



# **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



## Contents

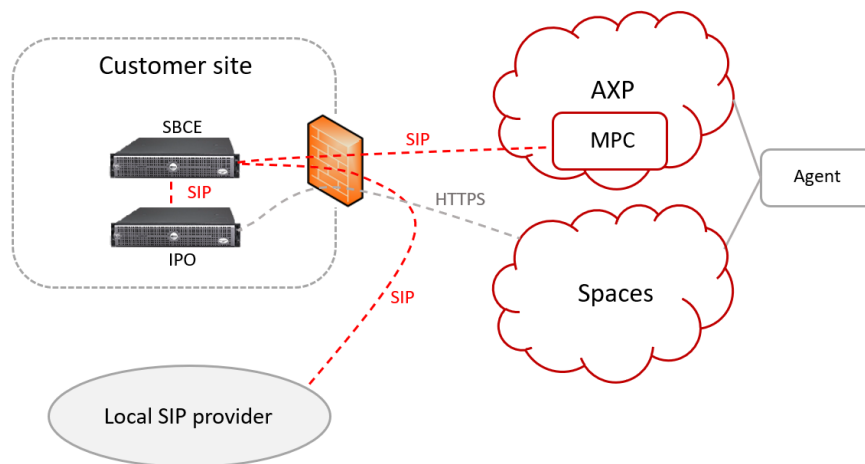
---

Overview .....	- 4 -
Prerequisites .....	- 5 -
SBCE .....	- 5 -
IPO.....	- 5 -
Spaces .....	- 5 -
AXP .....	- 5 -
Firewall configuration .....	- 5 -
Certificates .....	- 6 -
Certificate Requirements .....	- 6 -
Validate 3 <sup>rd</sup> party Certificate.....	- 6 -
Configuring SBCE.....	- 7 -
AS-SIP Mode.....	- 7 -
MPC Certificate Authority chain .....	- 7 -
SBCE Identity Certificate .....	- 7 -
TLS Profiles .....	- 8 -
External Interface.....	- 9 -
Media Interface.....	- 10 -
Signaling Interface.....	- 10 -
Server Interworking .....	- 10 -
SIP Server .....	- 11 -
Topology Hiding .....	- 12 -
End Point Policy Group .....	- 13 -
URI Groups .....	- 14 -
Routing.....	- 14 -
Server Flows .....	- 16 -
Configuring IPO .....	- 17 -
VoIP Setup.....	- 17 -
Avaya Cloud Services .....	- 18 -
SIP Line .....	- 18 -
Incoming Call Route .....	- 20 -
Short Code .....	- 21 -
ARS .....	- 21 -
User .....	- 22 -
API key.....	- 22 -



Configuring Spaces.....	- 23 -
API key.....	- 23 -
IPO users .....	- 23 -
AXP Users .....	- 24 -
Configuring AXP .....	- 25 -
Account .....	- 25 -
Layout.....	- 25 -
Testing.....	- 27 -
Summary .....	- 27 -
Details .....	- 27 -

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 customer's 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/Verifying\\_the\\_Company\\_Domain.html](https://documentation.avaya.com/bundle/IPOfficeWorkplaceInstall/page/Verifying_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, 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> party certificates where usually there are multiple Intermediate CAs.

1. Make sure you have the ID certificate from the 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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

Periodic Statistics	Feature Control	SIP Options	Network Options	Port Ranges	RTCP Monitoring	Load Monitoring
Advanced SIP Options						
DNS Caching						<input checked="" type="checkbox"/> Enabled
AS-SIP Mode						<input type="checkbox"/> 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

Install Certificate	
Type	<input type="radio"/> Certificate <input checked="" type="radio"/> CA Certificate <input type="radio"/> Certificate Revocation List
Name	<input type="text" value="entrust_g2_ca"/>
Overwrite Existing	<input type="checkbox"/>
Allow Weak Certificate/Key	<input checked="" type="checkbox"/>
Certificate File	<input type="button" value="Choose File"/> entrust_g2_ca.cer
<input type="button" value="Upload"/>	

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

**Install Certificate** X

Type:  Certificate  
 CA Certificate  
 Certificate Revocation List

Name: sbce\_public\_ip

Overwrite Existing:

Allow Weak Certificate/Key:

Certificate File: Choose File sbce.pem

Trust Chain File: Choose File No file chosen

Key:  Use Existing Key  
 Upload Key File

Key File: Choose File sbce.key

Key Passphrase: .....

Upload

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**

**TLS Profile**

Profile Name: sbce\_mpc

Certificate: sbce\_public\_ip.pem

SNI:  Enabled

**Certificate Verification**

Peer Verification: Required

Peer Certificate Authorities: ISRG\_Root\_X1.pem, entrust\_g2\_ca.cer, avayaitrustca2.pem, root.pem

Peer Certificate Revocation Lists: [Empty]

Verification Depth: 3

Extended Hostname Verification:

Server Hostname: [Empty]

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



Renegotiation Parameters	
Renegotiation Time	<input type="text" value="0"/> seconds
Renegotiation Byte Count	<input type="text" value="0"/>

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input type="radio"/> Default <input type="radio"/> FIPS <input checked="" type="radio"/> Custom
Value <small>(What's this?)</small>	<input type="text" value="HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STI"/>

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

TLS Profile	
Profile Name	<input type="text" value="sbce"/>
Certificate	<input type="text" value="sbce_public_ip.pem"/>
SNI Options	<input type="text" value="None"/>
SNI Group	<input type="text" value="None"/>

Certificate Verification	
Peer Verification	<input type="text" value="None"/>
Peer Certificate Authorities	<input type="text" value="entrust_g2_ca.cer&lt;br/&gt;avayaitrootca2.pem&lt;br/&gt;AvayaDeviceEnrollmentCAchain.crt&lt;br/&gt;godaddy_chain.crt"/>
Peer Certificate Revocation Lists	<input type="text"/>
Verification Depth	<input type="text" value="0"/>

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

Renegotiation Parameters	
Renegotiation Time	<input type="text" value="0"/> seconds
Renegotiation Byte Count	<input type="text" value="0"/>

Handshake Options	
Version	<input checked="" type="checkbox"/> TLS 1.2 <input type="checkbox"/> TLS 1.1 <input type="checkbox"/> TLS 1.0
Ciphers	<input type="radio"/> Default <input type="radio"/> FIPS <input checked="" type="radio"/> Custom
Value <small>(What's this?)</small>	<input type="text" value="HIGH:!DH:!ADH:!3DES:!MD5:!aNULL:!eNULL:@STI"/>

## External Interface

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

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

Name	external
Default Gateway	192.168.0.190
Network Prefix or Subnet Mask	255.255.255.0
Interface	B1
<input type="button" value="Add"/>	

IP Address	Public IP	Gateway Override	
192.168.0.151	35	Use Default	<input type="button" value="Delete"/>

## 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**

Name	ext-trunk
IP Address	external (B1, VLAN 0)
	192.168.0.151
Port Range	35000 - 40000

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**

Name	ext-trunk
IP Address	external (B1, VLAN 0)
	192.168.0.151
TCP Port <small>Leave blank to disable</small>	
UDP Port <small>Leave blank to disable</small>	
TLS Port <small>Leave blank to disable</small>	5061
TLS Profile	sbce
Enable Shared Control	<input type="checkbox"/>
Shared Control Port	

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**

SIP Timers		
Min-SE	<input type="text"/>	seconds, [90 - 86400]
Init Timer	<input type="text"/>	milliseconds, [50 - 1000]
Max Timer	<input type="text"/>	milliseconds, [200 - 8000]
Trans Expire	<input type="text" value="16"/>	seconds, [1 - 64]
Invite Expire	<input type="text"/>	seconds, [180 - 300]
Retry After	<input type="text"/>	seconds, [2 - 32]

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**

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides <input type="radio"/> Dialog-Initiate Only (Single Side) <input type="radio"/> Dialog-Initiate Only (Both Sides)
Include End Point IP for Context Lookup	<input type="checkbox"/>
Extensions	<input type="text" value="None"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Condition	<input type="text" value="None"/>
Diversion Header URI	<input type="text"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Relay INVITE Replace for SIPREC	<input type="checkbox"/>
MOBX Re-INVITE Handling	<input type="checkbox"/>
NATing for 301/302 Redirection	<input checked="" type="checkbox"/>
DTMF	
DTMF Support	<input checked="" type="radio"/> None-> <input type="radio"/> SIP Notify-> <input type="radio"/> RFC 2833 Relay & SIP Notify-> <input type="radio"/> SIP Info-> <input type="radio"/> RFC 2833 Relay & SIP Info-> <input type="radio"/> Inband->

## 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**

Server Type can not be changed while this SIP Server Profile is associated to a Server Flow.

Server Type	Trunk Server
SIP Domain	
DNS Query Type	SRV
TLS Client Profile	sbce_mpc

Add

FQDN	Port	Transport
sbce-euwest.mpaas.avayacloud.com		TLS

Delete

- Authentication is not needed, click **Next**
- 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**

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	OPTIONS
Frequency	60 seconds
From URI	sip@sbce-euwest.mpaas.avayacloud.com
To URI	sip@sbce-euwest.mpaas.avayacloud.com

- Registration is not needed, click **Next**
- Ping is not needed, click **Next**
- Check **Enable Grooming**, set **Interworking Profile** to **mpc**, then click **Finish**

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	mpc
Signaling Manipulation Script	None
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	
TLS Failover Port	
Tolerant	<input type="checkbox"/>
URI Group	None
NG911 Support	<input type="checkbox"/>

## Topology Hiding

- Go to **Configuration Profiles / Topology Hiding**, select **default** and click **Clone**
- Set **Clone Name** to **mpc**, then click **Finish**
- Select **mpc** profile and click **Edit**
- 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
- 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	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Video Encryption	
Preferred Format #1	SRTP_AES_256_CM_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime Leave blank to match any value.	2^
Interworking	<input checked="" type="checkbox"/>
Symmetric Context Reset	<input checked="" type="checkbox"/>
Key Change in New Offer	<input type="checkbox"/>

Miscellaneous	
Capability Negotiation	<input type="checkbox"/>

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**

Application Rule	default-trunk
Border Rule	default
Media Rule	mpc
Security Rule	default-low
Signaling Rule	default
Charging Rule	None
RTCP Monitoring Report Generation	Off

## 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.

Scheme	<input checked="" type="radio"/> sip/sips: <input type="radio"/> tel:
Type	<input type="radio"/> Plain <input type="radio"/> Dial Plan <input checked="" type="radio"/> Regular Expression
URI	+4420[ ]3.*

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:

URI Group		Add
URI Listing		
*3[0-9]{2}@.*	Edit	Delete
+4420[ ]3.*	Edit	Delete

## 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**



URI Group	mpc	Time of Day	default
Load Balancing	DNS/SRV	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	ldap	LDAP Base DN (Search)	ou=people,dc=example,dc=com
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
				mpc	sbc-euwest.mj	None

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:

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	LDAP Routing	<input type="checkbox"/>
LDAP Server Profile	ldap	LDAP Base DN (Search)	ou=people,dc=example,dc=com
Matched Attribute Priority	<input type="checkbox"/>	Alternate Routing	<input type="checkbox"/>
Next Hop Priority	<input checked="" type="checkbox"/>	Next Hop In-Dialog	<input type="checkbox"/>
Ignore Route Header	<input type="checkbox"/>		
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	LDAP Search Attribute	LDAP Search Regex Pattern	LDAP Search Regex Result	SIP Server Profile	Next Hop Address	Transport
1				ipo	192.168.0.111	None

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

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	mpc	default	DNS/SRV	sbc-euwest.mpaas.avayacloud.com	TLS
2	*	default	Priority	192.168.0.111:5070	TCP

### from-ipo

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
1	mpc	default	DNS/SRV	sbc-euwest.mpaas.avayacloud.com	TLS
2	*	default	Priority	34.199.130.130	TCP

## from-mpc

Priority	URI Group	Time of Day	Load Balancing	Next Hop Address	Transport	
1	ipo	default	Priority	192.168.0.111:5070	TCP	Edit Delete
2	*	default	Priority	34.119.229.124:5070	TCP	Edit Delete

## 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	<input checked="" type="checkbox"/>
FQDN Support	<input type="checkbox"/>
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 <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

SIP Server: mpc						
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 <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
2	mpc-int-trunk	*	int-trunk	ext-trunk	mpc	from-mpc <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

SIP Server: provider						
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 <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>
2	provider-int-trunk	*	int-trunk	ext-trunk	trunk	from-provider <a href="#">View</a> <a href="#">Clone</a> <a href="#">Edit</a> <a href="#">Delete</a>

## Configuring IPO

### VoIP Setup

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

- 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.

The screenshot shows the Avaya configuration interface for the VoIP tab. The 'SIP Trunks Enable' checkbox is checked. Under 'SIP Registrar Enable', the 'SIP Registrar Enable' checkbox is checked, and 'Allowed SIP User Agents' is set to 'Block blacklist only'. The 'SIP Domain Name' and 'SIP Registrar FQDN' fields are populated with redacted text. Under 'Layer 4 Protocol', 'UDP' and 'TCP' are checked, with ports set to 5060. 'Remote UDP Port' and 'Remote TCP Port' are also set to 5060. 'Challenge Expiration Time (sec)' is set to 10. Under 'RTP', 'Port Number Range' is set with a minimum of 40750 and a maximum of 50750.

## Avaya Cloud Services

This configuration is essential to synchronize IPO users to Avaya Spaces

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

The screenshot shows the Avaya configuration interface for the Avaya Cloud Services tab. The 'Enable Avaya Cloud Account' checkbox is checked. The 'Account URL' is set to 'accounts.avayacloud.com'. The 'Company Domain' field is populated with redacted text. The 'Enable Settings file URL sync' dropdown is set to 'Disabled'. The 'Enable User Synchronization' checkbox is checked. Under 'AVAYA CLOUD AUTHORIZATION', the 'Enable Avaya Cloud Account Authorization' checkbox is unchecked, and the 'Token Cache Time (mins)' is set to 15.

## 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.

- Under **Lines** add a new **SIP Line**
- 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

SIP Line Transport Call Details VoIP SIP Credentials SIP Advanced Engineering

Codec Selection: Custom

Unused: OPUS

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

Local Hold Music:

Re-invite Supported:

Codec Lockdown:

Allow Direct Media Path:

Force direct media with phones:

PRACK/100rel Supported:

Fax Transport Support: None

DTMF Support: RFC2833/RFC4733

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

Standard Voice Recording Destinations

Bearer Capability: Any Voice

Line Group ID: 1

Incoming Number: +4420 7599 2

Incoming Sub Address:

Incoming CLI:

Locale:

Priority: 1 - Low

Tag:

Hold Music Source: System Source

Ring Tone Override: None

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

TimeProfile	Destination
▶ Default Value	301 Pepa

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

Standard	Voice Recording	Destinations
Bearer Capability	Any Voice	
Line Group ID	1	
Incoming Number	3XX	
Incoming Sub Address		
Incoming CLI		
Locale		
Priority	1 - Low	
Tag		
Hold Music Source	System Source	
Ring Tone Override	None	

- 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.

Standard	Voice Recording	Destinations
	TimeProfile	Destination
	Default Value	.

## 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:

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

Short Code	
Code	399
Feature	Dial
Telephone Number	+442
Line Group ID	1
Locale	
Force Account Code	<input type="checkbox"/>
Force Authorization Code	<input type="checkbox"/>

## 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.

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



ARS

ARS Route ID: 50

Route Name: Main

Dial Delay Time: System Default (3)

Description:

In Service:  Out of Service Route: <None>

Time Profile: <None> Out of Hours Route: <None>

Secondary Dial tone:  SystemTone

Check User Call Barring:

Code ?	Telephone Number	Feature Dial	Line Group ID
	.		1

Add...  
Remove  
Edit...

## 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

User	Voicemail	DND	Short Codes	Source Numbers	Telephony	Forwarding	Dial In	Voice Recording	B
Name	Pepa								
Password	●●●●●●								
Confirm Password	●●●●●●								
Unique Identity	pepa@								
Conference PIN									
Confirm Audio Conference PIN									
Account Status	Enabled								
Full Name	Pepa Pig								
Extension	301								
Email Address									
Locale									
Priority	5								
System Phone Rights	None								
Profile	Power User								
	<input type="checkbox"/> Receptionist								
	<input checked="" type="checkbox"/> Enable Softphone								
	<input checked="" type="checkbox"/> Enable one-X Portal Services								
	<input checked="" type="checkbox"/> Enable one-X TeleCommuter								
	<input checked="" type="checkbox"/> Enable Remote Worker								
	<input checked="" type="checkbox"/> Enable Desktop/Tablet VoIP client								
	<input checked="" type="checkbox"/> Enable Mobile VoIP Client								
	<input checked="" type="checkbox"/> Enable MS Teams Client								
	<input type="checkbox"/> Send Mobility Email								
	<input type="checkbox"/> Web Collaboration								

## 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

The screenshot shows the 'Security Settings' page for a system named 'ipo'. The left sidebar shows a tree view with 'Security' expanded, containing 'General', 'System (1)', 'Services (7)', 'Rights Groups (16)', and 'Service Users (10)'. The main content area is titled 'System: ipo' and has tabs for 'System Details', 'Unsecured Interfaces', and 'Certificates'. Under 'System Details', there are sections for 'Base Configuration' (Services Base TCP Port: 50804, Maximum Service Users: 64, Maximum Rights Groups: 32), 'System Discovery' (TCP Discovery Active: checked, UDP Discovery Active: checked), 'Security' (Session ID Cache: 10, HTTP Challenge Timeout: 10, RFC2617 Session Cache: 10, Minimum Protocol Version: TLS 1.2), 'HTTP Ports' (HTTP Port: 80, HTTPS Port: 443, Web Services Port: 8443), and 'Websocket Proxy' (Enabled: checked, Enforce Secure: checked). At the bottom, the 'Avaya Spaces Keys' section shows 'Avaya Spaces API Key' and 'Avaya Spaces Key Secret' fields, both filled with dots.

## 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**

The screenshot shows the 'API Key' configuration page in the Avaya Spaces interface. The breadcrumb is 'Home > Manage Companies > Company Profile'. The 'API Key' tab is selected, and a green 'Add API key +' button is visible.

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

The screenshot shows the 'Add API key' dialog box. The 'Role' dropdown is set to 'IPOFFICE'. There are 'Add API key' and 'Cancel' buttons.

### IPO users

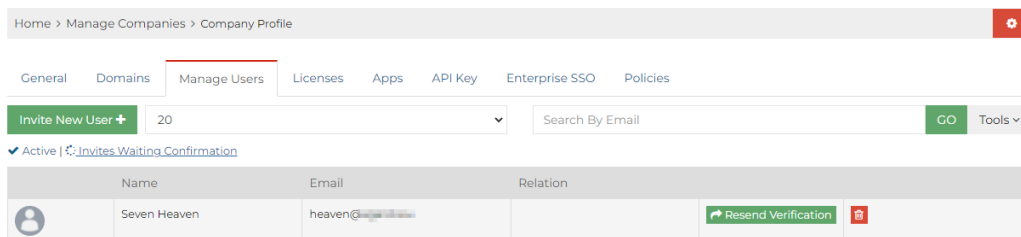
When company domain is verified, API key is generated and IPO is configured, users will be automatically synced from IPO to Spaces. Spaces sends welcome email to the new users once automatic synchronization from IPO is done. The users will not be searchable in CCW until the initial setup wizard is



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

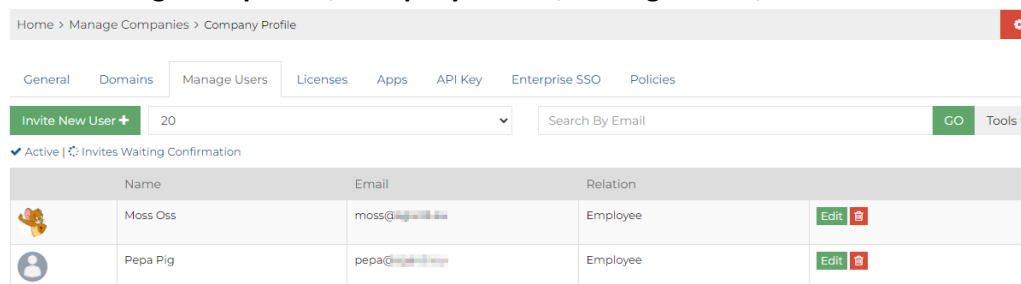
Check the list of users who have not yet completed the wizard:

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

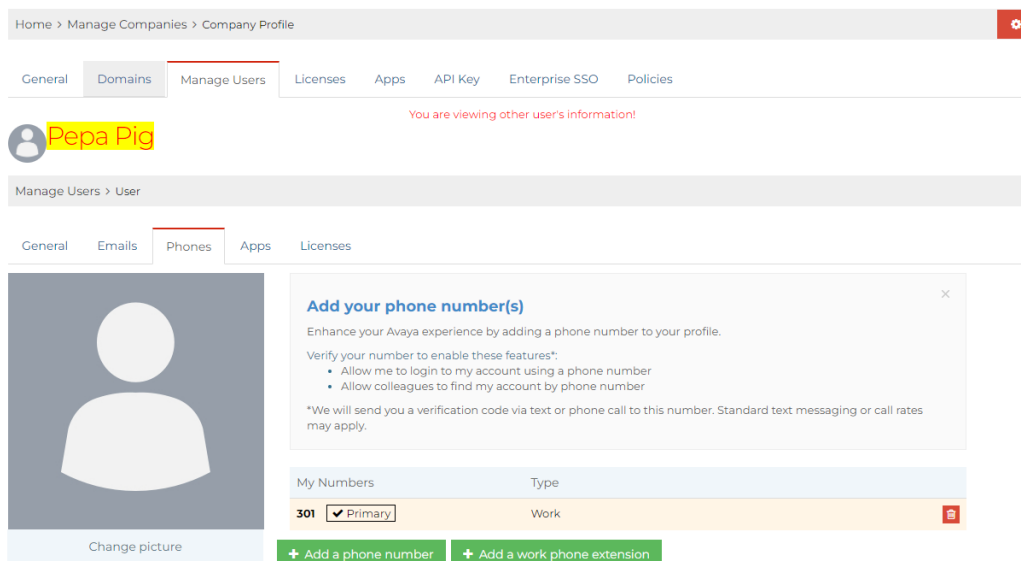


Verify that active IPO users have proper extension number after the sync:

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



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



## AXP Users

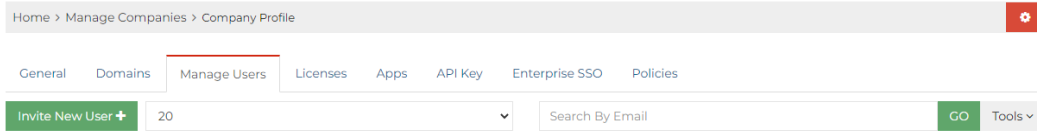
Each AXP agent needs a user account on Avaya Spaces so that CCW can login and search for IPO contacts. These users can be added manually one by one or by importing from a csv file.

Adding manually:

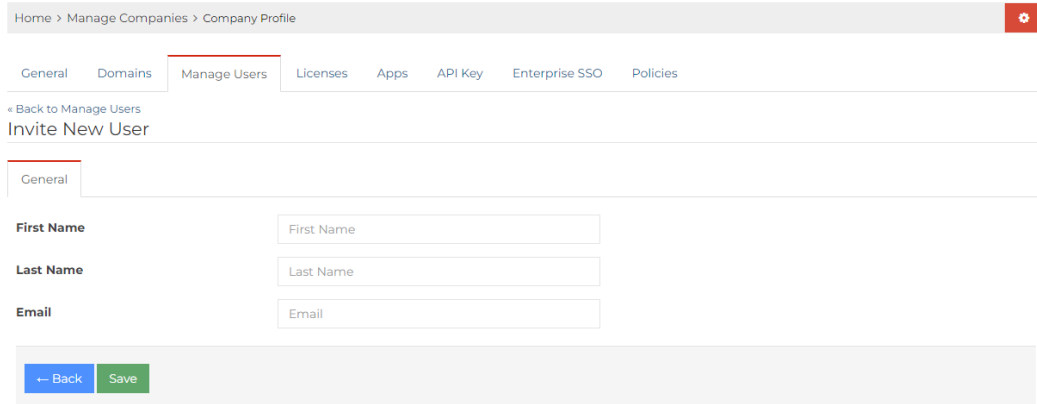
1. Login to **accounts.avayacloud.com** as the company administrator.



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:

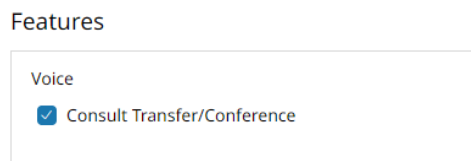
[https://documentation.avaya.com/bundle/IPOfficeWorkplaceInstall/page/Importing\\_the\\_CSV\\_File.html](https://documentation.avaya.com/bundle/IPOfficeWorkplaceInstall/page/Importing_the_CSV_File.html)

## 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

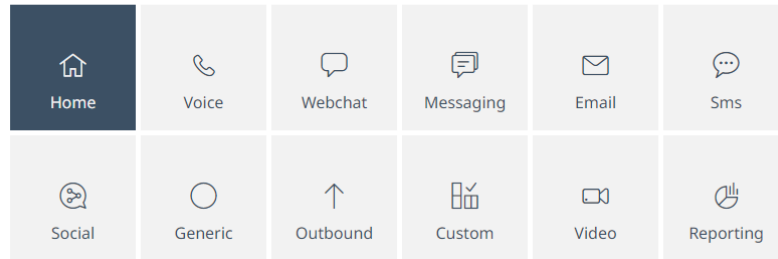
The Corporate Contact Widget must be added to the Layout

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

## Layout Manager > Default Account Layout

Layouts Views Tabs Customize Tab

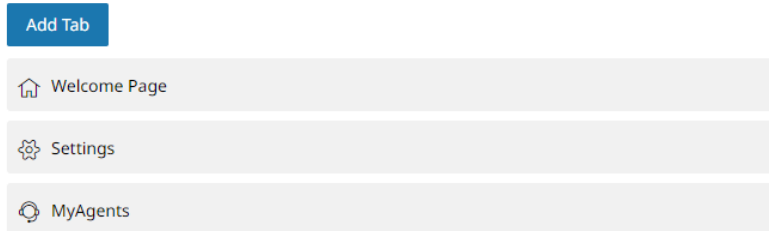
Select a View



### 5. Click Add Tab

## Layout Manager > Default Account Layout > Home

Layouts Views Tabs Customize Tab



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

Layouts Views Tabs Customize Tab

Tab Options

Name \*

Role \*

Icon \*

Select a Layout

Select Widgets

Widget 1

### 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)

The screenshot shows the Avaya Customer Details interface for a call from +44208984888. The call is categorized as 'Called' and 'Active'. The logs below show the SIP signaling sequence:

```

10:00:40.977 INVITE sip:+44208984888@192.168.0.141:5060;transport=TCP F:+44208984888 T:+44208984888 (SDP: 64.16.228.75:28798 RTP/AVP 9 0 8 18 101 sendrecv)
10:00:40.977 Trying
10:00:40.977 INVITE sip:+44208984888@sbc-ewest.mpaas.avayacloud.com;transport=tls F:+44208984888 T:+44208984888 (SDP: 35.158.38.189:35016 RTP/SAVP 9 0 8 18 101 sendrecv)
10:00:40.977 trying
10:00:40.977 Ringing
10:00:40.977 Ringing
10:00:41.279 Ringing
10:00:41.279 Ringing
10:00:41.782 200 OK (INVITE) (SDP: 155.184.6.102:3284 RTP/SAVP 9 101 sendrecv)
10:00:41.782 200 OK (INVITE) (SDP: 155.184.6.102:3284 RTP/SAVP 9 101 sendrecv)
10:00:41.984 ACK
10:00:41.984 ACK
10:03:43.603 BYE
10:03:43.603 BYE
10:03:43.805 200 OK (BYE)
10:03:43.805 200 OK (BYE)
  
```

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

The screenshot shows the SIP signaling sequence for an inbound call to IPO:

```

10:08:52.599 INVITE sip:+44208984888@192.168.0.141:5060;transport=TCP F:+44208984888 T:+44208984888 (SDP: 64.16.228.75:20300 RTP/AVP 9 0 8 18 101 sendrecv)
10:08:52.599 Trying
10:08:52.599 INVITE sip:+44208984888@192.168.0.141:5060;transport=tcp F:+44208984888 T:+44208984888 (SDP: 192.168.0.141:35012 RTP/AVP 9 0 8 18 101 sendrecv)
10:08:52.599 trying
10:08:52.599 Ringing
10:08:52.599 Ringing
10:08:57.028 200 OK (INVITE) (SDP: 192.168.0.111:40760 RTP/AVP 9 101)
10:08:57.028 200 OK (INVITE) (SDP: 192.168.0.111:40760 RTP/AVP 9 101)
10:08:57.230 ACK
10:08:57.230 ACK
10:09:02.869 BYE
10:09:02.869 BYE
10:09:03.071 200 OK (BYE)
10:09:03.071 200 OK (BYE)
  
```

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

**Customer Details**

Interaction Details

Originating Address: 10000@udtyxd.uk.cc.avayacloud.com  
Destination Address: +36308888887

Created At: Aug 4, 2023 10:20:10  
Interaction Type: Calling

Channel Type: Voice  
State: Active

Contact ID: 03333002101691137210  
Workflows ID: 7bc0625-6405-4096-8612-427badecf08

Direction: Outgoing  
Transfers ID: UDTYXD

Transferred to Service: No  
Transferred to User: No

**Additional Info**

Caller Name: +3630888887  
Caller Number: 10000@udtyxd.uk.cc.avayacloud.com

Start Date: 2023-08-04(UTC)  
Start Time: 08:28:10(UTC)

---

35.246.34.78      34.89.225.122

SBC

```

10:22:19.848 --INVITE--> SIP: sip:+3630@udtyxd.uk.cc.avayacloud.com;transport=tls F:+4420... T:+3630... (SDP: 155.184.6.1:3128 RTP/SAVP 9 8 0 18 101)
10:22:19.848 <--Trying-- SIP: 100 Trying
10:22:19.848 --INVITE--> SIP: sip:+3630@...;transport=tcp F:+4420... T:+3630... (SDP: ...:35030 RTP/SAVP 9 8 0 18 101)
10:22:19.949 <--Proxy A--> SIP: 407 Proxy Authentication Required
10:22:19.949 --ACK--> SIP: sip:+3630@...;transport=tcp
10:22:19.949 --INVITE--> SIP: sip:+3630@...;transport=tcp F:+4420... T:+3630... (SDP: ...:35030 RTP/SAVP 9 8 0 18 101)
10:22:19.949 <--trying--> SIP: 100 trying -- your call is important to us
10:22:20.351 <--Ringing--> SIP: 180 Ringing
10:22:20.351 <--Ringing--> SIP: 180 Ringing
10:22:23.573 <--Session--> SIP: 183 Session Progress (SDP: 64.16.226.79:21088 RTP/AVP 9 101 13 sendrcv)
10:22:23.573 <--Session--> SIP: 183 Session Progress (SDP: ...:35028 RTP/SAVP 9 101 13 sendrcv)
10:22:25.183 <--200 OK--> SIP: 200 OK (INVITE) (SDP: 64.16.226.79:21088 RTP/AVP 9 101 13 sendrcv)
10:22:25.183 <--200 OK--> SIP: 200 OK (INVITE) (SDP: ...:35028 RTP/SAVP 9 101 13 sendrcv)
10:22:25.284 <--ACK--> SIP: sip:+3630@...;transport=tls :5061;transport=tls
10:22:27.600 <--ACK--> SIP: sip:+3630@...;transport=udp :5060;transport=udp
10:22:27.600 <--BYE--> SIP: sip:+4420@...;transport=tcp :5060;transport=tcp
10:22:27.600 <--200 OK--> SIP: sip:+4420@...;transport=tls :5064;transport=tls
10:22:27.700 <--200 OK--> SIP: 200 OK (BYE)
10:22:27.700 <--200 OK--> SIP: 200 OK (BYE)
    
```

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

192.168.0.111      34.89.225.122

SBC

```

10:33:47.583 --INVITE--> SIP: sip:+3630@192.168.0.141 F:+4420... T:+3630... (SDP: 192.168.0.111:40780 RTP/AVP 9 8 0 18 101)
10:33:47.583 <--Trying-- SIP: 100 Trying
10:33:47.583 --INVITE--> SIP: sip:+3630@... F:+4420... T:+3630... (SDP: ...:35030 RTP/AVP 9 8 0 18 101)
10:33:47.583 <--Proxy A--> SIP: 407 Proxy Authentication Required
10:33:47.583 --ACK--> SIP: sip:+3630@...
10:33:47.583 --INVITE--> SIP: sip:+3630@... F:+4420... T:+3630... (SDP: ...:35030 RTP/AVP 9 8 0 18 101)
10:33:47.684 <--trying--> SIP: 100 trying -- your call is important to us
10:33:47.986 <--Ringing--> SIP: 180 Ringing
10:33:47.986 <--Ringing--> SIP: 180 Ringing
10:33:50.705 <--Session--> SIP: 183 Session Progress (SDP: 64.16.227.76:27210 RTP/AVP 8 101 sendrcv)
10:33:50.705 <--Session--> SIP: 183 Session Progress (SDP: 192.168.0.141:35020 RTP/AVP 8 101 sendrcv)
10:33:53.725 <--200 OK--> SIP: 200 OK (INVITE) (SDP: 64.16.227.76:27210 RTP/AVP 8 101 sendrcv)
10:33:53.725 <--200 OK--> SIP: 200 OK (INVITE) (SDP: 192.168.0.141:35020 RTP/AVP 8 101 sendrcv)
10:33:53.725 <--ACK--> SIP: sip:+3630@192.168.0.141:5060;transport=tcp
10:33:53.725 <--ACK--> SIP: sip:+3630@10.13.38.24:5070;transport=udp
10:33:55.436 <--BYE--> SIP: sip:+4420@...:5060;transport=tcp
10:33:55.437 <--200 OK--> SIP: sip:+4420@192.168.0.111:5070;transport=tcp
10:33:55.437 <--200 OK--> SIP: 200 OK (BYE)
10:33:55.437 <--200 OK--> SIP: 200 OK (BYE)
    
```

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

192.168.0.111      34.105.218.189

SBC

```

11:58:27.064 --INVITE--> SIP: sip:+4420@192.168.0.141 F:+4420... T:+4420... (SDP: 192.168.0.111:40844 RTP/AVP 9 8 0 18 101)
11:58:27.064 <--Trying-- SIP: 100 Trying
11:58:27.064 --INVITE--> SIP: sips:+4420@sbc-ewest.mpaas.avayacloud.com F:+4420... T:+4420... (SDP: ...:35060 RTP/SAVP 9 8 0 18 101)
11:58:27.165 <--trying--> SIP: 100 trying -- your call is important to us
11:58:27.165 <--Ringing--> SIP: 180 Ringing
11:58:27.165 <--Ringing--> SIP: 180 Ringing
11:58:27.366 <--Ringing--> SIP: 180 Ringing
11:58:27.366 <--Ringing--> SIP: 180 Ringing
11:58:27.568 <--200 OK--> SIP: 200 OK (INVITE) (SDP: 155.184.6.10:3048 RTP/SAVP 9 101 sendrcv)
11:58:27.568 <--200 OK--> SIP: 200 OK (INVITE) (SDP: 192.168.0.141:35052 RTP/AVP 9 101 sendrcv)
11:58:27.568 <--ACK--> SIP: sip:192.168.0.141:5060;transport=tcp
11:58:27.568 <--ACK--> SIP: sips:10.154.0.118:5063;transport=tls
11:58:30.186 <--BYE--> SIP: sip:192.168.0.141:5060;transport=tcp
11:58:30.186 <--200 OK--> SIP: sips:10.154.0.118:5063;transport=tls
11:58:30.186 <--200 OK--> SIP: 200 OK (BYE)
11:58:30.186 <--200 OK--> SIP: 200 OK (BYE)
    
```

### 6. Search IPO contact in CCW (SUCCESS)

Corporate Contacts

Users Groups

pepa

Avaya Spaces (1)

PP Pig, Pepa

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

Corporate Contacts

Users Groups

Search users

Only favorites users are displayed in this list. You may use the "Search" box to find more users.

Avaya Spaces (1)

PP ★ Pig, Pepa

8. Call IPO user from CCW (SUCCESS)

Corporate Contacts

Users Groups

Search users

Only favorites users are displayed in this list. You may use the "Search" box to find more users.

Avaya Spaces (1)

PP ★ Pig, Pepa

Call

301 06:14

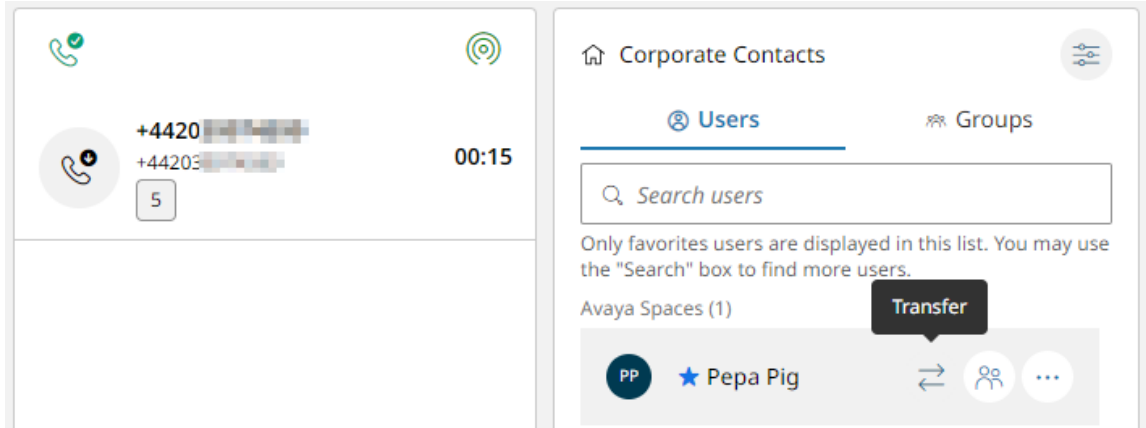
301 Customer Details

Interaction Details	
Participants	
AGENT - Agnès, Ester	
CUSTOMER - 301	
Originating Address	Destination Address
10000@ubdyd.uk.cc.avayacloud.com	301
Channel At	Interaction Type
Aug 6, 2023 09:52:20	Calling
Channel Type	Status
Voice	Active
Contact ID	WorkRequest ID
03333002001691135540	9a7c9134-f146-4c38-8226-62a681af6046
Direction	Tenant ID
Outgoing	LE700
Transferred to Service	Transferred to User
No	No
Additional Info	
Caller Name	Caller Number
301	10000@ubdyd.uk.cc.avayacloud.com
Start Date	Start Time
2023-08-04(UTC)	07:52:20(UTC)

```

34.105.218.189      192.168.0.111
SBC
09:55:01.285      --INVITE-->      SIP: sip:301@udtyxd.uk.cc.avayacloud.com;transport=tls F:+4420-... T:301 (SDP: 155.184.6.10:3164 RTP/SAVP 9 0 8 100 98 96 18 13 101 sendrcv)
09:55:01.285      <--Trying-->      SIP: 100 Trying
09:55:01.285      --INVITE-->      SIP: sip:301@...;transport=tcp F:+4420-... T:301 (SDP: 192.168.0.141:35010 RTP/AVP 9 0 8 100 98 96 18 13 101 sendrcv)
09:55:01.285      <--Trying-->      SIP: 100 Trying
09:55:01.285      --Ringing-->      SIP: 180 Ringing
09:55:01.285      <--Ringing-->      SIP: 180 Ringing
09:55:05.815      --200 OK-->      SIP: 200 OK (INVITE) (SDP: 192.168.0.111:40756 RTP/AVP 9 101)
09:55:05.815      <--200 OK-->      SIP: 200 OK (INVITE) (SDP: ...:35014 RTP/SAVP 9 101)
09:55:09.916      --ACK-->      SIP: sip:301@...:5061;transport=tls
09:55:09.916      <--ACK-->      SIP: sip:301@192.168.0.111:5070;transport=tcp
09:55:13.164      --BYE-->      SIP: sip:301@...:5061;transport=tls
09:55:13.164      <--BYE-->      SIP: sip:301@192.168.0.111:5070;transport=tcp
09:55:13.164      --200 OK-->      SIP: 200 OK (BYE)
09:55:13.164      <--200 OK-->      SIP: 200 OK (BYE)
  
```

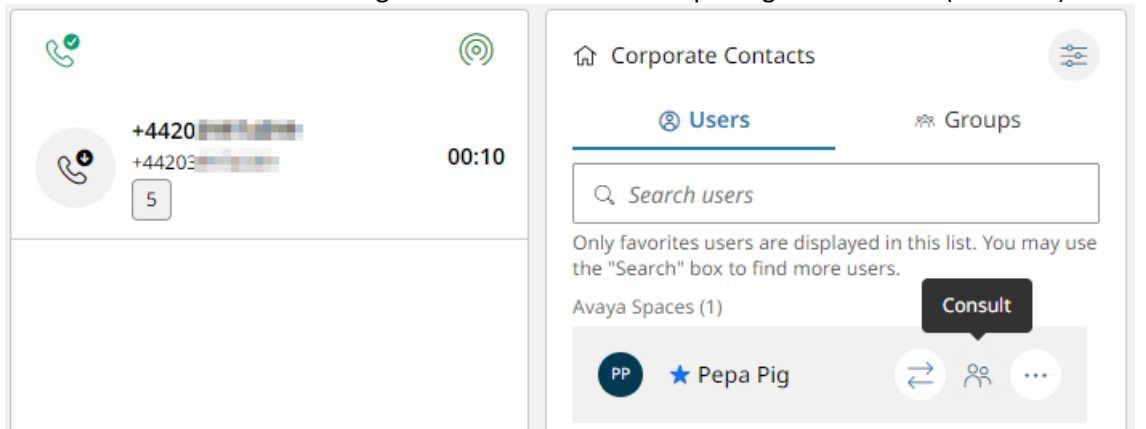
9. Transfer customer to IPO user from AXP using CCW transfer button (SUCCESS)



```

34.89.225.122      34.105.218.189      192.168.0.111
SBC      SBC      SBC
12:06:38.480      --INVITE-->      SIP: sip:+4420-...:5060;Transport=TCP F:+4420-... T:+4420-... (SDP: 64.16.227.77:26560 RTP/AVP 9 0 8 100 98 96 18 13 101 sendrcv)
12:06:38.480      <--Trying-->      SIP: 100 Trying
12:06:38.480      --INVITE-->      SIP: sip:+4420@...@sbc-ewest.mpaas.avayacloud.com;transport=tls F:+4420-... T:+4420-... (SDP: ...:35066)
12:06:38.480      <--trying-->      SIP: 100 trying -- your call is important to us
12:06:38.480      --Ringing-->      SIP: 180 Ringing
12:06:38.480      <--Ringing-->      SIP: 180 Ringing
12:06:38.681      --Ringing-->      SIP: 180 Ringing
12:06:38.681      <--Ringing-->      SIP: 180 Ringing
12:06:38.983      --200 OK-->      SIP: 200 OK (INVITE) (SDP: 155.184.6.10:3146 RTP/SAVP 9 101 sendrcv)
12:06:38.983      <--200 OK-->      SIP: 200 OK (INVITE) (SDP: ...:35068 RTP/AVP 9 101 sendrcv)
12:06:39.084      --ACK-->      SIP: sip:...:5060;transport=tcp
12:06:39.084      <--ACK-->      SIP: sip:301@udtyxd.uk.cc.avayacloud.com;transport=tls F:+4420-... T:301 (SDP: 155.184.6.10:3168 RTP/SAVP 9 0 8 100 98 96 18 13 101 sendrcv)
12:08:31.842      --INVITE-->      SIP: sip:301@...;transport=tcp F:+4420-... T:301 (SDP: 192.168.0.141:35054 RTP/AVP 9 0 8 100 98 96 18 13 101 sendrcv)
12:08:31.842      <--Trying-->      SIP: 100 Trying
12:08:31.842      --Ringing-->      SIP: 180 Ringing
12:08:31.842      <--Ringing-->      SIP: 180 Ringing
12:08:37.077      --200 OK-->      SIP: 200 OK (INVITE) (SDP: 192.168.0.111:40850 RTP/AVP 9 101)
12:08:37.077      <--200 OK-->      SIP: 200 OK (INVITE) (SDP: ...:35070 RTP/SAVP 9 101)
12:08:37.178      --ACK-->      SIP: sip:301@...:5061;transport=tls
12:08:37.178      <--ACK-->      SIP: sip:301@192.168.0.111:5070;transport=tcp
12:08:39.896      --BYE-->      SIP: sip:192.168.0.141:5060;transport=tcp
12:08:39.896      <--BYE-->      SIP: sip:10.154.0.117:5069;transport=tls
12:08:39.997      --200 OK-->      SIP: 200 OK (BYE)
12:08:39.997      <--200 OK-->      SIP: 200 OK (BYE)
12:08:40.299      --BYE-->      SIP: sip:mod_sofia@...:5061;transport=tls
12:08:40.299      <--BYE-->      SIP: sip:mod_sofia@10.13.39.24:6000
12:08:40.400      --200 OK-->      SIP: 200 OK (BYE)
12:08:40.400      <--200 OK-->      SIP: 200 OK (BYE)
  
```

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



The screenshot displays a call log on the left and SIP messages on the right. The call log shows a sequence of events: INVITE, Trying, Ringing, 200 OK, ACK, INVITE, Trying, Ringing, 200 OK, ACK, BYE, 200 OK, and BYE. The SIP messages show the corresponding signaling, including INVITE, 100 Trying, 180 Ringing, 200 OK (INVITE), and 200 OK (BYE) for various SIP addresses and ports.

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

The screenshot shows the Avaya console interface during a consultation process. The top section shows a call with a duration of 00:10. The 'Corporate Contacts' panel is open, displaying a search for users. A 'Consult' button is highlighted over the 'Pepa Pig' contact. Below, the console shows the call duration increasing to 01:00, and a 'Complete as Conference' button is visible. The 'Interaction Details' panel shows the participants: AGENT - Agent, Peter and CUSTOMER - 301. A second call window shows the call duration at 02:02, with the 'Interaction Details' panel listing participants: CUSTOMER - 301, AGENT - Agent, Peter, and CUSTOMER - +4420...



```
34.89.225.122          SBC          34.105.218.189          192.168.0.111
12:44:51.357 --INVITE--> SIP: sip:+44207...:5060;Transport=TCP F:+4420... T:+4420... (SDP: 64.16.227.73:32068 RTP/AVP 9 0 8 15 101 sendre
12:44:51.357 <--Trying--> SIP: 100 Trying
12:44:51.357 --INVITE--> SIP: sip:+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: sip:10.154.0.117:5070;transport=tls
12:45:27.099 --INVITE--> SIP: sip:301@dytyd.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
12:45:27.100 --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)
12:45:31.026 --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: sip: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)
```