Avaya Solution & Interoperability Test Lab

Application Notes for CallScripter with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CallScripter to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. CallScripter is an agent scripting application.

In the compliance testing, each agent logged into CallScripter, and used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor the agent station on Avaya Aura® Communication Manager, to provide screen pop and call control via an Internet Explorer browser window from the agent desktop.

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.

©2015 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required for CallScripter to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. CallScripter is an agent scripting application.

In the compliance testing, each agent logged into CallScripter, and used the Device, Media, and Call Control (DMCC) .NET interface from Avaya Aura® Application Enablement Services to monitor the agent station on Avaya Aura® Communication Manager, to provide screen pop and call control via an Internet Explorer browser window from the agent desktop.

For the compliance testing, a sample script with standard Communication Toolbar buttons was provided by CallScripter. Note that any scripts involving call control customization and deviation from the standard Communication Toolbar will require separate compliance test.

2. General Test Approach and Test Results

The feature test cases were performed manually. Agents used the telephone to perform agent login, logout, and change work modes. Incoming ACD calls were placed with available agents that were logged into the ACD and to the CallScripter server. Manual call controls were exercised from the agent desktops via the Internet Explorer browser window to verify proper call handling such as answer and transfer.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the CallScripter agent desktop and server.

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.

©2015 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on CallScripter:

- Use of DMCC monitoring services to monitor agent stations.
- Use of DMCC call control services to support call control.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, conference, transfer, and long duration.

The serviceability testing focused on verifying the ability of CallScripter to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the CallScripter agent desktop and server.

2.2. Test Results

All test cases were executed, and the following were observations on CallScripter:

- In general, mixed use of agent desktop and telephone to perform call control actions are supported. For the transfer and conference features, however, all actions need to start and complete from the same source. Also, the agent desktop only supports transfer/conference of inbound calls and not outbound calls by design.
- The application does not support screen pop of PSTN calling party information at the transfer-to and conference-to agent desktops by design.
- The application provides limited support for conference scenarios by design, and the telephone can be used as a workaround if needed to control the conference call.
- After the agent logs back into CallScripter post an Ethernet disruption, any active call on the agent telephone may not be reflected on the agent desktop, and the agent can use the telephone to manually drop the active call.

2.3. Support

Technical support on CallScripter can be obtained through the following:

- **Phone:** +44 (0) 844-544-8882
- **Email:** support@callscripter.com
- **Web :** https://helpdesk.callscripter.com

©2015 Avaya Inc. All Rights Reserved.

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center devices are not the focus of these Application Notes and will not be described. In addition, the development of the sample script is outside the scope of the compliance test and will not be described.

In the compliance testing, each agent desktop was installed with CallScripter CT Providers, monitored an agent station extension shown in the table below, and used the Internet Explorer browser window for screen pop and call control.

Device Type	Extension
VDNs	60001, 60002
Skill Groups	65081, 65082
Supervisor	65000
Agent Stations	65001, 65002
Agent IDs	65881, 65882
Agent Passwords	65881, 65882

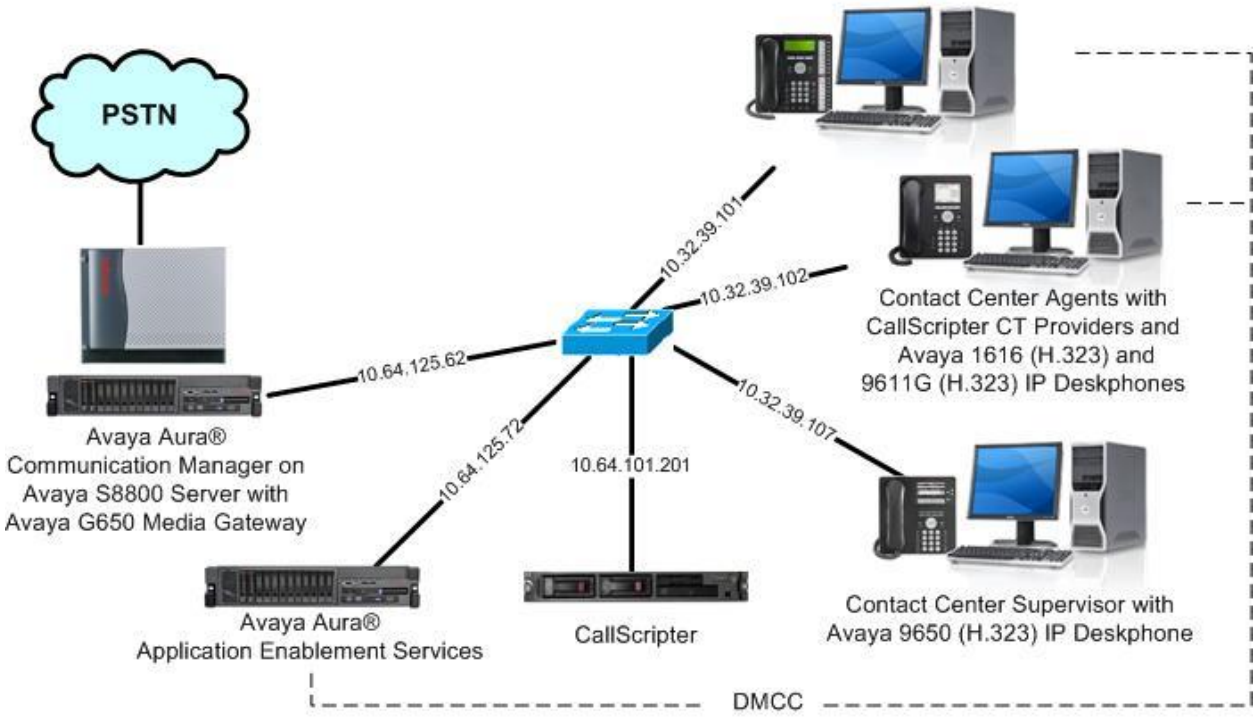


Figure 1: Compliance Testing Configuration

©2015 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway	6.3.9 (R016x.03.0.124.0-21971)
Avaya Aura® Application Enablement Services	6.3.3 SP1 (6.3.3.1.10-0)
Avaya 1616 IP Deskphone (H.323)	1.350B
Avaya 9611G IP Deskphone (H.323)	6.4.0.14
Avaya 9650 IP Deskphone (H.323)	3.230A
CallScripter on Windows Server 2012	4.5.40.18864 R2 Standard
CallScripter CT Providers • Avaya DMCC .NET	4.41.19801 6.2.0.29

©2015 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer CTI link
- Obtain VDN names

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "display system-parameters customer-options" command to verify that the **Computer Telephony Adjunct Links** customer option is set to "y" on **Page 3**. If this option is not set to "y", then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                  ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
```

5.2. Administer CTI Link

Add a CTI link using the "add cti-link n" command, where "n" is an available CTI link number. Enter an available extension number in the **Extension** field. Note that the CTI link number and extension number may vary. 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 2                                                  Page   1 of   3
                                    CTI LINK
 CTI Link: 2
Extension: 60100
     Type: ADJ-IP
                                                                   COR: 1
     Name: AES CTI Link
```


©2015 Avaya Inc. All Rights Reserved.

5.3. Obtain VDN Names

Use the "list vdn" command to display a list of pre-configured VDNs. Make a note of the **Name** for each VDNs from **Section 3**, which will be used later to configure CallScripter. In the compliance testing, the two VDNs shown below were used.

```
list vdn                                                                Page   1

                          VECTOR DIRECTORY NUMBERS

                                                                        Evnt
                                        VDN         Vec           Orig    Noti
Name (22 characters)   Ext/Skills     Ovr COR TN  PRT Num  Meas Annc    Adj

CallScripter Sales     60001           n  1   1    V  1    none          1

CallScripter Support   60002           n  1   1    V  2    none          1
```


©2015 Avaya Inc. All Rights Reserved.

6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Disable security database
- Restart service
- Administer CallScripter user
- Administer ports

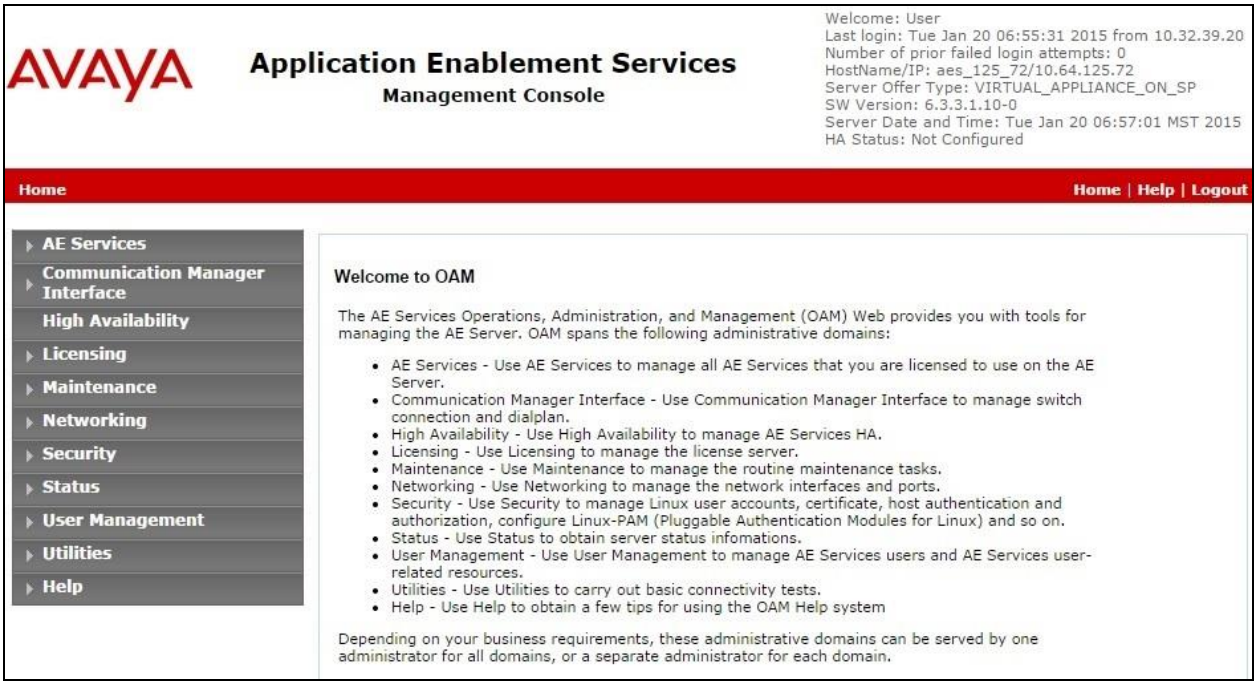
6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.

©2015 Avaya Inc. All Rights Reserved.

The **Welcome to OAM** screen is displayed next.



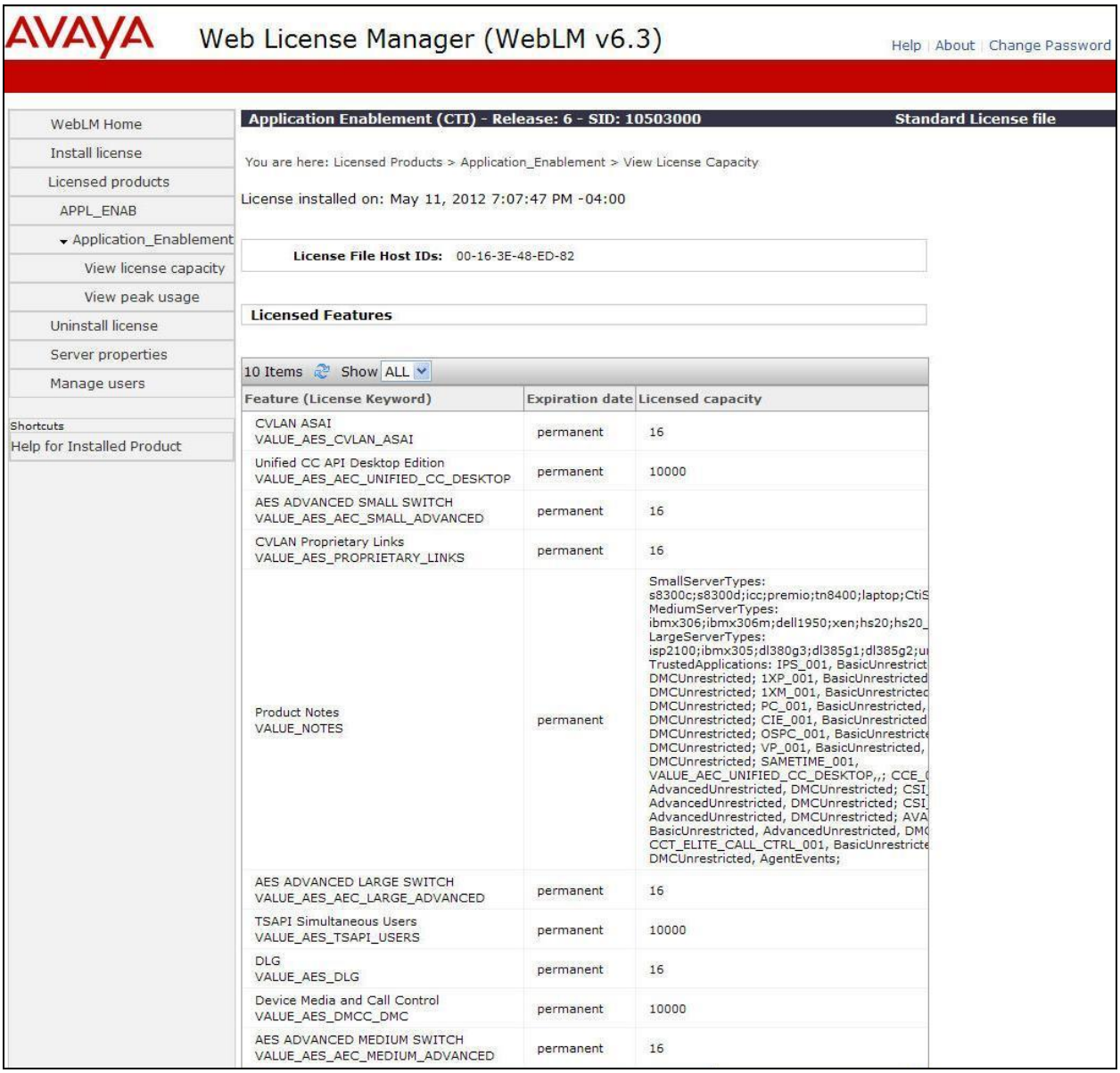
6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.

©2015 Avaya Inc. All Rights Reserved.

The **Web License Manager** screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane, to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. Note that the TSAPI license is used for device monitoring and call control via DMCC, and that no specific DMCC license is required for integration with CallScripter.



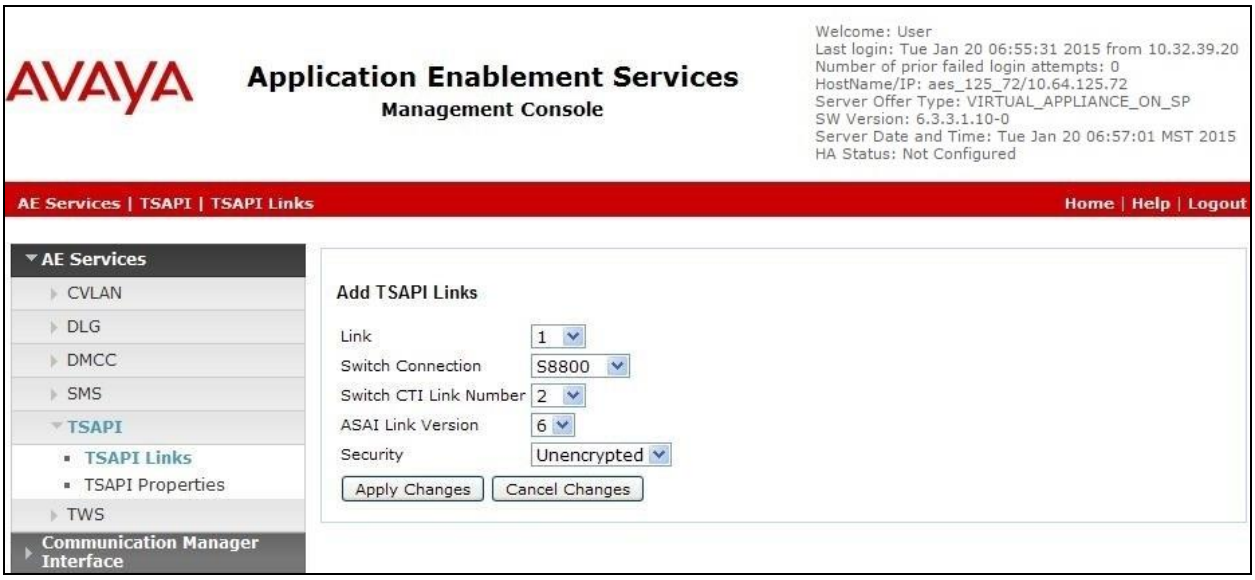
©2015 Avaya Inc. All Rights Reserved.

6.3. Administer TSAPI Link

Select **AE Services → TSAPI → TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.

The **Add TSAPI Links** screen is displayed next.

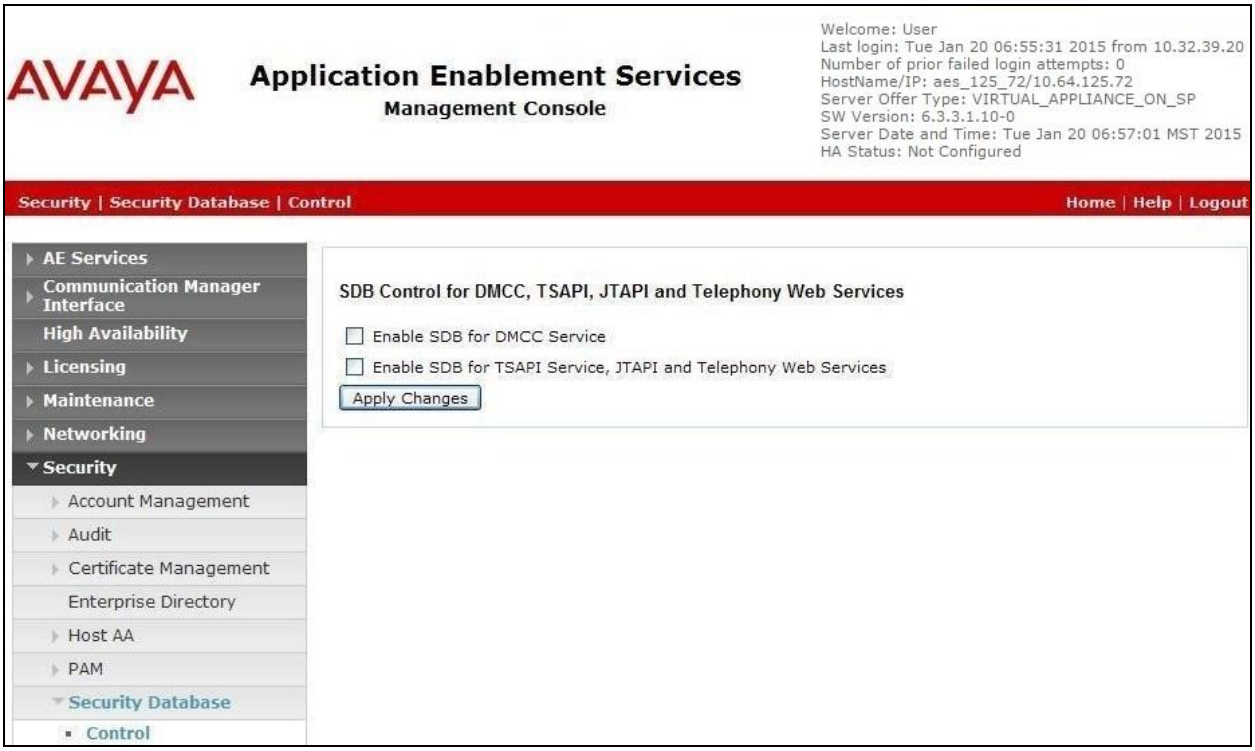
The **Link** field is only local to the Application Enablement Services server, and may be set to any available number. For **Switch Connection**, select the relevant switch connection from the drop-down list. In this case, the existing switch connection "S8800" is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. Retain the default values in the remaining fields.



©2015 Avaya Inc. All Rights Reserved.

6.4. Disable Security Database

Select **Security → Security Database → Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck both fields below.



©2015 Avaya Inc. All Rights Reserved.

6.5. Restart Service

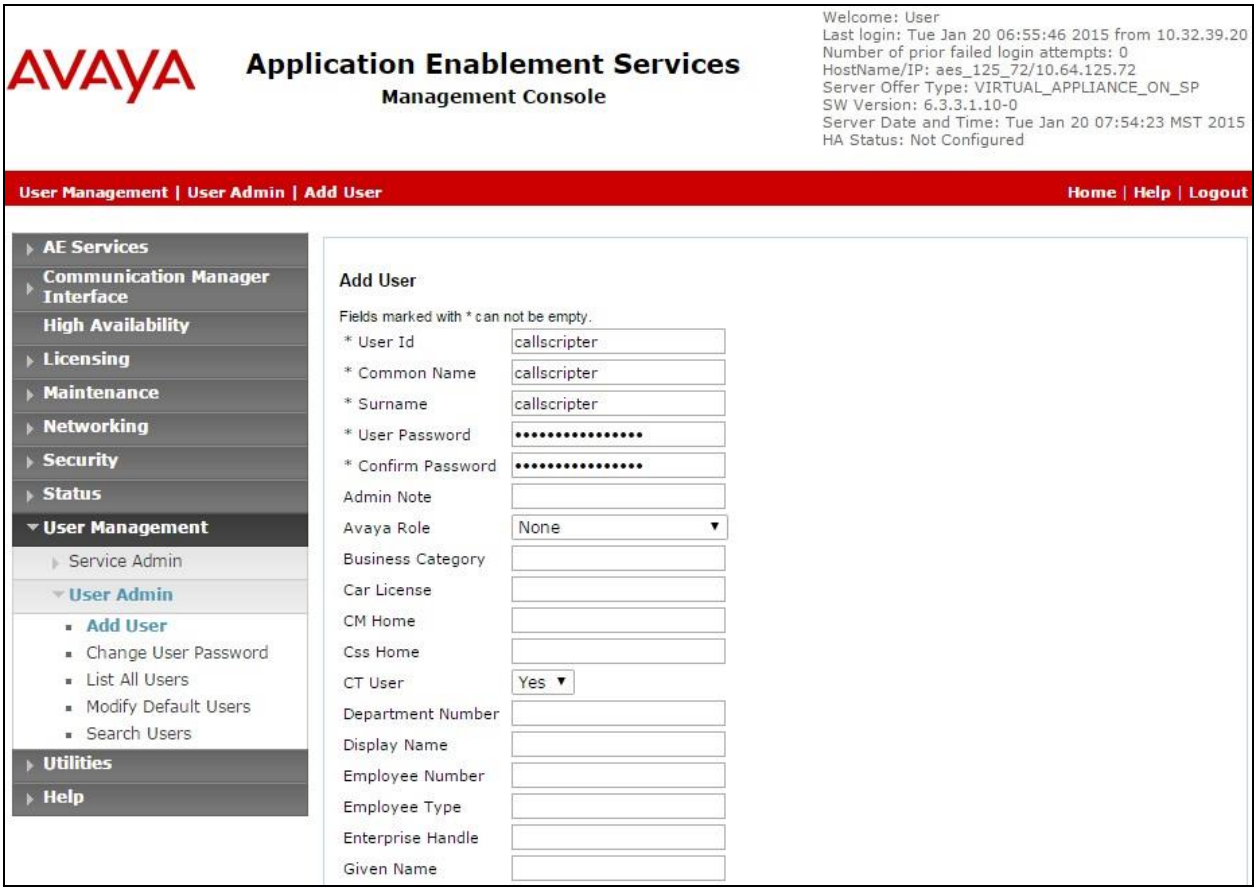
Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service** as shown below, and click **Restart Service**.

©2015 Avaya Inc. All Rights Reserved.

6.6. Administer CallScripter User

Select **User Management → User Admin → Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select "Yes" from the drop-down list. Retain the default value in the remaining fields.

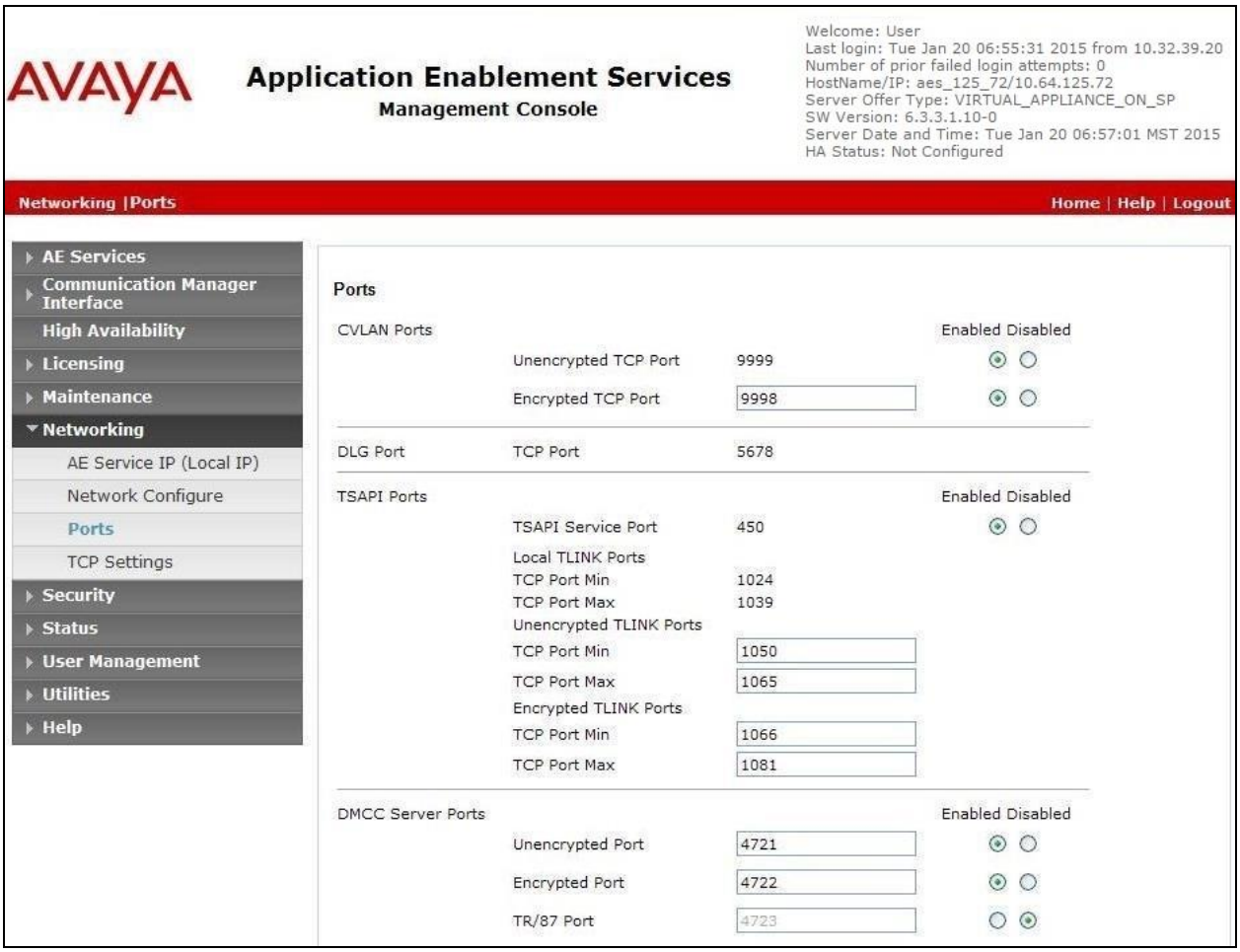


©2015 Avaya Inc. All Rights Reserved.

6.7. Administer Ports

Select **Networking → Ports** from the left pane, to display the **Ports** screen in the right pane.

In the **DMCC Server Ports** section, select the radio button for **Encrypted Port** under the **Enabled** column, as shown below. Retain the default values in the remaining fields.



©2015 Avaya Inc. All Rights Reserved.

7. Configure CallScripter

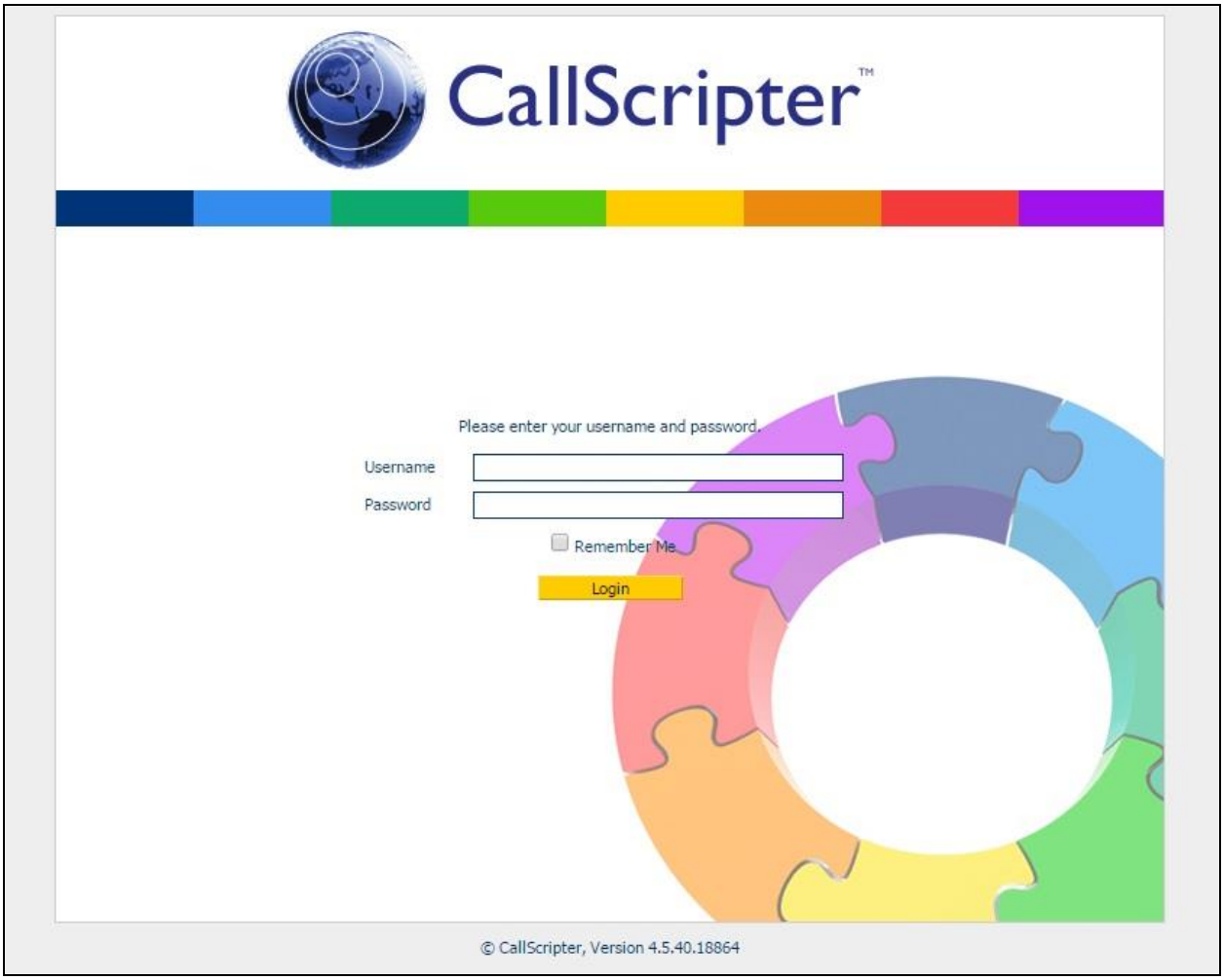
This section provides the procedures for configuring CallScripter. The procedures include the following areas:

- Launch web interface
- Administer AES provider
- Administer users
- Administer DDI

7.1. Launch Web Interface

Launch the web interface by using the URL "http://ip-address:7000" in an Internet Explorer browser window, where "ip-address" is the IP address of the CallScripter server.

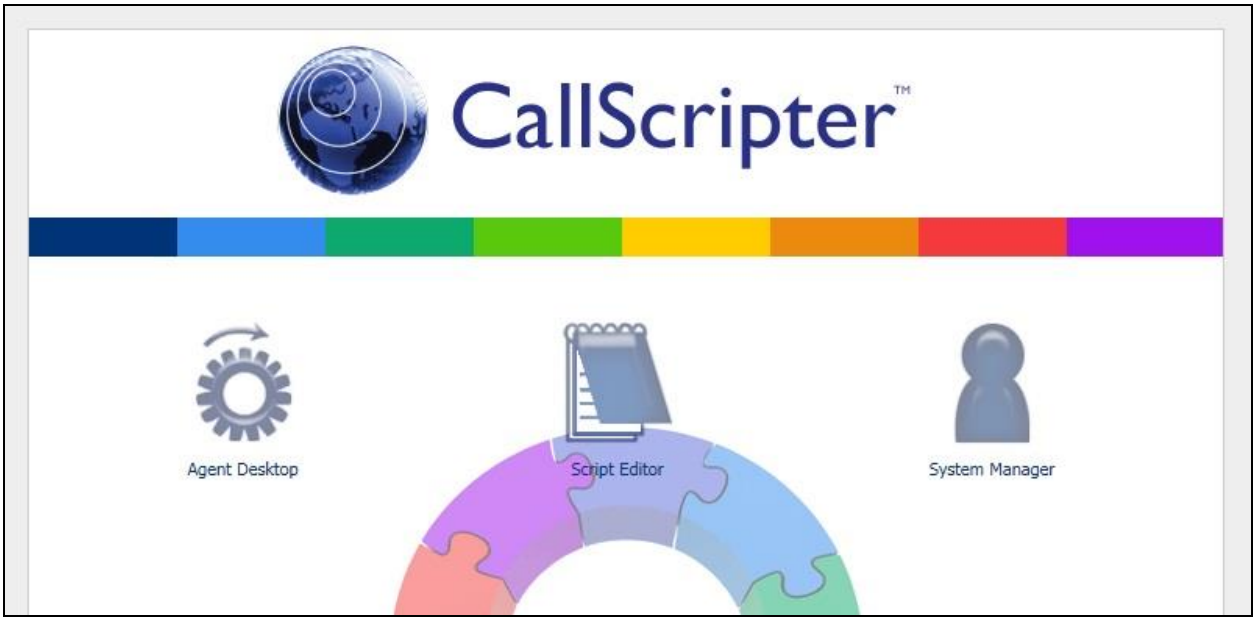
The **CallScripter** screen below is displayed. Log in using the appropriate credentials.



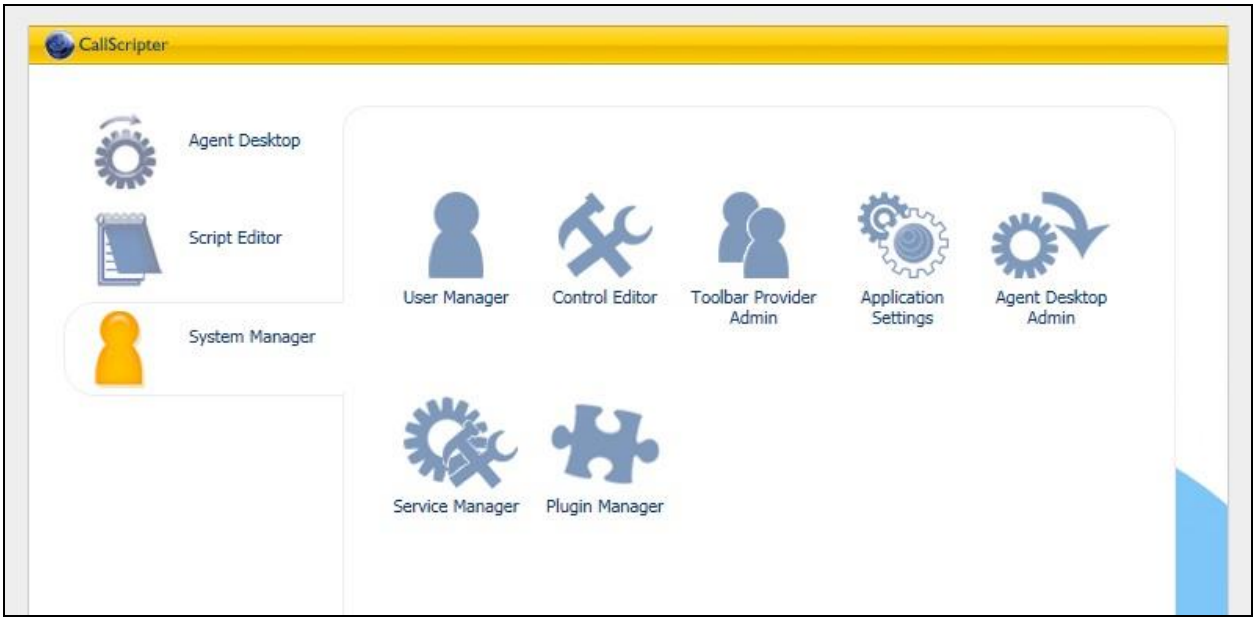
©2015 Avaya Inc. All Rights Reserved.

7.2. Administer AES Provider

The screen below is popped-up in a separate window. Select **System Manager**.



The screen below, which is referred to as the Splash Page, is displayed next. Select **Application Settings** in the right pane.



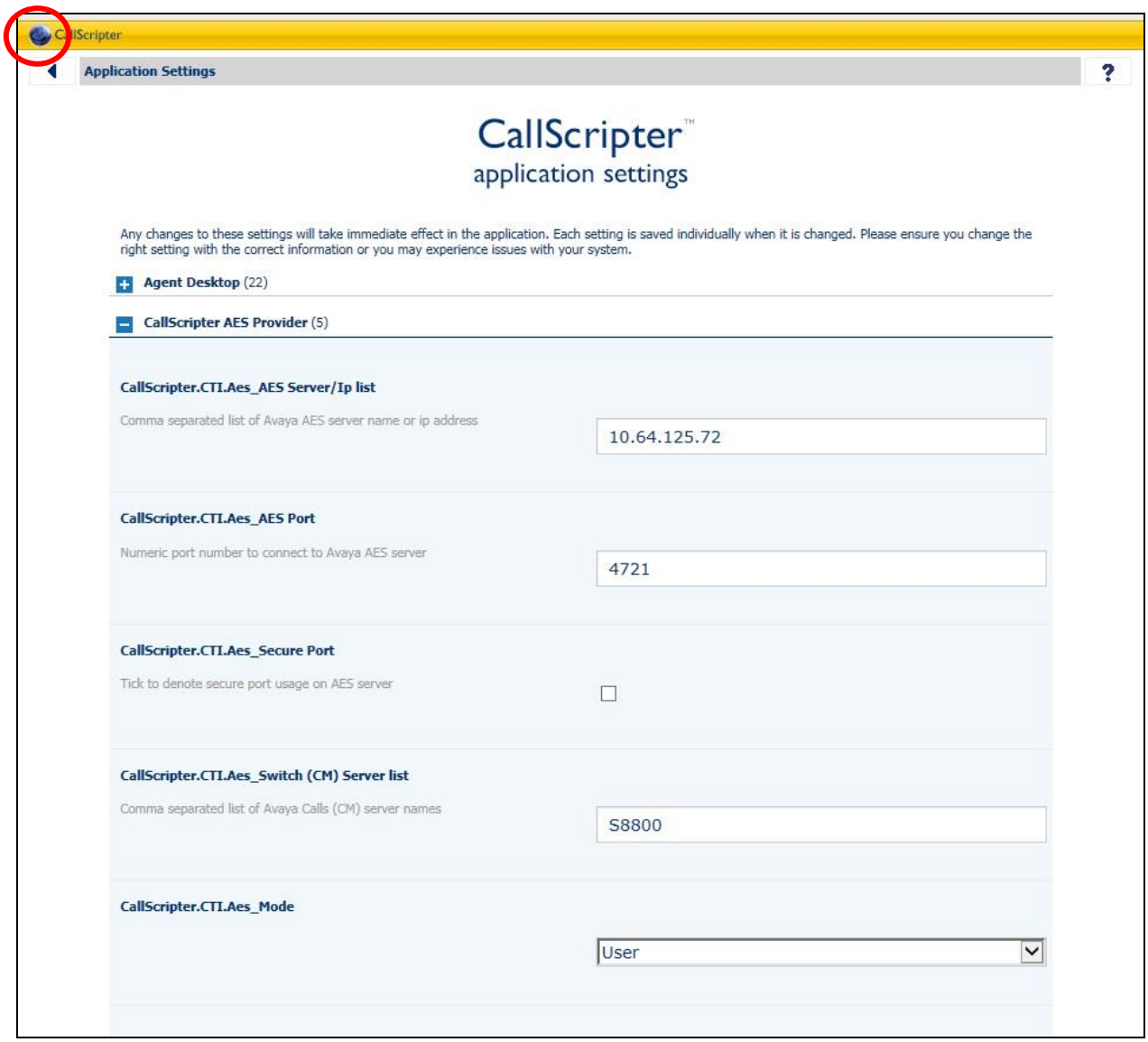
©2015 Avaya Inc. All Rights Reserved.

The screen below is displayed. Expand the **CallScripter AES Provider** sub-section.

For **CallScripter.CTI.Aes_AES Server/Ip list**, enter the IP address of Application Enablement Services.

For **CallScripter.CTI.Aes_Switch (CM) Server list**, enter the switch connection name from **Section 6.3**.

Retain the default values in the remaining fields. Click on the globe icon in the upper left corner of the screen to return the Splash Page.

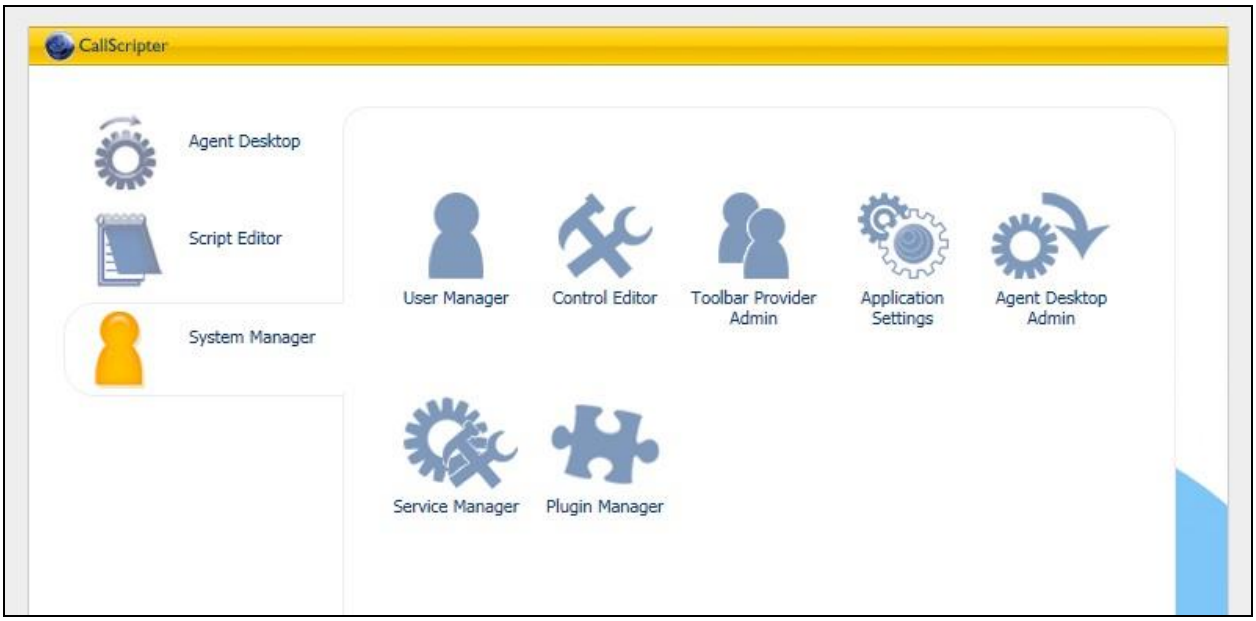


©2015 Avaya Inc. All Rights Reserved.

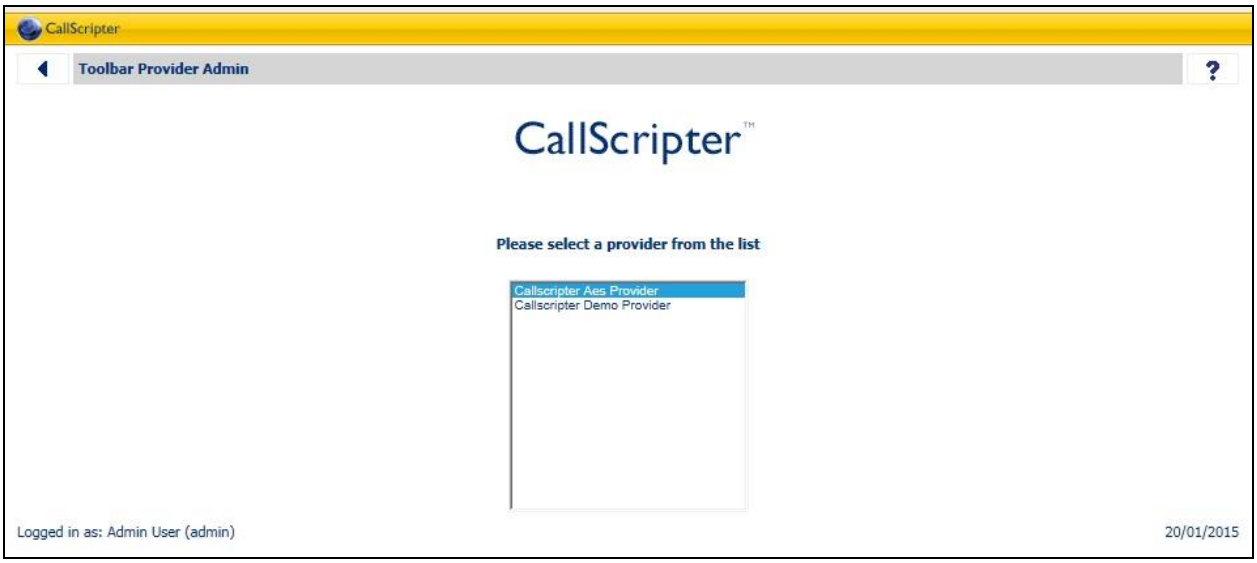
7.3. Administer Users

The Splash Page below is displayed next. Follow [3] to add a user for each agent from **Section 3**. In the compliance testing, two users with names "Agent 1" and "Agent 2" were pre-created.

Select **Toolbar Provider Admin** in the right pane.

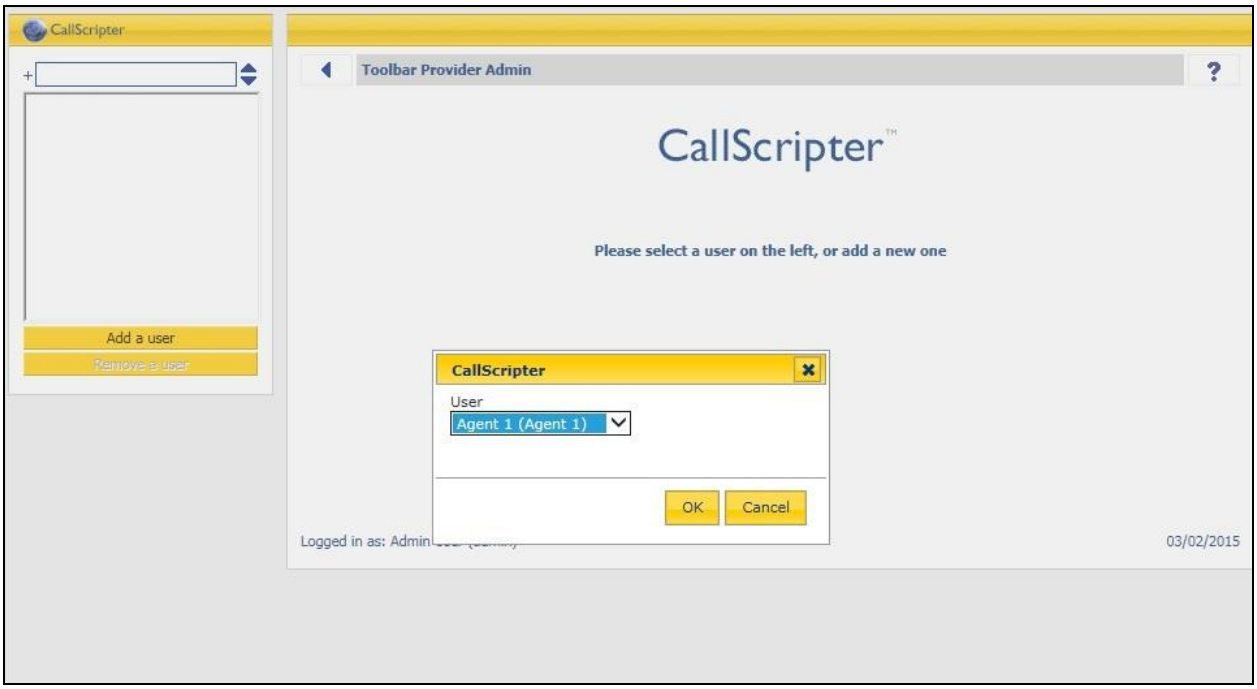


The screen below is displayed. Double click on the **Callscripter Aes Provider** entry.



©2015 Avaya Inc. All Rights Reserved.

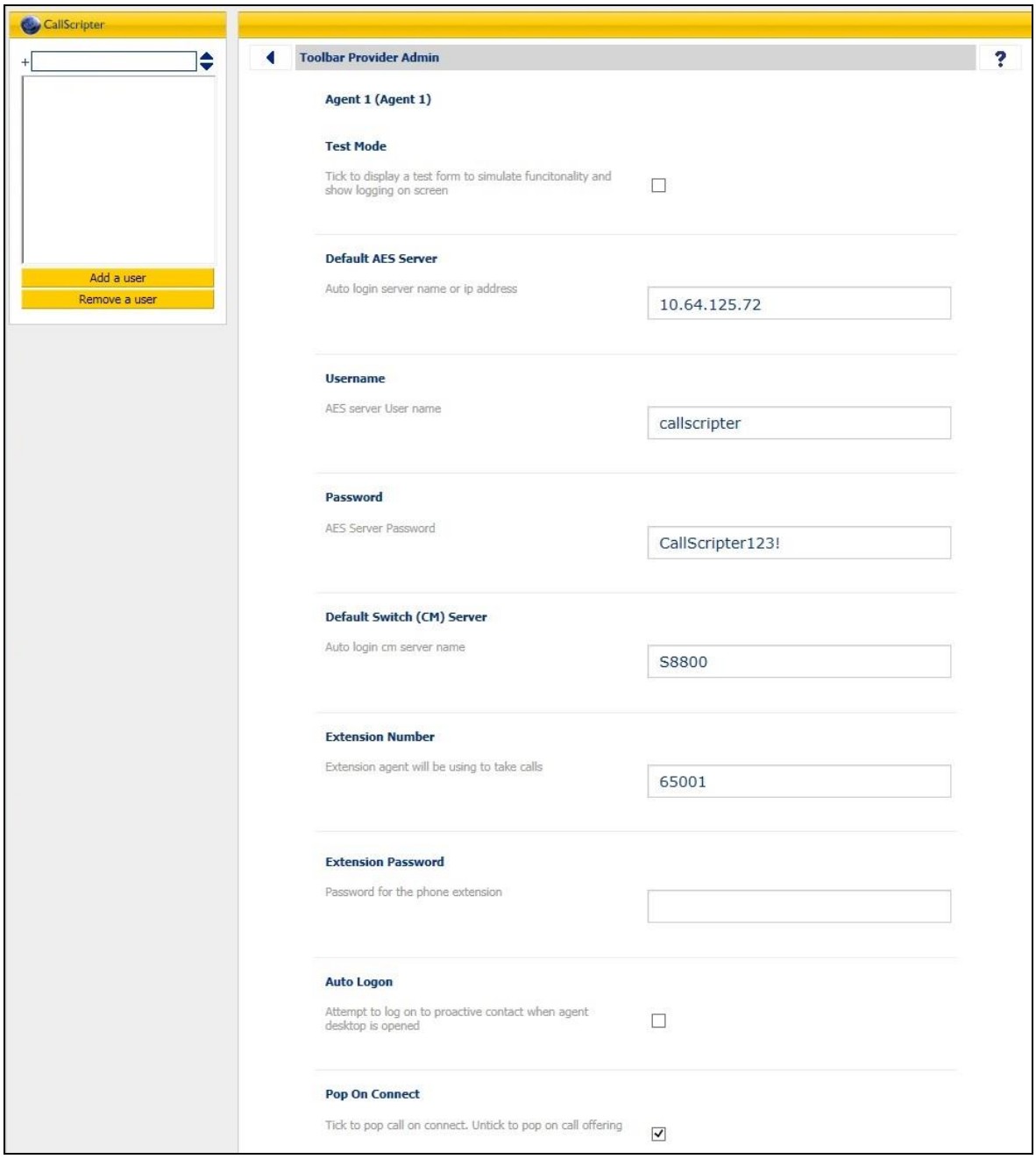
The screen below is displayed next. Select **Add a user** in the left pane, followed by the first newly created user name in the pop-up box, in this case "Agent 1".



©2015 Avaya Inc. All Rights Reserved.

The right pane is updated as shown below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Default AES Server:** The IP address of Application Enablement Services.
- **Username:** The CallScripter user credentials from **Section 6.6**.
- **Password:** The CallScripter user credentials from **Section 6.6**.
- **Default Switch (CM) Server:** The relevant switch connection name from **Section 6.3**.
- **Extension Number:** The default extension number to display for agent login.
- **Pop On Connect:** Check this field.



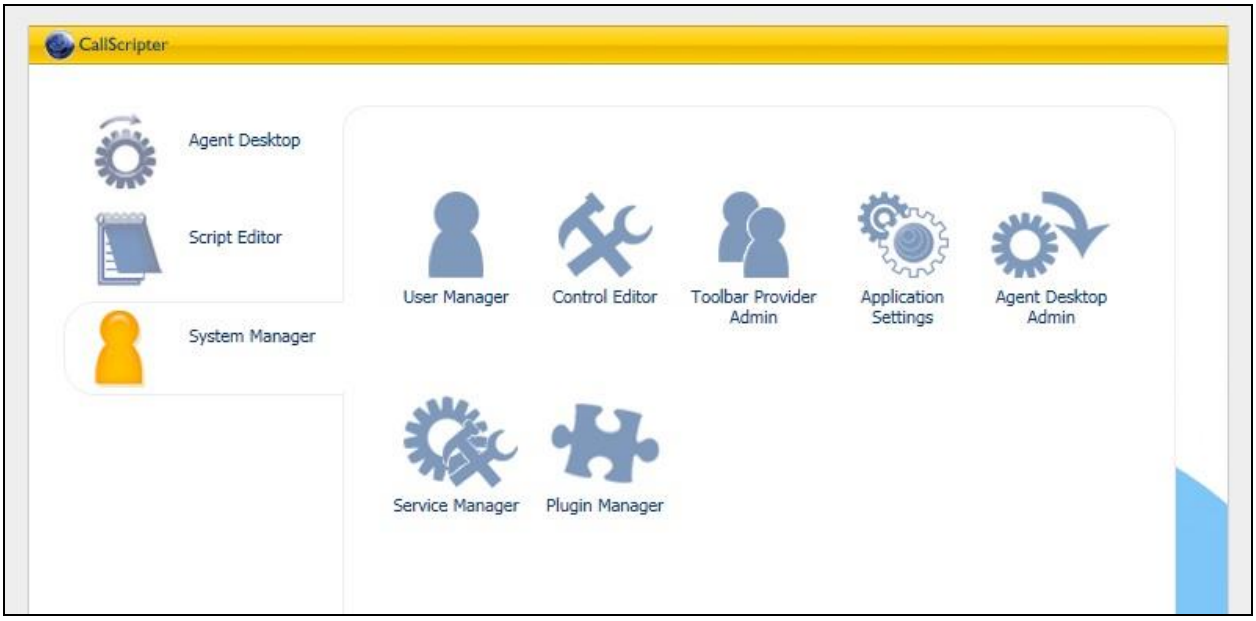
©2015 Avaya Inc. All Rights Reserved.

Repeat this section to add each newly created user to the AES provider. In the compliance testing, two users were configured, as shown below in the left pane.

Click on the globe icon in the upper left corner of the screen to return the Splash Page.

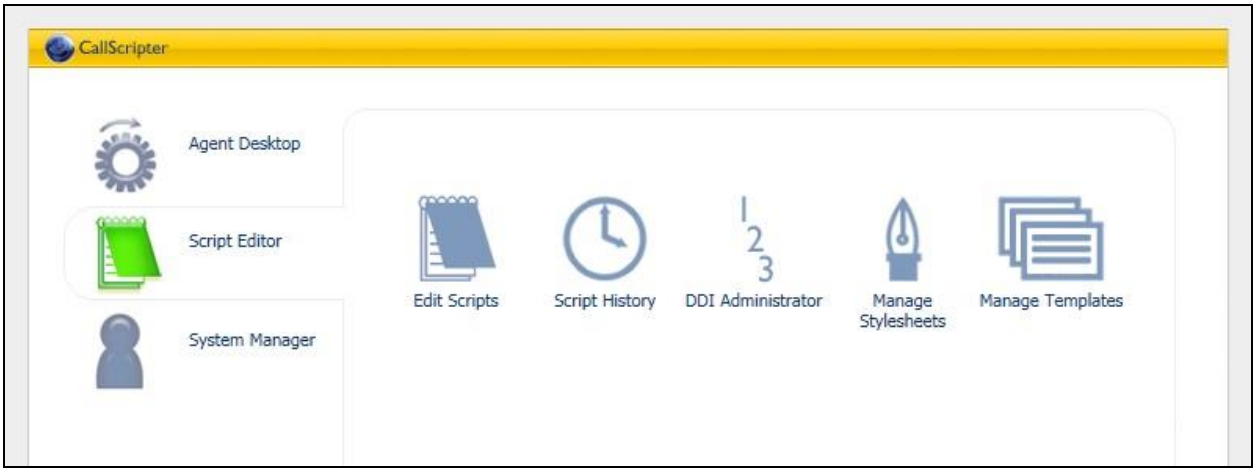
7.4. Administer DDI

The Splash Page below is displayed next. Select **Script Editor** in the left pane.



©2015 Avaya Inc. All Rights Reserved.

The screen below is displayed. Select **DDI Administrator** in the right pane.

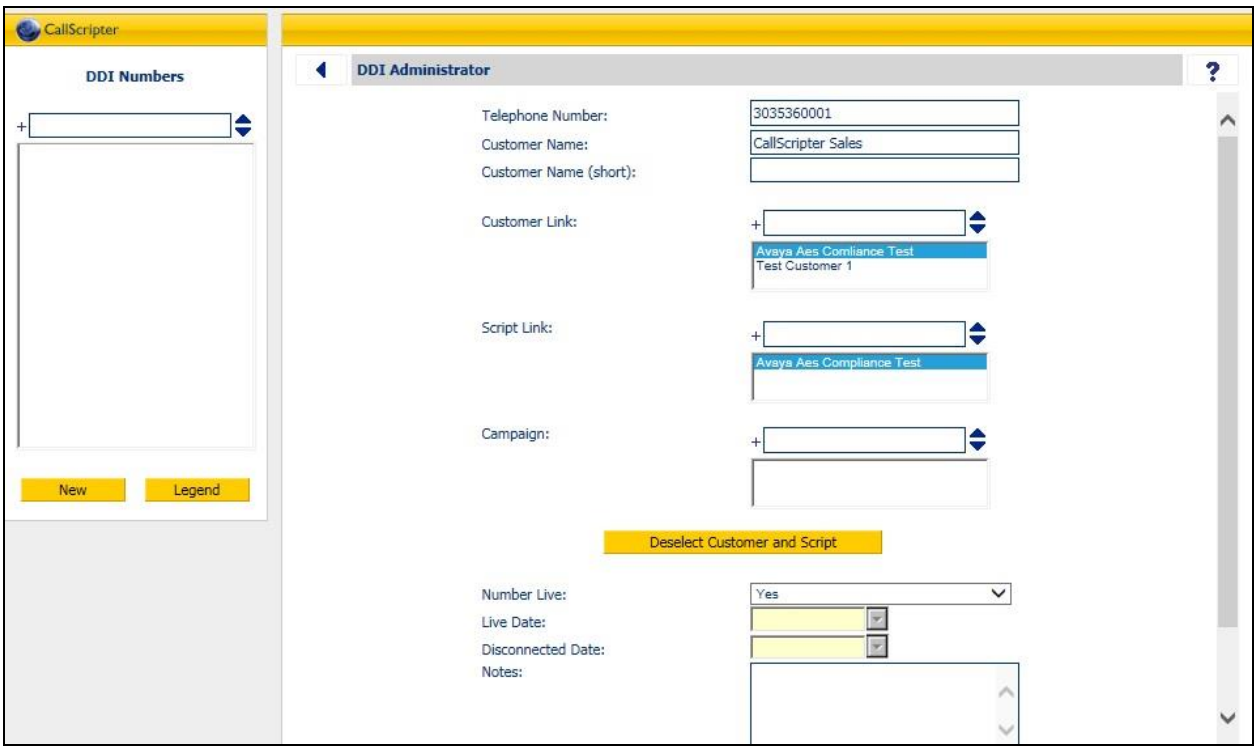


The screen below is displayed next. Select **New** in the left pane.

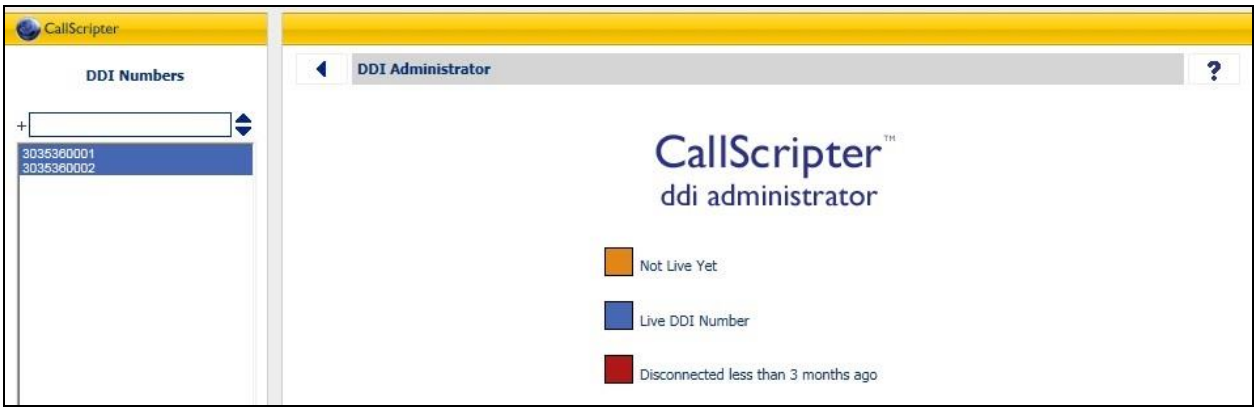
©2015 Avaya Inc. All Rights Reserved.

The right pane is updated as shown below. Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Telephone Number:** The DDI number associated with the first VDN from **Section 3**.
- **Customer Name:** The applicable VDN name from **Section 5.3**.
- **Customer Link:** Select the relevant pre-existing customer.
- **Script Link:** Select the relevant pre-existing script.



Repeat this section to add a DDI number for each VDN from **Section 3**. In the compliance testing, two DDI numbers were configured, as shown below in the left pane.



©2015 Avaya Inc. All Rights Reserved.

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

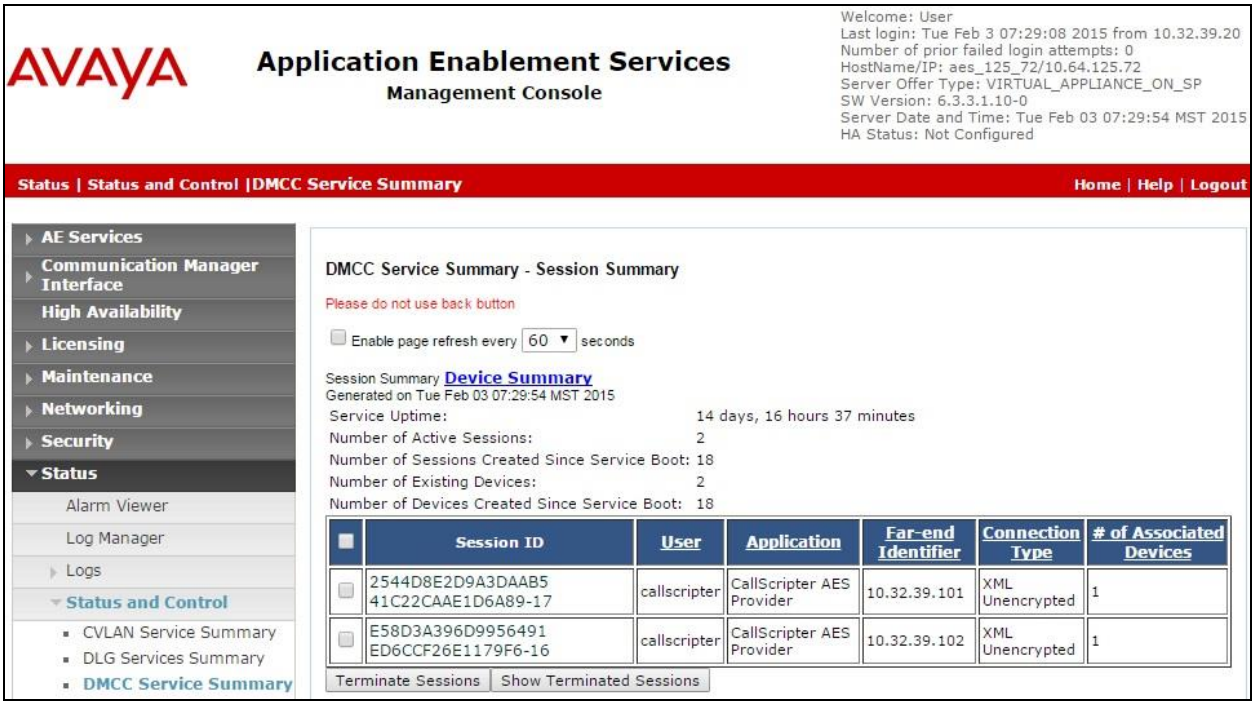
On Communication Manager, verify the status of the administered CTI link by using the "status aesvcs cti-link" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                         AE SERVICES CTI LINK STATUS

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

1               no                      down          0        0
2      6        no     aes_125_72       established   30       28
```

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

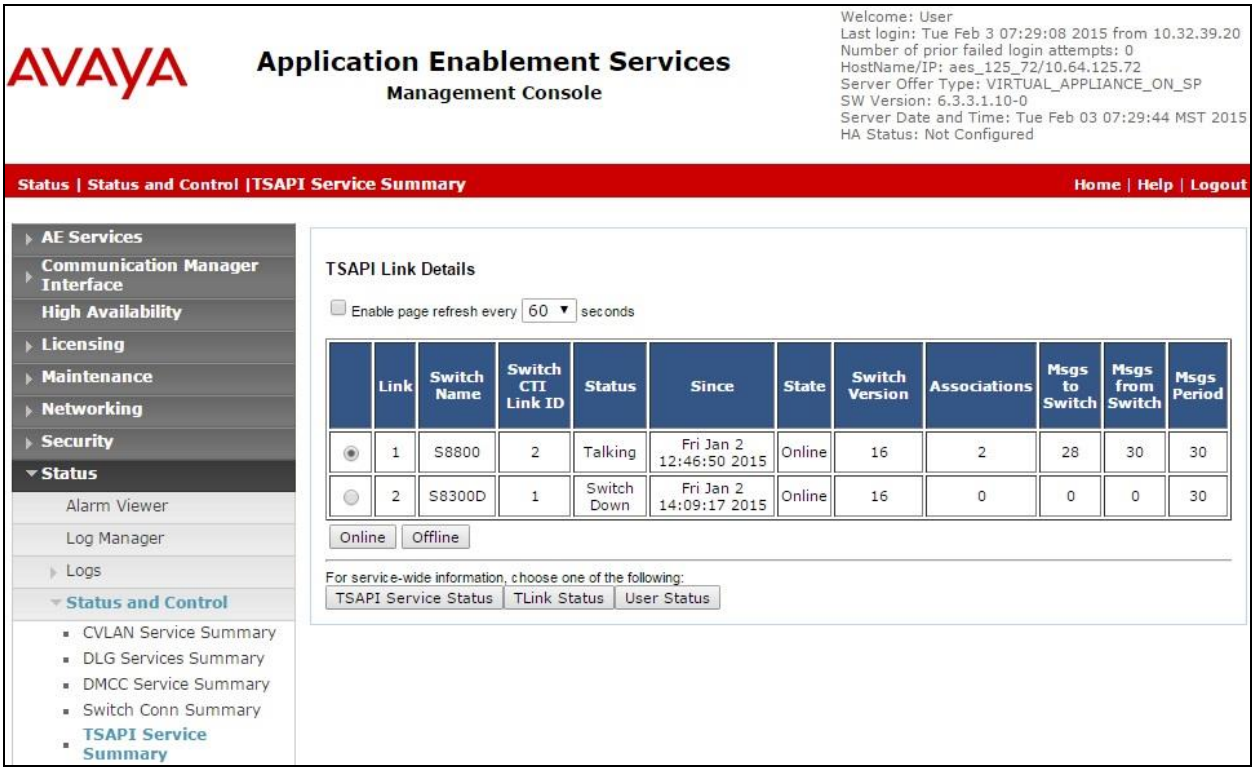
Verify that there is an active session with each agent logged into CallScripter, and that the **User** column shows the CallScripter user name from **Section 6.6**.



©2015 Avaya Inc. All Rights Reserved.

Verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

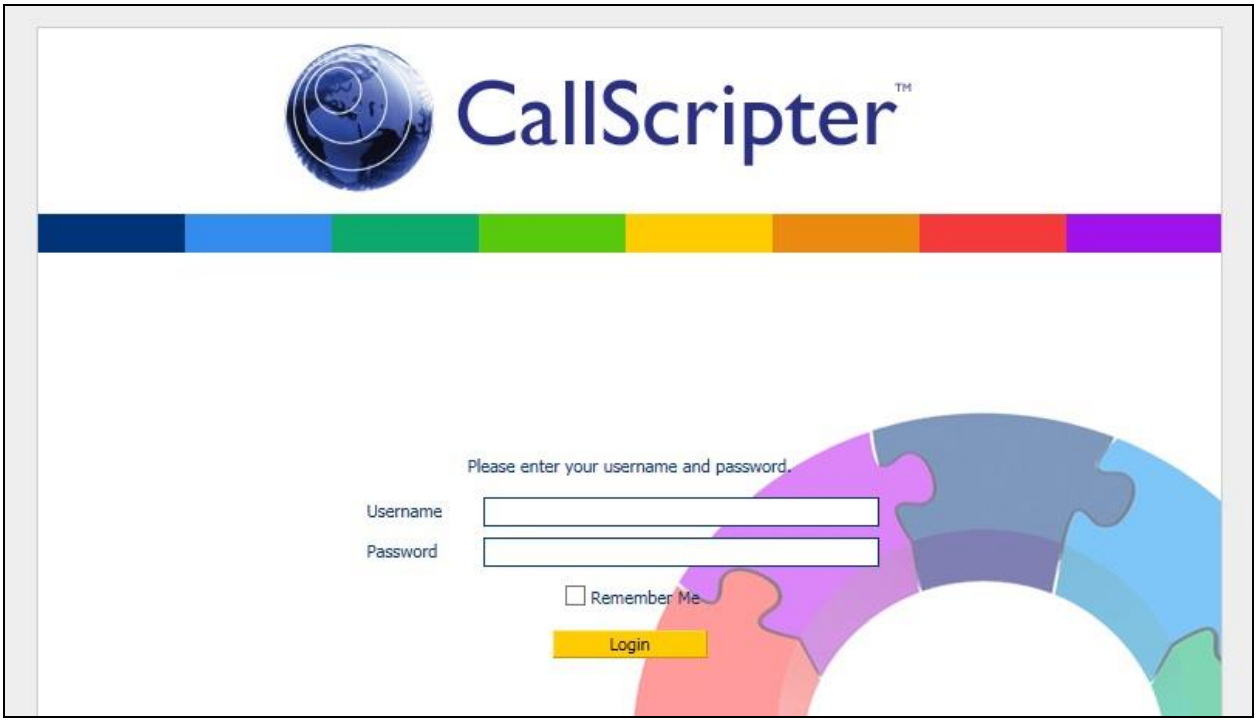
Verify the **Status** is "Talking" for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of agents from **Section 3** that are currently logged into CallScripter and therefore monitored, in this case "2".



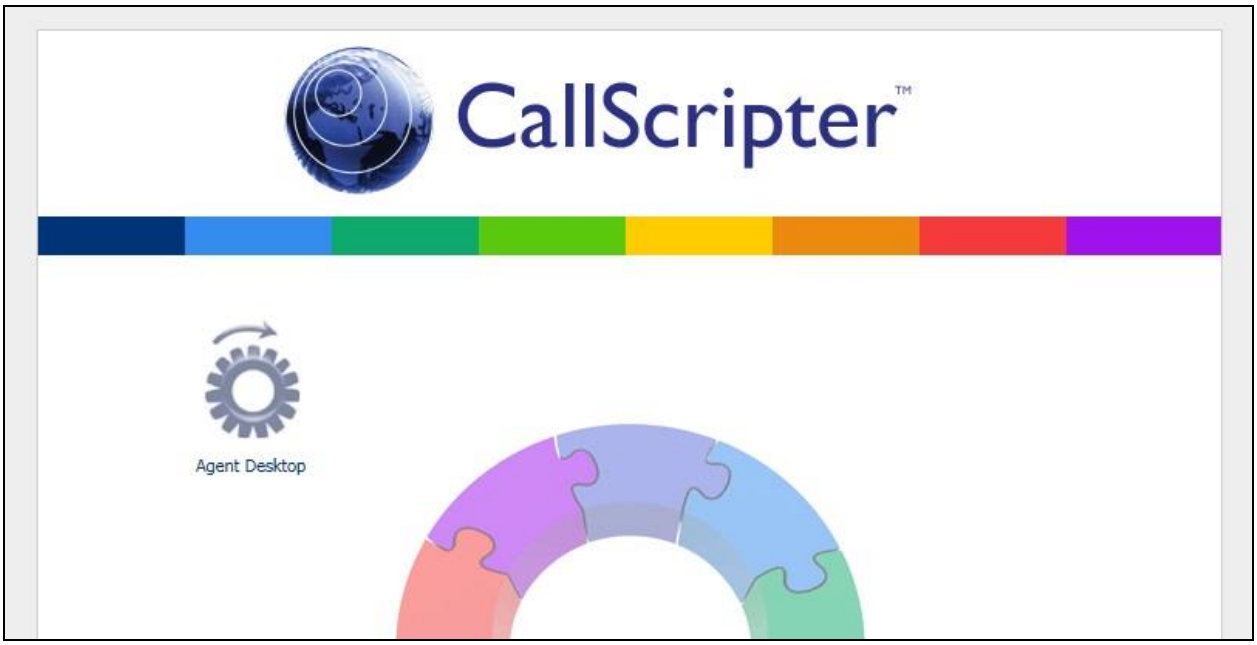
©2015 Avaya Inc. All Rights Reserved.

8.3. Verify CallScripter

From the agent PC, launch the web interface by using the URL “http://ip-address:7000” in an Internet Explorer browser window, where “ip-address” is the IP address of the CallScripter server. The **CallScripter** screen below is displayed. Log in using the appropriate credentials.



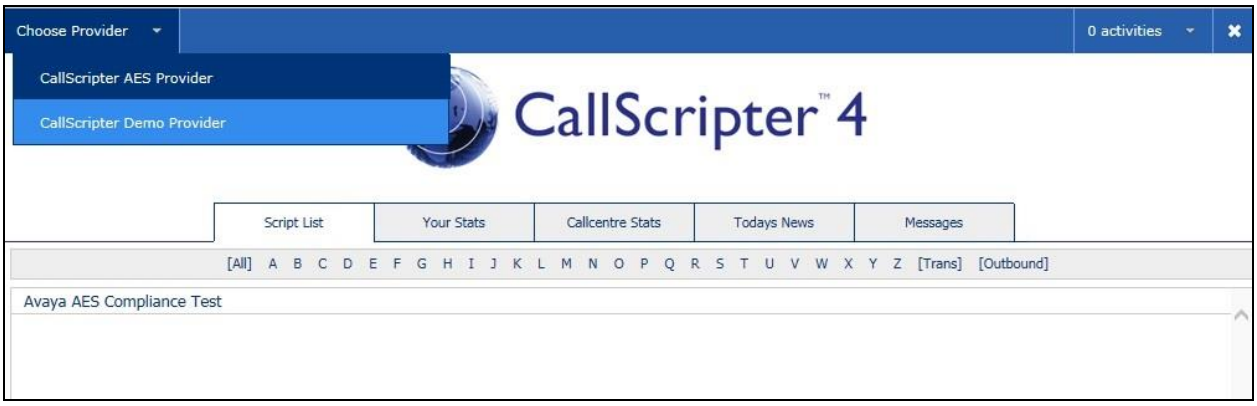
The screen below is displayed next. Select **Agent Desktop**.



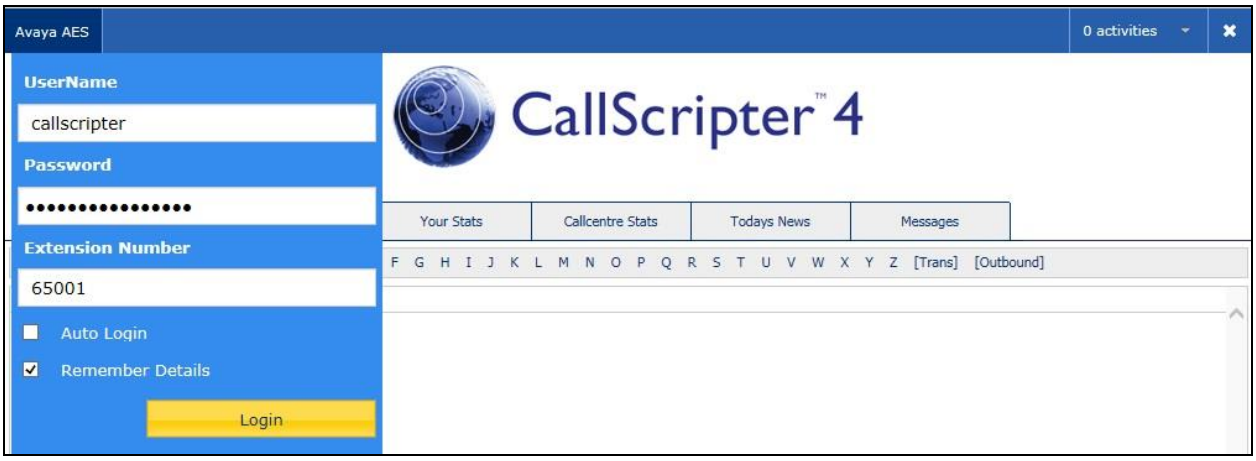
©2015 Avaya Inc. All Rights Reserved.

The screen below is displayed. Select **Agent Desktop** from the right pane.

The screen below is displayed next. For **Choose Provider** in the upper left corner, select **CallScripter AES Provider** from the drop-down list.

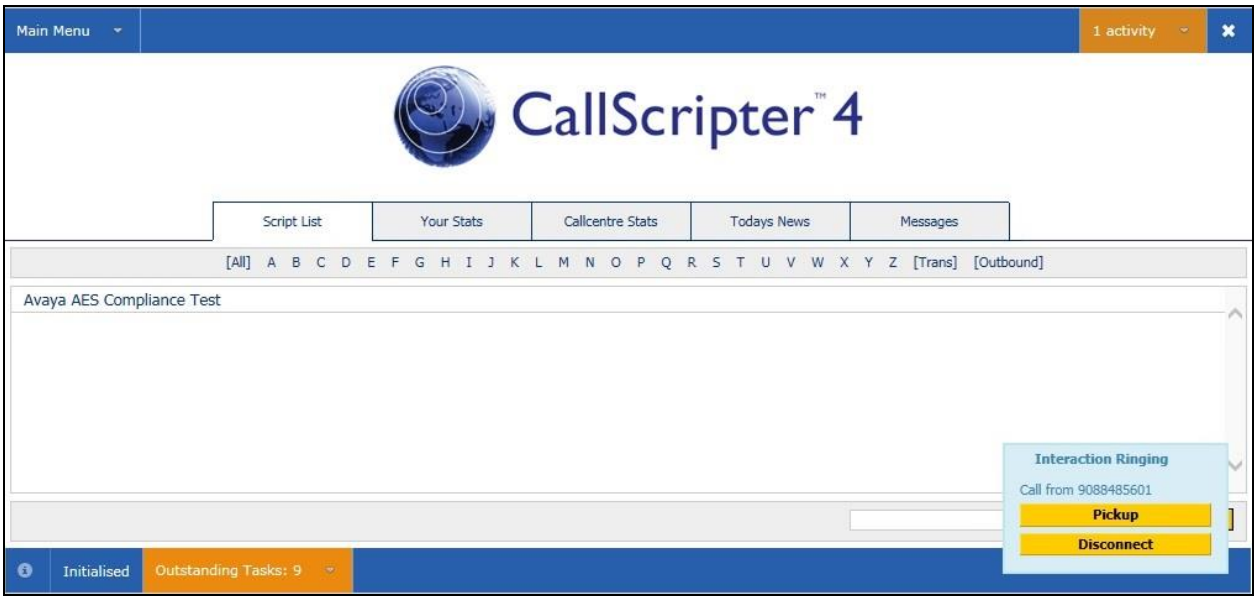


The screen is updated as shown below. For **Extension Number**, update as necessary with actual station extension the agent is using. Retain the default values in the remaining fields, and click **Login**.



©2015 Avaya Inc. All Rights Reserved.

Make an incoming ACD call. Verify that an **Interaction Ringing** pop-up box appears on an available agent, along with the calling party number, as shown below. Click **Pickup**.



Verify that the agent is connected to the PSTN caller with two-way talk paths, and that the screen is updated with retrieved customer information from the database along with the standard Communication Toolbar buttons, as shown below.

©2015 Avaya Inc. All Rights Reserved.

9. Conclusion

These Application Notes describe the configuration steps required for CallScripter to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 6.3, June 2014, available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 6.3, 02-300357, June 2014, available at http://support.avaya.com.

3. *CallScripter for Avaya AES Installation and Configuration Guide*, January 28, 2015, Version 1.1, available upon request to CallScripter Support.

©2015 Avaya Inc. All Rights Reserved.

©2015 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.