Avaya Solution & Interoperability Test Lab

Application Notes for Inisoft synTelate Enterprise Agent with Avaya Proactive Outreach Manager – Issue 1.1

Abstract

These Application Notes describe the configuration steps required to integrate the Inisoft synTelate Enterprise Agent with Avaya Proactive Outreach Manager. Inisoft synTelate Enterprise Agent integrates with Avaya Proactive Outreach Manager using the Agent Desktop API.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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.

KJA; Reviewed:
SPOC 1/28/2016
Solution & Interoperability Test Lab Application Notes
©2016 Avaya Inc. All Rights Reserved.
1 of 35
synTelateSynPOM

1. Introduction

These Application Notes describe the configuration steps required to integrate Inisoft synTelate Enterprise Agent with Avaya Proactive Outreach Manager.

Inisoft synTelate Enterprise Agent uses the Agent Desktop API of Avaya Proactive Outreach Manager (POM) to integrate agent functionality and manage agents using agent desktops. Agents log on via Inisoft synTelate Enterprise. Inisoft synTelate Enterprise Agent is a thick client application that is installed on a Windows based agent desktop. The Inisoft synTelate Enterprise solution consists of synTelate Designer, synTelate Supervisor, synTelate Enterprise, and a generic Database server. synTelate Designer is a graphical tool used to define the call flow and custom agent desktop screen. Configuration for Avaya POM is performed on synTelate Enterprise. When Inisoft synTelate Enterprise Agent is launched, to connect to Avaya POM, configuration is retrieved from synTelate Enterprise. During the compliance testing, Avaya POM was configured as CCElite to allow communications with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Avaya POM was installed on Avaya Aura® Experience Portal. Calls to and from Experience Portal were routed via a SIP trunk to Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The feature tests were performed manually. General test approach was to ensure that the features provided by Agent Desktop API were implanted on synTelate Enterprise Agent.

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

Interoperability compliance testing included feature and serviceability testing. The feature testing focused on the following functionality:

- Agents Login and Logout.
- Agent states: Ready, Not Ready and changing Aux Reason code.
- Nailing agents and new call notifications.
- Updating contact details.
- Callbacks.
- Adding and removing contacts from Do Not Call (DNC) lists.
- Call features such as: Hold/Unhold, send DTMF, Consult, Transfer and Conference

The serviceability testing focused on verifying the ability of the synTelate server to recover from adverse conditions, such as power failures and network disconnects.

2.2.　Test Results

All test cases were executed and verified.

2.3.　Support

For technical support on the synTelate Enterprise Agent, contact Inisoft via phone, email, or internet.

- **Phone:**　+44 (0)800 668 1290
- **Email:**　support@inisoft.co.uk
- **Web:**　www.syntelate.com

3. Reference Configuration

Figure 1 illustrates the configuration used for testing. In this configuration, Experience Portal interfaces with Session Manager via SIP. POM was installed as co-resident on Experience Portal. Application Enablement Services interfaced with POM via a CTI link. The synTelate server hosted the synTelate Enterprise solution. The synTelate clients were used as agent desktops. synTelate server and clients were deployed as virtual appliances.
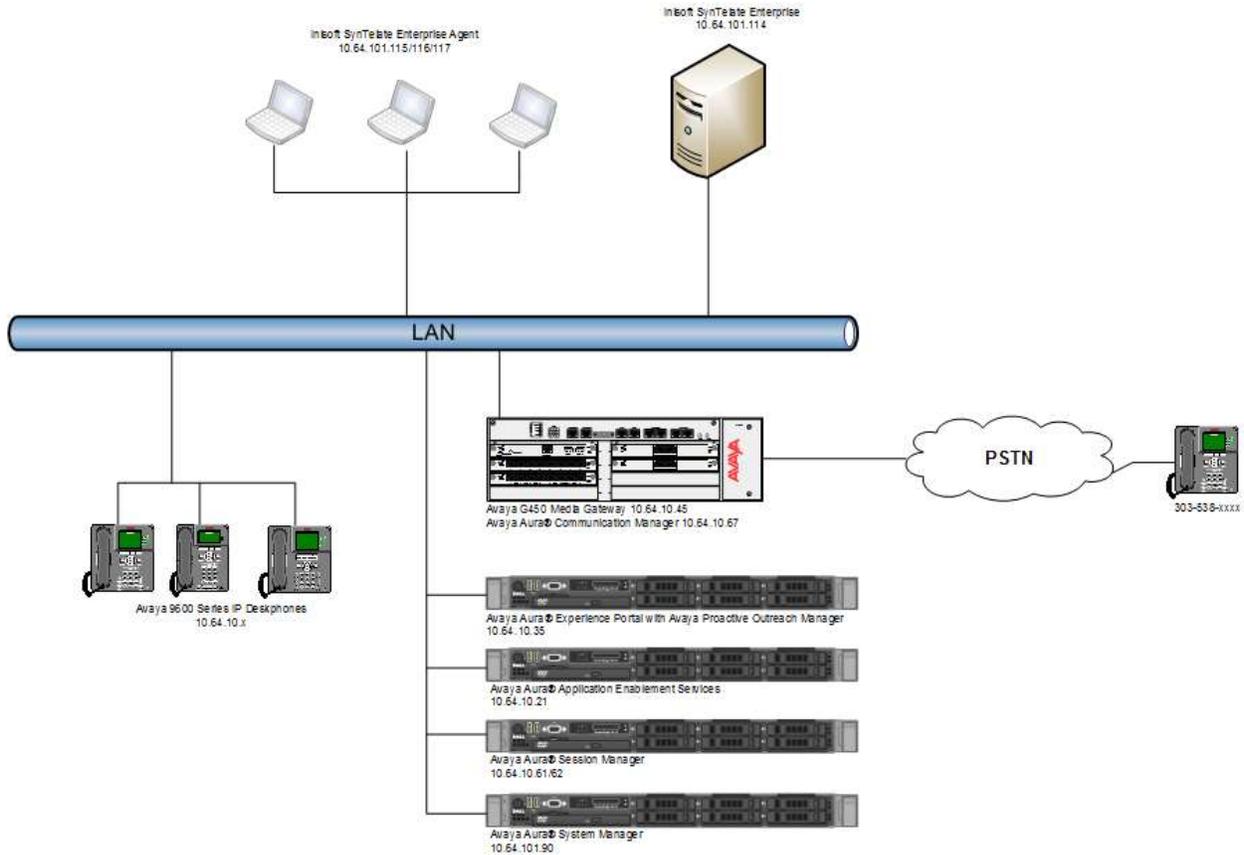
Figure 1: Configuration of Avaya Proactive Outreach Manager with synTelate

3.1. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® Experience Portal	7.0.0.0.6605
Avaya Proactive Outreach Manager	03.00.01.00.150
Avaya Aura® Application Enablement Services	6.3.3
Avaya Aura® System Manager	6.3.12.9.3022
Avaya Aura® Session Manager	6.3.12.0.631208
Avaya Aura® Communication Manager	R016x.03.0.124.0-21754
Inisoft synTelate Enterprise Agent running on Windows 7 Enterprise	4.4
Inisoft synTelate Enterprise running on Windows Server 2008 R2 Server	4.4.5.6

4. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager via the System Access Terminal (SAT).

4.1. Administer Hunt Groups

This section provides the Hunt Group configuration for the call center agents. This hunt group will later be configured in POM.

Agents will log into Hunt Group 1 configured below. Provide a descriptive name and set the **Group Extension** field to a valid extension. Enable the **ACD**, **Queue**, and **Vector** options. This hunt group will be specified in the Agent LoginIDs configured in **Section 4.2**.

```
add hunt-group 1                                         Page   1 of   4
                             HUNT GROUP

         Group Number: 1                                     ACD? y
           Group Name: Skill 1                             Queue? y
      Group Extension: 11001                              Vector? y
           Group Type: ucd-mia
                   TN: 1
                  COR: 1                    MM Early Answer? n
        Security Code:                 Local Agent Preference? n
 ISDN/SIP Caller Display:

           Queue Limit: unlimited
Calls Warning Threshold:       Port:
 Time Warning Threshold:       Port:
```

On Page 2 of the Hunt Group form, enable the **Skill** option.

```
add hunt-group 1                                         Page   2 of   4
                             HUNT GROUP

                    Skill? y      Expected Call Handling Time (sec): 180
                      AAS? n
                 Measured: none
    Supervisor Extension:


     Controlling Adjunct: none




  Multiple Call Handling: none


 Timed ACW Interval (sec):        After Xfer or Held Call Drops? n
```

4.2. Administer Agent IDs

This section provides the Agent Login IDs for the agents.

Add an Agent LoginID for each agent in the call center as shown below. In this configuration, agent login IDs 2501 and 2502 were created for two agents.

```
add agent-loginID 2501                                         Page   1 of   2
                              AGENT LOGINID

                Login ID: 2501                                    AAS? n
                    Name: IP Agent 1                            AUDIX? n
                      TN: 1                          LWC Reception: spe
                     COR: 1                  LWC Log External Calls? n
           Coverage Path:                  AUDIX Name for Messaging:
           Security Code: 1234
                                          LoginID for ISDN/SIP Display? n
                                                        Password: 123456
                                         Password (enter again): 123456
                                                     Auto Answer: station
                                             MIA Across Skills: system
                                   ACW Agent Considered Idle: system
                                   Aux Work Reason Code Type: system
                                      Logout Reason Code Type: system
                 Maximum time agent in ACW before logout (sec): system
                                         Forced Agent Logout Time:   :


      WARNING:  Agent must log in again before changes take effect
```

On Page 2 of the Agent LoginID form, set the skill number (**SN**) to hunt group 1, which is the hunt group (skill) that the agents will log into.

```
add agent-loginID 2501                                         Page   2 of   2
                              AGENT LOGINID
      Direct Agent Skill:                           Service Objective? n
Call Handling Preference: skill-level              Local Call Preference? n

    SN   RL SL         SN   RL SL
 1:  1       1      16:
 2:                 17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
```

4.3. Administer Stations

This section provides the extension that agents will log on.

Add a **station** for each extension in the call center as shown below. In this configuration, station 25001 and station 25002 were created.

```
add station 25001                                              Page   1 of   5
                                 STATION

Extension: 25001                      Lock Messages? n              BCC: 0
    Type: 9630                       Security Code: 123456           TN: 1
    Port: S00217                  Coverage Path 1:                  COR: 1
    Name: IP Station 1            Coverage Path 2:                  COS: 1
                                     Hunt-to Station:            Tests? y
STATION OPTIONS
                                         Time of Day Lock Table:
             Loss Group: 19      Personalized Ringing Pattern: 1
                                         Message Lamp Ext: 25001
           Speakerphone: 2-way          Mute Button Enabled? y
      Display Language: english            Button Modules: 0
 Survivable GK Node Name:
         Survivable COR: internal        Media Complex Ext:
  Survivable Trunk Dest? y                   IP SoftPhone? y

                                        IP Video Softphone? n
                      Short/Prefixed Registration Allowed: default

                                       Customizable Labels? y
```

Note: Please note that the configuration of SIP trunk and routing between Communication Manager and Session Manager was preconfigured and is not shown in this document.

5. Configure Avaya Aura® Experience Portal and Avaya Proactive Outreach Manager

This section covers the administration of Experience Portal. Configuration for POM is also covered in the section as POM was co resident on Experience Portal

Experience Portal is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter http://[IP-Address]/ as the URL in an internet browser, where IP-Address is the IP address of the EPM. Log in using the Administrator user role. The screen shown below is displayed.

Note: Some of the screens in this section are shown after the Experience Portal had been configured. Don't forget to save the screen parameters as one configures Avaya Aura® Experience Portal.

KJA; Reviewed:
SPOC 1/28/2016

Solution & Interoperability Test Lab Application Notes
©2016 Avaya Inc. All Rights Reserved.

9 of 35
synTelateSynPOM

5.1. Configure a SIP VoIP Connection

To configure an SIP connection, navigate to the **VoIP Connections** page and then click on the **SIP** tab (not shown) and select **Add**. On the **Change SIP Connection** page, configure as follows:

- Set **Enable** to **Yes**.
- Set **Proxy Transport** to **TCP**.
- For **Proxy Server**:
    - Type in the Session Manager SIP interface IP address in **Address**.
    - Type in the Session Manager SIP Port in **Port**.
- Set **Listener Port** to **5060**.
- Set **SIP Domain** to **avaya.com**, as configured in Session Manager.
- Type in a value for **Maximum Simultaneous Calls**, as needed.
- Select **All Calls can be either inbound or outbound**.

5.2. Verify Applications

Note that the applications needed for POM were configured during POM installation. To view the list of application, navigate to **System Configuration → Applications**.

KJA; Reviewed:
SPOC 1/28/2016

Solution & Interoperability Test Lab Application Notes
©2016 Avaya Inc. All Rights Reserved.

11 of 35
synTelateSynPOM

5.3.   Configure POM

When POM is installed on Experience Portal, a sub menu is added to EPM. On the left pane, select **POM Home** under **POM**. All configurations for POM are performed from this page, **POM Home**.
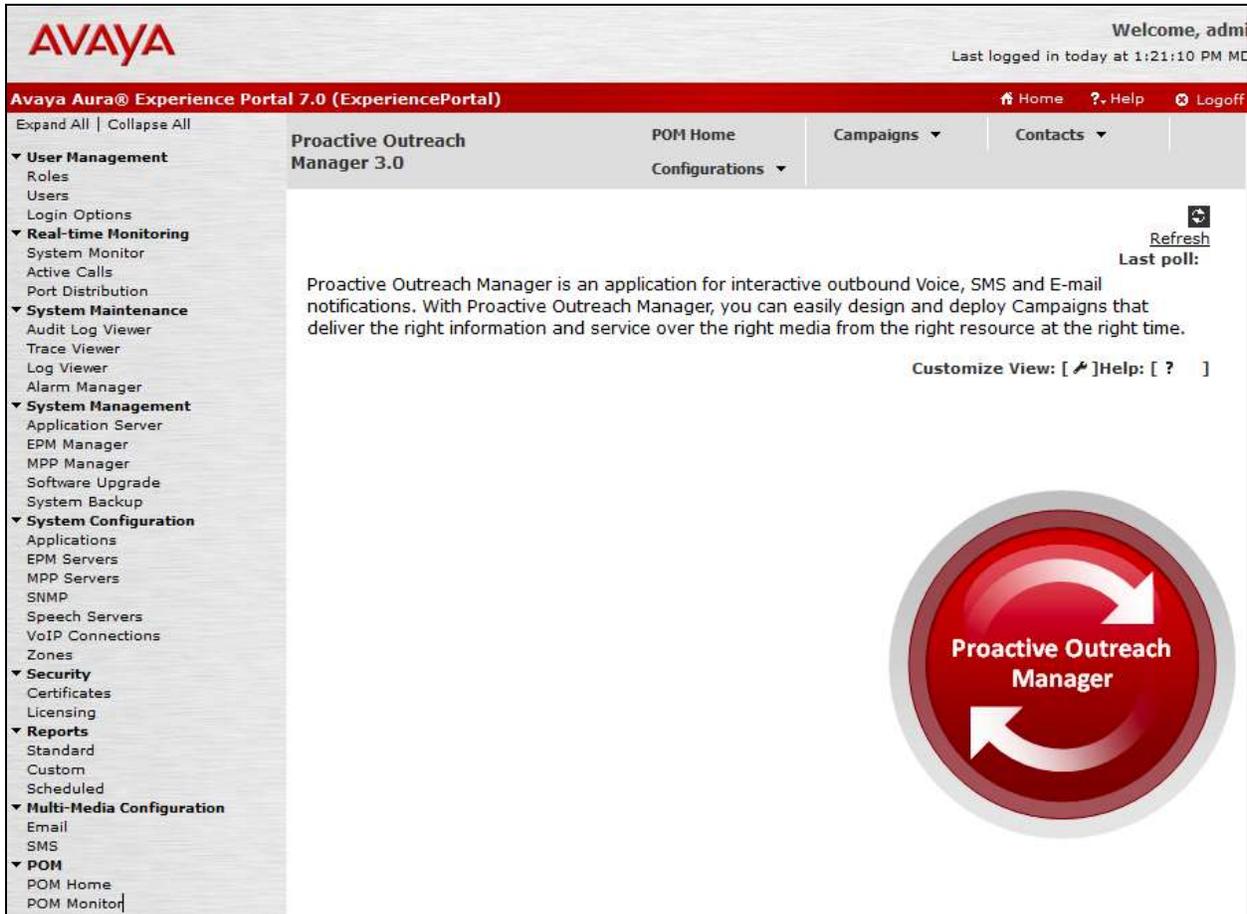
5.4. Add POM Server

From **POM Home**, hover over **Configurations** and select **POM Servers**; click **Add** to add a POM server. On the **Add POM Server** page, type in a name in **POM Server Name** and type in the POM IP Address in **POM Server IP Address** and select **Continue**. Note that since POM was installed on the same server as Experience Portal, IP Address of Experience Portal was used.

On the **Edit POM Server** page check the box for **Trust this certificate** and select **Save**.

5.5. Configure POM Server

Outbound settings will need to be configured for POM to place outbound calls. Navigate to **Configurations → POM Servers → Outbound Setting** (not shown). On the **Voice Servers** page, click on the name of Voice Server; **EPM**, in this case.

On the **Edit Voice Server** page, type in values for **User Name** and **Password**, as configured for Experience Portal. This username and password is obtained from the **Outcall** section of **System Configuration → EPM Server → EPM Settings**.

5.6. Configure CTI

From **POM Home**, navigate to **Configurations → CC Elite Configurations** and select **Add CTI Detail** under **CTI Configuration** (not shown). On the **Add CTI Detail** page, configure as follows:

- Type in a name in **CTI group name**.
- Type in the Communication Manager IP Address in **CM IP address**.
- Type in the username and password in **CM Login** and **CM Password**.
- Type in the AES IP Address in **AES IP address**.
- From the **CTI group role** drop down menu, select **Active**.

Solution & Interoperability Test Lab Application Notes

On the **Configure CTI setup details, CMS setup details and POM Skills** page, select **Add Skill** (not shown). Type in the skill as configured in **Section 4.1** for **CC Elite Skill Number**, type in a name in **POM Skill Name** and select **outbound** from the **Skill Type** drop down menu.

5.7. Configure Contacts

From **POM Home**, navigate to **Contacts → Contact Lists** and select **Add**. Type in a name in **Name** and brief **Description** and select **Save**.
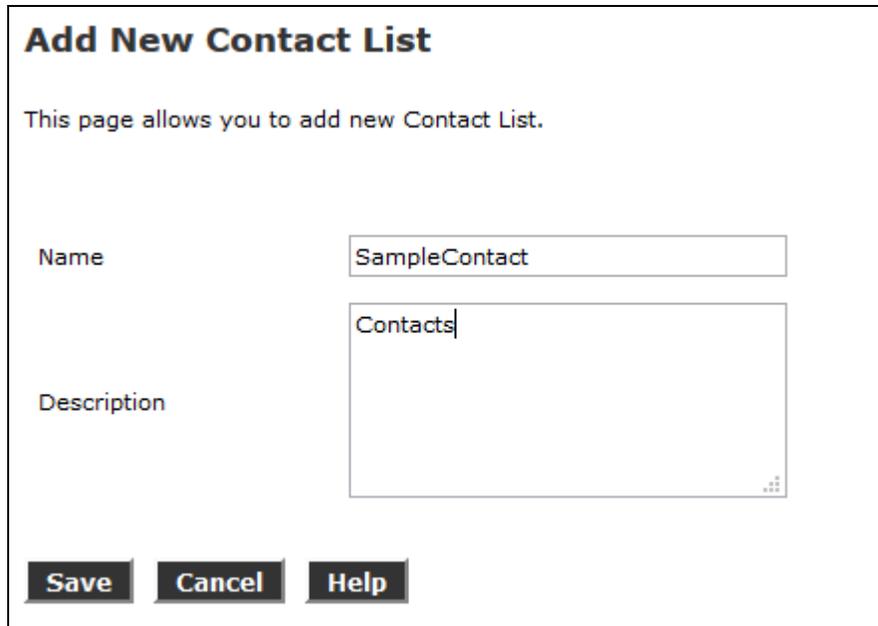
On the next page, select **Upload Contacts now** (not shown). Select **Browse**, and browse to the location of .csv for the contacts and select **Upload**.
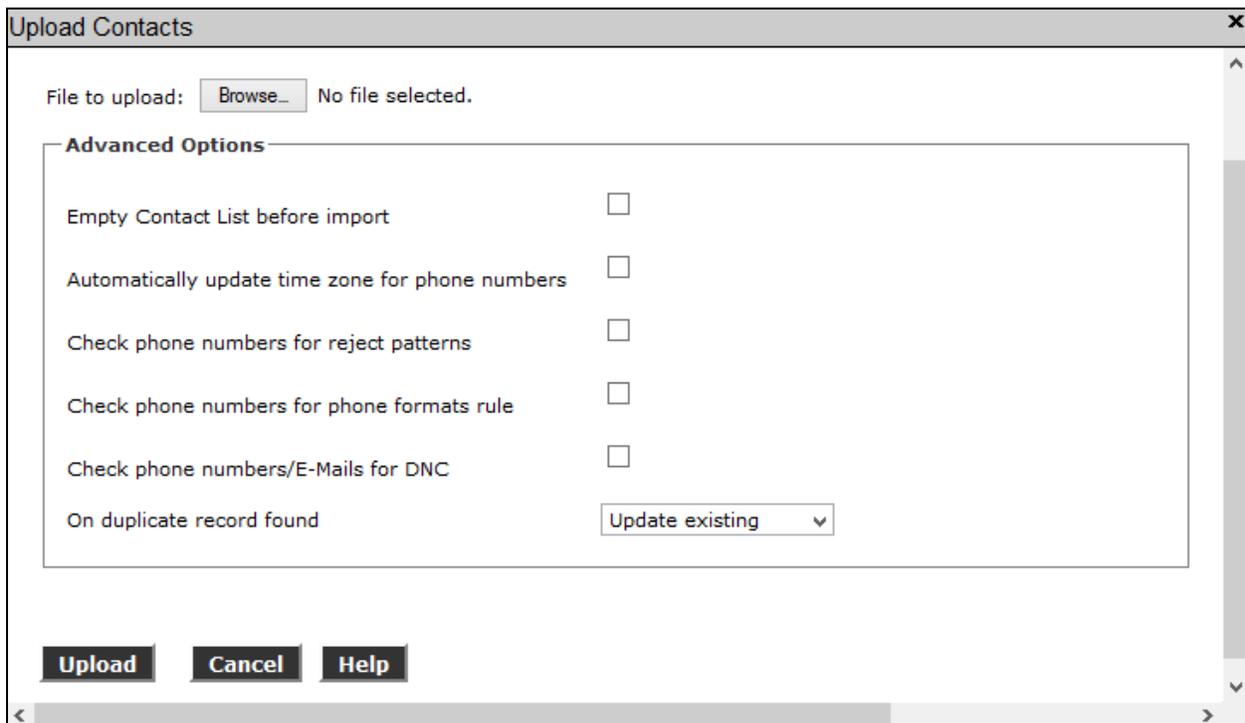
5.8. Configure Campaign

5.8.1. Configure Campaign Strategy

From **POM Home**, navigate to **Campaigns → Campaign Strategy** and select **Add**. Type in a name in **Name** field and select **Continue**.

Name	Sample
Use template	☐
Template	Select ▾

Continue **Cancel**

Campaign Strategy Editor will open as a pop up**.** Configure a strategy as needed. Below is an example of the strategy configured during compliance testing.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:AvayaPIMContactStrategy
xsi:schemaLocation="http://www.avaya.com/ContactStrategy ContactStrategy.xsd
" xmlns:tns="http://www.avaya.com/ContactStrategy"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Handler foundError="false" state="initial">
    <action CallPacingType="Progressive" DriverApp="PomDriverApp"
EnhancedCCA="ON" HoldApp="AvayaPOMAnnouncement" NailerApp="Nailer"
NuisanceApp="AvayaPOMAnnouncement" OnMediaServerFailure="retry" acwTime="10"
allocationType="0" defaultCompCode="CompletionCode1" foundError="false"
guardTime="Disable" maxAgents="3" minAgents="1" numOfACWExtns="0"
outboundSkill="1" outboundSkillName="1" overDialRatio="10" priority="5"
type="call">
      <address foundError="false" isBranch="false" weekDaysOnly="false">
        <ContactAttribute>phoneNumber1</ContactAttribute>
      </address>
      <resultprocessors customProcessor="None" foundError="false"
nextState="done">
        <result foundError="false" nextState="wait" value="Answer_Human">
          <Agent agentScript="1" agentScriptName="Googl"
campaignCallBack="Enable" canCancelCallback="Enable" foundError="false"
generalCallBack="Enable" prefAgentCallback="Enable"/>
        </result>
      </resultprocessors>
    </action>
  </Handler>
</tns:AvayaPIMContactStrategy>
```

5.8.2. Configure Campaign Manager

From **POM Home**, navigate to **Campaigns** ➔ **Campaign Manager** and select **Add**. Type in a name in **Name** field and select **Continue**.

Solution & Interoperability Test Lab Application Notes
©2016 Avaya Inc. All Rights Reserved.

On the **Define Campaign** page, select the strategy added in **Section 5.8.1**. Select the contact list from **Section 4.7** and select **Finish**.

Solution & Interoperability Test Lab Application Notes
©2016 Avaya Inc. All Rights Reserved.

5.9. Start POM Server

Once POM server is added, start it by navigating to **Configurations → POM Servers → POM Manager**. On the **POM Manager** page, check the box for the POM server and select **Start**.

KJA; Reviewed:
SPOC 1/28/2016

Solution & Interoperability Test Lab Application Notes
©2016 Avaya Inc. All Rights Reserved.

22 of 35
synTelateSynPOM

6. Configure Avaya Aura® Session Manager

Configuration for Session manager is performed via System Manager. From a web browser type in https://[IP-Address]/SMGR where IP-Address is the IP Address of System Manager. Log in using appropriate credentials.

Please note that configuration of each item is not shown in detail. In the following sections, screen captures of the configured items during compliance testing are shown. For details steps on configuration of each item, refer to Document [3].
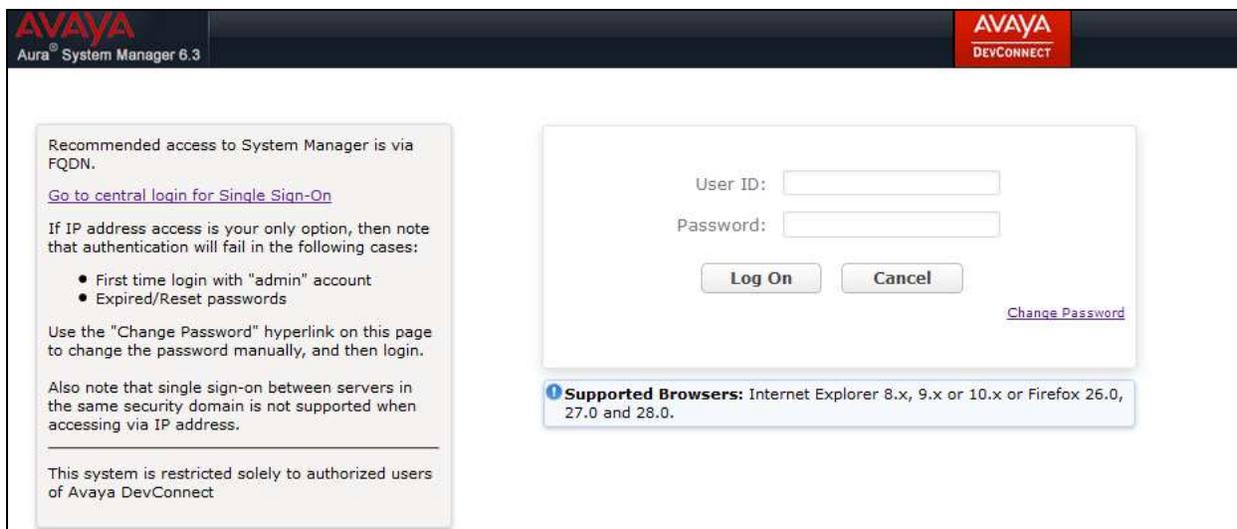

6.1. Configure Domain

Once logged in, select **Routing** (not shown). On the left pane select **Domains**. Click **New** to add a new domain. For compliance testing, domain of **avaya.com** was added.

6.2. Configure Locations

From the left pane, select **Locations**. To add a new location, select **New**. For compliance testing, location of **Test Room 1** was added.
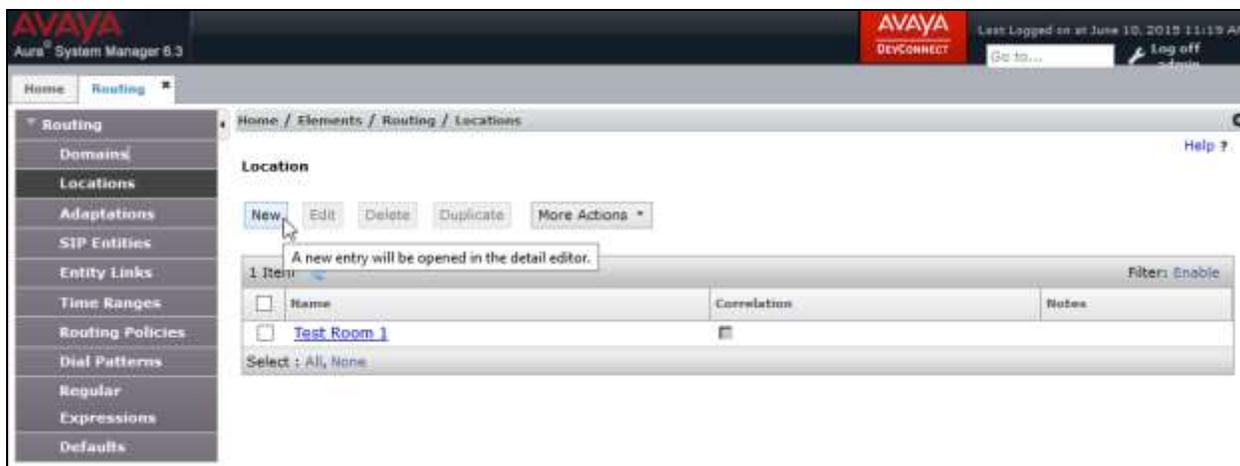
6.3. Configure SIP Entities

From the left pane, select **SIP Entities**. To add a new SIP Entity, select **New**. For compliance testing, three SIP Entities were added as shown below.

- **aaep-mpp**: Experience Portal SIP Entity.
- **asm-tr1-**: Session Manager SIP Entity.
- **cm-tr1**: Communication Manager SIP Entity.
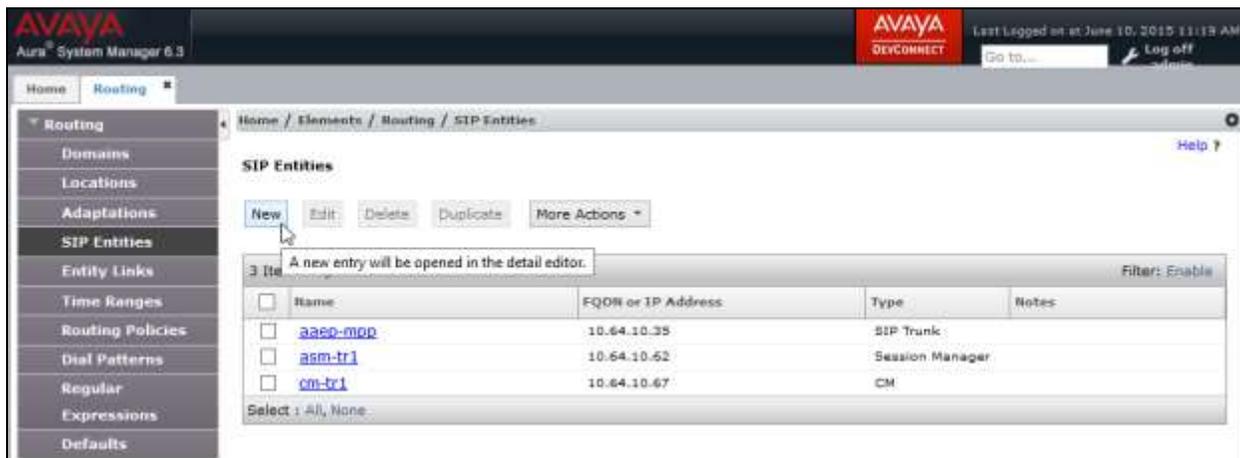
6.4.   Configure Entity Links

For each SIP Entity, with the exception of Session Manager, an entity link needs to be added. On the left pane, select **Entity Links**. To add a new entity link, select **New**. For compliance testing two entity links, one for Communication Manager and another for Experience Portal, were added.
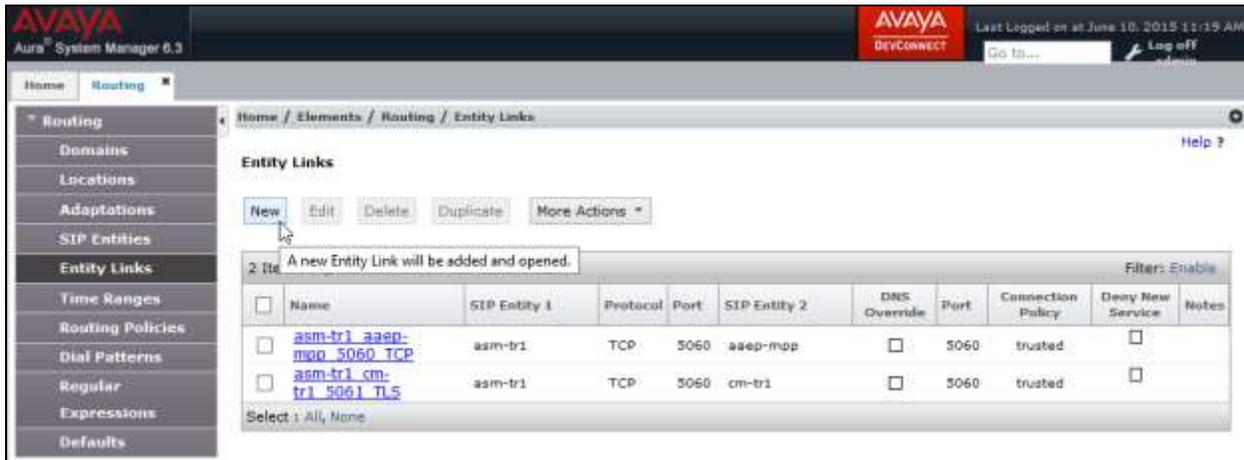

6.5.   Configure Time Ranges

On the left pane, select **Time Ranges**. To add a new time range, select **New**. For compliance testing, time range of 24/7 was added.

6.6.   Configure Routing Policies

On the left pane, select **Routing Policies**. To add a new routing policy, select **New**. For compliance testing, two routing policies were added, one for Communication Manager and another for Experience Portal.
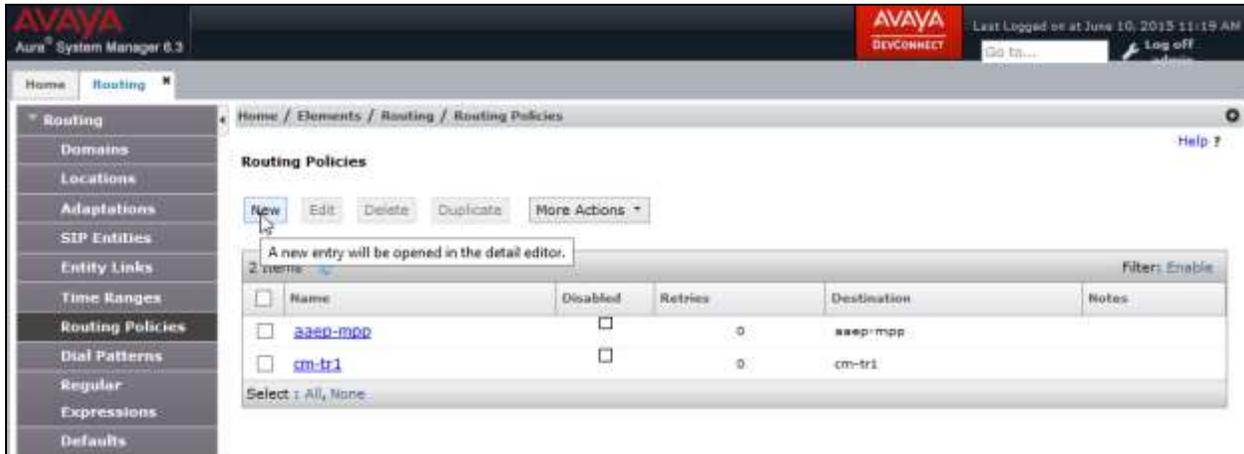
6.7.   Configure Dial Patterns

On the left pane, select **Dial Patterns**. To add a new dial pattern, select **New**. For compliance testing three dial patterns were added:

- **250**: All calls starting with pattern 250 with either 4 or 5 digits were routed to Communication Manager. For compliance test, Experience Portal routed calls to extensions 250xx, which were routed to Communication Manager.
- **257**: All calls starting with pattern 257 and 5 digits long were routed to Experience Portal.
- **9**: All calls starting with 9 and either 11 or 12 digits long were routed to Communication Manager. This was used for routing calls out to PSTN via Communication Manager.
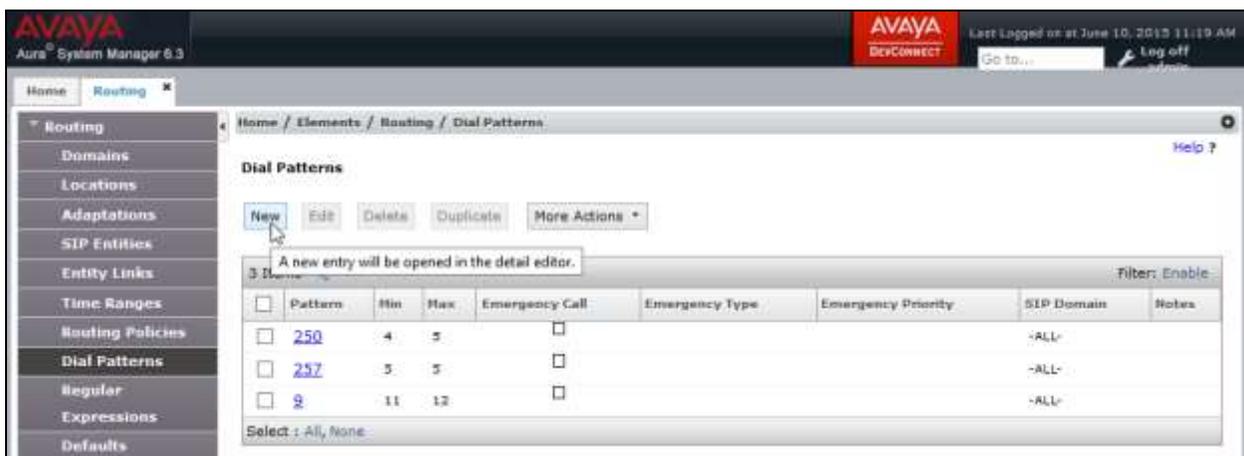
7. Configure Inisoft synTelate

Configuration for POM is performed on synTelate Enterprise server. Log onto the synTelate Enterprise server using appropriate credentials. All the configuration mentioned in this section is performed on synTelate Enterprise server.

7.1. Configure synTelate Supervisor

From the **Start** menu, navigate to **All Programs → synTelate Enterprise → synTelate Supervisor**. Select **CTI Config**, and click **Add**.
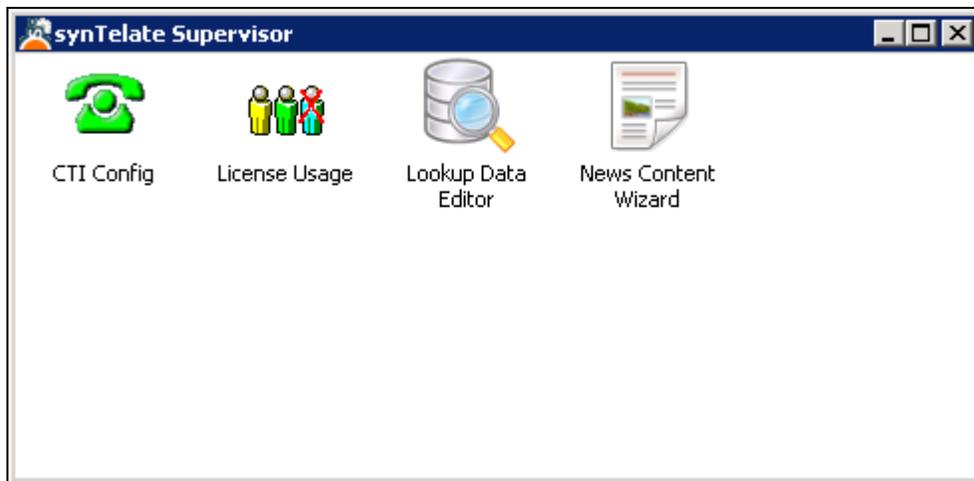
Type in a name in **Name** and select **AVAYA POM** from the **Telephone Server** drop down menu. Click **Addition Configuration**.

On the **Avaya POM Configuration** window, select **Add**. Type in the **IP Address** of Experience Portal and **Port** for the POM Agent Desktop interface. Note that **9970** is the default port. Click **OK** when done.
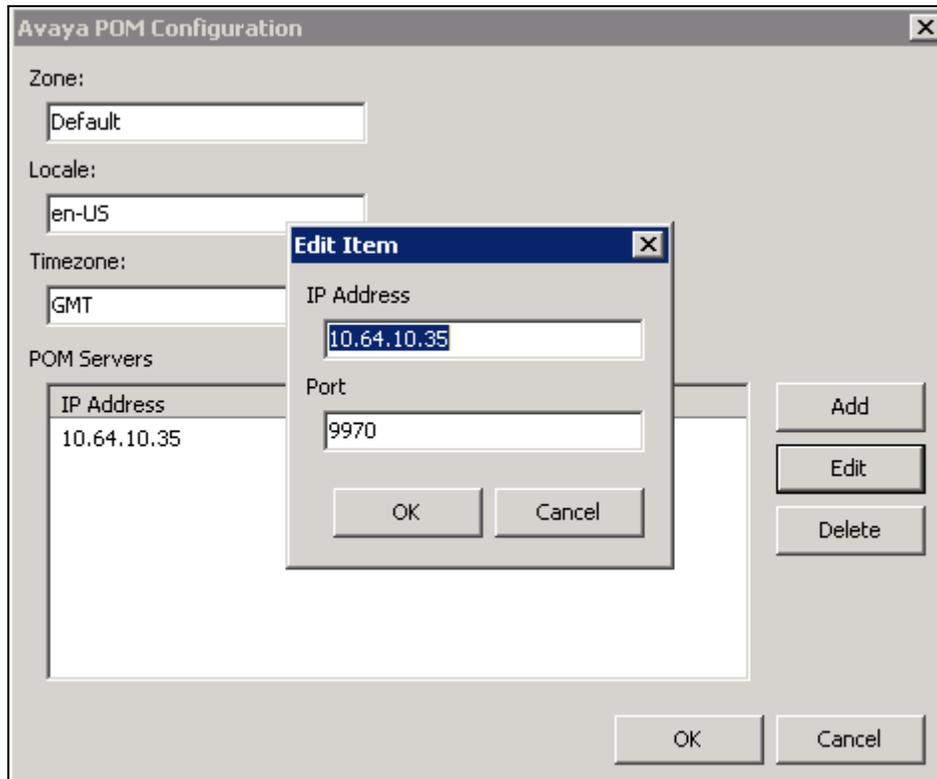
7.2. Configure General Settings

From the **Start** menu, navigate to **All Programs → synTelate Enterprise → synTelate Utilities → General Table Editor**. From the **General Settings** window, locate **POMAPIWebService** and configure it as http://[IP-Address]/axis2/services, where IP-Address is the IP Address of Experience Portal. Apply the changes when done.
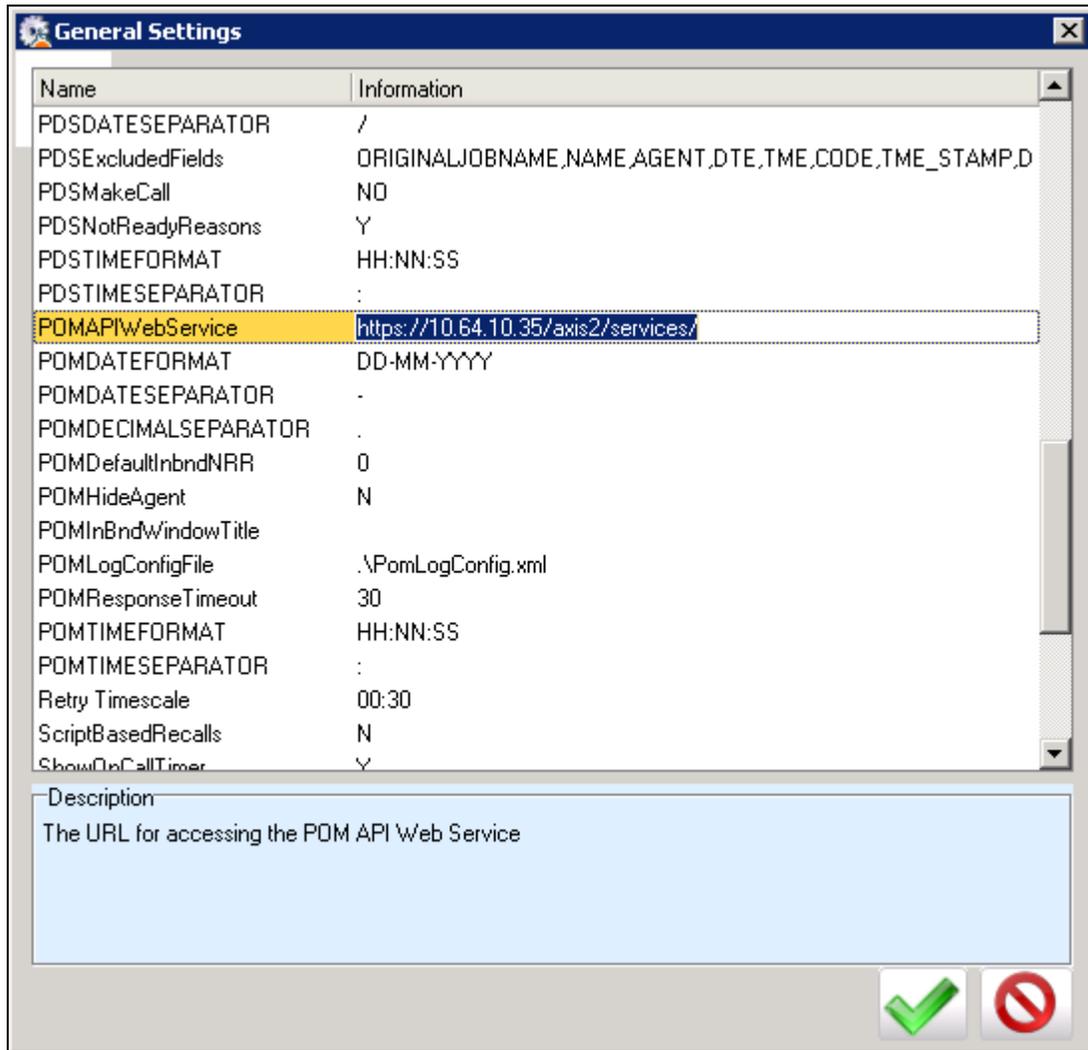
7.3.   Configure Campaign

From the **Start** menu, navigate to **All Programs → synTelate Enterprise → synTelate Designer**.
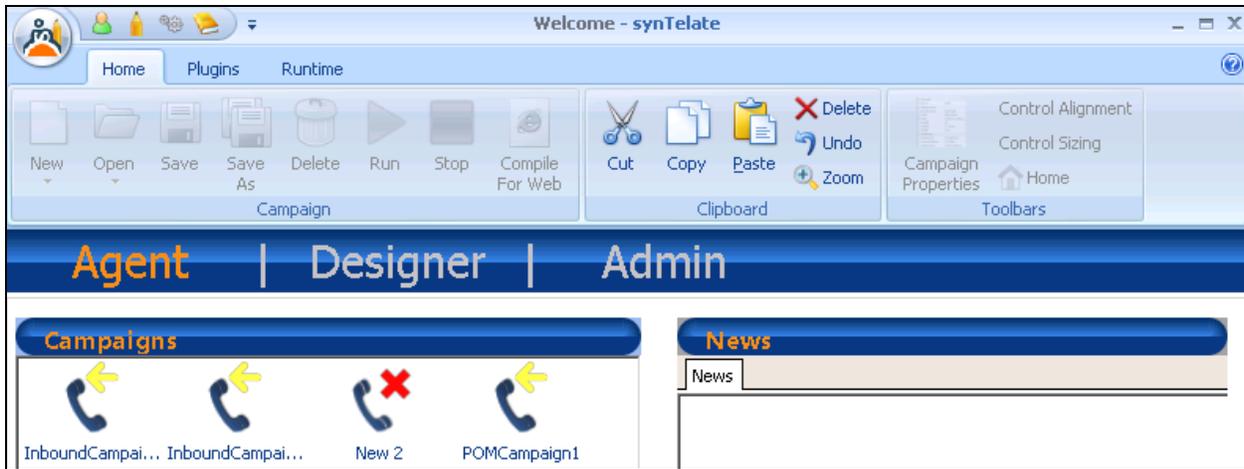

Select **Designer**, and from the top pane navigate to **New → Wizard → POM Wizard**. Finish the configuration by following the steps in document [6]
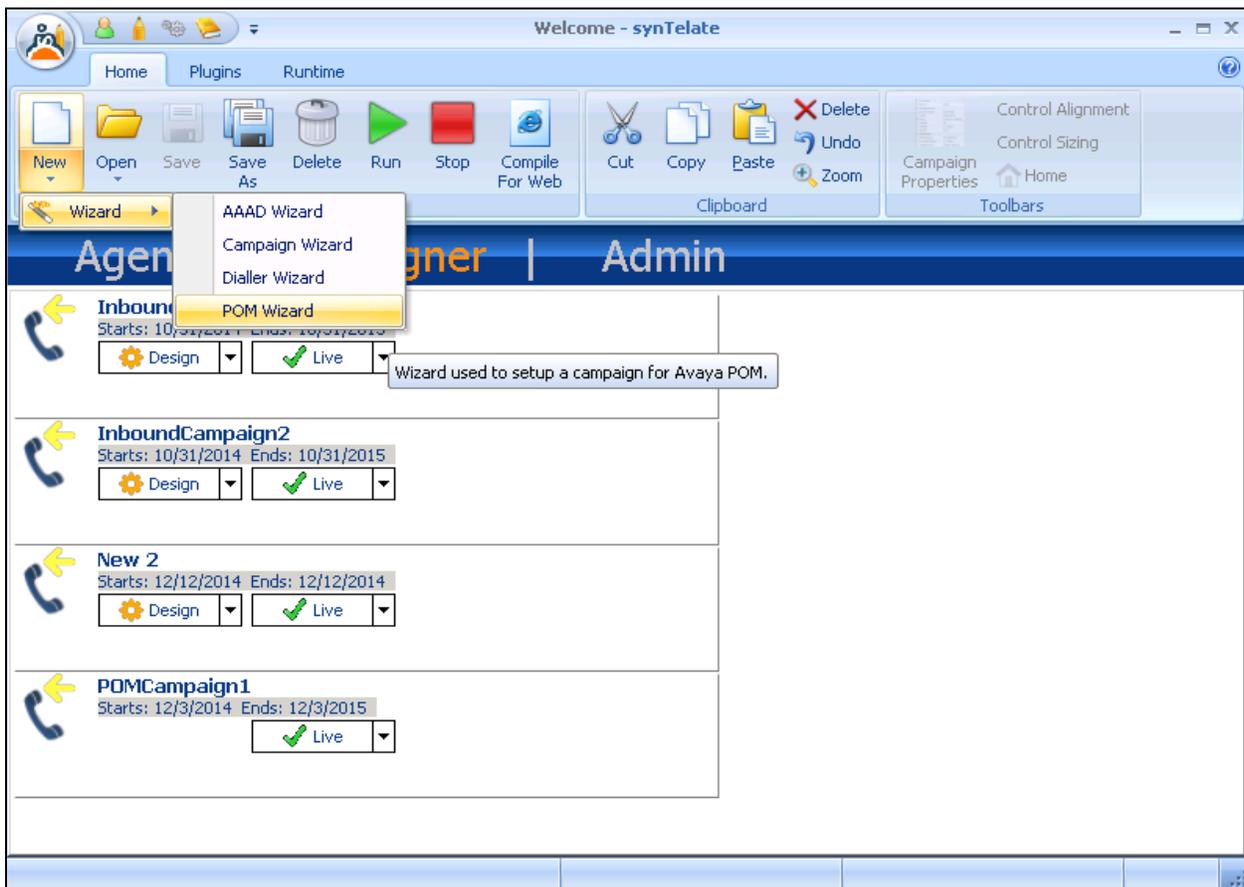
7.4. Configure Agents

Configure the agents that will be used for Agent Desktops. Continuing from previous section, select **Admin → Agents** from the main window. Select **New** to add a new agent. Under the **Agent** tab, type in a name for the agent.

Note: The name for the agent must match the windows login created for the Agent Desktop.
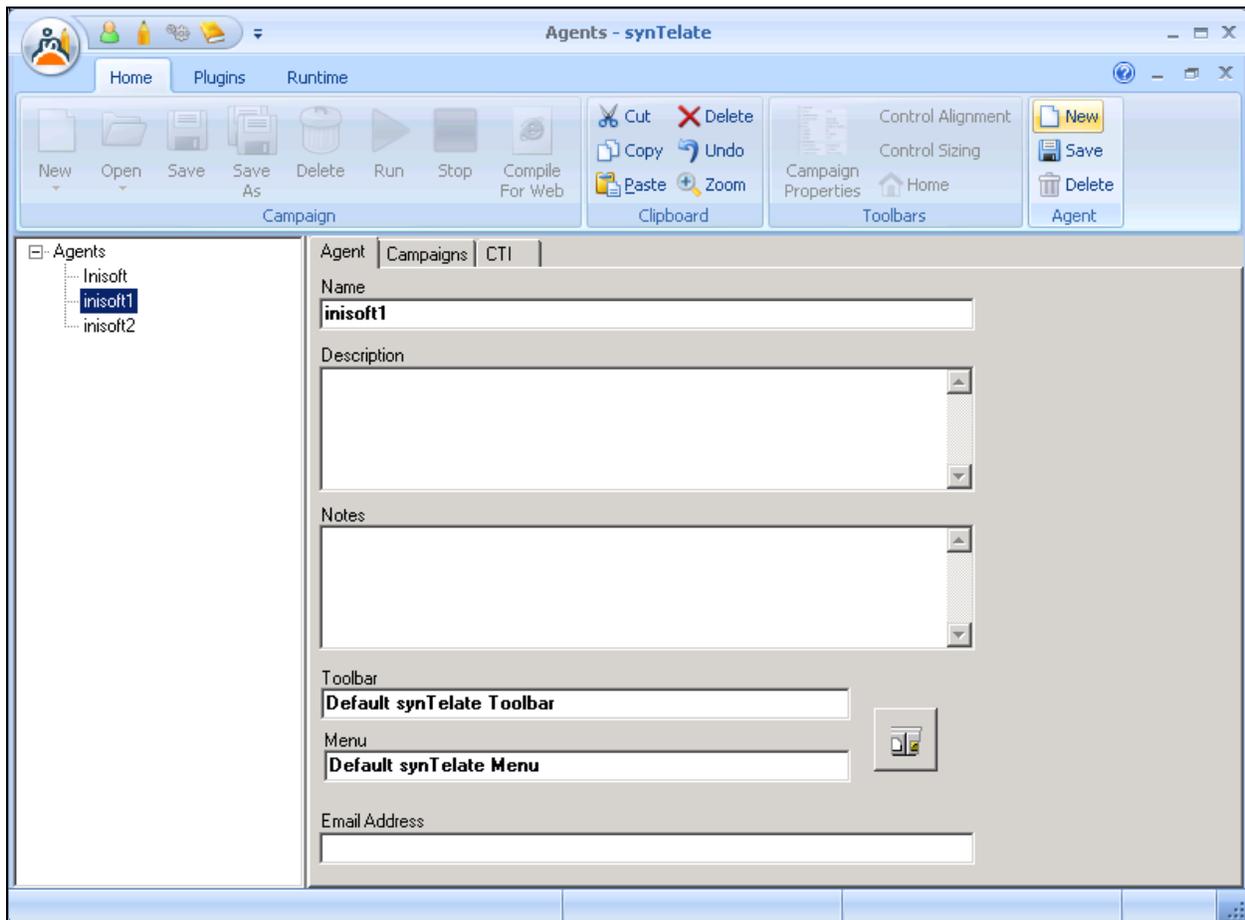
Under the **CTI** tab, from the **Available CTI Modules**, select the CTI config created for POM in **Section 7.1,** and select **Allocate**. Click **Save** when done (not shown).

Solution & Interoperability Test Lab Application Notes
©2016 Avaya Inc. All Rights Reserved.
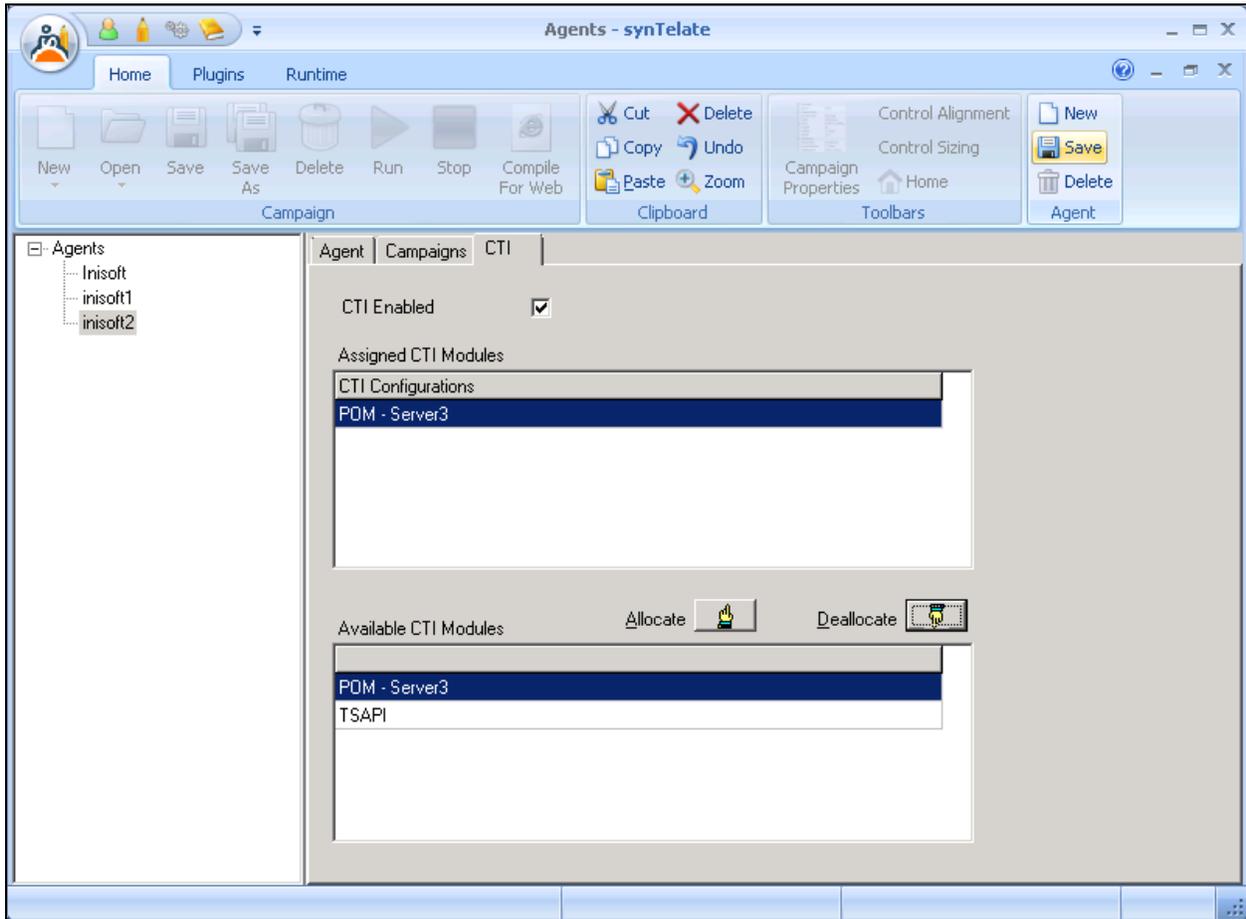
8. Verification Steps

From an Agent Desktop, launch the Enterprise Agent application via **Start → synTelate Enterprise → Enterprise Agent**. On the **Avaya POM Login** screen:
- Type in the **Agent Extension** from **Section 4.3**.
- Type in the **Agent ID** from **Section 4.2**.
- Type in the **Password** for the assigned password in **Section 4.2**.
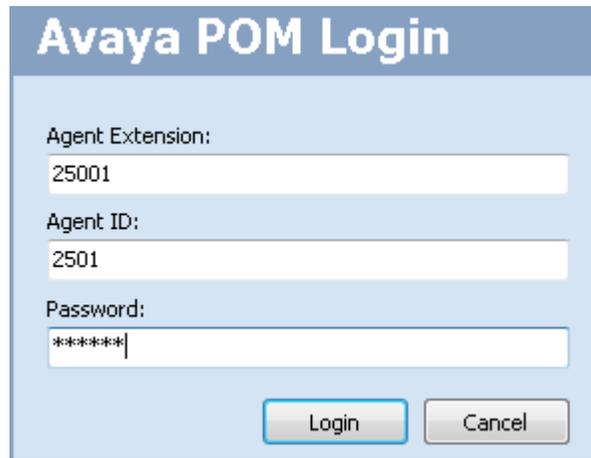
If the agent is able to log in successfully, **Ready** and **Not Ready** buttons are displayed. Select **Ready** on the top left corner. Agent is now ready to accept calls.
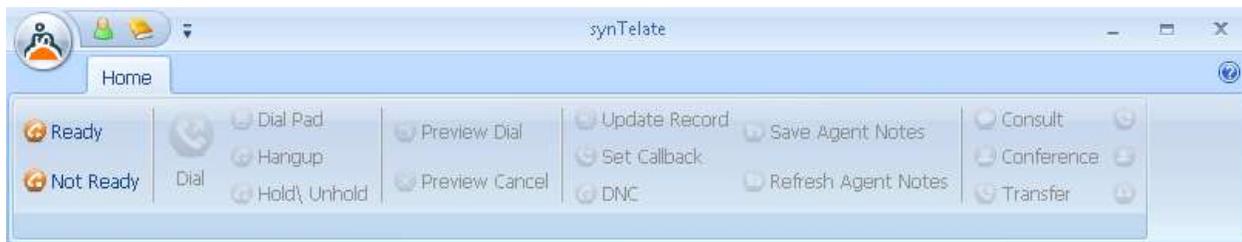
9. Conclusion

These Application Notes describe the configuration steps required to integrate the synTelate Enterprise Agent with Avaya Proactive Outreach Manager. All feature and serviceability test cases were completed successfully.

10. Additional References

This section references the product documentation that is relevant to these Application Notes. Documentation for Avaya products may be obtained via http://support.avaya.com

[1] Implementing Proactive Outreach Manager, Release 3.0.1, March 2014
[2] Administering Avaya Aura® Communication Manager, Release 6.3, Document 03-300509, Issue 10, June 2015
[3] Administering Avaya Aura® Session Manager, Release 6.3, Issue 7, September 2014
[4] Administering Avaya Aura® Experience Portal, Release 7.0.1, April 2015
[5] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.3, Document 02-300357, June 2014

Documentation related to synTelate may directly be obtained from inisoft.
[6] synTelate POM – User Notes v13-3
[7] synTelate v4 User Document, 2014