Administering Avaya IP Office 9.1 and Avaya Session Border Controller for Enterprise 7.0 to support Avaya Communicator and Avaya One-X Mobile Preferred as Remote Workers

Abstract

This document provides step-by-step instructions about how to configure IP Office 9.1 (IPO) and Avaya Session Border Controller for Enterprise 7.0 (SBCE) to support different SIP 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 and Avaya One-X Mobile Preferred (Android and IOS) in VoIP mode using signaling and media encryption, and to have Presence and Instant Messaging on them in an IP Office / SBCE environment.

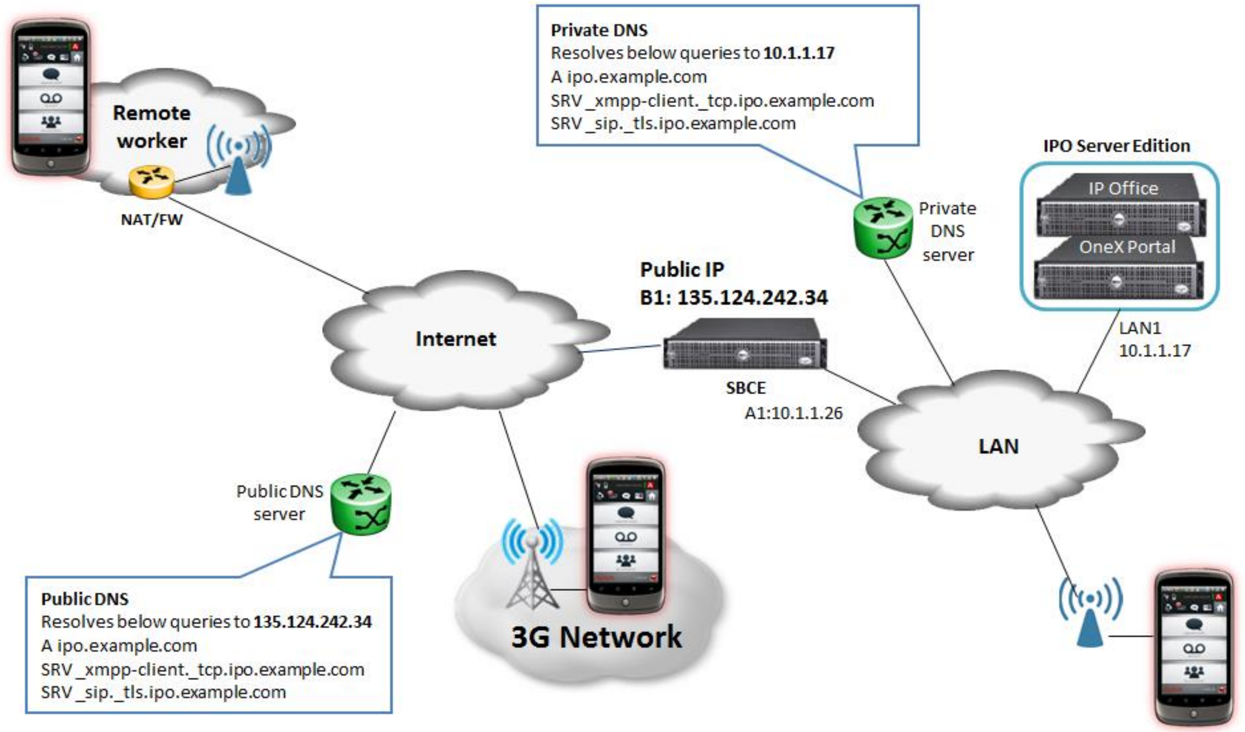
Issue 1.0

23 February 2016

Contents

Overview

A typical deployment with SBCE 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. In this case the simplest configuration is to use the FQDN of the IPO Server Edition Virtual Machine for both the XMPP domain on OneX Portal component and SIP domain on IPO, then create DNS A and DNS SRV records for this FQDN on the private and public DNS servers.

Prerequisites

VMware

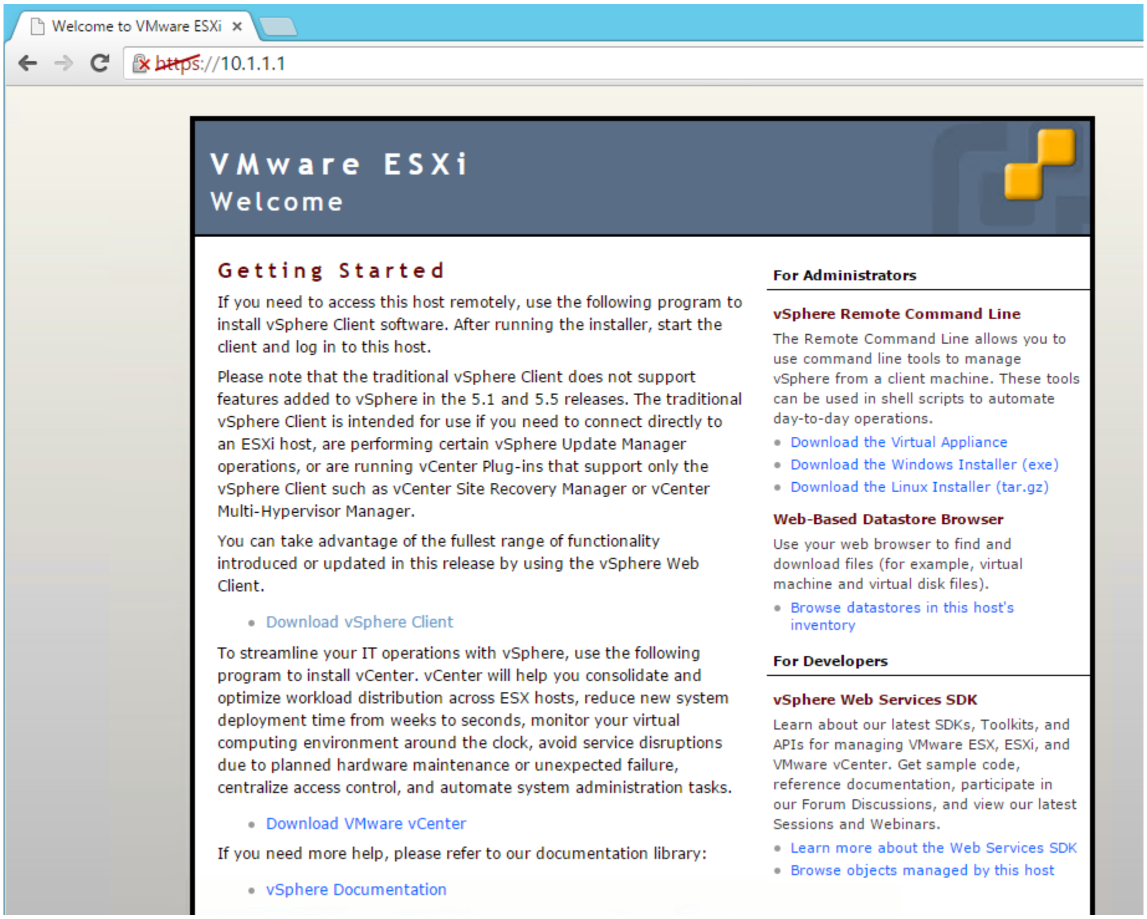
VMware ESXi deployment is out of the scope of this document. The assumption is that VMware environment or Avaya Virtualization Platform (AVP) has already been deployed.

WebLM

Virtualized SBCE requires external WebLM server for licensing. Installation of this server is out of scope of this document. Deploy new WebLM server or reuse any existing.

vSphere Client

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



VMware ESXi
Welcome

Getting Started

If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.

Please note that the traditional vSphere Client does not support features added to vSphere in the 5.1 and 5.5 releases. The traditional vSphere Client is intended for use if you need to connect directly to an ESXi host, are performing certain vSphere Update Manager operations, or are running vCenter Plug-ins that support only the vSphere Client such as vCenter Site Recovery Manager or vCenter Multi-Hypervisor Manager.

You can take advantage of the fullest range of functionality introduced or updated in this release by using the vSphere Web Client.

- Download vSphere Client

To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.

- Download VMware vCenter

If you need more help, please refer to our documentation library:

- vSphere Documentation

For Administrators

vSphere Remote Command Line

The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.

- Download the Virtual Appliance
- Download the Windows Installer (exe)
- Download the Linux Installer (tar.gz)

Web-Based Datastore Browser

Use your web browser to find and download files (for example, virtual machine and virtual disk files).

- Browse datastores in this host's inventory

For Developers

vSphere Web Services SDK

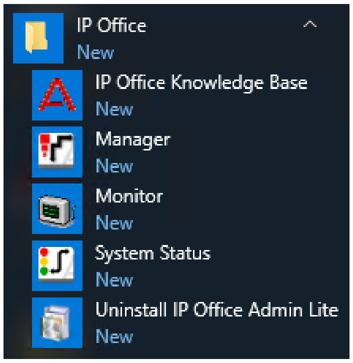
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.

- Learn more about the Web Services SDK
- Browse objects managed by this host

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

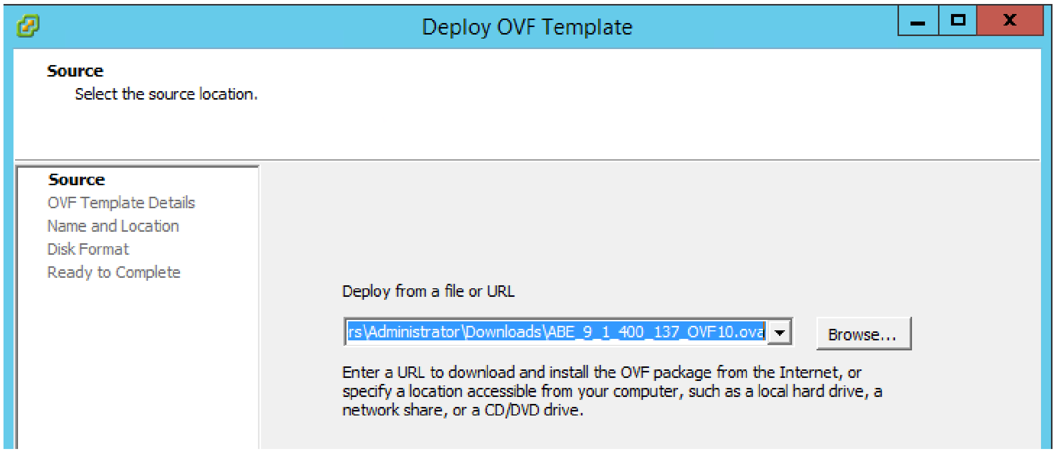
IP Office Administration Tools

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:



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**



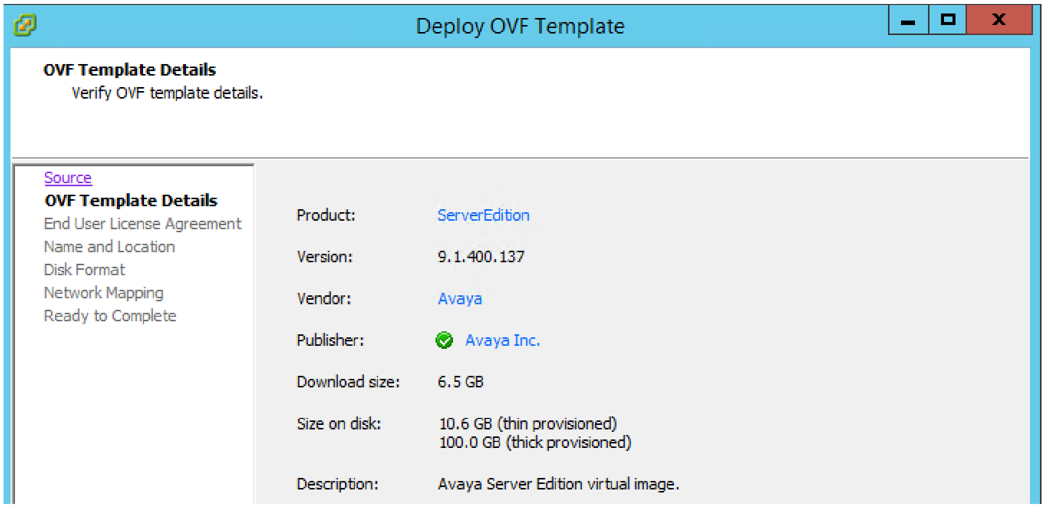
Source
Select the source location.

Deploy from a file or URL

rs\Administrator\Downloads\ABE_9_1_400_137_OVF10.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

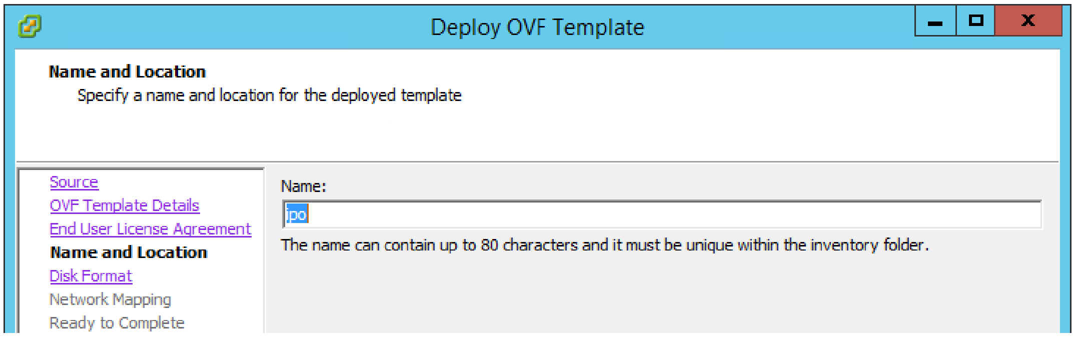
5. Click **Next**



OVF Template Details
Verify OVF template details.

Product:	ServerEdition
Version:	9.1.400.137
Vendor:	Avaya
Publisher:	✓ Avaya Inc.
Download size:	6.5 GB
Size on disk:	10.6 GB (thin provisioned) 100.0 GB (thick provisioned)
Description:	Avaya Server Edition virtual image.

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



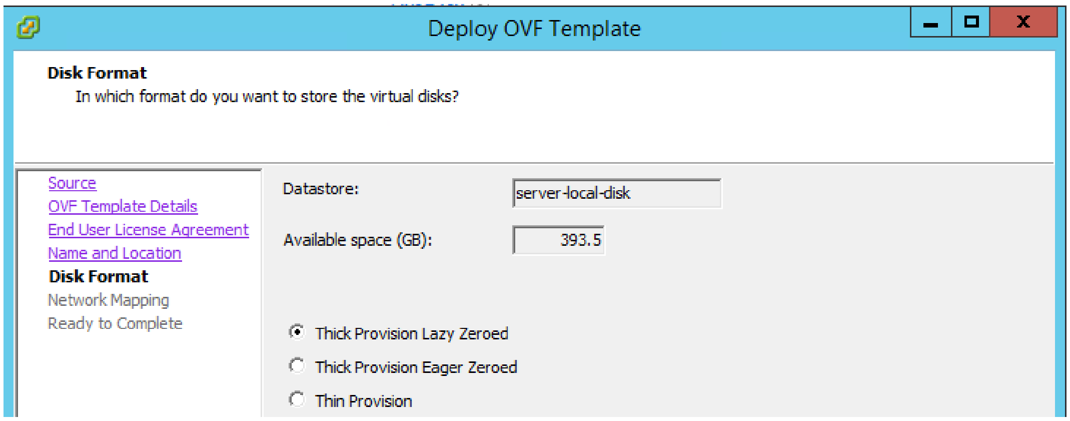
Name and Location

Specify a name and location for the deployed template

Name: ipo

The name can contain up to 80 characters and it must be unique within the inventory folder.

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



Disk Format

In which format do you want to store the virtual disks?

Datastore: server-local-disk

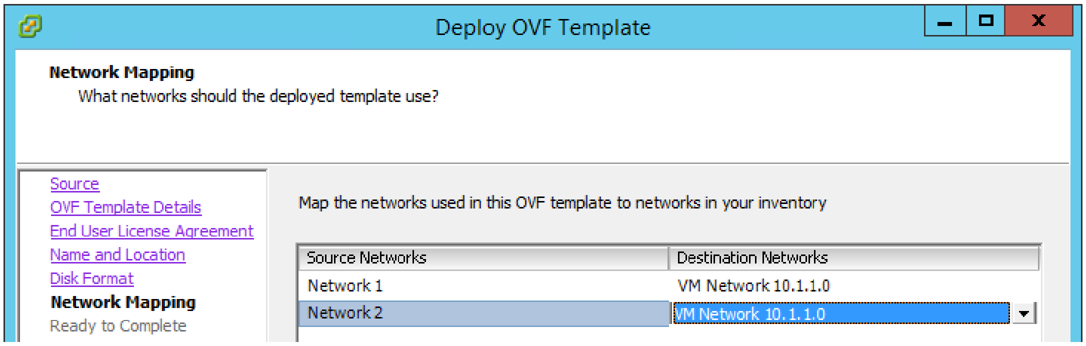
Available space (GB): 393.5

● Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

○ Thin Provision

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



Network Mapping

What networks should the deployed template use?

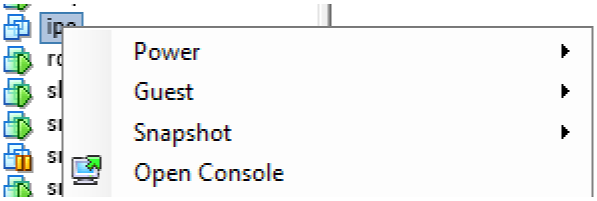
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Network 1	VM Network 10.1.1.0
Network 2	VM Network 10.1.1.0

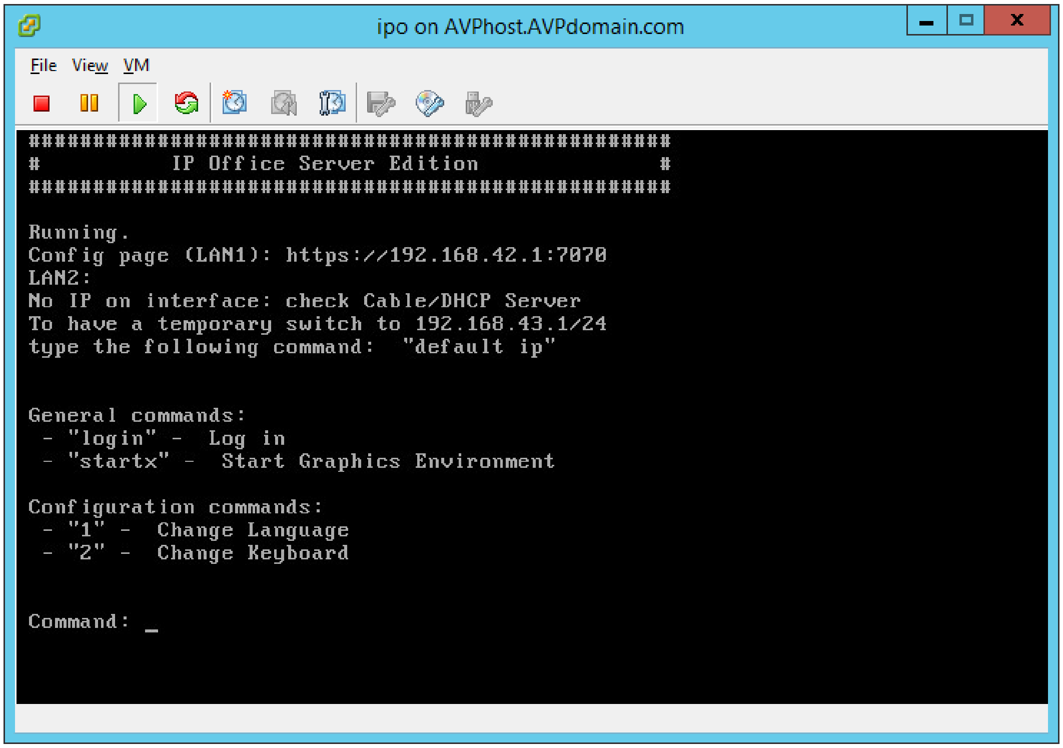
11. Wizard will display the summary, click **Finish**
12. Once deployment has completed, the new virtual machine appears in the inventory of virtual machines. Select the virtual machine and start it.

Changing default IP

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

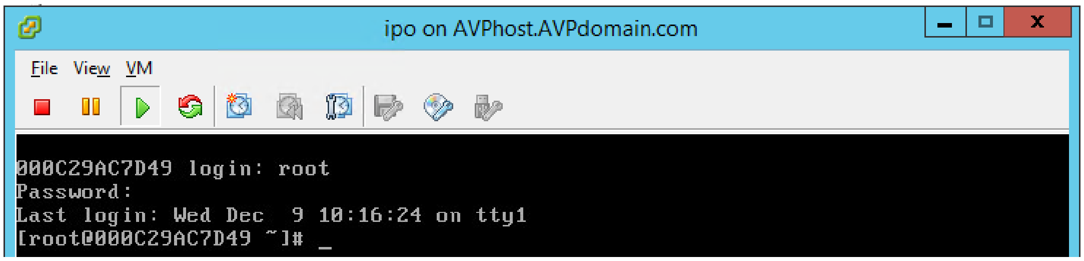


2. If this is the first boot, wait for the virtual machine to boot up until the following can be seen in the console window



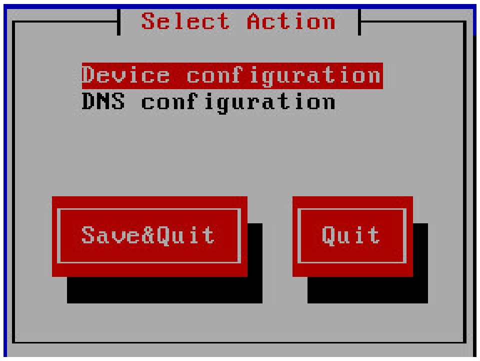
```
####################################################
#              IP Office Server Edition            #
####################################################

Running.
Config page (LAN1): https://192.168.42.1:7070
LAN2:
No IP on interface: check Cable/DHCP Server
To have a temporary switch to 192.168.43.1/24
type the following command:  "default ip"


General commands:
 - "login" -  Log in
 - "startx" -  Start Graphics Environment

Configuration commands:
 - "1" -  Change Language
 - "2" -  Change Keyboard


Command: _
```

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**

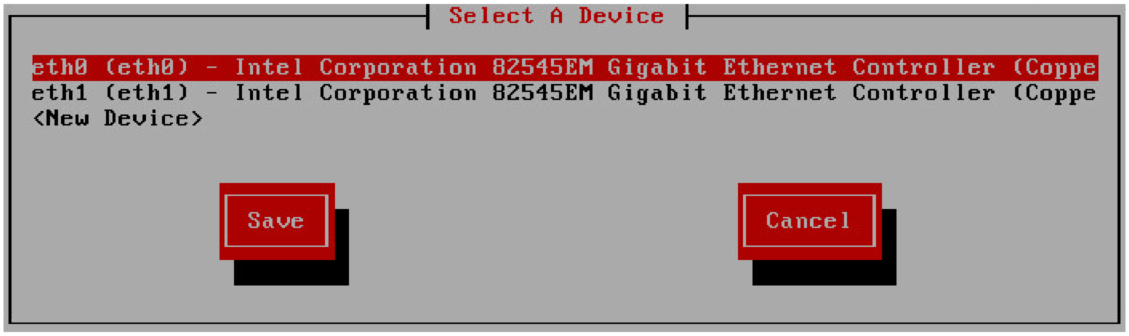


```
000C29AC7D49 login: root
Password:
Last login: Wed Dec  9 10:16:24 on tty1
[root@000C29AC7D49 ~]# _
```

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**

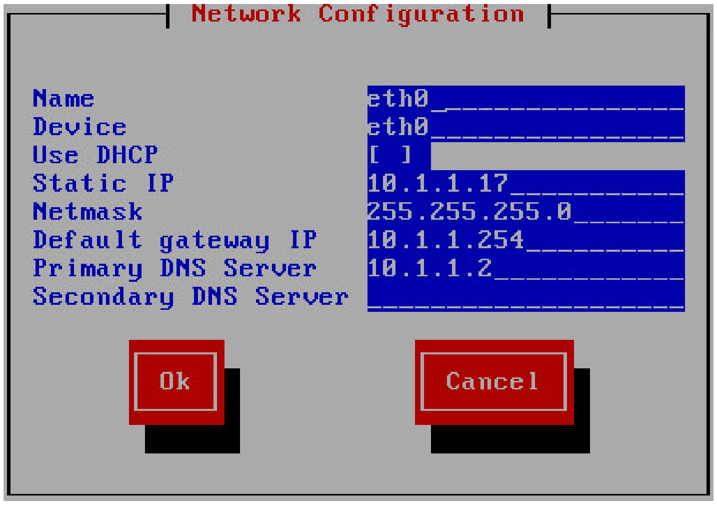


8. Select the network interface to configure and press **Enter**



```
Select A Device

eth0 (eth0) - Intel Corporation 82545EM Gigabit Ethernet Controller (Coppe
eth1 (eth1) - Intel Corporation 82545EM Gigabit Ethernet Controller (Coppe
<New Device>
```

9. Enter network parameters for the interface

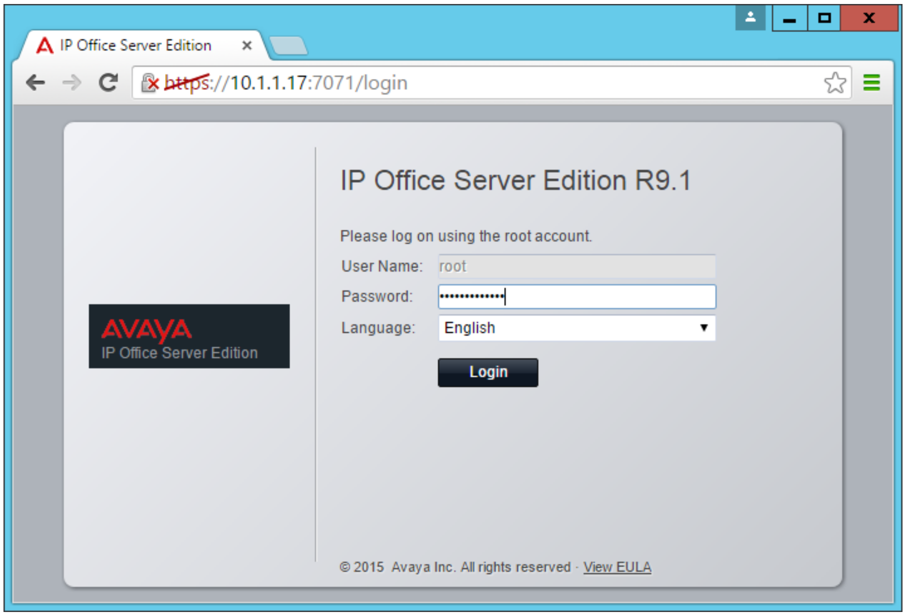


```
Network Configuration

Name                    eth0_________________
Device                  eth0_________________
Use DHCP                [ ]
Static IP               10.1.1.17____________
Netmask                 255.255.255.0________
Default gateway IP      10.1.1.254___________
Primary DNS Server      10.1.1.2_____________
Secondary DNS Server    _____________________
```

10. Select **OK** and press **Enter**
11. Select **Save** and press **Enter**
12. Select **Save & Quit** and press **Enter**
13. Enter the command **service network restart**
14. To logout, enter **exit**
15. Power off and then power on the virtual machine again

Server Ignition

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



IP Office Server Edition R9.1

Please log on using the root account.

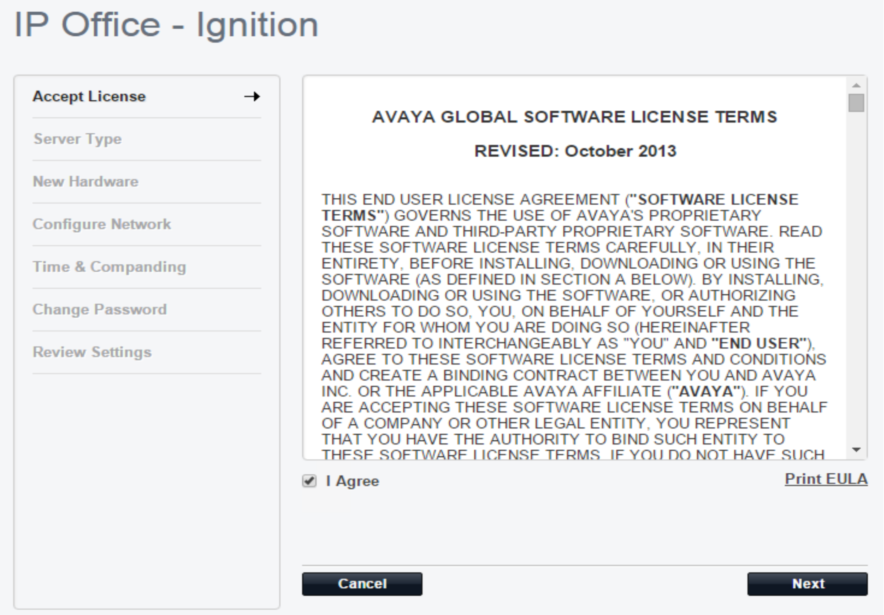
User Name: root

Password: ••••••••••••

Language: English

© 2015 Avaya Inc. All rights reserved · View EULA

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



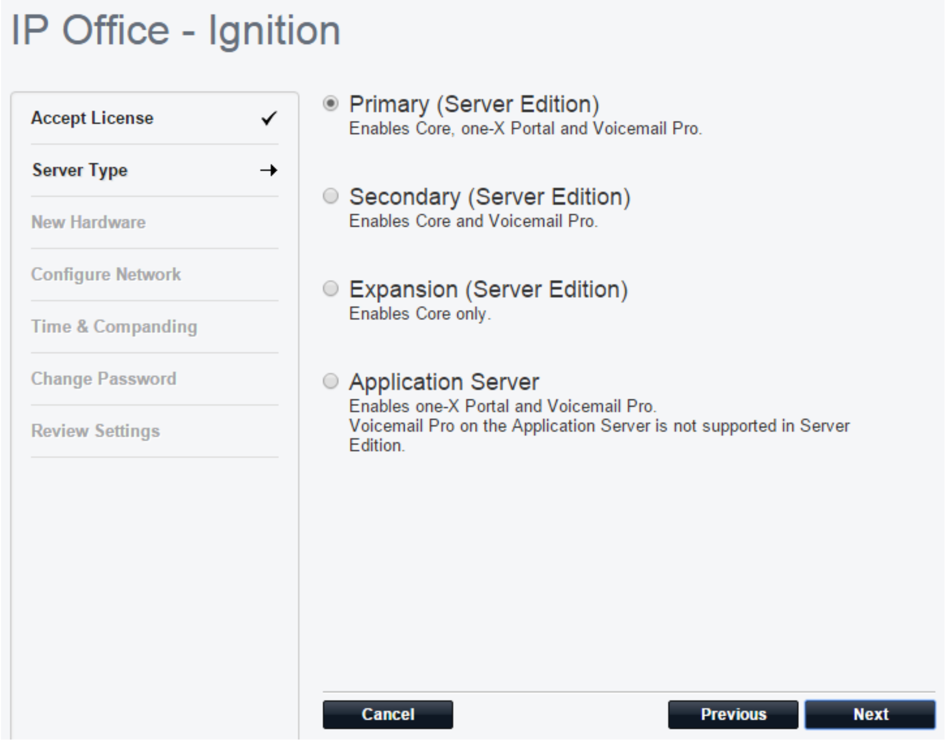
AVAYA GLOBAL SOFTWARE LICENSE TERMS

REVISED: October 2013

THIS END USER LICENSE AGREEMENT (**"SOFTWARE LICENSE TERMS"**) GOVERNS THE USE OF AVAYA'S PROPRIETARY SOFTWARE AND THIRD-PARTY PROPRIETARY SOFTWARE. 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" 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 LICENSE TERMS. IF YOU DO NOT HAVE SUCH

☑ I Agree

4. Select Primary (Server Edition) and click Next



IP Office - Ignition

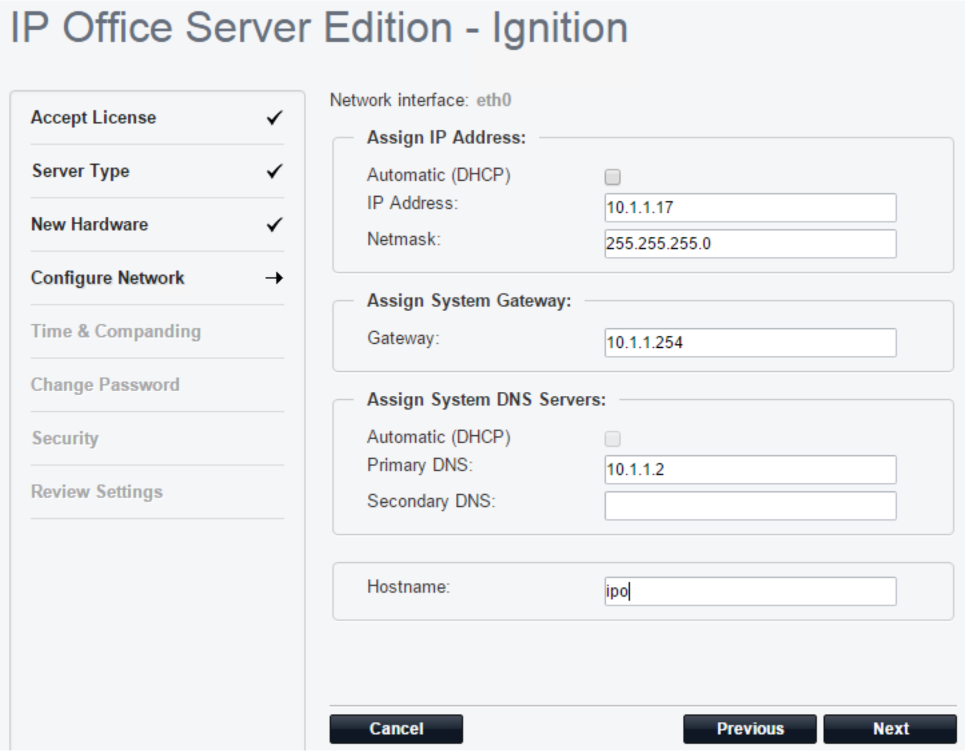
● Primary (Server Edition)
Enables Core, one-X Portal and Voicemail Pro.

○ Secondary (Server Edition)
Enables Core 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.

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



IP Office Server Edition - Ignition

Network interface: eth0

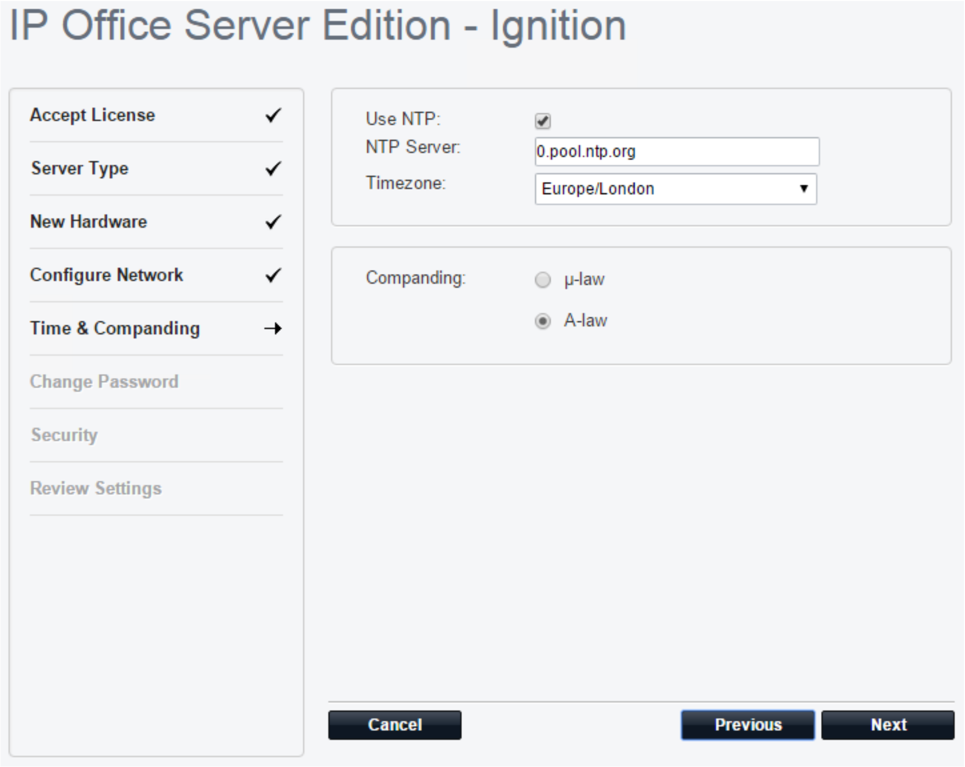
Assign IP Address:
Automatic (DHCP) □
IP Address: 10.1.1.17
Netmask: 255.255.255.0

Assign System Gateway:
Gateway: 10.1.1.254

Assign System DNS Servers:
Automatic (DHCP) □
Primary DNS: 10.1.1.2
Secondary DNS:

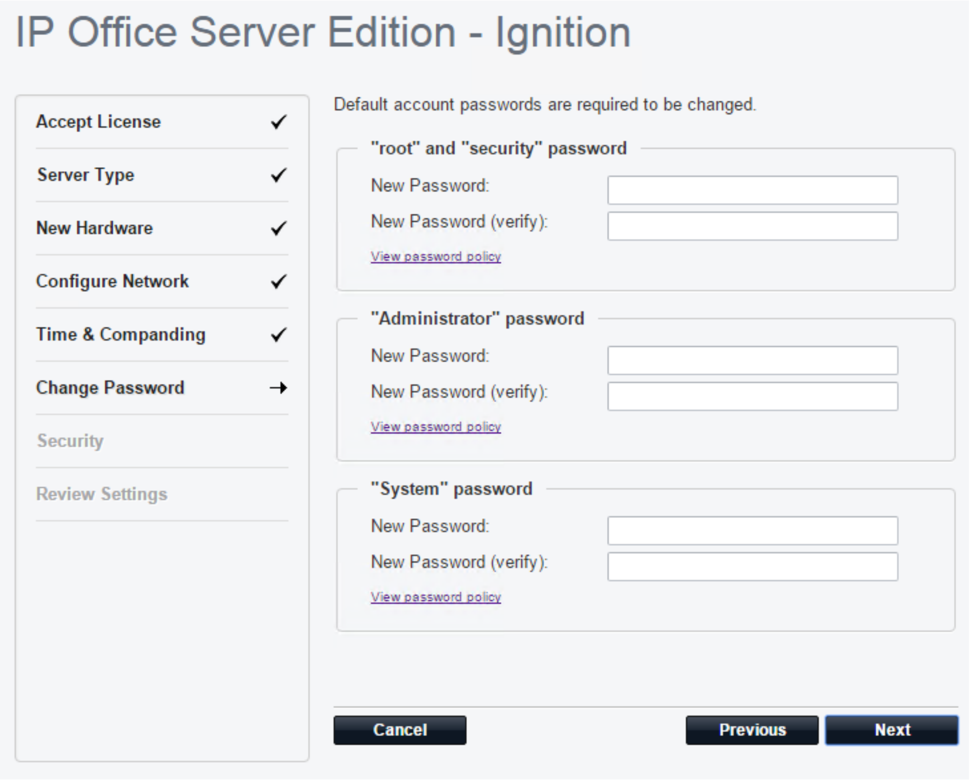
Hostname: ipo

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



Use NTP: ☑
NTP Server: 0.pool.ntp.org
Timezone: Europe/London
Companding: ○ µ-law ● A-law

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



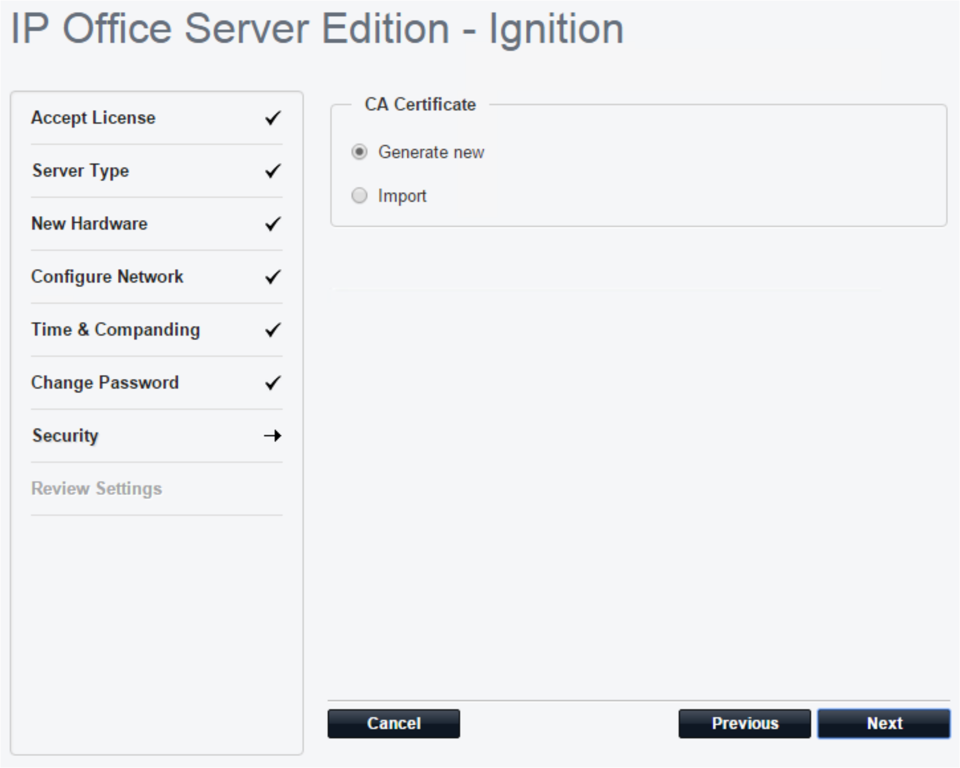
Default account passwords are required to be changed.

"root" and "security" password
New Password:
New Password (verify):

"Administrator" password
New Password:
New Password (verify):

"System" password
New Password:
New Password (verify):

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

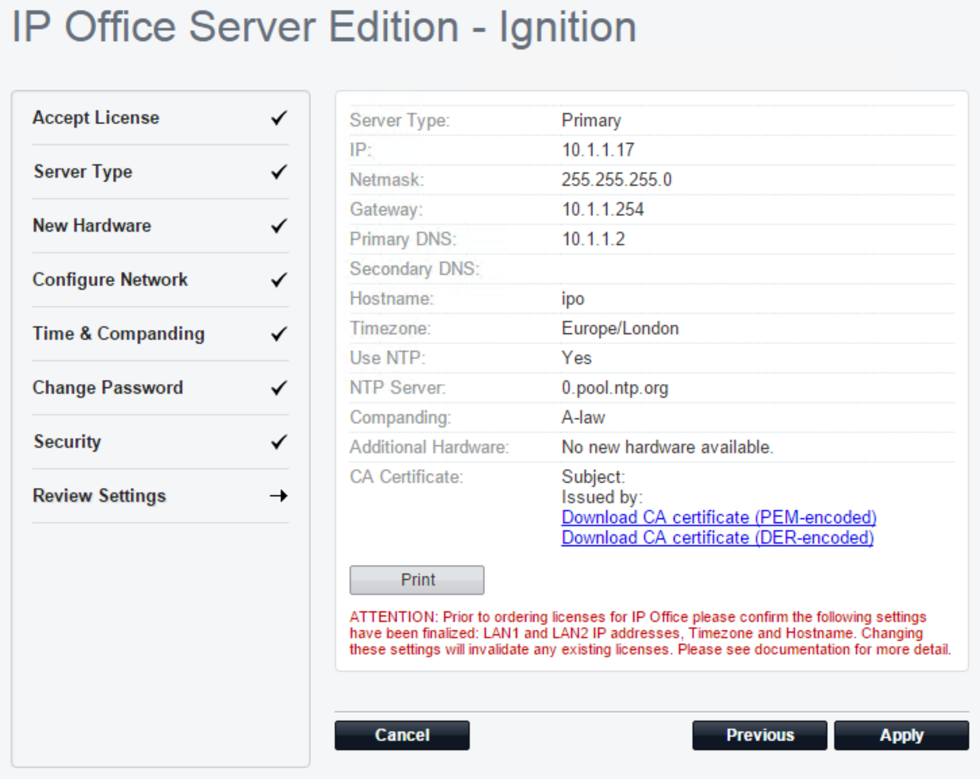


CA Certificate

● Generate new

○ Import

10. At the summary click Apply



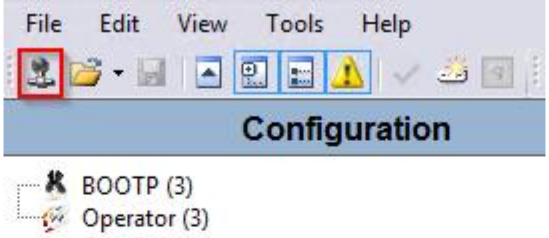
Server Type:	Primary
IP:	10.1.1.17
Netmask:	255.255.255.0
Gateway:	10.1.1.254
Primary DNS:	10.1.1.2
Secondary DNS:	
Hostname:	ipo
Timezone:	Europe/London
Use NTP:	Yes
NTP Server:	0.pool.ntp.org
Companding:	A-law
Additional Hardware:	No new hardware available.
CA Certificate:	Subject: Issued by: Download CA certificate (PEM-encoded) Download CA certificate (DER-encoded)

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.

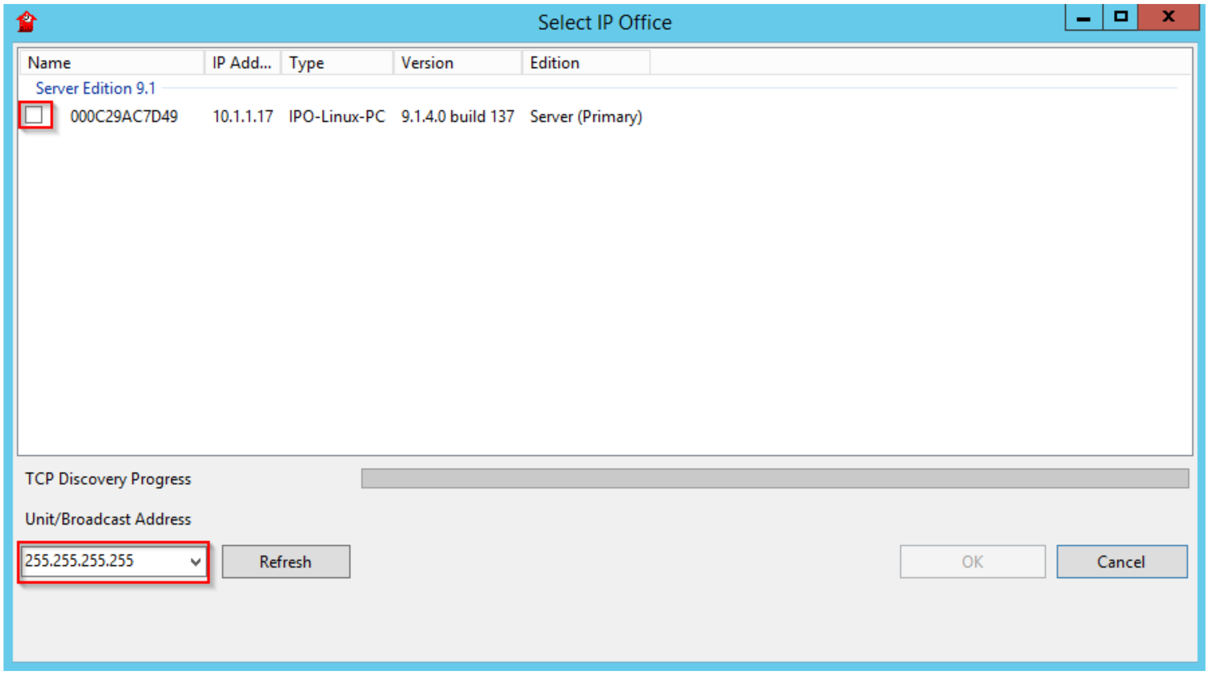
IP Office Initial Configuration

1. Start **IP Office / Manager** on your PC

2. Click on the **Open configuration from IP Office** icon



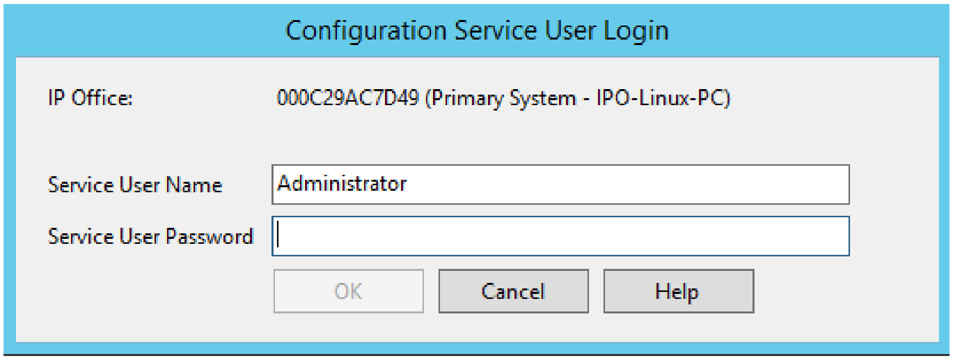
3. Select the IP Office box and click **OK**. If list is empty, type the IP address of the server in **Unit/Broadcast Address**, then click **Refresh**



Name	IP Add...	Type	Version	Edition
Server Edition 9.1				
□ 000C29AC7D49	10.1.1.17	IPO-Linux-PC	9.1.4.0 build 137	Server (Primary)

Unit/Broadcast Address: 255.255.255.255

4. Login with the Administrator password you set during Ignition

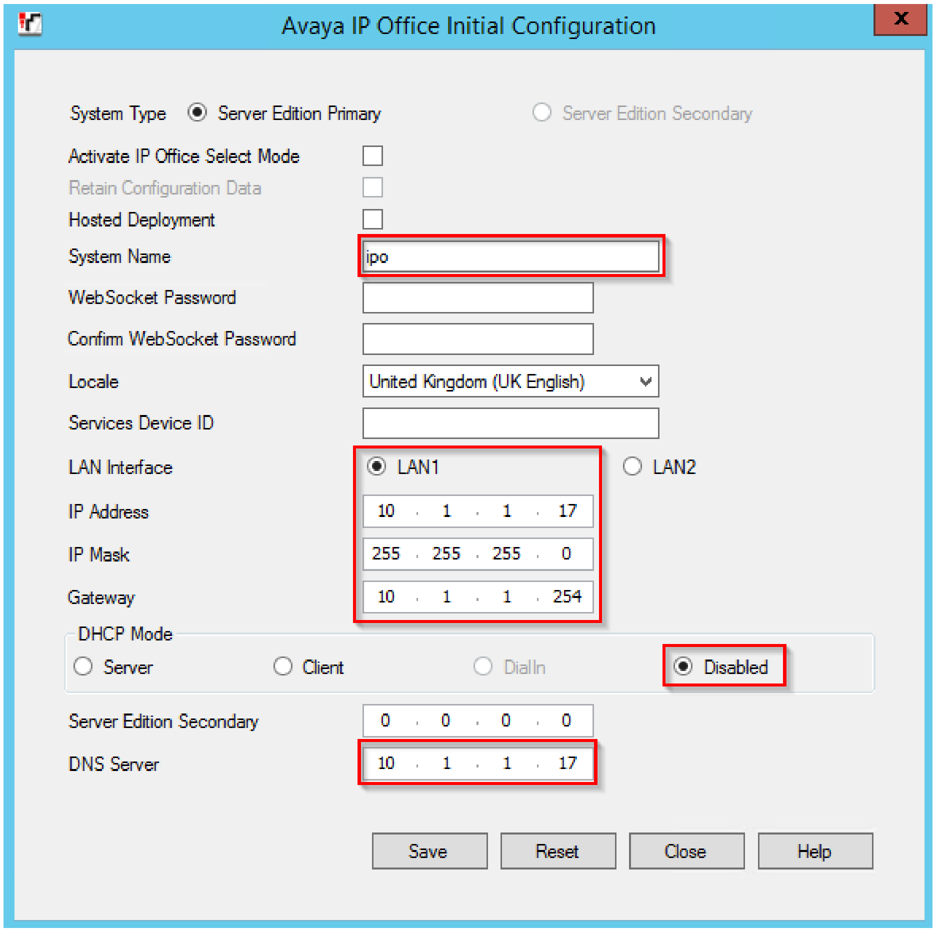


IP Office: 000C29AC7D49 (Primary System - IPO-Linux-PC)

Service User Name: Administrator

Service User Password:

5. Edit **System Name, LAN1 Interface, DHCP Mode, DNS server**, leave the rest on default, then click **Save**. For full details of this form, refer to the IP Office Manager help.



Avaya IP Office Initial Configuration

System Type ● Server Edition Primary ○ Server Edition Secondary

Activate IP Office Select Mode □

Retain Configuration Data □

Hosted Deployment □

System Name: ipo

WebSocket Password:

Confirm WebSocket Password:

Locale: United Kingdom (UK English)

Services Device ID:

LAN Interface ● LAN1 ○ LAN2

IP Address: 10 . 1 . 1 . 17

IP Mask: 255 . 255 . 255 . 0

Gateway: 10 . 1 . 1 . 254

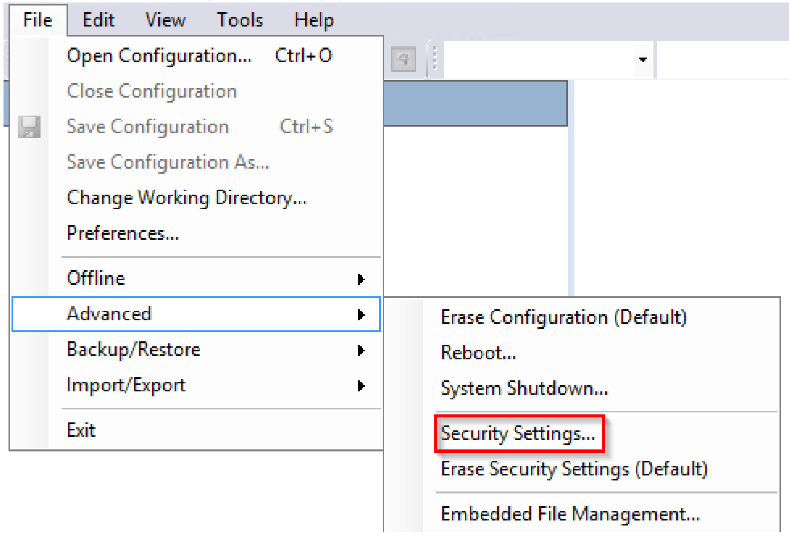
DHCP Mode ○ Server ○ Client ○ DialIn ● Disabled

Server Edition Secondary: 0 . 0 . 0 . 0

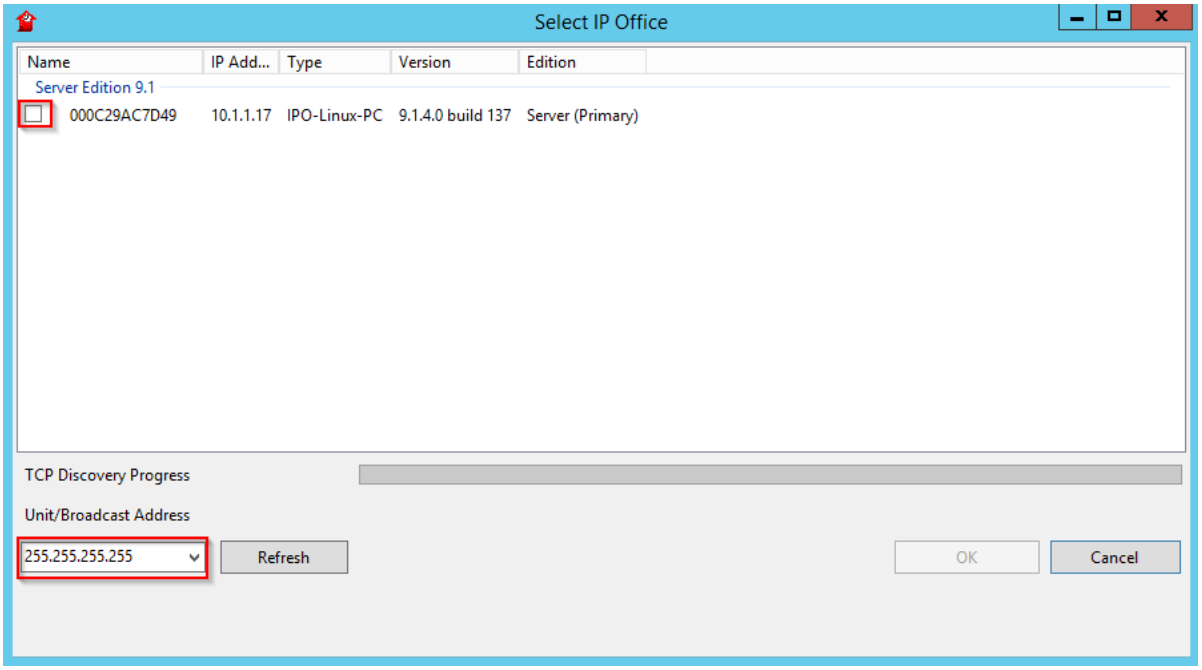
DNS Server: 10 . 1 . 1 . 17

NOTE: both the LAN1 and LAN2 IP addresses affect the virtual machine's System Identification used for licensing . Therefore, we strongly recommended that before obtaining any licenses, you ensure that these are set to their final values.

6. Change Security settings so that station user can have digit only password. In IP Office Manager go to **File / Advanced Settings /Security**



7. 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**

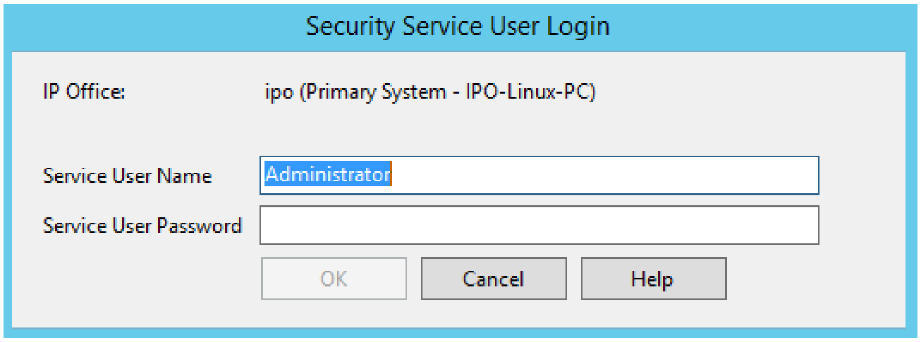


Name	IP Add...	Type	Version	Edition
Server Edition 9.1				
□ 000C29AC7D49	10.1.1.17	IPO-Linux-PC	9.1.4.0 build 137	Server (Primary)

TCP Discovery Progress

Unit/Broadcast Address: 255.255.255.255

8. Login with the Administrator password set during Ignition

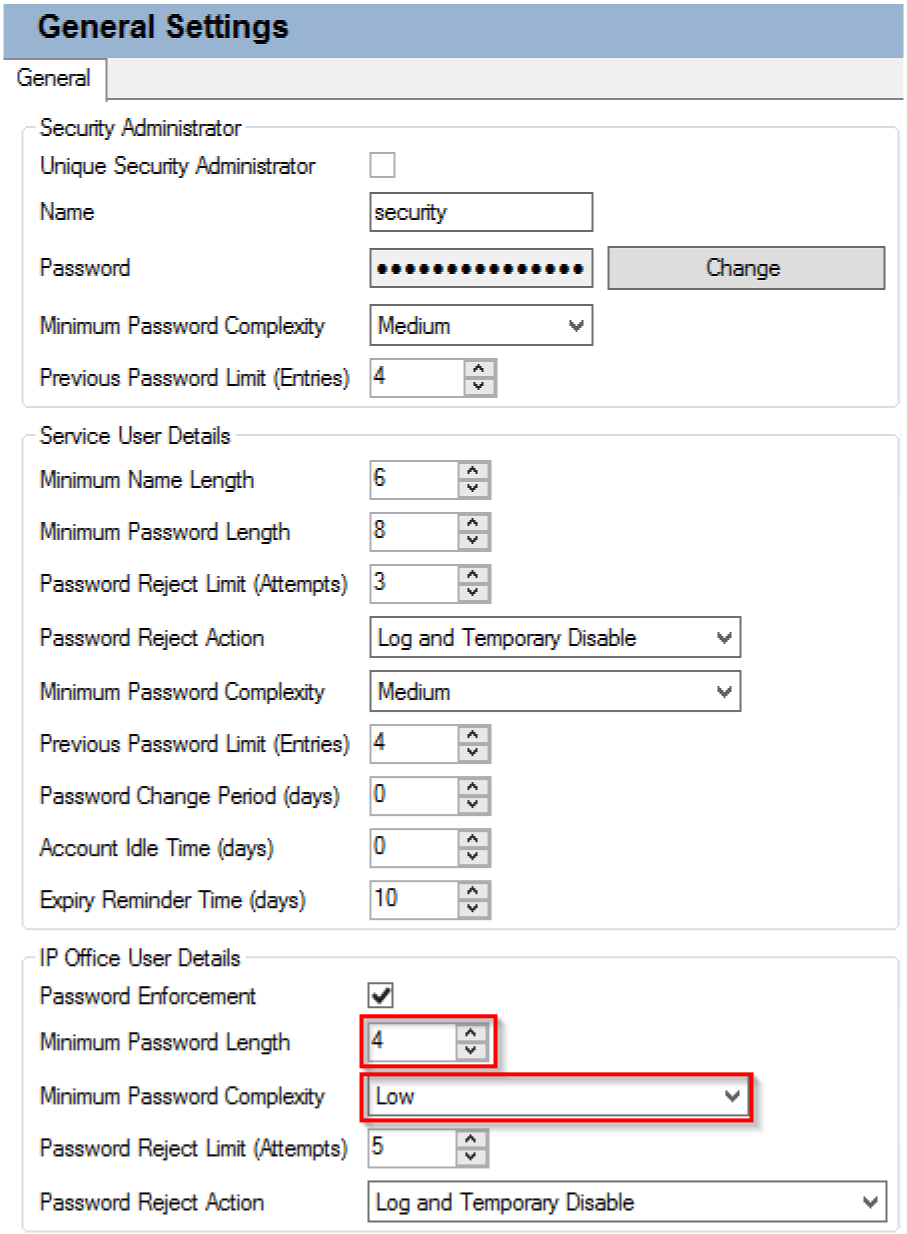


IP Office: ipo (Primary System - IPO-Linux-PC)

Service User Name: Administrator

Service User Password:

9. Under **General Settings** set **Minimum Password Length** and **Minimum Password Complexity** then click OK



General Settings

General

Security Administrator

Unique Security Administrator	☐
Name	security
Password	••••••••••••••• [Change]
Minimum Password Complexity	Medium
Previous Password Limit (Entries)	4

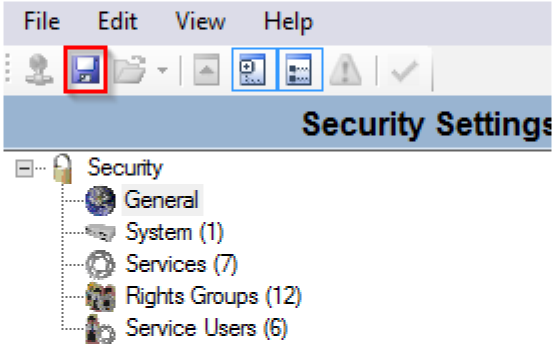
Service User Details

Minimum Name Length	6
Minimum Password Length	8
Password Reject Limit (Attempts)	3
Password Reject Action	Log and Temporary Disable
Minimum Password Complexity	Medium
Previous Password Limit (Entries)	4
Password Change Period (days)	0
Account Idle Time (days)	0
Expiry Reminder Time (days)	10

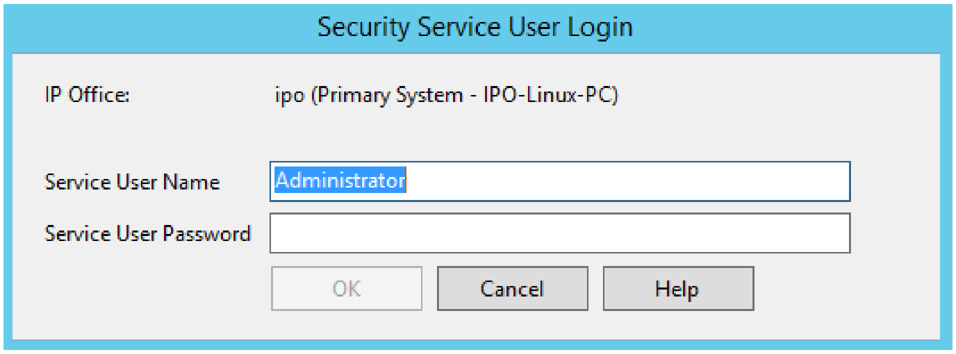
IP Office User Details

Password Enforcement	☑
Minimum Password Length	4
Minimum Password Complexity	Low
Password Reject Limit (Attempts)	5
Password Reject Action	Log and Temporary Disable

10. Click on **Save** icon



11. Enter the Administrator password and click **OK**



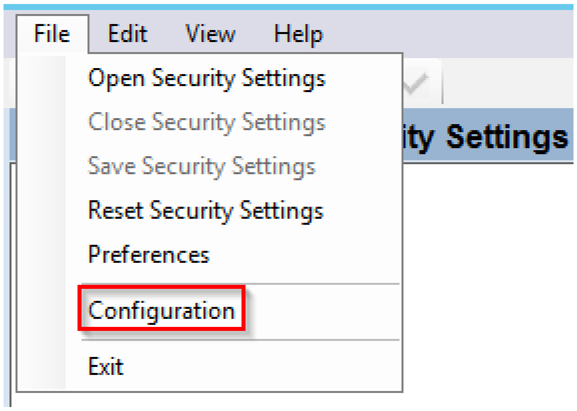
Security Service User Login

IP Office: ipo (Primary System - IPO-Linux-PC)

Service User Name: Administrator

Service User Password:

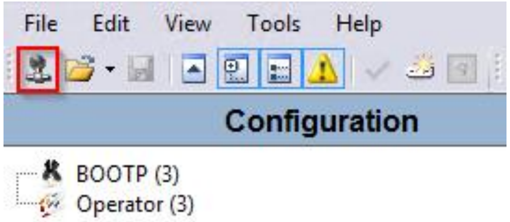
12. Switch back to configuration mode by clicking at **File / Configuration**



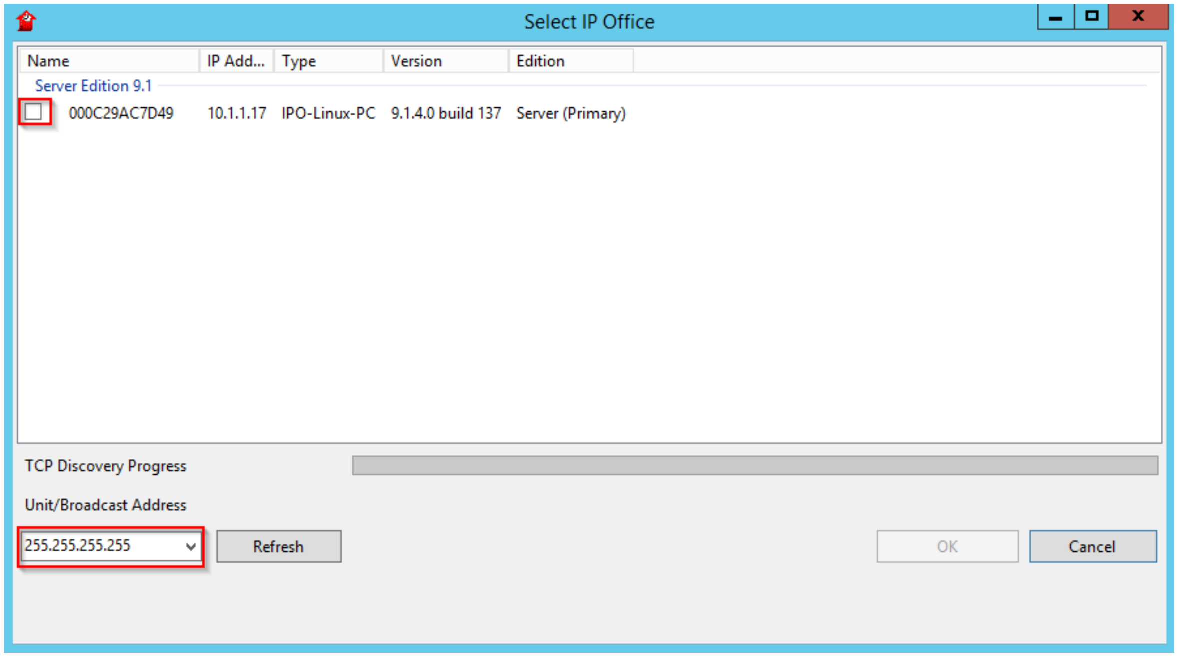
Configuring IP Office

Connecting to IP Office

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**



Select IP Office

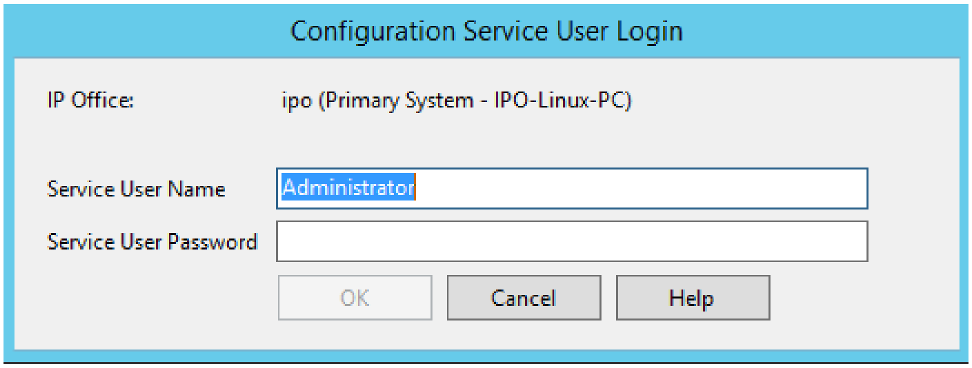
Name	IP Add...	Type	Version	Edition
Server Edition 9.1				
□ 000C29AC7D49	10.1.1.17	IPO-Linux-PC	9.1.4.0 build 137	Server (Primary)

TCP Discovery Progress

Unit/Broadcast Address

255.255.255.255

4. Login with the Administrator password set during Ignition



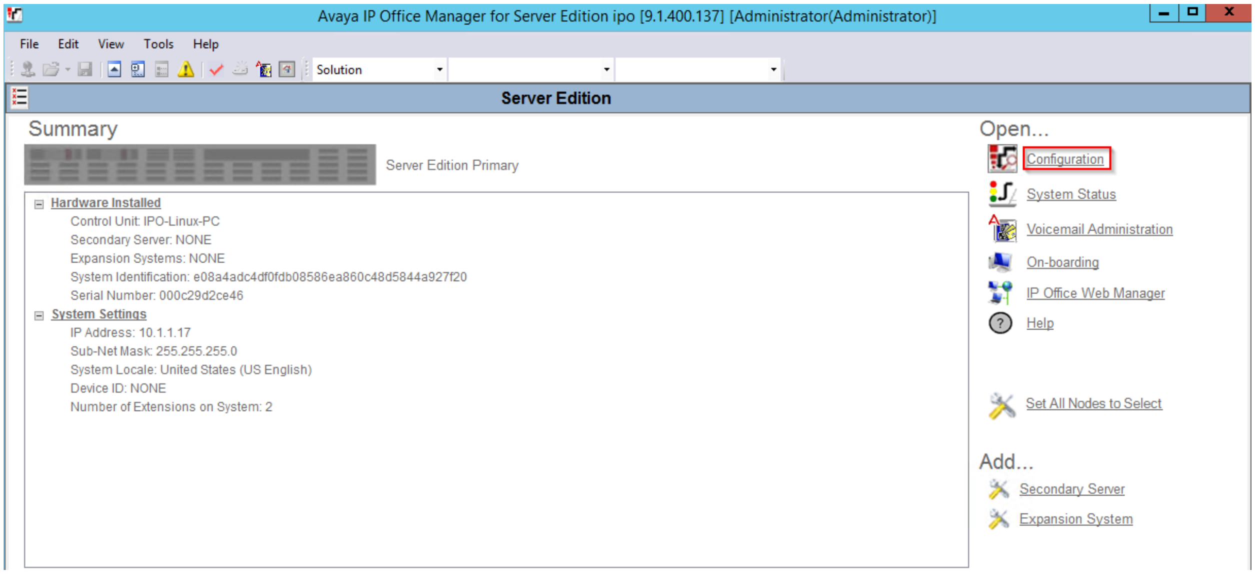
Configuration Service User Login

IP Office: ipo (Primary System - IPO-Linux-PC)

Service User Name: Administrator

Service User Password:

5. Click on Configuration link



Avaya IP Office Manager for Server Edition ipo [9.1.400.137] [Administrator(Administrator)]

Server Edition

Summary

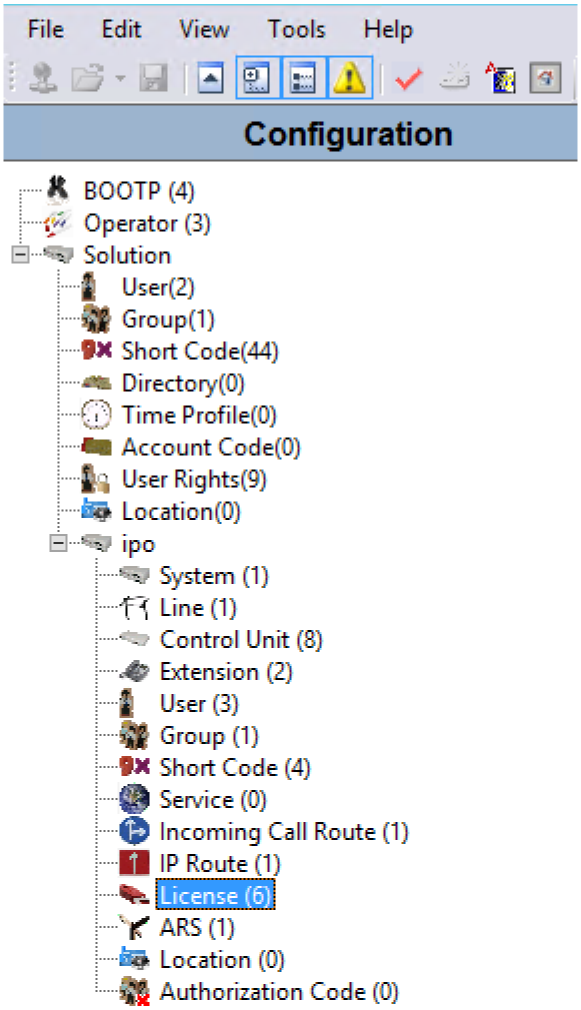
Server Edition Primary

Hardware Installed
- Control Unit: IPO-Linux-PC
- Secondary Server: NONE
- Expansion Systems: NONE
- System Identification: e08a4adc4df0fdb08586ea860c48d5844a927f20
- Serial Number: 000c29d2ce46

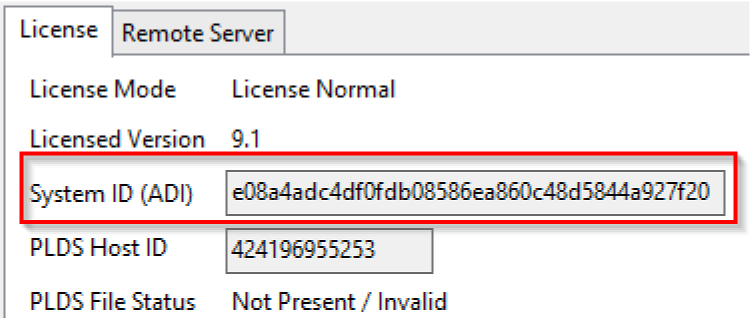
System Settings
- IP Address: 10.1.1.17
- Sub-Net Mask: 255.255.255.0
- System Locale: United States (US English)
- Device ID: NONE
- Number of Extensions on System: 2

Licenses

1. Expand you IP Office element under **Solution** and select **License**

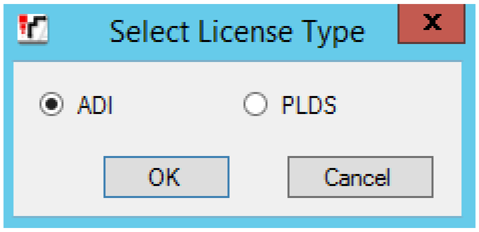


2. Generate **Server Edition R9.1** and **Power User** licenses based on the **System ID**



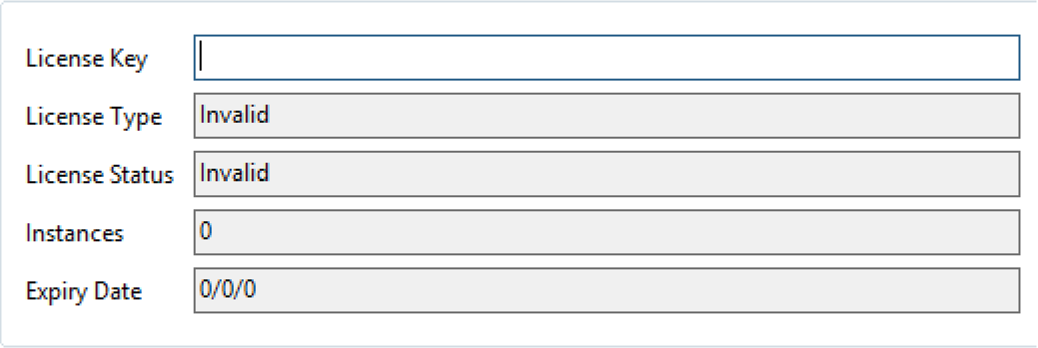
License Mode	License Normal
Licensed Version	9.1
System ID (ADI)	e08a4adc4df0fdb08586ea860c48d5844a927f20
PLDS Host ID	424196955253
PLDS File Status	Not Present / Invalid

3. Once you have the license keys, click **Add**
4. Select **ADI** and click **OK**



● ADI ○ PLDS

5. Copy/Paste the **License Key** and click **OK**

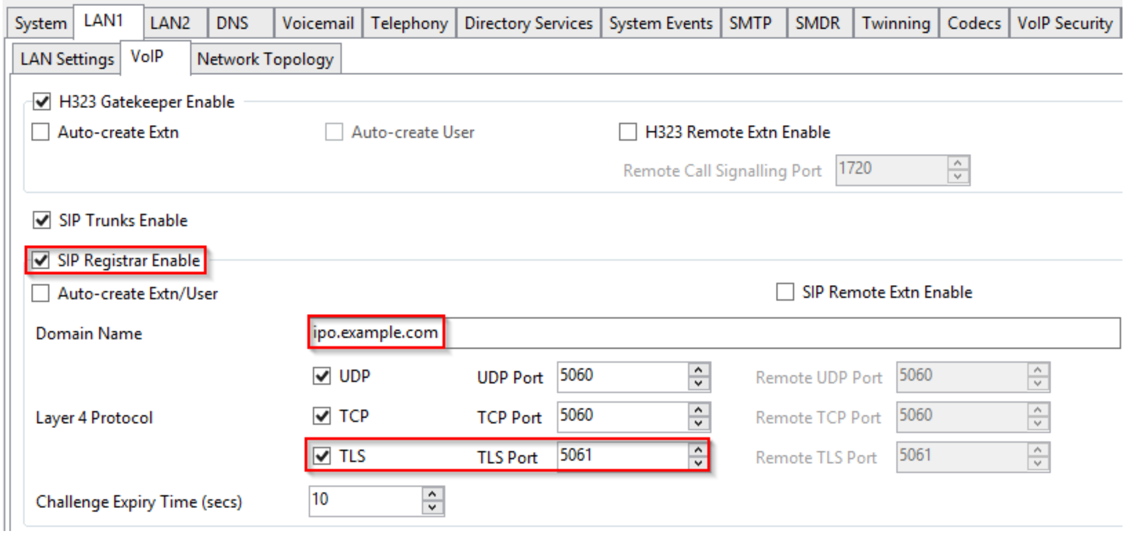


License Key	
License Type	Invalid
License Status	Invalid
Instances	0
Expiry Date	0/0/0

6. Repeat the above steps for all the license keys, finally click **OK** on the License form
7. Save the configuration

VoIP Setup

1. Expand you 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 **Domain Name**: this will be the SIP domain for the clients
    e. Check Layer 4 protocols and set relevant ports



☑ H323 Gatekeeper Enable

☐ Auto-create Extn ☐ Auto-create User ☐ H323 Remote Extn Enable

Remote Call Signalling Port 1720

☑ SIP Trunks Enable

☑ SIP Registrar Enable

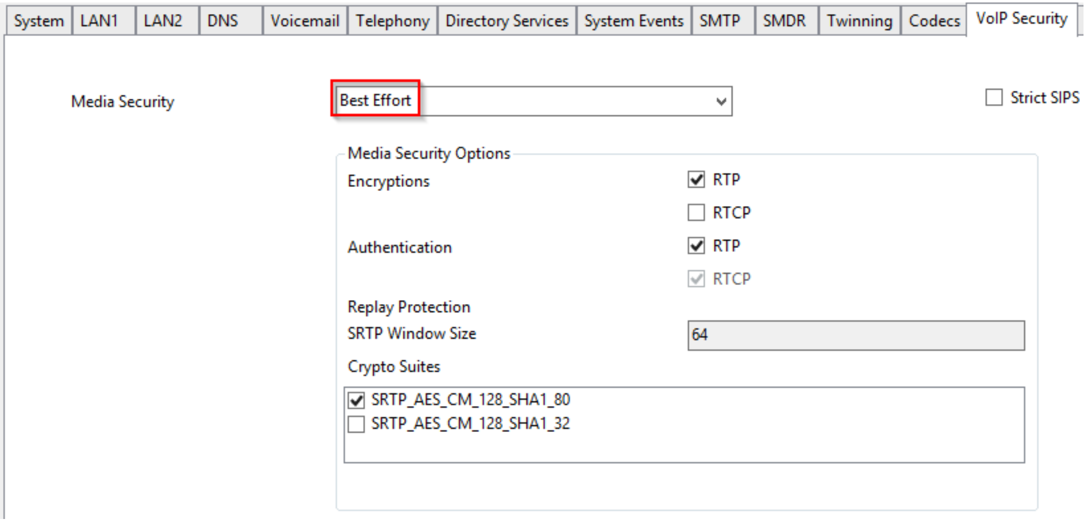
☐ Auto-create Extn/User ☐ SIP Remote Extn Enable

Domain Name ipo.example.com

Layer 4 Protocol	☑ UDP	UDP Port	5060	Remote UDP Port	5060
	☑ TCP	TCP Port	5060	Remote TCP Port	5060
	☑ TLS	TLS Port	5061	Remote TLS Port	5061

Challenge Expiry Time (secs) 10

3. Go to **VoIP Security** tab and set the **Media Security** to **Best Effort**



Media Security Best Effort

☐ Strict SIPS

Media Security Options

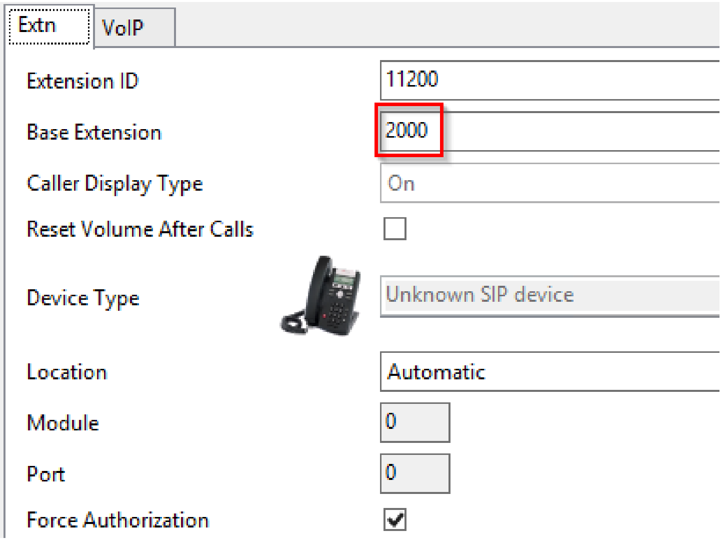
Encryptions	☑ RTP ☐ RTCP
Authentication	☑ RTP ☑ RTCP
Replay Protection	
SRTP Window Size	64
Crypto Suites	

☑ SRTP_AES_CM_128_SHA1_80
☐ SRTP_AES_CM_128_SHA1_32

4. Click **OK** and **Save** configuration

Extensions

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



Extension ID	11200
Base Extension	2000
Caller Display Type	On
Reset Volume After Calls	☐
Device Type	Unknown SIP device
Location	Automatic
Module	0
Port	0
Force Authorization	☑

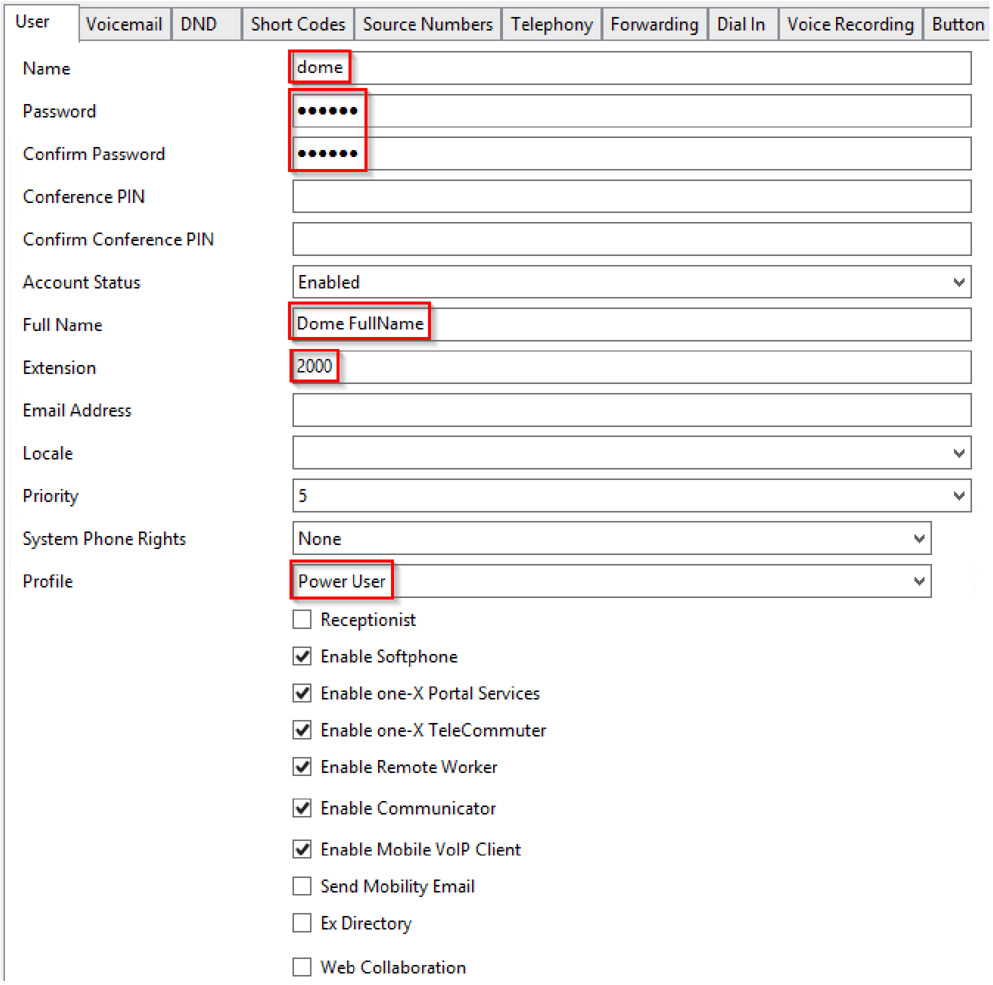
5. Click **OK** and **Save** configuration

Users

1. Expand you 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

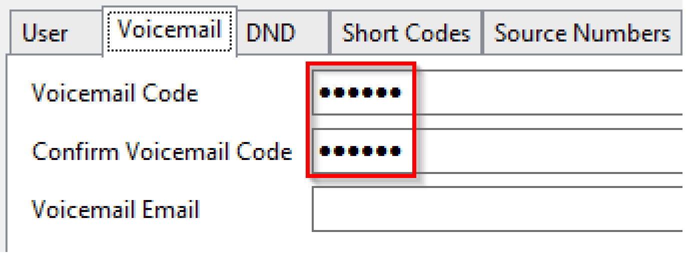
e. **Profile**: select **Power User**



Name	dome
Password	••••••
Confirm Password	••••••
Conference PIN	
Confirm Conference PIN	
Account Status	Enabled
Full Name	Dome FullName
Extension	2000
Email Address	
Locale	
Priority	5
System Phone Rights	None
Profile	Power User

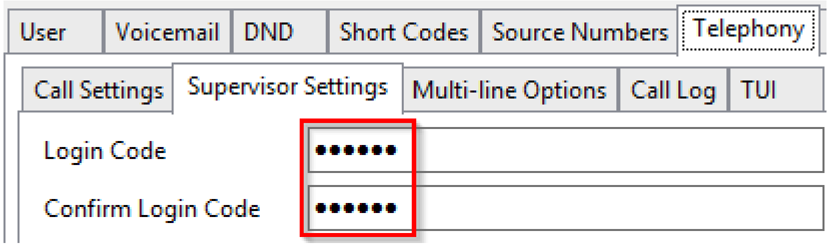
☐ Receptionist
☑ Enable Softphone
☑ Enable one-X Portal Services
☑ Enable one-X TeleCommuter
☑ Enable Remote Worker
☑ Enable Communicator
☑ Enable Mobile VoIP Client
☐ Send Mobility Email
☐ Ex Directory
☐ Web Collaboration

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



Voicemail Code	••••••
Confirm Voicemail Code	••••••
Voicemail Email	

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



Login Code	••••••
Confirm Login Code	••••••

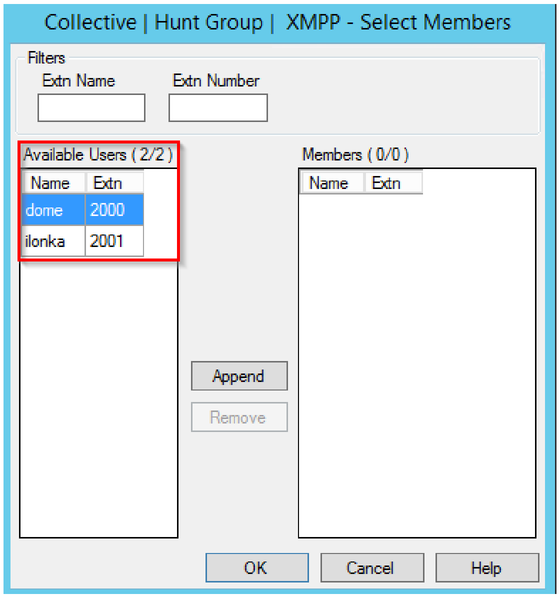
NOTE: This code is used by Communicator for Android and Communicator for iPhone as password for the user. Other clients use the Password on the User tab.

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 you IP Office element under **Solution** and select **Group**
2. Right-click on **Group** and select **New**
3. Under Group tab set the followings:
   a. **Name**: name of the group
   b. **Profile**: select **XMPP Group**
4. Click **Edit**
5. Select all **Available Users** and click **Append**, then click **OK**



Collective | Hunt Group | XMPP - Select Members

Filters

Extn Name

Extn Number

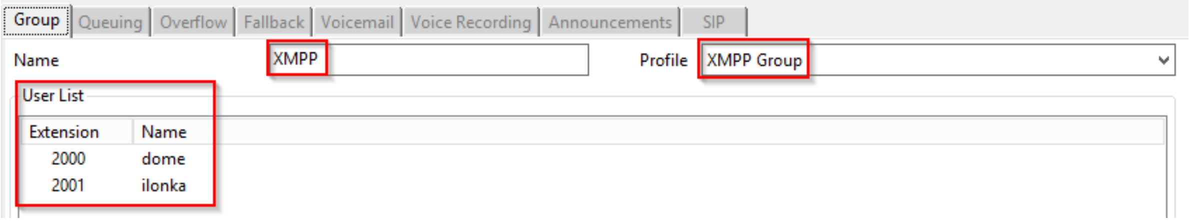
Available Users (2/2)

Name	Extn
dome	2000
ilonka	2001

Members (0/0)

Name	Extn

6. Hunt group should look like this:



Name: XMPP

Profile: XMPP Group

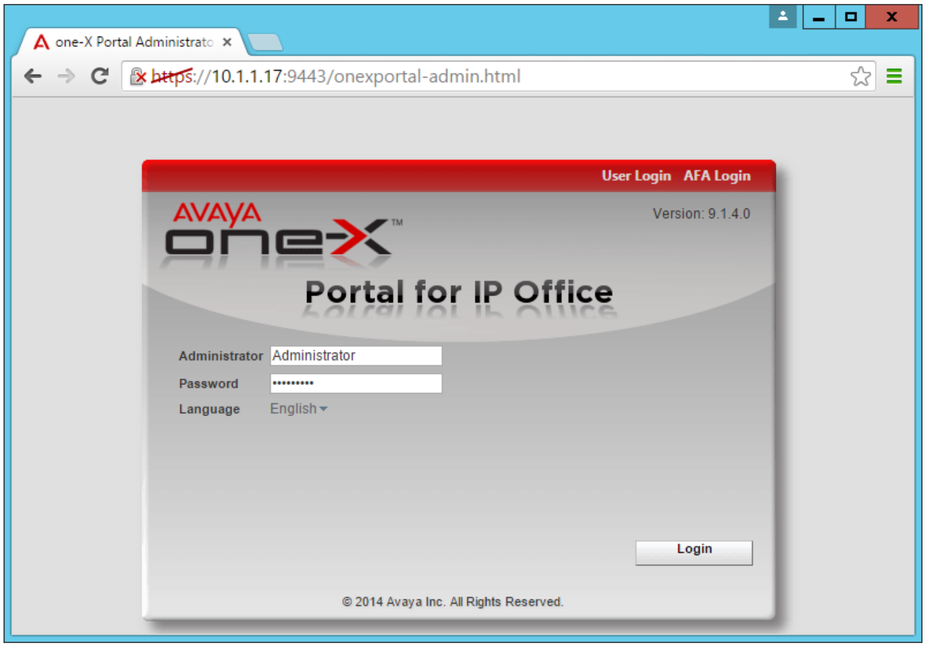
User List

Extension	Name
2000	dome
2001	ilonka

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

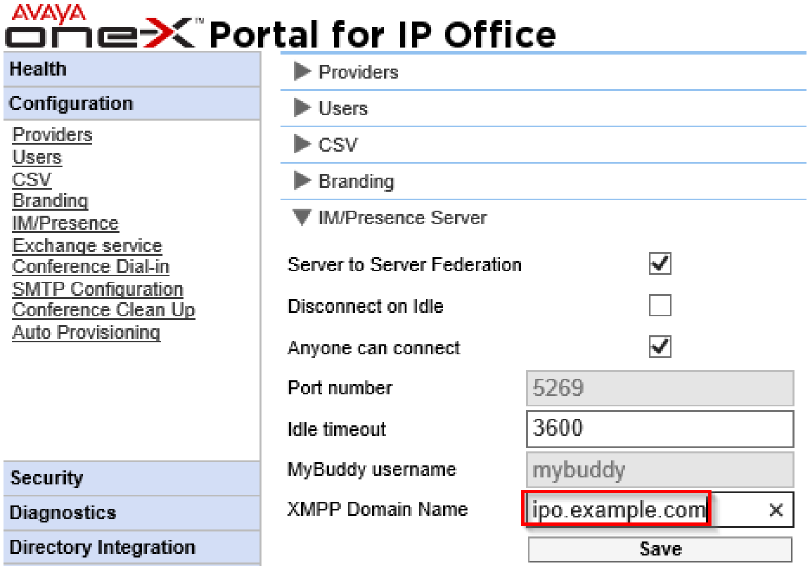
Configuring XMPP domain on One-X Portal

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


one-X Portal Administrato
https://10.1.1.17:9443/onexportal-admin.html
User Login
AFA Login
AVAYA one-X
Version: 9.1.4.0
Portal for IP Office
Login
© 2014 Avaya Inc. All Rights Reserved.

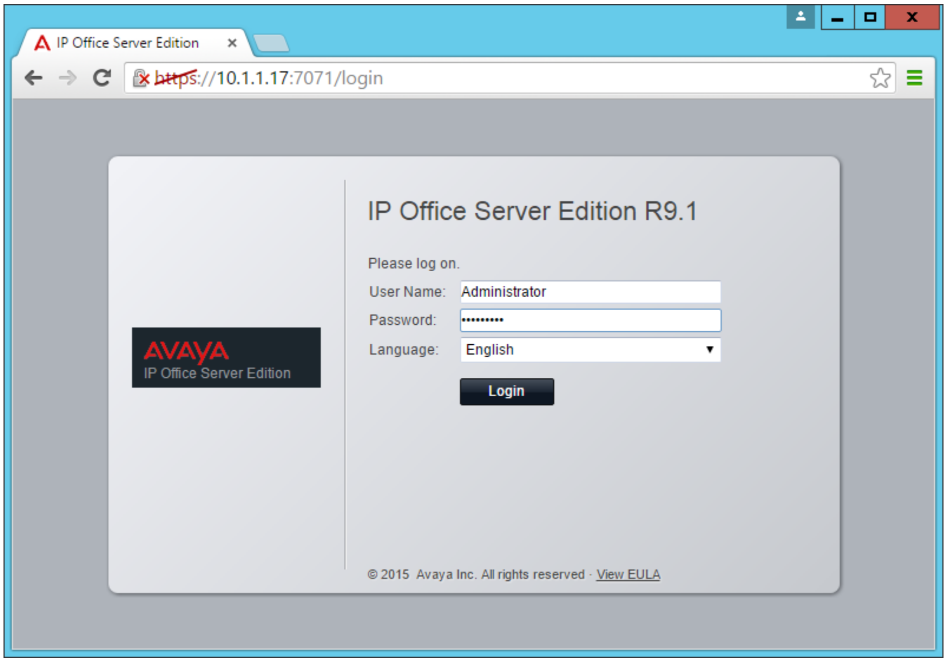
Administrator: Administrator
Password: •••••••••
Language: English

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



Server to Server Federation ☑
Disconnect on Idle □
Anyone can connect ☑
Port number: 5269
Idle timeout: 3600
MyBuddy username: mybuddy
XMPP Domain Name: ipo.example.com

3. One-X Portal needs to be restarted after changing the XMPP domain. Open a browser and connect to https://<IP>:7071/login, use the **Administrator** login and password you set during Ignition



IP Office Server Edition R9.1

Please log on.

User Name: Administrator

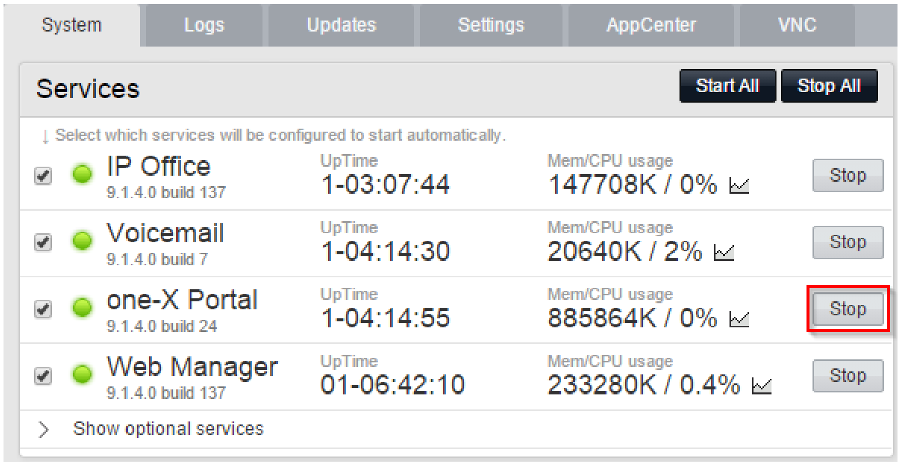
Password: ••••••••••

Language: English

Login

© 2015 Avaya Inc. All rights reserved · View EULA

4. Click **Stop** at one-X portal, wait until it stops, then click **Start**



Services

↓ Select which services will be configured to start automatically.

		UpTime	Mem/CPU usage	
☑	IP Office 9.1.4.0 build 137	1-03:07:44	147708K / 0%	Stop
☑	Voicemail 9.1.4.0 build 7	1-04:14:30	20640K / 2%	Stop
☑	one-X Portal 9.1.4.0 build 24	1-04:14:55	885864K / 0%	Stop
☑	Web Manager 9.1.4.0 build 137	01-06:42:10	233280K / 0.4%	Stop

> Show optional services

Installing SBCE

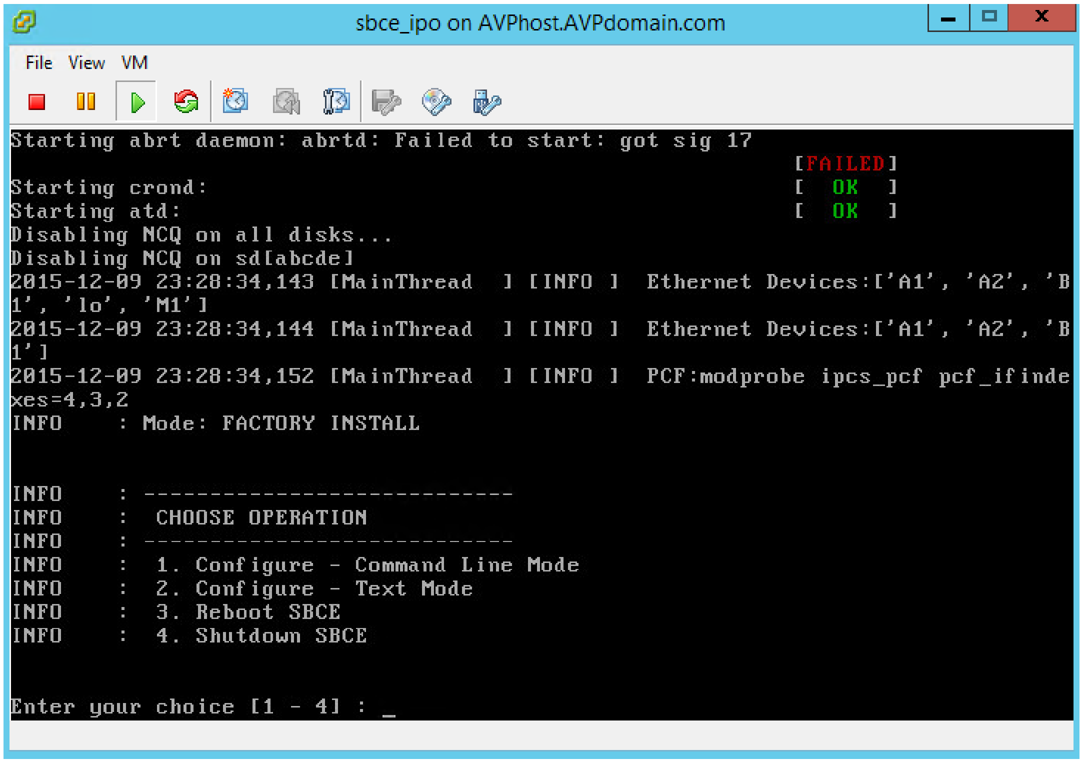
Deploying OVA

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

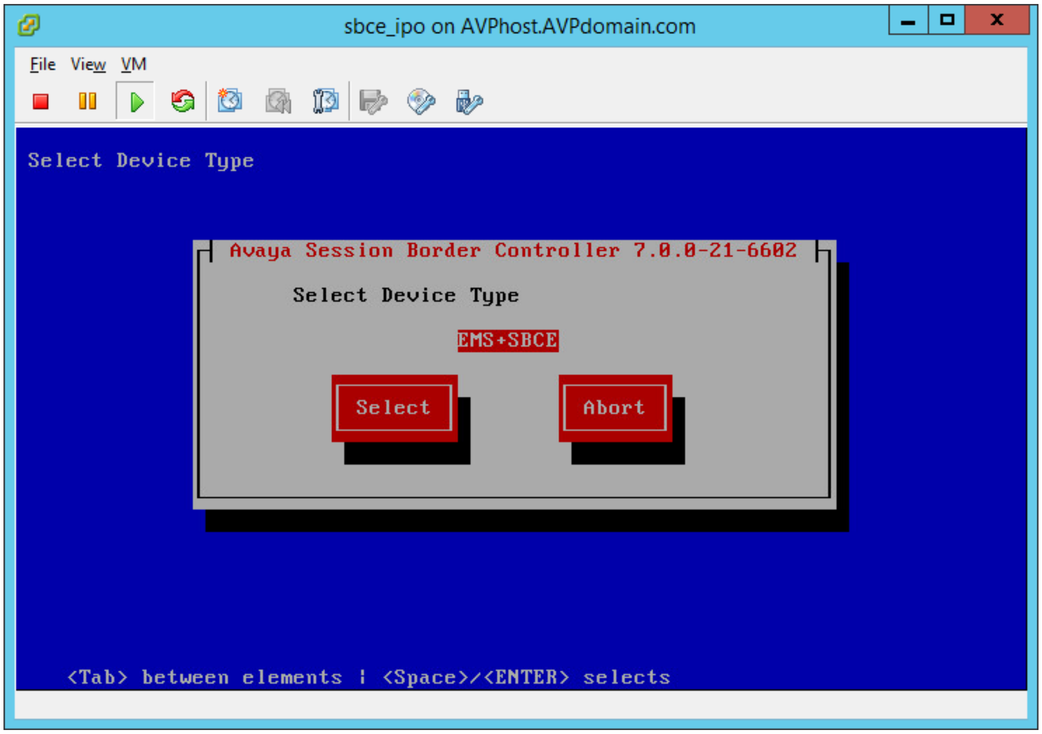
Setting Management IP

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:



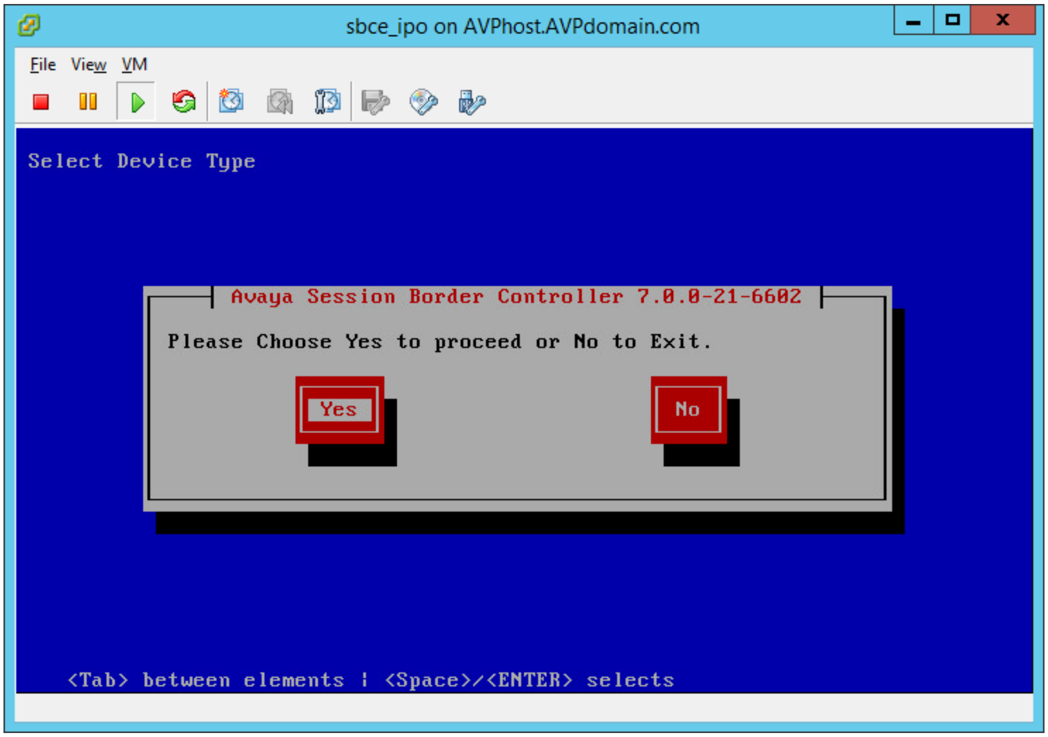
```
Starting abrt daemon: abrtd: Failed to start: got sig 17
                                                           [FAILED]
Starting crond:                                            [  OK  ]
Starting atd:                                              [  OK  ]
Disabling NCQ on all disks...
Disabling NCQ on sd[abcde]
2015-12-09 23:28:34,143 [MainThread  ] [INFO ]  Ethernet Devices:['A1', 'A2', 'B
1', 'lo', 'M1']
2015-12-09 23:28:34,144 [MainThread  ] [INFO ]  Ethernet Devices:['A1', 'A2', 'B
1']
2015-12-09 23:28:34,152 [MainThread  ] [INFO ]  PCF:modprobe ipcs_pcf pcf_ifinde
xes=4,3,2
INFO     : Mode: FACTORY INSTALL


INFO     : ----------------------------
INFO     :  CHOOSE OPERATION
INFO     : ----------------------------
INFO     :  1. Configure - Command Line Mode
INFO     :  2. Configure - Text Mode
INFO     :  3. Reboot SBCE
INFO     :  4. Shutdown SBCE


Enter your choice [1 - 4] : _
```

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



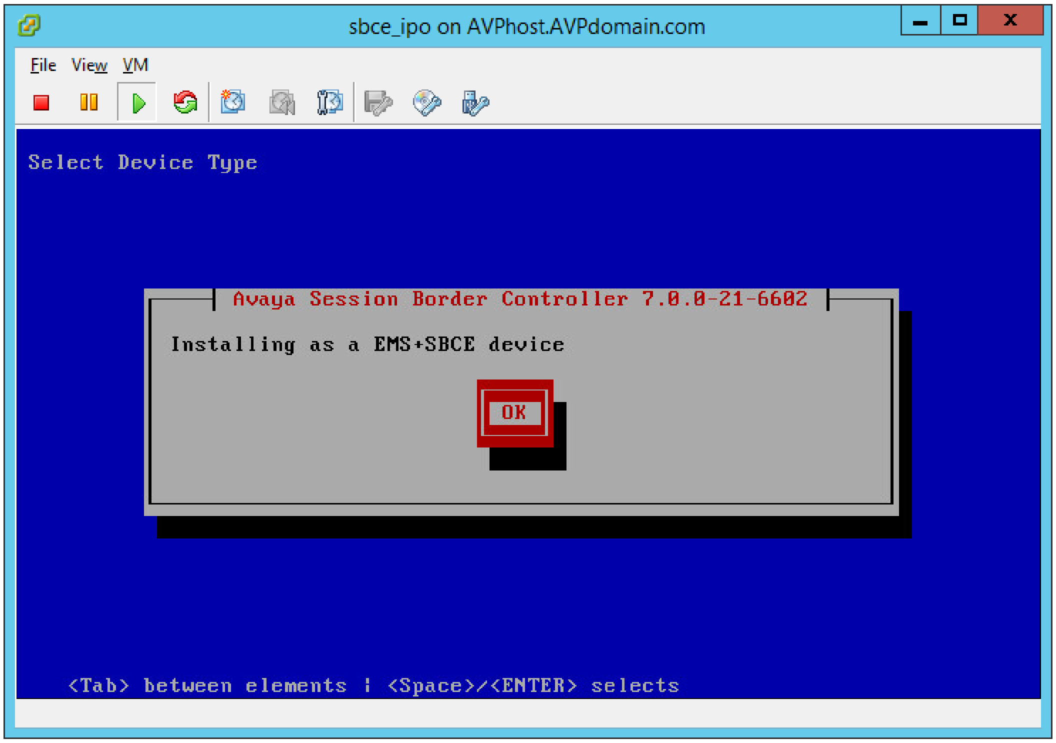
```
Select Device Type

Avaya Session Border Controller 7.0.0-21-6602
Select Device Type
EMS+SBCE
Select      Abort

<Tab> between elements | <Space>/<ENTER> selects
```

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



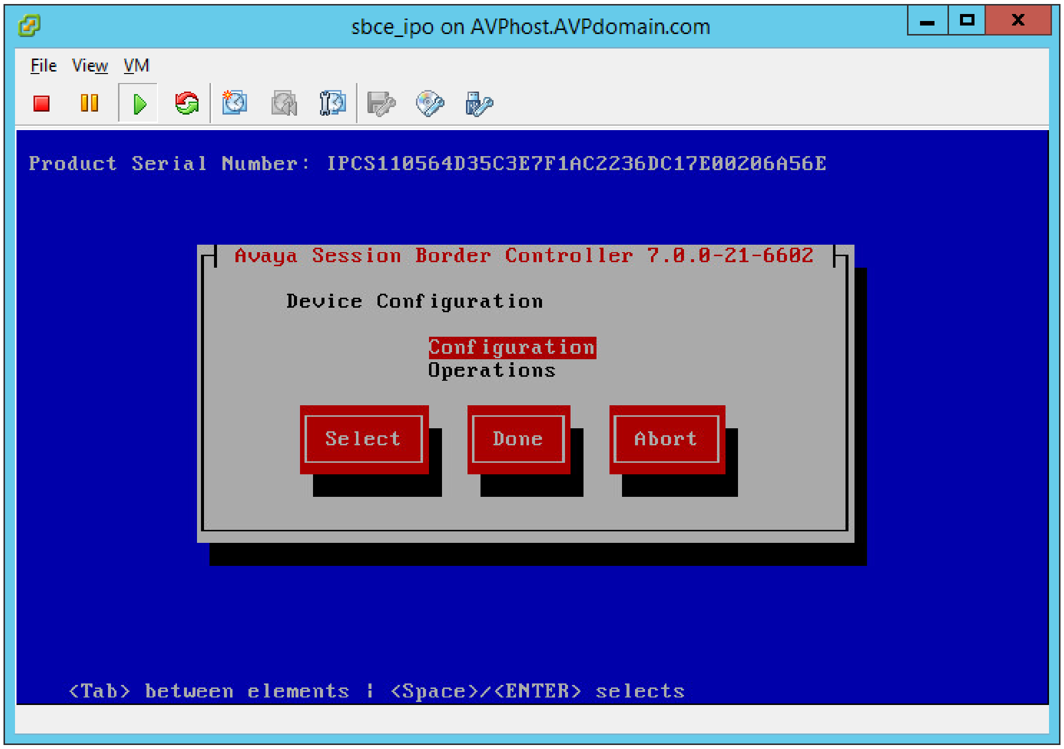
```
Select Device Type

Avaya Session Border Controller 7.0.0-21-6602
Please Choose Yes to proceed or No to Exit.
Yes      No

<Tab> between elements | <Space>/<ENTER> selects
```

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



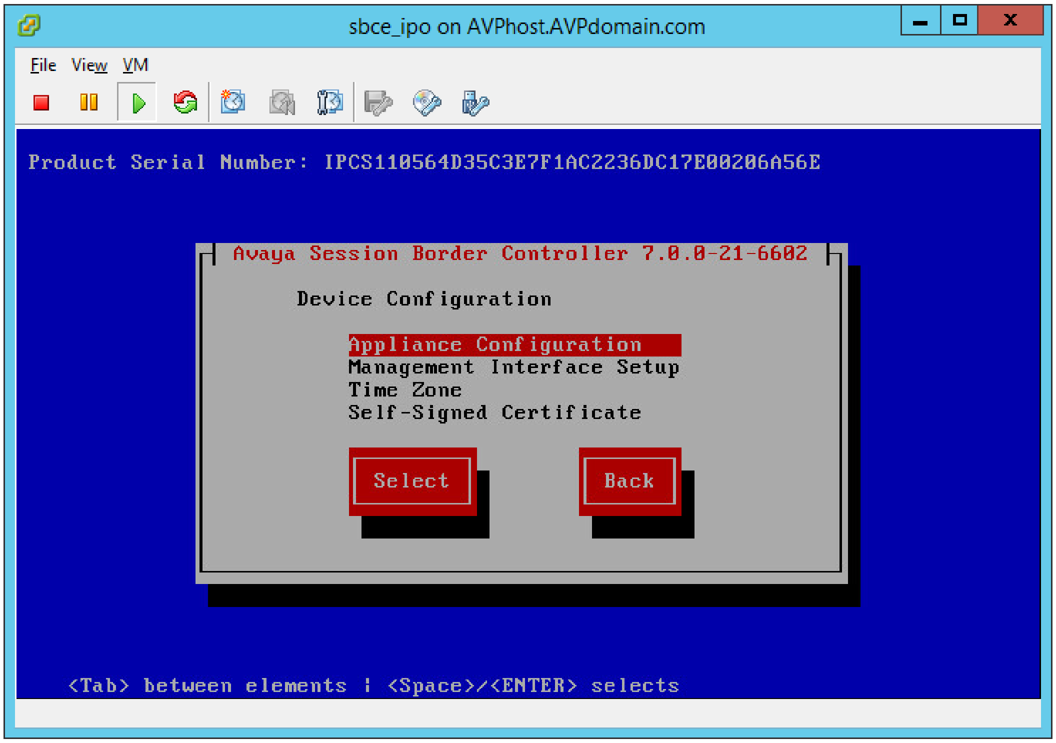
```
Select Device Type

Avaya Session Border Controller 7.0.0-21-6602

Installing as a EMS+SBCE device

OK

<Tab> between elements | <Space>/<ENTER> selects
```

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



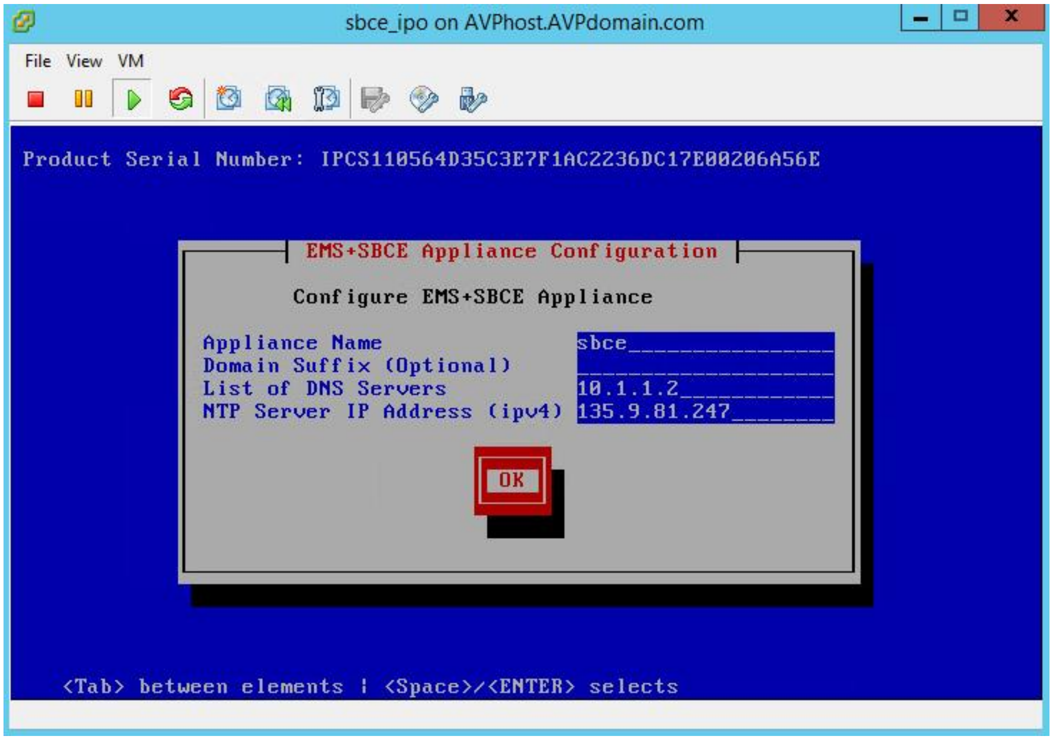
```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

Avaya Session Border Controller 7.0.0-21-6602

Device Configuration

Configuration
Operations

Select    Done    Abort

<Tab> between elements | <Space>/<ENTER> selects
```

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



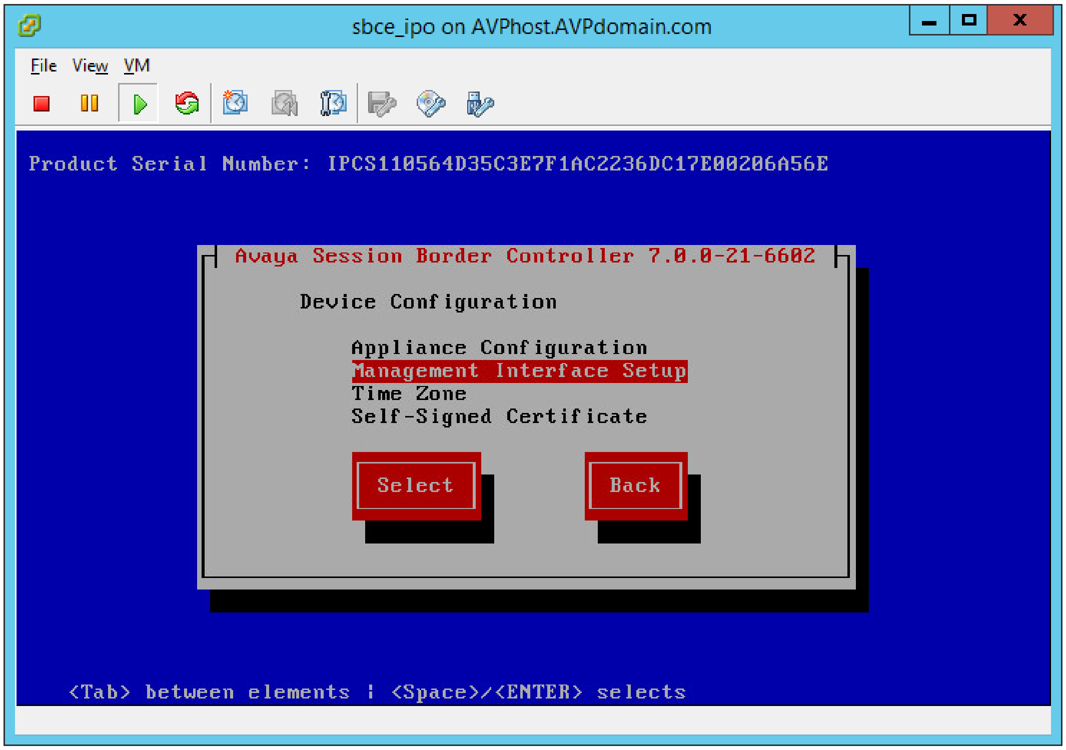
```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

        Avaya Session Border Controller 7.0.0-21-6602

            Device Configuration

                Appliance Configuration
                Management Interface Setup
                Time Zone
                Self-Signed Certificate

                  Select              Back

   <Tab> between elements | <Space>/<ENTER> selects
```

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



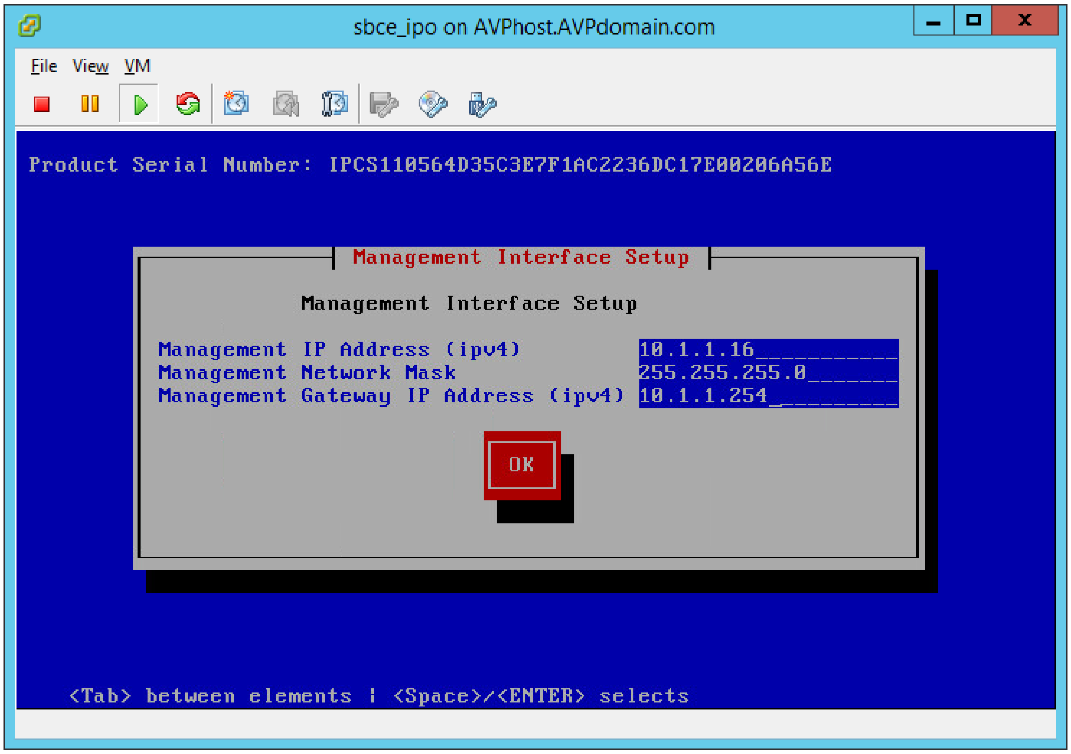
```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

          EMS+SBCE Appliance Configuration

            Configure EMS+SBCE Appliance

   Appliance Name                   sbce_______________
   Domain Suffix (Optional)         ___________________
   List of DNS Servers              10.1.1.2___________
   NTP Server IP Address (ipv4)     135.9.81.247_______

                         OK

   <Tab> between elements | <Space>/<ENTER> selects
```

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



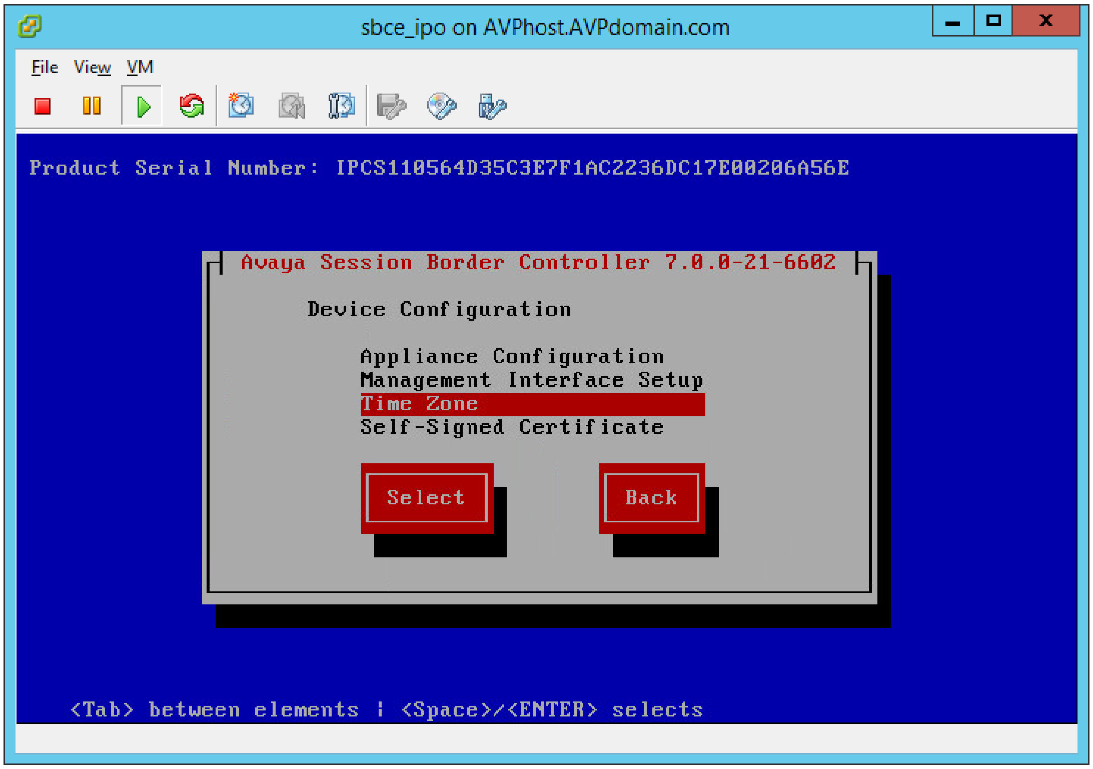
```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

Avaya Session Border Controller 7.0.0-21-6602

Device Configuration

    Appliance Configuration
    Management Interface Setup
    Time Zone
    Self-Signed Certificate

    Select        Back

<Tab> between elements | <Space>/<ENTER> selects
```

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



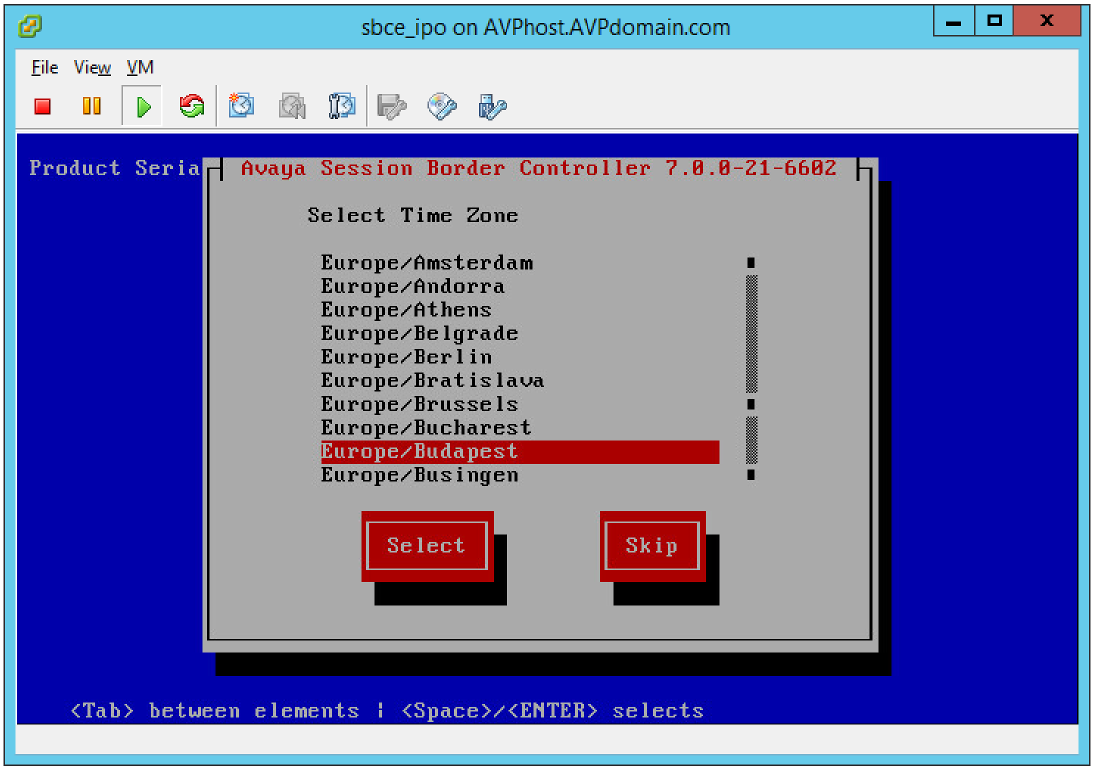
```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

Management Interface Setup

Management Interface Setup

Management IP Address (ipv4)          10.1.1.16___________
Management Network Mask               255.255.255.0_______
Management Gateway IP Address (ipv4)  10.1.1.254__________

                 OK

<Tab> between elements | <Space>/<ENTER> selects
```

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



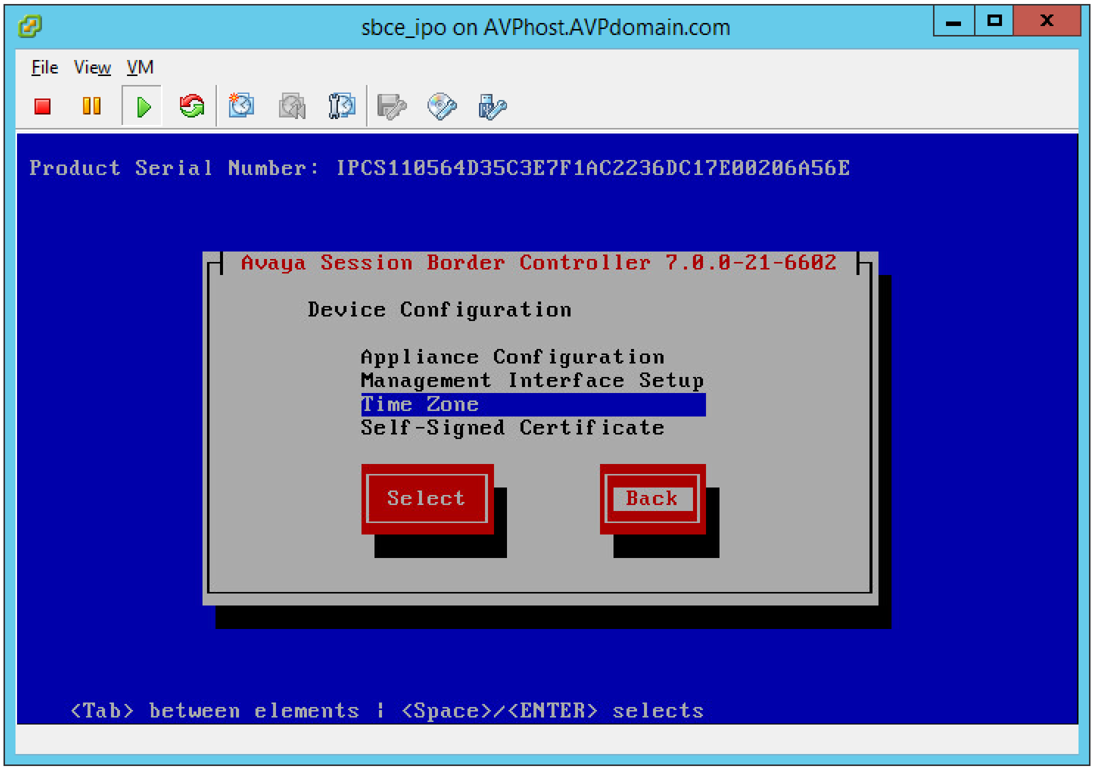
```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

        Avaya Session Border Controller 7.0.0-21-6602

            Device Configuration

                Appliance Configuration
                Management Interface Setup
                Time Zone
                Self-Signed Certificate

                   Select            Back

  <Tab> between elements | <Space>/<ENTER> selects
```

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



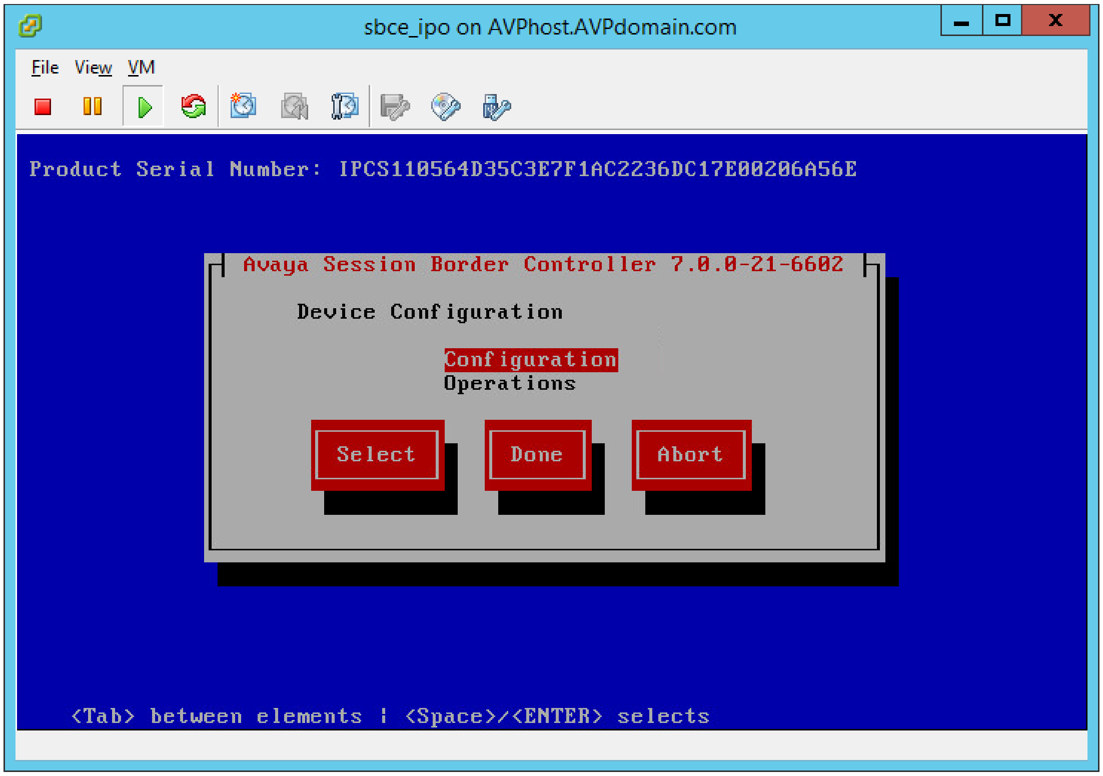
```
Product Seria   Avaya Session Border Controller 7.0.0-21-6602

            Select Time Zone

              Europe/Amsterdam
              Europe/Andorra
              Europe/Athens
              Europe/Belgrade
              Europe/Berlin
              Europe/Bratislava
              Europe/Brussels
              Europe/Bucharest
              Europe/Budapest
              Europe/Busingen

                   Select            Skip

  <Tab> between elements | <Space>/<ENTER> selects
```

14. Hit **Enter** on **Back**



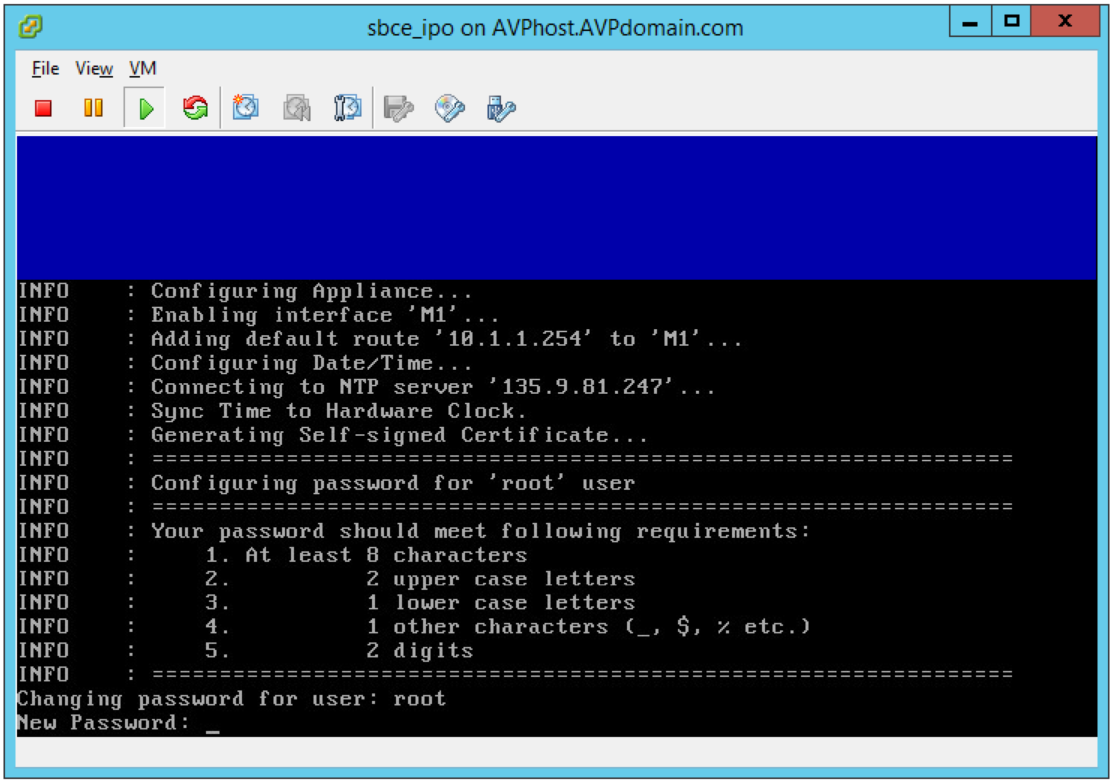
```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

Avaya Session Border Controller 7.0.0-21-6602

    Device Configuration

        Appliance Configuration
        Management Interface Setup
        Time Zone
        Self-Signed Certificate

<Tab> between elements | <Space>/<ENTER> selects
```

15. Hit **Enter** on **Done**



```
Product Serial Number: IPCS110564D35C3E7F1AC2236DC17E00206A56E

Avaya Session Border Controller 7.0.0-21-6602

    Device Configuration

            Configuration
            Operations

<Tab> between elements | <Space>/<ENTER> selects
```

16. Enter new **root** password

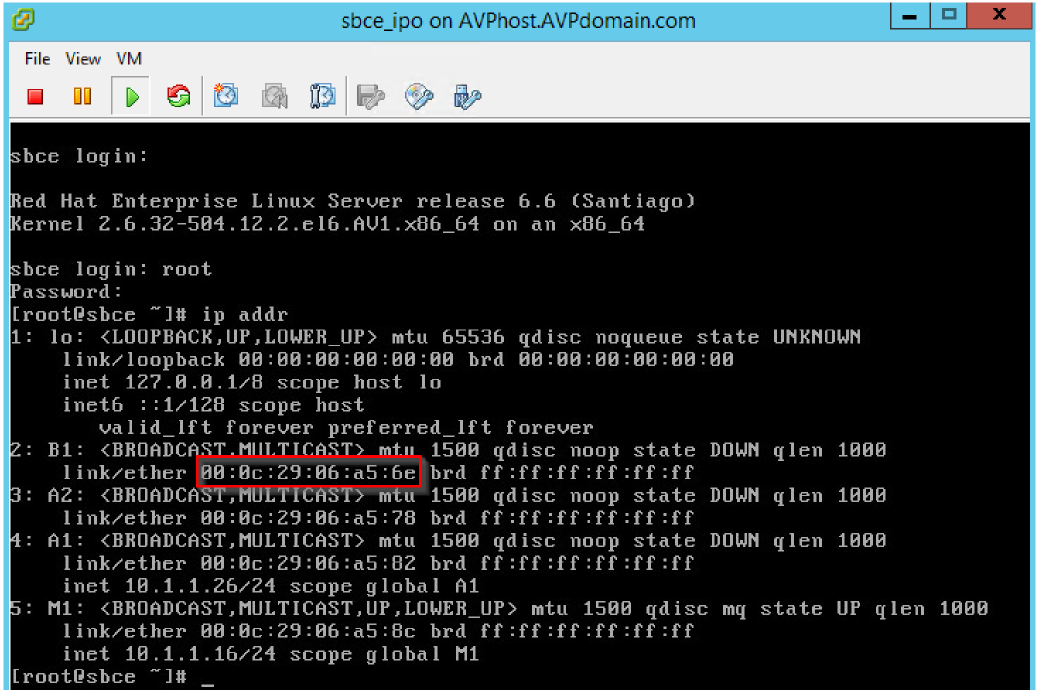


```
INFO     : Configuring Appliance...
INFO     : Enabling interface 'M1'...
INFO     : Adding default route '10.1.1.254' to 'M1'...
INFO     : Configuring Date/Time...
INFO     : Connecting to NTP server '135.9.81.247'...
INFO     : Sync Time to Hardware Clock.
INFO     : Generating Self-signed Certificate...
INFO     : ================================================================
INFO     : Configuring password for 'root' user
INFO     : ================================================================
INFO     : Your password should meet following requirements:
INFO     :     1. At least 8 characters
INFO     :     2.          2 upper case letters
INFO     :     3.          1 lower case letters
INFO     :     4.          1 other characters (_, $, % etc.)
INFO     :     5.          2 digits
INFO     : ================================================================
Changing password for user: root
New Password: _
```

17. Enter new password for **ipcs** login

Setting VMware network for external interface

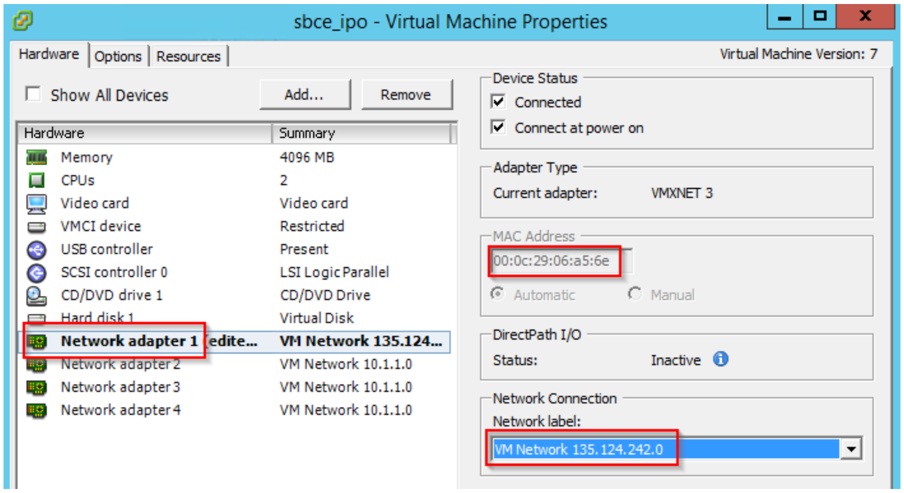
1. At the console login with **root** using the new password
2. Issue the command **ip addr** and note the **MAC** address of **B1** interface



```
sbce login:

Red Hat Enterprise Linux Server release 6.6 (Santiago)
Kernel 2.6.32-504.12.2.el6.AV1.x86_64 on an x86_64

sbce login: root
Password:
[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
    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:29:06:a5:6e brd ff:ff:ff:ff:ff:ff
3: A2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:0c:29:06:a5:78 brd ff:ff:ff:ff:ff:ff
4: A1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether 00:0c:29:06:a5:82 brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.26/24 scope global A1
5: M1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 00:0c:29:06:a5:8c brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.16/24 scope global M1
[root@sbce ~]# _
```

3.
4. In vSphere client right click on the SBCE VM and select **Edit Settings**

5. Select the **Network adapter** where MAC address matches the **MAC address of B1** interface, change the **Network Connection** and click **OK**



sbce_ipo - Virtual Machine Properties

Hardware | Options | Resources — Virtual Machine Version: 7

□ Show All Devices — Add... — Remove

Hardware	Summary
Memory	4096 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
USB controller	Present
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD Drive
Hard disk 1	Virtual Disk
Network adapter 1 (edite...	**VM Network 135.124...**
Network adapter 2	VM Network 10.1.1.0
Network adapter 3	VM Network 10.1.1.0
Network adapter 4	VM Network 10.1.1.0

Device Status
☑ Connected
☑ Connect at power on

Adapter Type
Current adapter: VMXNET 3

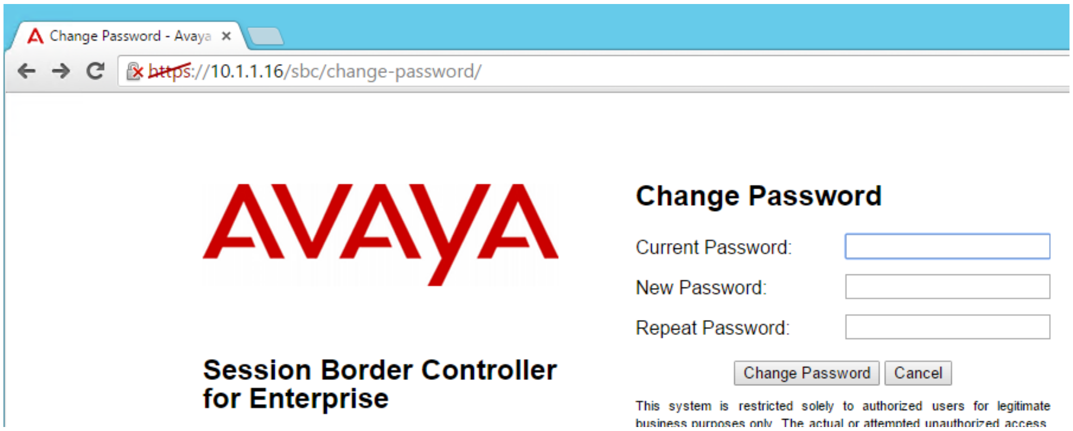
MAC Address
00:0c:29:06:a5:6e
● Automatic ○ Manual

DirectPath I/O
Status: Inactive

Network Connection
Network label:
VM Network 135.124.242.0

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



Change Password - Avaya ×

~~https~~://10.1.1.16/sbc/change-password/

AVAYA

Session Border Controller for Enterprise

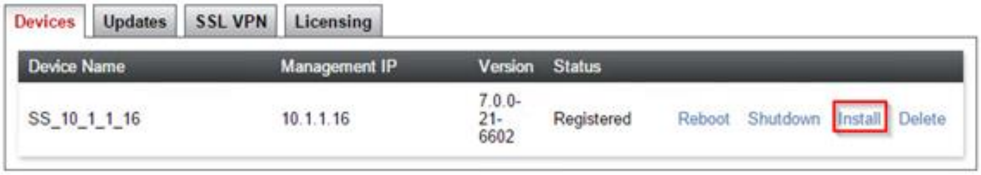
Change Password

Current Password:
New Password:
Repeat Password:

Change Password — Cancel

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access

4. Login again with ucsec using the new password
5. Go to **System Management** and click **Install**

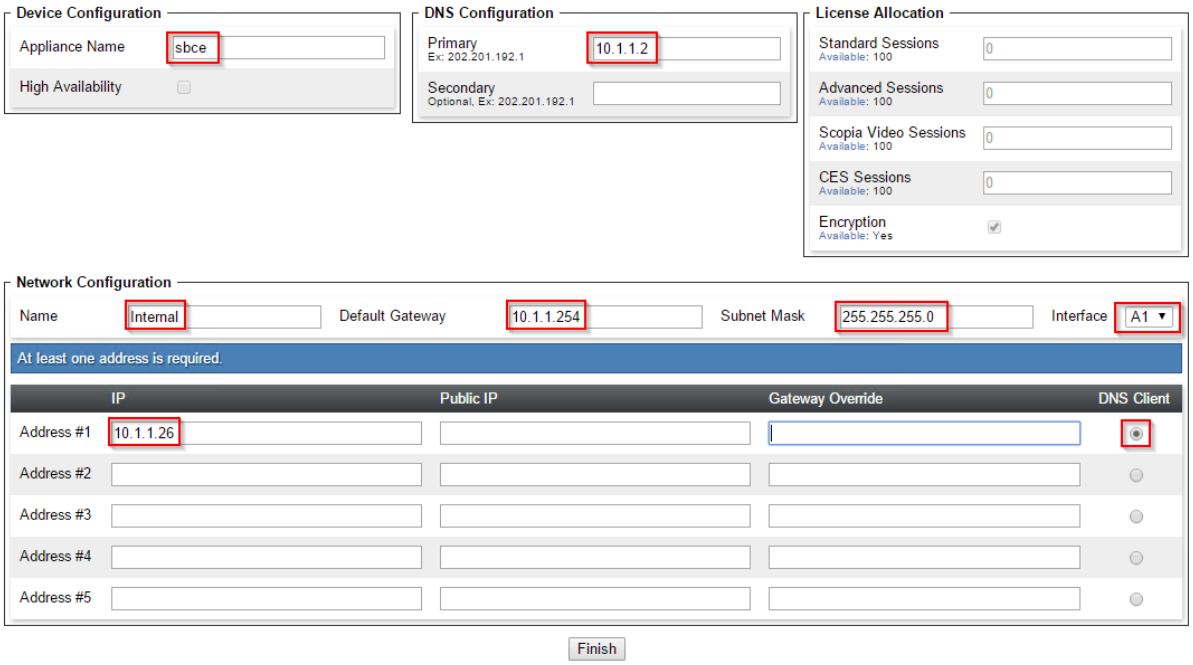


Devices | Updates | SSL VPN | Licensing

Device Name	Management IP	Version	Status				
SS_10_1_1_16	10.1.1.16	7.0.0-21-6602	Registered	Reboot	Shutdown	Install	Delete

6. Set the following fields:
   a. **Device Configuration**
      i. **Appliance Name**: internal name of the SBCE
   b. **DNS Configuration**
      i. **Primary**: IP of internal 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



Device Configuration

Appliance Name	sbce
High Availability	☐

DNS Configuration

Primary Ex: 202.201.192.1	10.1.1.2
Secondary Optional, Ex: 202.201.192.1	

License Allocation

Standard Sessions Available: 100	0
Advanced Sessions Available: 100	0
Scopia Video Sessions Available: 100	0
CES Sessions Available: 100	0
Encryption Available: Yes	☑

Network Configuration

Name: Internal | Default Gateway: 10.1.1.254 | Subnet Mask: 255.255.255.0 | Interface: A1

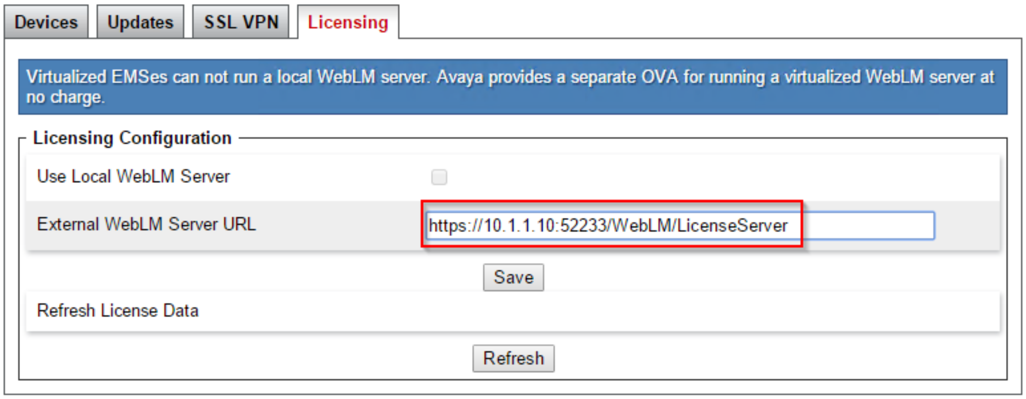
At least one address is required.

	IP	Public IP	Gateway Override	DNS Client
Address #1	10.1.1.26			●
Address #2				○
Address #3				○
Address #4				○
Address #5				○

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 external WebLM server
2. Go to **System Management / Licensing** tab
3. Enter the **External WebLM Server URL** and click **Save**



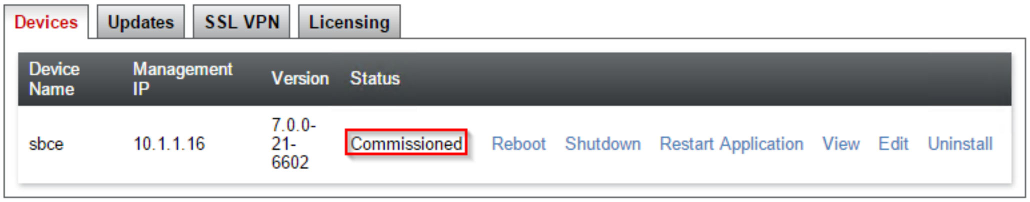
Virtualized EMSes can not run a local WebLM server. Avaya provides a separate OVA for running a virtualized WebLM server at no charge.

Licensing Configuration

Use Local WebLM Server	☐
External WebLM Server URL	https://10.1.1.10:52233/WebLM/LicenseServer

Refresh License Data

4. Verify that new device is in **Commissioned** state under **System Management / Devices** tab

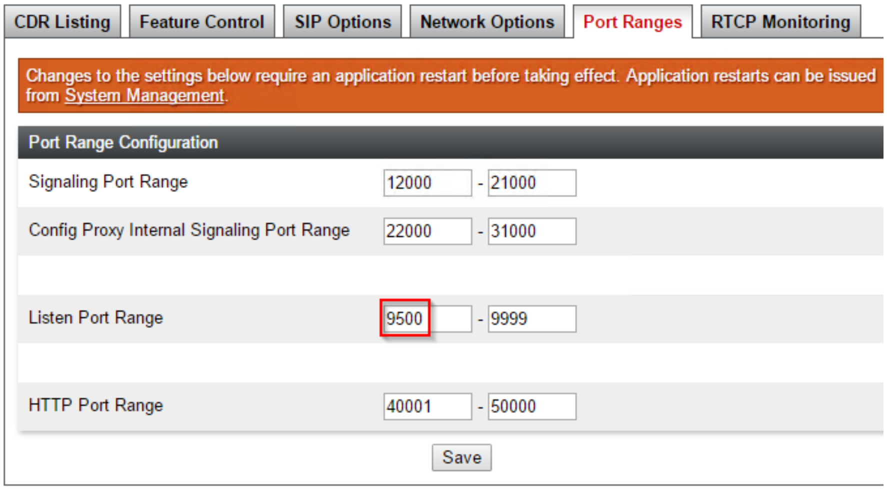


Device Name	Management IP	Version	Status						
sbce	10.1.1.16	7.0.0-21-6602	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Uninstall

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**



Changes to the settings below require an application restart before taking effect. Application restarts can be issued from System Management.

Port Range Configuration

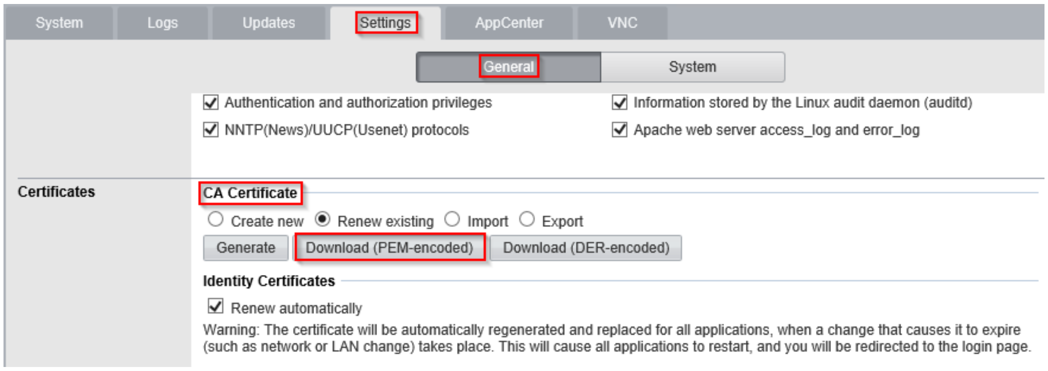
Signaling Port Range	12000	21000
Config Proxy Internal Signaling Port Range	22000	31000
Listen Port Range	9500	9999
HTTP Port Range	40001	50000

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

Certificates

Exporting IP Office Root CA

1. Open a browser and connect to https://<IPO_IP>: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



☑ Authentication and authorization privileges
☑ Information stored by the Linux audit daemon (auditd)
☑ NNTP(News)/UUCP(Usenet) protocols
☑ Apache web server access_log and error_log

Certificates

CA Certificate

○ Create new ● Renew existing ○ Import ○ Export

Identity Certificates

☑ Renew automatically

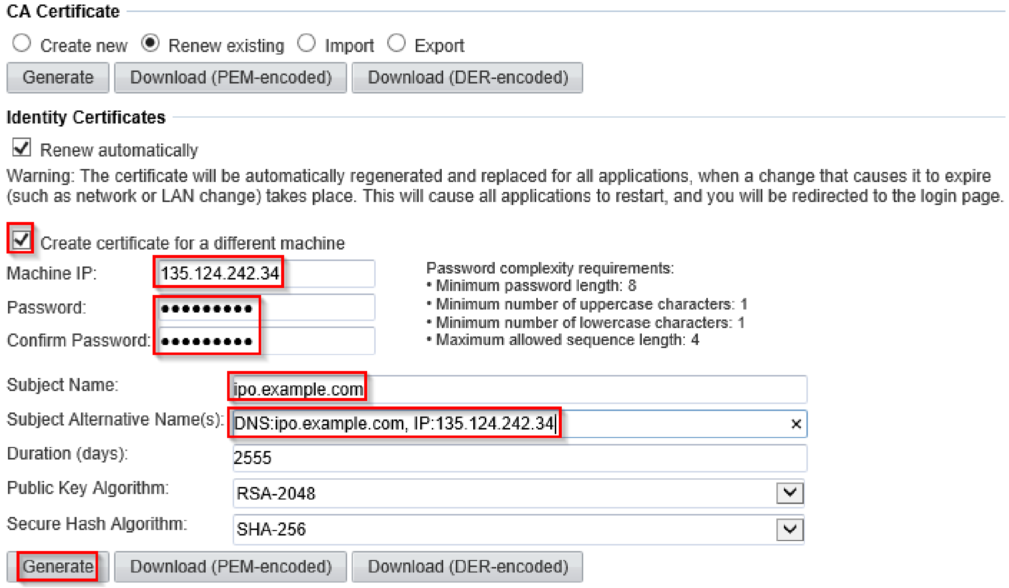
Warning: The certificate will be automatically regenerated and replaced for all applications, when a change that causes it to expire (such as network or LAN change) takes place. This will cause all applications to restart, and you will be redirected to the login page.

5. Rename the file on your PC to **IPO_RootCA.crt**

Generating Identity Certificate for SBCE

1. Open a browser and connect to https://<IPO_IP>: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 **Generate**
    a. **Machine IP**: external IP of SBCE
    b. **Password**: password to encrypt the certificate and key, for example **Avaya123$**
    c. **Subject Name**: name or FQDN of SBCE
    d. **Subject Alternative Name(s)**: list of DNS, IP or other entries

    NOTE: If you use different FQDN for One-X Portal, IP Office, XMPP and SIP domains, enter all FQDNs as a comma separated list of DNS entries in the Subject Alternate Name



CA Certificate

○ Create new ● Renew existing ○ Import ○ Export

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: 135.124.242.34

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: ipo.example.com

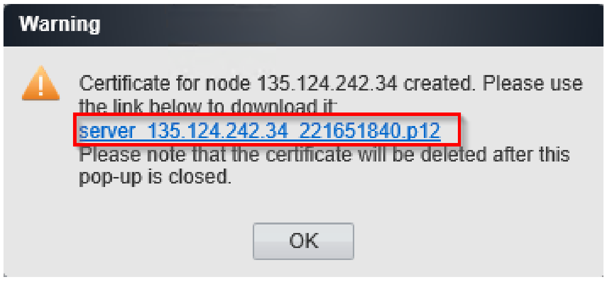
Subject Alternative Name(s): DNS:ipo.example.com, IP:135.124.242.34

Duration (days): 2555

Public Key Algorithm: RSA-2048

Secure Hash Algorithm: SHA-256

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



Warning

Certificate for node 135.124.242.34 created. Please use the link below to download it:
server_135.124.242.34_221651840.p12
Please note that the certificate will be deleted after this pop-up is closed.

7. Rename the downloaded file to **SBCE_ID.p12**

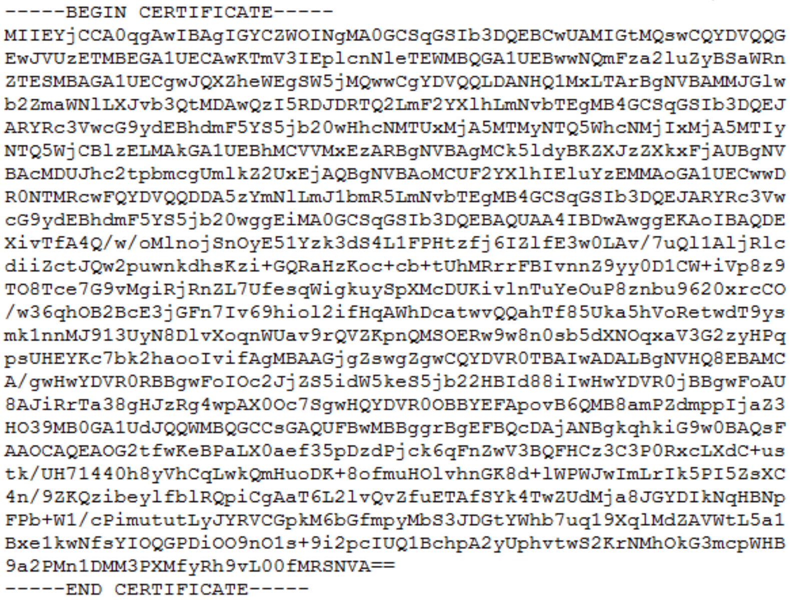
Extracting Private Key and Identity Certificate

1. Open WinSCP to SBCE **Management IP** using port **222** and **ipcs** login
2. Copy **SBCE_ID.p12** from your PC to SBCE /tmp directory
3. Ssh to SBCE **Management IP** using port **222** and **ipcs** login
4. Issue command **sudo su** and type the root password

5. Issue the commands in bold:

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

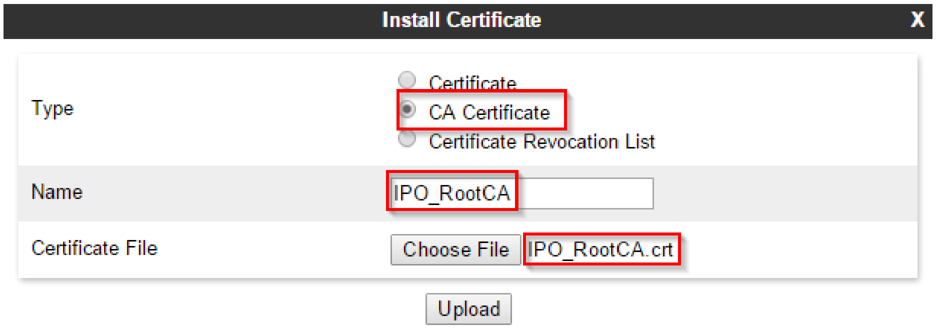
6. Copy the new **SBCE_ID.crt** and **SBCE_ID.key** files from SBCE to your PC
7. The SBCE_ID.crt file will contain the ID certificate we generated for SBCE, the IPO root CA certificate, and the private key. To be able to properly import this file on SBCE, the CA certificate and the private key must be removed from this file. Open SBCE_ID.crt in WordPad on your PC, and remove all lines except those which are between the **first** BEGIN CERTIFICATE / END CERTIFICATE lines. Result file should look something similar:



```
-----BEGIN CERTIFICATE-----
MIIEYjCCA0qgAwIBAgIGYCZWOINgMA0GCSqGSIb3DQEBCwUAMIGtMQswCQYDVQQG
EwJVUzETMBEGA1UECAwKTmV3IEplcnNleTEWMBQGA1UEBwwNQmFza2luZyBSaWRn
ZTESMBAGA1UECgwJQXZheWEgSW5jMQwwCgYDVQQLDANHQ1MxLTArBgNVBAMMJGlw
b2ZmaWNlLXJvb3QtMDAwQzI5RDJDRTQ2LmF2YXlhLmNvbTEgMB4GCSqGSIb3DQEJ
ARYRc3VwcG9ydEBhdmF5YS5jb20wHhcNMTUxMjA5MTMyNTQ5WhcNMjIxMjA5MTIy
NTQ5WjCBlzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCk5ldyBKZXJzZXkxFjAUBgNV
BAcMDUJhc2tpbmcgUmlkZ2UxEjAQBgNVBAoMCUF2YXlhIEluYzEMMAoGA1UECwwD
R0NTMRcwFQYDVQQDDA5zYmNlLmJ1bmR5LmNvbTEgMB4GCSqGSIb3DQEJARYRc3Vw
cG9ydEBhdmF5YS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDE
XivTfA4Q/w/oMlnojSnOyE51Yzk3dS4L1FPHtzfj6IZlfE3w0LAv/7uQl1AljRlc
diiZctJQw2puwnkdhsKzi+GQRaHzKoc+cb+tUhMRrrFBIvnnZ9yy0D1CW+iVp8z9
TO8Tce7G9vMgiRjRnZL7UfesqWigkuySpXMcDUKivlnTuYeOuP8znbu9620xrcCO
/w36qhOB2BcE3jGFn7Iv69hiol2ifHqAWhDcatwvQQahTf85Uka5hVoRetwdT9ys
mk1nnMJ913UyN8DlvXoqnWUav9rQVZKpnQMSOERw9w8n0sb5dXNOqxaV3G2zyHPq
psUHEYKc7bk2haooIvifAgMBAAGjgZswgZgwCQYDVR0TBAIwADALBgNVHQ8EBAMC
A/gwHwYDVR0RBBgwFoIOc2JjZS5idW5keS5jb22HBId88iIwHwYDVR0jBBgwFoAU
8AJiRrTa38gHJzRg4wpAX0Oc7SgwHQYDVR0OBBYEFApovB6QMB8amPZdmppIjaZ3
HO39MB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjANBgkqhkiG9w0BAQsF
AAOCAQEAOG2tfwKeBPaLX0aef35pDzdPjck6qFnZwV3BQFHCz3C3P0RxcLXdC+us
tk/UH71440h8yVhCqLwkQmHuoDK+8ofmuHOlvhnGK8d+1WPWJwImLrIk5PI5ZsXC
4n/9ZKQzibeylfblRQpiCgAaT6L2lvQvZfuETAfSYk4TwZUdMja8JGYDIkNqHBNp
FPb+W1/cPimututLyJYRVCGpkM6bGfmpyMbS3JDGtYWhb7uq19XqlMdZAVWtL5a1
Bxe1kwNfsYIOQGPDiOO9nO1s+9i2pcIUQ1BchpA2yUphvtwS2KrNMhOkG3mcpWHB
9a2PMn1DMM3PXMfyRh9vL00fMRSNVA==
-----END CERTIFICATE-----
```

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. **Certificate File**: click **Choose File** and open **IPO_RootCA.crt**



Install Certificate X

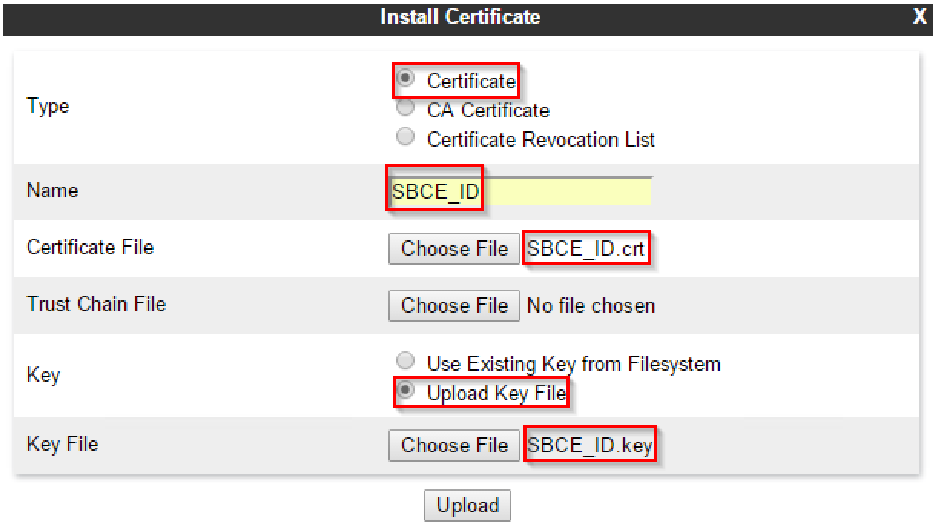
Type	○ Certificate ● CA Certificate ○ Certificate Revocation List
Name	IPO_RootCA
Certificate File	Choose File IPO_RootCA.crt

Upload

5. 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**: descriptive name for the SBCE identity certificate, for example **SBCE_ID**
    c. **Certificate File**: click **Choose File** and open **SBCE_ID.crt**
    d. **Trust Chain File**: leave empty
    e. **Key:** select **Upload Key File**
    f. **Key File**: click **Choose File** and open **SBCE_ID.key**



Install Certificate X

Type	● Certificate ○ CA Certificate ○ Certificate Revocation List
Name	SBCE_ID
Certificate File	Choose File SBCE_ID.crt
Trust Chain File	Choose File No file chosen
Key	○ Use Existing Key from Filesystem ● Upload Key File
Key File	Choose File SBCE_ID.key

Upload

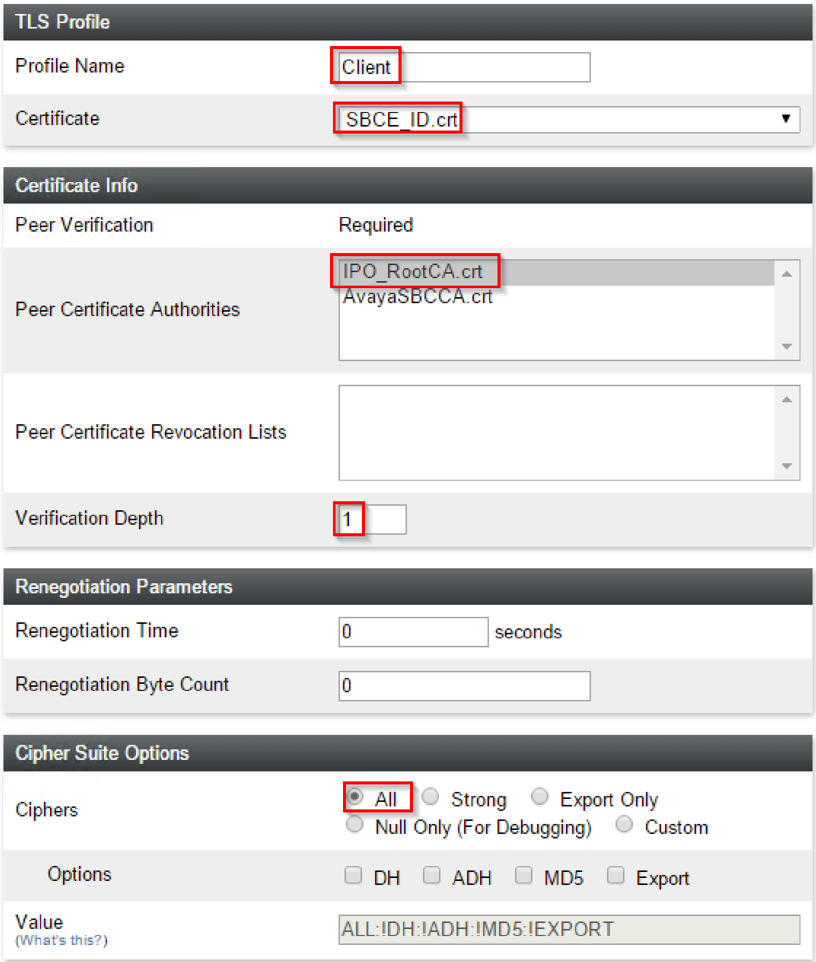
5. Certificate will be displayed, click **Install,** then **Finish**
6. Ssh to SBCE **Management IP** using port **222** and **ipcs** login
7. Issue command **sudo su** and type the root password
8. Issue the commands in bold:

```
[root@sbce ipcs]# cd /usr/local/ipcs/cert/key
[root@sbce key]# enc_key SBCE_ID.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 **Finish**
    a. **Profile Name:** descriptive name
    b. **Certificate:** select **SBCE_ID.crt**
    c. **Peer Certificate Authorities:** select **IPO_RootCA.crt**
    d. **Verification Depth:** enter **1**
    e. **Ciphers:** select **All**



TLS Profile

Profile Name	Client
Certificate	SBCE_ID.crt ▼

Certificate Info

Peer Verification	Required
Peer Certificate Authorities	IPO_RootCA.crt AvayaSBCCA.crt
Peer Certificate Revocation Lists	
Verification Depth	1

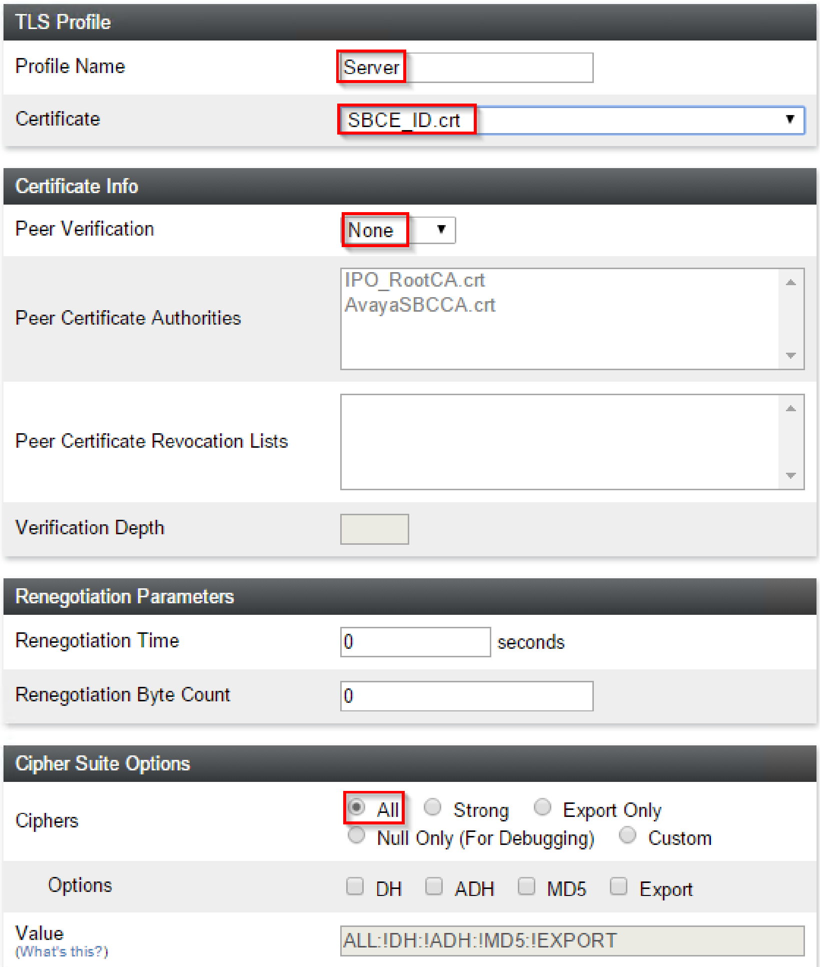
Renegotiation Parameters

Renegotiation Time	0 seconds
Renegotiation Byte Count	0

Cipher Suite Options

Ciphers	● All ○ Strong ○ Export Only ○ Null Only (For Debugging) ○ Custom
Options	□ DH □ ADH □ MD5 □ Export
Value (What's this?)	ALL:!DH:!ADH:!MD5:!EXPORT

4. Go to **TLS Management / Server Profiles** and click **Add**
5. Enter the following data then click **Finish**
    a. **Profile Name:** descriptive name
    b. **Certificate:** select **SBCE_ID.crt**
    c. **Peer Verification:** select **None**
    d. **Ciphers:** select **All**



TLS Profile

Profile Name	Server
Certificate	SBCE_ID.crt

Certificate Info

Peer Verification	None
Peer Certificate Authorities	IPO_RootCA.crt AvayaSBCCA.crt
Peer Certificate Revocation Lists	
Verification Depth	

Renegotiation Parameters

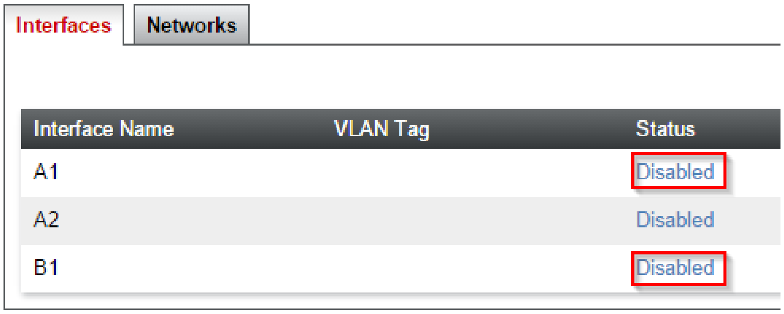
Renegotiation Time	0 seconds
Renegotiation Byte Count	0

Cipher Suite Options

Ciphers	● All ○ Strong ○ Export Only ○ Null Only (For Debugging) ○ Custom
Options	□ DH □ ADH □ MD5 □ Export
Value (What's this?)	ALL:!DH:!ADH:!MD5:!EXPORT

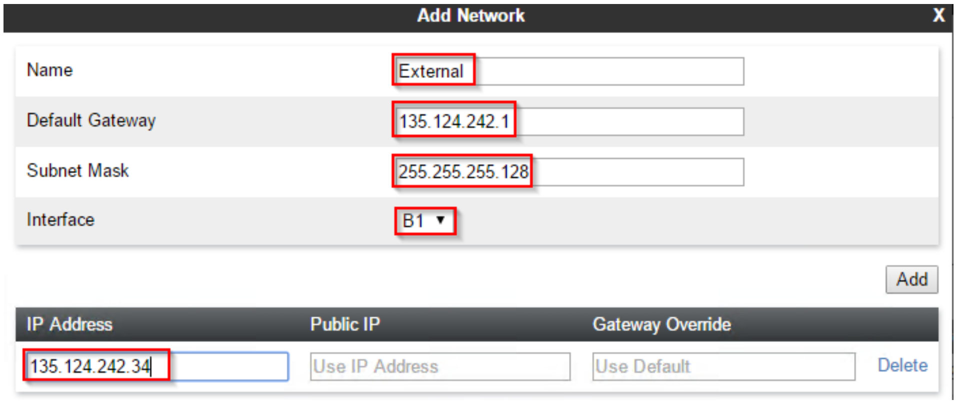
External Interface

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



Add Network

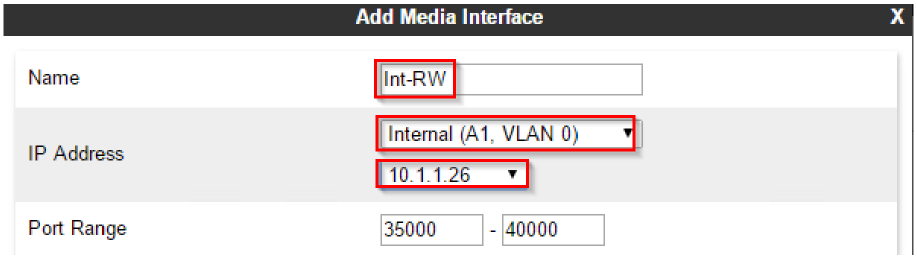
Name	External
Default Gateway	135.124.242.1
Subnet Mask	255.255.255.128
Interface	B1

IP Address	Public IP	Gateway Override
135.124.242.34	Use IP Address	Use Default

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

Media Interfaces

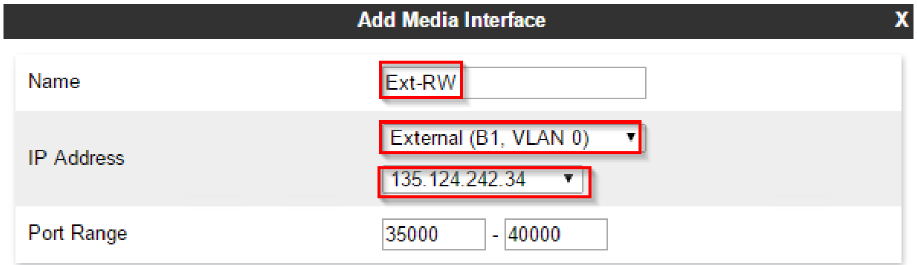
1. Go to **Device Specific Settings / Media Interface** and click **Add**
2. Set **Name** for internal interface, choose **A1** from the drop down of **IP Address** then click **Finish**



Add Media Interface

Name	Int-RW
IP Address	Internal (A1, VLAN 0) 10.1.1.26
Port Range	35000 - 40000

3. Repeat above to add external media interface, choose **B1** this time

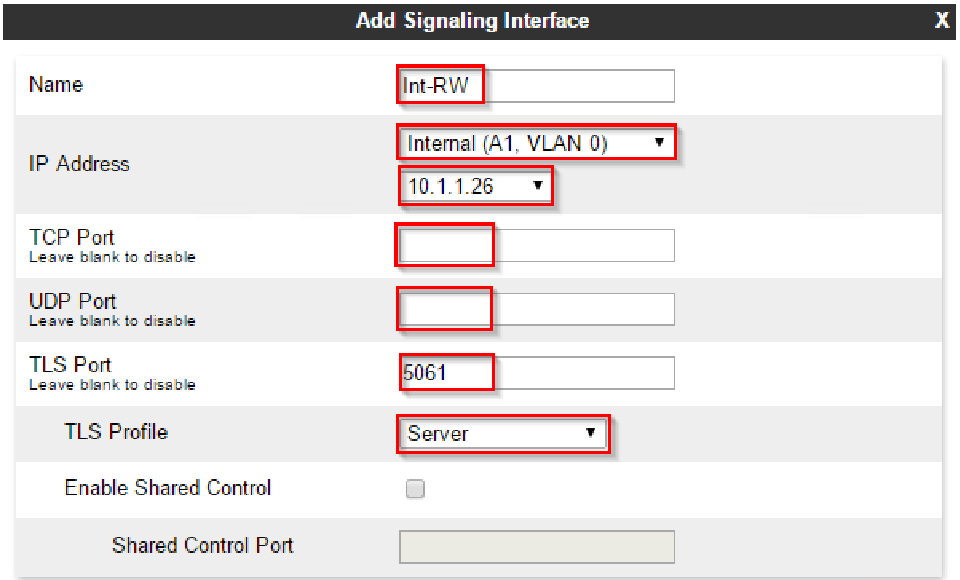


Add Media Interface

Name	Ext-RW
IP Address	External (B1, VLAN 0) 135.124.242.34
Port Range	35000 - 40000

Signaling Interfaces

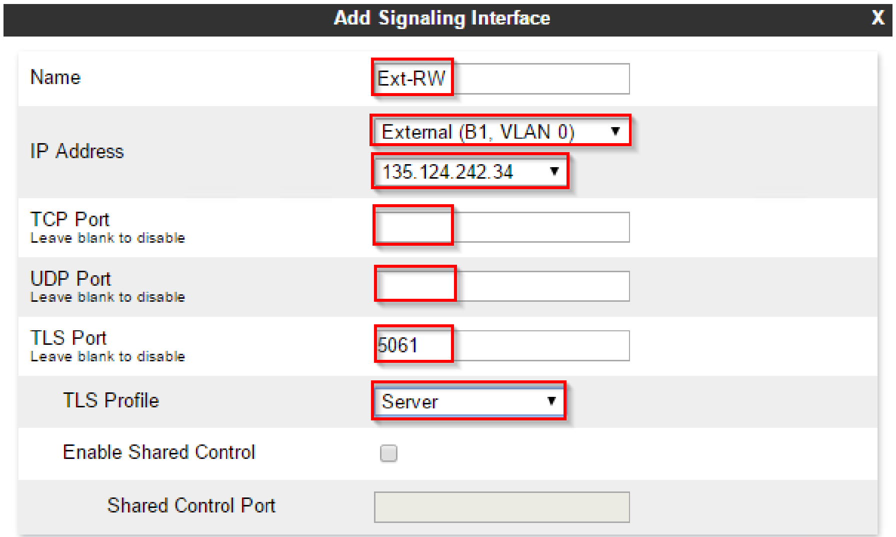
1. Go to **Device Specific Settings / Signaling Interface** and click **Add**
2. Set **Name** for internal interface, choose **A1** from the drop down of **IP Address,** remove TCP and UDP port, set **TLS Port**, select **Server** for **TLS Profile**, then click **Finish**



Add Signaling Interface

Name	Int-RW
IP Address	Internal (A1, VLAN 0) 10.1.1.26
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	Server
Enable Shared Control	□
Shared Control Port	

3. Repeat above to add external media interface, choose **B1** this time

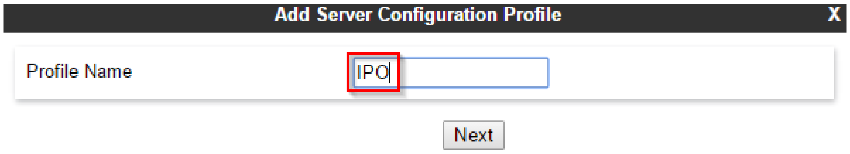


Add Signaling Interface

Name	Ext-RW
IP Address	External (B1, VLAN 0) 135.124.242.34
TCP Port Leave blank to disable	
UDP Port Leave blank to disable	
TLS Port Leave blank to disable	5061
TLS Profile	Server
Enable Shared Control	□
Shared Control Port	

Server Profile

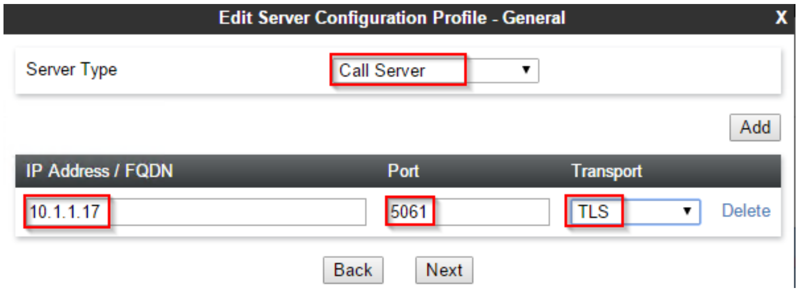
1. Go to **Global Profiles / Server Configuration** and click **Add**
2. Enter **Profile Name** and click **Next**



Add Server Configuration Profile

Profile Name	IPO

3. Set **Server Type** to **Call Server**, enter **IP/Port/Transport** and click **Next**

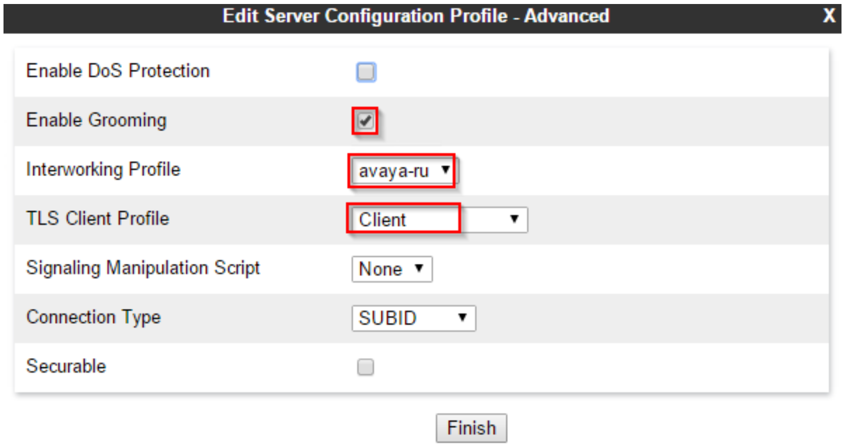


Edit Server Configuration Profile - General

Server Type	Call Server

IP Address / FQDN	Port	Transport	
10.1.1.17	5061	TLS	Delete

4. Authentication is not needed toward IPO so just click **Next**
5. Heartbeat is not needed, just click **Next**
6. Check-in **Enable Grooming** (SBCE will reuse TCP socket, without this option requests coming from IPO might be denied by SBCE), set **Interworking Profile** to **avaya-ru**, set **TLS Client Profile** to **Client**, then click **Finish**

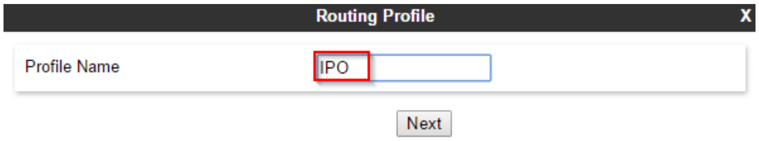


Edit Server Configuration Profile - Advanced

Enable DoS Protection	☐
Enable Grooming	☑
Interworking Profile	avaya-ru
TLS Client Profile	Client
Signaling Manipulation Script	None
Connection Type	SUBID
Securable	☐

Routing

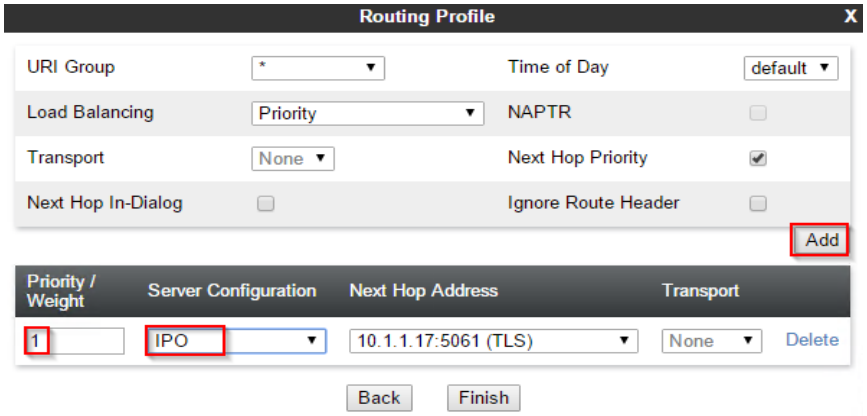
1. Go to **Global Profiles / Routing** and click **Add**
2. Enter **Profile Name** and click **Next**



Routing Profile

Profile Name	IPO

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



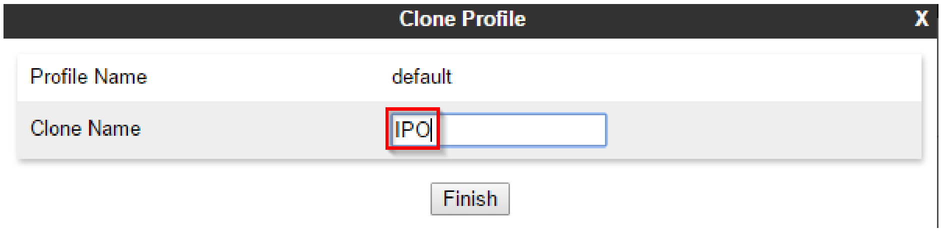
Routing Profile

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	☐
Transport	None	Next Hop Priority	☑
Next Hop In-Dialog	☐	Ignore Route Header	☐

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	IPO	10.1.1.17:5061 (TLS)	None	Delete

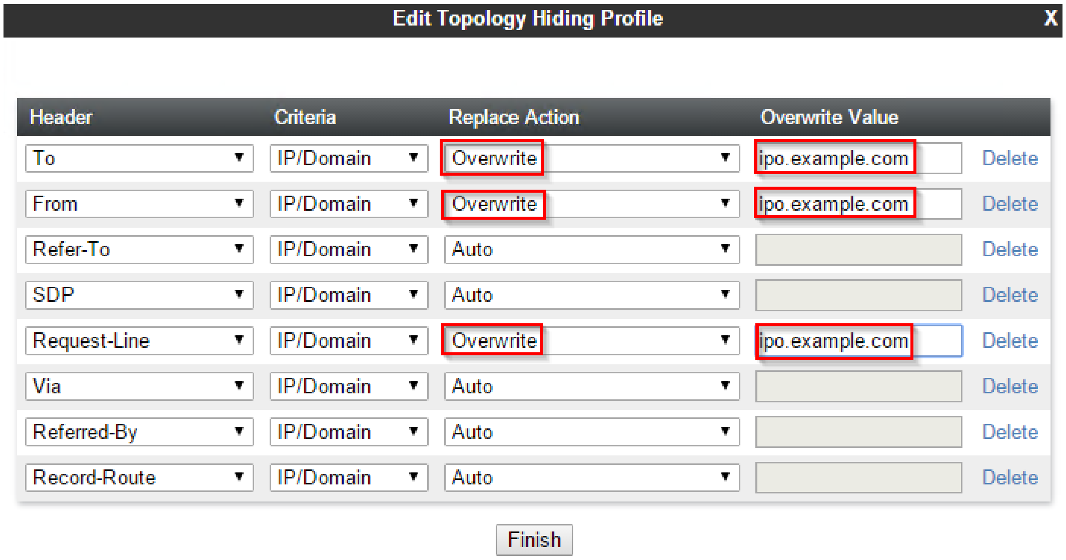
Topology Hiding

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



Profile Name	default
Clone Name	IPO

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

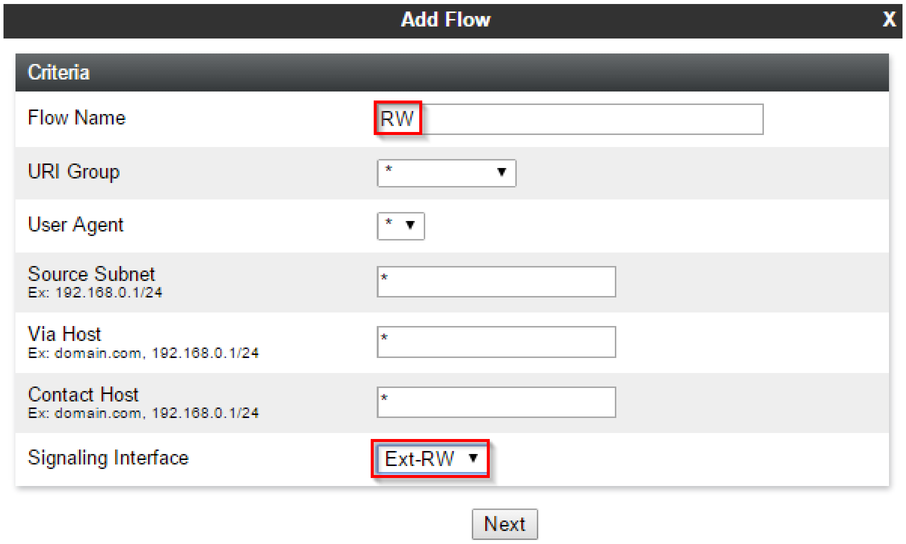


Header	Criteria	Replace Action	Overwrite Value	
To	IP/Domain	Overwrite	ipo.example.com	Delete
From	IP/Domain	Overwrite	ipo.example.com	Delete
Refer-To	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Request-Line	IP/Domain	Overwrite	ipo.example.com	Delete
Via	IP/Domain	Auto		Delete
Referred-By	IP/Domain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

NOTE: We need this modified topology hiding because using the default topology hiding, during the registration of Communicator for Windows, the IPO would include the internal IP address instead of XMPP domain in the onex_server field of the 200 OK xml body. As a result the client would not be able to register to One-X Portal and would not have presence.

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**

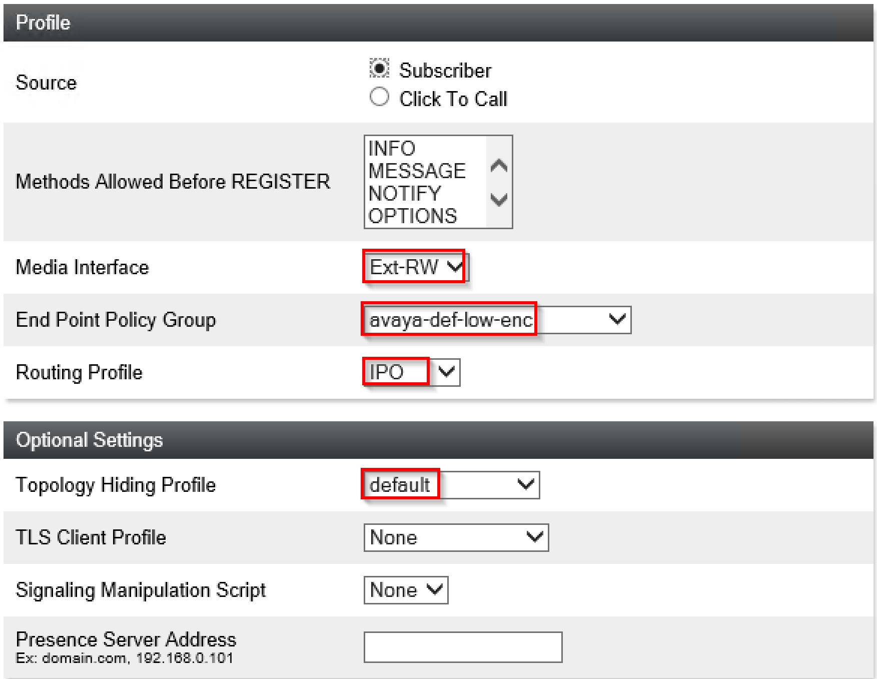


Add Flow

Criteria

Flow Name	RW
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-RW

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	● Subscriber ○ Click To Call
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	Ext-RW
End Point Policy Group	avaya-def-low-enc
Routing Profile	IPO

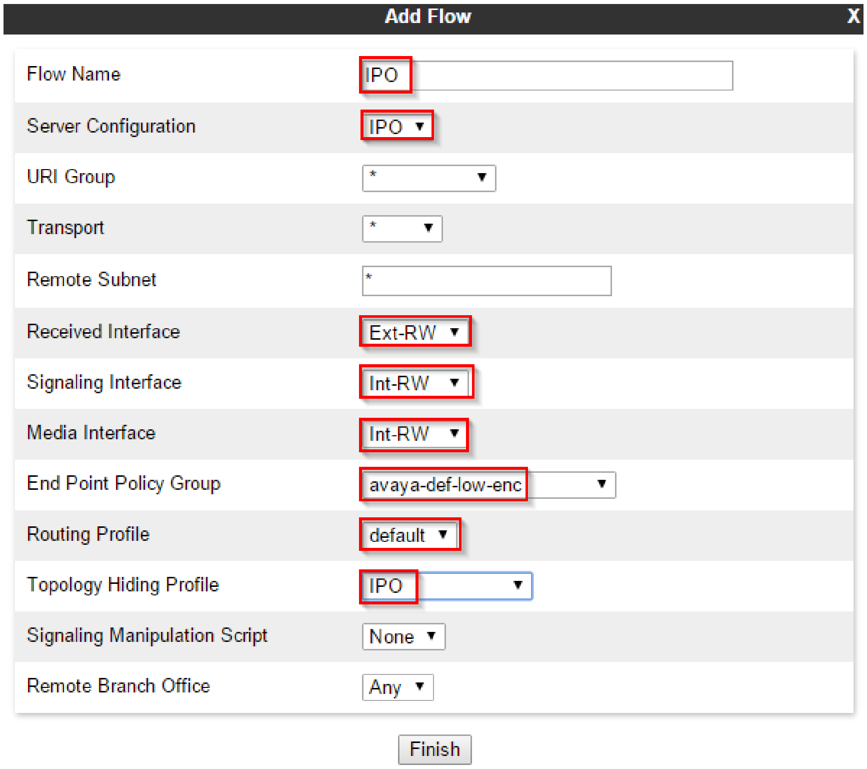
Optional Settings

Topology Hiding Profile	default
TLS Client Profile	None
Signaling Manipulation Script	None
Presence Server Address Ex: domain.com, 192.168.0.101	

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**



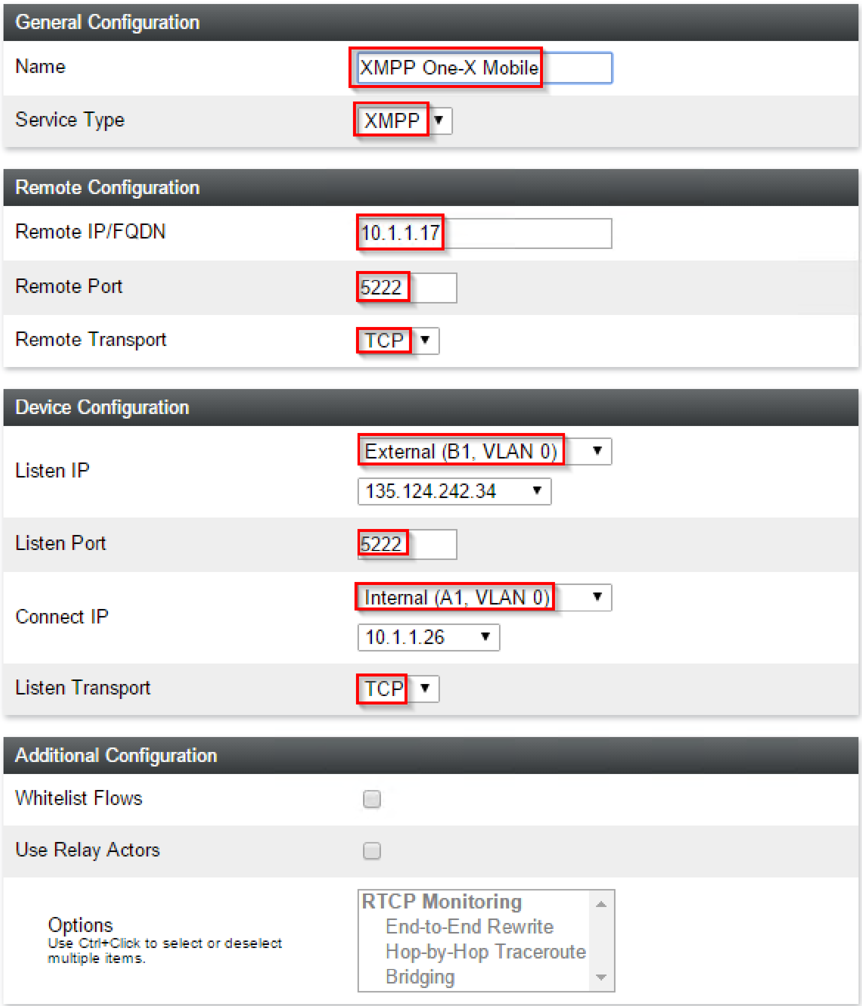
Add Flow

Flow Name	IPO
Server Configuration	IPO
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext-RW
Signaling Interface	Int-RW
Media Interface	Int-RW
End Point Policy Group	avaya-def-low-enc
Routing Profile	default
Topology Hiding Profile	IPO
Signaling Manipulation Script	None
Remote Branch Office	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 **XMPP**
    - c. **Remote IP/FQDN**: enter the IP of **One-X Portal** (same as IPO in our case)
    - 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	XMPP One-X Mobile
Service Type	XMPP ▾

Remote Configuration

Remote IP/FQDN	10.1.1.17
Remote Port	5222
Remote Transport	TCP ▾

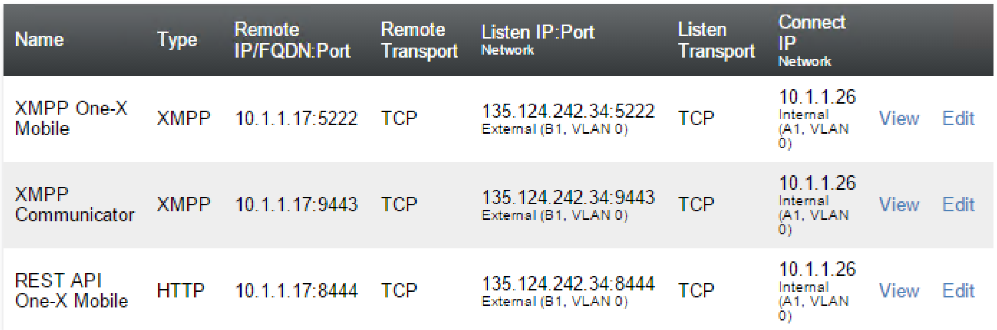
Device Configuration

Listen IP	External (B1, VLAN 0) ▾ 135.124.242.34 ▾
Listen Port	5222
Connect IP	Internal (A1, VLAN 0) ▾ 10.1.1.26 ▾
Listen Transport	TCP ▾

Additional Configuration

Whitelist Flows	□
Use Relay Actors	□
Options Use Ctrl+Click to select or deselect multiple items.	RTCP Monitoring End-to-End Rewrite Hop-by-Hop Traceroute Bridging

3. Repeat the above procedure for port 9443 (XMPP) and 8444 (HTTP)



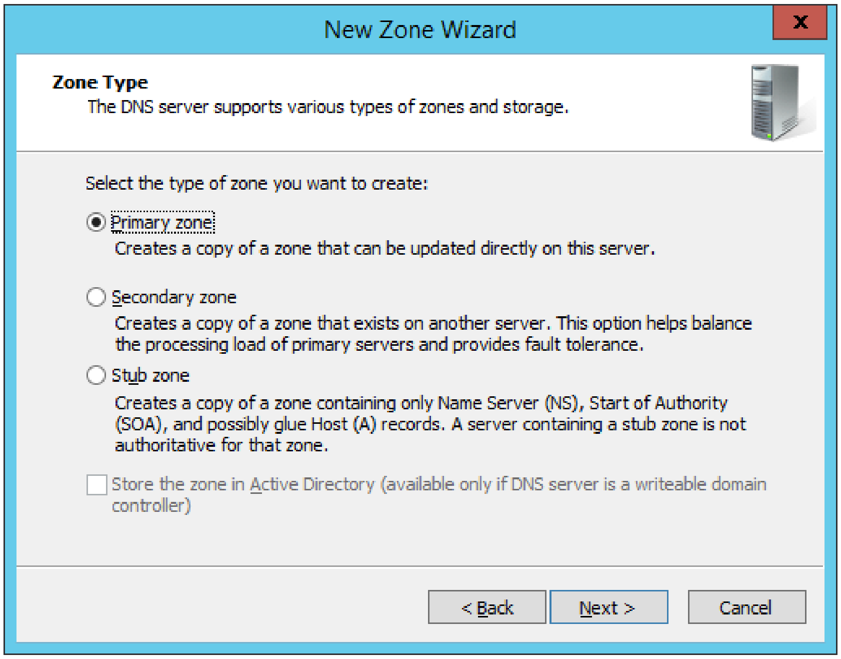
Name	Type	Remote IP/FQDN:Port	Remote Transport	Listen IP:Port Network	Listen Transport	Connect IP Network		
XMPP One-X Mobile	XMPP	10.1.1.17:5222	TCP	135.124.242.34:5222 External (B1, VLAN 0)	TCP	10.1.1.26 Internal (A1, VLAN 0)	View	Edit
XMPP Communicator	XMPP	10.1.1.17:9443	TCP	135.124.242.34:9443 External (B1, VLAN 0)	TCP	10.1.1.26 Internal (A1, VLAN 0)	View	Edit
REST API One-X Mobile	HTTP	10.1.1.17:8444	TCP	135.124.242.34:8444 External (B1, VLAN 0)	TCP	10.1.1.26 Internal (A1, VLAN 0)	View	Edit

DNS Configuration

Installation and configuration of DNS servers is out of scope of this document, but we will cover through some example screenshots the important configurations, which are needed for the clients to be able to register locally and remotely. The examples are form DNS servers running on Windows 2012 R2.

Configuration using single FQDN for XMPP, SIP domain and hostname:

1. Add a new Forward Lookup Zone for the FQDN ipo.example.com



Zone Type

The DNS server supports various types of zones and storage.

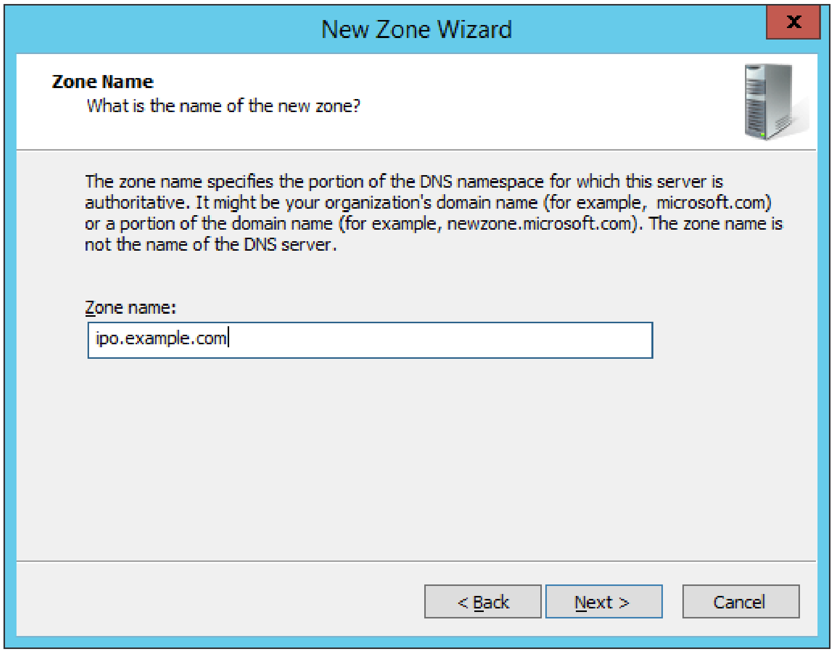
Select the type of zone you want to create:

● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

□ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

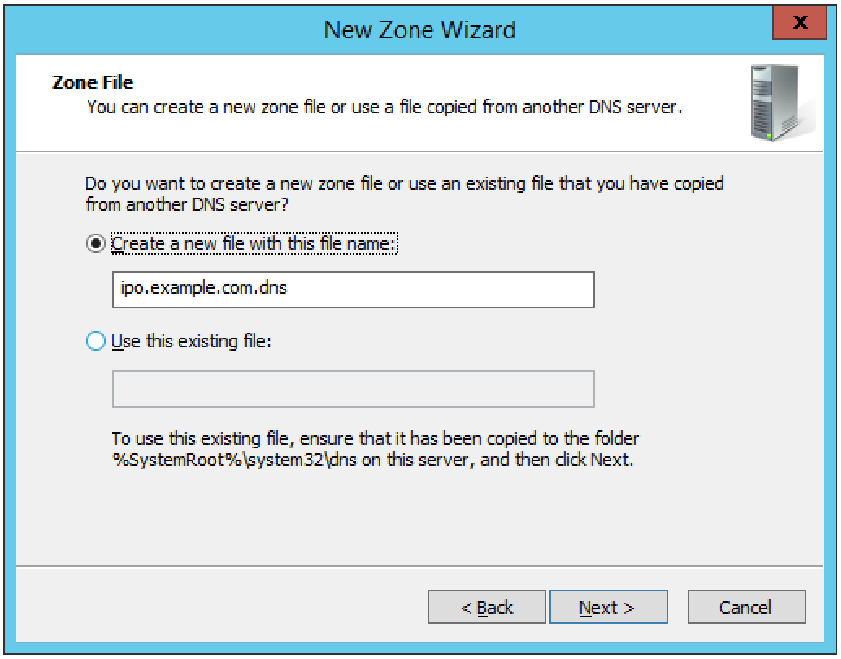


Zone Name

What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: ipo.example.com



Zone File

You can create a new zone file or use a file copied from another DNS server.

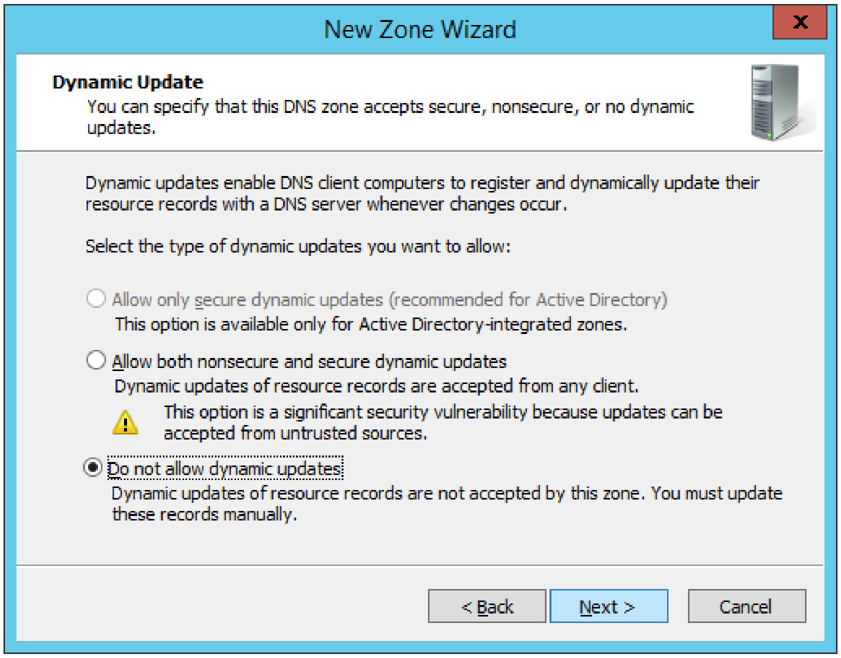
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

● Create a new file with this file name:

ipo.example.com.dns

○ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.



Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

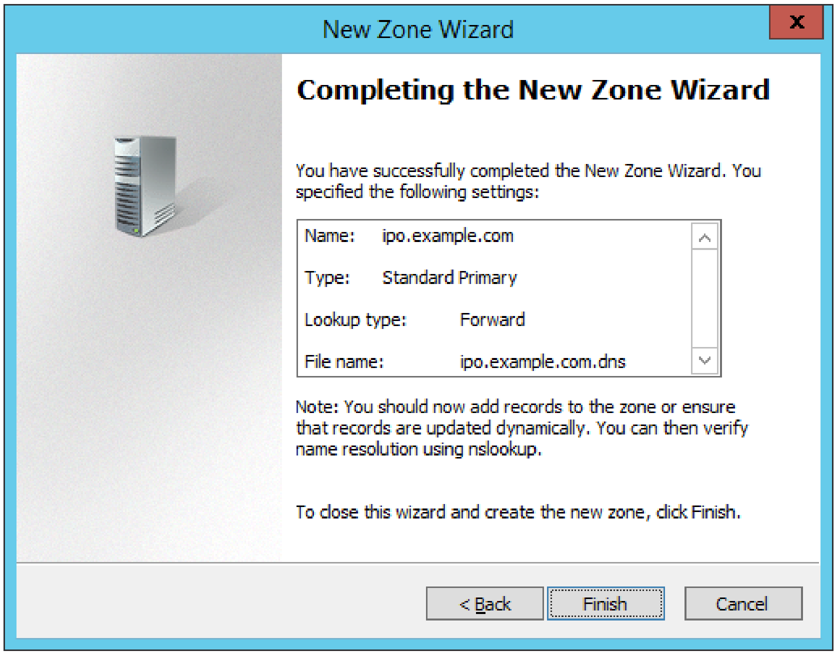
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

○ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

● Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.



New Zone Wizard

Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name: ipo.example.com

Type: Standard Primary

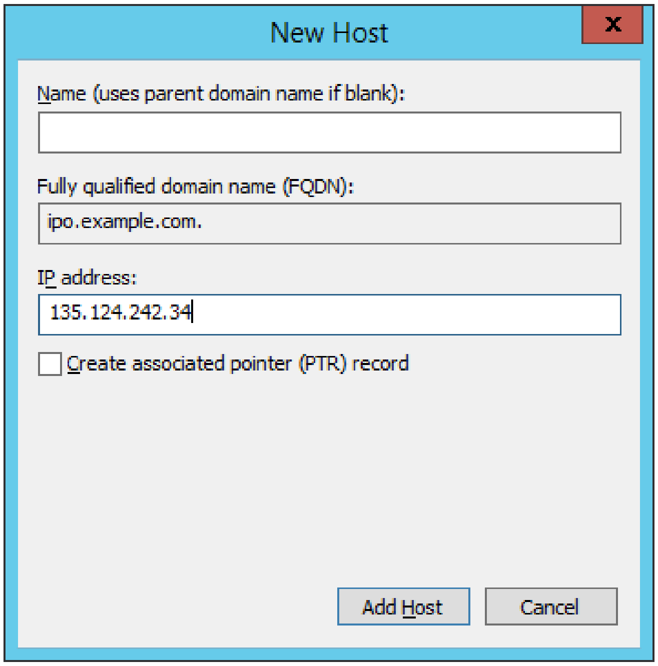
Lookup type: Forward

File name: ipo.example.com.dns

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

2. Add an **A** record **without** name



New Host

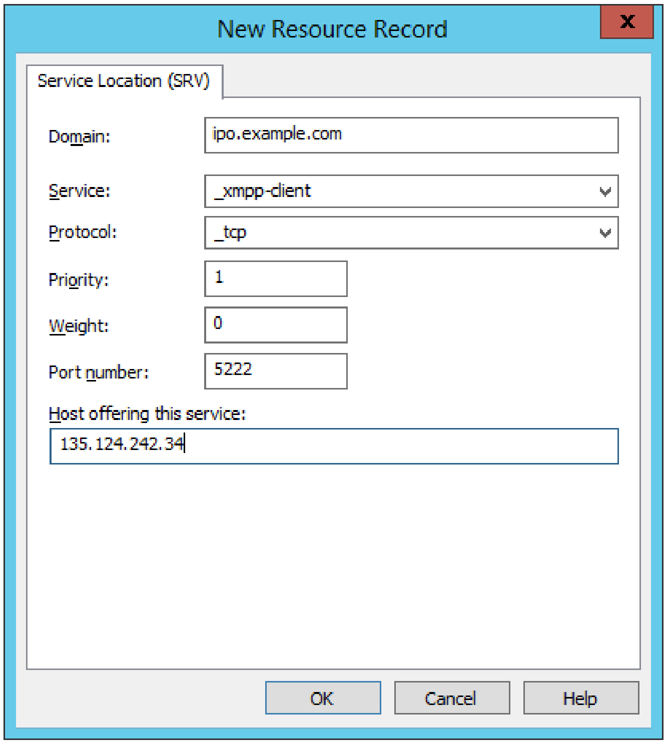
Name (uses parent domain name if blank):

Fully qualified domain name (FQDN): ipo.example.com.

IP address: 135.124.242.34

□ Create associated pointer (PTR) record

3. Add **_xmpp-client._tcp** and **_sip._tls SRV** records



Domain: ipo.example.com

Service: _xmpp-client

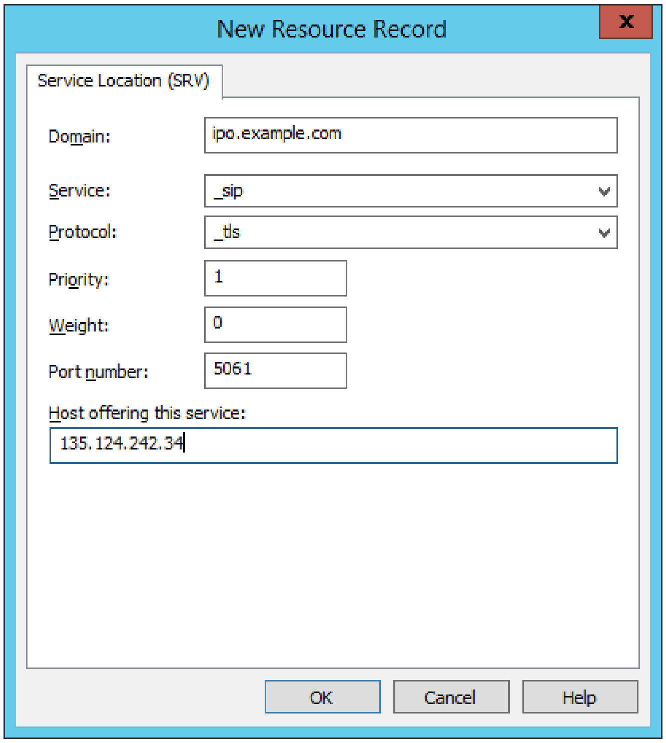
Protocol: _tcp

Priority: 1

Weight: 0

Port number: 5222

Host offering this service: 135.124.242.34



Domain: ipo.example.com

Service: _sip

Protocol: _tls

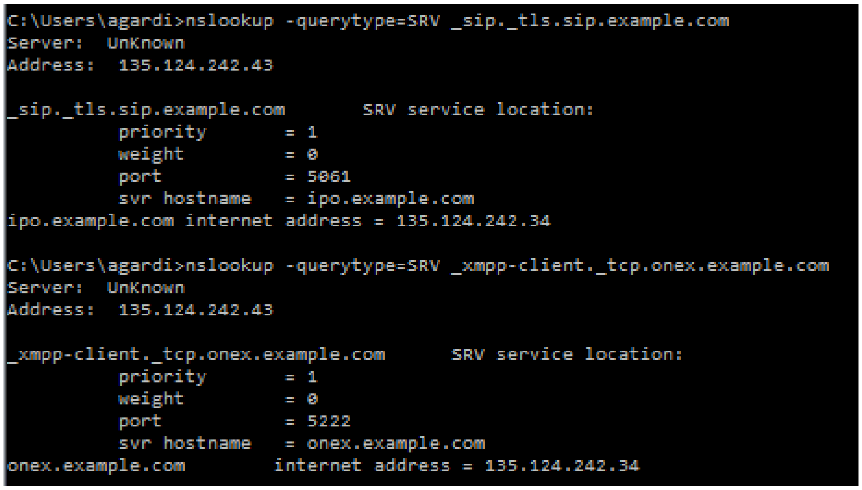
Priority: 1

Weight: 0

Port number: 5061

Host offering this service: 135.124.242.34

4. Verify DNS

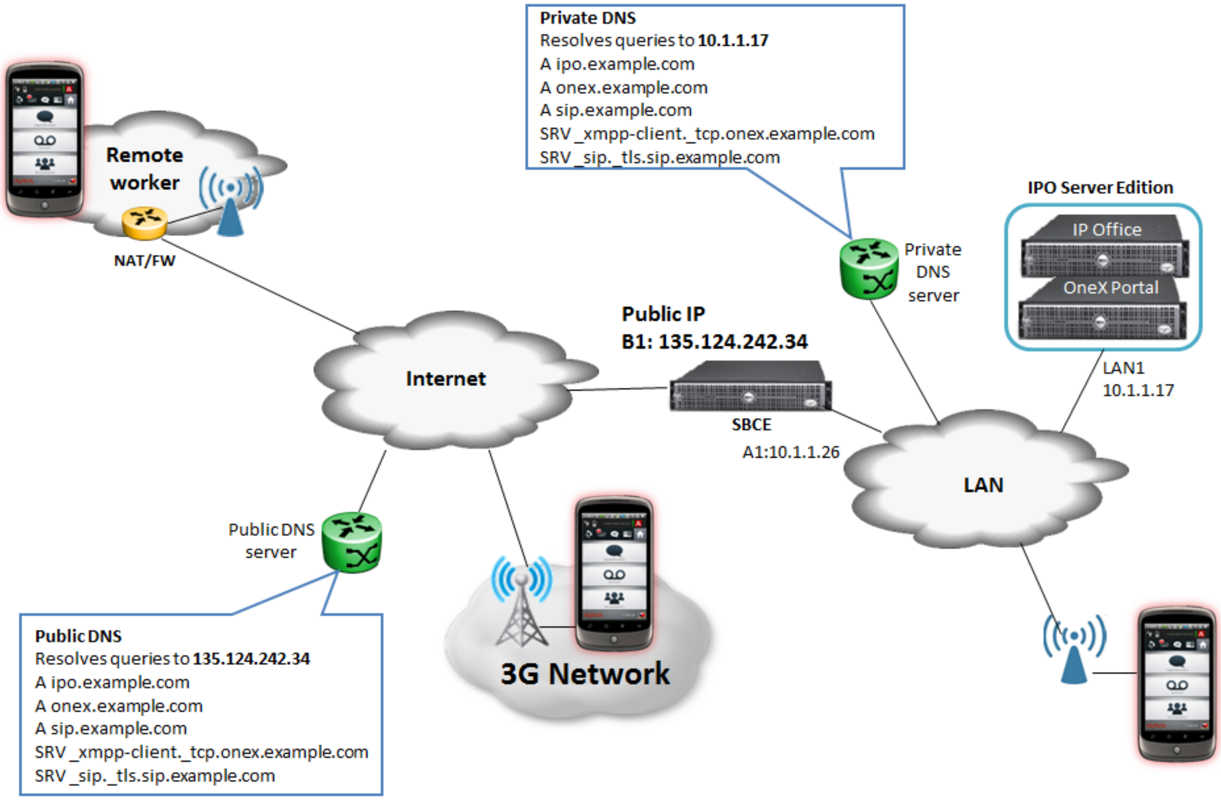


```
C:\Users\agardi>nslookup -querytype=SRV _sip._tls.sip.example.com
Server:  UnKnown
Address:  135.124.242.43

_sip._tls.sip.example.com       SRV service location:
          priority       = 1
          weight         = 0
          port           = 5061
          svr hostname   = ipo.example.com
ipo.example.com internet address = 135.124.242.34

C:\Users\agardi>nslookup -querytype=SRV _xmpp-client._tcp.onex.example.com
Server:  UnKnown
Address:  135.124.242.43

_xmpp-client._tcp.onex.example.com      SRV service location:
          priority       = 1
          weight         = 0
          port           = 5222
          svr hostname   = onex.example.com
onex.example.com        internet address = 135.124.242.34
```

4. Repeat above configuration on the internal DNS server using the private IP of IPO

Client behavior

For troubleshooting purposes it is important to understand how the different domains are related, and how the soft clients use the information configured on the application and the information received from One-X Portal / IPO. To demonstrate this, we can use separate FQDN for IPO server, XMPP domain and SIP domain.



This domain separation requires the following configuration changes:

1. Change XMPP domain to onex.example.com. See Configuring XMPP domain on One-X Portal
2. Change SIP domain to sip.example.com. See VoIP Setup
3. Change Topology Hiding to sip.example.com. See Topology Hiding
4. Create new certificate for SBCE. Include **DNS:onex.example.com, DNS:ipo.example.com, DNS:sip.example.com** in the **Subject Alternative Name** field. Install the certificate on SBCE, create new TLS Server Profile with the new certificate, and assign it to the external signaling interface. Finally do a **Restart Application** on the SBCE. See Certificates, TLS Profiles and Signaling Interfaces
5. Create and update identity certificate for IPO with **DNS:onex.example.com, DNS:ipo.example.com, DNS:sip.example.com** in the **Subject Alternative Name** field. Procedure is similar to Generating Identity Certificate for SBCE but **do not** check **Create certificate for a different machine** Clicking on Generate will install the new certificate and restart IPO automatically.
6. Create Forward Lookup Zone for each 3 FQDN on both DNS server, create A record with empty name in each zone pointing to public IP (external DNS) or IPO (internal DNS). Create SRV record _xmpp._tcp for onex.example.com and _sip._tls for sip.example.com. See DNS Configuration

The following table summarizes the ports and DNS queries used by different applications.

Application	**Ports**	**DNS queries**
Communicator for Windows	5061 SIP 9443 XMPP	A ipo.example.com A onex.example.com
Communicator for iPad	5061 SIP 5222 XMPP	A ipo.example.com A onex.example.com
Communicator for Android	5061 SIP	A ipo.example.com
Communicator for iPhone	5061 SIP	A ipo.example.com
Onex-X Mobile Preferred for Android	8444 REST 5222 XMPP 5061 SIP	A onex.example.com SRV _xmpp-client._tcp.onex.example.com SRV _sip._tls.sip.example.com
One-X Mobile Preferred for IOS	8444 REST 5222 XMPP 5061 SIP	A onex.example.com SRV _xmpp-client._tcp.onex.example.com A sip.example.com

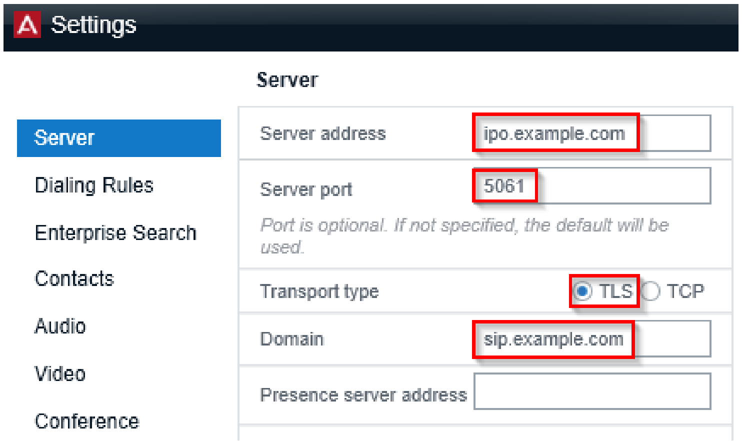
Communicator for Windows

The Avaya Communicator for Windows first registers to IPO on the configured SIP port, then connects to the One-X Portal using the information it received during the registration. On the client we need to configure the **FQDN, SIP port, transport and SIP domain of the IPO**.

NOTE: Not every version of Avaya Communicator for Windows is supported by IPO. Use the one that is listed under IP Office downloads. Its current version is 2.0.3.33.

Detailed procedure:

1. Configure the client



Settings

Server

Server address: ipo.example.com

Server port: 5061

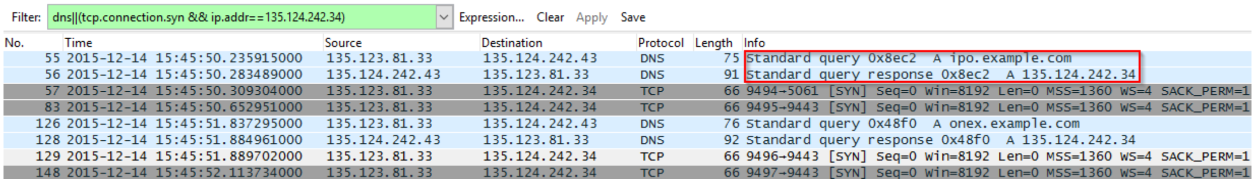
Port is optional. If not specified, the default will be used.

Transport type: ● TLS ○ TCP

Domain: sip.example.com

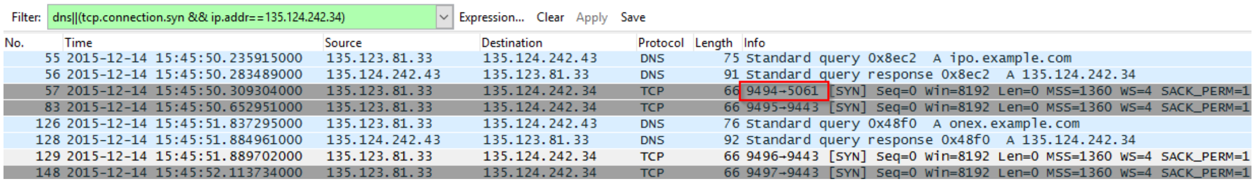
Presence server address:

2. Client sends DNS A query with the FQDN set on the client to learn the IP of IPO

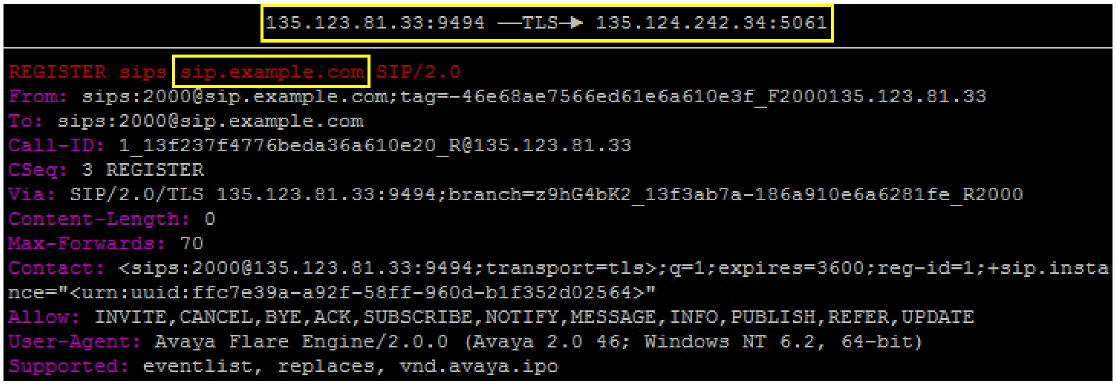


```
Filter: dns||(tcp.connection.syn && ip.addr==135.124.242.34)   Expression...  Clear  Apply  Save

No.  Time                           Source          Destination     Protocol Length Info
  55 2015-12-14 15:45:50.235915000  135.123.81.33   135.124.242.43  DNS       75 Standard query 0x8ec2  A ipo.example.com
  56 2015-12-14 15:45:50.283489000  135.124.242.43  135.123.81.33   DNS       91 Standard query response 0x8ec2  A 135.124.242.34
  57 2015-12-14 15:45:50.309304000  135.123.81.33   135.124.242.34  TCP       66 9494→5061 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
  83 2015-12-14 15:45:50.652951000  135.123.81.33   135.124.242.34  TCP       66 9495→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 126 2015-12-14 15:45:51.837295000  135.123.81.33   135.124.242.43  DNS       76 Standard query 0x48f0  A onex.example.com
 128 2015-12-14 15:45:51.884961000  135.124.242.43  135.123.81.33   DNS       92 Standard query response 0x48f0  A 135.124.242.34
 129 2015-12-14 15:45:51.889702000  135.123.81.33   135.124.242.34  TCP       66 9496→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 148 2015-12-14 15:45:52.113734000  135.123.81.33   135.124.242.34  TCP       66 9497→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
```

3. Client sends SIP REGISTER message to IPO with the configured SIP domain on the configured port and transport

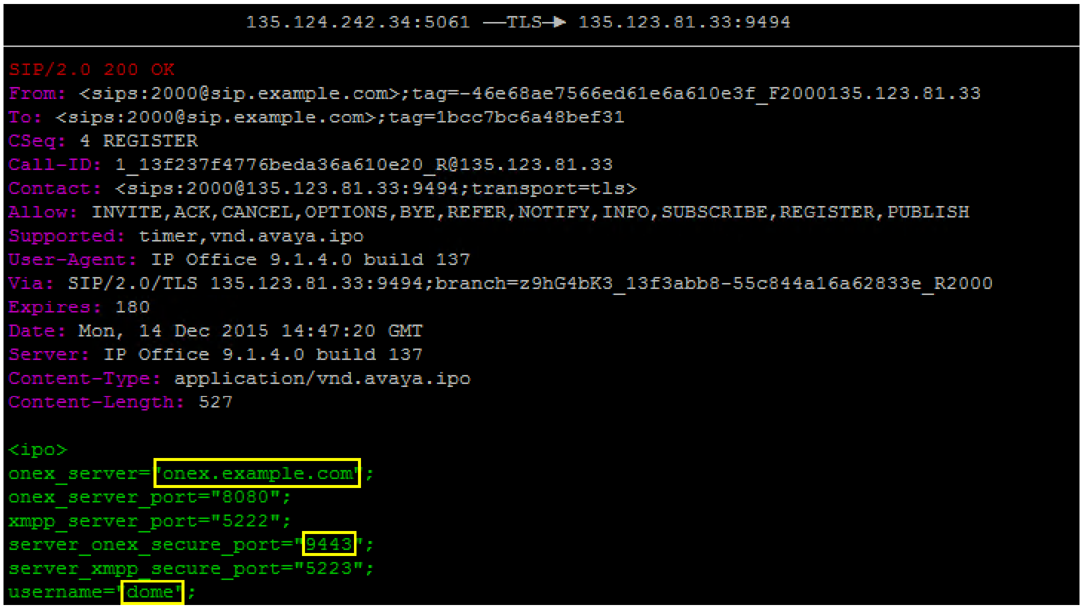


```
Filter: dns||(tcp.connection.syn && ip.addr==135.124.242.34)   Expression...  Clear  Apply  Save

No.  Time                           Source          Destination     Protocol Length Info
  55 2015-12-14 15:45:50.235915000  135.123.81.33   135.124.242.43  DNS       75 Standard query 0x8ec2  A ipo.example.com
  56 2015-12-14 15:45:50.283489000  135.124.242.43  135.123.81.33   DNS       91 Standard query response 0x8ec2  A 135.124.242.34
  57 2015-12-14 15:45:50.309304000  135.123.81.33   135.124.242.34  TCP       66 9494→5061 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
  83 2015-12-14 15:45:50.652951000  135.123.81.33   135.124.242.34  TCP       66 9495→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 126 2015-12-14 15:45:51.837295000  135.123.81.33   135.124.242.43  DNS       76 Standard query 0x48f0  A onex.example.com
 128 2015-12-14 15:45:51.884961000  135.124.242.43  135.123.81.33   DNS       92 Standard query response 0x48f0  A 135.124.242.34
 129 2015-12-14 15:45:51.889702000  135.123.81.33   135.124.242.34  TCP       66 9496→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 148 2015-12-14 15:45:52.113734000  135.123.81.33   135.124.242.34  TCP       66 9497→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
```



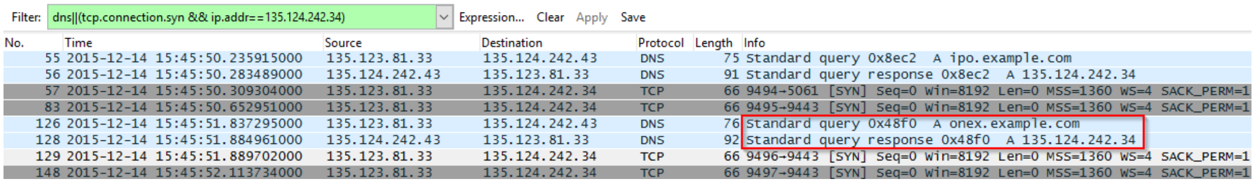
```
135.123.81.33:9494 —TLS→ 135.124.242.34:5061

REGISTER sips:sip.example.com SIP/2.0
From: sips:2000@sip.example.com;tag=-46e68ae7566ed61e6a610e3f_F2000135.123.81.33
To: sips:2000@sip.example.com
Call-ID: 1_13f237f4776beda36a610e20_R@135.123.81.33
CSeq: 3 REGISTER
Via: SIP/2.0/TLS 135.123.81.33:9494;branch=z9hG4bK2_13f3ab7a-186a910e6a6281fe_R2000
Content-Length: 0
Max-Forwards: 70
Contact: <sips:2000@135.123.81.33:9494;transport=tls>;q=1;expires=3600;reg-id=1;+sip.insta
nce="<urn:uuid:ffc7e39a-a92f-58ff-960d-b1f352d02564>"
Allow: INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE
User-Agent: Avaya Flare Engine/2.0.0 (Avaya 2.0 46; Windows NT 6.2, 64-bit)
Supported: eventlist, replaces, vnd.avaya.ipo
```

4. In the 200 OK from IPO, the body contains the address of One-X Server (XMPP domain) and the ports



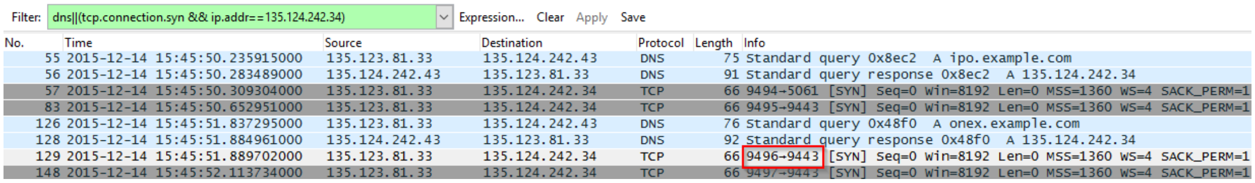
```
                    135.124.242.34:5061 ——TLS—▶ 135.123.81.33:9494

SIP/2.0 200 OK
From: <sips:2000@sip.example.com>;tag=-46e68ae7566ed61e6a610e3f_F2000135.123.81.33
To: <sips:2000@sip.example.com>;tag=1bcc7bc6a48bef31
CSeq: 4 REGISTER
Call-ID: 1_13f237f4776beda36a610e20_R@135.123.81.33
Contact: <sips:2000@135.123.81.33:9494;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: timer,vnd.avaya.ipo
User-Agent: IP Office 9.1.4.0 build 137
Via: SIP/2.0/TLS 135.123.81.33:9494;branch=z9hG4bK3_13f3abb8-55c844a16a62833e_R2000
Expires: 180
Date: Mon, 14 Dec 2015 14:47:20 GMT
Server: IP Office 9.1.4.0 build 137
Content-Type: application/vnd.avaya.ipo
Content-Length: 527

<ipo>
onex_server="onex.example.com";
onex_server_port="8080";
xmpp_server_port="5222";
server_onex_secure_port="9443";
server_xmpp_secure_port="5223";
username="dome";
```

5. Client sends DNS A query to learn the IP which belongs to XMPP domain



```
Filter: dns||(tcp.connection.syn && ip.addr==135.124.242.34)    Expression...  Clear  Apply  Save

No.  Time                           Source           Destination      Protocol  Length  Info
 55 2015-12-14 15:45:50.235915000   135.123.81.33    135.124.242.43   DNS        75 Standard query 0x8ec2  A ipo.example.com
 56 2015-12-14 15:45:50.283489000   135.124.242.43   135.123.81.33    DNS        91 Standard query response 0x8ec2  A 135.124.242.34
 57 2015-12-14 15:45:50.309304000   135.123.81.33    135.124.242.34   TCP        66 9494→5061 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 83 2015-12-14 15:45:50.652951000   135.123.81.33    135.124.242.34   TCP        66 9495→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
126 2015-12-14 15:45:51.837295000   135.123.81.33    135.124.242.43   DNS        76 Standard query 0x48f0  A onex.example.com
128 2015-12-14 15:45:51.884961000   135.124.242.43   135.123.81.33    DNS        92 Standard query response 0x48f0  A 135.124.242.34
129 2015-12-14 15:45:51.889702000   135.123.81.33    135.124.242.34   TCP        66 9496→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
148 2015-12-14 15:45:52.113734000   135.123.81.33    135.124.242.34   TCP        66 9497→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
```

6. Clients starts XMPP communication on port 9443 with One-X Portal



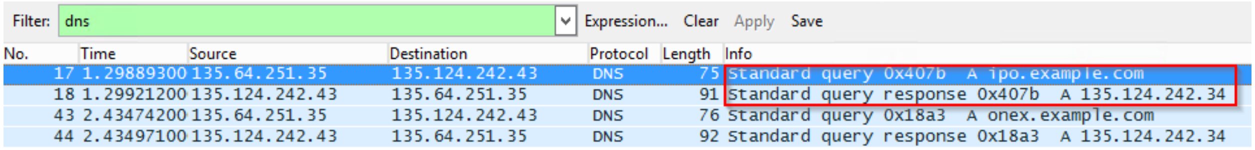
```
Filter: dns||(tcp.connection.syn && ip.addr==135.124.242.34)    Expression...  Clear  Apply  Save

No.  Time                           Source           Destination      Protocol  Length  Info
 55 2015-12-14 15:45:50.235915000   135.123.81.33    135.124.242.43   DNS        75 Standard query 0x8ec2  A ipo.example.com
 56 2015-12-14 15:45:50.283489000   135.124.242.43   135.123.81.33    DNS        91 Standard query response 0x8ec2  A 135.124.242.34
 57 2015-12-14 15:45:50.309304000   135.123.81.33    135.124.242.34   TCP        66 9494→5061 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
 83 2015-12-14 15:45:50.652951000   135.123.81.33    135.124.242.34   TCP        66 9495→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
126 2015-12-14 15:45:51.837295000   135.123.81.33    135.124.242.43   DNS        76 Standard query 0x48f0  A onex.example.com
128 2015-12-14 15:45:51.884961000   135.124.242.43   135.123.81.33    DNS        92 Standard query response 0x48f0  A 135.124.242.34
129 2015-12-14 15:45:51.889702000   135.123.81.33    135.124.242.34   TCP        66 9496→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
148 2015-12-14 15:45:52.113734000   135.123.81.33    135.124.242.34   TCP        66 9497→9443 [SYN] Seq=0 Win=8192 Len=0 MSS=1360 WS=4 SACK_PERM=1
```

Communicator for iPad

The Avaya Communicator for iPad first registers to IPO, then connects to the One-X Portal using the information it received during the registration. On the client we need to configure the **FQDN, SIP port, transport and SIP domain of the IPO**.

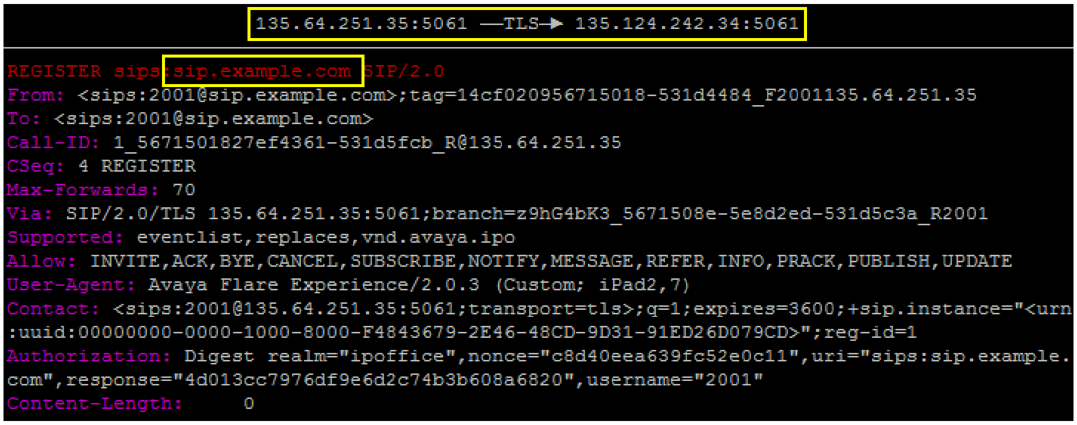
Detailed procedure:

1. Configure the client
   a. In **Settings / Accounts and Services / Phone Service** set the followings:
      i. **Phone Server Address:** FQDN of IPO
      ii. **Phone Server Port:** 5061
      iii. **Phone Service Domain:** SIP domain
      iv. **TLS:** enable
      v. **Extension: Extension** from User tab of IPO User form
      vi. **Password: Password** from User tab of IPO User form
   b. In **Settings / Accounts and Services / Presence Service** enable **Presence Service** and leave empty the **Presence Server Address**
2. Client sends DNS A query with the FQDN set on the client to learn the IP of IPO



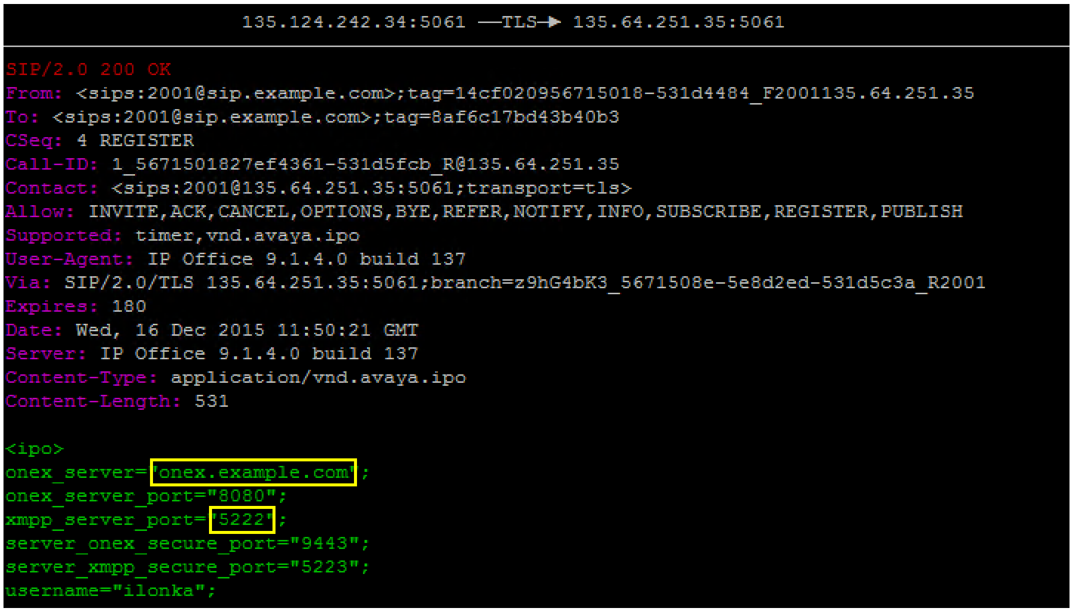
```
No.  Time        Source          Destination     Protocol Length Info
  17 1.29889300 135.64.251.35   135.124.242.43  DNS         75 Standard query 0x407b  A ipo.example.com
  18 1.29921200 135.124.242.43  135.64.251.35   DNS         91 Standard query response 0x407b  A 135.124.242.34
  43 2.43474200 135.64.251.35   135.124.242.43  DNS         76 Standard query 0x18a3  A onex.example.com
  44 2.43497100 135.124.242.43  135.64.251.35   DNS         92 Standard query response 0x18a3  A 135.124.242.34
```

3. Client sends SIP REGISTER message to IPO with the configured SIP domain on the configured port and transport



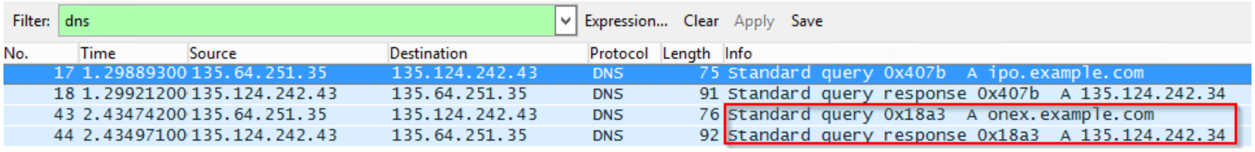
```
135.64.251.35:5061 —TLS→ 135.124.242.34:5061

REGISTER sips:sip.example.com SIP/2.0
From: <sips:2001@sip.example.com>;tag=14cf020956715018-531d4484_F2001135.64.251.35
To: <sips:2001@sip.example.com>
Call-ID: 1_5671501827ef4361-531d5fcb_R@135.64.251.35
CSeq: 4 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TLS 135.64.251.35:5061;branch=z9hG4bK3_5671508e-5e8d2ed-531d5c3a_R2001
Supported: eventlist,replaces,vnd.avaya.ipo
Allow: INVITE,ACK,BYE,CANCEL,SUBSCRIBE,NOTIFY,MESSAGE,REFER,INFO,PRACK,PUBLISH,UPDATE
User-Agent: Avaya Flare Experience/2.0.3 (Custom; iPad2,7)
Contact: <sips:2001@135.64.251.35:5061;transport=tls>;q=1;expires=3600;+sip.instance="<urn
:uuid:00000000-0000-1000-8000-F4843679-2E46-48CD-9D31-91ED26D079CD>";reg-id=1
Authorization: Digest realm="ipoffice",nonce="c8d40eea639fc52e0c11",uri="sips:sip.example.
com",response="4d013cc7976df9e6d2c74b3b608a6820",username="2001"
Content-Length:     0
```

4. In the 200 OK from IPO, the body contains the address of One-X Server (XMPP domain) and the ports



```
135.124.242.34:5061 —TLS→ 135.64.251.35:5061

SIP/2.0 200 OK
From: <sips:2001@sip.example.com>;tag=14cf020956715018-531d4484_F2001135.64.251.35
To: <sips:2001@sip.example.com>;tag=8af6c17bd43b40b3
CSeq: 4 REGISTER
Call-ID: 1_5671501827ef4361-531d5fcb_R@135.64.251.35
Contact: <sips:2001@135.64.251.35:5061;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: timer,vnd.avaya.ipo
User-Agent: IP Office 9.1.4.0 build 137
Via: SIP/2.0/TLS 135.64.251.35:5061;branch=z9hG4bK3_5671508e-5e8d2ed-531d5c3a_R2001
Expires: 180
Date: Wed, 16 Dec 2015 11:50:21 GMT
Server: IP Office 9.1.4.0 build 137
Content-Type: application/vnd.avaya.ipo
Content-Length: 531

<ipo>
onex_server="onex.example.com";
onex_server_port="8080";
xmpp_server_port="5222";
server_onex_secure_port="9443";
server_xmpp_secure_port="5223";
username="ilonka";
```

5. Client sends DNS A query to learn the IP which belongs to XMPP domain



```
No.  Time        Source          Destination     Protocol Length Info
  17 1.29889300 135.64.251.35   135.124.242.43  DNS         75 Standard query 0x407b  A ipo.example.com
  18 1.29921200 135.124.242.43  135.64.251.35   DNS         91 Standard query response 0x407b  A 135.124.242.34
  43 2.43474200 135.64.251.35   135.124.242.43  DNS         76 Standard query 0x18a3  A onex.example.com
  44 2.43497100 135.124.242.43  135.64.251.35   DNS         92 Standard query response 0x18a3  A 135.124.242.34
```

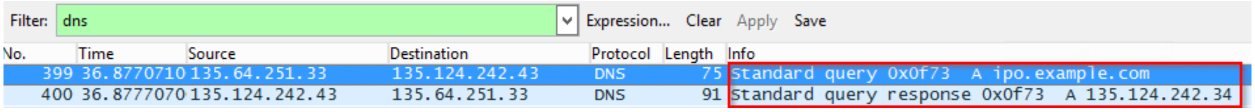
6. Clients starts XMPP communication on port 5222 with One-X Portal

Communicator for Android

Avaya Communicator for Android is **not supported** by IPO. However it can still be registered as a VoIP only client. The Avaya Communicator for Android registers to IPO using the configured address, port, transport and SIP domain. On the client we need to configure the **FQDN, SIP port, transport and SIP domain of the IPO**. User Name can be either the **Name or Extension** from User tab of IPO User form, Password is **Login Code** from **Telephony / Supervisor Settings** of IPO User form

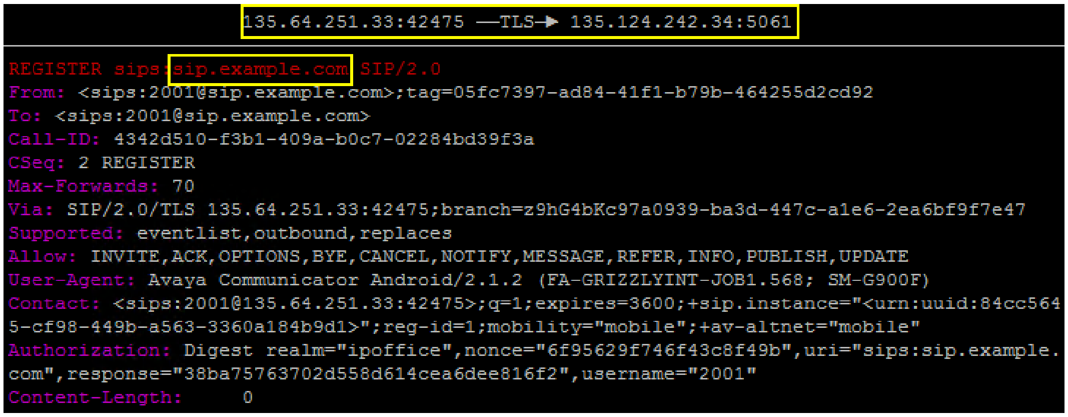
Detailed procedure:

1. Configure the client
    a. In **Settings / Accounts and Services / VoIP Account Information** set the followings:
        i. **Service Enabled:** enable
        ii. **Use VoIP for calls:** set **Always**
        iii. **Extension: Extension** from User tab of IPO User form
        iv. **Password: Login Code** from **Telephony / Supervisor Settings** of IPO User form
        v. **Domain:** SIP domain
        vi. **Server:** FQDN of IPO
        vii. **Port:** 5061
        viii. **Secure Connection:** enable
2. Client sends DNS A query with the FQDN set on the client to learn the IP of IPO



No.	Time	Source	Destination	Protocol	Length	Info
399	36.8770710	135.64.251.33	135.124.242.43	DNS	75	Standard query 0x0f73 A ipo.example.com
400	36.8777070	135.124.242.43	135.64.251.33	DNS	91	Standard query response 0x0f73 A 135.124.242.34

3. Client sends SIP REGISTER message to IPO with the configured SIP domain on the configured port and transport



```
135.64.251.33:42475 ——TLS—▶ 135.124.242.34:5061

REGISTER sips:sip.example.com SIP/2.0
From: <sips:2001@sip.example.com>;tag=05fc7397-ad84-41f1-b79b-464255d2cd92
To: <sips:2001@sip.example.com>
Call-ID: 4342d510-f3b1-409a-b0c7-02284bd39f3a
CSeq: 2 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TLS 135.64.251.33:42475;branch=z9hG4bKc97a0939-ba3d-447c-a1e6-2ea6bf9f7e47
Supported: eventlist,outbound,replaces
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent: Avaya Communicator Android/2.1.2 (FA-GRIZZLYINT-JOB1.568; SM-G900F)
Contact: <sips:2001@135.64.251.33:42475>;q=1;expires=3600;+sip.instance="<urn:uuid:84cc564
5-cf98-449b-a563-3360a184b9d1>";reg-id=1;mobility="mobile";+av-altnet="mobile"
Authorization: Digest realm="ipoffice",nonce="6f95629f746f43c8f49b",uri="sips:sip.example.
com",response="38ba75763702d558d614cea6dee816f2",username="2001"
Content-Length:     0
```

Communicator for iPhone

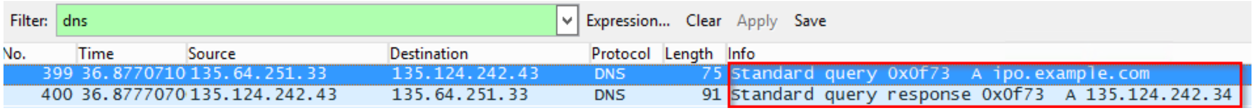
Avaya Communicator for iPhone is **not supported** by IPO. However it can still be registered as a VoIP only client. The Avaya Communicator for iPhone registers to IPO using the configured address, port, transport and SIP domain. On the client we need to configure the **FQDN, SIP port, transport and SIP domain of the IPO**. User Name can be either the **Name or Extension** from User tab of IPO User form, Password is **Login Code** from **Telephony / Supervisor Settings** of IPO User form

Detailed procedure:

1. Configure the client
    a. In **Settings / Accounts and Services / VoIP** set the followings:
        i. **VoIP:** enable
        ii. **Extension: Extension** from User tab of IPO User form

iii. **Password: Login Code** from **Telephony / Supervisor Settings** of IPO User form
iv. **Address:** FQDN of IPO
v. **Port:** 5061
vi. **Domain:** SIP domain
vii. **TLS:** enable
viii. **Use VoIP for calls:** set **Always**

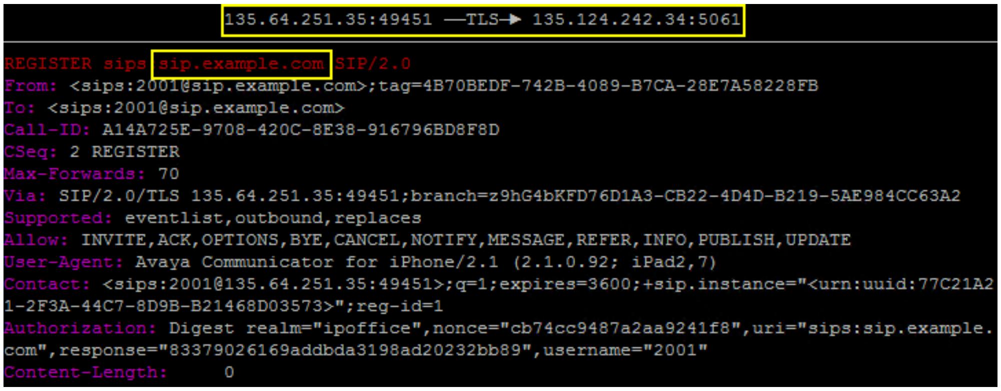
2. Client sends DNS A query with the FQDN set on the client to learn the IP of IPO



Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
399	36.8770710	135.64.251.33	135.124.242.43	DNS	75	Standard query 0x0f73 A ipo.example.com
400	36.8777070	135.124.242.43	135.64.251.33	DNS	91	Standard query response 0x0f73 A 135.124.242.34

3. Client sends SIP REGISTER message to IPO with the configured SIP domain on the configured port and transport



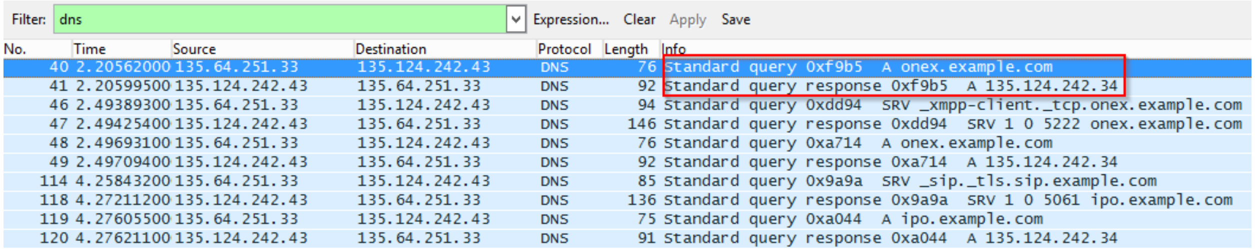
```
135.64.251.35:49451 —TLS→ 135.124.242.34:5061

REGISTER sips sip.example.com SIP/2.0
From: <sips:2001@sip.example.com>;tag=4B70BEDF-742B-4089-B7CA-28E7A58228FB
To: <sips:2001@sip.example.com>
Call-ID: A14A725E-9708-420C-8E38-916796BD8F8D
CSeq: 2 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TLS 135.64.251.35:49451;branch=z9hG4bKFD76D1A3-CB22-4D4D-B219-5AE984CC63A2
Supported: eventlist,outbound,replaces
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent: Avaya Communicator for iPhone/2.1 (2.1.0.92; iPad2,7)
Contact: <sips:2001@135.64.251.35:49451>;q=1;expires=3600;+sip.instance="<urn:uuid:77C21A2
1-2F3A-44C7-8D9B-B21468D03573>";reg-id=1
Authorization: Digest realm="ipoffice",nonce="cb74cc9487a2aa9241f8",uri="sips:sip.example.
com",response="83379026169addbda3198ad20232bb89",username="2001"
Content-Length:     0
```

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 8444) to learn the XMPP and SIP domain, then does DNS SRV query to learn the XMPP and SIP service addresses and ports, finally registers to One-X Portal and IPO. On the client we need to configure the **FQDN of One-X Portal.** User Name can be either the **Name or Extension** from User tab of IPO User form, Password is **Password** from User tab of IPO User form

Detailed procedure:

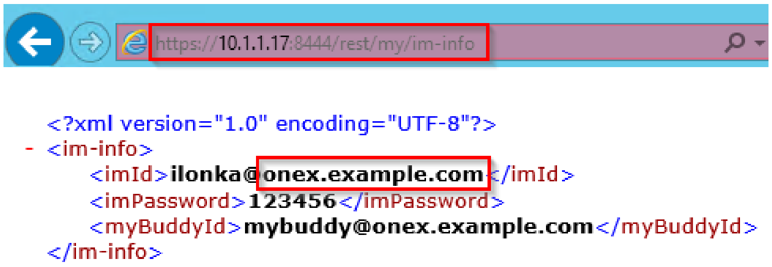
1. Configure the client.
   a. In **Settings / Server ID and user account** set the **FQDN of One-X Portal**, the **user name** and **password**
   b. In **Settings / Voice Over IP / VoIP operation mode** set **Always**
   c. Uncheck **Settings / Validate Server Certificates**
   d. In **Settings / Advanced / Advanced VoIP** check **Secure Connection.** This option is needed for encrypted signaling and media.
2. Client sends DNS A query with the FQDN set on the client to learn the IP of One-X Portal



Filter: dns

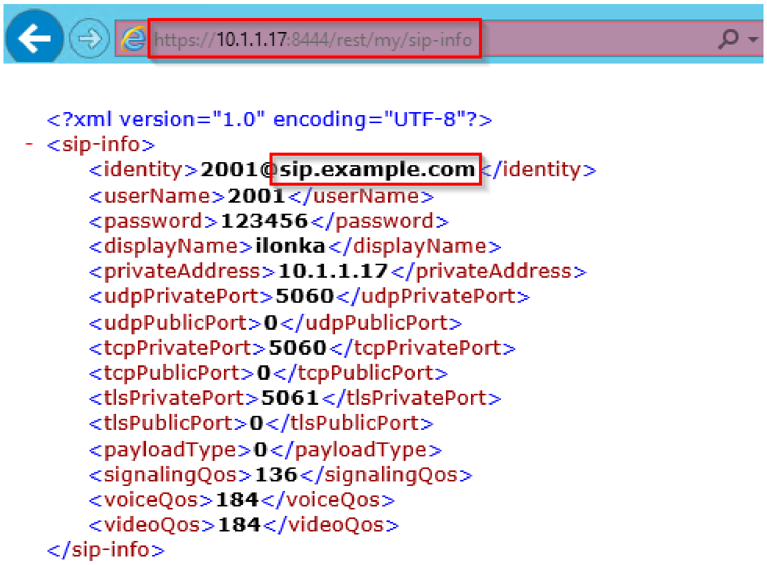
No.	Time	Source	Destination	Protocol	Length	Info
40	2.20562000	135.64.251.33	135.124.242.43	DNS	76	Standard query 0xf9b5 A onex.example.com
41	2.20599500	135.124.242.43	135.64.251.33	DNS	92	Standard query response 0xf9b5 A 135.124.242.34
46	2.49389300	135.64.251.33	135.124.242.43	DNS	94	Standard query 0xdd94 SRV _xmpp-client._tcp.onex.example.com
47	2.49425400	135.124.242.43	135.64.251.33	DNS	146	Standard query response 0xdd94 SRV 1 0 5222 onex.example.com
48	2.49693100	135.64.251.33	135.124.242.43	DNS	76	Standard query 0xa714 A onex.example.com
49	2.49709400	135.124.242.43	135.64.251.33	DNS	92	Standard query response 0xa714 A 135.124.242.34
114	4.25843200	135.64.251.33	135.124.242.43	DNS	85	Standard query 0x9a9a SRV _sip._tls.sip.example.com
118	4.27211200	135.124.242.43	135.64.251.33	DNS	136	Standard query response 0x9a9a SRV 1 0 5061 ipo.example.com
119	4.27605500	135.64.251.33	135.124.242.43	DNS	75	Standard query 0xa044 A ipo.example.com
120	4.27621100	135.124.242.43	135.64.251.33	DNS	91	Standard query response 0xa044 A 135.124.242.34

3. Client contacts One-X Portal on port 8444 and downloads the XMPP and SIP access details including the XMPP and SIP domains. Same information can be manually checked from a browser:



https://10.1.1.17:8444/rest/my/im-info

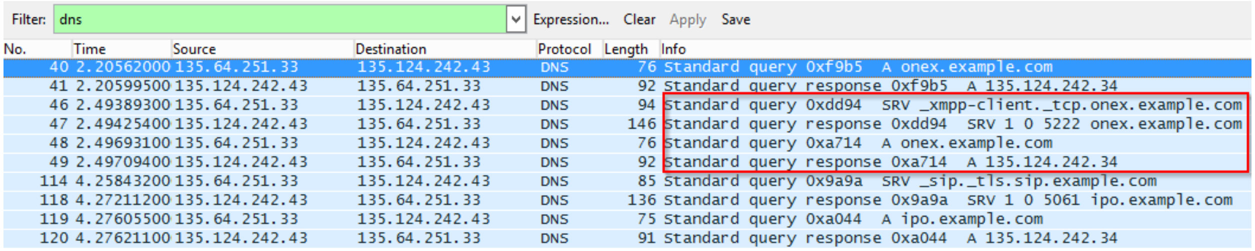
```
  <?xml version="1.0" encoding="UTF-8"?>
- <im-info>
      <imId>ilonka@onex.example.com</imId>
      <imPassword>123456</imPassword>
      <myBuddyId>mybuddy@onex.example.com</myBuddyId>
  </im-info>
```



https://10.1.1.17:8444/rest/my/sip-info

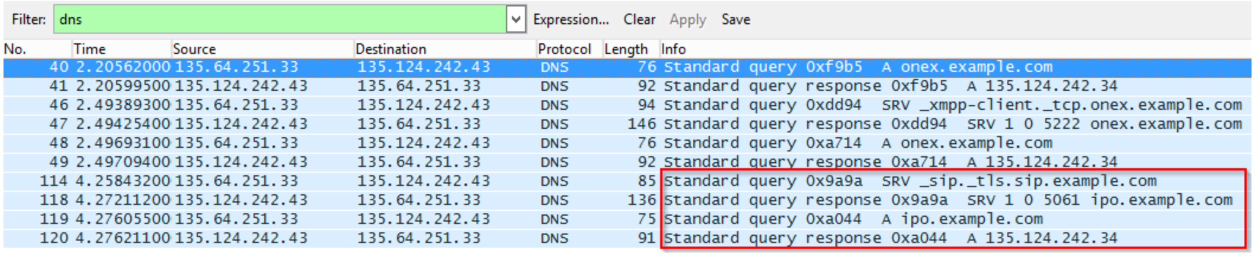
```
  <?xml version="1.0" encoding="UTF-8"?>
- <sip-info>
      <identity>2001@sip.example.com</identity>
      <userName>2001</userName>
      <password>123456</password>
      <displayName>ilonka</displayName>
      <privateAddress>10.1.1.17</privateAddress>
      <udpPrivatePort>5060</udpPrivatePort>
      <udpPublicPort>0</udpPublicPort>
      <tcpPrivatePort>5060</tcpPrivatePort>
      <tcpPublicPort>0</tcpPublicPort>
      <tlsPrivatePort>5061</tlsPrivatePort>
      <tlsPublicPort>0</tlsPublicPort>
      <payloadType>0</payloadType>
      <signalingQos>136</signalingQos>
      <voiceQos>184</voiceQos>
      <videoQos>184</videoQos>
  </sip-info>
```

4. Client does DNS SRV query for _xmpp-client._tcp.<XMPP domain> to learn the IP and port of the XMPP service (One-X Portal)



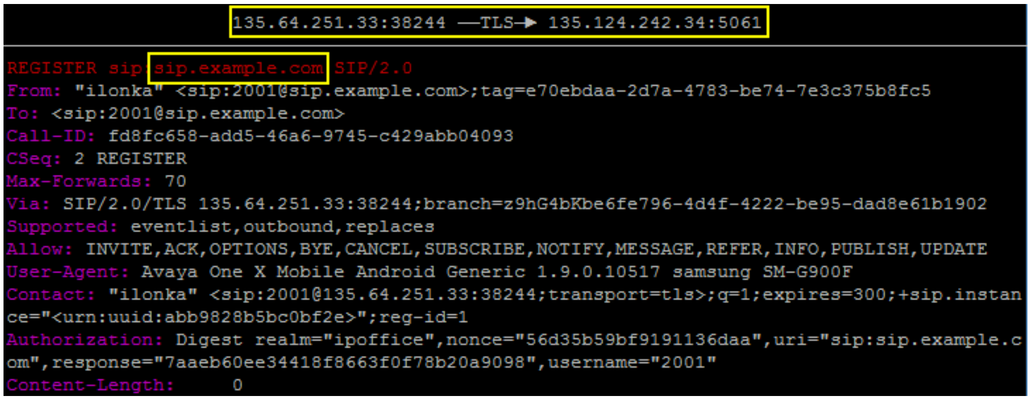
```
Filter: dns                                   Expression... Clear Apply Save
No.  Time       Source          Destination     Protocol Length Info
 40 2.20562000 135.64.251.33   135.124.242.43  DNS       76 Standard query 0xf9b5  A onex.example.com
 41 2.20599500 135.124.242.43  135.64.251.33   DNS       92 Standard query response 0xf9b5  A 135.124.242.34
 46 2.49389300 135.64.251.33   135.124.242.43  DNS       94 Standard query 0xdd94  SRV _xmpp-client._tcp.onex.example.com
 47 2.49425400 135.124.242.43  135.64.251.33   DNS      146 Standard query response 0xdd94  SRV 1 0 5222 onex.example.com
 48 2.49693100 135.64.251.33   135.124.242.43  DNS       76 Standard query 0xa714  A onex.example.com
 49 2.49709400 135.124.242.43  135.64.251.33   DNS       92 Standard query response 0xa714  A 135.124.242.34
114 4.25843200 135.64.251.33   135.124.242.43  DNS       85 Standard query 0x9a9a  SRV _sip._tls.sip.example.com
118 4.27211200 135.124.242.43  135.64.251.33   DNS      136 Standard query response 0x9a9a  SRV 1 0 5061 ipo.example.com
119 4.27605500 135.64.251.33   135.124.242.43  DNS       75 Standard query 0xa044  A ipo.example.com
120 4.27621100 135.124.242.43  135.64.251.33   DNS       91 Standard query response 0xa044  A 135.124.242.34
```

5. Client connects to XMPP service using the learnt information
6. Client does DNS SRV query for _sip._tls.<SIP domain> to learn the IP and port of SIP service (IPO)



```
Filter: dns                                   Expression... Clear Apply Save
No.  Time       Source          Destination     Protocol Length Info
 40 2.20562000 135.64.251.33   135.124.242.43  DNS       76 Standard query 0xf9b5  A onex.example.com
 41 2.20599500 135.124.242.43  135.64.251.33   DNS       92 Standard query response 0xf9b5  A 135.124.242.34
 46 2.49389300 135.64.251.33   135.124.242.43  DNS       94 Standard query 0xdd94  SRV _xmpp-client._tcp.onex.example.com
 47 2.49425400 135.124.242.43  135.64.251.33   DNS      146 Standard query response 0xdd94  SRV 1 0 5222 onex.example.com
 48 2.49693100 135.64.251.33   135.124.242.43  DNS       76 Standard query 0xa714  A onex.example.com
 49 2.49709400 135.124.242.43  135.64.251.33   DNS       92 Standard query response 0xa714  A 135.124.242.34
114 4.25843200 135.64.251.33   135.124.242.43  DNS       85 Standard query 0x9a9a  SRV _sip._tls.sip.example.com
118 4.27211200 135.124.242.43  135.64.251.33   DNS      136 Standard query response 0x9a9a  SRV 1 0 5061 ipo.example.com
119 4.27605500 135.64.251.33   135.124.242.43  DNS       75 Standard query 0xa044  A ipo.example.com
120 4.27621100 135.124.242.43  135.64.251.33   DNS       91 Standard query response 0xa044  A 135.124.242.34
```

7. Client registers to IPO



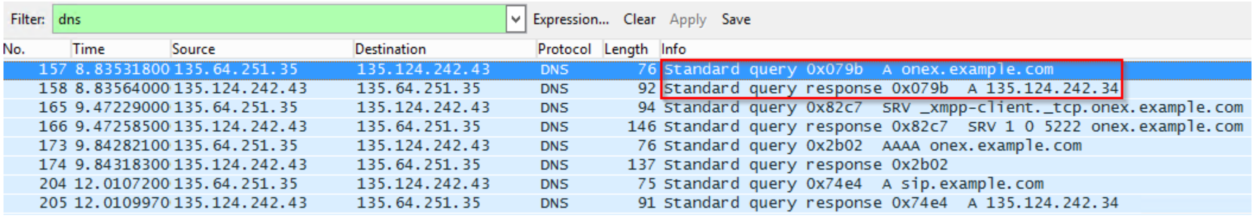
```
135.64.251.33:38244 —TLS→ 135.124.242.34:5061

REGISTER sip:sip.example.com SIP/2.0
From: "ilonka" <sip:2001@sip.example.com>;tag=e70ebdaa-2d7a-4783-be74-7e3c375b8fc5
To: <sip:2001@sip.example.com>
Call-ID: fd8fc658-add5-46a6-9745-c429abb04093
CSeq: 2 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TLS 135.64.251.33:38244;branch=z9hG4bKbe6fe796-4d4f-4222-be95-dad8e61b1902
Supported: eventlist,outbound,replaces
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent: Avaya One X Mobile Android Generic 1.9.0.10517 samsung SM-G900F
Contact: "ilonka" <sip:2001@135.64.251.33:38244;transport=tls>;q=1;expires=300;+sip.instan
ce="<urn:uuid:abb9828b5bc0bf2e>";reg-id=1
Authorization: Digest realm="ipoffice",nonce="56d35b59bf9191136daa",uri="sip:sip.example.c
om",response="7aaeb60ee34418f8663f0f78b20a9098",username="2001"
Content-Length:     0
```

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 8444) to learn the XMPP and SIP domains, then does DNS SRV query to learn the XMPP service address and port, registers to One-X portal using the gathered information, then does DNS A query for SIP domain learnt from REST API, and finally registers to IPO. On the client we need to configure the **FQDN of One-X Portal**. User Name can be either the **Name or Extension** from User tab of IPO User form, Password is **Password** from User tab of IPO User form

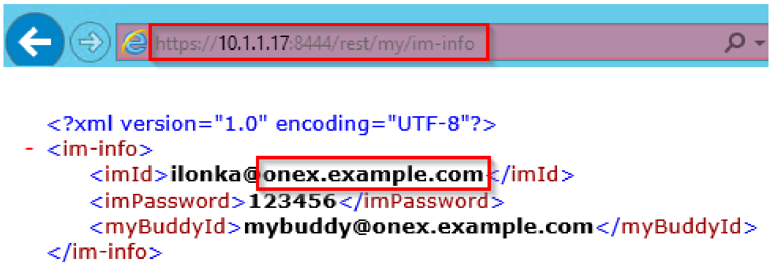
Detailed procedure:

1. Configure the client.
   a. In **Settings / UC Server Settings** set the **FQDN of One-X Portal**, the **User Name** and **Password**
   b. In **Settings / Application Configuration / VoIP Mode** set **Always**
   c. Uncheck **Settings / Security Settings / Validate Server Certificates**
   d. In **Settings / Advanced Settings / Advanced VoIP** check **Secure Connection.** This option is needed for encrypted signaling and media.
2. Client sends DNS A query with the FQDN set on the client to learn the IP of One-X Portal

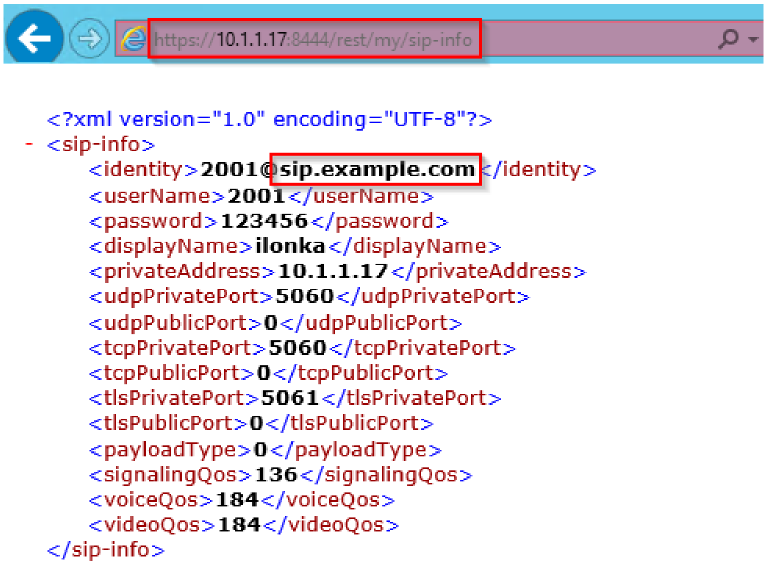


```
No.    Time       Source          Destination     Protocol Length Info
  157 8.83531800 135.64.251.35   135.124.242.43  DNS        76 Standard query 0x079b  A onex.example.com
  158 8.83564000 135.124.242.43  135.64.251.35   DNS        92 Standard query response 0x079b  A 135.124.242.34
  165 9.47229000 135.64.251.35   135.124.242.43  DNS        94 Standard query 0x82c7  SRV _xmpp-client._tcp.onex.example.com
  166 9.47258500 135.124.242.43  135.64.251.35   DNS       146 Standard query response 0x82c7  SRV 1 0 5222 onex.example.com
  173 9.84282100 135.64.251.35   135.124.242.43  DNS        76 Standard query 0x2b02  AAAA onex.example.com
  174 9.84318300 135.124.242.43  135.64.251.35   DNS       137 Standard query response 0x2b02
  204 12.0107200 135.64.251.35   135.124.242.43  DNS        75 Standard query 0x74e4  A sip.example.com
  205 12.0109970 135.124.242.43  135.64.251.35   DNS        91 Standard query response 0x74e4  A 135.124.242.34
```

3. Client contacts One-X Portal on port 8444 and downloads the XMPP and SIP access details including the XMPP and SIP domains. Same information can be manually checked from a browser:



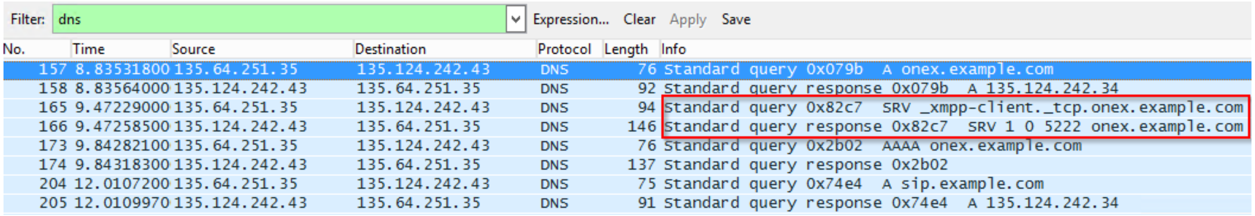
```
https://10.1.1.17:8444/rest/my/im-info

<?xml version="1.0" encoding="UTF-8"?>
- <im-info>
     <imId>ilonka@onex.example.com</imId>
     <imPassword>123456</imPassword>
     <myBuddyId>mybuddy@onex.example.com</myBuddyId>
  </im-info>
```



https://10.1.1.17:8444/rest/my/sip-info

```
<?xml version="1.0" encoding="UTF-8"?>
- <sip-info>
    <identity>2001@sip.example.com</identity>
    <userName>2001</userName>
    <password>123456</password>
    <displayName>ilonka</displayName>
    <privateAddress>10.1.1.17</privateAddress>
    <udpPrivatePort>5060</udpPrivatePort>
    <udpPublicPort>0</udpPublicPort>
    <tcpPrivatePort>5060</tcpPrivatePort>
    <tcpPublicPort>0</tcpPublicPort>
    <tlsPrivatePort>5061</tlsPrivatePort>
    <tlsPublicPort>0</tlsPublicPort>
    <payloadType>0</payloadType>
    <signalingQos>136</signalingQos>
    <voiceQos>184</voiceQos>
    <videoQos>184</videoQos>
  </sip-info>
```

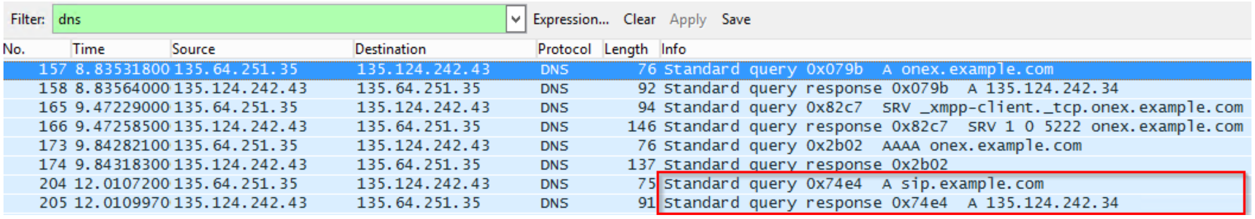
4. Client does DNS SRV query for _xmpp-client._tcp.<XMPP domain> to learn the IP and port of the XMPP service (One-X Portal)



Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
157	8.83531800	135.64.251.35	135.124.242.43	DNS	76	Standard query 0x079b A onex.example.com
158	8.83564000	135.124.242.43	135.64.251.35	DNS	92	Standard query response 0x079b A 135.124.242.34
165	9.47229000	135.64.251.35	135.124.242.43	DNS	94	Standard query 0x82c7 SRV _xmpp-client._tcp.onex.example.com
166	9.47258500	135.124.242.43	135.64.251.35	DNS	146	Standard query response 0x82c7 SRV 1 0 5222 onex.example.com
173	9.84282100	135.64.251.35	135.124.242.43	DNS	76	Standard query 0x2b02 AAAA onex.example.com
174	9.84318300	135.124.242.43	135.64.251.35	DNS	137	Standard query response 0x2b02
204	12.0107200	135.64.251.35	135.124.242.43	DNS	75	Standard query 0x74e4 A sip.example.com
205	12.0109970	135.124.242.43	135.64.251.35	DNS	91	Standard query response 0x74e4 A 135.124.242.34

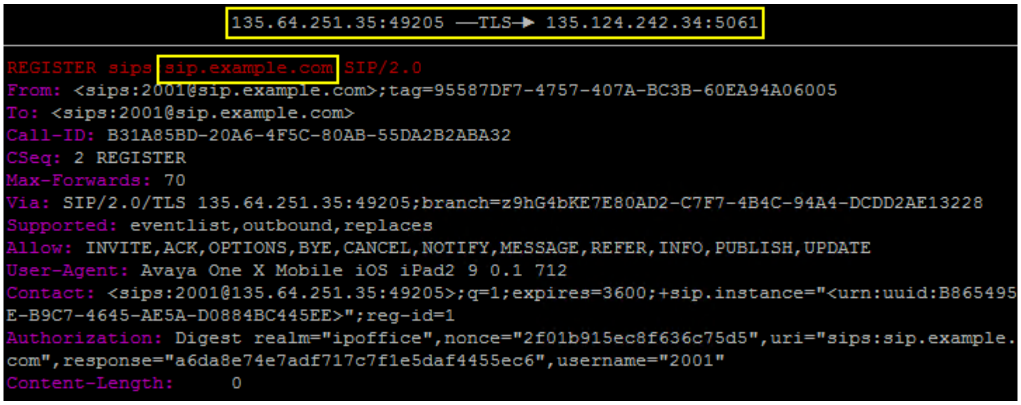
5. Client connects to XMPP service using the learnt information
6. Client does DNS A query for SIP domain to learn the IP of SIP service (IPO)



Filter: dns

No.	Time	Source	Destination	Protocol	Length	Info
157	8.83531800	135.64.251.35	135.124.242.43	DNS	76	Standard query 0x079b A onex.example.com
158	8.83564000	135.124.242.43	135.64.251.35	DNS	92	Standard query response 0x079b A 135.124.242.34
165	9.47229000	135.64.251.35	135.124.242.43	DNS	94	Standard query 0x82c7 SRV _xmpp-client._tcp.onex.example.com
166	9.47258500	135.124.242.43	135.64.251.35	DNS	146	Standard query response 0x82c7 SRV 1 0 5222 onex.example.com
173	9.84282100	135.64.251.35	135.124.242.43	DNS	76	Standard query 0x2b02 AAAA onex.example.com
174	9.84318300	135.124.242.43	135.64.251.35	DNS	137	Standard query response 0x2b02
204	12.0107200	135.64.251.35	135.124.242.43	DNS	75	Standard query 0x74e4 A sip.example.com
205	12.0109970	135.124.242.43	135.64.251.35	DNS	91	Standard query response 0x74e4 A 135.124.242.34

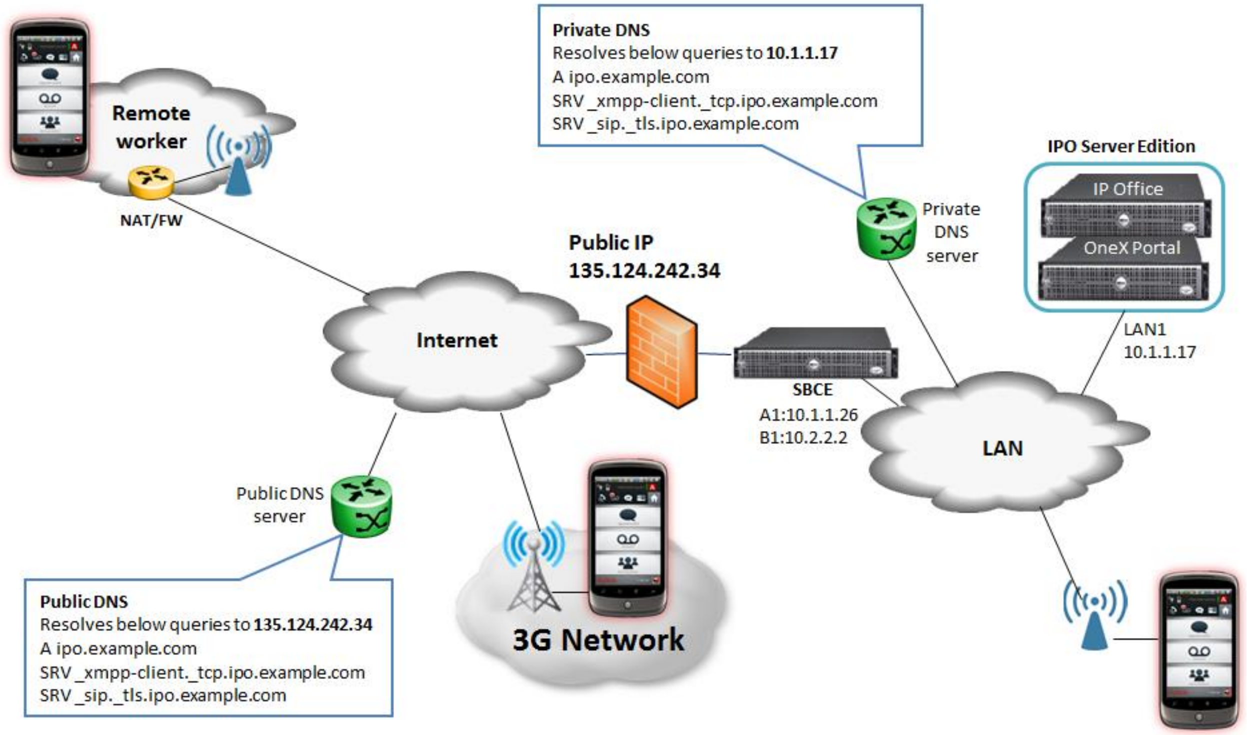
7. Client registers to IPO



```
                    135.64.251.35:49205 —TLS→ 135.124.242.34:5061
REGISTER sips sip.example.com SIP/2.0
From: <sips:2001@sip.example.com>;tag=95587DF7-4757-407A-BC3B-60EA94A06005
To: <sips:2001@sip.example.com>
Call-ID: B31A85BD-20A6-4F5C-80AB-55DA2B2ABA32
CSeq: 2 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TLS 135.64.251.35:49205;branch=z9hG4bKE7E80AD2-C7F7-4B4C-94A4-DCDD2AE13228
Supported: eventlist,outbound,replaces
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,NOTIFY,MESSAGE,REFER,INFO,PUBLISH,UPDATE
User-Agent: Avaya One X Mobile iOS iPad2 9 0.1 712
Contact: <sips:2001@135.64.251.35:49205>;q=1;expires=3600;+sip.instance="<urn:uuid:B865495
E-B9C7-4645-AE5A-D0884BC445EE>";reg-id=1
Authorization: Digest realm="ipoffice",nonce="2f01b915ec8f636c75d5",uri="sips:sip.example.
com",response="a6da8e74e7adf717c7f1e5daf4455ec6",username="2001"
Content-Length:     0
```

SBCE behind Firewall

When SBCE is not on the edge of the network but in DMZ, and the firewall in front of it does Layer 3 NAT, some small changes are needed in SBCE configuration.

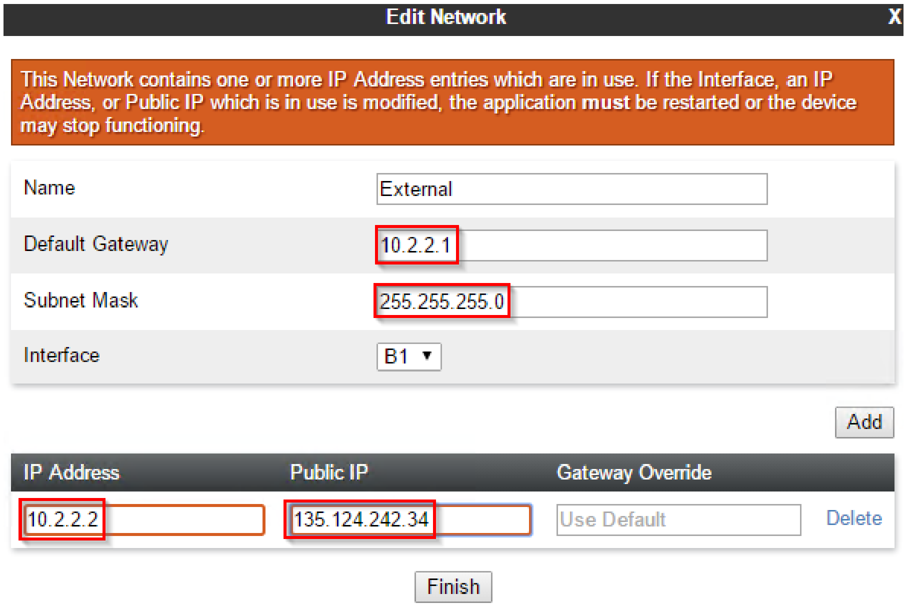


Firewall configuration

1. Allow Layer 3 NAT only, disable all SIP aware functionality, ALG, etc.
2. Forward the TCP signaling ports to the B1 interface of the SBCE which are needed for the given clients
3. Forward the RTP ports to the B1 interface of the SBCE. The port range can be found on the external Media Interface of the SBCE, by default it is UDP 35000-40000. See Media Interfaces

SBCE configuration

1. Go **to Device Specific Settings / Network Management** and go to **Networks** tab
2. Click **Edit** at the external interface
3. Enter the following data then click **Finish**
   a. **Default Gateway**: gateway for the external interface
   b. **Subnet Mask**: mask for the external interface
   c. **IP Address**: IP of external interface
   d. **Public IP**: external IP of the Firewall



This Network contains one or more IP Address entries which are in use. If the Interface, an IP Address, or Public IP which is in use is modified, the application **must** be restarted or the device may stop functioning.

Name	External
Default Gateway	10.2.2.1
Subnet Mask	255.255.255.0
Interface	B1 ▼

IP Address	Public IP	Gateway Override	
10.2.2.2	135.124.242.34	Use Default	Delete

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