



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.



Contents

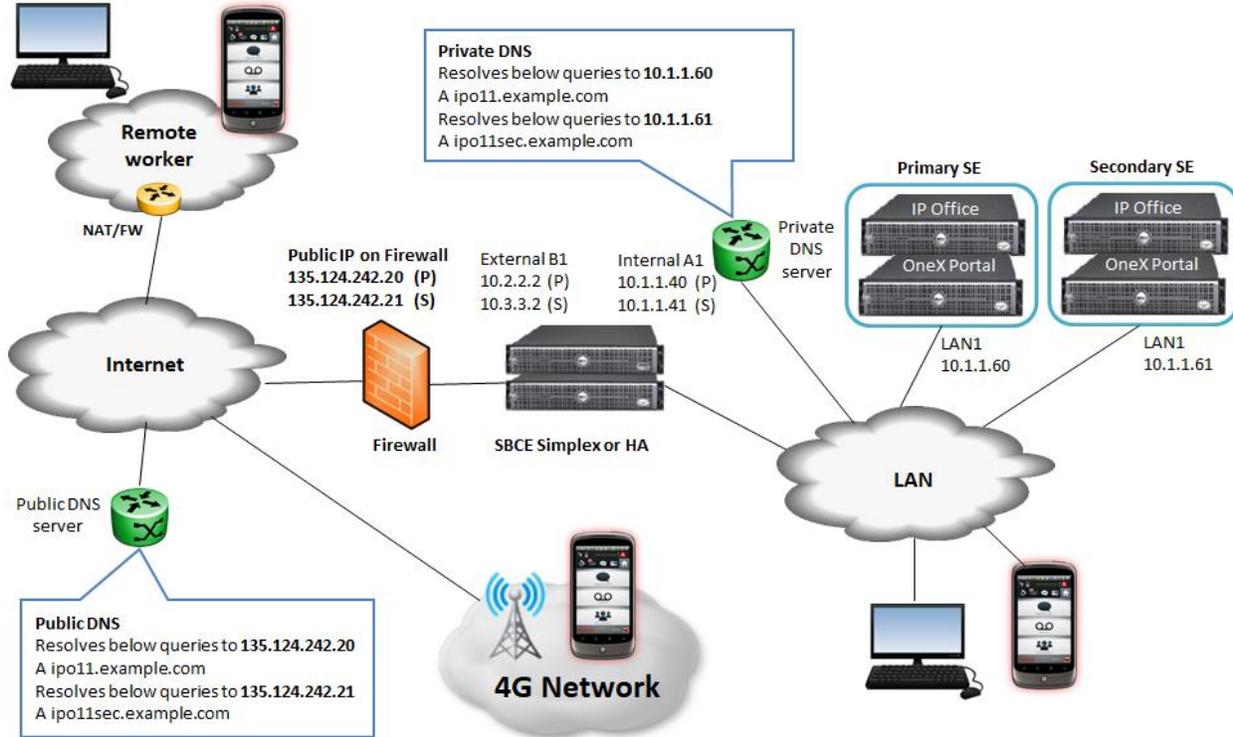
Overview	4 -
Prerequisites	5 -
VMware.....	5 -
vSphere Client	5 -
IP Office Administration Tools	5 -
Firewall configuration	6 -
Installing Primary IP Office.....	6 -
Deploying OVA	6 -
Changing default IP	8 -
Primary Server Ignition	10 -
Initial Configuration	13 -
Installing License	15 -
Installing Secondary IP Office.....	16 -
Secondary Server Ignition	16 -
Adding Secondary Server to the Solution	20 -
Configuring IP Office	23 -
VoIP Setup.....	23 -
Extensions	24 -
Users	25 -
XMPP Hunt Group.....	26 -
Configuring One-X Portal	27 -
Installing SBCE.....	29 -
Deploying OVA	29 -
Setting Management IP	29 -
Setting VMware network for external interface.....	33 -
SBCE initial configuration.....	34 -
Licensing.....	35 -
Changing default Listen Port Range.....	35 -
Certificates for IPO	36 -
Exporting IP Office Root CA	36 -
Generating Identity Certificate for Primary Server.....	36 -
Generating Identity Certificate for Secondary Server	37 -
Installing Identity Certificate on Secondary Server	38 -
Certificates for SBCE.....	39 -



Generating Identity Certificates for SBCE	- 39 -
Extracting Private Key and Identity Certificate	- 40 -
Adding IPO Root CA Certificate on SBCE.....	- 40 -
Adding SBCE Identity Certificate on SBCE.....	- 41 -
Configuring SBCE.....	- 42 -
TLS Profiles	- 43 -
External Interface.....	- 44 -
Media Interfaces	- 45 -
Signaling Interfaces	- 46 -
Server Profile.....	- 48 -
Routing.....	- 50 -
Topology Hiding	- 51 -
Subscriber Flow.....	- 52 -
Server Flow	- 54 -
Application Relays.....	- 56 -
TURN/STUN service.....	- 58 -
Configuring WebRTC Gateway.....	- 60 -
SIP Clients.....	- 61 -
Communicator for Windows.....	- 61 -
Communicator for iPad.....	- 62 -
Onex-X Mobile Preferred for Android	- 62 -
One-X Mobile Preferred for IOS.....	- 62 -
Equinox	- 63 -
Troubleshooting.....	- 63 -
WebRTC Clients.....	- 65 -
PhoneService.....	- 65 -
IP Office Web Client	- 67 -
Avaya Communicator for Web.....	- 69 -
Troubleshooting tools.....	- 72 -

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.

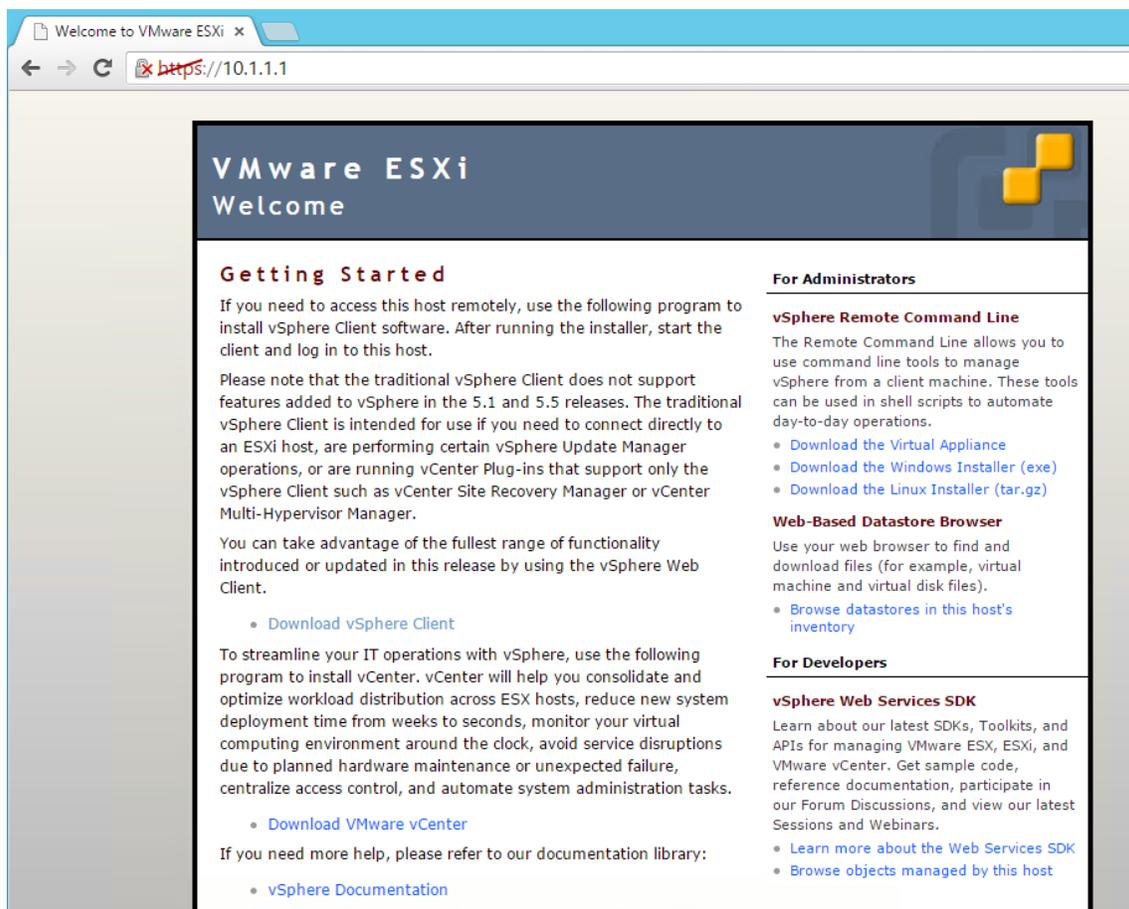
Prerequisites

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

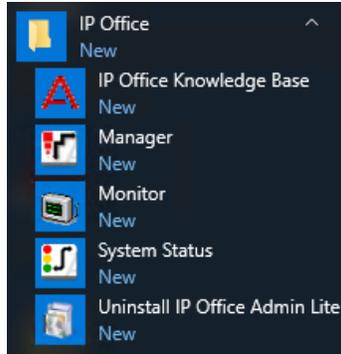
1. Open a browser to **https://<IP of VMware ESXi host>**



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

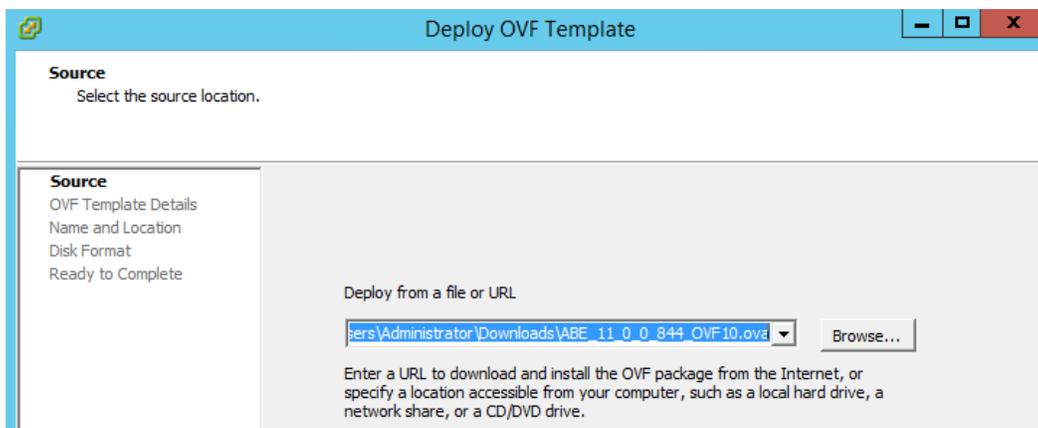
1. Allow Layer 3 NAT only, disable all SIP aware functionality, ALG, etc.
2. Forward the following ports to the B1 interface of the SBCE

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

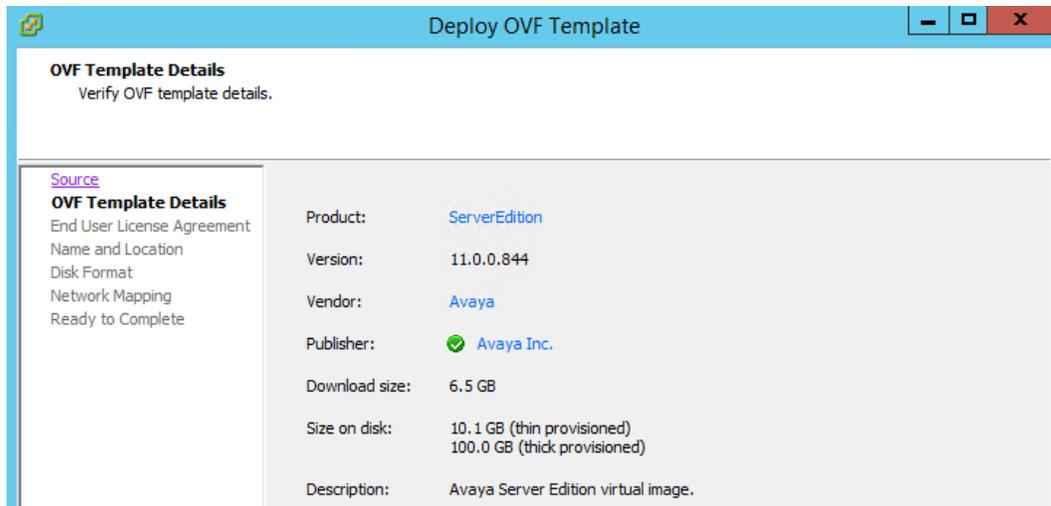
Installing Primary IP Office

Deploying OVA

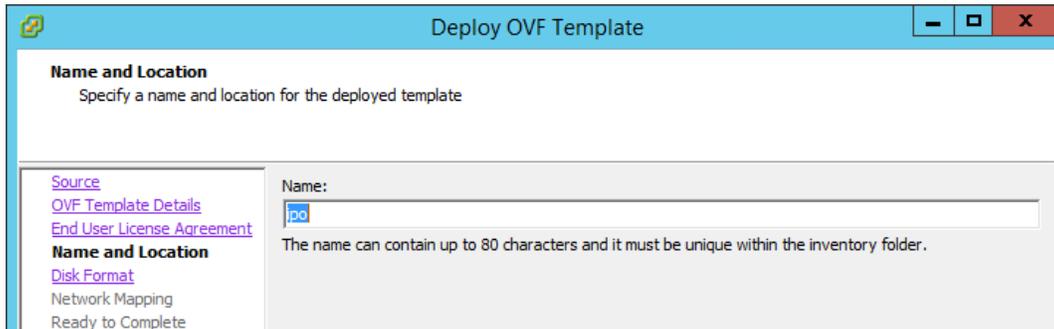
1. Download latest IP Office OVA file from **plds.avaya.com**
2. Start vSphere Client and connect to vCenter / AVP host
3. Go to **File / Deploy OVF Template**
4. Click **Browse** , select the OVA file and click **Open**



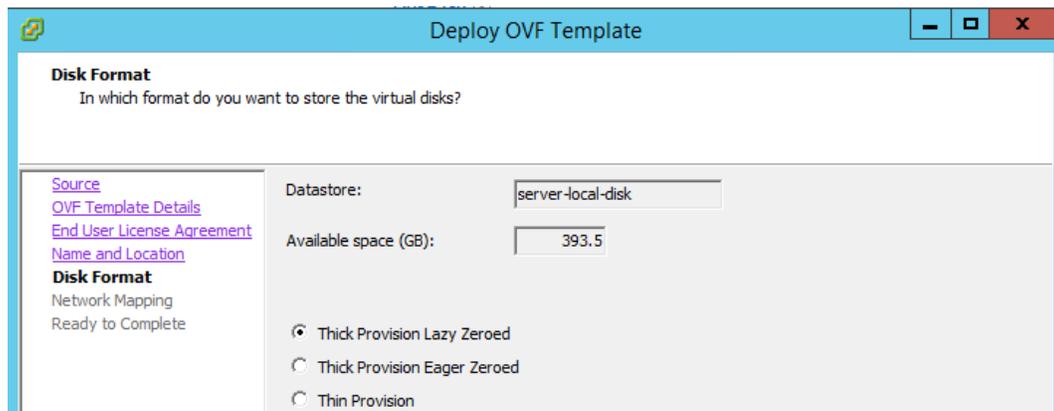
5. Click **Next**



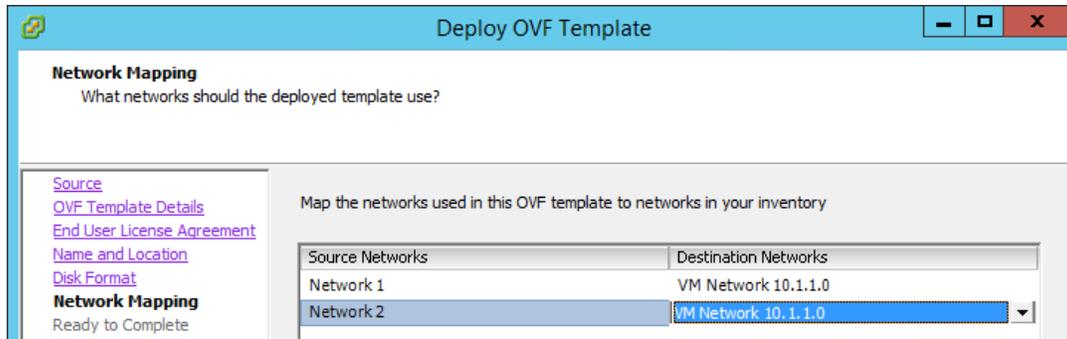
6. Click **Next**
7. License Agreement will be displayed, click **Accept** then **Next**
8. Set the name then click **Next**



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



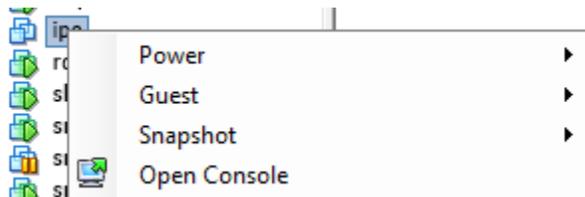
10. Select network mappings, then click **Next**



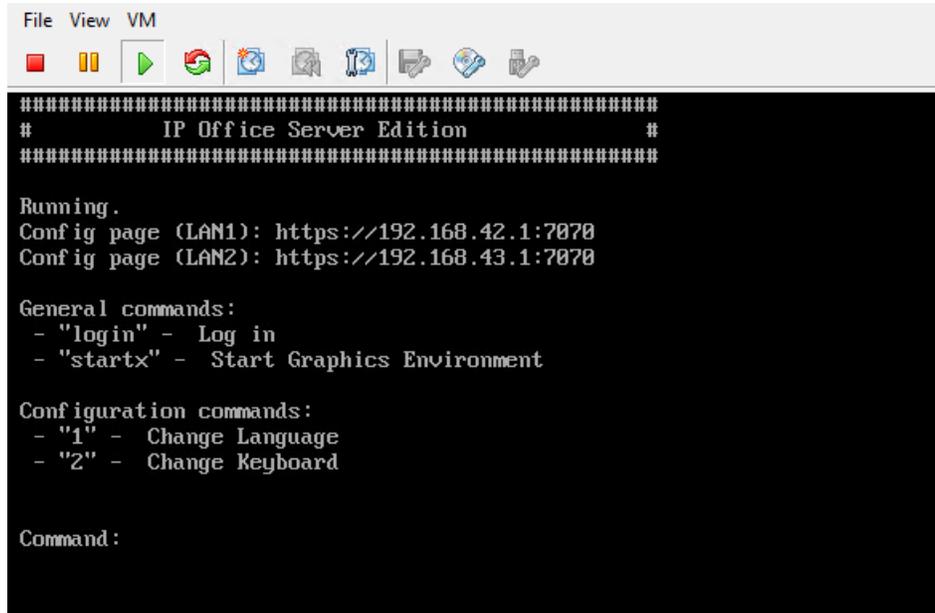
11. Wizard will display the summary, click **Finish**
12. Once deployment has completed, the new virtual machine appears in the inventory of virtual machines. Select the virtual machine and start it.

Changing default IP

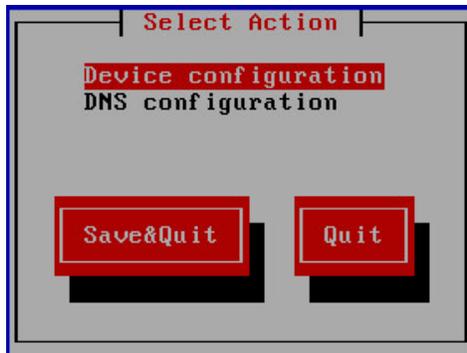
1. Right click on the IP Office virtual machine then click on **Open Console**



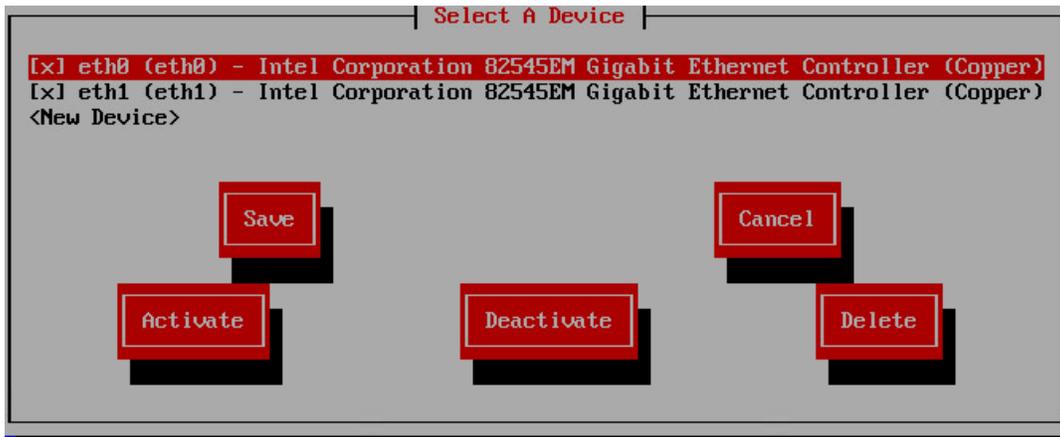
2. If this is the first boot, wait for the virtual machine to boot up until the following can be seen in the console window



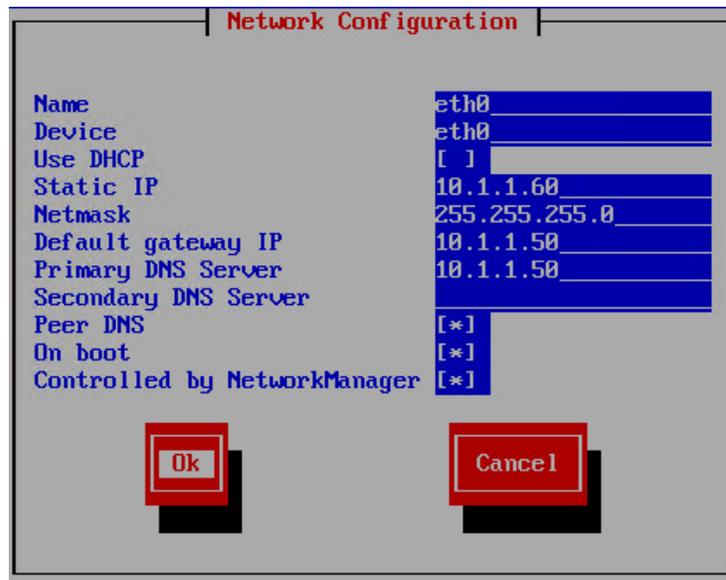
3. Click in the window (to release cursor from console window use the left CTRL+ALT keys)
4. Enter the command **login**
5. Default login is **root** with password **Administrator**
6. Enter the command **system-config-network**. The menu that appears is navigated using the cursor keys, tab key and Enter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

IP Office Server Edition R11.0

Please log on using the root account.

User Name: root

Password:

Language: English

Login

© 2018 Avaya Inc. All rights reserved - [View EULA](#)

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

IP Office - Ignition

Accept License →

Server Type

New Hardware

Configure Network

Time & Companding

Change Password

Review Settings

AVAYA GLOBAL SOFTWARE LICENSE TERMS

REVISED: March 2015

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW). BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU," "YOUR," AND "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF YOU ARE ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE

I Agree [Print EULA](#)

Cancel Next

4. Select Primary (Server Edition) and click Next

IP Office - Ignition

Accept License ✓

Server Type →

New Hardware

Configure Network

Time & Companding

Change Password

Review Settings

- Primary (Server Edition)**
Enables Core, one-X Portal and Voicemail Pro.
- Secondary (Server Edition)**
Enables Core, one-X Portal and Voicemail Pro.
- Expansion (Server Edition)**
Enables Core only.
- Application Server**
Enables one-X Portal and Voicemail Pro.
Voicemail Pro on the Application Server is not supported in Server Edition.

Cancel **Previous** **Next**

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

IP Office Server Edition - Ignition

Accept License ✓

Server Type ✓

New Hardware ✓

Configure Network →

Time & Companding

Change Password

Security

Review Settings

Network interface: eth0

Assign IP Address:

Automatic (DHCP)

IP Address:

Netmask:

Assign System Gateway:

Gateway:

Assign System DNS Servers:

Automatic (DHCP)

Primary DNS:

Secondary DNS:

Hostname:

Cancel **Previous** **Next**

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

IP Office Server Edition - Ignition

Accept License	✓
Server Type	✓
New Hardware	✓
Configure Network	✓
Time & Companding	→
Change Password	
Security	
Review Settings	

Use NTP:

NTP Server:

Timezone:

Companding: μ-law
 A-law

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

IP Office Server Edition - Ignition

Default account passwords are required to be changed.

"root" and "security" password

New Password:

New Password (verify):

[View password policy](#)

"Administrator" password

New Password:

New Password (verify):

[View password policy](#)

"System" password

New Password:

New Password (verify):

[View password policy](#)

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

IP Office Server Edition - Ignition

Accept License	✓
Server Type	✓
New Hardware	✓
Configure Network	✓
Time & Companding	✓
Change Password	✓
Security	→
Review Settings	

CA Certificate

Generate new

Import

Cancel Previous Next

10. At the summary click **Apply**

IP Office Server Edition - Ignition

Accept License	✓
Server Type	✓
New Hardware	✓
Configure Network	✓
Time & Companding	✓
Change Password	✓
Security	✓
Review Settings	→

Server Type:	Primary
IP:	10.1.1.60
Netmask:	255.255.255.0
Gateway:	10.1.1.50
Primary DNS:	10.1.1.50
Secondary DNS:	
Hostname:	ipo11.example.com
Timezone:	Europe/Budapest
Use NTP Client:	Yes
NTP Server:	135.9.81.247
Companding:	A-law
Additional Hardware:	No new hardware available.
CA Certificate:	Subject: Issued by: Download CA certificate (PEM-encoded) Download CA certificate (DER-encoded)

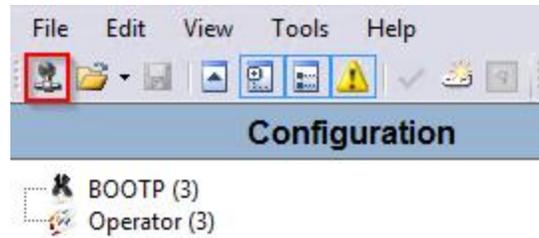
Print

ATTENTION: Prior to ordering licenses for IP Office please confirm the following settings have been finalized: LAN1 and LAN2 IP addresses, Timezone and Hostname. Changing these settings will invalidate any existing licenses. Please see documentation for more detail.

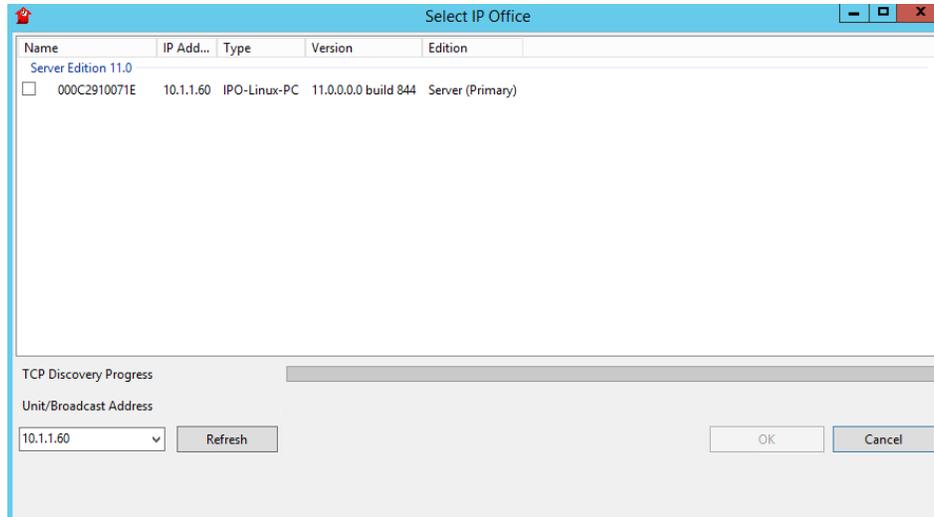
Cancel Previous Apply

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**.

Avaya IP Office Initial Configuration

Please click here to use web based initial configuration wizard.

System Type Server Edition Primary Server Edition Secondary

Activate IP Office Select Mode

Retain Configuration Data

Hosted Deployment

System Name

WebSocket Password

Confirm WebSocket Password

Locale

Services Device ID

LAN Interface LAN1 LAN2

IP Address

IP Mask

Gateway

DHCP Mode

Server Client Dial In Disabled

Server Edition Secondary

DNS Server

Subscription System

Save Reset Close Help

Installing License

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



Web License Manager



User Name:

Password:

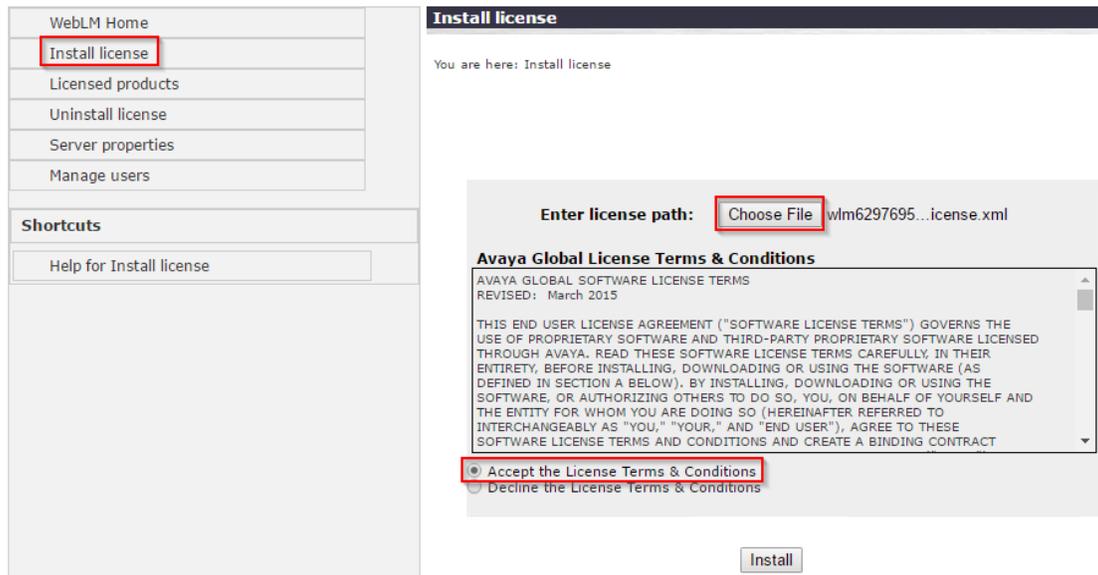
Log On Clear

© 2016 Avaya Inc. All Rights Reserved.

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**



IP Office Server Edition R11.0

Please log on using the root account.

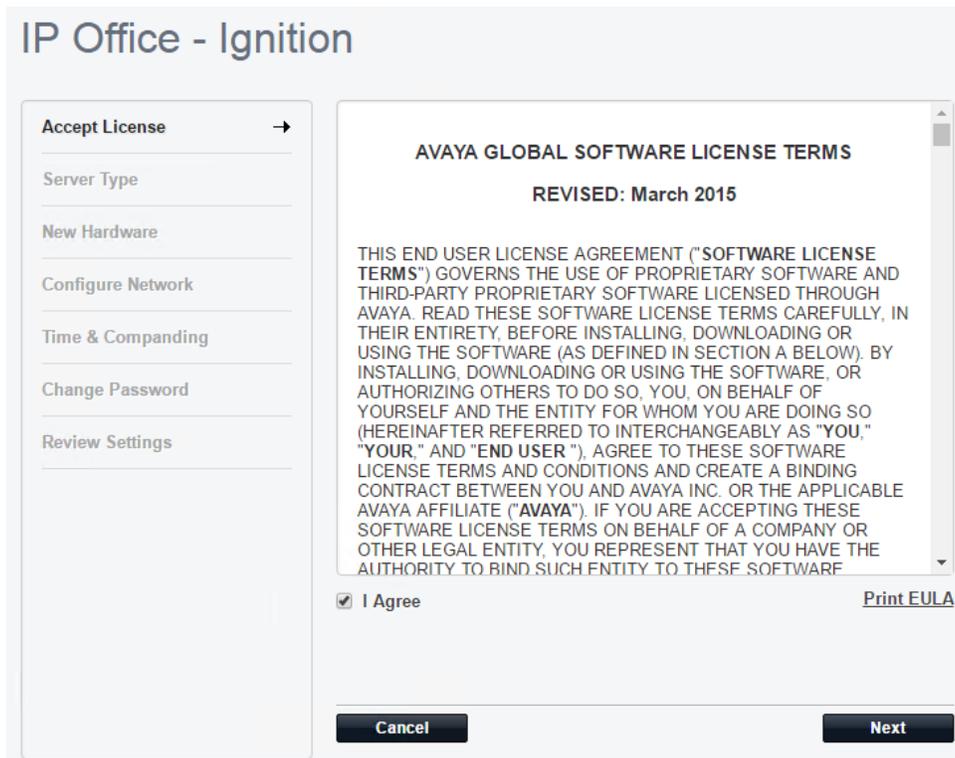
User Name:

Password:

Language:

© 2018 Avaya Inc. All rights reserved - [View EULA](#)

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



IP Office - Ignition

Accept License →

Server Type

New Hardware

Configure Network

Time & Companding

Change Password

Review Settings

AVAYA GLOBAL SOFTWARE LICENSE TERMS

REVISED: March 2015

THIS END USER LICENSE AGREEMENT ("SOFTWARE LICENSE TERMS") GOVERNS THE USE OF PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW). BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU," "YOUR," AND "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF YOU ARE ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE

I Agree [Print EULA](#)

4. Select Secondary (Server Edition) and click Next

IP Office - Ignition

Accept License ✓	<input type="radio"/> Primary (Server Edition) Enables Core, one-X Portal and Voicemail Pro.
Server Type →	<input checked="" type="radio"/> Secondary (Server Edition) Enables Core, one-X Portal and Voicemail Pro.
New Hardware	<input type="radio"/> Expansion (Server Edition) Enables Core only.
Configure Network	<input type="radio"/> Application Server Enables one-X Portal and Voicemail Pro. Voicemail Pro on the Application Server is not supported in Server Edition.
Time & Companding	
Change Password	
Review Settings	

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

IP Office Server Edition - Ignition

Accept License ✓	Network interface: eth0
Server Type ✓	Assign IP Address:
New Hardware ✓	Automatic (DHCP) <input type="checkbox"/>
Configure Network →	IP Address: <input type="text" value="10.1.1.61"/>
Time & Companding	Netmask: <input type="text" value="255.255.255.0"/>
Change Password	Assign System Gateway:
Review Settings	Gateway: <input type="text" value="10.1.1.50"/>
	Assign System DNS Servers:
	Automatic (DHCP) <input type="checkbox"/>
	Primary DNS: <input type="text" value="10.1.1.50"/>
	Secondary DNS: <input type="text"/>
	Hostname: <input type="text" value="ipo11sec.example.com"/>

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

IP Office Server Edition - Ignition

Accept License	✓	Timezone:	Europe/Budapest
Server Type	✓		
New Hardware	✓	Companing:	<input type="radio"/> µ-law
Configure Network	✓		<input checked="" type="radio"/> A-law
Time & Companing	→		
Change Password			
Review Settings			

Cancel **Previous** **Next**

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

IP Office Server Edition - Ignition

Default account passwords are required to be changed.

Accept License	✓	"root" and "security" password
Server Type	✓	New Password: <input type="text"/>
New Hardware	✓	New Password (verify): <input type="text"/>
Configure Network	✓	View password policy
Time & Companing	✓	"Administrator" password
Change Password	→	New Password: <input type="text"/>
Security		New Password (verify): <input type="text"/>
Review Settings		View password policy
		"System" password
		New Password: <input type="text"/>
		New Password (verify): <input type="text"/>
		View password policy

Cancel **Previous** **Next**

9. At the summary click **Apply**

IP Office Server Edition - Ignition

Accept License	✓
Server Type	✓
New Hardware	✓
Configure Network	✓
Time & Companding	✓
Change Password	✓
Review Settings	→

Server Type:	Secondary
IP:	10.1.1.61
Netmask:	255.255.255.0
Gateway:	10.1.1.50
Primary DNS:	10.1.1.50
Secondary DNS:	
Hostname:	ipo11sec.example.com
Timezone:	Europe/Budapest
Companding:	A-law
Additional Hardware:	No new hardware available.

ATTENTION: Prior to ordering licenses for IP Office please confirm the following settings have been finalized: LAN1 and LAN2 IP addresses, Timezone and Hostname. Changing these settings will invalidate any existing licenses. Please see documentation for more detail.

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



The image shows the Avaya IP Office Web Manager login interface. On the left is a vertical red bar with the Avaya logo. The main area has a white background with the title 'Avaya IP Office Web Manager'. Below the title are three input fields: 'User Name' with 'Administrator' entered, 'Password' with masked characters, and 'Select Language' with 'English' selected. There is an 'Offline Mode' checkbox with an information icon, and a 'Login' button. At the bottom, it says '© 2018 Avaya Inc. All Rights Reserved.'

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

The screenshot shows the Avaya Solution Manager interface. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security Manager', and 'Applications'. The main area is titled 'Solution' and contains a search bar and a list of system objects. A dropdown menu is open for the system 'ipo11', with the option 'Add System to Solution' highlighted in red. Other options in the menu include 'Remove System from Solution', 'Set all Nodes to Select', 'Resiliency Administration', 'Set All Nodes License Source', and 'Link Expansions'.

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

The screenshot shows the 'Add System to Solution' form. The 'Select system to add' section has 'Secondary server' selected. The 'IP Address of the system to add' field contains '10 . 1 . 1 . 61'. The 'WebSocket Password' and 'Confirm WebSocket Password' fields are filled with dots. A 'Discover' button is visible. Below the form is a table with columns: IP Office, IP Address, Type, Version, and Edition.

IP Office	IP Address	Type	Version	Edition
<input checked="" type="checkbox"/>				

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

The screenshot shows the 'Add System to Solution' form with the 'Discover' button clicked. The table below the form now contains one entry:

IP Office	IP Address	Type	Version	Edition
<input checked="" type="checkbox"/>	000C296E0361	10.1.1.61	IPO-Linux-PC	11.0.0.0 build 844
				Server (Secondary)

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

Primary IP Address to link

OK

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

AVAYA Solution Call Management System Settings Security Manager Applications

Add System to Solution

Select System
 To add a system to the solution enter details or find the system.

Initial Configuration
 The system will be reconfigured as per Initial Configuration selection.

GENERAL

System Name*

Activate IP Office Select Mode YES NO

Hosted Deployment YES NO

Services Device ID

DNS Server

Locale

LAN Interface

LAN1 CONFIGURATION

IP Address

IP Subnet Mask

DHCP Mode

LAN2 CONFIGURATION

IP Address

IP Subnet Mask

DHCP Mode

Gateway

SOLUTION RELATED

Server Edition Primary*

WebSocket Password*

Confirm WebSocket Password*

Cancel Back Next

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

AVAYA Solution Call Management System Settings Security Manager Applications

Solution

Solution Settings

SOLUTION OBJECTS

View All (2)

SERVER STATUS

Online (2)

Offline (0)

SERVER TYPE

Servers (2)

Expansions (0)

Application Servers (0)

Actions

Configure

Enter search criteria

ip011

ip011sec

Add System to Solution

Remove System from Solution

Set all Nodes to Select

Resiliency Administration

Set All Nodes License Source

Link Expansions

Primary: Select

Secondary: Select

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

The screenshot shows the 'Resiliency Administration' page. Under 'Backup Primary Server', the checkbox 'Backup Primary server IP phones, hunt groups, voicemail and one-X Portal on the Secondary server.' is checked. Below it, the text reads 'Currently only IP Phones, Hunt Groups, Voicemail is backed up.' Under 'Backup Secondary Server', the checkbox 'Backup Secondary server IP phones and hunt groups on the Primary server.' is also checked.

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

The screenshot shows the 'VoIP' configuration page under the 'LAN1' tab. The 'SIP Registrar Enable' checkbox is checked and highlighted with a red box. The 'SIP Domain Name' field contains 'example.com' and the 'SIP Registrar FQDN' field contains 'ipo11.example.com', both highlighted with red boxes. Under 'Layer 4 Protocol', the 'UDP', 'TCP', and 'TLS' checkboxes are checked. The 'TLS Port' is set to 5061, also highlighted with a red box. Other settings include 'H.323 Gatekeeper Enable' checked, 'Auto-create Extension' and 'Auto-create User' unchecked, and 'H.323 Remote Extension Enable' unchecked. The 'Remote Call Signaling Port' is set to 1720.

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

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VoIP
--------	------	------	-----	-----------	-----------	--------------------	---------------	------	------	------

Ignore DTMF Mismatch For Phones
 Allow Direct Media Within NAT Location
 RFC2833 Default Payload:

Available Codecs

- G.711 ULAW 64K
- G.711 ALAW 64K
- G.722 64K
- G.729(a) 8K CS-ACELP

Default Codec Selection

Unused

>>>
↑
↓
<<<

Selected

- G.711 ALAW 64K
- G.711 ULAW 64K
- G.729(a) 8K CS-ACELP

- Go to **VoIP Security** tab and set the **Media** to **Preferred**

System	LAN1	LAN2	DNS	Voicemail	Telephony	Directory Services	System Events	SMTP	SMDR	VoIP	VoIP Security
--------	------	------	-----	-----------	-----------	--------------------	---------------	------	------	------	---------------

Media: Preferred Strict SIPS

Media Security Options

Encryptions: RTP, RTCP

Authentication: RTP, RTCP

Replay Protection: SRTP Window Size:

Crypto Suites: SRTP_AES_CM_128_SHA1_80, SRTP_AES_CM_128_SHA1_32

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

Extensions

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

Extension	VoIP
Extension ID	<input type="text" value="8000"/>
Base Extension	<input type="text" value="2000"/>
Phone Password	<input type="password" value="•••••"/>
Confirm Phone Password	<input type="password" value="•••••"/>
Caller Display Type	<input type="text" value="On"/>
Reset Volume After Calls	<input type="checkbox"/>
Device Type	 <input type="text" value="Unknown SIP device"/>
Location	<input type="text" value="Automatic"/>
Fallback As Remote Worker	<input type="text" value="Auto"/>
Module	<input type="text" value="0"/>
Port	<input type="text" value="0"/>
Disable Speakerphone	<input type="checkbox"/>

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.

User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	Button Programming
Name	peter								
Password	••••••								
Confirm Password	••••••								
Unique Identity	peter@example.com								
Conference PIN									
Confirm Audio Conference PIN									
Account Status	Enabled								
Full Name	Peter A								
Extension	2001								
Email Address									
Locale									
Priority	5								
System Phone Rights	None								
Profile	Power User								
	<input type="checkbox"/> Receptionist <input checked="" type="checkbox"/> Enable Softphone <input checked="" type="checkbox"/> Enable one-X Portal Services <input checked="" type="checkbox"/> Enable one-X TeleCommuter <input checked="" type="checkbox"/> Enable Remote Worker <input checked="" type="checkbox"/> Enable Desktop/Tablet VoIP client <input checked="" type="checkbox"/> Enable Mobile VoIP Client <input type="checkbox"/> Send Mobility Email <input type="checkbox"/> Web Collaboration								

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

User	Voicemail	DND	Short Codes	Source Numbers
Voicemail Code	••••••			
Confirm Voicemail Code	••••••			
Voicemail Email				

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

User	Voicemail	DND	Short Codes	Source Numbers	Telephony
Call Settings	Supervisor Settings	Multi-line Options	Call Log	TUI	
Login Code	••••••				
Confirm 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**



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

AVAYA one-X™ Portal for IP Office

Health	▶ Providers
Configuration	▶ Users
Providers	▶ CSV
Users	▶ Branding
CSV	▼ IM/Presence Server
Branding	Server to Server Federation <input checked="" type="checkbox"/>
IM/Presence	Disconnect on Idle <input type="checkbox"/>
Exchange service	Anyone can connect <input checked="" type="checkbox"/>
SMTP Configuration	Port number 5269
Conference Dial-in	Idle timeout 3600
Resiliency	MyBuddy user name mybuddy
Host Domain Name	XMPP Domain Name ipo11.example.com
Conference Clean Up	Days to archive IMs 182
Central CTI Link	
Security	Note: Days to archive IMs field will be disabled until IM/Presence server is available.
Diagnostics	<input type="button" value="Save"/> <input type="button" value="Clear"/> <input type="button" value="Refresh"/>
Directory Integration	▶ IM/Presence Exchange Service
Gadgets Configuration	▶ SMTP Configuration
IM Archive	
Web Conferences	
Help & Support	

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

AVAYA one-X™ Portal for IP Office

Health

Configuration

[Providers](#)

[Users](#)

[CSV](#)

[Branding](#)

[IM/Presence](#)

[Exchange service](#)

[SMTP Configuration](#)

[Conference Dial-in](#)

[Resiliency](#)

[Host Domain Name](#)

[Conference Clean Up](#)

[Central CTI Link](#)

Security

Diagnostics

Directory Integration

Gadgets Configuration

IM Archive

Web Conferences

Help & Support

- ▶ Providers
- ▶ Users
- ▶ CSV
- ▶ Branding
- ▶ IM/Presence Server
- ▶ IM/Presence Exchange Service
- ▶ SMTP Configuration
- ▶ Conference Dial-in Information
- ▶ Resiliency
- ▼ Host Domain Name

Primary Host Domain Name	ipo11.example.com
Secondary Host Domain Name	ipo11sec.example.com
Web Collaboration Domain Name	ipo11.example.com

Note:

- Web Collaboration Domain Name will be used to generate Conference Web Collaboration URL.
- Changes to Domain Name configuration require one-X Portal server restart.

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

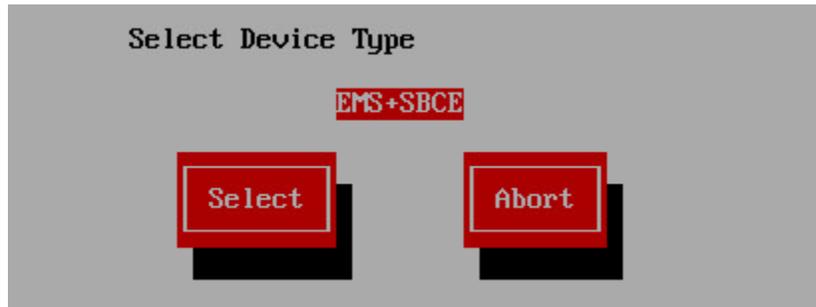
1. Right click on the SBCE virtual machine then click on **Open Console**
2. Wait for the virtual machine to boot up until the following can be seen in the console window:

```

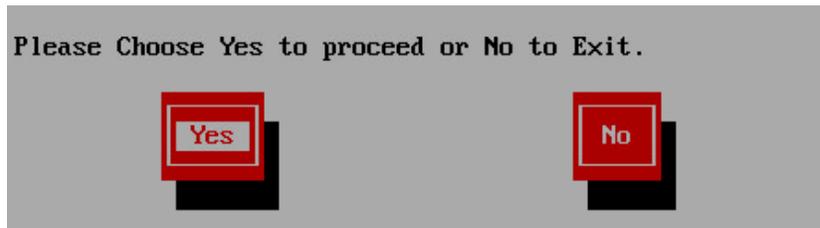
INFO      : -----
INFO      : CHOOSE OPERATION
INFO      : -----
INFO      : 1. Configure - Command Line Mode
INFO      : 2. Configure - Text Mode
INFO      : 3. Reboot SBCE
INFO      : 4. Shutdown SBCE
INFO      : 5. SBCE Shell Login
Enter your choice [1 - 5] :

```

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



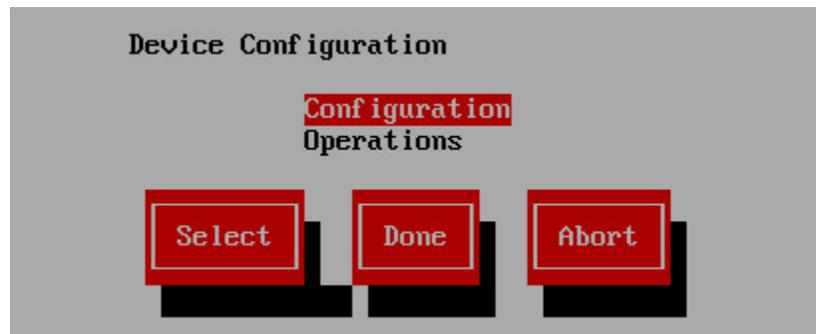
5. Hit **Enter** on **Yes**



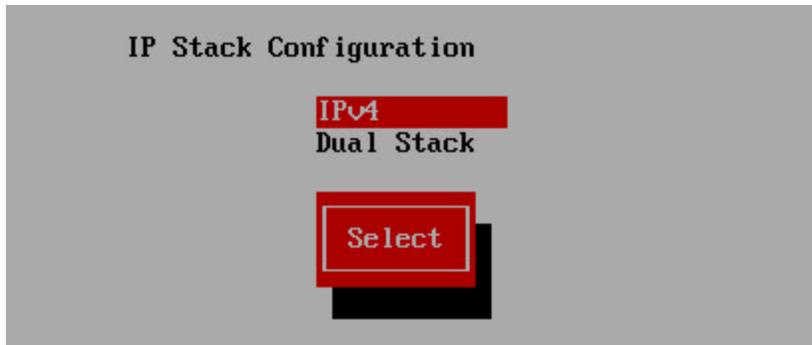
6. Hit **Enter** on **OK**



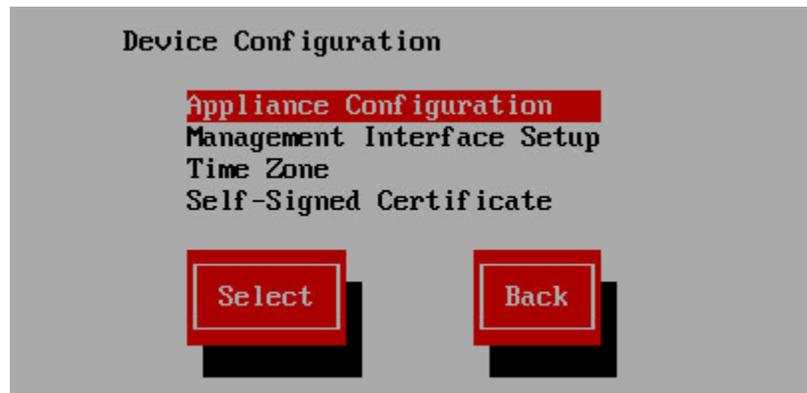
7. Select **Configuration**, then hit **Enter** on **Select**



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



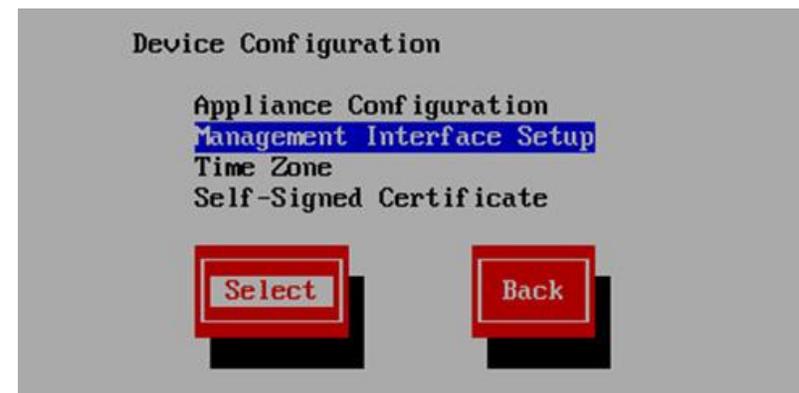
9. Select **Appliance Configuration** and hit **Enter** on **Select**



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



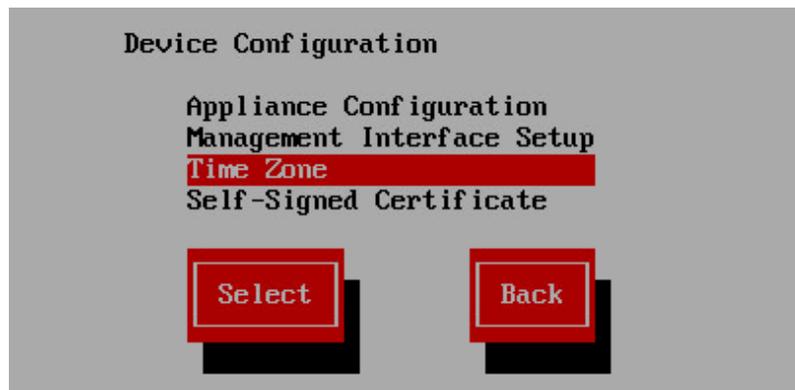
11. Select **Management Interface Setup** and hit **Enter** on **Select**



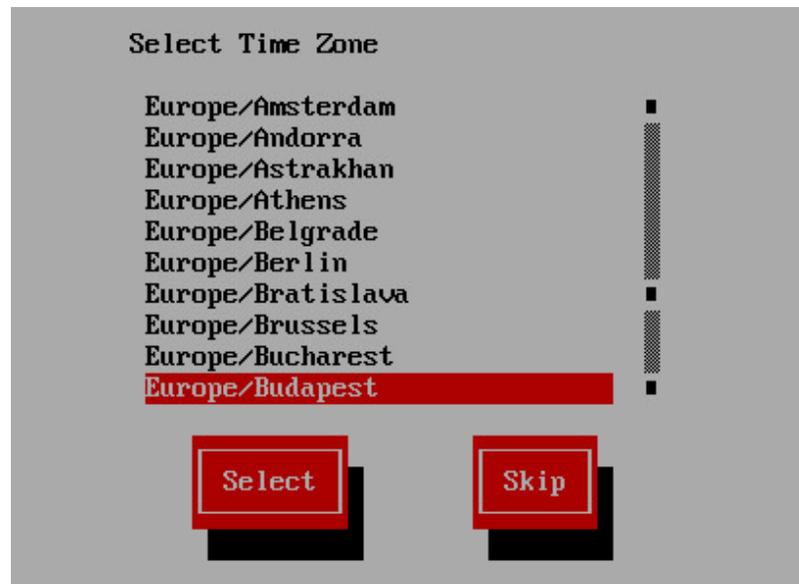
12. Fill in the IP details of management interface and hit **Enter** on **OK**



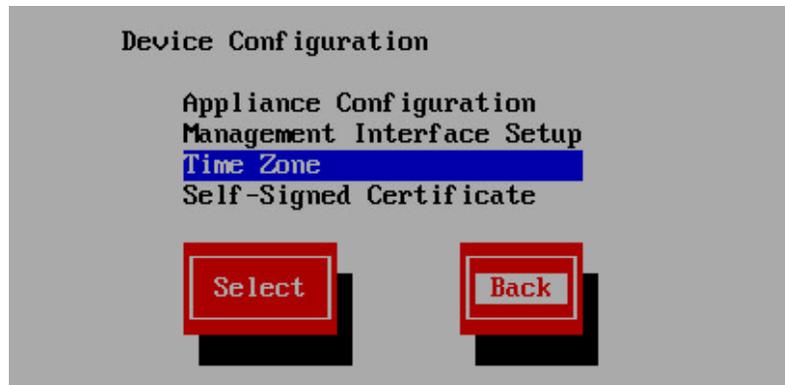
13. Select **Time Zone** and hit **Enter** on **Select**



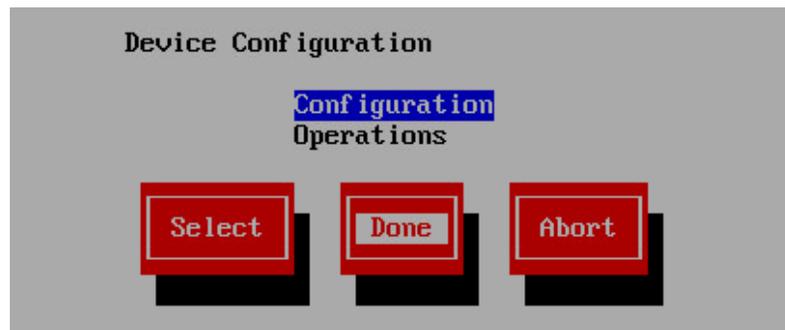
14. Select your time zone and hit **Enter** on **Select**



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

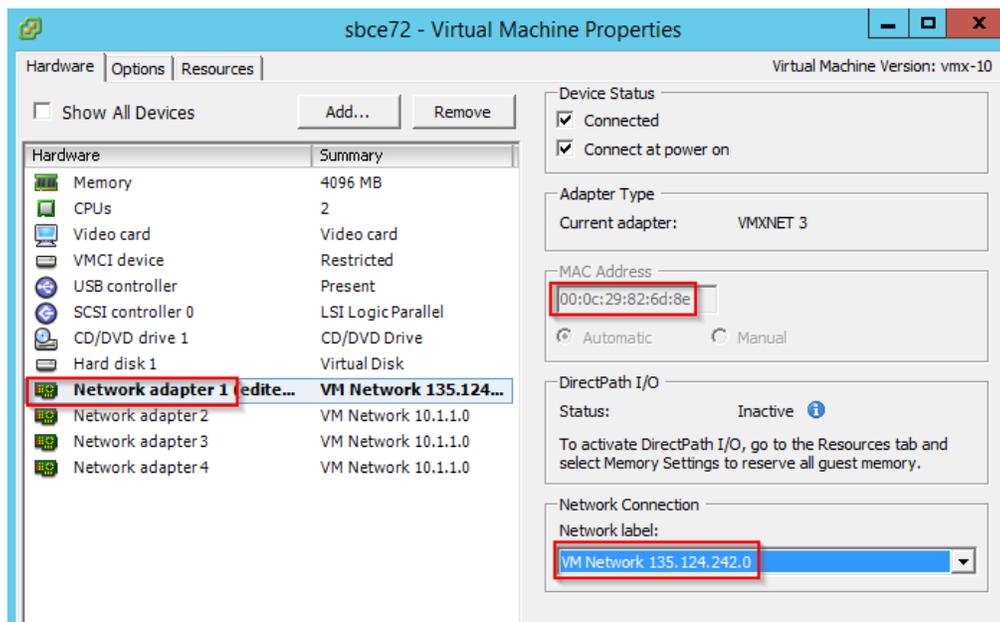
```

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

The screenshot shows a configuration wizard with four main sections:

- Device Configuration:** Appliance Name: sbce
- DNS Configuration:** Primary: 10.1.1.50, Secondary: (empty)
- License Allocation:** Standard Sessions: 0, Advanced Sessions: 0, Scopia Video Sessions: 0, CES Sessions: 0, Transcoding Sessions: 0, CLID: (empty), Encryption:
- Network Configuration:** Name: Internal, Default Gateway: 10.1.1.50, Subnet Mask or Prefix Length: 255.255.255.0, Interface: A1

Below the Network Configuration section, there is a table for IP addresses:

IP	Public IP	Gateway Override	DNS Client
Address #1: 10.1.1.40	Use IP Address	Use Default	<input checked="" type="radio"/>
Address #2: 10.1.1.41	Use IP Address	Use Default	<input type="radio"/>

- 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**

The screenshot shows the Licensing Configuration page with the following elements:

- Navigation tabs: Devices, Updates, SSL VPN, **Licensing**, Key Bundles
- Message: Virtualized EMSes can not run a local WebLM server. Avaya provides a separate OVA for running a virtualized WebLM server at no charge.
- Use Local WebLM Server:
- External WebLM Server URL: https://10.1.1.10:52233/WebLM/LicenseServer
- Save button

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**

The screenshot shows the 'Port Ranges' configuration page. At the top, there are tabs for 'Periodic Statistics', 'Feature Control', 'SIP Options', 'Network Options', 'Port Ranges', 'RTCP Monitoring', and 'Load Monitoring'. Below the tabs is a warning message: 'Changes to the settings below require an application restart before taking effect. Application restarts can be issued from System Management.' The main section is titled 'Port Range Configuration' and contains several rows of input fields:

- Signaling Port Range: 12000 - 21000
- Config Proxy Internal Signaling Port Range: 22000 - 31000
- Listen Port Range: 9500 - 9999 (The '9500' is highlighted with a red box)
- HTTP Port Range: 40001 - 50000

A 'Save' button is located at the bottom right of the configuration area.

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

The screenshot shows the 'CA Certificate' configuration page. It has a title 'CA Certificate' and four radio buttons: 'Create new', 'Renew existing' (which is selected), 'Import', and 'Export'. Below the radio buttons are three buttons: 'Regenerate', 'Download (PEM-encoded)' (which is highlighted with a red box), and 'Download (DER-encoded)'.

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

Identity Certificates

Renew automatically

Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

Create certificate for a different machine

Subject Name:

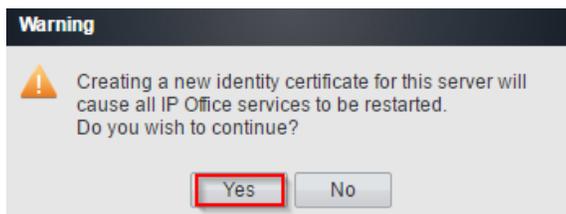
Subject Alternative Name(s):

Duration (days):

Public Key Algorithm:

Secure Hash Algorithm:

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

Identity Certificates

Renew automatically

Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

Create certificate for a different machine

Machine IP:

Password:

Confirm Password:

Subject Name:

Subject Alternative Name(s):

Duration (days):

Public Key Algorithm:

Secure Hash Algorithm:

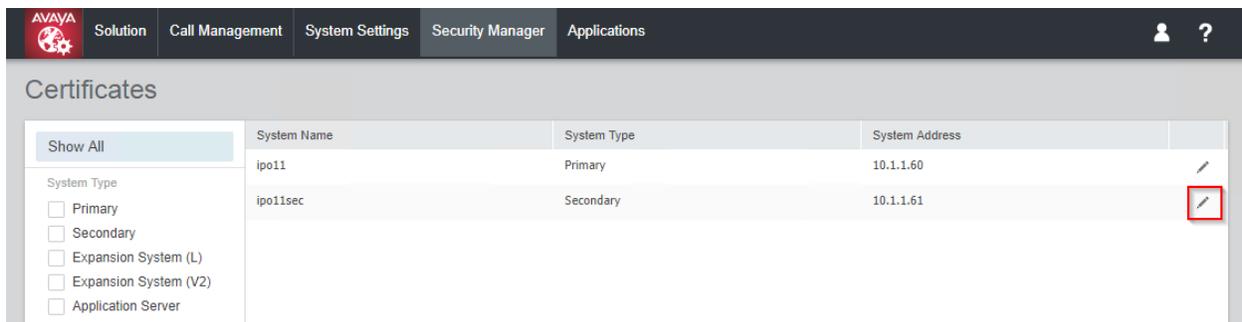
6. Click on the link in the popup window and save the file

Warning

 Certificate for node 10.1.1.61 created. Please use the link below to download it:
[server_10.1.1.61_1087330436.p12](#)
 Please note that the certificate will be deleted after this pop-up is closed.

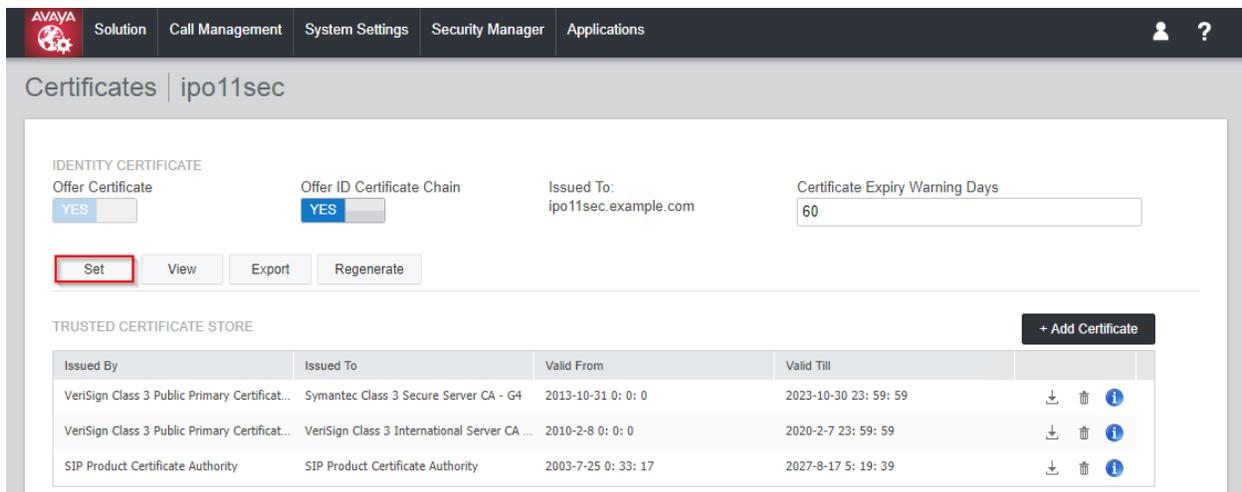
Installing Identity Certificate on Secondary Server

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



The screenshot shows the Avaya Security Manager interface. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security Manager', and 'Applications'. The main heading is 'Certificates'. On the left, there is a 'Show All' button and a 'System Type' filter with checkboxes for Primary, Secondary, Expansion System (L), Expansion System (V2), and Application Server. The main table lists certificates with columns for System Name, System Type, and System Address. Two entries are visible: 'ipo11' (Primary, 10.1.1.60) and 'ipo11sec' (Secondary, 10.1.1.61). A red box highlights the pencil icon in the rightmost column of the 'ipo11sec' row.

5. Click on **Set**



The screenshot shows the configuration page for the 'ipo11sec' certificate. The top navigation bar is the same as the previous screenshot. The main heading is 'Certificates | ipo11sec'. Below the heading, there are four sections: 'Offer Certificate' with a 'YES' button, 'Offer ID Certificate Chain' with a 'YES' button, 'Issued To: ipo11sec.example.com', and 'Certificate Expiry Warning Days' with a text input field containing '60'. Below these are buttons for 'Set', 'View', 'Export', and 'Regenerate'. A red box highlights the 'Set' button. At the bottom, there is a 'TRUSTED CERTIFICATE STORE' section with a '+ Add Certificate' button and a table of certificates.

Issued By	Issued To	Valid From	Valid Till	
VeriSign Class 3 Public Primary Certificat...	Symantec Class 3 Secure Server CA - G4	2013-10-31 0: 0: 0	2023-10-30 23: 59: 59	  
VeriSign Class 3 Public Primary Certificat...	VeriSign Class 3 International Server CA ...	2010-2-8 0: 0: 0	2020-2-7 23: 59: 59	  
SIP Product Certificate Authority	SIP Product Certificate Authority	2003-7-25 0: 33: 17	2027-8-17 5: 19: 39	  

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

Add Certificate

Select certificate file from local machine

C:\fakepath\server_10.1.1.61_1087: ...

Password

.....

Upload Cancel

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

Identity Certificates

Renew automatically

Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

Create certificate for a different machine

Machine IP:

Password:

Confirm Password:

Password complexity requirements:

- Minimum password length: 8
- Minimum number of uppercase characters: 1
- Minimum number of lowercase characters: 1
- Maximum allowed sequence length: 4

Subject Name:

Subject Alternative Name(s):

Duration (days):

Public Key Algorithm:

Secure Hash Algorithm:

Regenerate **Download (PEM-encoded)** **Download (DER-encoded)**

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



Identity Certificates

Renew automatically

Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

Create certificate for a different machine

Machine IP:

Password:

Confirm Password:

Password complexity requirements:

- Minimum password length: 8
- Minimum number of uppercase characters: 1
- Minimum number of lowercase characters: 1
- Maximum allowed sequence length: 4

Subject Name:

Subject Alternative Name(s):

Duration (days):

Public Key Algorithm:

Secure Hash Algorithm:

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**

Install Certificate X

Type: Certificate, CA Certificate, Certificate Revocation List

Name: IPO_RootCA

Overwrite Existing:

Allow Weak Certificate/Key:

Certificate File: Choose File IPO_RootCA.crt

Upload

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

Install Certificate X

Warning: The provided certificate is not a valid CA certificate, but is a valid self-signed certificate.

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**

Type	<input checked="" type="radio"/> Certificate <input type="radio"/> CA Certificate <input type="radio"/> Certificate Revocation List
Name	sbce_ipo11
Overwrite Existing	<input type="checkbox"/>
Allow Weak Certificate/Key	<input type="checkbox"/>
Certificate File	Choose File sbce_ipo11.pem
Trust Chain File	Choose File IPO_RootCA.crt
Key	<input type="radio"/> Use Existing Key from Filesystem <input checked="" type="radio"/> Upload Key File
Key File	Choose File sbce_ipo11.key
<input type="button" value="Upload"/>	

- Certificate will be displayed, click **Install**, then **Finish**
- Repeat the procedure for secondary

Type	<input checked="" type="radio"/> Certificate <input type="radio"/> CA Certificate <input type="radio"/> Certificate Revocation List
Name	sbce_ipo11sec
Overwrite Existing	<input type="checkbox"/>
Allow Weak Certificate/Key	<input type="checkbox"/>
Certificate File	Choose File sbce_ipo11sec.pem
Trust Chain File	Choose File IPO_RootCA.crt
Key	<input type="radio"/> Use Existing Key from Filesystem <input checked="" type="radio"/> Upload Key File
Key File	Choose File sbce_ipo11sec.key
<input type="button" value="Upload"/>	

- Ssh to SBCE **Management IP** using port **222** and **ipcs** login
- Issue command **su -** and type the root password
- 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**

TLS Profile

Profile Name: Client_ipo11

Certificate: sbce_ipo11.pem

Certificate Verification

Peer Verification: Required

Peer Certificate Authorities: IPO_RootCA.crt, IssuingCA.pem, RootCA.pem

Peer Certificate Revocation Lists: (empty)

Verification Depth: 1

Extended Hostname Verification:

Custom Hostname Override: (empty)

Next

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

Renegotiation Parameters

Renegotiation Time: 0 seconds

Renegotiation Byte Count: 0

Handshake Options

Version: TLS 1.2 TLS 1.1 TLS 1.0

Ciphers: Default FIPS Custom

Value (What's this?): HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

Back

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**

TLS Profile	
Profile Name	<input type="text" value="Server_ipo11"/>
Certificate	<input type="text" value="sbce_ipo11.pem"/>
Certificate Verification	
Peer Verification	<input type="text" value="None"/>
Peer Certificate Authorities	<input type="text" value="IPO_RootCA.crt
IssuingCA.pem
RootCA.pem"/>
Peer Certificate Revocation Lists	<input type="text"/>
Verification Depth	<input type="text" value="0"/>

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

Renegotiation Parameters	
Renegotiation Time	<input type="text" value="0"/> seconds
Renegotiation Byte Count	<input type="text" value="0"/>
Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input checked="" type="checkbox"/> TLS 1.1 <input checked="" type="checkbox"/> TLS 1.0
Ciphers	<input checked="" type="radio"/> Default <input type="radio"/> FIPS <input type="radio"/> Custom
Value <small>(What's this?)</small>	HIGH:!DH:!ADH:!MD5:!aNULL:!eNULL:@STRENGTH

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

Interface Name	VLAN Tag	Status
A1		Disabled
A2		Disabled
B1		Disabled

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

Name	Ext_Firewall_Pri
Default Gateway	10.2.2.1
Network Prefix or Subnet Mask	255.255.255.0
Interface	B1

IP Address	Public IP	Gateway Override	
10.2.2.2	135.124.242.20	Use Default	Delete

Name	Ext_Firewall_Sec
Default Gateway	10.3.3.1
Network Prefix or Subnet Mask	255.255.255.0
Interface	B1

IP Address	Public IP	Gateway Override	
10.3.3.2	135.124.242.21	Use Default	Delete

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**

Name	<input type="text" value="Int-RW-ipo11"/>
IP Address	<input type="text" value="Internal (A1, VLAN 0)"/> <input type="text" value="10.1.1.40"/>
Port Range	<input type="text" value="35000"/> - <input type="text" value="40000"/>

3. Repeat for secondary

Name	<input type="text" value="Int-RW-ipo11sec"/>
IP Address	<input type="text" value="Internal (A1, VLAN 0)"/> <input type="text" value="10.1.1.41"/>
Port Range	<input type="text" value="35000"/> - <input type="text" value="40000"/>

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

Name	<input type="text" value="Ext-FW-RW-ipo11"/>
IP Address	<input type="text" value="Ext_Firewall_Pri (B1, VLAN 0)"/> <input type="text" value="10.2.2.2"/>
Port Range	<input type="text" value="35000"/> - <input type="text" value="40000"/>

5. Repeat for secondary

Name	<input type="text" value="Ext-FW-RW-ipo11sec"/>
IP Address	<input type="text" value="Ext_Firewall_Sec (B1, VLAN 0)"/> <input type="text" value="10.3.3.2"/>
Port Range	<input type="text" value="35000"/> - <input type="text" value="40000"/>

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**

Name	<input type="text" value="Int-RW-ipo11"/>
IP Address	<input type="text" value="Internal (A1, VLAN 0)"/> <input type="text" value="10.1.1.40"/>
TCP Port	<input type="text"/>
UDP Port	<input type="text"/>
TLS Port	<input type="text" value="5061"/>
TLS Profile	<input type="text" value="Server_ipo11"/>
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	<input type="text"/>

3. Repeat for secondary

Name	<input type="text" value="Int-RW-ipo11sec"/>
IP Address	<input type="text" value="Internal (A1, VLAN 0)"/> <input type="text" value="10.1.1.41"/>
TCP Port	<input type="text"/>
UDP Port	<input type="text"/>
TLS Port	<input type="text" value="5061"/>
TLS Profile	<input type="text" value="Server_ipo11sec"/>
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	<input type="text"/>

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

Name	Ext-FW-RW-ipo11
IP Address	Ext_Firewall_Pri (B1, VLAN 0) 10.2.2.2
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	Server_ipo11
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

5. Repeat for secondary

Name	Ext-FW-RW-ipo11sec
IP Address	Ext_Firewall_Sec (B1, VLAN 0) 10.3.3.2
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	Server_ipo11sec
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

Finish

Server Profile

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

Profile Name	ipo11
--------------	-------

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**

Server Type	Call Server
SIP Domain	example.com
DNS Query Type	NONE/A
TLS Client Profile	Client_ipo11

IP Address / FQDN	Port	Transport	
10.1.1.60	5061	TLS	<input type="button" value="Delete"/>

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**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	avaya-ru
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None

9. Repeat the procedure for secondary

Profile Name	ipo11sec
--------------	----------

Server Type	Call Server
SIP Domain	example.com
DNS Query Type	NONE/A
TLS Client Profile	Client ipo11sec

IP Address / FQDN	Port	Transport	
10.1.1.61	5061	TLS	<input type="button" value="Delete"/>

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	avaya-ru
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061
Tolerant	<input type="checkbox"/>
URI Group	None

Routing

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

Profile Name	ipo11
--------------	-------

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

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ipo11	10.1.1.60:5061 (TLS)	None

Delete Finish

4. Repeat the procedure for secondary

Profile Name

Next

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	ipo11sec	10.1.1.61:5061 (TLS)	None

Delete Finish

Topology Hiding

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

Clone Profile X

Profile Name	default
Clone Name	<input type="text" value="IPO"/>

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**

Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Overwrite	example.com	Delete
Via	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
To	IP/Domain	Overwrite	example.com	Delete
Record-Route	IP/Domain	Auto		Delete
From	IP/Domain	Overwrite	example.com	Delete

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**

Criteria	
Flow Name	RW-ipo11
URI Group	*
User Agent	*
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	Ext-FW-RW-ipo11

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**

Profile	
Source	<input checked="" type="radio"/> Subscriber <input type="radio"/> Click To Call
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	Ext-FW-RW-ipo11
Secondary Media Interface	None
Received Interface	None
End Point Policy Group	avaya-def-low-enc
Routing Profile	ipo11
Optional Settings	
TLS Client Profile	None
Signaling Manipulation Script	None
Presence Server Address Ex: domain.com, 192.168.0.101	
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

5. Repeat the procedure for secondary

Criteria	
Flow Name	RW-ipo11sec
URI Group	*
User Agent	*
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	Ext-FW-RW-ipo11sec
<input type="button" value="Next"/>	

Profile	
Source	<input checked="" type="radio"/> Subscriber <input type="radio"/> Click To Call
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	Ext-FW-RW-ipo11sec ▼
Secondary Media Interface	None ▼
Received Interface	None ▼
End Point Policy Group	avaya-def-low-enc ▼
Routing Profile	ipo11sec ▼
Optional Settings	
TLS Client Profile	None ▼
Signaling Manipulation Script	None ▼
Presence Server Address Ex: domain.com, 192.168.0.101	<input type="text"/>
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

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**

Flow Name	<input type="text" value="ipo11"/>
Server Configuration	<input type="text" value="ipo11"/>
URI Group	<input type="text" value="*"/>
Transport	<input type="text" value="*"/>
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="Ext-FW-RW-ipo11"/>
Signaling Interface	<input type="text" value="Int-RW-ipo11"/>
Media Interface	<input type="text" value="Int-RW-ipo11"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="avaya-def-low-enc"/>
Routing Profile	<input type="text" value="default"/>
Topology Hiding Profile	<input type="text" value="IPO"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>

6. Repeat for secondary

Flow Name	<input type="text" value="ipo11sec"/>
Server Configuration	<input type="text" value="ipo11sec"/>
URI Group	<input type="text" value="*"/>
Transport	<input type="text" value="*"/>
Remote Subnet	<input type="text" value="*"/>
Received Interface	<input type="text" value="Ext-FW-RW-ipo11sec"/>
Signaling Interface	<input type="text" value="Int-RW-ipo11sec"/>
Media Interface	<input type="text" value="Int-RW-ipo11sec"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="avaya-def-low-enc"/>
Routing Profile	<input type="text" value="default"/>
Topology Hiding Profile	<input type="text" value="IPO"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>

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**

General Configuration	
Name	ipo11-5222
Service Type	Other

Remote Configuration	
Remote IP/FQDN	10.1.1.60
Remote Port	5222
Remote Transport	TCP

Device Configuration	
Listen IP	Ext_Firewall_Pri (B1, VLAN 0) 10.2.2.2
Listen Port	5222
Connect IP	Internal (A1, VLAN 0) 10.1.1.40
Listen Transport	TCP

Additional Configuration	
Whitelist Flows	<input type="checkbox"/>
Use Relay Actors	<input type="checkbox"/>
Options <small>Use Ctrl+Click to select or deselect multiple items.</small>	RTCP Monitoring End-to-End Rewrite Hop-by-Hop Traceroute Bridging

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

Parameter Name	Parameter Value
Profile Name	TURN
UDP Listen Port	3478
TCP/TLS Listen Port	
TLS Server Profile	None
Media Relay Port Range	50000 - 55000
Authentication	<input checked="" type="checkbox"/>
Client Authentication	<input type="checkbox"/>
Server Authentication	<input checked="" type="checkbox"/>
UserName	turnuser
Password
Confirm Password
Realm	example.com
FingerPrint	<input type="checkbox"/>
UDP Relay	<input checked="" type="checkbox"/>
TCP Relay	<input type="checkbox"/>
DTLS	<input type="checkbox"/>
Media Learning	<input type="checkbox"/>
Alternate Server1	
Alternate Server2	
Alternate Server3	

Finish

- 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**.

Listen IP	Media Relay IP	Service FQDN	TURN / STUN Profile
Internal (A1, VLAN 0)	Ext_Firewall_Pri (B1,		TURN
10.1.1.40	10.2.2.2		

Finish

3. Add TURN Relay for secondary

Listen IP	Media Relay IP	Service FQDN	TURN / STUN Profile
Internal (A1, VLAN 0)	Ext_Firewall_Sec (B1)		TURN
10.1.1.41	10.3.3.2		

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.

The screenshot shows the Avaya WebRTC Gateway configuration interface. The top navigation bar includes 'Solution', 'Call Management', 'System Settings', 'Security Manager', and 'Applications'. The main content area is titled 'WebRTC Gateway | ipo11' and has a 'WebRTC Configuration' dropdown menu. On the left, there is a sidebar with 'System Settings', 'SIP Server Settings', and 'Media Gateway Settings'. The main configuration area is titled 'MEDIA GATEWAY SETTINGS' and contains several sections:

- RTP Port Range (Private)**: Minimum 58002, Maximum 60002
- RTP Port Range (Public)**: Minimum 56000, Maximum 58000
- Codecs - Audio**: 1. PCMU, 2. PCMA, 3. telephone-event
- Codecs - Video**: 1. VP8
- DTMF Payload Type**: 101
- STUN Server Address**: 135 . 124 . 242 . 20
- STUN Server Port**: 3478
- TURN Server Address**: 10 . 1 . 1 . 40
- TURN Server Port**: 3478
- TURN User Name**: turnuser
- TURN Password**: [masked]
- Enforce TURN**: YES

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

WebRTC Gateway | ipo11

System Settings
SIP Server Settings
Media Gateway Settings

MEDIA GATEWAY SETTINGS

RTP Port Range (Private)

Minimum: 58002, Maximum: 60002

RTP Port Range (Public)

Minimum: 56000, Maximum: 58000

WebRTC Configuration

On Selected Server

- ipo11 10.1.1.60
- ipo11sec 10.1.1.61**

OK

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

WebRTC Gateway | ipo11sec

System Settings
SIP Server Settings
Media Gateway Settings

MEDIA GATEWAY SETTINGS

RTP Port Range (Private)

Minimum: 58002, Maximum: 60002

RTP Port Range (Public)

Minimum: 56000, Maximum: 58000

Codecs - Audio

- PCMU
- PCMA
- telephone-event

Codecs - Video

- VP8

DTMF Payload Type: 101

STUN Server Address: 135 . 124 . 242 . 21

STUN Server Port: 3478

TURN Server Address: 10 . 1 . 1 . 41

TURN Server Port: 3478

TURN User Name: turnuser

TURN Password:

Enforce TURN: YES

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:

- In **Settings / Server** set the followings:
 - 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=-7755f465afba5f877878b8c_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="ipoll.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@ipoll.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="ipollsec.example.com";
rfc2833_payload="101";
</ipo>
```

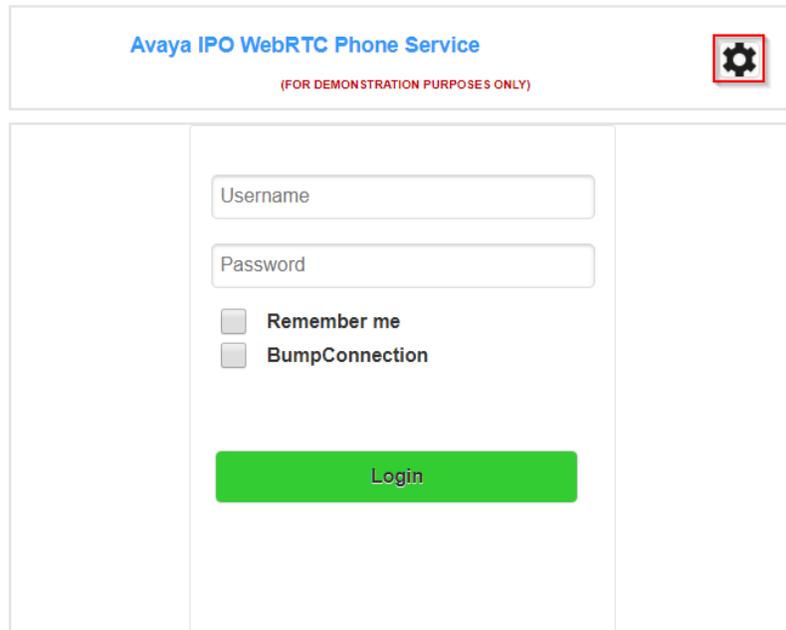
During failover the onex_server should contain the FQDN of Secondary One-X Portal and backup_ipoffice_server should contain 0.0.0.0.

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



Avaya IPO WebRTC Phone Service
(FOR DEMONSTRATION PURPOSES ONLY)

Username

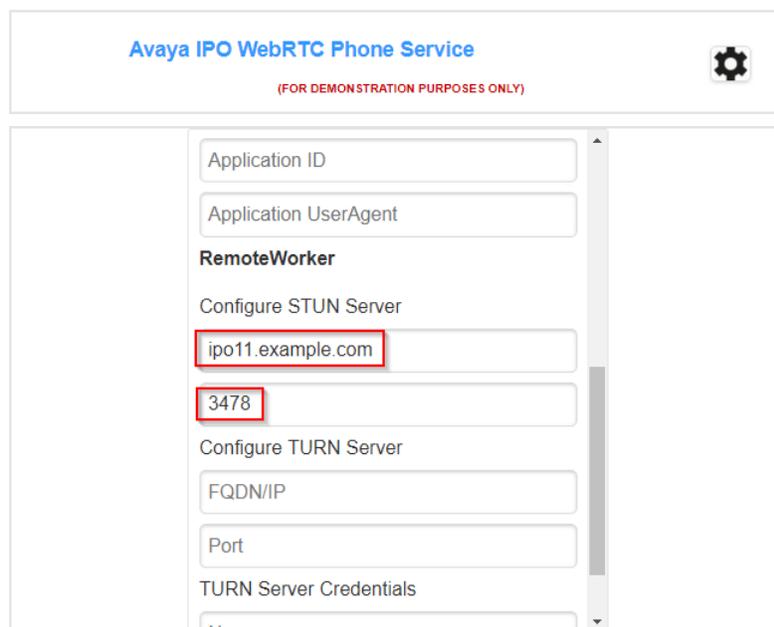
Password

Remember me

BumpConnection

Login

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



Avaya IPO WebRTC Phone Service
(FOR DEMONSTRATION PURPOSES ONLY)

Application ID

Application UserAgent

RemoteWorker

Configure STUN Server

ipo11.example.com

3478

Configure TURN Server

FQDN/IP

Port

TURN Server Credentials

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

Avaya IPO WebRTC Phone Service
(FOR DEMONSTRATION PURPOSES ONLY)

peter

.....

Remember me
 BumpConnection

Log In

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

Avaya IPO WebRTC Phone Service
(FOR DEMONSTRATION PURPOSES ONLY)

peter

1 2 3
4 5 6
7 8 9
* 0 #

Call Video

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**

AVAYA IP Office Web Client

USER NAME peter

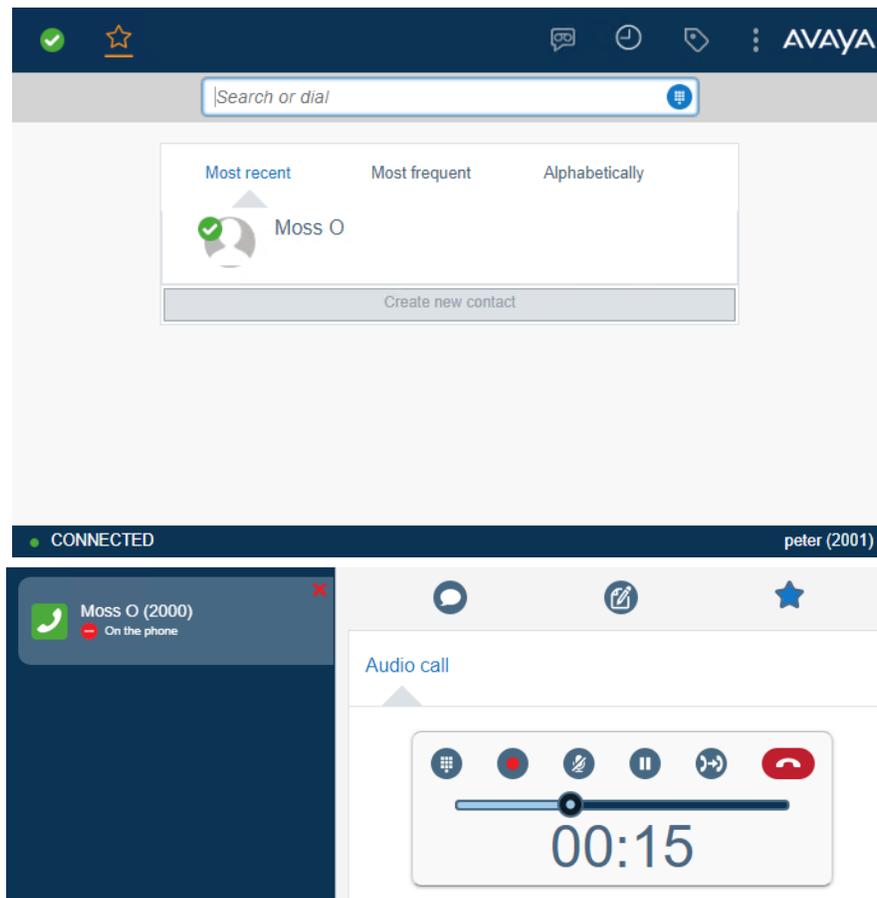
PASSWORD

LANGUAGE English ▾

Login Cancel

© 2018 Avaya Inc. All Rights Reserved
[View EULA](#)

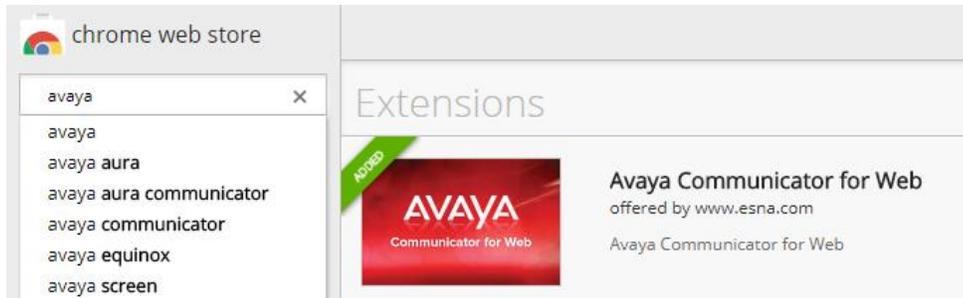
3. After successful login verify presence, then make a call to a local user either using Dialpad or by calling directly a contact.



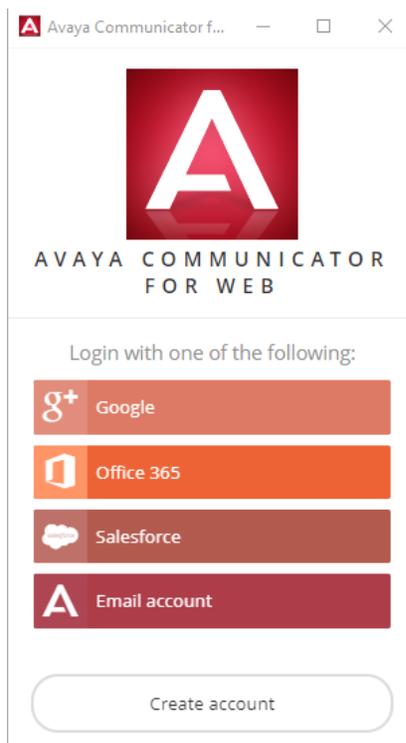
Avaya Communicator for Web

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.



AVAYA COMMUNICATOR FOR WEB

Presence server: ?

Media server(s): ?

User: ?

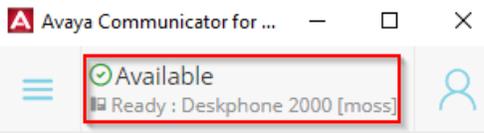
Password: ?

Save credentials ?

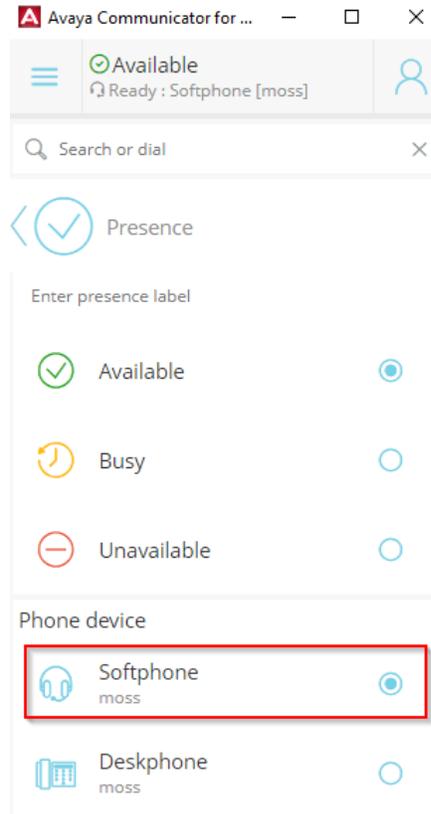
[Change account](#)

[CONNECT](#)

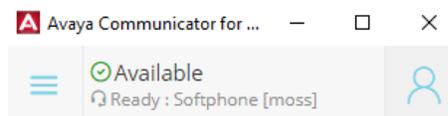
4. When logged in, click on presence status



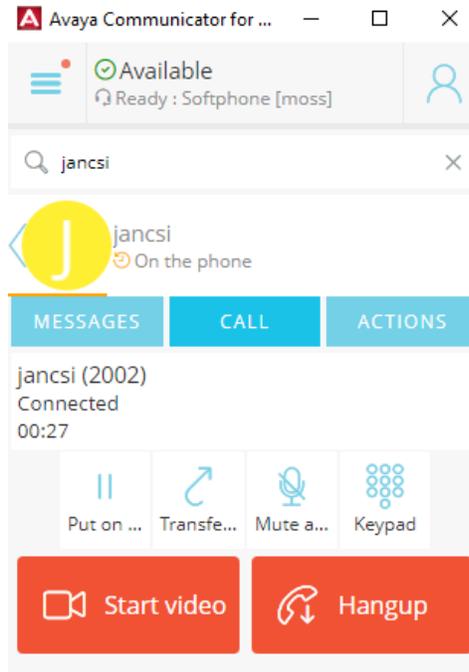
5. Change the Phone device to **Softphone**



6. Verify both presence and softphone is available/ready



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

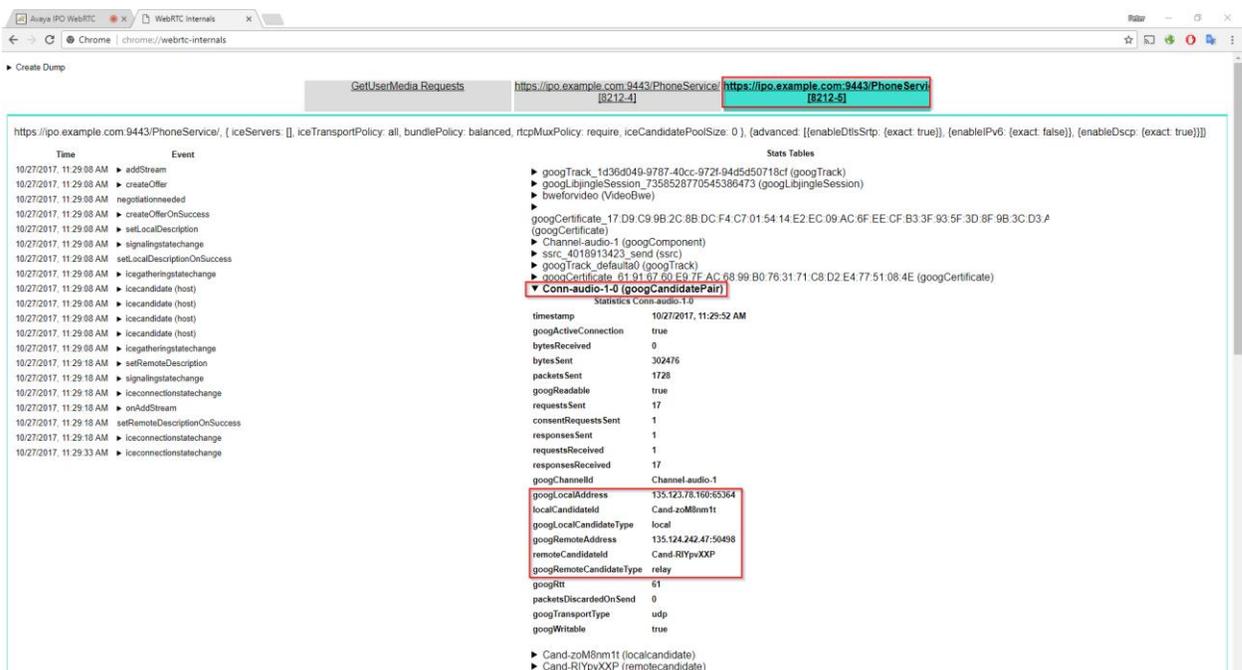


Troubleshooting tools

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 webrtc-internals and check the icecandidates, the connection, etc.



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



```
135.124.166.102      10.1.1.60      10.0.2.15
SBC
09:40:31.891  ←BindReq→
09:40:31.892  ←BindSuc←
09:40:37.981  ←TurnAll←
09:40:37.982  →TurnAll→
09:40:37.983  ←TurnAll←
09:40:37.984  →TurnAll→
09:40:38.027  ←Channel←
09:40:38.027  →Channel→
09:40:38.027  ←Channel←
09:40:38.027  →Channel→
09:40:38.048  ←Channel←
09:40:38.048  →Channel→
09:40:38.048  ←Channel←
09:40:38.048  →Channel→
09:40:38.079  ←BindReq→
09:40:38.079  →BindSuc←
09:40:38.079  ←Channel←
09:40:38.079  →Channel→
09:40:38.079  ←BindReq→
09:40:38.079  →BindSuc←
09:40:38.080  ←Channel←
09:40:38.080  →Channel→
09:40:38.128  ←BindReq→
09:40:38.128  →BindSuc←
09:40:38.130  ←Channel←
09:40:38.130  →Channel→
09:40:38.183  ←BindReq→
09:40:38.183  →BindSuc←
09:40:38.184  ←Channel←
09:40:38.184  →Channel→
09:40:39.346  ←BindReq→
09:40:39.346  →BindSuc←
09:40:39.346  ←Channel←
09:40:39.346  →Channel→
09:40:40.383  ←BindReq→
09:40:40.383  →BindSuc←
09:40:40.383  ←Channel←
09:40:40.383  →Channel→
09:40:41.898  ←BindReq→
09:40:41.898  →BindSuc←
09:40:42.983  ←BindReq→
09:40:42.983  →BindSuc←
09:40:42.984  ←Channel←
09:40:42.984  →Channel→
09:40:45.509  ←Refresh←
09:40:45.509  →Refresh→
09:40:45.529  ←ICMP←
09:40:45.539  →BindReq→
09:40:45.539  ←Channel←
09:40:45.539  →ICMP→

STUN: Binding Request
STUN: Binding Success 135.124.166.102:64749 135.124.166.102:64749 10.2.2.2:3478 10.2.2.2:3479
STUN: Allocate Request turnuser
STUN: Allocate Error 401 Unauthorised
STUN: Allocate Request turnuser
STUN: Allocate Success 135.124.242.20:50327 10.1.1.60:56094
STUN: ChannelBind Request 10.0.2.15:56819 0x4000 turnuser
STUN: ChannelData 0x4000 Binding Request ICE-CONTROLLED fYxM:rVV42x3K
STUN: ChannelBind Success
STUN: Binding Request ICE-CONTROLLED fYxM:rVV42x3K
STUN: ChannelBind Request 135.124.166.102:64749 0x4001 turnuser
STUN: ChannelBind Success
STUN: ChannelData 0x4001 Binding Request ICE-CONTROLLED fYxM:rVV42x3K
STUN: Binding Request ICE-CONTROLLED fYxM:rVV42x3K
STUN: ChannelData 0x4001 Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Request ICE-CONTROLLED fYxM:rVV42x3K
STUN: Binding Request ICE-CONTROLLED fYxM:rVV42x3K
STUN: ChannelData 0x4001 Binding Success 135.124.166.102:64749
STUN: Binding Success 135.124.166.102:64749
STUN: Binding Success 135.124.242.20:50327
STUN: ChannelData 0x4001 Binding Success 135.124.242.20:50327
STUN: Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Success 135.124.166.102:64749
STUN: Binding Success 135.124.166.102:64749
STUN: Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Success 135.124.166.102:64749
STUN: Binding Success 135.124.166.102:64749
STUN: Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Success 135.124.166.102:64749
STUN: Binding Success 135.124.166.102:64749
STUN: Binding Request
STUN: Binding Success 135.124.166.102:64749 135.124.166.102:64749 10.2.2.2:3478 10.2.2.2:3479
STUN: Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Success 135.124.166.102:64749
STUN: Binding Success 135.124.166.102:64749
STUN: Refresh Request turnuser
STUN: Refresh Success
Destination unreachable (Port unreachable)
STUN: Binding Request rVV42x3K:fYxM ICE-CONTROLLING
STUN: ChannelData 0x4001 Binding Request rVV42x3K:fYxM ICE-CONTROLLING
Destination unreachable (Port unreachable)

Capture filter: <NO FILTER>
Display filter: <NO FILTER>
SIP FPM STUN TLS WEBRTC AMS
s=Stop q=Quit ENTER=Details (f=Filters a=ApplySession e=Erase w=Write c=Clear
```

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**

Avaya IPO WebRTC Phone Service

(FOR DEMONSTRATION PURPOSES ONLY)

Settings
Cancel
Save

Service Type

PhoneService

Configure Signal Gateway

FQDN/IP

Enable Video

Enable Logs

RemoteWorker

Avaya IPO WebRTC Phone Service

(FOR DEMONSTRATION PURPOSES ONLY)

peter

Settings
Cancel
Save

1 2 3

4 5 6

7 8 9

* 0 #

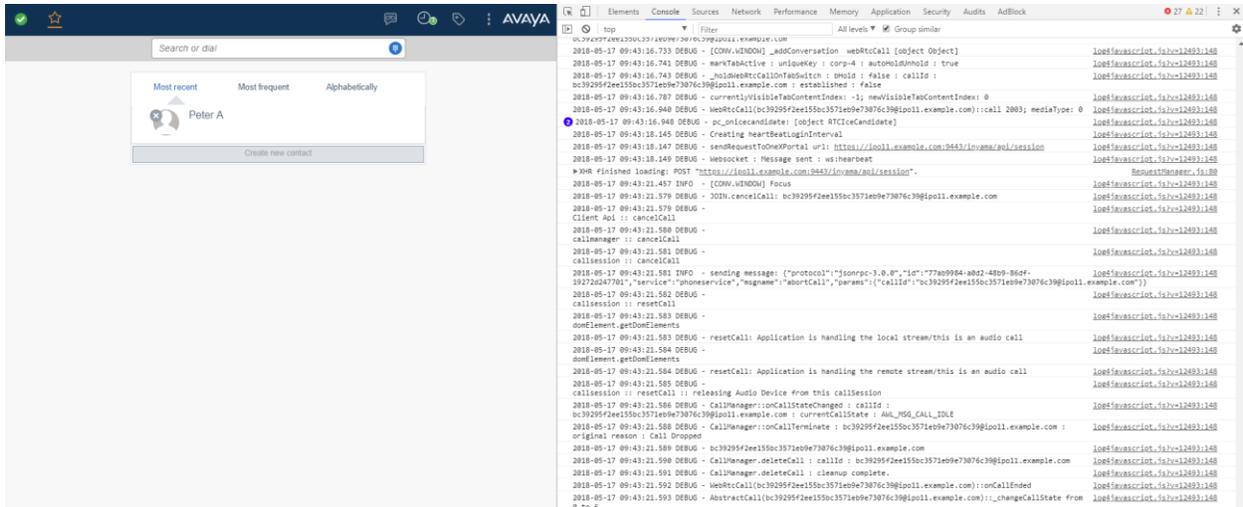
📞 📠

```

Elements Console Sources Network Performance Memory Application Security Audits AdBlock
  Filter
  All levels Group similar
  listener registered for event: phoneservice.GatewayURLNodeChanged
  sending message: {"protocol":"jsonrpc-3.0.0","id":"b355440f-e5d6-4962-972e-d13f8f3e808b","service":"phoneservice","msname":"getGatewaySettings","params":{"type":"all"}}
  ***DEBUG*** ApplicationInstanceID: 2497009086
  sending message: {"protocol":"jsonrpc-3.0.0","id":"1480804d-79ec-4d5c-9ec3-25210836d50","service":"phoneservice","msname":"login","params":{"applicationID":"phoneservice-11.0","applicationUA":"AHLTestClient-3.0.0","applicationInstanceID":"2497009086","userID":"peter","authType":"password","authToken":null,"bumpConnection":"false"}}
  handleIncomingMsg: {"protocol":"jsonrpc-3.0.0","service":"phoneservice","id":"b355440f-e5d6-4962-972e-d13f8f3e808b","msname":"gatewaySettingsResponse","params":{"responseCode":"200","responseString":"OK","codec":{"dsterPayload":"101"},"nat":{"stun":{"serverAddr":"135.124.242.20","serverPort":"3478"},"turn":{"serverAddr":"10.1.1.61","serverPort":"3478","username":"turnuser","password":"Avaya1234","enforce":"true"},"other":{"gatewayVersion":"Avaya webRTC 713dev","dscp":"184-184"}}}}
  gatewaySettingsResponseHandler: Success
  OTMP Payload:101
  Stun details : {
    "ip": "135.124.242.20",
    "port": "3478"
  }
  Turn details : {
    "ip": "10.1.1.61",
    "port": "3478",
    "user": "turnuser"
  }
  Enforce Turn : true
  Gateway Version :Avaya webRTC 713dev
  DSCP :184-184
  set STUN configuration:
  Stunserver url {
    "url": "stun:135.124.242.20:3478"
  }
  handleIncomingMsg: {"protocol":"jsonrpc-3.0.0","service":"phoneservice","id":"1480804d-79ec-4d5c-9ec3-25210836d50","msname":"loginResponse","params":{"responseCode":"200","responseString":"OK","loginSessionData":{"natData":{"notSupported":true,"natMethod":"NAT_FALLBACK","natFallbackLine":"100","backUpData":{"serverType":"IPOL_SECONDARY","address":"10.1.1.61","domain":"ipolsec.example.com","port":"9443"}}}}}}
  Registration_11_0version: evtLoginStatusHandler - Registration successful
  config.getConfiguration
  config.getConfiguration
  Registration_11_0version: Authentication token will be renewed in 176.9 minutes
  onRegistrationStateChange :: RESULT = AHL_MSG_LOGIN_SUCCESS
  onRegistrationStateChange :: reason = SIP registration success
  IPaddress:ipol.example.com
  Client Api :: _getAlternateServerConfig
  
```

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

