IP Office™ Platform 10.0

IP Office SIP Phones with ASBCE

Issue 01g - (18 July 2017)

Notice
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service
THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, 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 THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. 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 INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)
Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software
"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright
Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization
The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components
"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider
THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws
Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud
"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention
If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities
Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support
See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1. Overview

1. Overview

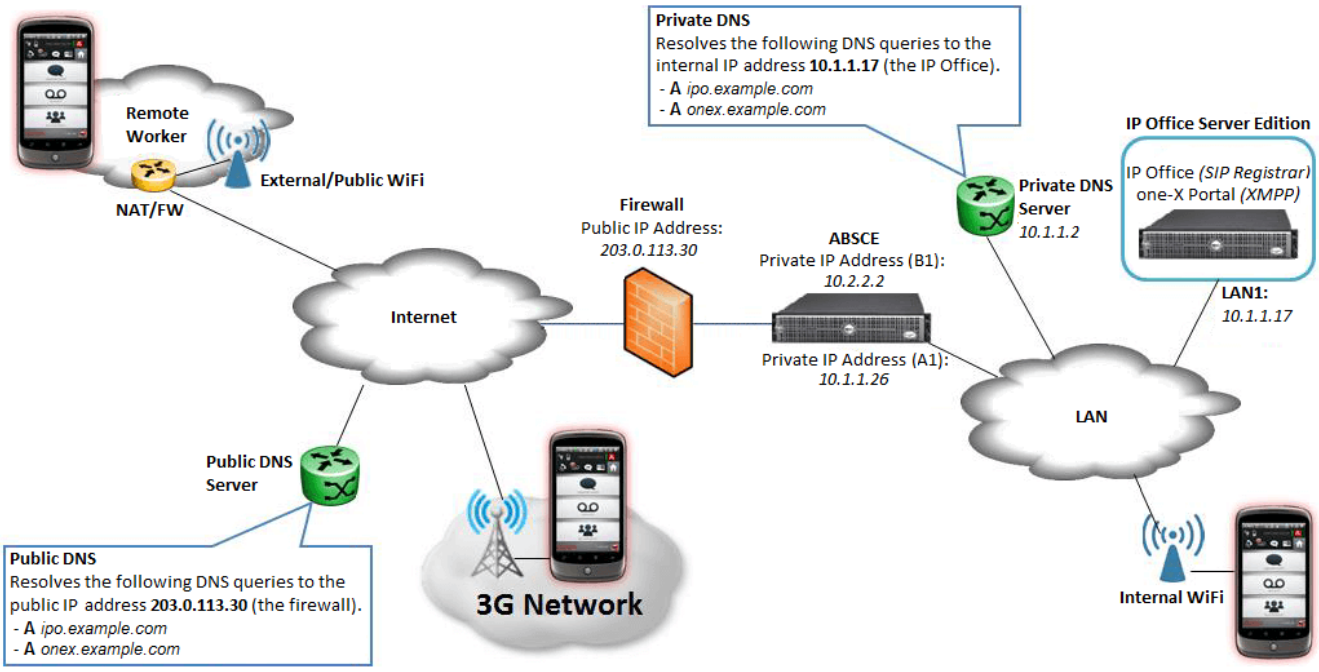
This document is for IP Office Release 10 and ASBCE Release 7.0. It looks at an example* of supporting Avaya SIP clients and remote SIP deskphones when also using an Avaya Session Border Controller for Enterprise (ASBCE) server.

Supported SIP Clients	Supported Remote SIP Deskphones
• Avaya Communicator for Windows • Avaya Communicator for iPad • Avaya one-X Mobile Preferred for Android • Avaya one-X Mobile Preferred for iOS	• 1120, 1140, 1220, 1230. • E129 • H175

*These are just an examples used to illustrate how the different components interact and exchange information. Actual installations will have different requirements specific to the individual customer sites. Refer to the Avaya Session Border Controller for Enterprise manuals for details.

1.1 Example Schematic

The deployment example used in the first parts of this document is as follows:



The IP Office is the SIP registrar for telephony services. The one-X Portal for IP Office service connects to the IP Office and in this scenario acts as the XMPP presence provider for the users.

The ASBCE sits on the edge of the customer's network with both internal and external IP interfaces. Using these, it acts as the gateway for SIP traffic into and out of the network.

When used internally, SIP clients register to the IP Office directly. When used externally, the SIP clients connect to the ASBCE. This is achieved using **Split DNS**. That automatically resolves the FQDNs to the internal IP address of the IP Office or the public IP address of the ASBCE depending on where the clients is currently located.

It assumes that the IP Office is an IP Office Server Edition or IP Office Select primary server. This means it hosts the IP Office and one-X Portal for IP Office services on the same physical or virtual server. Therefore in this case they share the same IP address. They could also use the same single FQDN for the IP Office SIP domain and one-X Portal for IP Office XMPP domain, however for this example we have used separate addresses for the domains to better illustrate their usage.

1.2 Glossary

A Record
Address Record. A basic DNS that maps a domain name to an IP address (or addresses).

ASBCE
Avaya Session Border Controller for Enterprise. This is Avaya's own recommended platform for providing SBC *(see below)* services with a customer business.

DNS
Domain Name Server. A server, or service running on a server, that provides IP address information in response to a domain name query. For example, when an application is asked to connect to the domain name *www.example.com*, it first contacts the DNS server on its network to discover to which IP address it should send traffic for *www.example.com*. This process is called "DNS lookup".

Domain Name
The text address used to identify a network and shared as part of their fully qualified domain names *(see below)* by the devices (servers, services and clients) which belong to that network. A DNS server *(see above*) translates the domain name and fully qualified domain names to specific IP addresses.

FQDN
Fully Qualified Domain Name. The full text name assigned to a specific server, service or client within a domain.

IP Office
An Avaya server, or service running on a server, that provides a range of telephony services including in this case, SIP extension and trunk support.

Management IP
This is the IP address used for administrator access to the ASBCE server. This is a different address from those used for the internal and external VoIP traffic interfaces provided by the ASBCE.

one-X Portal for IP Office
An Avaya service that works with the IP Office (see above) to provide additional telephony features. In this case its main role is the provision of XMPP instant messaging and presence indication between users of SIP telephony devices.

SBC
Session Border Controller. An SBC is a device intended to allow control of VoIP signaling and media traffic between two networks, the device being the border between those networks. SBCs exist at many levels in a VoIP network. In this document we are solely concerned with an SBC controlling traffic between a business customers private internal LAN network and their connection to the public Internet.

Split DNS
The use of domain names and DNS servers to route traffic within and between networks greatly simplifies network maintenance. However, issue arise when the same domain name or fully qualified domain name is used for both internal and external network traffic. This can cause internal traffic to an internal services to still be partially routed externally, expose internal services that should remain hidden from external traffic, or expose internal IP addresses which should either remain hidden or are not valid when used by external traffic.

The solution to these issues is to use Split DNS. This can take many forms but essentially refers to the use of one DNS source for external traffic to the domain and another for internal traffic within the domain. The simplest implementation of this is separate public DNS (external) and private DNS (internal) servers.

SRV Record
A DNS 'A Record' *(see above)* provides basic mapping between a domain name and relevant IP address. Service records provide mapping for specific services that may be running within a domain and the IP addresses of the appropriate servers for those service. There are historically many different type of specific service record, for example **MX** (Mail Exchange) records which can be used to route a domain's email traffic.

An SRV service record is a generic type of service record which can be used to define the IP address destination for a specific protocol or protocol and port (RFC 2782). SRV records are widely used with SIP and XMPP services.

XMPP
Extensible Messaging and Presence Protocol. XMPP is an open standards protocol to allow devices to exchange instant message, presence and contacts information. In this case the one-X Portal for IP Office acts as an XMPP service provider for SIP clients connected to the IP Office.

Chapter 2.
IP Office Configuration

2. IP Office Configuration

This section provides a general summary of the IP Office settings relevant to SIP softphone operation.

Summary:

2.1 Licenses

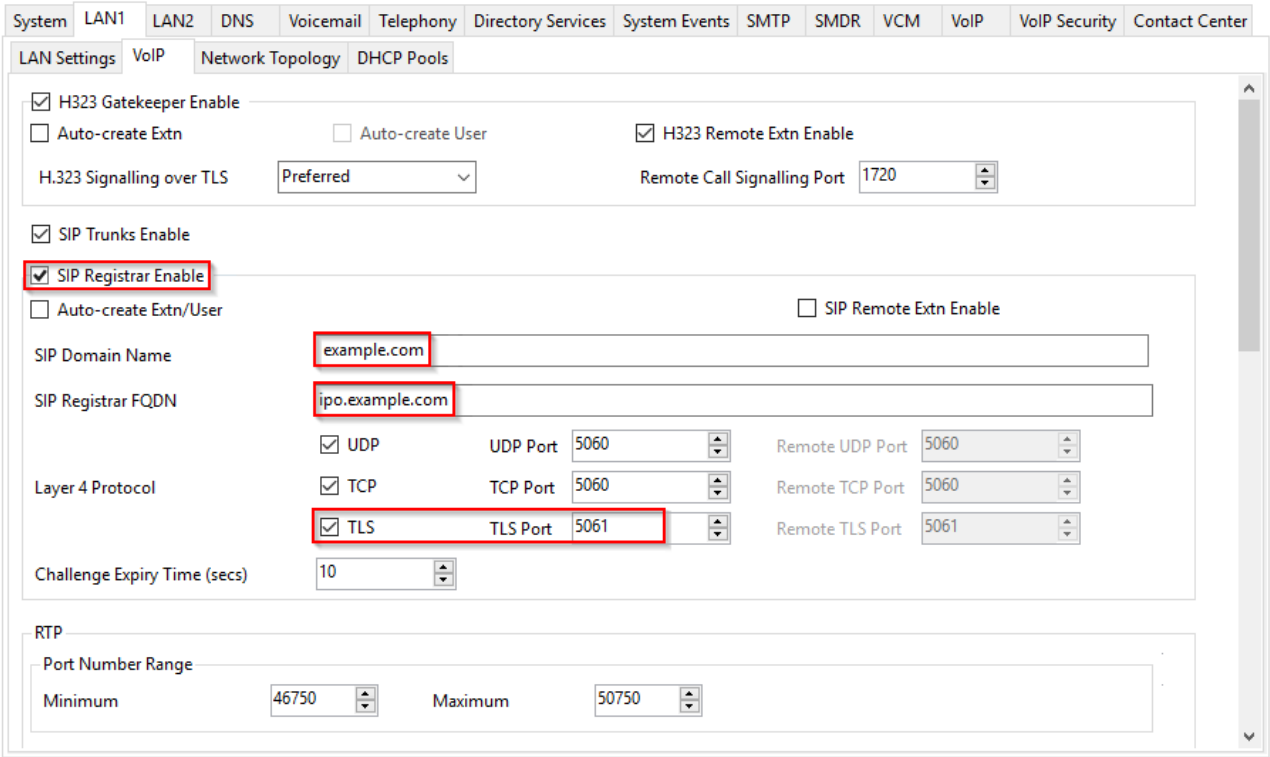
For Release 10 and higher, IP Office only supports PLDS licensing. This uses a PLDS XML license file uploaded to the IP Office system, or for IP Office Server Edition and IP Office Select, uploaded to the WebLM service running on the IP Office primary server.

In both cases, the licenses must include the following user licenses:

- For the one-X Mobile Preferred applications, **Power User**.
- For the Avaya Communicator applications, **Office Worker** or **Power User**.

2.2 SIP VoIP Setup

1. Using IP Office Manager, load the IP Office configuration. Select the primary server configuration.
2. Click **System**.
3. Select the **LAN1** tab and then the **VoIP** sub-tab.



a. **SIP Registrar Enable**: Selecting this option allows SIP devices to register with the IP Office.

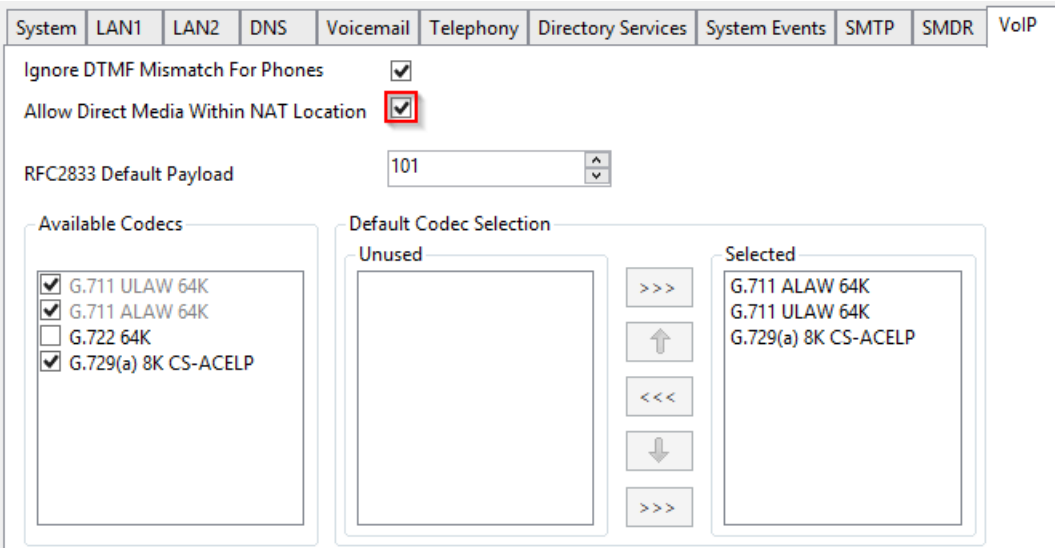
b. **SIP Remote Extn Enable**: Deselect this option. The ASBCE handles the remote extension connections, so the IP Office does not need to handle their NAT requirements.

c. **SIP Domain Name**: Set this to the domain that SIP clients need to use for registration.

d. **SIP Registrar FQDN:** Set this to the fully qualified domain name for SIP connections to the IP Office server.

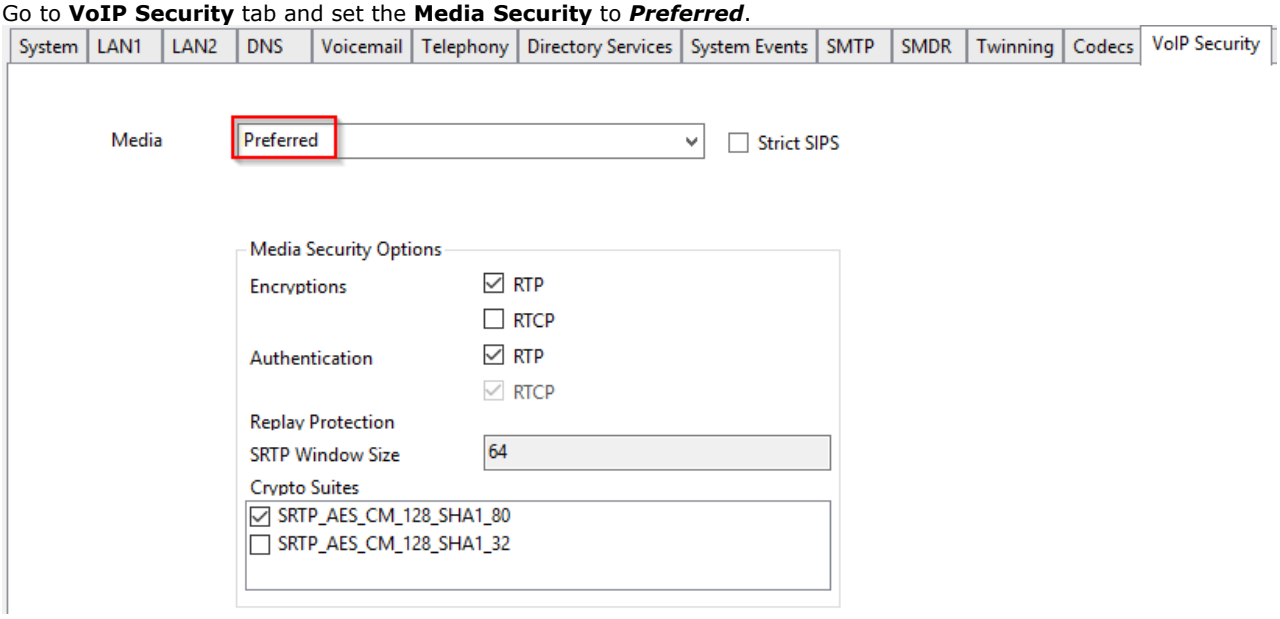
e. **Layer 4 Protocol:** Check the required Layer 4 protocols and set relevant ports. In this example TLS has been enabled in addition to the default UDP and TCP.

4. Select the VoIP tab.



a. **Allow Direct Media With NAT Location:** Selecting this option allows direct media to be attempted between devices that reside on the same side of any NAT that may be occurring. Note that direct media may still not be possible if there are codec or other VoIP setting mismatches.

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



6. Click **OK**.

7. Save the configuration.

2.3 Password Complexity Rules

The default IP Office user password complexity requirements are that passwords must be at least 8 characters which must be a mix of alphanumeric characters and no consecutive characters. There are some SIP softphone clients that only all the entry of numeric passwords. If that is the case, you must decide if you want to continue supporting those clients, since the process to enable number only user passwords significantly reduces the security of the IP Office system.

- **! WARNING**
  This process should only be used if absolutely necessary. It reduces the password security for all user access to the IP Office system and does so in a scenario where external access is also being configured.

To change the user password security requirements:

1. Using IP Office Manager, select **File | Advanced Settings | Se**curity.
2. Select the primary server and click **OK**. Login with the **Administrator** account.
3. Select **General**.
4. Set the **Minimum Password Complexity** to ***Low***. This allows the use of passwords containing only digits.
5. Click **OK**.
6. Click on the save icon.

2.4 Creating Users

Use the process below to create a new user or to amend the settings of any existing users.

To create a user:

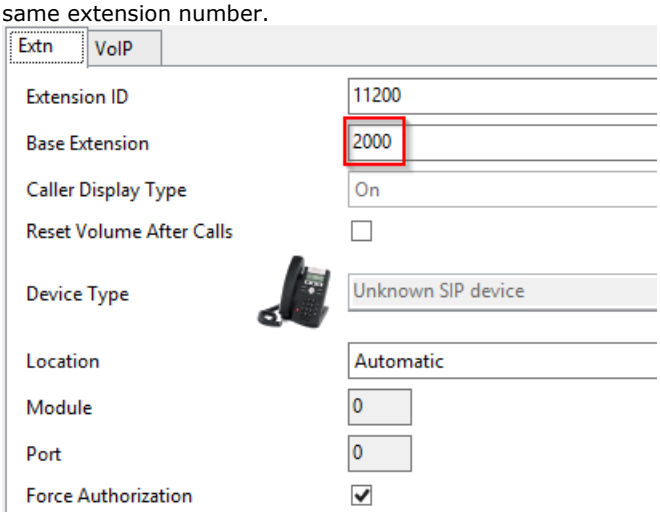
1. Using IP Office Manager, load the IP Office configuration. Select the primary server configuration.
2. Select **User**.
3. Click on the icon and select **User**.
4. Select the **User** tab and set the following:
   a. **Name:** This is the short name for the user. It is the user's user name for client login. It only displayed in applications if the **Full Name** (below) is not set.
   b. **Password:** This field is used for login to IP Office user applications. It may be necessary to digits only as not all clients support the entry of alphanumeric passwords. If so, the IP Office security settings have to also be adjusted to permit this, see Security Settings 15.
   c. **Extension:** This is the user's extension number.
   d. **Full Name:** This is the full name of the user. This is name displayed within applications and on phone calls.
   e. **Profile:** Select the profile that supports the applications and features the user wants to use.
      - **For one-X Mobile Preferred:**
        a. Select either **Power User**.
        b. Select **Enable Mobile VoIP Client**.
      - **For Avaya Communicator:**
        a. Select **Office Worker** or **Power User**.
        b. Select **Enable Communicator**.
5. Select the **Voicemail** tab.
   a. Enter and confirm a **Voicemail Code**. This is the pin code used for voicemail mailbox access.
6. Click **OK**.
7. Depending on the selected profile, IP Office Manager may insist that other user configuration fields are set. Follow the instructions given by IP Office Manager.
8. If the extension number doesn't match any existing extension, IP Office Manager prompts you whether it should create an extension. If so, select **SIP Extension** and click **OK**.
9. Save the configuration.

2.5 Creating SIP Extensions

Each SIP softphone requires a user and an extension entry in the IP Office configuration. If users have been created 15 without a SIP extension, use the following process to add the necessary extensions.

To create an extension:

1. Using IP Office Manager, load the IP Office configuration. Select the primary server configuration.
2. Select **Extension**.
3. Click on the icon and select **New | SIP Extension**.
4. In **Base Extension**, enter the extension number. This associates the extension entry with the user who has the same extension number.



5. Click **OK**.
6. Save the configuration.

2.6 Creating Presence Groups (XMPP)

The one-X Portal for IP Office acts as an XMPP server to provide presence indication to selected users. Within the IP Office configuration, XMPP groups are used to control which users can see each other's presence.

To create an XMPP hunt group:

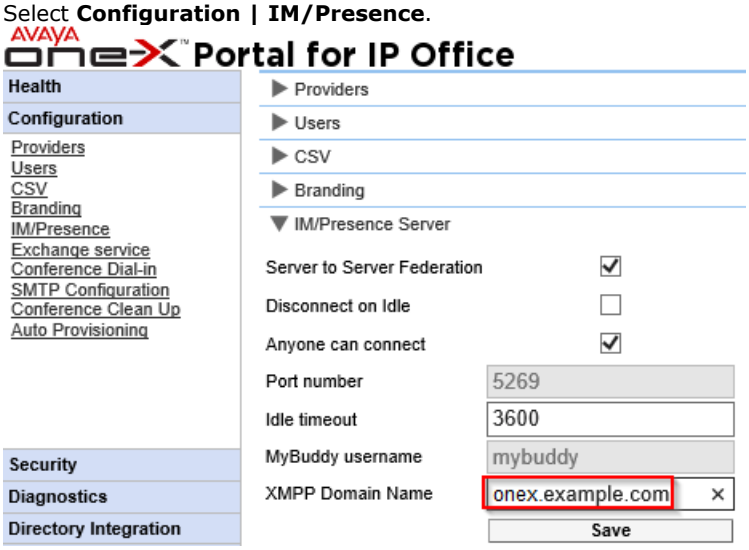
1. Using IP Office Manager, load the IP Office configuration.
2. Select **Group.**
3. Click the icon and select **Hunt Group**.
4. Select the **Group** tab and set the following:
   a. **Name:** Enter a name for the group.
   b. **Profile:** Select ***XMPP Group***.
   c. Under the **User List** click **Edit**. Select and append all the users who you want to be able to share their presence with each other.
   d. Click **OK**.
5. Click **OK**.
6. Save the configuration.

2.7 Setting the one-X Portal for IP Office XMPP Domain

The one-X Portal for IP Office needs to be configured with its fully qualified domain names. It supports several different domain names, for use by the different functions that it provides (portal host, XMPP domain and web collaboration domain). Whilst these can differ if required, for this example we are using the same FQDN for each function.

To configure the portal presence server:

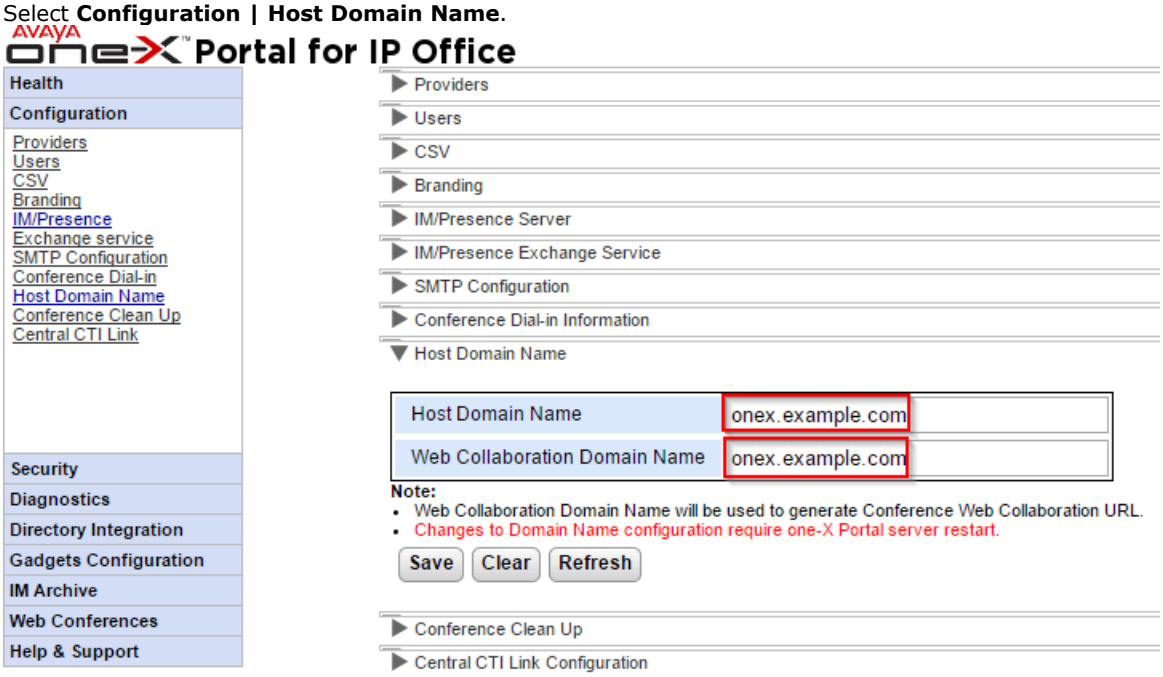
1. Login to the one-X Portal for IP Office administrator menus, either:
   - Within IP Office Web Manager, select **Applications | one-X Portal**.
   - or browse to *https://<portal IP address>:9443/onexportal-admin.html* and login as the Administrator.
2. Select **Configuration | IM/Presence**.



   a. Set the **XMPP Domain Name**. In this example we are using *onex.example.com*.

   b. Click **Save**.

3. Select **Configuration | Host Domain Name**.



   a. Set the **Host Domain Name**. In this example we are again using *onex.example.com*.

   b. Set the **Web Collaboration Domain Name**. In this example we are again using *onex.example.com*.

   c. Click **Save**.

4. Click on the icon at the top of the menus to restart the portal service.

Chapter 3.
Installing an ASBCE

3. Installing an ASBCE

This is a simple overview of the ASBCE installation. Actual installation should be done using the full set of ASBCE manuals.

Summary:

3.1 Deploying the OVA

To deploy the ASBCE OVA:

1. Download latest ASBCE OVA file from plds.avaya.com
2. Start vSphere Client and connect to the 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.

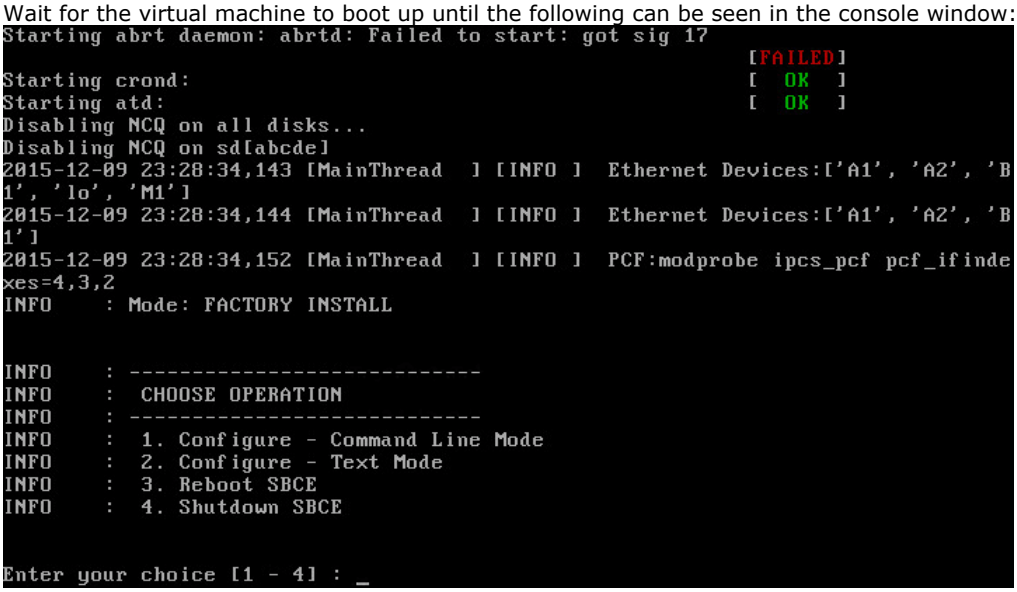
3.2 Setting Up ASBCE Management

This process configures the internal IP address used for ASBCE management and the root and ipcs user passwords.

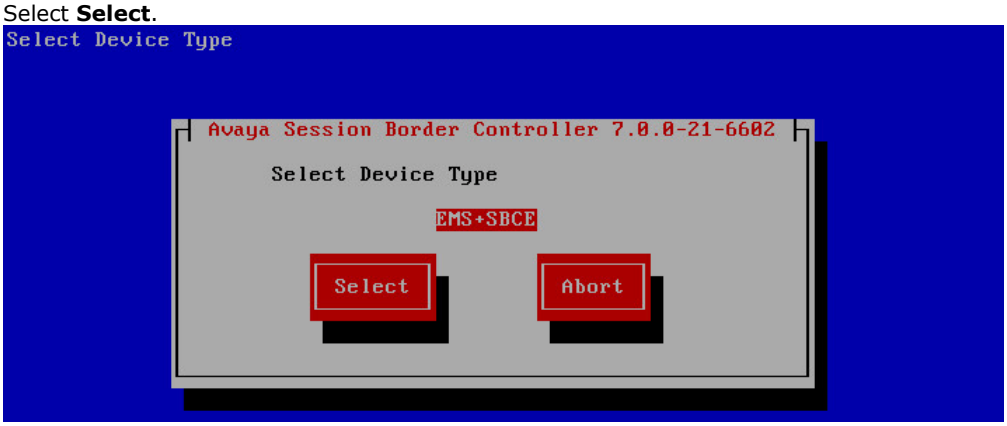
- It is strongly recommended that the ASBCE management IP address is on a different sub-net from the external and internal interfaces.

To set the ASBCE management IP address:

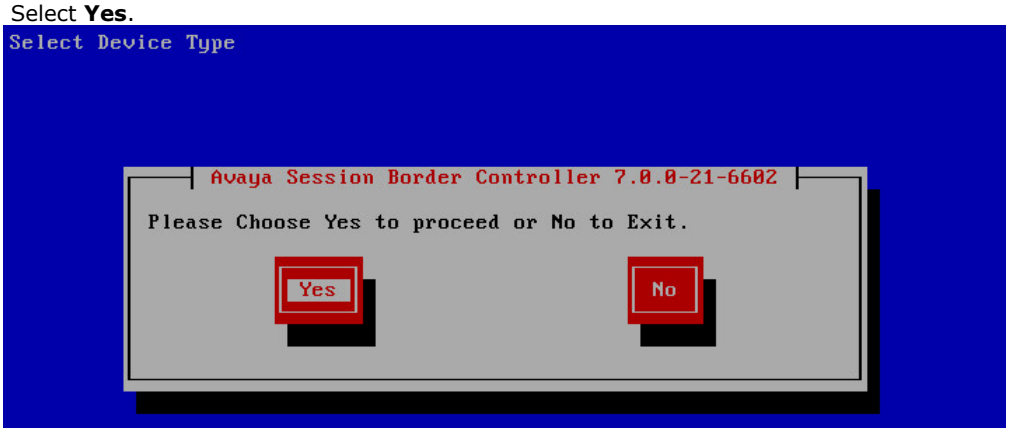
1. Right click on the ASBCE virtual machine and click on **Open Console**.
2. Wait for the virtual machine to boot up until the following can be seen in the console window:



3. Enter 2 to select **Configure - Text Mode**.
4. Select **Select**.

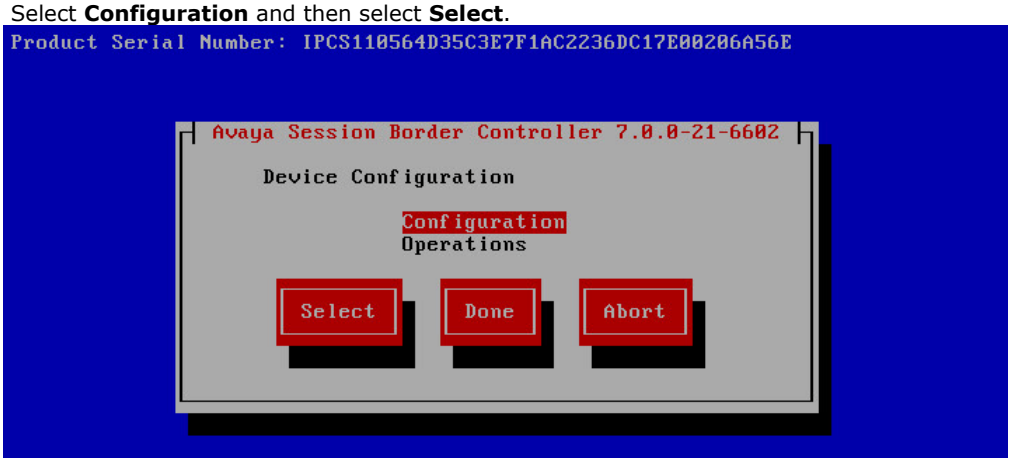


5. Select **Yes**.

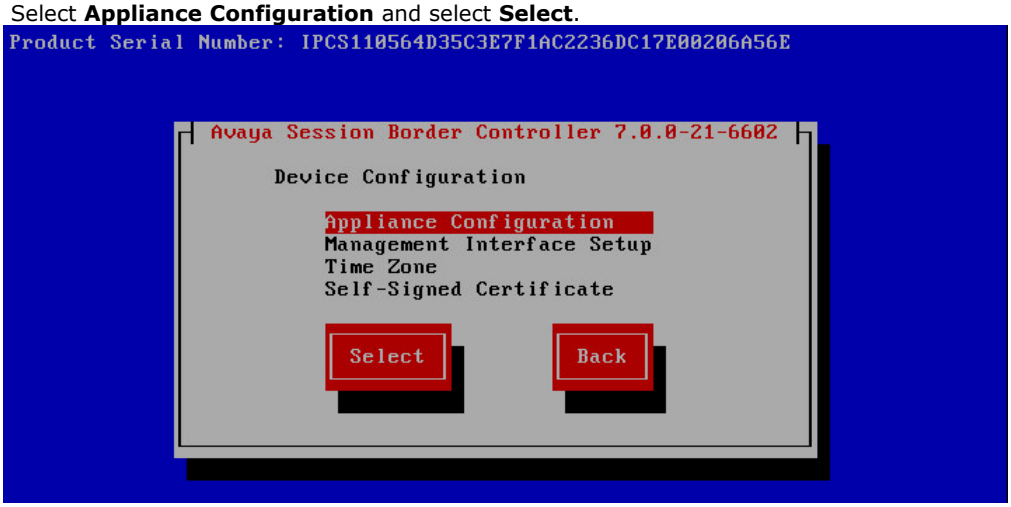


6. Select **OK**.

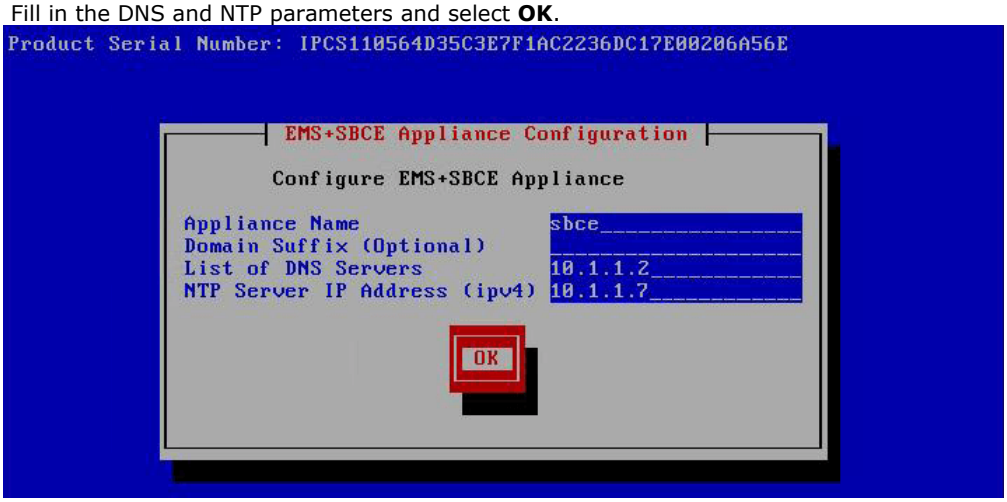
7. Select **Configuration** and then select **Select**.



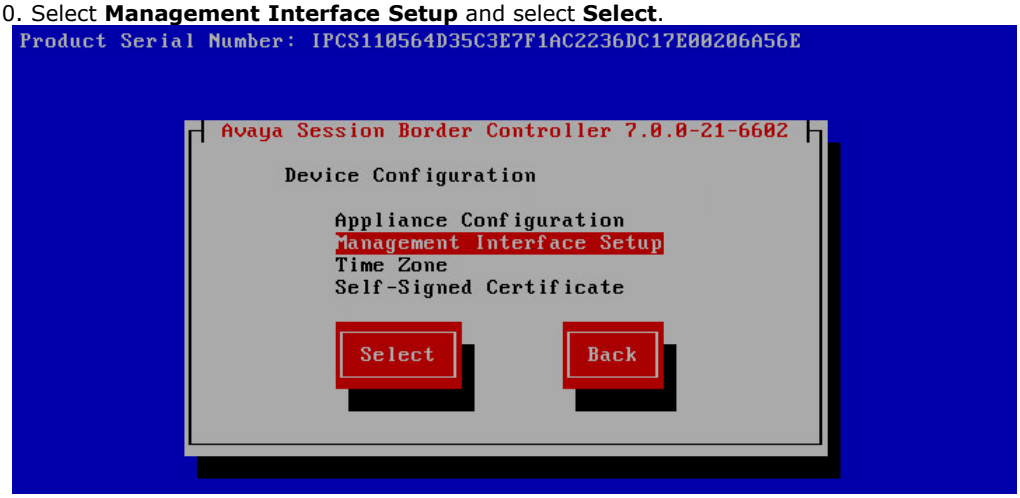
8. Select **Appliance Configuration** and select **Select**.



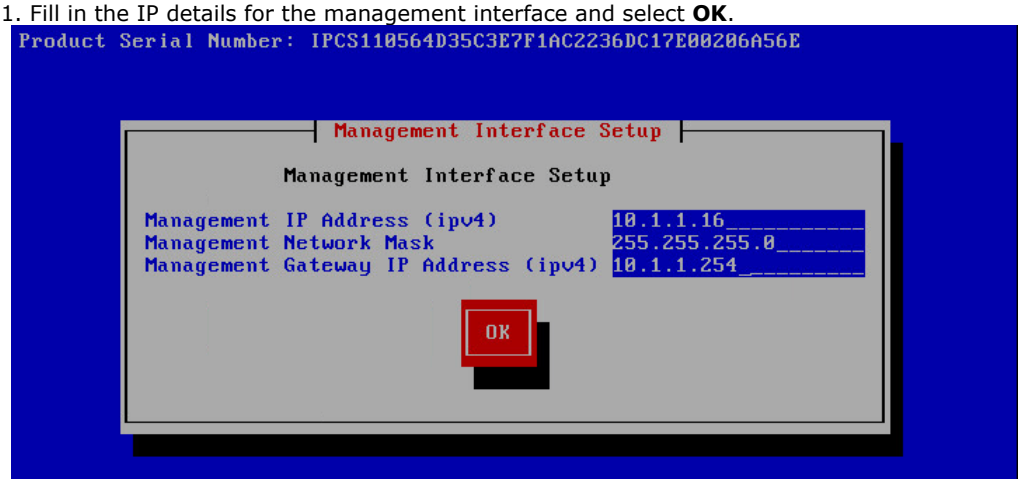
9. Fill in the DNS and NTP parameters and select **OK**.



10. Select **Management Interface Setup** and select **Select**.



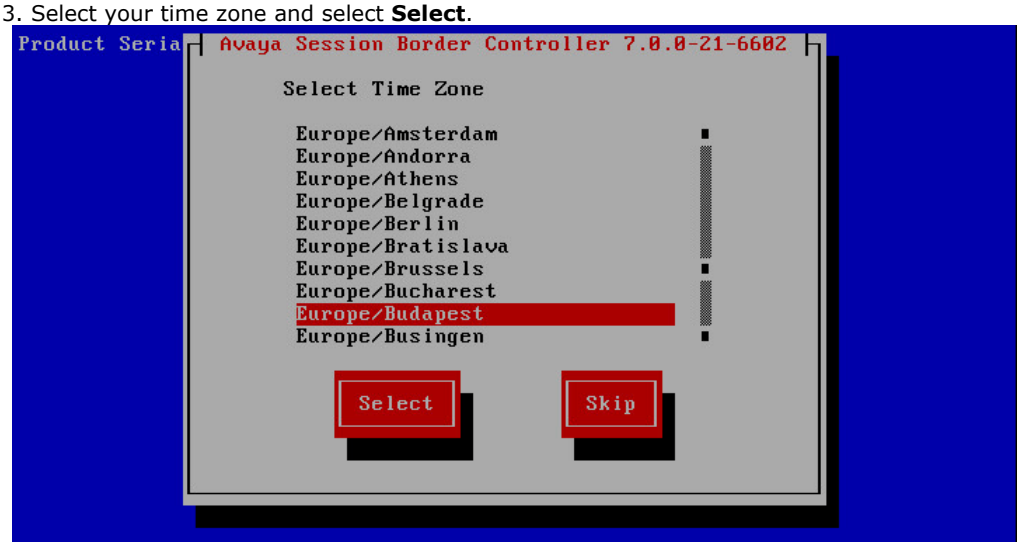
11. Fill in the IP details for the management interface and select **OK**.



- It is strongly recommended that the ASBCE management IP address is on a different sub-net from the external and internal interfaces.

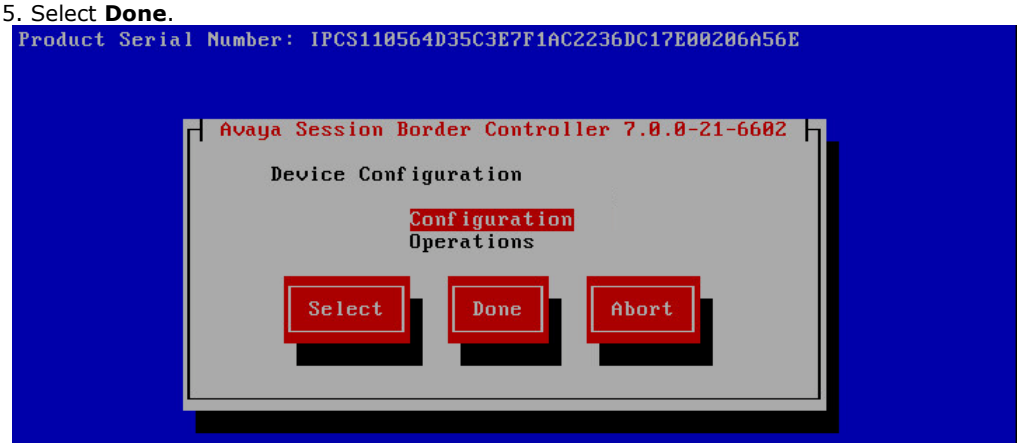
12. Select **Time Zone** and select **Select**.

13. Select your time zone and select **Select**.



14. Select **Back**.

15. Select **Done**.



16. You are now prompted to enter new passwords for a number of functions.

```
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: _
```

a. Enter new root password.

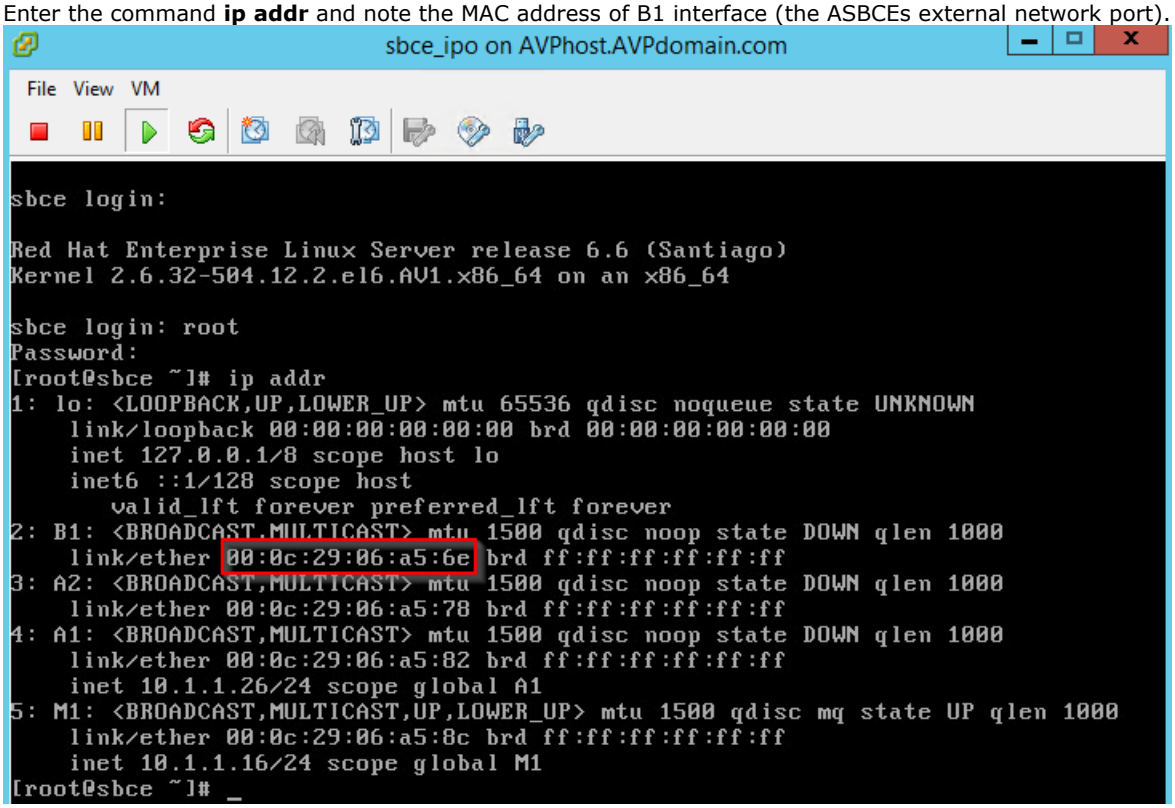
b. Enter new password for ipcs login.

c. Enter a new password for the ASBCE database.

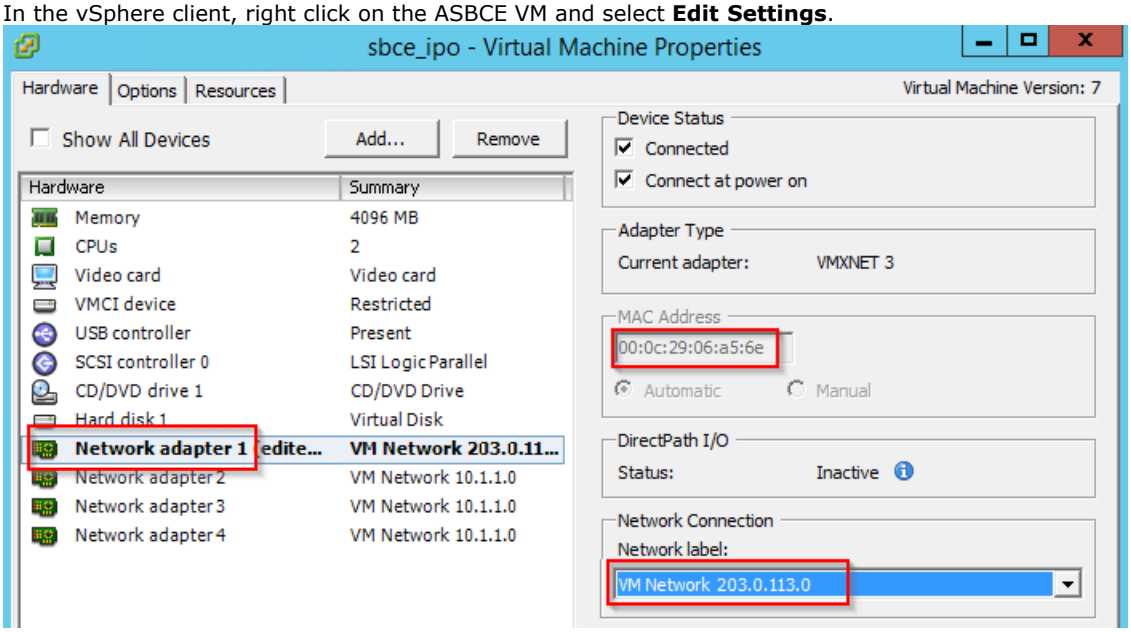
3.3 Set the External Interface

To set the VMware external interface:

1. At the console login with root using the new password.
2. Enter the command **ip addr** and note the MAC address of B1 interface (the ASBCEs external network port).



3. In the vSphere client, right click on the ASBCE VM and select **Edit Settings**.



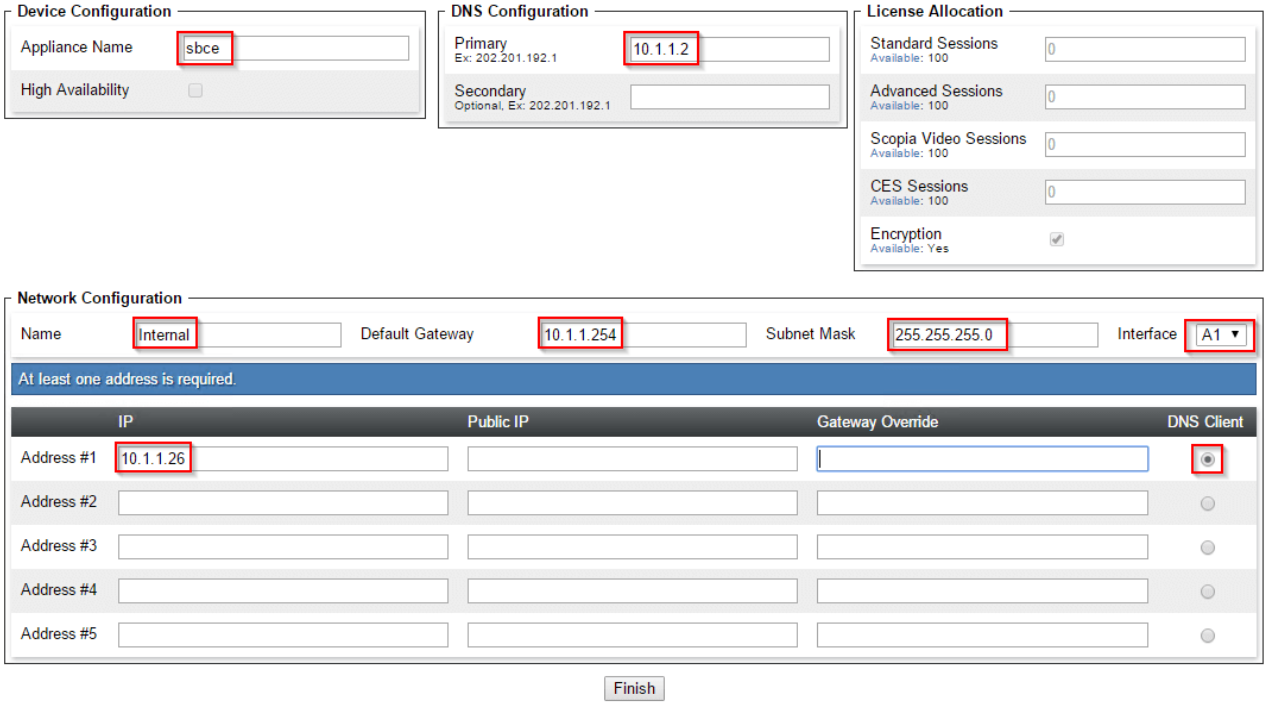
4. Select the **Network adapter** whose MAC address matches the MAC address of B1 interface.
5. Change the **Network Connection**.
6. Click **OK**.

3.4 ASBCE Initial Configuration

To setup the initial ASBCE configuration:

1. Using a browser, connect to https://<Management IP>/ , ie. the IP address setup previously 20.
2. Login with the user name ***ucsec*** and default password ***ucsec***.
3. As this is the first time login, the default password has to be changed. Enter a new password and click **Change Password**.
4. Login again using the new password.
5. Select **System Management**.

6. Click **Install**.



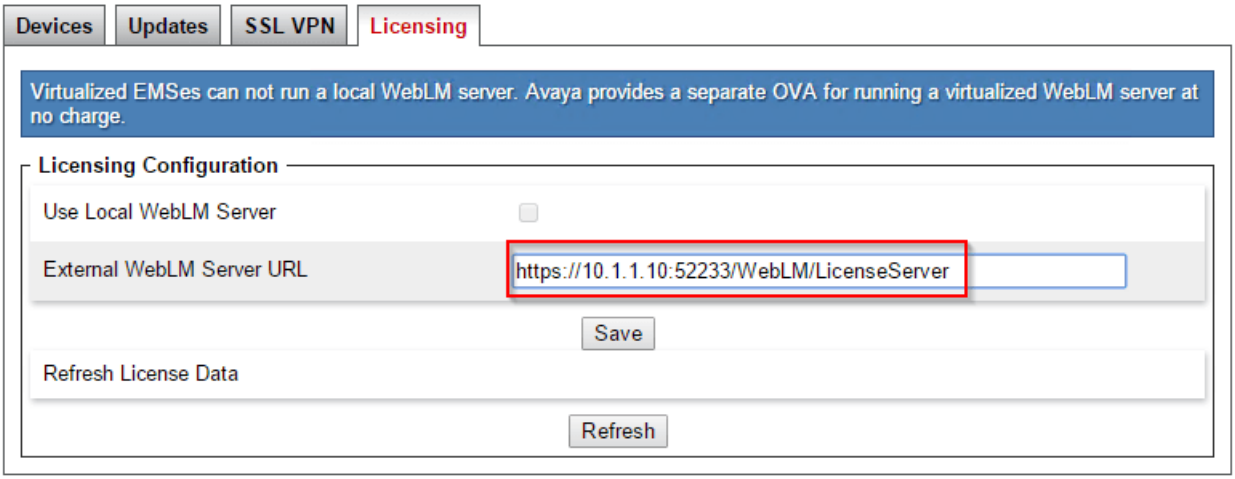
7. Set the following fields:
   a. **Device Configuration**
      i. **Appliance Name:** The internal name for the ASBCE.
   b. **DNS Configuration**
      i. **Primary:** The IP address of the internal DNS server.
   c. **Network Configuration**
      i. **Name:** Enter a name for the internal network.
      ii. **Default Gateway:** Enter the IP address of the gateway for the internal network.
      iii. **Subnet Mask:** Enter the subnet mask for the internal network.
      iv. **Interface:** Set the interface to **A1** for internal traffic
      v. **Address #1:** Enter the IP address for the internal interface
8. Click **Finish**.
9. Close the **Installation Wizard** browser window

3.5 Set the License Server Address

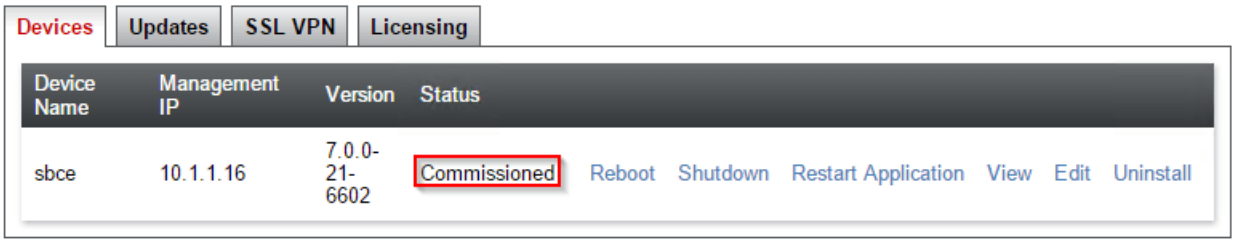
The ASBCE is licensed via a WebLM server. Note that that cannot be the WebLM service running on an IP Office system.

To set the ASBCE license server address:

1. Obtain ASBCE 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**.



4. Using the **System Management / Devices** tab verify that new device's Status is ***Commissioned***.



Chapter 4. Certification

4. Certification

The example in this document assumes that the IP Office system own self-certified certificates will be used. In that case, the ASBCE needs to have a copy of that certificate and also an identity certificate issued for it by the IP Office.

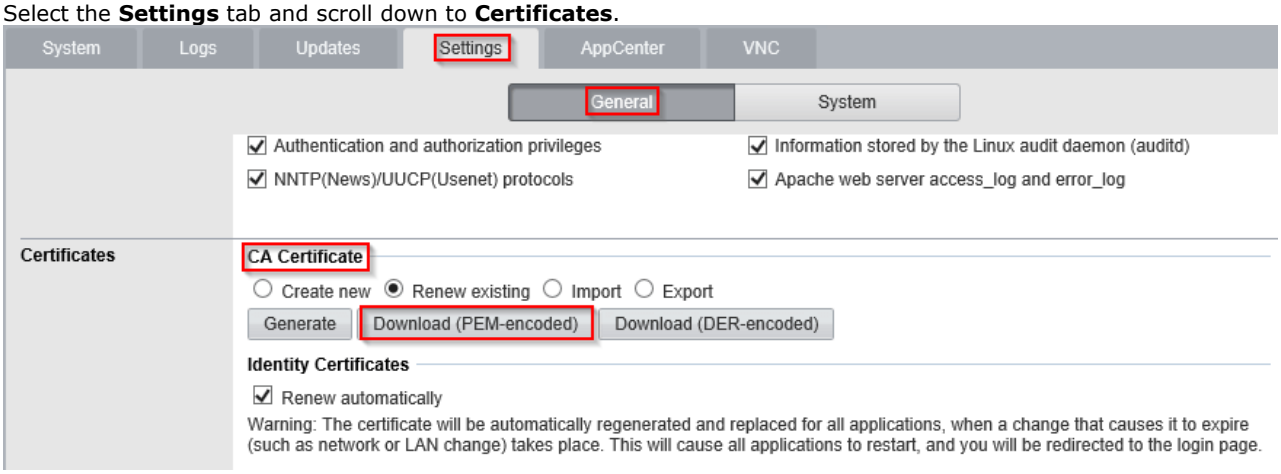
Summary:

4.1 Downloading the IP Office Root Certificate

A copy of the IP Office root certificate is needed. It will be loaded onto the ASBCE.

To download the IP Office root certificate:

1. Login to the IP Office's Web Control menus by either:
   - From within IP Office Web Manager, select the server. Click on ☰ and select **Platform View**.
   - or browse to *https://<IP Office IP address>:7071* and login as the **Administrator**.
2. Select the **Settings** tab and scroll down to **Certificates**.

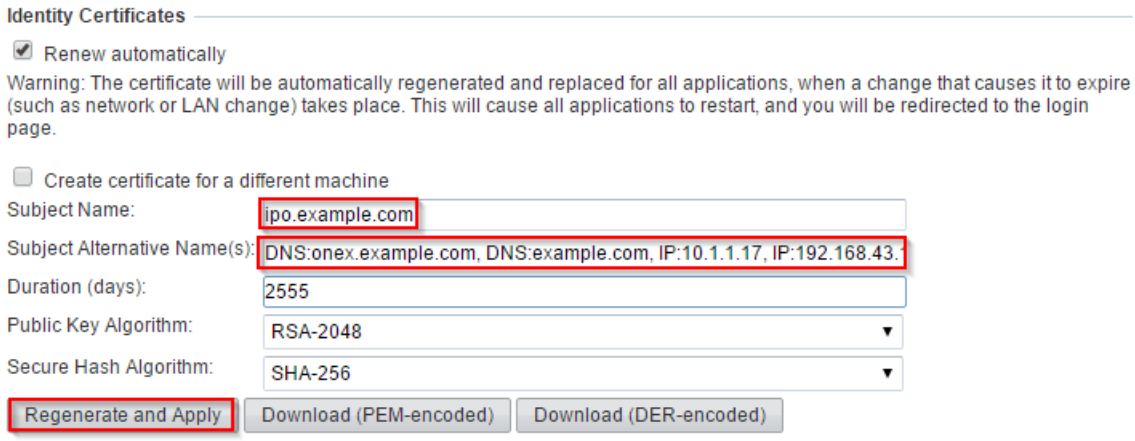


3. Under **CA Certificate**, click on **Download (PEM-encoded)** and save the file to your PC.
4. Rename the file as ***IPO_RootCA.crt***.

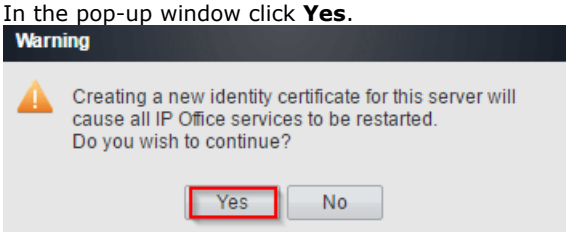
4.2 Generating an IP Office Identity Certificate

To generate an identity certificate for the IP Office:

1. Login to the IP Office's Web Control menus by either:
   - From within IP Office Web Manager, select the server. Click on ☰ and select **Platform View**.
   - or browse to *https://<IP Office IP address>:7071* and login as the **Administrator**.
2. Go to **Settings** tab and scroll down to **Certificates**.



3. Enter the following data:
   a. **Subject Name:** Enter the FQDN of the IP Office SIP domain.
   b. **Subject Alternative Name(s):** Enter comma separate **DNS:*<FQDN>*** and **IP:*<IP address>*** entries. These should include entries for the FQDNs of the one-X Portal for IP Office, XMPP Domain, IP Office SIP Domain and both the LAN1 and LAN2 IP addresses.
5. Click **Regenerate and Apply**.
6. In the pop-up window click **Yes**.

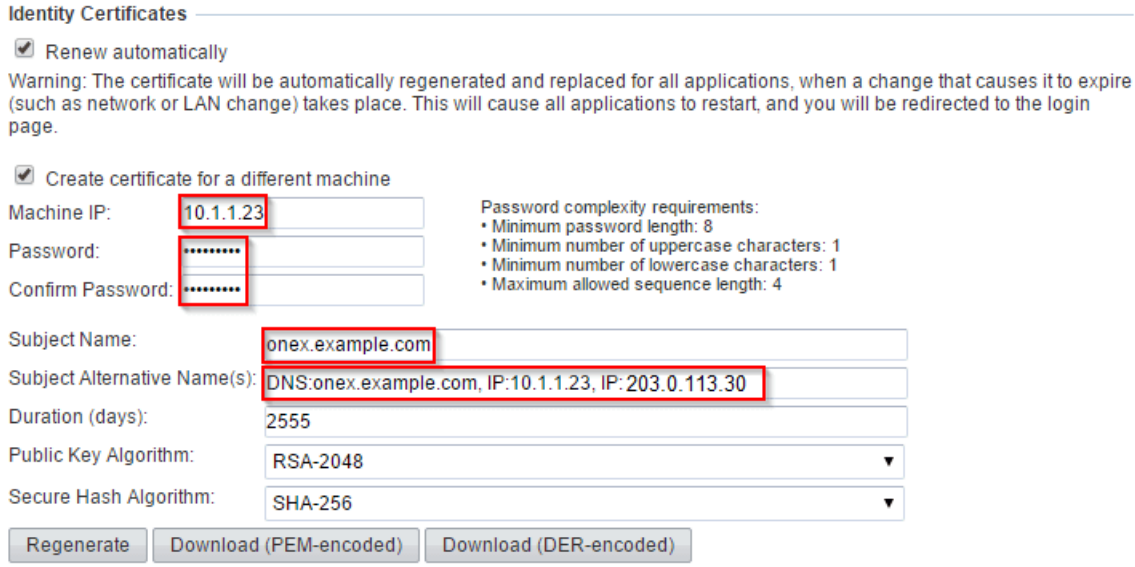


4.3 Generating a one-X Portal for IP Office Identity Certificate

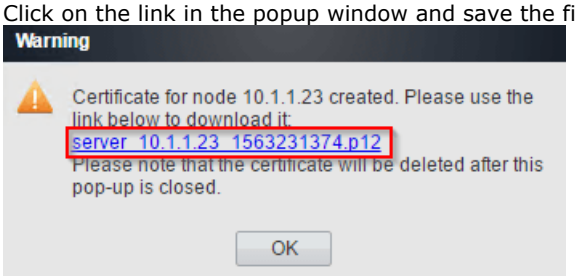
This stage is only required is the one-X Portal for IP Office is run on a separate Application Server. If that is the case, the portal requires its own identity certificate.

To generate an identity certificate for the one-X Portal for IP Office:

1. Login to the IP Office's Web Control menus by either:
   - From within IP Office Web Manager, select the server. Click on ☰ and select **Platform View**.
   - or browse to *https://<IP Office IP address>:7071* and login as the **Administrator**.
2. Go to **Settings** tab and scroll down to **Certificates**.
3. Check **Create certificate for a different machine**.



4. Enter the following data:
   a. **Machine IP:** Enter the IP address of the portal server.
   b. **Password:** Enter a password to encrypt the certificate and key.
      - Note that if any special characters are used in the password, to enter that password at the command line requires the character to be prefixed with a \. For example, a **@** in the password would be typed as **\@** at the command line.
   c. **Subject Name:** Enter the FQDN of the portal server.
   d. **Subject Alternative Name(s):** Enter comma separate **DNS:*<FQDN>*** and **IP:*<IP address>*** values for the portal's domain names and IP addresses.
5. Click **Regenerate**.
6. Click on the link in the popup window and save the file.

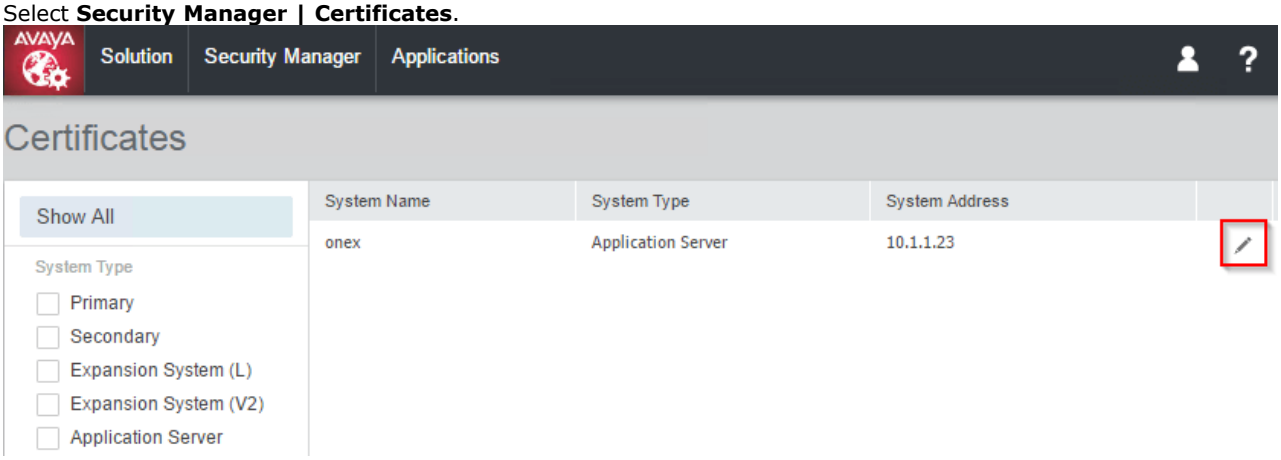


7. Rename the downloaded file to ***ONEX_ID.p12***.

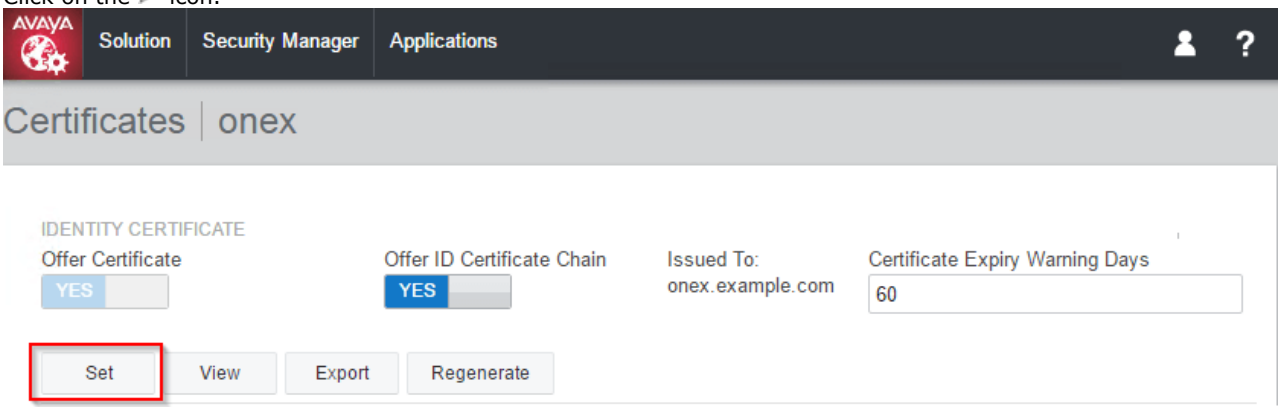
4.3.1 Installing a one-X Portal for IP Office Identity Certificate

To install a one-X Portal for IP Office identity certificate:

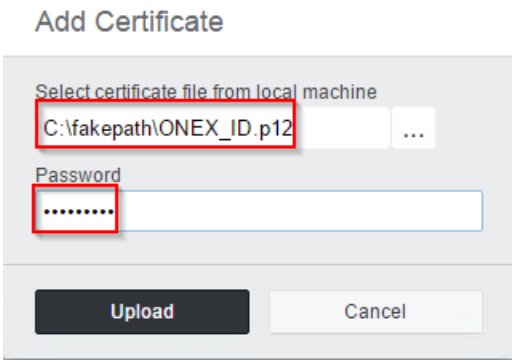
1. Browse to *https://<IP Office IP address>:7070* and login as the **Administrator**.
2. Select **Security Manager | Certificates**.



3. Click on the icon.



4. Click on **Set**.



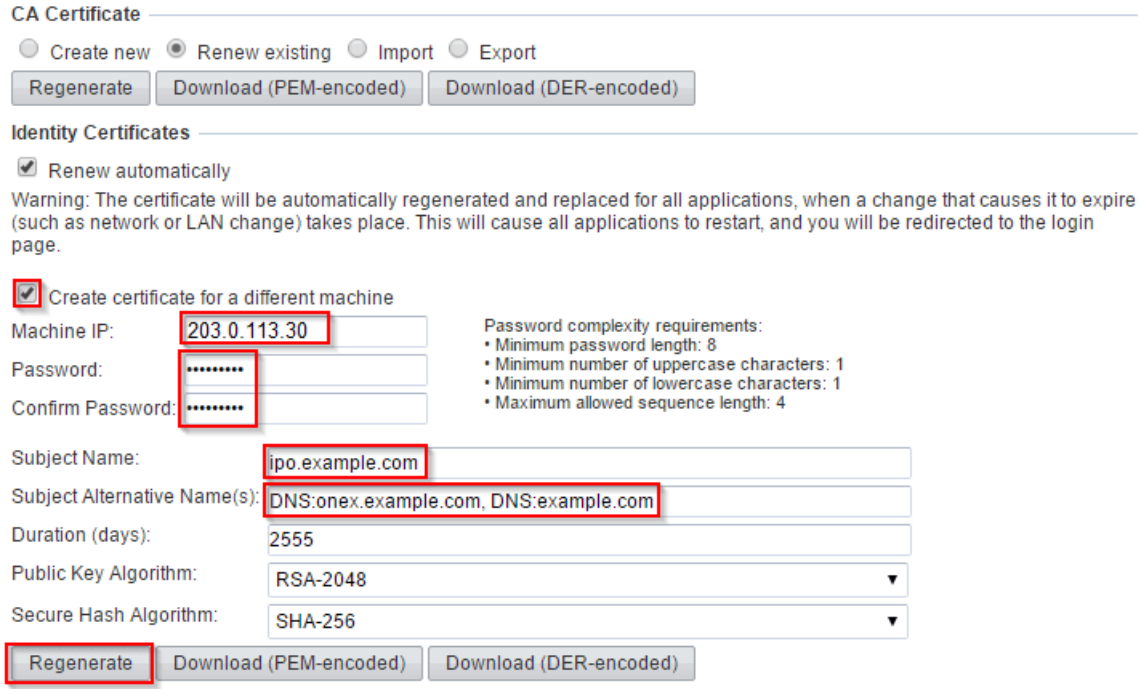
5. Browse to the location of the identity file created for the portal server.
6. Enter the certificate password.
7. Click **Upload**.

4.4 Generating an Identity Certificate for the ASBCE

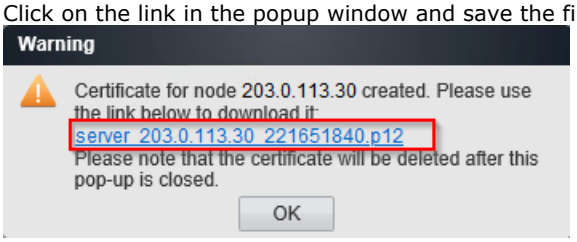
In addition to the IP Office root certificate, we also need to provide the ASBCE with an identity certificate. This certificate needs to include FQDN and IP address information for all the IP Office servers and services for which the ASBCE will be handling traffic.

To generate an identity certificate for the ASBCE:

1. Login to the IP Office's Web Control menus by either:
   - From within IP Office Web Manager, select the server. Click on ☰ and select **Platform View**.
   - or browse to *https://<IP Office IP address>:7071* and login as the **Administrator**.
2. Go to **Settings** tab and scroll down to **Certificates**.
3. Check **Create certificate for a different machine**.



4. Enter the following data:
   a. **Machine IP:** Enter the external IP address of the ASBCE.
   b. **Password:** Enter a password to encrypt the certificate and key.
      - Note that if any special characters are used in the password, to enter that password at the command line requires the character to be prefixed with a \. For example, a **@** in the password would be typed as **\@** at the command line.
   c. **Subject Name:** Enter the FQDN of the ASBCE.
   d. **Subject Alternative Name(s):** Enter comma separate values for **DNS:*<FQDN>*** and **IP:*<IP address>***.
      - Note: If you were using different FQDNs 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**.
5. Click **Regenerate**.
6. Click on the link in the popup window and save the file.



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

4.5 Extracting the ASBCE Private Key and Identity Certificate

The IP Office identity certificate created for the ASBCE is a single file. For the ASBCE configuration it needs to be split into two files.

To extract the ASBCE private key and certificate:

1. Using WinSCP, connect to the ASBCE management IP address using port 222 and the ipcs login.
2. Copy the IP Office identity certificate created for the ASBCE 35 (***SBCE_ID.p12***) to the ***ASBCE /tmp*** directory.
3. Ssh to ASBCE Management IP using port 222 and ipcs login.
4. Enter the command ***sudo su*** and type the root password.
5. Enter the following commands. When prompted for a password or PEM pass phrase, enter the password specified when generating an identity certificate for the ASBCE 35.
   - Note that if any special characters are used in the password, to enter that password at the command line requires the character to be prefixed with a \. For example, a **@** in the password would be typed as **\@** at the command line.

   a. **cd /tmp**

   a. **openssl pkcs12 -in SBCE_ID.p12 -out SBCE_ID.crt**

   b. **openssl pkcs12 -nocerts -in SBCE_ID.p12 -out SBCE_ID.key**

   The whole sequence should look similar to the following:

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

6. Copy the new ***SBCE_ID.crt*** and ***SBCE_ID.key*** files from ASBCE to your PC
7. The ***SBCE_ID.crt*** file contains the ID certificate we generated for ASBCE 35, the IP Office root CA certificate, and the private key. To be able to properly import this file to the ASBCE, the CA certificate and the private key must be removed from this file.

   a. Open ***SBCE_ID.crt*** in WordPad on your PC.

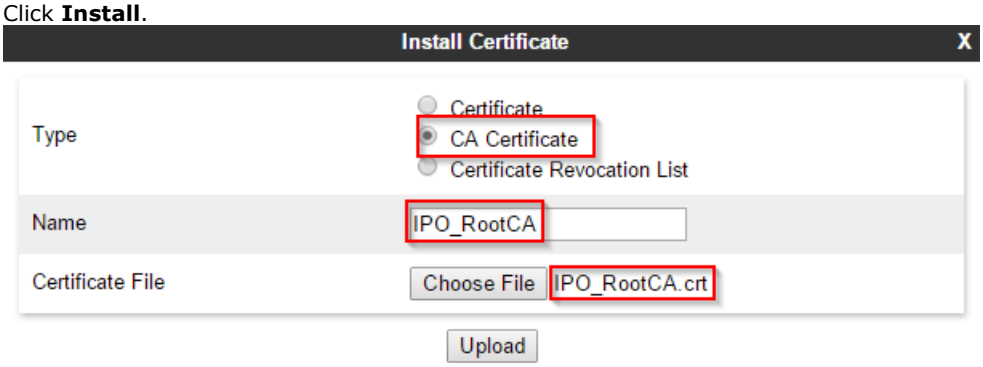
   b. Remove all lines except those which are between the first **BEGIN CERTIFICATE** and **END CERTIFICATE** lines. The resulting file should look similar to the following:


```
-----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+lWPWJwImLrIk5PI5ZsXC
4n/9ZKQzibeylfblRQpiCgAaT6L2lvQvZfuETAfSYk4TwZUdMja8JGYDIkNqHBNp
FPb+W1/cPimututLyJYRVCGpkM6bGfmpyMbS3JDGtYWhb7uq19XqlMdZAVWtL5a1
Bxe1kwNfsYIOQGPDiOO9nO1s+9i2pcIUQ1BchpA2yUphvtwS2KrNMhOkG3mcpWHB
9a2PMn1DMM3PXMfyRh9vL00fMRSNVA==
-----END CERTIFICATE-----
```

4.6 Adding the IP Office Root CA to the ASBCE

To upload the IP Office Root CA Certificate:

1. Login to ASBCE web interface.
2. Go to **TLS Management | Certificates**.
3. Click **Install**.



   a. **Type:** Select ***CA Certificate***.

   b. **Name:** Enter a descriptive name for the root CA certificate.

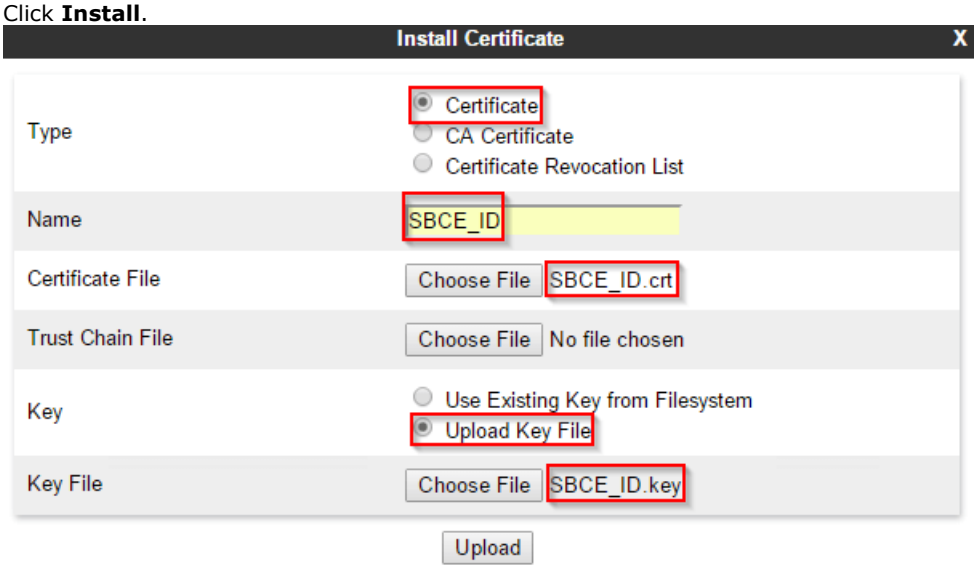
   c. **Certificate File:** Click **Choose File** and select the ***IPO_RootCA.crt*** file.

4. Click **Upload**. The certificate is displayed
5. Click **Install** and then **Finish**.

4.7 Adding the ASBCE Identity Certificate

To upload the ASBCE identity certificate:

1. Login to ASBCE web interface.
2. Go to **TLS Management | Certificates**.
3. Click **Install**.



   a. **Type:** Select **Certificate**.

   b. **Name:** Enter a descriptive name for the certificate.

   c. **Certificate File:** Click **Choose File** and select ***SBCE_ID.crt***.

   d. **Trust Chain File:** Leave this field empty.

   e. **Key:** Select **Upload Key File**.

   f. **Key File:** Click **Choose** File and open ***SBCE_ID.key***.

4. Click **Upload**. The certificate is displayed.
5. Click **Install** and then **Finish**.
6. Using Ssh, access the ASBCE Management IP address using port 222 and the ipcs login.

   a. Enter the command **sudo su** and enter the root password.

   b. Enter the following commands, replacing ******** with the password set when generating the ID certificate for the ASBCE:

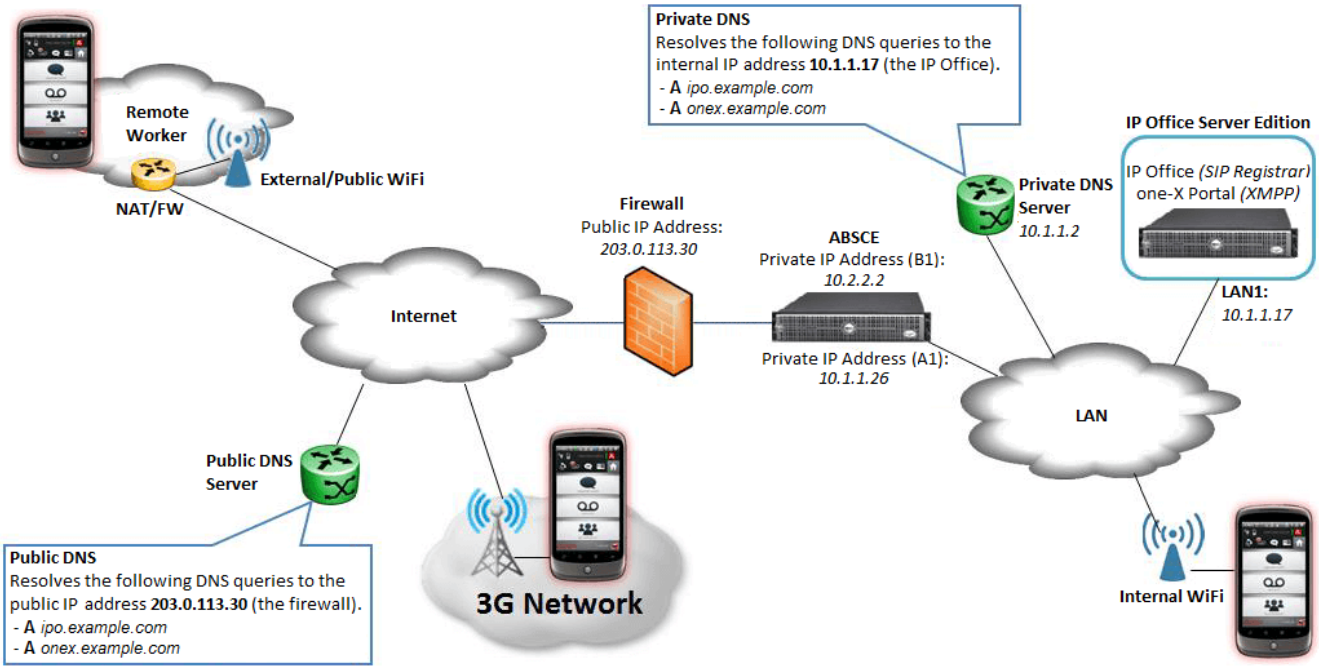
```
cd /usr/local/ipcs/cert/key
enc_key SBCE_ID.key ********
```

   - Note that if any special characters are used in the password, to enter that password at the command line requires the character to be prefixed with a \. For example, a **@** in the password would be typed as **\@** at the command line.

Chapter 5.
ASBCE Configuration

5. ASBCE Configuration

This section continues the ASBCE configuration 26 but this time looking at the specific configuration required for the example schematic 9.



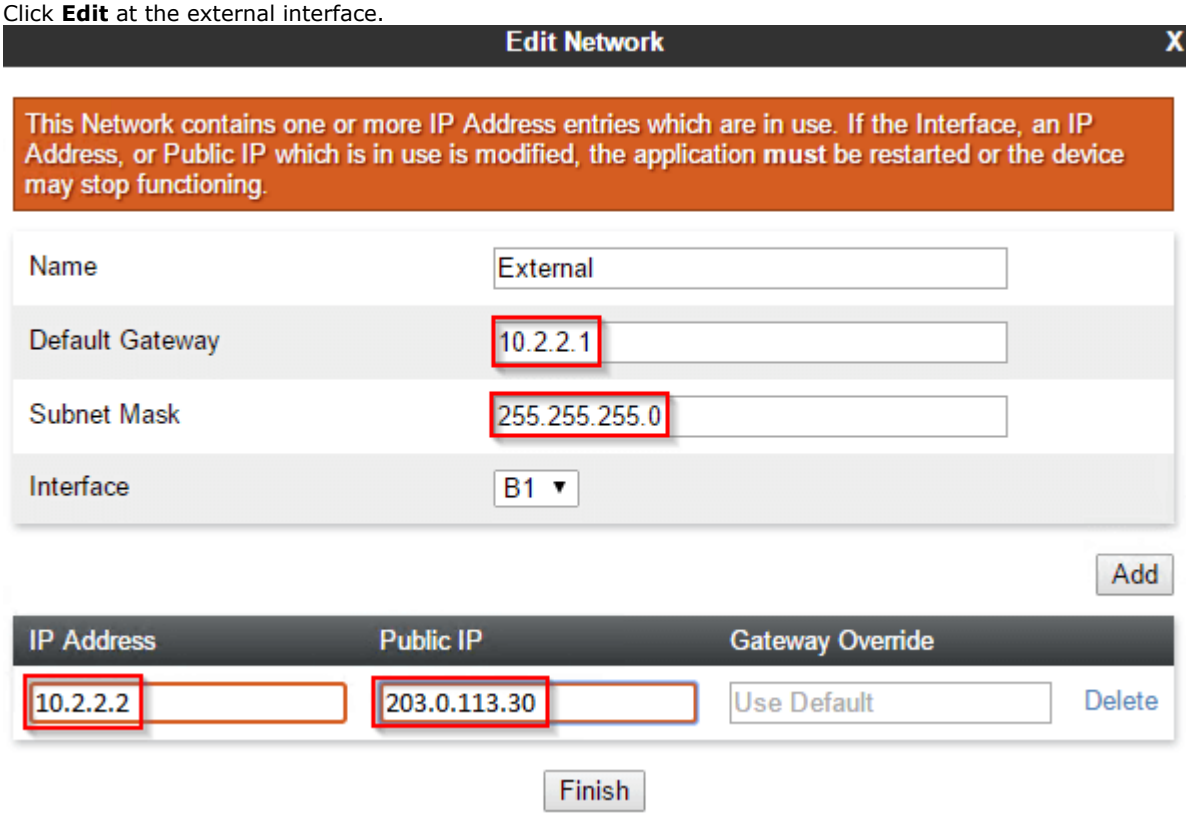
Summary:

5.1 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 ASBCE which are needed for the given clients.
3. Forward the RTP ports to the B1 interface of the ASBCE. The port range can be found on the external **Media Interface** of the ASBCE, by default it is UDP 35000-40000. See Media Interfaces 46.

5.2 Firewall Address Translation

1. Go to **Device Specific Settings** and then **Network Management**
2. Go to the **Network Configuration** tab.
3. Click **Edit** at the external interface.



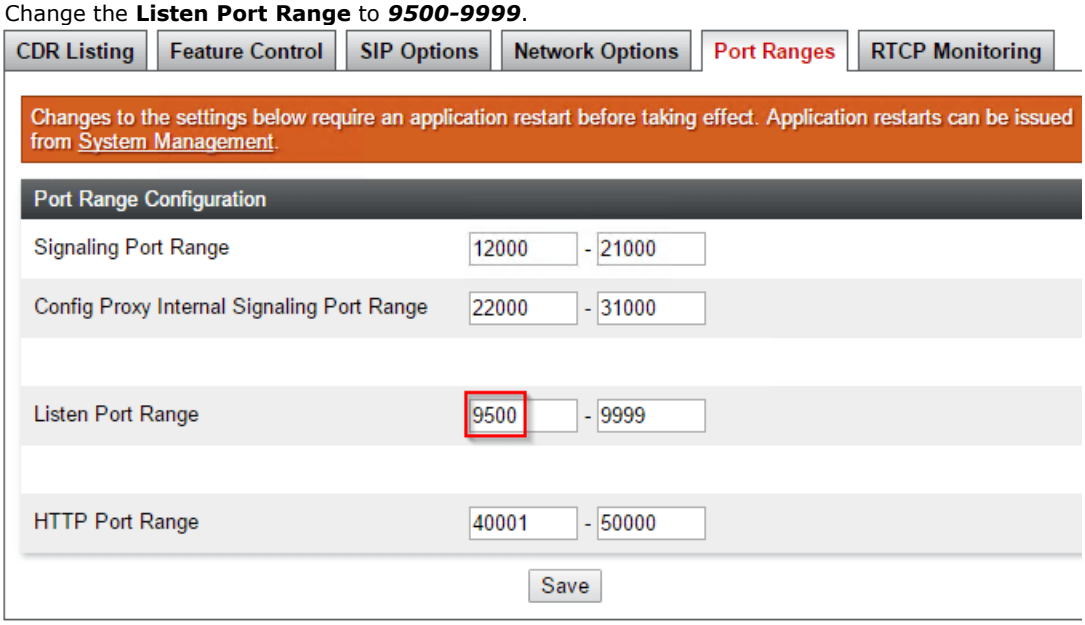
4. Enter the following data then click **Finish**. This applies NAT between the IP address and Public IP address settings.
   a. **Default Gateway:** Gateway IP address for the external interface.
   b. **Subnet Mask:** IP mask for the external interface.
   c. **IP Address:** IP address of the external interface.
   d. **Public IP:** External IP address of the Firewall.
5. Go to **System Management** and click **Restart Application**.

5.3 Changing the Default Listen Port Range

This step is necessary so that later we are able to configure listen port 9443 in Application Relay 56.

To change the default listening port range:

1. Go to **Device Specific Settings | Advanced Options**.
2. Select the **Port Ranges** tab.
3. Change the **Listen Port Range** to ***9500-9999***.



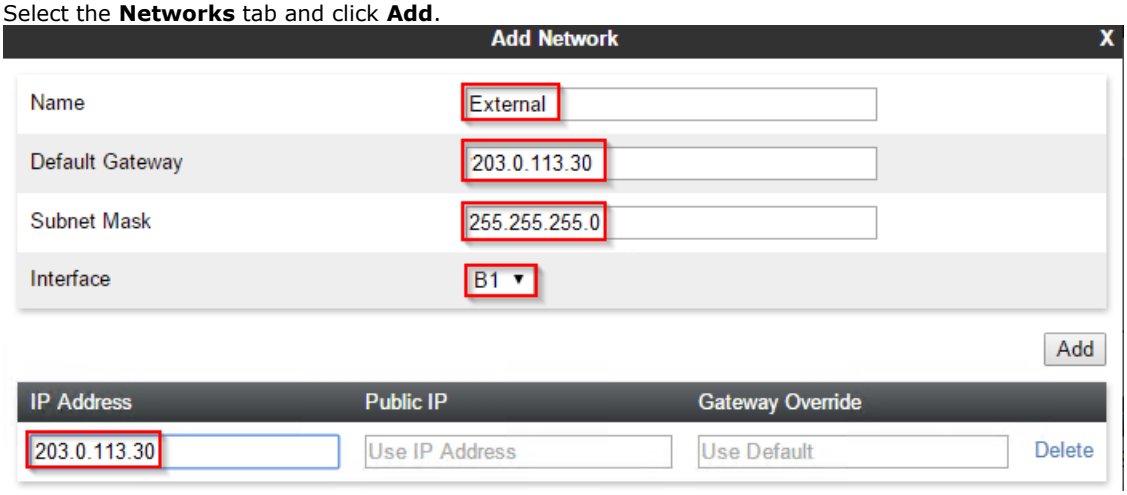
4. Click **Save**.
5. Go to **System Management** and on the **Devices** tab click **Restart Application**.
6. You now need to enable the internal and external ASBCE interfaces. See Enable the Internal/External Interfaces 43.

5.4 Enable the Internal/External Interfaces

To enable the interfaces:

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

3. Select the **Networks** tab and click **Add**.



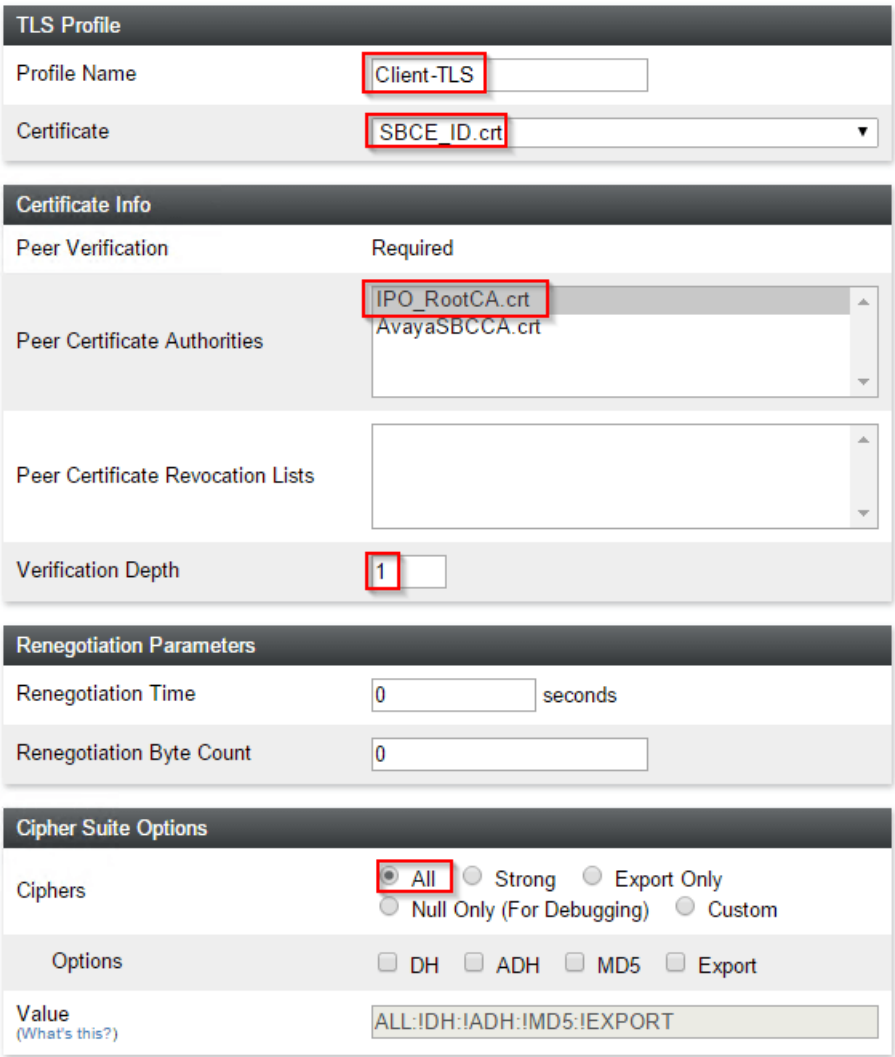
4. Enter the following data:
   a. **Name:** Enter a name for the external interface.
   b. **Default Gateway:** Enter the IP address of the default gateway for the external interface.
   c. **Subnet Mask:** Set the IP address mask.
   d. **Interface:** Select **B1**.
   e. **IP Address:** Set the IP address of the external interface.
5. Click **Finish**.
6. Go to **System Management** and click on **Restart Application**.
7. You now need to create TLS profiles. See Create TLS Profiles 44.

5.5 Create TLS Profiles

We need to create TLS connection profiles which, amongst other settings, specify the certificates to use.

To add a TLS profile:

1. Login to ASBCE web interface.
2. Go to **TLS Management | Client Profiles** and click **Add**.



   a. **Profile Name:** Enter a descriptive name. The name is used later to select the profile in the server profile 48 created for the IP Office server.

   b. **Certificate:** Select the ***SBCE_ID.crt*** file.

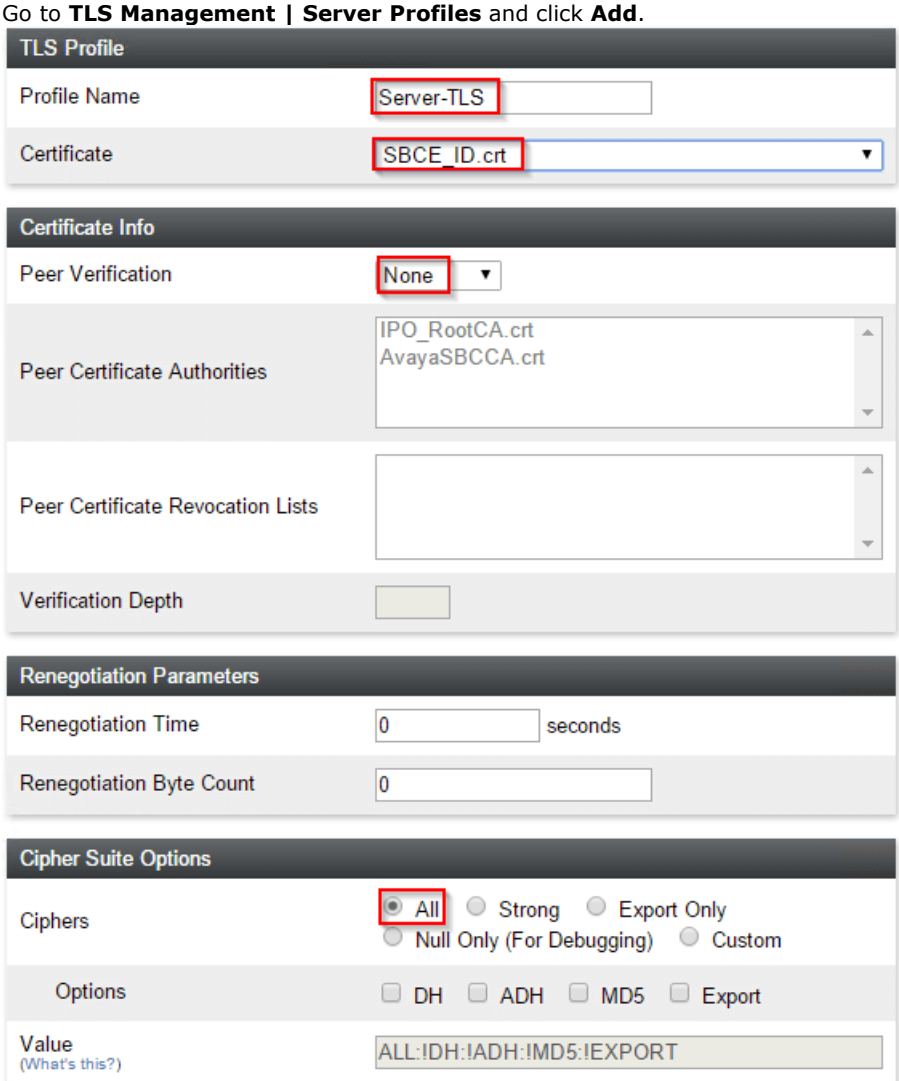
   c. **Peer Certificate Authorities:** Select ***IPO_RootCA.crt***.

   d. **Verification Depth:** Enter ***1***.

   e. **Ciphers:** Select ***All***.

3. Click **Finish**.

4. Go to **TLS Management | Server Profiles** and click **Add**.



a. **Profile Name:** Enter a descriptive name. The name is used later to select the profile in the signalling interfaces 47 created for the remote workers.

b. **Certificate:** Select ***SBCE_ID.crt***.

c. **Peer Verification:** Select ***None***.

d. **Ciphers:** Select ***All***.

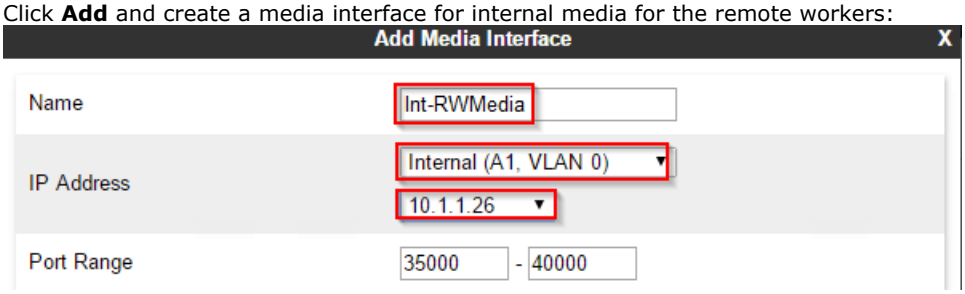
5. Click **Finish**.

6. You now need to create media interfaces for the remote worker traffic. See Create Media Interfaces 46.

5.6 Create Media Interfaces

To configure the media interfaces:

1. Go to **Device Specific Settings | Media Interface**.
2. Click **Add** and create a media interface for internal media for the remote workers:

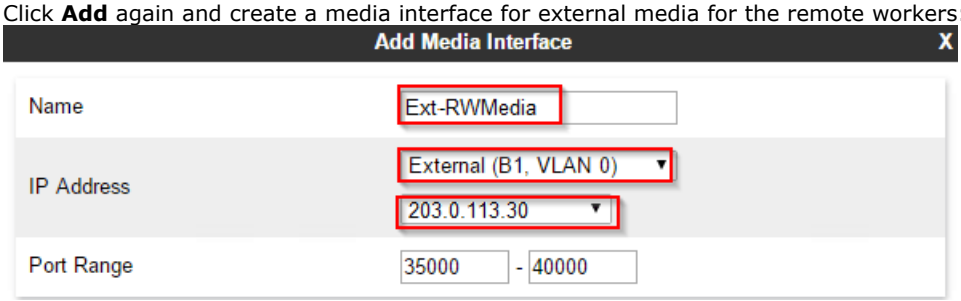


   a. Enter a **Name** for the internal interface. This name is used to select the interface when creating the server flow 55 to the IP Office server.

   b. Choose ***A1*** from the drop-down list of IP Address.

   c. Click **Finish**.

3. Click **Add** again and create a media interface for external media for the remote workers:



   a. Enter a **Name** for the internal interface. This name is used to select the interface when creating the subscriber flow 53 to the remote workers.

   b. Choose ***B1*** from the drop-down list of IP Address.

   c. Click **Finish**.

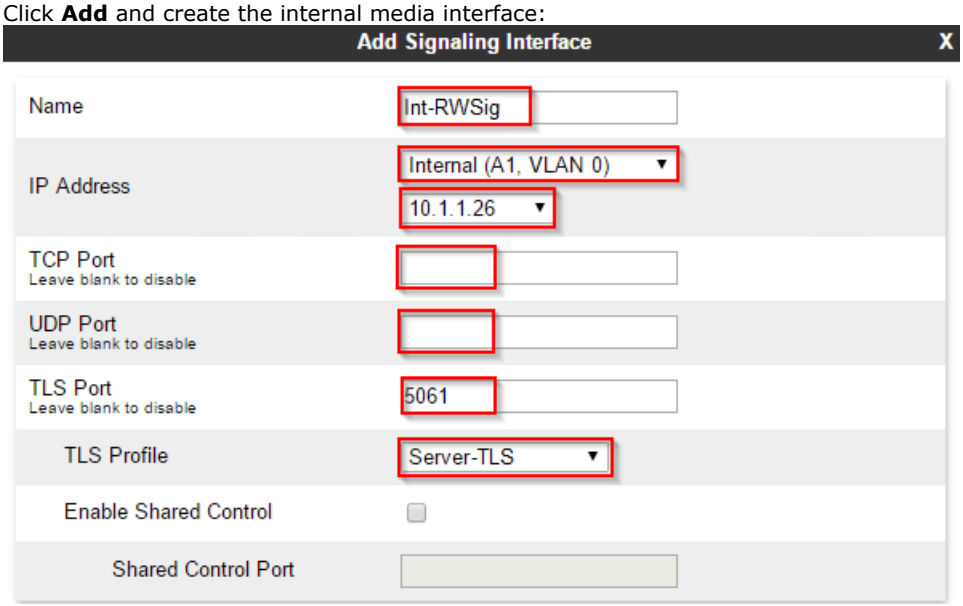
4. You now need to create signalling interface for the remote worker traffic. See Create Signaling Interfaces 47.

5.7 Create Signaling Interfaces

We need to create signalling interfaces that match the SIP ***Layer 4 Protocols*** configured in the IP Office SIP settings 13. In this example we are allowing just TLS connection using port 5061.

To configure the signaling interfaces:

1. Go to **Device Specific Settings | Signaling Interface**.
2. Click **Add** and create the internal media interface:



   a. **Name:** Enter a descriptive name for the interface. This name is used to select the interface when creating the server flow 55 for the IP Office server.

   b. **IP Address:** Choose ***A1*** from the drop-down list (the ASBCE's internal port).

   c. **TCP Port:** Leave this blank to disable TCP.

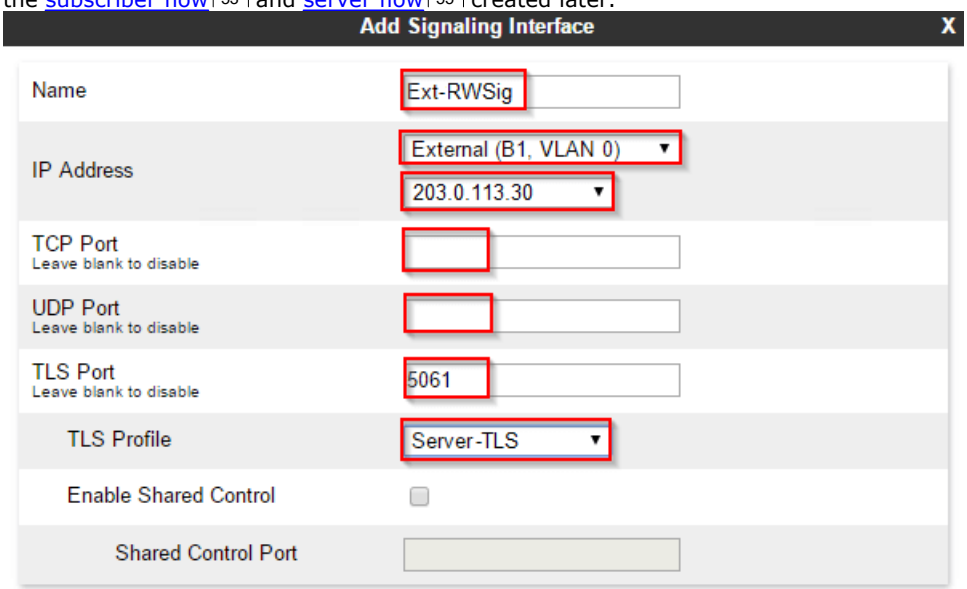
   d. **UDP Port:** Leave this blank to disable UDP.

   e. **TLS Port:** Set this to match the IP Office TLS port (default 5061).

   f. **TLS Profile:** Select the TLS profile 44 previously created for the server, in this example ***Server-TLS***.

   g. Click **Finish**.

3. Repeat the above to add an external media interface, choosing ***B1*** this time. This configuration entry is used in the subscriber flow 53 and server flow 55 created later.



4. You now need to create a server profile for the IP Office server. See Create a Server Profile 48.

5.8 Configure Server Interworking Profile

Procedure

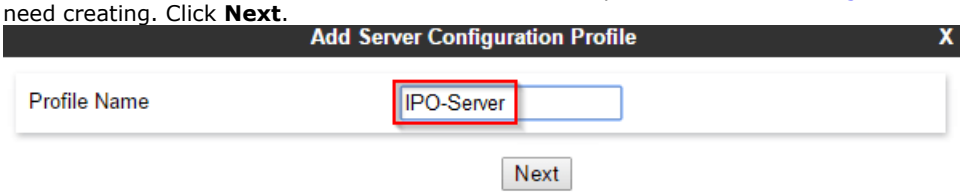
1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Server Interworking**.
4. The profile used for remote workers on the IP Office is ***avaya-ru*** server interworking. Highlight the ***avaya-ru*** profile.
5. Click **Clone**.
6. Enter a name for the profile and click **Finish**.

5.9 Create a Server Profile

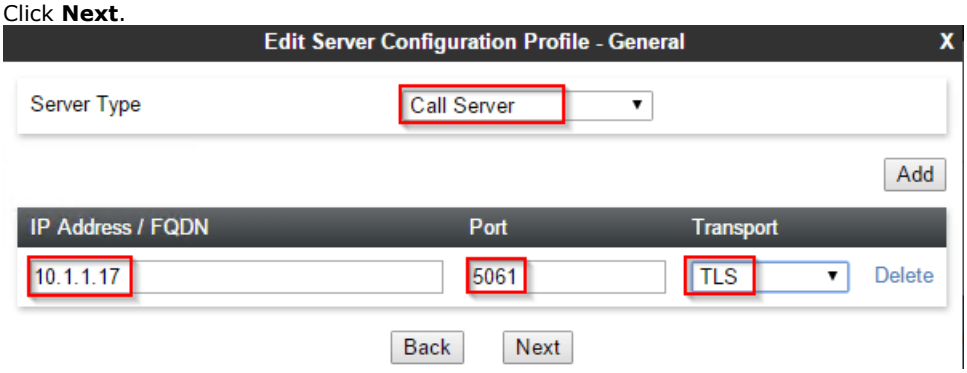
We need to create a server profile for the IP Office.

To add a server profile:

1. Go to **Global Profiles | Server Configuration**.
2. Click **Add**.
3. Enter a **Profile Name**. This name is used to select the profile in server routing 50 and server flow 55 entries that need creating. Click **Next**.



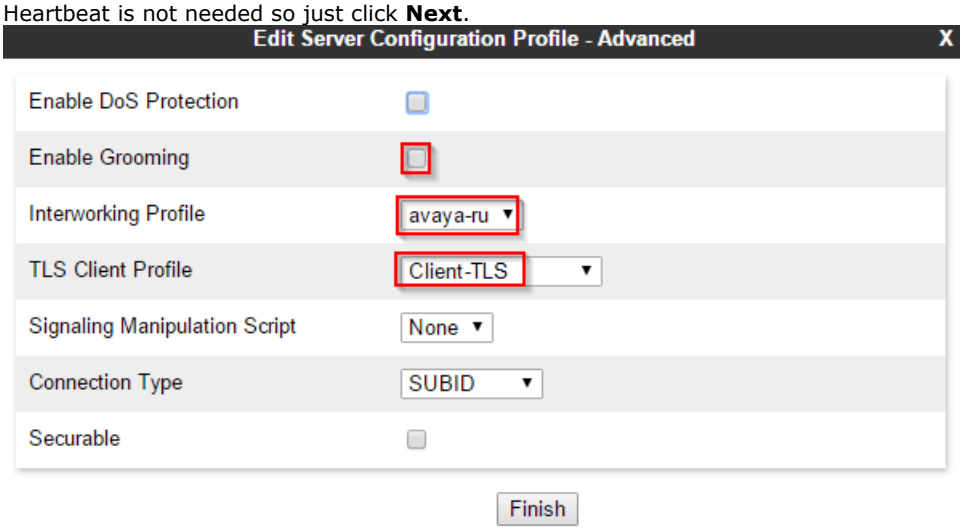
4. Click **Next**.



   1. Set the **Server Type** to ***Call Server***.
   2. Enter the details for the layer 4 port SIP connections set in the IP Office configuration 13. For this example we are using TLS on port 5061 for the external extensions. Click **Next**.

5. Authentication is not needed so just click **Next**.

6. Heartbeat is not needed so just click **Next**.



   a. **Enable Grooming:** Deselect this option.

   b. **Interworking Profile:** Set to ***avaya-ru*** or the previously created clone 48 of that profile.

   c. **TLS Client Profile:** Set to the TLS profile 44 previously created for the remote workers, in this example ***Client-TLS***.

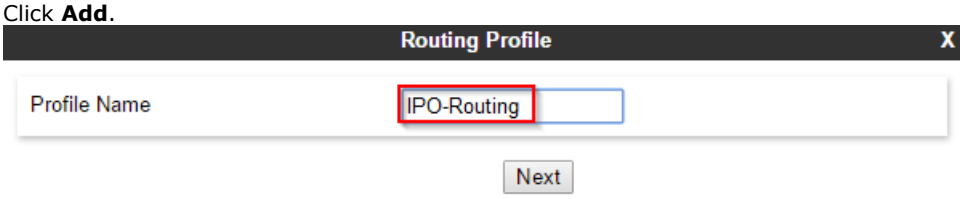
7. Click **Finish**.

8. You now need to create a server routing entry for the IP Office server. See Create Server Routing 50.

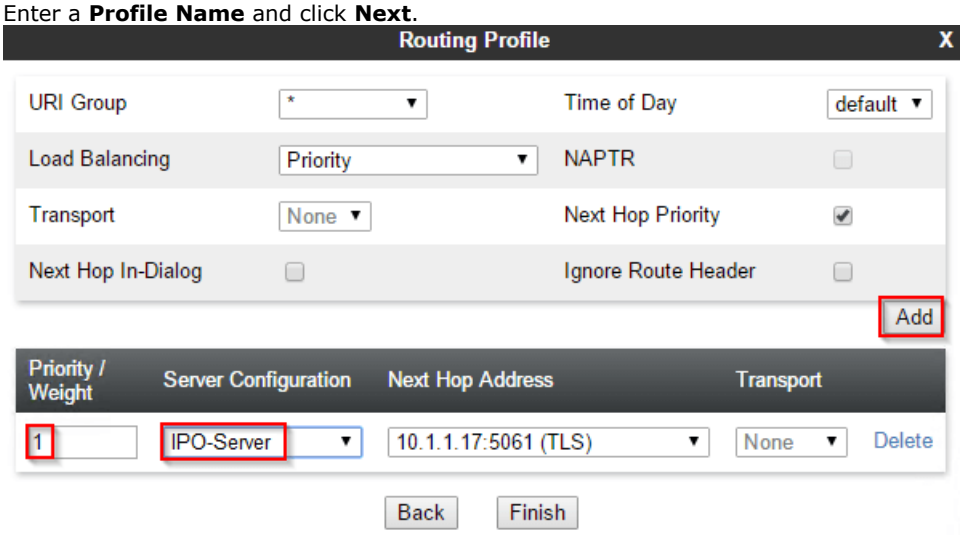
5.10 Create Server Routing

To configure routing:

1. Go to **Global Profiles | Routing**.
2. Click **Add**.



3. Enter a **Profile Name** and click **Next**.



4. Click **Add**.
5. Enter the **Priority** and set the **Server Configuration** to the server profile 48 created for the IP Office server, in this example ***IPO-Server***.
6. In the **Next Hop Address** enter the IP address or FQDN of the IP Office.
7. Click **Finish**.
8. You now need to a topology hiding entry for the IP Office applications. See Create a Topology Hiding 51.

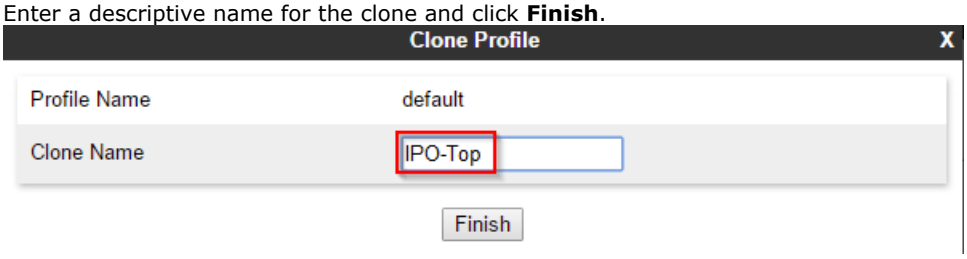
5.11 Create a Topology Hiding

Topology hiding allows selected information in SIP messages to be replaced when necessary, for example when a particular application uses an IP address when it should use the corresponding domain name.

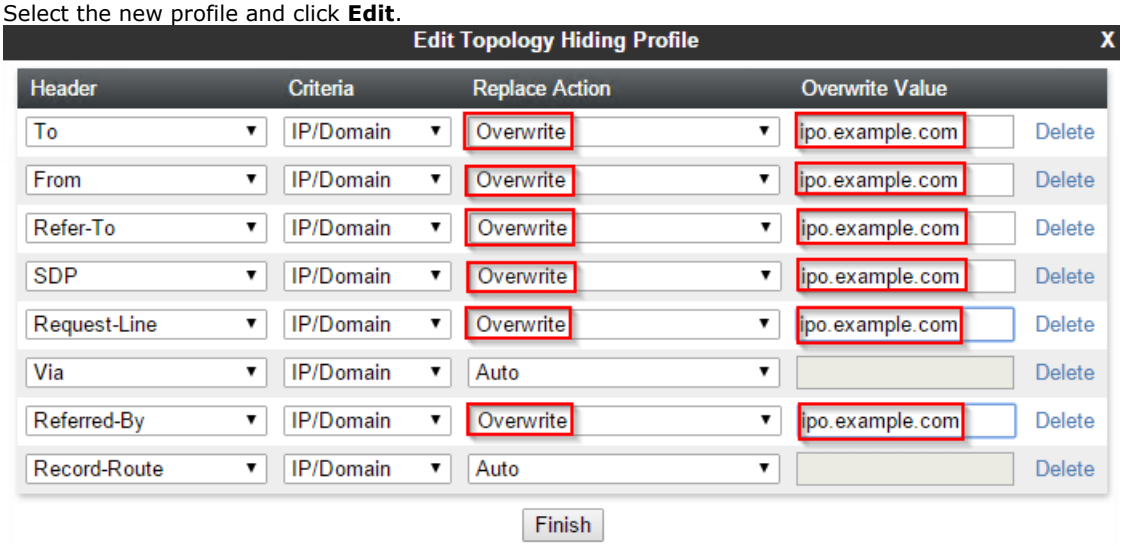
- **Avaya Communicator for Windows**
  During Avaya Communicator for Windows registration, the IP Office includes the internal IP address of the XMPP domain in the ***onex_server*** field of the 200 OK XML body. As a result, external clients are not able to register with the one-X Portal for IP Office and have presence. Creating a custom topology hiding setting allows the IP address to be replaced with the required FQDN.

To create a topology hiding profile:

1. Go to **Global Profiles | Topology Hiding**.
2. Select the default profile and click **Clone**.
3. Enter a descriptive name for the clone and click **Finish**.



4. Select the new profile and click **Edit**.



5. For the **To**, **From**, **Refer-To**, **SDP**, **Request-Line** and **Referred-By** fields; set the **Replace Action** to ***Overwrite*** and enter the IP Office FQDN as the **Overwrite Value**.
6. Click **Finish**.
7. You now need to create a subscriber flow for traffic to/from the remote workers. See create a Subscriber Flow 53
.

5.12 Configuring User Agent Profiles

User Agent profiles can be created using what the endpoints send in the user agent header. When these profiles are put in a subscriber flow 53, only phones that match that User Agent are allowed to send registration or other messages through the SBCE.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Global Parameters** and then **User Agents**.
3. Click **Add**.
4. Enter a description then put in the type of user agent the endpoint you want to allow using regular expression. You can use one type per policy or you can put multiple types in one user agent profile.
5. Click **Finish**.
6. You can add the user agent header to a subscriber flow during the flow configuration or by editing an existing flow. In the subscriber flow **User Agent** field, select the user agent profile.

5.13 Configure Phone Interworking Profile

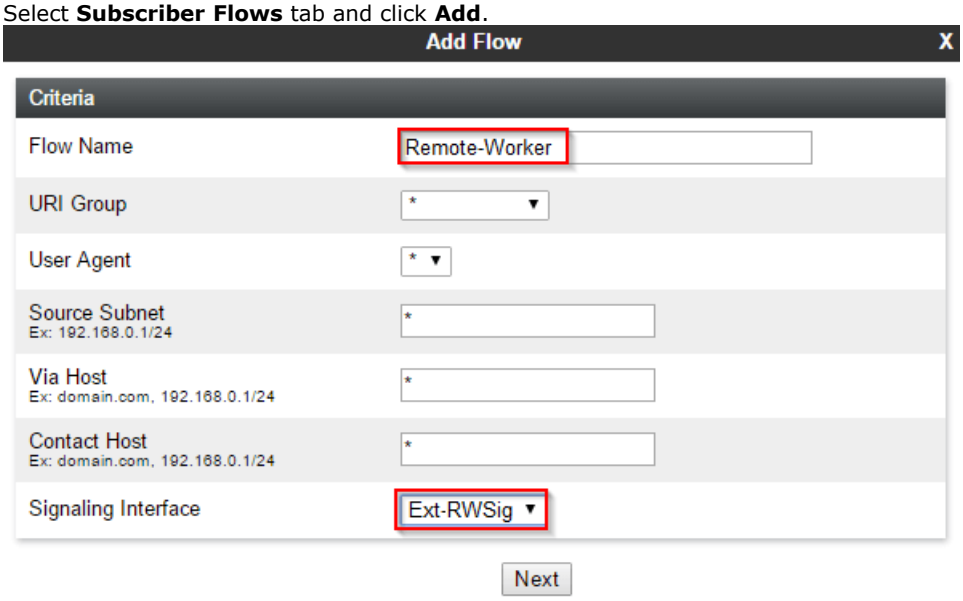
Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Device Specific Settings** and then **Global Profiles**.
3. Select **Phone Interworking**.
4. Select the **avaya-ru** profile and click **Clone**.
5. Enter a name for the profile and click **Finish**.

5.14 Create a Subscriber Flow

To configure the subscribe flow:

1. Go to **Device Specific Settings | End Point Flows**.
2. Select **Subscriber Flows** tab and click **Add**.

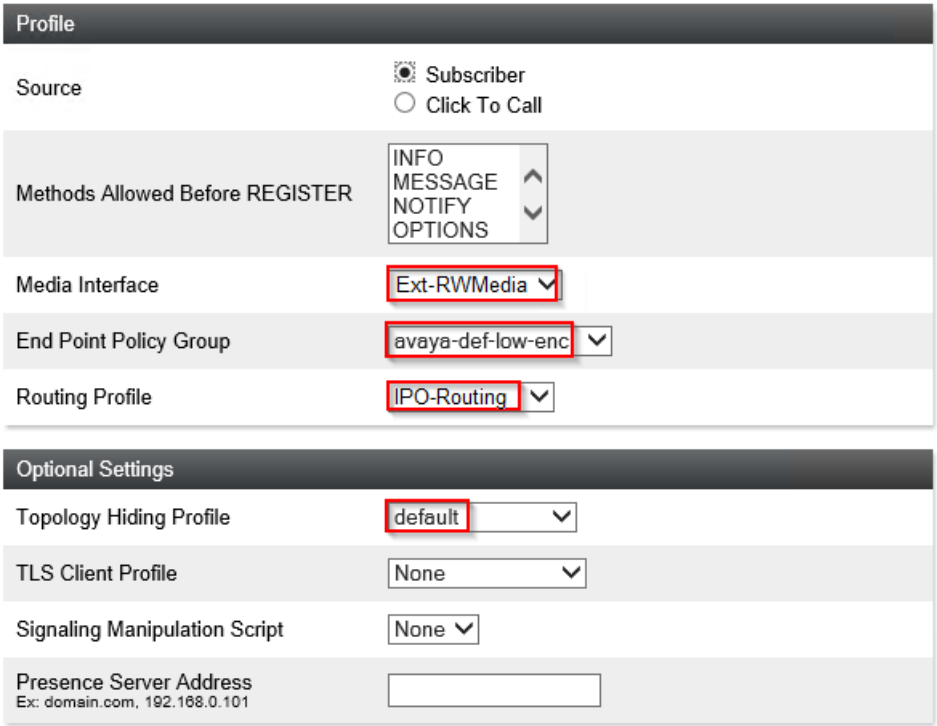


   a. **Flow Name:** Enter a descriptive name for the subscriber flow's usage. This name is used in other menus.

   b. **User Agent:** If created, select the user agent profile 52 intended to restrict connections.

   c. **Signaling Interface:** Select the external signalling interface 47 created for the remote workers.

3. Click **Next**.



   a. **Media Interface:** Select the external media interface 46 previously created for the remote workers.

   b. **End Point Policy Group:** Select ***avaya-def-low-enc***.

   c. **Routing Profile:** Select the server routing 50 profile previously created for the IP Office.

   d. **Topology Hiding Profile:** Select ***default***.

   e. If using TLS, put in the default **TLS Client Profile** called ***AvayaSBCClient***. Client TLS from Create TLS Profiles 44.

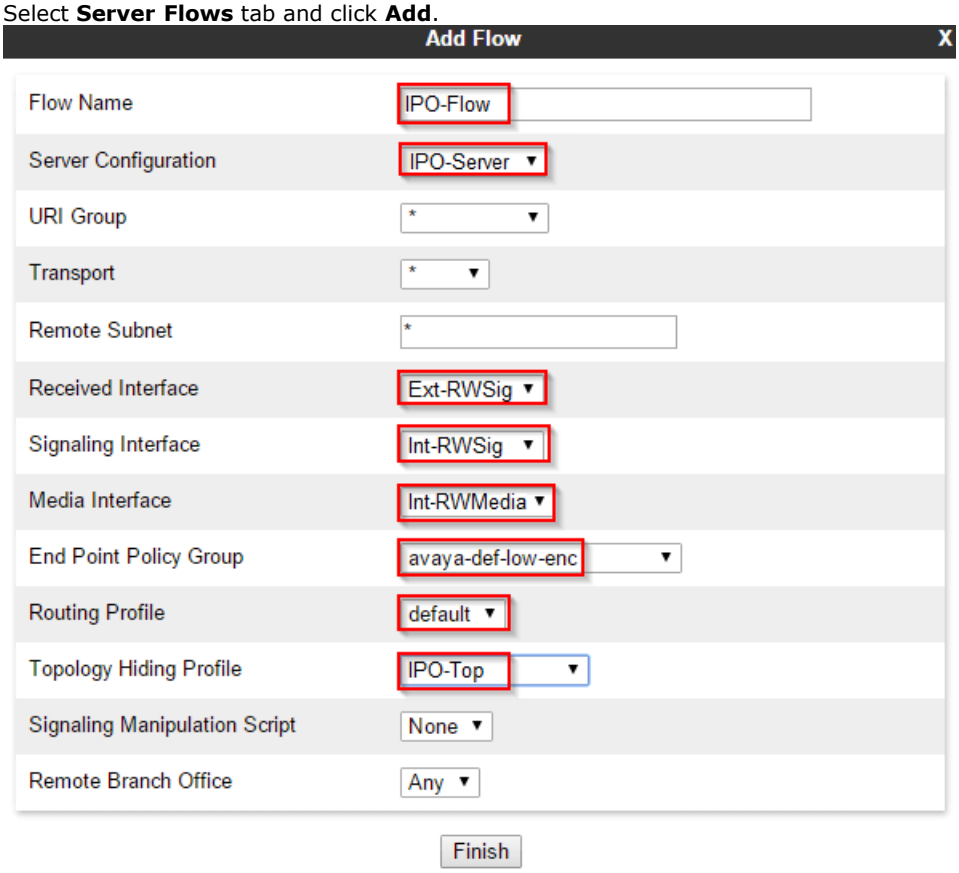
   f. In the **Phone Interworking Profile** field, select ***avaya-ru*** or as recommended the cloned copy. See Phone Interworking Profile 52.

4. Click **Finish**.
5. We now need to create a server flow for remote worker traffic to/from the IP Office. See Create a Server Flow 55
.

5.15 Create a Server Flow

To create a server flow:

1. Go to **Device Specific Settings | End Point Flows**.
2. Select **Server Flows** tab and click **Add**.



   a. **Flow Name:** Enter a descriptive name.
   b. **Server Configuration:** Select the server profile 48 created for the IP Office server.
   c. **Received Interface:** Select the external signaling interface 47 created for the remote workers.
   d. **Signaling Interface:** Select the internal signaling interface 47 created for the remote workers.
   e. **Media Interface:** Select the internal media interface 46 created for the remote workers.
   f. **End Point Policy Group:** Select ***avaya-def-low-enc***.
   g. **Routing Profile:** Select ***default***.
   h. **Topology Hiding Profile:** Select the topology hiding profile 51 created for IP Office remote SIP client.
4. Click **Finish**.
5. You now need to create application relays for the specific ports used by the IP Office applications. See Create Application Relays 56.

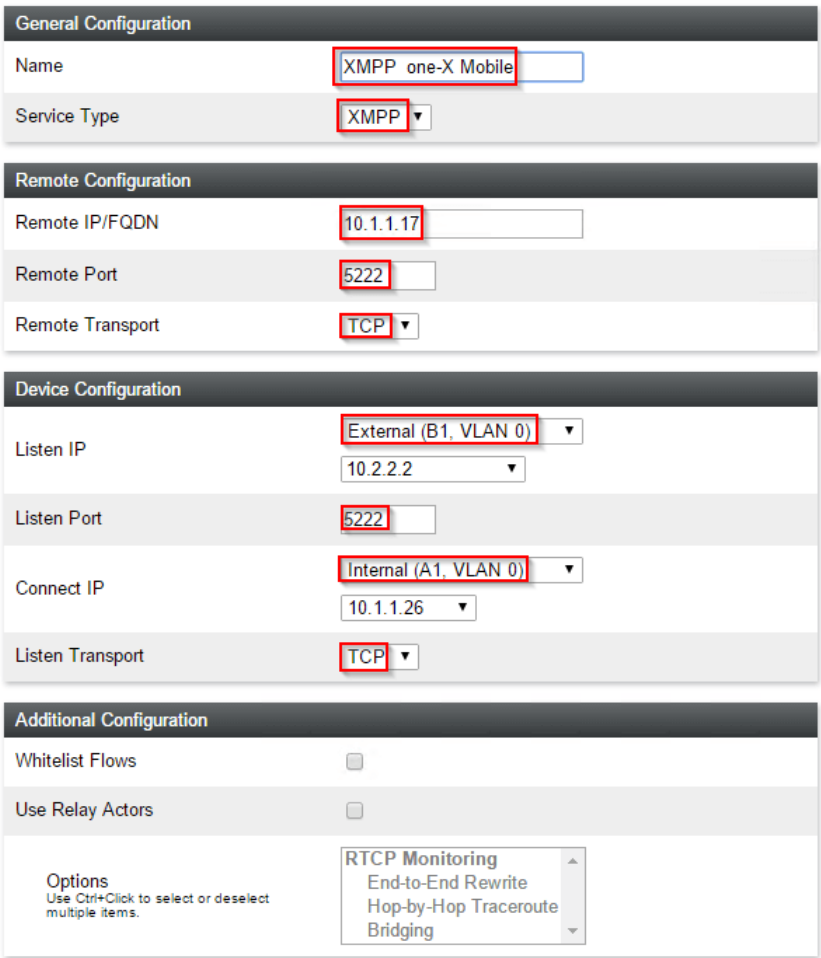
5.16 Create Application Relays

Application relays function as port forwards. Different clients require different application relays. See more detail about necessary ports under the Client Behavior 64 topic. The example below is an application relay for one-X Mobile Preferred.

Application	Ports and Protocols		DNS Queries
Avaya Communicator for Windows	5061	SIP	**A** <ServerID> *(ipo.example.com)*
	9443	XMPP	**A** <HostDomain> *(onex.example.com)*
Avaya Communicator for iPad	5061	SIP	**A** <ServerID> *(ipo.example.com)*
	5222	XMPP	**A** <Hos Domain> *(onex.example.com)*
one-X Mobile Preferred for Android	9443 *	REST	**A** <ServerID> *(onex.example.com)*
	5222	XMPP	**A** <ServerID> *(onex.example.com)*
	5061	SIP	**A** <sipRegistrarFqdn> *(ipo.example.com)*
one-X Mobile Preferred for iOS	9443 *	REST	**A** <ServerID> *(onex.example.com)*
	5222	XMPP	**A** <XMPPDomain> *(onex.example.com)*
	5061	SIP	**A** <sipRegistrarFqdn> *(ipo.example.com)*

To add an application relay for one-X Mobile Preferred applications:

1. Go to **Device Specific Settings | DMZ Services | Relay Services**.
2. Select **Application Relay** tab and click **Add**.



a. **Name:** Enter a descriptive name for the application relay.

b. **Service Type:** Select ***XMPP***.

c. **Remote IP/FQDN:** Enter the IP of the one-X Portal for IP Office (same as IP Office in this example).

d. **Remote Port:** Enter ***5222***.

e. **Remote Transport:** Select ***TCP***.

f. **Listen IP:** Select the external interface.

g. **Listen Port:** Enter ***5222***.

h. **Connect IP:** Select the internal interface.

i. **Listen Transport:** Select ***TCP***.

3. Click **Finish**.

4. Repeat the above procedure for port 9443 (XMPP).

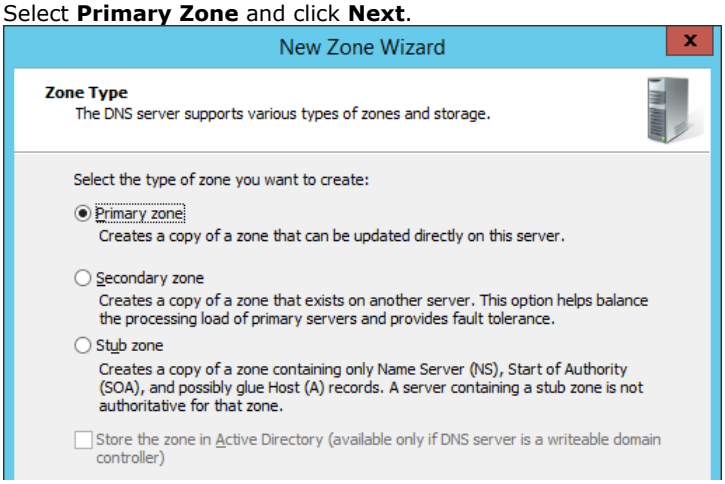
Chapter 6.
DNS Configuration

6. DNS Configuration

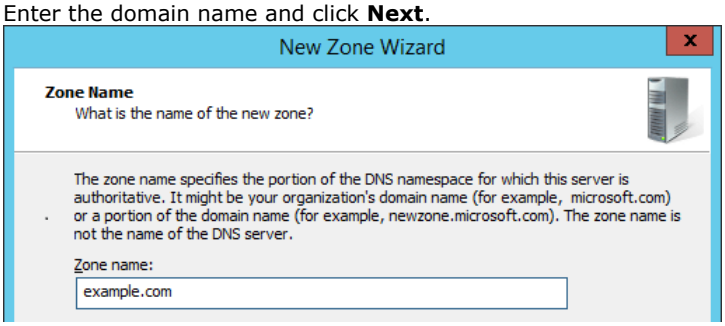
Installation and configuration of DNS servers is out of scope of this document. The follow is an outline example for a Windows 2012 R2 server. It shows the creation of the A record for the IP Office Server Edition server and SVR records for its XMPP and SIP services.

To configure DNS on a Windows 2012 R2 Server:

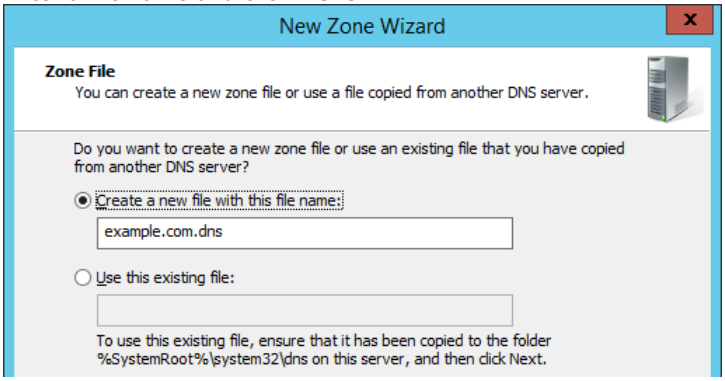
1. Add a new Forward Lookup Zone for the FQDN *ipo.example.com*.
2. Select **Primary Zone** and click **Next**.



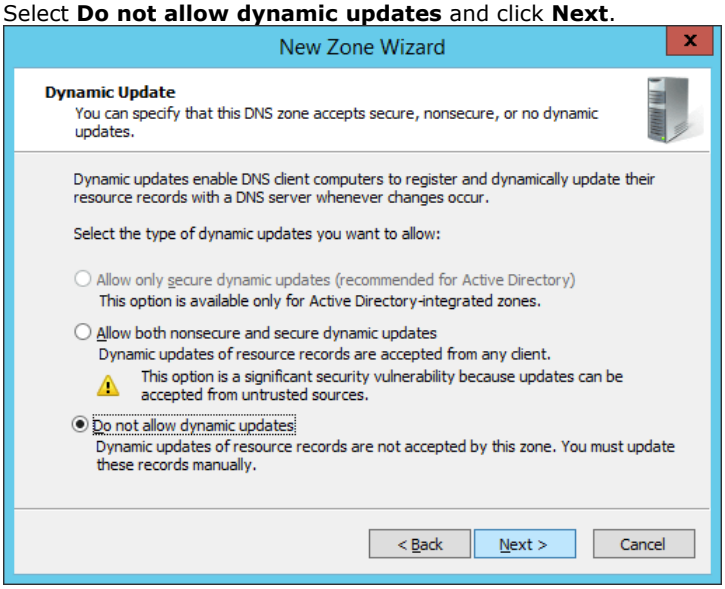
3. Enter the domain name and click **Next**.



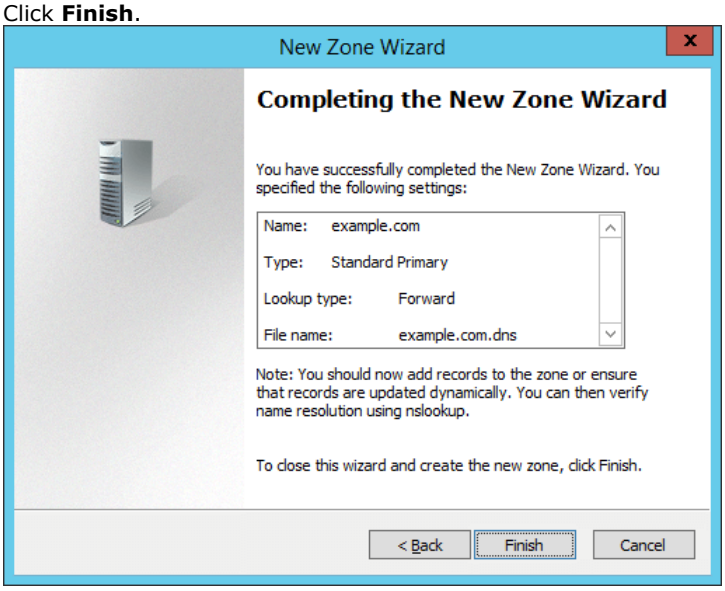
4. Enter a file name and click **Next**.



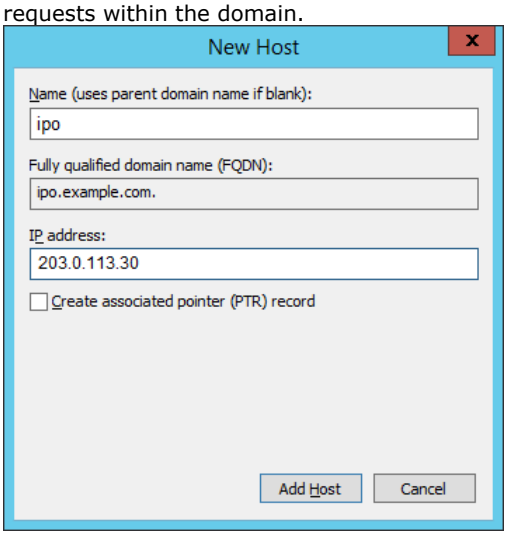
5. Select **Do not allow dynamic updates** and click **Next**.



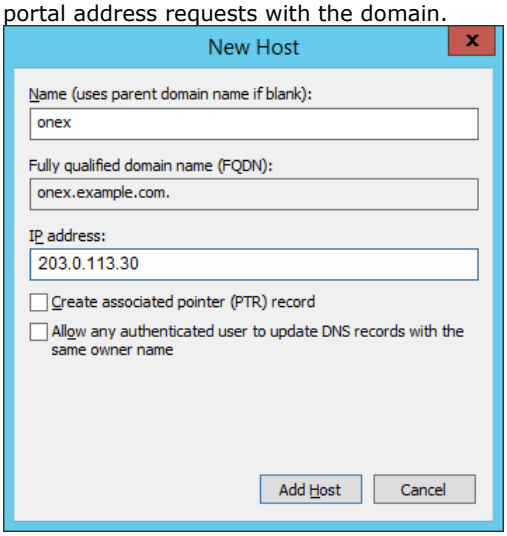
6. Click **Finish**.



7. Add an **A** record for the IP Office service's host name. This will be used as the A record the IP Office address requests within the domain.



8. Add an **A** record for the one-X Portal for IP Office services XMPP domain name. This will be used as the A record portal address requests with the domain.



9. Verify the DNS.

```
C:\Users\Administrator>nslookup -querytype=A onex.example.com 203.0.113.43
Server:  UnKnown
Address:  203.0.113.43

Name:    onex.example.com
Address:  203.0.113.34


C:\Users\Administrator>nslookup -querytype=A ipo.example.com 203.0.113.43
Server:  UnKnown
Address:  203.0.113.43

Name:    ipo.example.com
Address:  203.0.113.34
```

10. Repeat above configuration on the internal DNS server using the private IP of IP Office.

Chapter 7.
Client Behaviour

7. Client Behaviour

This section provides a brief overview of how the different SIP softphone applications use the DNS values to locate and register with the IP Office and one-X Portal for IP Office servers.

7.1 Ports and DNS Queries

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

Application	Ports and Protocols		DNS Queries
Avaya Communicator for Windows	5061	SIP	**A** <ServerID> *(ipo.example.com)*
	9443	XMPP	**A** <HostDomain> *(onex.example.com)*
Avaya Communicator for iPad	5061	SIP	**A** <ServerID> *(ipo.example.com)*
	5222	XMPP	**A** <Hos Domain> *(onex.example.com)*
one-X Mobile Preferred for Android	9443 *	REST	**A** <ServerID> *(onex.example.com)*
	5222	XMPP	**A** <ServerID> *(onex.example.com)*
	5061	SIP	**A** <sipRegistrarFqdn> *(ipo.example.com)*
one-X Mobile Preferred for iOS	9443 *	REST	**A** <ServerID> *(onex.example.com)*
	5222	XMPP	**A** <XMPPDomain> *(onex.example.com)*
	5061	SIP	**A** <sipRegistrarFqdn> *(ipo.example.com)*

* 8443 is used for Windows-based portal server access, 9443 for Linux-based portal server access.

- ***<ServerID>*** = FQDN configured on the client.
- ***<HostDomain>*** = Host domain name on the one-X Portal for IP Office.
- ***<XMPPDomain>*** = XMPP domain name on the one-X Portal for IP Office.
- ***<sipRegistrarFqdn>*** = SIP Registrar FQDN on the IP Office.

7.2 Avaya Communicator for Windows

The Avaya Communicator for Windows first registers to IP Office on the configured SIP port and then connects to the one-X Portal for IP Office using the information it receives during the registration.

- Not every version of Avaya Communicator for Windows is supported by IP Office. Use the one that is listed under IP Office downloads.

Detailed procedure:

1. Configure the client. Select **Settings | Server**:
   a. **Server address:** The FQDN of the IP Office (set as the **SIP Registrar FQDN** in the IP Office configuration).
   b. **Server port:** The layer 4 port.
   c. **Transport Type:** ***TLS***
   d. **Domain:** The SIP domain to use for registration (set as the **SIP Domain Name** in the IP Office configuration).
2. The client sends a DNS A query with the FQDN set on the client to learn the IP address of the IP Office.

1988	157.185025	203.0.113.106	203.0.113.43	DNS	75	Standard query 0x159d A ipo.example.com
1989	157.185324	203.0.113.43	203.0.113.106	DNS	91	Standard query response 0x159d A 203.0.113.30

3. The client sends a SIP REGISTER message to the IP Office with the configured SIP domain on the configured port and transport.

```
203.0.113.104:35107 —TLS→ 203.0.113.30:5061

REGISTER sips:example.com SIP/2.0
From: sips:2001@example.com;tag=-7a60cadb577638077c4f8fbf_F2001203.0.113.104
To: sips:2001@example.com
Call-ID: 1_24d955a7-55873ee77c4f8daf_R@203.0.113.104
CSeq: 2 REGISTER
Via: SIP/2.0/TLS 203.0.113.104:35107;branch=z9hG4bK2_24d955f5-34a8b3d87c4f9004_R2001
Content-Length: 0
Max-Forwards: 70
Contact: <sips:2001@203.0.113.104:35107;transport=tls>;q=1;expires=3600;reg-id=1;+sip.instance="<urn:uuid:129e3bce-a008-50f3-a33c-6e152345c5f9>"
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
Authorization: Digest username="2001",realm="ipoffice",nonce="cf127aa363d2959be64d",uri="sips:example.com",response="b8f2246469942d8391be911b8aadf074"
```

4. In the 200 OK from the IP Office, the body contains the FQDN of one-X Portal for IP Office (HOST Domain Name) and the ports.

```
203.0.113.35:5061 —TLS→203.0.113.104:9494

SIP/2.0 200 OK
From: <sips:2000@sip.example.com>;tag=-46e68ae7566ed61e6a610e3f_F2000203.0.113.35
To: <sips:2000@sip.example.com>;tag=1bcc7bc6a48bef31
CSeq: 4 REGISTER
Call-ID: 1_13f237f4776beda36a610e20_R@203.0.113.35
Contact: <sips:2000@203.0.113.35:9494;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: timer,vnd.avaya.ipo
User-Agent: IP Office 1.0.0.0 build 0
Via: SIP/2.0/TLS 203.0.113.35:9494;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="example"
```

5. The client sends a DNS A query to learn the IP address that matches the portal FQDN it just received.

2049	165.578087	203.0.113.106	203.0.113.43	DNS	76	Standard query 0x57c0 A onex.example.com
2050	165.578396	203.0.113.43	203.0.113.106	DNS	92	Standard query response 0x57c0 A 203.0.113.30

6. The client starts XMPP communication with the one-X Portal for IP Office on port 9443.

7.3 Avaya Communicator for iPad

The Avaya Communicator for iPad first registers to IP Office, then connects to the one-X Portal for IP Office 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 IP Office.

Detailed procedure:

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

1661	104.732537	203.0.113.106	203.0.113.43	DNS	75	Standard query 0xdc85 A ipo.example.com
1662	104.875374	203.0.113.43	203.0.113.106	DNS	91	Standard query response 0xdc85 A 203.0.113.30

3. The client sends a SIP REGISTER message to IP Office with the configured SIP domain on the configured port and transport.

```
203.0.113.104:35107 ——TLS→ 203.0.113.30:5061

REGISTER sips:example.com SIP/2.0
From: <sips:2001@example.com>;tag=4e8a01e9578f3ad8-50e18808_F2001203.0.113.104
To: <sips:2001@example.com>
Call-ID: 1_578f3ad8-5efa2f4f-50e18a4d_R@203.0.113.104
CSeq: 2 REGISTER
Max-Forwards: 70
Via: SIP/2.0/TLS 203.0.113.104:5062;branch=z9hG4bK2_578f3ad9-6d12d40d-50e18a07_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/2.0.5 (Custom; iPad2,7)
Contact: <sips:2001@203.0.113.104:5062;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="4eafd751598a6a22fd5f",uri="sips:example.com",response="21b4f79a36d3ddce6e06da0121c23a8a",username="2001"
Content-Length:     0
```

4. The 200 OK from the IP Office contains the IP address of one-X Server (XMPP domain) and the ports.

```
203.0.113.30:5061 ——TLS→ 203.0.113.104:5062

SIP/2.0 200 OK
From: <sips:2001@example.com>;tag=4e8a01e9578f3ad8-50e18808_F2001203.0.113.104
To: <sips:2001@example.com>;tag=e83d039d25805c11
CSeq: 2 REGISTER
Call-ID: 1_578f3ad8-5efa2f4f-50e18a4d_R@203.0.113.104
Contact: <sips:2001@203.0.113.104:5062;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: timer,vnd.avaya.ipo
User-Agent: IP Office 10.0.0.0.0 build 543
Via: SIP/2.0/TLS 203.0.113.104:5062;branch=z9hG4bK2_578f3ad9-6d12d40d-50e18a07_R2001
Expires: 180
Date: Wed, 20 Jul 2016 08:48:24 GMT
Server: IP Office 10.0.0.0.0 build 543
Content-Type: application/vnd.avaya.ipo
Content-Length: 530

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

5. The client sends a DNS A query to learn the IP address of the XMPP domain.

1693	108.328272	203.0.113.106	203.0.113.43	DNS	76	Standard query 0xbb49 A onex.example.com
1696	108.390944	203.0.113.43	203.0.113.106	DNS	92	Standard query response 0xbb49 A 203.0.113.30

6. The clients starts XMPP communication with the one-X Portal for IP Office on port 5222.

7.4 one-X Mobile Preferred for Android

The one-X Mobile Preferred for Android first contacts the one-X Portal for IP Office through the REST API (port 9443) to learn the sipRegistrarFqdn value. It then does a DNS A query using the sipRegistrarFqdn to learn the IP address of the IP Office, finally registers to one-X Portal for IP Office and IP Office.

On the client we need to configure the FQDN of one-X Portal for IP Office.

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. In **Settings | Advanced | Advanced VoIP** check **Secure Connection**. This option is needed for encrypted signaling and media.
2. The client sends a DNS A query with the FQDN set on the client to learn the IP address of the one-X Portal for IP Office.

94	7.53801700	203.0.113.106	203.0.113.43	DNS	76 Standard query 0x54ed A onex.example.com
95	7.53833900	203.0.113.43	203.0.113.106	DNS	92 Standard query response 0x54ed A 203.0.113.30

3. The client contacts the one-X Portal for IP Office on port 8444 and downloads the XMPP and SIP access details including the XMPP and SIP domains. The same information can be manually checked using a browser:

https://onex.example.com:9443/inkaba/user/my/im-info

```
▼<im-info>
  <imId>example@onex.example.com</imId>
  <imPassword>123456</imPassword>
  <myBuddyId>mybuddy@onex.example.com</myBuddyId>
</im-info>
```

https://onex.example.com:9443/inkaba/user/my/sip-info

```
▼<sip-info>
  <identity>2000@example.com</identity>
  <userName>2000</userName>
  <password>123456</password>
  <displayName>Fullname</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>14</payloadType>
  <signalingQos>136</signalingQos>
  <voiceQos>184</voiceQos>
  <videoQos>184</videoQos>
  <sipRegistrarFqdn>ipo.example.com</sipRegistrarFqdn>
</sip-info>
```

4. The client sends a DNS A query for the IP address of the ***sipRegistrarFQDN*** received above (the IP Office).

139	8.74501600	203.0.113.106	203.0.113.43	DNS	75 Standard query 0x43bc A ipo.example.com
140	8.74513900	203.0.113.43	203.0.113.106	DNS	91 Standard query response 0x43bc A 203.0.113.30

5. The client registers to the IP Office and the one-X Portal for IP Office.

7.5 one-X Mobile Preferred for iOS

The one-X Mobile Preferred for iOS first contacts the one-X Portal for IP Office through the REST API (port 9443) to learn the ***XMPP Domain*** and the ***sipRegistrarFqdn*** values. Using these values it does a DNS A query on the XMPP Domain value to learn the IP address of the one-X Portal for IP Office and then a DNS A query on the sipRegistrarFqdn value to learn the IP address of the IP Office. It then registers with the one-X Portal for IP Office and IP Office.

On the client we need to configure the FQDN of one-X Portal for IP Office.

Detailed procedure:

1. Configure the client.
   a. In **Settings | UC Server Settings** set:
      - **FQDN of one-X Portal**: The FQDN set for the XMPP Domain of the one-X Portal for IP Office.
      - **User Name**: The user's **Name** as set in the IP Office configuration.
      - **Password**: The user's **Password** as set in the IP Office configuration.
   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. The client sends a DNS A query with the FQDN set above to learn the IP address of the one-X Portal for IP Office.

893	72.7254140	203.0.113.106	203.0.113.43	DNS	76 Standard query 0x6607 A onex.example.com
894	72.7257450	203.0.113.43	203.0.113.106	DNS	92 Standard query response 0x6607 A 203.0.113.30

3. The client contacts the one-X Portal for IP Office on port 9443 and downloads the XMPP and SIP access details including the XMPP and SIP domains. The same information can be manually checked using a browser:

https://onex.example.com:9443/inkaba/user/my/im-info

```
▼<im-info>
   <imId>example@onex.example.com</imId>
   <imPassword>123456</imPassword>
   <myBuddyId>mybuddy@onex.example.com</myBuddyId>
 </im-info>
```

https://onex.example.com:9443/inkaba/user/my/sip-info

```
▼<sip-info>
   <identity>2001@example.com</identity>
   <userName>2001</userName>
   <password>123456</password>
   <displayName>example</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>14</payloadType>
   <signalingQos>136</signalingQos>
   <voiceQos>184</voiceQos>
   <videoQos>184</videoQos>
   <sipRegistrarFqdn>ipo.example.com</sipRegistrarFqdn>
 </sip-info>
```

4. The client sends a DNS A query for the XMPP domain to learn the IP address and port of the one-X Portal for IP Office.

891	69.5383420	203.0.113.106	203.0.113.43	DNS	76 Standard query 0x2fc8 A onex.example.com
892	69.5386060	203.0.113.43	203.0.113.106	DNS	92 Standard query response 0x2fc8 A 203.0.113.30

5. The client sends a DNS A query for the IP address of the ***sipRegistrarFQDN*** received above (the IP Office).

942	76.0407370	203.0.113.106	203.0.113.43	DNS	75 Standard query 0x9100 A ipo.example.com
943	76.0409910	203.0.113.43	203.0.113.106	DNS	91 Standard query response 0x9100 A 203.0.113.30

6. The client registers to the IP Office and one-X Portal for IP Office (port 5222).

Chapter 8.
Remote SIP Deskphones

8. Remote SIP Deskphones

This section covers an example for deploying Avaya SIP desk phones (1120, 1140, 1220, 1230, E129 and H175) as the remote IP Office worker extension. The setup is similar to that used for Avaya SIP softphone clients.

8.1 Provisioning the Deskphones

For maintenance purposes it is desirable to have the desk phones able to connect to the IP Office using HTTP/HTTPS traffic relayed by the ASBCE. However, for initial installation the SIP phones should first be provisioned locally on the IP Office network. The phones can then be moved to their remote location on the ASBCE public side.

No User Source Numbers for Remote SIP Desk Phones

To support remote SIP desk phones with an ASBCE, you need to add the following **User Source Numbers** to the configuration of the NoUser user.

- **RW_SBC_REG=**<ASBCE B1 public IP address>
  If **RW_SBC_REG** and **RW_SBC_PROV** below are not entered, the other source number are also ignored.
- **RW_SBC_PROV=**<ASBCE B1 private IP address>
  The IP Office checks whether SIP phone file requests are coming from the configured **RW_SBC_PROV** IP address. If so:
  - It removes an config, provisioning and phonebook path path information from the auto-generated settings sent to the phone. Instead the values must be manually configured on the phone.
  - It also sends the **RW_SBC_REG** value to the phone (as the SIP Server for E129 sets, S1/S2 value for 1100/1200 Series phones, SIP CONTROLLER LIST for H175 phones).
- **Port User Source Numbers**
  One of three ASBCE ports (**RW_SBC_TLS**, **RW_SBC_TCP** or **RW_SBC_UDP**) values must be entered. The recommended configuration is to use homogeneous protocols. For example, if TLS is used between Remote Workers and the ASBCE, then TLS should be used between the ASBCE and IP Office.
  - **RW_SBC_TLS=**<ASBCE public TLS port>
  - **RW_SBC_TCP=**<ASBCE public TCP port>
  - **RW_SBC_UDP=**<ASBCE public-UDP port>

- **For 1100/1200 Series Phones:**
  All port values are sent to the set and the set chooses the protocol to register to SBC in the order TLS, TCP, UDP.
- **For E129 Phones:**
  The IP Office sends the ASBCE TLS port if configured, otherwise the ASBCE TLS if configured, else the ASBCE UDP port.
- **For H175 Phones:**
  The IP Office chooses the SBC TLS/TCP port if TLS/TCP is configured in LAN1/LAN2, with TLS given the precedence over TCP.

8.2 Configuring Application Rules

Clone an existing application rule as a starting point or create a new one. Do not change the default.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Domain Policies** and then **Application Rules**.
3. Click **Add** and enter a name for the one to be used by the IP Office End Point Policy Group.
4. Click **Next**.
5. Check **In and Out for Voice** and put in the amount of concurrent sessions required for the license. Put the same value for **Max Concurrent Sessions** and **Max Sessions Per Endpoint**.
   - It is best practice to put more than the licenses available as this is not counted one-to-one with license session. For example, if they have licenses for 300 concurrent sessions, put 500 for each box.
   - If you need video, you must do the same for video. If you clone the default, Audio is already enabled you only need to adjust the values and then enable video.
6. Click **Finish**.
7. Repeat to create a rule used by the Subscriber Flow End Point Policy Group. For the subscriber flow rule, put the **Max Concurrent Sessions** higher than the license. However, for **Max Sessions Per Endpoint**, the recommended value is 10. You can use a higher value if required.

8.3 Configuring Media Rules

Clone an existing media rule as a starting point or create a new one. Do not change the default.

Media rules are defined under **System Management | Domain Policies | Media Rules**. The requirements for media rules are as follows.

- It is recommended to clone a profile like the ***default-low-med*** profile. The default Media Rule has the **Media QoS** setting of ***DSCP EF*** enabled.
- On the **Media Encryption** tab, set the SBC to RTP or SRTP to an endpoint or IP Office. For **Media Encryption**, set the **Preferred Audio Format** as ***RTP*** in the rule for IP Office. Towards the endpoints, the rule used can be set to ***SRTP*** if the endpoint supports it, otherwise use ***RTP***. Ensure **Encrypted RTCP** is unchecked and **Interworking** is checked. For **Video** ensure ***RTP*** is selected.
- For all other tabs, use the default settings.

8.4 Configuring Signalling Rules

Clone an existing media rule as a starting point or create a new one. Do not change the default Media rules are defined under **System Management | Domain Policies | Signalling Rules**. The requirements for signalling rules are as follows.

- It is recommended to clone a profile like the ***default-low-med*** profile. The default Media Rule has the **Signalling QoS** setting of ***DSCP AF41*** enabled.
- When you create a new signalling rule, the default is ***TOS***. This must be changed to ***DSCP AF41*** or another option that meets the current requirements.
- For all other tabs, use the default settings.

8.5 Configuring endpoint policy groups

Create a new endpoint policy group. Do not change the default group.

Procedure

1. In the navigation tree on the left, expand **System Management**.
2. Select **Domain Policies** and then **End Point Policy Groups**.
3. Click **Add** and enter a name for the IP Office server flow.
4. Click **Next**.
5. Choose the appropriate **Rules** and click **Finish**.
6. Click **Add** and enter a name for the subscriber flow.
7. Click **Next**.
8. Choose the appropriate **Rules** and click **Finish**.

Index

T

U

W

X