Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Application Enablement Services with Partner Teknoloji Outbound Campaign Management – Issue 1.0

Abstract

These Application Notes describe the steps to configure Partner Teknoloji Campaign Management to operate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. The Partner Teknoloji Outbound Campaign Management performs configurable automated outbound dialing tasks.

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.

©2012 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required for Partner Teknoloji Outbound Campaign Management (OCM) to successfully interoperate with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services (AES) and Avaya. Partner Teknoloji Outbound Campaign Management provides a platform with which scheduled outbound campaigns can be generated and managed. Partner Teknoloji Outbound Campaign Management is configured to call each number in a calling list based on predefined criteria and to play each number which answers an announcement. Partner Teknoloji Outbound Campaign Management can be used to create informational, collection or sales based dialing campaigns. Partner Teknoloji Outbound Campaign Management connects to Avaya Aura® Application Enablement Services using JTAPI to provide the telephony functionality available from Avaya Aura® Communication Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of the Outbound Campaign Management to successfully place outbound calls and play an announcement when the outbound call was answered. Correct classification of calls and multiple simultaneous campaigns were verified and real time monitoring was evaluated for accuracy.

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 following tests were performed as part of the compliance testing, all calls were routed to an announcement only:

- Use of Pool Trunks
- Use of Dedicated Trunks
- Single Campaign
- Multiple Simultaneous Campaigns
- Call Classification
- Recall scenarios e.g. engaged, no answer

Recovery from power and network failure was not tested.

2.2. Test Results

All test cases were completed successfully with the following observations:

- Only outbound answered calls routed to an announcement are supported.
- The number of active calls on the Real Time Monitor relates to active application threads, not real active calls.

©2012 Avaya Inc. All Rights Reserved.

- The number of scheduled calls on the Real Time Monitor relates to the number of calls which are to be recalled. Once the recall period has expired, the scheduled call is put back into the active calling list.
- In the event of multiple simultaneous campaigns, it was observed that the call would disconnect upon answer. This issue is addressed by a software patch from Partner Teknoloji.

2.3. Support

Technical Support can be obtained for the Partner Teknoloji products as follows:

- Email: info@partnerteknoloji.com.tr
- Phone: +90-216-368-07-68

©2012 Avaya Inc. All Rights Reserved.

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8800 server running Communication Manager with an Avaya G650 Media Gateway. An Avaya S8800 server hosts Application Enablement Services. The Tomcat application server on which the OCM configuration is made is hosted on a Generic VMWare server running the Debian operating system.

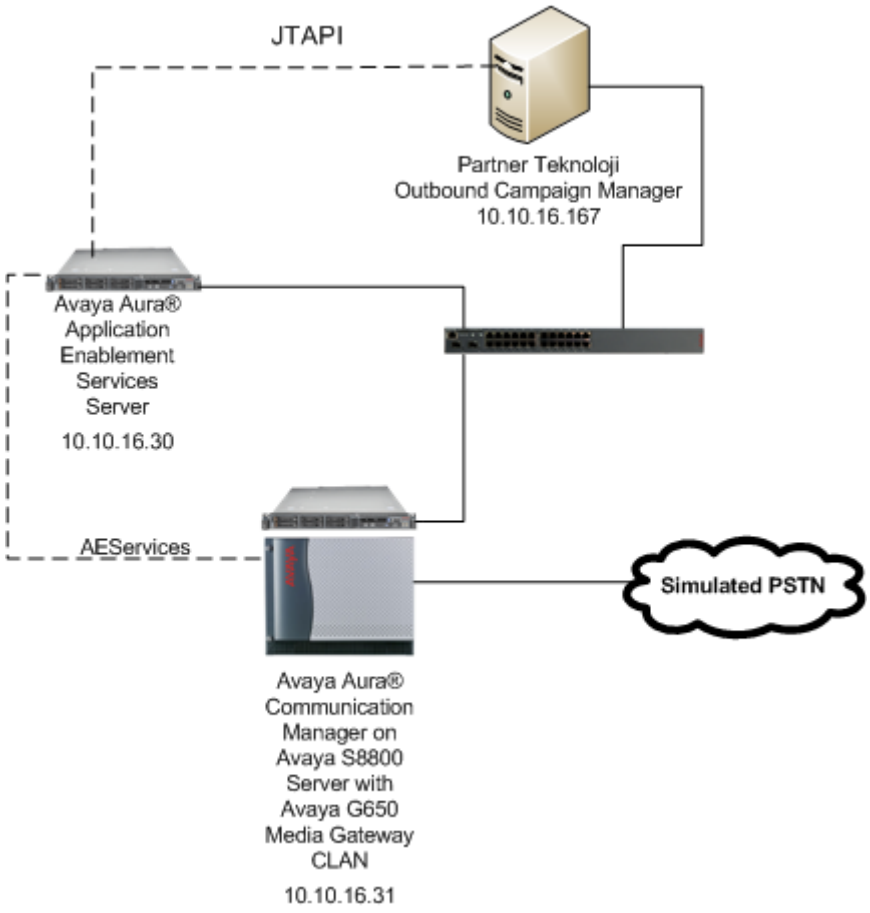


Figure 1: Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services Configuration with Partner Teknoloji Outbound Campaign Manager Solution

©2012 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager R6.0.1 SP6 R16.00.1.510.1-19350
Avaya G650 Media Gateway : • TN799DP • TN2302AP • TN750C • TN2464CP	 HW1 FW40 HW20 FW121 000014 HW02 FW024
Avaya S8800 Server	Avaya Aura® Application Enablement Services R6.1.1 r6-1-1-30-0
Generic VMWare Server	VMWare ESXi 4.1 Debian Linux 6 Apache Tomcat 7 Outbound Campaign Manager 0.1.0.1138 Central Management 0.1.0.1146 TSCS 0.1.0.1172 DCS 0.1.0.1180

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section were all performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. The Application Notes assume trunk connectivity and call routing between Communication Manager and the PSTN is established

- Define Feature Access Codes
- Configure Announcement
- Configure CLAN for Avaya AES Connectivity
- Configure Transport Link for AES Connectivity
- Configure CTI Link for TSAPI Service
- Configure CTI Extensions

©2012 Avaya Inc. All Rights Reserved.

5.1. Define Feature Access Codes

Use the **change feature-access-codes** command to define the required access codes. On **Page 1** define a FAC for **Announcement Access Code.**

```
change feature-access-codes                                    Page   1 of  10
                              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: *14
                       Answer Back Access Code: *13
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 5
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act: *11    Deactivation: *12
                         Call Park Access Code:
                       Call Pickup Access Code: *10
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                  Contact Closure   Open Code:          Close Code:
```

5.2. Configure Announcement

Enter the command **add announcement next**, take a note of the extension number and assign a descriptive **Annc Name**, in the **Annc Type** field enter **integrated** and in the **Group/Board** field enter the location of the announcement board, in this case **01a12**.

```
add announcement next                                          Page   1 of   1

                        ANNOUNCEMENTS/AUDIO SOURCES

  Extension: 774                                  COR: 1
  Annc Name: hello_fake_answer                     TN: 1
  Annc Type: integrated                         Queue? y
Group/Board: 01a12
  Protected? n                                   Rate: 64
```

5.3. Configure CLAN for Avaya Aura® Application Enablement Services Connectivity

Define a node name for the CLAN by using the command **change node-names ip** and add an IP address and node name for the CLAN.

```
change node-names ip                                           Page   1 of   2
                                    IP NODE NAMES
    Name                  IP Address
devconaes611            10.10.16.29
clancm601               10.10.16.31
```


©2012 Avaya Inc. All Rights Reserved.

Add the CLAN to the system configuration using the **add ip-interface n** command where **n** is the CLAN board location. Enter the CLAN node name assigned in the previous step to the **Node Name** field. Enter values for the **Subnet Mask** and **Gateway Address** fields. In this case, **/24** and **Gateway** are used to correspond to the network configuration in these Application Notes. Set the **Enable Interface** field to **y**, default values may be used in the remaining fields.

```
add ip-interface 01a02                                          Page   1 of   3
                                IP INTERFACES

                 Type: C-LAN
                 Slot: 01A02        Target socket load and Warning level: 400
          Code/Suffix: TN799  D           Receive Buffer TCP Window Size: 8320
      Enable Interface? y                          Allow H.323 Endpoints? y
                 VLAN: n                            Allow H.248 Gateways? y
       Network Region: 1                             Gatekeeper Priority: 5

                               IPV4 PARAMETERS
            Node Name: clancm601                      IP Address:

     Gateway Node Name: netscreen                    IP Address:
           Subnet Mask: /24

          Ethernet Link: 1
          Network uses 1's for Broadcast Addresses? y
```


©2012 Avaya Inc. All Rights Reserved.

5.4. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Set to **AESVCS**
- **Enabled:** Set to **y**
- **Local Node:** Set to the node name assigned for the CLAN in **Section 5.3**
- **Local Port:** Retain the default value of **8765**.

```
change ip-services                                                  Page   1 of   3

                                  IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y          CLAN         8765
```

Go to **Page 3** of the ip-services form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **devconaes611**
- **Password:** Enter a password to be administered on the AES server
- **Enabled:** Set to **y**

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.1**. The **AE Services Server** should match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.

```
change ip-services                                                  Page   3 of   3
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      devconaes611        Avayapassword1        y        in use
      2:      :
```

5.5. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

```
add cti-link 1                                                      Page   1 of   3
                                   CTI LINK
 CTI Link: 1
Extension: 4999
     Type: ADJ-IP
                                                                      COR: 1
     Name: devconaes
```


©2012 Avaya Inc. All Rights Reserved.

5.6. Configure CTI Extensions

Outbound Campaign Manager uses CTI extensions (trunks) to place outbound calls. Enter the command **add station next**, take a note of the **Extension**, set the **Type** as **CTI**, set the **Port** to **X** and assign an identifying **Name**.

```
add station next                                          Page   1 of   5
                                    STATION

Extension: 1855                        Lock Messages? n               BCC: 0
     Type: CTI                         Security Code:                  TN: 1
     Port: X                         Coverage Path 1:                 COR: 1
     Name: Acquire 6                 Coverage Path 2:                 COS: 1
                                     Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
             Loss Group: 1          Personalized Ringing Pattern: 1
           Data Module? n                      Message Lamp Ext: 1855
         Display Module? n


         Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y
```

6. Configure Avaya Aura® Application Enablement Services Server

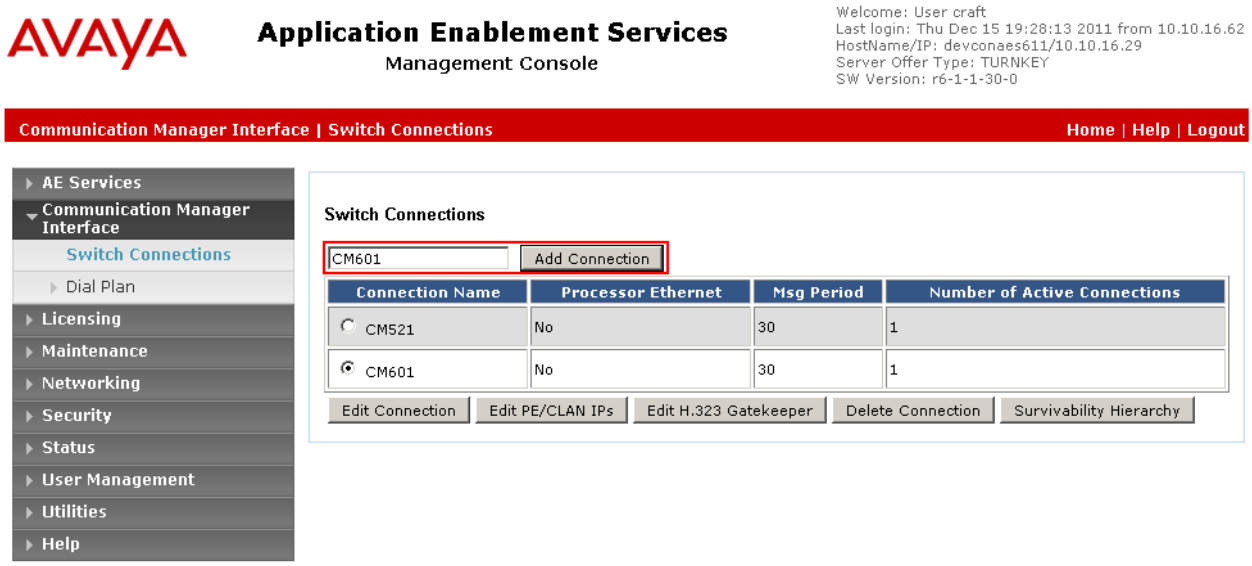
This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Create Switch Connection
- Administer TSAPI link
- Create CTI User
- Enable CTI Link User
- Identify Tlinks

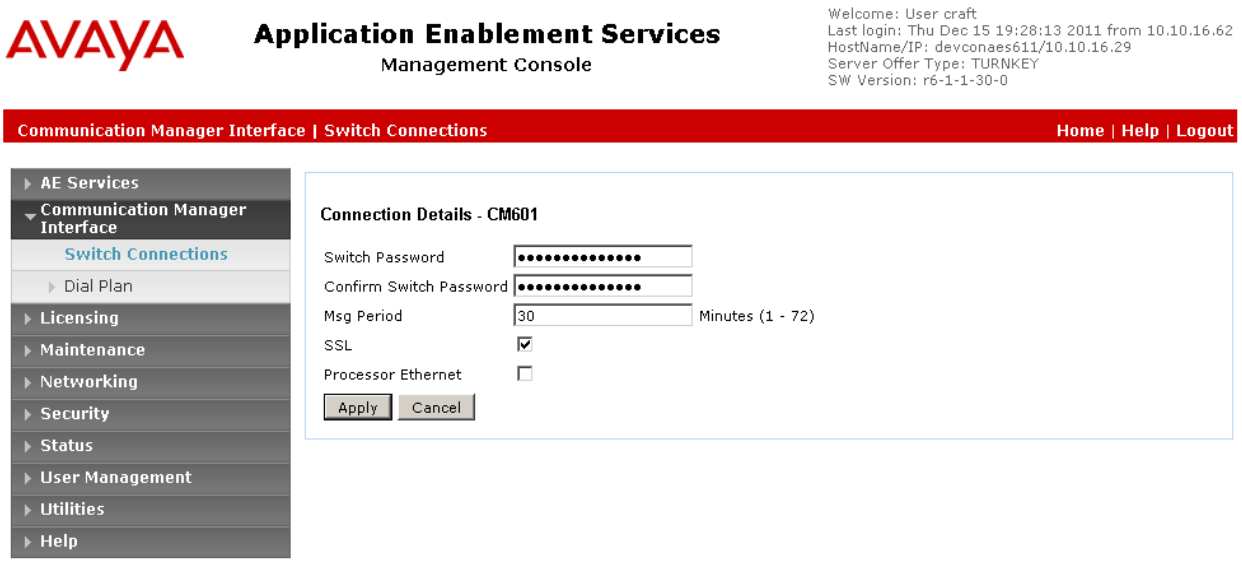
©2012 Avaya Inc. All Rights Reserved.

6.1. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface → Switch Connections** to set up a switch connection. Enter in a name for the Switch Connection to be added and click the **Add Connection** button.

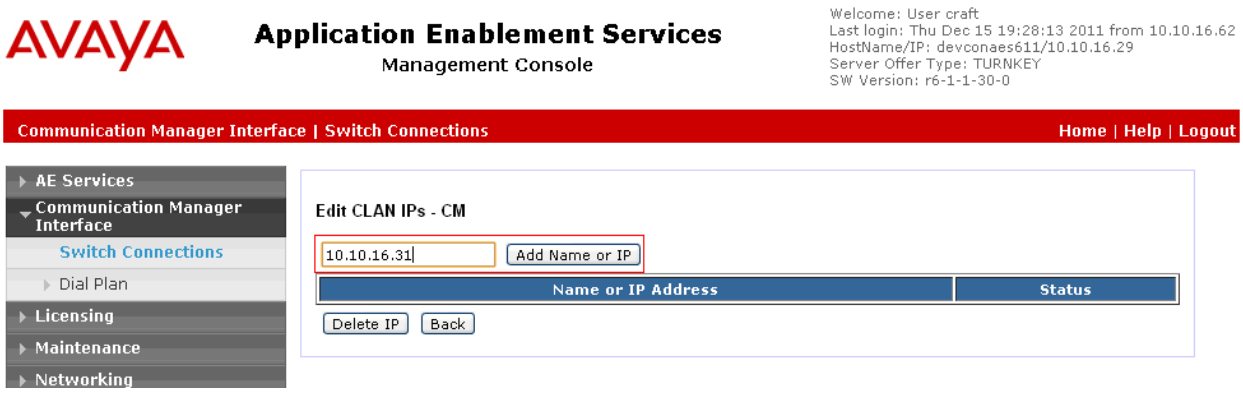


In the resulting screen enter the **Switch Password,** the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.4**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.



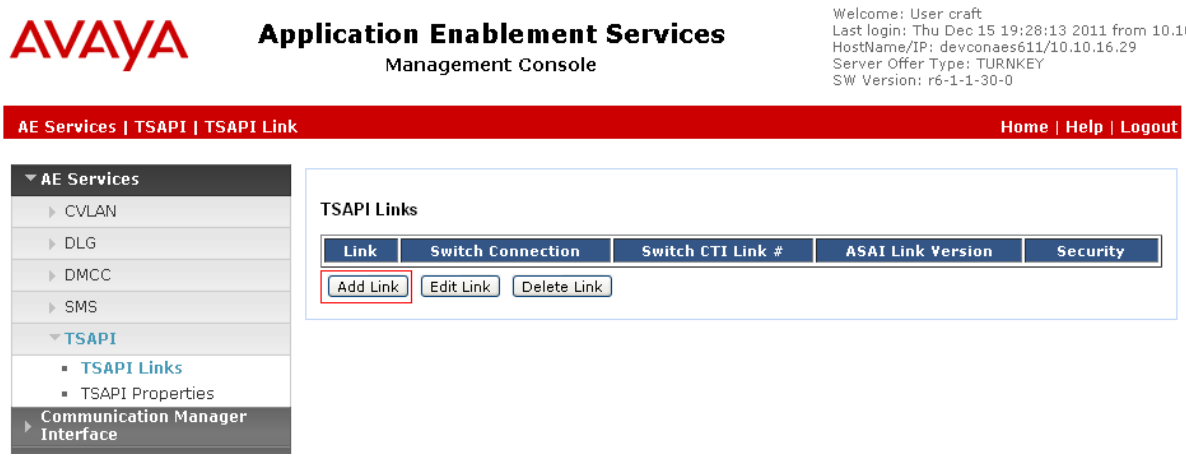
©2012 Avaya Inc. All Rights Reserved.

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the CLAN that will be used for the AES connection and select the **Add Name or IP** button.



6.2. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.

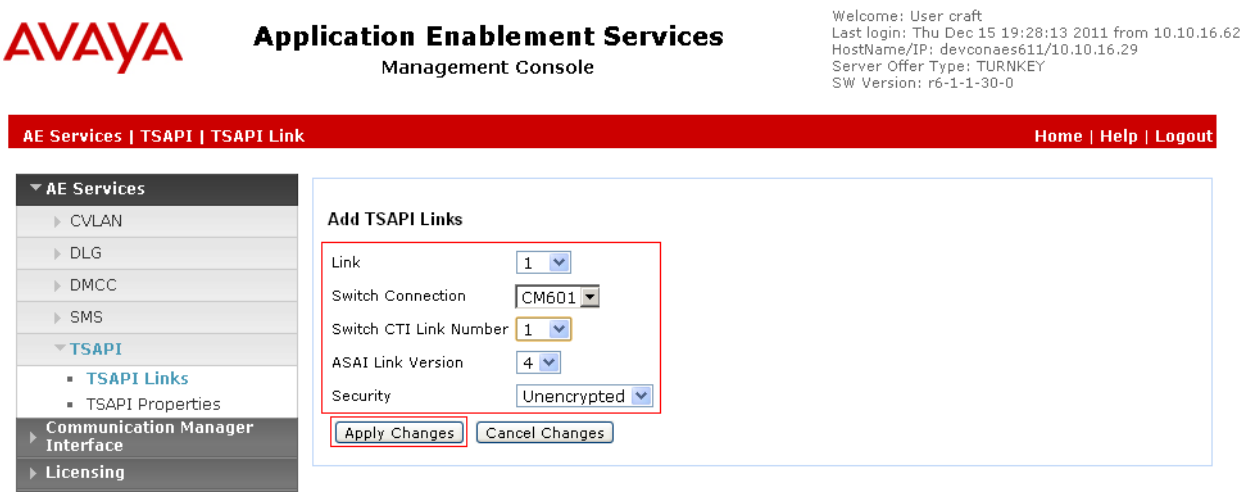


©2012 Avaya Inc. All Rights Reserved.

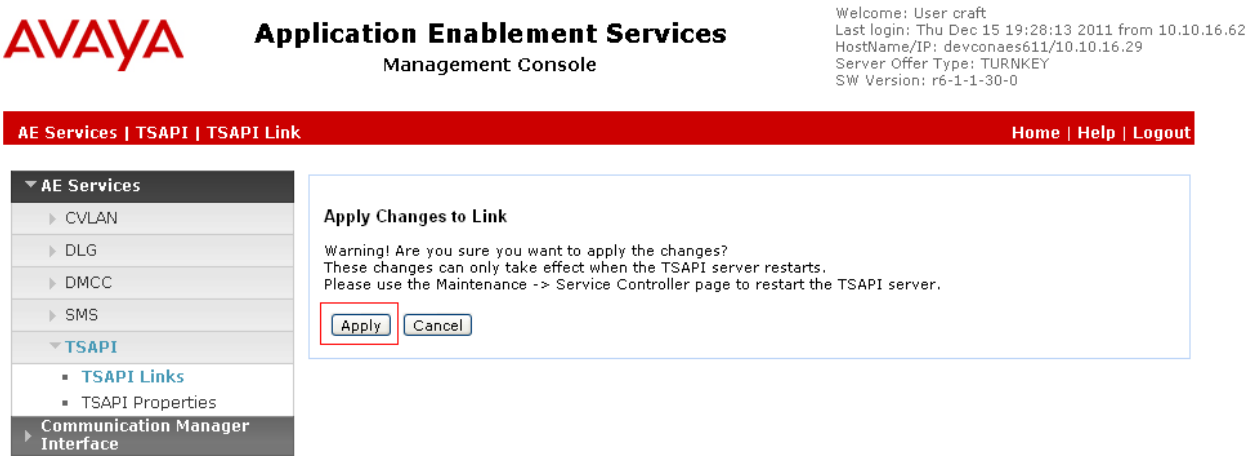
On the **Add TSAPI Links** screen, enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM**, which has already been configured in **Section 6.1**, from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.5** which is **1.**
- **ASAI Link Version:** This can be left at the default value of **4**.
- **Security:** This can be left at the default value of **Unencrypted.**

Once completed, select **Apply Changes**.

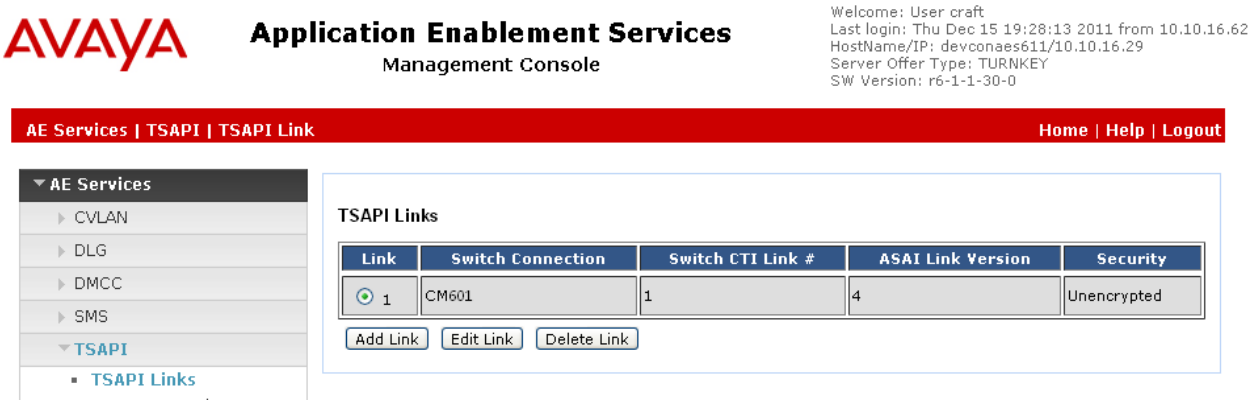


Another screen appears for confirmation of the changes. Choose **Apply**.

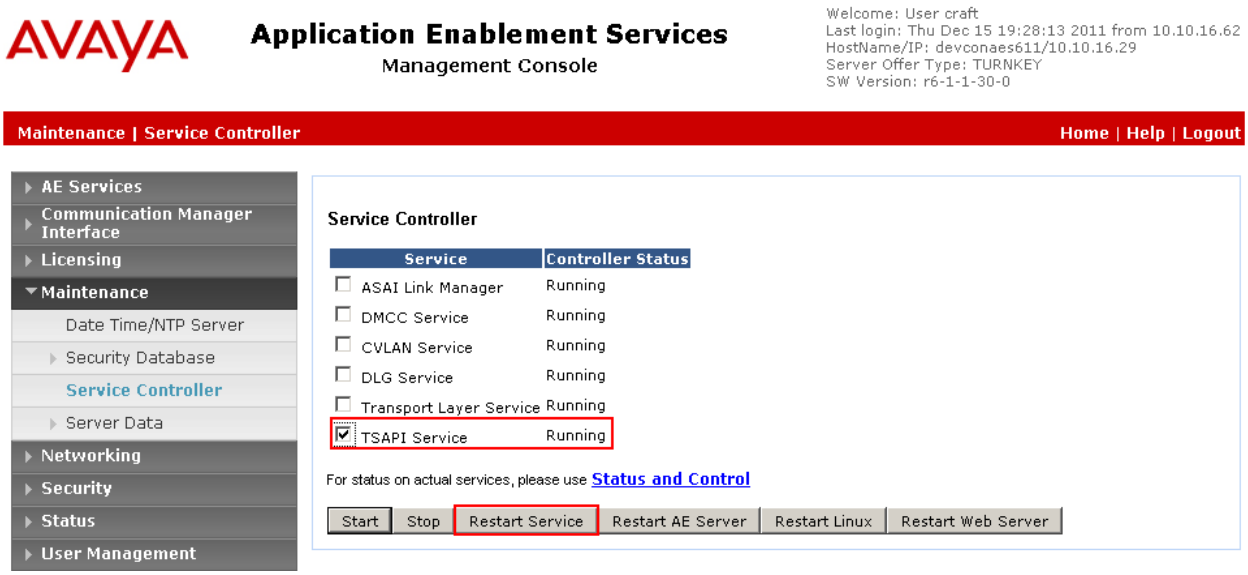


©2012 Avaya Inc. All Rights Reserved.

When the TSAPI Link is completed, it should resemble the screen below.



The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



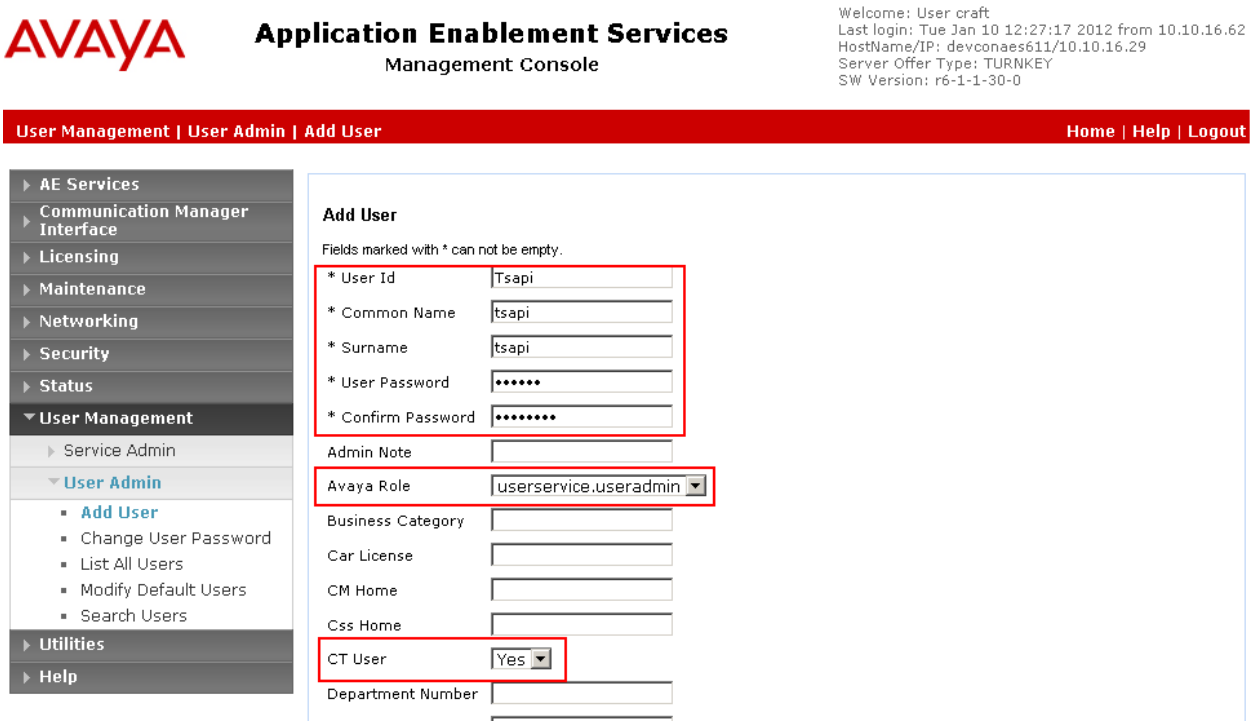
©2012 Avaya Inc. All Rights Reserved.

6.3. Create Avaya CTI User

User ID and password needs to be configured for OCM to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option. In the **Add User** screen shown below, enter the following values:

- **User Id -** This will be used by the OCM in **Section 7.1.**
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with the **User Id** in **Section 7.1**.
- **Avaya Role – userservice.useradmin**
- **CT User -** Select **Yes** from the drop-down menu.

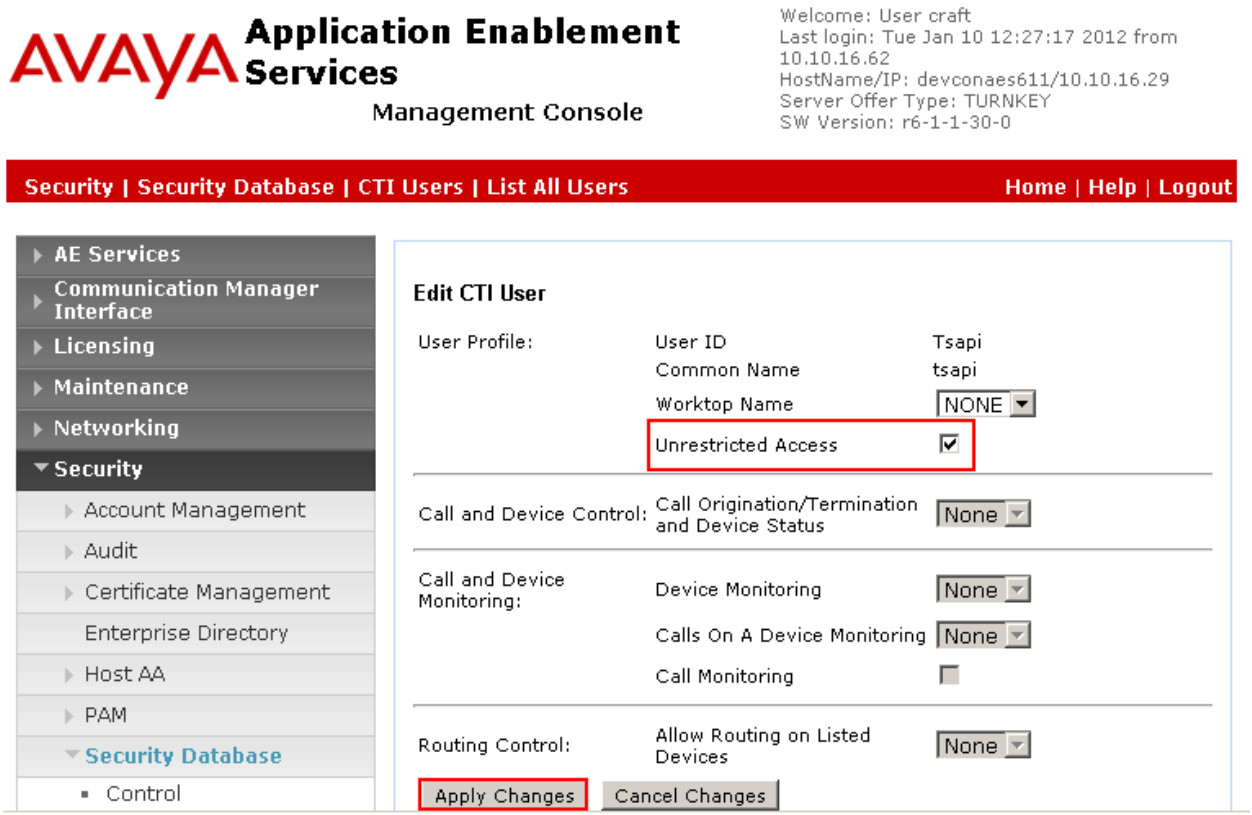
Complete the process by choosing **Apply** at the bottom of the screen (not shown).



©2012 Avaya Inc. All Rights Reserved.

6.4. Enable Unrestricted Access for CTI User

Navigate to the **CTI Users** screen by selecting **Security → Security Database → CTI Users → List All Users**. Select the user that was set up in **Section 6.4** and select the **Edit** option (not shown). The **Edit CTI User** screen appears. Check the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.



A screen (not shown) appears to confirm applied changes to CTI User, click **Apply**.

©2012 Avaya Inc. All Rights Reserved.

6.5. Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure OCM in **Section 7.1**.

7. Configure Partner Teknoloji Outbound Campaign Manager

For the purposes of the compliance test, Outbound Campaign Manager was installed and provided by Partner Teknoloji, the configuration can be summarized as follows:

- Create CTI Connection and Trunks
- Create Campaign
- Generate Customer File
- Create Segment
- Create Action
- Load Action
- Start Action

©2012 Avaya Inc. All Rights Reserved.

7.1. Create CTI Connection

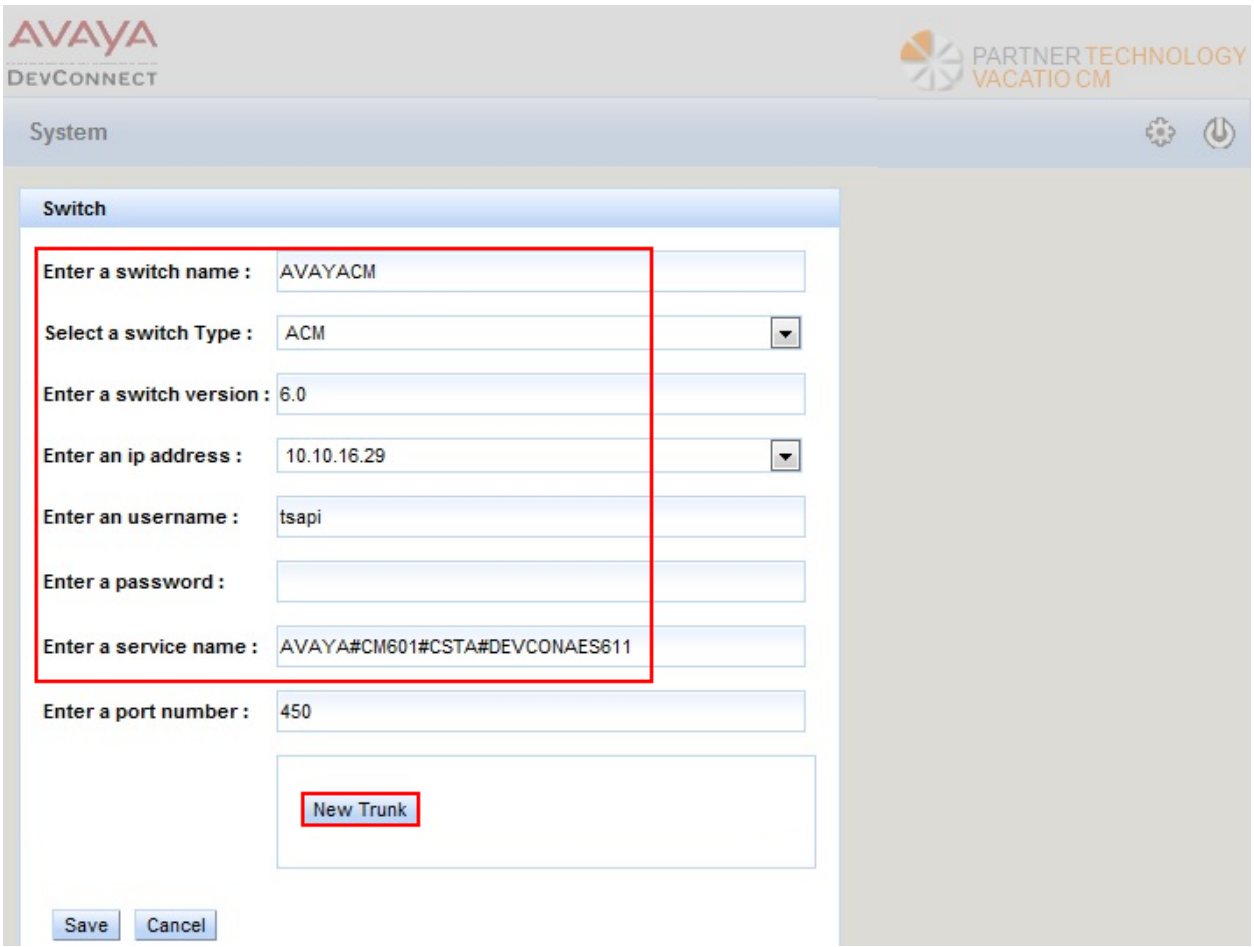
Configuration of the CTI connection between OCM and the Avaya solution is performed from the web interface, browse to http://<ip_of_ocm:8080/ConfigurationManager in this case http://10.10.16.167:8080/ConfigurationManager, enter the relevant login details as shown below and click **Sign in**.

The screen shown below will display, click on **System → Switch.**

©2012 Avaya Inc. All Rights Reserved.

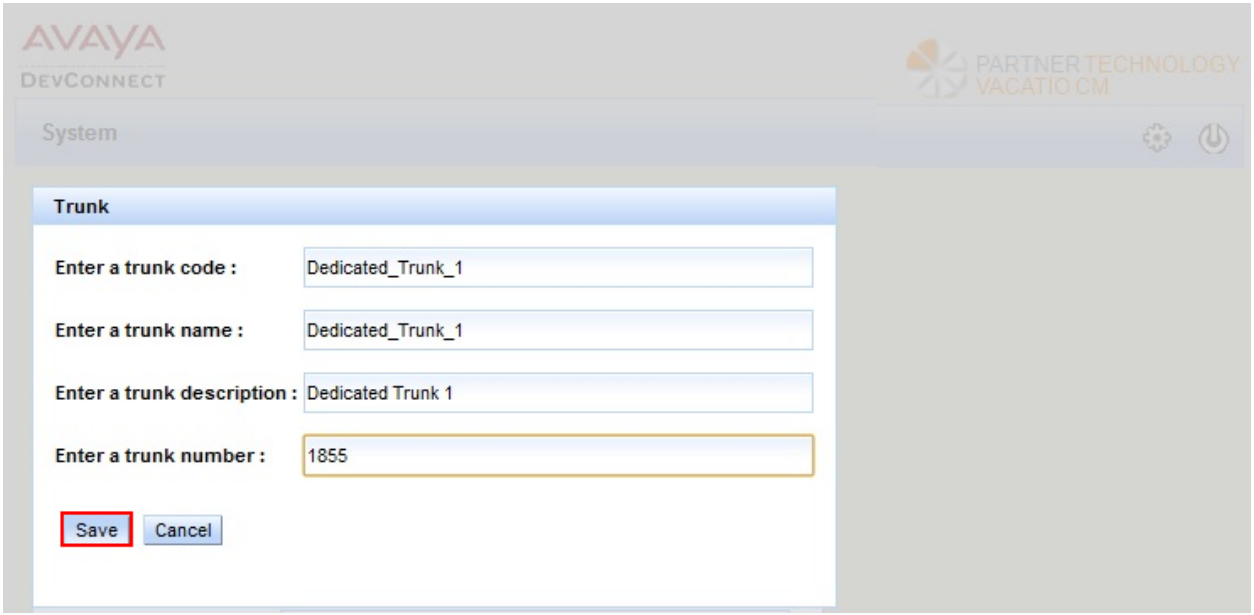
Click on **New Switch**, as shown below.

The screen below will appear, enter the relevant AES details as explained below where the **switch name** is an identifying name, the **switch Type** is **ACM**, the **switch version** is **6.0**, the **ip address** is the IP address of the AES, the **username** is the username configured in **Section 6.3** and the **service name** is the TLINK string noted in **Section 6.5**, when complete click on **New Trunk.**



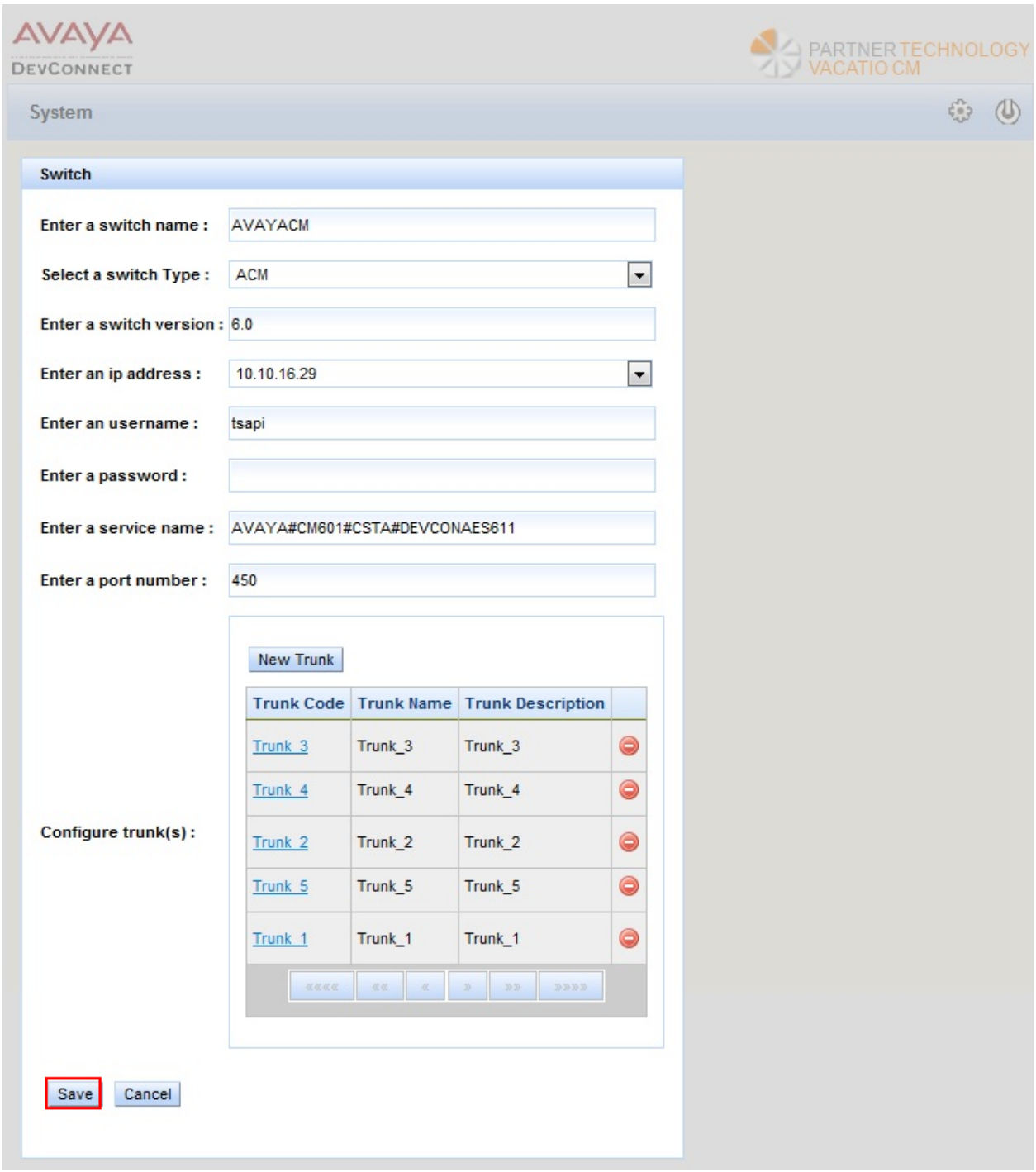
©2012 Avaya Inc. All Rights Reserved.

The following screen will appear, enter an identifying **trunk code, trunk name** and **trunk description**, assign the trunk number according to the CTI extension configured in **Section 5.6** and click **Save**, repeat this task according to the number of trunks required.



©2012 Avaya Inc. All Rights Reserved.

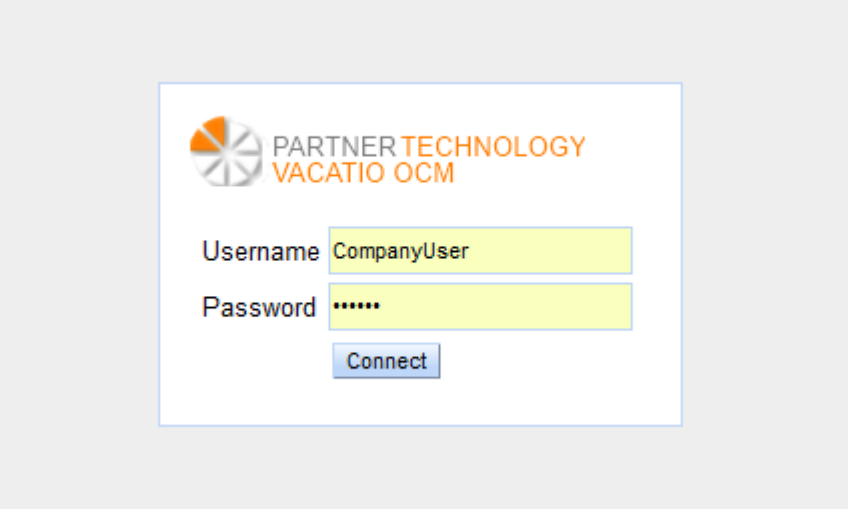
The following screen displays the CTI parameters and trunks configured, click **Save** when complete.



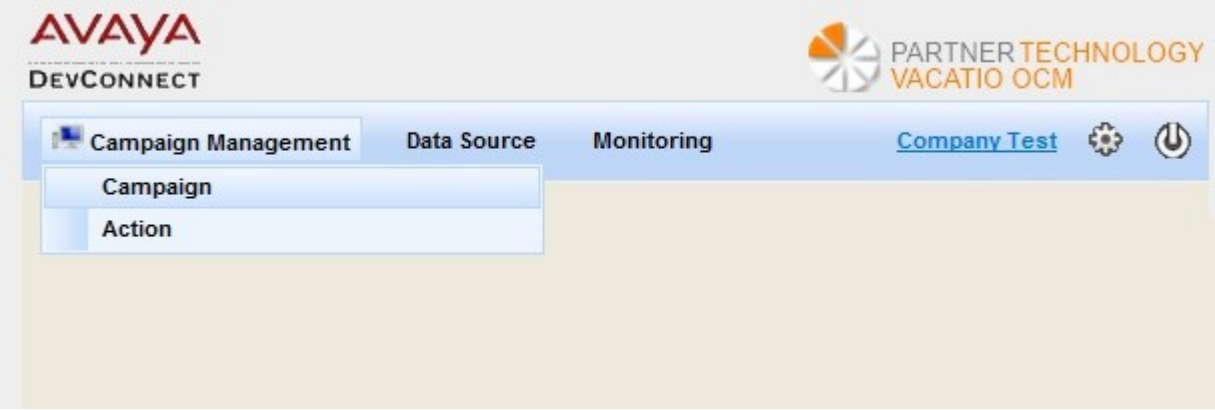
©2012 Avaya Inc. All Rights Reserved.

7.2. Create Campaign

Configuration of the OCM outbound campaign is performed from the web interface, browse to http://<ip_of_ocm:8080/OutboundCampaignManager in this case http://10.10.16.167:8080/OutboundCampaignManager, enter the relevant login details as shown below and click **Connect**.



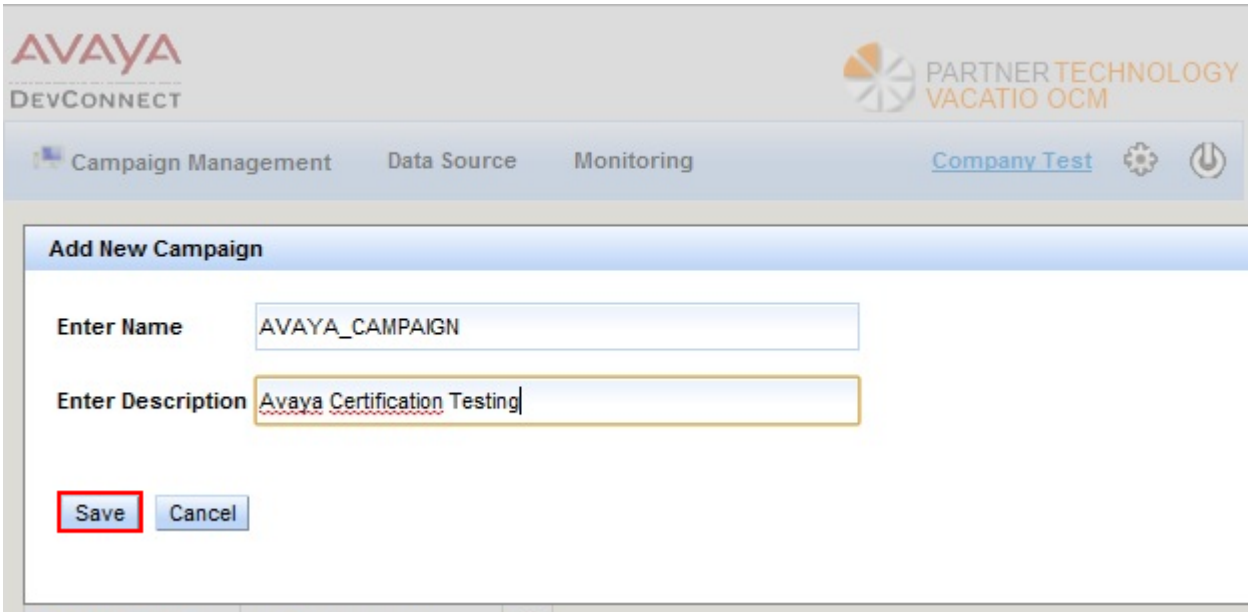
The screen shown below will display, click on **Campaign Management → Campaign.**



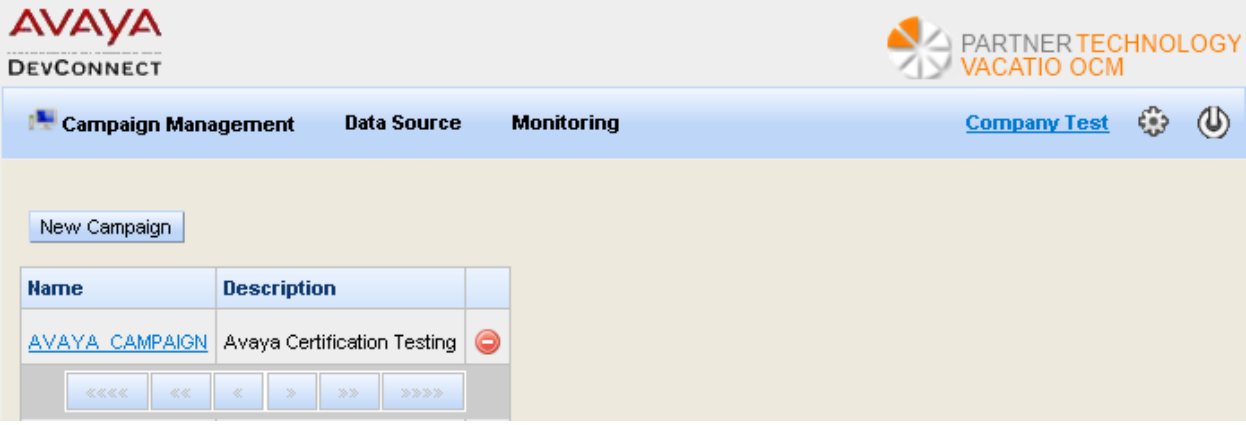
©2012 Avaya Inc. All Rights Reserved.

Click on **New Campaign.**

The **Add New Campaign** dialog box will appear, enter a **Name** and **Description** to identify the campaign and click **Save.**



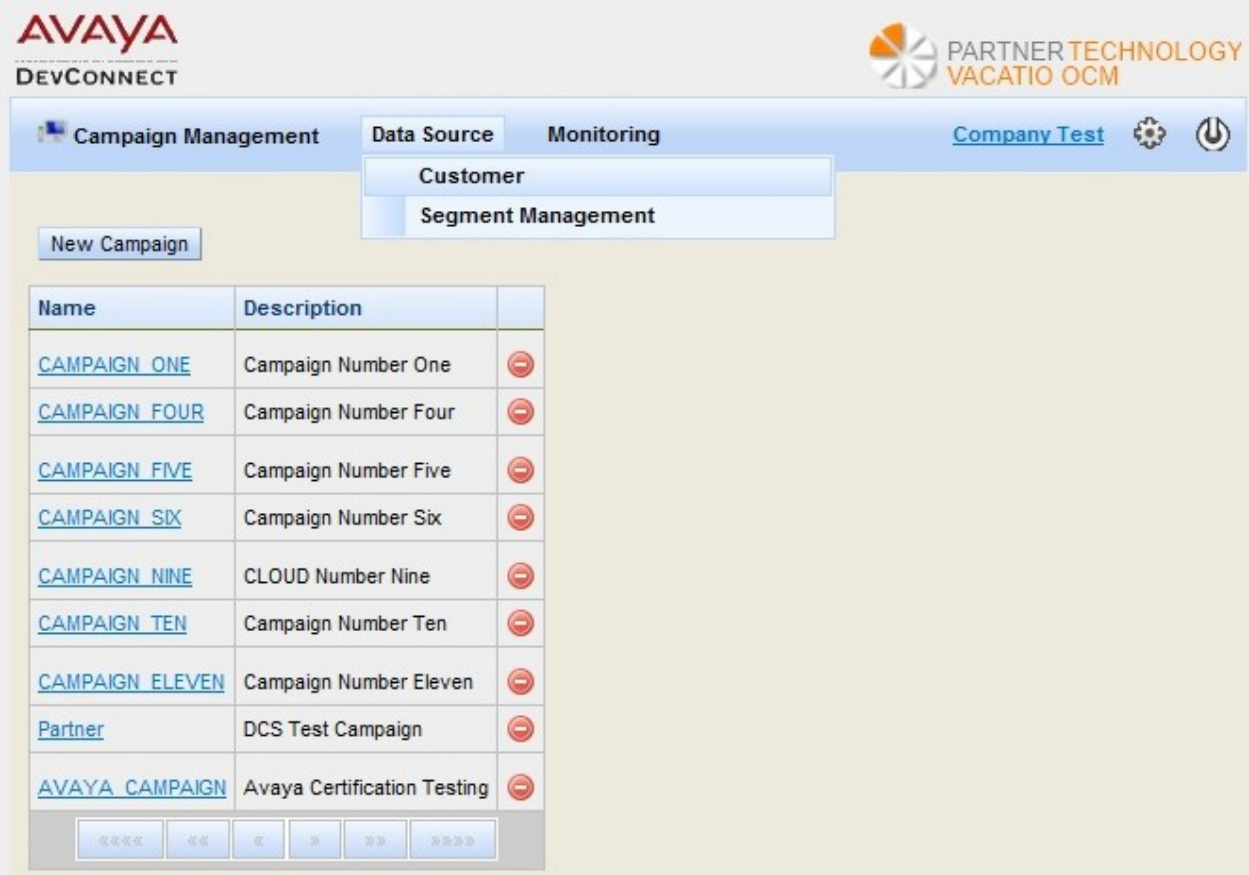
The following screen will appear displaying the new campaign.



©2012 Avaya Inc. All Rights Reserved.

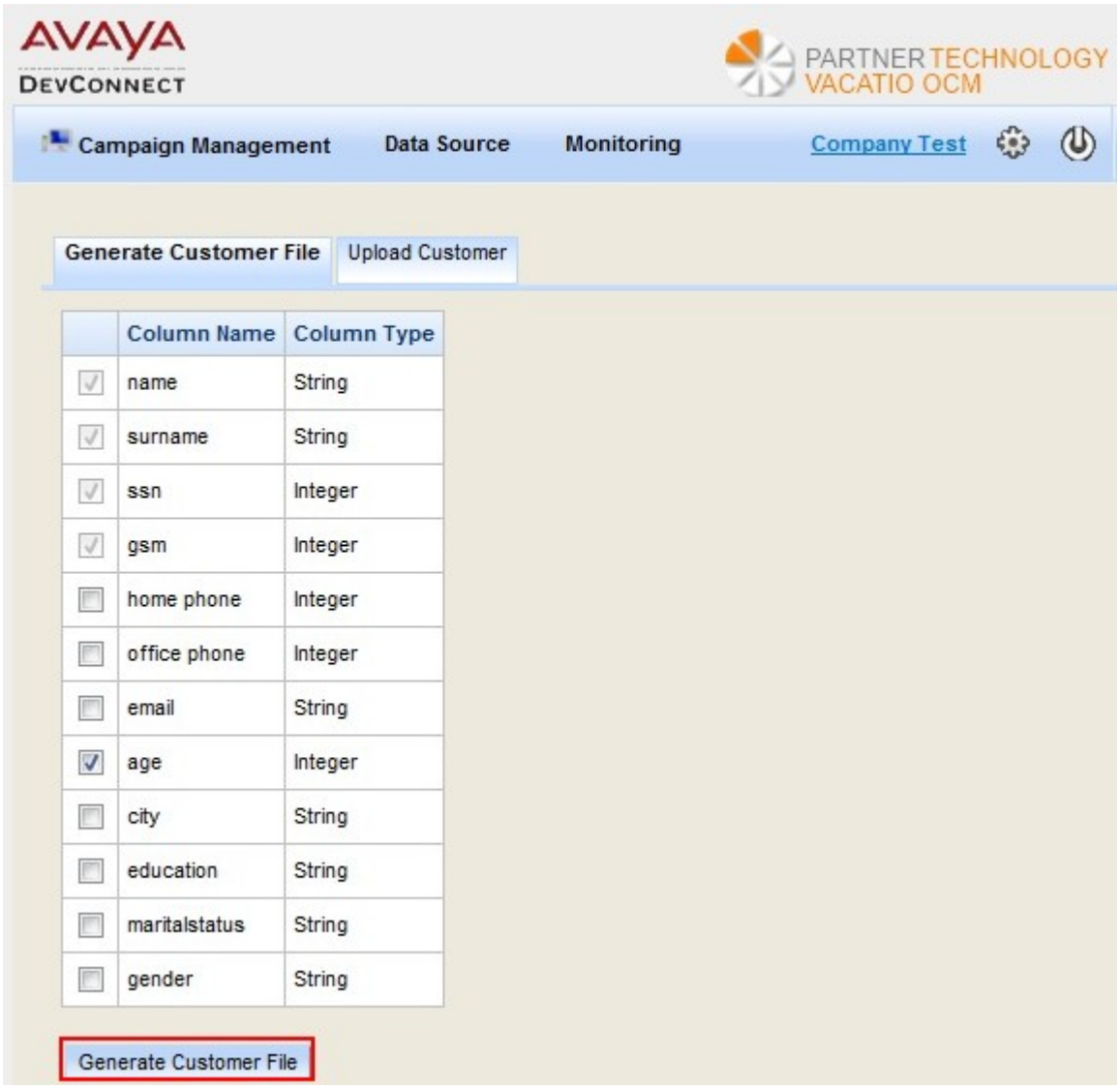
7.3. Generate Customer File

A customer file must be created, this specifies the template in which the customer data will be formatted.. Click on **Data Source → Customer.**



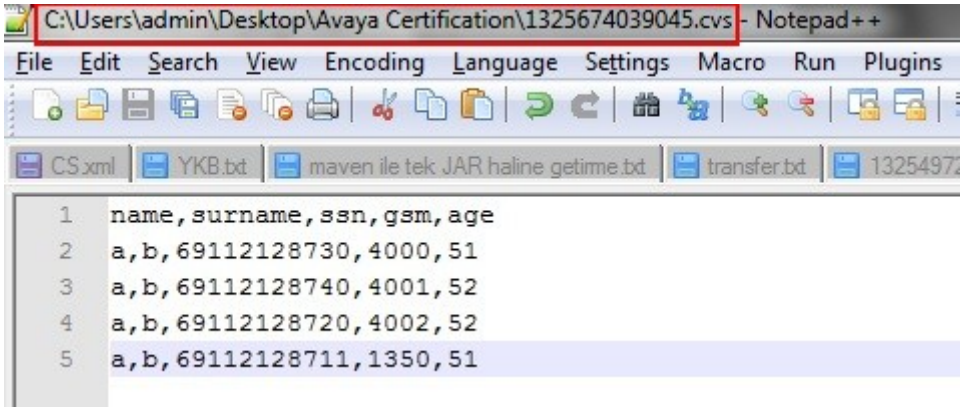
©2012 Avaya Inc. All Rights Reserved.

Place a tick next to the information to be contained in the data source, in this case **name, surname, ssn, gsm** and **age**, click **Generate Customer File** when complete.

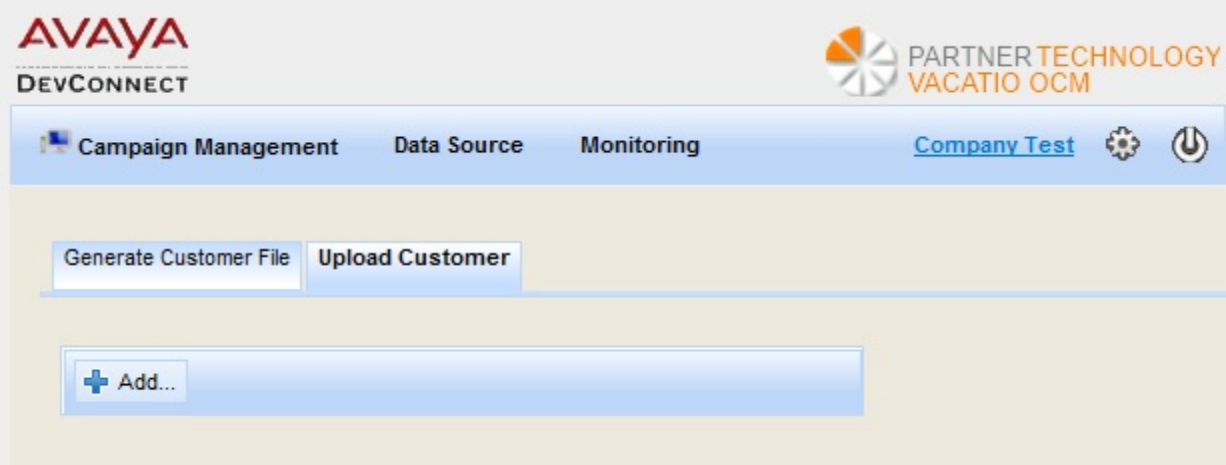


©2012 Avaya Inc. All Rights Reserved.

A **.cvs** file will be generated and a prompt will appear to download the file. The downloaded file can be opened with an appropriate text editor. Enter customer data in the comma separate format as shown below. In this example file **1325674039045.cvs** is saved on **C:\Users\admin\Desktop\Avaya Certification\.**

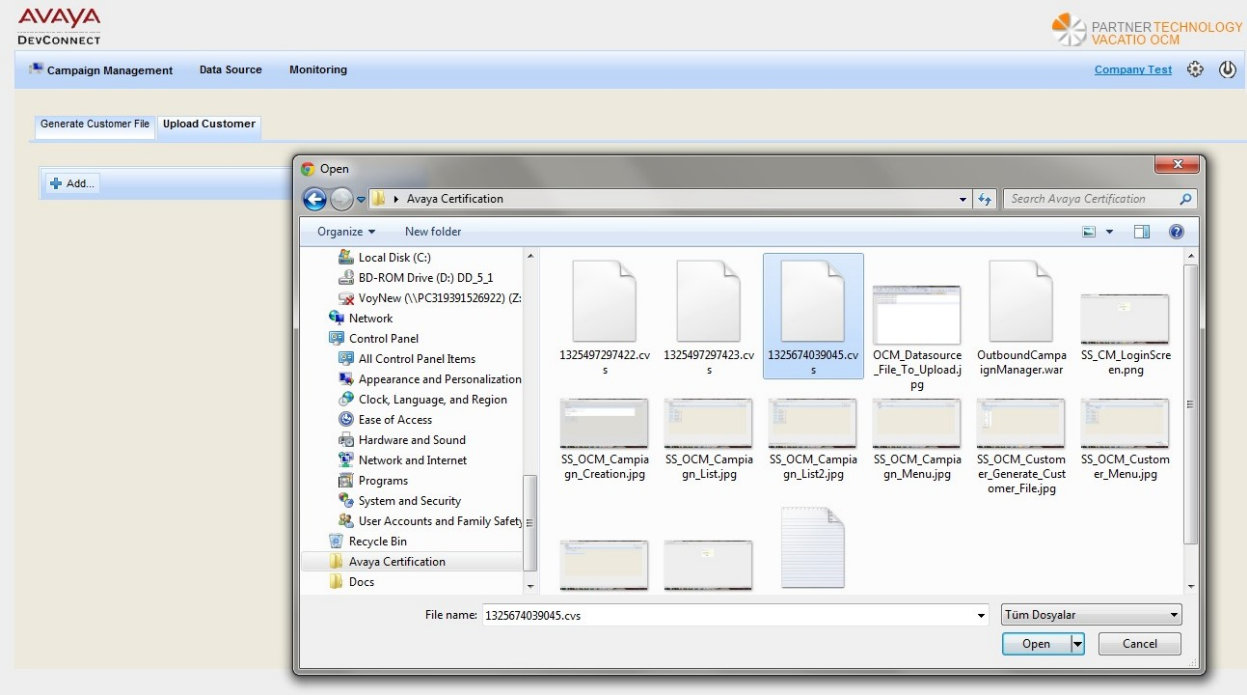


Save the file once the customer information has been added. On the OCM web interface click the **Upload Customer** tab and then click **Add.**

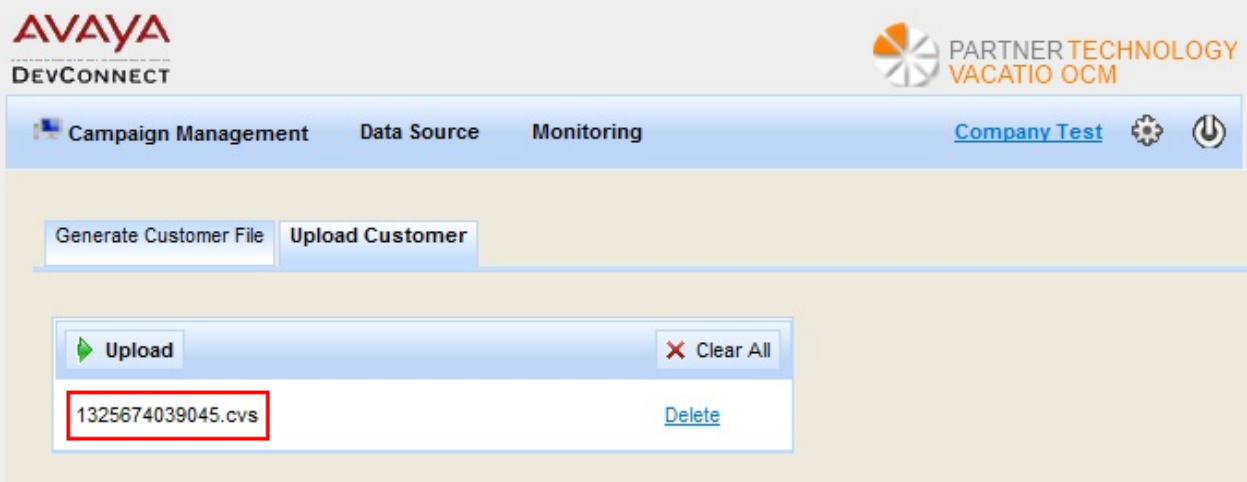


©2012 Avaya Inc. All Rights Reserved.

Browse to the saved .cvs file and click **Open.**



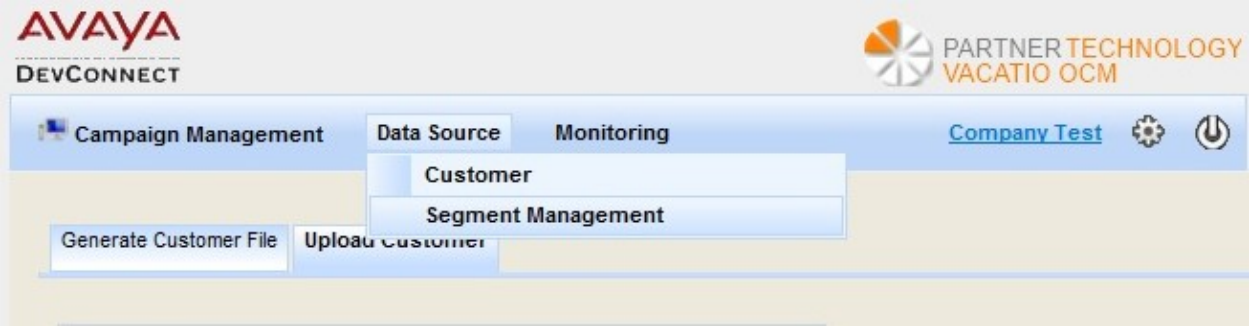
The .cvs file will be uploaded to OCM and the screen below will appear, showing the uploaded customer file.



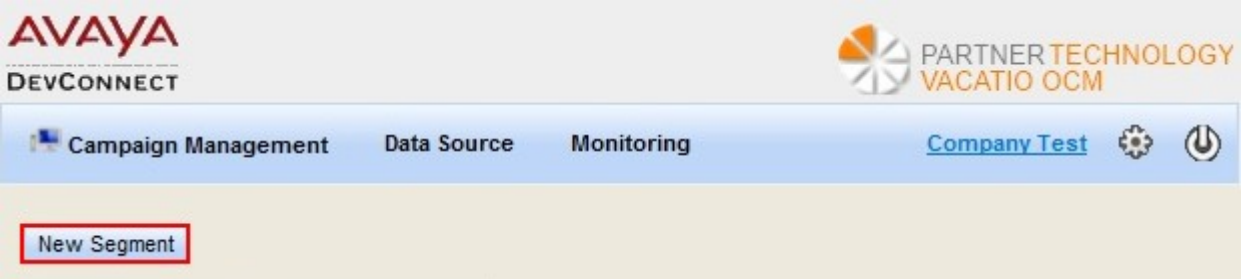
©2012 Avaya Inc. All Rights Reserved.

7.4. Create Segment

A Segment must be created, this is a filter which selects records from the customer file based on defined criteria. Click on **Data Source → Segment Management.**

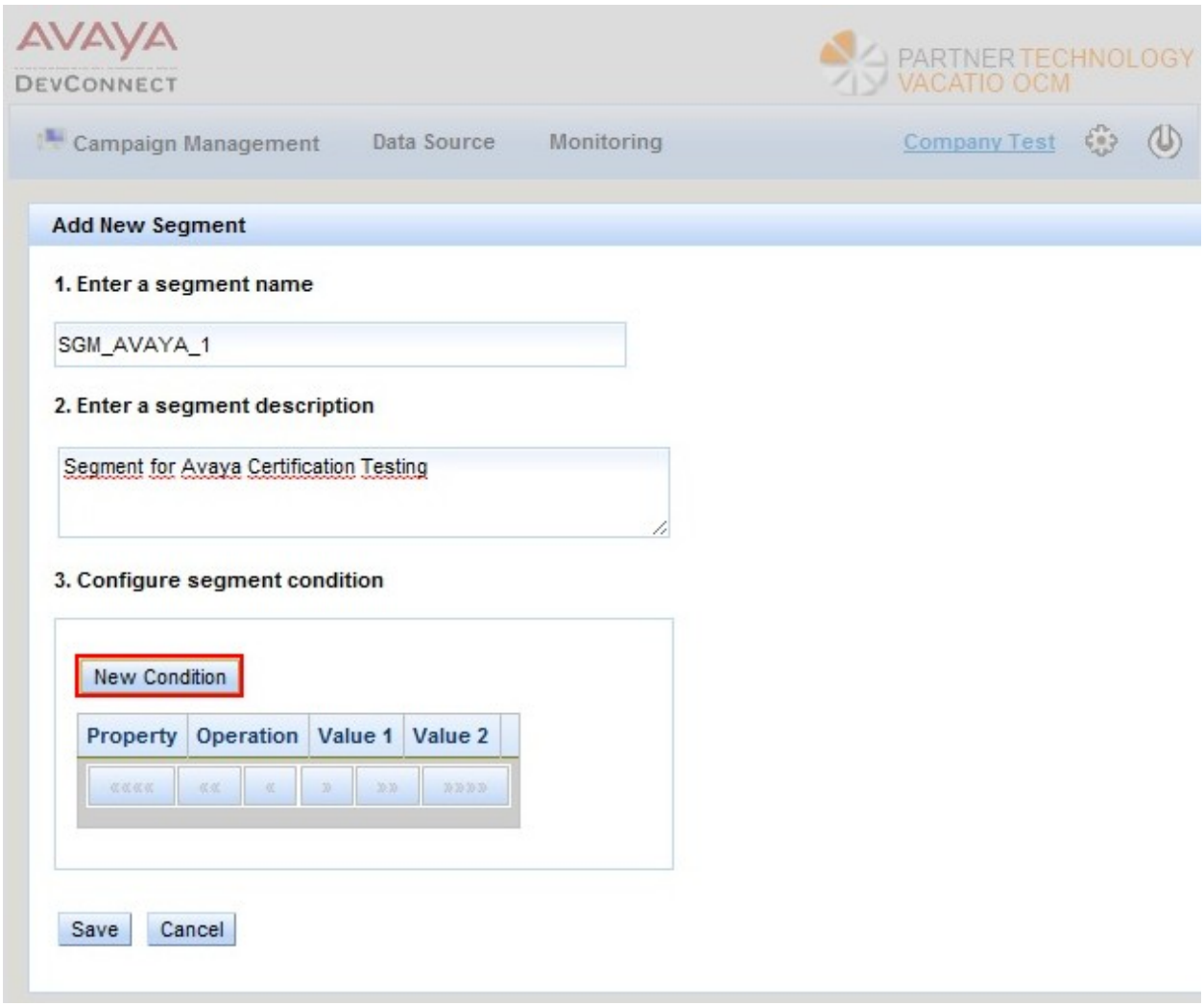


The following screen will appear, click **New Segment.**



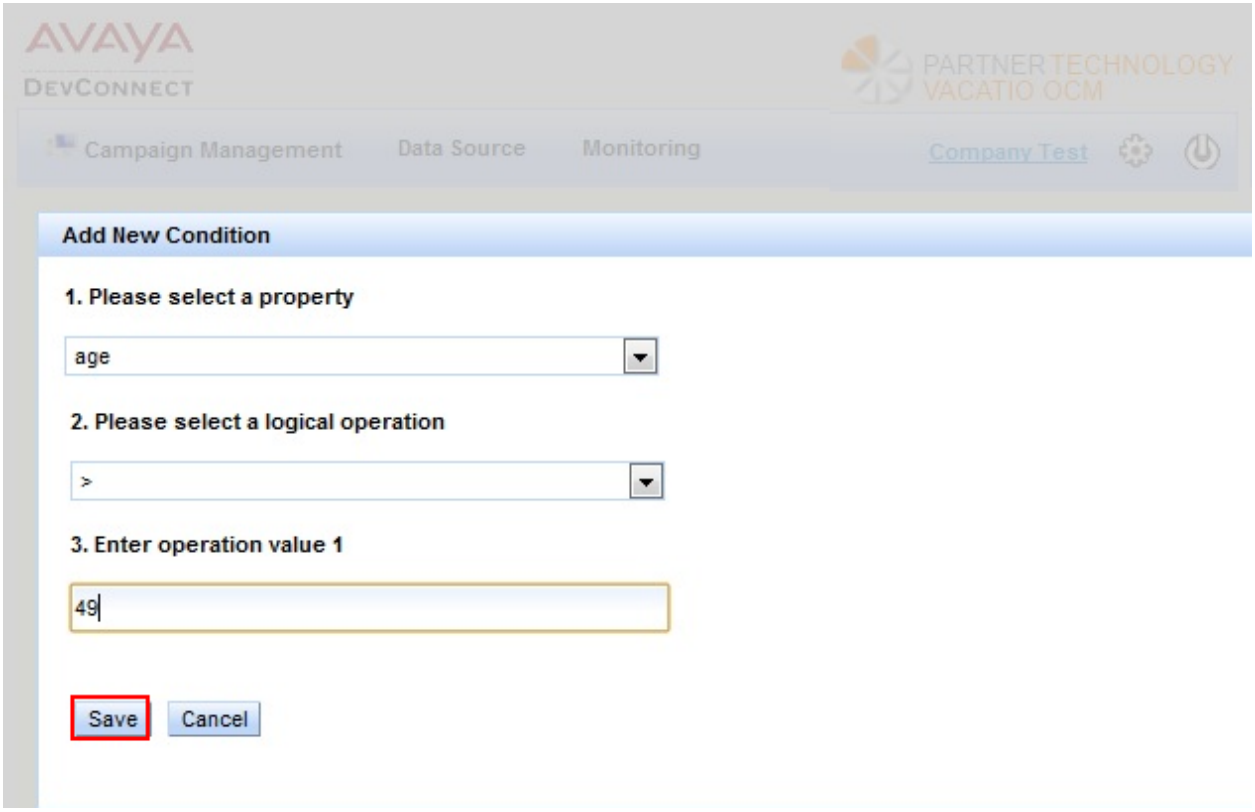
©2012 Avaya Inc. All Rights Reserved.

Enter an identifying **segment name** and **segment description** and click on **New Condition.**



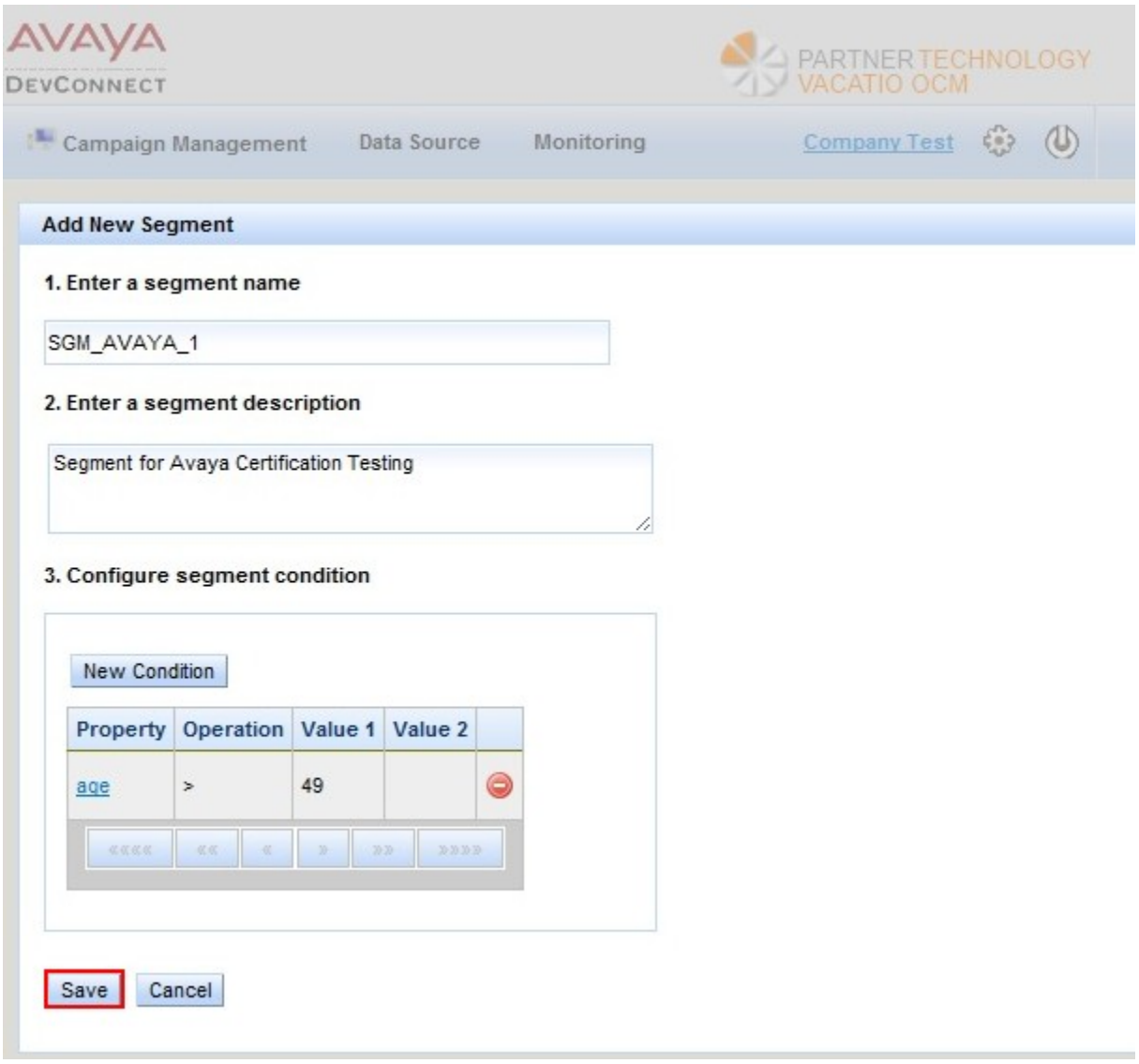
©2012 Avaya Inc. All Rights Reserved.

On the screen which appears, set the segment condition properties to be applied to the customer list, in this case records will be selected for the campaign where the **age** is more than **(>) 49**, click **Save** when done.



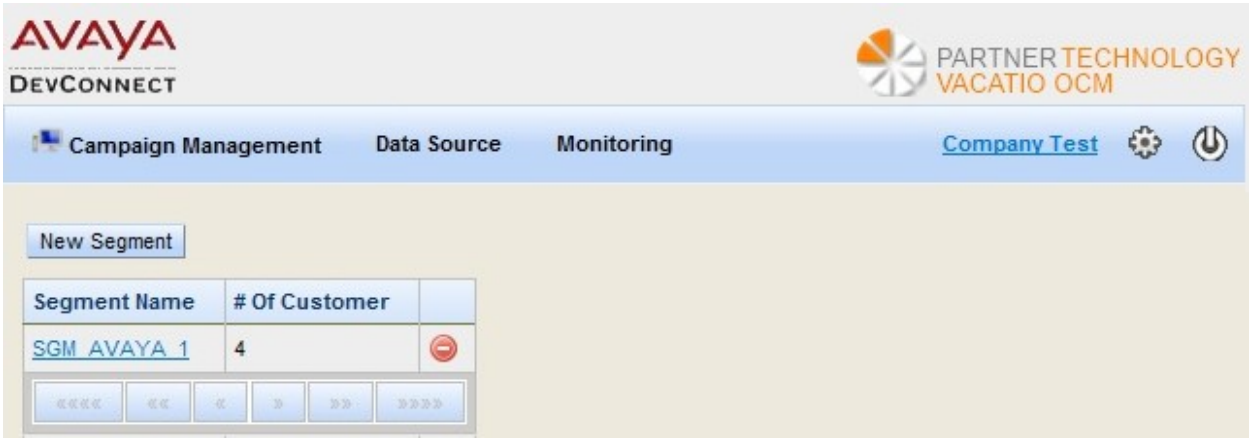
©2012 Avaya Inc. All Rights Reserved.

The screen below will be shown, displaying the new segment and condition, click **Save** when complete.



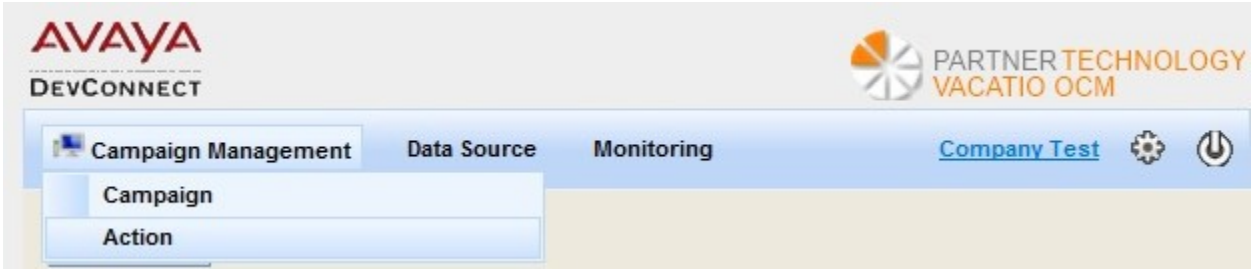
©2012 Avaya Inc. All Rights Reserved.

The screen below will appear showing the new segment and the number of customers in the customer file that match the condition.

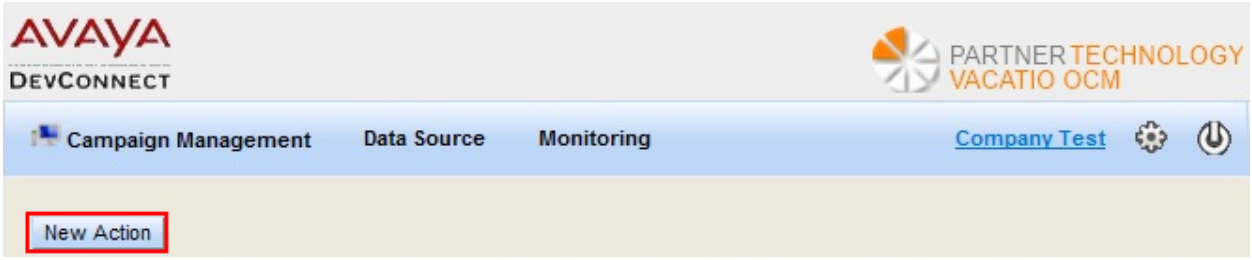


7.5. Create Action

An action must be created on OCM, the action references the campaign created in **Section 7.2.** Click on **Campaign Management → Action.**

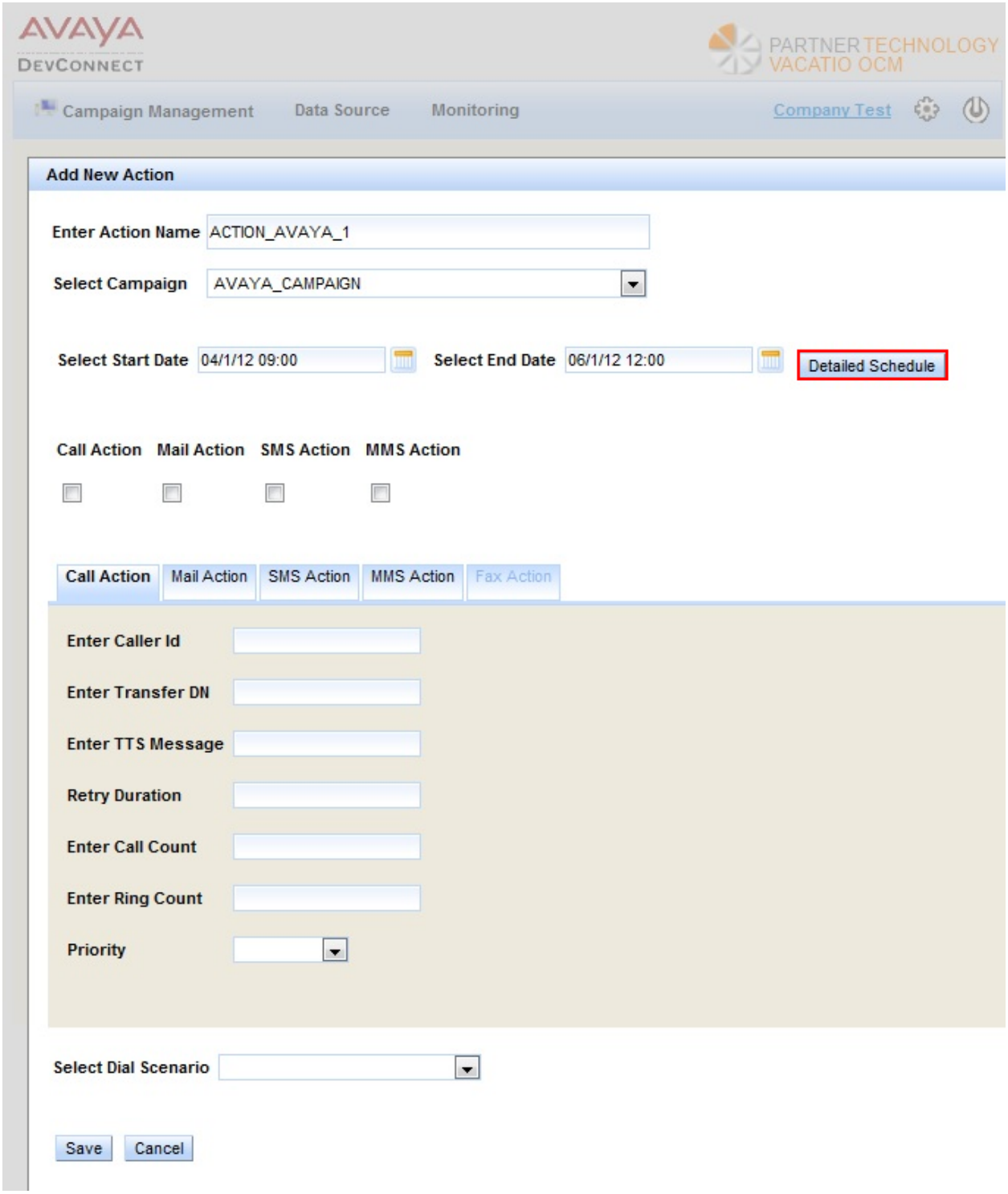


Click on **New Action.**



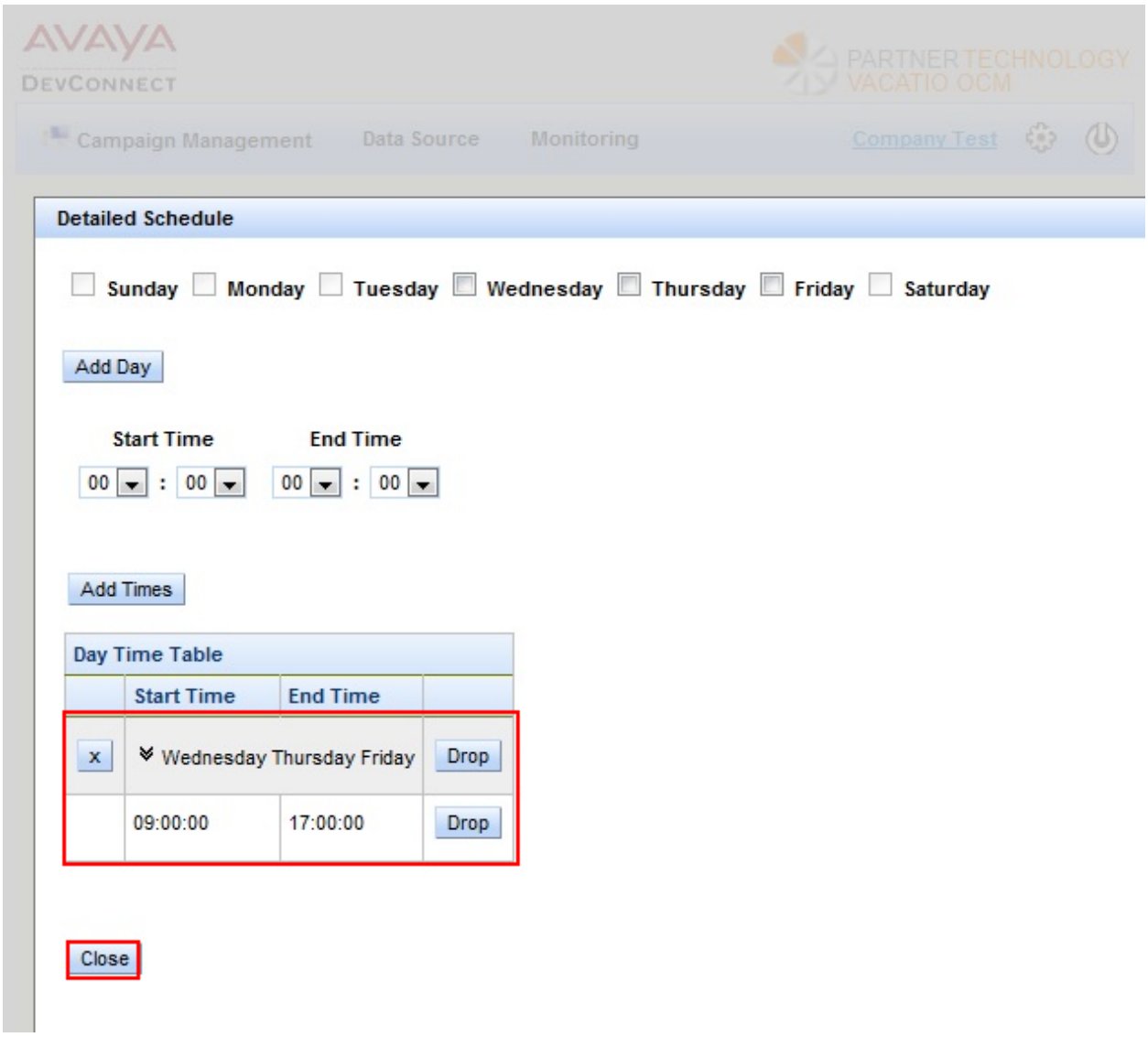
©2012 Avaya Inc. All Rights Reserved.

The screen below will appear, enter an identifying **Action Name,** and select the campaign created previously. Set the **Start Date** and **End Date** and click **Detailed Schedule.**



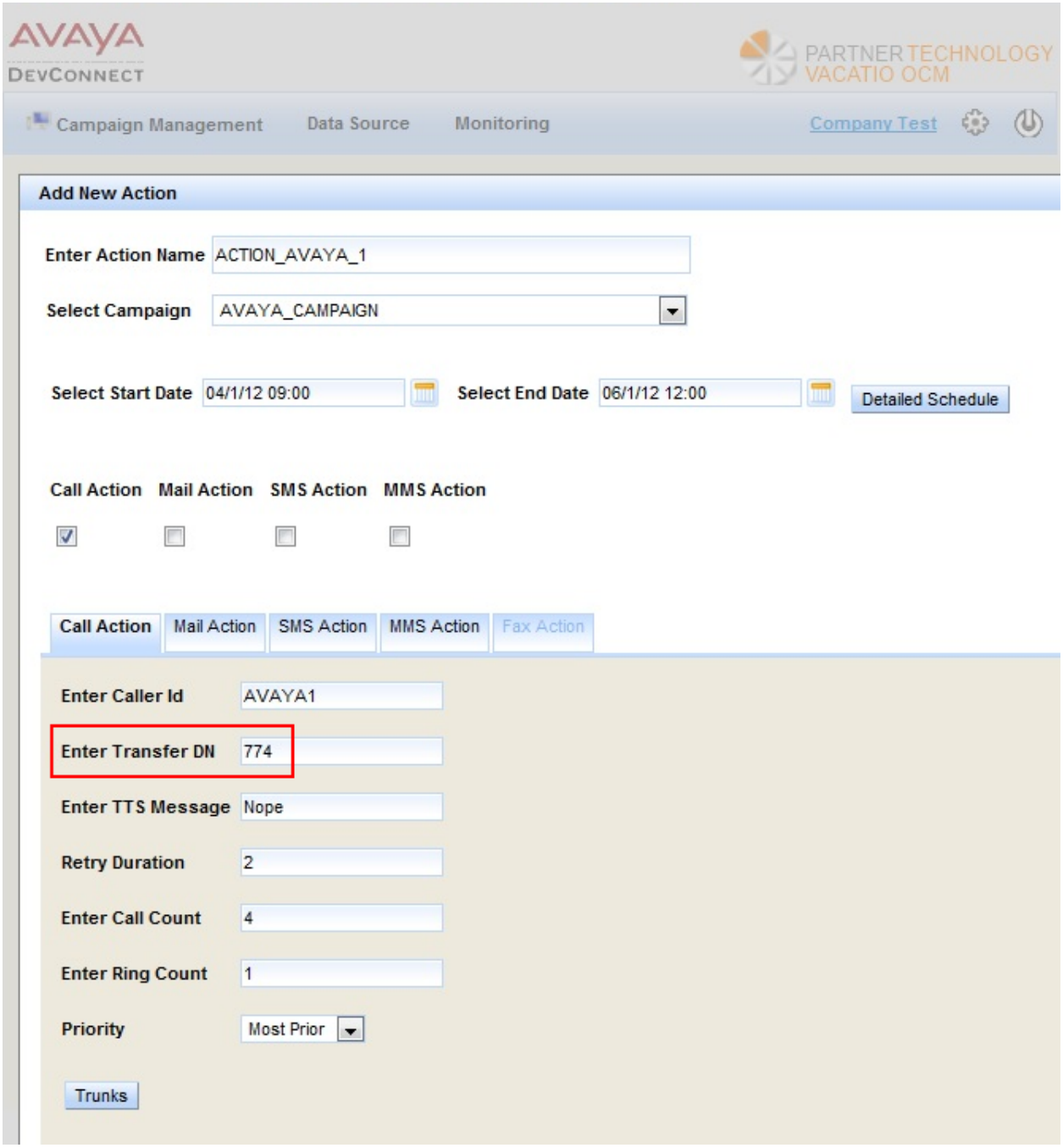
©2012 Avaya Inc. All Rights Reserved.

Choose the **Day** of the week and **Start** and **End** time for the action schedule. In this instance, Wednesday to Friday, 9.00 – 17.00 are selected. Click **Close** when complete.



©2012 Avaya Inc. All Rights Reserved.

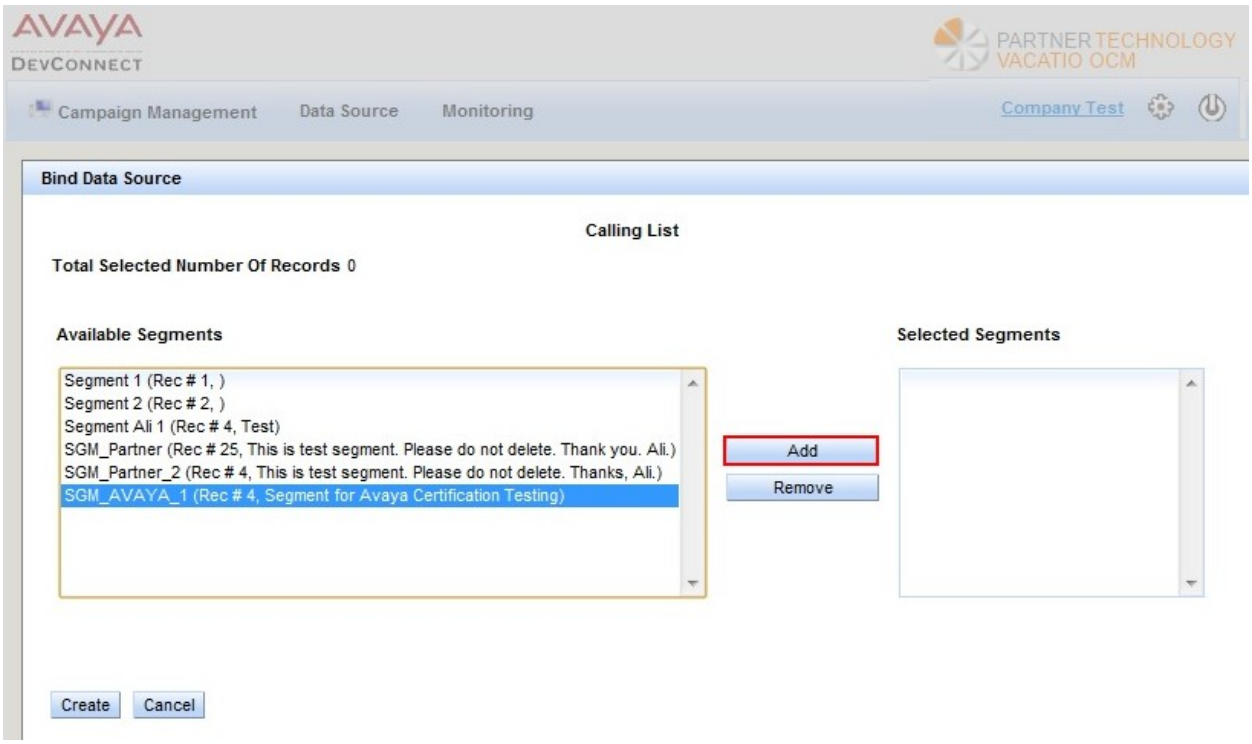
The screen below will reappear, place a tick in the **Call Action** box, enter an identifying **Caller Id**, set the **Transfer DN** as the announcement configured in **Section 5.2,** set the **Retry Duration** and **Call Count** (recall count) accordingly and click on **Save** (not shown).



©2012 Avaya Inc. All Rights Reserved.

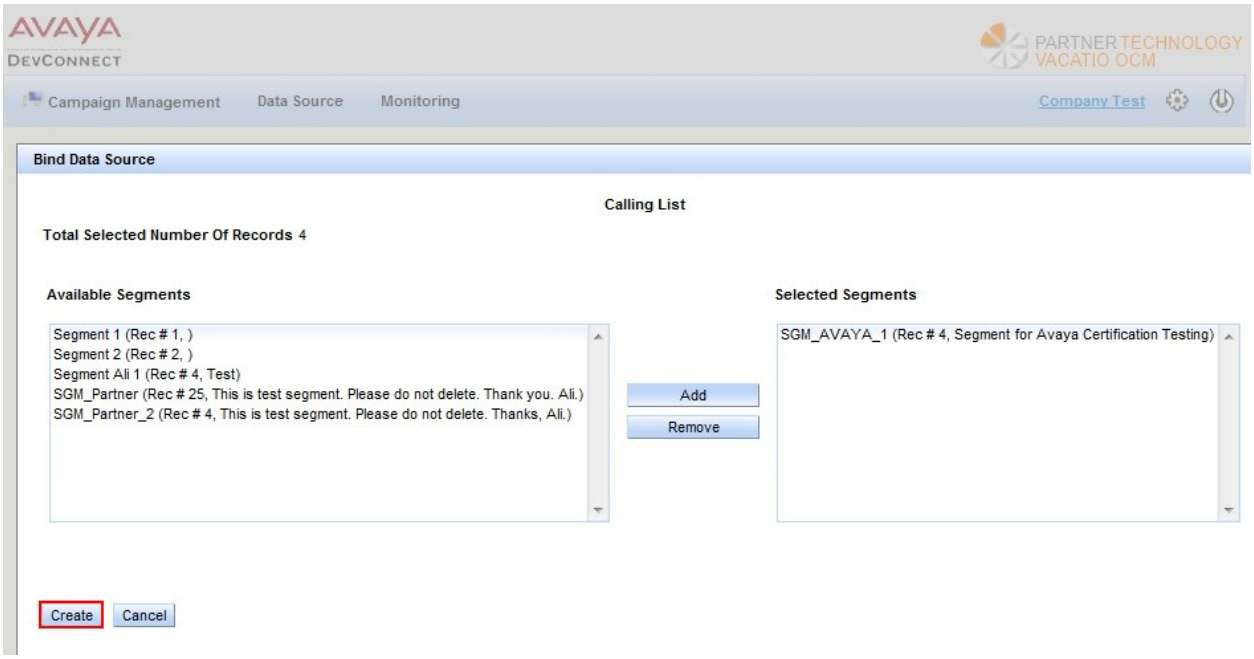
The screen below will appear displaying the newly added action. Click on **Data Source**.

The screen below will appear, select the **Segment** created in **Section 7.4** from the **Available Segments** box and click on **Add.**



©2012 Avaya Inc. All Rights Reserved.

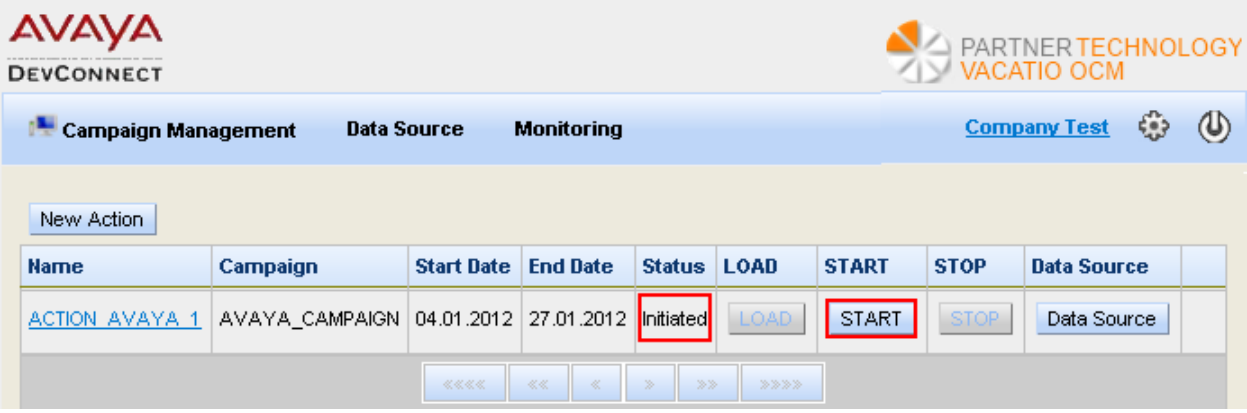
Click **Create**, this binds the data source to the segment.



The screen below will appear, click **Load.**

©2012 Avaya Inc. All Rights Reserved.

The **Status** will update to **Initiated,** click **Start** to begin the action.



8. Verification Steps

This section provides the tests that can be performed to verify correct configuration of Communication Manager, Application Enablement Services and OCM.

8.1. Verify Avaya Aura® Communication Manager CTI Link

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the TSAPI link status with Application Enablement Services by using the command **status aesvcs cti-link**. Verify the **Service State** of the TSAPI link is **established**.

```
status aesvcs cti-link

                        AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

1     4        no    devconaes611     established   87       61
```

Use the command **status aesvcs interface** to verify that the status **Local Node CLAN** of Application Enablement Services interface is connected and **listening**.

```
status aesvcs interface

                        AE SERVICES INTERFACE STATUS

Local Node         Enabled?  Number of     Status
                             Connections

clancm601          yes       1            listening
```


©2012 Avaya Inc. All Rights Reserved.

Verify that the there is a link with the Application Enablement Services and that messages are being sent and received by using the command **status aesvcs link**.

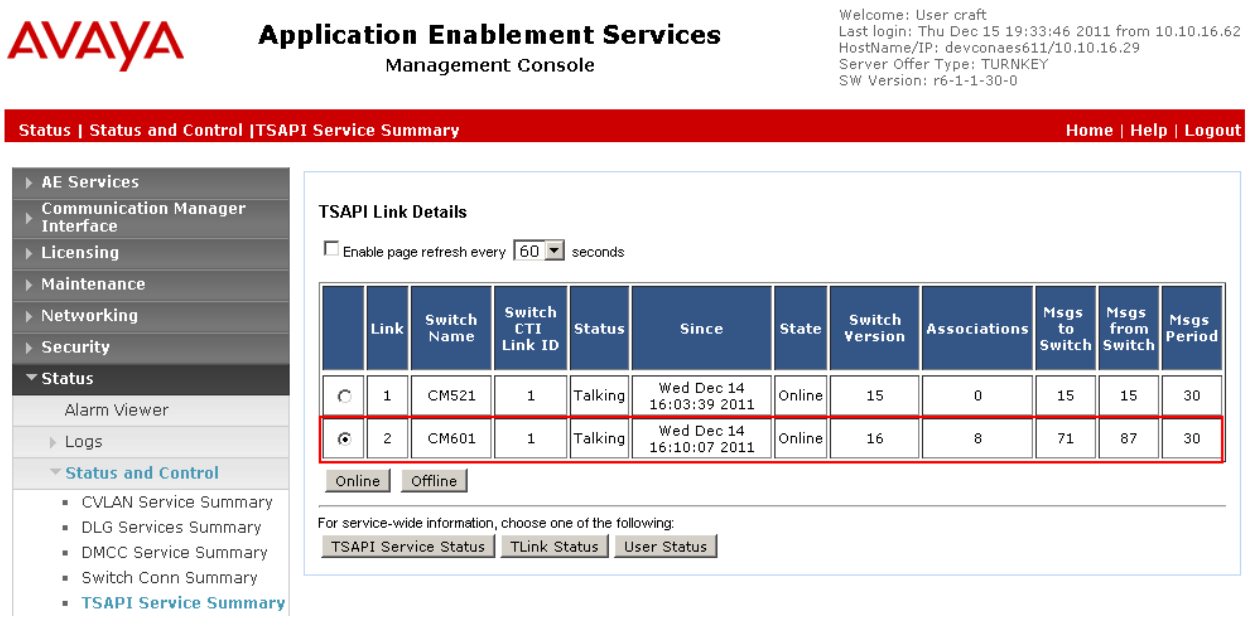
```
status aesvcs link

                          AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                          Port                    Sent    Rcvd

01/01  devconaes611    10.10.16.29      45883   clancm601       683     665
```

8.2. Verify Avaya Aura® Application Enablement Services CTI Connection

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Communication Manager, the Application Enablement Services server and OCM is functioning correctly.

8.2.1. TSAPI Link

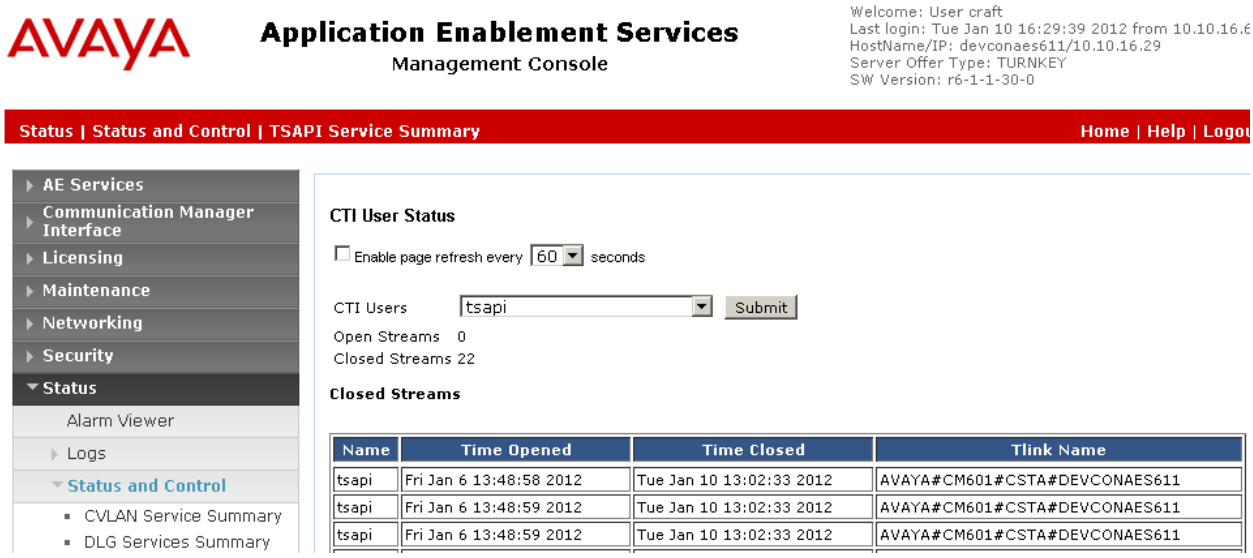
On the Application Enablement Services Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.



©2012 Avaya Inc. All Rights Reserved.

8.2.2. TSAPI User Status

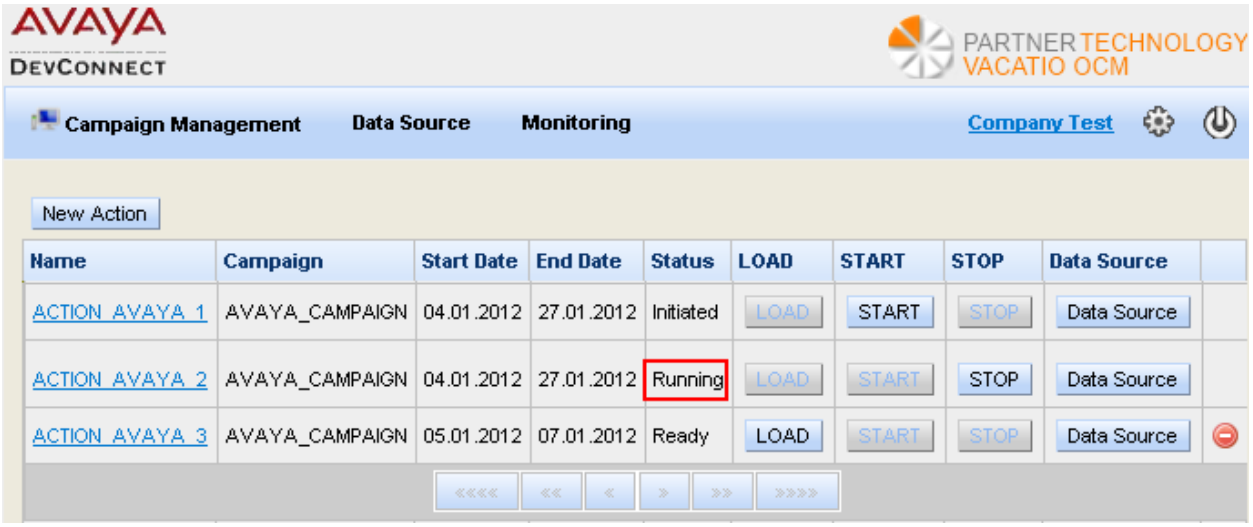
On the Application Enablement Services Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary → User Status** to display the **CTI User Status** page. Select the CTI user created in **Section 6.3** from the drop down list and click on **Show Closed Streams.** Verify that streams have been opened by the CTI user during the time the OCM campaign was running.



8.3. Verify Partner Teknoloji Outbound Campaign Manager

8.3.1. Verify Action is Running

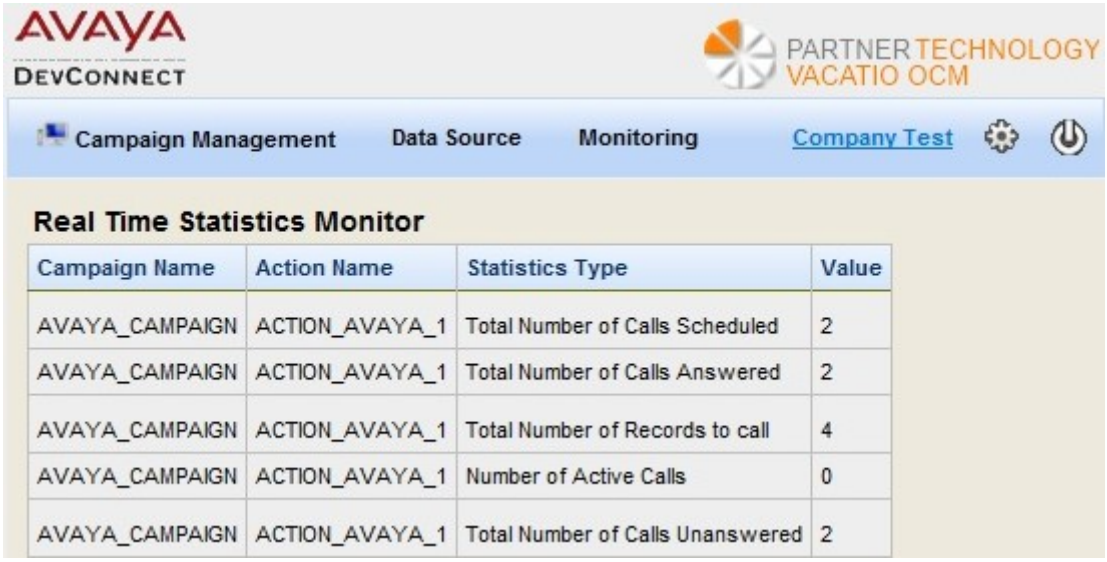
Click **Campaign Management → Action** verify the status of the relevant action is **Running.**



©2012 Avaya Inc. All Rights Reserved.

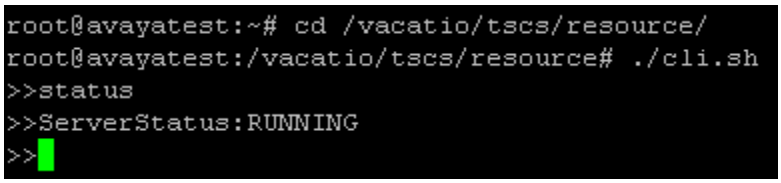
8.3.2. Verify Action Statistics

Click on **Monitoring → Real Time Monitor**, verify statistics reflect current activity.



8.3.3. Verify TSCS Service Status

From the Debian shell, navigate to **/vacatio/tscs/resource** and execute the **./cli.sh** command. At the prompt enter the **status** command and verify **ServerStatus:RUNNING** as shown below.



©2012 Avaya Inc. All Rights Reserved.

8.3.4. Verify TSCS Trunks Status

At the same prompt, enter the **trunks** command, verify trunks status are **IDLE** or **IN_USE** accordingly.

```
>>trunks
>>Pbx Id        Extension         Status    Company Id    Action Id
-------       ----------        ------    ----------    ---------
     10             1852          IDLE             0            0
     10             1851          IDLE             0            0
     10             1850          IDLE             0            0
     10             1854          IDLE             0            0
     10             1853        IN_USE             0            0
```

9. Conclusion

These Application Notes describe the configuration steps required for the Partner Teknoloji Outbound Campaign Management solution to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2.**

10. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

[1] Administering Avaya Aura® Communication Manager – Release 6.0, Issue 6.0, June 2010

Product documentation for Partner Teknoloji Products can be found at http://www.partnerteknoloji.com.tr

©2012 Avaya Inc. All Rights Reserved.

©2012 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.