



Avaya DevConnect Program

Application Notes for Swampfox Intelligent Customer Experience (ICX) with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya Experience Portal – Issue 1.0

Abstract

These Application Notes describe the steps required to integrate Swampfox Intelligent Customer Experience (ICX) 4.0.1 with Avaya Aura® Communication Manager 10.1, Avaya Aura® Application Enablement Services 10.1, and Avaya Experience Portal 8.1.2. Swampfox ICX provides intelligent call center routing, connecting callers to the best agent based on business rules, and monitors contact center statistics and agents in real-time. Swampfox ICX provides a differentiated customer experience through dynamic voice (IVR) applications and managing to customers' service levels. Swampfox ICX interacts with Avaya Experience Portal via a CCXML application and Avaya Aura® Application Enablement Services via a TSAPI link.

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.

1. Introduction

These Application Notes describe the steps required to integrate Swampfox Intelligent Customer Experience (ICX) 4.0.1 with Avaya Aura® Communication Manager 10.1, Avaya Aura® Application Enablement Services 10.1, and Avaya Experience Portal 8.1.2. Swampfox ICX provides intelligent call center routing, connecting callers to the best agent based on business rules, and monitors contact center statistics and agents in real-time. Swampfox ICX provides a differentiated customer experience through dynamic voice (IVR) applications and managing to customers' service levels. Swampfox ICX interacts with Avaya Experience Portal via a CCXML application and Avaya Aura® Application Enablement Services via a TSAPI link.

For the compliance test, a sample CCXML application was configured on Avaya Experience Portal, hosted on the Swampfox ICX server, that greeted the customer, prompted the customer to enter the department to which to route the call (i.e., sales or support), and then based on the ANI or DNIS, routed the customer's call to the best agent/skill providing either "gold level" or "bronze level" service. While the customer waited to be connected to an agent, the customer received the appropriate Advanced Wait Treatment (e.g., Music on Hold). When the call was routed to an agent and answered, the agent received Whisper Treatment, which played a message to the agent. In this case, the agent heard the service level of the caller (i.e., "gold" or "bronze" customer). The customer was then connected to the agent. Swampfox ICX monitored the contact center statistics and agents using a TSAPI link on Avaya Aura® Application Enablement Services (AES). Swampfox ICX generated call reports and tracked agent status on the Web portal.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on placing calls to an application on Experience Portal and verifying that Swampfox ICX routed the call to the appropriate agents based on ANI and DNIS.

Serviceability testing focused on verifying that Swampfox ICX returned to service after re-connecting the network or rebooting the 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Swampfox ICX used the following encryption features. Experience Portal used HTTPS to access the Swampfox ICX application server and Swampfox ICX used an encrypted TSAPI link to Application Enablement Services.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Use of TSAPI query service to query agent state.
- Use of TSAPI snapshot and monitoring services to monitor calls.
- Use of TSAPI event report service to monitor VDNs and skill groups.
- Use of TSAPI service status service to receive changes in system status.
- Calls from PSTN and internal users to a CCXML application on Experience Portal. Based on the ANI, DNIS, and caller input, Swampfox ICX routed the call the appropriate agent/skill.
- Advanced Wait Treatment for the caller and Whisper Treatment for the agent prior to the customer being connected to agent.
- Proper system recovery after a restart of the Swampfox ICX server or loss of network connectivity.

2.2. Test Results

All test cases passed.

2.3. Support

For Swampfox ICX technical support, contact Swampfox Support via phone or website.

- **Phone:** +1 (803) 451-4540
- **Web:** <https://swampfoxinc.com/support>

3. Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya Aura® Environment that includes the following products:

- Communication Manager with a G430 Media Gateway and Avaya Aura® Media Server providing media resources.
- Session Manager connected to Communication Manager via a SIP trunk.
- Session Manager connected to the PSTN via Avaya Session Border Controller (SBC).
- Avaya Aura® System Manager used to configure Session Manager and SIP stations on Communication Manager.
- Application Enablement Services configured to communicate with Avaya Aura® Communication Manager via TSAPI.
- Experience Portal configured to launch a sample CCXML application that routes callers to the appropriate agent/skill using the Swampfox ICX routing engine.
- Avaya H.323 / SIP Deskphones and Avaya Agent for Desktop serving as agents.
- Swampfox ICX with an encrypted TSAPI link to Application Enablement Services and hosting a sample CCXML application. HTTPS was used between Swampfox ICX application server and Experience Portal.

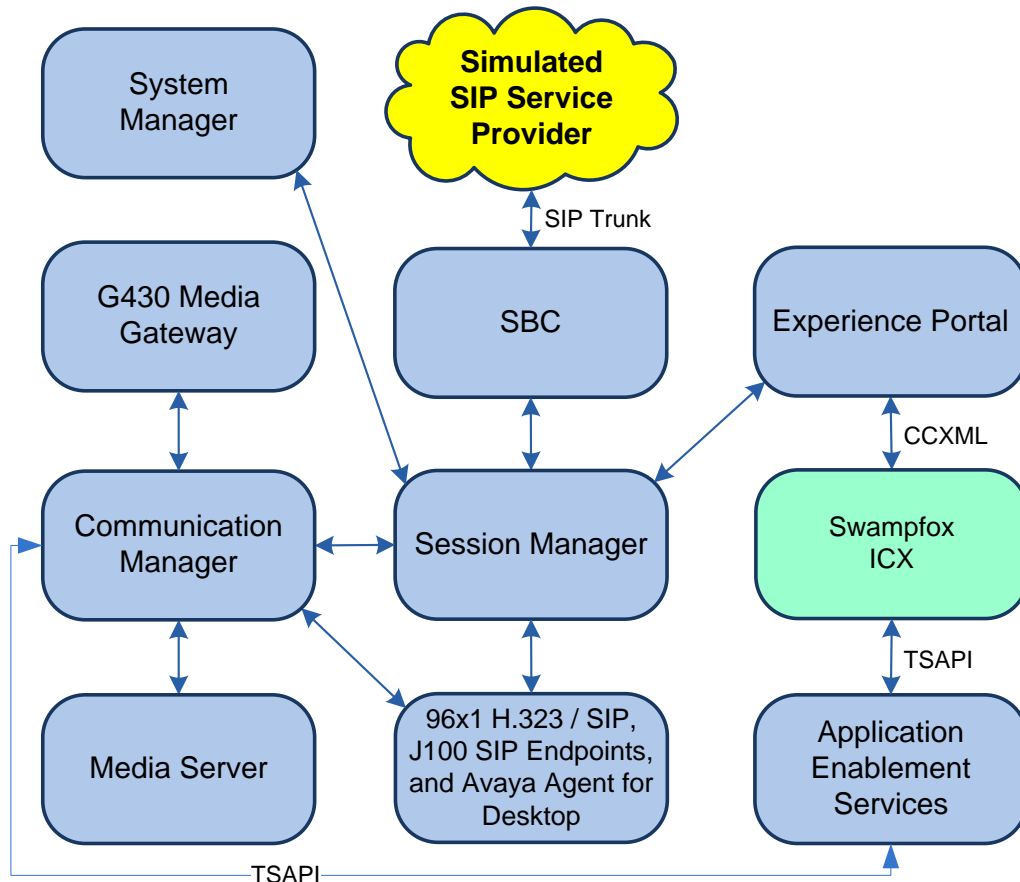


Figure 1: Avaya Aura® Environment with Swampfox ICX

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	10.1.3.1.0-FP3SP1
Avaya G430 Media Gateway	FW 42.2.0
Avaya Aura® Media Server	10.1.0.125
Avaya Experience Portal	8.1.2
Avaya Aura® Application Enablement Services	10.1.3.1.0.49-0
Avaya Aura® System Manager	10.1.3.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.3.1.0716149 Service Pack 1
Avaya Aura® Session Manager	10.1.3.1.1013103
Avaya Session Border Controller	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8.5.4.10 (H.323)
Avaya J100 Series SIP Phones	4.1.1.0.7 (SIP)
Avaya Agent for Desktop	2.0.6.25.3006
Swampfox Intelligent Customer Experience (ICX)	4.0.1.0.4

5. Configure Avaya Aura® Communication Manager

This section provides the steps for configuring Communication Manager. Administration of Communication Manager was performed using the System Access Terminal (SAT). This covers the following areas:

- Verify License
- Administer AES Connection
- Administer CTI Link
- Administer Vectors and VDNs

5.1. Verify License

Log into the System Access Terminal (SAT) 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. Navigate to **Page 4** and verify that the **Computer Telephony Adjunct Links** customer option is set to “y”.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                                Page 4 of 12
                                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? y             DCS Call Coverage? y
ASAI Link Plus Capabilities? y             DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC? n          Digital Loss Plan Modification? y
Async. Transfer Mode (ATM) Trunking? n     DS1 MSP? y
ATM WAN Spare Processor? n                 DS1 Echo Cancellation? y
ATMS? y
Attendant Vectoring? y

(NOTE: You must logoff & login to effect the permission changes.)
```

Navigate to **Page 7** and verify that the **Vectoring (Basic)** customer option is set to “y”.

display system-parameters customer-options				Page 7 of 12	
CALL CENTER OPTIONAL FEATURES					
Call Center Release: 8.0					
ACD? y			Reason Codes? y		
BCMS (Basic)? y			Service Level Maximizer? n		
BCMS/VuStats Service Level? y			Service Observing (Basic)? y		
BSR Local Treatment for IP & ISDN? y			Service Observing (Remote/By FAC)? y		
Business Advocate? n			Service Observing (VDNs)? y		
Call Work Codes? y			Timed ACW? y		
DTMF Feedback Signals For VRU? y			Vectoring (Basic)? y		
Dynamic Advocate? n			Vectoring (Prompting)? y		
Expert Agent Selection (EAS)? y			Vectoring (G3V4 Enhanced)? y		
EAS-PHD? y			Vectoring (3.0 Enhanced)? y		
Forced ACD Calls? n			Vectoring (ANI/II-Digits Routing)? y		
Least Occupied Agent? y			Vectoring (G3V4 Advanced Routing)? y		
Lookahead Interflow (LAI)? y			Vectoring (CINFO)? y		
Multiple Call Handling (On Request)? y			Vectoring (Best Service Routing)? y		
Multiple Call Handling (Forced)? y			Vectoring (Holidays)? y		
PASTE (Display PBX Data on Phone)? y			Vectoring (Variables)? y		
(NOTE: You must logoff & login to effect the permission changes.)					

5.2. Administer AES Connection

In the **IP Services** form, add an entry for AES. On Page 1, configure the following fields:

- **Service Type:** Set to *AESVCS*.
- **Enabled:** Set to y.
- **Local Node:** Set to *procr* for the Processor Ethernet interface.
- **Local Port:** Use the default of 8765.

change ip-services					Page	1 of 3
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	TLS Encryption
AESVCS	y	procr	8765			

On **Page 3** of the **IP Services** form, configure the following fields:

- **AE Services Server:** Set to the AES server hostname from the **IP Node Names** form (not shown).
- **Password:** Set to a password to be administered on AES in **Section 0**.
- **Enabled:** Set to *y*.

change ip-services				Page	3 of	3
AE Services Administration						
Server ID	AE Services Server	Password	Enabled	Status		
1:	devcon-aes	*	y	in use		

5.3. Administer CTI Link

Add a CTI link using the **add cti-link** command. 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 1		Page 1 of 3	
CTI LINK			
CTI Link: 1			
Extension: 77700			
Type: ADJ-IP			
		COR: 1	
Name: AES TSAPI Link			
Unicode Name? n			

5.4. Configure Call Center

To support the sample call center used in the compliance test, the following Hunt Groups, VDNs and Vectors were configured. The actual configuration screens will not be included in these Application Notes, because the configuration was basic and straightforward with the end result simply routing a call to a skill group. Customers should configure them to meet their business needs. They are being listed here to provide context for the Swampfox ICX configuration in **Section 8.4**.

5.4.1. Hunt Groups

Administer four Hunt Groups for Sales Gold, Sales Bronze, Support Gold and Support Bronze. Agents logged into each of the skill groups.

Hunt Group Number	Hunt Group Extension	Purpose
81	77801	Skill for Sales Gold Group.
82	77802	Skill for Support Bronze Group.
83	77803	Skill for Service Gold Group.
84	77804	Skill for Support Bronze Group.

5.4.2. Vectors and VDNs

Administer four VDNs and four Vectors for Sales Gold, Sales Bronze, Support Gold and Support Bronze. The Vectors queued the call to the appropriate skill in **Section 5.4.1**.

VDN	Vector	Purpose
77811	81	VDN & Vector for Sales Gold Group.
77812	82	VDN & Vector for Sales Bronze Group.
77813	83	VDN & Vector for Support Gold Group.
77814	84	VDN & Vector for Support Bronze Group.

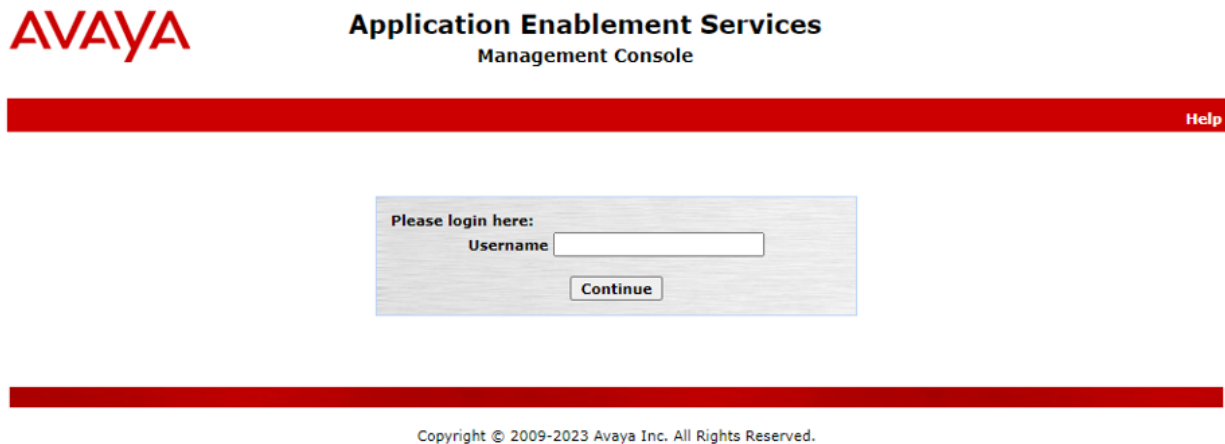
6. Configure Avaya Aura® Application Enablement Services

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

- Launch OAM Interface
- Verify License
- Administer Switch Connection
- Administer TSAPI Link
- Restart Service
- Obtain Tlink Name
- Administer User
- Verify Security Database

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 login screen is displayed. Log in using the appropriate credentials.



The screenshot displays the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo, and to its right is the text "Application Enablement Services Management Console". A red horizontal bar spans the width of the page, with a "Help" link in the top right corner. In the center, there is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, another red horizontal bar is present, with the copyright notice "Copyright © 2009-2023 Avaya Inc. All Rights Reserved." centered below it.

6.2. Verify License

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

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Wed Sept 13 11:54:53 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:14:27 EDT 2023
HA Status: Not Configured

Licensing | WebLM Server AccessHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▼ Licensing

WebLM Server Address

WebLM Server Access

Reserved Licenses

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

WebLM Server Access

WebLM Server Access helps you to access the WebLM server specified on the WebLM Server Address page.

- If you are using a local Avaya WebLM server, the AE Services management console redirects you to the Web License Manager page for WebLM configuration.
- If you are using a standalone WebLM server, you must manually log in to the WebLM server for WebLM configuration.

Copyright © 2009-2023 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** (**VALUE_AES_TSAPI_USERS**) as shown below.

Application Enablement (CTI) - Release: 10 - SID: 10503000 Standard License file

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: May 31, 2022 10:32:15 AM -04:00

License File Host IDs: V9-DF-31-89-CD-2A-01

Licensed Features

13 Items Show All



Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16

SmallServerTypes:
s8300c;s8300d;icc;premio;tn8400;laptop;CtiS

Scroll down to see the rest of the licenses. Note that Swampfox ICX uses **VALUE_AES_TSAPI_USERS** license as shown in the **Acquired Licenses** section below.

Product Notes VALUE_NOTES	permanent	AdvancedUnrestricted, DMCUnrestricted, AgentBasicUnrestricted, AdvancedUnrestricted, DMCUNIFIED_DESKTOP_001, BasicUnrestricted, AgentDMCUnrestricted, AgentEvents; AACC_001, BasicAdvancedUnrestricted, DMCUnrestricted; CE_ABasicUnrestricted, AdvancedUnrestricted, DMCOTP_CLIENT_001, BasicUnrestricted, , , AgentEvents; EXT_CLIENT_002, , , , AgentEvents; EXT_CLIENT_004, , , , AgentEvents; EXT_CLIENT_006, , , , AgentEvents; EXT_CLIENT_008, , , , AgentEvents; EXT_CLIENT_010, , , , AgentEvents; AAWFO_SELECT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; OFFICELINX_0AdvancedUnrestricted, DMCUnrestricted, AgentBasicUnrestricted, , DMCUnrestricted, AgentEvents; BasicUnrestricted, AdvancedUnrestricted, DMC_ECD_001, , AdvancedUnrestricted, , AgentEvents; VERINT_ESSENTIAL_001, BasicUnrestricted, AgentDMCUnrestricted; ACI_001, BasicUnrestricted, AgentEvents; CALABRIO_001, BasicUnrestricted, DMCUnrestricted;
AES HA SMALL VALUE_AES_HA_SMALL	permanent	1

Acquired Licenses

1 Item  Show All 			
Feature	Acquired by	Acquirer ID	Count
VALUE_AES_TSAPI_USERS	TSAPI (devcon-aes)	devcon-aes:1694613592:1175291:140411028138112:0000	4

6.3. Administer Switch Connection

To administer a **Switch Connection** for Communication Manager, navigate to **Communication Manager Interface → Switch Connections** and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as *devcon* as shown below.

Welcome: User cust
Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:20:05 EDT 2023
HA Status: Not Configured

AVAYA Application Enablement Services Management Console

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

Navigation menu: AE Services, Communication Manager Interface, Switch Connections, Dial Plan, High Availability, Licensing, Maintenance.

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> devcon	Yes	30	1

Click **Edit Connection** button to configure the connection details. Enter the **Switch Password** and check the **Processor Ethernet** box, if using the **procr** interface, as shown below. The password must match the one configured when adding AESVCS connection in Communication Manager in **Section 5.2**. A secure switch connection was used as shown below.

Welcome: User cust
Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:21:23 EDT 2023
HA Status: Not Configured

AVAYA Application Enablement Services Management Console

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

Navigation menu: AE Services, Communication Manager Interface, Switch Connections, Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, Help.

Connection Details - devcon

Switch Password:

Confirm Switch Password:

Msg Period: Minutes (1 - 72)


Provide AE Services certificate to switch: ☒

Secure H323 Connection: ☐

Processor Ethernet: ☒

Enable TLS Certificate Validation: ☒

Click **Edit PE/CLAN IPs** on the **Switch Connection** page and configure the **procr** or **CLAN** IP address of Communication Manager and click **Add/Edit Name or IP**.


Application Enablement Services
Management Console

Welcome: User cust
 Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
 Number of prior failed login attempts: 0
 HostName/IP: devcon-aes/10.64.102.119
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.3.1.0.49-0
 Server Date and Time: Fri Sep 15 11:26:04 EDT 2023
 HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout


AE Services
 Communication Manager Interface
Switch Connections
 Dial Plan
 High Availability
 Licensing
 Maintenance

Edit Processor Ethernet IP - devcon

Name or IP Address	Status
10.64.102.115	In Use

6.4. 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**.


Application Enablement Services
Management Console

Welcome: User cust
 Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
 Number of prior failed login attempts: 0
 HostName/IP: devcon-aes/10.64.102.119
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.3.1.0.49-0
 Server Date and Time: Fri Sep 15 11:27:20 EDT 2023
 HA Status: Not Configured

AE Services | TSAPI | TSAPI Links Home | Help | Logout

AE Services
 CVLAN
 DLG
 DMCC
 SMS
 TSAPI
 TSAPI Links
 TSAPI Properties
 TWS

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	devcon	1	12	Both

The **Add TSAPI Links** screen is displayed next. The **Link** field is only local to Application Enablement Services 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 *devcon* is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. **Security** was set to *Both* to allow secure and unsecure TSAPI links. For the compliance test, a secure TSAPI link was used. Retain the default values in the remaining fields.

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:28:16 EDT 2023
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links

Home | Help | Logout

▼ AE Services

▶ CVLAN

▶ DLG

▶ DMCC

▶ SMS

▼ TSAPI

▪ TSAPI Links

▪ TSAPI Properties

▶ TWS

Edit TSAPI Links

Link1

Switch Connectiondevcon ▼

Switch CTI Link Number1 ▼

ASAI Link Version12 ▼

SecurityBoth ▼

Apply ChangesCancel ChangesAdvanced Settings

6.5. Restart Service

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

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:30:37 EDT 2023
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

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input 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
<input type="checkbox"/> WTI Service	Running

Note: DMCC Service must be restarted for WTI service changes to take effect.
For status on actual services, please use [Status and Control](#)

Start Stop Restart Service Restart AE Server Restart Linux Restart Web Server

6.6. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks** from the left pane. The **Tlinks** screen shows a listing of Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name to be used later for configuring Swampfox ICX.

In this case, the associated Tlink name is “AVAYA#DEVCON#CSTA-S#DEVCON-AES” for the secure TSAPI link. Note the use of the switch connection “DEVCON” from **Section 0** as part of the Tlink name.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top right, a welcome message for user 'cust' is shown, including the last login time (Fri Sept 15 11:17:15 E.S.T. 2023) and server information. The main header is 'AVAYA Application Enablement Services Management Console'. Below this is a red navigation bar with 'Security | Security Database | Tlinks' and links for 'Home | Help | Logout'. The left sidebar contains a tree view with categories like 'AE Services', 'Communication Manager Interface', 'High Availability', 'Licensing', 'Maintenance', 'Networking', 'Security', and 'Security Database'. Under 'Security Database', 'Tlinks' is selected. The main content area, titled 'Tlinks', shows two radio button options for 'Tlink Name': 'AVAYA#DEVCON#CSTA#DEVCON-AES' (selected) and 'AVAYA#DEVCON#CSTA-S#DEVCON-AES' (highlighted with a red box). A 'Delete Tlink' button is also present.

6.7. Administer 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.

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:34:08 EDT 2023
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

6.8. Verify Security Database

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

Verify that **Enable SDB for TSAPI Service, JTAPI and Telephony Web Services** is unchecked. In the event that security database is used by the customer with this parameter already enabled, then follow [2] to configure access privileges for the user from **Section 6.7**.

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Sept 15 11:17:15 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:35:10 EDT 2023
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

CTI Users

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

☐ Enable SDB for DMCC and WTI Service

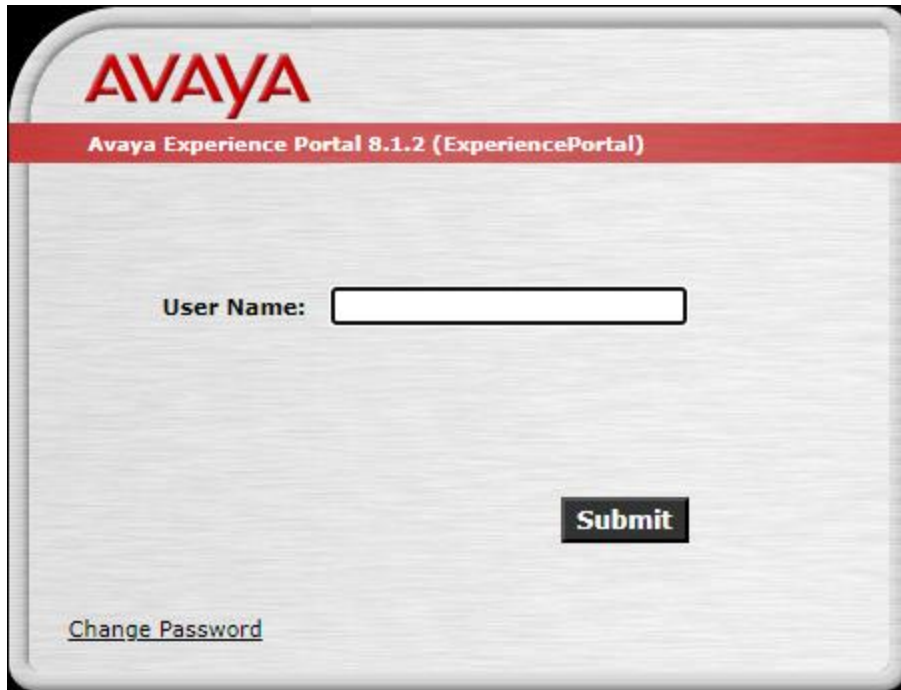
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

Apply Changes

7. Configure Avaya Experience Portal

This section covers the configuration of a sample CCXML application in Experience Portal using the Experience Portal Manager (EPM) web interface.

Experience Portal is configured via the Experience Portal Manager (EPM) web interface. To access the web interface, enter **https://<ip-addr>** as the URL in a web browser, where <ip-addr> is the IP address of EPM. Log in using the appropriate credentials.

The image shows the login page of the Avaya Experience Portal 8.1.2. At the top, the Avaya logo is displayed in red. Below it, a red banner contains the text "Avaya Experience Portal 8.1.2 (ExperiencePortal)". The main area is white and contains a "User Name:" label followed by a text input field. Below the input field is a black "Submit" button. At the bottom left, there is a link labeled "Change Password".

The main page of the EPM web interface is displayed as shown below.

AVAYA Welcome, eadmin
Last logged in Sep 13, 2023 at 1:48:12 PM MDT

Avaya Experience Portal 8.1.2 (ExperiencePortal) Home Help Logoff

Expand All | Collapse All

▼ User Management
Roles
Users
Login Options

▼ Real-time Monitoring
System Monitor
Active Calls
Port Distribution

▼ System Maintenance
Audit Log Viewer
Trace Viewer
Log Viewer
Alarm Manager

▼ System Management
Application Server
EPM Manager
MPP Manager
Software Upgrade
System Backup

▼ System Configuration
Applications
EPM Servers
MPP Servers
SNMP
Speech Servers
VoIP Connections
Zones

▼ Security
Certificates
Licensing

▼ Reports
Standard
Custom
Scheduled

▼ Multi-Media Configuration
Email
HTML
SMS

▼ Proactive Outreach
Manager
Monitor
Dashboard

You are here: Home

Avaya Experience Portal Manager

Avaya Experience Portal Manager (EPM) is the consolidated web-based application for administering Experience Portal. Through the EPM interface you can configure Experience Portal, check the status of an Experience Portal component, and generate reports related to system operation.

Installed Components

Media Processing Platform
Media Processing Platform (MPP) is an Avaya media processing server. When an MPP receives a call from a PBX, it invokes a VoiceXML (or CCXML) application on an application server. It then communicates with ASR and TTS servers as necessary to process the call.

Email Service
Email Service is an Experience Portal feature which provides e-mail capabilities.

HTML Service
HTML Service is an Experience Portal feature which supports web applications with HTML5 capabilities. It includes support for browser based services for mobile devices.

Proactive Outreach Manager
Avaya Proactive Outreach Manager (POM) provides a solution for unified, multichannel, inbound and outbound architecture, with the capability to communicate through different channels of interaction, from Short Message Service (SMS) to e-mail to the traditional voice.

SMS Service
SMS Service is an Experience Portal feature which provides SMS capabilities.

Legal Notice

AVAYA GLOBAL SOFTWARE LICENSE TERMS
REVISED: June 1st, 2020

THESE GLOBAL SOFTWARE LICENSE TERMS ("SOFTWARE LICENSE TERMS") GOVERN THE USE OF PROPRIETARY SOFTWARE AND THIRD- PARTY PROPRIETARY SOFTWARE LICENSED THROUGH AVAYA. READ THESE SOFTWARE LICENSE TERMS CAREFULLY, IN THEIR ENTIRETY, BEFORE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (AS DEFINED IN SECTION A BELOW). BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, THE END USER, ON BEHALF OF THEMSELF AND THE ENTITY FOR WHOM THEY ARE DOING SO (HEREINAFTER REFERRED TO AS "END USER"), AGREE TO THESE SOFTWARE LICENSE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN END USER AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA"). IF THE END USER IS ACCEPTING THESE SOFTWARE LICENSE TERMS ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, THE END USER REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE SOFTWARE LICENSE

On the left pane, navigate to **System Configuration → Applications**. The **Applications** page is displayed (not shown). Click **Add**. In the **Add Application** page shown below, configure the application. For the compliance test, a CCXML applications was configured as shown below.

- **Name:** Provide a descriptive name (e.g., *Swampfox Test*).
- **Enable:** Set to **Yes** to enable the application.
- **Type:** Set to **CCXML**.
- **CCXML URL:** Specify the CCXML application URL. Click **Verify** to check application accessibility.
- **ASR Speech Servers:** Not required.
- **TTS Speech Servers:** Select TTS Speech Server. Required as tested.
- **Application Launch:** Set the **Called Number** (e.g., *78560*) associated with the application and click **Add**.

The screenshot displays the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, user information (Welcome, epadmin), and a timestamp (Last logged in Sep 13, 2023 at 1:48:12 PM MDT). The left sidebar shows a tree view of system configuration options, with 'System Configuration' expanded. The main content area is titled 'Change Application' and contains the following configuration fields:

- Name:** Swampfox Test
- Enable:** ☒ Yes ☐ No
- Type:** CCXML (selected from a dropdown)
- Reserved SIP Calls:** ☒ None ☐ Minimum ☐ Maximum
- Requested:** (empty text field)
- URI:**
 - ☒ Single ☐ Fail Over ☐ Load Balance
 - CCXML URL:** https://10.64.102.104:9443/DRMServer/StartCallFlow.jsp?avp_core=DevConnect (with a **Verify** button)
 - Mutual Certificate Authentication:** ☐ Yes ☒ No
 - Basic Authentication:** ☐ Yes ☒ No
- ASR Speech Servers:**
 - Engine Types:** Nuance
 - Selected Engine Types:** <None>
- TTS Speech Servers:**
 - Voices:** <None>
 - Selected Voices:** English(USA) en-US Jennifer F
- Application Launch:**
 - ☒ Inbound ☐ Inbound Default ☐ Outbound
 - ☒ Number ☐ Number Range ☐ URI
 - Called Number:** (empty text field) (with an **Add** button)
 - 78560 (with a **Remove** button)

Scroll down and expand the **Advanced Parameters** section and configure the following parameters:

- **Generate UCID:** Set to *Yes*.
- **Operation Mode:** Set to *Shared UUI*.
- **Transport UCID in Shared Mode:** Set to *Yes*.
- **Maximum UUI Length:** Use default value of *128*.

The screenshot displays the Avaya Experience Portal 8.1.2 (ExperiencePortal) interface. The top navigation bar includes the Avaya logo, the user name 'Welcome, eadmin', and the last login time 'Last logged in Sep 13, 2023 at 1:48:12 PM MDT'. The left sidebar shows a tree view of the system configuration, with 'Advanced Parameters' expanded. The main content area shows the 'Advanced Parameters' configuration page. A red box highlights the following parameters:

- Generate UCID:** Set to *Yes* (radio button selected).
- Operation Mode:** Set to *Shared UUI* (dropdown menu).
- Transport UCID in Shared Mode:** Set to *Yes* (radio button selected).
- Maximum UUI Length:** Set to *128* (text input field).

Other visible parameters include:

- Support Remote DTMF Processing:** Set to *No* (radio button selected).
- DTMF Type Ahead Enabled:** Set to *Yes* (radio button selected).
- Converse-On:** Set to *No* (radio button selected).
- Network Media Service:** Set to *No* (radio button selected).
- Early Media:** Set to *No* (radio button selected).
- Sync FROM and PAI Headers:** Set to *No* (radio button selected).
- Dialog URL Pattern:** (text input field).
- VoiceXML Event Handler:** Set to *<Default>* (dropdown menu).
- CCXML Event Handler:** Set to *<Default>* (dropdown menu).
- Fax Detection Enabled:** Set to *No* (radio button selected).
- Fax Phone Number:** (text input field).
- Video Enabled:** Set to *No* (radio button selected).
- Video Screen Format:** Set to *QCIF* (dropdown menu).
- Video Minimum Picture Interval:** Set to *2* (text input field).

At the bottom of the configuration page, there are buttons for **Save**, **Apply**, **Cancel**, and **Help**.

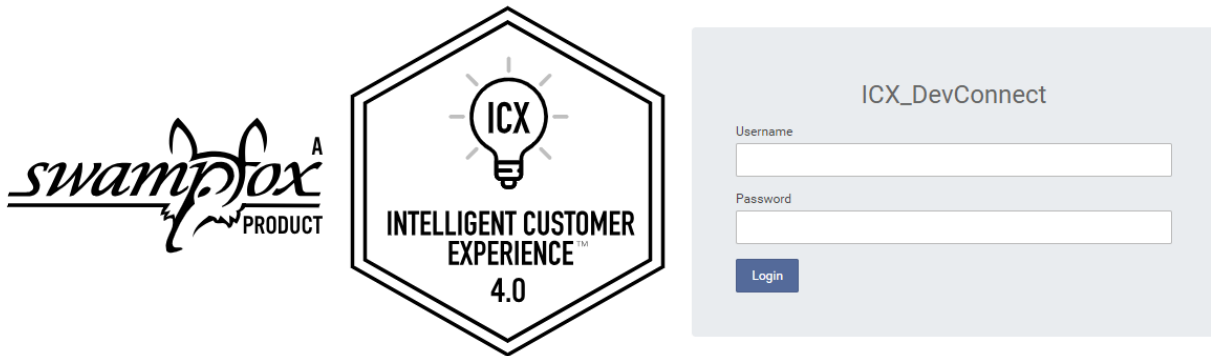
8. Configure Swampfox ICX

This section provides steps for configuring Swampfox ICX. Configuration of Swampfox ICX is performed via Swampfox ICX web interface and covers the following areas:

- Log into Swampfox ICX Web Interface
- Administer CTI Connection
- Create Snapshots
- Administer Transfer VDNs and Skills
- Administer Call Routing based on ANI or DNIS
- Promote Changes

8.1. Log into Swampfox ICX Web Interface

Access the Swampfox ICX web interface by using the URL “<https://<ip-address>:8443/icx>” in an Internet browser, where <ip-address> is the IP address of the Swampfox IXC server. Log in using appropriate credentials.



The **System Dashboard** is displayed as shown below.

The screenshot displays the 'System Dashboard' of the SWAMPFOX Technologies Intelligent Customer Experience (ICX) environment. The interface includes a dark sidebar with navigation options such as 'Dashboard and Reports', 'System Dashboard', 'Contact Center Dashboard', 'Session Details Report', 'Custom Reports', 'Business Parameter Management', 'Manage Snapshots', 'Assets', 'SCXML Dialogs', 'Global Announcement Sets', 'Recordings', 'Scripts', 'Contact Center Management', 'Route Points', and 'CTI Connections'. The main content area shows a 'System Dashboard' header with a 'Last Refresh' timestamp of 9/13/2023, 3:35:00 PM EDT and a 'Download Diagnostic Data' button. Below the header, there are four green boxes indicating zero errors: '0 Monitor Errors', '0 Routing Errors', '0 Database Errors', and '0 Active Alarms'. A 'Monitor Summary' table shows the 'AES DevConnect E' source with a status of 'OK' and 100% OK. Two server status summaries are also present: 'Routing Servers Summary' for 'SWAMPFOX' (Running, Healthy, Synchronized) and 'Management Servers Summary' for 'SWAMPFOX - Primary' (Running, Healthy). At the bottom, there are tabs for 'Active Alarms' and 'Recent Alarms', with the 'Active Alarms' tab showing 'No Active Alarms'.

SWAMPFOX TECHNOLOGIES
Intelligent Customer Experience

ENVIRONMENT
ICX_DevConnect

System Dashboard Last Refresh: 9/13/2023, 3:35:00 PM EDT Download Diagnostic Data

0 Monitor Errors 0 Routing Errors 0 Database Errors 0 Active Alarms

Monitor Summary

Source	Status	% OK
AES DevConnect E	OK	100%

Routing Servers Summary

SWAMPFOX

- Running
- Healthy
- Synchronized

Management Servers Summary

SWAMPFOX - Primary

- Running
- Healthy

Detailed Server Report

Active Alarms Recent Alarms

No Active Alarms

8.2. Administer CTI Connection

From the ICX web interface, navigate to **CTI Connections**. Click **New** to add a new CTI Connection. The CTI Connection used for the compliance test will be reviewed.

The screenshot displays the 'CTI Connections' page in the ICX web interface. The top header shows 'SWAMPFOX TECHNOLOGIES Intelligent Customer Experience' and 'ENVIRONMENT ICX_DevConnect'. The left sidebar contains navigation links such as 'Dashboard and Reports', 'System Dashboard', 'Contact Center Dashboard', 'Session Details Report', 'Custom Reports', 'Business Parameter Management', 'Manage Snapshots', 'Assets', 'SCXML Dialogs', 'Global Announcement Sets', 'Recordings', 'Scripts', 'Contact Center Management', 'Route Points', and 'CTI Connections'. The main content area features a table with the following columns: Name, Route Point/ICX ACD, Description, CTI Server, and CTI/TLINK Service. The table lists four connections: AES CM 6, AES CM 8, AES DevConnect, and AES DevConnect E. A 'New' button is located in the top right corner, and a 'Duplicate' button is positioned above the table. The bottom of the page shows pagination: (Page 1 of 1) and 25 rows/page.

<input type="checkbox"/>	Name	Route Point/ICX ACD	Description	CTI Server	CTI/TLINK Service
<input type="checkbox"/>	AES CM 6	1	---	10.91.2.90	AVAYA#CM633#CSTA#FOX-LAB-AES633
<input type="checkbox"/>	AES CM 8	2	---	10.91.10.94	AVAYA#CM10#CSTA#AES10
<input type="checkbox"/>	AES DevConnect	2	---	10.64.102.119	AVAYA#DEVCON#CSTA#DEVCON-AES
<input type="checkbox"/>	AES DevConnect E	2	---	10.64.102.119	AVAYA#DEVCON#CSTA-S#DEVCON-AES

In **CTI Connection Properties**, configure the following parameters:

- **CTI Connection Name:** Provide a descriptive name (e.g., *AES DevConnect E*).
- **Enable CTI Connection:** Select the checkbox.
- **Route Point/ACD:** Set to available route point/ACD identifier (e.g., 2).
- **CTI Server Address:** Set to AES IP address (e.g., *10.64.102.119*).
- **CTI/TLINK String:** Set to the TLINK name from **Section 6.6** (e.g., *AVAYA#DEVCON#CSTA-S#DEVCON-AES*).
- **CTI Login:** Set to the AES user configured in **Section 6.7** (e.g., *swampfox*).
- **CTI Password:** Set to the AES user password configured in **Section 6.7**.

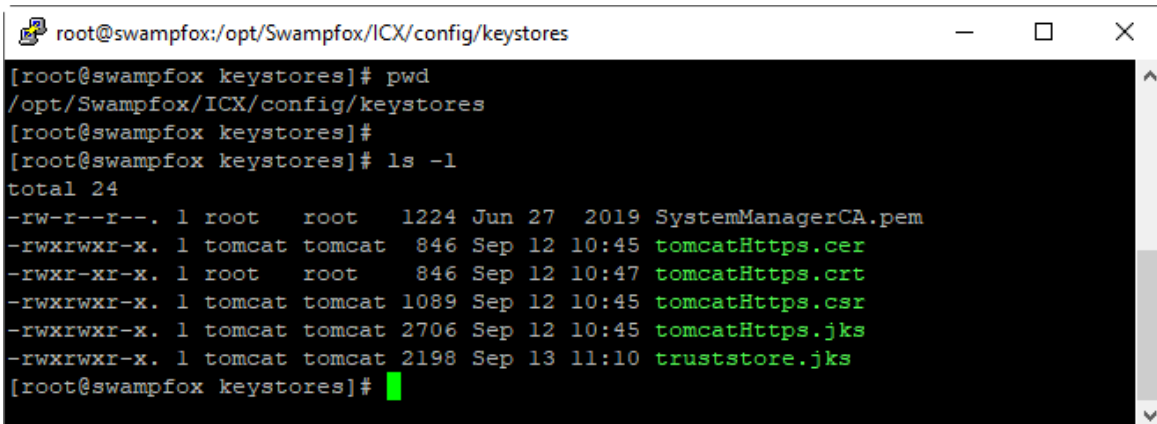
The screenshot displays the 'ICX DevConnect' application interface. The top header includes the 'SWAMPFOX TECHNOLOGIES Intelligent Customer Experience' logo and the 'ENVIRONMENT ICX_DevConnect' label. A sidebar on the left contains navigation links: 'Dashboard and Reports', 'System Dashboard', 'Contact Center Dashboard', 'Session Details Report', 'Custom Reports', 'Business Parameter Management', 'Manage Snapshots', 'Assets', 'SCXML Dialogs', 'Global Announcement Sets', 'Recordings', 'Scripts', 'Contact Center Management', 'Route Points', 'CTI Connections', and 'Reporting Connections'. The main content area is titled 'CTI Connection Properties: AES DevConnect E'. It features two tabs: 'General' (selected) and 'Vector Variables'. The 'General' tab is divided into 'Details' and 'CTI Settings' sections. The 'Details' section includes fields for 'CTI Connection Name *' (AES DevConnect E), 'Enable CTI Connection' (checked), 'Route Point/ACD *' (2), and a 'Description' field. It also shows modification details: 'Modified: 09/13/2023 11:16:54 EDT' and 'Modified by: devconnect:192.168.100.251:icx:GUI'. The 'CTI Settings' section includes fields for 'CTI Server Address *' (10.64.102.119), 'CTI/TLINK String *' (AVAYA#DEVCON#CSTA-S#DEVCON-AES), 'CTI Username *' (swampfox), and 'CTI Password *' (masked). Below these is an 'Advanced Integration Credentials' section with fields for 'Route Point Server Address', 'Route Point/ACD Login', and 'Route Point/ACD Password' (masked). At the bottom of the form are 'Save' and 'Cancel' buttons.

8.2.1. Import Certificate

Swampfox ICX used an encrypted TSAPI link to Application Enablement Services. This required storing the root CA certificate in the keystores directory on the Swampfox ICX server as shown below. The keystores directory was

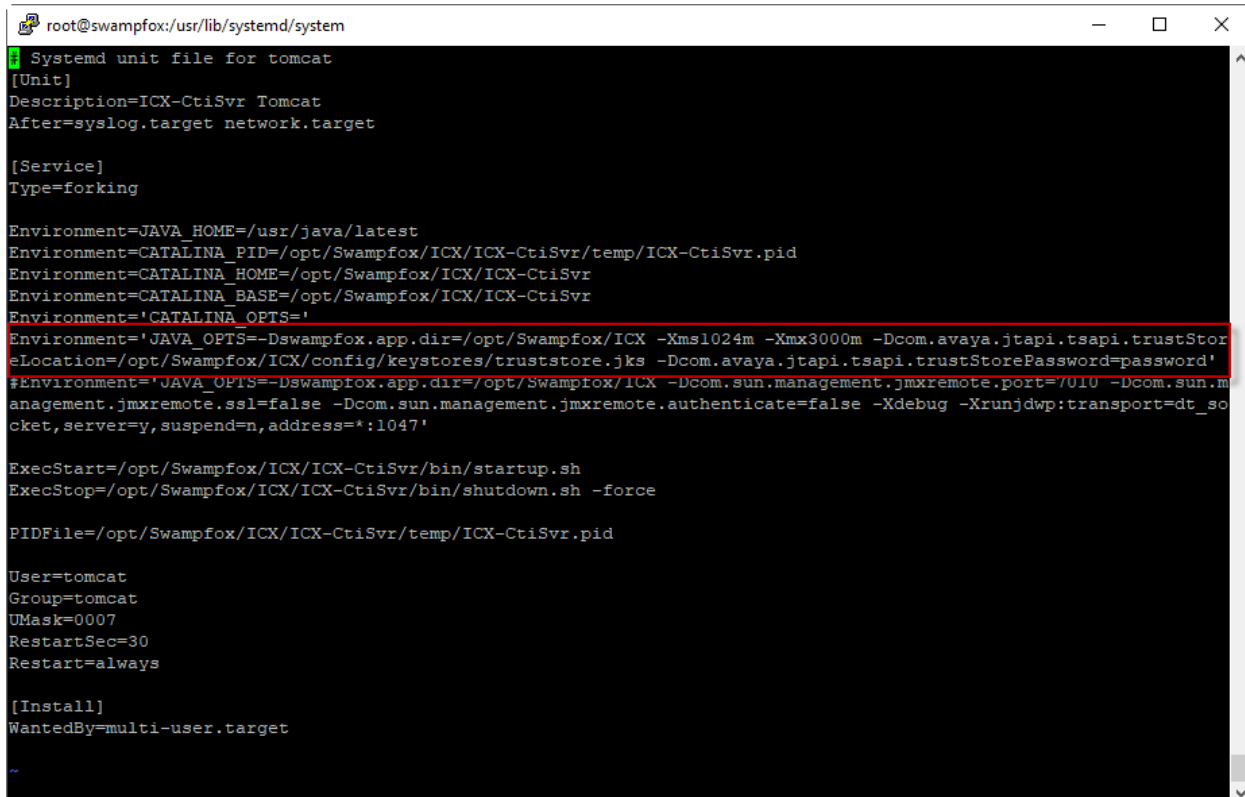
/opt/Swampfox/ICX/config/keystores and the certificate was

SystemManagerCA.pem. For the compliance test, System Manager was the Certificate Authority.



```
root@swampfox:/opt/Swampfox/ICX/config/keystores
[root@swampfox keystores]# pwd
/opt/Swampfox/ICX/config/keystores
[root@swampfox keystores]#
[root@swampfox keystores]# ls -l
total 24
-rw-r--r--. 1 root root 1224 Jun 27 2019 SystemManagerCA.pem
-rwxrwxr-x. 1 tomcat tomcat 846 Sep 12 10:45 tomcatHttps.cer
-rwxr-xr-x. 1 root root 846 Sep 12 10:47 tomcatHttps.crt
-rwxrwxr-x. 1 tomcat tomcat 1089 Sep 12 10:45 tomcatHttps.csr
-rwxrwxr-x. 1 tomcat tomcat 2706 Sep 12 10:45 tomcatHttps.jks
-rwxrwxr-x. 1 tomcat tomcat 2198 Sep 13 11:10 truststore.jks
[root@swampfox keystores]#
```

The /usr/lib/systemd/system/ICX-CtiSrv.service file had to be modified to point to the keystore location of the certificate as shown below.



```
root@swampfox:/usr/lib/systemd/system
Systemd unit file for tomcat
[Unit]
Description=ICX-CtiSvr Tomcat
After=syslog.target network.target

[Service]
Type=forking

Environment=JAVA_HOME=/usr/java/latest
Environment=CATALINA_PID=/opt/Swampfox/ICX/ICX-CtiSvr/temp/ICX-CtiSvr.pid
Environment=CATALINA_HOME=/opt/Swampfox/ICX/ICX-CtiSvr
Environment=CATALINA_BASE=/opt/Swampfox/ICX/ICX-CtiSvr
Environment='CATALINA_OPTS='
Environment='JAVA_OPTS=-Dswampfox.app.dir=/opt/Swampfox/ICX -Xms1024m -Xmx3000m -Dcom.avaya.jtapi.tsapi.trustStoreLocation=/opt/Swampfox/ICX/config/keystores/truststore.jks -Dcom.avaya.jtapi.tsapi.trustStorePassword=password'
#Environment='JAVA_OPTS=-Dswampfox.app.dir=/opt/Swampfox/ICX -Dcom.sun.management.jmxremote.port=7010 -Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false -Xdebug -Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=:1047'

ExecStart=/opt/Swampfox/ICX/ICX-CtiSvr/bin/startup.sh
ExecStop=/opt/Swampfox/ICX/ICX-CtiSvr/bin/shutdown.sh -force

PIDFile=/opt/Swampfox/ICX/ICX-CtiSvr/temp/ICX-CtiSvr.pid

User=tomcat
Group=tomcat
UMask=0007
RestartSec=30
Restart=always

[Install]
WantedBy=multi-user.target
```

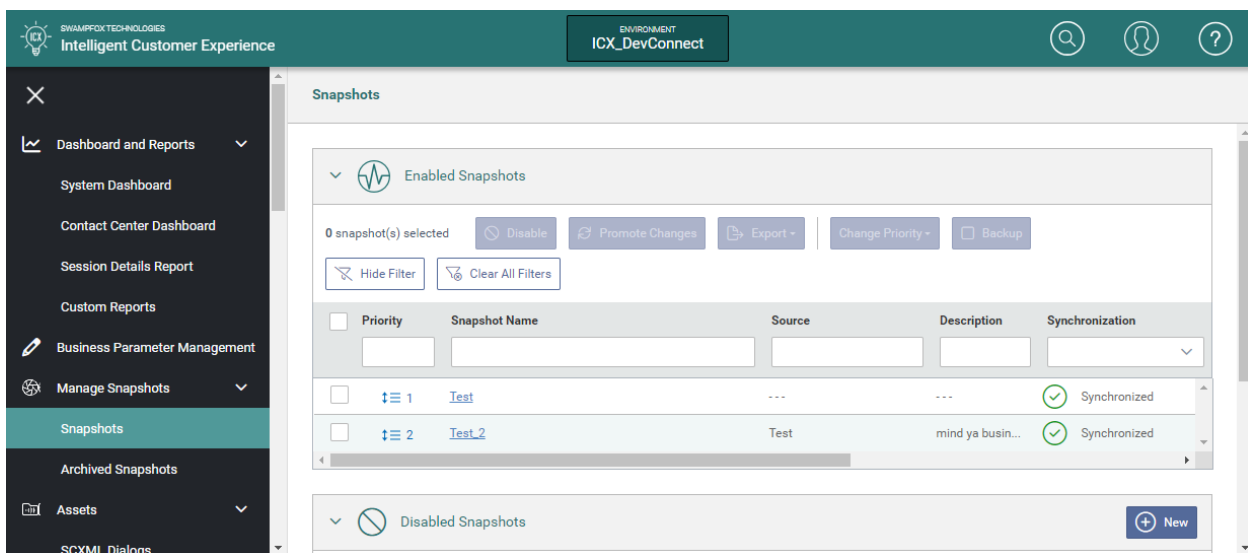
Lastly, for the changes to take effect, restart the following services.

```
root@swampfox:/opt/Swampfox/ICX/config/keystores
[root@swampfox keystores]# systemctl restart ICX-DrmSvr
[root@swampfox keystores]# systemctl restart ICX-CtiSvr
[root@swampfox keystores]#
```

8.3. Create Snapshots

A **Snapshot** contains its own Application Rules, Interaction Flows, and Functions, including Entries/Intents and Exits. Functions are the key collection of routing elements. The Function **Exit** specifies to which VDN and skill group to route the call and will be covered in **Section 8.4**.

From the ICX web interface, navigate to **Snapshots**. The configuration of the Snapshots is outside the scope of these Application Notes. For details on configuring Snapshots, refer to [4]. Click on an existing Snapshot (e.g., *Test*) to configure the VDNs and skill groups.



In **Managing Snapshot: Test**, select the **Functions** tab. For the compliance test, two functions were created for *sales* and *support*. To configure the VDNs and skills for Sales, click on the *sales* function.

The screenshot displays the Avaya DevConnect application interface. The top header shows 'SWAMPFOX TECHNOLOGIES Intelligent Customer Experience' and 'ENVIRONMENT ICX_DevConnect'. The left sidebar contains a navigation menu with options like 'Dashboard and Reports', 'System Dashboard', 'Contact Center Dashboard', 'Session Details Report', 'Custom Reports', 'Business Parameter Management', 'Manage Snapshots', 'Snapshots', 'Archived Snapshots', 'Assets', 'SCXML Dialogs', and 'Global Announcement Sets'. The main content area is titled 'Managing Snapshot: Test' and shows a 'Synchronization Status: Synchronized' with a 'Promote Changes' button. Below this is a 'CUSTOMER JOURNEY' tab bar with options: General, Ingress Rules, Application Groups, Interaction Flows, Modules, Entries/Intents, Functions (selected), Exits, and MORE. A '+ New' button is visible. The 'Functions' tab displays a table with columns: Function, Description, Function Group, and Region. The table contains two rows: 'sales' with description 'It's selling time' and 'support' with description '---'. Both functions are associated with 'herebeFunctionGroup' and 'South Carolina'. The table has a search bar and a '0 Functions selected' indicator. Below the table is a pagination bar showing '(Page 1 of 1)' and '25 rows/page'. At the bottom are 'Save' and 'Cancel' buttons.

Function	Description	Function Group	Region
sales	It's selling time	herebeFunctionGroup	South Carolina
support	---	herebeFunctionGroup	South Carolina

8.4. Administer Transfer VDNs and Skills

This section covers the configuration of the transfer VDNs and skills used for this sample contact center and call flows. From the ICX web interface, navigate to **Snapshots** and click on a snapshot as mentioned above. In **Managing Snapshot**, select the **Functions** tab. For the compliance test, two functions were created for *sales* and *support*. To configure the VDNs and skills for Sales, click on the *sales* function. The same procedure would be performed for the *support* Function, except that the transfer VDNs and skills would be different.

SWAMPFOX TECHNOLOGIES

Intelligent Customer Experience

ENVIRONMENT

ICX_DevConnect

Dashboard and Reports

System Dashboard

Contact Center Dashboard

Session Details Report

Custom Reports

Business Parameter Management

Manage Snapshots

Snapshots

Archived Snapshots

Assets

SCXML Dialogs

Global Announcement Sets

Recordings

Managing Snapshot: Test

Synchronization Status: Synchronized

Promote Changes

CUSTOMER JOURNEY

General

Ingress Rules

Application Groups

Interaction Flows

Modules

Entries/Intents

Functions

Exits

MORE

New

0 Functions selected

Duplicate

Delete

Hide Filter

Clear All Filters

Function

↓ ↑

Description

Function Group

Region

sales

It's selling time

herebeFunctionGroup

South Carolina

support

herebeFunctionGroup

South Carolina

(Page 1 of 1)

<<

<

1

>

>>

25

rows/page

Save

Cancel

In the **Function Properties** for *sales*, select the **Exits** tab. Exits specify where to route the call in a contact center. In this example, **Exits** are used to route calls to a transfer VDN that will connect the caller to a sales agent serving “Bronze” or “Gold” customers. The Exit for *salesBronze* is reviewed below.

The screenshot shows the 'Function Properties: Test > sales' configuration page in the ICX DevConnect application. The 'Exits' tab is active, showing a table of exits. The table has columns for 'Exit', 'Description', 'Channel', and 'Request Type'. Two exits are listed: 'salesBronze' and 'salesGold', both with a 'CALL' channel and 'Generic' request type. The interface includes a sidebar with navigation options like 'Dashboard and Reports', 'Business Parameter Management', and 'Manage Snapshots'. At the bottom, there are 'Save' and 'Cancel' buttons.

Exit	Description	Channel	Request Type
salesBronze	---	CALL	Generic
salesGold	---	CALL	Generic

The Exit for “Bronze” customers was configured as follows. In the **Routing** section, configure the following parameters:

- **Transfer VDN/Service:** Set to the transfer VDN associated with “Bronze” customers (e.g., 77812) contacting sales. Refer to **Section 5.4.2** for the VDN list relevant to this example call flow.
- **Route Point:** Specify the route point configured for the CTI connection in **Section 8.2**.

In the **Skills and DRM-to-DRM Stats** section, configure the following parameters:

- **Identifier:** Specify skill group number for the Sales Bronze group (i.e., 82) in **Section 5.4.1**.
- **Skill Extension:** Specify skill group extension for the Sales Bronze group (i.e., 77802) in **Section 5.4.1**.

Exit Properties: Test > sales > salesBronze

Routing

Transfer VDN/Service: 77812

Route Point: 2

Callback Queue for Route Point: None

Skills and DRM-to-DRM Stats

Enable DRM-to-DRM: ☐ Enabled ☒ Disabled

Table:

Identifier	Skill Extension	Description	Last Modified	Modified By
82	77802	---	09/12/2023 11:15:36 EDT	devconnect:192.168.100.251:icx:GUI

(Page 1 of 1) << < 1 > >> 25 rows/page

Buttons: Save, Cancel, Duplicate, Delete, Hide Filter, Clear All Filters, New

Scroll down to the **Queuing** section and configure the VDN for “Bronze” customers contacting Sales (i.e., 77812) in **Section 5.4.2**.

Exit Properties: Test > sales > salesBronze

General Routing Overrides

Queuing

+ New

Duplicate Delete Hide Filter Clear All Filters

VDN	Priority	Description	Last Modified	Modified By
77812	MEDIUM	---	09/12/2023 11:15:36 EDT	devconnect:192.168.100.251:icx:GUI

(Page 1 of 1) << < 1 > >> 25 rows/page

Save Cancel

Repeat the procedure above to add an exit for “Gold” customers contacting Sales, but specify the appropriate **Transfer VDN** and **Skill Extension** for Sales “Gold” customers.

8.5. Administer Call Routing based on ANI or DNIS

Incoming customer calls can be routed to appropriate agents/skills based on ANI or DNIS. For the compliance test, DNIS was used to route calls to specific snapshot. ANI was used to route calls to agents serving “Bronze” or “Gold” customers.

In the **Application Groups** tab within a **Snapshot** shown below, create a new Application Group (e.g., *Test*) and then click on it to specify whether to route calls based on ANI or DNIS.

The screenshot displays the Avaya DevConnect interface for managing a snapshot named 'Test'. The 'Application Groups' tab is selected, showing a table with the following data:

Priority	Application Group	Enabled	Locators	Resources
1	Test	✓	DNIS: 78560 Expression: true	

The interface also includes a sidebar with navigation options, a top bar with the environment name 'ICX_DevConnect', and a synchronization status of 'Synchronized'. The bottom of the page shows 'Save' and 'Cancel' buttons.

In **Application Groups Properties**, select the **Locators** tab as shown below. Add an entry that routes based on DNIS. In this example, the **Name** would be set to *dnisRegex.1* and **Value** would be set to match the dialed number (e.g., 78560). This would allow incoming calls with a matching DNIS to use this Snapshot. Alternatively, routing could also be based on ANI. For example, the **Name** would be set to *aniRegex.1* and **Value** would be an ANI, such as 17324441000. For the compliance test, routing based on ANI was handled in one of the application scripts.

The screenshot shows the 'Application Group Properties' dialog for 'Test > Test'. The 'Locators' tab is selected. Below the 'Type' dropdown (set to 'None'), there is a table of locators.

Name	Value	Enabled	Description	Remove Locator
dnisRegex.1	78560	<input checked="" type="checkbox"/> Enabled		
expression.1	true	<input checked="" type="checkbox"/> Enabled		

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

8.6. Promote Changes

Not all configuration changes take effect immediately. To push new data to Swampfox ICX server, promote the changes by clicking the **Promote Changes** button shown below.

SWAMPFOX TECHNOLOGIES
Intelligent Customer Experience

ENVIRONMENT
ICX_DevConnect

Managing Snapshot: Test Synchronization Status: ✔ Synchronized Promote Changes

CUSTOMER JOURNEY

General Ingress Rules Application Groups Interaction Flows Modules Entries/Intents Functions Exits MORE

0 Application Groups selected Duplicate Delete Hide Filter Clear All Filters

☐ Priority Application Group Enabled Locators

☐ 1 Test ☒ DNIS: 78560
Expression: true

(Page 1 of 1) << < 1 > >> 25 rows/page

Save Cancel

Swampfox Dynamic Route Manager



Dashboard Routing Rules Scripting Resources Recordings Vectors Staging Settings Utilities

DevConnect (Active - Priority 1) Logout

DRM Server Status

	Server	State	Health	Active Calls	Holding Calls	Rates (per minute)					WS Request	DRM Routing	Databases
						Received	Routed	Delivered	Other				
II	SWAMPFOX	RUNNING	HEALTHY	0.000	0.000	0.049	0.171	0.099	0.000	0.000	17.178	1.68	

Last Updated 03/29/2021 12:14:26 PM

Snapshot Status

		Name	Regions	Entries	Functions	Exits	Call Rate (per minute)	Calls Today	Status
Manage	Sync	DevConnect	1	4	2	4	0.000	7	Out of sync!
Manage	Sync	DevConnectAcme	1	4	2	4	0.000	0	Synchronized

9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, Avaya Experience Portal, and Swampfox ICX.

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the AES connection using the **status aesvcs interface** command.

```
status aesvcs interface
```

AE SERVICES INTERFACE STATUS			
Local Node	Enabled?	Number of Connections	Status
procr	yes	1	listening

Verify communication between Communication Manager and AES using the **status aesvcs link** command.

```
status aesvcs link
```

AE SERVICES LINK STATUS						
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	devcon-aes	10.64.102.119	61830	procr	2007	2564


Verify the status of the CTI link between Communication Manager and AES using the **status aesvcs cti-link** command. Verify the **Service State** is *established*.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	12	no	devcon-aes	established	1850	1850

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services Management Console, navigate to **Status → Status and Control → Switch Conn Summary**. Verify the Switch Connection to Communication Manager is *Talking* and *Online*.

**Application Enablement Services**
Management Console

Welcome: User cust
Last login: Fri Sep 15 11:17:15 E.S.T. 2023 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.3.1.0.49-0
Server Date and Time: Fri Sep 15 11:37:09 EDT 2023
HA Status: Not Configured

Status | Status and Control | Switch Conn SummaryHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Log Manager

▼ Status and Control

▪ CVLAN Service Summary

▪ DLG Services Summary

▪ DMCC Service Summary

▪ **Switch Conn Summary**

▪ TSAPI Service Summary


Switch Connections Summary

☐ Enable page refresh every 60 seconds

	Switch Conn	Conn State	Processor Ethernet	Since	Online/Offline	Active/Standby/Admin'd AEP Conns	Num of TCI Conns	SSL	Msgs To Switch	Msgs From Switch	Msg Period
<input checked="" type="radio"/>	devcon	Talking	Yes	Wed Sep 13 09:59:47 2023	Online	1 / 0 / 1	2	Enabled	2603	2042	30

OnlineOfflineConnection DetailsPer Service Connections Details

Navigate to **Status → Status and Control → TSAPI Service Summary** in the left pane. Verify the TSAPI link is *Talking* and *Online*.


Application Enablement Services
 Management Console

Welcome: User cust
 Last login: Fri Sep 15 11:17:15 E.S.T. 2023 from 192.168.100.250
 Number of prior failed login attempts: 0
 HostName/IP: devcon-aes/10.64.102.119
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.3.1.0.49-0
 Server Date and Time: Fri Sep 15 11:38:17 EDT 2023
 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
 - ▶ Logs
 - ▶ Log Manager
 - ▼ **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 CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
<input checked="" type="radio"/>	1	devcon	1	Talking	Wed Sep 13 09:59:48 2023	Online	20	8	1847	1847	30

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

Continuing from above, select **User Status**. Verify the swampfox user is connected to Application Enablement Services.


Application Enablement Services
 Management Console

Welcome: User cust
 Last login: Fri Sep 15 11:17:15 E.S.T. 2023 from 192.168.100.250
 Number of prior failed login attempts: 0
 HostName/IP: devcon-aes/10.64.102.119
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.3.1.0.49-0
 Server Date and Time: Fri Sep 15 11:39:19 EDT 2023
 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
 - ▶ Logs
 - ▶ Log Manager
 - ▼ **Status and Control**
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - **TSAPI Service Summary**

CTI User Status

☐ Enable page refresh every 60 seconds

CTI Users All Users

Open Streams 3
Closed Streams 5

Open Streams

Name	Time Opened	Time Closed	Tlink Name
swampfox	Thu 14 Sep 2023 03:24:38 PM EDT		AVAYA#DEVCON#CSTA-S#DEVCON-AES
DMCCLCSUserDoNotModify	Wed 13 Sep 2023 10:01:15 AM EDT		AVAYA#DEVCON#CSTA#DEVCON-AES
DMCCLCSUserDoNotModify	Wed 13 Sep 2023 10:01:15 AM EDT		AVAYA#DEVCON#CSTA#DEVCON-AES

9.3. Verify Swampfox ICX

Verify that **Contact Center Dashboard** reflects the accurate agent states as shown below.

The screenshot displays the Swampfox ICX Contact Center Dashboard. The interface includes a sidebar with navigation options, a top header with the logo and environment name, and a main content area with tabs for different summary views. The 'Realtime Function Summary' tab is active, showing a table of agent states.

SWAMPFOX TECHNOLOGIES
Intelligent Customer Experience

ENVIRONMENT
ICX_DevConnect

Contact Center Dashboard

Snapshot Summary | **Realtime Function Summary** | Historical Function Summary

Last Refresh: 9/13/2023, 4:04:48 PM EDT ☐ Freeze [Columns](#)

Filter By [Clear Filters](#)

Function Group: Function: Region: Exit: Channel:

Action: Transfer Point:

Region	Exits	Status	EWT	Agents Avail.	Staffed	In Queue	Serviced	Action
SC	2		0:00	0	2	1	0	
SC	salesBronze	OPEN	0:08	0	1	1	0	77812
SC	salesGold	OPEN	0:00	0	1	0	0	77811

(Page 1 of 1) << < 1 > >> 25 rows/page

Place a call to the Swampfox ICX application on Experience Portal and route the call to an agent. Verify in the Swampfox ICX reports that the call was handled as expected. Navigate to **Session Details Report** and then click **Build Report** to generate a report with recent call log.

The screenshot displays the Swampfox ICX application interface. The top header shows the Swampfox Technologies logo and the environment name 'ICX_DevConnect'. The sidebar on the left contains navigation options: Dashboard and Reports, System Dashboard, Contact Center Dashboard, Session Details Report (highlighted), Custom Reports, Business Parameter Management, Manage Snapshots, Snapshots, Archived Snapshots, Assets, SCXML Dialogs, Global Announcement Sets, Recordings, Scripts, Contact Center Management, and Route Points.

The main content area is titled 'Session Details Report'. It features a filter section with the following options:

- Time: Last 15 Minutes (dropdown)
- Only Completed Calls: Disabled (radio button)
- Snapshot: -Select One or More (dropdown)
- More Filters... (dropdown)

Below the filters are two buttons: 'Build Report' and 'Reset Filters'.

The search results section shows '19 Records Found'. It includes an 'Export' button and a 'Columns' button. The table below lists the search results:

	Receive Time	UCID	Entry/Intent	DNIS	ANI	Function	Request Type
Details	09/13/2023 16:18:22 EDT	00027141361694657902	supportEntry	78560	17324441000	support	Generic
Details	09/13/2023 16:17:44 EDT	00027141331694657864	supportEntry	78560	17324441001	support	Generic
Details	09/13/2023 16:17:03 EDT	00027141301694657822	supportEntry	78560	78002	support	Generic
Details	09/13/2023 16:15:24 EDT	00027141101694657723	salesEntry	78560	17324441000	sales	Generic
Details	09/13/2023 16:11:10 EDT	00027140921694657469	salesEntry	78560	78002	sales	Generic
Details	09/13/2023 16:10:39 EDT	00027140911694657439	78560	78560	17324441000		

10. Conclusion

These Application Notes describe the steps required to integrate Swampfox ICX with Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, and Avaya Experience Portal. Customer calls were routed to the appropriate agents/skill groups based on the ANI or DNIS by Swampfox ICX. All tests passed.

11. Additional References

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

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 6, June 2023, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 8, August 2023, available at <http://support.avaya.com>.
- [3] *Administering Avaya Experience Portal*, Release 8.1.2, Issue 1, October 2022, available at <http://support.avaya.com>.
- [4] *Swampfox Intelligent Customer Experience User Support Manual*, Version 4.0, available from Swampfox.

©2023 Avaya LLC. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.