IP Office™ Platform R11.0

IP Office SIP Phones with ASBCE

Issue 03h - (Thursday, April 16, 2020)

Contents

Chapter 1.
Overview

1. Overview

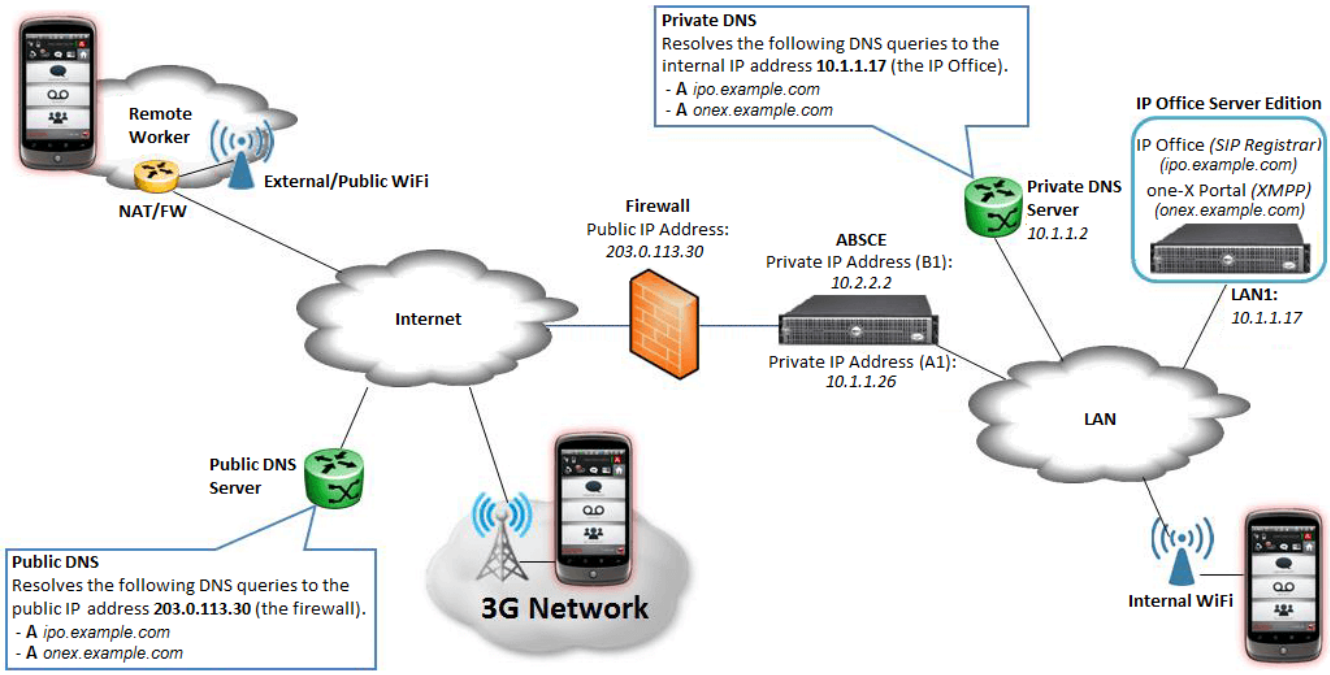
This document is for IP Office Release R11.0 and ASBCE Release 7.2. It looks at examples* of supporting Avaya SIP clients and remote SIP desk phones when also using an Avaya Session Border Controller for Enterprise (ASBCE) server.

Supported SIP Clients	Supported Remote SIP Deskphones	Other
• Avaya Communicator for Windows • Avaya Communicator for iPad • Avaya one-X Mobile Preferred for Android • Avaya one-X Mobile Preferred for iOS • Equinox clients	• 1120, 1140, 1220, 1230. • E129 • H175 • J129, J139, J169, J179 • K155, K165, K175	• WebRTC

- *These are just 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:

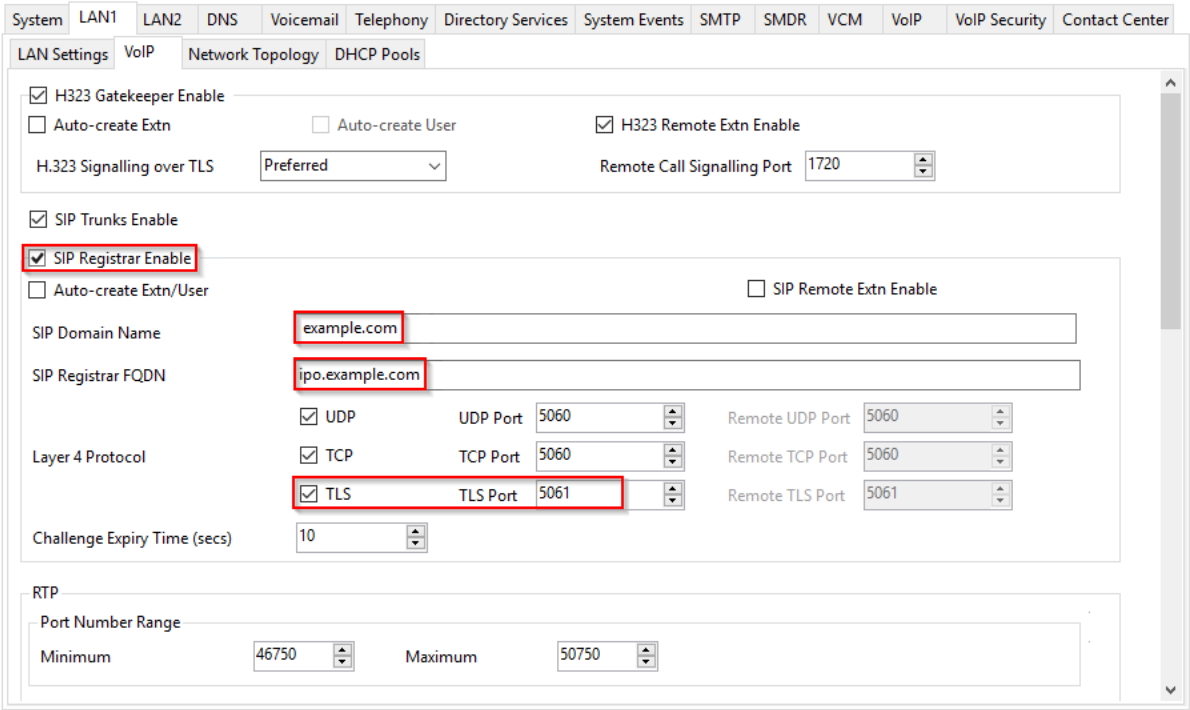
2.1 Licenses

The IP Office does not require any additional licenses to support operation with an ASBCE. The application connected to the IP Office via the ASBCE require the same licenses as for local non-SBC operation.

Note that the IP Office is not supported as the WebLM license server for the ASBCE.

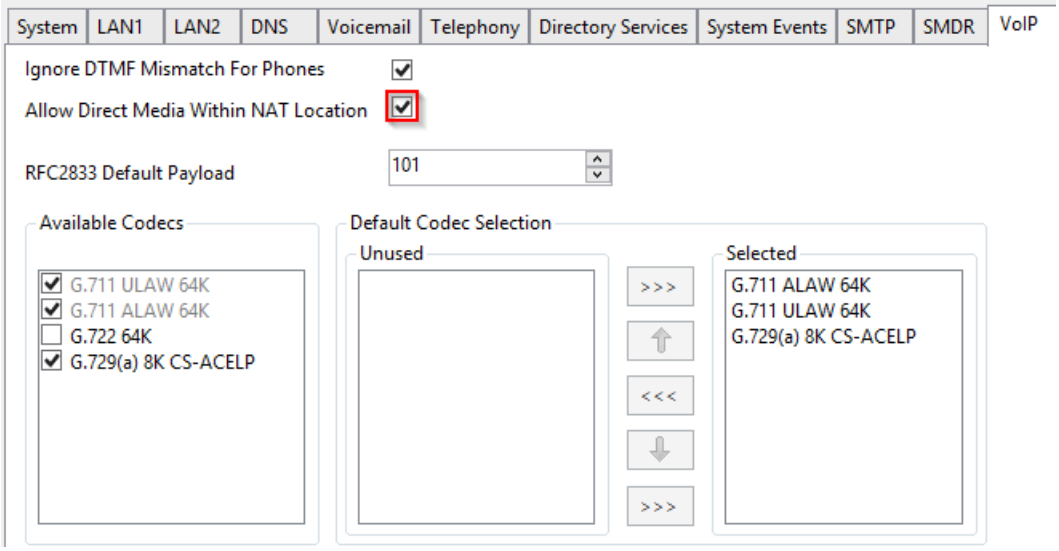
2.2 SIP VoIP Setup

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.



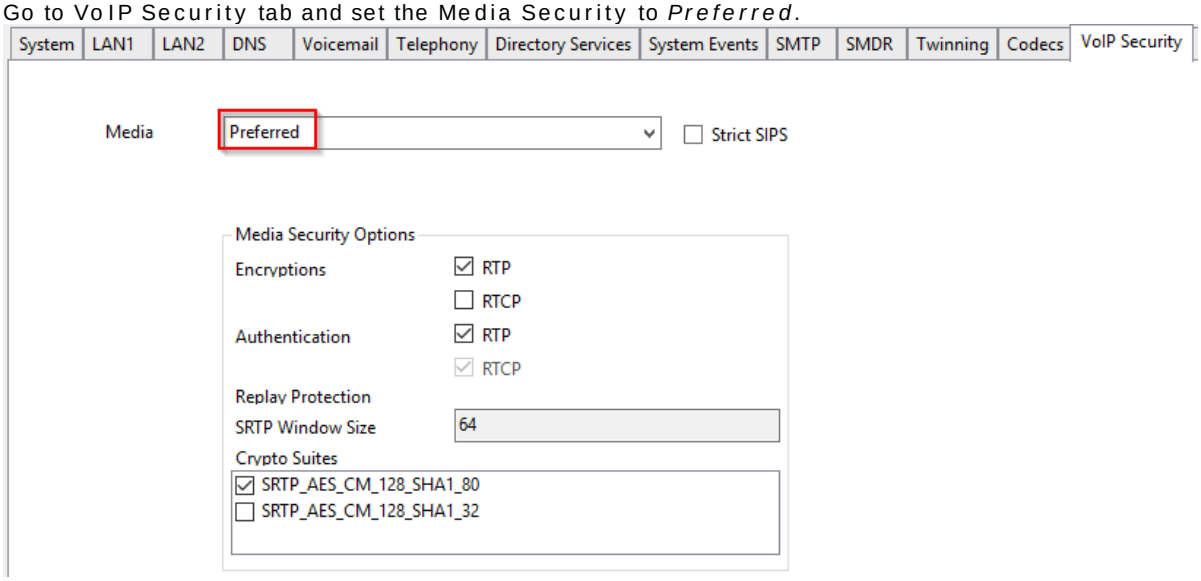
   a. SIP Registrar Enable: Selecting this option allows SIP devices to register with the IP Office.
   b. SIP Remote Extn Enable: Deselect this option. The ASBCE handles the remote extension connections, so the IP Office does not need to handle their NAT requirements.
   c. SIP Domain Name: Set this to 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 | Security.
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:

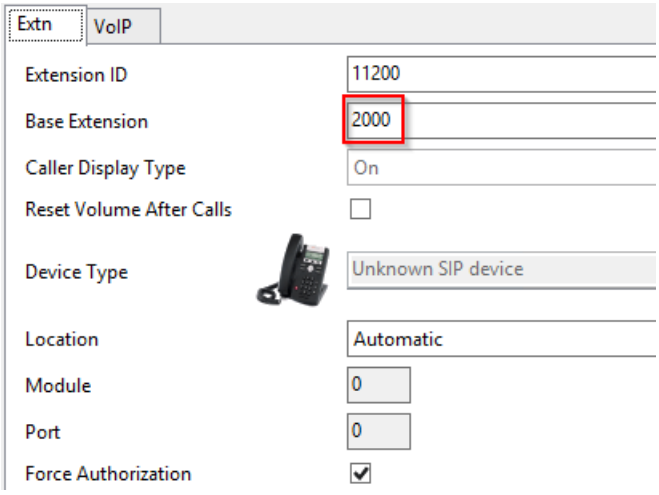
1. Using IP Office Manager, load the IP Office configuration. Select the primary server configuration.
2. Select User.
3. Click on the icon and select User.
4. Select the User tab and set the following:
   a. Name: This is the short name for the user. It is the user's user name for client login. It only displayed in applications if the Full Name (below) is not set.
   b. Password: This field is used to 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 10 .
   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. Refer to the appropriate IP Office installation manual for the application.
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 10 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:

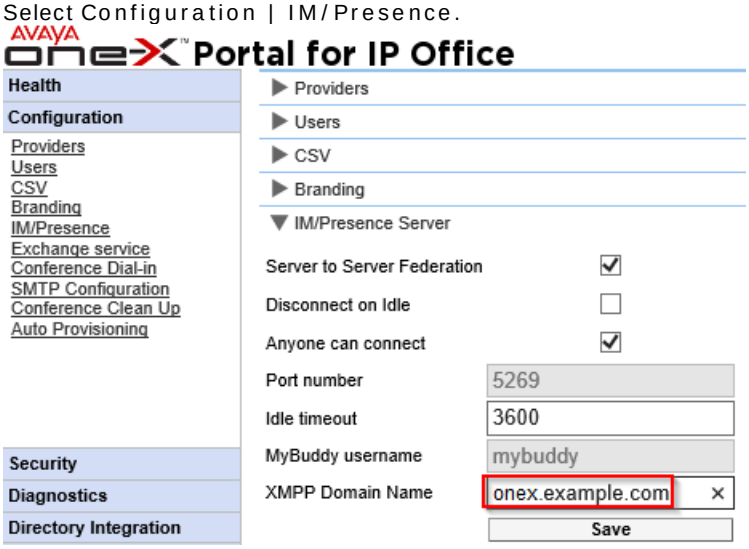
1. Using IP Office Manager, load the IP Office configuration.
2. Select Group.
3. Click the icon and select Hunt Group.
4. Select the Group tab and set the following:
   a. Name: Enter a name for the group.
   b. Profile: Select *XMPP Group*.
   c. Under the User List click Edit. Select and append all 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:

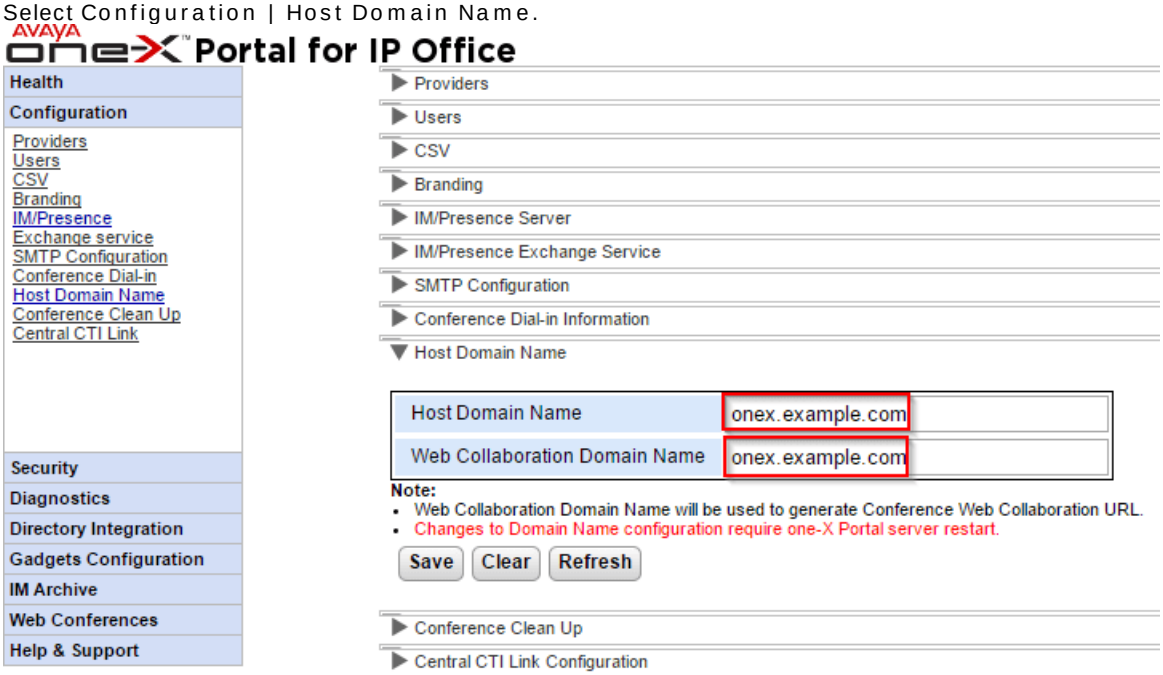
1. Login to the one-X Portal for IP Office administrator menus, either:
   - Within IP Office Web Manager, select Applications | one-X Portal.
   - or browse to *https://<portal IP address>:9443/onexportal-admin.html* and login as the Administrator.
2. Select Configuration | IM/Presence.



   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. Certification

3. Certification

The example in this document assumes that the IP Office system's own self-signed certificate is being used. In that case, the ASBCE needs to have a copy of both the IP Office certificate and also an identity certificate issued for it by the IP Office. If the one-X Portal for IP Office is running on a separate IP Office Application Server, that too requires an identity certificate issued by the IP Office.

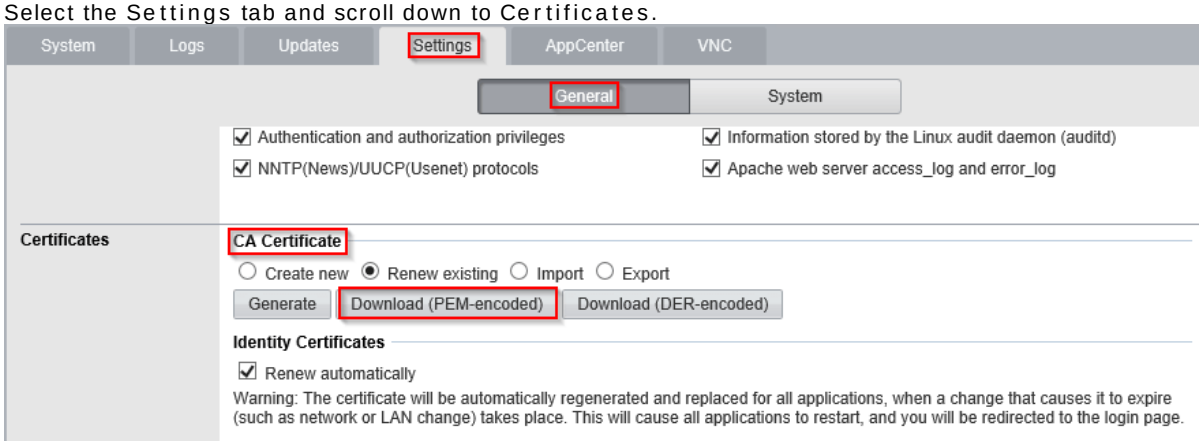
Summary:

3.1 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 primary 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.



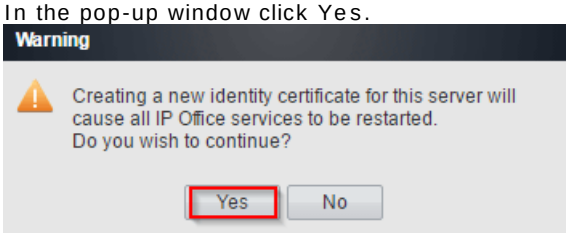
3. Under CA Certificate, click on Download (PEM-encoded) and save the file to your PC.
4. Rename the file as *IPO_RootCA.crt*.

3.2 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 primary 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 FQDNs andIP Office LAN IP addresses LAN1 and/or LAN2) on which extensions are connecting.
5. Click Regenerate and Apply.
6. In the pop-up window click Yes.



3.3 one-X Portal for IP Office Identity Certificate

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

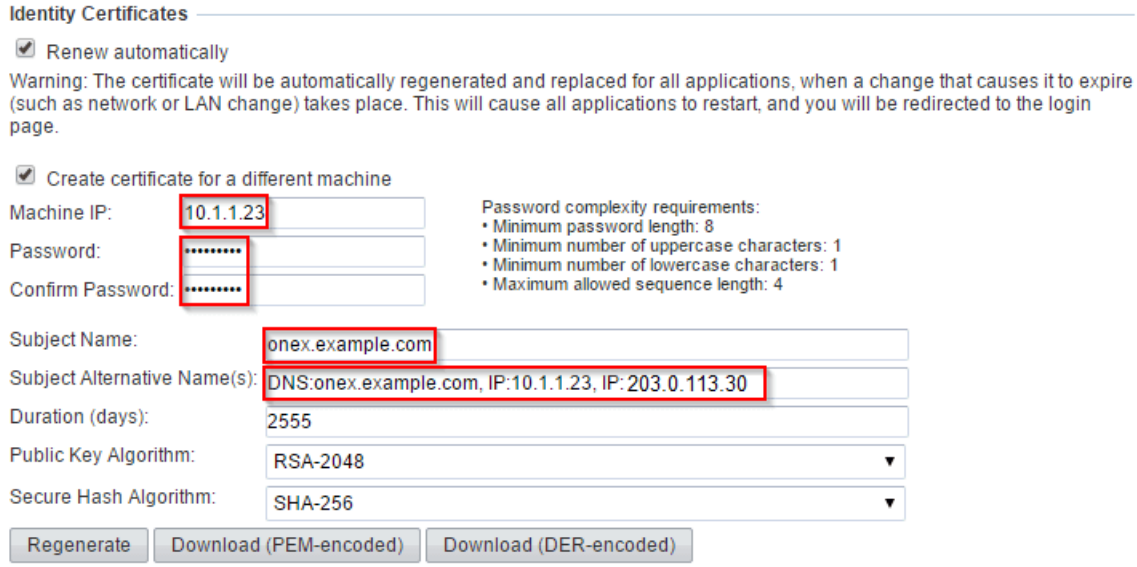
1. Generate an Identity Certificate for the one-X Portal for IP Office 17
2. Install the Identity Certificate on the IP Office Application Server 18

3.3.1 Generating an Identity Certificate for the Portal Server

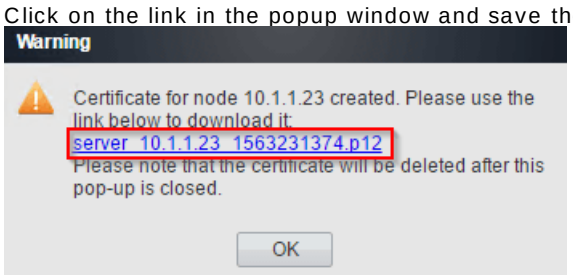
This stage is only required if the one-X Portal for IP Office is run on a separate IP Office Application Server. If that is the case, the portal requires its own identity certificate.

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



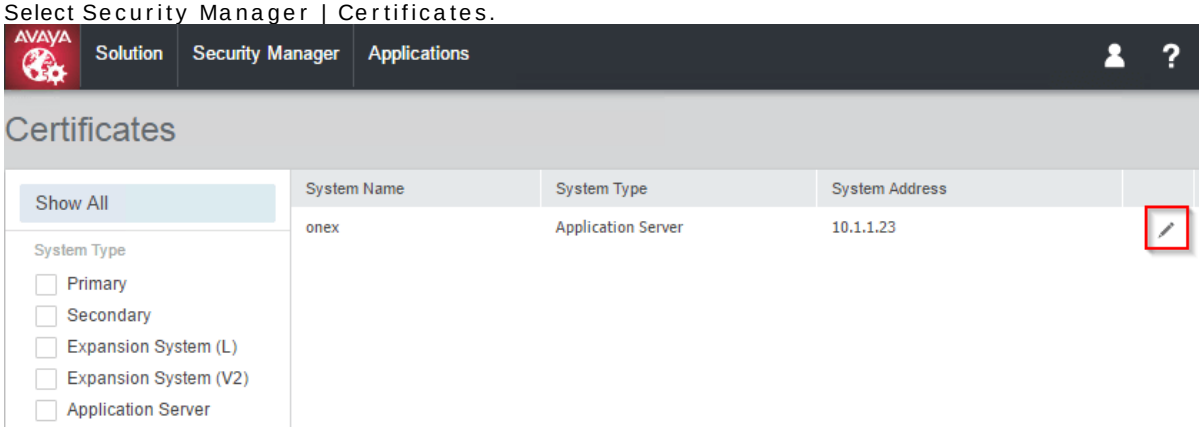
7. You can now add the identity certificate to the one-X Portal for IP Office server 18 .

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

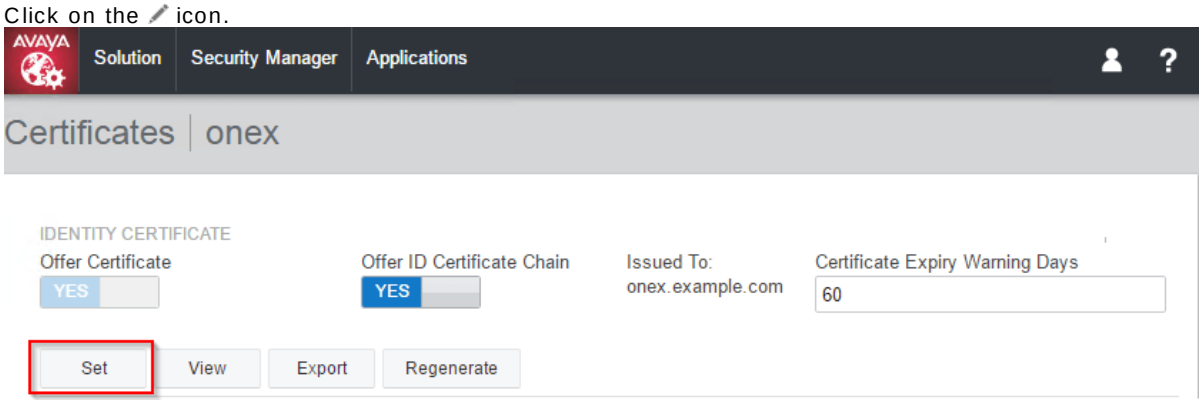
Having created an identity certificate for the IP Office Application Server[17], it needs to be installed on the server.

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

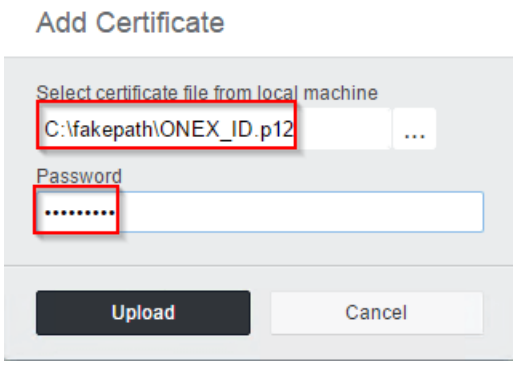
1. Browse to *https://<IP Office IP address>:7070* and login as the Administrator.
2. Select Security Manager | Certificates.



3. Click on the icon.



4. Click on Set.



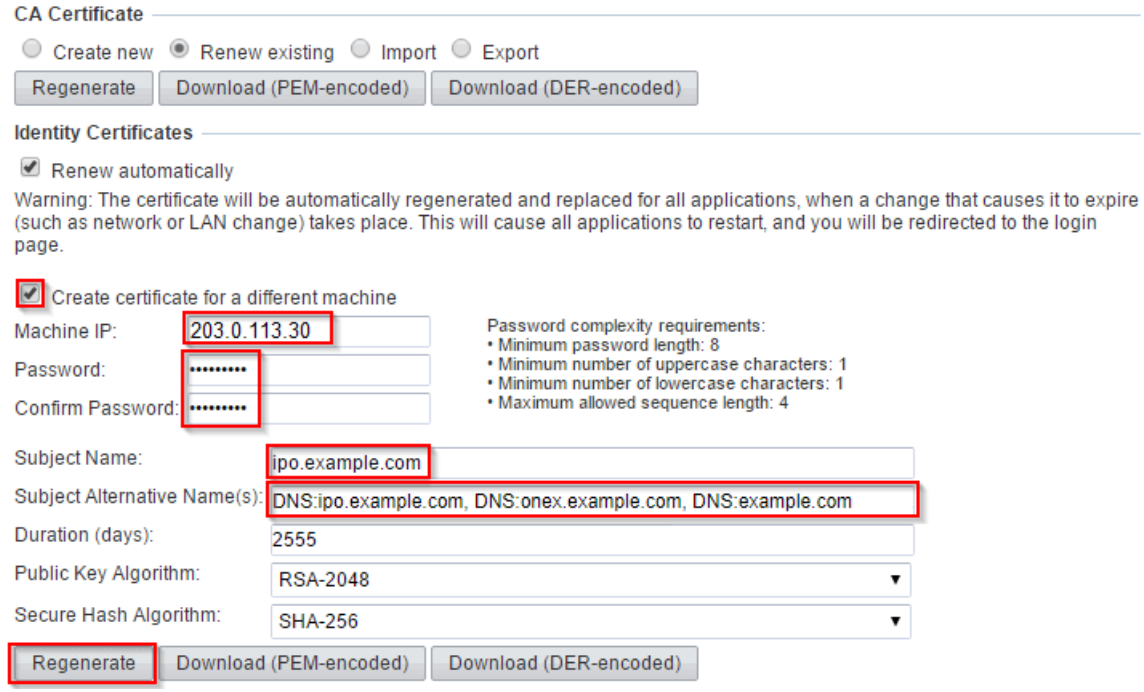
5. Browse to the location of the identity file created for the portal server.
6. Enter the certificate password.
7. Click Upload.

3.4 Generating an Identity Certificate for the ASBCE

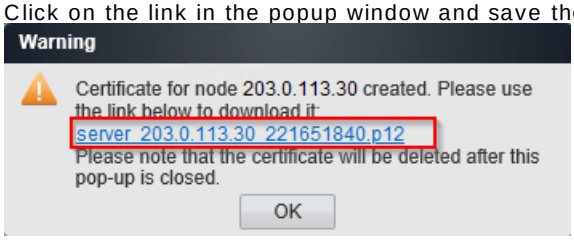
In addition to the IP Office root certificate, we also need to provide the ASBCE with an identity certificate. This certificate needs to include FQDN and IP address information for all the IP Office servers and services for which the ASBCE will be handling traffic.

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 primary 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 the 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*.

3.5 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 19 (*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 19 .

   - 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 19 , 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.

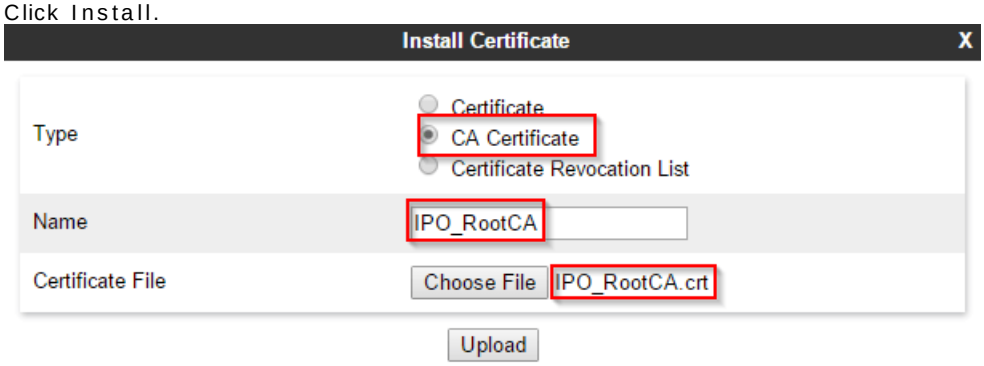
   b. Remove all lines except those which are between the first BEGIN CERTIFICATE and END CERTIFICATE lines. The resulting file should look similar to the following:


```
-----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-----
```

3.6 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.

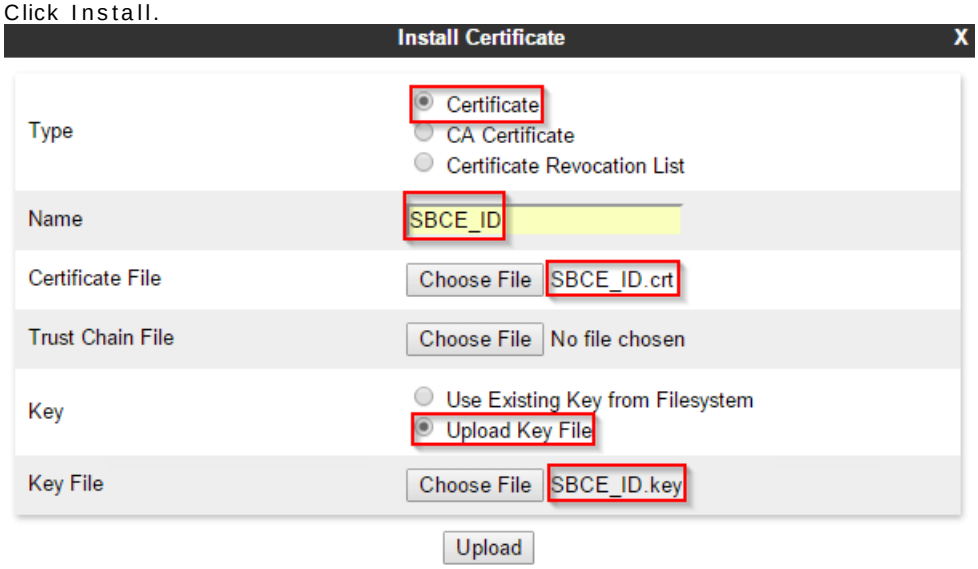


   a. Type: Select *CA Certificate*.
   b. Name: Enter a descriptive name for the root CA certificate.
   c. Allow Weak Certificate/Key: Enable this option.
   d. Certificate File: Click Choose File and select the *IPO_RootCA.crt* file.
4. Click Upload.
5. A warning that this is a self-signed certificate will be displayed. Click Proceed.
6. The certificate is displayed. Click Install and then Finish.

3.7 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:

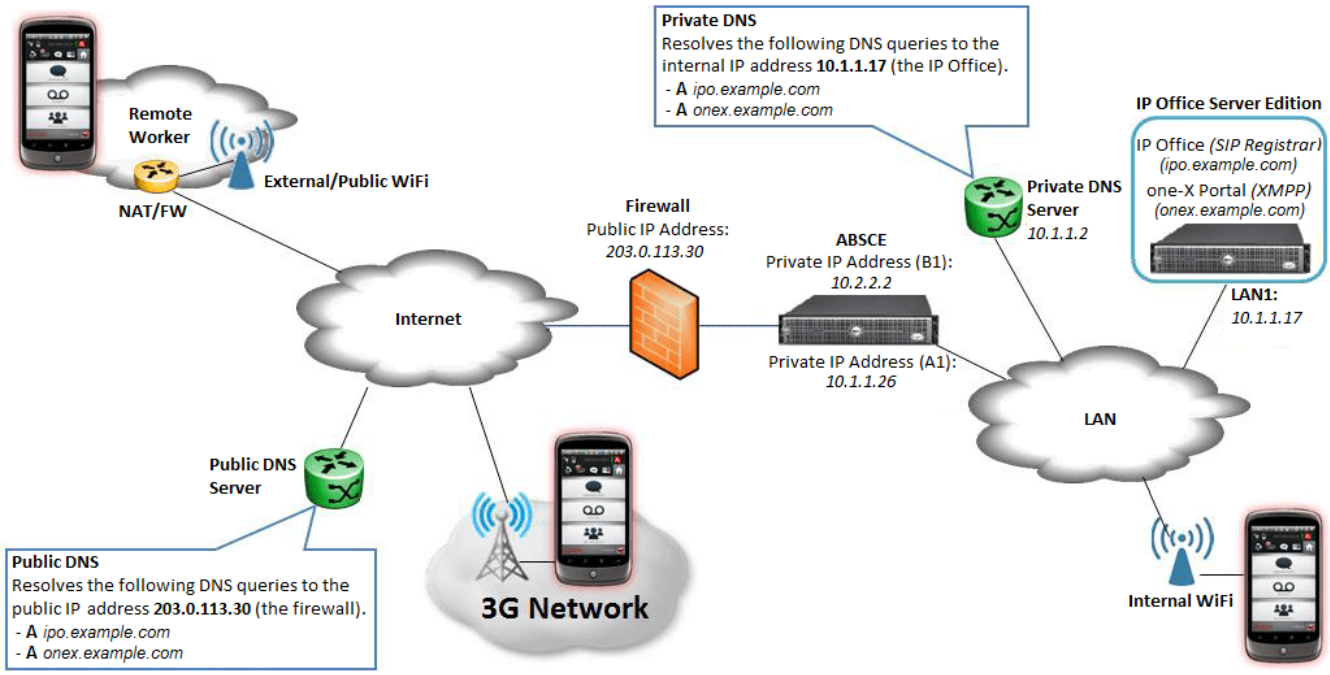
```
cd /usr/local/ipcs/cert/key
enc_key SBCE_ID.key ********
```

   - 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 4.
ASBCE Configuration

4. ASBCE Configuration

This section looks at the specific ASBCE configuration required for the example schematic 4 .



Summary:

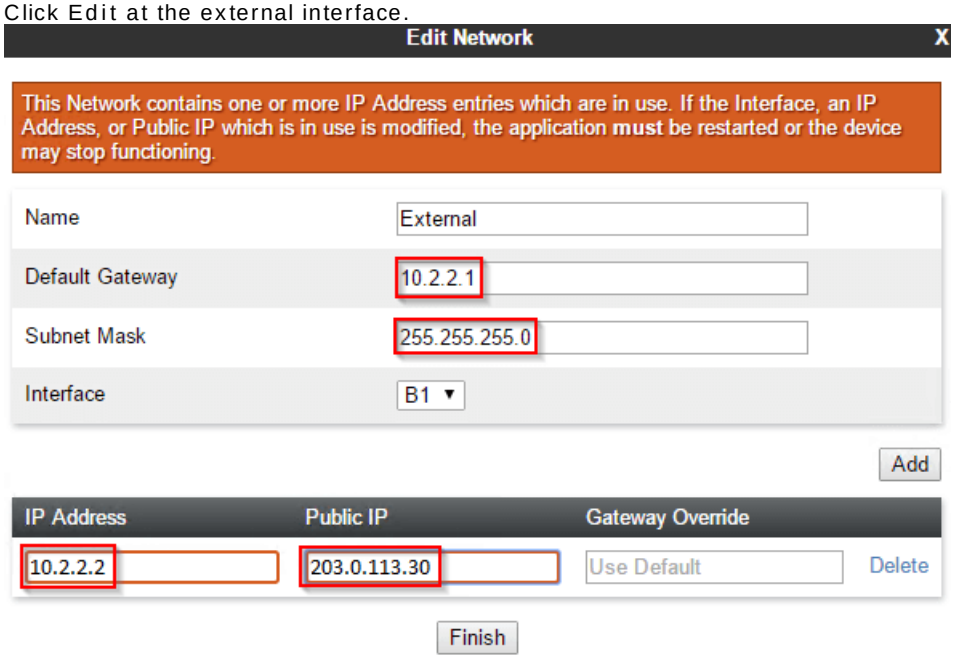
4.1 Firewall Configuration

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 30 .

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

4.2 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.



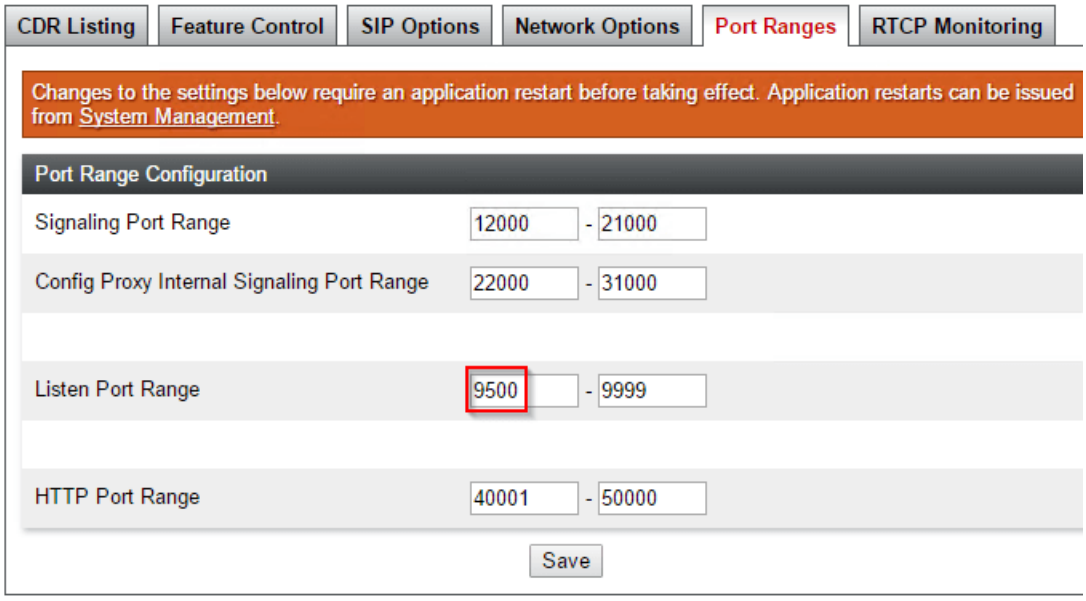
4. Enter the following data then click Finish. This applies NAT between the IP address and Public IP address settings.
   a. Default Gateway: Gateway IP address for the external interface.
   b. Subnet Mask: IP mask for the external interface.
   c. IP Address: IP address of the external interface.
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

4.3 Changing the Default Listen Port Range

This step is necessary so that later we are able to configure listen port 9443 in Application Relay 37 .

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*.



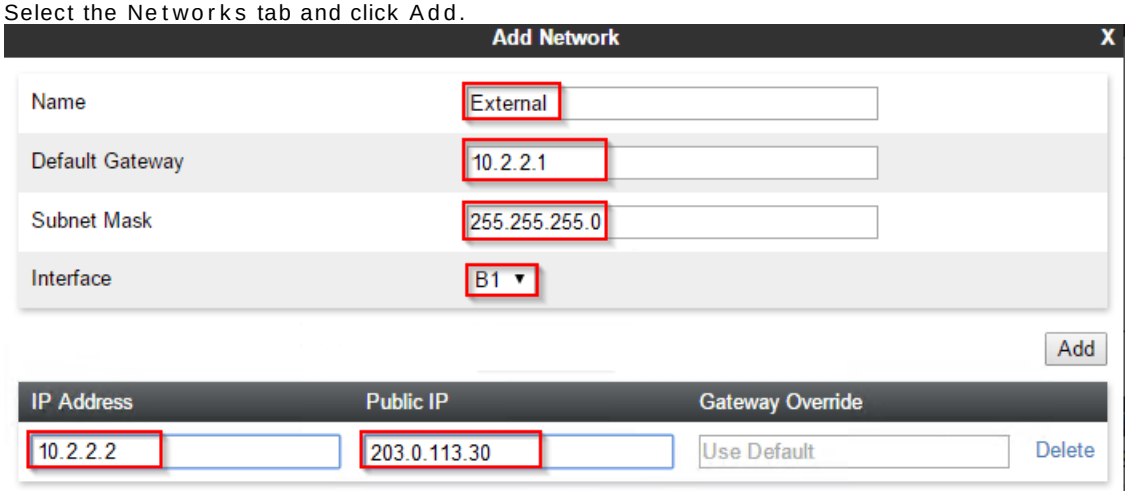
4. Click Save.
5. Go to System Management and on the Devices tab click Restart Application.
6. You now need to enable the internal and external ASBCE interfaces. See Enable the Internal/External Interfaces 27 .

4.4 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.



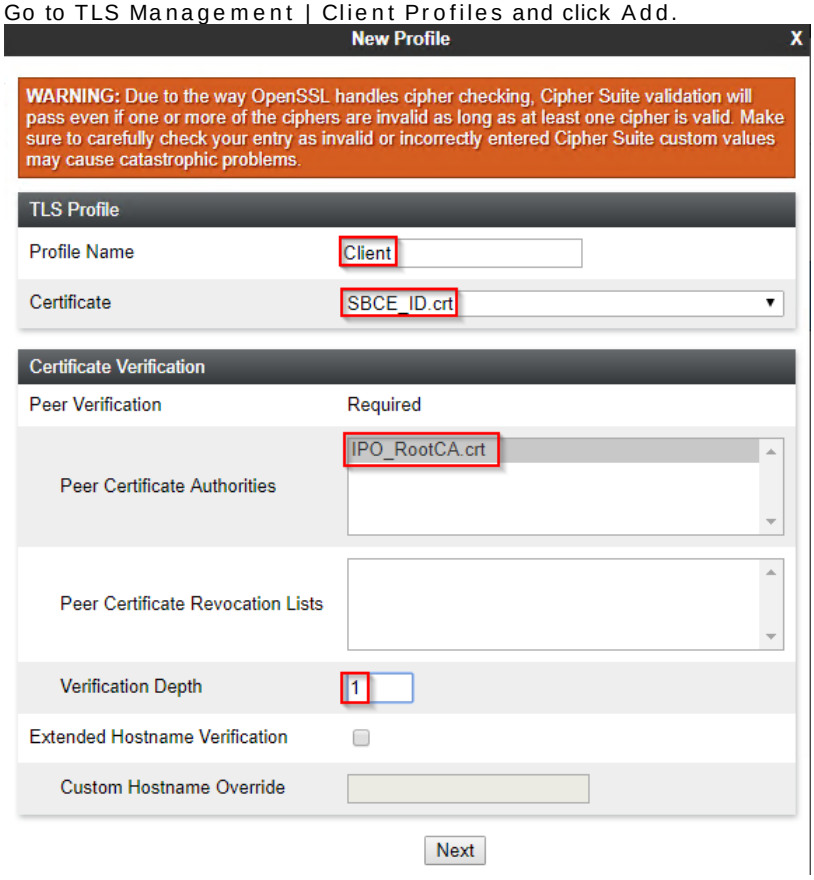
4. Enter the following data:
   a. Name: Enter a name for the external interface.
   b. Default Gateway: Enter the IP address of the default gateway for the external interface.
   c. Subnet Mask: Set the IP address mask.
   d. Interface: Select B1.
   e. IP Address: Set the IP address of the external 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 28 .

4.5 Create a TLS Profile

You 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 to help select this profile later in other menus.

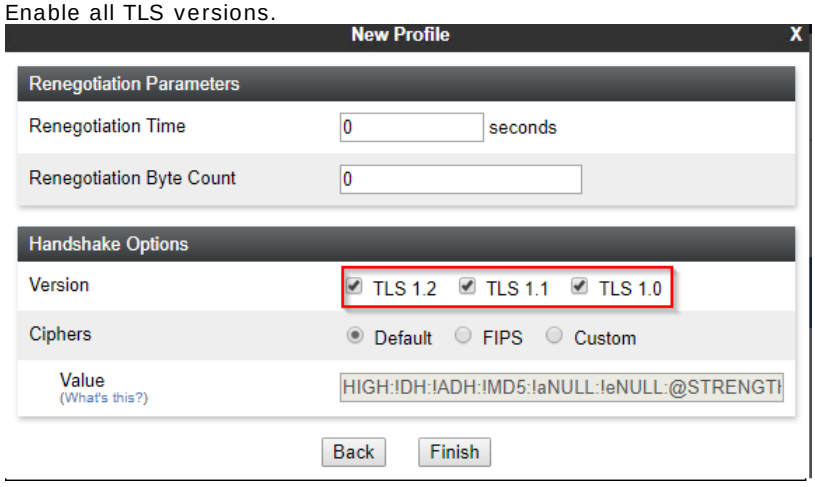
   b. Certificate: Select the *SBCE_ID.crt* file.

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

   d. Verification Depth: Enter *1*.

   e. Click Next.

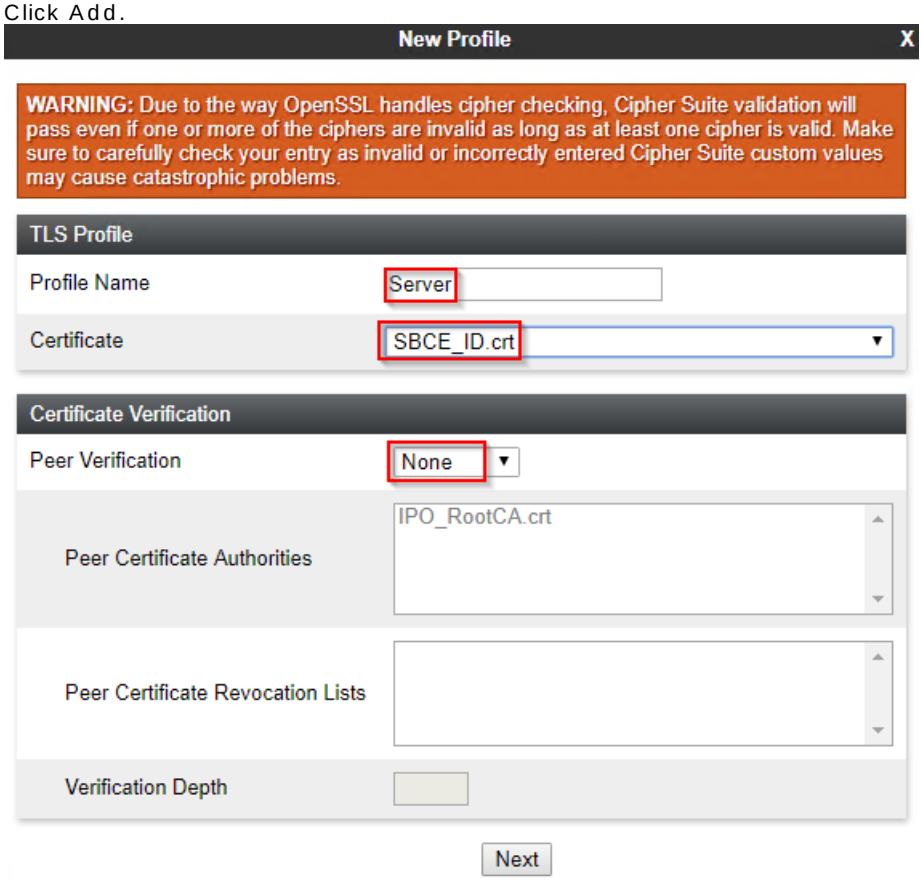
   f. Enable all TLS versions.



   g. Click Finish.

3. Go to TLS Management | Server Profiles and repeat the process to add a server TLS policy.

4. Click Add.



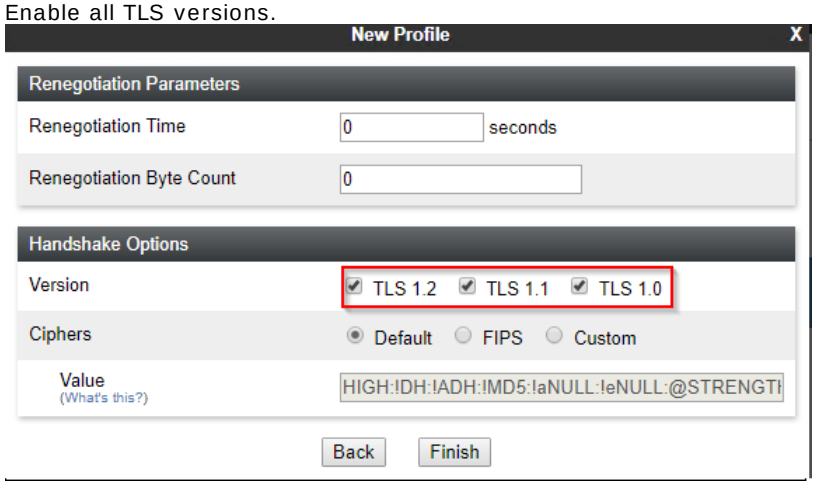
a. Profile Name: Enter a descriptive name to help select this profile later in other menus.

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

c. Peer Verification: Select *None*.

d. Click Next.

e. Enable all TLS versions.



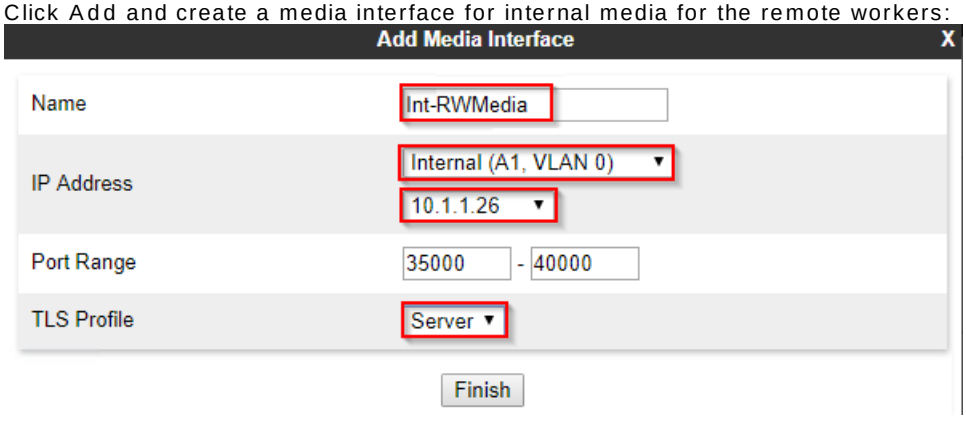
f. Click Finish.

5. You now need to create media interfaces for the remote worker traffic. See Create Media Interfaces 30.

4.6 Create the 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:



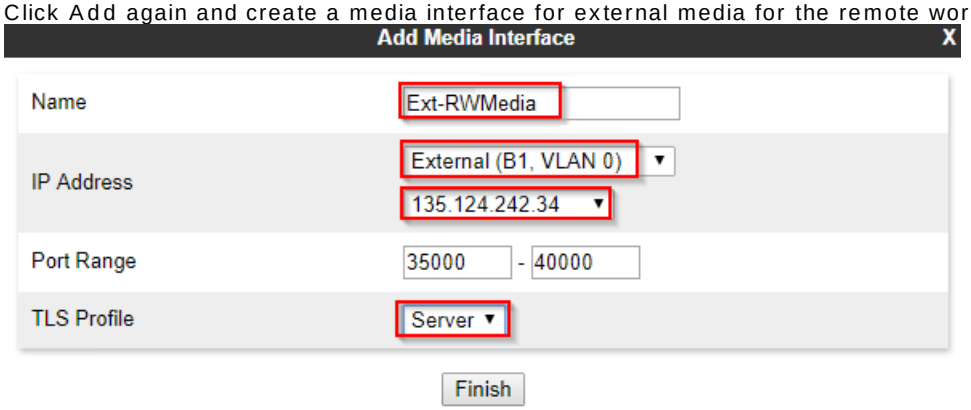
   a. Name: This name is used to select the interface when creating the server flow[36] to the IP Office server.

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

   c. TLS Profile: Select the TLS server profile created previously[28] .

   d. Click Finish.

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



   a. Name: This name is used to select the interface when creating the subscriber flow[35] to the remote workers.

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

   c. TLS Profile: Select the TLS server profile created previously[28] .

   d. Click Finish.

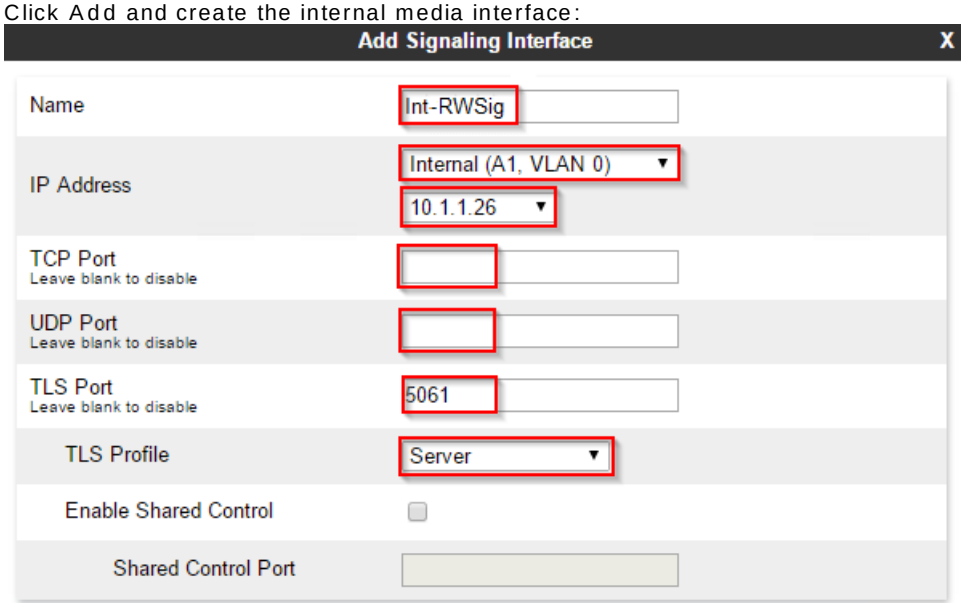
4. You now need to create signaling interface for the remote worker traffic. See Create Signaling Interfaces[31] .

4.7 Create the Signaling Interfaces

We need to create signalling interfaces that match the SIP *Layer 4 Protocols* configured in the IP Office SIP settings[8] . 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[36] 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.

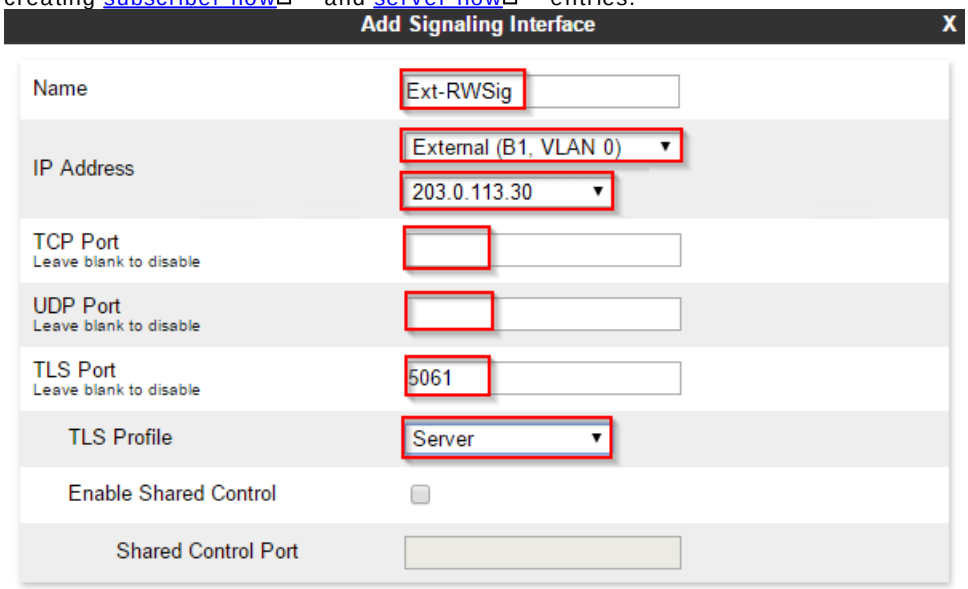
   d. UDP Port: Leave this blank to disable UDP.

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

   f. TLS Profile: Select the TLS profile[28] 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 is used when later creating subscriber flow[35] and server flow[36] entries.



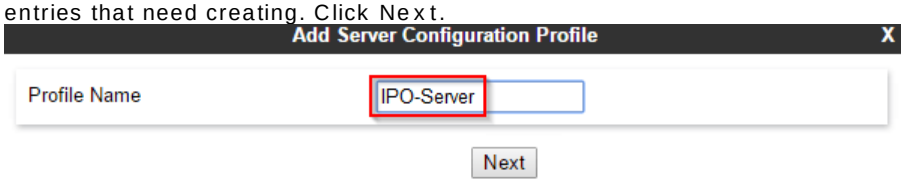
4. You now need to create a server profile for the IP Office server. See Create a Server Profile[32] .

4.8 Create a Server Profile

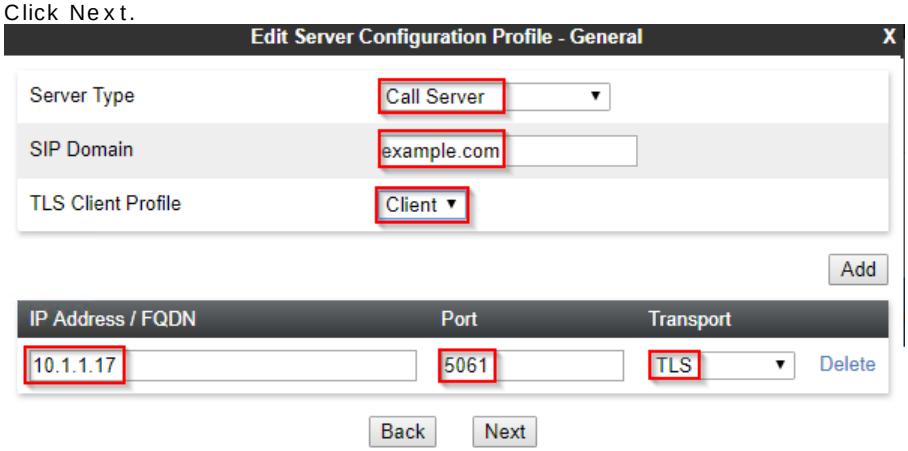
We need to create a server profile for the IP Office.

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 33 and server flow 36 entries that need creating. Click Next.



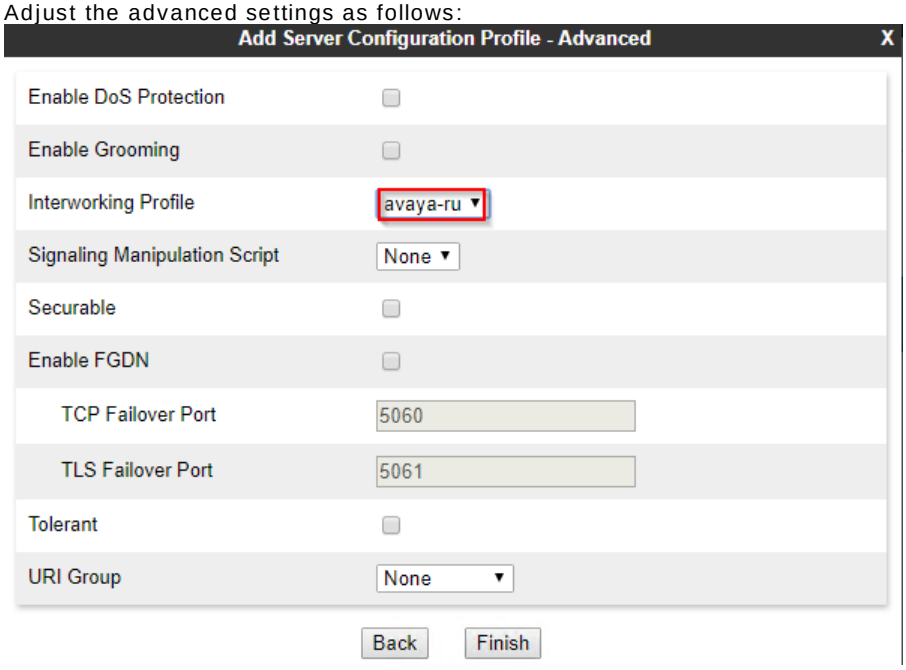
4. Click Next.



   a. Set the Server Type to *Call Server*.

   b. Enter the details for the layer 4 port SIP connections set in the IP Office configuration 8 . For this example we are using TLS on port 5061 for the external extensions. Click Next.

5. Authentication is not needed on the SBC to IP Office connection, click Next.
6. Heartbeat is not needed, click Next.
7. Adjust the advanced settings as follows:



   a. Enable Grooming: Deselect this option. Grooming is not recommended for SIP extension connections.

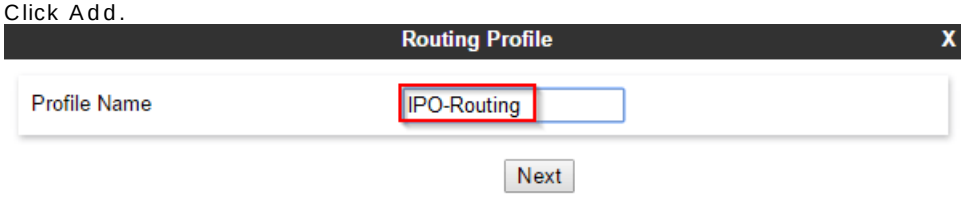
   b. Interworking Profile: Set to *avaya-ru*.

8. Click Finish. You now need to create a server routing entry for the IP Office server. See Create Server Routing 33 .

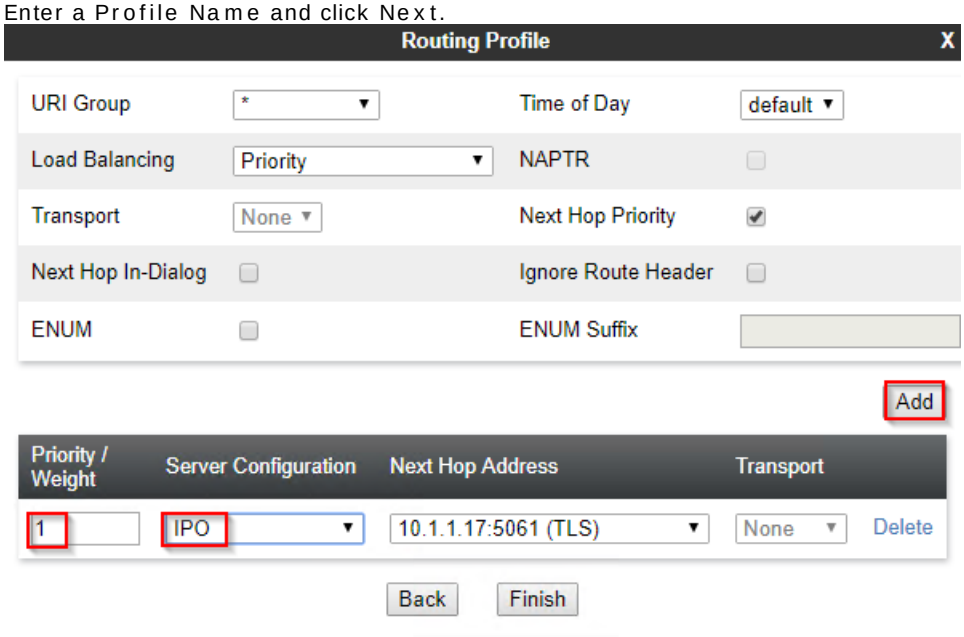
4.9 Create Server Routing

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 32 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 34 .

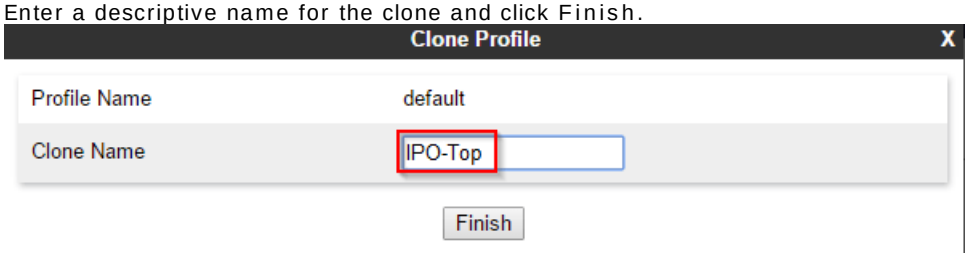
4.10 Create a Topology Hiding

Topology hiding allows selected information in SIP messages to be removed or replaced when necessary. For example, when an application uses an IP address in its signaling when it should use the corresponding domain name.

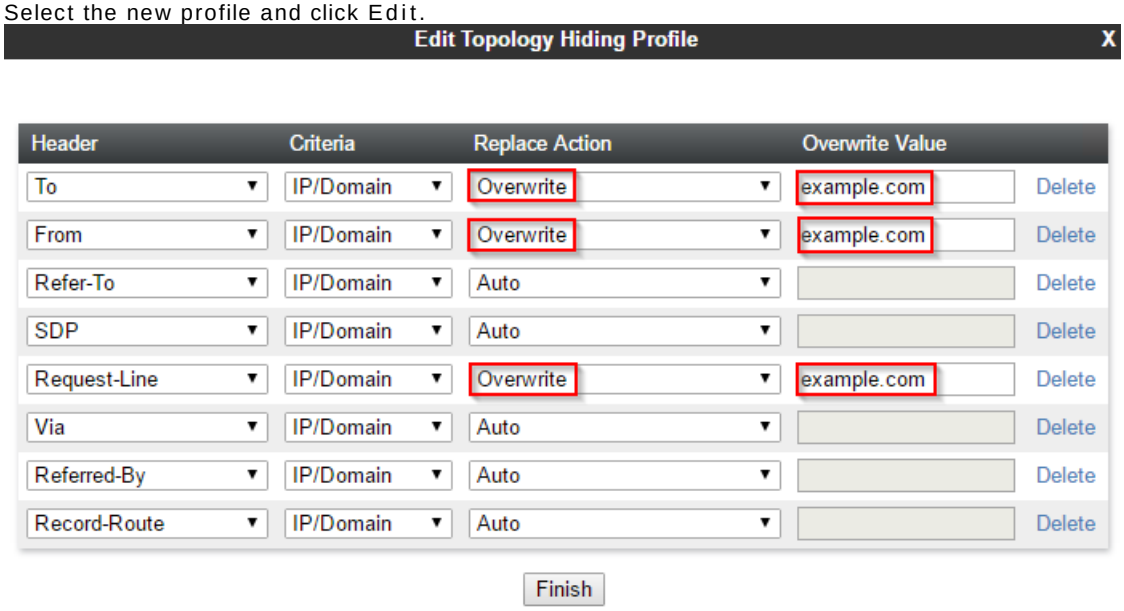
- Avaya Communicator for Windows
  During Avaya Communicator for Windows registration, the IP Office sends the internal IP address of the XMPP domain in its registration response[34] . As a result, external Avaya Communicator for Windows clients are not able to register with the one-X Portal for IP Office and have presence. Creating a custom topology allows the IP address to be replaced with the required FQDN value.

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.

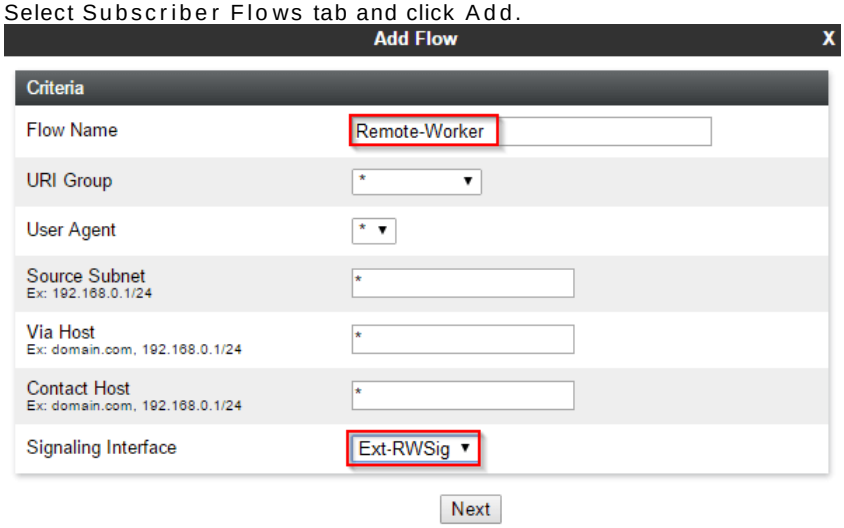


5. For the To, From, Refer-To, SDP and Request-Line fields; set the Replace Action to *Overwrite* and enter the IP Office domain as the Overwrite Value.
6. Click Finish.
7. You now need to create a subscriber flow for traffic to/from the remote workers. See create a Subscriber Flow[35] .

4.11 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.

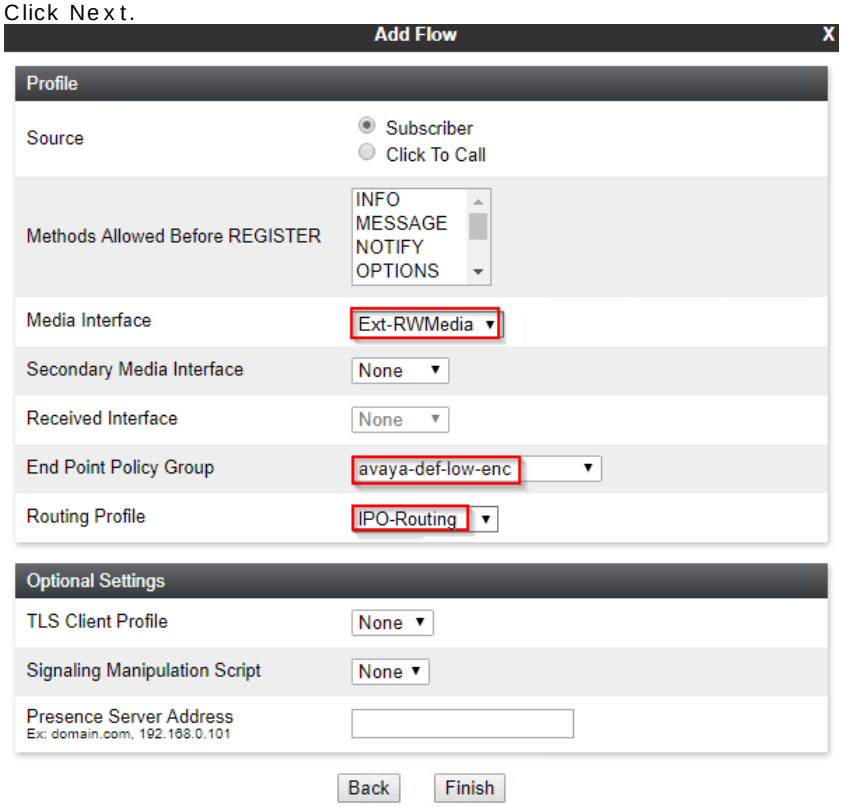


   a. Flow Name: Enter a descriptive name for the subscriber flow's usage. This name is used in other menus.

   b. User Agent: If created, select the user agent profile [39] intended to restrict connections.

   c. Signaling Interface: Select the external signalling interface [31] created for the remote workers.

3. Click Next.



   a. Media Interface: Select the external media interface [30] previously created for the remote workers.

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

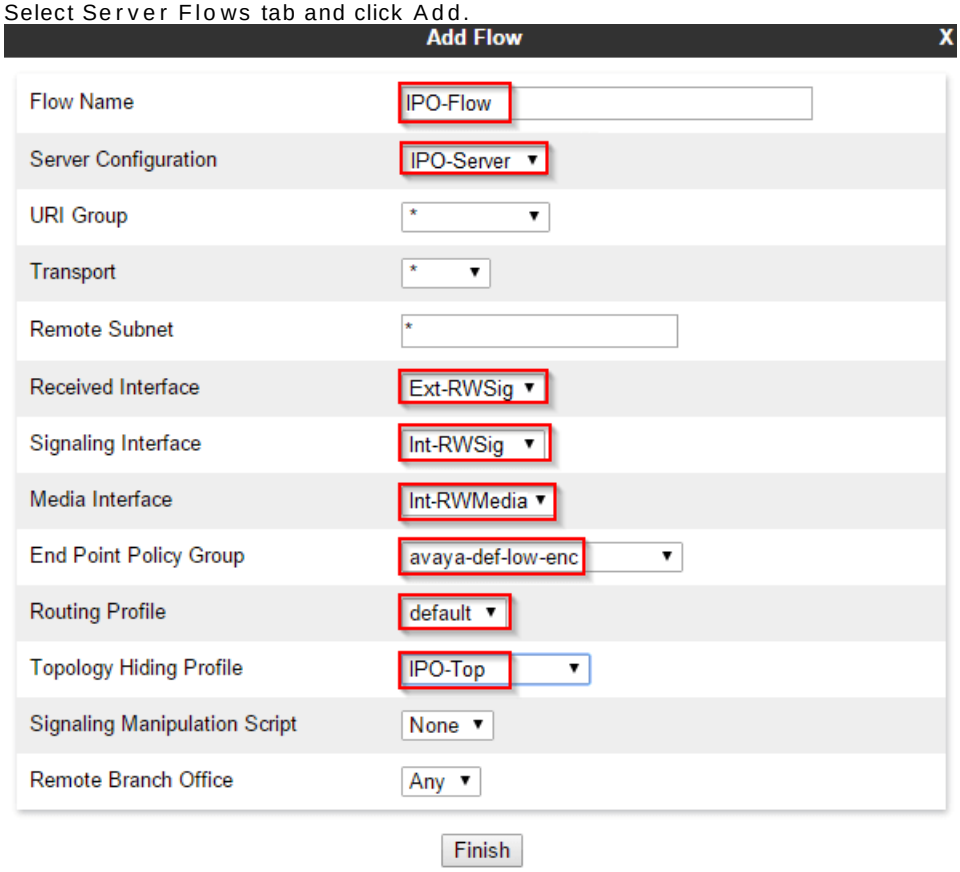
   c. Routing Profile: Select the server routing [33] profile previously created for the IP Office.

4. Click Finish. You now need to create a server flow for remote worker traffic to/from the IP Office. See Create a Server Flow [36] .

4.12 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 32 created for the IP Office server.
   c. Received Interface: Select the external signaling interface 31 created for the remote workers.
   d. Signaling Interface: Select the internal signaling interface 31 created for the remote workers.
   e. Media Interface: Select the internal media interface 30 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 34 created for IP Office remote SIP clients.

3. Click Finish.
4. You now need to create application relays for the specific ports used by the IP Office applications. See Create Application Relays 37 .

4.13 Create Application Relays

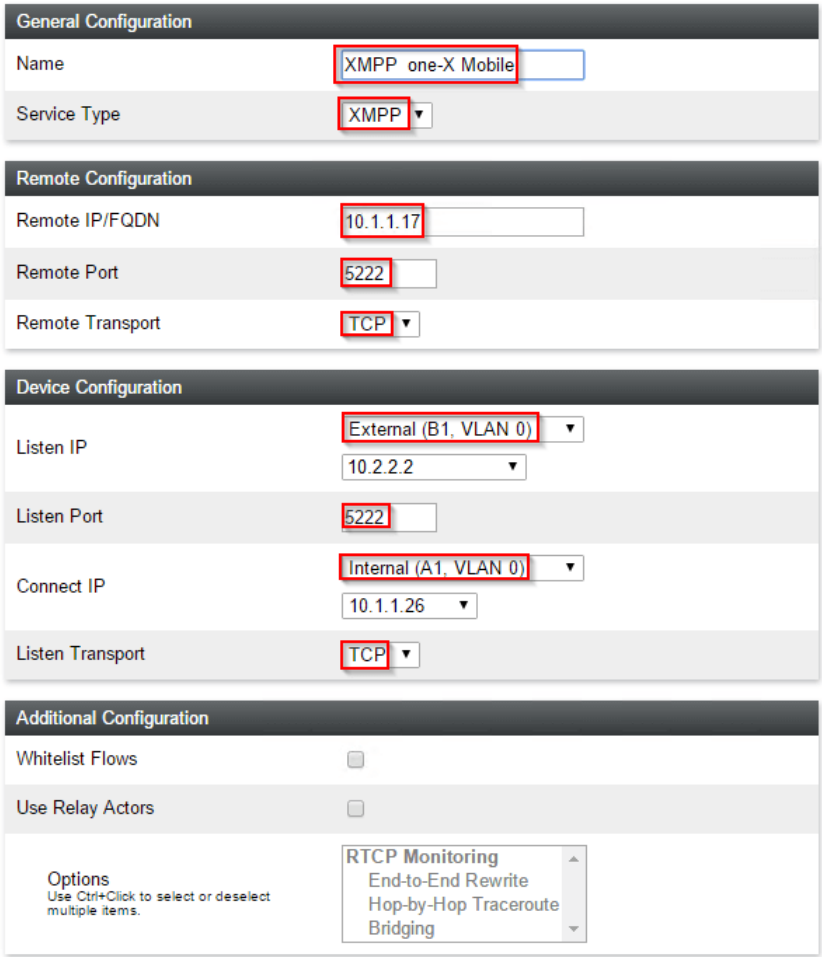
Application relays function as port forwards. Different clients require different application relays. See more detail about necessary ports under the Client Behavior 45 topic. The example below is an application relay for one-X Mobile Preferred.

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 <HostDomain> *(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.

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).

4.14 Configuring User Agent Profiles

This stage is optional. User Agent profiles can be created to for the user agent (UA) header sent by the particular phones and clients being supported. When such profiles are added to the subscriber flow 35 , only phones that match the UA header are allowed to send registration and other messages through the ASBCE.

The UA string of a particular phone or softphone can be viewed in System Monitor by registering the phone internally.

To create a user agent profile:

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.
5. Put in the user agent string that you want to allow. You can enter multiple user agent strings if required. You can use regular expressions (regexp) to define a complex match.
6. Click Finish.

To apply a user agent profile:

In the subscriber flow 35 , use the User Agent field to select the required user agent profile.

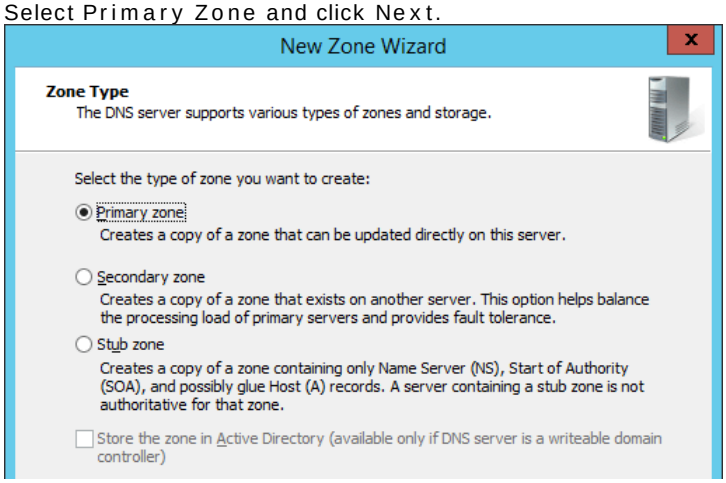
Chapter 5.
DNS Configuration

5. DNS Configuration

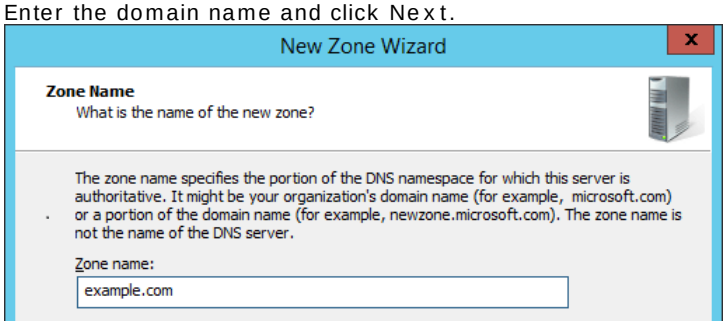
Installation and configuration of DNS servers is out of scope of this document. The follow is an outline example for a Windows 2012 R2 server. It shows the creation of the A record for the IP Office Server Edition server and SVR records for its XMPP and SIP services.

To configure DNS on a Windows 2012 R2 Server:

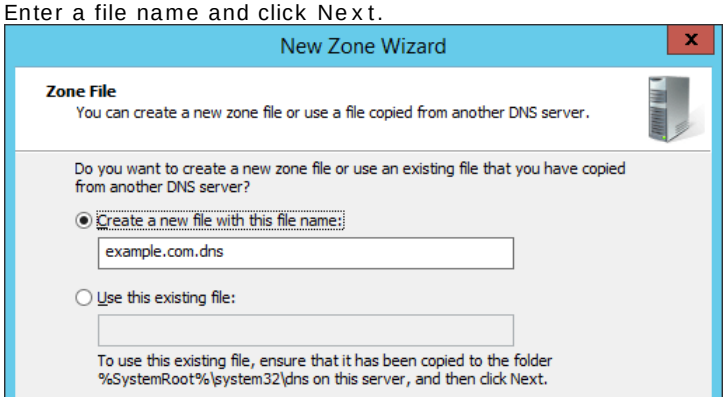
1. Add a new Forward Lookup Zone for the FQDN *ipo.example.com*.
2. Select Primary Zone and click Next.



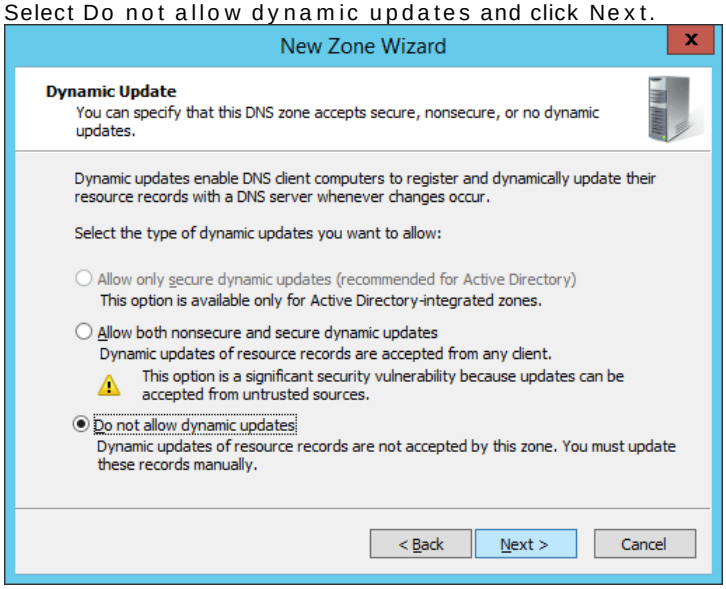
3. Enter the domain name and click Next.



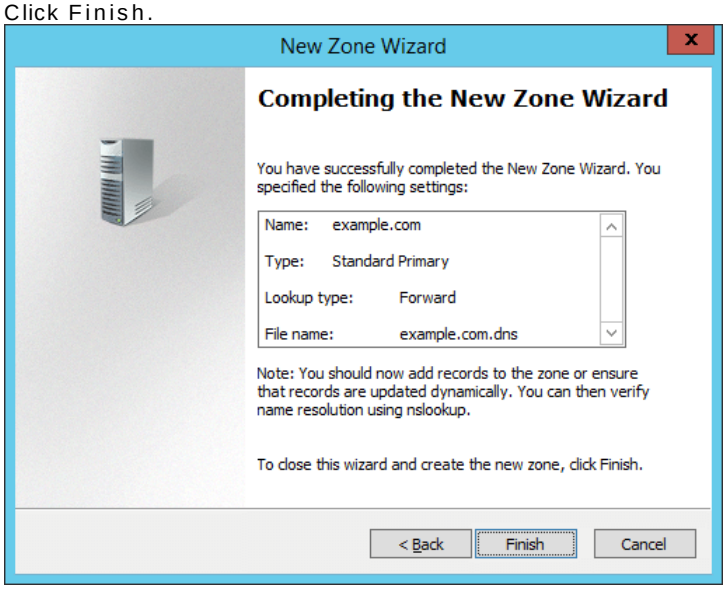
4. Enter a file name and click Next.



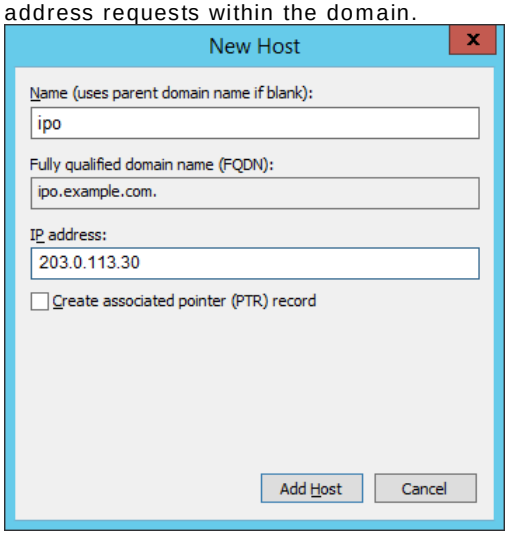
5. Select Do not allow dynamic updates and click Next.



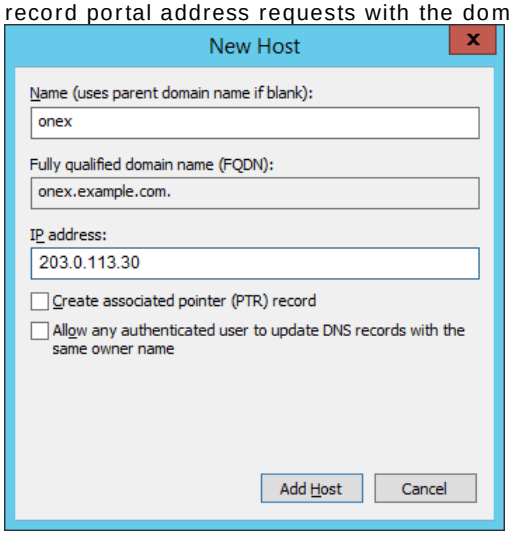
6. Click Finish.



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 6.
Client Behaviour

6. 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.

6.1 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 <HostDomain> *(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.

6.2 Avaya Communicator for Windows

The Avaya Communicator for Windows is configured with the FQDN of the IP Office. With that, it:

1. Registers to the IP Office on the configured SIP port.
2. Then connects to the one-X Portal for IP Office using the information it receives during the registration.

- By default the IP Office includes the internal IP address of the XMPP domain in the *onex_server* field. That prevents external clients from getting presence from the one-X Portal for IP Office. To solve this a custom topology[34] is required to replace the IP address the required FQDN.

Detailed process:

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.

6.3 Avaya Communicator for iPad

The Avaya Communicator for iPad is configured with the FQDN of the IP Office. With this, it:

1. Registers to the IP Office as a SIP extension.
2. Connects to the one-X Portal for IP Office using the information it received during the registration.

Detailed process:

1. Configure the client.
   a. In Settings | Accounts and Services | Phone Service set the following:
      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.

6.4 one-X Mobile Preferred for Android

The one-X Mobile Preferred for Android is configured with the FQDN of the one-X Portal for IP Office server. Using that value, it:

1. Contacts the one-X Portal for IP Office through the REST API (port 9443) to learn the *sipRegistrarFqdn* value.
2. Does a DNS A query using the *sipRegistrarFqdn* value to learn the IP address of the IP Office.
3. Registers with the one-X Portal for IP Office and IP Office.

Detailed process:

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.

6.5 one-X Mobile Preferred for iOS

The one-X Mobile Preferred for iOS client is configured with the FQDN of the one-X Portal for IP Office server. Using that value, it:

1. Contacts the one-X Portal for IP Office through the REST API (port 9443) to learn the *XMPP Domain* and the *sipRegistrarFqdn* values.
2. Does a DNS A query on the *XMPP Domain* value to learn the IP address of the one-X Portal for IP Office
3. Does a DNS A query on the *sipRegistrarFqdn* value to learn the IP address of the IP Office.
4. Registers with the one-X Portal for IP Office and IP Office.

Detailed process:

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).

6.6 Equinox

Equinox clients are available on multiple platforms; Windows, Android, iOS, MAC. They all have a common behavior, common configuration, etc.

Equinox registration starts with a DNS A query to the FQDN given to it as the SIP_CONTROLLER_LIST value in the 46xxsettings.txt file. It then attempts registration to the IP address returned by the DNS server. For presence and directory services the client also starts a TLS connection to the same address on port 443.

- The source of the SIP_CONTROLLER_LIST value in the 46xxsettings.txt file can be set using the RW_SBC_PROV= NoUser source number[59] .

There are two methods used to/register Equinox, refer to the "SIP Telephone Installation Notes". In summary:

1. Email based configuration where the user enters an email address when they first start the Equinox client. The client will contact accounts.zang.io and check if the email address and email domain have been registered in Avaya Spaces. If yes, it attempts to download the public settings file for the domain which supplies address information for the IP Office system. If successful, the client uses the Client_Settings_File_Url setting in that file to request settings from the IP Office address given. For example:

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

2. Web based configuration where the user enters the IP Office address when they first start the Equinox client. The URL takes the form *http://<primary_IPOffice_FQDN>/46xxsettings.txt*

In both cases, once the 46xxsettings.txt file is downloaded, the client will ask the SIP extension and password.

Checking the Settings

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

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

Name:    ipo11.example.com
Address:  135.124.242.20


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

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

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

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

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

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

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

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

4. Run a traceSBC on the ASBCE and check the registration of the client. In the 200 OK of REGISTER, check the onex_server and backup_ipoffice_server fields. During normal operation, the onex_server should contain the FQDN of Primary one-X Portal for IP Office and backup_ipoffice_server should contain the FQDN of Secondary IP Office.

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

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

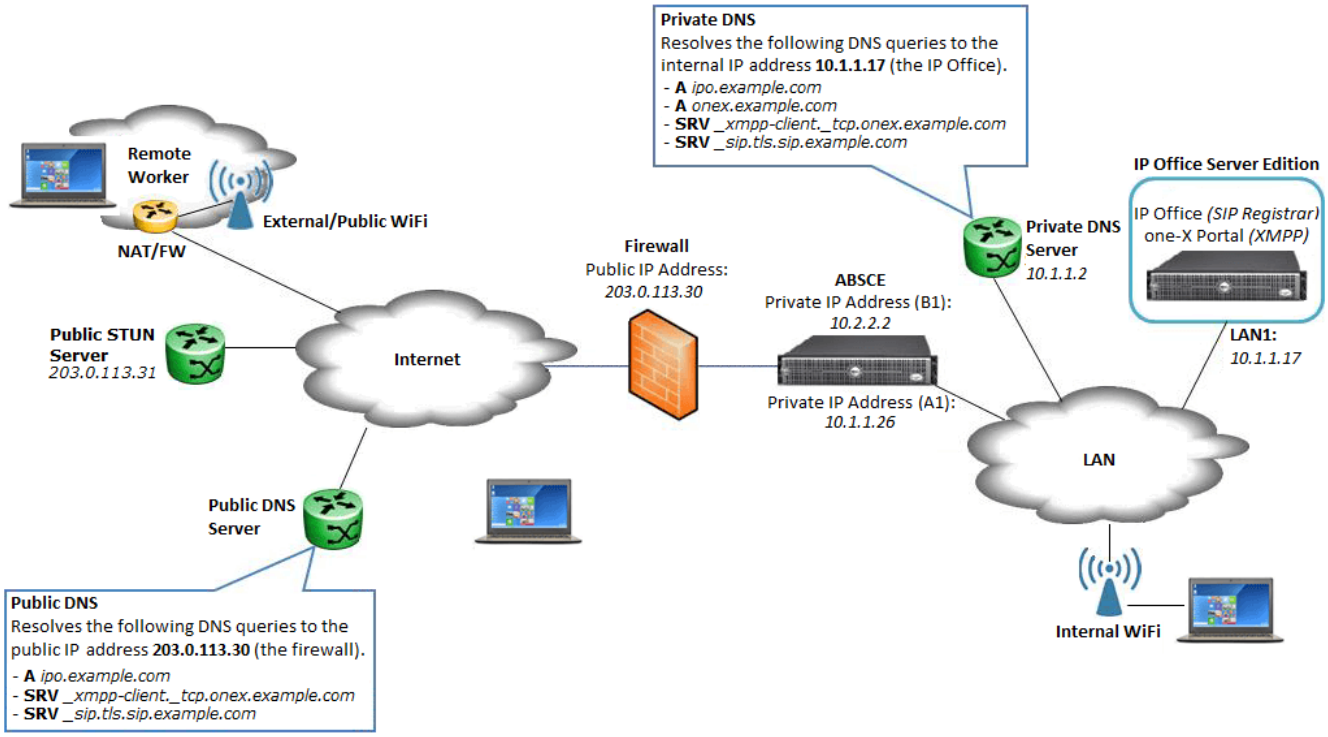
Chapter 7.
Configuration for WebRTC

7. Configuration for WebRTC

An ASBCE can be used to help secure and support incoming WebRTC calls to the IP Office via the WebRTC Gateway service. That service runs on the same server that hosts one-X Portal for IP Office. WebRTC Clients use 9443 for signaling and 56000-58000 for media (default) towards the WebRTC Gateway service.

For remote WebRTC connection, the main methods used to achieve this are:

- An application relay for connections to port 9443 on the portal server.
- The use of STUN and TURN for media relay and NAT resolution to the WebRTC Gateway service on the portal server.



This example scenario assumes that the external WebRTC clients may be using NAT to connect to the internal network.

Firewall Configuration

The enterprise firewall needs to be configured to:

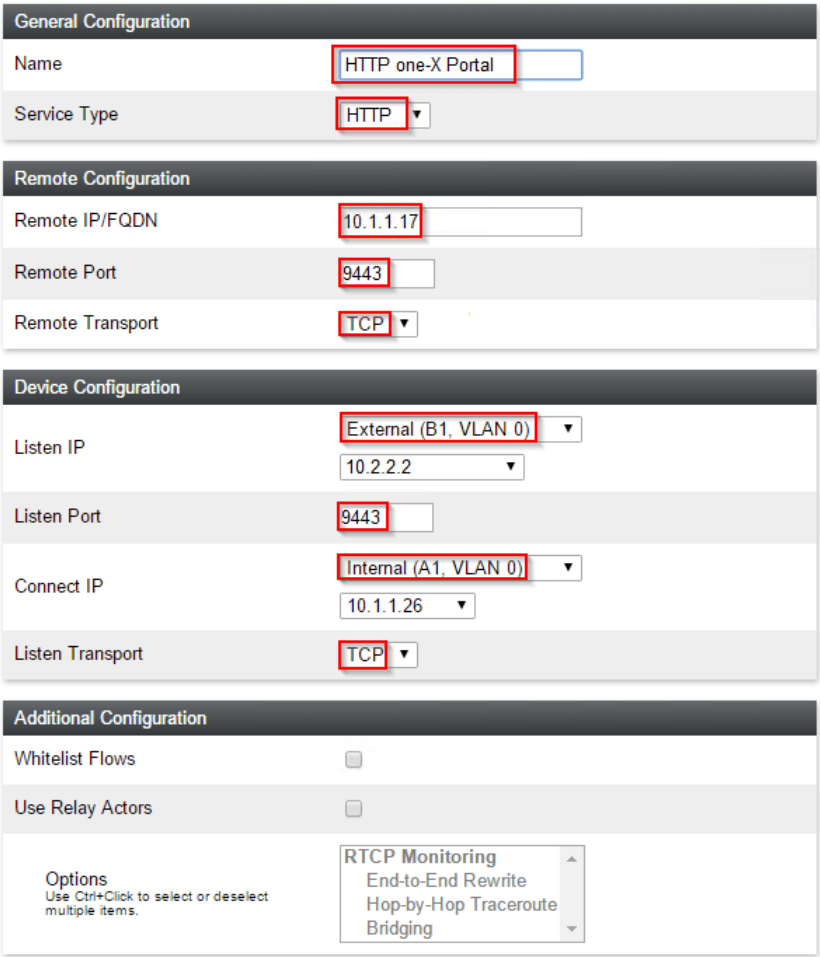
1. Allow Layer 3 NAT only.
2. Disable all SIP aware functionality such as ALG.
3. Forward the TCP signalling ports (by default 9443 and 5060) to the B1 interface of the ASBCE.
4. Forward the RTP ports (by default 56000 to 58000 to the B1 interface of the ASBCE.

7.1 Create Application Relays

Application relays function as port forwards. Different clients require different application relays. The example below creates application relays for WebRTC using ports 5061 and 9443.

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.



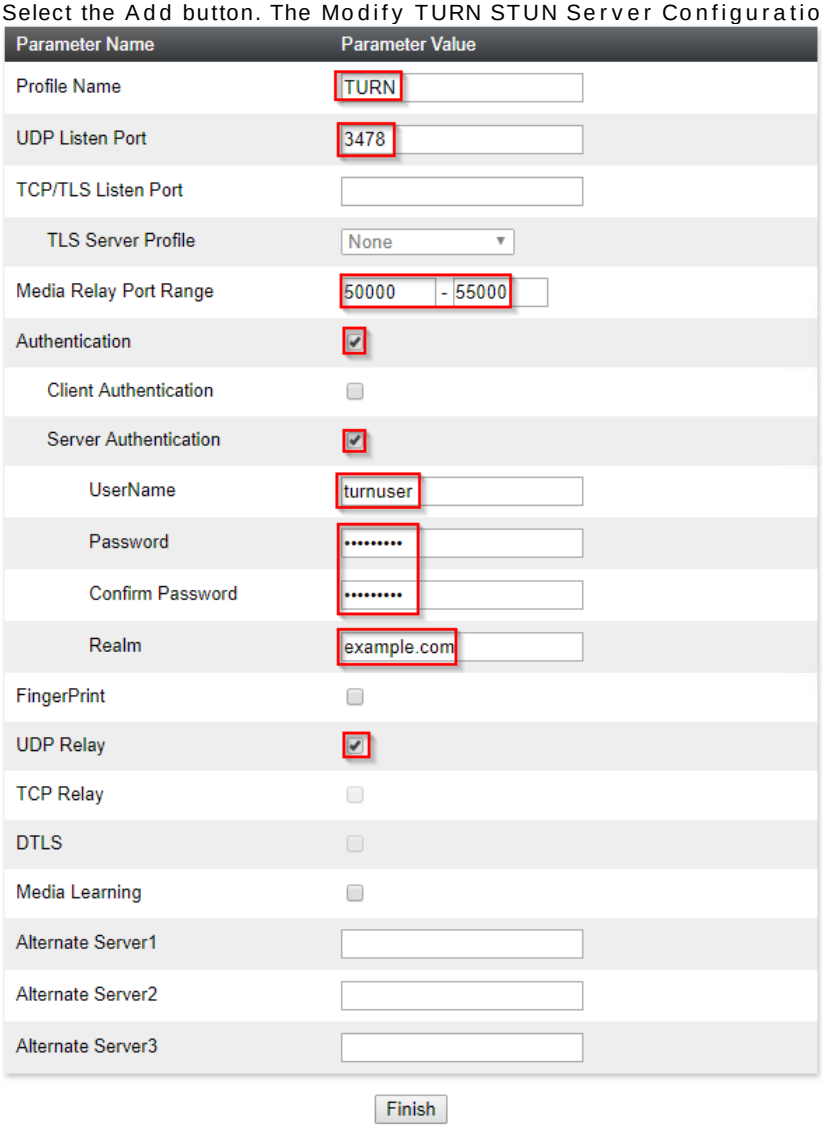
   a. Name: Enter a descriptive name for the application relay.
   b. Service Type: Select *HTTP*.
   c. Remote IP/FQDN: Enter the IP of the one-X Portal for IP Office (same as IP Office in this example).
   d. Remote Port: Enter *9443*
   e. Remote Transport: Select *TCP*.
   f. Listen IP: Select the external interface.
   g. Listen Port: Enter *9443*.
   h. Connect IP: Select the internal interface.
   i. Listen Transport: Select *TCP*.
3. Click Finish.
4. Repeat the above procedure for port 5061 (SIP).

7.2 Configuring a STUN/TURN Service

Use the following process to configure STUN/TURN settings on the ASBCE to support WebRTC.

To configure STUN/TURN for WebRTC:

1. On the ASBCE, select Device Specific Settings > TURN/STUN Settings.
2. Select the Add button. The Modify TURN STUN Server Configuration dialog box opens.



Parameter Name	Parameter Value
Profile Name	TURN
UDP Listen Port	3478
TCP/TLS Listen Port	
TLS Server Profile	None
Media Relay Port Range	50000 - 55000
Authentication	☑
Client Authentication	☐
Server Authentication	☑
UserName	turnuser
Password	••••••••
Confirm Password	••••••••
Realm	example.com
FingerPrint	☐
UDP Relay	☑
TCP Relay	☐
DTLS	☐
Media Learning	☐
Alternate Server1	
Alternate Server2	
Alternate Server3	

Finish

3. In the Listen Port, enter the port on which the ASBCE should listen for STUN/TURN connections. The default is *3478*. Ensure that matches the STUN Server Port set in the IP Office WebRTC Gateway service's Media Gateway settings.
4. In the Media Relay Port Range field, enter the port range to be used for the TURN server. This range should match the RTP Port Range (Public) set in the IP Office WebRTC Gateway service's Media Gateway settings.
5. Select Authentication. This will display several additional fields.
6. Select Server Authentication and define a user name and password.
7. Set the Realm to match the domain being used for the IP Office systems.
8. Click Finish.
9. If the system displays the message *"At least one Listen/Media Relay IP Pair is required to complete the configuration. Click here to create a new pairing" click* . Click *'here'* in the message. Otherwise go to Device Specific Settings / TURN/STUN service and on the TURN Relay tab click Add.

10. Select a Listen IP interface and a Media Relay IP interface for the WebRTC Gateway and click Finish.

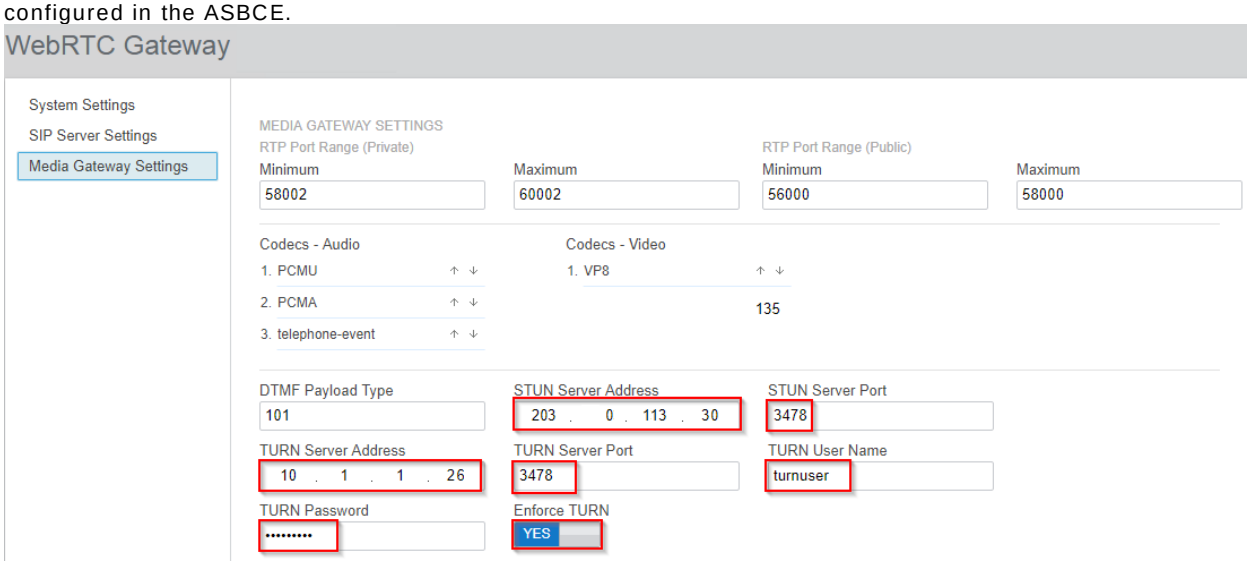
11. Save the configuration.

7.3 Configuring the WebRTC Gateway

Within the IP Office WebRTC gateway service's configuration, enable TURN support using the ASBCE.

To enable the WebRTC gateway:

1. Login to the server's web configuration menus.
2. Click Solutions.
3. Click Applications and select WebRTC Configuration.
4. Select the Media Gateway Settings menu. Set the TURN server details to match the TURN service configured in the ASBCE.



   a. STUN Server Address: Set to the public IP address of the firewall.
   b. STUN Server Port: 3478
   c. TURN Server Address: Internal interface address of the ASBCE.
   d. TURN Server Port: 3478
   e. TURN User Name / TURN Password: Match the user name and password defined in the ASBCE TURN configuration.
   f. Enforce TURN: Set to *Yes*.
5. Click Save to save any changes.

Chapter 8.
Remote SIP Deskphones

8. Remote SIP Deskphones

This section covers an example for deploying Avaya SIP desk phones as the remote IP Office worker extension. The setup is similar to that used for Avaya SIP softphone clients.

Supported remote SIP desk phones are:

- 1120, 1140, 1220, 1230.
- E129
- H175
- J129, J139, J169, J179
- K155, K165, K175

Note

- H175 phones connect to the one-X Portal for IP Office for personal contacts. Therefore, they require an appropriate XMPP port application relay[37] to be configured.

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.

- Note that RW_SBC_TLS, RW_SBC_TCP and RW_SBC_UDP are ignored if RW_SBC_REG and RW_SBC_PROV are not set.
  - RW_SBC_REG=*<ASBCE B1 public IP address>*
    Indicates the public IP address of the ASBCE.
  - RW_SBC_PROV=*<ASBCE A1 private IP address>*
    Indicates the private IP address of the ASBCE. The IP Office checks whether SIP phone file requests are coming from this address. If so, the IP Office performs the following actions:
    - It removes any configuration, provisioning and phonebook path information from the auto-generated settings sent in response to those phones. Instead the values must be manually configured on the remote phones.
    - It sends the RW_SBC_REG value to the phone:
      - as the SIP Server for E129 sets
      - as the S1/S2 value for 1100/1200 Series phones
      - as the SIP CONTROLLER LIST for H175 phones.
      - as the SIP CONTROLLER LIST for Equinox clients.
  - 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>*
- PUBLIC_HTTP=x
  This setting can be used when the IP Office is providing phone firmware files through file redirection using the HTTP Server IP Address and HTTP Redirection settings. The source number defines the public file server redirection address given to remote worker/SBC connected phones.
- SET_STIMULUS_SBC_REG_INTERVAL=x
  Used to set the registration interval for J100 Series stimulus phones (J139, J169, J179). The recommend value is 180 seconds. If not specified the default is 1 hour (3600 seconds). Range 180 to 3600 seconds.
- REM_BACKLIGHTOFF=N
  Sets the backlight timer value (SET BAKLIGHTOFF N) provided through the auto-generated settings file to remote extensions.

Phone Model Specific Notes

- For 1100/1200 Series Phones:
  All port values are sent to the set and the phone 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.

Chapter 9.

ASBCE and IP Office Resilience

9. ASBCE and IP Office Resilience

IP Office systems can be configured to support a range of resiliency options. That includes resilient support of IP phones including SIP phones and SIP softphone applications. Refer to the *"IP Office Resilience Overview"* manual for details of resilience operation and the phones/softphones supported for resilience.

Whilst phone resilience is supported by IP Office Server Edition systems, support for one-X Mobile Preferred clients and presence features requires IP Office Select systems.

For resilient support of remote phones, the ASBCE connection is configured with 2 public/private IP address pairs. One pair is mapped to the IP Office network's primary server, the other pair is mapped to the network's secondary server. It does not matter if the SBC itself is Simplex, HA or even two independent servers. The logic of the configuration will be the same in all those scenarios.

Process Summary

This section of this document gives an overview of the additional configuration processes required to add resilience support to an existing ASBCE/IP Office configuration. The main additional steps are:

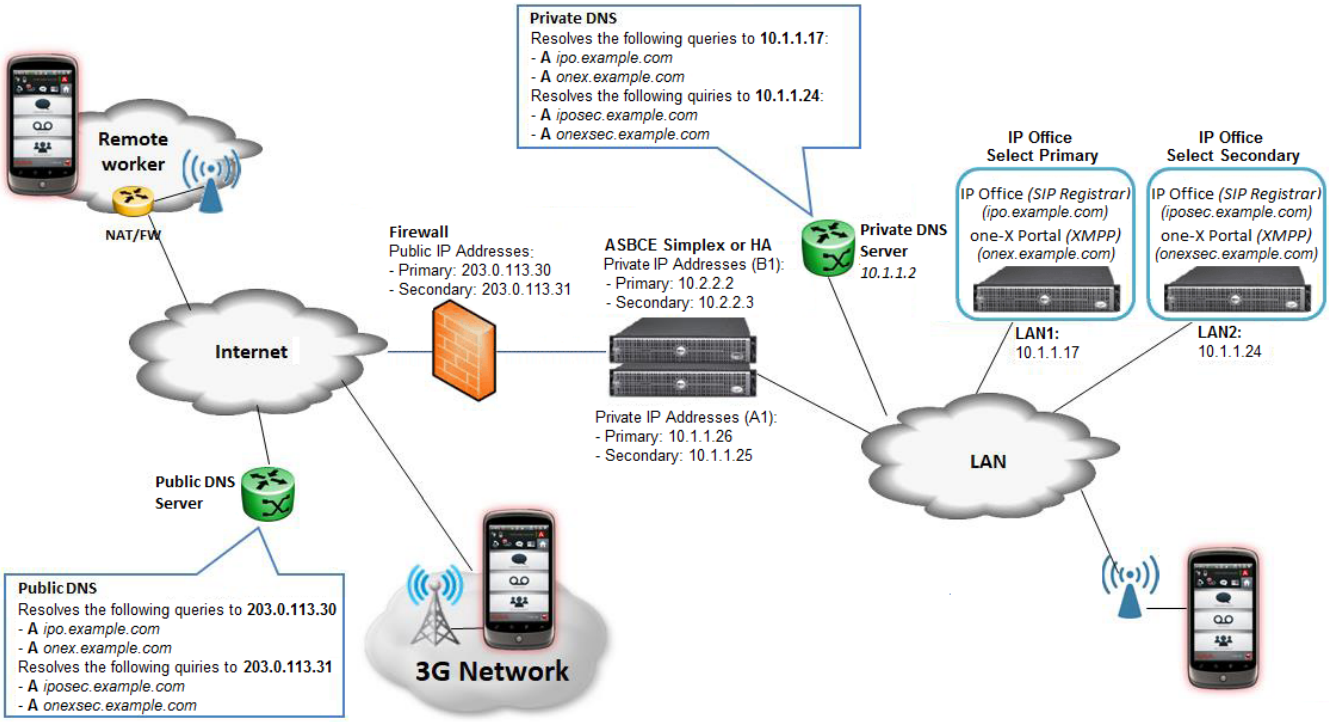
1. Create an identity certificate for the secondary server 66 .
2. Install the identity certificate 67 .
3. Configure the one-X Portal for IP Office 68 .
4. Configure the ASBCE 68 .
5. Configure DNS 68 .
6. Check operation 69 .

Notes

- IP Office resilience only protects against server outages, not against network issues between the client and the server. If the link between the client and the primary server goes down while the server itself is up and can still communicate with secondary server, the client will NOT be able to register either to primary or secondary. The client can register to secondary only if the primary server itself goes down.
- Using ASBCE for resiliency can have negative impact on H323 phones, since they use HTTP/HTTPS for obtaining configuration/firmware/backup files. The solution is to either use a different file server for H323 phones (not IP Office) or configure SBC to not interfere with HTTP/HTTPS ports used by H323 phones.
- Auto provisioning of SIP hard phones can provide the ASBCE address to the phones instead of the IP Office address (the ASBCE address can be specified as a NoUser source number 59). In the case where the SBC address is provided, the IP Office will not include the resilient server address and we do not have means to provide the resilient ASBCE address as a parameter. This means that if resiliency needs to be used with ASBCE, phones should be provisioned with a separate file server.
- When routed via the ASBCE, the SIP endpoint IP address cannot be used to match it to an IP Office location. Therefore, if using the IP Office location settings for resilience, the extension location need the location to be specifically configured in the extension's configuration record.

9.1 Resiliency Schematic

The following is an example* schematic of a resilient configuration.



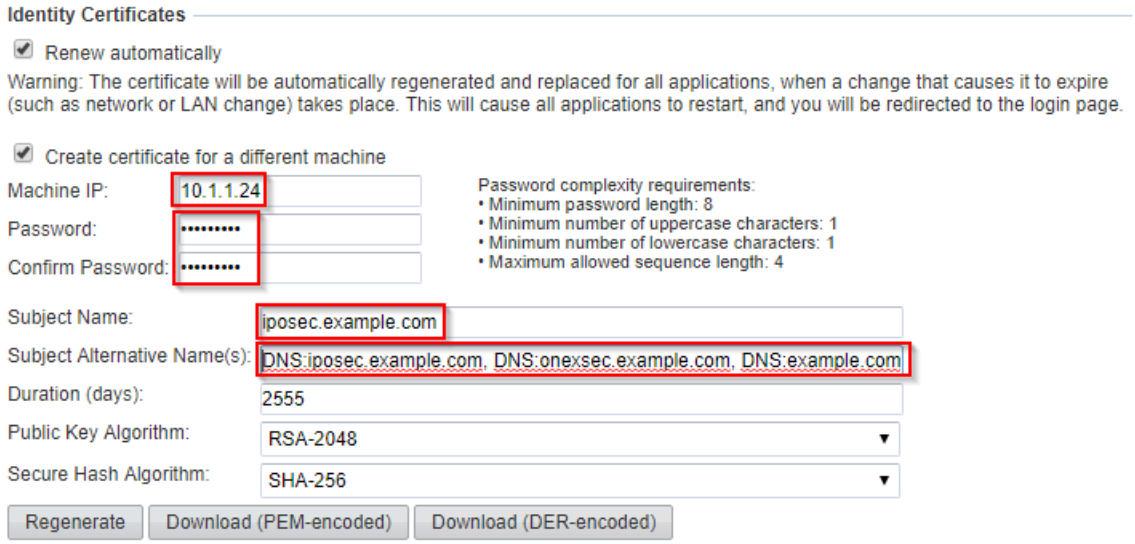
- *These are just examples used to illustrate how the different components interact and exchange information. Actual installations will have different requirements specific to the individual customer sites. Refer to the Avaya Session Border Controller for Enterprise manuals for details.

9.2 Generating an Identity Certificate for the Secondary Server

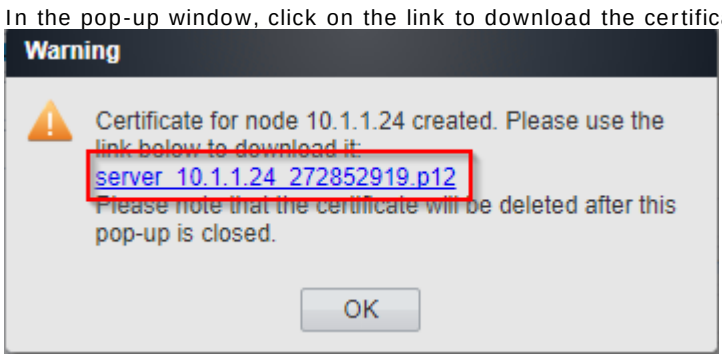
The secondary server requires an identity certificate issued by the primary server.

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 primary 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. Machine IP: Enter the IP address of the secondary server
   b. Password: Enter a password to encrypt the certificate and key. For example *Avaya123$*.
   c. Subject Name: Enter the FQDN of the secondary server
   d. Subject Alternative Name(s): List the the FQDN of the secondary server, the secondary XMPP domain, the SIP domain and the secondary server's internal and external IP addresses.
5. Click Regenerate and Apply.
6. In the pop-up window, click on the link to download the certificate.



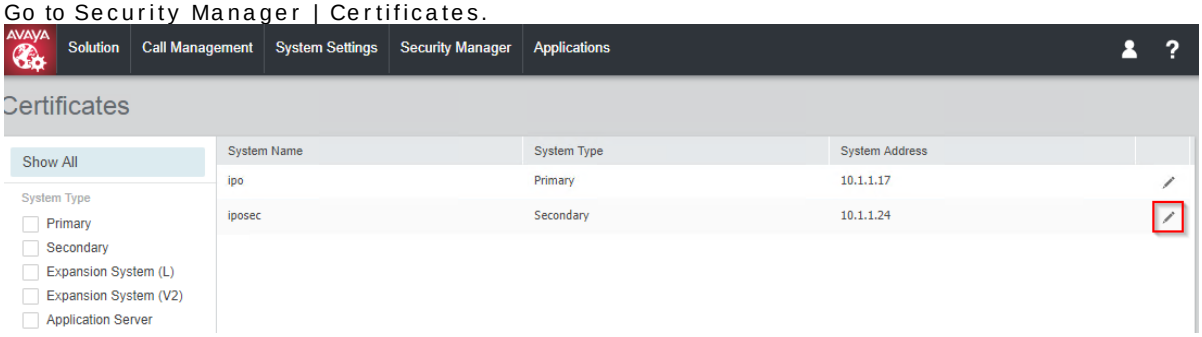
7. Click OK.
8. Rename the downloaded file to *IPOSEC_ID.p12*.

9.3 Installing the Secondary Server's Identity Certificate

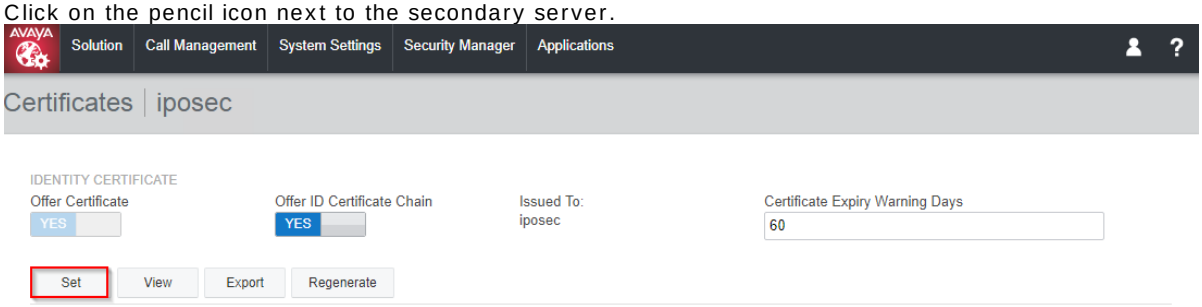
The identity certificate created for the secondary server needs to be installed on that server.

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 primary server. Click on ☰ and select Platform View.
   - or browse to *https://<IP Office IP address>:7071* and login as the Administrator.
2. Go to Security Manager | Certificates.



3. Click on the pencil icon next to the secondary server.



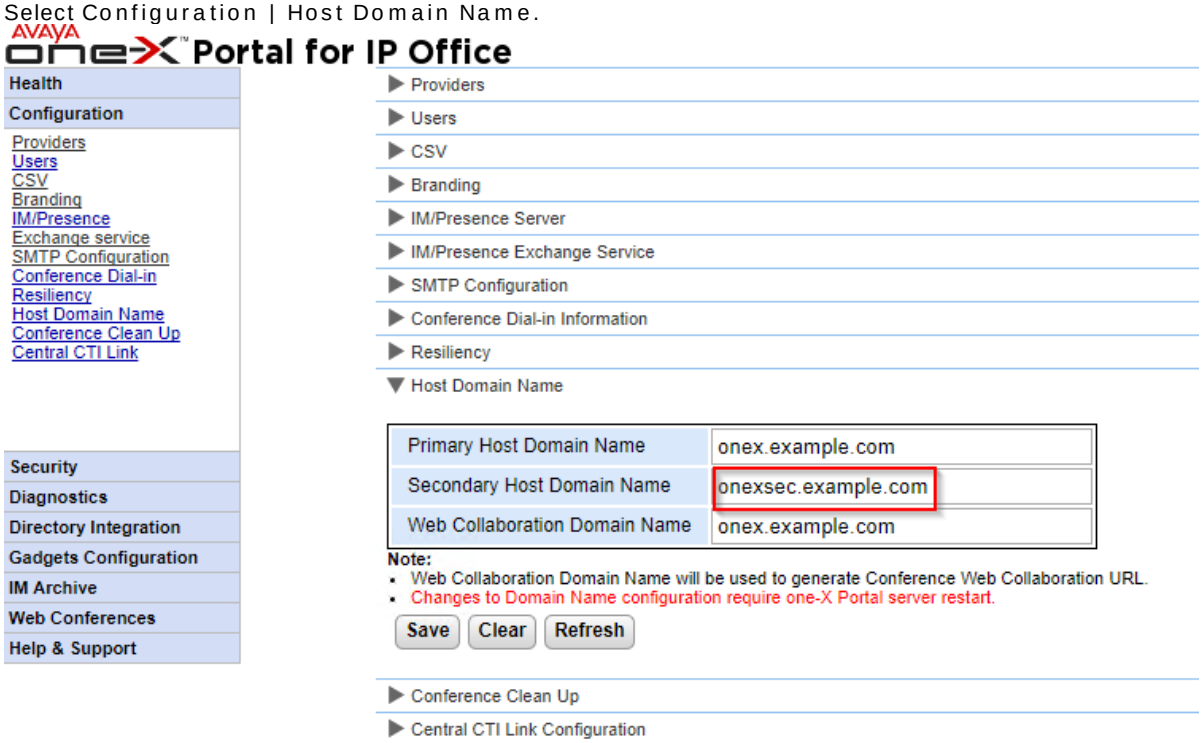
4. Click on Set.
5. Browse to the identity certificate file and enter the password.
6. Click Upload.

9.4 Configuring the one-X Portal for IP Office

The one-X Portal for IP Office server's needs to be configured with the secondary server's domain name. This is done through the primary server configuration which is then automatically shared with the secondary server.

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 | Host Domain Name.



   a. Set the Secondary Host Domain Name to the FQDN of the secondary one-X Portal for IP Office.
   b. Click Save.
3. Click on the icon at the top of the menus to restart the portal service.

9.5 Configuring the ASBCE

The ASBCE configuration steps are similar to single server setup 24 . The requirement is to create additional matching entries but using the public and private IP addresses of the secondary IP Office server.

9.6 Configuring the DNS

The DNS server configuration is similar to that for a single server 41 . SVR records are required for the secondary server's XMPP and SIP services.

9.7 Checking Operation

There are a number of ways to check that the correct information is being provided in response to client requests.

9.7.1 DNS Routing

Verify the DNS Routing

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

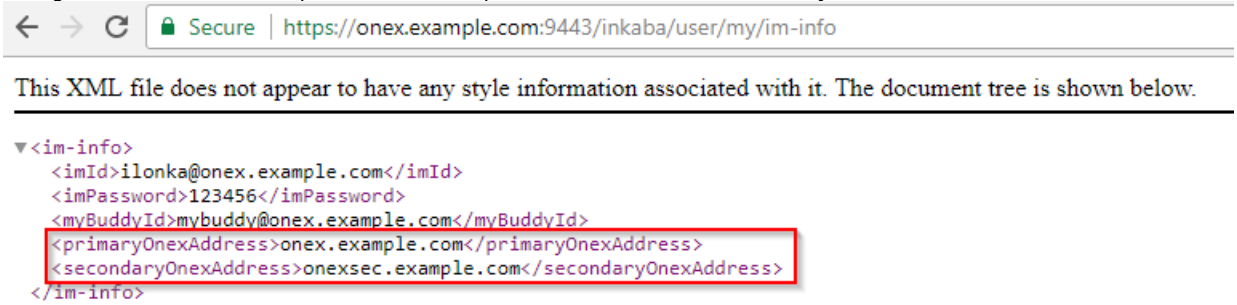
```
C:\Users\agardi>nslookup
Default Server:  UnKnown
Address:  203.0.113.205

> ipo.example.com
Server:  UnKnown
Address:  203.0.113.205

Name:    ipo.example.com
Address:  203.0.113.30

> onex.example.com
Server:  UnKnown
Address:  203.0.113.205

Name:    onex.example.com
Address:  203.0.113.30

> iposec.example.com
Server:  UnKnown
Address:  203.0.113.205

Name:    iposec.example.com
Address:  203.0.113.31

> onexsec.example.com
Server:  UnKnown
Address:  203.0.113.205

Name:    onexsec.example.com
Address:  203.0.113.31
```

9.7.2 Portal Responses

Viewing the one-X Portal for IP Office Settings During Normal Operation

When any phone or application requests XMPP information from the primary portal server, the response should contain the specified primary and secondary XMPP addresses.

1. Using a browser, enter *https://onex.example.com:9443/inkaba/user/my/im-info*.



2. The response should include the FQDNs of both the primary and secondary portal servers.

Some clients, for example one-X Mobile Preferred, also start by requesting the SIP registrar address from portal server.

1. Using a browser, enter *https://onex.example.com:9443/inkaba/user/my/sip-info*.

2. The response should include the FQDN of the primary IP Office server.

Viewing the one-X Portal for IP Office Settings During Failover

During primary server failover, the im-info contain the same values but needs to be obtained from the address of the secondary portal.

Secure | https://onexsec.example.com:9443/inkaba/user/my/im-info

This XML file does not appear to have any style information associated with it. The document tree is shown below.


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


The sip-info obtained from the secondary portal use the FQDN of the secondary IP Office.

Secure | https://onexsec.example.com:9443/inkaba/user/my/sip-info

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
▼<sip-info>
   <identity>2001@example.com</identity>
   <userName>2001</userName>
   <password>123456</password>
   <displayName>ilonka</displayName>
   <privateAddress>10.1.1.24</privateAddress>
   <udpPrivatePort>5060</udpPrivatePort>
   <udpPublicPort>0</udpPublicPort>
   <tcpPrivatePort>5060</tcpPrivatePort>
   <tcpPublicPort>0</tcpPublicPort>
   <tlsPrivatePort>5061</tlsPrivatePort>
   <tlsPublicPort>0</tlsPublicPort>
   <payloadType>101</payloadType>
   <signalingQos>136</signalingQos>
   <voiceQos>184</voiceQos>
   <videoQos>184</videoQos>
   <sipRegistrarFqdn>iposec.example.com</sipRegistrarFqdn>
 </sip-info>
```

9.7.3 Viewing an SBC Trace

The following are example traceSBC sessions run on the ASBCE during the registration of a Avaya Communicator for Windows client.

Normal Operation traceSBC Session

During normal operation, the 200 OK response shows the *onex_server* and *backup_ipoffice_server* fields set the the primary and secondary servers respectively.

```
                                    203.0.113.30:5061 ──TLS─► 203.0.113.200:61517

SIP/2.0 200 OK
From: <sips:2000@example.com>;tag=2efd31f8599d215e5e6a9be0_F2000203.0.113.200
To: <sips:2000@example.com>;tag=b726012c7faa7948
CSeq: 2 REGISTER
Call-ID: 1_4cd79e9407b8fdb5e6a9b68_R@203.0.113.200
Contact: <sips:2000@203.0.113.200:61517;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: timer,vnd.avaya.ipo
User-Agent: IP Office 10.1.0.0.0 build 237
Via: SIP/2.0/TLS 203.0.113.200:61517;branch=z9hG4bK2_4cd7a3767d58e315e6a9c04_R2000
Expires: 180
Date: Wed, 23 Aug 2017 06:31:56 GMT
Server: IP Office 10.1.0.0.0 build 237
Content-Type: application/vnd.avaya.ipo
Content-Length: 543

<ipo>
onex_server="onex.example.com";
onex_server_port="8080";
xmpp_server_port="5222";
server_onex_secure_port="9443";
username="dome";
username_twin="&0.dome";
voicemail_collect="VM.2000";
video="1";
obtain_contacts_from_ipo="0";
conferencing="1";
conf_server="ConfServer@ipo.example.com";
conf_server_adhoc="ConfAdhoc";
transfer="1";
extended_mwi="1";
video_capable="1";
blind_transfer="1";
auto_ans="1";
change_password="1";
xmpp_group="1";
backup_ipoffice_server="iposec.example.com";
```

Failover Operation traceSBC Session

During failover, the *onex_server* contains the FQDN of secondary portal and the *backup_ipoffice_server* contains *0.0.0.0*.

```
                                    203.0.113.31:5061 ──TLS─► 203.0.113.200:61517

SIP/2.0 200 OK
From: <sips:2000@example.com>;tag=-1964e607599d28ec5e8825b8_F2000203.0.113.200
To: <sips:2000@example.com>;tag=66f598546977b5b1
CSeq: 26 REGISTER
Call-ID: 1_4eafcc8-25f80b6b5e8825c0_R@203.0.113.200
Contact: <sips:2000@135.123.85.107:61797;transport=tls>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,REFER,NOTIFY,INFO,SUBSCRIBE,REGISTER,PUBLISH
Supported: timer,vnd.avaya.ipo
User-Agent: IP Office 10.1.0.0.0 build 237
Via: SIP/2.0/TLS 203.0.113.200:61703;branch=z9hG4bK6_4fd0377-76cd9ffa5e9a3ba4_R2000
Expires: 180
Date: Wed, 23 Aug 2017 07:24:09 GMT
Server: IP Office 10.1.0.0.0 build 237
Content-Type: application/vnd.avaya.ipo
Content-Length: 538

<ipo>
onex_server="onexsec.example.com";
onex_server_port="8080";
xmpp_server_port="5222";
server_onex_secure_port="9443";
username="dome";
username_twin="&0.dome";
voicemail_collect="VM.2000";
video="1";
obtain_contacts_from_ipo="0";
conferencing="1";
conf_server="ConfServer@iposec.example.com";
conf_server_adhoc="ConfAdhoc";
transfer="1";
extended_mwi="1";
video_capable="1";
blind_transfer="1";
auto_ans="1";
change_password="1";
xmpp_group="1";
backup_ipoffice_server="0.0.0.0";
```

Chapter 10.
Document History

10. Document History

Date	Issue	Change Summary
3rd March 2018	03a	Update for IP Office Release 11.0.
22nd May 2018	03b	• J169 and J179 missing from list of supported remote SIP desk phones. • Equinox missing from list of supported remote clients.
22nd August 2018	03c	• Updates for 11.0 SP1 - Support for Vantage phones as remote workers.
9th October 2018	03d	o Minor corrections.
27th February 2019	03e	o Correction: Grooming disabled is the recommendation for SIP phones.
4th April 2019	03f	o SET_STIMULUS_SBC_REG_INTERVAL NoUser source number 59 for phone registration interval for J100 Stimulus phones (J139, J169, J179) to improve operation with non-grooming ASBCE. o J129 added to list of supported remote phones.
10th February 2020	03g	• Screenshot incorrectly showed Grooming enabled.
16th April 2020	03h	• General updates.

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.

Index