



Avaya Solution & Interoperability Test Lab

Application Notes for Teo IP Phones 7810 and 7810 TSG-6 Series with Avaya Aura[®] Session Manager 6.3 and Avaya Aura[®] Communication Manager 6.2 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Teo IP Phones 7810 and 7810 TSG-6 Series to interoperate with Avaya Aura[®] Session Manager 6.3 and Avaya Aura[®] Communication Manager 6.2.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

This document describes the configuration steps required to integrate Teo IP Phones 7810 and 7810 TSG-6 Series with an Avaya SIP-enabled telephony enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 6.3, Avaya Aura[®] Communication Manager Evolution Server 6.2 and other Avaya endpoints.

Both the Teo IP Phones 7810 and the 7810 TSG-6 Series are executive level SIP deskphones designed for government, military, and commercial users. The 7810 TSG-6 Series are built with special circuitry using ultra-low emissions technology, as they are designed for on-hook secure applications in sensitive areas.

There are three models currently available in the 7810 TSG-6 Series: 7810-TSG, 7810PoE-TSGA and 7810PoE-TSGB, each model using different hardware and power variations. During the interoperability test, 7810PoE-TSGB sets were used. Since all models share the same core SIP firmware, it is expected that the results of the interoperability tests can be extended to all the models in the series.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between the Teo IP Phones and Avaya Session Manager and Communication Manager.

Testing consisted of typical call scenarios involving internal endpoints at the enterprise, as well as external endpoints on a simulated PSTN, for the verification of support for various basic and supplementary features. Additionally, serviceability testing was performed to verify the ability for the telephones to recover from various failure scenarios.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and functionality verification, as well as serviceability testing.

The following features and functionality were covered during the compliance test:

- Telephone SIP registration using transport protocols UDP, TCP and TLS.
- Calling to and from various Avaya telephone models including SIP, H.323, digital and analog sets.
- Calling to and from simulated PSTN endpoints.
- Codec support and proper codec negotiation.
- DTMF tone transmissions passed as out-of-band RTP events per RFC 2833.
 - Voicemail coverage with message waiting indicator (MWI) and message retrieval.
- Direct IP-to-IP Media (Shuffling).
- Quality of Service.
- Basic user features such as Hold, Call Transfer, Call Forward, Conference and Bridged Call Appearance.
- Supplementary Telephony features using Communication Manager Feature Name Extensions including Call Park, Call Pickup, Automatic Callback and Calling Party Number Block/Unblock.

For the serviceability tests, the response of the Teo telephones was tested during various failure scenarios including loss of IP connectivity and a reboot of the telephone.

2.2. Test Results

Interoperability testing was completed with successful results with the exception of the observations/limitations described below:

- Codec G.722 – Certain hold/resume and conference scenarios involving the Teo IP Phones and the Avaya G450 Media Gateway while using codec G.722 failed during the compliance tests. Thus, the use of codec G.722 is not recommended with this solution.

2.3. Support

For technical support on the Teo solution described in these Application Notes, visit <http://www.teotech.com/support>.

3. Reference Configuration

Figure 1 illustrates the sample reference architecture used during the compliance test of the Teo Tech and Avaya solution. The components used to create the configuration included:

- Avaya Aura® Session Manager.
- Avaya Aura® Communication Manager.
- Avaya Aura® System Manager.
- Avaya Aura® Messaging.
- Avaya G450 Media Gateway.
- Avaya 96x0 and 96x1 Series IP Telephones (SIP).
- Avaya 96x0 and 96x1 Series IP Telephones (H.323).
- Avaya digital and analog telephones.
- Teo IP Phones 7810 and 7810 TSG-6.

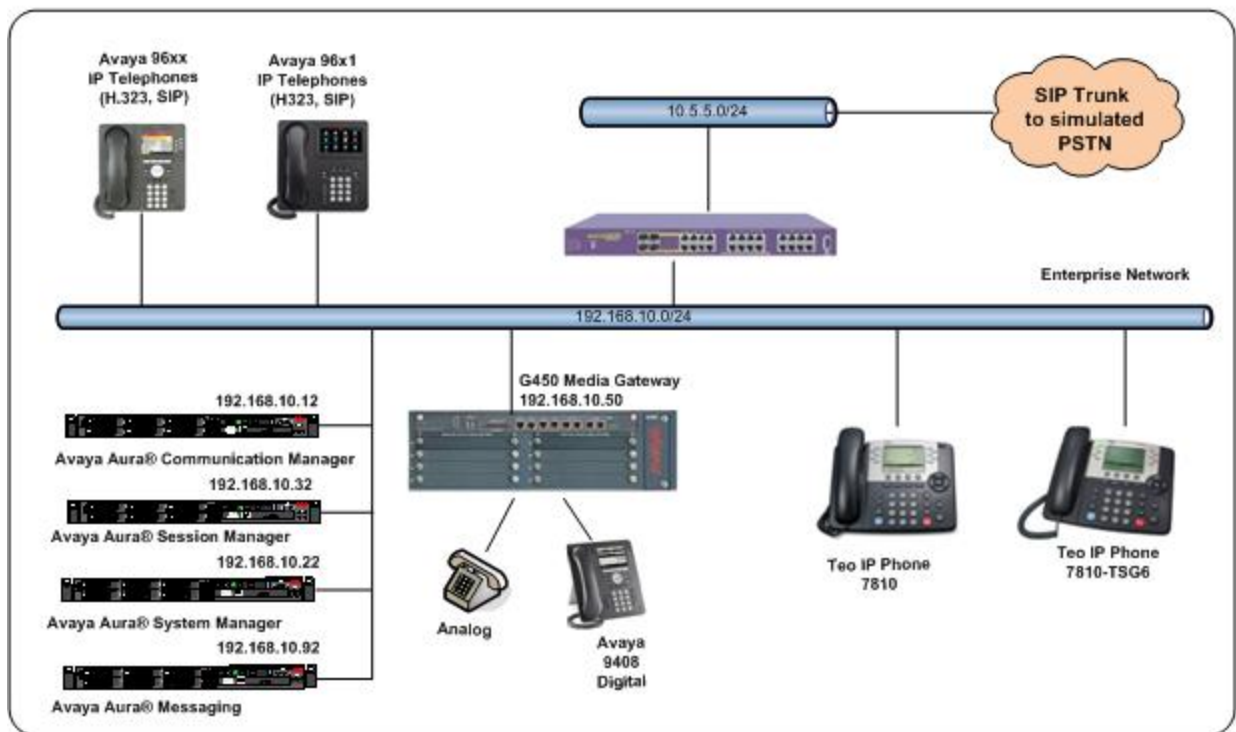


Figure 1: Test Configuration

In the reference configuration, Session Manager acts as the registrar for Teo and Avaya SIP endpoints. Session Manager also provides centralized dial plan, user profiles and call routing for the SIP entities in the enterprise. Communication Manager is configured as an evolution server, functioning as the telephony application server for Session Manager. H.323 endpoints are registered with Communication Manager. System Manager provides a web-based interface for the provisioning and maintenance of Session Manager. The G450 Media Gateway provides VoIP resources and contains the media modules for the connectivity of analog and digital telephones.

A SIP trunk from Session Manager to a separate PBX system in the Lab is used to simulate external PSTN calls to and from the enterprise.

Messaging was used during the compliance test to verify voice mail redirection, navigation and the delivery of MWI (Message Waiting Indicator) messages to the enterprise telephones. Messaging functioned on a single standalone server located on the enterprise network, administered as a separate SIP entity in Session Manager. Since the configuration of Messaging is standard and not directly related to the interoperability with the Teo telephones, they are not included in these Application Notes.

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Component	Version
Avaya	
Avaya Aura® Communication Manager on a HP® Proliant DL360 G7 Server.	6.2 Service Pack 5
Avaya Aura® Session Manager on a HP® Proliant DL360 G7 Server.	6.3 Service pack 1
Avaya Aura® System Manager on a HP® Proliant DL360 G7 Server.	6.3 Service Pack 1
Avaya Aura® Messaging on a Dell PowerEdge R610	6.2 Service pack 2
Avaya G450 Media Gateway	32.24.0
Avaya 96x0 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 3.2
Avaya 96x0 Series IP Telephones (SIP)	Avaya one-X Deskphone Edition SIP 2.6.9
Avaya 96x1 Series IP Telephones (H.323)	Avaya one-X Deskphone Edition H.323 6.2
Avaya 96x1 Series IP Telephones (SIP)	Avaya one-X® Deskphone Edition SIP 6.2
Avaya 9408 Digital Telephone	2.00
Avaya 6210 Analog Telephone	n/a
Teo	
Teo IP Phone 7810	05.04.12
Teo IP Phone 7810PoE-TSGB	05.04.12

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring Communication Manager in the reference configuration. It is assumed that the general installation of Communication Manager and the Avaya G450 Media Gateway has been previously completed and is not discussed here.

Most configuration tasks shown in the following screens were already in place in the lab environment, completed during the initial installation of the Avaya Aura® solution. However, these screens are presented as a reference to illustrate the Communication Manager configuration used in the compliance test, and for the verification of items required for the integration of the Teo telephones with the Avaya solution.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Off-PBX Telephones - OPS** value on **Page 1** is sufficient to support the desired number of SIP extensions at the enterprise. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

```
display system-parameters customer-options Page 1 of 11
OPTIONAL FEATURES

G3 Version: U16                      Software Package: Enterprise
Location: 2                          System ID (SID): 1
Platform: 28                         Module ID (MID): 1

                                USED
Platform Maximum Ports: 65000 317
Maximum Stations: 36000 26
Maximum XMOBILE Stations: 41000 0
Maximum Off-PBX Telephones - EC500: 36000 3
Maximum Off-PBX Telephones - OPS: 36000 11
Maximum Off-PBX Telephones - PBFMC: 36000 0
Maximum Off-PBX Telephones - PVFMC: 36000 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 0
```

On **Page 2**, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient for the solution.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES			USED	
Maximum Administered H.323 Trunks:			12000	10
Maximum Concurrently Registered IP Stations:			18000	4
Maximum Administered Remote Office Trunks:			12000	0
Maximum Concurrently Registered Remote Office Stations:			18000	0
Maximum Concurrently Registered IP eCons:			414	0
Max Concur Registered Unauthenticated H.323 Stations:			100	0
Maximum Video Capable Stations:			41000	2
Maximum Video Capable IP Softphones:			18000	4
Maximum Administered SIP Trunks:			24000	281
Maximum Administered Ad-hoc Video Conferencing Ports:			24000	0

5.2. Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes telephone extensions, Feature Access Codes (FACs), OPS Feature Name Extensions (FNEs), Dial Access Codes (DACs), etc. In the sample configuration, Feature Access Codes used a **Dialed String** that began with the digit **0**, had a **Total Length** that was three digits long and **Call Type fac**. FNEs were four digits long, beginning with **1**, and defined as **ext Call Type**. SIP telephone extensions were four digits long, starting with the digit **2**. Other extension types, hunt groups, etc. used during the test began with the digit **3** and were also four digits long. Both were defined as **Call Type ext**. Dial Access Codes were three digits long, starting with **6** and **Call Type dac**.

change dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	3	fac						
1	4	ext						
2	4	ext						
3	4	ext						
4	4	ext						
5	5	ext						
6	3	dac						
7	4	ext						

5.3. Feature Access Codes and Feature Name Extensions

Third Party SIP telephones generally don't have buttons associated with Communication Manager features. The equivalent functionality is accomplished by defining Feature Access Codes (FAC) and the corresponding Feature Name Extensions (FNE) for Off-PBX Stations (OPS) in Communication Manager. In the compliance test, Teo users dialed the FNE codes, which invoked the associated FAC for the desired feature.

Use the **change feature-access-codes** command to define the required access codes. The screen below shows a sample of some of the FAC used during the tests.

```
change feature-access-codes                                     Page 1 of 11
FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code: _____
Abbreviated Dialing List2 Access Code: _____
Abbreviated Dialing List3 Access Code: _____
Abbreviated Dial - Prgm Group List Access Code: _____
Announcement Access Code: 099
Answer Back Access Code: 015
Attendant Access Code: _____
Auto Alternate Routing (AAR) Access Code: 8
Auto Route Selection (ARS) - Access Code 1: 9 Access Code 2: _____
Automatic Callback Activation: 016 Deactivation: 017
Call Forwarding Activation Busy/DA: 018 All: 019 Deactivation: 020
Call Forwarding Enhanced Status: _____ Act: _____ Deactivation: _____
Call Park Access Code: 010
Call Pickup Access Code: 011
CAS Remote Hold/Answer Hold-Unhold Access Code: _____
```

Use the **change off-pbx-telephone feature-name-extensions set 1** command to define the associated FNEs. The screen below shows some of the FNE values used during the tests.

```
change off-pbx-telephone feature-name-extensions set 1        Page 1 of 2
EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
Set Name: Teo Tech Test
Active Appearance Select: _____
Automatic Call Back: 1016
Automatic Call-Back Cancel: 1017
Call Forward All: 1019
Call Forward Busy/No Answer: 1018
Call Forward Cancel: 1020
Call Park: 1010
Call Park Answer Back: 1015
Call Pick-Up: 1011
Calling Number Block: 1012
Calling Number Unblock: 1013
Conditional Call Extend Enable: _____
Conditional Call Extend Disable: _____
Conference Complete: _____
Conference on Answer: 1023
Directed Call Pick-Up: _____
Drop Last Added Party: 1024
```


5.4. Class of Service

Use the **change cos-group 1** command to set the appropriate service permissions to support OPS features. Class of Service 1 was used for all Teo extensions. The highlighted values were the ones modified and relevant to the reference configuration.

change cos-group 1																Page	1 of	2	
CLASS OF SERVICE	COS Group: 1																COS Name: <div></div>		
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15			
Auto Callback	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>			
Call Fwd-All Calls	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Data Privacy	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Priority Calling	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Console Permissions	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Off-hook Alert	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Client Room	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Restrict Call Fwd-Off Net	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Call Forwarding Busy/DA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Personal Station Access (PSA)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

5.5. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of the Communication Manager (**procr**) and Session Manager (**asm**) signaling interfaces. These node names will be used later in the configuration process.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
asm	192.168.10.32	
default	0.0.0.0	
msgserver	192.168.10.12	
procr	192.168.10.12	
procr6	::	
rsefab	192.168.0.220	

5.6. Codecs

Use the **change ip-codec-set** command to specify the codecs to be used for calls to and from the Teo telephones. For the compliance test, ip-codec-set 1 was used for this purpose. Enter **G.711MU** and **G.729A** in the **Audio Codec** column of the table. Default values can be used for all other fields.

change ip-codec-set 1					Page 1 of 2
IP Codec Set					
Codec Set: 1					
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)		
1: G.711MU	n	2	20		
2: G.729A	n	2	20		
3:					

5.7. IP Network Region

Use the **change ip-network-region** command to set the configuration of the network region used by the Teo telephones. In the reference configuration, this was network region **1**, previously defined. Network region 1 also contained all the devices in the enterprise network relevant to the compliance test. Set/verify the parameters highlighted below:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the test configuration, the domain name was **sil.miami.avaya.com**
- Enter a descriptive name in the **Name** field.
- Leave both **Intra-region** and **Inter-region IP-IP Direct Audio** set to **yes**, the default setting. This will enable **IP-IP Direct Audio** (shuffling), to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.6**.
- Default values can be used for all other fields.

```
change ip-network-region 1                                     Page 1 of 20
                                                                IP NETWORK REGION
Region: 1
Location: 1 Authoritative Domain: sil.miami.avaya.com
Name: Enterprise Network
MEDIA PARAMETERS
Codec Set: 1 Intra-region IP-IP Direct Audio: yes
Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048 IP Audio Hairpinning? n
UDP Port Max: 8001
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
```

5.8. Signaling Group

Use the **change signaling-group** command to set the configuration of the signaling group to be used by the trunk group between Communication Manager and Session Manager. Signaling group 1, previously defined, was used in the compliance test. Set/verify the parameters highlighted below:

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for the Session Manager.
- Set the **Transport Method** to the recommended default value of **tls** (Transport Layer Security). To facilitate tracing and fault analysis, the compliance test was conducted with the **Transport Method** set to **tcp**.
- Set the **Peer Detection Enabled** field to **y**.
- Set the **Near-end Node Name** to **procr** and the **Far-end Node Name** to **asm**. These node names map to the IP addresses of Communication Manager and Session Manager, as defined in **Section 5.5**.
- Set the values for the **Near-end Listen Port** and the **Far-end Listen Port** fields. For **tcp**, the well known port value is **5060**. For **tls**, the well known port value is **5061**.
- Set the **Far-end Network Region** to **1**, the IP network region of the enterprise, as seen in **Section 5.7**.
- Set the **Far-end Domain** to the domain of the enterprise.
- Set the **DTMF over IP** field to **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- Set **Direct IP-IP Audio Connections** to **y**, to allow audio traffic to be sent directly between IP endpoints.
- Default values may be used for all other fields.

```
change signaling-group 1                                     Page 1 of 2
SIGNALING GROUP
Group Number: 1      Group Type: sip
IMS Enabled? n      Transport Method: tcp
Q-SIP? n
IP Video? y      Priority Video? n      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y      Peer Server: SM
Near-end Node Name: procr      Far-end Node Name: asm
Near-end Listen Port: 5060      Far-end Listen Port: 5060
Far-end Network Region: 1
Far-end Domain: sil.miami.avaya.com      Far-end Secondary Node Name:
Incoming Dialog Loopbacks: eliminate      Bypass IF IP Threshold Exceeded? n
DTMF over IP: rtp-payload      RFC 3389 Comfort Noise? n
Session Establishment Timer(min): 3      Direct IP-IP Audio Connections? y
Enable Layer 3 Test? y      IP Audio Hairpinning? n
H.323 Station Outgoing Direct Media? n      Initial IP-IP Direct Media? n
Alternate Route Timer(sec): 6
```

5.9. Trunk Group

Use the **change trunk-group** command to set the configuration of the trunk group for call routing between Communication Manager and Session Manager. This trunk group carries all the call signaling between SIP and non-SIP extensions, application sequence traffic, etc. Trunk group 1, previously defined, was used in the compliance test. Set/verify the parameters highlighted below:

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set **Direction** to **two-way**.
- Set the **Service Type** field to **tie**.
- Set the **Signaling Group** to the signaling group defined in **Section 5.8**.
- Set the **Number of Members** field to the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk.

```
change trunk-group 1                                     Page 1 of 21
TRUNK GROUP
Group Number: 1      Group Type: sip      CDR Reports: y
Group Name: CM-Session Manager      COR: 1      TN: 1      TAC: 601
Direction: two-way      Outgoing Display? n
Dial Access? n      Night Service:
Queue Length: 0
Service Type: tie      Auth Code? n
                        Member Assignment Method: auto
                        Signaling Group: 1
                        Number of Members: 255
```

On **Page 3**, set the **Numbering Format** field to **private**. Default values may be used for all other fields.

```
change trunk-group 1                                     Page 3 of 21
TRUNK FEATURES
ACA Assignment? n      Measured: none      Maintenance Tests? y
Numbering Format: private      UI Treatment: service-provider
Replace Restricted Numbers? n
Replace Unavailable Numbers? n
```

5.10. Calling Party Information

Use the **change private-numbering 1** command to configure/verify the calling party number sent to the far-end over the SIP trunk group. In the reference configuration, local extensions that are four digits long, beginning with **2** and **3** and whose calls are routed over SIP trunk group **1**, have their extension number sent unaltered to the far-end for display and identification purposes.

change private-numbering 1					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
4	1			4	Total Administered: 9
4	2	1		4	Maximum Entries: 540
4	3	1		4	
4	4			4	
5	5			5	

5.11. Routing

Use the **change aar analysis 2** command to configure/verify the routing of the digits dialed to reach SIP extensions. In the example below, a **Dialed String** beginning with **2**, four digits long (2xxx extension range assigned to SIP extensions in the compliance test) is configured to use **Route Pattern 1**. The **Call Type** is set to **aar**. The screen below also shows an entry for the dial string **3888**, which is the pilot number dialed to reach Messaging in the reference configuration, also using Route Pattern **1** to Session Manager.

change aar analysis 1							Page 1 of 2
AAR DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
2	4	4	1	aar		n	
304	4	4	5	aar		n	
3888	4	4	1	aar		n	
3999	4	4	99	aar		n	
5	5	5	10	aar		n	

The route pattern defines which trunk group will be used for the call and performs any necessary digit manipulation. Use the **change route-pattern** command to set/verify the route pattern used by Communication Manager to reach SIP extensions registered to Session Manager.

- **Pattern Name**: Enter a descriptive name.
- **Grp No**: Enter trunk group **1**, configured in **Section 5.9**.
- Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of **0** is the least restrictive level.
- Set the **Numbering Format** to **unk-unk**.

change route-pattern 1											Page 1 of 3		
Pattern Number: 1											Pattern Name: CM to SM		
SCCAN? n											Secure SIP? n		
Grp No	FRL	NPA	Pfx Mrk	Hop Lmt	Toll List	No. Del	Inserted Dgts				DCS/ QSIG Intw	IXC	
1:	1	0									n	user	
2:											n	user	
3:											n	user	
4:											n	user	
5:											n	user	
6:											n	user	
BCC		VALUE		TSC	CA-TSC	ITC		Service/Feature		PARM	No.	Numbering	LAR
0	1	2	M	4	W	Request					Dgts	Format	
											Subaddress		
1:	u	u	u	u	u	n	n	rest				unk-unk	none
2:	u	u	u	u	u	n	n	rest					none

5.12. Save Translation

Use the **save translation** command to save any changes to made to the Communication Manager configuration.

save translation	
SAVE TRANSLATION	
Command Completion Status	Error Code
Success	0

6. Configure Avaya Aura® Session Manager

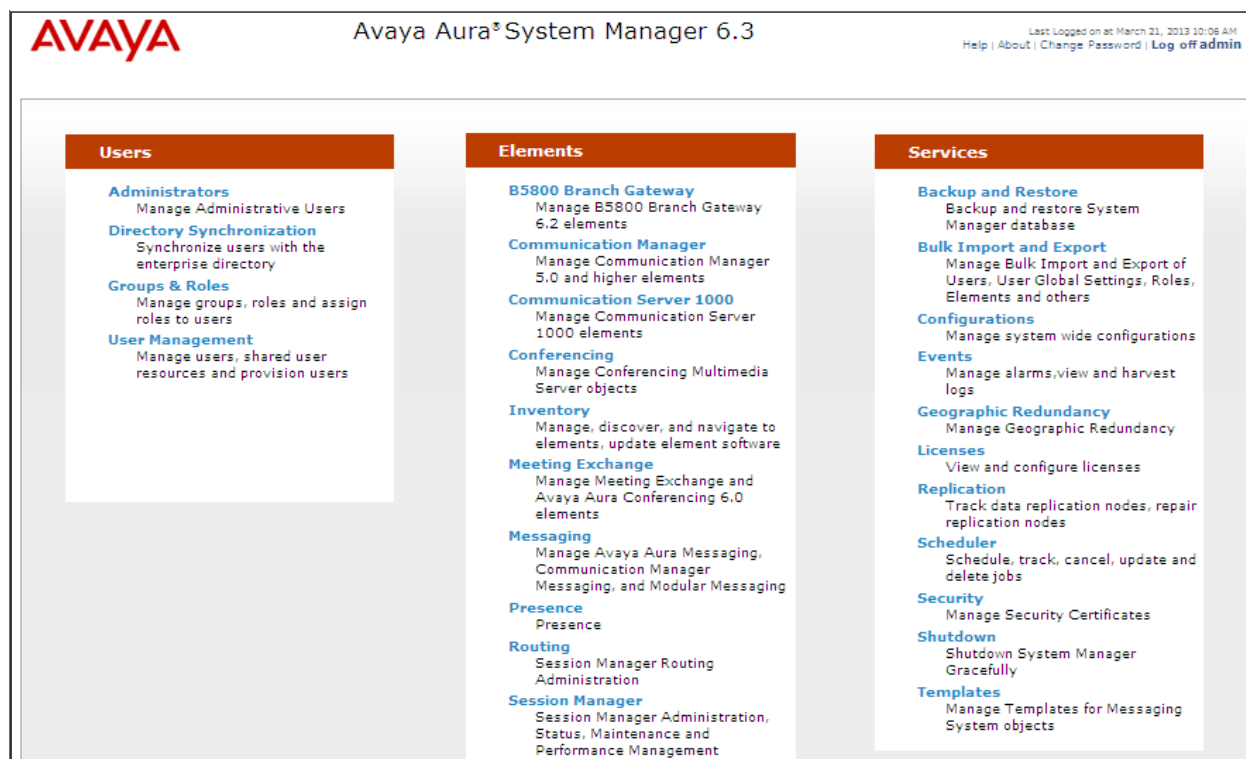
This section provides the Session Manager procedures required to integrate the Teo IP Phones users to the Avaya enterprise solution. The following items are covered:

- SIP domain.
- Location.
- SIP Entities and Entity Link for Communication Manager and Session Manager.
- Communication Manager Instance.
- Application and Application Sequence.
- User Management.
- Communication Manager data synchronization with Session Manager.

It may not be necessary to create all the items preceding the User Management section on the list above, since some of them would have already been defined as part of the initial Session Manager installation. However, each item will be visited to verify the configuration and to gather information needed to complete the addition of the Teo users, later in **Section 6.8**.

6.1. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **Log On** (not shown). The **Home** screen shown below is then displayed.



6.2. Domains

From the Home screen navigate to **Elements → Routing → Domains**. Select **Edit** to review an existing domain or **New** to create a new one (not shown). Enter/verify the data as shown in the following screen. Enter the domain name under **Name**, which corresponds to the domain administered in the IP Network Region in Communication Manager in **Section 5.7**. Select **sip** from the pull-down menu under **Type** and add a brief description under **Notes** (optional). Click **Commit**.

The screenshot shows the 'Domain Management' page. On the left is a navigation menu with 'Routing' expanded, showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', and 'Time Ranges'. The main content area has a breadcrumb 'Home / Elements / Routing / Domains' and a 'Help ?' link. Below the breadcrumb are 'Commit' and 'Cancel' buttons. A table lists domains with columns 'Name', 'Type', and 'Notes'. There is one item: 'sil.miami.avaya.com' with type 'sip' and notes 'MA Lab Domain'. Above the table is a '1 Item Refresh' link and a 'Filter: Enable' link.

Name	Type	Notes
* sil.miami.avaya.com	sip	MA Lab Domain

6.3. Locations

Navigate to **Routing → Locations** in the left navigation pane. Select **Edit** to review an existing domain or **New** to create a new one (not shown). Enter/verify the data as shown in the following screen. Enter a descriptive **Name** for the location, add a brief description (optional).

The screenshot shows the 'Location Details' page. On the left is a navigation menu with 'Routing' expanded, showing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', and 'Time Ranges'. The main content area has a breadcrumb 'Home / Elements / Routing / Locations' and a 'Help ?' link. Below the breadcrumb are 'Commit' and 'Cancel' buttons. The 'General' section contains two fields: 'Name' with the value 'SIL Lab' and 'Notes' with the value 'Equipment in Lab'.

In the **Location Pattern** section, click **Add** and enter an **IP address Pattern** to identify the location. Verify that the range of IP addresses assigned to the Teo telephones is included under this pattern, or add a new pattern if necessary. Click **Commit** to save.

The screenshot shows the 'Location Pattern' page. At the top are 'Add' and 'Remove' buttons. Below is a table with columns 'IP Address Pattern' and 'Notes'. There is one item: '192.168.10.*'. Above the table is a '1 Item Refresh' link and a 'Filter: Enable' link. At the bottom is a 'Select : All, None' link.

IP Address Pattern	Notes
* 192.168.10.*	

6.4. SIP Entities

Navigate to **Routing** → **SIP Entities** in the left navigation pane. Select **Edit** to review an existing SIP entity or **New** to create a new one (not shown). Enter/verify the data as described below and shown in the following screens.

In the **General** section, enter a descriptive **Name**. Enter the **FQDN or IP address** that is used for SIP signaling on the SIP Entity. Under **Type** select **Session Manager** for Session Manager or **CM** for Communication Manager. Select the **Location** that applies to the SIP Entity being created. Select the **Time Zone** for the location. Under **SIP Link Monitoring**, select **Use Session Manager Configuration**.

The following screen shows the Session Manager SIP entity. The IP address of the Session Manager Security Module is entered for **FQDN or IP Address**.

The screenshot shows the 'SIP Entity Details' form for a Session Manager entity. The left navigation pane is expanded to 'SIP Entities'. The form has a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. The 'General' section contains the following fields: 'Name' (MA_Session Manager), 'FQDN or IP Address' (192.168.10.32), 'Type' (Session Manager), 'Notes' (Security Module), 'Location' (SIL Lab), 'Outbound Proxy' (empty), 'Time Zone' (America/New_York), and 'Credential name' (empty). The 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are in the top right.

Scroll down to the **Port** section of the screen. This section is only present for **Session Manager** SIP entities. Add/verify the entries for **Port**, **Protocol** and **Default Domain** needed to support the registration of the Teo telephones, as shown below. Click **Commit** to save.

The screenshot shows the 'Port' configuration section. It includes input fields for 'TCP Failover port' and 'TLS Failover port', and 'Add' and 'Remove' buttons. Below is a table with 7 items, showing the configuration for three ports. The table has columns for 'Port', 'Protocol', 'Default Domain', and 'Notes'. The 'Filter: Enable' button is in the top right of the table area.

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	sil.miami.avaya.com	
<input type="checkbox"/>	5060	UDP	sil.miami.avaya.com	
<input type="checkbox"/>	5061	TLS	sil.miami.avaya.com	

The following screen shows the SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of the **procr** interface in Communication Manager.

The screenshot shows the 'SIP Entity Details' configuration page for 'C.M. Trunk 1'. The left navigation pane is expanded to 'Routing' > 'SIP Entities'. The main content area has a 'General' tab selected. The 'FQDN or IP Address' field is set to '192.168.10.12'. Other fields include 'Name' (C.M. Trunk 1), 'Type' (CM), 'Notes' (empty), 'Adaptation' (empty), 'Location' (SIL Lab), 'Time Zone' (America/New_York), 'Override Port & Transport with DNS SRV' (unchecked), 'SIP Timer B/F (in seconds)' (4), 'Credential name' (empty), 'Call Detail Recording' (none), and 'SIP Link Monitoring' (Use Session Manager Configuration).

6.5. Entity Links

Navigate to **Routing** → **Entity Links** in the left navigation pane and select **Edit** to review the existing entity link between Session Manager and Communication Manager, or **New** to create a new one (not shown). Enter/verify the data as described next and shown on the screen below. Enter a descriptive **Name**, select the Session Manager SIP entity under **SIP Entity 1** from the drop-down menu. Select the transport **Protocol** used for this link, and the **Port** number on which Session Manager will receive SIP requests from the far-end. Under **SIP Entity 2**, select the Communication Manager SIP entity. Enter the **Port** number on which Communication Manager receives SIP requests from Session Manager. Select **Trusted** under **Connection Policy**. Click **Commit** to save.

The screen below shows the Entity Link to Communication Manager. The protocol and ports defined here must match the values used on the Communication Manager signaling group form in **Section 5.8**.

The screenshot shows the 'Entity Links' configuration page. The left navigation pane is expanded to 'Routing' > 'Entity Links'. The main content area shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Deny New Service. The item is 'SM to CM trunk 1' with SIP Entity 1 'MA_Session Manager', Protocol 'TCP', Port '5060', SIP Entity 2 'C.M. Trunk 1', Port '5060', and Connection Policy 'Trusted'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
* SM to CM trunk 1	* MA_Session Manager	TCP	* 5060	* C.M. Trunk 1	* 5060	Trusted	<input type="checkbox"/>

It should be noted that in a customer environment the Entity Link to Communication Manager would normally use TLS, for security. During the compliance test, TCP was used to facilitate troubleshooting and trace capturing.

6.6. Communication Manager Instance

From the Home screen navigate to **Elements** → **Inventory** → **Manage Elements**. Select **View** to review an existing Communication Manager instance or **New** to create a new one (not shown). Enter/verify the data as shown in the following screens. Set an appropriate **Name**, set the **Type** to **Communication Manager**, add a **Description** (optional) and for the **Node**, enter the ip address of the Communication Manager **procr** interface.

The screenshot shows the 'Edit Communication Manager: CM1_ES' form. The left sidebar contains a navigation menu with 'Inventory' expanded, showing 'Manage Elements', 'Collected Inventory', 'Install and Upgrade Management', 'Manage Serviceability Agents', 'Inventory Management', 'Synchronization', and 'CS 1000 and CallPilot Synchronization'. The main header is 'Home / Elements / Inventory / Manage Elements'. The form title is 'Edit Communication Manager: CM1_ES' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected, showing fields for 'Name' (CM1_ES), 'Type' (Communication Manager), 'Description' (HP Server), and 'Node' (192.168.10.12). There are red asterisks next to 'Name', 'Type', and 'Node'.

In the **Attributes** tap, specify a **Login** and **Password** that has permissions to perform administration tasks on Communication Manager. Other fields keep their default values. Click **Commit** to save.

The screenshot shows the 'Attributes' tab of the 'Edit Communication Manager' form. The 'SNMP Attributes' section has 'Version' set to 'None' (selected with a radio button). The 'Attributes' section has 'Login' set to 'avaya', 'Password' and 'Confirm Password' masked with dots, 'Is SSH Connection' checked, and 'Port' set to '5022'. Red asterisks are present next to 'Login', 'Password', 'Confirm Password', and 'Port'.

6.7. Application and Application Sequence

From the Home screen navigate to **Elements → Session Manager → Application Configuration → Applications**. Select **Edit** to review an existing application or **New** to create a new one (not shown). Enter/verify the data as shown in the following screen. Set an appropriate **Name**, select the Communication Manager **SIP Entity** as seen in **Section 6.4**, and on the **CM System for SIP Entity** field select the Communication Manager instance shown in **Section 6.6**. Click **Commit** (not shown) to save.

The screenshot shows the 'Application Editor' web interface. On the left is a navigation menu with the following items: Session Manager (expanded), Dashboard, Session Manager Administration, Communication Profile Editor, Network Configuration (expanded), Device and Location Configuration, Application Configuration (expanded), and Applications (highlighted in blue). The main content area has a breadcrumb trail: Home / Elements / Session Manager / Application Configuration / Applications. Below the breadcrumb is the title 'Application Editor'. Under the 'Application' heading, there are four fields: '* Name' with the value 'CM-ES App'; '* SIP Entity' with a dropdown menu showing 'C.M. Trunk 1'; '* CM System for SIP Entity' with a dropdown menu showing 'CM1_ES', a 'Refresh' button, and a link 'View/Add CM Systems'; and 'Description' with an empty text box.

Session Manager		Home / Elements / Session Manager / Application Configuration / Applications	
Dashboard		Application Editor	
Session Manager Administration		Application	
Communication Profile Editor		* Name	CM-ES App
Network Configuration		* SIP Entity	C.M. Trunk 1
Device and Location Configuration		* CM System for SIP Entity	CM1_ES Refresh View/Add CM Systems
Application Configuration		Description	
Applications			

Navigate to **Application Configuration → Application Sequences** in the left navigation pane. Select **Edit** to review an existing application or **New** to create a new one (not shown). Enter/verify the data as shown in the following screen. Set an appropriate **Name** and **Description**. Select the application defined previously from the list of **Available Applications**, by clicking the “+” sign next to the application name. The selected application will then populate the **Applications in this Sequence** section. Click **Commit** to save.

Session Manager

Dashboard

Session Manager Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

Applications

Application Sequences

Conference Factories

Implicit Users

NRS Proxy Users

System Status

System Tools

Performance

Home / Elements / Session Manager / Application Configuration / Application Sequences

Help ?

Commit Cancel

Application Sequence Editor

Application Sequence

*Name

CM_ES App Seq

Description

HP Server

Applications in this Sequence

Move First

Move Last

Remove

1 Item

	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	⬆ ⬇ ⬆	CM-ES App	C.M. Trunk 1	<input checked="" type="checkbox"/>	

Select : All, None

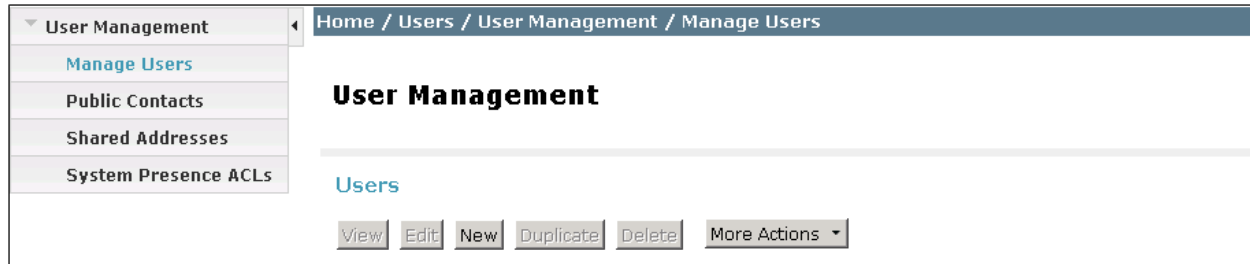
Available Applications

2 Items Refresh Filter: Enable

	Name	SIP Entity	Description
+	CM-ES App	C.M. Trunk 1	
+	Lab-HG CM-APP	HG CM Trunk 1	

6.8. Manage Users

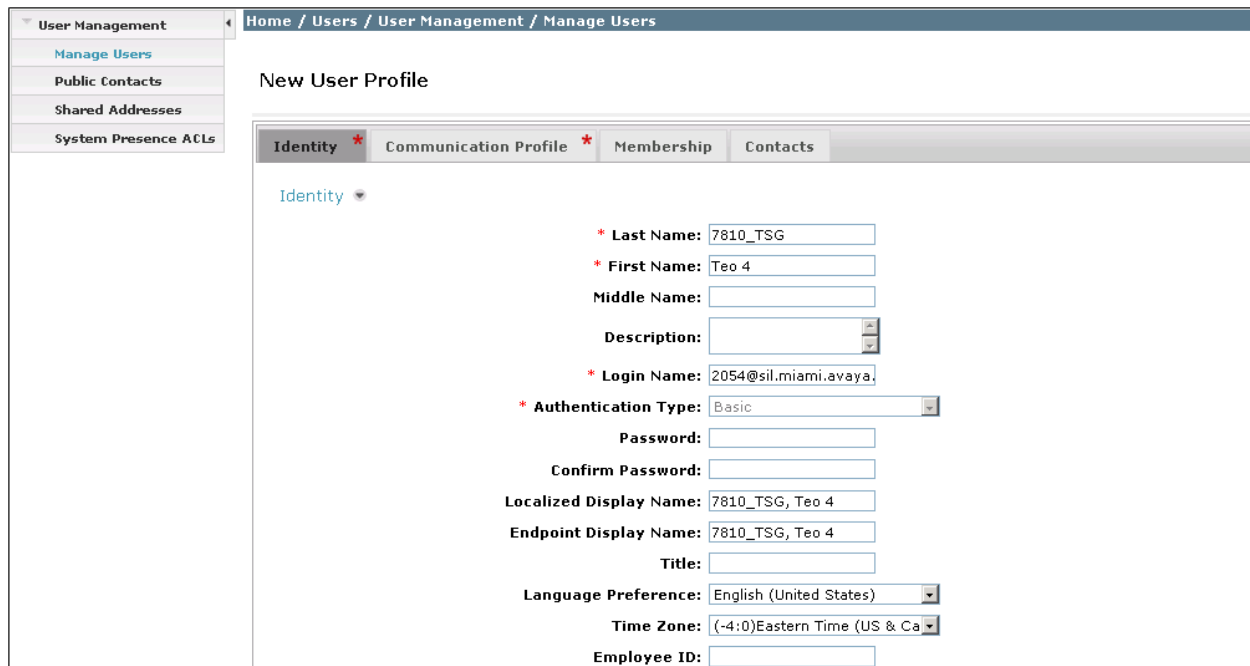
From the Home screen navigate to **Users → User Management → Manage Users → New** to create the profiles for the Teo users.



The screenshot shows the 'Manage Users' page in the User Management section. The left sidebar contains a menu with 'User Management' expanded, showing 'Manage Users' (highlighted), 'Public Contacts', 'Shared Addresses', and 'System Presence ACLs'. The main content area has a breadcrumb trail 'Home / Users / User Management / Manage Users' and a title 'User Management'. Below the title is a 'Users' section with buttons for 'View', 'Edit', 'New', 'Duplicate', 'Delete', and a 'More Actions' dropdown.

6.8.1. Identity Tab

On the **New User Profile** form, **Identity** tab, enter a meaningful description for the **Last Name** and **First Name** fields. Enter the **Login Name** in “extension@domain” format in this field (2054@sil.miami.avaya.com was used in the example). Keep the **Authentication Type** as **Basic**, the default value. Enter a preferred display name in the **Localized Display Name** and **Endpoint Display Name** fields. Select the **Language Preference** and **Time Zone** for the endpoint.



The screenshot shows the 'New User Profile' form with the 'Identity' tab selected. The form contains the following fields and values:

- Last Name:** 7810_TSG
- First Name:** Teo 4
- Middle Name:** (empty)
- Description:** (empty)
- Login Name:** 2054@sil.miami.avaya.com
- Authentication Type:** Basic
- Password:** (empty)
- Confirm Password:** (empty)
- Localized Display Name:** 7810_TSG, Teo 4
- Endpoint Display Name:** 7810_TSG, Teo 4
- Title:** (empty)
- Language Preference:** English (United States)
- Time Zone:** (-4:0)Eastern Time (US & Ca)
- Employee ID:** (empty)

6.8.2. Communication Profile Tab

On the **Communication Profile** tab, enter and confirm the **Communication Profile Password** for the user. This is the password that the user of the Teo telephone must enter to log in to the phone. Keep **Primary** under the **Name** field and the **Default** box checked. Click **New** on the **Communication Address** section.

The screenshot shows the 'Communication Profile' tab selected in a navigation bar with 'Identity', 'Membership', and 'Contacts'. Below the tabs, the 'Communication Profile' section has two password fields: 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these are buttons for 'New', 'Delete', 'Done', and 'Cancel'. A table lists communication profiles with one entry, 'Primary', which is selected. Below the table, the 'Name' field is set to 'Primary' and the 'Default' checkbox is checked. The 'Communication Address' section below has 'New', 'Edit', and 'Delete' buttons. It contains a table with columns 'Type', 'Handle', and 'Domain', which is currently empty with the text 'No Records found'.

On the **Communication Address** section newly expanded fields, select **Avaya SIP** from the **Type** pull-down list. On the **Fully Qualified Address** field, enter the extension number assigned to the Teo user, and select the enterprise domain from the list, as shown. Click the **Add** button.

The screenshot shows the 'Communication Address' section with 'New', 'Edit', and 'Delete' buttons. It features a table with columns 'Type', 'Handle', and 'Domain', which is empty with the text 'No Records found'. Below the table, the 'Type' field is a dropdown menu set to 'Avaya SIP'. The 'Fully Qualified Address' field is split into two parts: an extension number '2054' and a domain 'sil.miami.avaya.com' selected from a dropdown. At the bottom right are 'Add' and 'Cancel' buttons.

Select the **Session Manager Profile** check box. Under **SIP Registration**, select the SIP Entity of the **Primary Session Manager**, as seen on **Section 6.4**, from the drop-down list. Under **Application Sequences**, for the **Origination Sequence** and **Termination Sequence** fields, select the Communication Manager application sequence, as seen on **Section 6.7**. Under the **Home Location** field, select the **SIL Lab** location defined in **Section 6.3**.

The screenshot shows the 'Session Manager Profile' configuration interface. It includes sections for SIP Registration, Application Sequences, and Call Routing Settings. The 'Primary Session Manager' is set to 'MA_Session Manager', and the 'Home Location' is set to 'SIL Lab'. A table on the right shows the Primary, Secondary, and Maximum values for the Session Manager.

Primary	Secondary	Maximum
11	0	11

Select the **CM Endpoint Profile** check box. From the **System** drop-down list, select the Communication Manager instance, as defined on **Section 6.6**. Select **Endpoint** for the **Profile Type**. In the **Extension** field, enter the extension number that will be created on Communication Manager for the new user. For the compliance test, template **9600SIP_DEFAULT_CM_6_2** was used. Once the template is selected, the **Set Type** field is populated with **9600SIP**, and the **Port** field with **IP**.

The screenshot shows the 'CM Endpoint Profile' configuration interface. It includes fields for System, Profile Type, Extension, Template, Set Type, Security Code, Port, Voice Mail Number, and Preferred Handle. The 'System' is set to 'CM1_ES', 'Profile Type' is 'Endpoint', 'Extension' is '2054', 'Template' is '9600SIP_DEFAULT_CM_6_2', 'Set Type' is '9600SIP', and 'Port' is 'IP'.

Clicking the **Endpoint Editor** button on the previous screen allows to edit Communication Manager station data, like features and buttons. In the example on the next screen, under the **General Options** tab, **Class of Restriction (COR) 1**, **Class of Service (COS) 1** and **Coverage Path 2** were assigned to the user. Coverage Path 2, which was used in the lab environment for

voicemail coverage to Messaging, was previously defined as part of the Messaging installation, and its configuration is not covered in these Application Notes.

* System	CM1_ES	* Extension	2054
* Template	9600SIP_DEFAULT_CM_6_2	* Set Type	9600SIP
* Port	IP	* Security Code	
Name			

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)	Group Membership (M)			

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	2054	* Message Lamp Ext.	2054
* Tenant Number	1		
* SIP Trunk	Qaar	Type of 3PCC Enabled	None
Coverage Path 1	2	Coverage Path 2	
Lock Message	<input type="checkbox"/>	Localized Display Name	
Multibyte Language	Not Applicable		

*Required

Done Cancel

Select **Done** to return to the Communications Profile tab. Press **Commit** (not shown) to save.

6.9. Synchronize Communication Manager Data with System Manager Database

Once all configuration tasks have been completed, from the System Manager Home screen, navigate to **Elements** → **Inventory** → **Synchronization** → **Communication System**. Select the Communication Manager entity to be synchronized. Select **Initialize data for selected devices**. Select **Now** or **Schedule** to perform the synchronization immediately or at a specified time. If **Now** is selected, pressing the **Refresh** button will show the progress of the synchronization tasks, under the **Sync. Status** field. Once the synchronization is complete, **Completed** should be displayed under **Sync. Status**, like shown on the screen below.

Inventory	Home / Elements / Inventory / Synchronization / Communication System
-----------	--

Manage Elements
Collected Inventory
Install and Upgrade Management
Manage Serviceability Agents
Inventory Management
Synchronization
Communication System
B5800 Branch Gateway
Messaging System
CS 1000 and CallPilot Synchronization

Synchronize CM Data and Configure Options

Note: Please avoid any administration task on CM while synchronization or audit is in progress.

Synchronize CM Data/Launch Element Cut Through

Element Name	FQDN/IP Address	Last Sync Time	Last Translation Time	Sync Type	Sync Status	Location	Software Version	CM Notification
<input checked="" type="checkbox"/> CM1_ES	192.168.10.12	April 4, 2013 5:09:37 PM - 04:00	5:19 pm THU APR 4, 2013	Initialization	Completed		R016x.02.0.823.0	false
<input type="checkbox"/> Lab-HG_CM	172.16.5.12	April 3, 2013 11:00:02 PM - 04:00	10:00 pm WED APR 3, 2013	Incremental	Completed		R016x.02.0.823.0	false

Select : All, None

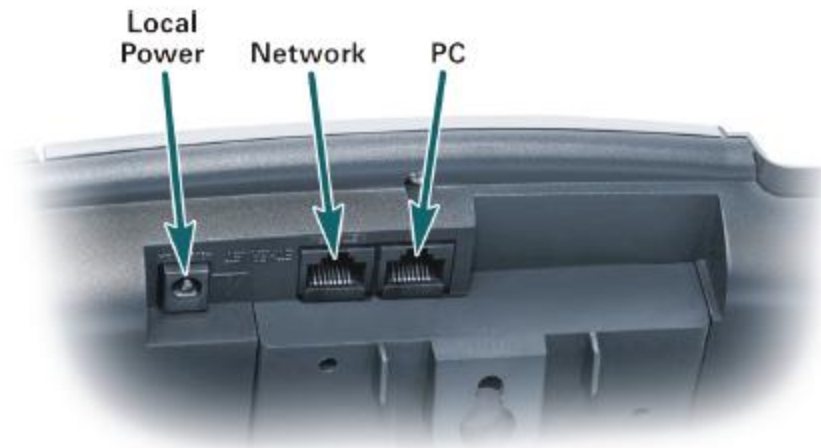
☒ Initialize data for selected devices
☐ Incremental Sync data for selected devices
☐ Execute 'save trans all' for selected devices
☐ Audit

Now Schedule Cancel Launch Element Cut Through View Audit Report

7. Configure Teo IP Phones

7.1. Power and Network Connection

Connect power to the Teo telephone using the **Local Power** option, or in models where PoE is supported, connecting a CAT 5 or better cable to the **Network** jack of the telephone. Both the Teo IP Phones 7810 and the 7810PoE-TSGB models used in the compliance test support PoE, and they were connected to the LAN via an Avaya C364T-PWR PoE switch. A DHCP server on the LAN segment provided IP addressing for the telephones.



7.2. Telephone Configuration

The configuration steps in this section represent the basic steps required to achieve the registration of the Teo telephones with Session Manager. A detailed description of the different menu options on the telephones is beyond the scope of these Application Notes. For detailed information on the installation and configuration of the Teo IP Phones, see **References [6] and [7]**.

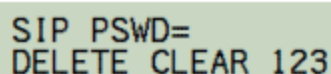
Once power is applied and the telephone initializes, the display shows different progress messages and it will then prompt for the **LINE ID**. This is the extension number assigned to the user, previously in **Section 6.8.2**. Extension **2054** was used in the example and it was entered at the prompt below. Press the **OK** key on the phone when the entry is completed.

```
LINE ID=  
DELETE CLEAR 123
```

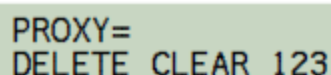
The telephone prompts next for the Authentication ID. Enter the same extension number that was assigned to the **LINE ID**. Press the **OK** key on the phone when the entry is completed.

```
AUTH ID=  
DELETE CLEAR 123
```

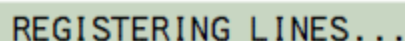
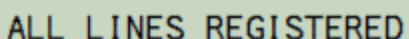
Next the phone will prompt for the SIP Authentication Password. This is the **Communication Profile Password** assigned to the user previously in **Section 6.8.2**. Press the **OK** key on the phone when the entry is completed.

A green rectangular screen with a black border. The text "SIP PSWD=" is on the first line, and "DELETE CLEAR 123" is on the second line.

The next prompt will be for the proxy server IP address, if this address has not been previously provided by DHCP. This is the address of the Session Manager signaling interface, **192.168.10.32** in the reference configuration. Press the **OK** key on the phone when the entry is completed.

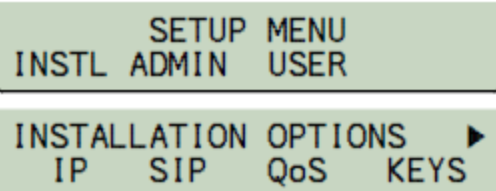
A green rectangular screen with a black border. The text "PROXY=" is on the first line, and "DELETE CLEAR 123" is on the second line.

At this point, the telephone will register with Session Manager. Upon successful registration, all affected line key indicators will turn solid green momentarily, and then will go out. The following status messages will be displayed.

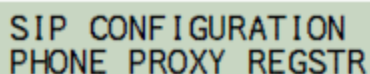
A green rectangular screen with a black border. The text "REGISTERING LINES..." is centered on the screen.A green rectangular screen with a black border. The text "ALL LINES REGISTERED" is centered on the screen.

The idle display will then appear, indicating that the phone is ready for use.

Once the telephone is registered, the SIP Configuration menu can be accessed by pressing the **SETUP** key on the phone and selecting **INSTL → SIP**.

Two stacked green rectangular screens with black borders. The top screen shows "SETUP MENU" on the first line and "INSTL ADMIN USER" on the second line. The bottom screen shows "INSTALLATION OPTIONS" on the first line with a right-pointing arrow, and "IP SIP QoS KEYS" on the second line.

Once on the SIP Configuration screen, selecting one of the available submenus allows to make changes or to review the following parameters, if needed:

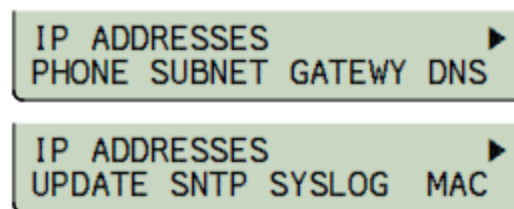
A green rectangular screen with a black border. The text "SIP CONFIGURATION" is on the first line, and "PHONE PROXY REGSTR" is on the second line.

- **PHONE** – Domain name, port, and RTP start port for the telephone.
- **PROXY** – SIP Proxy server IP address and port.
- **REGSTR** – Registration enable, SIP Registrar server IP address and port.

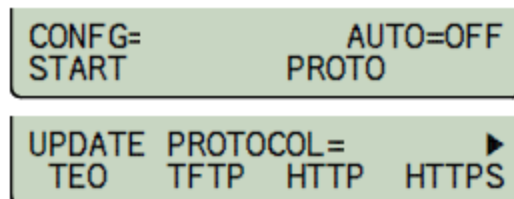
7.3. Configuration Update

Additionally, Teo Tech telephones settings can be configured using XML settings files, loaded to the telephones from a FTP, TFTP or HTTP update server. Even though the majority of settings changes during the compliance test were made directly on the telephones, XML files were used to make some changes that could not be achieved by the use of the telephone menus. These files were placed in the root folder of a HTTP server on the enterprise network, and re-named to match each phone's hardware MAC address.

The IP address of the update server can be assigned by DHCP, or can be manually set on the phone. To manually set the IP address, click **SETUP → INSTL → IP** (not shown). Press the right arrow key and select **UPDATE**. Enter the IP Address of the FTP/TFTP or HTTP server where the update files can be found. Press the **OK** key when the entry is completed.



To setup the protocol used by the configuration update server, press **SETUP → INSTL**. Press the right arrow key for more and select **UPDATE → CONFIG** (not shown). Select **PROTO** and choose the correct update server protocol. Press **OK** and the **SETUP** key to exit. To initiate the configuration update, return to the **CONFIG** menu as described above and press **START**.



The example below shows the XML file used to change the transport protocol on the Teo telephones from the default transport protocol UDP to TLS, for testing.

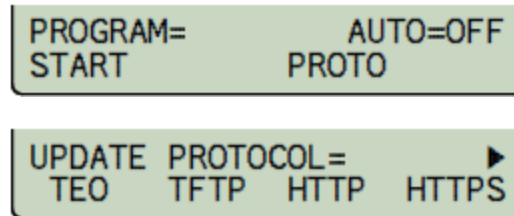
```
<?xml version="1.0" encoding="utf-8" ?>
<!-- This is an XML file for use in testing on the pbxnsip platform. -->
- <TEO_settings schema_vers="2.0">
- <TEO_phone model="ALL">
  <!-- General Phone Settings -->
  <sip_transport>TLS</sip_transport>
  <tls_require_cert>OFF</tls_require_cert>
  <sip_proxy_port>5061</sip_proxy_port>
  <sip_reg_port>5061</sip_reg_port>
  <phone_port>5061</phone_port>
</TEO_phone>
</TEO_settings>
```

7.4. Software Update

For the compliance test, the file “**signed_XX_04_12.zip**” containing the firmware load and upgrade settings file for the telephones was unzipped and its content placed in the root directory of the HTTP update server, as seen on the screen below.

Name	Size	Type	Date Modified
TEO_05.04.12		File Folder	3/15/2013 2:40 PM
TEO_06.04.12		File Folder	3/15/2013 2:40 PM
TEO_07.04.12		File Folder	3/15/2013 2:40 PM
TC57000B	1 KB	XML Document	3/15/2013 9:37 AM

To setup the protocol used by the software update server, press **SETUP → INSTL**. Press the right arrow key for more and select **UPDATE → PRGRM** (not shown). Select **PROTO** and choose the correct update server protocol. Press **OK** and the **SETUP** key to exit. To initiate the software update, return to the **PROGRAM** menu as described above and press **START**



8. Verification Steps

This section provides verification steps that may be used in the field to verify that the solution is configured properly. To verify the registration of the Teo telephones with Session Manager, from the System Manager web interface Home screen, navigate to **Elements → Session Manager → System Status → User Registrations**. The Primary (**Prim**) box under the **Registered** column should be checked and the **Address** and **IP Address** fields should be populated if the telephone has successfully registered, as shown on the screen below.

Home / Elements / Session Manager / System Status / User Registrations

Help ?

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View

User

Force Unregister

AST Device Notifications:

Reboot

Reload

Failback

As of 10:43 AM

Customize

Advanced Search

15 Items Refresh Show ALL

Filter: Enable

	Details	Address	Login Name	First Name	Last Name	Location	IP Address	Remote Office	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
<input type="checkbox"/>	► Show	2003@sil.miami.avaya.com	2003@sil.miami.avaya.com	Ext 2003	SIP	SIL Lab	192.168.10.202:5060	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	2005@sil.miami.avaya.com	Ext 2005	Softphone SIP	SIL Lab	---	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	2006@sil.miami.avaya.com	ext 2006	SIP	SIL Lab	---	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	2010@sil.miami.avaya.com	A175	Flare	SIL Lab	---	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	---	2011@sil.miami.avaya.com	A175	Flare_2	SIL Lab	---	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2012@sil.miami.avaya.com	2012@sil.miami.avaya.com	2012	SIP, 9608	SIL Lab	192.168.10.204:5060	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2015@sil.miami.avaya.com	2015@sil.miami.avaya.com	Ext. 2015, 9620	SIP	SIL Lab	192.168.10.62:5060	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2051@sil.miami.avaya.com	2051@sil.miami.avaya.com	Teo 1	7810_TSG	SIL Lab	192.168.10.180:5060	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2052@sil.miami.avaya.com	2052@sil.miami.avaya.com	Teo 2	7810_TSG	SIL Lab	192.168.10.181:5060	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	► Show	2053@sil.miami.avaya.com	2053@sil.miami.avaya.com	Teo 3	7810	SIL Lab	192.168.10.182:5061	<input type="checkbox"/>	1/1	<input type="checkbox"/>	<input checked="" type="checkbox"/> (AC)	<input type="checkbox"/>	<input type="checkbox"/>

Clicking **Show** under the **Details** column on a specific line will show additional information for that user. The example below shows additional **Registration** information for extension 2051.

<input type="checkbox"/>	► Show	2015@sil.miami.avaya.com	2015@sil.miami.avaya.com	Ext. 2015, 9620	SIP	SIL Lab	192.168.10.62:5060
<input type="checkbox"/>	▼ Hide	2051@sil.miami.avaya.com	2051@sil.miami.avaya.com	Teo 1	7810_TSG	SIL Lab	192.168.10.180:5060

User	Registration	Device	Simultaneous	History
------	--------------	--------	--------------	---------

Registration Address	2051@sil.miami.avaya.com
IP Address	192.168.10.180:5060
Active Controller	MA_Session Manager
PPM Subscription Time (AC)	---
Event Subscriptions	message-summary dialog
Instance Id	"<urn:uuid:c39b0000-4f96-1a00-1000-00048d002130>"
Primary Registration Time	Thu Mar 21 21:47:46 EDT 2013
Primary Registration Interrupted Time	---
Primary Registration Interrupted	0 d 0 hr 0 min
Secondary Registration Time	---
Secondary Registration Interrupted Time	---
Secondary Registration Interrupted	---
Survivable Registration Time	---
Survivable Registration Interrupted Time	---
Survivable Registration Interrupted	---

For troubleshooting and traffic analysis, **traceSM** is a powerful command line tool that can be used in Session Manager. Login to the Session Manager management interface to run this command.

9. Conclusion

This document describes the configuration steps required to integrate the Teo IP Phones 7810 and 7810 TSG-6 Series to Avaya Aura® Session Manager 6.3 and Avaya Aura® Communication Manager 6.2.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the observation/limitation described in **Section 2.2**.

10. Additional References

This section references the Avaya and Teo product documentation relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>

- [1] *Administering Avaya Aura® Communication Manager*, Release 6.2, December 2012, Document ID 03-300509.
- [2] *Administering Avaya Aura® Communication Manager Server Options*, Release 6.2, December 2012, Document ID 03-603479.
- [3] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.2, December 2012, Document ID 555-245-205.
- [4] *Administering Avaya Aura® Session Manager*, Release 6.3, December 2012.

The following Teo documentation may be found at www.teotech.com.

- [5] *IP Telephone Network Administration Guide*, March 2013, Document ID 13-280132.
- [6] *IP Phone 7810 TSG Series Installations Instructions*, March 2013, Document ID 13-280138.
- [7] *IP Phone 7810 Installation Instructions*, Document ID 13-280124, March 2013.
- [8] *IP Phone 7810 TSG Series User Guide*, March 2013, Document ID 14-280211.
- [9] *IP Phone 7810 User Guide*, March 2013, Document ID 14-280201.

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.