Administering Avaya IP Office 11.1.x with Avaya SBCE 10.1.x for Avaya Experience Platform

Abstract

This document describes how to integrate Avaya IP Office (IPO) with Avaya Experience Platform (AXP) via Avaya Session Border Controller for Enterprise (SBCE) using a Bring Your Own Carrier (BYOC) hybrid SIP trunk for SIP calling and Avaya Spaces for contact search. The document does not substitute the Installation or Administration Guides of various products, the focus is on setting up and testing the integration.

Issue 1.1

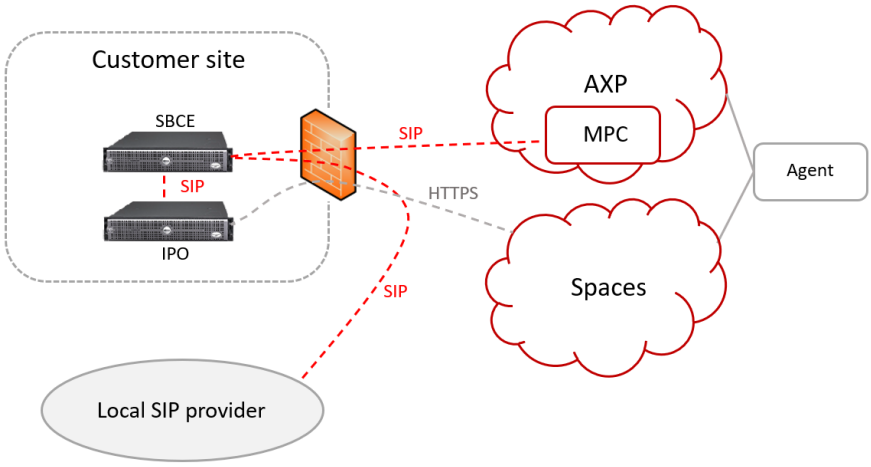
22 August 2023

AVAYA

Contents

Overview

Solution diagram:



IPO can be integrated with AXP using an SBCE where the SIP connection is a BYOC hybrid trunk from AXP perspective. Both internal (between AXP and IPO) and external (between AXP and PSTN) calls will use this BYOC hybrid trunk.

Customer's existing PSTN carrier can be integrated with AXP via the BYOC hybrid SIP trunk which is established between the on-premises SBCE and Media Processing Core (MPC) component of AXP. The customers' carrier can be connected directly to the SBCE (SIP) or via IPO (ISDN), in this example we will use SIP carrier connected to SBCE. Configuration of the carrier side trunk is vendor and carrier specific, and it is out of scope of this document.

Inbound call arrives from customer's carrier directly to SBCE. The SBCE, based on the called party number, sends the INVITE either to MPC where the SIP side of the AXP call terminates or to IPO.

The AXP agent will dial full E.164 numbers to call PSTN and will use Corporate Contact Widget (CCW) to call IPO extensions. Outbound SIP INVITE is sent by MPC to SBCE which forwards it either to IPO or to the customer's local carrier. The outbound caller ID will be the BYOC number which is selected on AXP under the voice channel.

CCW is a component of the agent's Workspaces client which connects to Avaya Spaces for contact lookup. The contacts are synchronized by IPO to Avaya Spaces.

Prerequisites

SBCE

SBCE is already installed, licensed and carrier side trunk is configured.

IPO

IPO is already installed, initialized, licensed and users are configured.

Spaces

Avaya Spaces company has already been created and domain has been verified. Details can be found at https://documentation.avaya.com/bundle/IPOfficeWorkplaceInstall/page/Verifiying_the_Company_Domain.html

AXP

Avaya Spaces integration is enabled on the tenant

Firewall configuration

1. Allow outbound traffic to **accounts.avayacloud.com** on port **TCP 443**
2. Allow Layer 3 NAT only, disable all SIP aware functionality, ALG, etc.
3. Forward the following ports to the B1 interface of the SBCE. If for any reason you would like to use different ports for signaling and media, make sure to use those ports on signaling and media interfaces of the SBCE as well.

TCP	5061	SIP signaling (TLS)
UDP	35000-40000	Media (SRTP)

4. Whitelist the following IP addresses:

   Signaling:

Region	**SRV**	**IP**
North America	sbc-nacentral.mpaas.avayacloud.com	34.75.57.131 35.190.184.83
Europe Central (EU)	sbc-eucentral.mpaas.avayacloud.com	34.159.231.102 35.234.123.201
Europe West (UK)	sbc-euwest.mpaas.avayacloud.com	34.105.218.189 35.246.34.78
South America	sbc-sabr.mpaas.avayacloud.com	34.95.255.33 35.199.72.147
Asia	sbc-asia.mpaas.avayacloud.com	34.87.164.74 35.198.192.120

   Media:

Region	**IP**
All	155.184.0.0/20 155.184.16.0/22

Certificates

The signaling connection between SBCE and MPC is TLS, so an identity certificate is needed for SBCE. SBCE must have ID certificate signed by a public, 3rd party certificate authority. Obtaining such certificate is out of scope of this document, however we detail how to install the certificate and configure the TLS connection on SBCE.

Certificate Requirements

1. **Algorithm**: SHA256 or SHA384
2. **Key Size**: 2048 or 4096 bits
3. **Key Usage Extensions**: Key Encipherment, Non-Repudiation, Digital Signature
4. **Extended Key Usage**: Client Authentication, Server Authentication
5. **Common Name**: public IP or FQDN of firewall
6. **Subject Alt Name**: public IP or FQDN of firewall
7. **PEM format**

Validate 3rd party Certificate

The procedure to generate such certificate is out of scope of this doc, it is customer's responsibility, but we give an example how to bring it to a format that can be installed on SBCE and IPO. The ID certificates that are installed on SBCE/IPO must contain the full trust chain including all Intermediate CA and the Root CA. This ensures that during TLS handshake, the SBCE/IPO sends the whole trust chain and far-end can verify the ID certificate having only the Root CA in its trust store. This is especially important in case of 3rd party certificates where usually there are multiple Intermediate CAs.

1. Make sure you have the ID certificate from the 3rd party CA in PEM format.
2. Make sure you have the certificates of all Intermediate CA and the Root CA. These can be requested or even publicly downloaded from the 3rd party CA.
3. Make sure you have the private key
4. Upload all files to a Linux box (SBCE for example) using WinSCP
5. Verify if all files are present, let's say a 3rd party provided the following files:

```
# ls
USERTrust.crt  ca_bundle.crt  certificate.crt  private.key
```

6. Verify ID certificate has proper Subject Alternative Name:

```
# openssl x509 -in certificate.crt -text|grep "Subject Alternative" -A 1
            X509v3 Subject Alternative Name:
                IP Address:35.158.xx.xx
```

   NOTE: Subject Alternative Name field has to contain the public IP or FQDN of firewall

7. Create a PEM file that contains the whole chain starting from the ID cert till the Root CA, using above files as example:

```
# cat certificate.crt ca_bundle.crt USERTrust.crt > sbce.pem
```

8. Create a key file which name is the same as the combined certificate above

```
# cp private.key sbce.key
```

9. Verify you have the full trust chain in sbce.pem:

```
# openssl storeutl -noout -text -certs sbce.crt|grep "Subject:\|Issuer:"
        Issuer: C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
        Subject: CN=35.158.xx.xx
        Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust
RSA Certification Authority
        Subject: C=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
        Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust
RSA Certification Authority
```

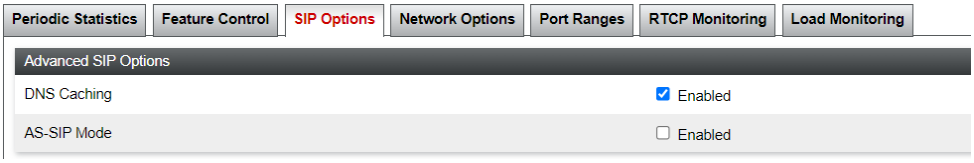
```
        Subject: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network,
CN=USERTrust RSA Certification Authority
```

10. Download **sbce.pem** and **sbce.key** files to the PC

Configuring SBCE

AS-SIP Mode

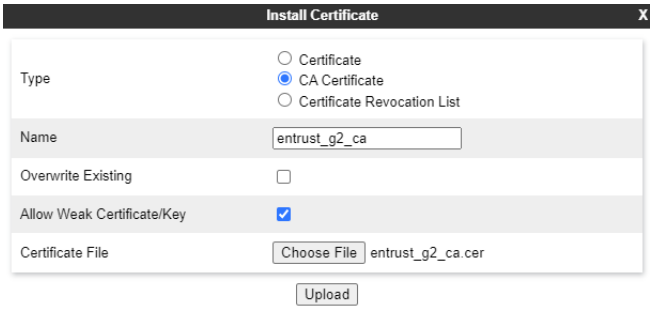
1. Go to **Network & Flows / Advanced Options**, select **SIP Options** tab
2. Make sure **AS-SIP Mode** is **not** Enabled



MPC Certificate Authority chain

Carrier Engineering team will provide the trust chain file that contains the root and all intermediate CA certificates.

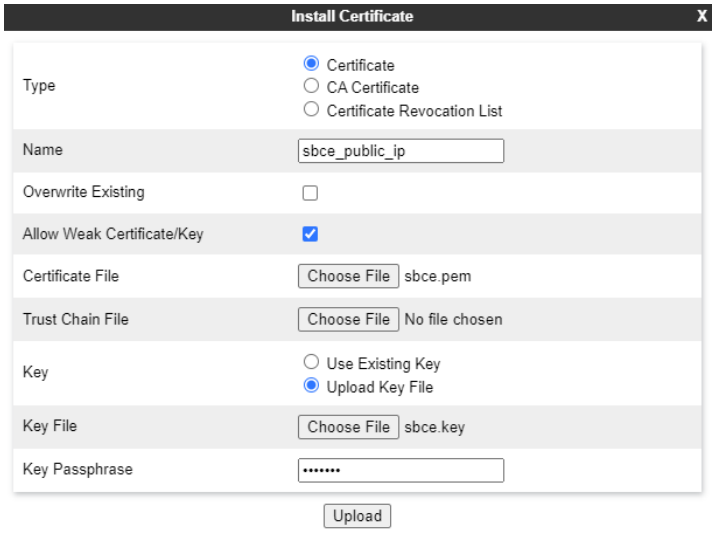
1. Go to **TLS Management / Certificates**
2. Click **Install**
3. Fill the form then click **Upload**
    a. **Type**: **CA Certificate**
    b. **Name**: name for the root CA certificate
    c. Check **Allow Weak Certificate/Key**
    d. **Certificate File**: click **Choose File** and open the file received from Carrier Engineering



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

SBCE Identity Certificate

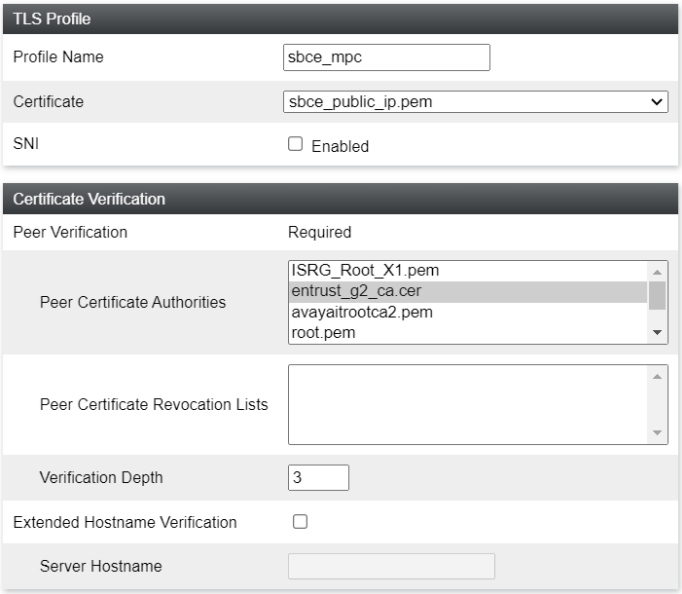
1. Go to **TLS Management / Certificates**
2. Click **Install**
3. Fill the form then click **Upload**
    a. **Type**: **Certificate**
    b. **Name**: name for the SBCE identity certificate
    c. **Certificate File**: click **Choose File** and open **sbce.pem**
    d. **Key:** select **Upload Key File**
    e. **Key File**: click **Choose File** and open **sbce.key**
    f. **Key Passphrase**: password used for encrypting the key



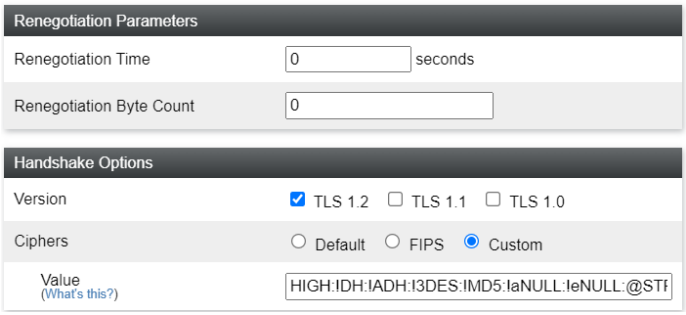
4. Certificate will be displayed, click **Install,** then **Finish**

TLS Profiles

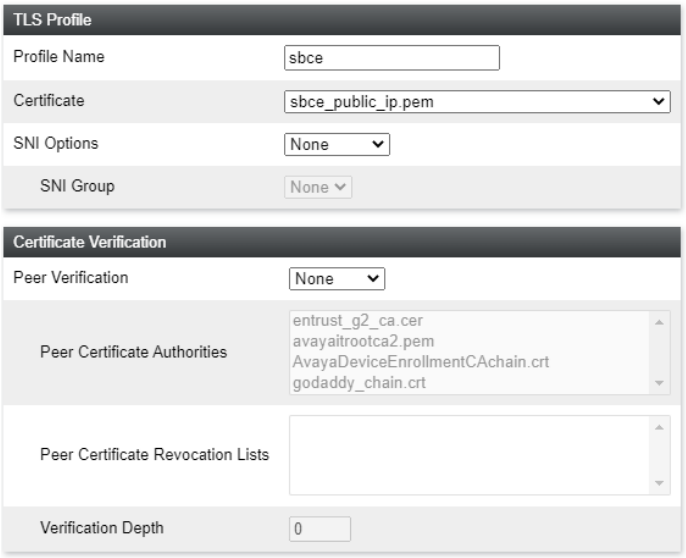
1. Go to **TLS Management / Client Profiles** and click **Add**
2. Enter the following data then click **Next:**
    a. **Profile Name**: name for the TLS profile
    b. **Certificate**: choose the ID certificate
    c. **Peer Certificate Authorities:** select the trust chain of MPC
    d. **Verification Depth**: enter **3**



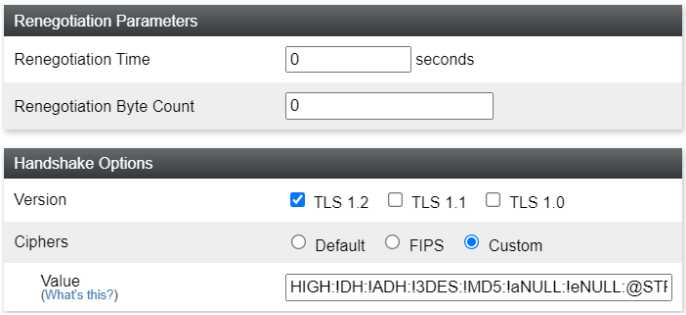
3. Enable **TLS 1.2** only, select **Custom** ciphers and set value to **HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STRENGTH**, then click **Finish**



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



6. Enable **TLS 1.2** only, select **Custom** ciphers and set value to **HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STRENGTH**, then click **Finish**



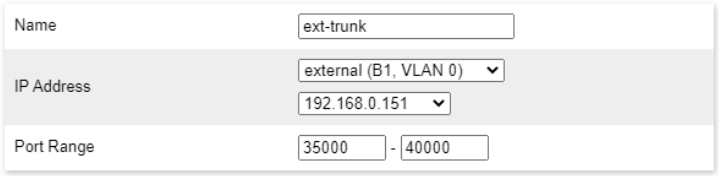
External Interface

1. Go to **Network & Flows / Network Management** and on the **Interfaces** tab make sure B1 interface is enabled
2. Go to **Networks** tab and click **Add**
3. Enter the following data then click **Finish**
    a. **Name:** name of external interface
    b. **Default Gateway:** gateway for external interface
    c. **Subnet Mask:** mask for external interface

d. **Interface:** select **B1**
e. **IP Address:** address of external interface
f. **Public IP:** public IP of firewall

Media Interface

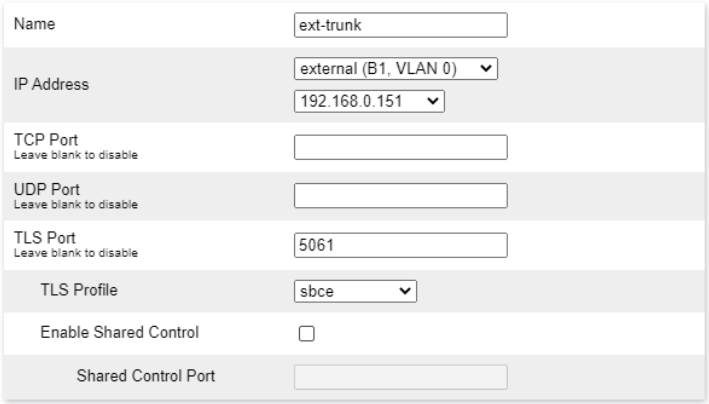
1. Go to **Network & Flows / Media Interface** and click **Add**
2. Set **Name** for external interface, choose **B1** interface and the external **IP Address**, then click **Finish**



NOTE: make sure the Port Range set on this page is forwarded by the Firewall to the IP address used on this page. The Port Range on this page must be the same as the ports opened on Firewall for media.

Signaling Interface

1. Go to **Network & Flows / Signaling Interface** and click **Add**
2. Set **Name** for external interface, choose **B1** interface and the external **IP Address,** remove TCP and UDP port, set **TLS Port**, select **TLS Profile**, then click **Finish**

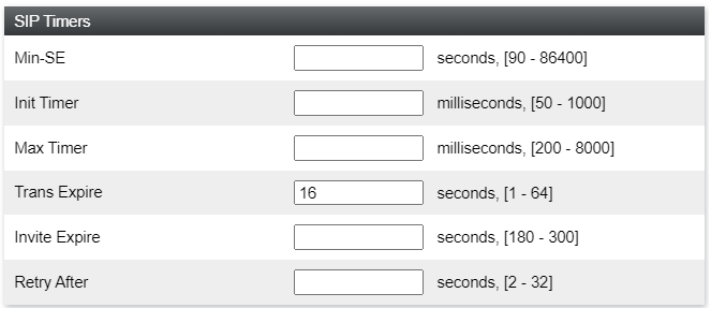


NOTE: make sure the TLS Port set on this page is forwarded by the Firewall to the IP address used on this page. The TLS Port on this page must be the same as the port opened on Firewall for signaling.

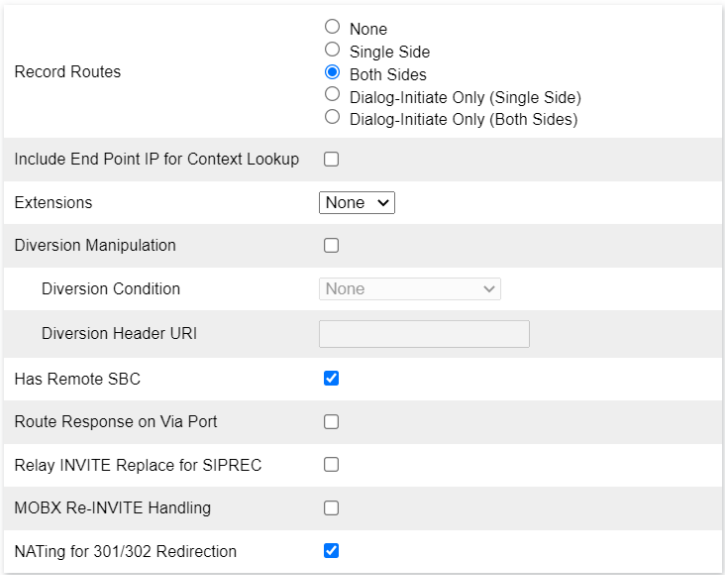
Server Interworking

1. Go to **Configuration Profiles / Server Interworking** and click **Add**

2. Set **Profile Name** to **mpc** then click **Next**
3. Leave default values and click **Next**
4. Set **Trans Expire** to **16** and click **Next**

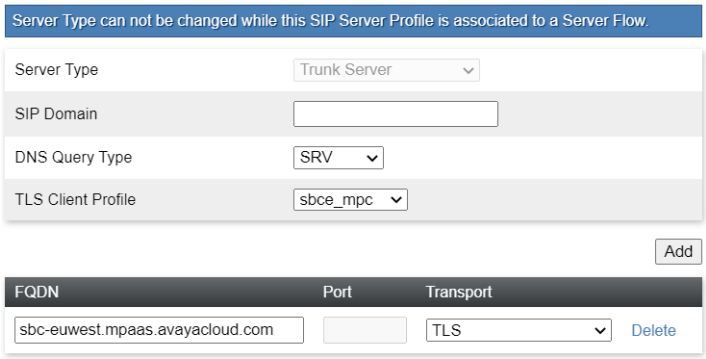


5. Leave default values and click **Next** until the last page
6. On the last page set **Record-Routes** to **Both Sides**, **Has Remote SBC** to **Yes** and **DTMF Support** to **None** then click **Finish**

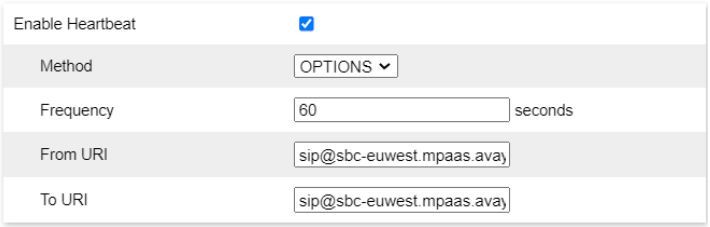


SIP Server

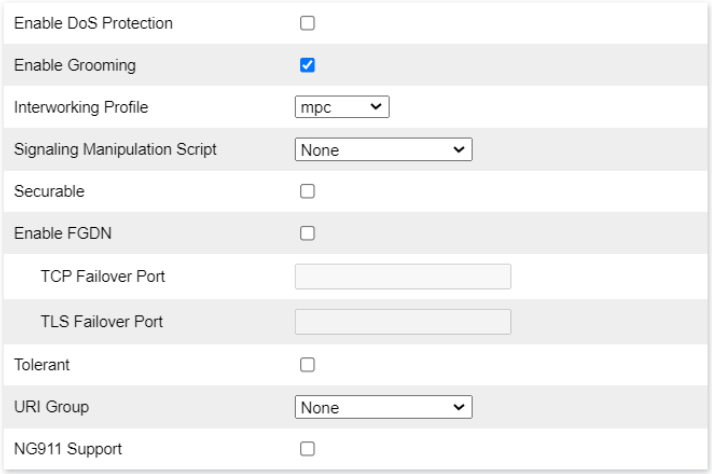
1. Go to **Services / SIP Servers** and click **Add**
2. Set **Profile Name** to **mpc** and click **Next**
3. Set **Server Type** to **Trunk Server**, set **DNS Query Type** to **SRV**, enter the **FQDN** that corresponds to the region of AXP tenant (see in the template document from Carrier Engineering team), set transport **TLS**. At this point **TLS Client Profile** becomes editable, choose the profile, and click **Next**



4. Authentication is not needed, click **Next**
5. **Enable Heartbeat**, set **Method** to **OPTIONS**, **Frequency** to **60** seconds, in the **From URI** and **To URI** fields use **sip@FQDN** where FQDN is the same as at step #3, click **Next**



6. Registration is not needed, click **Next**
7. Ping is not needed, click **Next**
8. Check **Enable Grooming**, set **Interworking Profile** to **mpc**, then click **Finish**



Topology Hiding

1. Go to **Configuration Profiles / Topology Hiding**, select **default** and click **Clone**
2. Set **Clone Name** to **mpc**, then click **Finish**
3. Select **mpc** profile and click **Edit**
4. Set **Replace Action** to **Overwrite** for the **Request-Line, From, To, Refer-To and Referred-By** headers. Set **Overwrite Value** to the FQDN used in SIP Server
5. Click **Finish**

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

End Point Policy Group

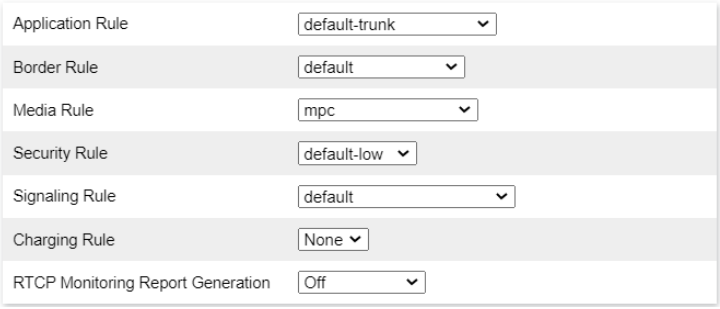
1. Go to **Domain Polices / Media Rules**, select **default-high-enc** and click **Clone**
2. Set **Clone Name** to **mpc**, then click **Finish**
3. Select **mpc** rule and on the **Encryption** tab click **Edit**
4. Fill the form as seen below and click **Finish**

Audio Encryption	
Preferred Format #1	SRTP_AES_256_CM_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	☑
MKI	☐
Lifetime Leave blank to match any value.	2^
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

Video Encryption	
Preferred Format #1	SRTP_AES_256_CM_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	☑
MKI	☐
Lifetime Leave blank to match any value.	2^
Interworking	☑
Symmetric Context Reset	☑
Key Change in New Offer	☐

Miscellaneous	
Capability Negotiation	☐

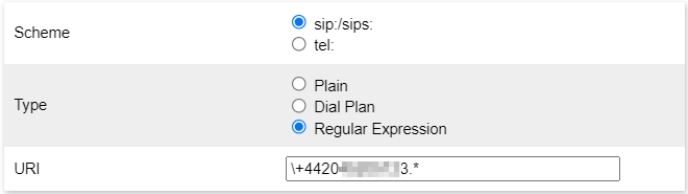
5. Go to **Domain Polices / End Point Policy Groups**, and click **Add**, set name to **mpc**
6. Set **Application Rule** to **default-trunk** and **Media Rule** to **mpc**



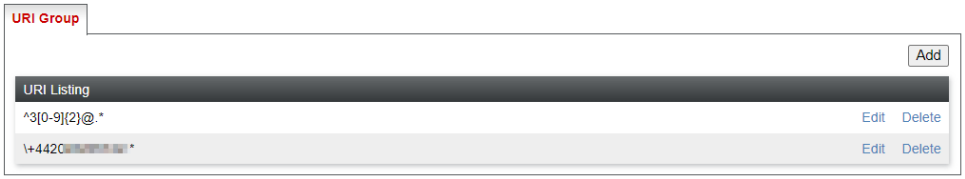
URI Groups

Let's define URI Groups for IPO and MPC which matches the numbers or number ranges of the given components.

1. Go to **Configuration Profiles / URI Groups** and click **Add**
2. Set **Group Name** to **mpc** and click **Next**
3. Set **Scheme** to **sip**, **Type** to **Regular Expression** and **URI** to the expression that matches the number or number range of MPC then click **Finish**. Consider what format the number arrives in. If full E.164 with +, use this example, otherwise tweak it to the proper format.



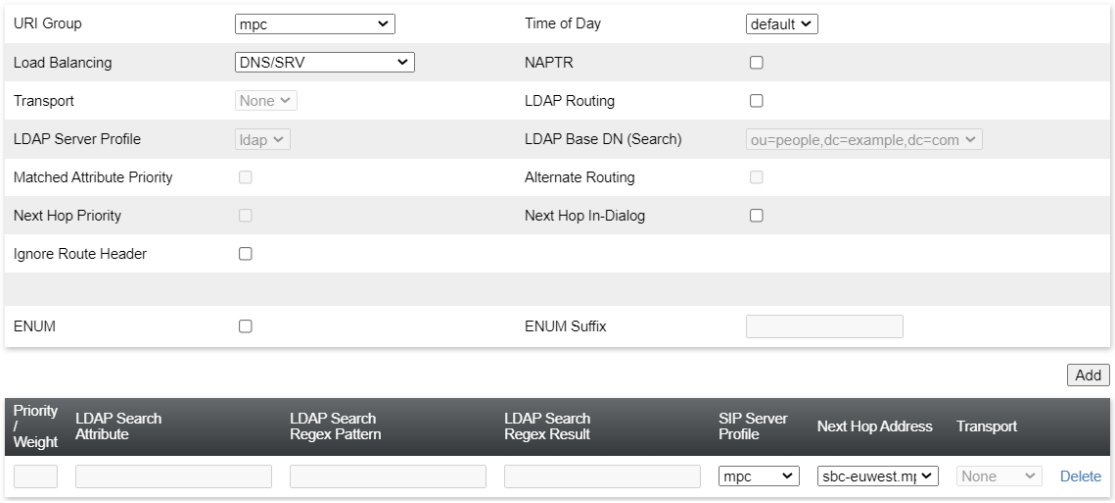
4. If further numbers or number ranges need to be added, select the URI Group and click **Add** to add further entries
5. Repeat the full procedure for IPO with Group Name **ipo**, make sure you add both E.164 range (inbound PSTN calls) and extension range (calls from MPC). For example:



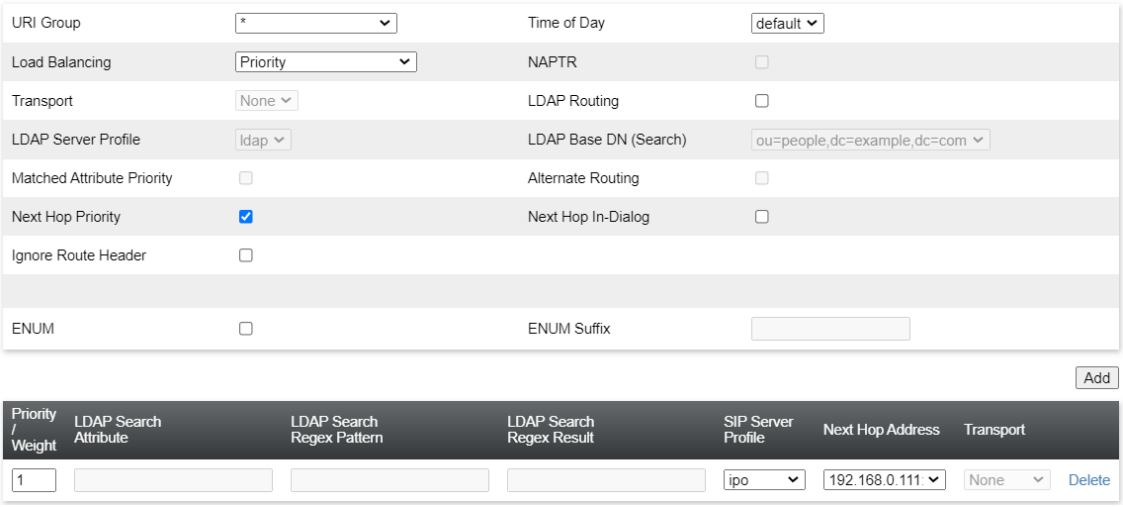
Routing

Define 3 new Routing Rule for the provider, the MPC and IPO using URI Groups. From provider we send calls to MPC, where called party number matches **mpc** URI Group and route anything else to IPO. From MPC we send calls to IPO, where called party number matches **ipo** URI Group and route anything else to provider. From IPO we send calls to MPC, where called party number matches **mpc** URI Group and route anything else to provider. In the Routing Profiles we will use the specific URI Groups to catch the specific numbers to a destination and will use * to catch everything else (default route).

1. Go to **Configuration Profiles / Routing** and click **Add**
2. Set **Profile Name** to **from-provider** and click **Next**
3. Set **URI Group** to **mpc** and **Load Balancing** to **DNS/SRV**
4. Click **Add**, set **SIP Server Profile** and select **Next Hop Address**
5. Click **Finish**



6. Select **from-provider** profile and click **Add** in it
7. Set **URI Group** to ***** and the rest as it was on the original routing profile for IPO, for example:

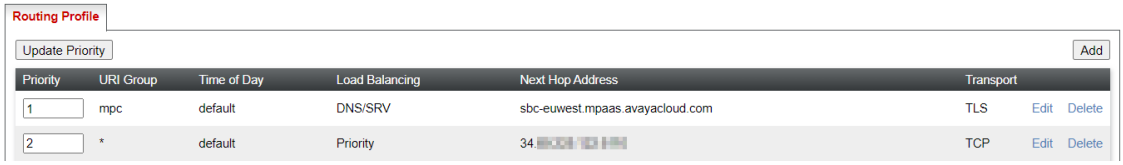


8. Repeat above steps for mpc and ipo using proper URI Groups and destinations

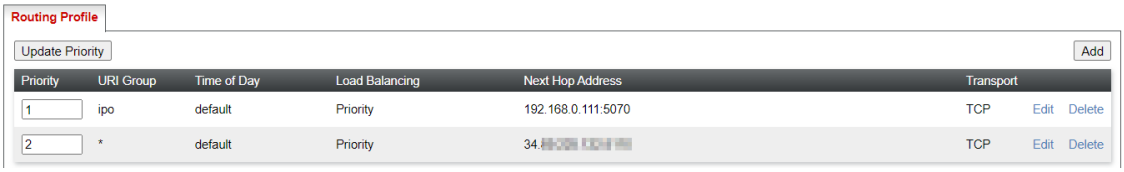
At the end the 3 Routing Profile should look like the following:

from-provider

from-ipo



from-mpc



Server Flows

A brief summary how routing works which may help to understand the server flow configuration used here. For simplicity only IP matching is detailed here, we do not use URI matching in the server flows anyway.

1. Search **SIP Server** that matches the **Source IP** of inbound INVITE
2. Search **Server Flow** for the identified source SIP Server where **Signaling Interface** matches the **Destination IP** of the **inbound INVITE**, so we look for a Server Flow of the source SIP Server where INVITE arrived on **Signaling Interface**
3. Determine destination **SIP Server** using the **Routing Profile** of the identified inbound Server Flow
4. Search **Server Flow** for the identified destination SIP Server where **Received Interface** matches the **Destination IP** of the **inbound INVITE**, so we look for a Server Flow of the destination SIP Server where INVITE came from **Received Interface**

For more detail on routing and policy invocation, refer to SBCE Administration Guide.

Configuration:

1. Go to **Network & Flows / End Point Flows**, select **Server Flows** tab and click **Add**
2. Enter the following data and click **Finish**
    a. **Flow Name**: enter **mpc-ext-trunk** (in this example provider is on the external interface so in the flow name ext-trunk just helps understanding MPC receives call from the interface called ext-trunk)
    b. **SIP Server Profile**: select **mpc**
    c. **Received Interface**: select the interface where the local carrier is connected to, usually internal for a gateway and external for direct sip trunk (in this example provider is on the external interface so we use **ext-trunk**)
    d. **Signaling Interface**: select the external interface (MPC is on external interface)
    e. **Media Interface**: select the external interface (MPC is on external interface)
    f. **End Point Policy Group**: select **mpc**
    g. **Routing Profile**: select the profile that points to local carrier
    h. **Topology Hiding Profile**: select **mpc**
    i. **Link Monitoring from Peer: enabled**

Flow Name	mpc-ext-trunk
SIP Server Profile	mpc
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	ext-trunk
Signaling Interface	ext-trunk
Media Interface	ext-trunk
Secondary Media Interface	None
End Point Policy Group	mpc
Routing Profile	from-mpc
Topology Hiding Profile	mpc
Signaling Manipulation Script	None
Remote Branch Office	Any
Link Monitoring from Peer	☑
FQDN Support	☐
FQDN	

3. Modify the existing IPO server flow and set **Routing Profile** to **from-ipo**
4. Modify the existing provider server flow and set **Routing Profile** to **from-provider**
5. Add a new server flow with identical settings as the existing provider server flow but set **Received Interface** to the internal interface. This flow will ensure to be able to send calls to provider from IPO which is on the internal interface.
6. Add a new server flow with identical settings as the existing MPC server flow but set **Received Interface** to the internal interface. This flow will ensure to be able to send calls to MPC from IPO which is on the internal interface.
7. After above steps the Server Flows should look like this:

SIP Server: ipo

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	ipo	*	ext-trunk	int-trunk	default-low	from-ipo	View Clone Edit Delete

SIP Server: mpc

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	mpc-ext-trunk	*	ext-trunk	ext-trunk	mpc	from-mpc	View Clone Edit Delete
2	mpc-int-trunk	*	int-trunk	ext-trunk	mpc	from-mpc	View Clone Edit Delete

SIP Server: provider

Update

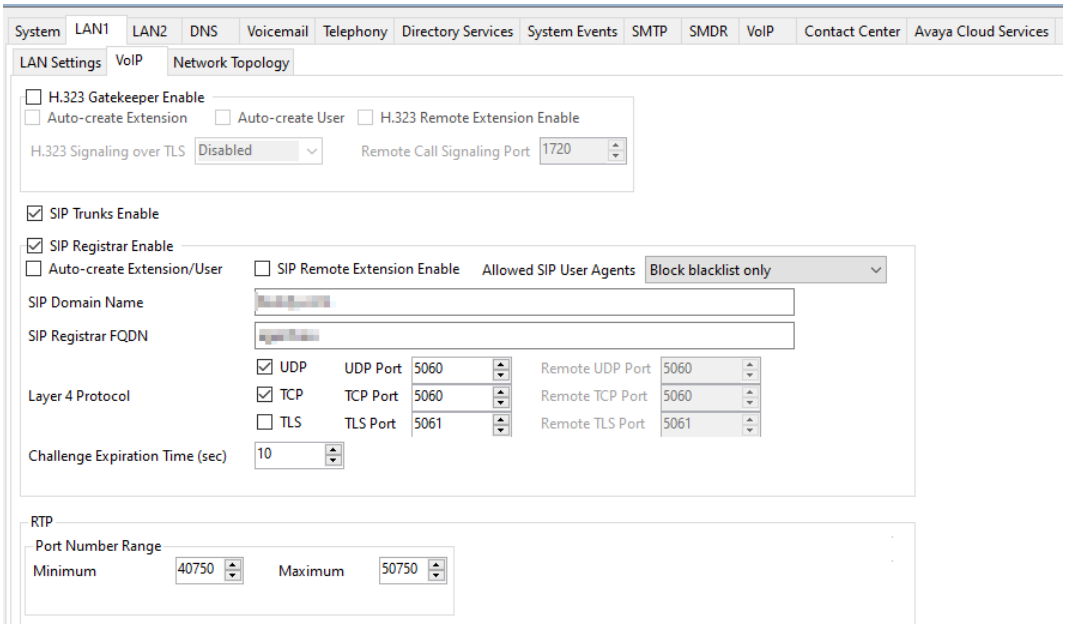
Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile	
1	provider-ext-trunk	*	ext-trunk	ext-trunk	trunk	from-provider	View Clone Edit Delete
2	provider-int-trunk	*	int-trunk	ext-trunk	trunk	from-provider	View Clone Edit Delete

Configuring IPO

VoIP Setup

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

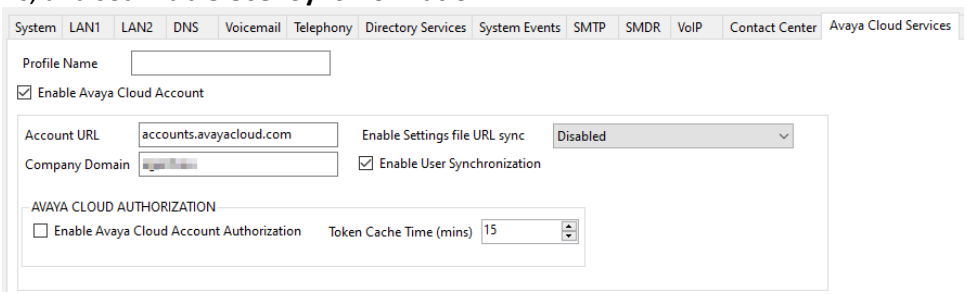
2. Under **LAN1 / VoIP** tab make sure **SIP Trunks Enable** is checked and RTP ports are on the default **40750** and **50750**. The SIP Registrar related configuration are needed only if SIP phones are registered on IPO.



Avaya Cloud Services

This configuration is essential to synchronize IPO users to Avaya Spaces

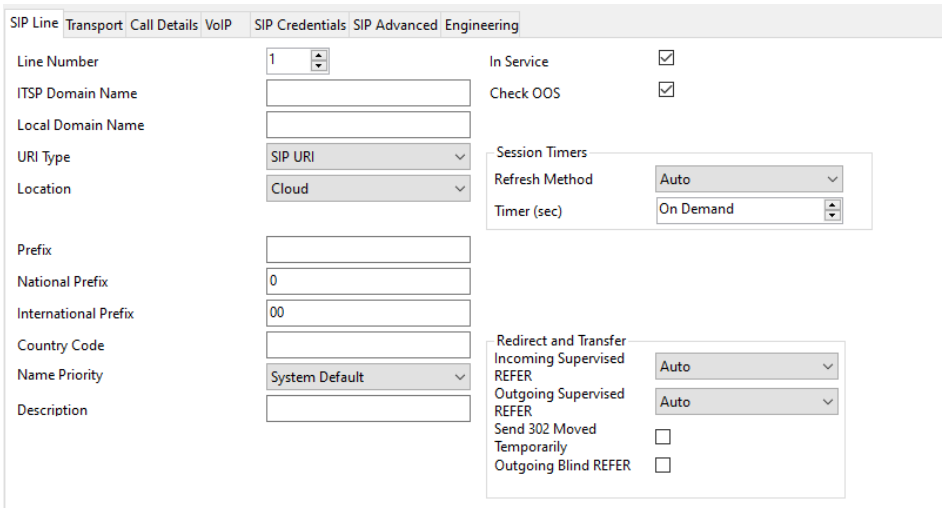
1. Expand the IP Office element under **Solution** and select **System**
2. On the **Avaya Cloud Services** tab make sure **Enable Avaya Cloud Account** is checked, set **Company Domain** to the same as in Avaya Spaces under Manage Companies / Company Profile / Domains, and set **Enable User Synchronization**.



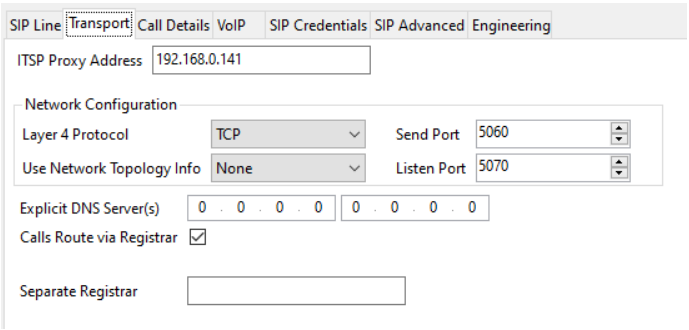
SIP Line

We just detail one possible line configuration, exact configuration like encryption, transport, ports, codecs, etc. are irrelevant from the integration point of view as SBCE will take care of the proper interface to MPC.

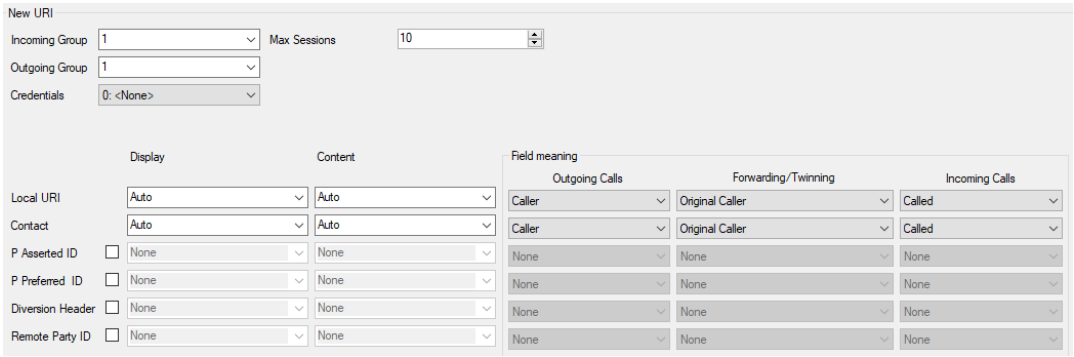
1. Under **Lines** add a new **SIP Line**
2. **SIP Line** tab



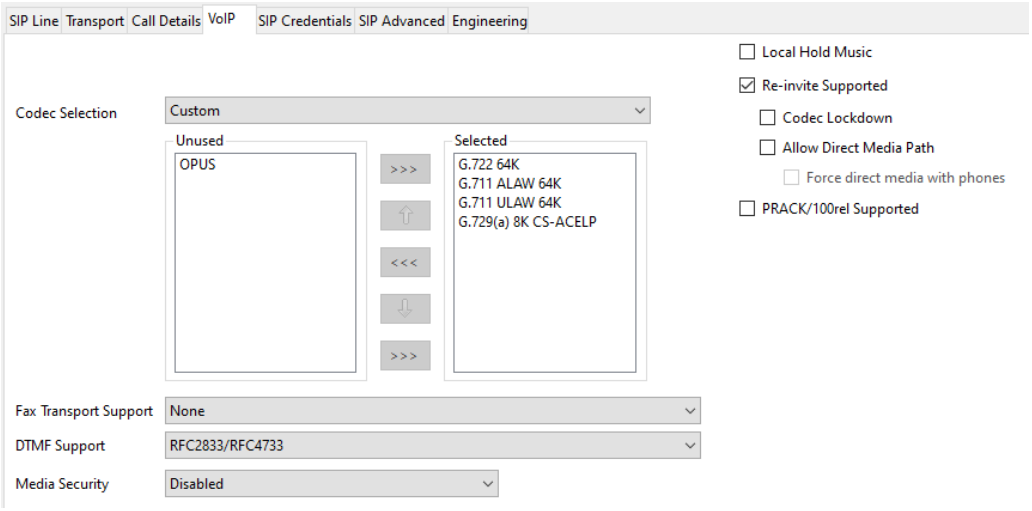
3. On the **Transport** tab set **ITSP Proxy Address** to the SBCE internal interface, set **Layer 4 Protocol** to **TCP**, **Listen Port** to **5070**



4. On the **Call Details** tab click **Add** in the **SIP Uri** section and set:
   a. **Incoming Group**: set to the same as the Line ID on SIP Line tab
   b. **Outgoing Group**: set to the same as the Line ID on SIP Line tab
   c. **Max Sessions**: maximum concurrent sessions
   d. **Local URI and Contact**: Auto



5. On the **VoIP** tab set:
   a. **Codec Selection**: **Custom** and set codecs
   b. **Re-Invite Supported**: enable
   c. **Fax Transport Support**: T38 if IPO sends any fax to PSTN, otherwise set None
   d. **DTMF Support**: RFC2833
   e. **Media Security**: Disabled

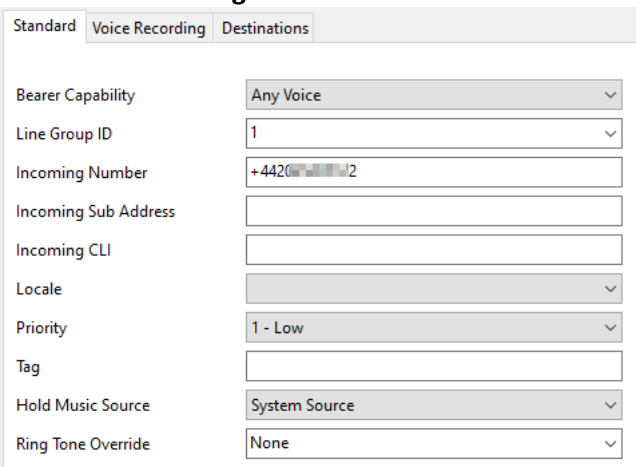


Incoming Call Route

We need to setup ICR for both inbound PSTN calls (E.164 numbers) and inbound calls from AXP (extension numbers). There are multiple ways to do it, refer to IPO Admin guide for details, we just show one example for both E.164 and extension.

E.164:

1. Add new **Incoming Call Route**
2. On the **Standard** tab set **Line Group ID** to the same that was used on SIP Line / Call Details / SIP URI / Incoming Group and in the **Incoming Number** set the full E.164 number

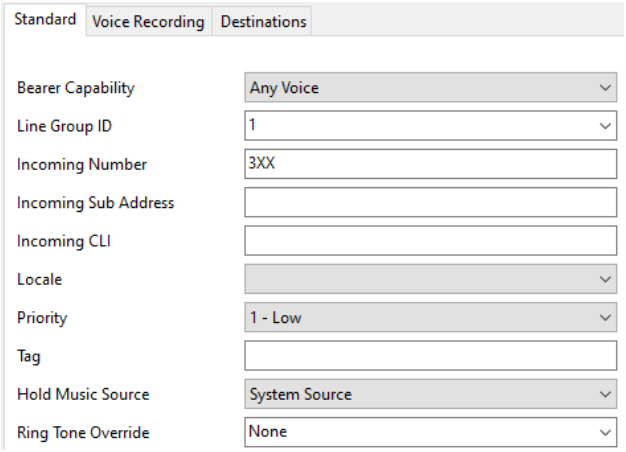


3. On the **Destinations** tab set **Destination** to the given user.

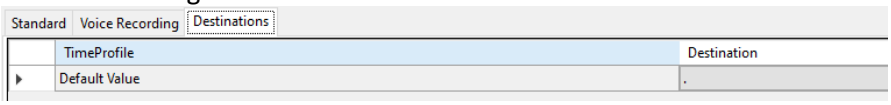
NOTE: This ICR entry is not only used for inbound call but outbound too. IPO will use the Incoming Number field as calling party number when specific user makes an outbound call.

Extension:

1. Add new **Incoming Call Route**
2. On the **Standard** tab set **Line Group ID** to the same that was used on SIP Line / Call Details / SIP URI / Incoming Group and in the **Incoming Number** set the full E.164 number



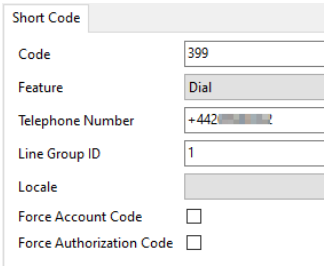
3. On the **Destinations** tab set **Destination** to a dot. This will ensure any call to 3xx number coming from MPC is routed to the given 3xx extension number on IPO.



Short Code

This is needed only if specific AXP numbers should be reachable via a short format. AXP expects full E.164, so we convert a short number to full E.164 number. For example:

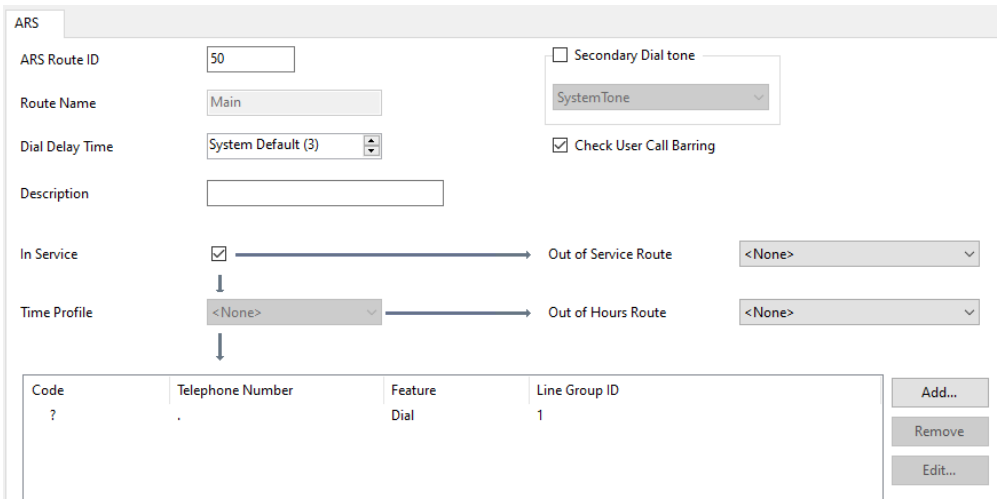
1. Add a new **Short Code**:
    a. **Code**: whatever number is needed to reach a specific AXP number
    b. **Telephone Number**: set the full E.164 AXP number
    c. **Line Group ID**: to the same that was used on SIP Line / Call Details / SIP URI / Outgoing Group



ARS

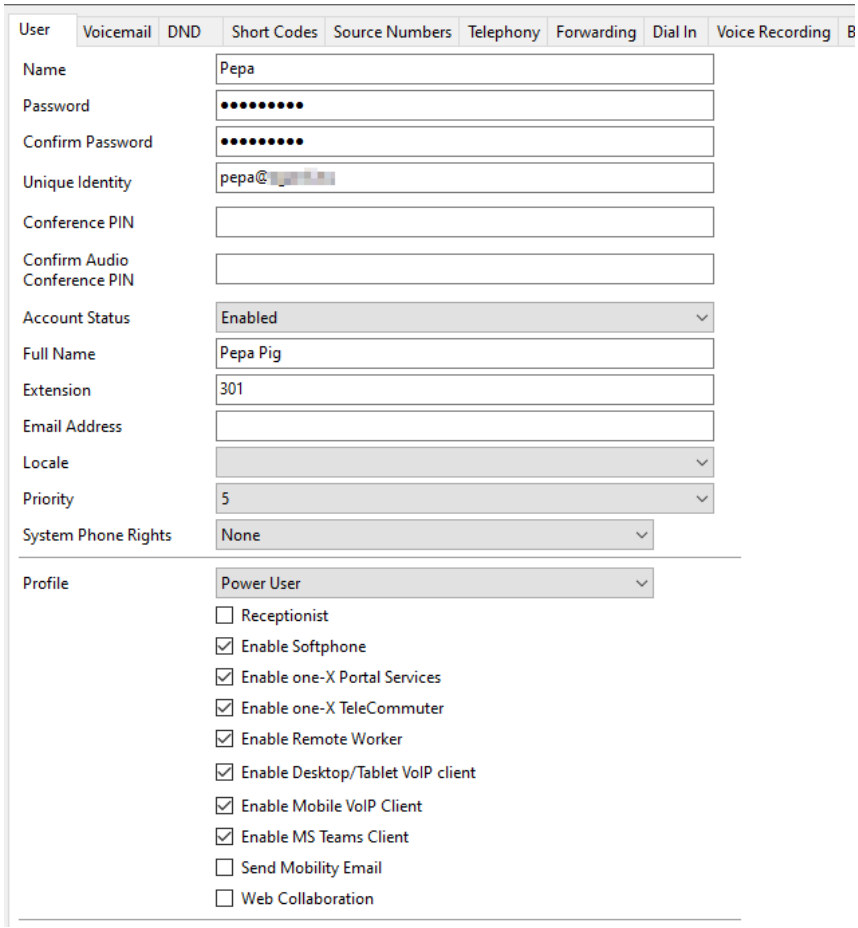
Needed for PSTN dialing and/or to reach MPC via full E.164 number. There are many ways to this this, we just use a 'catch all' config where any numbers that are not local extensions or short codes are routed to PSTN line.

1. Edit the Main ARS and add an entry, where:
    a. **Code**: '**?**' Ensures to match any number
    b. **Telephone number**: '**.**' Ensures to send the whole number
    c. **Feature**: **dial**
    d. **Line Group ID**: same that was used on SIP Line / Call Details / SIP URI / Outgoing Group



User

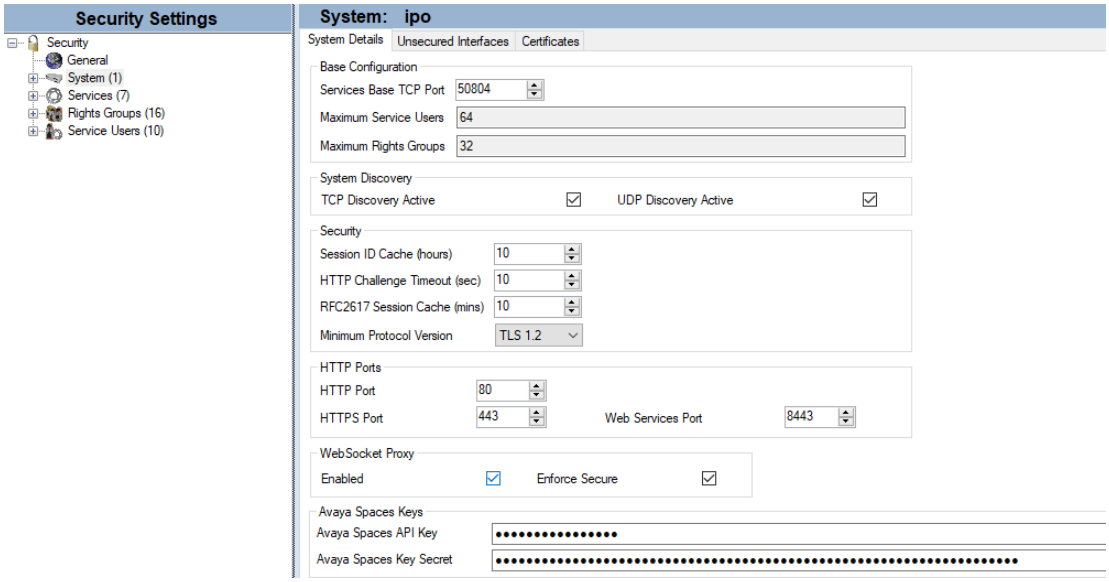
To synchronize an IPO user to Avaya Spaces, make sure the user's Unique Identity has an email where domain matches the Company Domain of Spaces, and one of the following features are enable: Enable one-X Portal Services, Enable Desktop/Tablet VoIP client, Enable Mobile VoIP Client



API key

First create an API key on Spaces, see under **Configuring Spaces / API key**. With the generated key and secret do the followings on IPO:

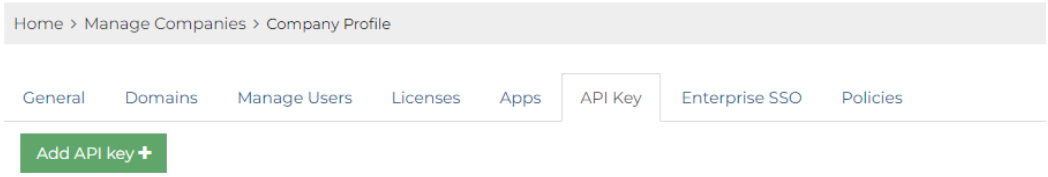
1. Under **Security Setting / System** enter the key and secret



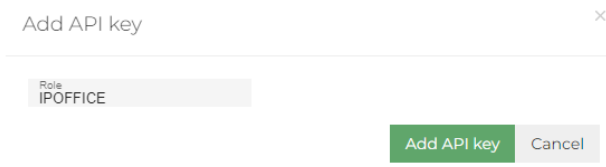
Configuring Spaces

API key

1. Login to **accounts.avayacloud.com** as the company administrator.
2. Go to **Manage Companies / Company Profile / API key** and click **Add API key**



3. Select **IPOFFICE** role, then click **Add API key**



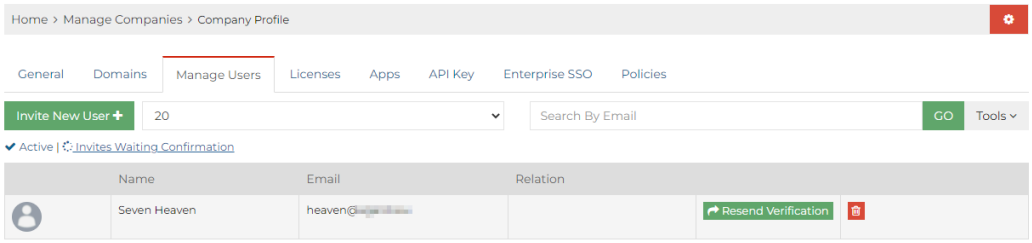
IPO users

When company domain is verified, API key is generated and IPO is configured, users will be automatically synced from IPO to Spaces. Spaces sends welcome email to the new users once automatic synchronization from IPO is done. The users will not be searchable in CCW until the initial setup wizard is

completed by the user who received the welcome email, so it is essential to ensure that all IPO users complete the wizard.

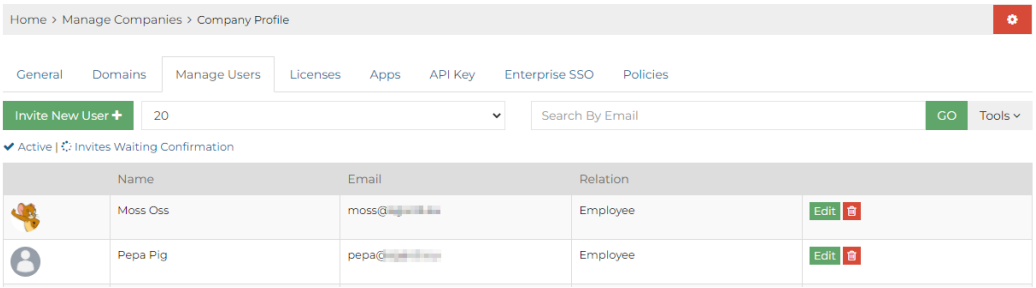
Check the list of users who have not yet completed the wizard:

4. Login to **accounts.avayacloud.com** as the company administrator.
5. Go to **Manage Companies / Company Profile / Manage Users / Invites Waiting Confirmation**

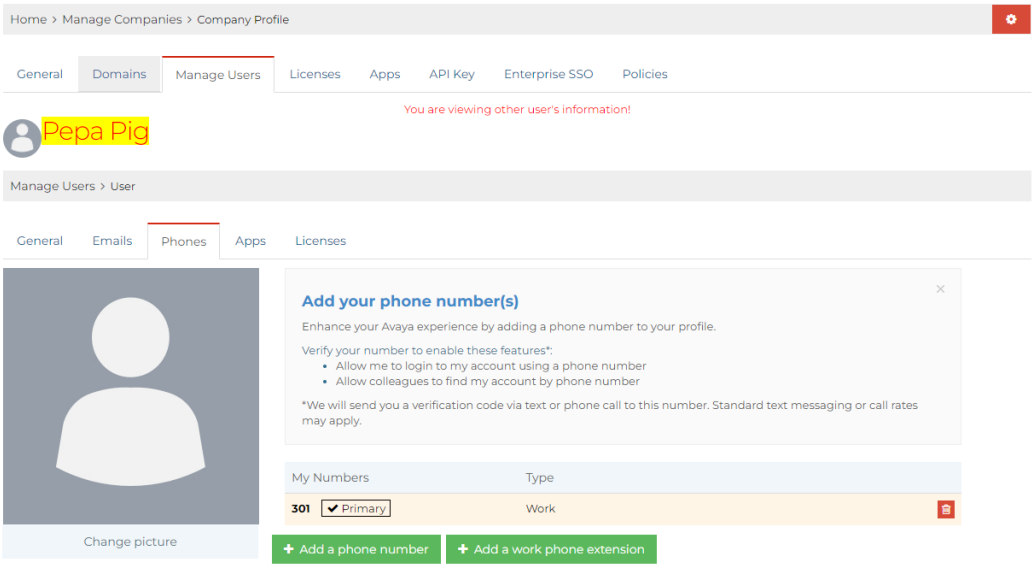


Verify that active IPO users have proper extension number after the sync:

1. Go to **Manage Companies / Company Profile / Manage Users / Active**



2. Edit a user and on Phones tab verify My Numbers



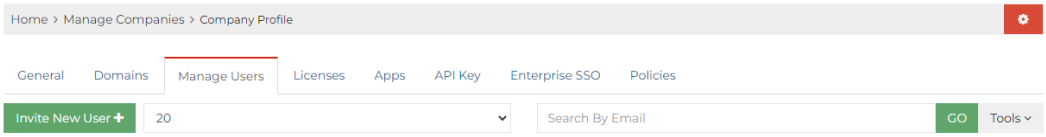
AXP Users

Each AXP agent needs a user account on Avaya Spaces so that CCW can login and search for IPO contacts. These users can be added manually one by one or by importing from a csv file.

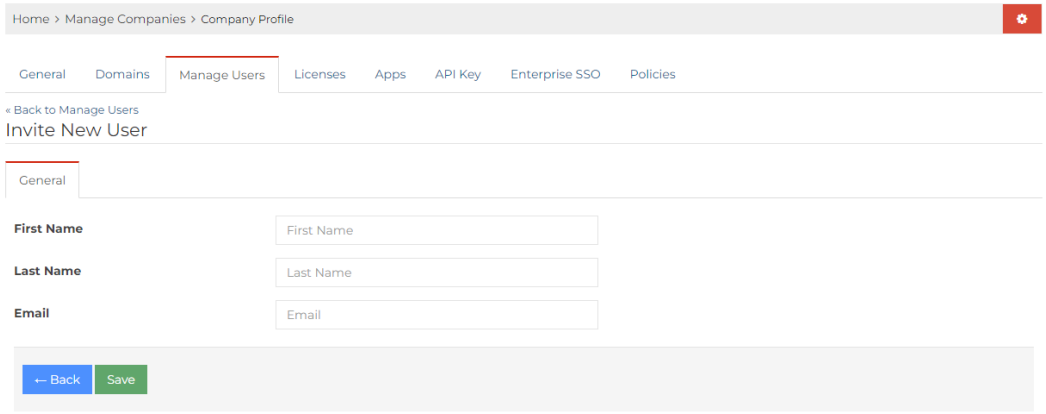
Adding manually:

1. Login to **accounts.avayacloud.com** as the company administrator.

2. Go to **Manage Companies / Company Profile / Manage Users** and click **Invite New User**



3. Set **First Name**, **Last Name** and **Email** then click **Save**. The email must be unique, and the domain must be the company domain used under **Manage Companies / Company Profile / Domains**.



4. Spaces will send welcome email, each AXP agent must complete the wizard to be able to login.

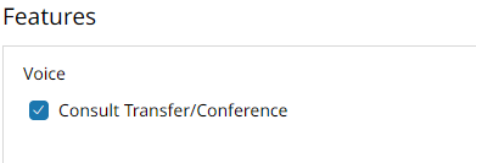
Importing from CSV file:
https://documentation.avaya.com/bundle/IPOfficeWorkplaceInstall/page/Importing_the_CSV_File.html

Configuring AXP

Account

The consult feature must be enabled on the account

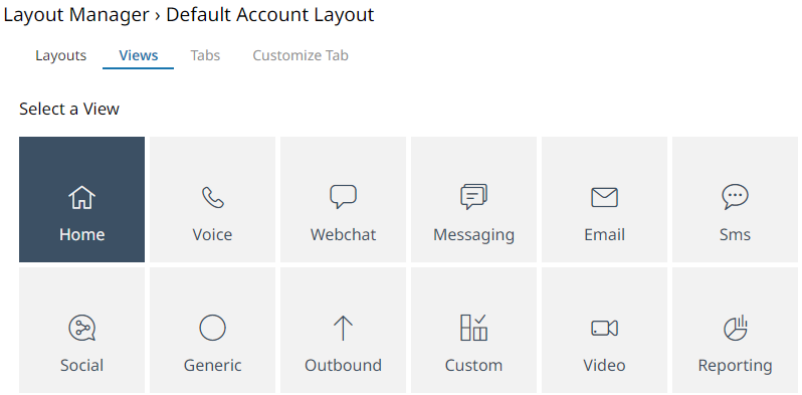
1. Login to AXP as tenant admin
2. On **Administration** go to **Workspaces / Layout Manager**
3. Edit the account and make sure **Consult Transfer/Conference** is enabled under the **Features** section



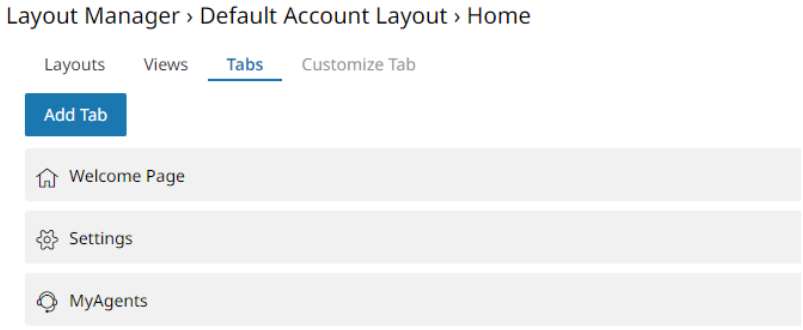
Layout

The Corporate Contact Widget must be added to the Layout

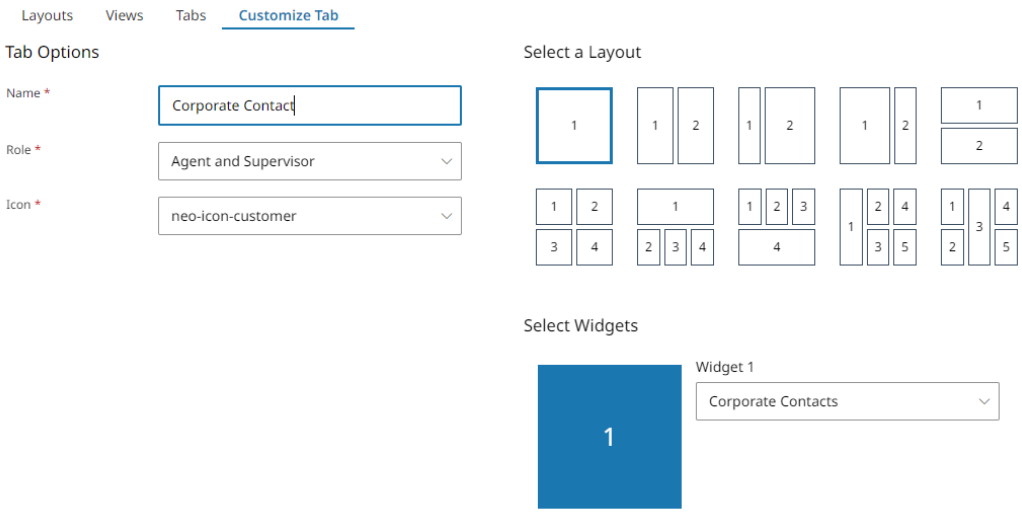
1. Login to AXP as tenant admin
2. On **Administration** go to **Workspaces / Layout Manager**
3. Edit the **Default Account Layout** or other layout used for the given agents
4. Select **Home** view



5. Click **Add Tab**



6. Set the form as seen below. Select Corporate Contacts from the Widget drop down list.



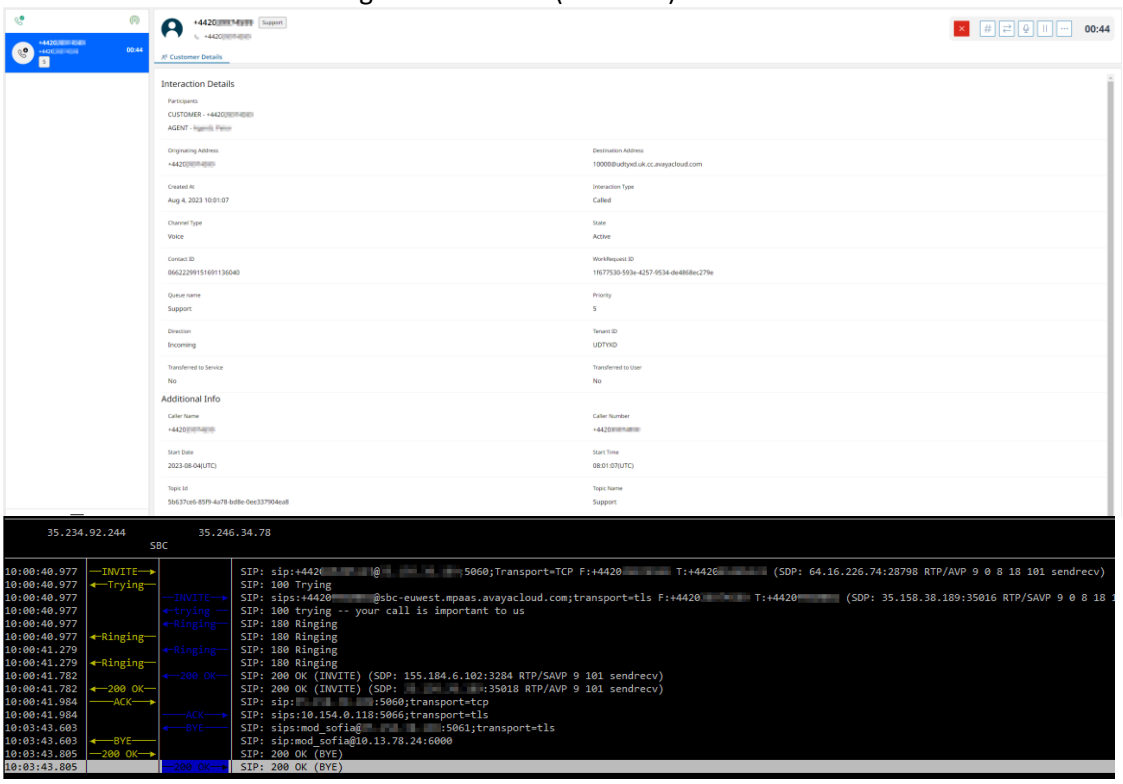
Testing

Summary

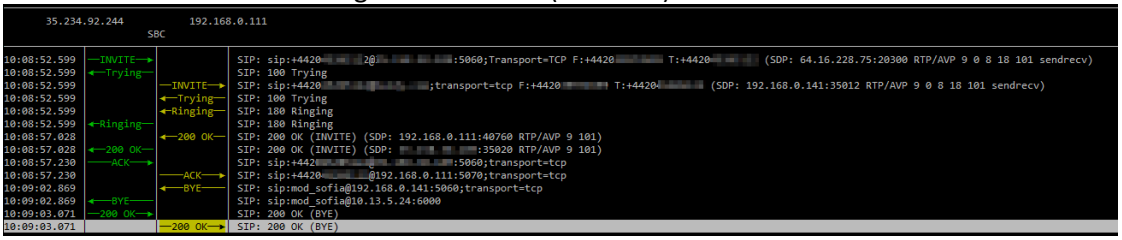
	Test case	Result
1	Inbound PSTN call to AXP using E.164 number	SUCCESS
2	Inbound PSTN call to IPO using E.164 number	SUCCESS
3	Outbound PSTN call from AXP using E.164 number	SUCCESS
4	Outbound PSTN call from IPO using E.164 number	SUCCESS
5	Call from IPO to AXP using E.164 number	SUCCESS
6	Search IPO contact in CCW	SUCCESS
7	Add IPO contact to the Favorites list in CCW	SUCCESS
8	Call IPO user from CCW	SUCCESS
9	Transfer customer to IPO user from AXP using CCW transfer button	SUCCESS
10	Consult IPO user from AXP using CCW consult button completing with transfer	SUCCESS
11	Consult IPO user from AXP using CCW consult button completing with conference	SUCCESS

Details

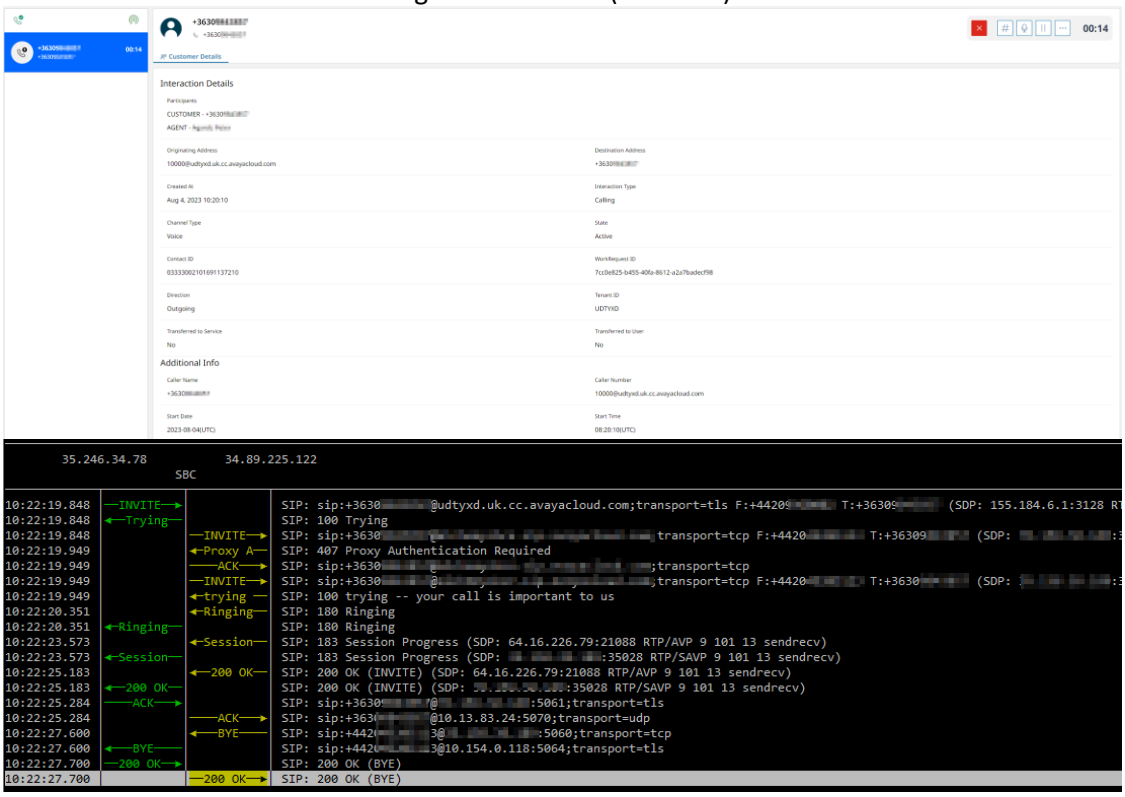
1. Inbound PSTN call to AXP using E.164 number (SUCCESS)



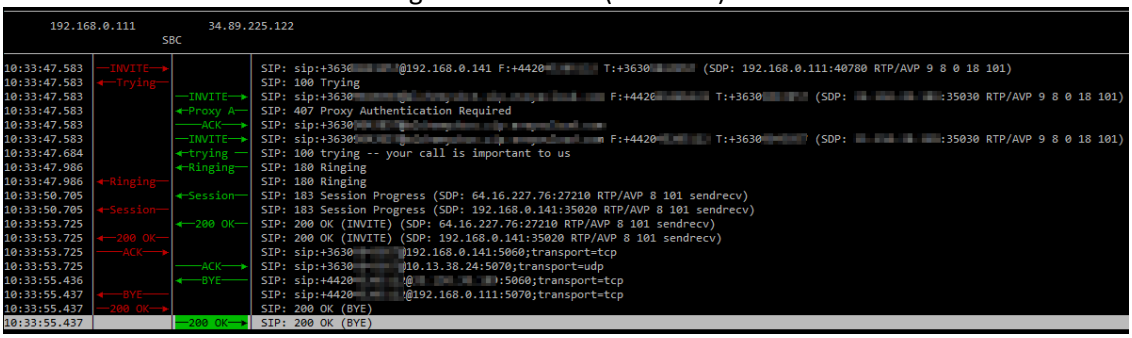
2. Inbound PSTN call to IPO using E.164 number (SUCCESS)



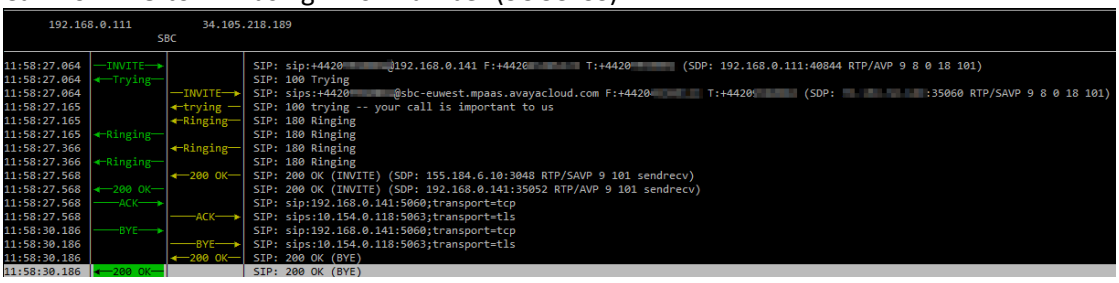
3. Outbound PSTN call from AXP using E.164 number (SUCCESS)



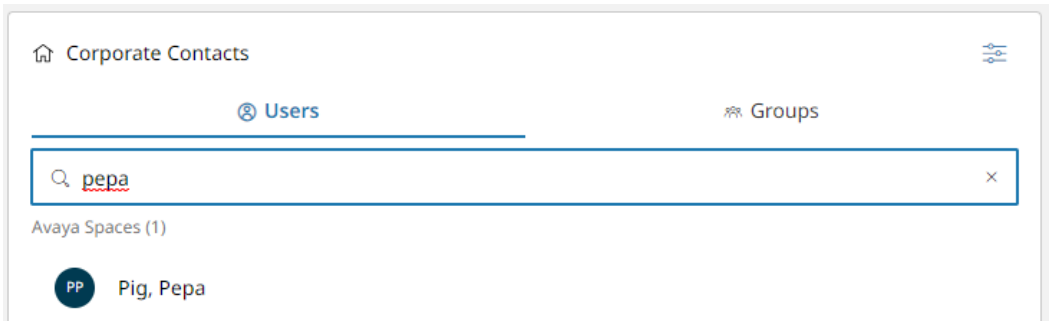
4. Outbound PSTN call from IPO using E.164 number (SUCCESS)



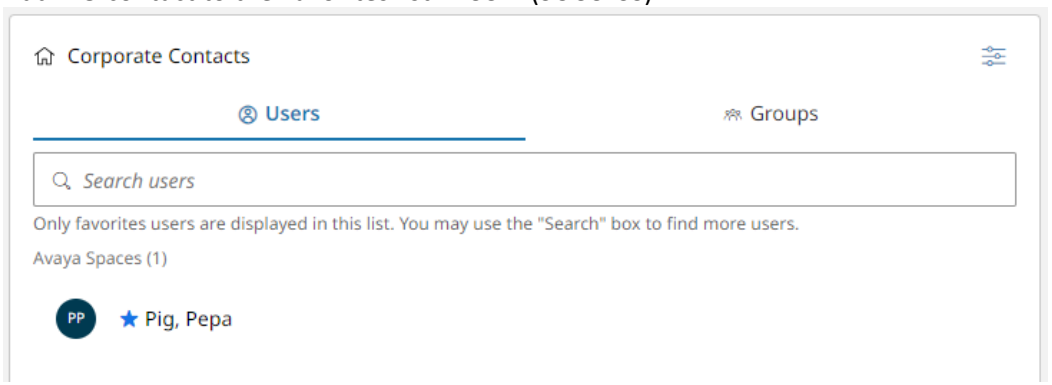
5. Call from IPO to AXP using E.164 number (SUCCESS)



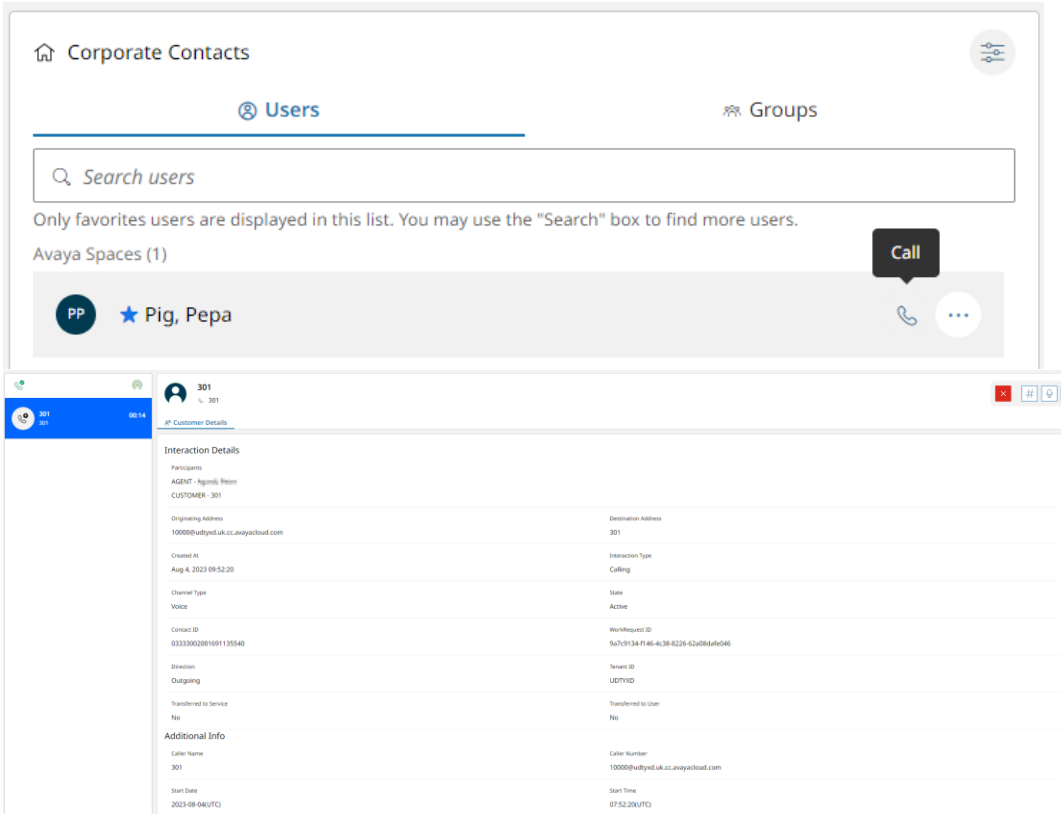
6. Search IPO contact in CCW (SUCCESS)

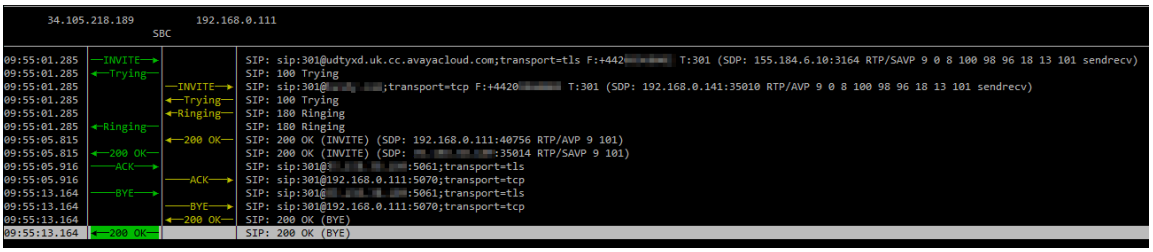


7. Add IPO contact to the Favorites list in CCW (SUCCESS)

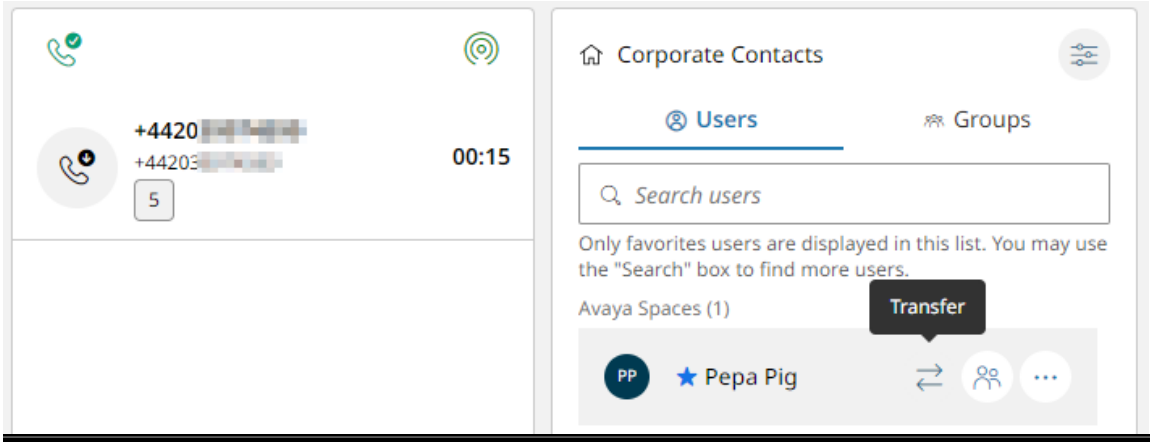


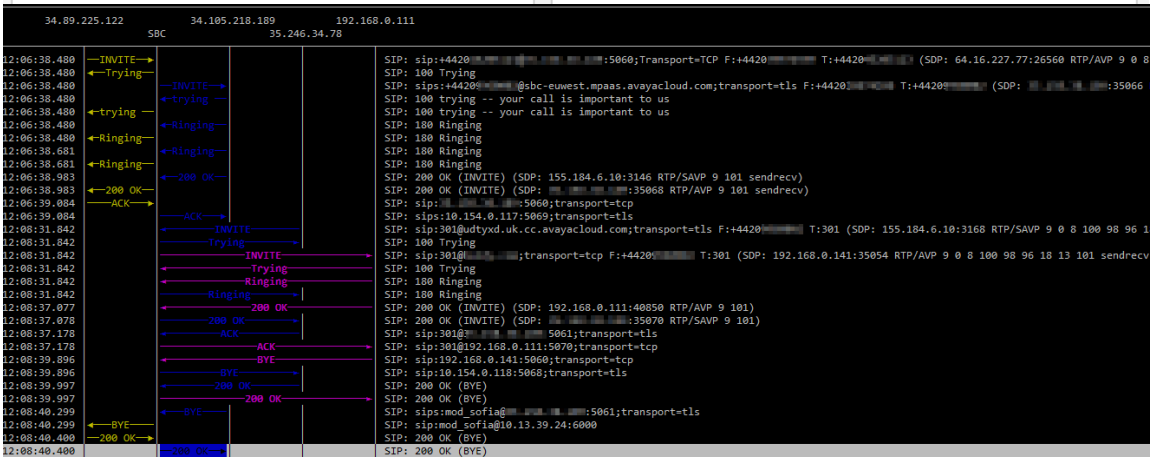
8. Call IPO user from CCW (SUCCESS)



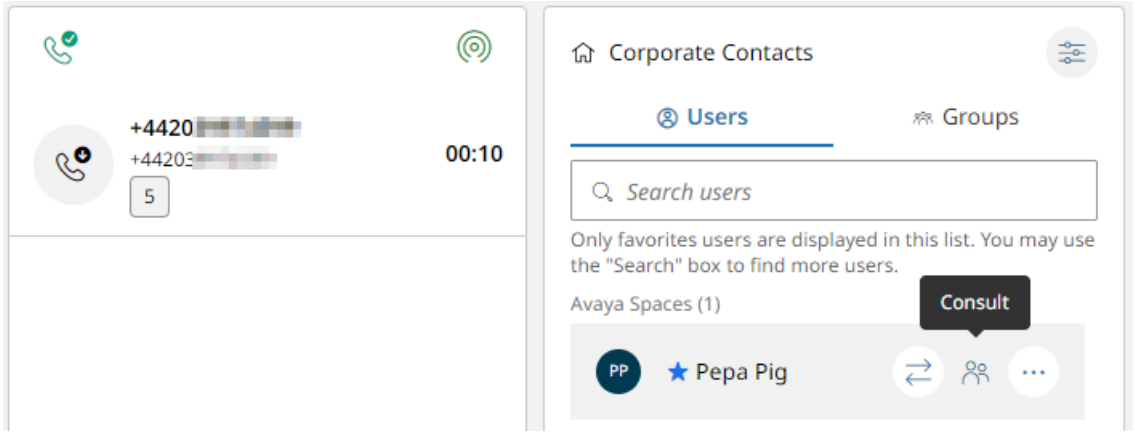


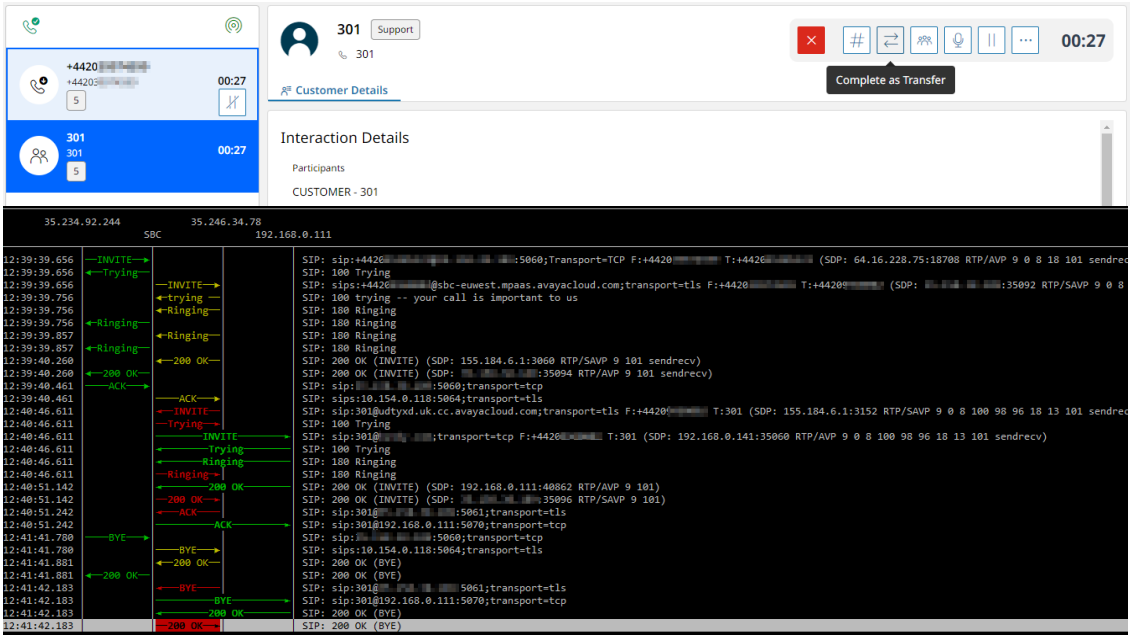
9. Transfer customer to IPO user from AXP using CCW transfer button (SUCCESS)



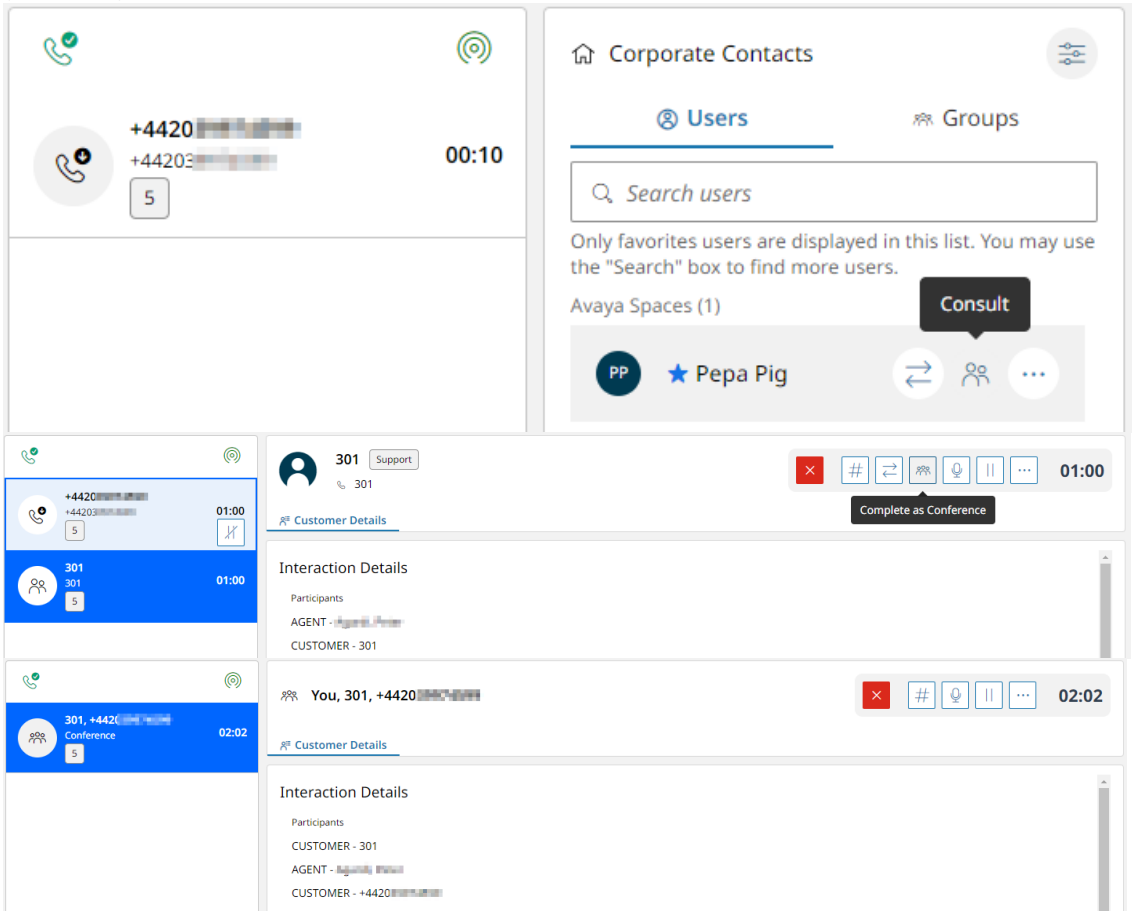


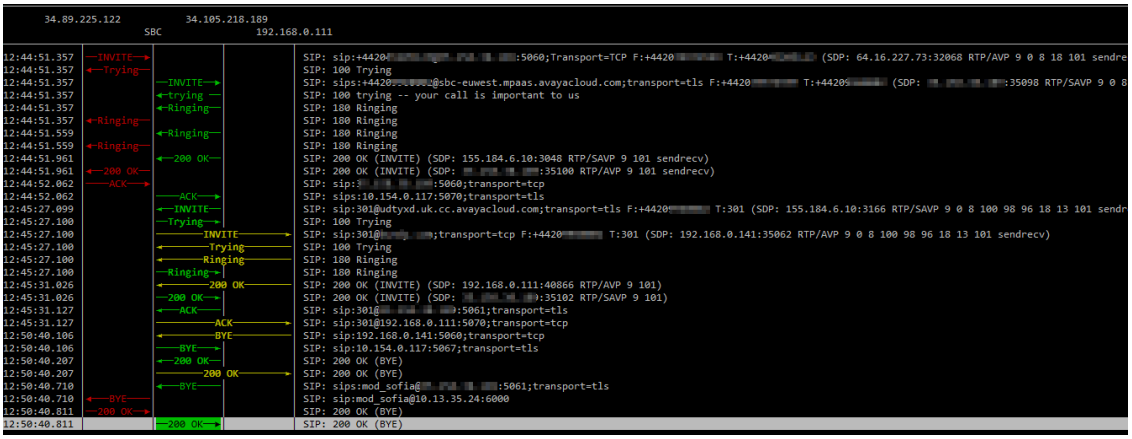
10. Consult IPO user from AXP using CCW consult button completing with transfer (SUCCESS)





11. Consult an IPO user from AXP using CCW consult button completing with a conference (SUCCESS)




34.89.225.122
34.105.218.189
SBC
192.168.0.111
12:44:51.357 INVITE SIP: sip:+4420 :5060;Transport=TCP F:+4420 T:+4420 (SDP: 64.16.227.73:32068 RTP/AVP 9 0 8 18 101 sendre
12:44:51.357 Trying SIP: 100 Trying
12:44:51.357 INVITE SIP: sips:+4420 @sbc-euwest.mpaas.avayacloud.com;transport=tls F:+4420 T:+4420 (SDP: :35098 RTP/SAVP 9 0 8
12:44:51.357 trying SIP: 100 trying -- your call is important to us
12:44:51.357 Ringing SIP: 180 Ringing
12:44:51.357 Ringing SIP: 180 Ringing
12:44:51.559 Ringing SIP: 180 Ringing
12:44:51.559 Ringing SIP: 180 Ringing
12:44:51.961 200 OK SIP: 200 OK (INVITE) (SDP: 155.184.6.10:3048 RTP/SAVP 9 101 sendrecv)
12:44:51.961 200 OK SIP: 200 OK (INVITE) (SDP: :35100 RTP/AVP 9 101 sendrecv)
12:44:52.062 ACK SIP: sip: :5060;transport=tcp
12:44:52.062 ACK SIP: sips:10.154.0.117:5070;transport=tls
12:45:27.099 INVITE SIP: sip:301@udtyxd.uk.cc.avayacloud.com;transport=tls F:+4420 T:301 (SDP: 155.184.6.10:3166 RTP/SAVP 9 0 8 100 98 96 18 13 101 sendr
12:45:27.100 Trying SIP: 100 Trying
12:45:27.100 INVITE SIP: sip:301@ ;transport=tcp F:+4420 T:301 (SDP: 192.168.0.141:35062 RTP/AVP 9 0 8 100 98 96 18 13 101 sendrecv)
12:45:27.100 Trying SIP: 100 Trying
12:45:27.100 Ringing SIP: 180 Ringing
12:45:27.100 Ringing SIP: 180 Ringing
12:45:31.026 200 OK SIP: 200 OK (INVITE) (SDP: 192.168.0.111:40866 RTP/AVP 9 101)
12:45:31.026 200 OK SIP: 200 OK (INVITE) (SDP: :35102 RTP/SAVP 9 101)
12:45:31.127 ACK SIP: sip:301@ :5061;transport=tls
12:45:31.127 ACK SIP: sip:301@192.168.0.111:5070;transport=tcp
12:50:40.106 BYE SIP: sip:192.168.0.141:5060;transport=tcp
12:50:40.106 BYE SIP: sip:10.154.0.117:5067;transport=tls
12:50:40.207 200 OK SIP: 200 OK (BYE)
12:50:40.207 200 OK SIP: 200 OK (BYE)
12:50:40.710 BYE SIP: sips:mod_sofia@ :5061;transport=tls
12:50:40.710 BYE SIP: sip:mod_sofia@10.13.35.24:6000
12:50:40.811 200 OK SIP: 200 OK (BYE)
12:50:40.811 200 OK SIP: 200 OK (BYE)