the SBCE

| | | |
|---|---|---|
| TCP | 5061 | SIP |
| TCP | 5222 | XMPP |
| TCP | 9443 | WebRTC, REST, XMPP |
| TCP | 7443 | BOSH/XMPP |
| UDP | 3478 | STUN |
| UDP | 50000-55000 | RTP relay |
| UDP | 35000-40000 | RTP media |

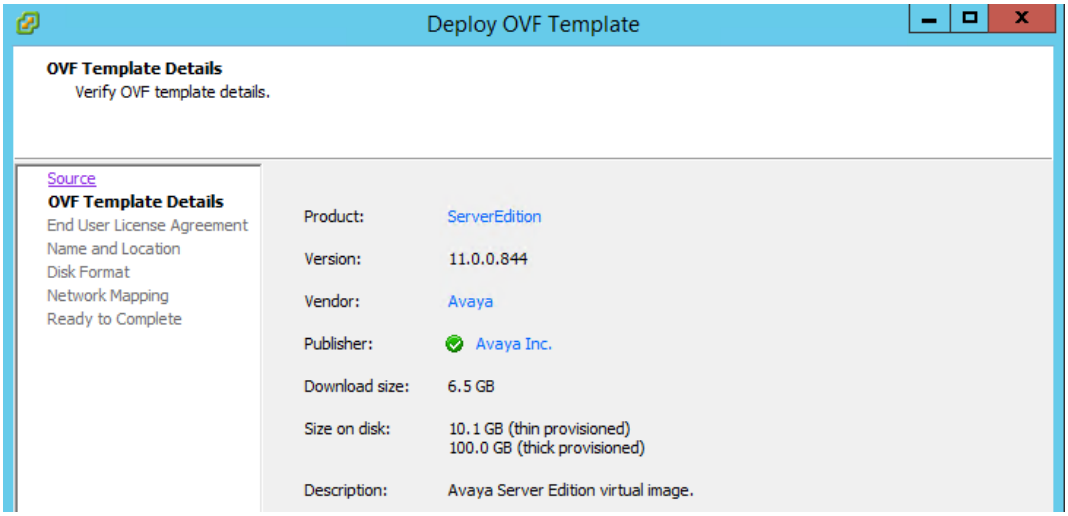
## Installing Primary IP Office

### Deploying OVA

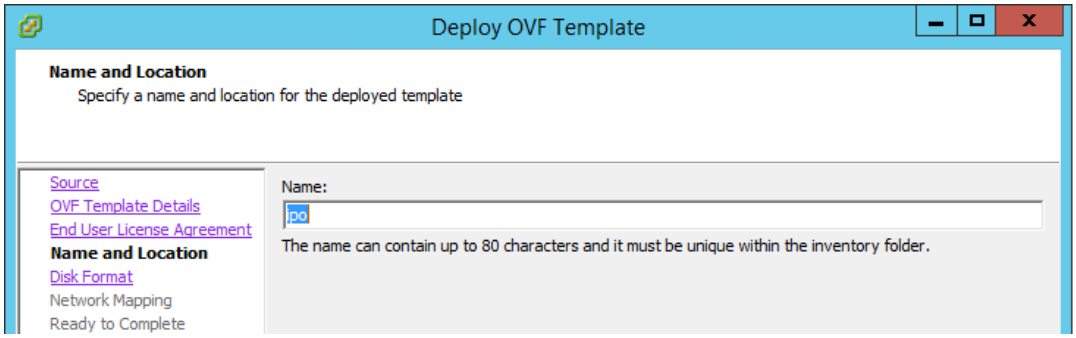
1. Download latest IP Office OVA file from **plds.avaya.com**
2. Start vSphere Client and connect to vCenter / AVP host
3. Go to **File / Deploy OVF Template**
4. Click **Browse** , select the OVA file and click **Open**



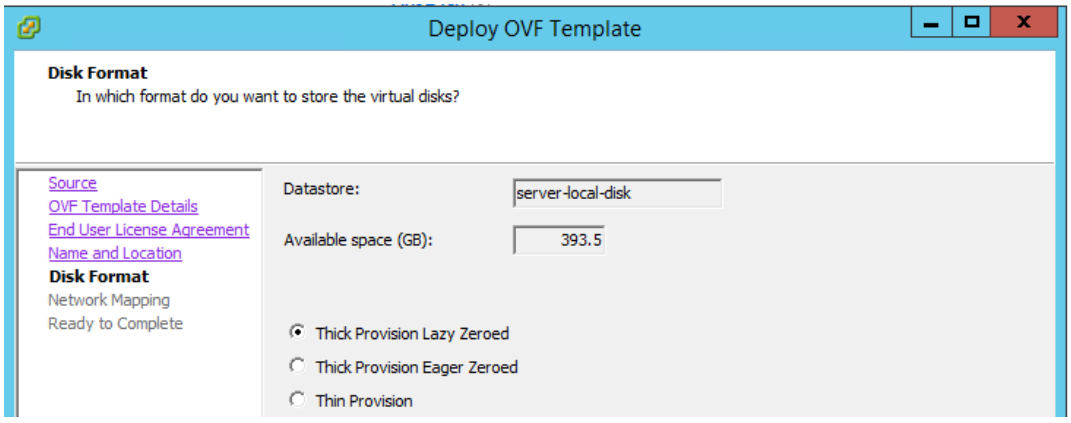

5. Click **Next**



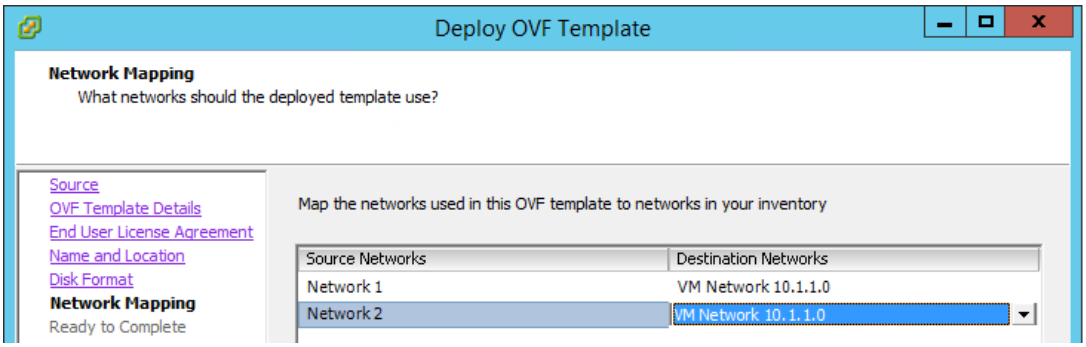

6. Click **Next**
7. License Agreement will be displayed, click **Accept** then **Next**
8. Set the name then click **Next**




9. Select data store and disk provision mode, then click **Next**



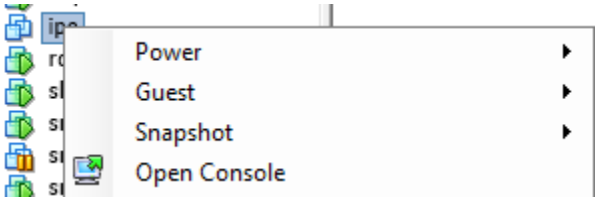

10. Select network mappings, then click **Next**



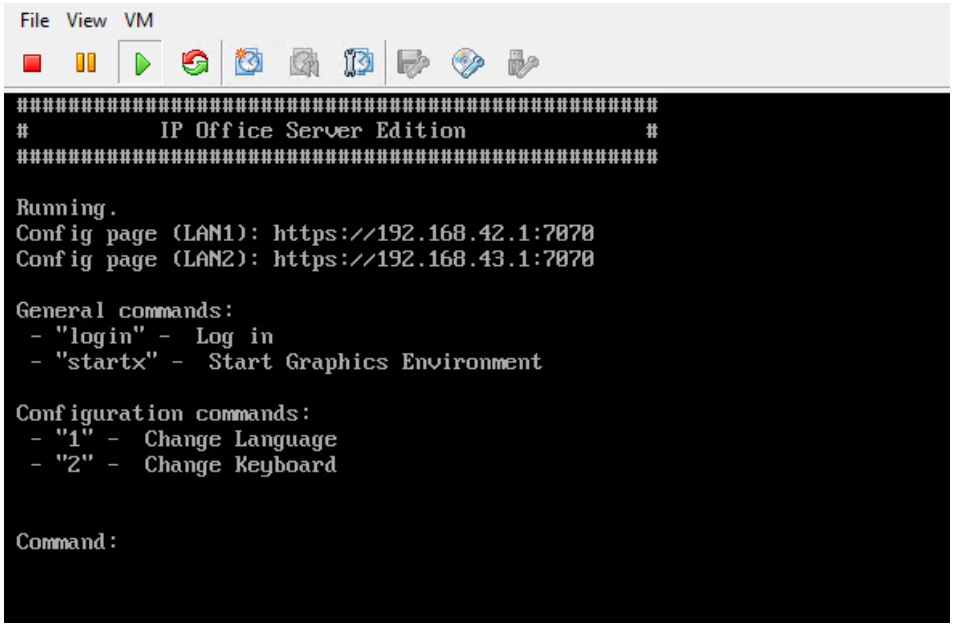

11. Wizard will display the summary, click **Finish**
12. Once deployment has completed, the new virtual machine appears in the inventory of virtual machines. Select the virtual machine and start it.

## Changing default IP

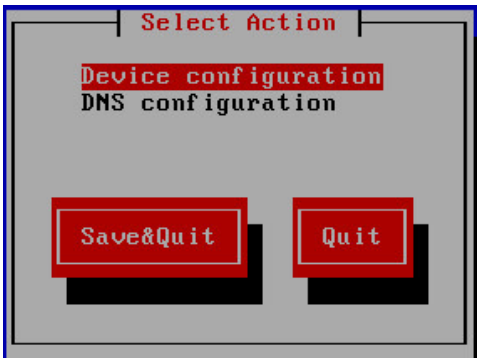
1. Right click on the IP Office virtual machine then click on **Open Console**



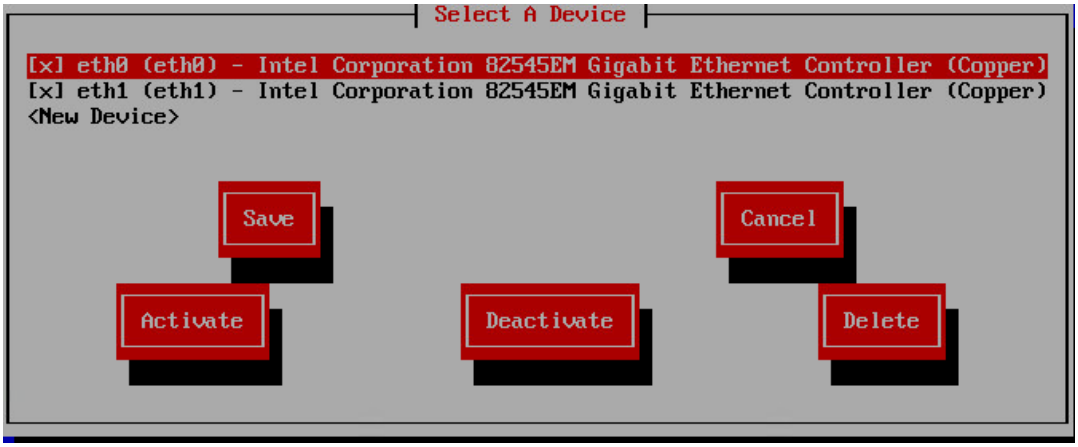

2. If this is the first boot, wait for the virtual machine to boot up until the following can be seen in the console window



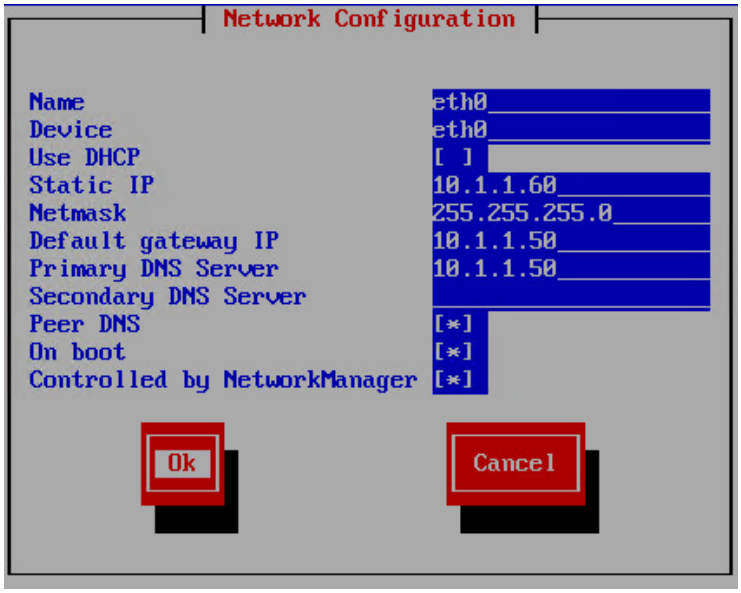

3. Click in the window (to release cursor from console window use the left CTRL+ALT keys)
4. Enter the command **login**
5. Default login is **root** with password **Administrator**
6. Enter the command **system-config-network.** The menu that appears is navigated using the cursor keys, tab key and Enter key.
7. Select **Device configuration** and press **Enter**




8. Select the network interface to configure and press **Enter**



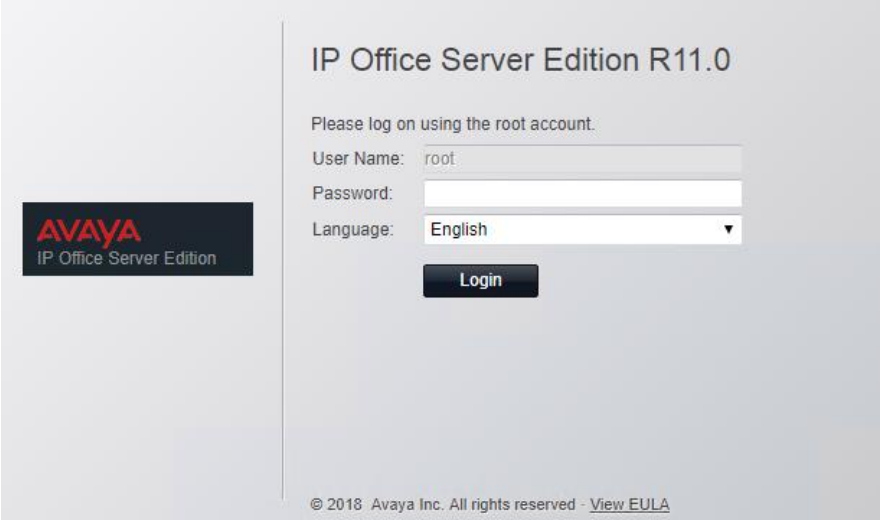

9. Enter network parameters for the interface



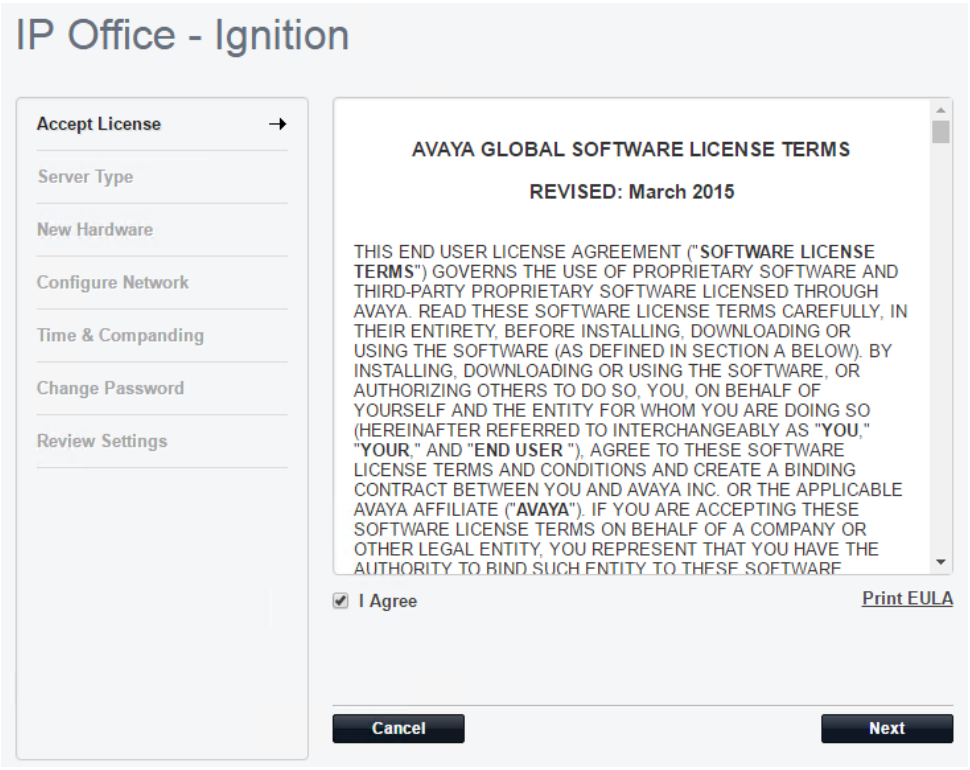

10. Select **OK** and press **Enter**
11. Select **Save** and press **Enter**
12. Select **Save & Quit** and press **Enter**
13. To logout, enter **exit**
14. Shut down and then power on the virtual machine again

## Primary Server Ignition

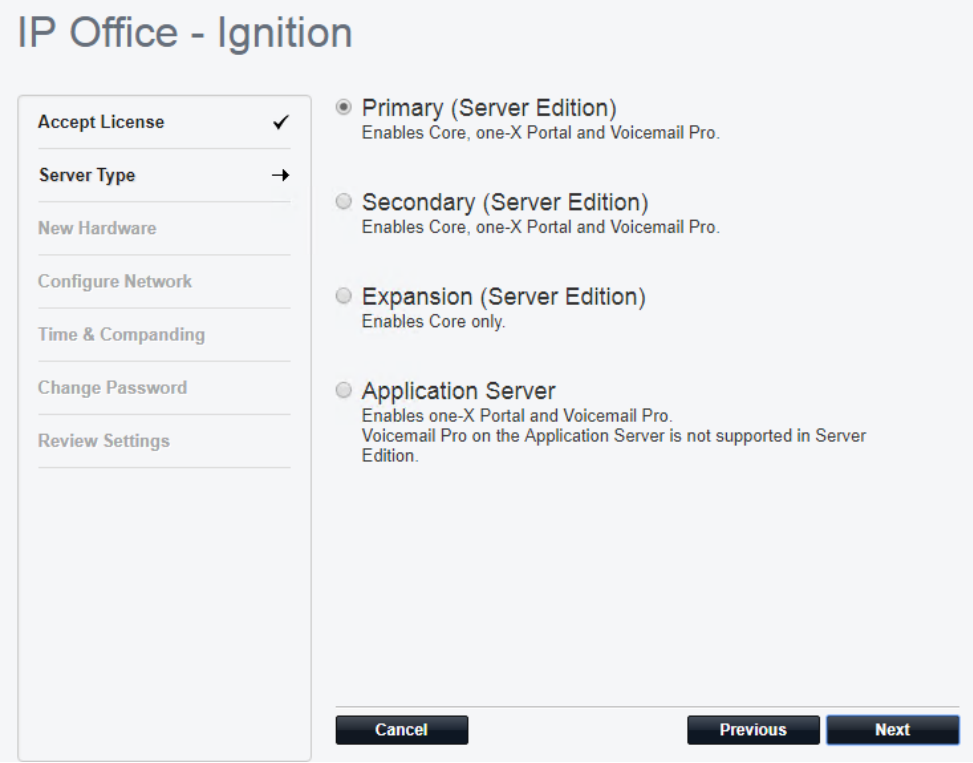
1. Open a browser and connect to **https://<PrimaryServerIP>:7071**
2. Use password **Administrator**



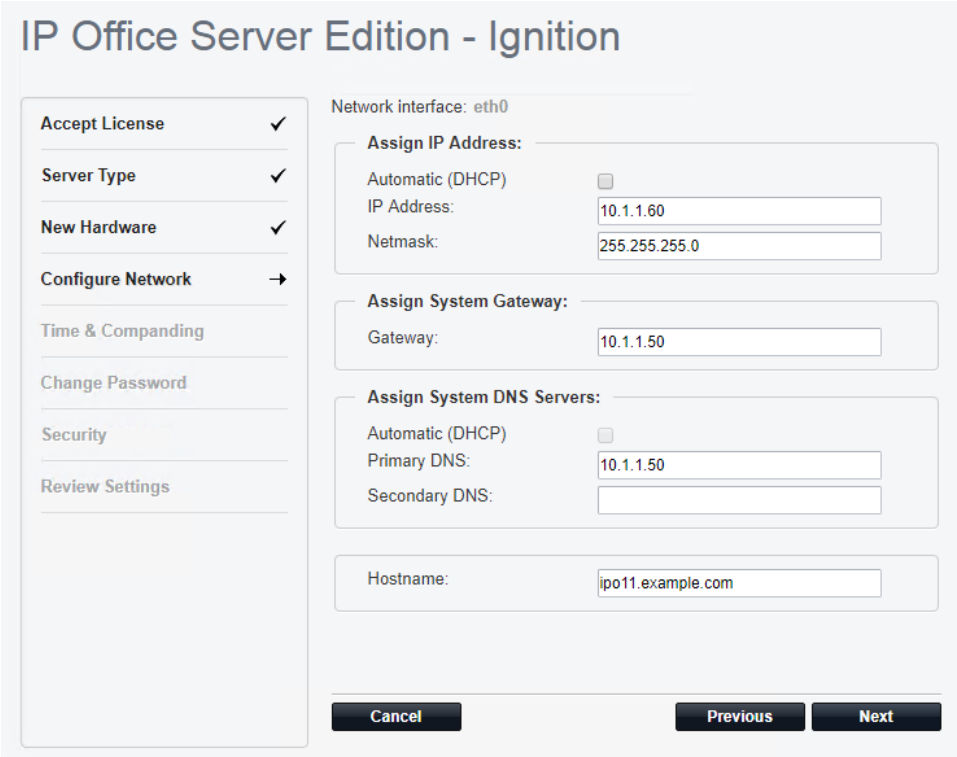

3. At the EULA check **I Agree** then click **Next**



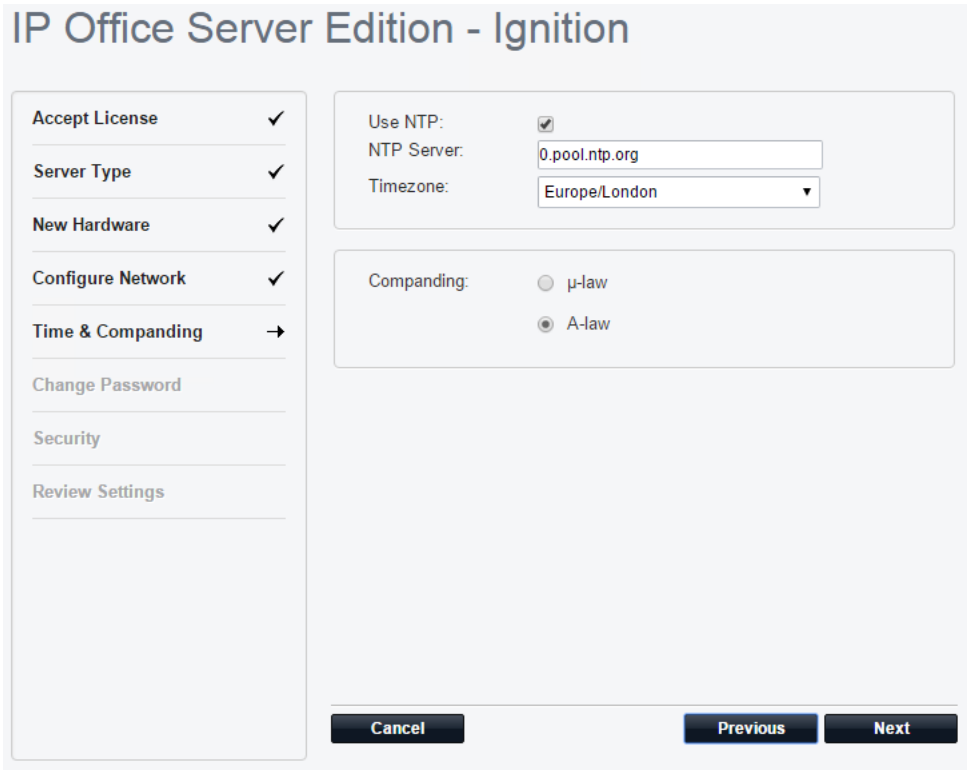

4. Select Primary (Server Edition) and click Next



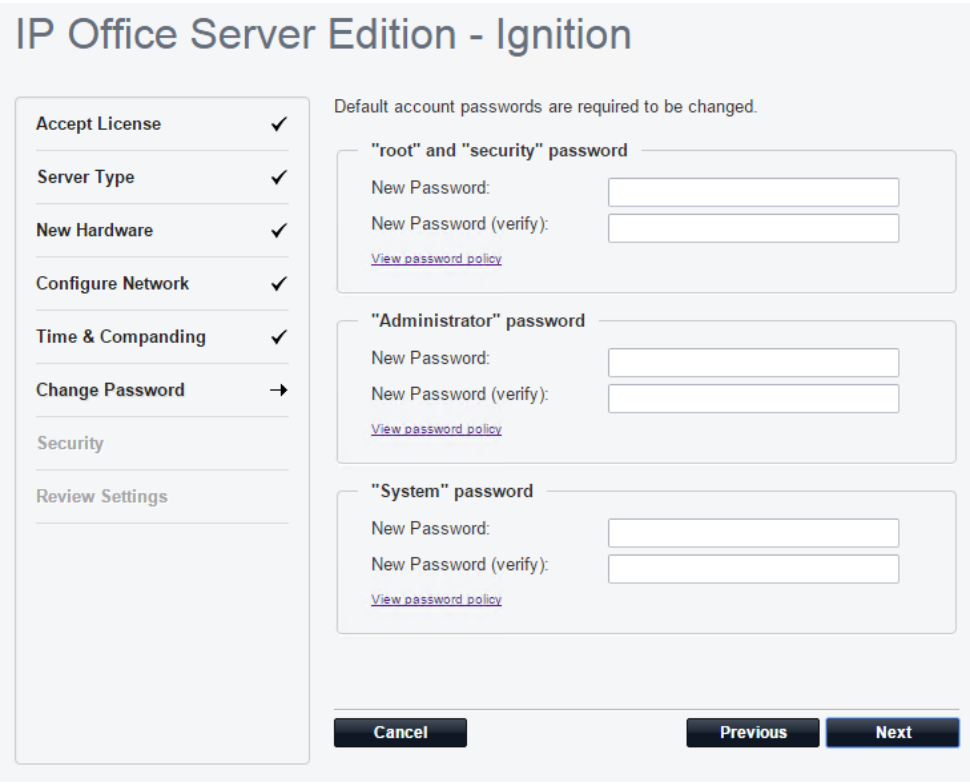

5. No new hardware available, click **Next**
6. Set network parameters as needed, enter hostname (**FQDN**), then click **Next**



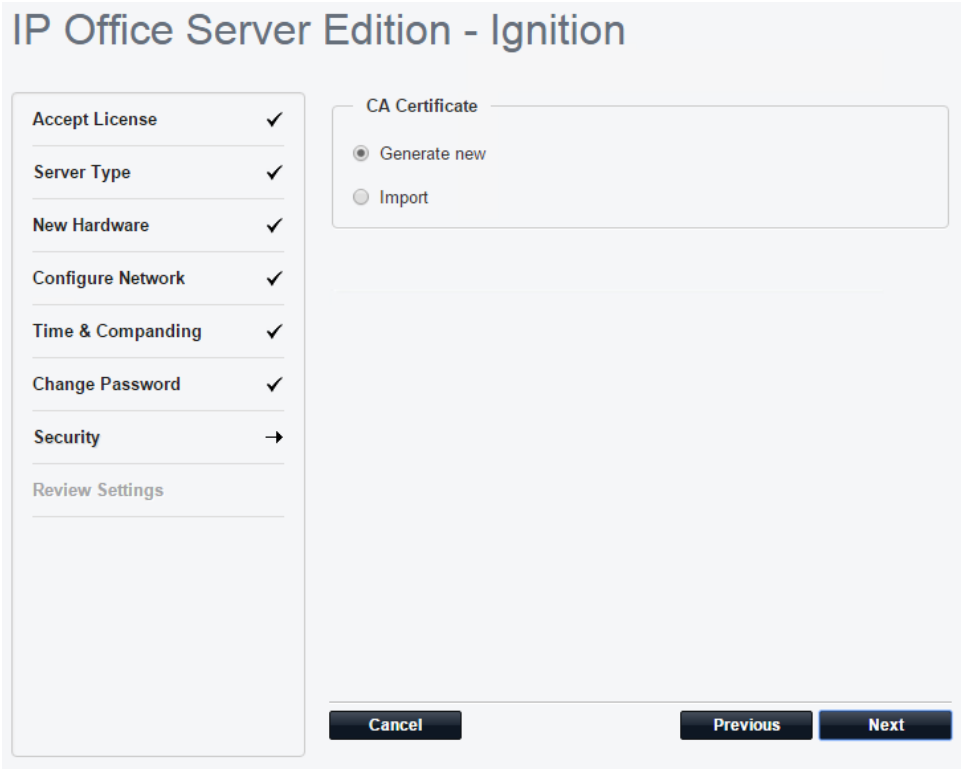

7. Set NTP server, Timezone and Companding, then click **Next**



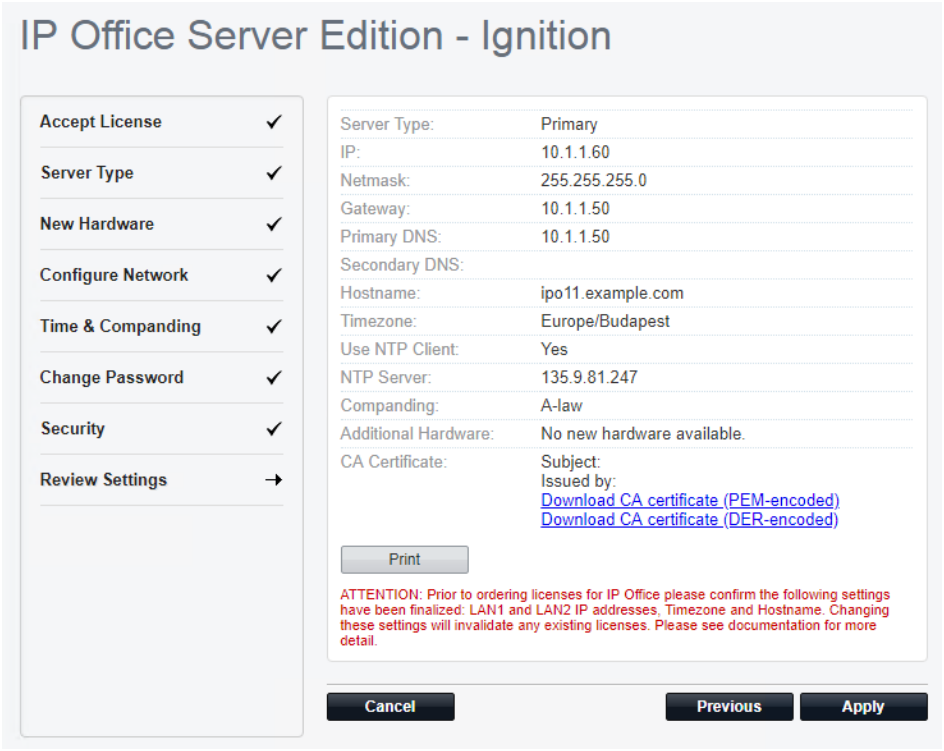

8. Set passwords, then click **Next**




9. Select **Generate new** CA Certificate and click **Next**

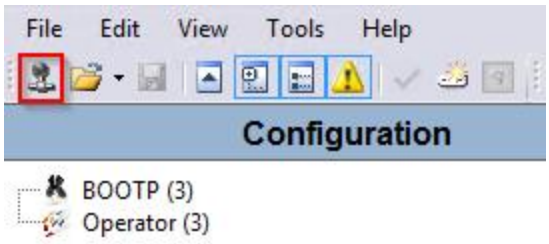



10. At the summary click **Apply**

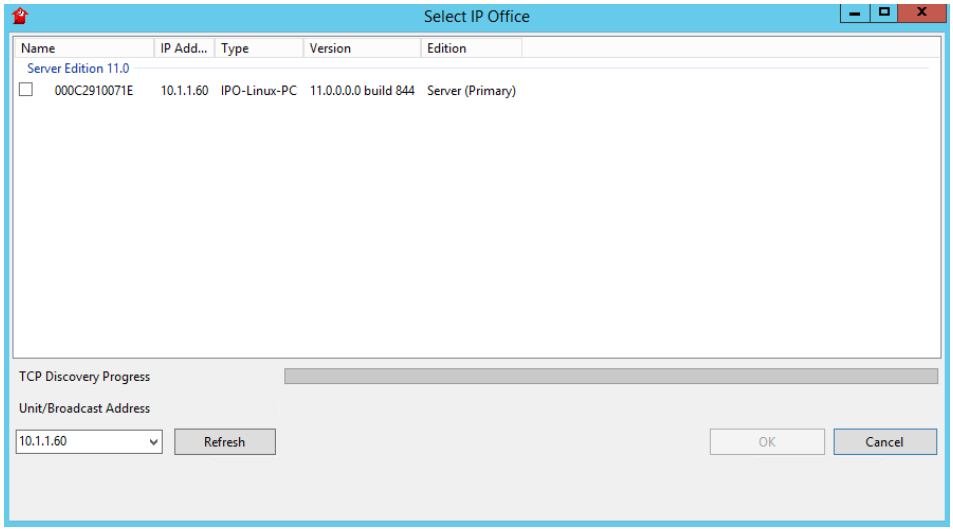



## Initial Configuration

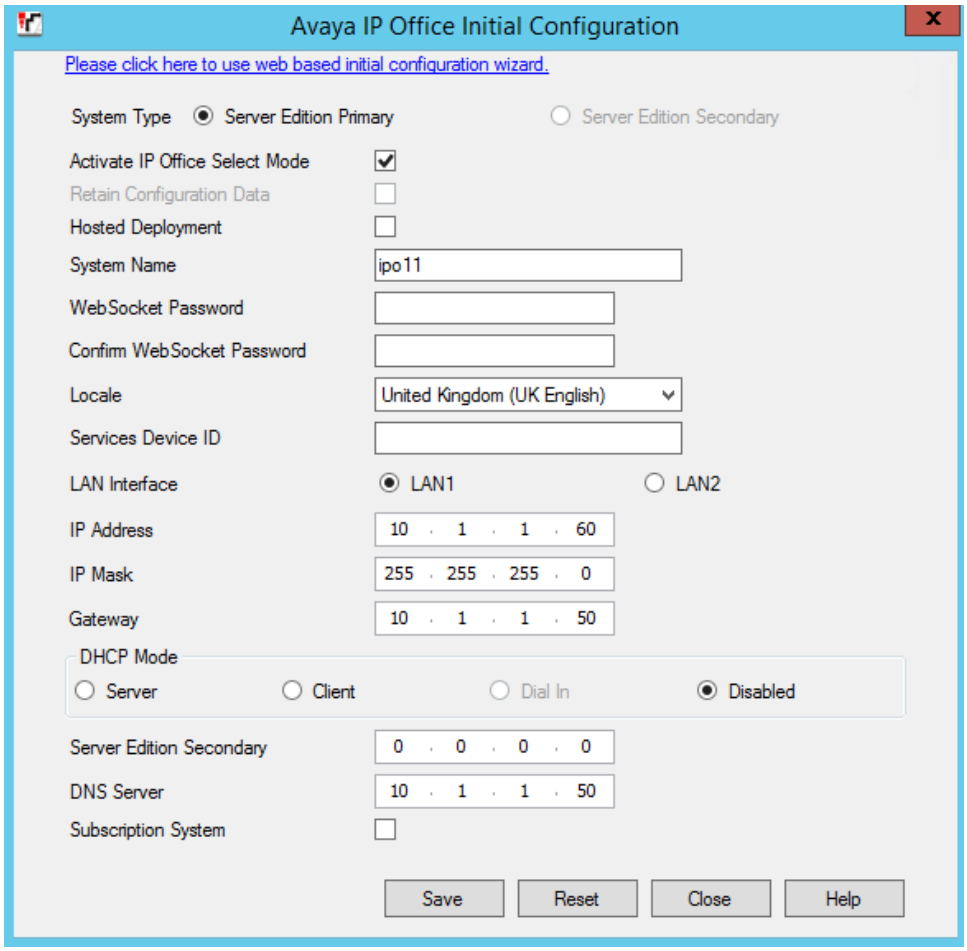
1. Start **IP Office / Manager** on your PC
2. Click on the **Open configuration from IP Office** icon




3. Select the IP Office box and click **OK**. If list is empty, type the IP address of the server in **Unit/Broadcast Address**, then click **Refresh**



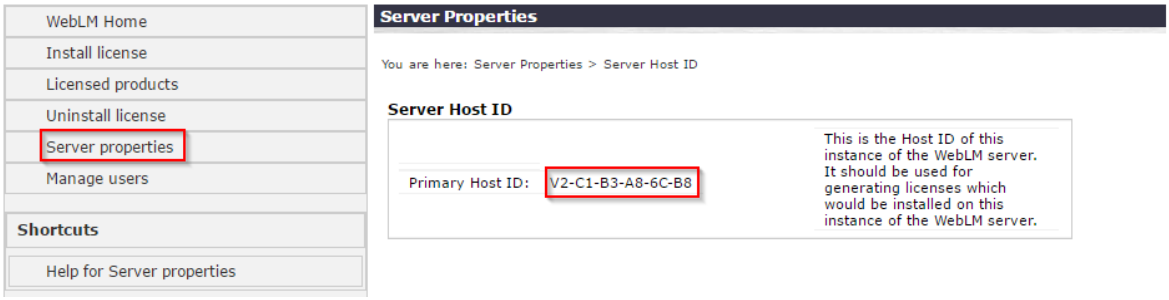

4. Login with the Administrator password you set during Ignition
5. Check **Activate IP Office Select Mode**, edit **System Name, LAN1 Interface, DHCP Mode, DNS server**, leave the rest on default, then click **Save**.



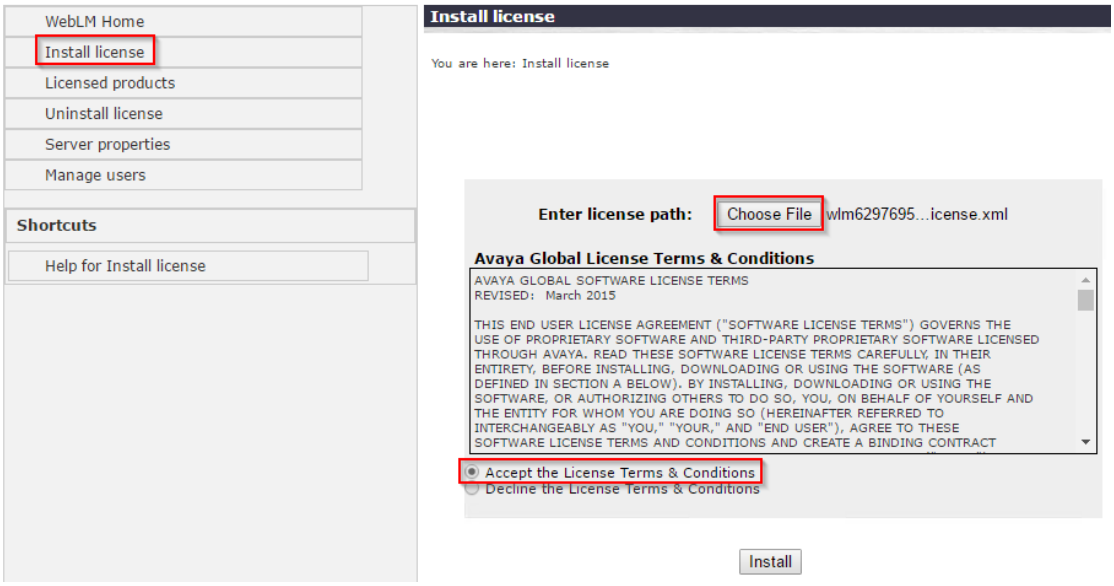

## Installing License

1. Open a browser to **https://<PrimaryServerIP>:52233/WebLM/index.jsp**


2. Log On with User Name **admin** and Password **weblmadmin**. On first login, the default password has to be changed.
3. After password change, login with the new password
4. Go to **Server properties** and note the **Primary Host ID**




5. Obtain license file using the above Host ID
6. Go to **Install license**, click on **Choose File** and select the license file, accept the terms & conditions, then click on **Install**

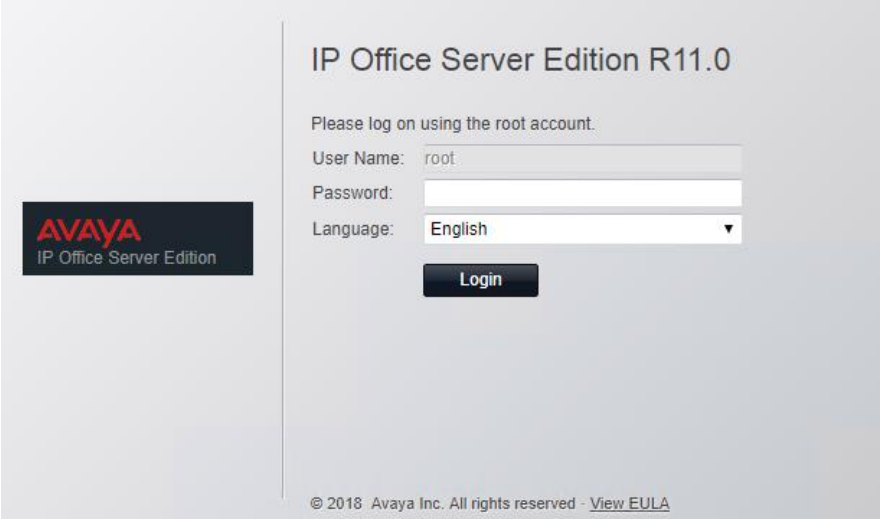



## Installing Secondary IP Office

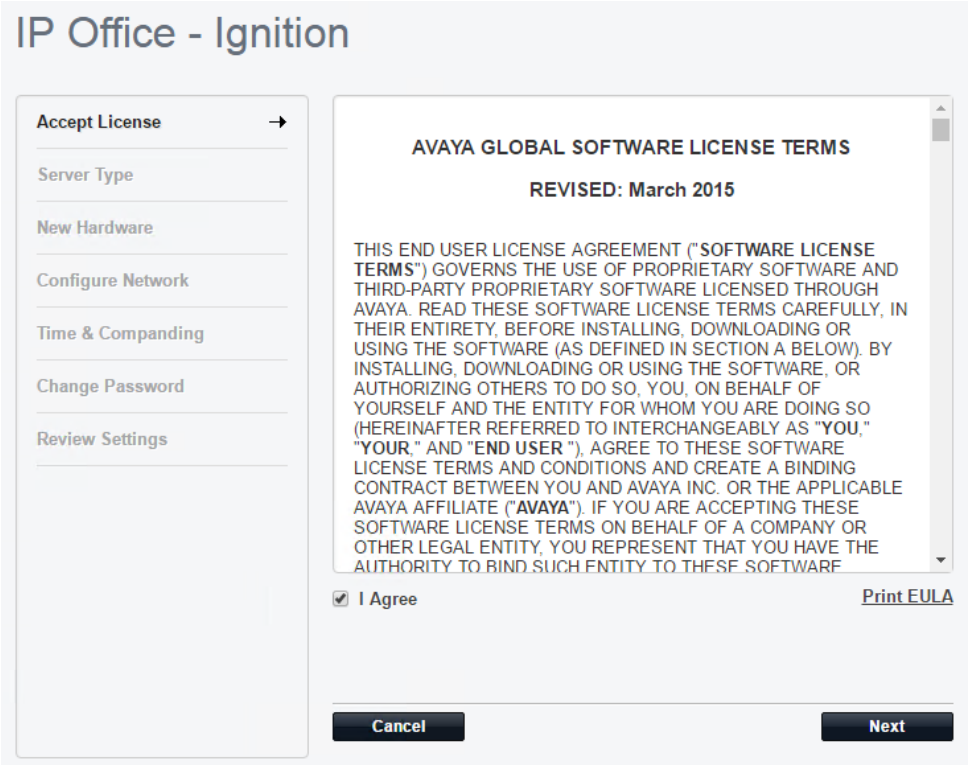
Deploy the OVA and set IP address same way as on primary.

### Secondary Server Ignition

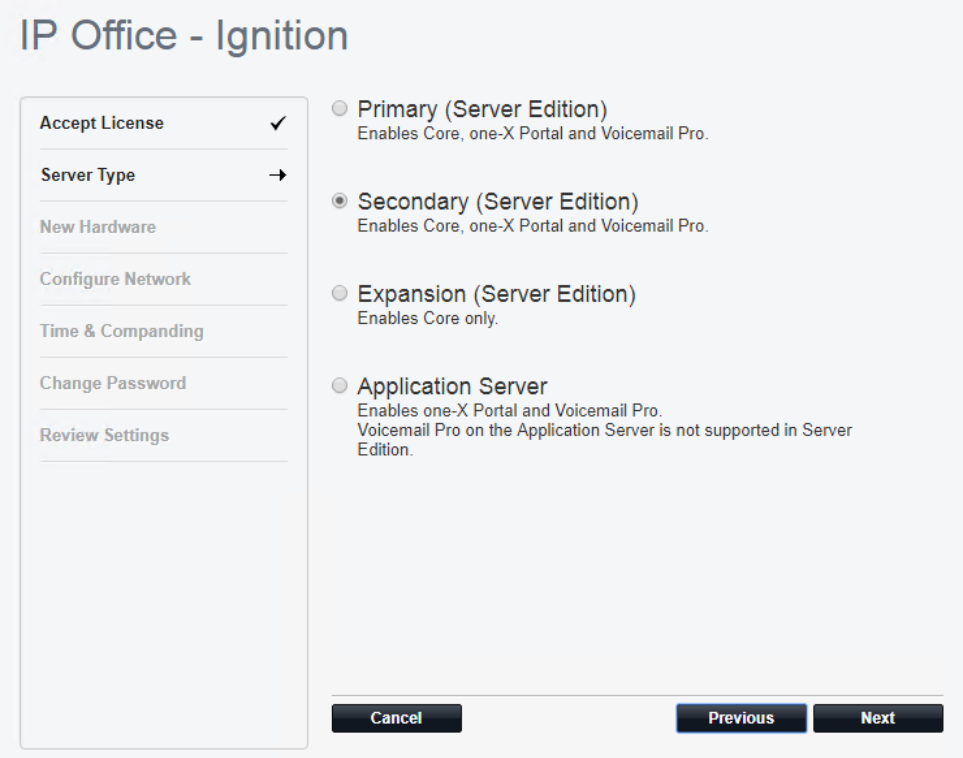
1. Open a browser and connect to **https://<SecondaryServerIP>:7071**
2. Use password **Administrator**



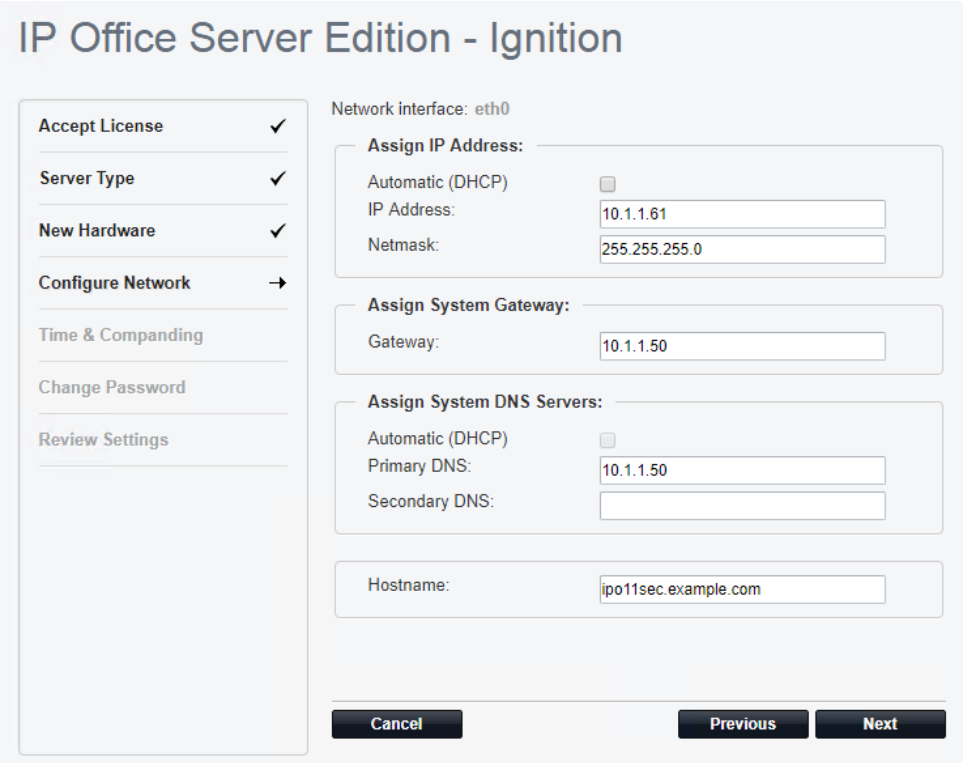

3. At the EULA check **I Agree** then click **Next**



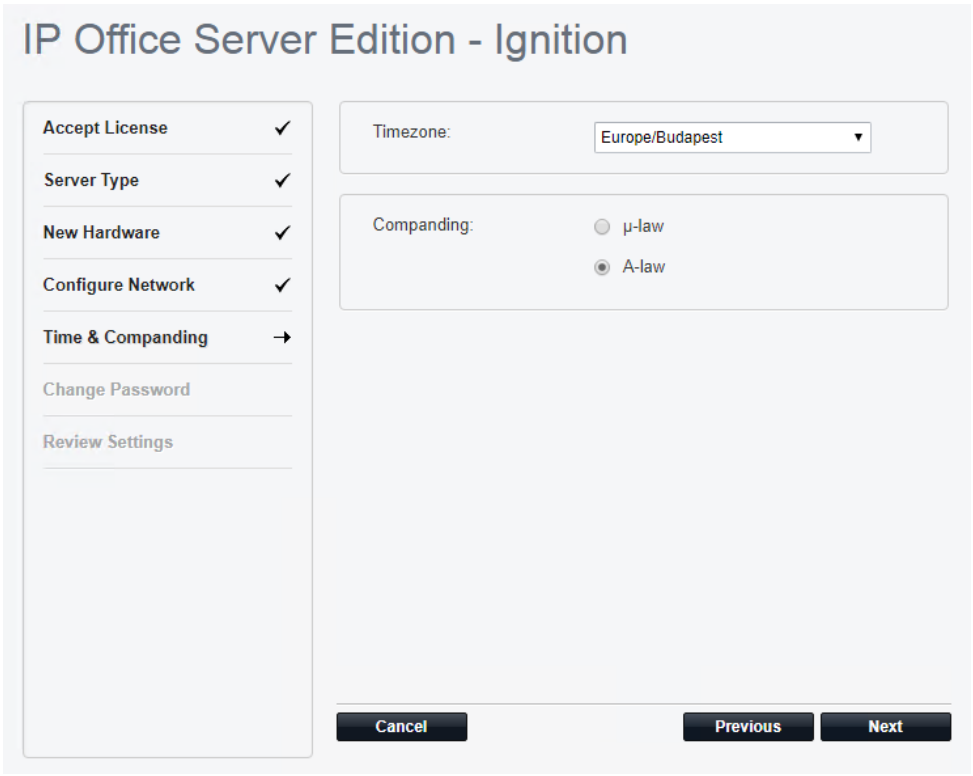

4. Select Secondary (Server Edition) and click Next



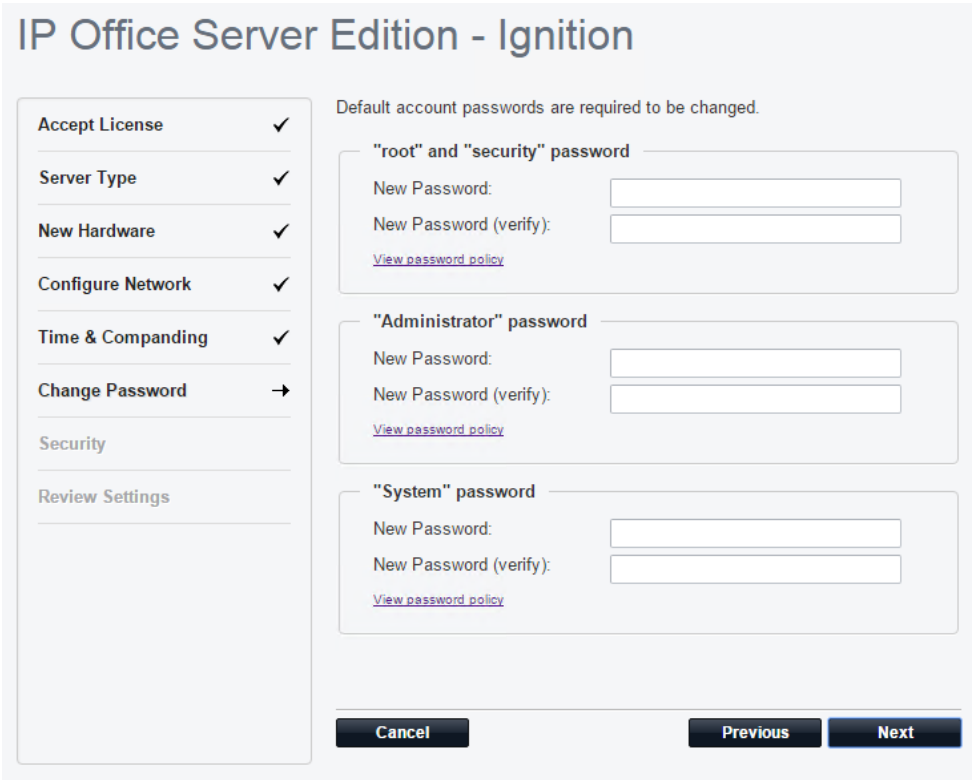

5. No new hardware available, click **Next**
6. Set network parameters as needed, enter hostname (**FQDN**), then click **Next**



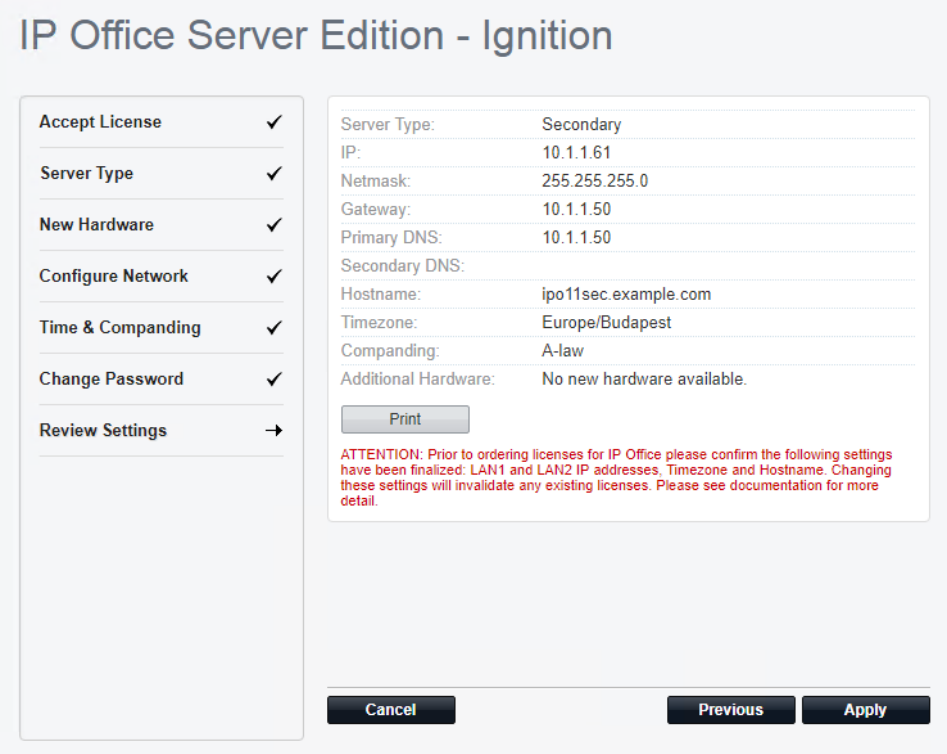

7. Set Timezone and Companding, then click **Next**




8. Set passwords, then click **Next**



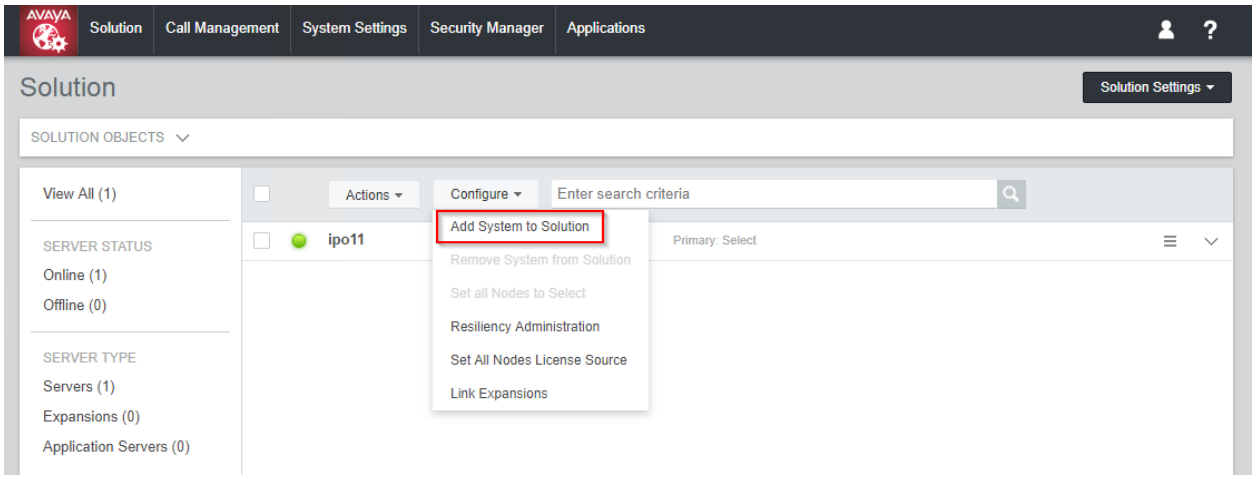

9. At the summary click **Apply**



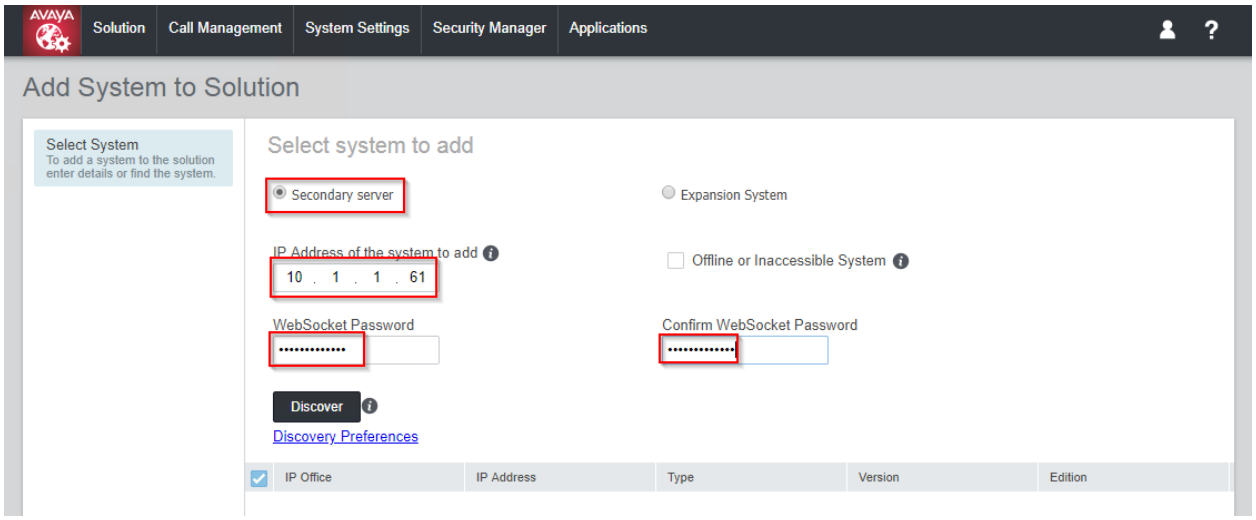

## Adding Secondary Server to the Solution

1. Open a browser and connect to **https://<PrimaryServerIP>:7070**, use the **Administrator** login and password you set during Ignition

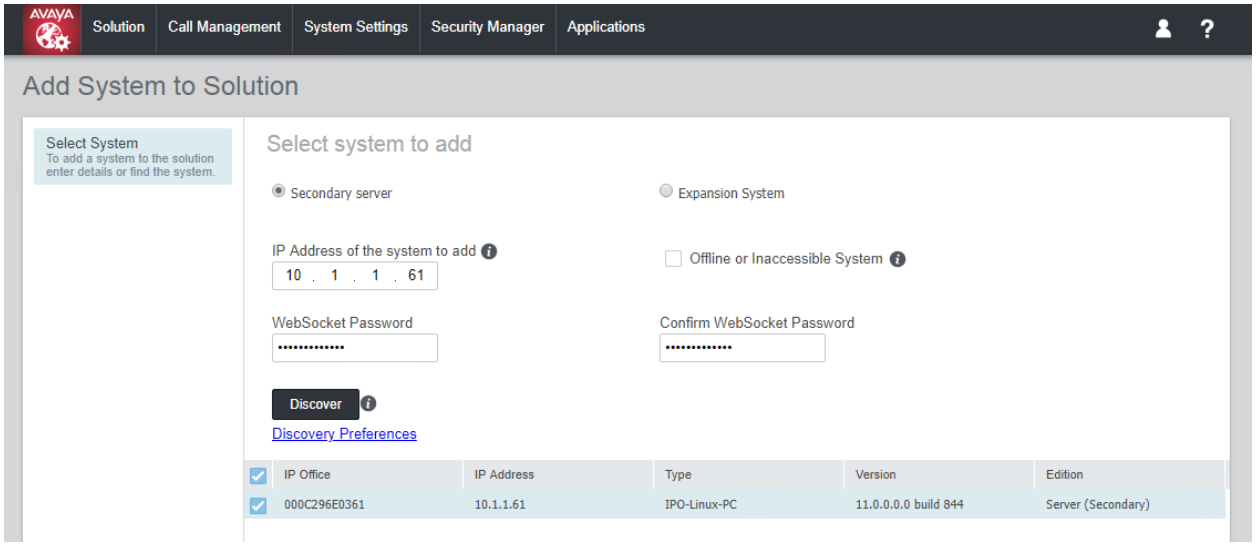

2. On the **Solution** tab click on **Configure** and select **Add System to Solution**



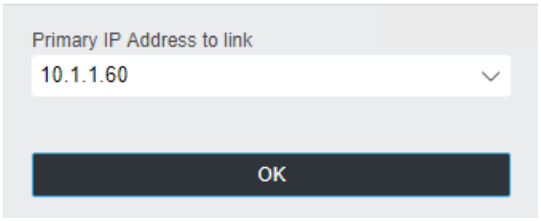

3. Select **Secondary Server**, enter its **IP** and **Web Socket Password** then click on **Discover**



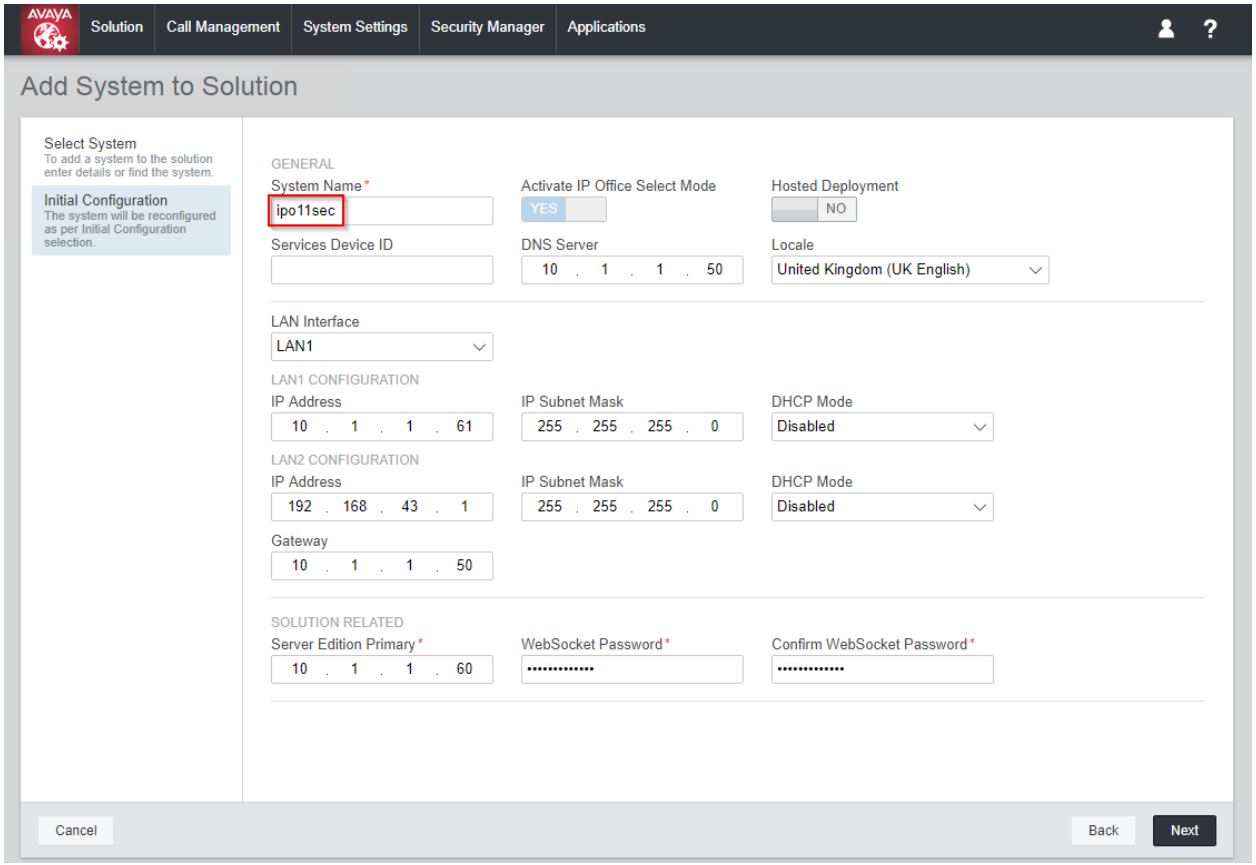

4. Select the discovered system and click **Next**



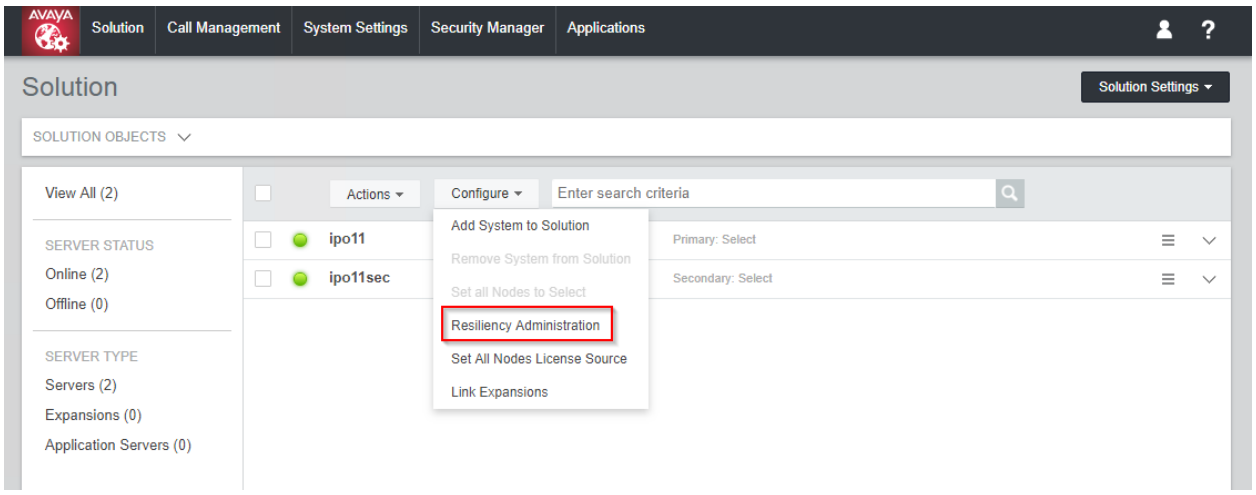

5. Select the Primary IP and click **OK**



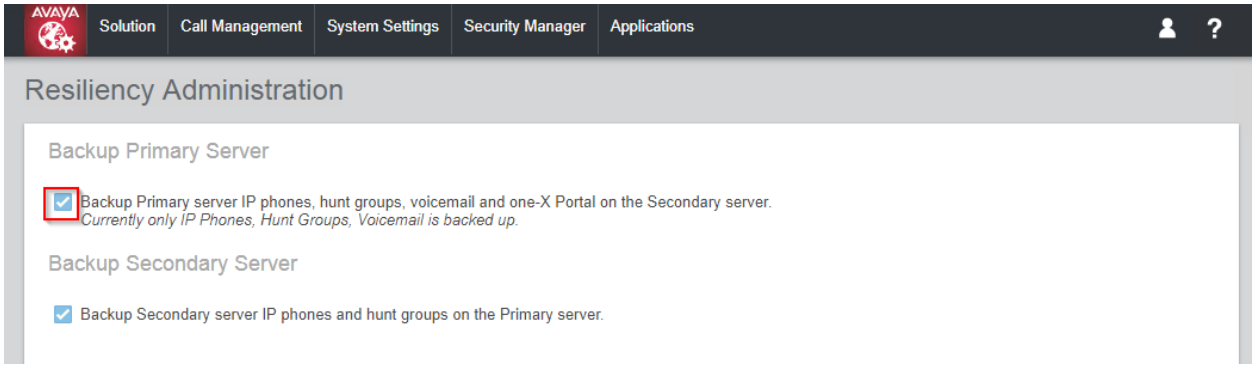

6. Enter System Name and verify/correct all other data




7. On the **Solution** tab click on **Configure** and select **Resiliency Administration**



8. Select **Backup Primary Server** and click **Update**

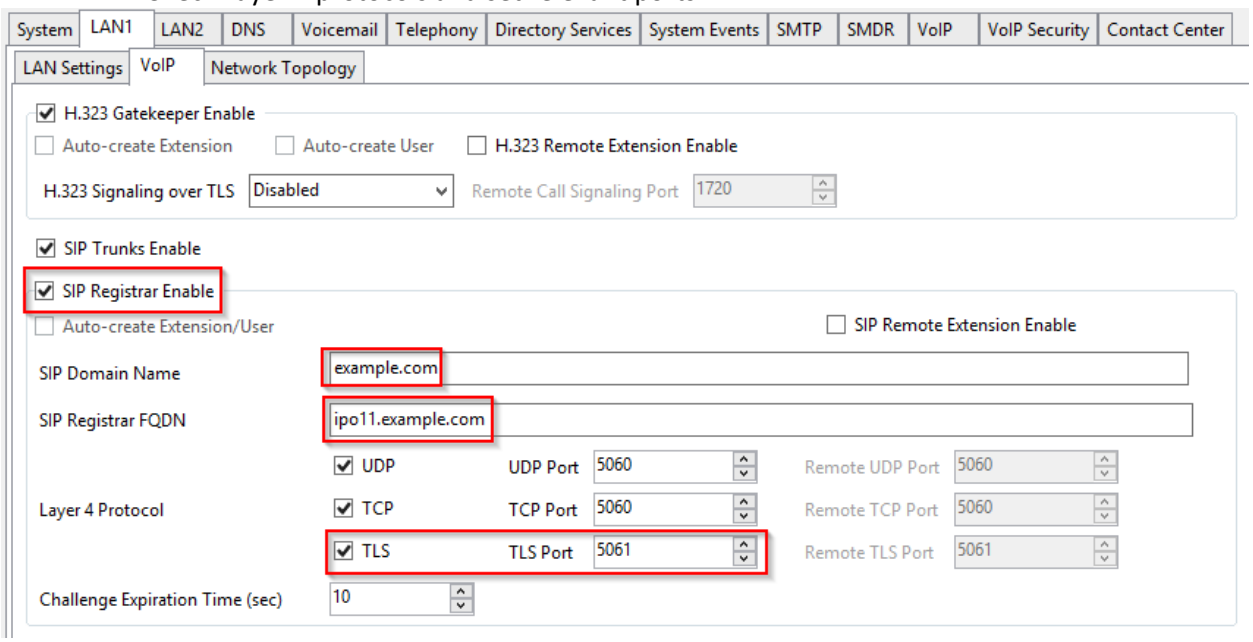



9. Reboot both servers

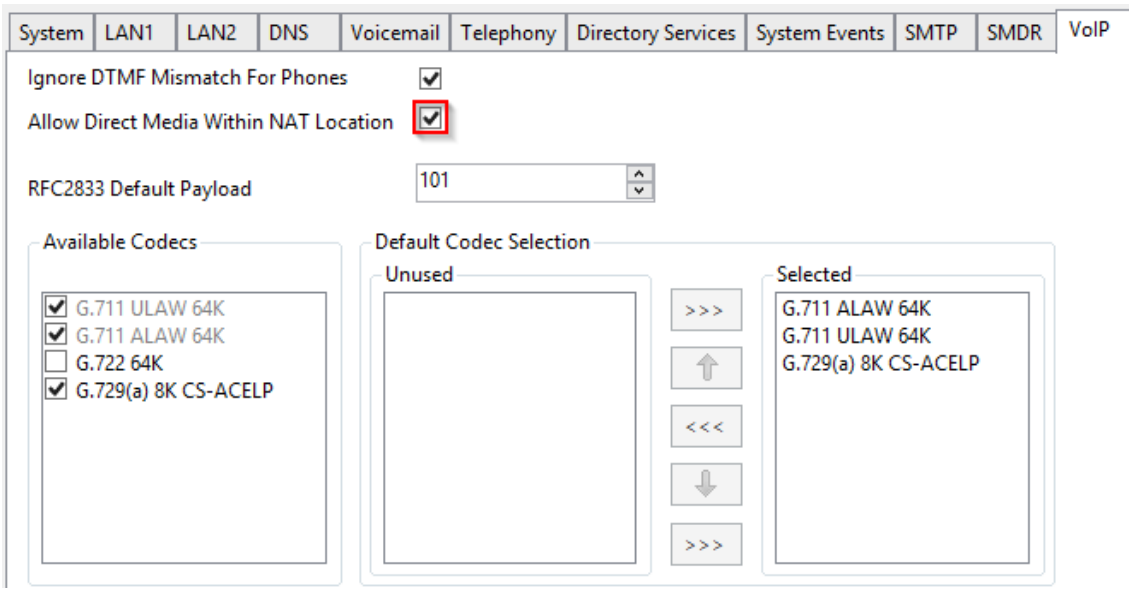
## Configuring IP Office

### VoIP Setup

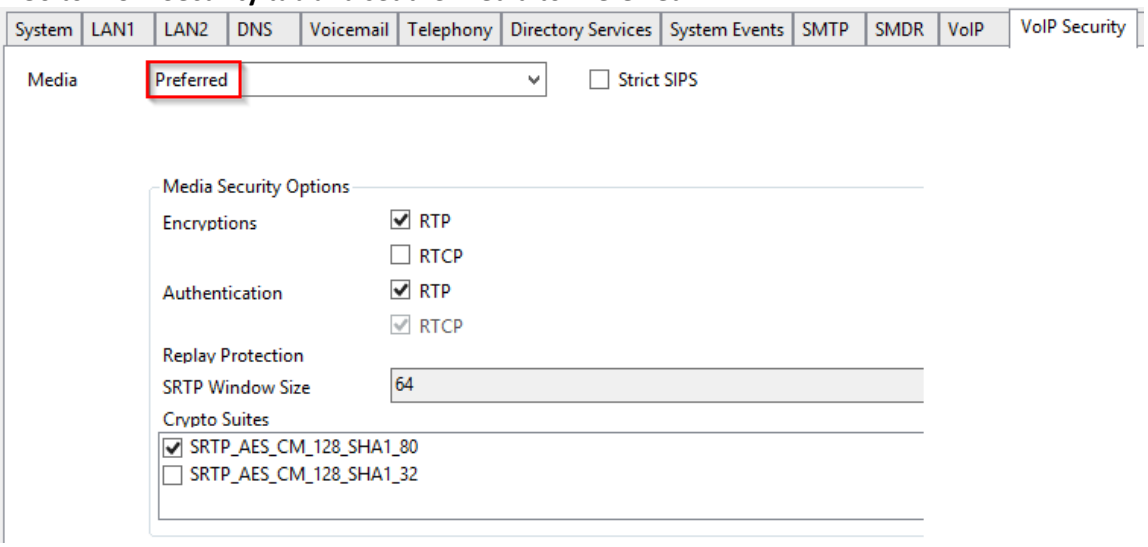
1. Expand the IP Office element under **Solution** and select **System**
2. Under **LAN1 / VoIP** tab set the followings:
   a. Check **SIP Registrar Enable**: allows to register SIP clients to IPO
   b. Un-check **Auto-create Extn/User**: we want to manually control what users can be added and registered
   c. Un-check **SIP Remote Extn Enable**: we will use SBCE for remote worker so IPO does not need to handle NAT scenarios
   d. Set **SIP Domain Name**: this is the local SIP domain the clients will register to
   e. Set **SIP Registrar FQDN**: the SIP registrar (IPO) fully qualified domain name
   f. Check Layer 4 protocols and set relevant ports




3. Go to **VoIP** tab and select **Allow Direct Media Within NAT Location**



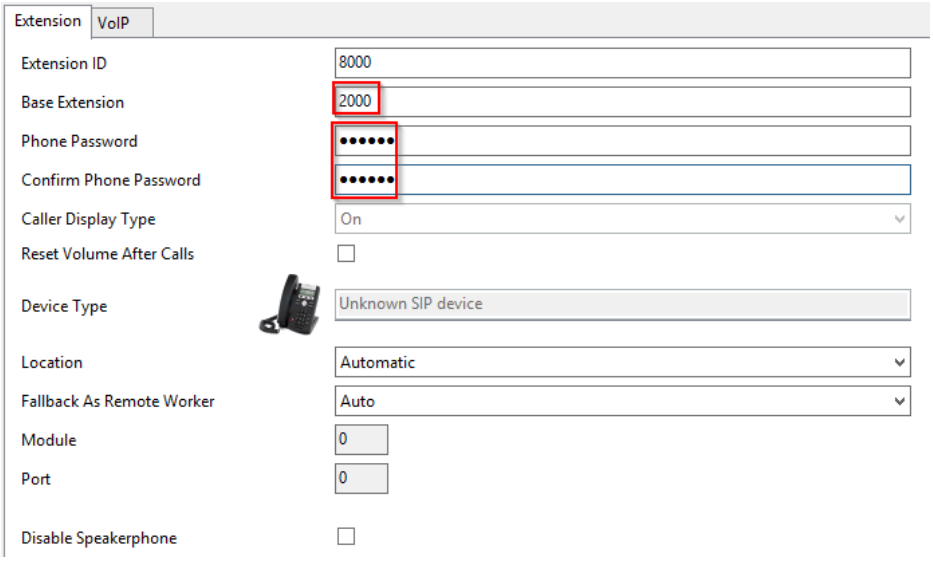

4. Go to **VoIP Security** tab and set the **Media** to **Preferred**




5. Click **OK** and **Save** configuration
6. Repeat above settings on secondary server using ipo11sec.example.com as SIP Registrar FQDN

## Extensions

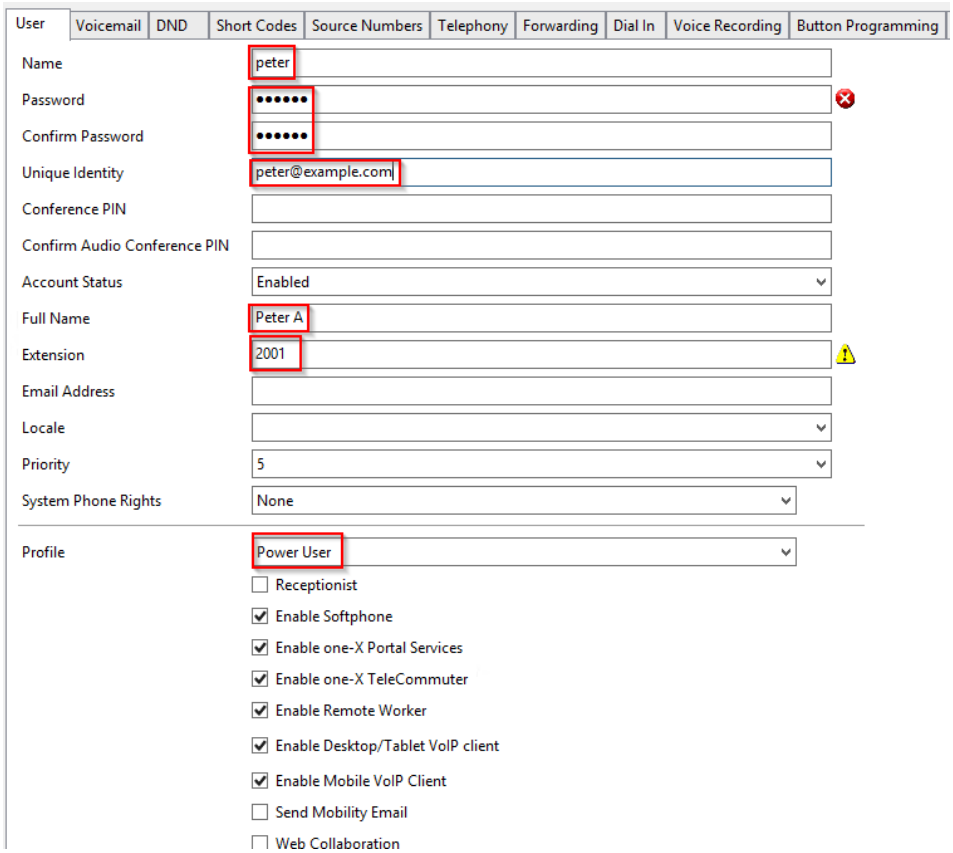
1. Expand the IP Office element under **Solution** and select **Extension**
2. Right-click on **Extension** and select **New / SIP Extension**
3. Enter **Base Extension**, this will be used on User form to assign extension to user, and set password



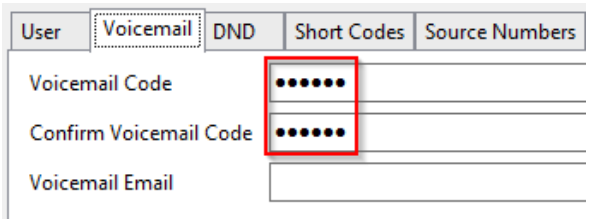

7. Click **OK** and **Save** configuration

## Users

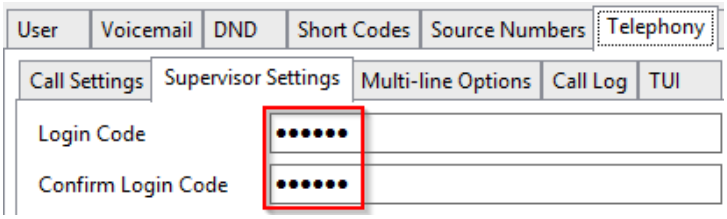
1. Expand the IP Office element under **Solution** and select **User**
2. Right-click on **User** and select **New**
3. Under User tab set the followings:
    a. **Name**: short user name
    b. **Password**: use digits only as this password will be used by most of the clients to register, and not all clients support alphanumeric password
    c. **Extension**: must match the Base Extension
    d. **Full Name**: full name of the user
    e. **Profile**: select **Power User**
    f. **Unique Identity:** set the email address that will belong to the given user in Zang as this will connect the IPO user with the Zang user. This configuration is needed for Equinox Instant Messaging.




4. Under **Voicemail** tab set **Voicemail Code**




5. Under **Telephony / Supervisor Settings** tab set the **Login Code**




NOTE: This code is used by Communicator for iPhone as password for the user. Other clients use the Password on the User tab.

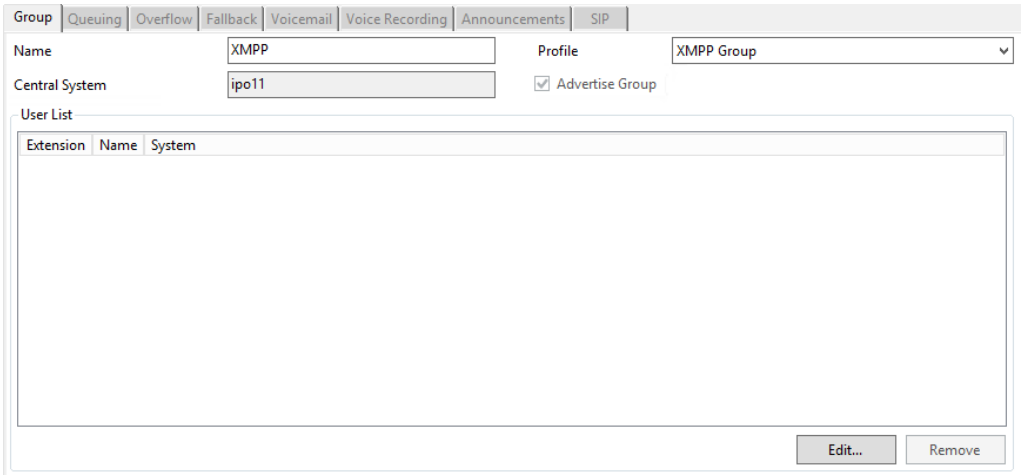
6. Click **OK** and **Save** configuration

## XMPP Hunt Group

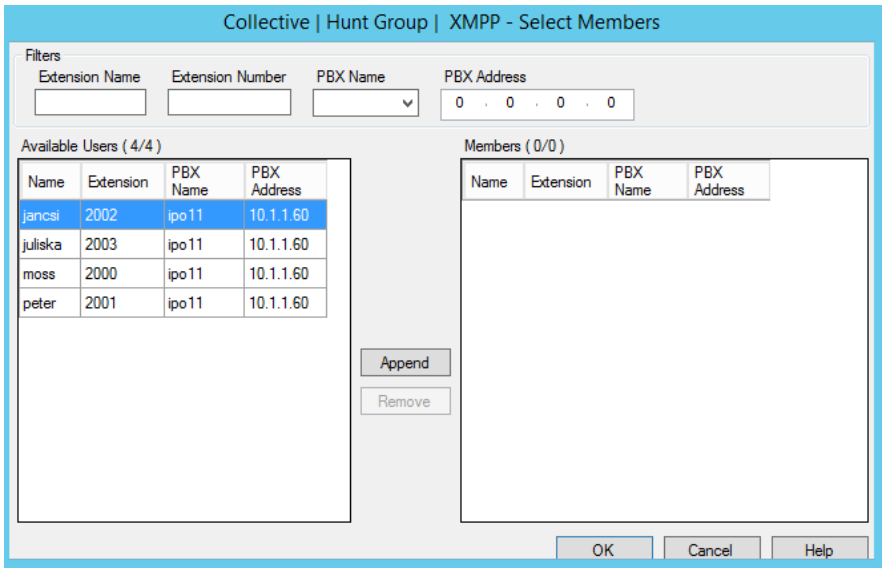
NOTE: This configuration is needed by One-X Mobil Preferred to be able to see Presence status of other users

1. Expand the IP Office element under **Solution** and select **Group**

2. Right-click on **Group** and select **New**
3. Under Group tab set the followings:
    a. **Name**: name of the group
    b. **Profile**: select **XMPP Group**




4. Click **Edit**
5. Select all **Available Users** and click **Append**, then click **OK**

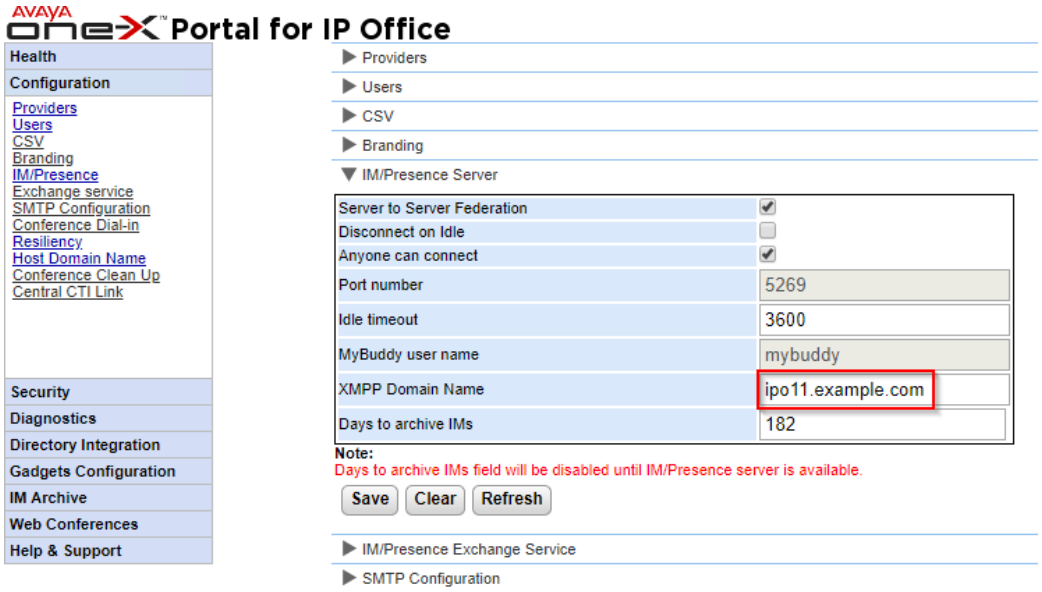



6. Click **OK** and **Save** configuration

## Configuring One-X Portal

1. Open a browser and connect to **https://<PrimaryServerIP>:9443/onexportal-admin.html**, use the **Administrator** login and password you set during Ignition


2. Under **Configuration / IM/Presence** set the **XMPP Domain Name** and click **Save.**




3. Go to **Configuration / Host Domain Name,** set the FQDN of primary and secondary server, then click **Save**


4. Reboot both servers

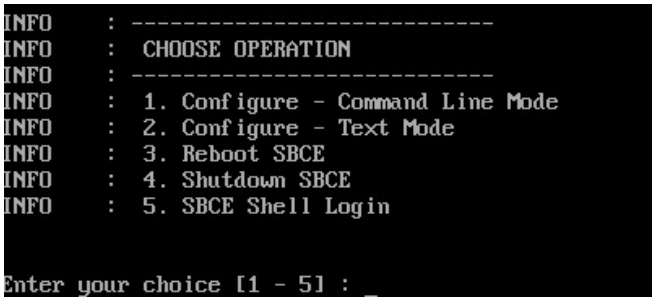
# Installing SBCE

## Deploying OVA

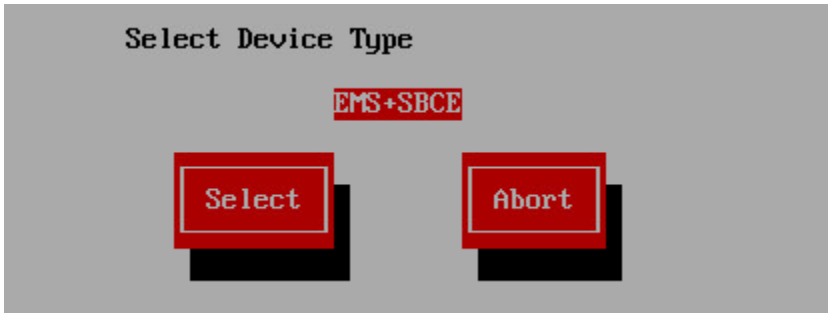
1. Download latest SBCE OVA file from **plds.avaya.com**
2. Start vSphere Client and connect to vCenter / AVP host
3. Go to **File / Deploy OVF Template**
4. **Browse** the OVA and click **Next**
5. At OVF Template Details click **Next**
6. Click **Accept** at EULA, then click **Next**
7. Enter **Name** for the virtual machine and click **Next**
8. Select **Small SBC** configuration and click **Next**
9. Select data store and disk provision mode, then click **Next**
10. Select Destination Network and click **Next**
11. Click **Finish** at the summary
12. Once VM is deployed, start it

## Setting Management IP

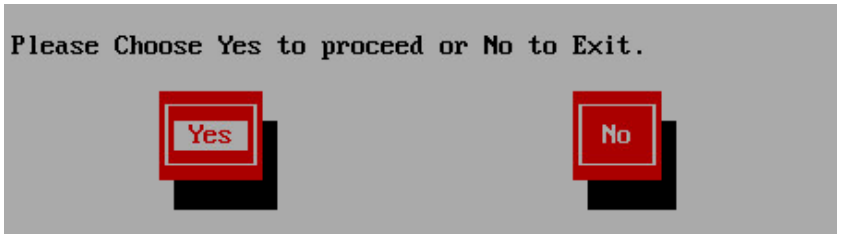
1. Right click on the SBCE virtual machine then click on **Open Console**
2. Wait for the virtual machine to boot up until the following can be seen in the console window:



3. Click in the console and enter **2**
4. Navigate to **Select** and hit **Enter**

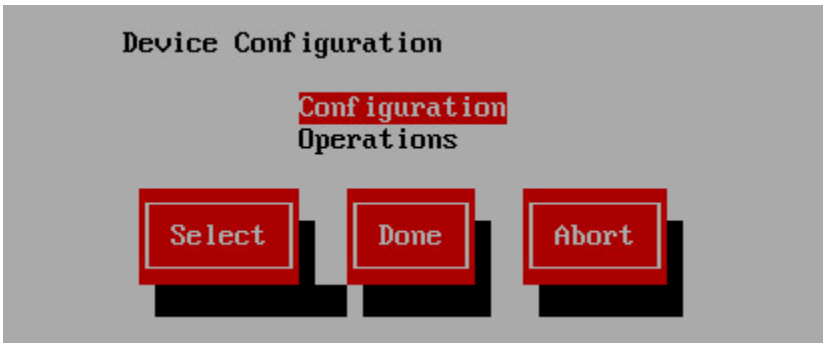



5. Hit **Enter** on **Yes**

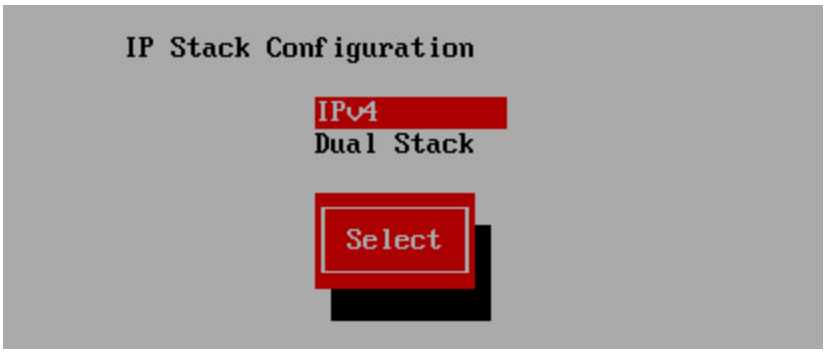



6. Hit **Enter** on **OK**

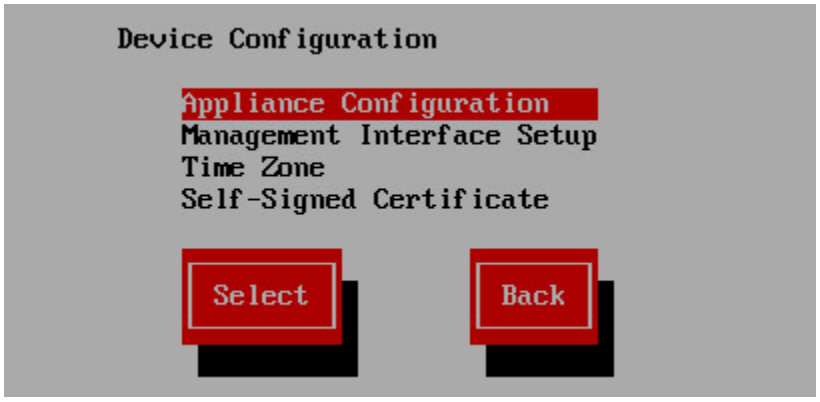

7. Select **Configuration**, then hit **Enter** on **Select**



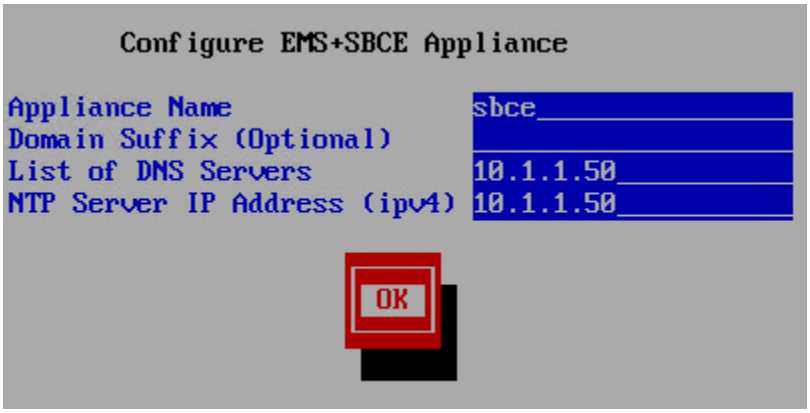

8. Select **IPv4** and hit **Enter** on **Select**



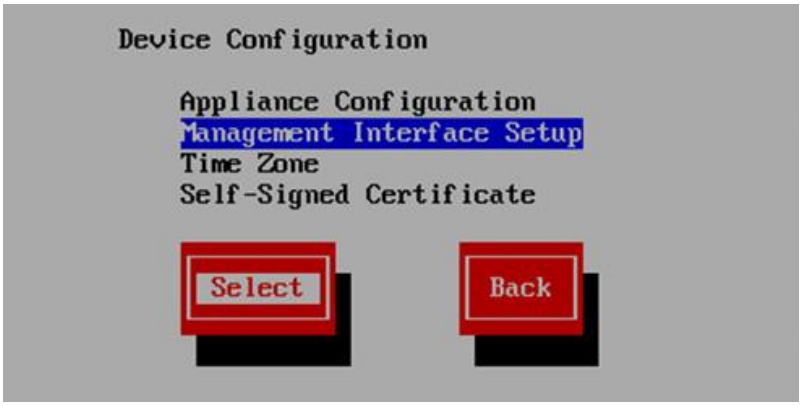

9. Select **Appliance Configuration** and hit **Enter** on **Select**



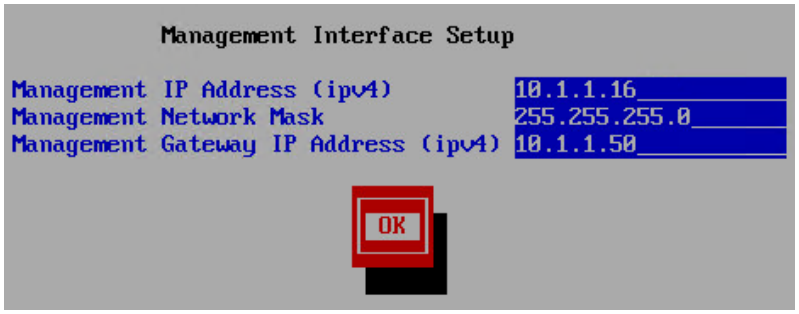

10. Fill in the DNS and NTP parameters and hit **Enter** on **OK**



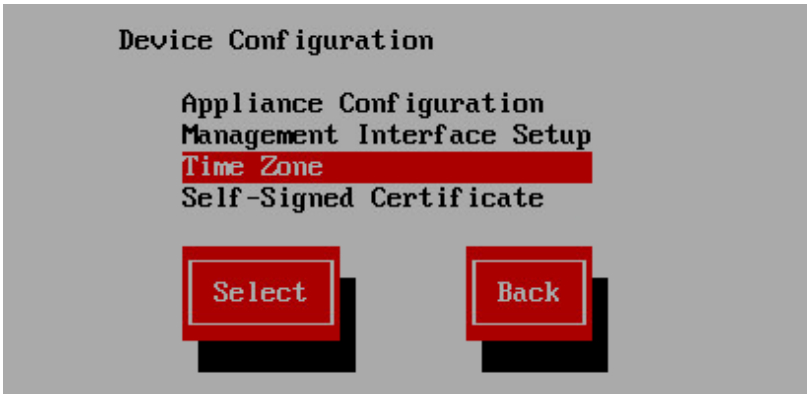

11. Select **Management Interface Setup** and hit **Enter** on **Select**



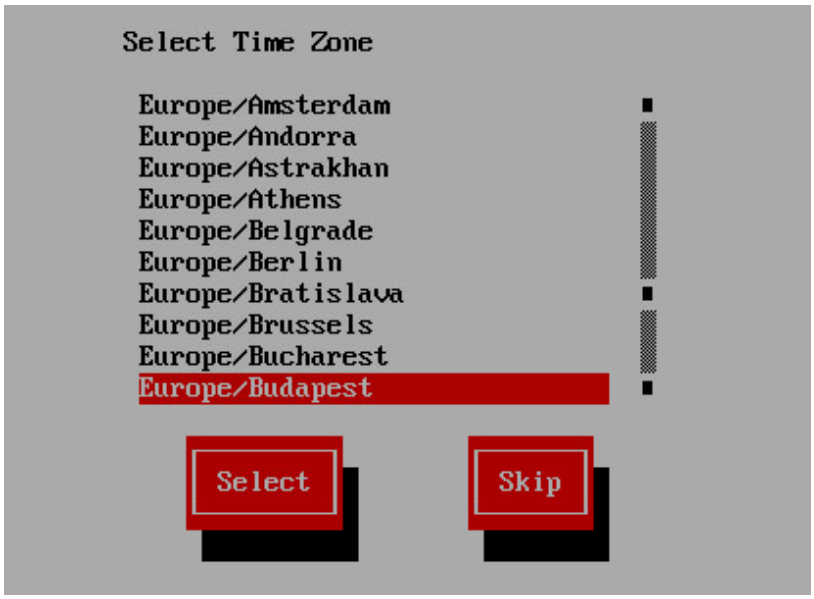
12. Fill in the IP details of management interface and hit **Enter** on **OK**



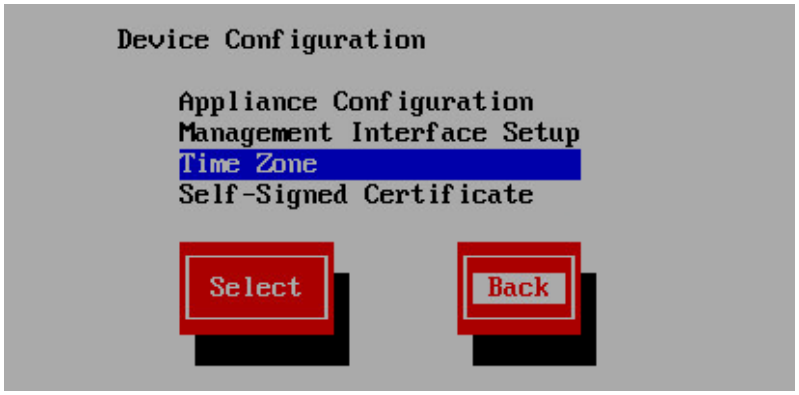

13. Select **Time Zone** and hit **Enter** on **Select**



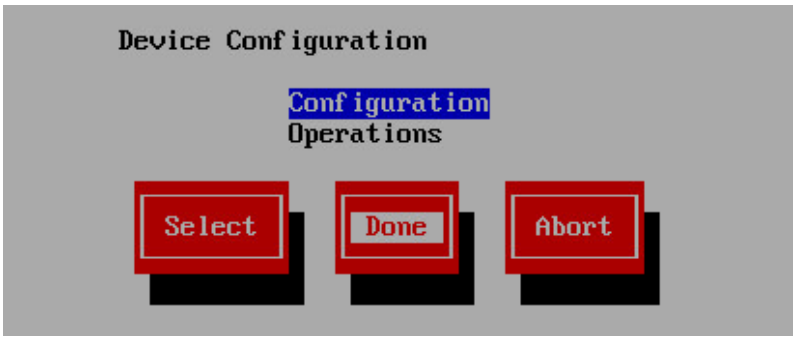

14. Select your time zone and hit **Enter** on **Select**




15. Hit **Enter** on **Back**




16. Hit **Enter** on **Done**




17. Enter new **root** password

```
INFO    : ================================================================
INFO    : Configuring password for 'root' user
INFO    : ================================================================
INFO    : Your password should meet following requirements:
INFO    :     1. At least 8 characters
INFO    :     2.          1 upper case letters
INFO    :     3.          1 lower case letters
INFO    :     4.          1 other characters (_, $, @,etc.)
INFO    :     5.          1 digits
INFO    : ================================================================
Changing password for user: root
New Password:
```

18. Enter new password for **ipcs** login
19. Enter new password for **grub**

## Setting VMware network for external interface

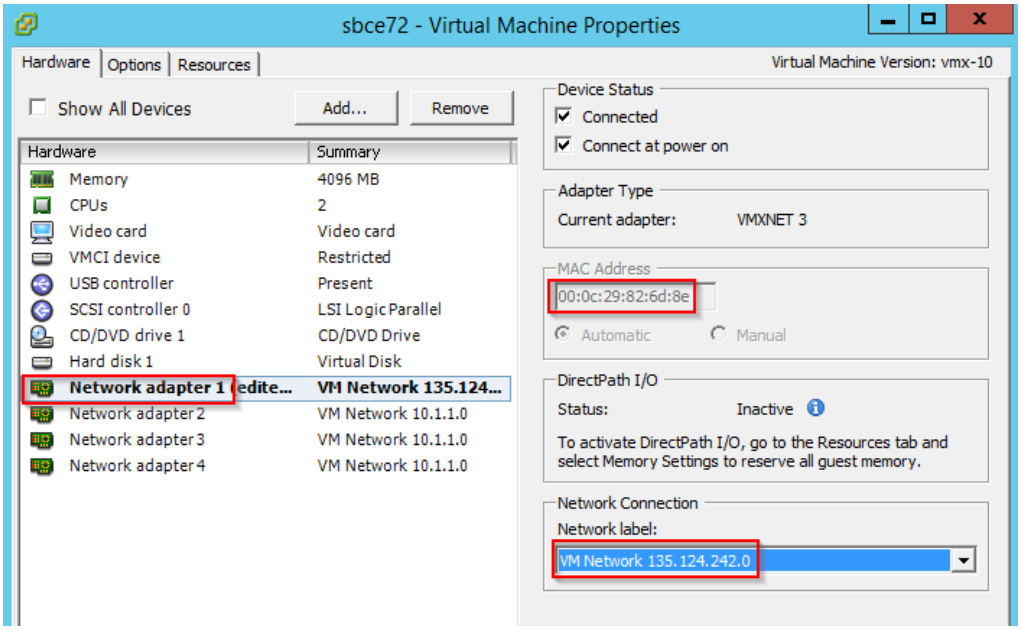
1. At the console login with **root** using the new password
2. Issue the command **ip addr** and note the **MAC** address of **B1** interface

```
                              WELCOME TO AVAYA SBC

Unauthorized access to this machine is prohibited. This system is for the use
authorized users only. Usage of this system may be monitored and recorded by system personnel.

Anyone using this system expressly consents to such monitoring and is
advised that if such monitoring reveals possible evidence of criminal activity,
system personnel may provide the  evidence from such monitoring to law enforcement officials.
sbce login: root
Password:
Last login: Mon Aug 21 11:45:01 CEST 2017 on cron
Last login: Mon Aug 21 11:47:27 on tty1
[root@sbce ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: B1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:0c:29:82:6d:8e brd ff:ff:ff:ff:ff:ff
3: A2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:0c:29:82:6d:98 brd ff:ff:ff:ff:ff:ff
4: A1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:0c:29:82:6d:a2 brd ff:ff:ff:ff:ff:ff
5: M1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0c:29:82:6d:ac brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.16/24 scope global M1
       valid_lft forever preferred_lft forever
[root@sbce ~]#
```

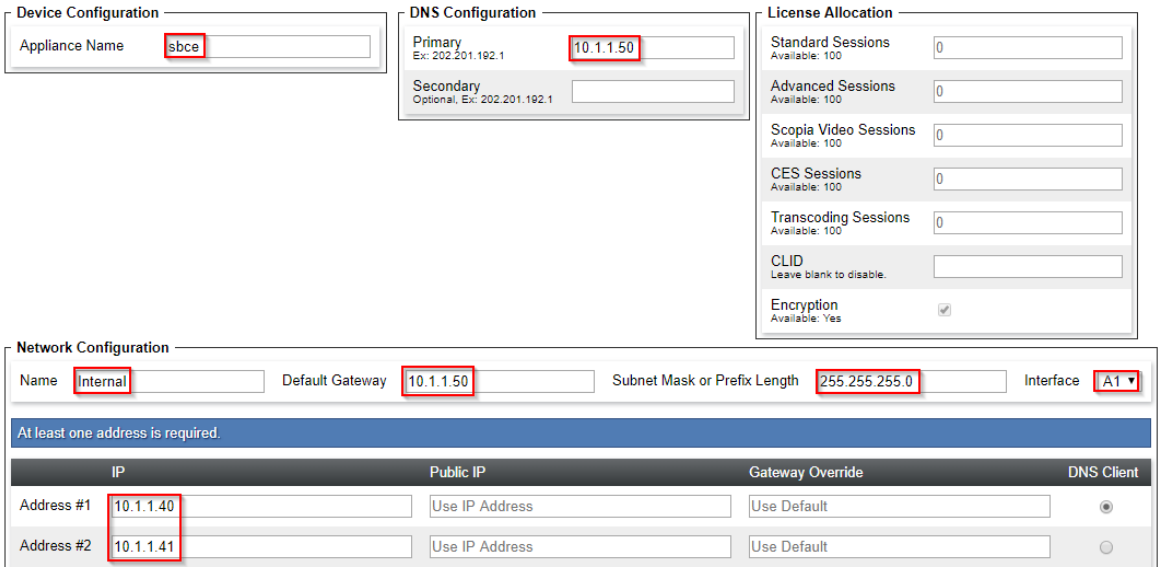
3. In vSphere client right click on the SBCE VM and select **Edit Settings**
4. Select the **Network adapter** where MAC address matches the **MAC address of B1** interface, change the **Network Connection** and click **OK**




## SBCE initial configuration

1. Open browser and connect to https://<Management IP>/
2. Login with Username **ucsec** and default password **ucsec**
3. As this is the first time login, **ucsec** default password has to be changed
4. Login again with **ucsec** using the new password
5. Go to **System Management** and click **Install**
6. Set the following fields:

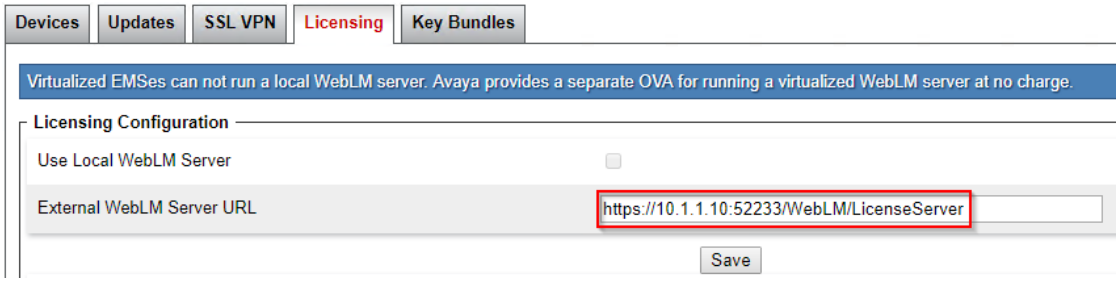
a. **Device Configuration**
   i. **Appliance Name**: internal name of the SBCE
b. **DNS Configuration**
   i. **Primary**: IP of DNS server
c. **Network Configuration**
   i. **Name**: name of internal network
   ii. **Default Gateway**: gateway for internal interface
   iii. **Subnet Mask**: subnet mask of internal interface
   iv. **Interface**: we use A1 for internal traffic
   v. **Address #1**: IP of internal interface used for primary IPO
   vi. **Address #2**: IP of internal interface used for secondary IPO




7. Click **Finish** when form is filled in
8. Close the Installation Wizard browser window

## Licensing

1. Obtain SBCE license and install it to the WebLM server
2. Go to **System Management / Licensing** tab
3. Enter the **External WebLM Server URL** and click **Save**

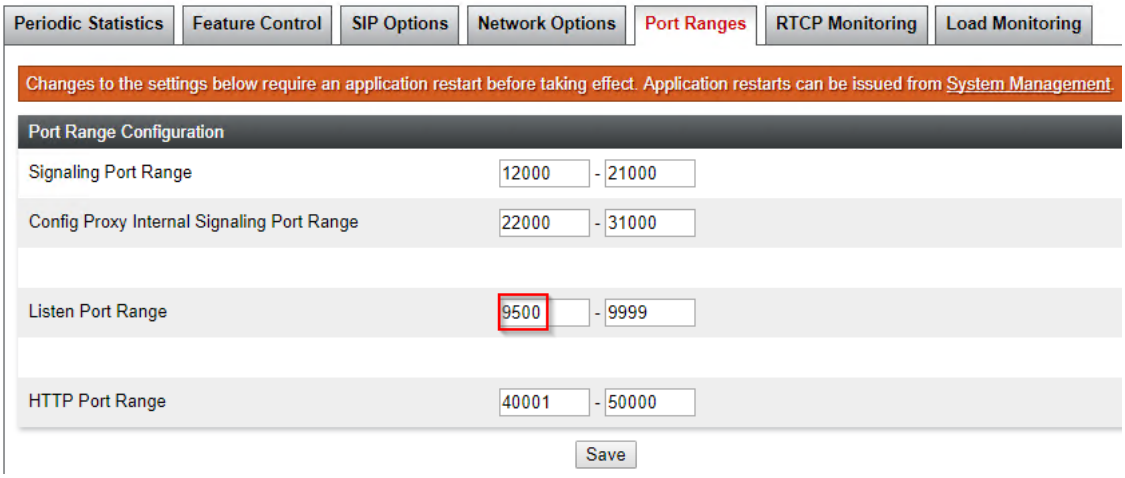



## Changing default Listen Port Range

NOTE: This step is necessary so that later we are able to configure listen port 9443 in Application Relay

1. Go to **Device Specific Settings / Advanced Options** and select **Port Ranges** tab

2. Change the **Listen Port Range** to **9500-9999** and click **Save**

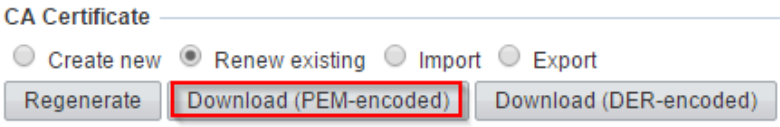



3. Go to **System Management** and on the **Devices** tab click on **Restart Application**

## Certificates for IPO

### Exporting IP Office Root CA

1. Open a browser and connect to **https://<PrimaryServerIP>:7071**
2. Login as **Administrator**
3. Go to **Settings** tab and scroll down to **Certificates**
4. Under **CA Certificate** click on **Download (PEM-encoded)** and save the file to your PC

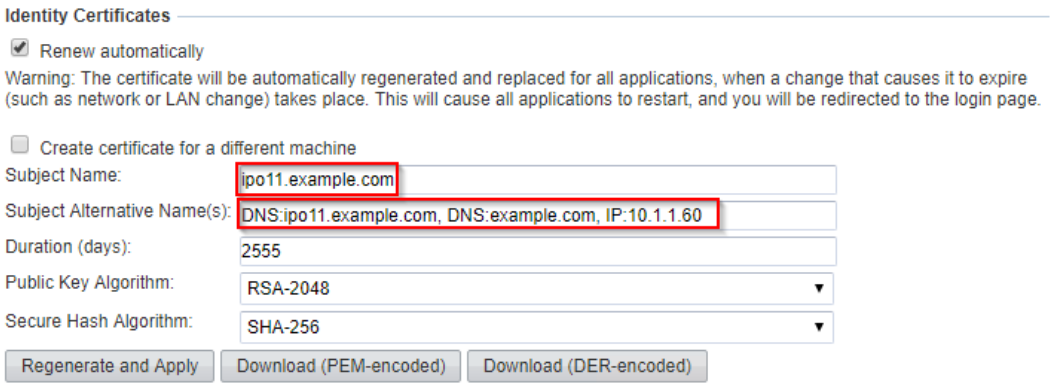



5. Rename the downloaded file (root-ca.pem) on your PC to **IPO_RootCA.crt**

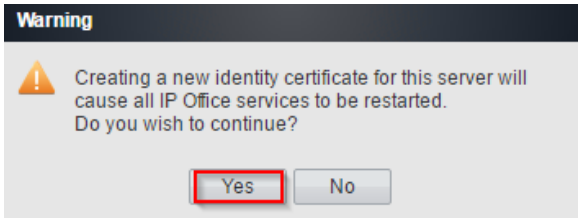
### Generating Identity Certificate for Primary Server

Note: Some clients are sensitive to what information is in the Subject Alternative Name field of the Identity Certificate of the IP Office, so it is recommended to list all the FQDNs and IP addresses in the Subject Alternative Name that clients might interact with during SIP and XMPP communication.

1. Open a browser and connect to **https://<PrimaryServerIP>:7071**
2. Login as **Administrator**
3. Go to **Settings** tab and scroll down to **Certificates**
4. Enter the following data then click **Regenerate and Apply**
    a. **Subject Name**: enter the FQDN of primary server
    b. **Subject Alternative Name(s)**: list the FQDN of primary server, the XMPP and SIP domains, the internal IP address of primary server



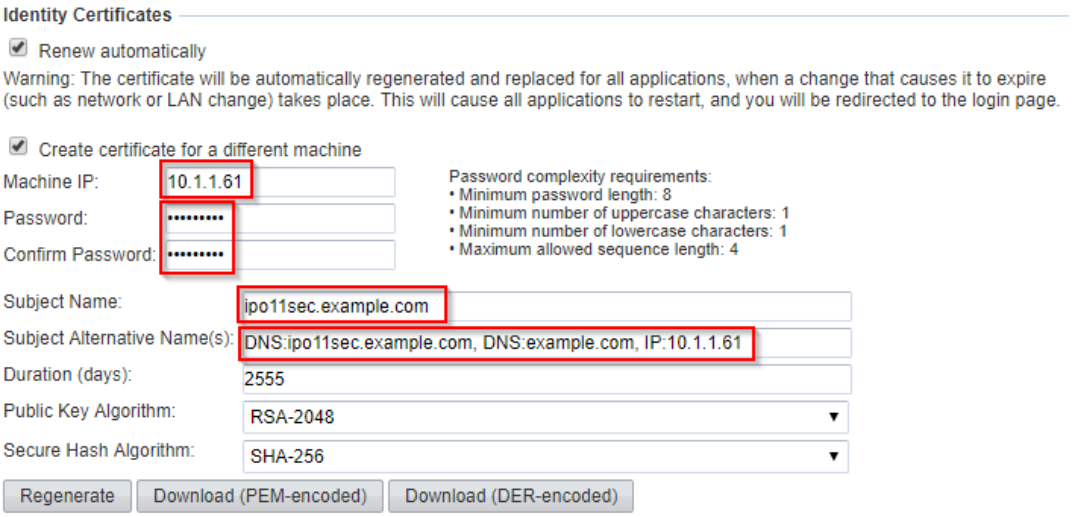

5. In the popup window click **Yes**



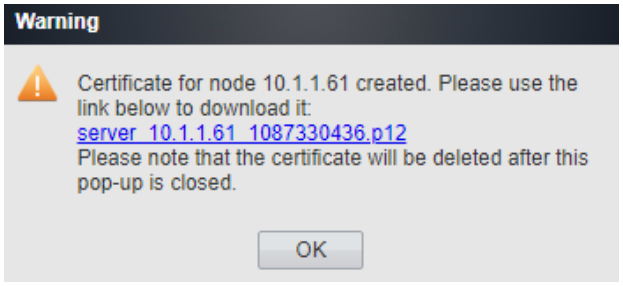

## Generating Identity Certificate for Secondary Server

NOTE: this is needed only if IP Office and One-X Portal are on different machines

1. Open a browser and connect to **https://<PrimaryServerIP>:7071**
2. Login as **Administrator**
3. Go to **Settings** tab and scroll down to **Certificates**
4. Check **Create certificate for a different machine**
5. Enter the following data then click **Regenerate**
    a. **Machine IP**: IP of secondary server
    b. **Password**: password to encrypt the certificate and key, for example **Avaya123$**
    c. **Subject Name**: enter the FQDN of secondary server
    d. **Subject Alternative Name(s)**: list the the FQDN of secondary server, the SIP domain, the internal IP address of secondary server

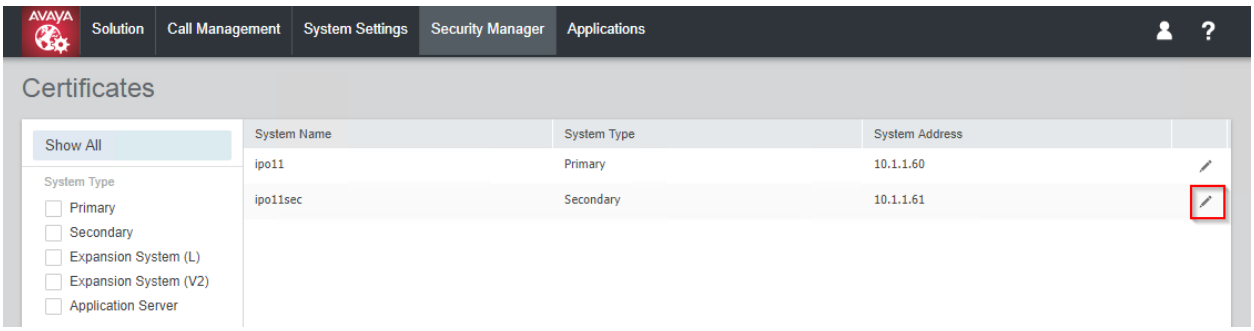



6. Click on the link in the popup window and save the file

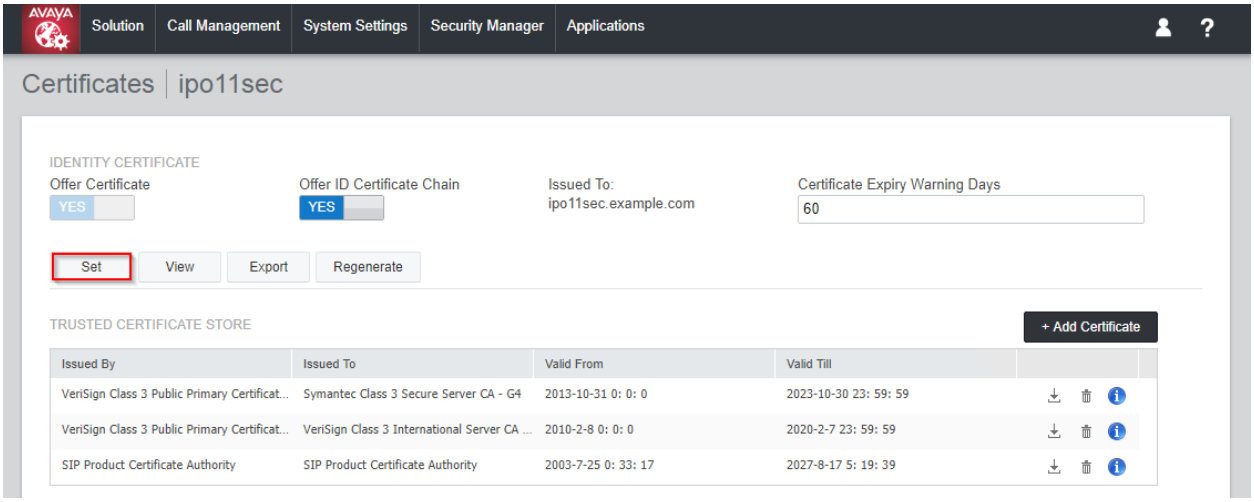



## Installing Identity Certificate on Secondary Server

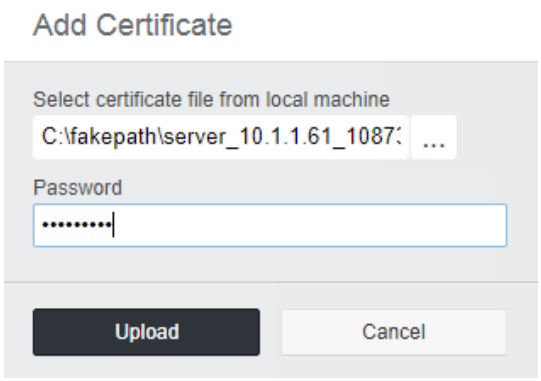
1. Open a browser and connect to **https://<PrimaryServerIP>:7070**
2. Login as **Administrator**
3. Go to **Security Manager / Certificates**
4. Click on the pencil icon to edit certificate




5. Click on **Set**




6. Browse for the certificate file and enter the password, then click **Upload**

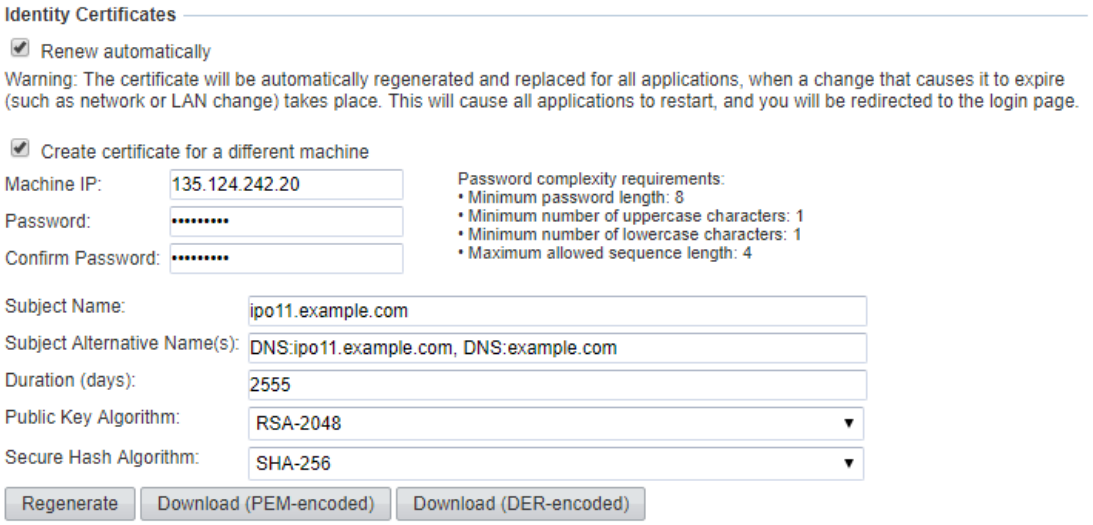



## Certificates for SBCE

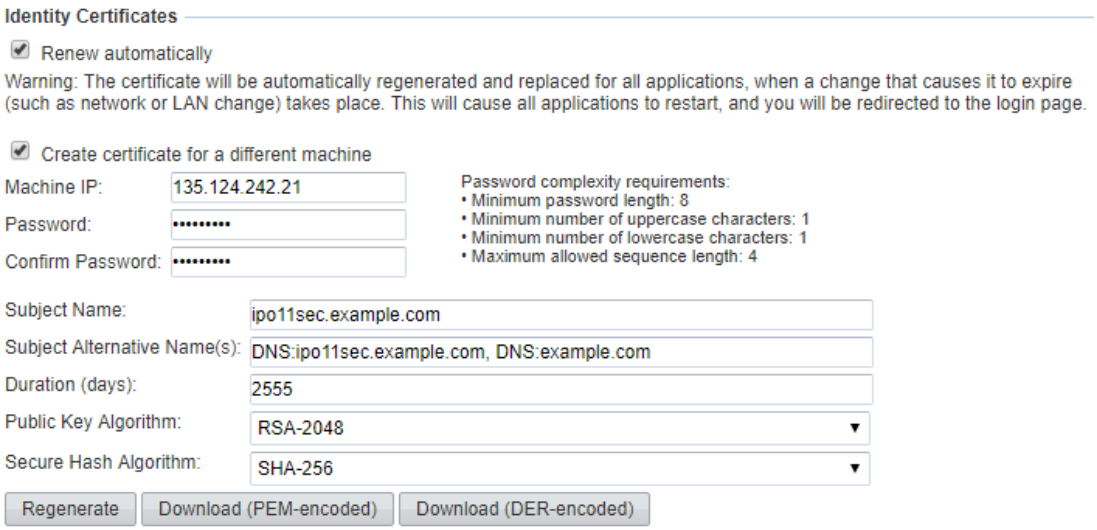
Different IP addresses and FQDNs are used on SBCE for primary and secondary IPO, so we need corresponding ID certificates.

### Generating Identity Certificates for SBCE

1. Open a browser and connect to **https://<PrimaryServerIP>:7071**
2. Login as **Administrator**
3. Go to **Settings** tab and scroll down to **Certificates**
4. Check **Create certificate for a different machine**
5. Enter the following data then click **Regenerate**
    a. **Machine IP**: external IP of SBCE
    b. **Password**: password to encrypt the certificate and key, for example **Avaya123$**
    c. **Subject Name**: enter the FQDN of primary IPO
    d. **Subject Alternative Name(s)**: list the FQDN of primary IPO, the XMPP and SIP domains




6. Click on the link in the popup window and save the file as sbce_ipo11.p12
7. Repeat the procedure for secondary using file name sbce_ipo11sec.p12




## Extracting Private Key and Identity Certificate

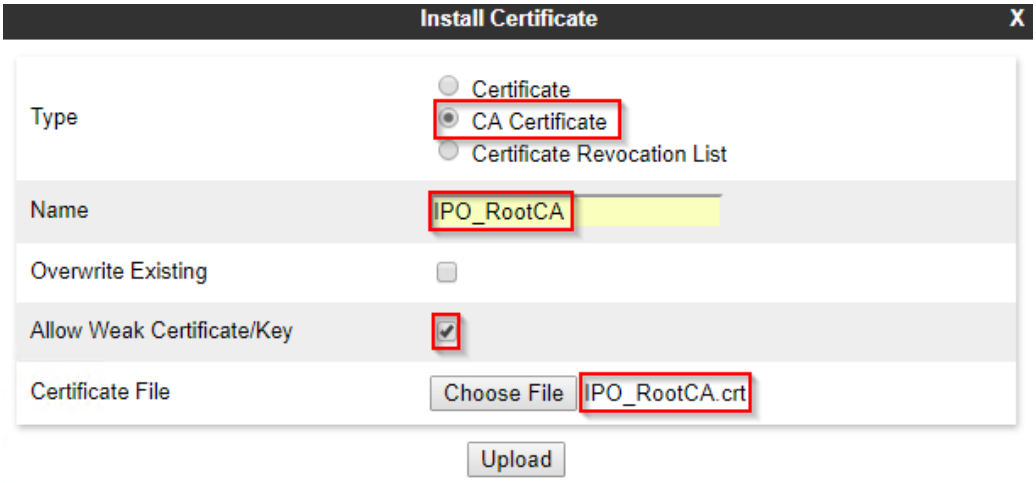
1. Open WinSCP to SBCE **Management IP** using port **222** and **ipcs** login
2. Copy the p12 file (for example sbce_ipo11.p12) from your PC to SBCE /tmp directory
3. Ssh to SBCE **Management IP** using port **222** and **ipcs** login
4. Issue command **su –** and type the **root** password
5. Issue the commands in bold:

```
[root@sbce ipcs]# cd /tmp
[root@sbce tmp]# openssl pkcs12 -in sbce_ipo11.p12 -out sbce_ipo11.pem
Enter Import Password: Avaya123$
MAC verified OK
Enter PEM pass phrase: Avaya123$
Verifying - Enter PEM pass phrase: Avaya123$
[root@sbce tmp]# openssl pkcs12 -nocerts -in sbce_ipo11.p12 -out
sbce_ipo11.key
Enter Import Password: Avaya123$
MAC verified OK
Enter PEM pass phrase: Avaya123$
Verifying - Enter PEM pass phrase: Avaya123$
```

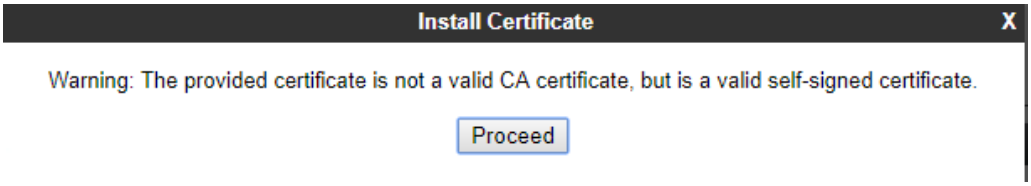
6. Copy the new **pem** and **key** files from SBCE to your PC
7. Repeat the procedure for secondary

## Adding IPO Root CA Certificate on SBCE

1. Login to SBCE web interface
2. Go to **TLS Management / Certificates**
3. Click **Install**
4. Fill the form then click **Upload**
    a. **Type**: **CA Certificate**
    b. **Name**: descriptive name for the root CA certificate, for example **IPO_RootCA**
    c. Check **Allow Weak Certificate/Key** to be able to add the self-signed IPO Root CA
    d. **Certificate File**: click **Choose File** and open **IPO_RootCA.crt**



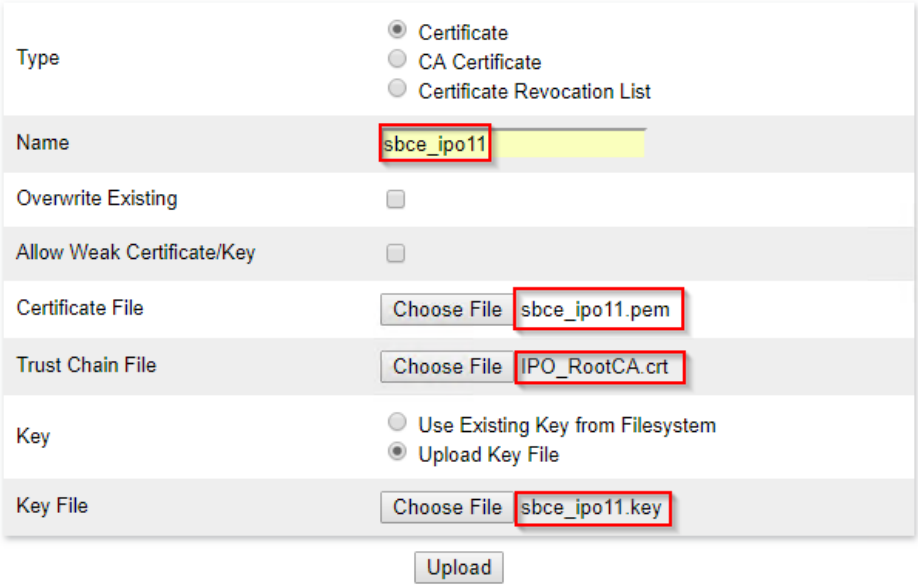

5. The IPO Root CA is a self-signed certificate, click on Proceed



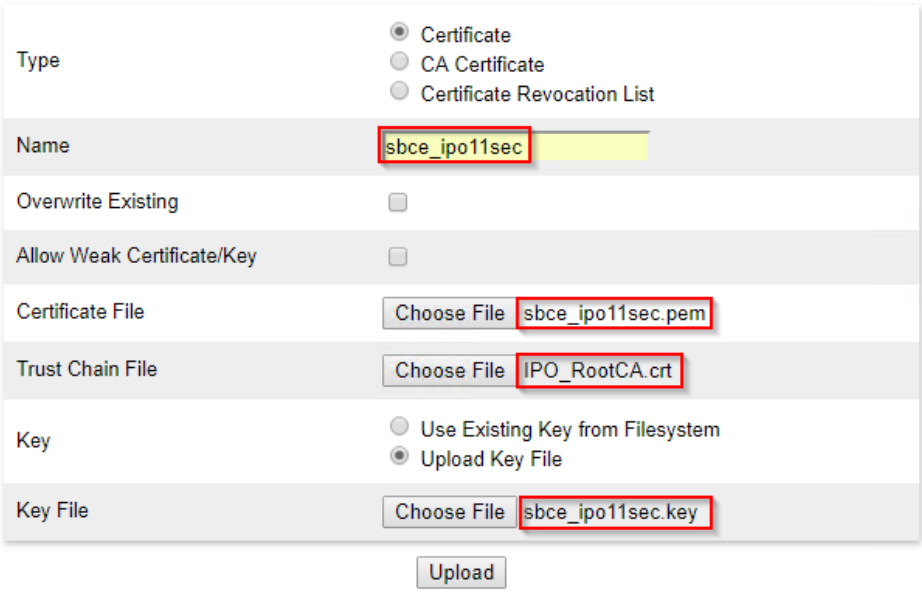

6. Certificate will be displayed, click **Install,** then **Finish**

## Adding SBCE Identity Certificate on SBCE

1. Login to SBCE web interface
2. Go to **TLS Management / Certificates**
3. Click **Install**
4. Fill the form then click **Upload**
    a. **Type**: **Certificate**
    b. **Name**: name for the SBCE identity certificate, for example **sbce_ipo11**
    c. **Certificate File**: click **Choose File** and open **sbce_ipo11.pem**
    d. **Trust Chain File**: click **Choose File** and open **IPO_RootCA.crt**
    e. **Key:** select **Upload Key File**
    f. **Key File**: click **Choose File** and open **sbce_ipo11.key**




5. Certificate will be displayed, click **Install,** then **Finish**
6. Repeat the procedure for secondary



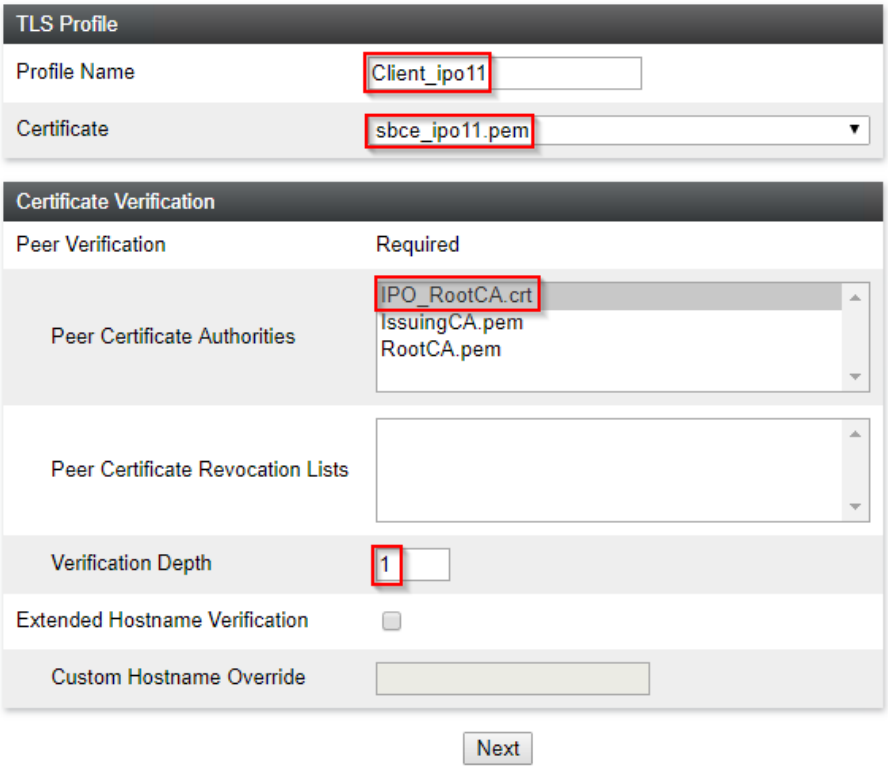

7. Ssh to SBCE **Management IP** using port **222** and **ipcs** login
8. Issue command **su -** and type the root password
9. Issue the commands in bold:

```
[root@sbce ipcs]# cd /usr/local/ipcs/cert/key
[root@sbce key]# enc_key sbce_ipo11.key Avaya123$
writing RSA key
[root@sbce key]# enc_key sbce_ipo11sec.key Avaya123$
writing RSA key
```

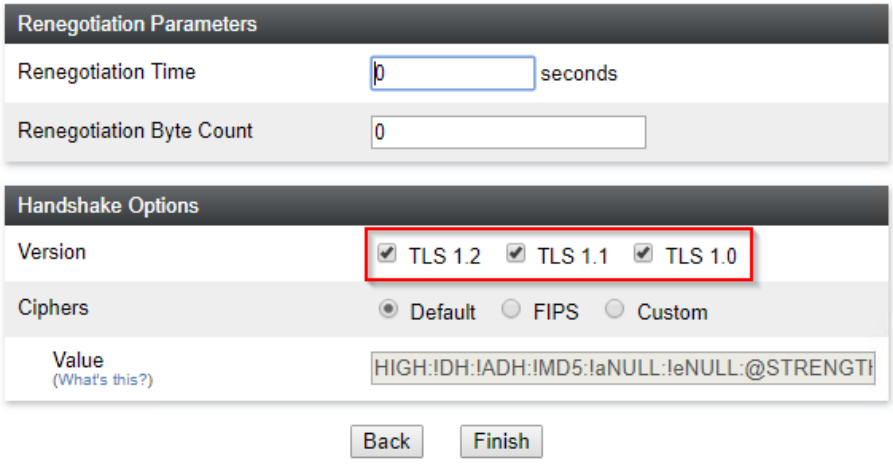
## Configuring SBCE

## TLS Profiles

1. Login to SBCE web interface
2. Go to **TLS Management / Client Profiles** and click **Add**
3. Enter the following data then click **Next**
    a. **Profile Name:** descriptive name
    b. **Certificate:** select **sbce_ipo11.pem**
    c. **Peer Certificate Authorities:** select **IPO_RootCA.crt**
    d. **Verification Depth:** enter **1**

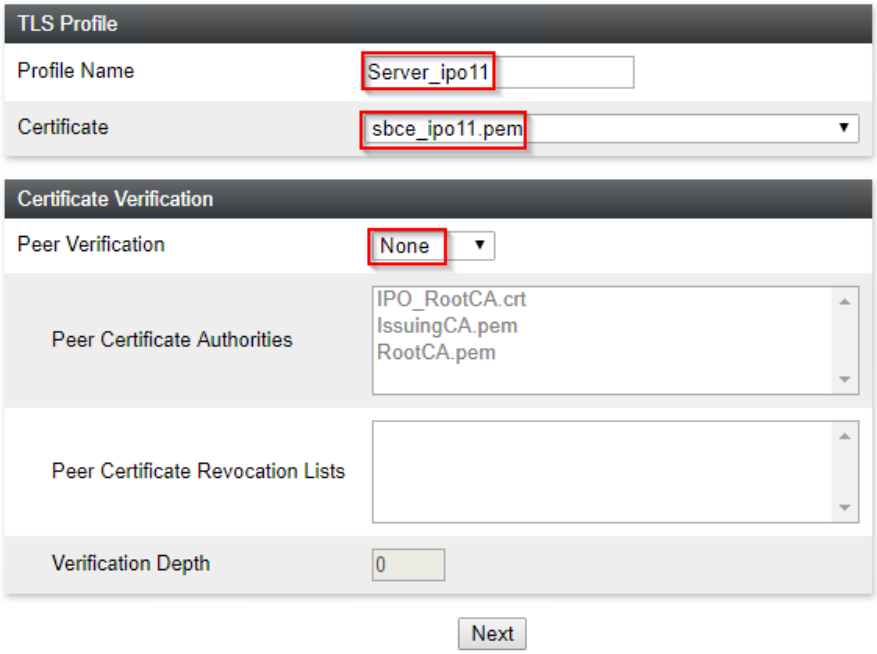



4. Enable all TLS versions, then click **Finish**

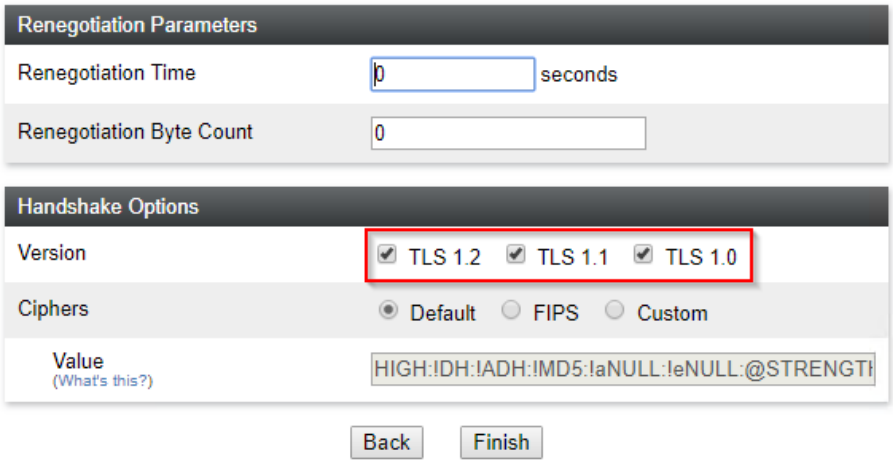



5. Go to **TLS Management / Server Profiles** and click **Next**
6. Enter the following data then click **Finish**

a. **Profile Name:** descriptive name
b. **Certificate:** select **SBCE_ID.crt**
c. **Peer Verification:** select **None**



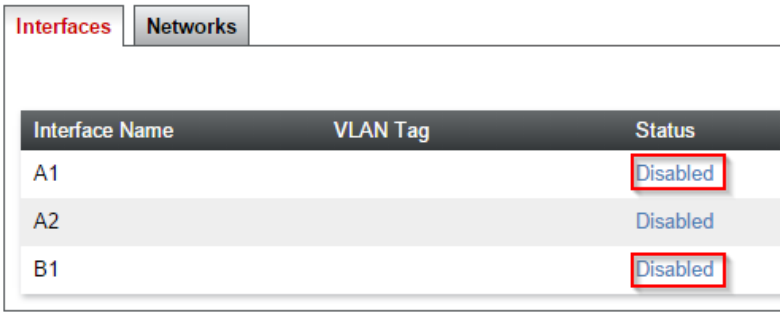

7. Enable all TLS, then click **Finish**



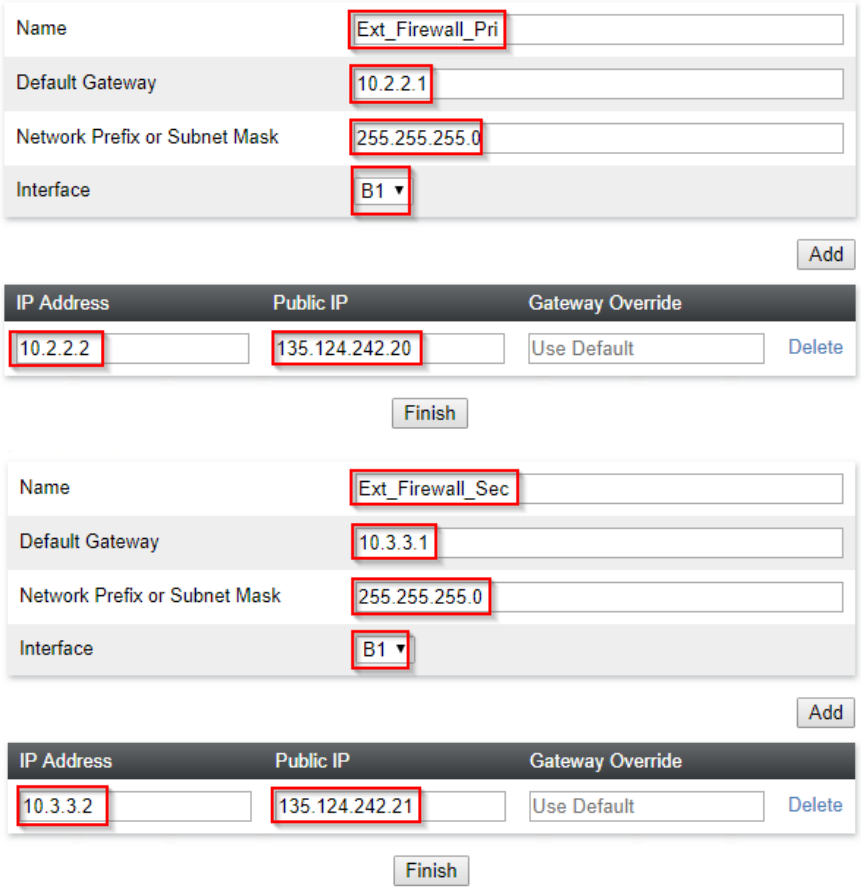

8. Repeat the procedure for secondary

## External Interface

1. Go to **Device Specific Settings / Network Management** and on the **Interfaces** tab click on **Disabled** link for both A1 and B1 interfaces to enable them




2. Go to **Networks** tab and click **Add**
3. Enter the following data then click **Finish**
    a. **Name:** name of external interface
    b. **Default Gateway:** gateway for external interface
    c. **Subnet Mask:** mask for external interface
    d. **Interface:** select **B1**
    e. **IP Address:** address of external interface

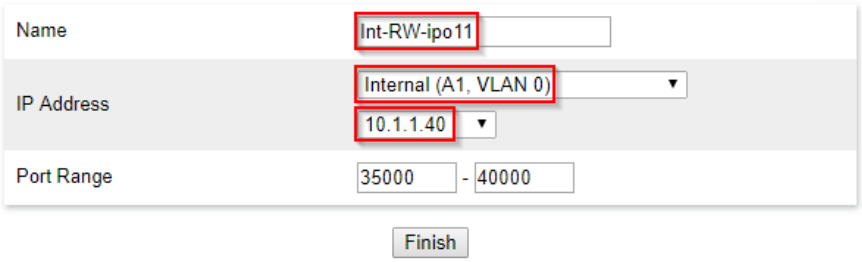



4. Go to **System Management** and click on **Restart Application**

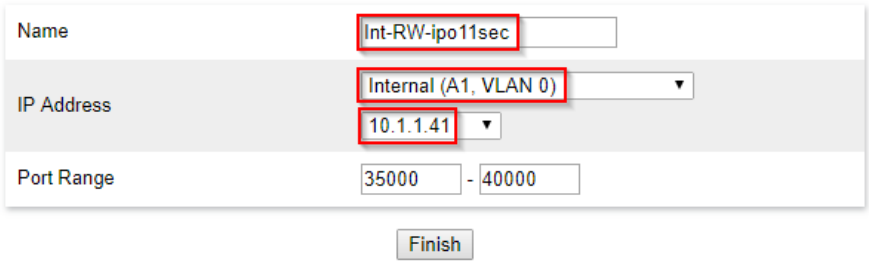
## Media Interfaces

1. Go to **Device Specific Settings / Media Interface** and click **Add**

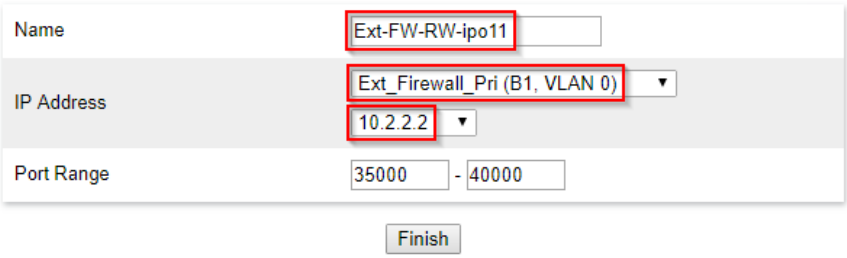
2. Set **Name** for internal interface, choose **A1** from the drop down of **IP Address**, select **TLS Profile**, then click **Finish**



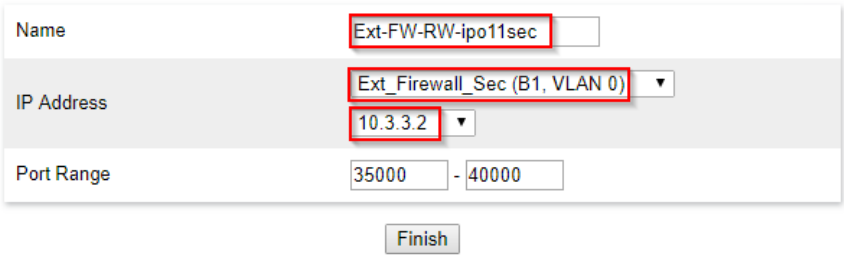

3. Repeat for secondary




4. Add external media interface, choose **B1** this time

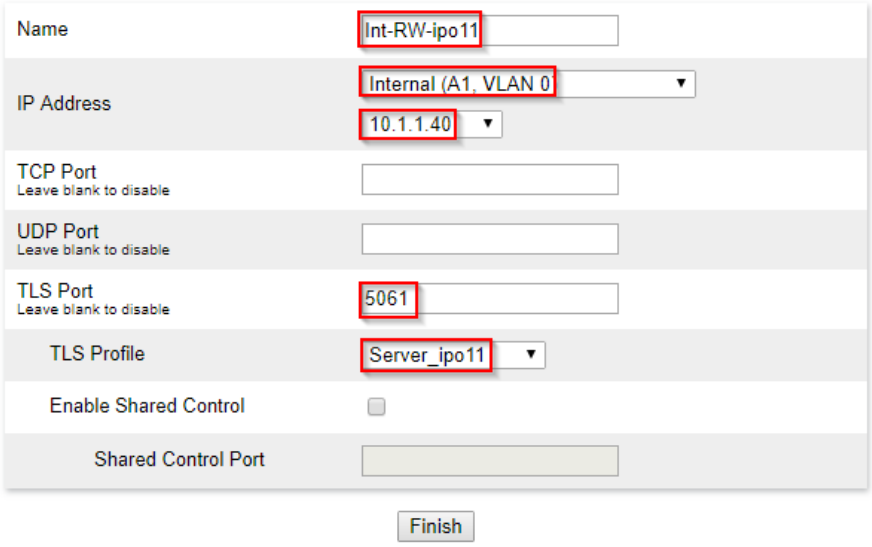



5. Repeat for secondary

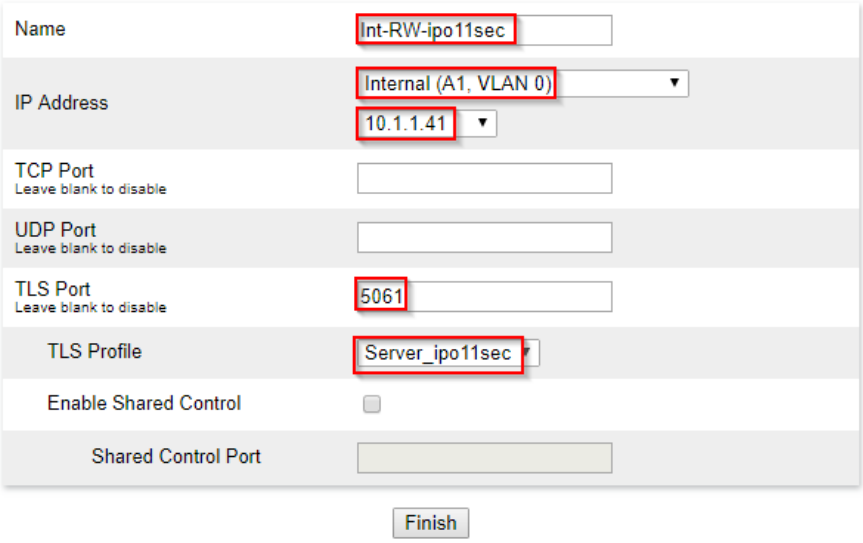



## Signaling Interfaces

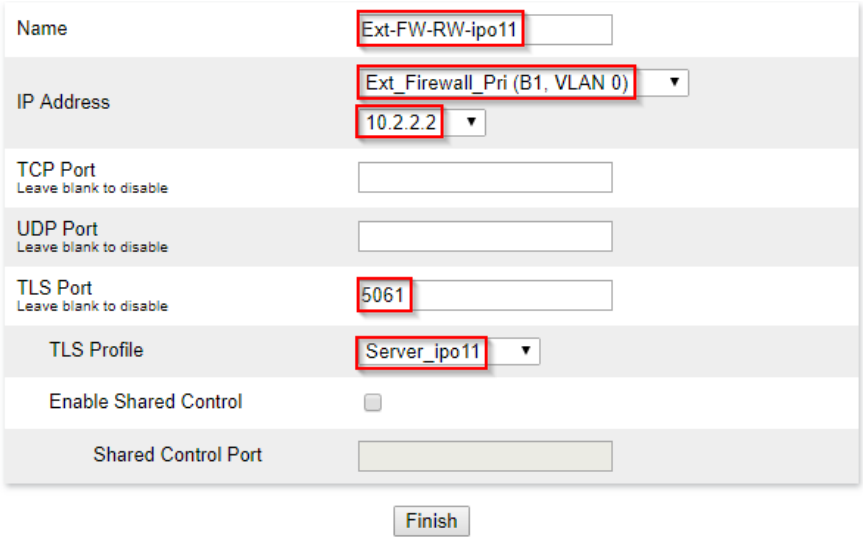
1. Go to **Device Specific Settings / Signaling Interface** and click **Add**
2. Set **Name** for internal interface, choose **A1** from the drop down of **IP Address,** remove TCP and UDP port, set **TLS Port**, select **Server** for **TLS Profile**, then click **Finish**



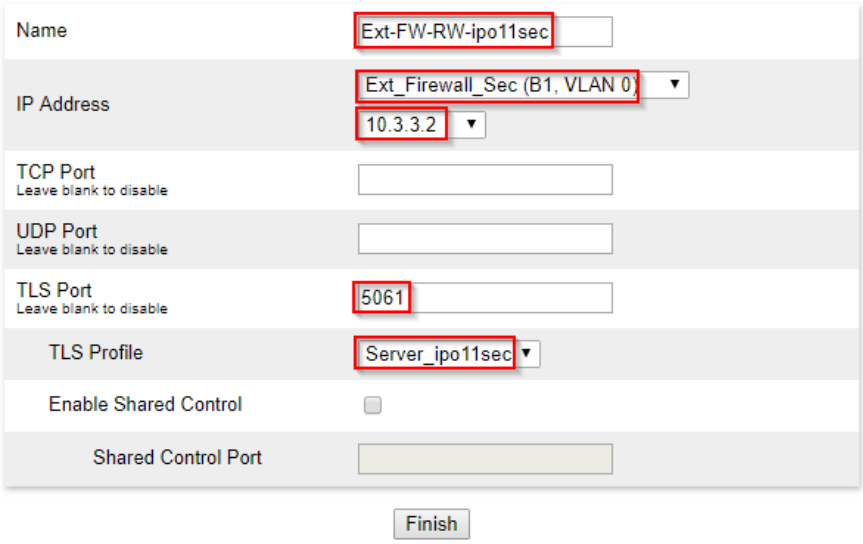

3. Repeat for secondary




4. Add external media interface, choose **B1** this time

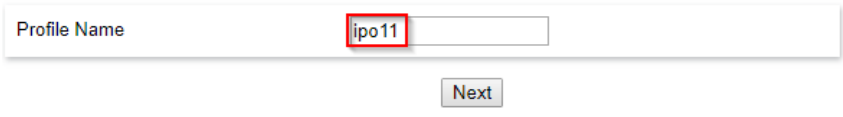



5. Repeat for secondary

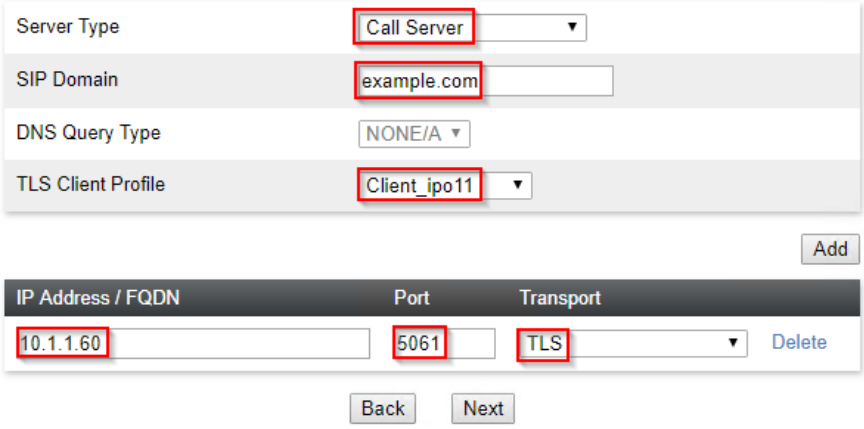



## Server Profile

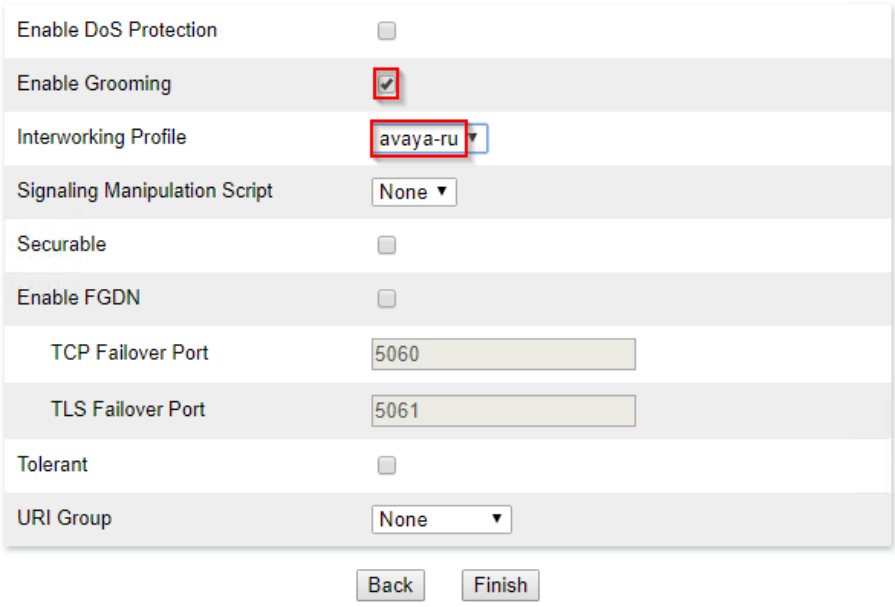
1. Go to **Global Profiles / Server Configuration** and click **Add**
2. Enter **Profile Name** and click **Next**



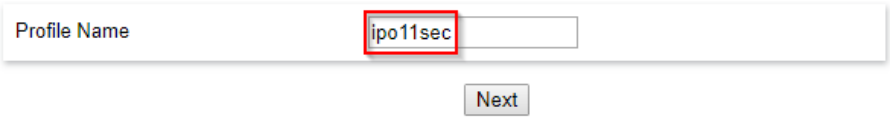

3. Set **Server Type** to **Call Server**, enter **SIP Domain**, select **TLS Client Profile**, enter **IP/Port/Transport** of IP Office and click **Next**

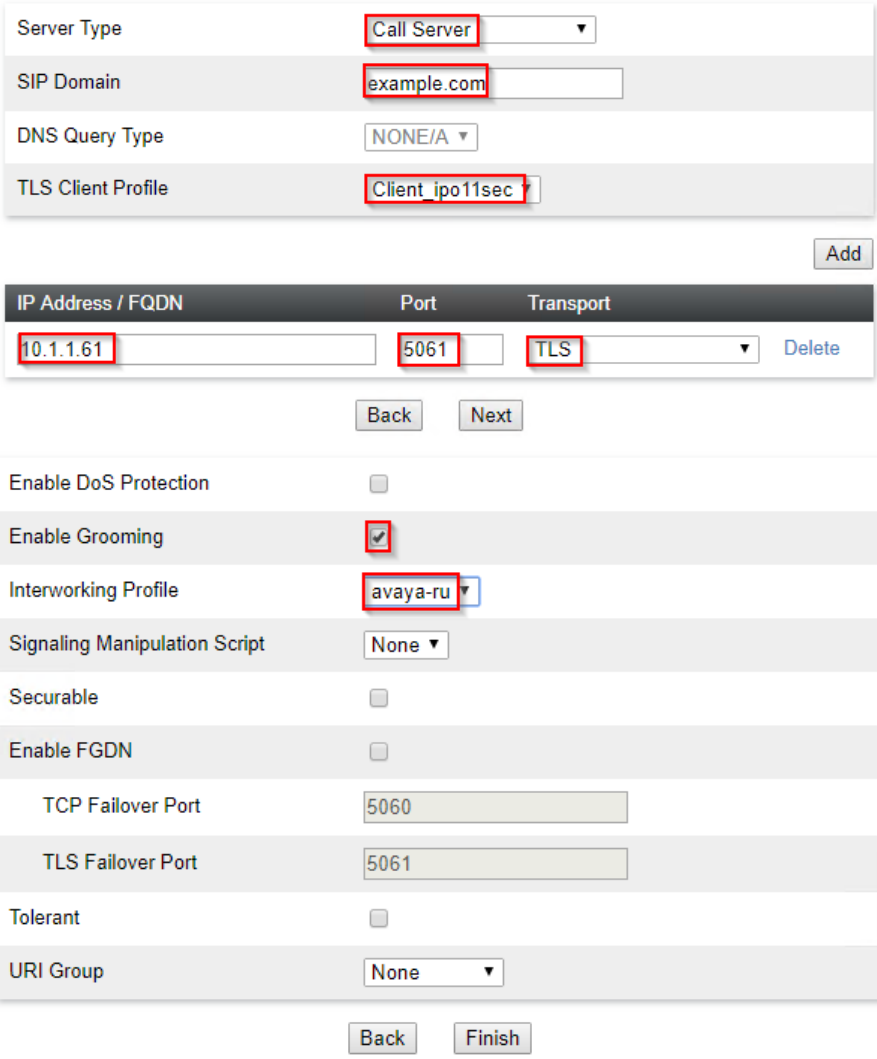



4. Authentication is not needed toward IP Office so just click **Next**
5. Heartbeat is not needed, just click **Next**
6. Registration is not needed, just click **Next**
7. Ping is not needed, just click **Next**
8. Check **Enable Grooming** otherwise TLS between SBCE and IP Office will not work correctly, set **Interworking Profile** to **avaya-ru**, then click **Finish**



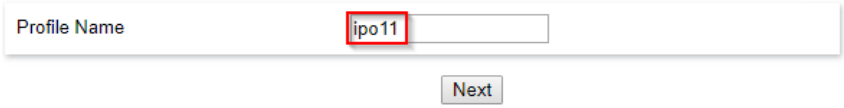

9. Repeat the procedure for secondary



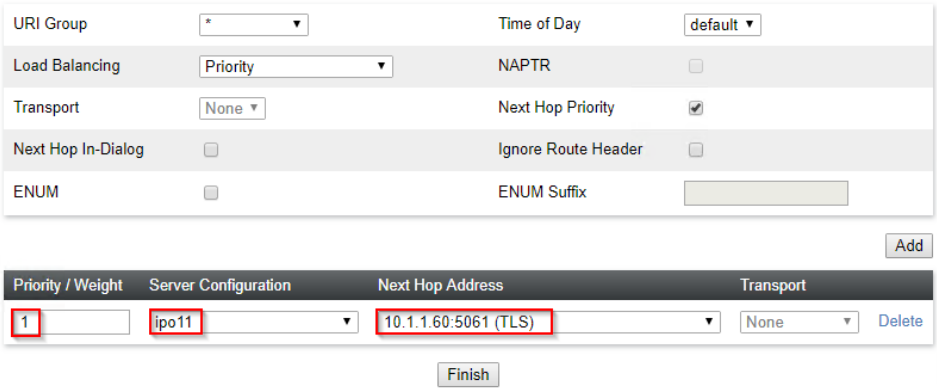



## Routing

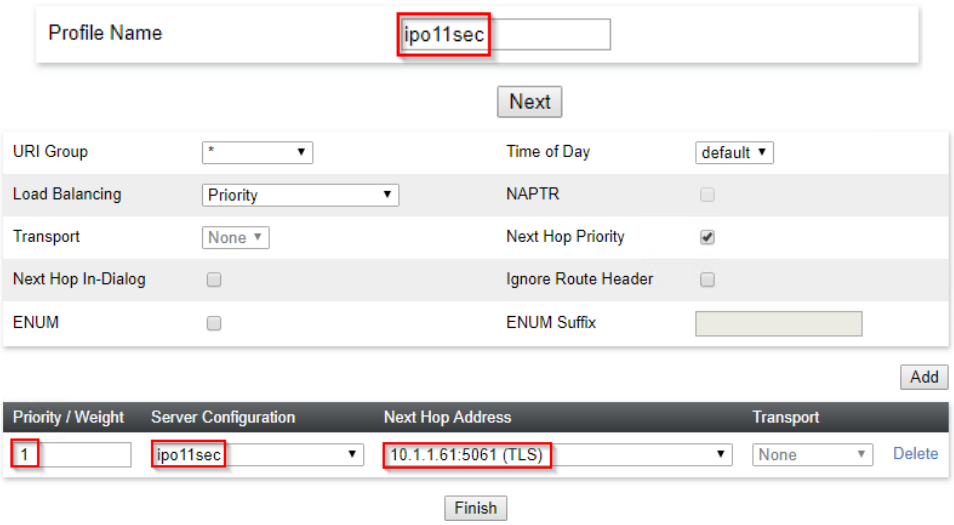
1. Go to **Global Profiles / Routing** and click **Add**
2. Enter **Profile Name** and click **Next**




3. Click **Add**, enter **Priority**, set **Server Configuration** to **IPO** and click **Finish**

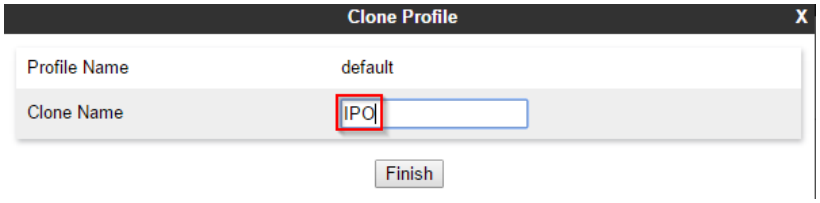



4. Repeat the procedure for secondary

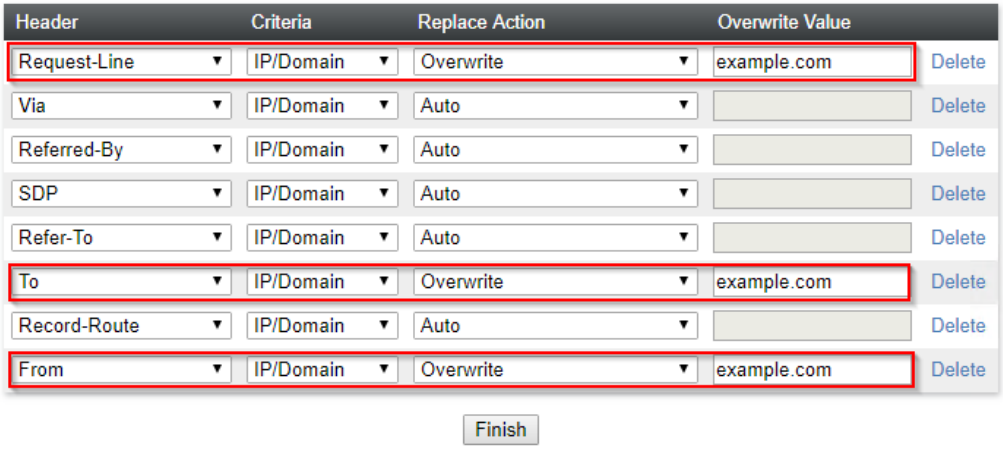



## Topology Hiding

1. Go to **Global Profiles / Topology Hiding**, click on **default** profile then click on **Clone**
2. Enter name and click **Finish**



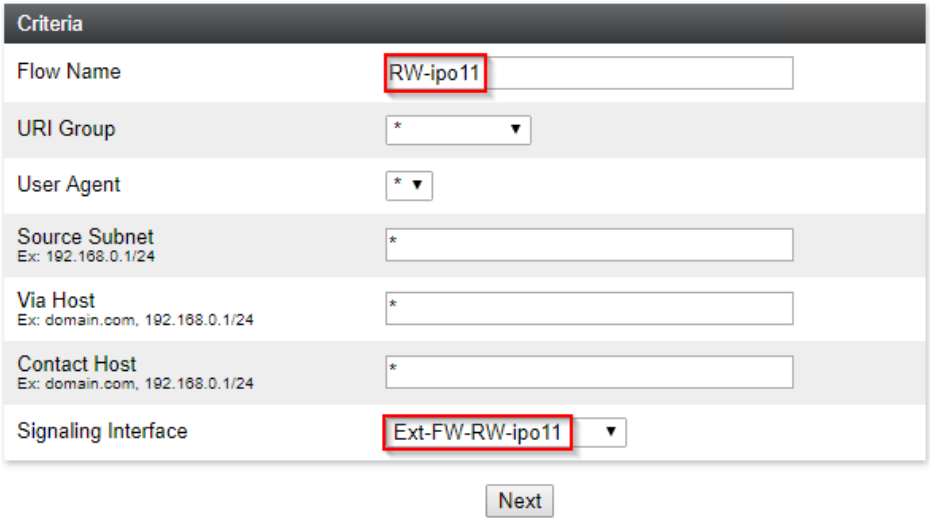

3. Click on the newly created **IPO** profile, then click on **Edit**
4. Set **Replace Action** to **Overwrite** and enter **example.com** as **Overwrite Value** for **Request-Line**, **From**, **To**, then click **Finish**



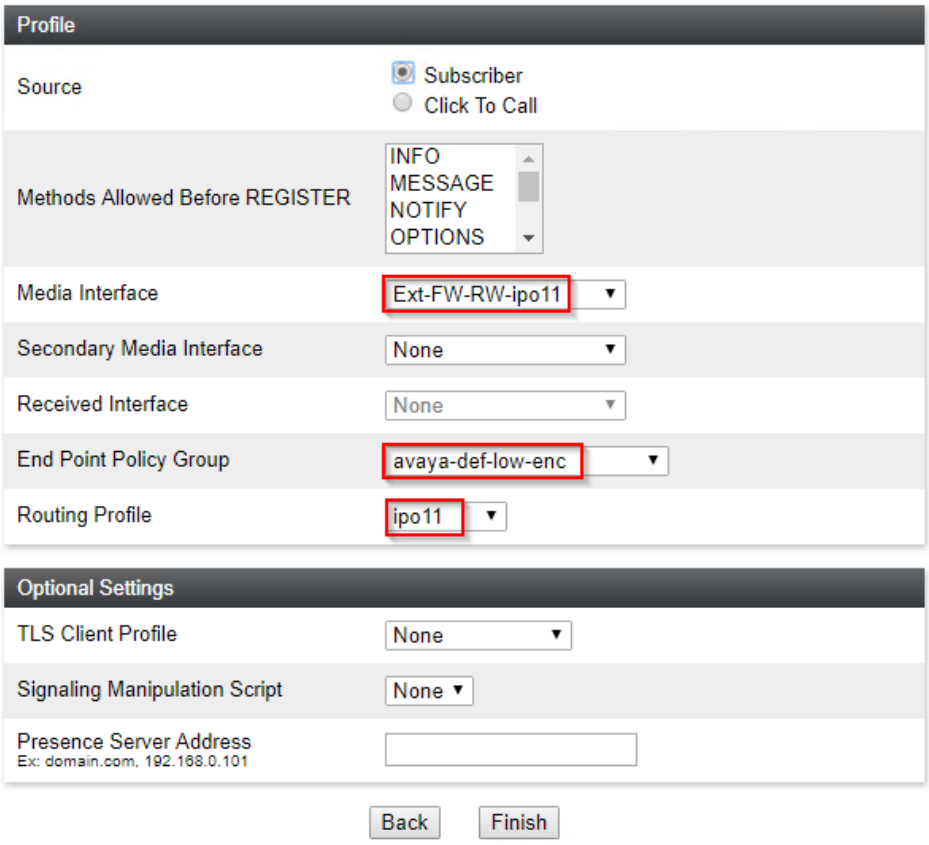

NOTE: Using the default topology hiding during the registration of Communicator for Windows, the SBCE would put the IP of IPO in the Request URI of the REGISTER message which would cause that the IPO includes the internal IP address instead of Host Domain Name in the onex_server field of the 200 OK xml body. This means that client would not be able to register to One-X Portal and would not have Presence/IM.

## Subscriber Flow

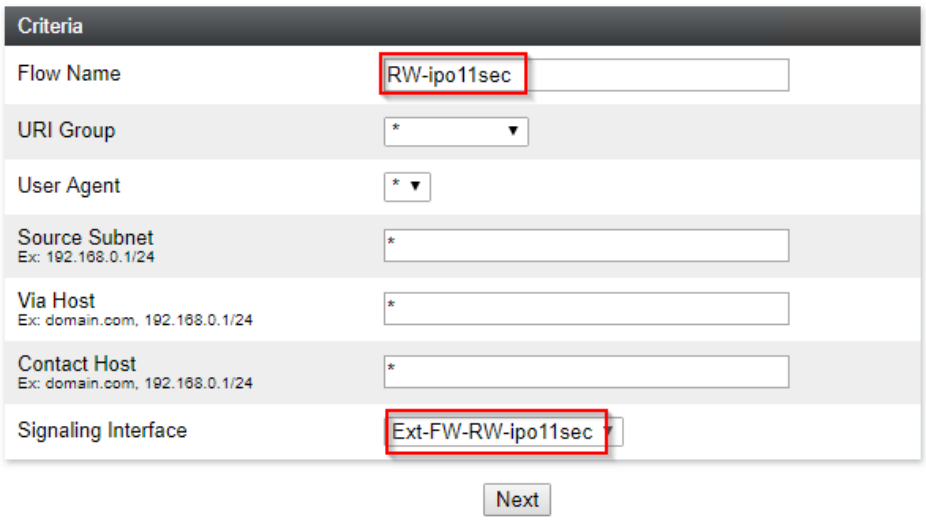
1. Go to **Device Specific Settings / End Point Flows**, select **Subscriber Flows** tab and click **Add**
2. Enter **Flow Name**, select the external interface for the **Signaling Interface** and click **Next**

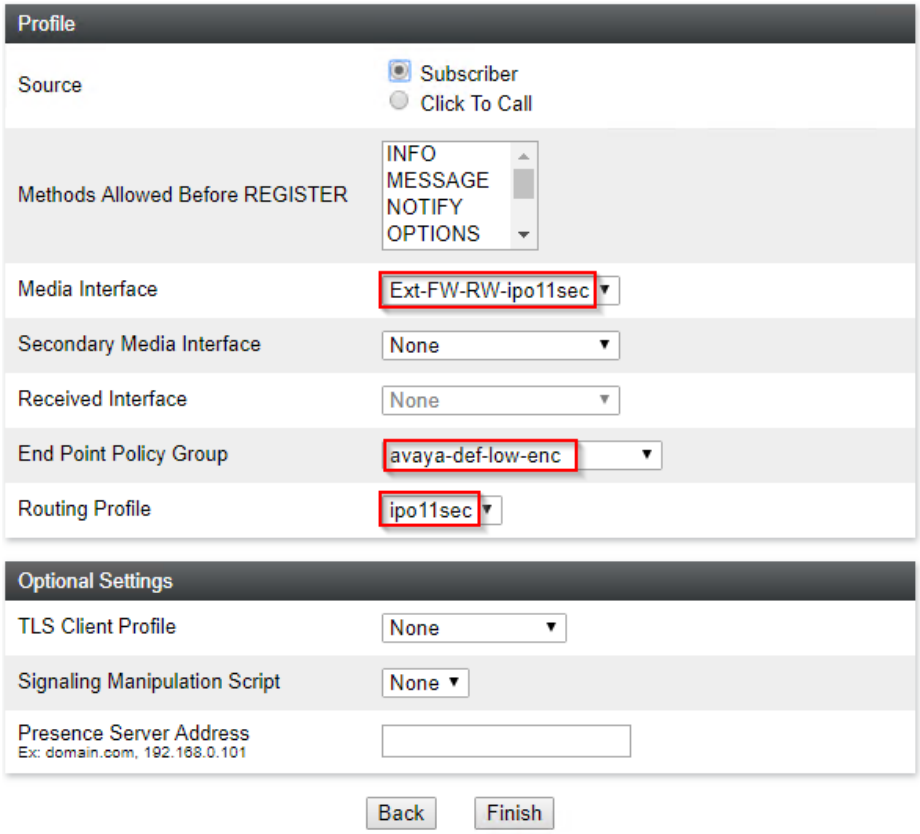



3. Enter the following data and click **Finish**
    a. **Media Interface**: select the external interface
    b. **End Point Policy Group**: select **avaya-def-low-enc**
    c. **Routing Profile**: select the **IPO** server profile
    d. **Topology Hiding Profile**: select **default**



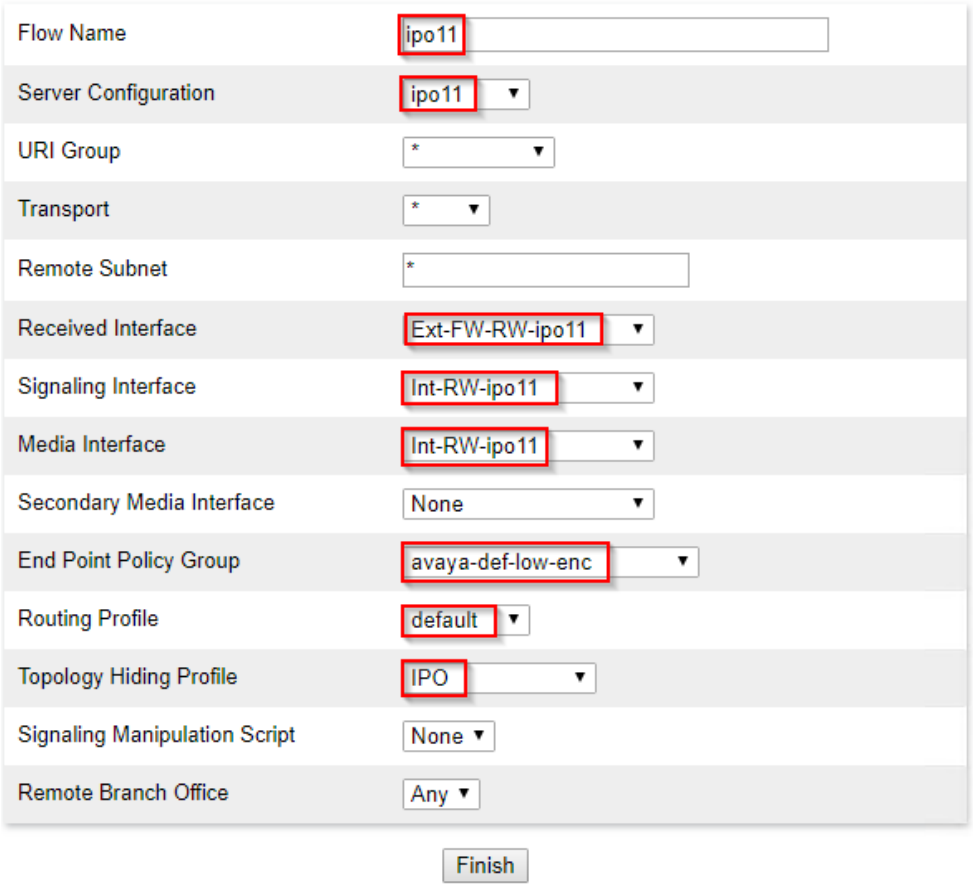

5. Repeat the procedure for secondary



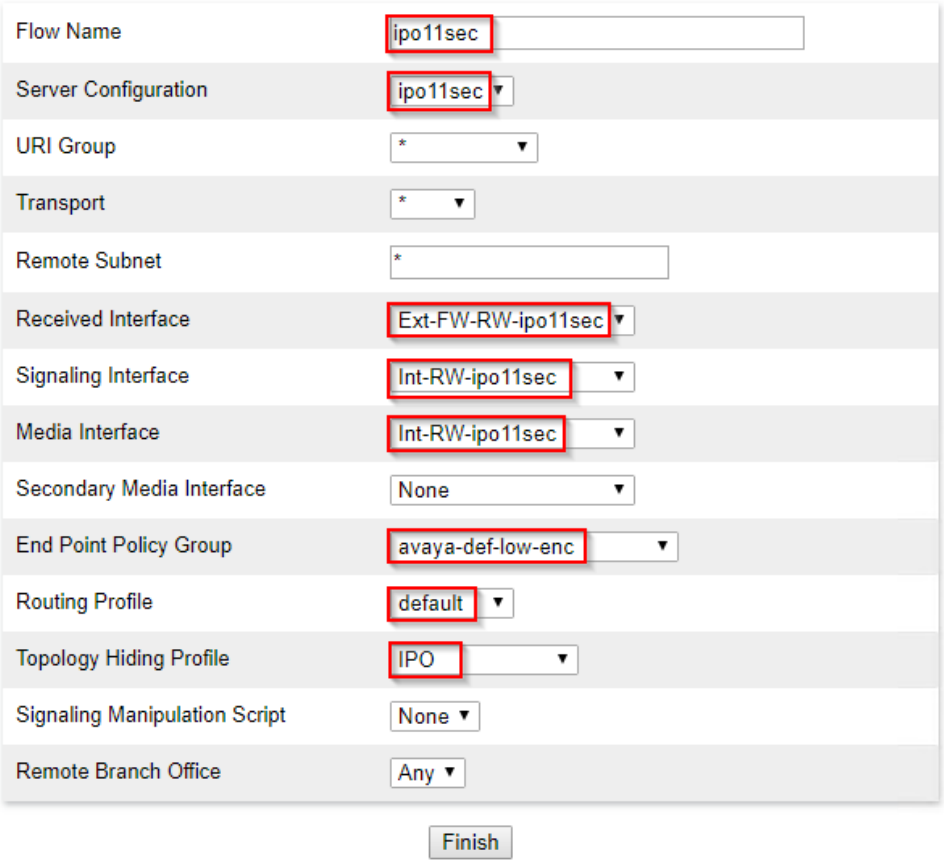



## Server Flow

1. Go to **Device Specific Settings / End Point Flows**, select **Server Flows** tab and click **Add**
2. Enter **Flow Name**, select the external interface for the **Signaling Interface** and click **Next**
3. Enter the following data and click **Finish**
    a. **Flow Name**: enter name
    b. **Server Configuration**: select **IPO**
    c. **Received Interface**: select the external interface
    d. **Signaling Interface**: select the internal interface
    e. **Media Interface**: select the internal interface
    f. **End Point Policy Group**: select **avaya-def-low-enc**
    g. **Routing Profile**: select **default**
    h. **Topology Hiding Profile**: select **IPO**



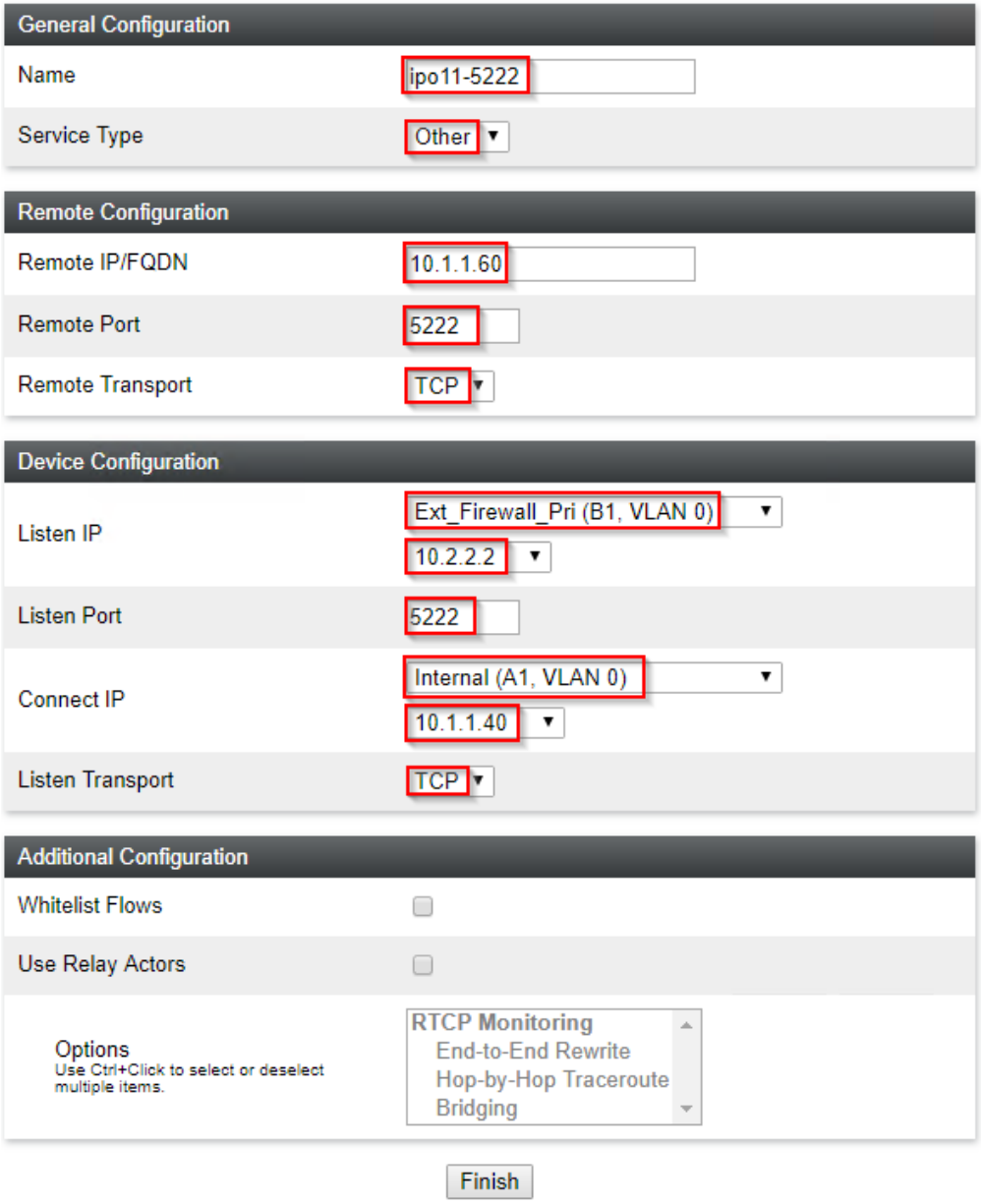

6. Repeat for secondary




## Application Relays

NOTE: Different clients require different Application Relays. These relays function as port forwards. See more detail about necessary ports under the Client Differences topic.

1. Go to **Device Specific Settings / DMZ Services / Relay Services**, select **Application Relay** tab and click **Add**
2. Enter the following data and click **Finish**
    a. **Name**: enter a name
    b. **Service Type**: select **Other**
    c. **Remote IP/FQDN**: enter the IP of the server
    d. **Remote Port**: enter **5222**
    e. **Remote Transport**: select **TCP**
    f. **Listen IP**: select the external interface
    g. **Listen Port**: enter **5222**
    h. **Connect IP**: select the internal interface
    i. **Listen Transport**: select **TCP**

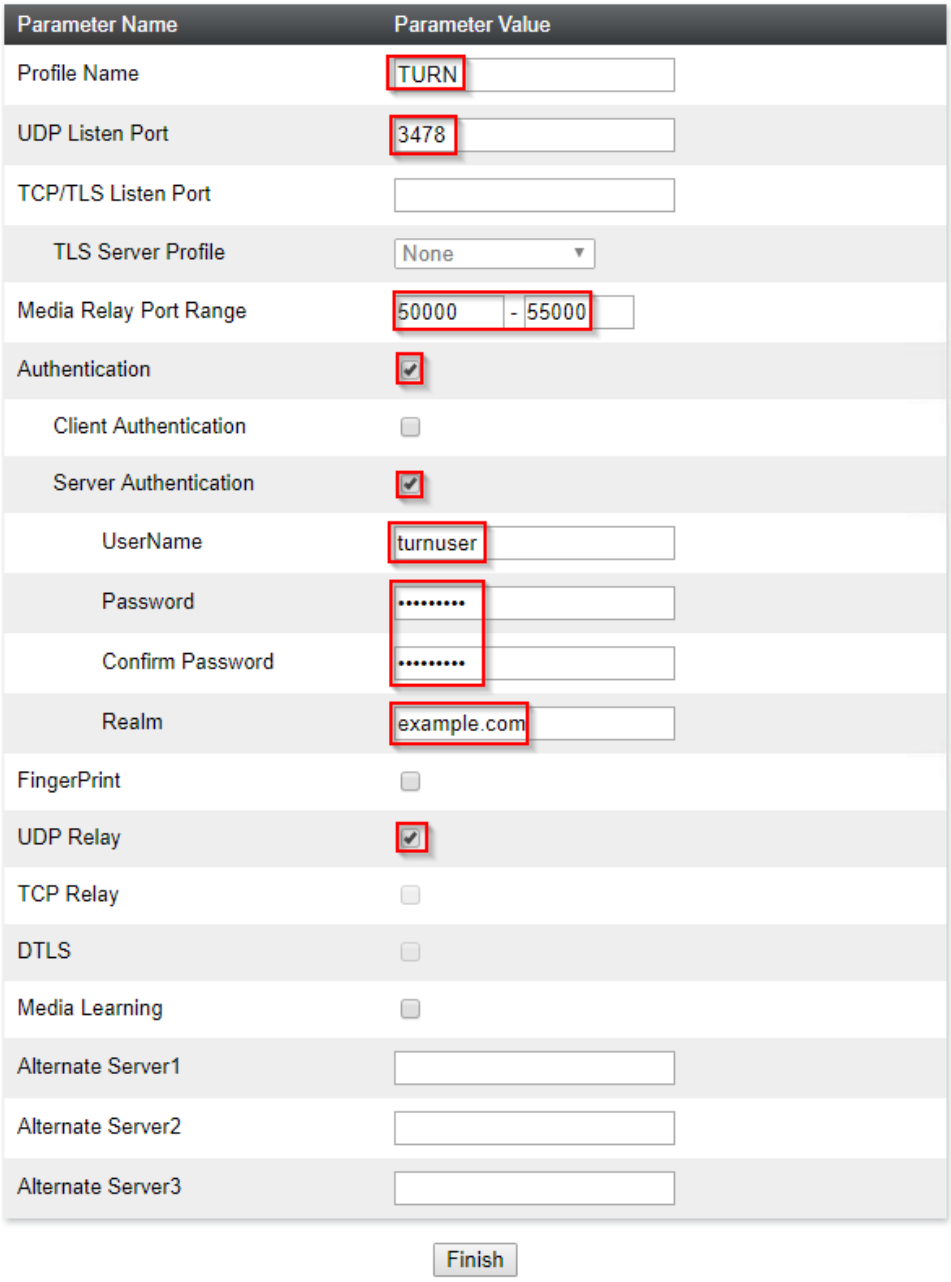



3. Repeat the above procedure for port 9443, 7443, 443 for both servers plus 80 and 411 for primary. At the end following list should be present:

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ipo11-9443 | Other | 10.1.1.60:9443 | TCP | 10.2.2.2:9443<br>Ext_Firewall_Pri (B1, VLAN 0) | TCP | 10.1.1.40<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11-5222 | Other | 10.1.1.60:5222 | TCP | 10.2.2.2:5222<br>Ext_Firewall_Pri (B1, VLAN 0) | TCP | 10.1.1.40<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11sec-9443 | Other | 10.1.1.61:9443 | TCP | 10.3.3.2:9443<br>Ext_Firewall_Sec (B1, VLAN 0) | TCP | 10.1.1.41<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11sec-7443 | Other | 10.1.1.61:7443 | TCP | 10.3.3.2:7443<br>Ext_Firewall_Sec (B1, VLAN 0) | TCP | 10.1.1.41<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11sec-5222 | Other | 10.1.1.61:5222 | TCP | 10.3.3.2:5222<br>Ext_Firewall_Sec (B1, VLAN 0) | TCP | 10.1.1.41<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11-443 | Other | 10.1.1.60:443 | TCP | 10.2.2.2:443<br>Ext_Firewall_Pri (B1, VLAN 0) | TCP | 10.1.1.40<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11sec-443 | Other | 10.1.1.61:443 | TCP | 10.3.3.2:443<br>Ext_Firewall_Sec (B1, VLAN 0) | TCP | 10.1.1.41<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11-80 | Other | 10.1.1.60:80 | TCP | 10.2.2.2:80<br>Ext_Firewall_Pri (B1, VLAN 0) | TCP | 10.1.1.40<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11-7443 | Other | 10.1.1.60:7443 | TCP | 10.2.2.2:7443<br>Ext_Firewall_Pri (B1, VLAN 0) | TCP | 10.1.1.40<br>Internal (A1, VLAN 0) | View | Edit | Delete |
| ipo11-411 | Other | 10.1.1.60:411 | TCP | 10.2.2.2:411<br>Ext_Firewall_Pri (B1, VLAN 0) | TCP | 10.1.1.40<br>Internal (A1, VLAN 0) | View | Edit | Delete |

## TURN/STUN service

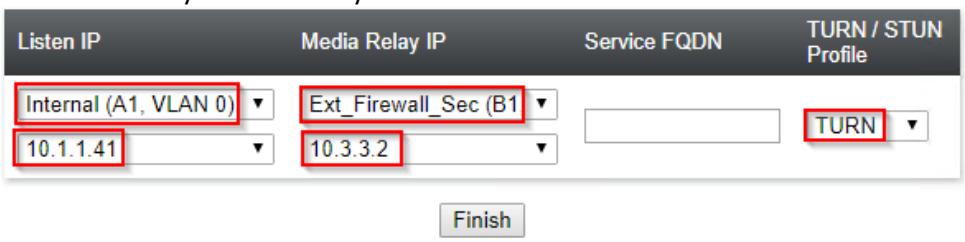
1. Go to **Device Specific Settings / TURN/STUN service** and on the **TURN/STUN Profiles** tab click **Add**. Enter the following data then click **Finish**
    a. **Profile Name**: set a name
    b. **UDP Listen Port:** 3478
    c. **Media Relay Port Range:** 50000-55000
    d. Enable **Authentication**
    e. Enable **Server Authentication**
    f. **Username:** enter a username that will be used by WebRTC Gateway
    g. **Password:** enter password
    h. **Realm:** enter domain
    i. Enable **UDP Relay**




2. Go to **Device Specific Settings / TURN/STUN service** and on the **TURN Relay** tab click **Add**. Enter the following data then click **Finish**

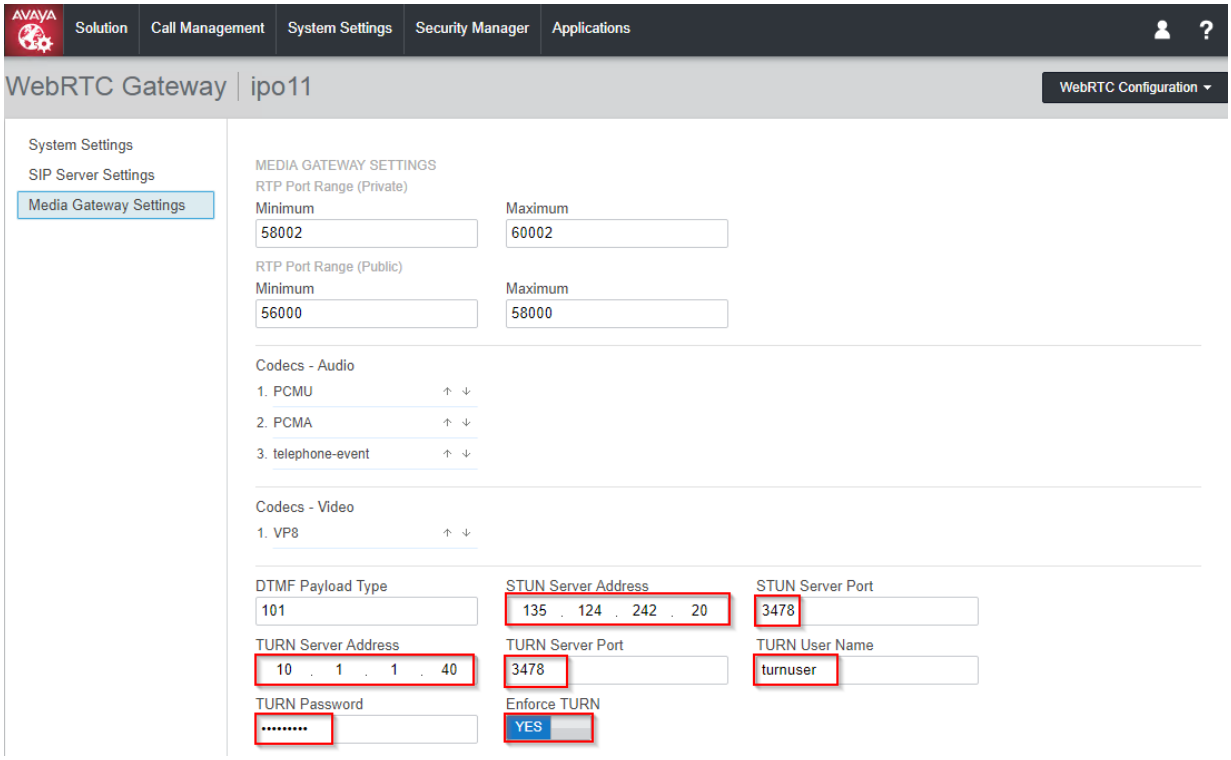
   Select the internal interface as Listen IP, the external interface as Media Relay IP, and the TURN/STUN Profile, then click **Finish**.

3. Add TURN Relay for secondary

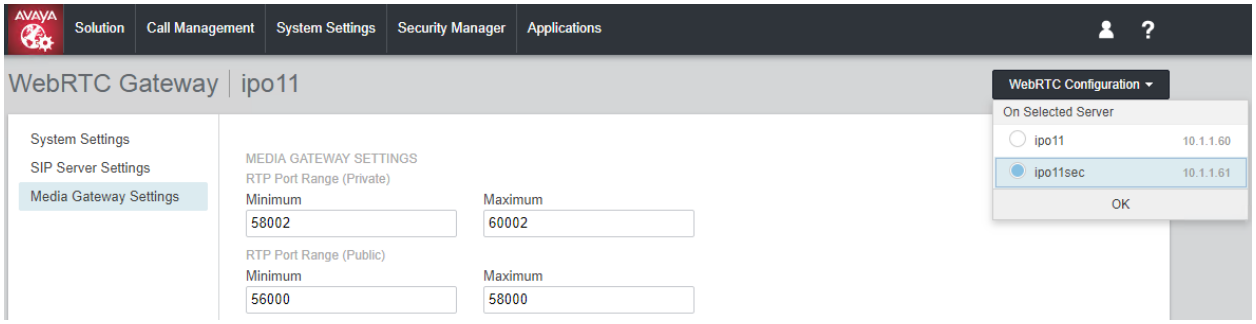



## Configuring WebRTC Gateway

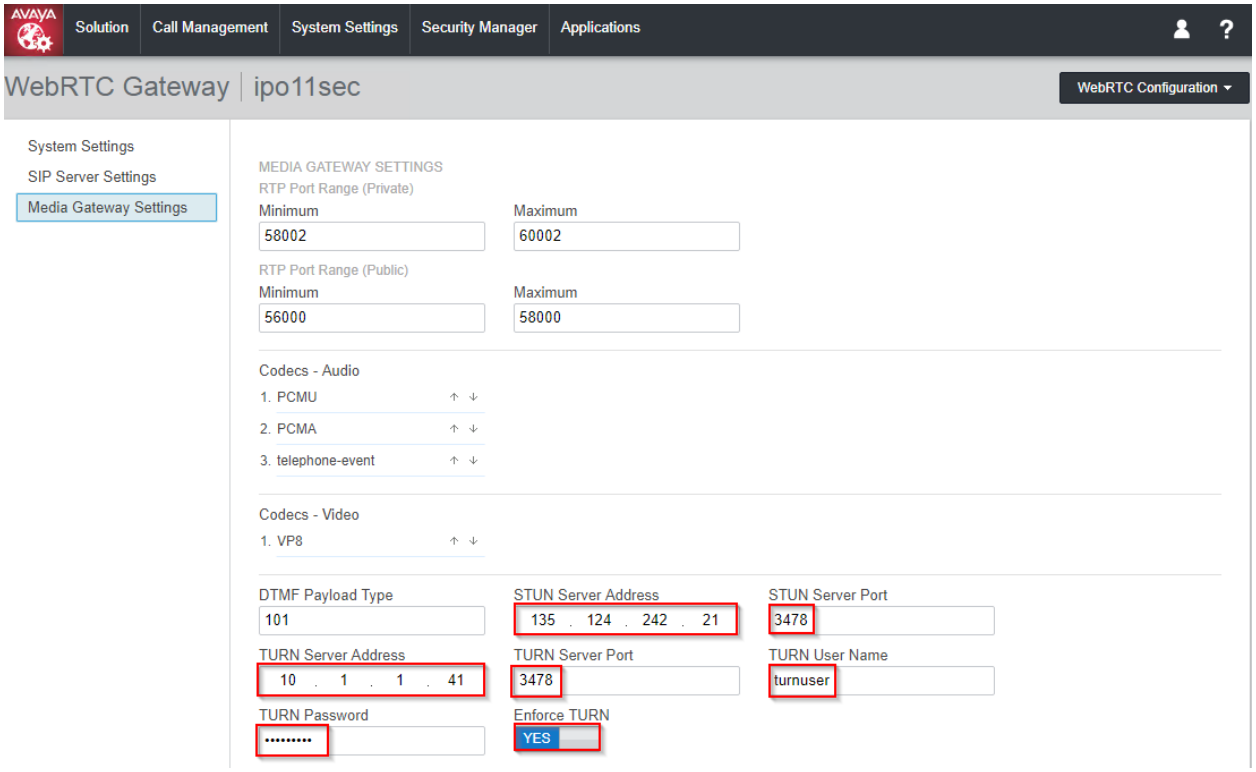
1. Open a browser and connect to **https://<PrimaryServerIP>:7070**, use the **Administrator** login and password
2. On the **Applications** menu click on **WebRTC Configuration**
3. Go to the **Media Gateway Settings** and enter the followings then click **Save**:
    a. **STUN Server Address**: public IP of corporate firewall (or the SBCE external interface if there is no corporate firewall)
    b. **STUN Server Port**: 3478
    c. **TURN Server Address**: internal interface of SBCE
    d. **TURN Server Port**: 3478
    e. **TURN User Name**: user name defined on SBCE TURN configuration
    f. **TURN Password**: password defined on SBCE TURN configuration
    g. **Enforce TURN**: set to **Yes** otherwise RTP will not necessarily go through the TURN server because in ICE candidate list the relay candidate is the last choice, if there are other working candidates, those will be preferred to relay.




4. From **the WebRTC Configuration** dropdown select secondary




5. Go to **Media Gateway Settings** and enter the details for secondary




# SIP Clients

## Communicator for Windows

The Avaya Communicator for Windows starts with a DNS A query on the configured Server Address (FQDN of IP Office), then initiates SIP registration to the IP address returned by the DNS server. The IP Office will send the FQDN of One-X Portal in the onex_server field of 200 OK SIP response. The client does a DNS A query on this onex_server value, and then initiates XMPP connection to the IP address learnt from DNS server. On the client we need to configure the **FQDN, SIP port, transport and SIP domain of the IP Office**. For failover the client uses the FQDN returned by IPO during the SIP registration. The FQDN is in the backup_ipoffice_server field of the 200 OK.

Configuration:

1. In **Settings / Server** set the followings:
    a. **Server Address:** FQDN of IP Office (SIP Registrar FQDN on IP Office)

b. **Server Port: 5061**
c. **Transport Type:**
d. **Domain:** SIP domain (SIP Domain Name on IP Office)

## Communicator for iPad

The Avaya Communicator for iPad starts with a DNS A query on the configured Server Address (FQDN of IP Office), then initiates SIP registration to the IP address returned by the DNS server. The IP Office will send the FQDN of One-X Portal in the onex_server field of 200 OK SIP response. The client does a DNS A query on this onex_server value, and then initiates XMPP connection to the IP address learnt from DNS server. On the client we need to configure the **FQDN, SIP port, transport and SIP domain of the IP Office**.

NOTE: This particular client requires that all the addresses it connects to (FQDN of IP Office and One-X Portal) are listed in the Subject Alternative Name field of the server certificate. Keep this in mind when generating Identity Certificate for IP Office or SBCE.

Configuration:

1. In **Settings / Accounts and Services / Phone Service** set the followings:
   a. **Phone Server Address:** FQDN of IPO
   b. **Phone Server Port:** 5061
   c. **Phone Service Domain:** SIP domain
   d. **TLS:** enable
   e. **Extension: Extension** from User tab of IPO User form
   f. **Password: Password** from User tab of IPO User form
2. In **Settings / Accounts and Services / Presence Service** enable **Presence Service** and leave empty the **Presence Server Address**

## Onex-X Mobile Preferred for Android

The Avaya One-X Mobile Preferred for Android first contacts the One-X Portal through the REST API (port 9443) and downloads im_info and sip_info to learn **primaryOnexAddress, secondaryOnexAddress** and **sipRegistrarFqdn.** The client does a DNS A query on these FQDNs and then registers to One-X Portal and IPO. On the client we need to configure the **FQDN of One-X Portal.** User Name is the **Name** from User tab of IPO User form, Password is **Password** from User tab of IPO User form. For failover the client queries sip_info from **secondaryOnexAddress** learnt from initial im_info, then registers to the **sipRegistrarFqdn**.

Configuration:

1. In **Settings / Server ID and user account** set the **FQDN of One-X Portal**, the **user name** and **password**
2. In **Settings / Voice Over IP / VoIP operation mode** set **Always**
3. In **Settings / Advanced / Advanced VoIP** check **Secure Connection.** This option is needed for encrypted signaling and media.

## One-X Mobile Preferred for IOS

The Avaya One-X Mobile Preferred for IOS first contacts the One-X Portal through the REST API (port 9443) to learn the **XMPP Domain** and the **SipRegistrarFqdn**, then does DNS A query on XMPP Domain to learn the IP of One-X Portal and a DNS A query on SipRegistrarFqdn to learn the IP of IP Office, finally registers to One-X Portal and IPO. On the client we need to configure the **FQDN of One-X Portal.** User

Name is the **Name** from User tab of IPO User form, Password is **Password** from User tab of IPO User form.

NOTE: Since this particular client does a DNS A query on the **XMPP domain**, it is highly recommended to set the **XMPP domain** to the same as **Host Domain Name** to make sure it is resolvable to the address of One-X Portal. If Resiliency is implemented, the REST API will include the **primaryOnexAddress** and **secondaryOnexAddress** fields in im-info which contains the Host Domain Names of Primary and Secondary servers. In that case the client uses these addresses instead of the XMPP Domain.

Failover works same way as on Android client.

Configuration:

1. In **Settings / UC Server Settings** set the **FQDN of One-X Portal**, the **User Name** and **Password**
2. In **Settings / Application Configuration / VoIP Mode** set **Always**
3. Uncheck **Settings / Security Settings / Validate Server Certificates**
4. In **Settings / Advanced Settings / Advanced VoIP** check **Secure Connection.** This option is needed for encrypted signaling and media.

## Equinox

Equinox client is available on multiple platforms, Windows, Android, iOS, MAC. They all have a common behavior, common configuration, etc. The Equinox registration starts with a DNS A query on the FQDN learnt from 46xxsettings (SIP_CONTROLLER_LIST), then initiates SIP registration to the IP address returned by the DNS server. The client also initiates TLS connection for presence and directory services to the same address on port 443. At the same time the client signs in to Zang Spaces for Instant Messaging. For failover the Equinox client uses the FQDN returned by IPO during the SIP registration. The FQDN is in the backup_ipoffice_server field of the 200 OK.

The two recommended way to configure Equinox:

1. Email based configuration where Zang email is used. The Client will contact accounts.zang.io and check if domain of the given email address exists as a valid domain in Zang. If yes, it attempts to download the Public Settings of Equinox Cloud Client application which is assigned to the given domain. Example configuration:

   ```
   {
     "Client_Settings_File_Address": [
       {
         "Profile_Name": "IPO11",
         "Client_Settings_File_Url": "http://ipo11.example.com/46xxsettings.txt"
       }
     ]
   }
   ```

   In case of successful download, the client extracts the Client_Settings_File_Url and downloads the settings file from the given URL.
2. Web based configuration where the URL is http://<FQDNofPrimary>/46xxsettings.txt

Once the settings file is downloaded, the client will ask the SIP extension and password. If email based configuration is used, client will also ask the password to sign in to Zang Spaces.

## Troubleshooting

1. Use ping or nslookup to verify that all FQDNs are resolvable to the appropriate IP addresses. For example on the external DNS:

```
C:\Users\agardi>nslookup ipo11.example.com
Server:  UnKnown
Address:  135.124.167.205

Name:    ipo11.example.com
Address:  135.124.242.20


C:\Users\agardi>nslookup ipo11sec.example.com
Server:  UnKnown
Address:  135.124.167.205

Name:    ipo11sec.example.com
Address:  135.124.242.21
```

2. Query the im-info and sip-info from One-X Portal and check if primaryOnexAddress, secondaryOnexAddress, sipRegistrarFqdn fields are populated with appropriate FQDNs.

   Enter in the browser: https://<FQDN>:9443/inkaba/user/my/im-info

```
<im-info>
  <imId>peter@ipo11.example.com</imId>
  <imPassword>123456</imPassword>
  <myBuddyId>mybuddy@ipo11.example.com</myBuddyId>
  <primaryOnexAddress>ipo11.example.com</primaryOnexAddress>
  <secondaryOnexAddress>ipo11sec.example.com</secondaryOnexAddress>
</im-info>
```

   Enter in the browser: https://<FQDN>:9443/inkaba/user/my/sip-info

```
<sip-info>
  <identity>2001@example.com</identity>
  <userName>2001</userName>
  <password>123456</password>
  <displayName>Peter A</displayName>
  <privateAddress>10.1.1.60</privateAddress>
  <udpPrivatePort>5060</udpPrivatePort>
  <udpPublicPort>0</udpPublicPort>
  <tcpPrivatePort>5060</tcpPrivatePort>
  <tcpPublicPort>0</tcpPublicPort>
  <tlsPrivatePort>5061</tlsPrivatePort>
  <tlsPublicPort>0</tlsPublicPort>
  <payloadType>101</payloadType>
  <signalingQos>136</signalingQos>
  <voiceQos>184</voiceQos>
  <videoQos>184</videoQos>
  <sipRegistrarFqdn>ipo11.example.com</sipRegistrarFqdn>
</sip-info>
```

   In case of failover, the im-info will contain the same values, but sip-info will point to Secondary IP Office.

3. Run a traceSBC on the SBCE and check the registration of a Communicator for Windows or Equinox client. In the 200 OK of REGISTER, check the onex_server and backup_ipoffice_server fields. During normal operation the onex_server should contain the FQDN of Primary One-X Portal and backup_ipoffice_server should contain the FQDN of Secondary IP Office.

```
SIP/2.0 200 OK
From: <sips:2002@example.com>;tag=-7755f465afbe5f877878b8c_F2002135.124.166.102
To: <sips:2002@example.com>;tag=8dbfecce20a1232a
CSeq: 2 REGISTER
Call-ID: 1_1c8ba29326683cd9778788b0_R@135.124.166.102
Contact: <sips:2002@135.124.166.102:59097;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: vnd.avaya.ipo
User-Agent: IP Office 11.0.0.0.0 build 849
Via: SIP/2.0/TLS 135.124.166.102:59097;branch=z9hG4bK2_1c8ba29373567ce977879eb2_R2002
Expires: 180
Date: Wed, 16 May 2018 08:04:08 GMT
Server: IP Office 11.0.0.0.0 build 849
Content-Type: application/vnd.avaya.ipo
Content-Length: 552

<ipo>
onex_server="ipo11.example.com";
onex_server_port="8080";
xmpp_server_port="5222";
server_onex_secure_port="9443";
username="jancsi";
username_twin="&0.jancsi";
voicemail_collect="VM.2002";
video="1";
obtain_contacts_from_ipo="0";
conferencing="1";
conf_server="ConfServer@ipo11.example.com";
conf_server_adhoc="ConfAdhoc";
transfer="1";
extended_mwi="1";
video_capable="1";
blind_transfer="1";
auto_ans="1";
change_password="1";
xmpp_group="1";
backup_ipoffice_server="ipo11sec.example.com";
rfc2833_payload="101";
</ipo>
```

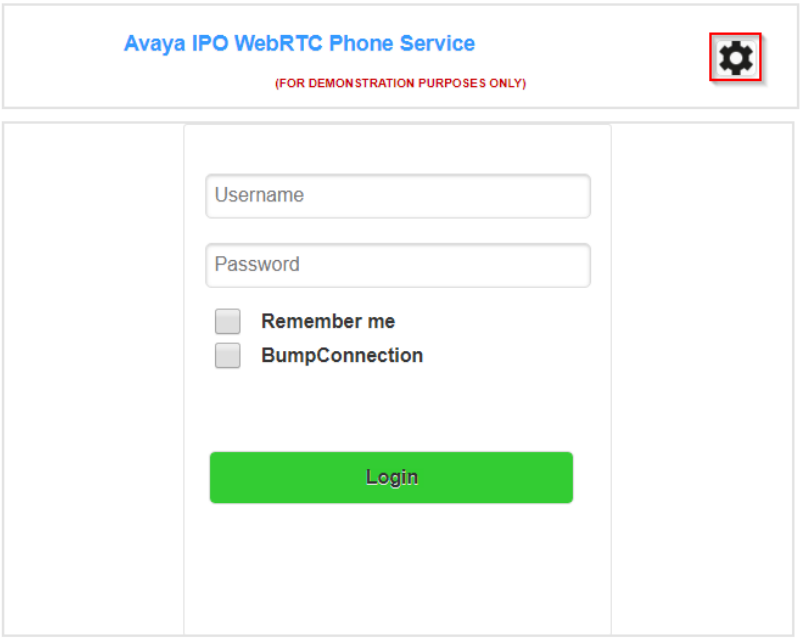
During failover the onex_server should contain the FQDN of Secondary One-X Portal and backup_ipoffice_server should contain 0.0.0.0.

## WebRTC Clients

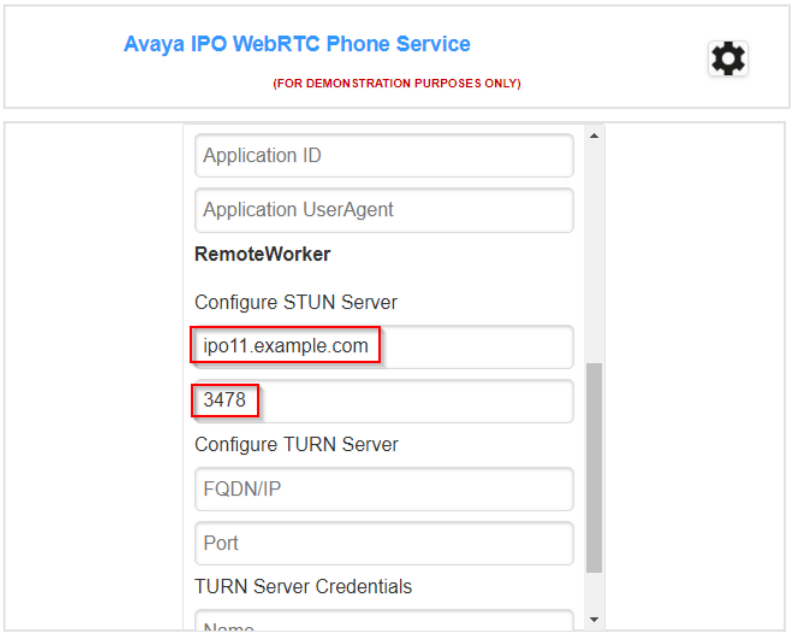
### PhoneService

To test the solution, use the PhoneService demo WebRTC client.

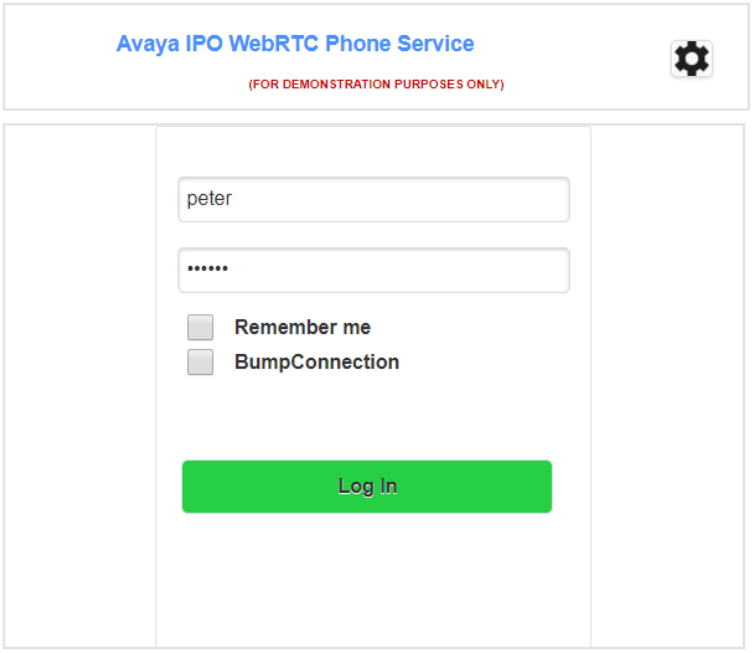
1. Open in Chrome https://<FQDNofOneX>:9443/PhoneService and click on **Settings** icon



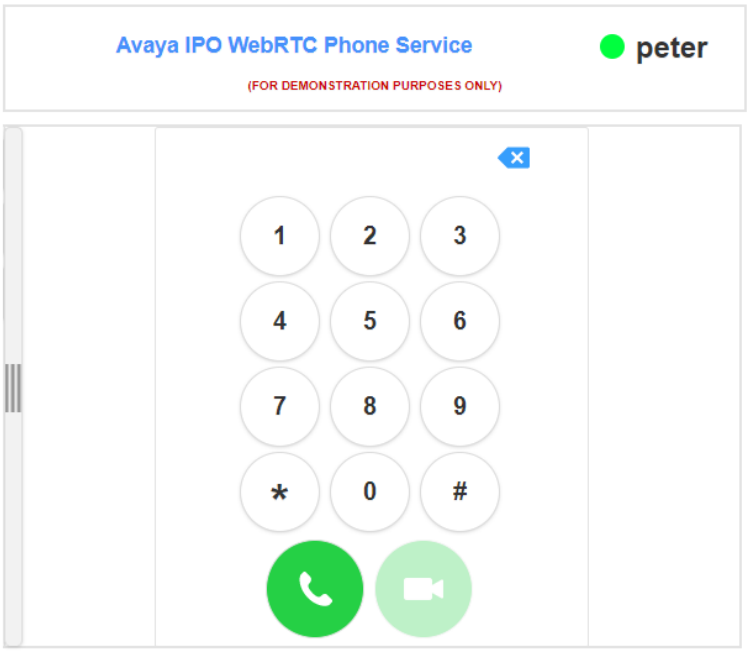

2. Scroll down to Remote Worker section and enter the FQDN of OneX portal at the STUN server (or you can configure any public STUN server) with port 3478




3. After saving the configuration enter **Username** and **Password** on the main screen and click **Login**

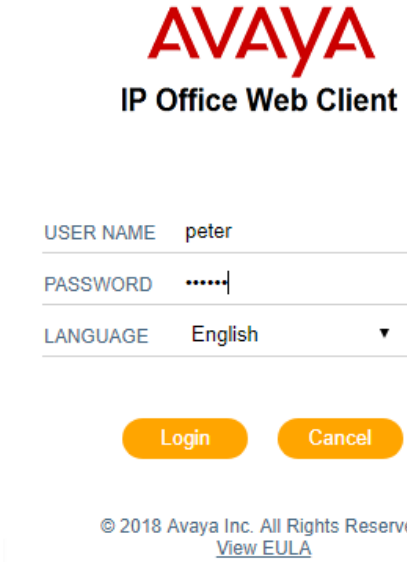



4. After successful login make a call to a local user and verify two way talk path

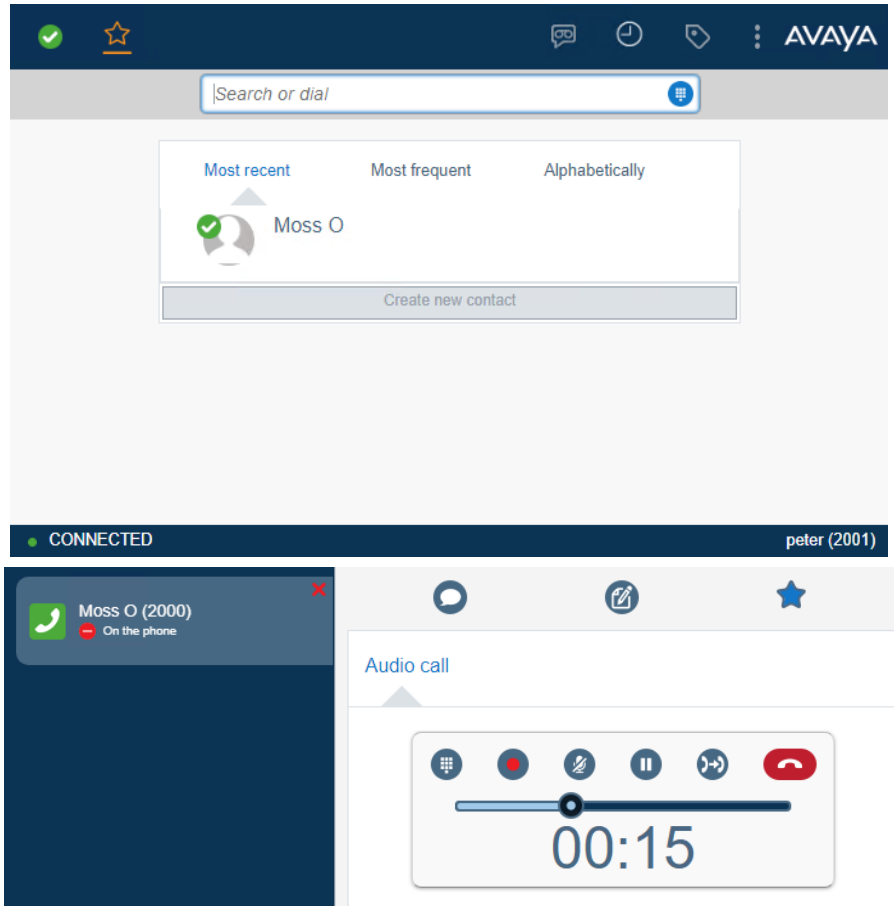



## IP Office Web Client

1. Open in Chrome https://<FQDNofOneX>:9443/webclient Make sure pop-ups are enabled.
2. Enter **Username** and **Password** on the main screen and click **Login**



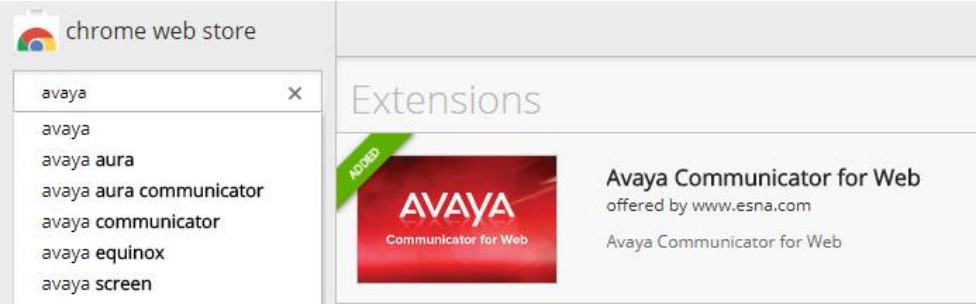

3. After successful login verify presence, then make a call to a local user either using Dialpad or by calling directly a contact.



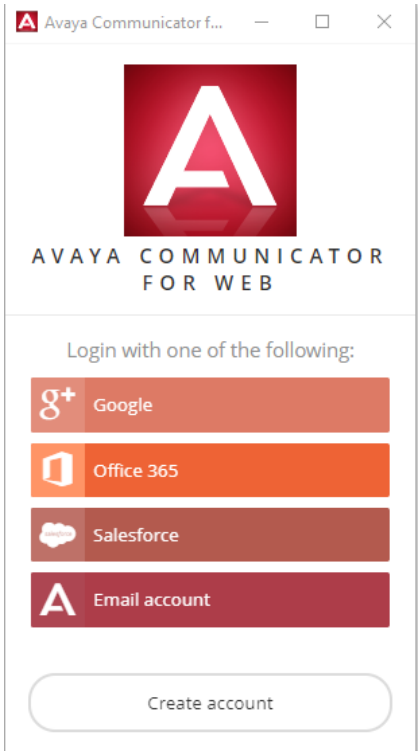
## Avaya Communicator for Web

Avaya Communicator for Web can be used either as a Chrome plugin or a standalone Windows application.

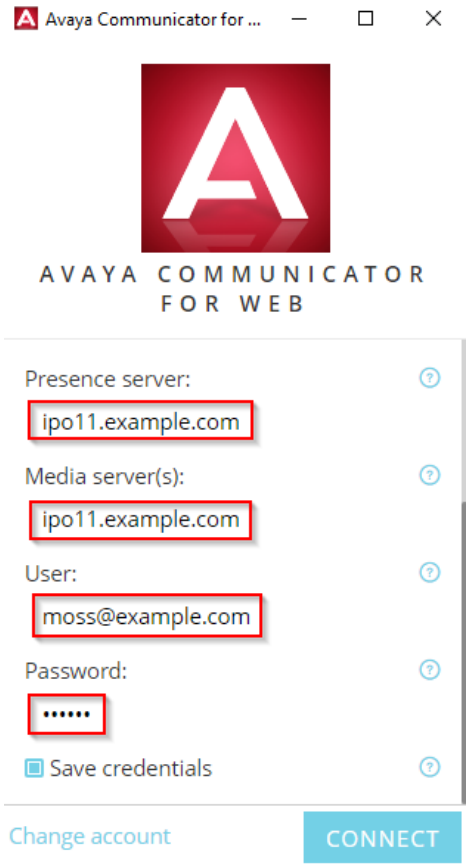
1. Open in Chrome and install Avaya Communicator for Web from the Chrome App Store



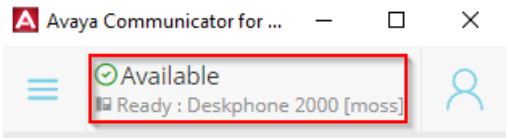

2. Start Avaya Communicator for Web and login with your account (or click on **Create account** if not yet created)



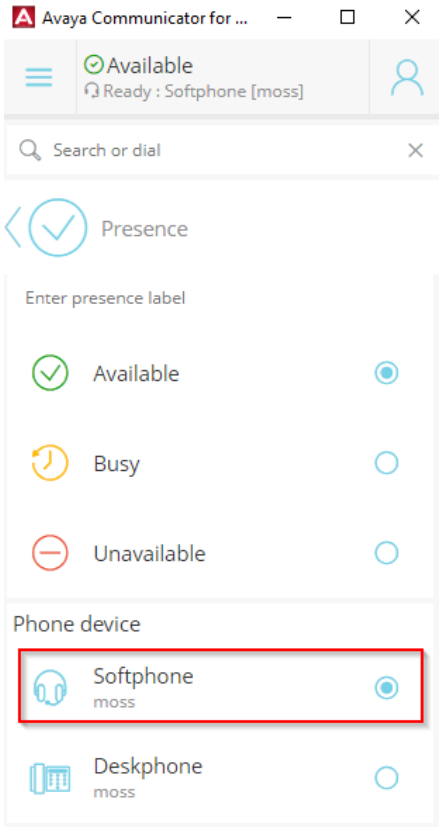

3. Once logged in with account, set **Authorize using** field to **Use explicit credentials**, then set the **Presence Server** and **Media Server** to the FQDN of One-X Portal, and use the login/password of the user on One-X Portal to connect.



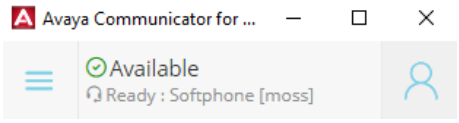

4. When logged in, click on presence status



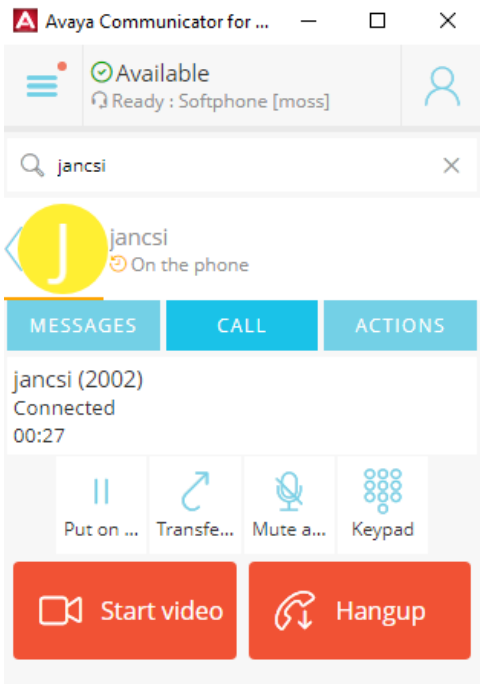

5. Change the Phone device to **Softphone**




6. Verify both presence and softphone is available/ready




7. Make a call using dial pad or contact and verify talk path

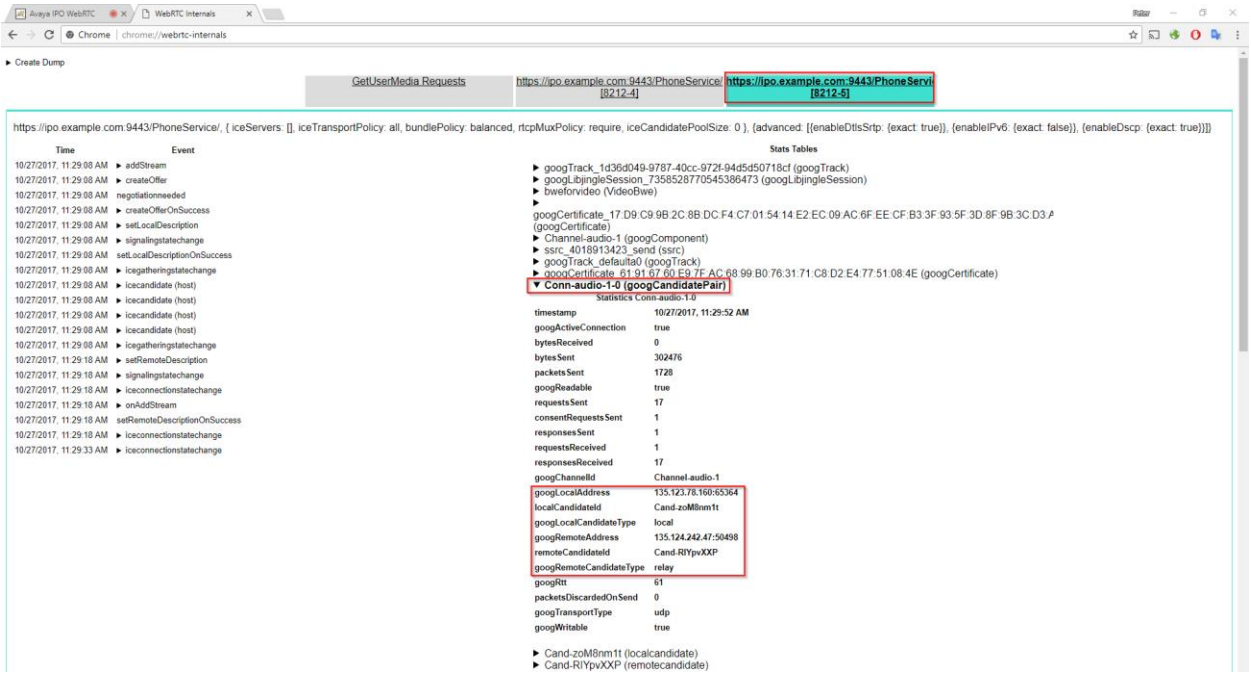



## Troubleshooting tools

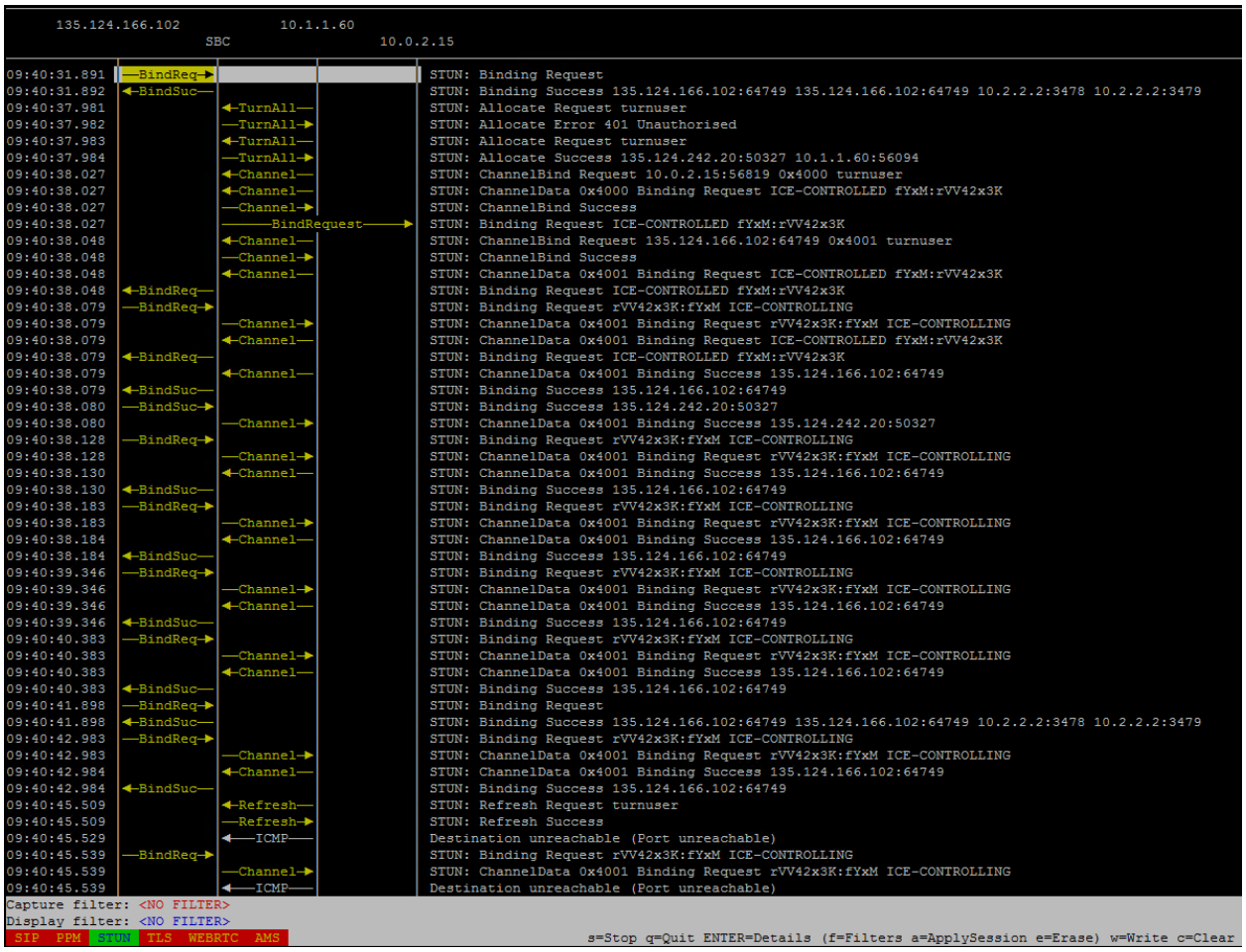
There are some common troubleshooting practices for all clients, and there are client specific options as well.

1. Common to all clients
    a. In Chrome open new tab with **chrome://webrtc-internals**

    Make a test call, select the latest call on webrt-internals and check the icecandidates, the connection, etc.

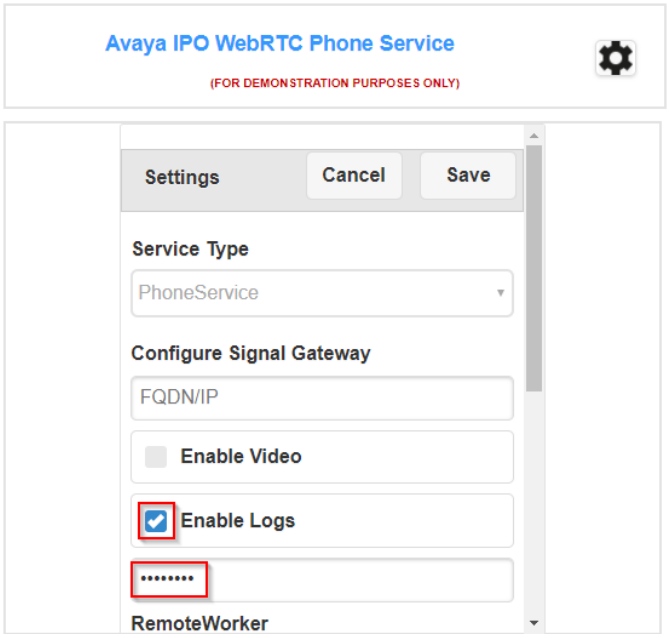


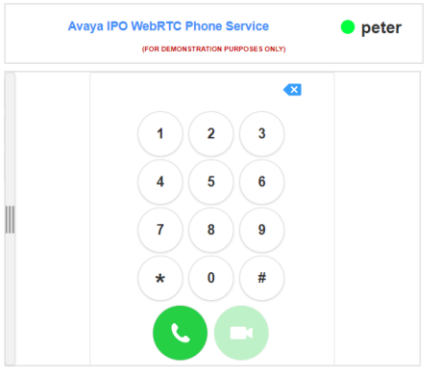

    b. Do a traceSBCE trace on SBCE and enable STUN/TURN/ICE capture

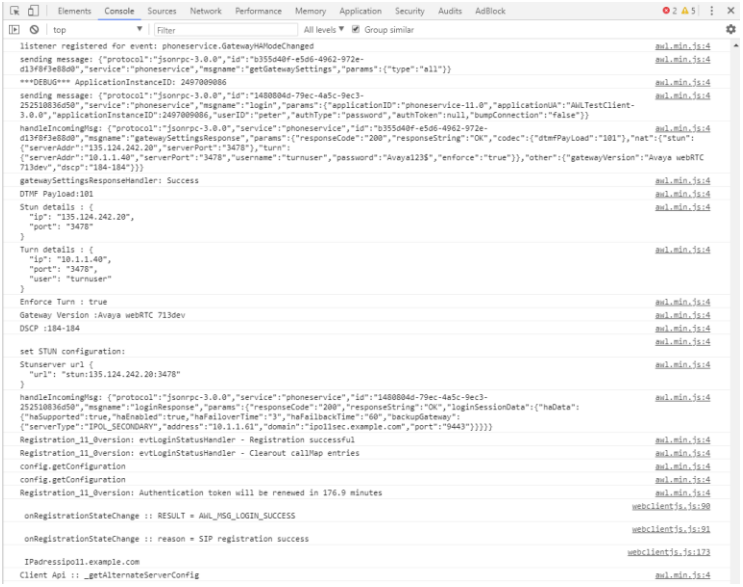



2. PhoneService

The debug logs can be captured in the Developer tool of the browser (CTRL+SHIFT+I in Chrome). To enable verbose logging, open Settings on the main screen, check **Enable Logs**, and set password to **Avaya123**, then click **Save**

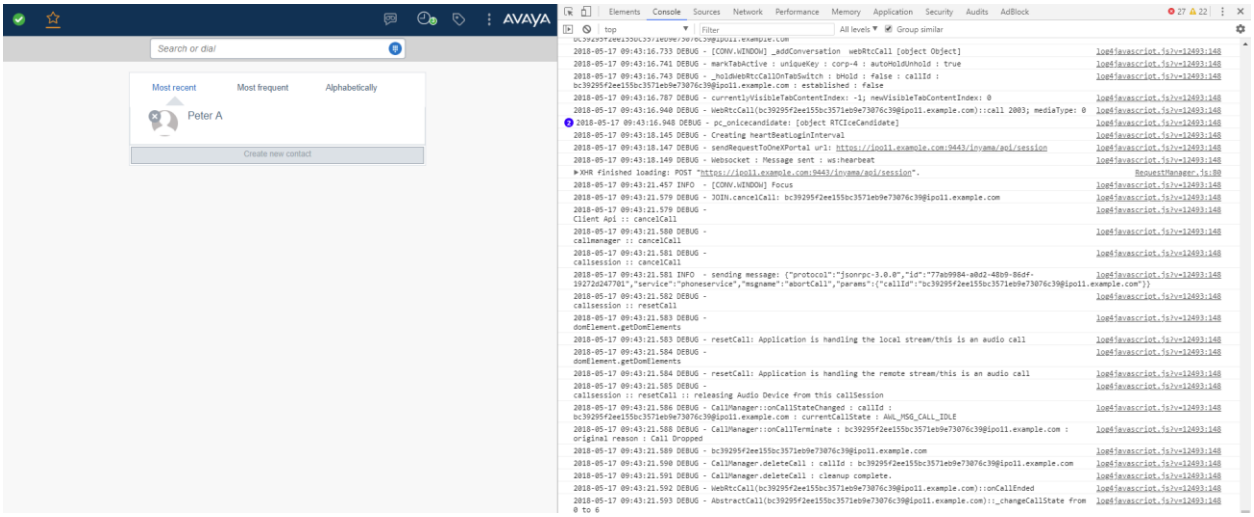



3. Web Client

The debug logs can be captured in the Developer tool of the browser (CTRL+SHIFT+I in Chrome).



4. Avaya Communicator for Web

The debug logs can be captured in Chrome opening app/avaya/background.html from the Extensions