



Avaya Solution & Interoperability Test Lab

Application Notes for NICE Engage Platform 6.15 with Avaya Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for NICE Engage Platform 6.15 to interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 8.1. NICE Engage Platform is a call recording solution.

In the compliance testing, NICE Engage Platform used the Event Services interface from Avaya Proactive Contact to obtain information on calls and agent states, and used the Multiple Registration feature from the Avaya Aura® Application Enablement Services Device, Media, and Call Control interface to capture media associated with the agent stations for call recording.

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 NICE Engage Platform (Engage) 6.15 to interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 8.1. Engage is a call recording solution.

In the compliance testing, Engage used the Event Services interface from Proactive Contact to obtain information on calls and agent states, and used the Multiple Registration feature from the Application Enablement Services Device, Media, and Call Control (DMCC) .XML interface to capture media associated with the agent stations for call recording.

The DMCC interface is used by Engage to register a virtual IP softphone against each agent station to pick up the media for call recording. When there was an active call at the agent station, Engage is informed of the call via events from the Event Services interface and starts the call recording by use of media from the associated virtual IP softphone. The Event Services events are also used to determine when to stop the call recordings.

Engage can be deployed with distributed components across multiple servers. The compliance testing used two Engage servers in the test configuration – one server running the Application Server, Database Server, and Interactions Center components, and the other server running the Advanced Interaction Recorder component. The Application Server component is responsible for the Engage web interface, the Interactions Center component is responsible for Event Services connection with Proactive Contact, and the Advanced Interaction Recorder component is responsible for DMCC connection with Application Enablement Services.

The compliance testing covered the recording of outbound and inbound calls that were delivered by Proactive Contact for the PG230 deployment option. The recording of inbound calls delivered by Communication Manager under the agent blending mode is outside the scope of this compliance test.

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the Engage application, the application automatically established Event Services connection with Proactive Contact and DMCC connection with Application Enablement Services.

For the manual part of testing, each call was handled manually at the agent with generation of unique audio content for recording. Necessary agent actions such as forward work and release line were performed from the Proactive Contact Agent application running on the agent desktops to test various call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to Engage.

The verification of tests included use of Engage logs for proper message exchanges and use of Engage web interface for proper logging and playback of call recordings.

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 these DevConnect Application Notes 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 interfaces between Engage and Avaya products included encrypted Event Services and DMCC connections.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Engage:

- Handling of Event Services agent states and call events.
- Use of DMCC registration services to register virtual IP softphones.
- Use of DMCC device services and media control events to obtain media from the virtual IP softphones.
- Proper recording, logging, and playback of calls for scenarios involving agent drop, customer drop, hold, reconnect, simultaneous calls, forward work, long duration, multiple agents, manual call, inbound call blending, outbound call blending, and outbound agent blending scenarios.

The serviceability testing focused on verifying the ability of Engage to recover from adverse conditions, such as disconnecting and reconnecting the Ethernet connection to Engage.

2.2. Test Results

All test cases were executed and verified. The following were the observations on Engage from the compliance testing.

- Recording of supervised forward work with conference scenarios are not supported in this release of Engage.
- In the unsupervised forward work scenario, the recording entry for the forward-from agent reported a hold count of “1”, and the recording entry for the forward-to agent reported direction of “Outgoing”.
- In the supervised forward work with transfer scenario, the recording entry for the forward-from agent reported values for hold count and hold duration. In addition, the conversation between the forward-to agent with the PSTN is part of the complete call entry for the forward-from agent.

2.3. Support

Technical support on Engage can be obtained through the following:

- **Web :** <http://www.extranice.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 Proactive Contact, between Communication Manager and Application Enablement Services, and of call center devices are not the focus of these Application Notes and will not be described.

The agent station extensions used in the compliance testing are shown in the table below.

Device Type	Extension
Agent Station	65001 (H.323), 66006 (SIP)

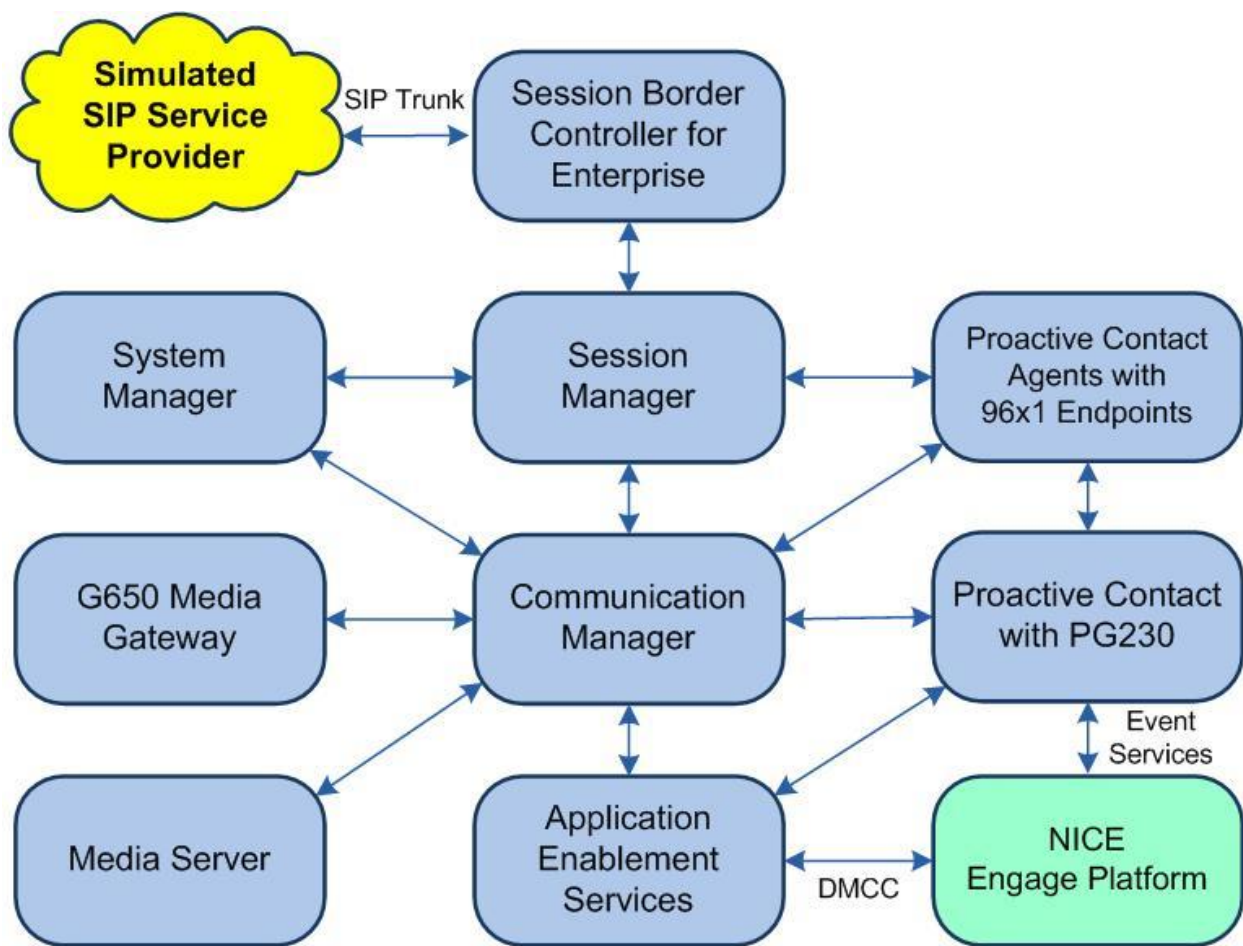


Figure 1: Compliance Testing Configuration

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 in Virtual Environment	8.1.1 (8.1.0.1.1.890.25763)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	8.0.1.121
Avaya Aura® Application Enablement Services in Virtual Environment	8.1.1 (8.1.1.0.1.8-0)
Avaya Aura® Session Manager in Virtual Environment	8.1.1 (8.1.1.0.811021)
Avaya Aura® System Manager in Virtual Environment	8.1.1 (8.1.1.0.0310912)
Avaya Proactive Contact	5.2.0.1
Avaya Proactive Contact Agent	5.2.0.1
Avaya 9611G IP Deskphone (H.323)	6.8202
Avaya 9641G IP Deskphone (SIP)	7.1.6.1.3
NICE Engage Platform on Windows Server 2016 <ul style="list-style-type: none"> Application Server Interactions Center Database Server Avaya Proactive Contact Event SDK 	6.15.0001.77 Standard 5.1.2
NICE Engage Platform on Windows Server 2016 <ul style="list-style-type: none"> Advanced Interaction Recorder Avaya DMCC XML 	6.15.0001.77 Standard 7.0.0.38

5. Configure Avaya Aura® Communication Manager

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

- Administer IP codec set
- Administer agent station

5.1. Administer Codec Set

Use the “change ip-codec-set n” command, where “n” is an existing codec set number used for integration with Engage. For **Audio Codec**, enter the relevant codec.

In the compliance testing, “G.711MU” and “G.729” were configured, and this codec set was used by the agent stations.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size (ms)
1: G.711MU          n           2         20
2: G.729           n           2         20
3:
4:
5:
6:
7:

Media Encryption                                Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: aes
3: none
4:
```

5.2. Administer Agent Station

Use the “change station n” command, where “n” is the first non-SIP agent station extension from **Section 3**. Enable **IP SoftPhone** to allow a virtual IP softphone to be registered against the station. Note the value of **Security Code**, which will be used later to configure Engage.

Repeat this section to administer all non-SIP agent stations from **Section 3**. In the compliance testing, one agent station was administered.

change station 65001	Page 1 of 5
STATION	
Extension: 65001	Lock Messages? n
Type: 9611	Security Code: 65001
Port: S000103	Coverage Path 1: 1
Name: CM Station 1	Coverage Path 2:
Unicode Name? n	Hunt-to Station:
STATION OPTIONS	
Loss Group: 19	Time of Day Lock Table:
Speakerphone: 2-way	Personalized Ringing Pattern: 1
Display Language: english	Message Lamp Ext: 65001
Survivable GK Node Name:	Mute Button Enabled? y
Survivable COR: internal	Button Modules: 0
Survivable Trunk Dest? y	Media Complex Ext:
	IP SoftPhone? y
	IP Video Softphone? n
	Short/Prefixed Registration Allowed: default
	Customizable Labels? y

6. Configure Avaya Aura® Application Enablement Services

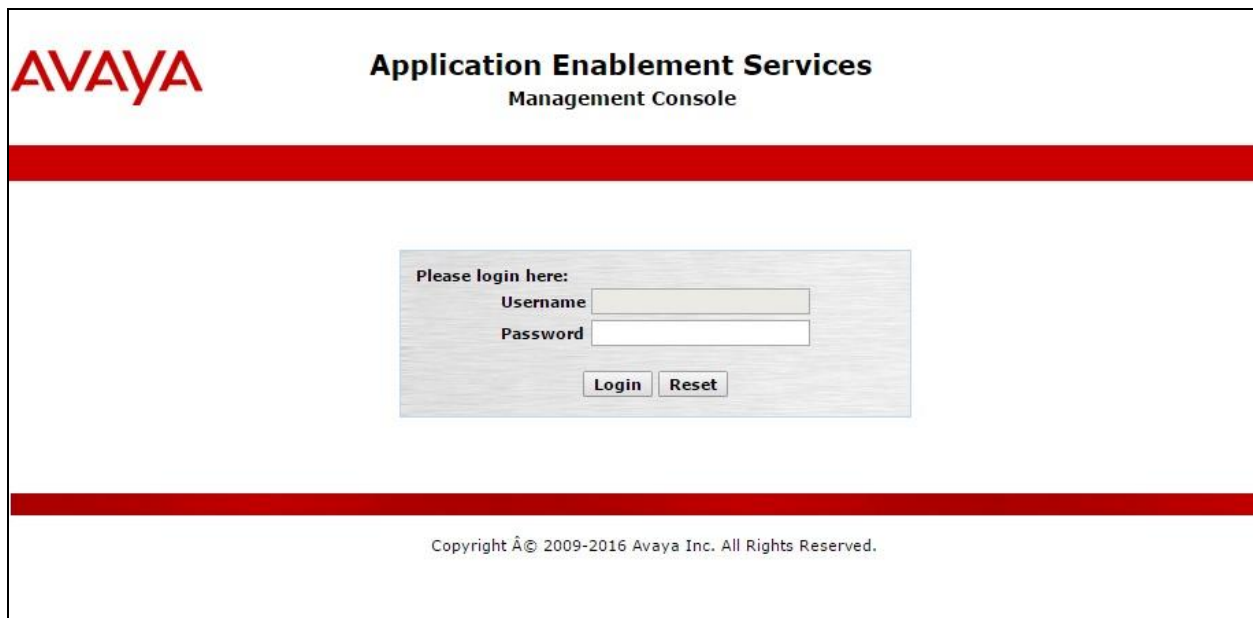
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer H.323 gatekeeper
- Administer NICE user
- Administer security database
- Administer ports
- Restart services
- Export CA certificate

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



The screenshot shows the Avaya Application Enablement Services Management Console login page. 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 thick red horizontal bar spans the width of the page below the header. In the center of the page is a light gray rectangular box containing the login form. The form has the text "Please login here:" followed by two input fields: "Username" and "Password". Below these fields are two buttons: "Login" and "Reset". Another thick red horizontal bar is located at the bottom of the page, just above the footer. The footer text at the very bottom reads: "Copyright © 2009-2016 Avaya Inc. All Rights Reserved."

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 and the title "Application Enablement Services Management Console". A user welcome message is shown in the top right corner, indicating the user is logged in from 192.168.200.20. The left sidebar contains a navigation menu with options: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area displays the "Welcome to OAM" message, which states that the OAM Web provides tools for managing the AE Server and lists the 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.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Thu Jan 23 13:07:59 2020 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.1.8-0
Server Date and Time: Thu Jan 23 14:23:22 EST 2020
HA Status: Not Configured

Home | Help | Logout

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 applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected in the left sidebar. The main content area displays the "Licensing" message, which provides instructions for setting up and maintaining the WebLM, importing and setting up the license, and administering TSAPI Reserved Licenses or DMCC Reserved Licenses. The left sidebar shows the navigation menu with "Licensing" selected, and sub-options: WebLM Server Address, WebLM Server Access, and Reserved Licenses.

AVAYA Application Enablement Services Management Console

Welcome: User
Last login: Thu Jan 23 13:07:59 2020 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.1.8-0
Server Date and Time: Thu Jan 23 14:23:22 EST 2020
HA Status: Not Configured

Licensing | Home | Help | Logout

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

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

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 is sufficient license for **Device Media and Call Control** as shown below.

AVAYA
Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ | Widgets ▾ Shortcuts ▾

Home User Management Licenses

L...

- WebLM Home
- Install license
- Licensed products
- APPL_ENAB
 - Application_Enablement
 - View by feature
 - View by local WebLM
 - Enterprise configuration
 - Local WebLM Configuration
 - Usages
 - Allocations
 - Periodic status
 - ASBCE
 - Session_Border_Controller_E_AE
 - CCTR
 - ContactCenter
 - COMMUNICATION_MANAGER
 - Call_Center
 - Communication_Manager
 - MESSAGING
 - Messaging
 - MSR
 - Media_Server
 - SYSTEM_MANAGER
 - System_Manager
 - SessionManager

Application Enablement (CTI) - Release: 8 - SID: 10503000(Enterprise)

You are here: Licensed Products > Application_Enablement > View by Feature

License installed on: August 8, 2019 4:43:51 PM -05:00

License File Host IDs:	VE-83-02-2D-26-52-01
Active License Mode	Standard
License State	NA
Pay Per Use License Available	No
Standard License Available	Yes

Feature (License Keyword)	License Capacity	Currently available
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3	3
DLG (VALUE_AES_DLG)	16	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000	1000

6.3. Administer H.323 Gatekeeper

Select **Communication Manager Interface** → **Switch Connections** from the left pane. The **Switch Connections** screen shows a listing of the existing switch connections.

Locate the connection name associated with the relevant Communication Manager, in this case “cm7”, and select the corresponding radio button. Click **Edit H.323 Gatekeeper**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays the 'Switch Connections' screen. At the top right, a welcome message for 'User' is shown, including the last login time (Thu Jan 23 13:07:59 2020) and other system information. Below the navigation pane, there is a table of switch connections. The table has four columns: 'Connection Name', 'Processor Ethernet', 'Msg Period', and 'Number of Active Connections'. The first row shows 'cm7' with 'Yes' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table, there are buttons for 'Edit Connection', 'Edit PE/CLAN IPs', 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm7	Yes	30	1

The **Edit H.323 Gatekeeper** screen is displayed next. Enter the IP address of a C-LAN circuit pack or the Processor C-LAN on Communication Manager to use as the H.323 gatekeeper, in this case “10.64.101.236” as shown below. Click **Add Name or IP**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Communication Manager Interface' and 'Switch Connections'. The main content area displays the 'Edit H.323 Gatekeeper - cm7' screen. At the top right, a welcome message for 'User' is shown, including the last login time (Thu Jan 23 13:07:59 2020) and other system information. Below the navigation pane, there is a form for editing the H.323 Gatekeeper. The form has a text input field containing '10.64.101.236' and a button labeled 'Add Name or IP'. Below the input field, there are buttons for 'Delete IP' and 'Back'.

6.4. Administer NICE 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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text 'Application Enablement Services Management Console'. A welcome message in the top right corner states: 'Welcome: User', 'Last login: Thu Jan 23 13:07:59 2020 from 192.168.200.20', 'Number of prior failed login attempts: 0', 'HostName/IP: aes7/10.64.101.239', 'Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE', 'SW Version: 8.1.1.0.1.8-0', 'Server Date and Time: Thu Jan 23 14:23:22 EST 2020', and 'HA Status: Not Configured'. A red navigation bar contains the links 'User Management | User Admin | Add User' and 'Home | Help | Logout'.

The left sidebar shows a tree view of the management console. The 'User Management' section is expanded, showing 'Service Admin' and 'User Admin'. Under 'User Admin', the 'Add User' option is selected.

The main content area displays the 'Add User' form. It includes a warning: 'Fields marked with * can not be empty.' The form fields are as follows:

- * User Id: nice
- * Common Name: nice
- * Surname: nice
- * User Password:
- * Confirm Password:
- Admin Note: (empty text box)
- Avaya Role: None (dropdown menu)
- Business Category: (empty text box)
- Car License: (empty text box)
- CM Home: (empty text box)
- Css Home: (empty text box)
- CT User: Yes (dropdown menu)
- Department Number: (empty text box)
- Display Name: (empty text box)
- Employee Number: (empty text box)
- Employee Type: (empty text box)
- Enterprise Handle: (empty text box)
- Given Name: (empty text box)

6.5. Administer 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.

Make certain both parameters are unchecked, as shown below.

In the event that the security database is used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the NICE user from **Section 6.4**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the title "Application Enablement Services Management Console". A welcome message in the top right corner provides user information: "Welcome: User", "Last login: Thu Jan 23 13:07:59 2020 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes7/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 8.1.1.0.1.8-0", "Server Date and Time: Thu Jan 23 14:23:22 EST 2020", and "HA Status: Not Configured".

The main navigation pane on the left lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, and Security. The Security section is expanded, showing sub-items: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, and Control. The Control item is selected and highlighted.

The main content area displays the "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services" configuration page. It contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". Below these checkboxes is an "Apply Changes" button.

6.7. Restart Services

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane.

Check **DMCC Service** and select **Restart Service**.

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 navigation pane shows a tree structure with "Maintenance" selected, and "Service Controller" highlighted. The main content area shows the "Service Controller" page with a table of services and their status. The "DMCC Service" is checked, and the "Restart Service" button is visible.

Welcome: User
Last login: Thu Jan 23 13:07:59 2020 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.1.8-0
Server Date and Time: Thu Jan 23 14:23:22 EST 2020
HA Status: Not Configured

Maintenance | Service Controller [Home](#) | [Help](#) | [Logout](#)

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 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](#)

6.8. Export CA Certificate

Select **Security** → **Certificate Management** → **CA Trusted Certificates** from the left pane, to display the **CA Trusted Certificates** screen in the right pane.

Select the pertinent CA certificate, in this case “SystemManagerCA”, and click **Export**.

AVAYA

Application Enablement Services
Management Console

Welcome: User
Last login: Thu Jan 23 13:07:59 2020 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.1.8-0
Server Date and Time: Thu Jan 23 14:23:22 EST 2020
HA Status: Not Configured

Security | Certificate Management | CA Trusted Certificates

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▼ Certificate Management

▪ CA Trusted Certificates

CA Trusted Certificates

View Import Export Delete

Alias	Status	Issued To	Issued By	Expiration Date
<input type="radio"/> serverCertDefault	valid	aes7-081738682-labUseOnly	aes7-081738682-labUseOnly	Aug 5, 2020
<input type="radio"/> avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	Aug 14, 2033
<input type="radio"/> avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	Aug 17, 2027
<input checked="" type="radio"/> SystemManagerCA	valid	System Manager CA	System Manager CA	Oct 8, 2028

The **Trusted Certificate Export** screen is displayed. Select and copy everything from the **BEGIN CERTIFICATE** to the **END CERTIFICATE** (not shown) lines. Paste the copied content to a Notepad file and save with a desired file name such as “caSMGR.crt”.

This CA certificate needs to be installed on Engage for establishment of encrypted DMCC connection with Application Enablement Services.

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 menu on the left lists various services, with "Security" expanded to show "Certificate Management". The "Trusted Certificate Export" screen is active, displaying the following information:

- Issued To:** System Manager CA
- Issued By:** System Manager CA
- Expiration Date:** Oct 8, 2028
- Certificate PEM:**

The Certificate PEM content is displayed in a text area, starting with "-----BEGIN CERTIFICATE-----" and ending with "-----END CERTIFICATE-----". The text is as follows:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBGGA1UEAwwRU3lzdG
IE1hbmFnZXIgaXQ0ExDTALBgNVBAsMIBE1HTVQxDjAMBgNVBAoMBUFWQVVBMB4XDTE4MTAxMTE4
NFoXDTI4MTAwODE4MTU0NFowOzEaMBGGA1UEAwwRU3lzdGVtIE1hbmFnZXIgaXQ0ExDTALBgNVB
BE1HTVQxDjAMBgNVBAoMBUFWQVVBMB4XDTE4MTAxMTE4NFoXDTI4MTAwODE4MTU0NFowOzEaMB
blFeekVIOePXG46TdUR7LjYz1NjkmBCp+vf/rLbyy8u+yO6YT9ZGzpaJxeyJJwZgOKSJrgdkvvv2
RWmi71UICM73wyTBQwpzK12HQ0OoS1ZAWjEwa/VuPQmbahGdC7UXO4DHMczzhekWhEOJjJ4
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6Wu03sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZYwIDAQABo2MwYTABBgNVHRMBAf8EBTADAQH/MB8G
IwQYMBaAFFojv4IgJO2AzKk709pJBI14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs
OTAOBgNVHQ8BAf8EBAMCAAYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptdFXjdeGUUxwC
VCrmwCz4z2V6QgmmRBBG2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttO
o8FQ6/chUYVCJfwrKqUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zn
m46H6SSivL7WDdowqlAxcVr4ScWghTpeeMBd1inp9R/e1bv0HK742oBATQGvem3rW36vRkUBaIc
-----END CERTIFICATE-----
```

A "Close" button is located at the bottom of the text area.

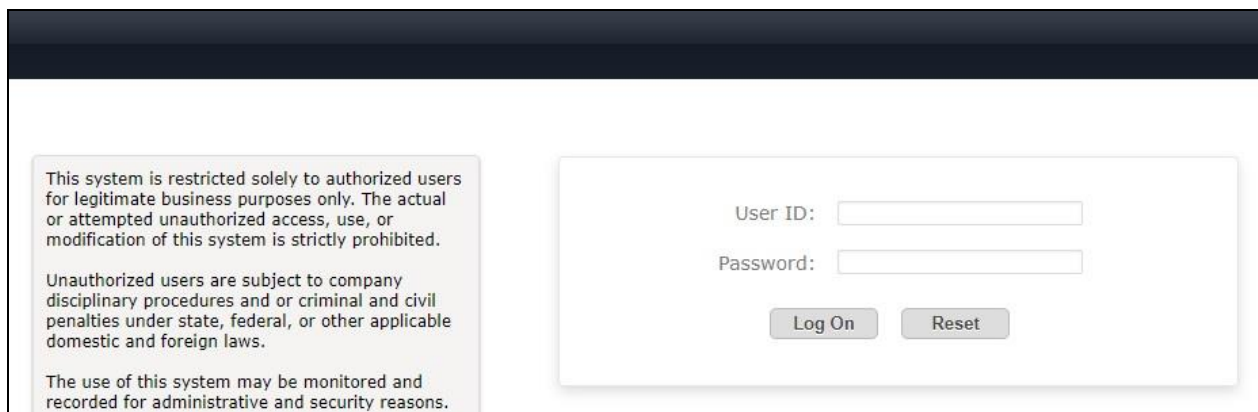
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

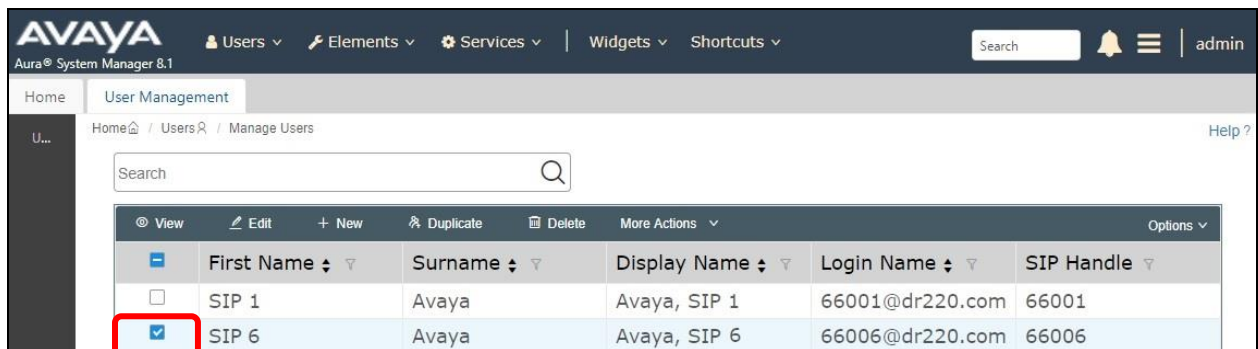
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



7.2. Administer Users

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

Select the entry associated with the first SIP agent station from **Section 3**, in this case “66006”, and click **Edit**.



View	Edit	New	Duplicate	Delete	More Actions	Options
<input type="checkbox"/>	SIP 1	Avaya	Avaya, SIP 1	66001@dr220.com	66001	
<input checked="" type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006	

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

For **Security Code**, enter a desired code, in this case “123456”. This security code is used for multiple registration authentication against a SIP endpoint when the security database is disabled in **Section 6.5**.

Click on the editor icon highlighted below.

The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled 'User Profile | Edit | 66006@dr220.com'. It features several tabs: Identity, Communication Profile, Membership, and Contacts. The 'Communication Profile' tab is selected, and within it, the 'CM Endpoint Profile' sub-tab is active. The 'Security Code' field is highlighted with a red box. The 'Extension' field also has a red box around its editor icon. Other fields include System (DR-CM), Profile Type (Endpoint), Set Type (9641SIFCC), Port (S000053), and Sip Trunk (aar).

Field	Value
System	DR-CM
Profile Type	Endpoint
Extension	66006
Set Type	9641SIFCC
Port	S000053
Sip Trunk	aar
Security Code

The popped-up screen below is displayed. Select the **General Options** tab, and set **Type of 3PCC Enabled** to “Avaya”.

The screenshot shows the Avaya Aura System Manager 8.1 User Management interface. The 'General Options (G)' tab is selected. The 'Type of 3PCC Enabled' dropdown menu is highlighted with a red box and set to 'Avaya'.

System	DR-CM	Extension	66006
Template	Select	Set Type	9641SIPCC
Port	S000053	Security Code	*****
Name	Avaya, SIP 6		

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Profile Settings (P)		Group Membership (M)	
* Class of Restriction (COR)	1	* Class Of Service (COS)	1				
* Emergency Location Ext	66006	* Message Lamp Ext.	66006				
* Tenant Number	1						
* SIP Trunk	Qaar						
Coverage Path 1		Type of 3PCC Enabled	Avaya				
		Coverage Path 2					

Select the **Feature Options** tab, and check **IP Softphone**.

Repeat this section to administer all SIP agent user from **Section 3**. In the compliance testing, one agent user was administered.

The screenshot shows the Avaya Aura System Manager 8.1 User Management interface. The 'Feature Options (F)' tab is selected. The 'IP SoftPhone' checkbox is highlighted with a red box and checked.

General Options (G) *		Feature Options (F)		Site Data (S)		Abbreviated Call Dialing (A)	
Enhanced Call Fwd (E)		Button Assignment (B)		Profile Settings (P)		Group Membership (M)	
Active Station Ringing	single	Auto Answer	none				
MWI Served User Type	None	Coverage After Forwarding					
Per Station CPN - Send Calling Number	None	Display Language	english				
IP Phone Group ID		Hunt-to Station					
Remote Soft Phone Emergency Calls	as-on-local	Loss Group	19				
LWC Reception	spe	Survivable COR	internal				
AUDIX Name	None	Time of Day Lock Table	None				
Short/Prefixed Registration Allowed	default	Music Source					
Voice Mail Number							
Bridging Tone for This Extension	no						
Features		<input type="checkbox"/> Idle Appearance Preference <input checked="" type="checkbox"/> IP SoftPhone <input checked="" type="checkbox"/> LWC Activation					
<input type="checkbox"/> Always Use <input type="checkbox"/> IP Audio Hairpinning <input type="checkbox"/> Bridged Call Alerting							

8. Configure Avaya Proactive Contact

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

- Obtain host name
- Obtain permission files

8.1. Obtain Host Name

Log in to the Linux shell of the Proactive Contact server. Use the “hostname” command to obtain the host name, which will be used later to configure Engage.

In the compliance testing, the host name of the Proactive Contact server is “lzpds4b”, as shown below.

```
$ hostname  
lzpds4b
```

8.2. Obtain Permission Files

Use a tool such as WinSCP, to copy the following permission files from the Proactive Contact server, which will be used later to configure Engage.

- /opt/avaya/pds/openssl/certificate/corbaServer_cert.pem
- /opt/avaya/pds/openssl/certificate/ProactiveContactCA.pem
- /opt/avaya/pds/openssl/private/corbaServer_key.pem

9. Configure NICE Engage Platform

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

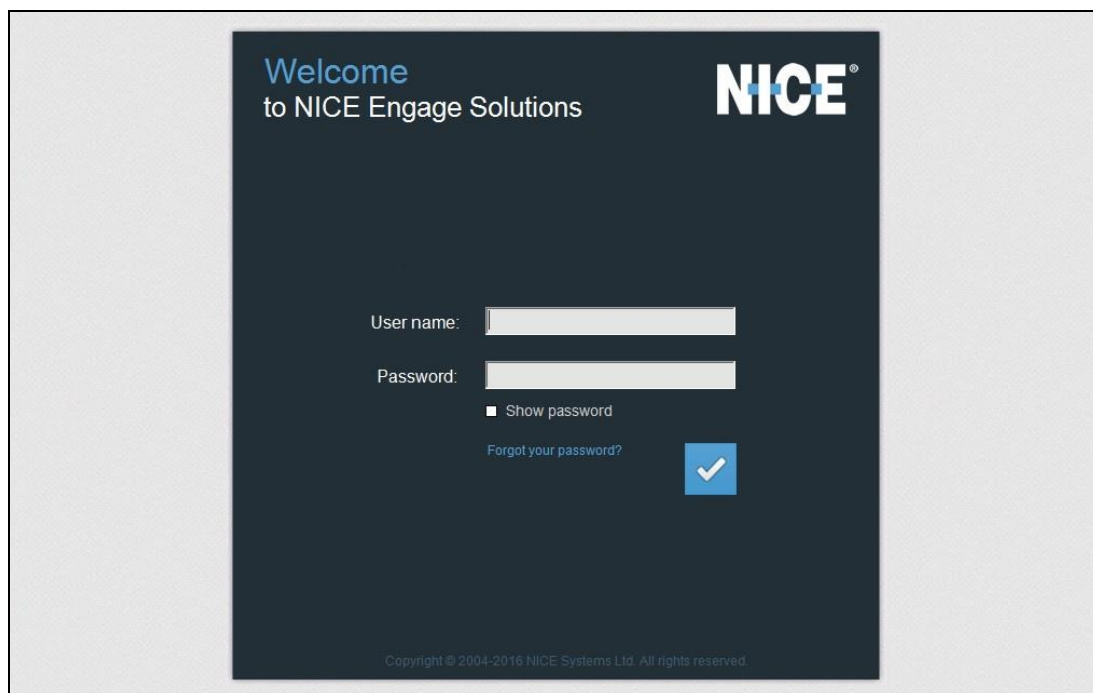
- Launch Engage web interface
- Administer CTI for PC
- Administer CTI for AES
- Administer Interactions Center
- Administer certificates
- Restart services
- Administer system mapping
- Administer agent users

The configuration of Engage is performed by NICE engineers. The procedural steps are presented in these Application Notes for informational purpose.

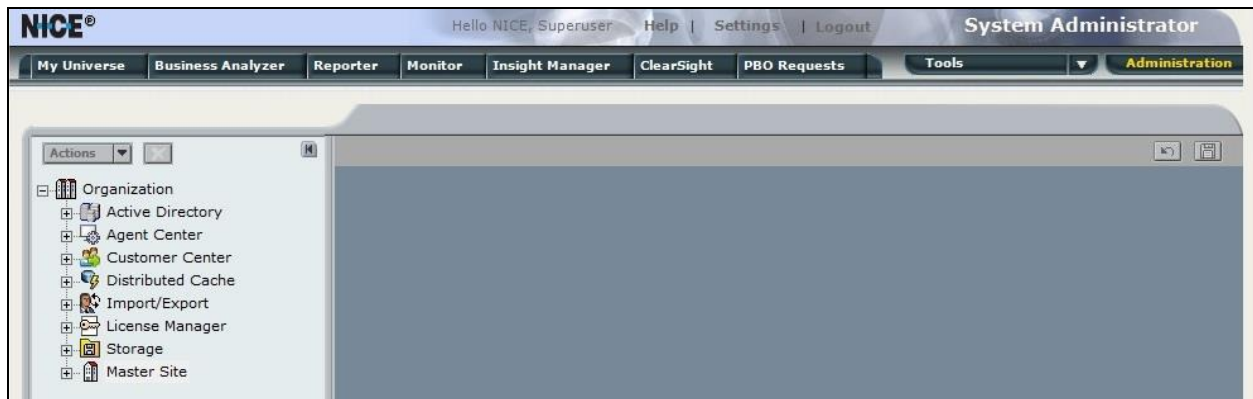
Prior to configuration, a pertinent interactions center is assumed to be pre-configured, and with TLS 1.2 enabled on the server running the Advanced Interaction Recorder component.

9.1. Launch Engage Web Interface

Access the Engage web interface by using the URL “http://hostname/nice” in an Internet Explorer browser window, where “hostname” is the host name of the Engage server with the Application Server component. The **Welcome** screen below is displayed. Log in using the appropriate credentials.

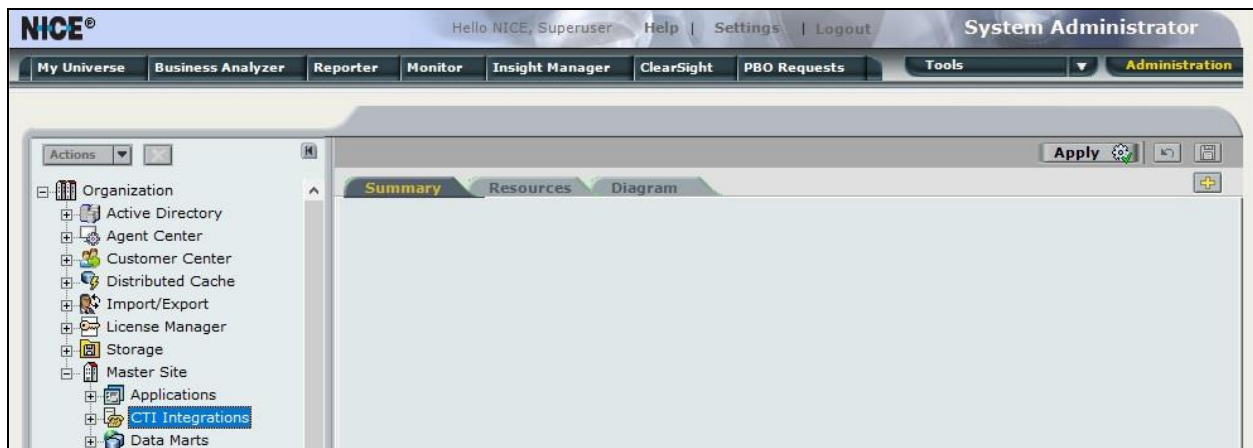


The **NICE** screen below is displayed next. Select **Administration** → **System Administrator** followed by **Settings** → **Technician Mode** from the top menu.

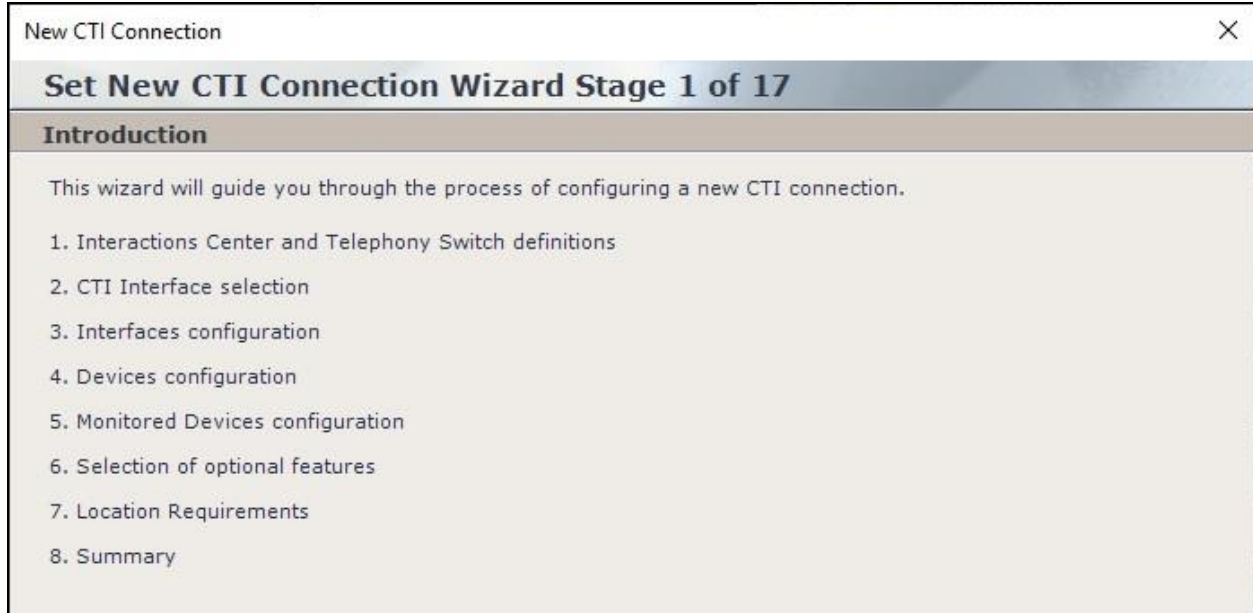


9.2. Administer CTI for PC

Expand **Organization** → **Master Site** as shown below. Right click on **CTI Integrations** and select **New CTI Connection** to add a connection with Proactive Contact.



The **New CTI Connection** pop-up screen is displayed. Click **Next** (not shown).



New CTI Connection

Set New CTI Connection Wizard Stage 1 of 17

Introduction

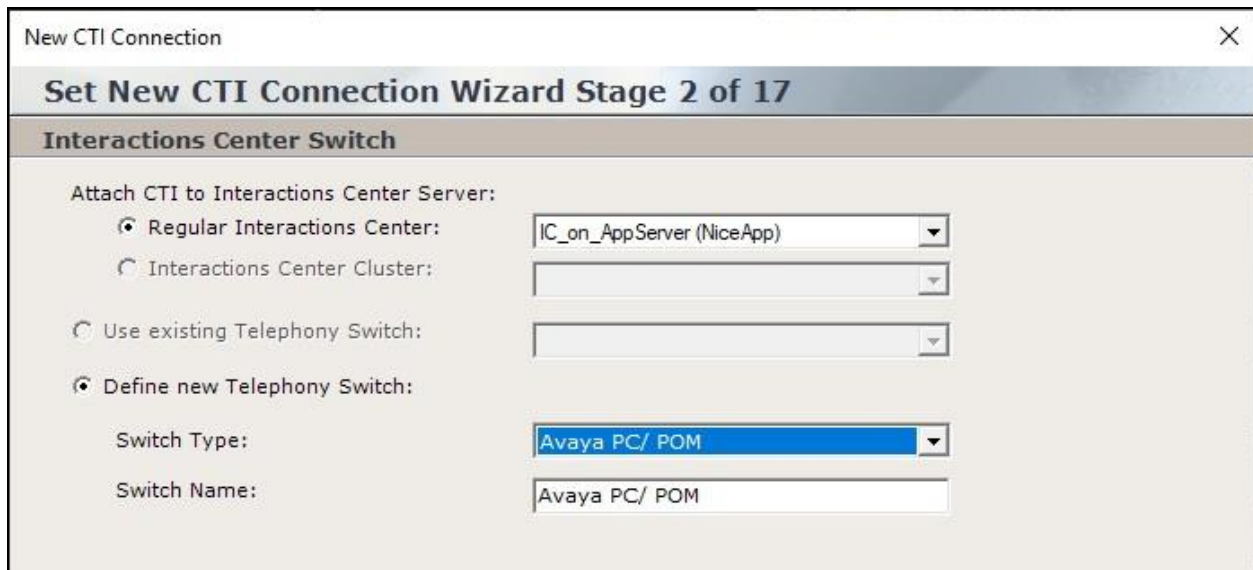
This wizard will guide you through the process of configuring a new CTI connection.

1. Interactions Center and Telephony Switch definitions
2. CTI Interface selection
3. Interfaces configuration
4. Devices configuration
5. Monitored Devices configuration
6. Selection of optional features
7. Location Requirements
8. Summary

The **Stage 2** screen is displayed as shown below.

For **Regular Interactions Center**, select the pertinent center, in this case “IC_on_AppServer (NiceApp)” which was pre-configured.

For **Switch Type**, select “Avaya PC/ POM”, which auto populates **Switch Name** with the same value.



New CTI Connection

Set New CTI Connection Wizard Stage 2 of 17

Interactions Center Switch

Attach CTI to Interactions Center Server:

☒ Regular Interactions Center: IC_on_AppServer (NiceApp)

☐ Interactions Center Cluster:

☐ Use existing Telephony Switch:

☒ Define new Telephony Switch:

Switch Type: Avaya PC/ POM

Switch Name: Avaya PC/ POM

Proceed to **Stage 3**. Retain “Event Service” as the default value for **Avaya PC/ POM CTI Interface** as shown below.

New CTI Connection

Set New CTI Connection Wizard Stage 3 of 17

Interface Type

CTI Interface Type

Avaya PC/ POM CTI Interface: **Event Service**
Avaya Proactive Contact / Avaya Proactive Outreach Manager Event Service

☐ VolP Mapping:

☐ Active Recording:

Proceed to **Stage 4**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **AvayaPD Version:** The closest version number, in this case “PC512”.
- **Event Service Host Name:** The Proactive Contact host name from **Section 8.1**.
- **Naming Service Host Name:** The Proactive Contact host name from **Section 8.1**.
- **AvayaPD Client Username:** The Proactive Contact Event Service client credentials.
- **AvayaPD Client Password:** The Proactive Contact Event Service client credentials.

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 17

Interface Parameters

CTI Interface Details

Interface Connection Details

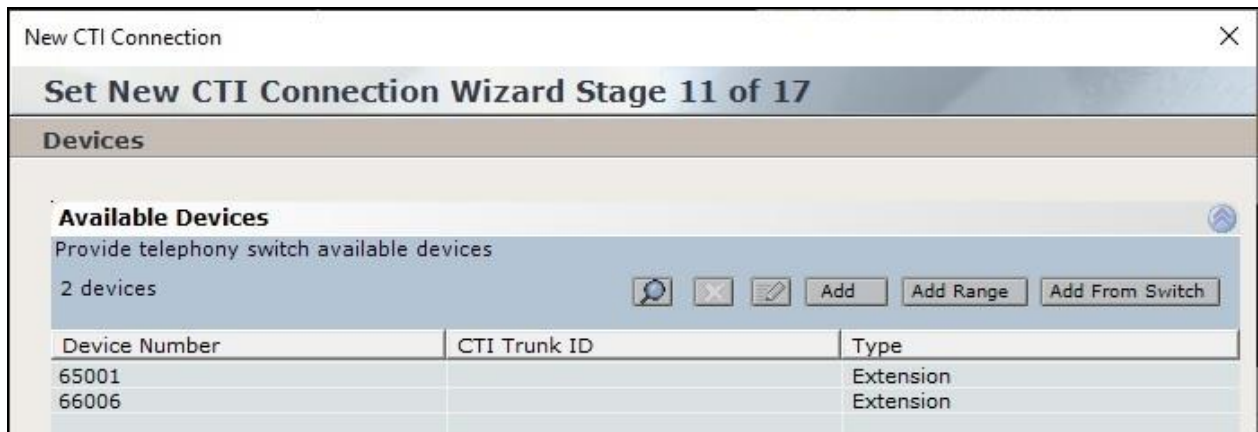
Mandatory fields are marked in bold

Parameter	Value
AvayaPD Version	PC512
Event Service Host Name	lzpds4b
Naming Service Host Name	lzpds4b
AvayaPD Client Username	client 1
AvayaPD Client Password	*****
Client Port ID	6666

Description: Avaya PC Client Password - The CTILink will use this parameter in order to login to the Avaya PC server.

Additional Interface Parameters

Proceed to **Stage 11**. Select **Add** to add a device entry for each agent station extension from **Section 3**. Set **Device Number** to the agent station extension and **Type** to “Extension” as shown below.



New CTI Connection

Set New CTI Connection Wizard Stage 11 of 17

Devices

Available Devices

Provide telephony switch available devices

2 devices

Device Number	CTI Trunk ID	Type
65001		Extension
66006		Extension

Proceed to **Stage 13**, and check **Call Flow Analysis**.

Proceed to complete the wizard.



New CTI Connection

Set New CTI Connection Wizard Stage 13 of 17

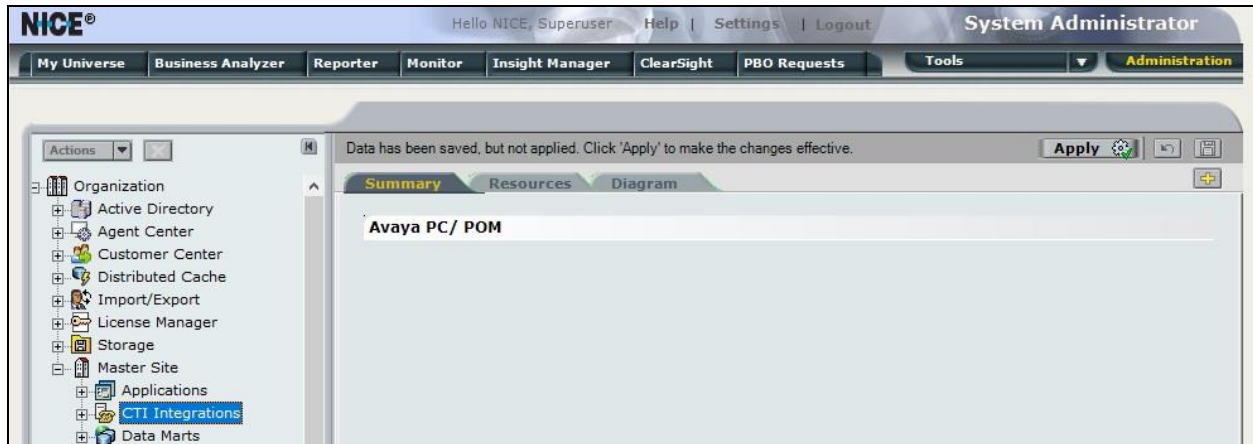
Optional

Select optional features relevant to integration. Some options may require further configuration.

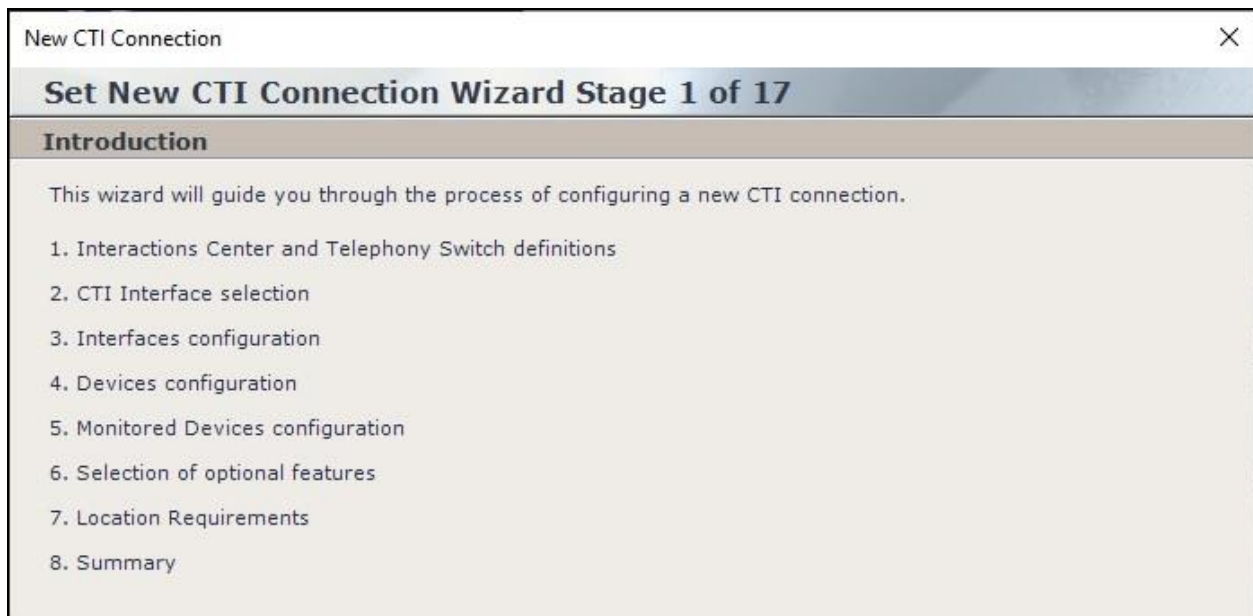
- ☐ SIP Trunk Correlation
- ☐ AOD VRSP Correlation
- ☐ Rejected Devices
- ☐ Filter Calls
- ☒ Call Flow Analysis

9.3. Administer CTI for AES

The NICE screen is updated to reflect the newly added CTI connection as shown below. Right click on **CTI Integrations** again and select **New CTI Connection** to add a connection with Application Enablement Services.



The **New CTI Connection** pop-up screen is displayed as shown below. Click **Next** (not shown).



The **Stage 2** screen is displayed. For **Regular Interactions Center**, select the pertinent center, in this case “IC_on_AppServer (NiceApp)” which was pre-configured.

For **Switch Type**, select “Avaya CM”, which auto populates **Switch Name** with the same value.

New CTI Connection

Set New CTI Connection Wizard Stage 2 of 17

Interactions Center Switch

Attach CTI to Interactions Center Server:

- ☒ Regular Interactions Center: IC_on_AppServer (NiceApp)
- ☐ Interactions Center Cluster:

☐ Use existing Telephony Switch: Avaya PC/ POM

☒ Define new Telephony Switch:

Switch Type: Avaya CM

Switch Name: Avaya CM

Proceed to **Stage 3**. For **Avaya CM CTI Interface**, select “AES TSAPI”.

Check **Active Recording** and select “DMCC (Advanced Interaction Recorder)” as shown below.

New CTI Connection

Set New CTI Connection Wizard Stage 3 of 17

Interface Type

CTI Interface Type

Avaya CM CTI Interface: AES TSAPI

Avaya Communication Manager
Avaya Application Enablement Services (AES) / Avaya CT - TSAPI

☐ VoIP Mapping: AES SMS

☐ Additional VoIP Mapping: AES SMS

☒ Active Recording: DMCC (Advanced Interaction Recorder)

Avaya Communication Manager
Device Media and Call Control

Proceed to **Stage 4**. Enter desired strings for **ServerName**, **LoginID**, and **Password**. These parameters are not pertinent to the integration but are required to be configured.

New CTI Connection

Set New CTI Connection Wizard Stage 4 of 17

Interface Parameters

CTI Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
ServerName	anything
LoginID	anything
Password	*****
UseWarmStandBy	No

Description: Server connection name.

Additional Interface Parameters

Proceed to **Stage 9**. Enter the following values for the specified fields and retain the default values for the remaining fields.

- **PrimaryAESServerAddress:** IP address of the Application Enablement Services server.
- **PrimaryAESUserName:** The NICE user credentials from **Section 6.4**.
- **PrimaryAESPassword:** The NICE user credentials from **Section 6.4**.

New CTI Connection

Set New CTI Connection Wizard Stage 9 of 17

Active Recording

Active Recording Interface Details

Interface Connection Details

Mandatory fields are marked in bold

Parameter	Value
PrimaryAESServerAddress	10.64.101.239
PrimaryAESDMCCPort	4722
PrimaryAESUserName	nice
PrimaryAESPassword	*****
PrimaryAESSecuredConnection	TRUE
UseAESWarmStandbvFeature	FALSE

Description: Password to logon with DMCC application

Expand **Media Provider Controllers – Location** toward bottom of screen. Enter host name of the Engage server with the Advanced Interaction Recorder component, in this case “niceair”, and click the add icon. The resultant screen is shown below.

New CTI Connection

Set New CTI Connection Wizard Stage 9 of 17

Active Recording

Active Recording Interface Details

Interface Connection Details

Additional Interface Parameters

Media Provider Controllers - Location

Media Provider Location

Server IP/Hostname

Connection Manager Port: 62094

Media Provider Controllers:

IP/Hostname	CM Port
niceair	62094

Proceed to **Stage 11**. Select **Add** to add a device entry for each agent station extension from **Section 3**. Enter the following values for the specified fields (not shown) and retain the default values for the remaining fields.

- **Device Type:** “Extension”
- **Device Number:** The agent station extension from **Section 3**.
- **Observation Type:** “Non-Resource-Based”
- **SymbolicName:** The switch connection name from **Section 6.3**, in this case “cm7”.
- **CodecsList:** Check pertinent codec, which were G711U and G729 in the testing.
- **EncAlgList:** Check “AES_128_HMAC”.

In the compliance testing, two entries were created as shown below.

New CTI Connection

Set New CTI Connection Wizard Stage 11 of 17

Devices

Available Devices

Provide telephony switch available devices

2 devices

Add Add Range Add From Switch

Device Number	CTI Trunk ID	Type
65001		Extension
66006		Extension

Proceed to **Stage 12**. Select all pertinent devices from the left pane and move to the right. The screen below shows the result of the move.

New CTI Connection

Set New CTI Connection Wizard Stage 12 of 17

Monitor

Please select the devices to be monitored
Double click on a monitored device for further configuration

Available Devices: 0 devices

Device	Type
--------	------

Monitored Devices: 2 devices

Device	Type
65001	Extension
66006	Extension

Proceed to **Stage 16**. For **Port**, select an available port number, in this case “62095” as shown below. Proceed and complete the wizard.

New CTI Connection

Set New CTI Connection Wizard Stage 16 of 17

Requirements

The Interactions Center server selected already has a Connection Manager.
Create a new Connection Manager, or select an existing one.

☒ Create a new Connection Manager

Port: 62095

☐ Select available Connection Manager

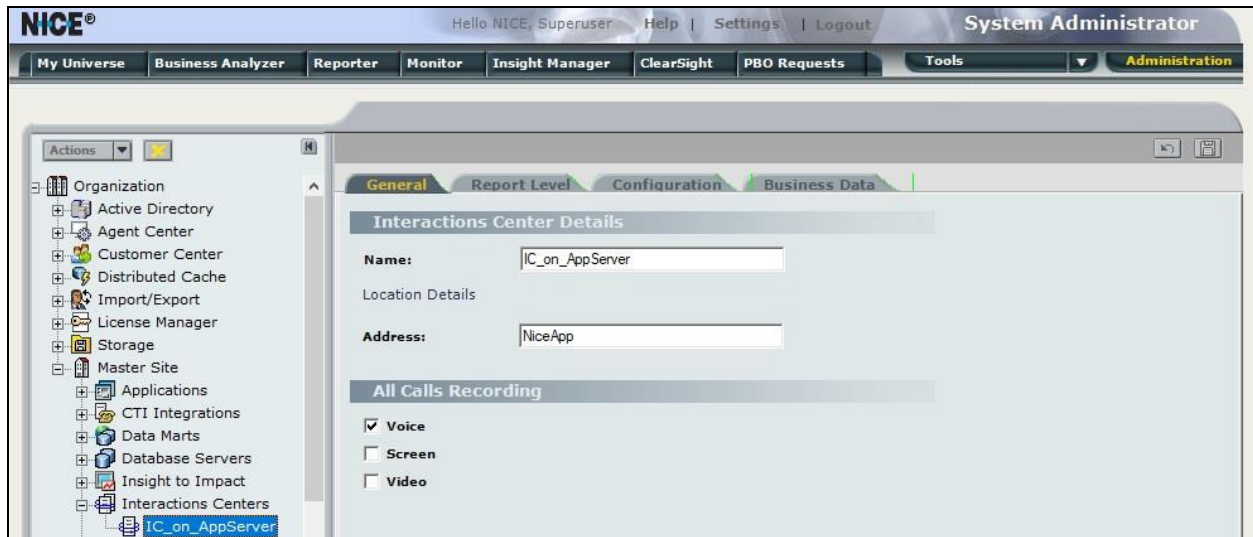
Ports in use:

- 62094

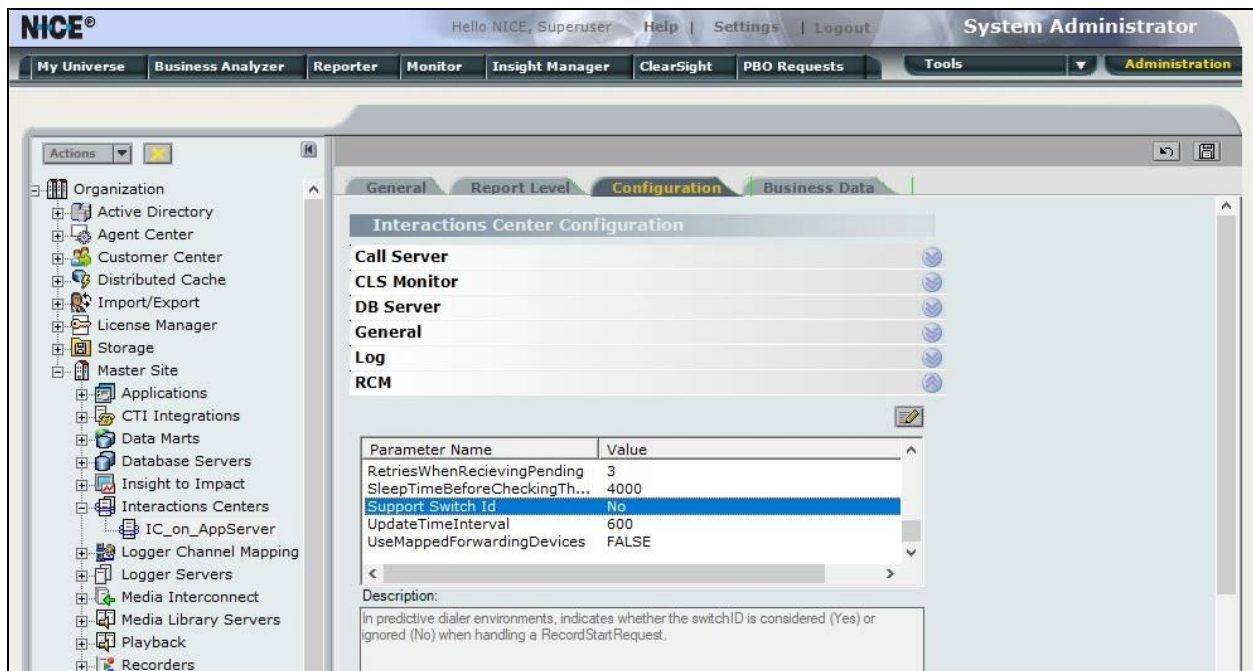
9.4. Administer Interactions Center

From the **NICE** screen, expand **Master Site** → **Interactions Center** and select the pertinent center, in this case “IC_on_AppServer”, which was pre-configured.

Select the **General** tab in the right pane, and check **Voice** as shown below.



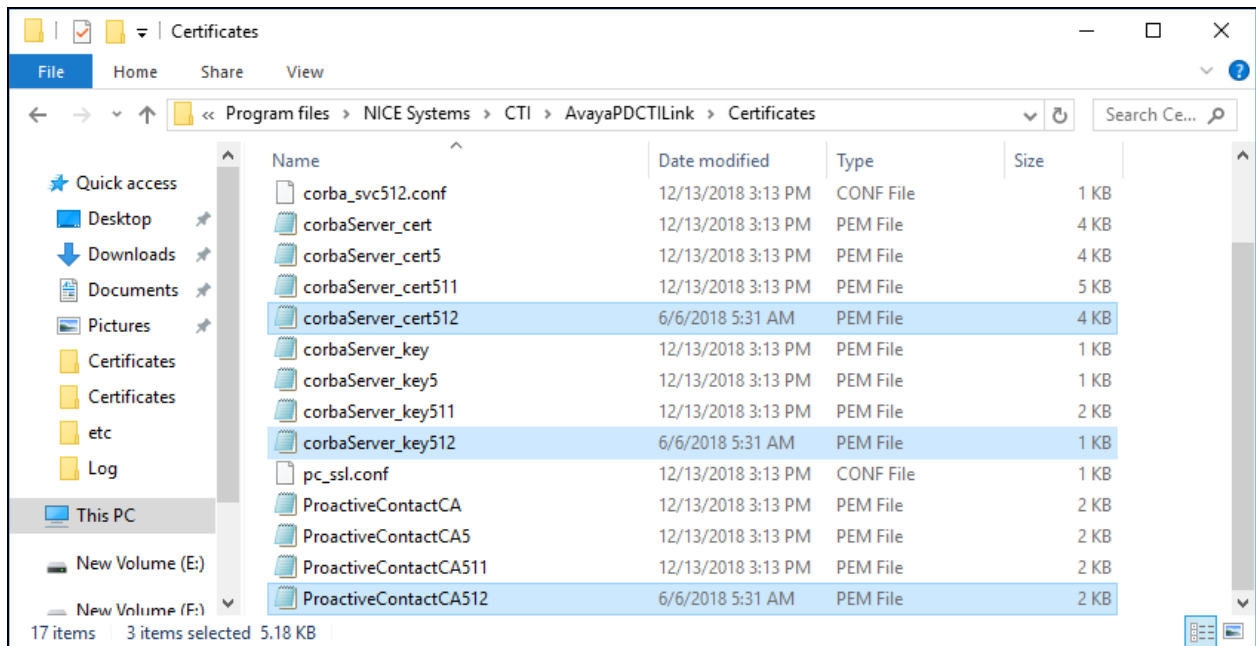
Select the **Configuration** tab and expand **RCM** in the right pane. Locate the **Support Switch Id** parameter and set it to “No” as shown below.



9.5. Administer Certificates

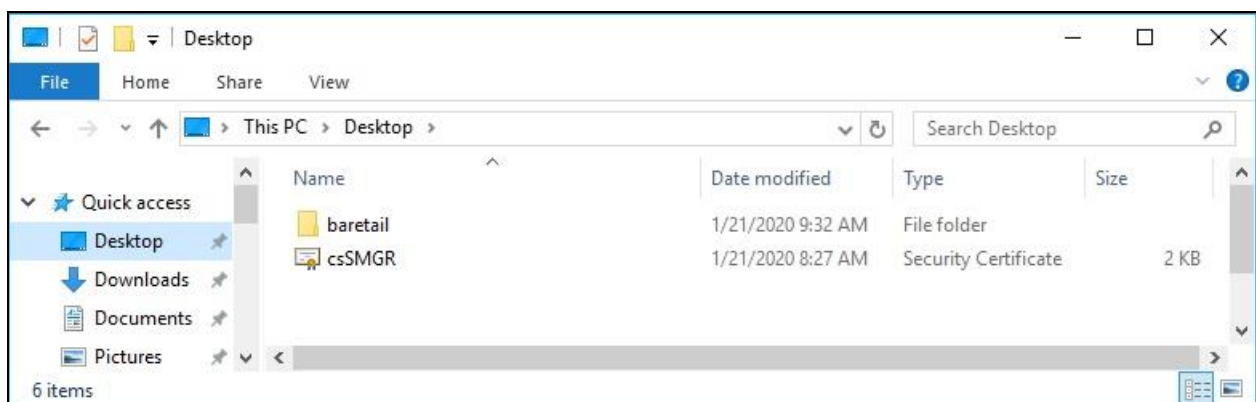
From the Engage server running the Interactions Center component, navigate to the **D:\Program files\NICE Systems\CTI\AvayaPDCTILink\Certificates** directory.

Rename the three Proactive Contact permission files obtained from **Section 8.2** to end with the configured AvayaPD version from **Section 9.2** and paste into the directory as shown below.



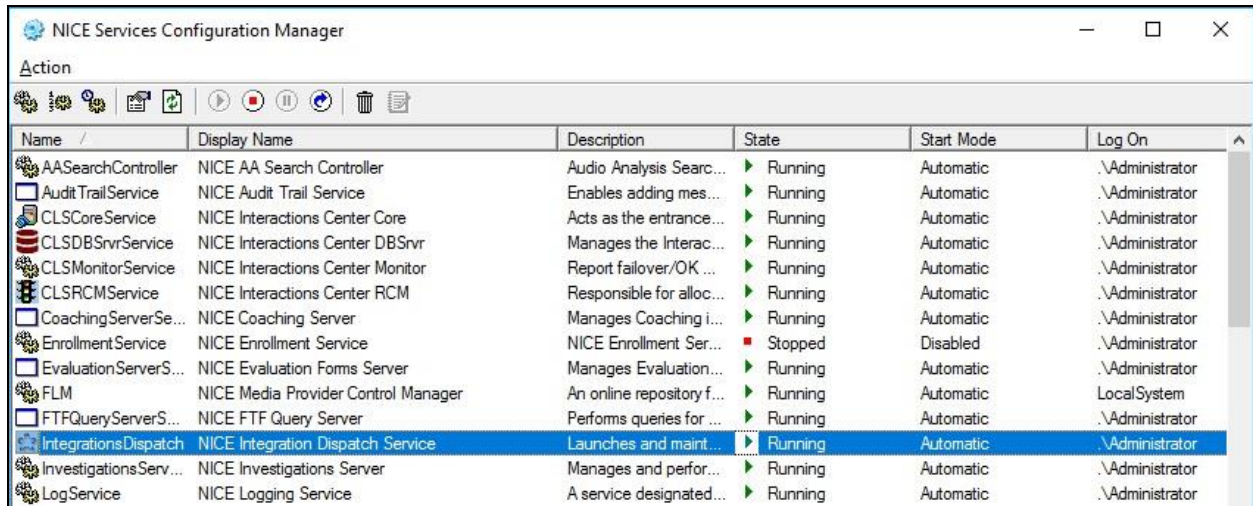
From the Engage server running the Advanced Interaction Recorder component, copy the CA certificate from **Section 6.8** to a desired directory.

Double click on the certificate and install onto the server.



9.6. Restart Services

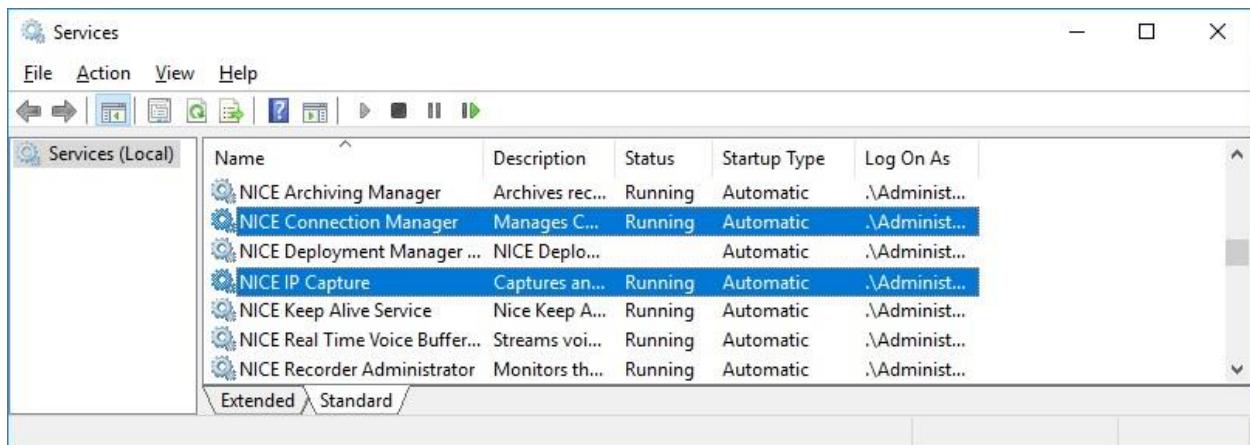
From the Engage server running the Interactions Center component, navigate to **Windows → Nice Systems** and launch **Nice Service Configuration Manager**. The **NICE Services Configuration Manager** screen below is displayed. Restart the **IntegrationsDispatch** service.



Name	Display Name	Description	State	Start Mode	Log On
AASearchController	NICE AA Search Controller	Audio Analysis Search...	Running	Automatic	.\Administrator
AuditTrailService	NICE Audit Trail Service	Enables adding mes...	Running	Automatic	.\Administrator
CLSCoreService	NICE Interactions Center Core	Acts as the entrance...	Running	Automatic	.\Administrator
CLSDBSvrService	NICE Interactions Center DBSvr	Manages the Interac...	Running	Automatic	.\Administrator
CLSMonitorService	NICE Interactions Center Monitor	Report failover/OK ...	Running	Automatic	.\Administrator
CLSRCMSvc	NICE Interactions Center RCM	Responsible for alloc...	Running	Automatic	.\Administrator
CoachingServerSe...	NICE Coaching Server	Manages Coaching i...	Running	Automatic	.\Administrator
EnrollmentService	NICE Enrollment Service	NICE Enrollment Ser...	Stopped	Disabled	.\Administrator
EvaluationServerS...	NICE Evaluation Forms Server	Manages Evaluation...	Running	Automatic	.\Administrator
FLM	NICE Media Provider Control Manager	An online repository f...	Running	Automatic	LocalSystem
FTFQueryServerS...	NICE FTF Query Server	Performs queries for ...	Running	Automatic	.\Administrator
IntegrationsDispatch	NICE Integration Dispatch Service	Launches and maint...	Running	Automatic	.\Administrator
InvestigationsServ...	NICE Investigations Server	Manages and perfor...	Running	Automatic	.\Administrator
LogService	NICE Logging Service	A service designated...	Running	Automatic	.\Administrator

From the Engage server running the Advanced Interaction Recorder component, navigate to **Windows → Windows System → Windows Administrative Tools → Services** to display the **Services** screen below.

Restart the **NICE Connection Manager** and **NICE IP Capture** services shown below.



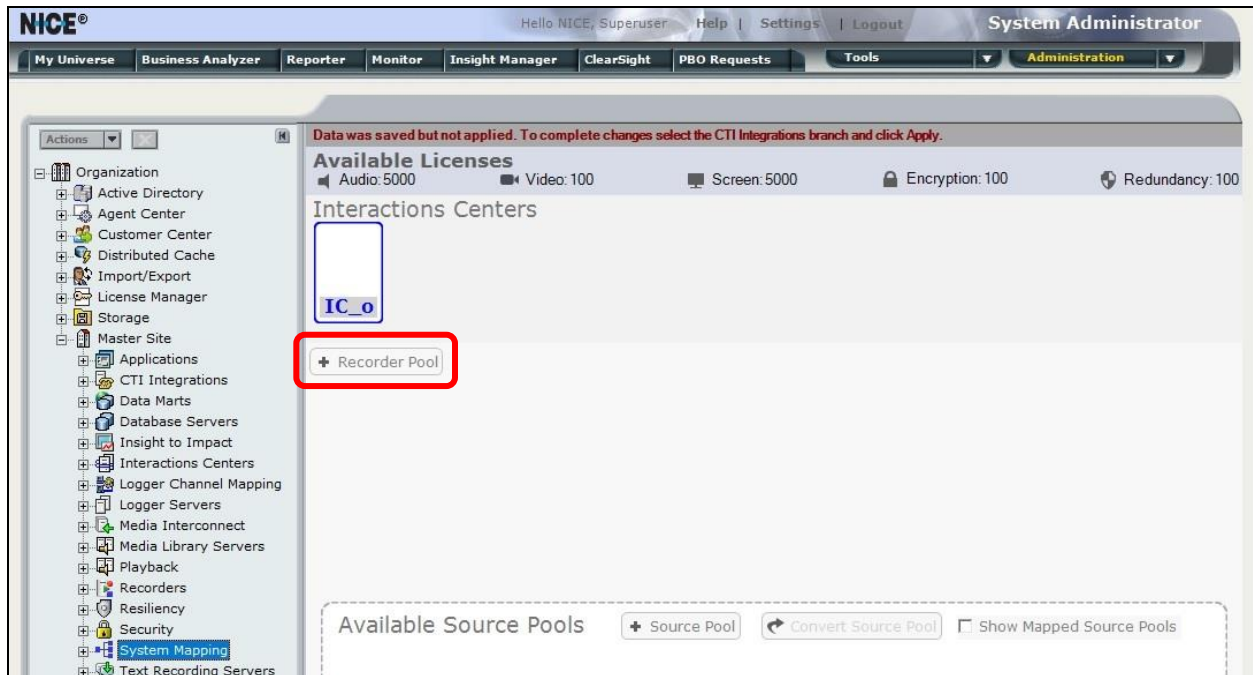
Name	Description	Status	Startup Type	Log On As
NICE Archiving Manager	Archives rec...	Running	Automatic	.\Administ...
NICE Connection Manager	Manages C...	Running	Automatic	.\Administ...
NICE Deployment Manager ...	NICE Deplo...		Automatic	.\Administ...
NICE IP Capture	Captures an...	Running	Automatic	.\Administ...
NICE Keep Alive Service	Nice Keep A...	Running	Automatic	.\Administ...
NICE Real Time Voice Buffer...	Streams voi...	Running	Automatic	.\Administ...
NICE Recorder Administrator	Monitors th...	Running	Automatic	.\Administ...

9.7. Administer System Mapping

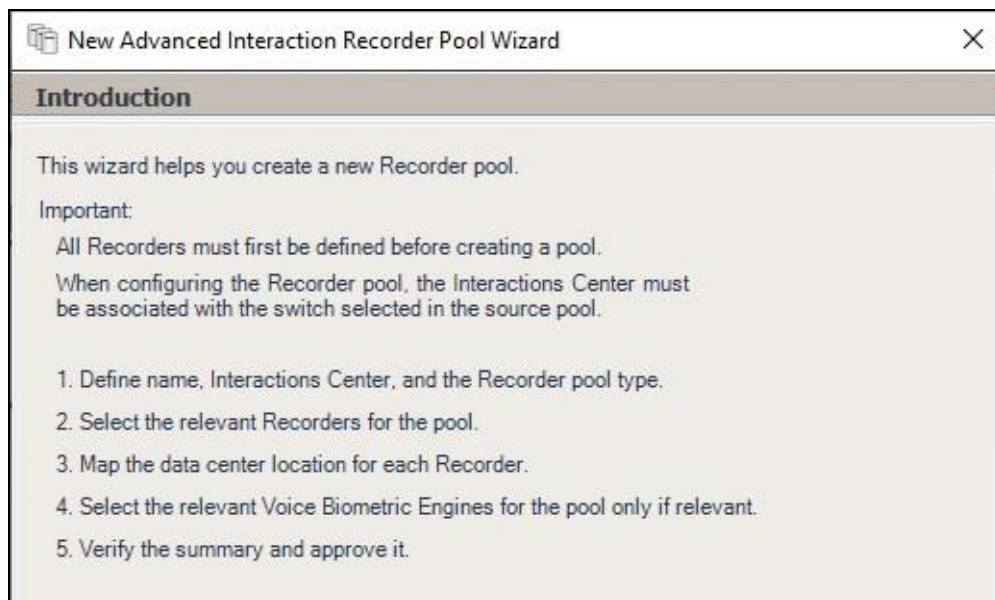
From the NICE screen, select **Master Site** → **System Mapping**.

9.7.1. Recorder Pool


The screen below is displayed. In the right pane, select **+ Recorder Pool**.



The **New Advanced Interaction Recorder Pool Wizard** pop-up screen is displayed as shown below. Click **Next** (not shown).



The screen below is displayed next. Enter a descriptive **Name** and retain the default values in the remaining fields.



The screenshot shows a window titled "New Advanced Interaction Recorder Pool Wizard" with a close button (X) in the top right corner. The main heading is "Define Recorder Pool". Below the heading, a note states: "Define the Recorder pool details. After completing this wizard, the pool type cannot be changed." The form contains three fields: a required field labeled "* Name:" with the text "DevConnect Pool" entered; a "Pool type:" dropdown menu set to "Basic"; and an "Interactions Center:" dropdown menu set to "IC_on_AppServer". At the bottom, a note reads: "Note: This Interactions Center must be associated with the switch selected in the source pool." and a legend indicates "* Required field."

In the next screen, select the relevant and pre-existing recorder from the left pane and move to the right. The screenshot below shows the result of the move.

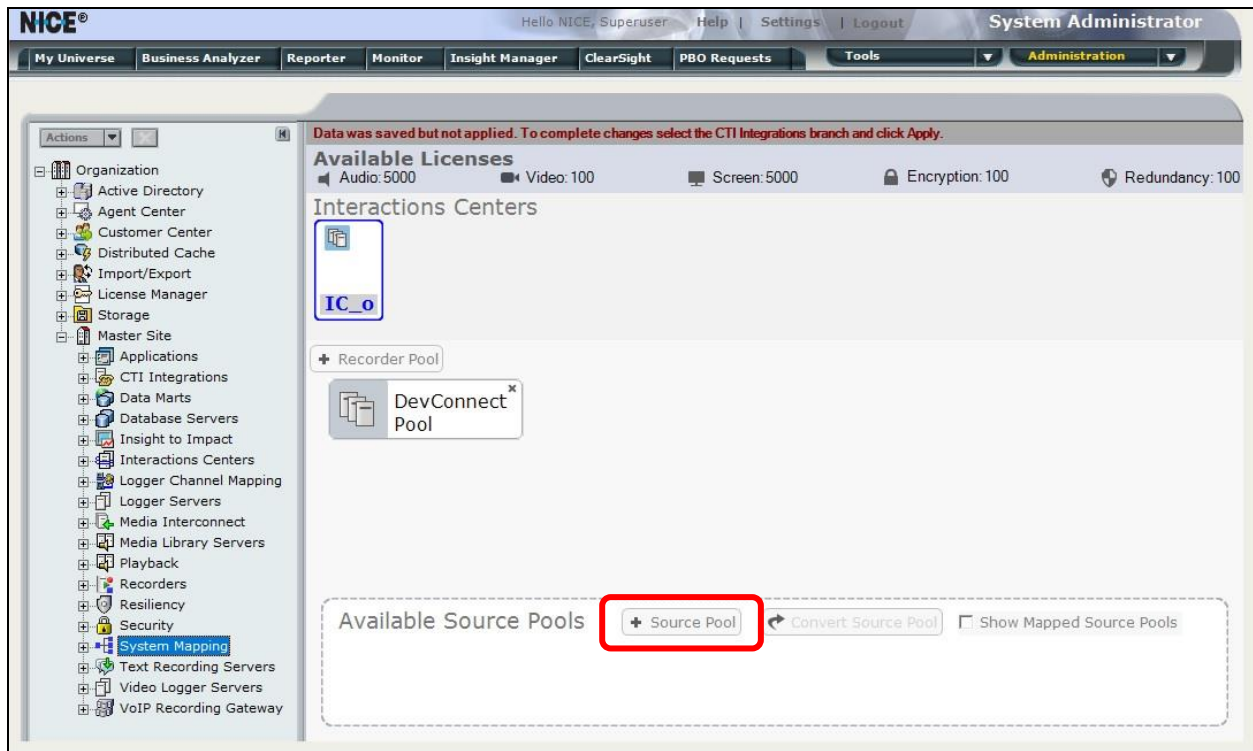
Proceed to complete the wizard.



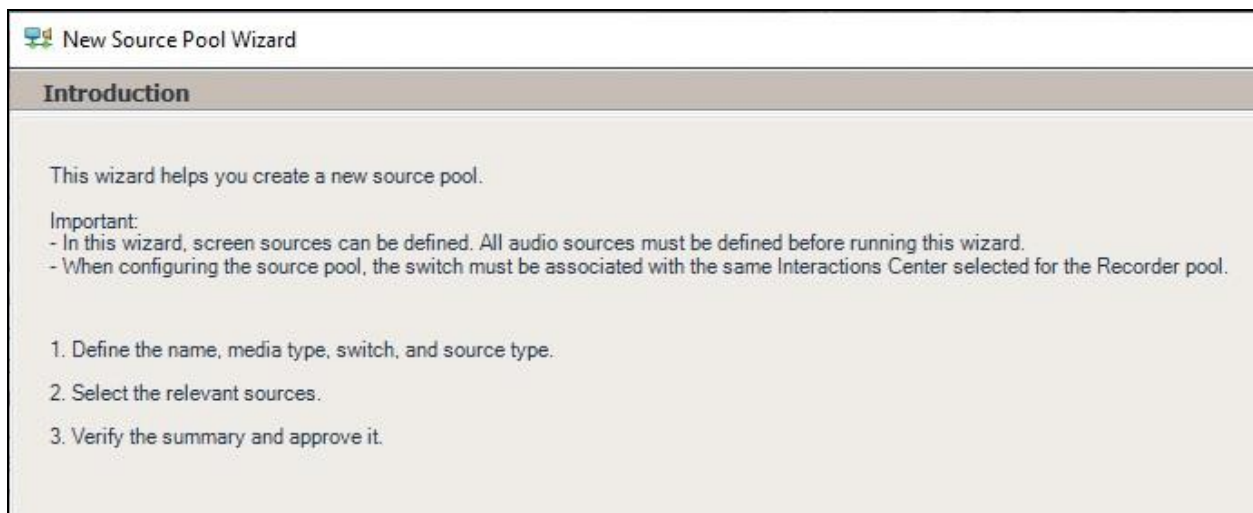
The screenshot shows a window titled "New Advanced Interaction Recorder Pool Wizard" with a close button (X) in the top right corner. The main heading is "Select Recorders". Below the heading, a note states: "Select the relevant Recorders for the pool. A basic pool must have a minimum of 1 Recorder." The screen is divided into two panes: "Available" on the left and "Selected" on the right. The "Selected" pane contains the text "AIR". Between the panes are two buttons: a right-pointing arrow (>) and a left-pointing arrow (<).

9.7.2. Source Pool

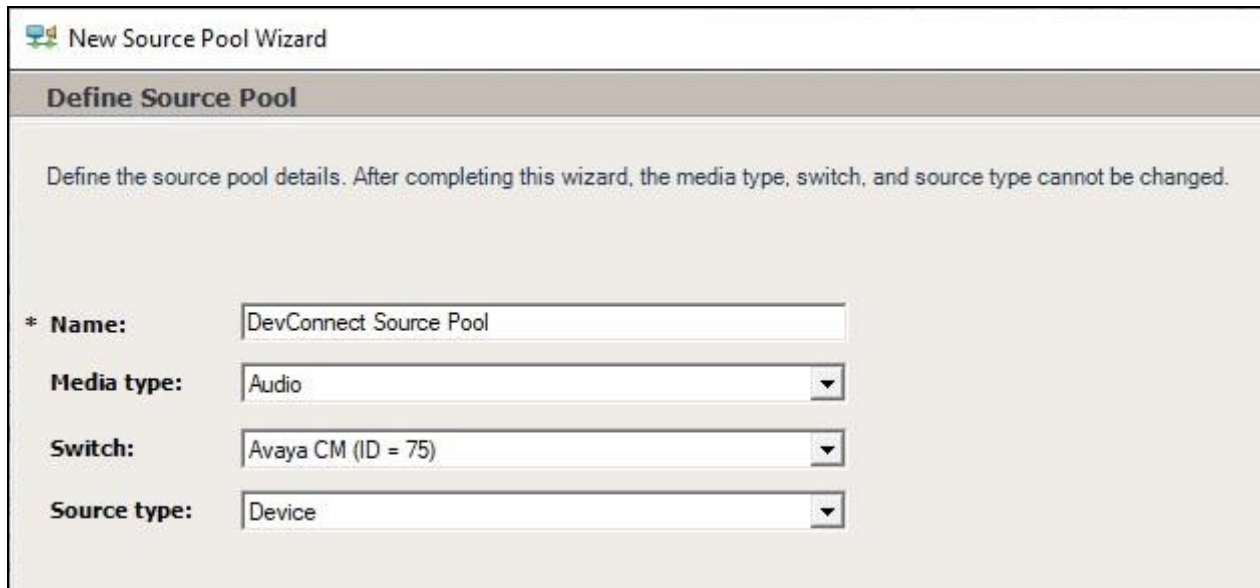
The NICE screen is updated as shown below. Select **+ Source Pool** to add a source pool.



The **New Source Pool Wizard** pop-up screen is displayed. Click **Next** (not shown).



The screen below is displayed next. Enter a descriptive **Name**. For **Switch**, select the switch name from **Section 9.3**.



New Source Pool Wizard

Define Source Pool

Define the source pool details. After completing this wizard, the media type, switch, and source type cannot be changed.

* **Name:**

Media type:

Switch:

Source type:

In the next screen, select the relevant device entries as shown below.

Proceed to complete the wizard.



New Source Pool Wizard

Select Sources

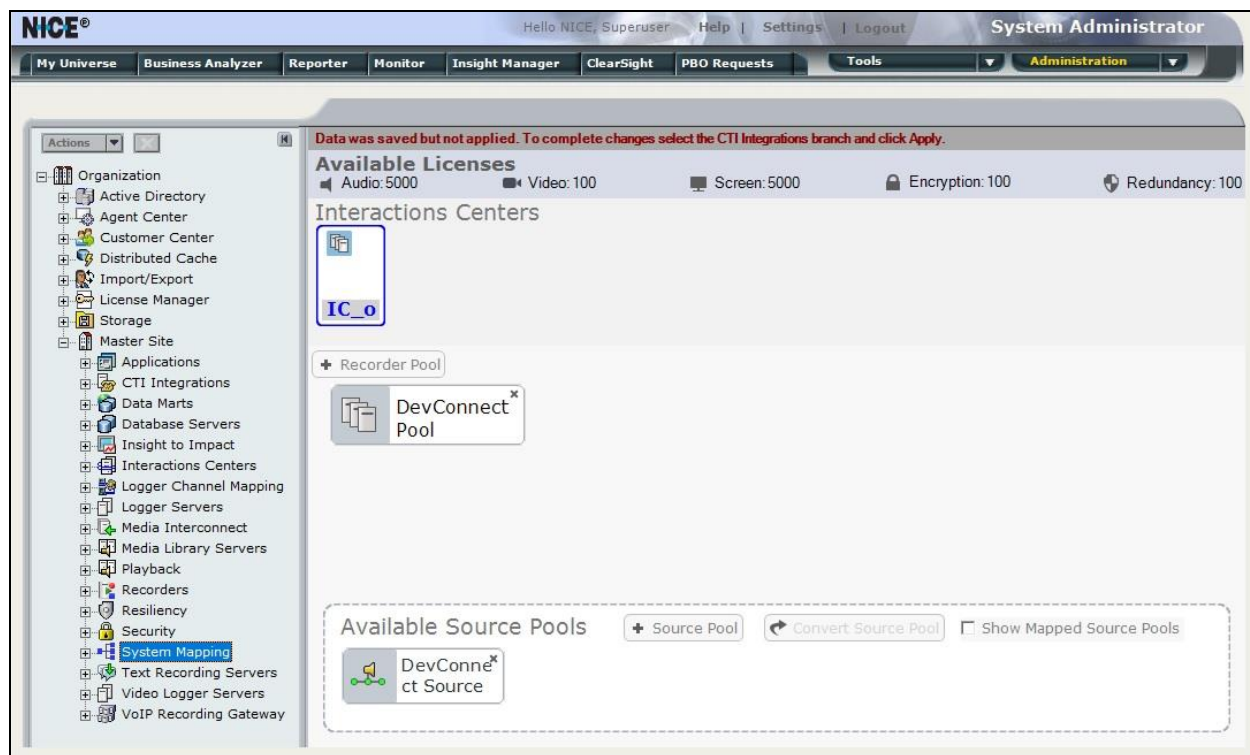
Find:

Selected: 2/2

	Name	Device Number	Unique Device ID	IP Address
<input checked="" type="checkbox"/>		65001		
<input checked="" type="checkbox"/>		66006		

9.7.3. Recording Profile

The NICE screen is updated as shown below. Drag the created source pool below and drop on top of the created recorder pool, in this case **DevConnect Source** and **DevConnect Pool** respectively.



The **New Recording Profile Wizard** pop-up screen is displayed. Click **Next** (not shown).



The screen below is displayed next. Enter a descriptive **Name**.

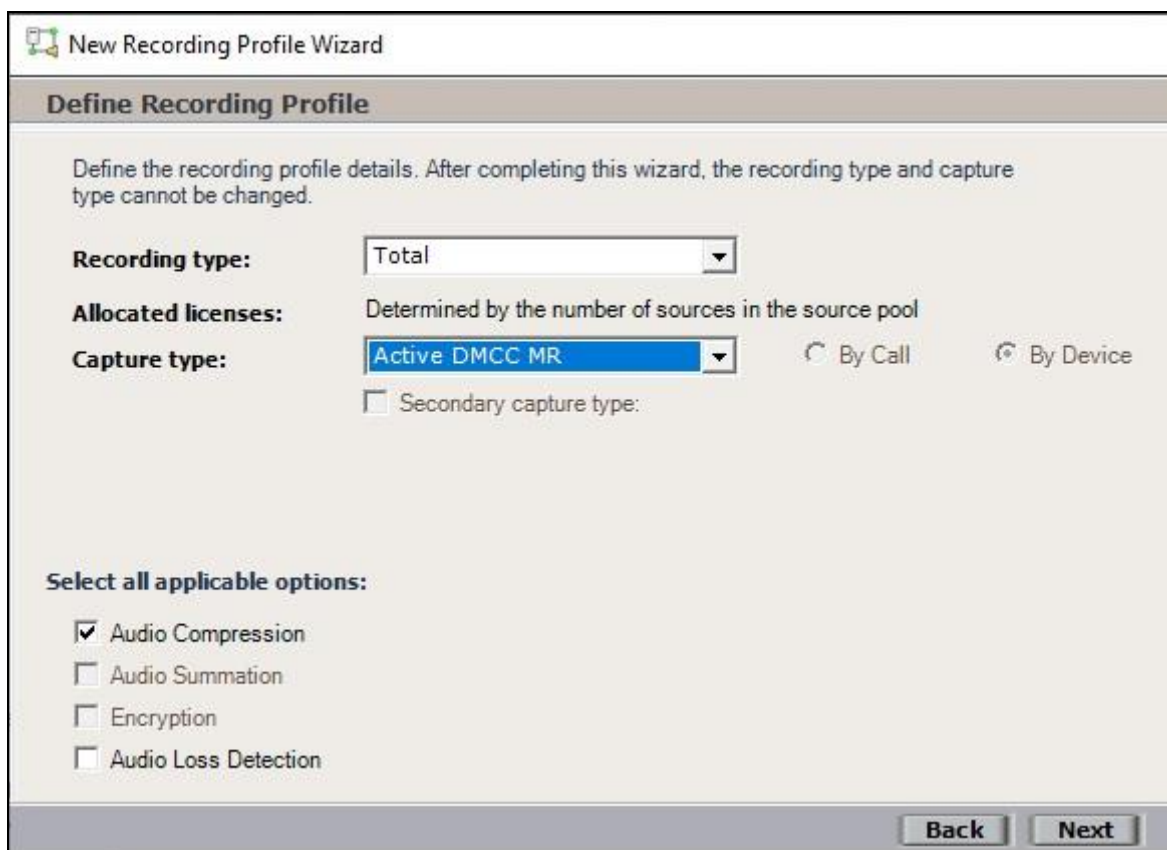


The screenshot shows the 'New Recording Profile Wizard' window. The title bar says 'New Recording Profile Wizard'. The main heading is 'Define the Recording Profile Name'. Below the heading, there is a text box with the instruction: 'Enter a meaningful recording profile name. After completing this wizard, the mapping and the recording type cannot be changed.' Below this, there is a label 'Name:' followed by a text input field containing the text 'DevConnect Recording Profile'.

In the next screen, enter the following values for the specified fields and retain the default values for the remaining fields.

- **Recording type:** “Total”
- **Capture type:** “Active DMCC MR”
- **Audio Compression:** Check this option.

Proceed to complete the wizard.



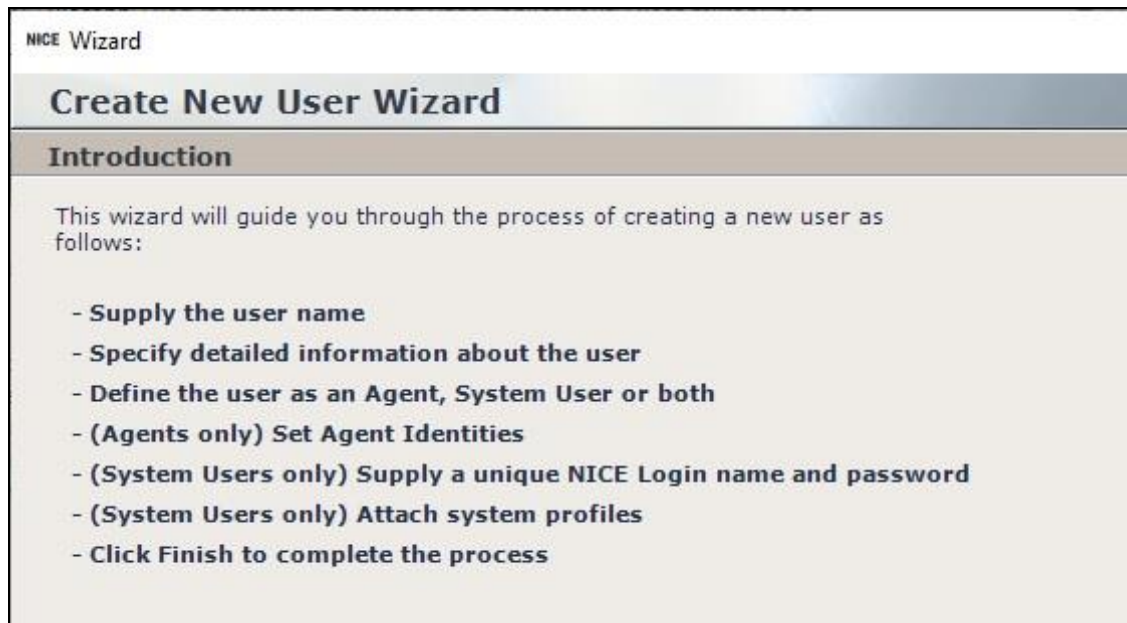
The screenshot shows the 'New Recording Profile Wizard' window, step 2. The title bar says 'New Recording Profile Wizard'. The main heading is 'Define Recording Profile'. Below the heading, there is a text box with the instruction: 'Define the recording profile details. After completing this wizard, the recording type and capture type cannot be changed.' Below this, there are several fields: 'Recording type:' with a dropdown menu showing 'Total'; 'Allocated licenses:' with the text 'Determined by the number of sources in the source pool'; 'Capture type:' with a dropdown menu showing 'Active DMCC MR' and two radio buttons labeled 'By Call' and 'By Device'; and a checkbox labeled 'Secondary capture type:'. Below these fields, there is a section titled 'Select all applicable options:' with four checkboxes: 'Audio Compression' (checked), 'Audio Summation', 'Encryption', and 'Audio Loss Detection'. At the bottom right, there are 'Back' and 'Next' buttons.

9.8. Administer Agent Users

The NICE screen is displayed again. Select **Administration** → **User Administrator** from the top menu, followed by **New User**.



The **Create New User Wizard** pop-up screen is displayed. Click **Next** (not shown).



The **Step 1** screen displayed next. Enter pertinent values for **First Name**, **Last Name**, and **Windows User Name** for the first agent user from **Section 3**. Retain the default values in the remaining fields.

NICE Wizard

Create New User Wizard Step 1 of 8

General Information

Enter the following information. A red asterisk (*) indicates required fields.

First Name: * Agent1

Middle Name:

Last Name: * Avaya

Email Address:

Windows User Name: * agent1

Domain:

Select a site to associate to the user:

Site: Master Site

Proceed to **Step 4** and check the **Agent** user type shown below.

NICE Wizard

Create New User Wizard Step 4 of 8

User Type

Choose one or both user types:

☒ **Agent (User interactions will be recorded/monitored)**

☐ **System User (User will log into NICE applications)**

Proceed to **Step 5** and click **Add**.

Create New User Wizard Step 5 of 8

Agent Details

RTA Agent: ☐

RTA Agents have permissions to initiate customer authentication, enrollment and consent updates.

Site	Switch	Agent ID	Extension	Email	Alias

Add

The **Agent Identity Dialog** pop-up box is displayed. For **Switch**, select the switch name from **Section 9.2**. Select **Extension** and enter the first agent user extension from **Section 3**. Retain the default values in the remaining fields and proceed to complete the Wizard.

Agent Identity Dialog

Site: Master Site

Switch: Avaya PC/ POM

☐ **Agent ID:**

☒ **Extension:** 65001

☐ **Email:**

☐ **Alias:**

OK **Cancel**

Repeat this section to add an agent user for each agent station extension in **Section 3**. In the compliance testing, two agent users were created as shown below.

NICE® Hello NICE, Superuser Help Settings Logout **Users Administrator**

My Universe Business Analyzer Reporter Monitor Insight Manager ClearSight PBO Requests Tools Administration

Click to scroll Contents list

All Users

General Profiles

All Users

Search Users:

1 - 6 of 6 User(s) **Reset Password** **New User** **Delete**

Name	Type	RTA Agent	Description	Domain	Location
Avaya, Agent1	Agent	No			
Avaya, Agent2	Agent	No			

10. Verification Steps

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

10.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the registration status of virtual IP softphones by using the “list registered-ip-stations” command. Verify that there is an entry for each agent station extension from **Section 3** along with the IP address of the Application Enablement Services server, as shown below.

```
list registered-ip-stations
```

REGISTERED IP STATIONS			
Station Ext or Orig Port Socket	Set Type/ Net Rgn	Prod ID/ Release	Station IP Address/ Gatekeeper IP Address
65001	9611	IP_Phone	192.168.200.217
tls	1	6.8202	10.64.101.236
65001	9611	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236
66006	9641SIPCC	IP_API_A	10.64.101.239
tcp	1	3.2040	10.64.101.236

10.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify 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 the **User** column shows an active session with the NICE user name from **Section 6.4**, and that the **# of Associated Devices** column reflects the number of agent users in **Section 3**, in this case “2”.

AVAYA **Application Enablement Services**
Management Console

Welcome: User
Last login: Thu Jan 23 13:07:59 2020 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.1.0.1.8-0
Server Date and Time: Thu Jan 23 14:23:08 EST 2020
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

▶ Logs

▶ Log Manager

▼ Status and Control

■ CVLAN Service Summary

■ DLG Services Summary

■ **DMCC Service Summary**

■ Switch Conn Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)

Generated on Thu Jan 23 14:23:08 EST 2020

Service Uptime: 0 days, 1 hours 15 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 4

Number of Existing Devices: 2

Number of Devices Created Since Service Boot: 8

	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	FBFAFC205A5939E5E 37A4833BDF66F66-3	nice		10.64.101.208	XML Encrypted	2

Terminate Sessions Show Terminated Sessions

Item 1-1 of 1
1 Go

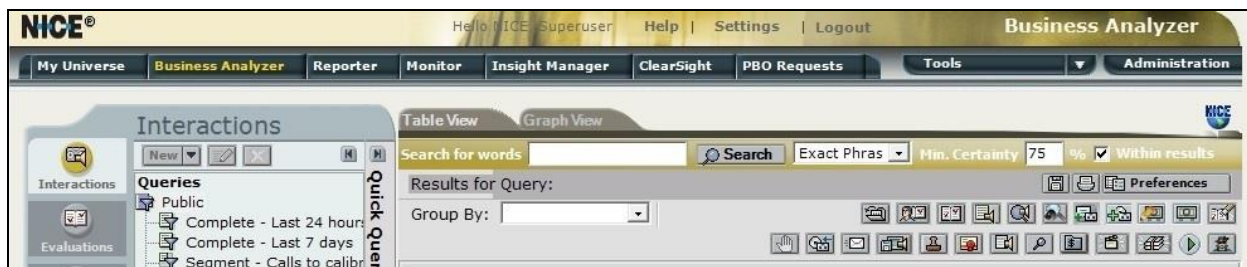
10.3. Verify Avaya Proactive Contact

Log in to the Linux shell of Proactive Contact and issue the “netstat | grep ensERVER” command. Verify that there is an entry showing an **ESTABLISHED** connection with the IP address of the Engage server running the Interactions Center component, in this case “10.64.101.207”, as shown below.

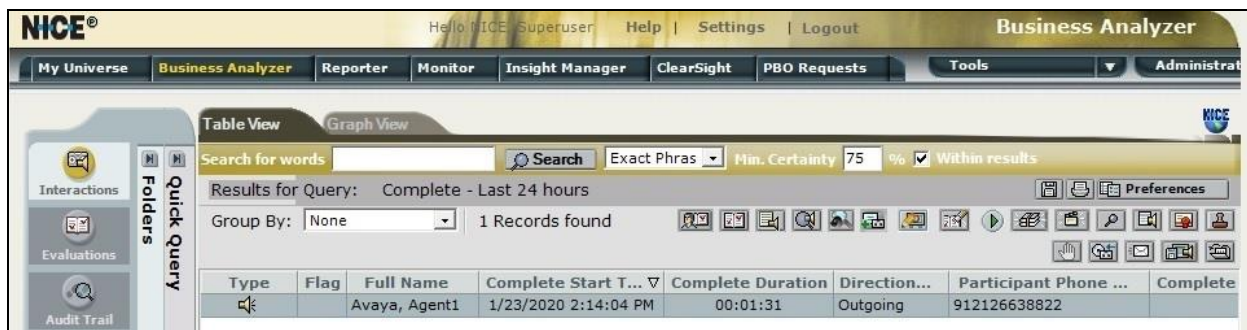
tcp	0	0	lzpds4b:enserver_ssl	10.64.101.207:51104	ESTABLISHED
tcp	0	0	lzpds4b:enserver_ssl	lzpds4b:31478	ESTABLISHED
tcp	0	0	lzpds4b:31478	lzpds4b:enserver_ssl	ESTABLISHED

10.4. Verify NICE Engage Platform

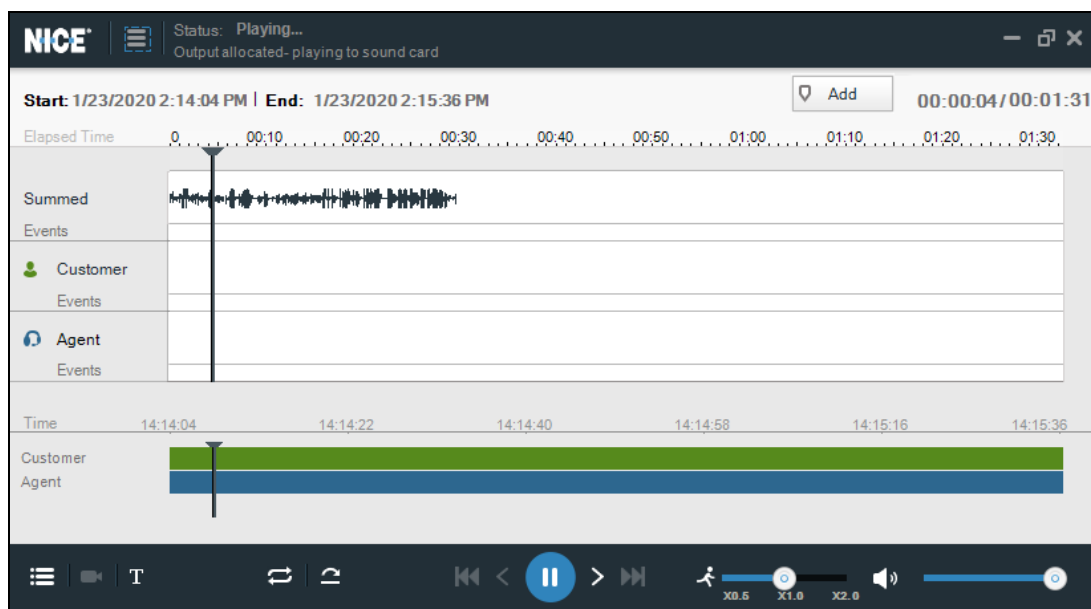
Start a job on Proactive Contact and log an agent in to handle and complete an outbound call. From the **NICE** screen, select **Business Analyzer** from the top menu to display the screen below. Select **Queries** → **Public** → **Complete – Last 2 hours** from the left pane.



Verify that there is an entry in the right pane reflecting the last call, with proper values in the relevant fields. Double click on the entry.



Verify that the pop-up screen below is displayed and that the recording can be played back.



11. Conclusion

These Application Notes describe the configuration steps required for NICE Engage Platform 6.15 to successfully interoperate with Avaya Proactive Contact 5.2 with PG230 and Avaya Aura® Application Enablement Services 8.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

12. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 5, November 2019, available at <http://support.avaya.com>.
2. *Administering Aura® Application Enablement Services*, Release 8.1.x, Issue 3, October 2019, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 8.1.1, Issue 2, October 2019, available at <http://support.avaya.com>.
4. *Administering Avaya Proactive Contact*, Release 5.2, Issue 1, July 2018, available at <http://support.avaya.com>.
5. *System Administrator Configuration Guide, NICE Engage Platform 6.x*, Revision A4, September 2018, available at <http://www.extranice.com>.
6. *Avaya PC Active-Passive Connectivity Guide, NICE Engage Platform 6.x*, Revision C8, January 2018, available at <http://www.extranice.com>.
7. *Avaya CM Active Connectivity Guide, NICE Engage Platform 6.x*, Revision B3, October 2019, available at <http://www.extranice.com>.

©2020 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.