



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.

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.

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>

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

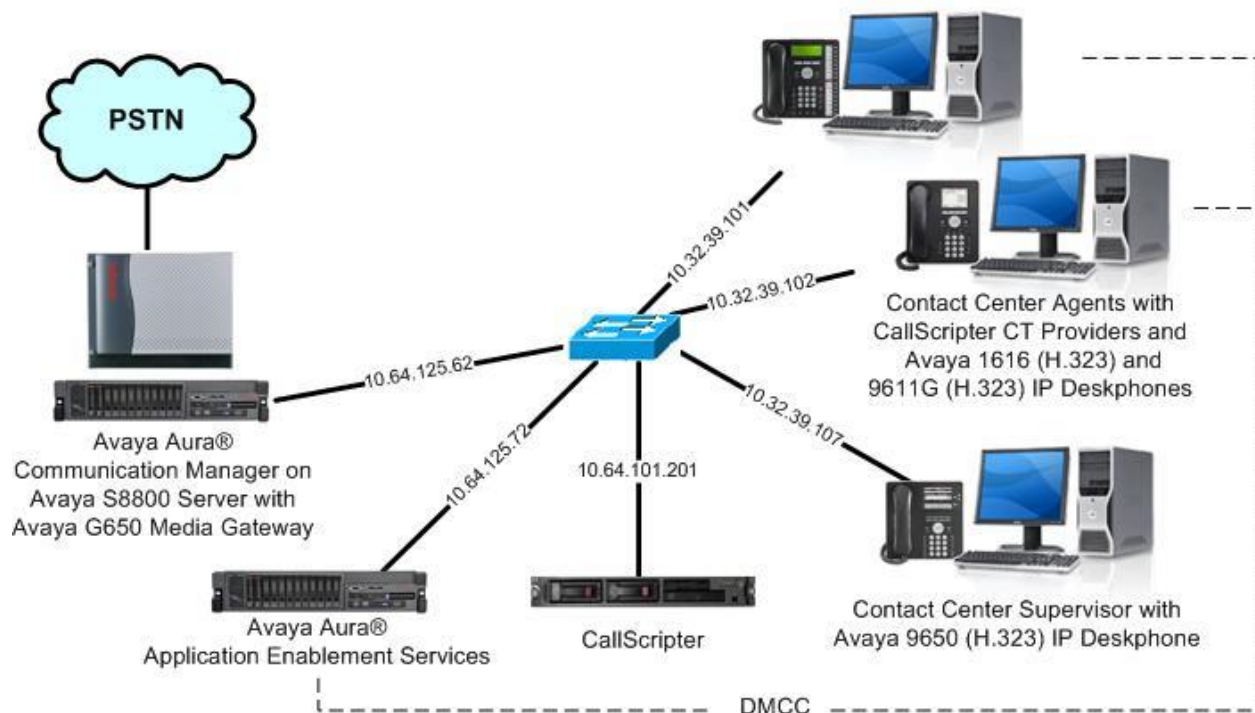


Figure 1: Compliance Testing Configuration

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 <ul style="list-style-type: none">• Avaya DMCC .NET	4.41.19801 6.2.0.29

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			

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											
Name (22 characters)	Ext/Skills	VDN			Vec		Orig		Evt		
		Ovr	COR	TN	PRT	Num	Meas	Annc	Noti	Adj	
CallScripter Sales	60001	n	1	1	V	1	none		1		
CallScripter Support	60002	n	1	1	V	2	none		1		

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.



The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in a large, bold font, with "Management Console" in a smaller font below it. A red horizontal bar spans the width of the page, with the word "Help" in white text on the right side. In the center of the page is a light gray rectangular box containing the text "Please login here:" followed by a label "Username" and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2014 Avaya Inc. All Rights Reserved." is displayed.

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area shows the "Welcome to OAM" screen, which provides an overview of the OAM web and lists administrative domains: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. It also mentions that these domains can be served by one administrator for all domains or a separate administrator for each domain.

Welcome: User
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Jan 20 06:57:01 MST 2015
HA Status: Not Configured

Home | Help | Logout

Home

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

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.

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area shows the "Licensing" screen, which provides instructions on how to set up and maintain the WebLM, import, set up, and maintain the license, and administer TSAPI Reserved Licenses or DMCC Reserved Licenses. It lists the following steps: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

Welcome: User
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Jan 20 06:57:01 MST 2015
HA Status: Not Configured

Home | Help | Logout

Licensing

AE Services
Communication Manager Interface
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking
Security

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:


- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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 CallScripser.


Web License Manager (WebLM v6.3)
Help | About | Change Password

WebLM Home
Install license
Licensed products
APPL_ENAB
▼ Application_Enablement
View license capacity
View peak usage
Uninstall license
Server properties
Manage users
Shortcuts
Help for Installed Product

Application Enablement (CTI) - Release: 6 - SID: 10503000
Standard License file

You are here: Licensed Products > Application_Enablement > View License Capacity
License installed on: May 11, 2012 7:07:47 PM -04:00

License File Host IDs: 00-16-3E-48-ED-82

Licensed Features

10 Items Show ALL

Feature (License Keyword)	Expiration date	Licensed capacity
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16
Product Notes VALUE_NOTES	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiS MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_ LargeServerTypes: isp2100;ibmx305;dl380g3;dl385g1;dl385g2;u TrustedApplications: IPS_001, BasicUnrestrict DMCUnrestricted; 1XP_001, BasicUnrestricted DMCUnrestricted; 1XM_001, BasicUnrestricted DMCUnrestricted; PC_001, BasicUnrestricted DMCUnrestricted; CIE_001, BasicUnrestricted DMCUnrestricted; OSPC_001, BasicUnrestrict DMCUnrestricted; VP_001, BasicUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,,, CCE_ AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; CSI AdvancedUnrestricted, DMCUnrestricted; AVA BasicUnrestricted, AdvancedUnrestricted, DMC CCT_ELITE_CALL_CTRL_001, BasicUnrestrict DMCUnrestricted, AgentEvents;
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
DLG VALUE_AES_DLG	permanent	16
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16

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 screenshot shows the Avaya Management Console interface. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The left navigation pane shows "AE Services" expanded, with "TSAPI" selected, and "TSAPI Links" highlighted. The main content area displays the "TSAPI Links" screen, which includes a table with columns: Link, Switch Connection, Switch CTI Link #, ASAI Link Version, and Security. Below the table are buttons for "Add Link", "Edit Link", and "Delete 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.

The screenshot shows the "Add TSAPI Links" screen in the Avaya Management Console. The left navigation pane is the same as the previous screenshot. The main content area displays the "Add TSAPI Links" form, which includes fields for Link, Switch Connection, Switch CTI Link Number, ASAI Link Version, and Security. The values entered are: Link: 1, Switch Connection: S8800, Switch CTI Link Number: 2, ASAI Link Version: 6, and Security: Unencrypted. Below the fields are buttons for "Apply Changes" and "Cancel Changes".

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for the user. The main navigation bar shows "Security | Security Database | Control" as the active path, with links for "Home | Help | Logout". The left sidebar contains a tree view of system components, with "Security" expanded and "Control" selected under "Security Database". The main content area is titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below the checkboxes.

Welcome: User
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Jan 20 06:57:01 MST 2015
HA Status: Not Configured

Security | Security Database | Control Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Account Management
Audit
Certificate Management
Enterprise Directory
Host AA
PAM
Security Database
Control

SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
Apply Changes

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**.



Application Enablement Services
Management Console

Welcome: User
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Jan 20 06:57:01 MST 2015
HA Status: Not Configured

Maintenance | Service Controller

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

▶ User Management

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

Start

Stop

Restart Service

Restart AE Server


Restart Linux

Restart Web Server

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.

**Application Enablement Services**
Management Console

Welcome: User
Last login: Tue Jan 20 06:55:46 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Jan 20 07:54:23 MST 2015
HA Status: Not Configured

User Management | User Admin | Add UserHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

■ Add User

■ Change User Password

■ List All Users

■ Modify Default Users

■ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

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.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Tue Jan 20 06:55:31 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Jan 20 06:57:01 MST 2015
HA Status: Not Configured

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▼ Networking

▶ AE Service IP (Local IP)

▶ Network Configure

▶ Ports

▶ TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999

Enabled Disabled

Encrypted TCP Port9998

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721

Enabled Disabled

Encrypted Port4722

TR/87 Port4723

7. Configure CallScripter

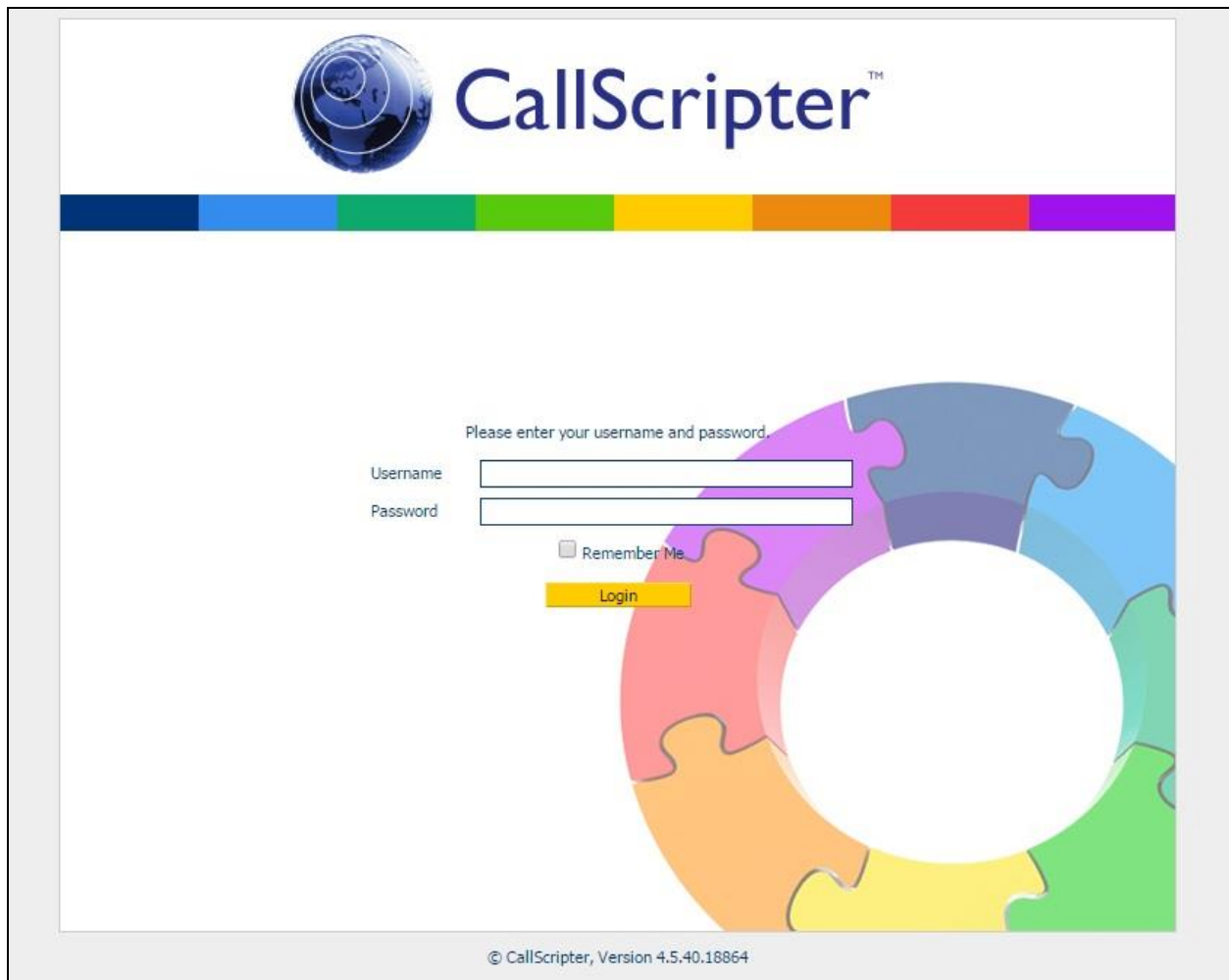
This section provides the procedures for configuring CallScripter. The procedures include the following areas:

- 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.

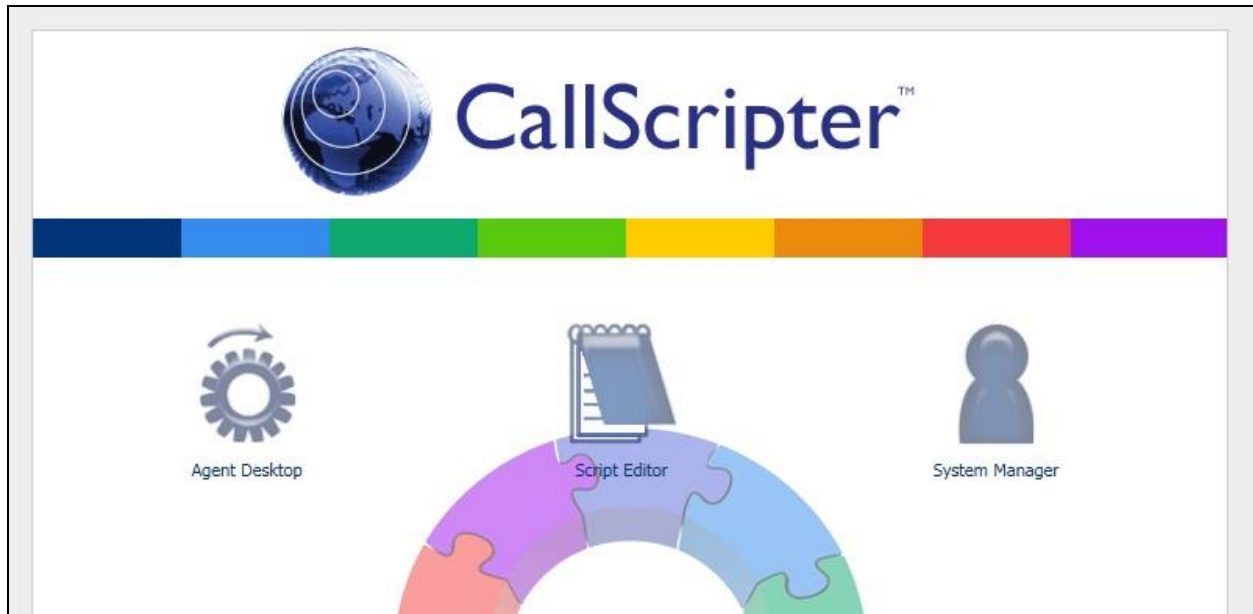
The **CallScripter** screen below is displayed. Log in using the appropriate credentials.



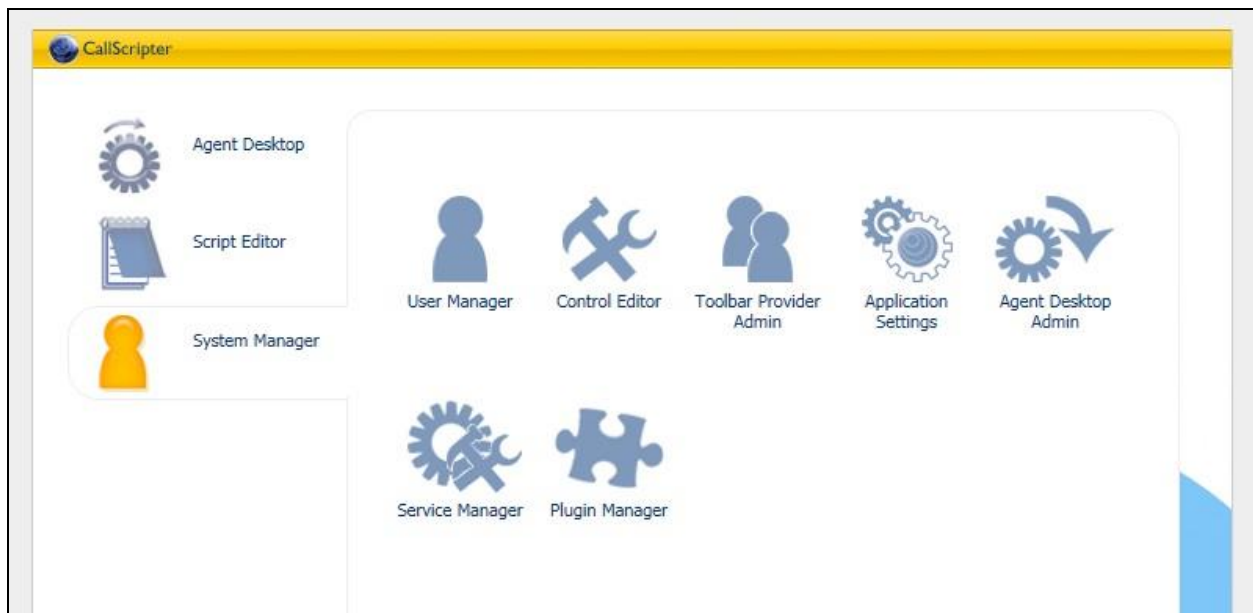
The image shows the CallScripter web interface login screen. At the top, there is a logo consisting of a blue globe with white lines, followed by the text "CallScripter™". Below the logo is a horizontal bar with eight colored segments: dark blue, light blue, green, yellow, orange, red, and purple. The main content area features a login form with the text "Please enter your username and password." above two input fields labeled "Username" and "Password". Below the password field is a checkbox labeled "Remember Me" and a yellow "Login" button. To the right of the login form is a large graphic of a circular arrangement of colorful puzzle pieces. At the bottom of the screen, there is a copyright notice: "© CallScripter, Version 4.5.40.18864".

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.

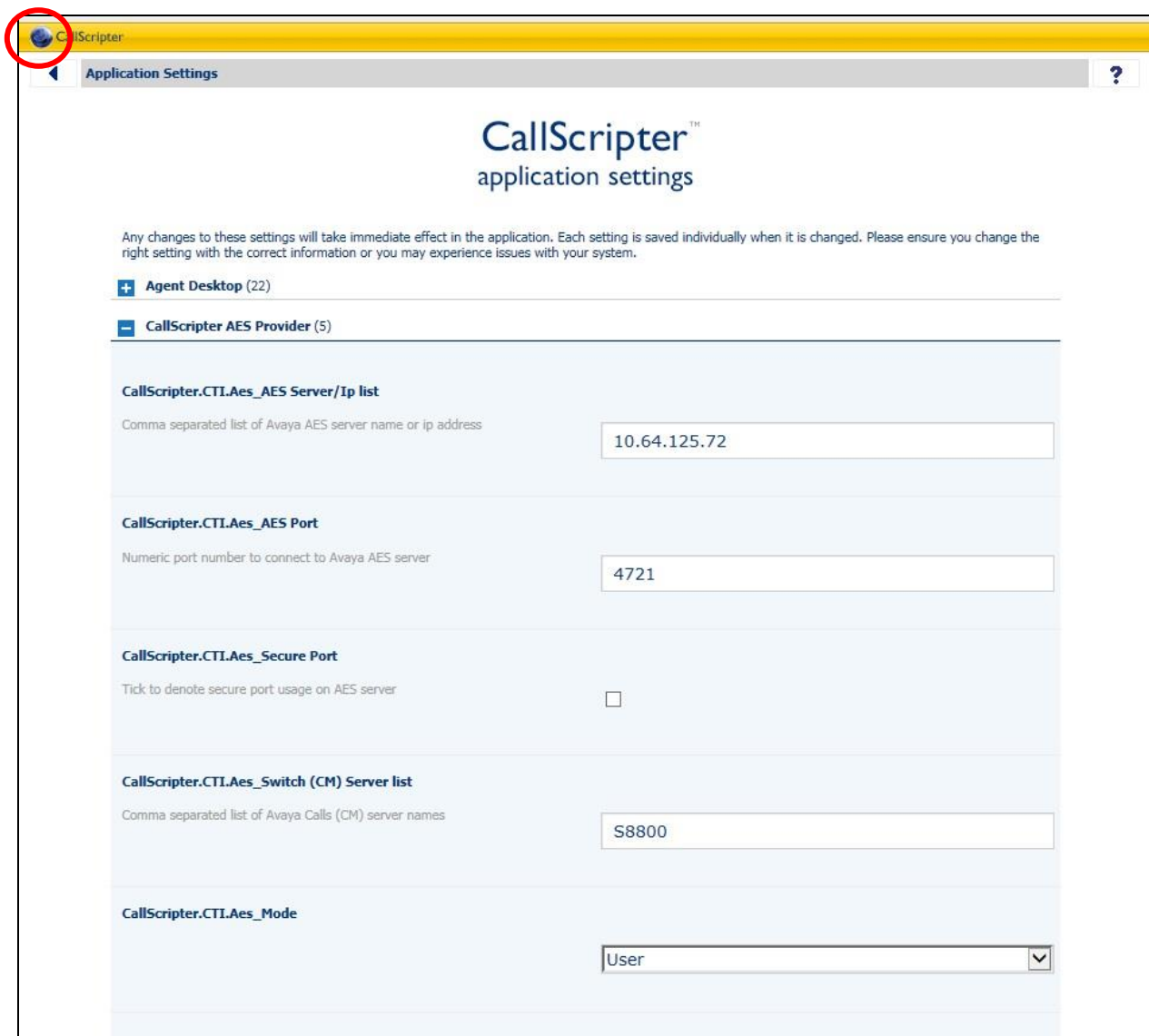


The screen below is displayed. Expand the **CallScripter AES Provider** sub-section.

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.



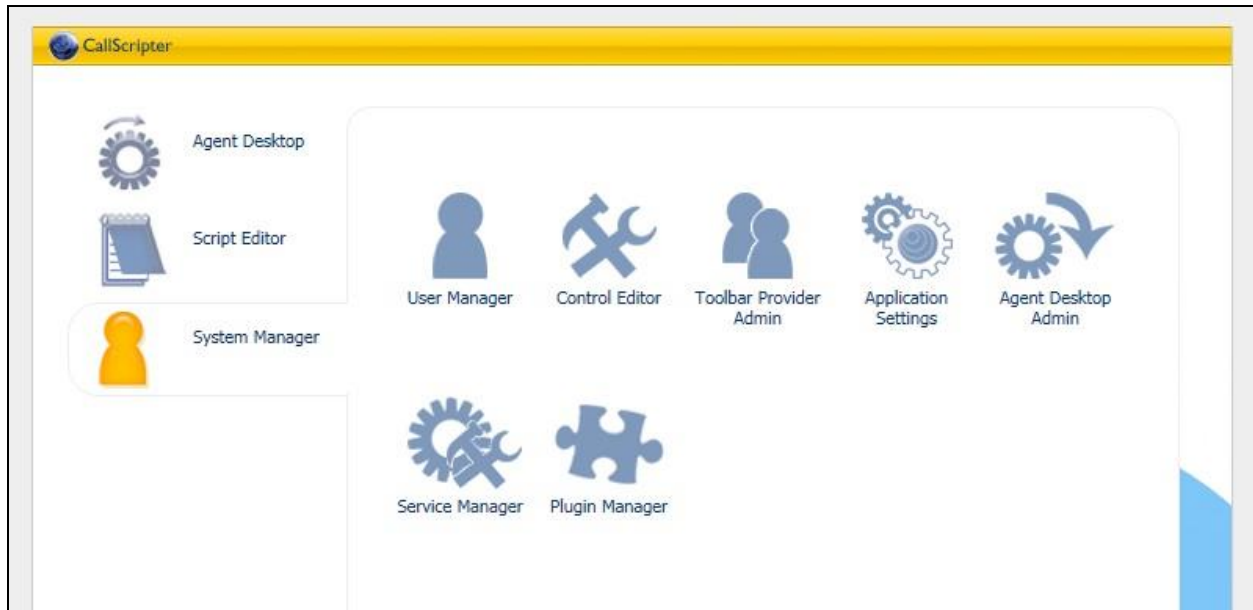
The screenshot shows the 'CallScripter application settings' interface. At the top, there is a yellow header bar with the 'CallScripter' logo and a globe icon circled in red. Below the header is a navigation bar with 'Application Settings' and a help icon. The main content area displays the 'CallScripter AES Provider' section, which is expanded to show five configuration items:

- CallScripter.CTI.Aes_AES Server/Ip list**: A text field containing '10.64.125.72'. The description below it reads: 'Comma separated list of Avaya AES server name or ip address'.
- CallScripter.CTI.Aes_AES Port**: A text field containing '4721'. The description below it reads: 'Numeric port number to connect to Avaya AES server'.
- CallScripter.CTI.Aes_Secure Port**: A checkbox that is currently unchecked. The description below it reads: 'Tick to denote secure port usage on AES server'.
- CallScripter.CTI.Aes_Switch (CM) Server list**: A text field containing 'S8800'. The description below it reads: 'Comma separated list of Avaya Calls (CM) server names'.
- CallScripter.CTI.Aes_Mode**: A dropdown menu with 'User' selected.

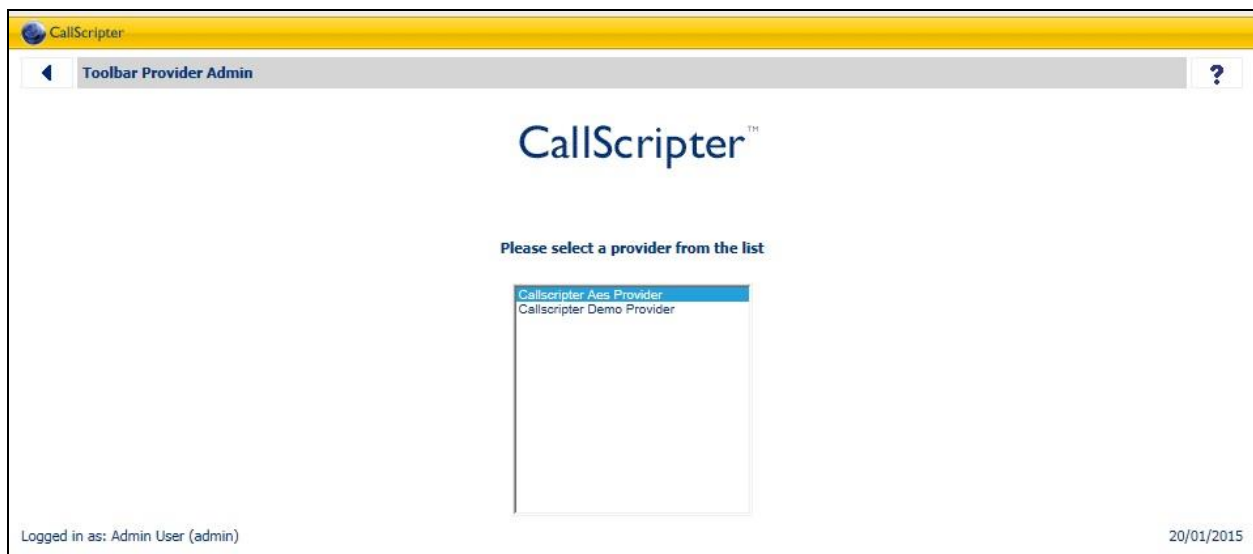
7.3. Administer Users

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.

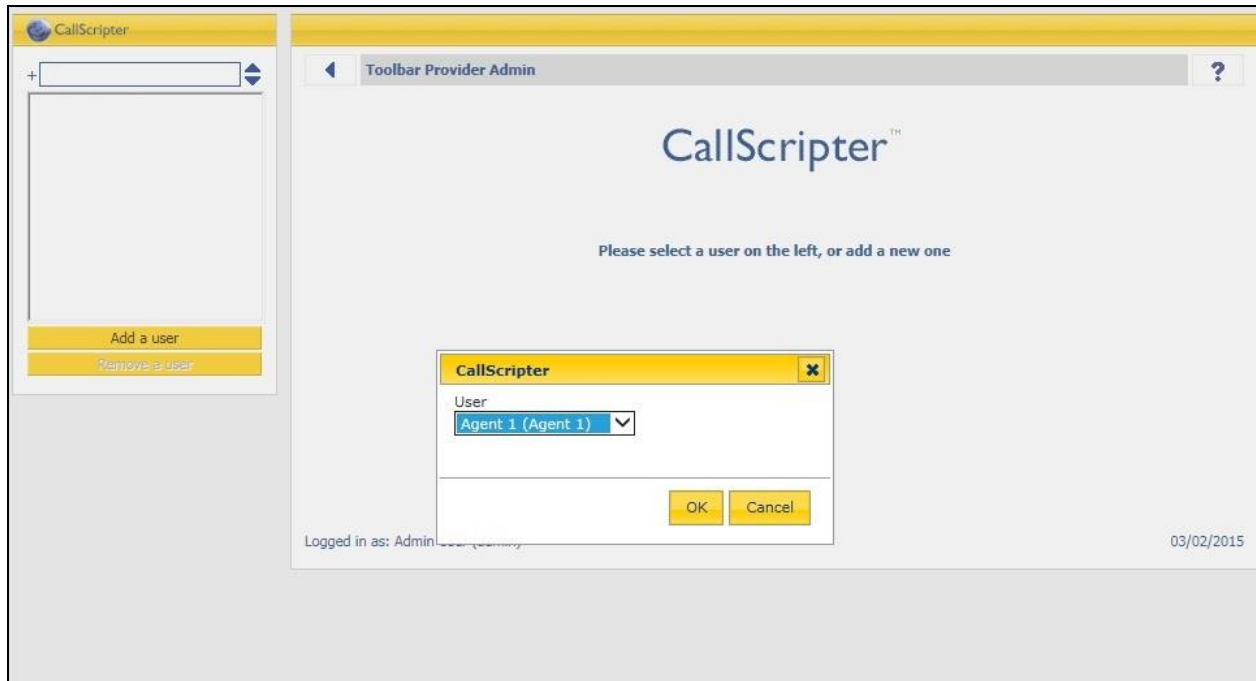
Select **Toolbar Provider Admin** in the right pane.



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



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”.



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.

The screenshot displays the 'CallScripter' application window with a sidebar on the left and a main configuration area on the right. The sidebar contains a search bar, a list of users, and buttons for 'Add a user' and 'Remove a user'. The main area is titled 'Toolbar Provider Admin' and shows configuration for 'Agent 1 (Agent 1)'. The configuration includes sections for 'Test Mode', 'Default AES Server', 'Username', 'Password', 'Default Switch (CM) Server', 'Extension Number', 'Extension Password', 'Auto Logon', and 'Pop On Connect'. Each section has a label, a description, and a corresponding input field or checkbox.

Field	Value
Test Mode	<input type="checkbox"/>
Default AES Server	10.64.125.72
Username	callscrip
Password	CallScripter123!
Default Switch (CM) Server	S8800
Extension Number	65001
Extension Password	
Auto Logon	<input type="checkbox"/>
Pop On Connect	<input checked="" type="checkbox"/>

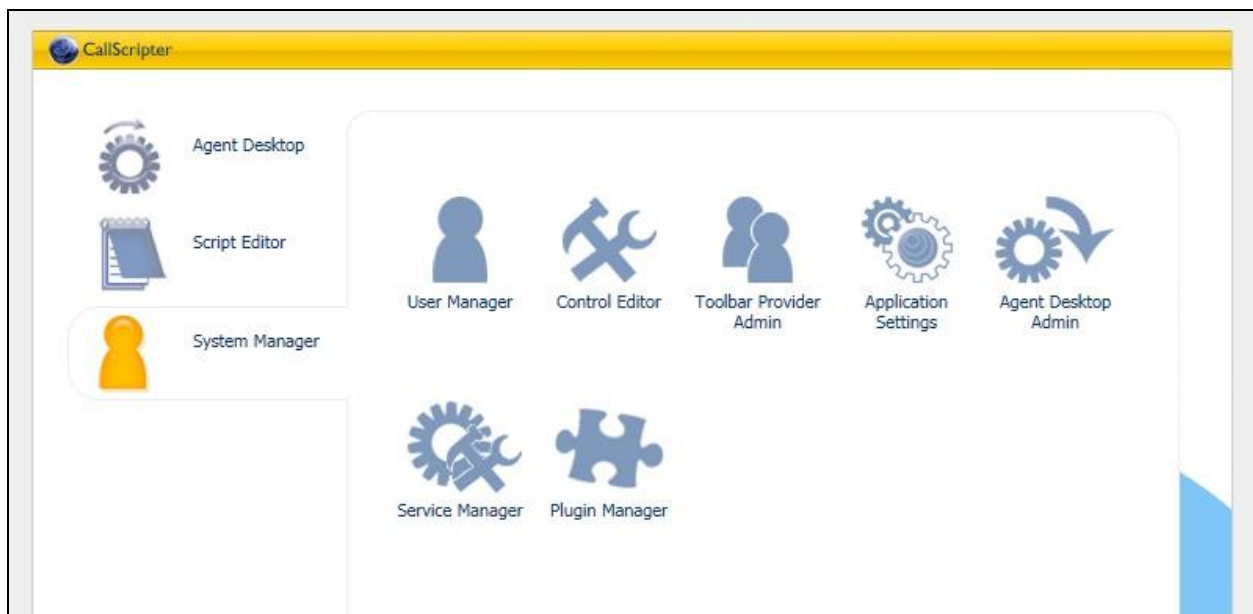
Repeat this section to add each newly created user to the AES provider. In the compliance testing, two users were configured, as shown below in the left pane.

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

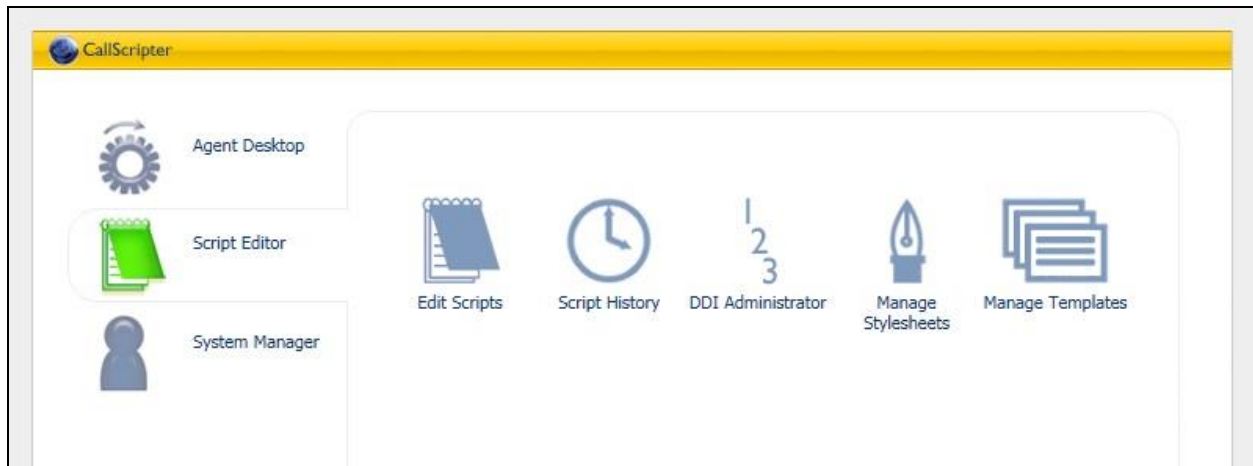


7.4. Administer DDI

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



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



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



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.

The screenshot shows the 'CallScripter' application window with the 'DDI Administrator' tab selected. The left pane, titled 'DDI Numbers', contains a list box with a '+' button and a 'New' button. The main pane contains the following fields:

- Telephone Number: 3035360001
- Customer Name: CallScripter Sales
- Customer Name (short):
- Customer Link: A dropdown menu showing 'Avaya Aes Compliance Test' and 'Test Customer 1'.
- Script Link: A dropdown menu showing 'Avaya Aes Compliance Test'.
- Campaign: A dropdown menu.
- Number Live: Yes (selected in a dropdown)
- Live Date: A date picker.
- Disconnected Date: A date picker.
- Notes: A text area.

A yellow button labeled 'Deselect Customer and Script' is located below the main form fields.

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.

The screenshot shows the 'CallScripter' application window with the 'DDI Administrator' tab selected. The left pane, titled 'DDI Numbers', contains a list box with a '+' button and two DDI numbers: 3035360001 and 3035360002. The main pane displays the 'CallScripter ddi administrator' logo and a legend:

- Not Live Yet (orange square)
- Live DDI Number (blue square)
- Disconnected less than 3 months ago (red square)

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 Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs 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**.



Application Enablement Services
Management Console

Welcome: User
Last login: Tue Feb 3 07:29:08 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Feb 03 07:29:54 MST 2015
HA Status: Not Configured

Status | Status and Control | DMCC Service SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

Log Manager

▶ Logs

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ DMCC Service Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Tue Feb 03 07:29:54 MST 2015

Service Uptime: 14 days, 16 hours 37 minutes

Number of Active Sessions: 2

Number of Sessions Created Since Service Boot: 18

Number of Existing Devices: 2


Number of Devices Created Since Service Boot: 18

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	2544D8E2D9A3DAAB5 41C22CAAE1D6A89-17	callscripter	CallScripter AES Provider	10.32.39.101	XML Unencrypted	1
<input type="checkbox"/>	E58D3A396D9956491 ED6CCF26E1179F6-16	callscripter	CallScripter AES Provider	10.32.39.102	XML Unencrypted	1

Terminate Sessions Show Terminated Sessions

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”.



Application Enablement Services
Management Console

Welcome: User
Last login: Tue Feb 3 07:29:08 2015 from 10.32.39.20
Number of prior failed login attempts: 0
HostName/IP: aes_125_72/10.64.125.72
Server Offer Type: VIRTUAL_APPLIANCE_ON_SP
SW Version: 6.3.3.1.10-0
Server Date and Time: Tue Feb 03 07:29:44 MST 2015
HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary
Home | Help | Logout

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status

Alarm Viewer
Log Manager
Logs
Status and Control
CVLAN Service Summary
DLG Services Summary
DMCC Service Summary
Switch Conn Summary
TSAPI Service Summary

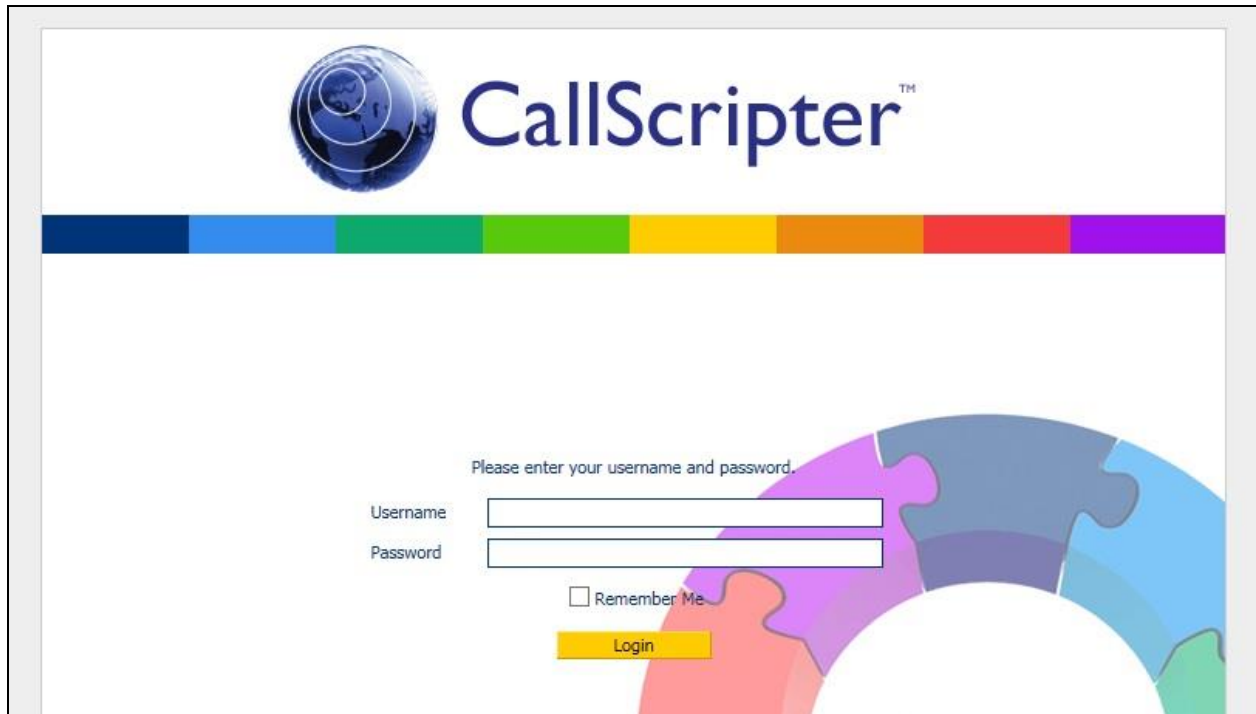
TSAPI Link Details
☐ Enable page refresh every 60 seconds

	Link	Switch Name	Switch CUI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	S8800	2	Talking	Fri Jan 2 12:46:50 2015	Online	16	2	28	30	30
<input type="radio"/>	2	S8300D	1	Switch Down	Fri Jan 2 14:09:17 2015	Online	16	0	0	0	30

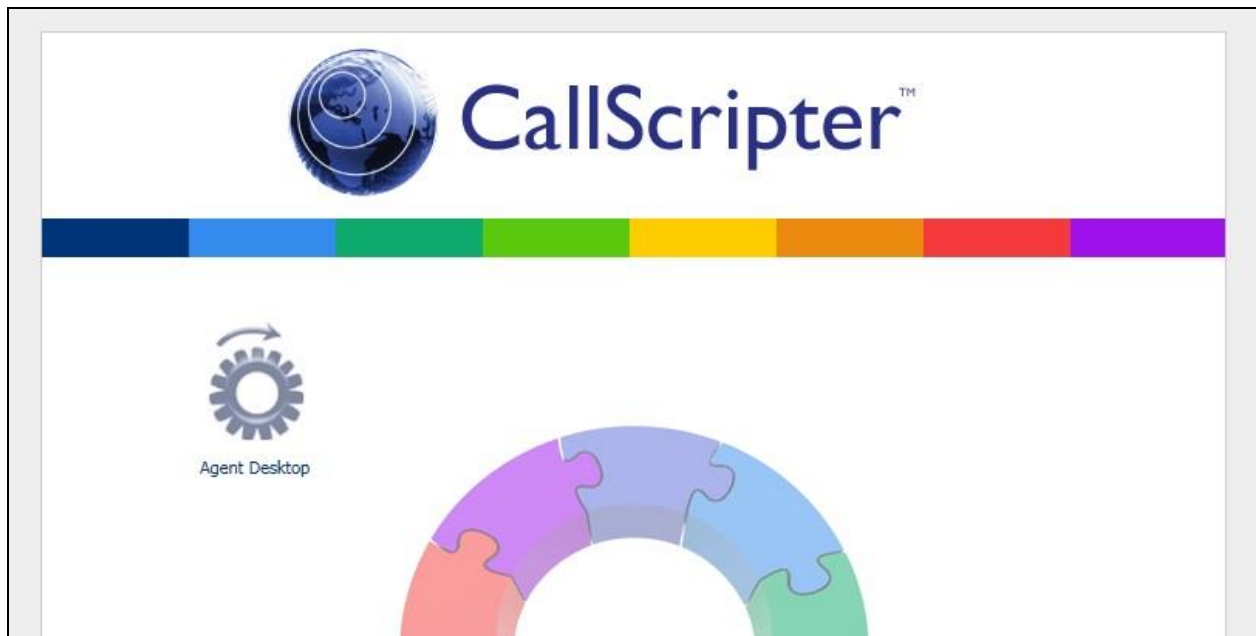
For service-wide information, choose one of the following:

8.3. Verify CallScripter

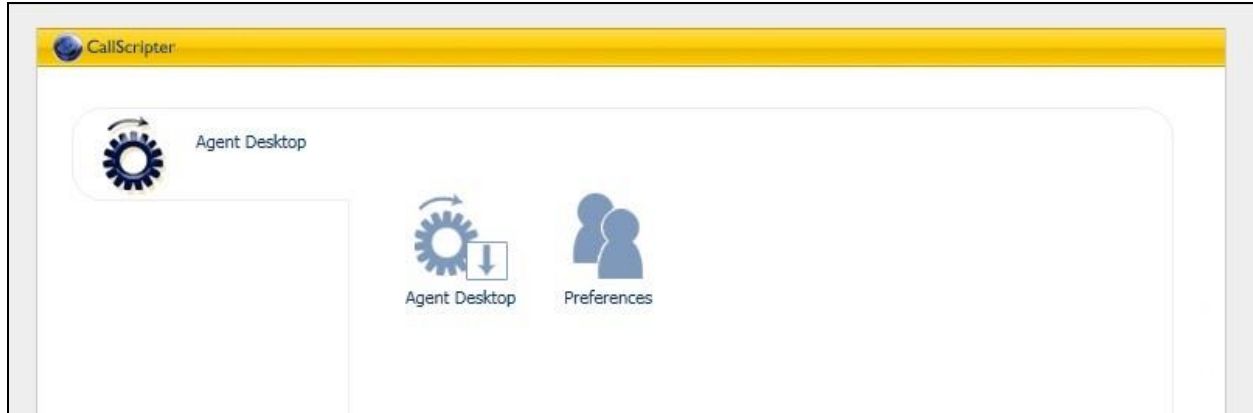
From the agent PC, launch the web interface by using the URL “http://ip-address:7000” in an Internet Explorer browser window, where “ip-address” is the IP address of the CallScripter server. The **CallScripter** screen below is displayed. Log in using the appropriate credentials.

The image shows the CallScripter login interface. At the top, there is a globe icon and the text "CallScripter™". Below this is a horizontal bar with seven colored segments: dark blue, light blue, green, yellow, orange, red, and purple. The main area contains a login form with the prompt "Please enter your username and password." followed by "Username" and "Password" labels, each with a corresponding text input field. Below the password field is a checkbox labeled "Remember Me" and a yellow "Login" button. The background features a large, colorful puzzle piece graphic on the right side.

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



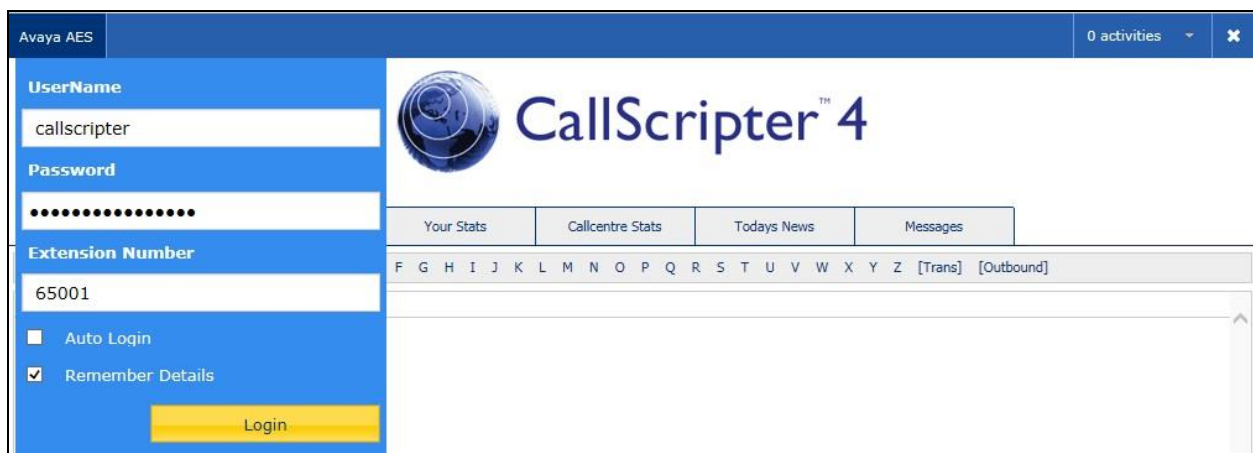
The screen below is displayed. Select **Agent Desktop** from the right pane.



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



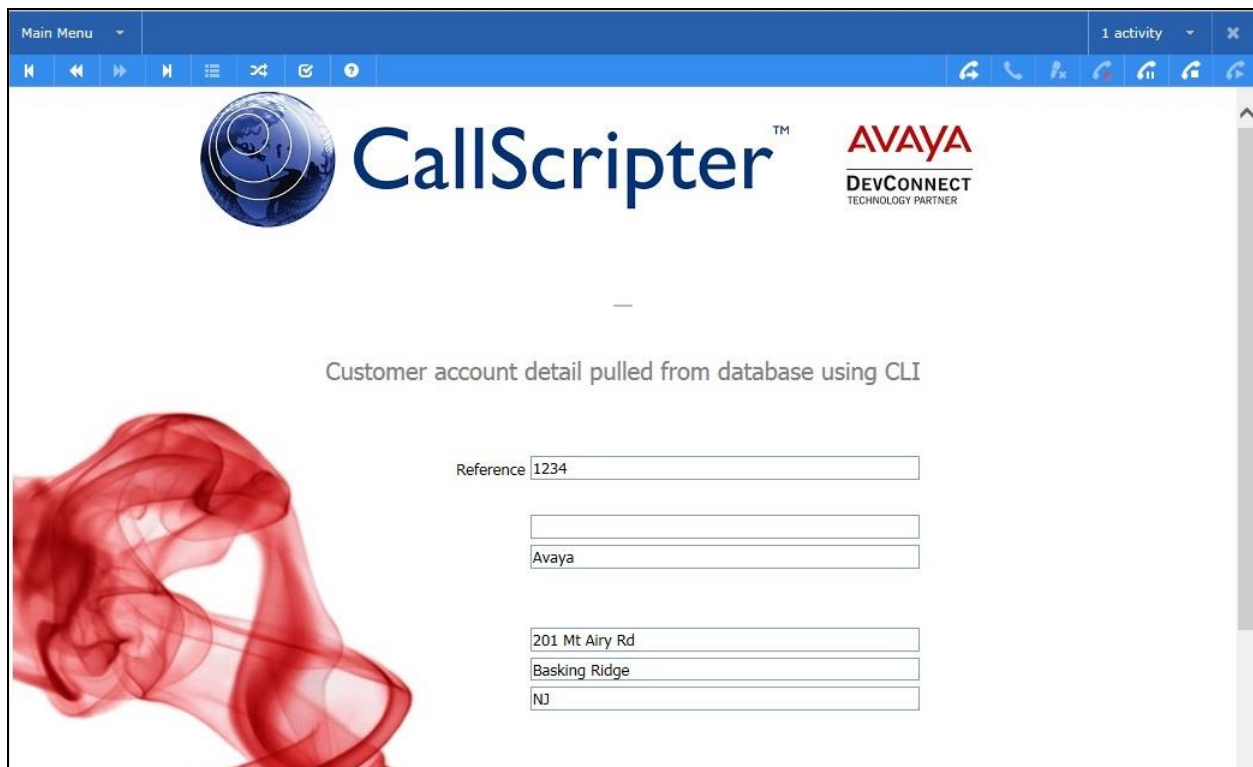
The screen is updated as shown below. For **Extension Number**, update as necessary with actual station extension the agent is using. Retain the default values in the remaining fields, and click **Login**.



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.



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.

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.