



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring NICE Interaction Management R4.1 with Avaya Aura® Contact Centre R6.2 and Avaya Aura® Application Enablement Services R6.1 for Call Recording in a Mission Critical High Availability Environment – Issue 1.0**

## **Abstract**

These Application Notes describe the configuration steps for provisioning NICE Interaction Management R4.1 with a SIP enabled Avaya Aura® Contact Centre R6.2 in a full High Availability Mission Critical environment for call recording. NICE Interaction Management records the RTP stream coming from the Avaya Media Server module of Avaya Aura® Contact Centre using events from the Communication Control Toolkit module of Avaya Aura® Contact Centre.

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 compliance tested configuration required for interoperability between NICE Interaction Management R4.1 and Avaya Aura® Contact Centre R6.2 in a Mission Critical High Availability environment. To achieve the highest level of Mission Critical High Availability with no single point of failure a SIP-based contact centre with the following criteria must be setup. (See **Section 3, Figure 1** for a diagram setup of the complete solution).

- Two co-resident Contact Centre Manager Server (CCMS), Communication Control Toolkit (CCT), and Contact Centre Manager Administration (CCMA) servers configured as a High Availability pair.
- Two or more Avaya Media Server Linux-based servers configured as a High Availability pair. Avaya Media Server High Availability is supported only on Linux-based servers.
- Two Avaya Aura® Session Manager instances, R6.1.
- Two Avaya Aura® Application Enablement Services servers configured as a High Availability pair.
- Two Avaya Aura® Communication Manager Servers configured as a High Availability pair.

NICE Interaction Management R4.1 is a software-only solution that offers various recording, playback and archiving features and options. By combining media redirection from Avaya Aura® Contact Centre, call recording can be achieved without the use of physical connections to the NICE server other than standard network connections. The NICE solution is fully integrated into a LAN (Local Area Network), and includes Web based applications (i.e. NICE Applications) that work with .NET framework that are used to retrieve telephone conversations from a database of recorded voice calls. These Application Notes focus on recording calls from agents on a skillset call. NICE Interaction Management's internal scheduling algorithm makes the determination on which calls should be recorded based on the events received from Web Services on the Communication Control Toolkit module of Avaya Aura® Contact Centre.

## 2. General Test Approach and Test Results

The compliance testing focuses on the recording of Avaya Aura® Contact Centre (Contact Centre) skillset calls on Communication Manager deskphones. NICE Interaction Management connects to Communication Control Toolkit (CCT) Web Services in order to obtain events pertaining to specific Contact Centre skillset calls. Interaction Management can then record the call based on the events it receives. When a call is to be recorded, the Interaction Management performs recording using CCT web service recording API to enable SIP recording with Avaya Media Server. Avaya Media Server then forwards all RTP packages to NICE SIP Logger.

In a High Availability Environment one set of Contact Centre applications, a CCMS, a CCT and a CCMA actively processes scripts and contacts. This set of applications is called the active set. Another set of Contact Centre applications in the same Contact Centre system monitors and shadows the active applications in the system. The standby applications track the state of active calls but do not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail, the standby applications recognize the failure and start processing contacts. Contact Centre Administrators use the active server in daily operation. Configuration changes made to the active system during normal operation are automatically copied to the standby applications, therefore the standby applications are configured and ready to take over processing from the active system. Statistical data is also automatically copied to the standby applications. Data is replicated to the standby applications in real time. When the Contact Centre fails over to the standby server a new socket connection must be made between the NICE Interaction Management and the Standby CCT Web Services. Please see **Section 2.2** for observations during the failover testing.

Recording of Contact Centre skillset calls is done using CCT web services, all other calls use Device Media and Call Control (DMCC) to perform service observe between the extension to be recorded and a configured virtual softphone enabled station. The recording application sends a message to the DMCC integration application to begin recording the voice stream coming to that softphone extension. NICE Interaction Management utilises a CTI through Avaya Aura® Application Enablement Services (AES) to record calls on Communication Manager deskphones using Service Observe. In this message, the recorder passes along the softphone extension to be recorded along with the location and filename of the recording. Test cases are executed to exercise a sufficiently broad segment of functionality to have a reasonable expectation of interoperability in production configurations.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

## 2.1. Interoperability Compliance Testing

The testing focuses on the following types of calls:

- **Communication Manager Inbound/Outbound calls** – Test call recording for inbound/outbound calls to the Communication Manager from PSTN callers.
- **Communication Manager Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **Contact Centre Inbound/Outbound Calls** - Test call recording for inbound/outbound calls to the Contact Centre Agents from PSTN callers.
- **Contact Centre Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **Contact Centre Record on demand/Stop on demand (ROD/SOD)** - allow agents to stop and start recordings during a telephone conversation.
- **HA Failover from Contact Centre active to Contact Centre standby** - The behaviour of NICE Recording Solution under different simulated LAN failure conditions on the Avaya Contact Centre Active Server.
- **HA Failover from Communication Server active to Communication Server standby** - The behaviour of NICE Recording Solution under different simulated LAN failure conditions on Communication Server.
- **HA Failover from Media Server active to Media Server standby** - The behaviour of NICE Recording Solution under different simulated LAN failure conditions on the Media Server.
- **HA Failover from AES active to AES standby** - The behaviour of NICE Recording Solution under different simulated LAN failure conditions on AES.

## 2.2. Test Results

All compliance test cases passed successfully. There were no errors observed on the Avaya Solution as a result of the addition of NICE Integration Management to the LAN. The following observations were noted during the failover testing of the Contact Centre from Active to standby.

- The Contact Centre failover from Active to Standby can occur in less than 3 seconds depending on the failure that occurs on the Active server.
- Web Services on the CCT module does not broadcast a terminate or failover message to the connected sessions.
- Timers on the NICE Interaction Management for a keep-alive message to Web Services on the Contact Centre CCT module were adjusted during the HA Failover from Contact Centre active to Contact Centre standby. This was to facilitate an issue were the CCT was failed over but the NICE interaction Management was not aware and was connected to an expired session on Web Services. In order to ensure that a new session was established on all occasions the NICE Interaction Management needed to send and receive a keep-alive message to Web Services every second to ensure it was aware when the active session was stopped and a switch over occurred.

## 2.3. Support

Support from Avaya is available at <http://support.avaya.com> and support from NICE can be obtained as shown below.

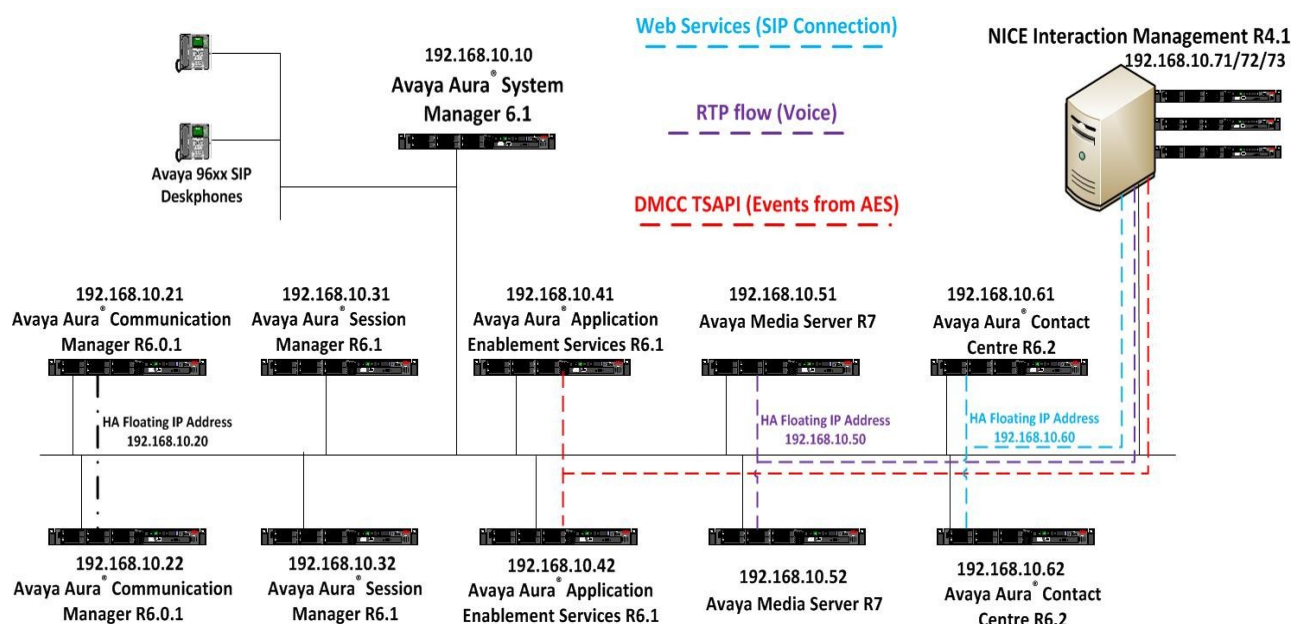
NICE International Corporate Headquarters, Israel

Tel: +972 9 775 3800

Email: [support@nice.com](mailto:support@nice.com)

## 3. Reference Configuration

**Figure 1** shows the compliance tested configuration which includes duplicate Communication Manager servers in High Availability, Session Manager to provide SIP functionality, AES to provide DMCC events from Communication Manager and Contact Centre which includes the CCT module to provide call events for Contact Centre calls and Media Server to provide the RTP for recording.



**Figure 1: Connection of NICE Interaction Management R4.1 for interoperability with Avaya Aura® Contact Centre R6.2 and Avaya Aura® Application Enablement Services R6.1 in a Mission Critical High Availability Environment.**

## 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura <sup>®</sup> System Manager running on Avaya S8800 Server	R6.1 SP4
Avaya Aura <sup>®</sup> Communication Manager running on Avaya S8800 Server	R6.0.1 SP3 (Active Server HA mode)
Avaya Aura <sup>®</sup> Communication Manager running on Avaya S8800 Server	R6.0.1 SP3 (Standby Server HA mode)
Avaya Aura <sup>®</sup> Session Manager running on Avaya S8800 Server	R6.1 SP4 (Primary -Active Server in Active-Active Mode)
Avaya Aura <sup>®</sup> Session Manager running on Avaya S8800 Server	R6.1 SP4 (Secondary -Active Server in Active-Active Mode)
Avaya Aura <sup>®</sup> Application Enablement Services running on Avaya S8800 Server	R6.1 (Active Server with System Platform in HA)
Avaya Aura <sup>®</sup> Application Enablement Services running on Avaya S8800 Server	R6.1 (Standby Server with System Platform in HA)
Avaya Aura <sup>®</sup> Contact Centre running on Avaya S8800 Server	R6.2 SIP enabled(Active Server in HA Mode)
Avaya Aura <sup>®</sup> Contact Centre running on Avaya S8800 Server	R6.2 SIP enabled(Standby Server in HA Mode)
Avaya Media Server running on Avaya S8800 Server	R7 running on Redhat Linux R5.4 (Active Sever)
Avaya Media Server running on Avaya S8800 Server	R7 running on Redhat Linux R5.4 (Standby Sever)
Avaya 96xx Series Deskphone	96xx H.323 Release 3.1 SP2
Avaya 96xx Series Deskphone	96xx SIP Release 2.6 SP3
NICE Interaction Management Server running Windows 2008 O/S	NICE Interaction Management 4.1 Update Pack 22
NICE Interaction Management Server running Windows 2008 O/S	NICE VoIP SIP Logger 4.1 Update Pack 22
NICE Interaction Management Server running Windows 2008 O/S	NICE VoIP DMCC Logger 4.1 Update Pack 22

## 5. Configure Avaya Aura® Communication Manager

The setup of Communication Manager in a High Availability environment is outside the scope of these Application Notes. It is therefore assumed that a fully functioning High Availability Communication Manager is in place with the necessary licensing and a SIP connection is already made to Session Manager. For further information on the configuration of Communication Manager please see **Section 12** of these Application Notes.

### 5.1. Configure TSAPI CTI Link

Enter the **add cti-link x** command, where **x** is a number between 1 and 64, inclusive. Enter a valid **Extension** under the provisioned dial plan. Set the **Type** field to **ADJ-IP** and assign a descriptive **Name** to the CTI link. Default values may be used in the remaining fields.

```
add cti-link 1                                     Page 1 of 3
CTI LINK
CTI Link: 1
Extension: 2100
Type: ADJ-IP
Name: AACC
COR: 1
```

Enter the **change node-names ip** command. In the compliance-tested configuration, the **procr** IP address was utilized for registering H.323 endpoints and connectivity to the Application Enablement Services server. Note also the AES server name and IP address added, **AES61** and IP Address **192.168.10.41**.

```
change node-names ip                               Page 1 of 2
IP NODE NAMES
Name      IP Address
AES61     192.168.10.41
SM100-1   192.168.10.31
SM100-2   192.168.10.32
clan      192.168.10.102
default   0.0.0.0
gateway   192.168.10.1
medpro    192.168.10.103
procr     192.168.10.20
procr6    ::
```

Enter the **change ip-services** command. On **Page 1**, configure the **Service Type** field to **AESVCS** and the **Enabled** field to **y**. The **Local Node** field should be pointed to **procr** that was configured previously in the node-name ip form. During the compliance test, the default port was utilized for the **Local Port** field.

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

On **Page 3**, enter the hostname of the AES server for the **AE Services Server** field. Enter an alphanumeric password for the **Password** field. Set the **Enabled** field to **y**. The same password will be configured on the Application Enablement Services in **Section 6.1**.

change ip-services					Page 3 of 3
AE Services Administration					
Server ID	AE Services Server	Password	Enabled	Status	
1:	aes1	Manchestercity12	y	in use	
2:					

## 5.2. Configure Virtual Stations for Service Observe

Add virtual stations to allow Interaction Management to record calls using Service Observe. Type **add station x** where x is the extension number of the station to be configured. Also note this extension number for configuration required in **Section 9.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**. Note the **COR** of the stations below.

display station 52001		Page 1 of 5
STATION		
Extension: 52001	Lock Messages? n	BCC: 0
Type: 4621	Security Code: 1234	TN: 1
Port: S00034	Coverage Path 1:	COR: 1
Name: Nice VE3	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Location:	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 52001	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	



Type **display cor x**, where **x** is the COR number in the screen above, to check the existing Class of Restriction. Ensure that **Can be Service Observed** is set to **y**. If not type **change cor 1** to make a change to Class or Restriction (cor) 1. This needs to be enabled for Service Observe to work properly.

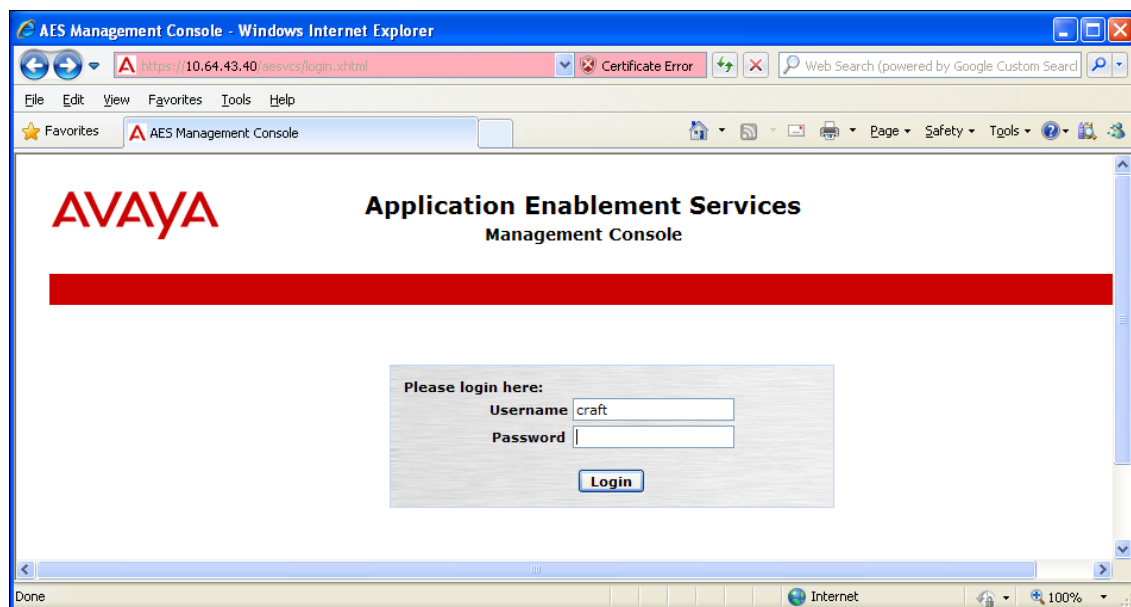
display cor 1		Page 1 of 23
CLASS OF RESTRICTION		
COR Number: 1		
COR Description:		
FRL: 0	APLT? y	
<b>Can Be Service Observed? y</b>	Calling Party Restriction: all-toll	
Can Be A Service Observer? y	Called Party Restriction: none	
Time of Day Chart: 1	Forced Entry of Account Codes? n	
Priority Queuing? n	Direct Agent Calling? y	
Restriction Override: all	Facility Access Trunk Test? n	
Restricted Call List? n	Can Change Coverage? n	
Unrestricted Call List: 1		
Access to MCT? y	Fully Restricted Service? n	
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n	
Send ANI for MFE? n	Add/Remove Agent Skills? n	
MF ANI Prefix:	Automatic Charge Display? n	
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n	
	Can Be Picked Up By Directed Call Pickup? y	
	Can Use Directed Call Pickup? y	
	Group Controlled Restriction: inactive	

## 6. Configure Avaya Aura® Application Enablement Services

Application Enablement Services enable Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager. Application Enablement Services (AES) receives requests from CTI applications, and forwards them to Communication Manager. Conversely, Application Enablement Services (AES) receives responses and events from Communication Manager and forwards them to the appropriate CTI applications.

**Note:** The installation and setup of the AES in a High Availability environment is outside the scope of these Application Notes and it is therefore assumed that installation and basic administration of the Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, creating a CTI link for TSAPI, and a CTI user. For further information on Avaya Application Enablement Services please refer to **Section 12** of these Application Notes.

Launch a web browser, enter **https://<IP address of AES server>** in the URL, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console page.



Click on **Communication Manager Interface** → **Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.

**AVAYA** Application Enablement Services Management Console

Welcome  
Last login:  
HostName:  
Server C  
SW Vers

**Communication Manager Interface | Switch Connections**

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management

Switch Connections

CMHA Add Connection

Connection Name	Processor Ethernet	Msg Period	Num
CMHA	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

The next window that appears prompts for the Switch Password. Enter the same password that was administered on Communication Manager in **Section 5.1**. Default values may be used in the remaining fields. Click on **Apply**.

**AVAYA** Application Enablement Services Management Console

**Communication Manager Interface | Switch Connections**

AE Services  
Communication Manager Interface  
Switch Connections  
Dial Plan  
Licensing  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

Connection Details - CMHA

Switch Password .....

Confirm Switch Password .....

Msg Period 30 Minutes (1 - 72)

SSL ☒

Processor Ethernet ☒

Apply Cancel

After returning to the **Switch Connections** page, select the radio button corresponding to the switch connection added previously, and click on **Edit PE/CLAN IPs**.

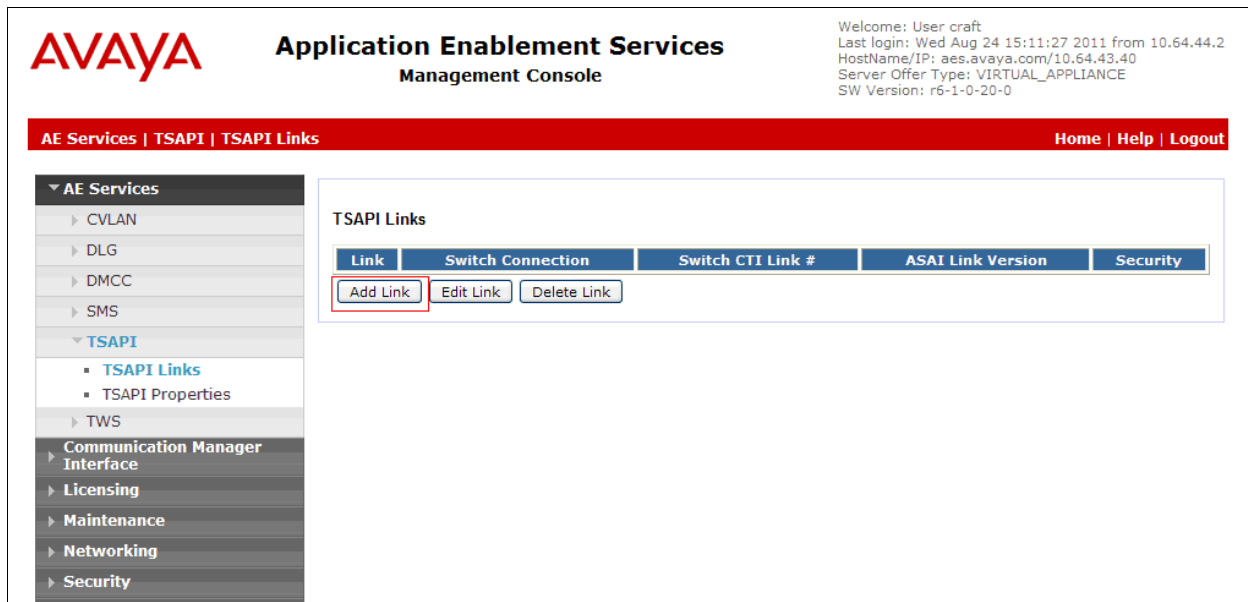
The screenshot shows the Avaya AES Management Console interface. The left sidebar contains a navigation menu with options like AE Services, Communication Manager Interface, Switch Connections, Dial Plan, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled 'Switch Connections' and features a table with columns: Connection Name, Processor Ethernet, Msg Period, and Number of Active Connections. A table entry for 'CMHA' is shown with 'Yes' for Processor Ethernet, '30' for Msg Period, and '1' for Number of Active Connections. Below the table, several buttons are visible: 'Edit Connection', 'Edit PE/CLAN IPs' (highlighted with a red box), 'Edit H.323 Gatekeeper', 'Delete Connection', and 'Survivability Hierarchy'.

Enter the IP address of the procr from **Section 5.1**, and click on **Add/Edit Name or IP**.

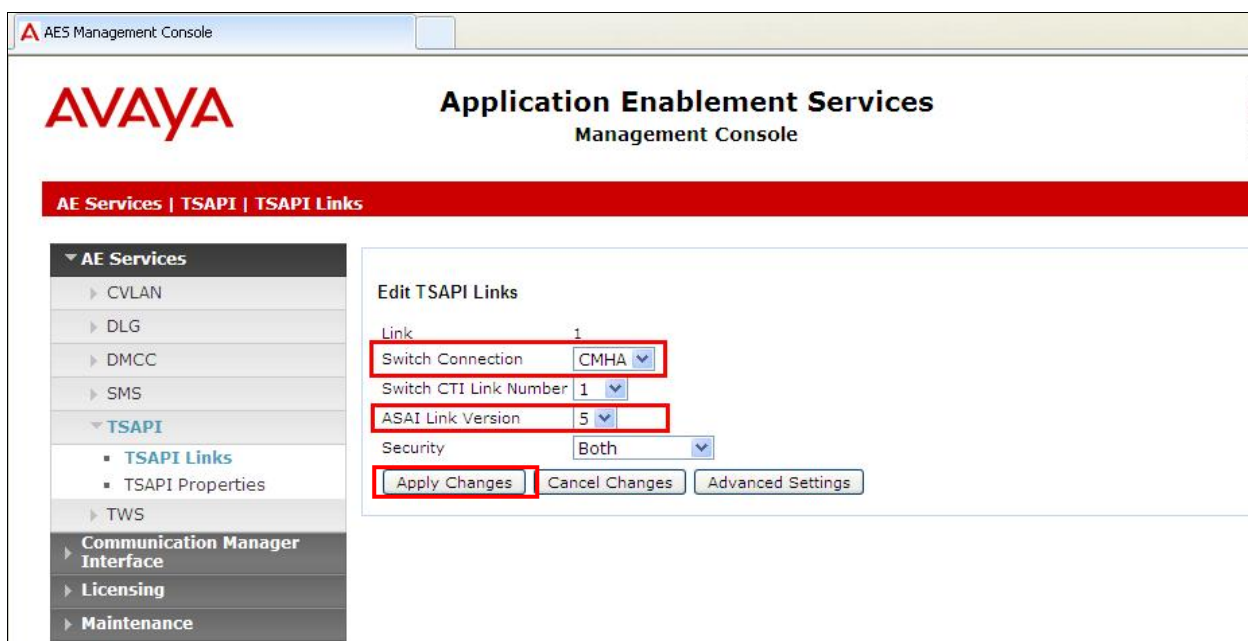
This screenshot displays the 'Edit Processor Ethernet IP - CMHA' dialog box within the Avaya AES Management Console. The dialog has a text input field containing the IP address '192.168.10.20' and a button labeled 'Add/Edit Name or IP', both of which are highlighted with red boxes. Below the input field, there is a table with a single row containing the same IP address '192.168.10.20' under the header 'Name or IP Address'. A 'Back' button is located at the bottom left of the dialog.

## 6.1. Configure TSAPI CTI Link

Navigate to **AE Services → TSAPI → TSAPI Links** to configure the TSAPI CTI link. Click the **Add Link** button to start configuring the TSAPI link.



Select the switch connection using the drop-down menu. Select the switch connection configured in **Section 6.1**. Select the **Switch CTI Link Number** using the drop-down menu. The **ASAI Link Version** is set to **5**. The CTI link number should match with the number configured in the CTI-link in **Section 5.1**. Click **Apply Changes**.



## 6.2. Configure CTI User

Navigate to **User Management** → **Add User**. On the **Add User** page, provide the following information.

- **User Id**
- **Common Name**
- **Surname**
- **User Password**
- **Confirm Password**

Select **Yes** using the drop-down menu on the **CT User** field. This enables the user as a CTI user. Click the **Apply** button (not shown here) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

AES Management Console

User Management | User Admin | List All Users

**Edit User**

\* User Id: nice

\* Common Name: nice

\* Surname: nice

User Password: .....

Confirm Password: .....

Admin Note:

Avaya Role: None

Business Category:

Car License:

CM Home:

Cms Home:

CT User: Yes

Department Number:

Display Name:

Employee Number:

Click on **Networking** → **Ports** enable port **4723** for the **TR87** SIP Interface as shown below.

**AES Management Console**

**Ports**

CVLAN Ports	Unencrypted TCP Port	9999	Enabled	Disabled
	Encrypted TCP Port	9998	<input checked="" type="radio"/>	<input type="radio"/>

---

DLG Port	TCP Port	5678	Enabled	Disabled
			<input checked="" type="radio"/>	<input type="radio"/>

---

TSAPI Ports	TSAPI Service Port	450	Enabled	Disabled
			<input checked="" type="radio"/>	<input type="radio"/>

---

Local TLINK Ports	TCP Port Min	1024	Enabled	Disabled
	TCP Port Max	1039	<input checked="" type="radio"/>	<input type="radio"/>

---

Unencrypted TLINK Ports	TCP Port Min	1050	Enabled	Disabled
	TCP Port Max	1065	<input checked="" type="radio"/>	<input type="radio"/>

---

Encrypted TLINK Ports	TCP Port Min	1066	Enabled	Disabled
	TCP Port Max	1081	<input checked="" type="radio"/>	<input type="radio"/>

---

DMCC Server Ports	Unencrypted Port	4721	Enabled	Disabled
	Encrypted Port	4722	<input checked="" type="radio"/>	<input type="radio"/>
	TR/87 Port	4723	<input checked="" type="radio"/>	<input type="radio"/>

Click on **Security** → **Host AA** → **Service Settings**. Ensure that **Require Trusted Host Entry** is ticked.

**AES Management Console**

**AVAYA**

**Application Enablement Services Management Console**

**Security | Host AA | Service Settings**

**Service Settings**

Services	Authenticate Client Cert with Trusted Certs	Require Trusted Host Entry
TR/87	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DMCC	<input type="checkbox"/>	<input type="checkbox"/>

**Apply Changes** **Cancel Changes**



Click on **Security** → **Host AA** → **Trusted Hosts**, click on **Add** to add a new trusted host.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. Under Security, the following options are listed: Account Management, Audit, Certificate Management, Enterprise Directory, Host AA (highlighted), Trusted Hosts (highlighted), Service Settings, PAM, and Security Database. The main content area is titled 'Trusted Hosts\*' and contains a table with the following data:

Certificate CN or SubAltName	Service Type	User Authentication Policy	User Authorization Policy
AACCSGM60	TR87	AUTHENTICATION_NOT_REQUIRED	UNRESTRICTED_ACCESS

Below the table are buttons for 'Add', 'Edit', and 'Delete'. A note at the bottom states: '\* Note: This page is only enforced to be configured if the "Require Trusted Host Entry" checkbox is checked on the "Service Settings" page.'

Enter the information as it is shown below. Ensure **Service Type** is **TR/87** and click on **Apply Changes**.

The screenshot shows the 'Add Trusted Host' form in the Avaya Application Enablement Services Management Console. The form is titled 'Add Trusted Host' and contains the following fields:

- Certificate CN or SubAltName: AACCSGM60
- Service Type\*: TR/87 (dropdown menu)
- User Authentication Policy\*: Not Required (dropdown menu)
- User Authorization Policy\*: Unrestricted Host (dropdown menu)

At the bottom of the form are two buttons: 'Apply Changes' and 'Cancel Changes'.



### 6.3. Avaya Aura® Application Enablement Services Certificate Management

Click on **Security** → **Certificate Management** → **CA Trusted Certificates**. Click on **Import** to import the **Certificates** from Contact Centre. The certificates required and their location are outlined in **Section 7.3** of these Application Notes. These certificates are as follows.

- **AACCSGM60Root.pem**
- **AEServicesRoot.cer**

**Note:** An avi video outlined in **Section 7.3** is available giving instructions on adding the certificates onto AES.

AVAYA Application Enablement Services Management Console

Welcome: User craft  
Last login: Tue Mar 13 14:15:57 2012 from 10.1  
HostName/IP: aes1/192.168.10.41  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

Security | Certificate Management | CA Trusted Certificates

CA Trusted Certificates

View Import Export Delete

Alias	Status	Issued To	Issued By	Expiration Date
<input type="checkbox"/> AEServicesRoot	valid	Avaya HDTG Product Root	Avaya Product Root CA	Aug 23, 2022
<input type="checkbox"/> AACCSGM60Root	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	Aug 17, 2027
<input type="checkbox"/> avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	Aug 14, 2033
<input type="checkbox"/> avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	Aug 17, 2027

Once imported is selected above the following screen appears. Below is an example of adding the **AEServicesRoot** certificate. Browse to the location of this certificate and once selected (not shown) click **Apply**.

AES Management Console

AVAYA

Application Enablement Services  
Management Console

Security | Certificate Management | CA Trusted Certificates

▶ AE Services

▶ Communication Manager  
Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▼ Certificate Management

▪ CA Trusted Certificates

Trusted Certificate Import

Certificate Alias

Certificate PEM:

File Path

Once the two **CA Trusted Certificates** are added, click on **Server Certificates**, click on **Import** to import the server certificate from Contact Centre. The location of this certificate is shown in **Section 7.3** of these Application Notes. This certificate is as follows.

- **AEServices**

**AVAYA** Application Enablement Services Management Console

Welcome: User craft  
Last login: Tue Mar 13 14:15:57 2012 from 10.  
HostName/IP: aes1/192.168.10.41  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-1-30-0

Security | Certificate Management | Server Certificate Home | Help

Server Certificates

Alias	Status	Issued To	Issued By	Expiration Date
<input type="checkbox"/> aeservices	valid	AEServices	Avaya HDTG Product Root	Jan 6, 2018

Once **Import** is selected above the following screen appears. Select **aeservices** from the drop-down menu, click on **Browse** to locate the certificate, once selected (not shown) click **Apply**.

**AVAYA** Application Enablement Services Management Console

Security | Certificate Management | Server Certificate

Server Certificate Import

Certificate Alias: **aeservices**

☒ Establish Chain of Trust

File Path:

Once all the certificates are added the services need to be restarted. Click **Maintenance** → **Service Controller**. Click on **Restart AE Server** as highlighted below to restart all the services.

The screenshot shows the Avaya AES Management Console interface. The top header includes the Avaya logo and the title 'Application Enablement Services Management Console'. A red banner below the header reads 'Maintenance | Service Controller'. On the left is a sidebar menu with categories like 'AE Services', 'Communication Manager Interface', 'Licensing', 'Maintenance', 'Security Database', 'Server Data', 'Networking', 'Security', 'Status', 'User Management', 'Utilities', and 'Help'. The 'Service Controller' link under 'Maintenance' is highlighted with a red box. The main content area is titled 'Service Controller' and contains a table with two columns: 'Service' and 'Controller Status'. The table lists several services, all of which are 'Running'. Below the table is a link 'Status and Control'. At the bottom of the main content area is a row of buttons: 'Start', 'Stop', 'Restart Service', 'Restart AE Server' (highlighted with a red box), 'Restart Linux', and 'Restart Web Server'.

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 type="checkbox"/> TSAPI Service	Running

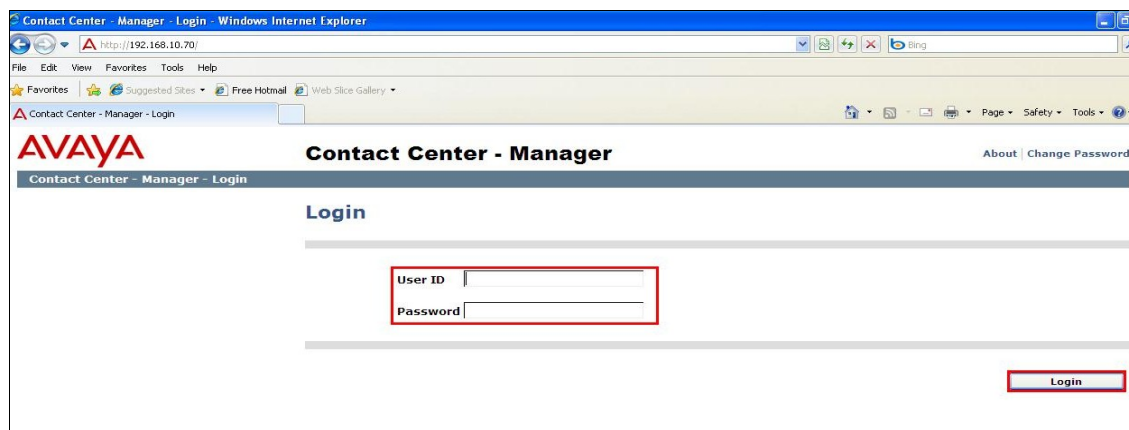
## 7. Configure Avaya Aura® Contact Centre

In order for NICE Interaction Management to be able to record calls from Contact Centre Agent calls a user must be configured on Contact Centre in CCT. This user can then log in to see events from CCT regarding the calls to Contact Centre agents. This section will go through the setup of this agent and the configuration necessary on both CCT and web services in order to record all calls coming into Avaya Contact Centre agents.

**Note:** The Installation and Setup of Contact Centre in a Mission Critical High Availability environment is outside the scope of these Application Notes. This section assumes that installation and basic administration of the Contact Centre server has been performed. The steps in this section describe the configuration of Contact Centre in order for NICE interaction Management to connect to CCT to receive events and successfully receive RTP from Avaya Media Server. For further information on Contact Centre please refer to **Section 12** of these Application Notes.

### 7.1. Configure NICE User on CCT

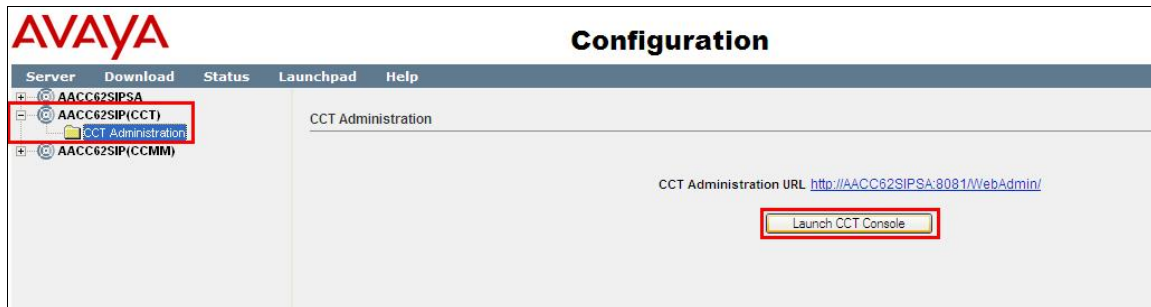
Launch a web browser, enter **https://<IP address of Contact Centre server>** in the URL, and log in with the appropriate credentials for accessing the **Contact Center - Manager** Console page.



Once logged in, click on **Configuration** as shown below.



Expand on the CCT server on the left-hand pane as shown and select **CCT Administration**. Click on **Launch CCT Console** in the right-hand pane.



Right click on **Uses** highlighted below.

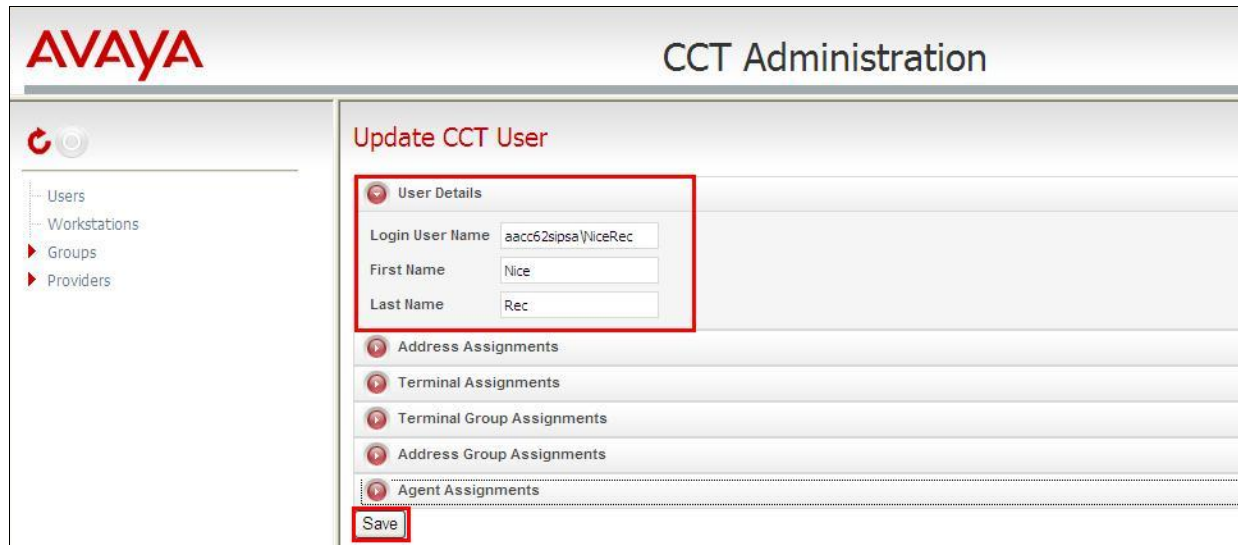


Click on **Add New User**.





Enter the credentials as shown below. Note these same credentials will be used in **Section 9.1** of these Application Notes.



**AVAYA** CCT Administration

**Update CCT User**

**User Details**

Login User Name: aacc62sipsa\NiceRec

First Name: Nice

Last Name: Rec

Address Assignments

Terminal Assignments

Terminal Group Assignments

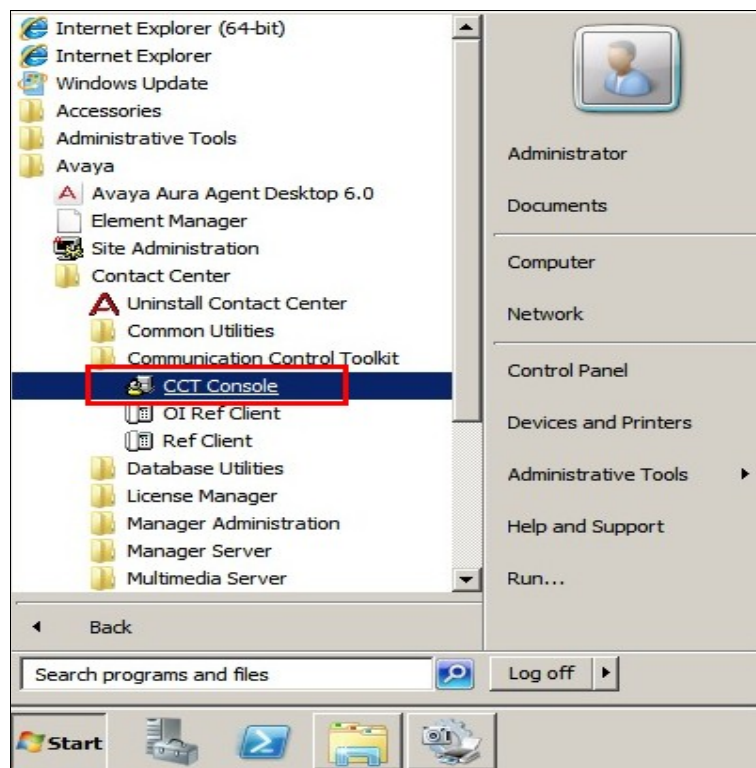
Address Group Assignments

Agent Assignments

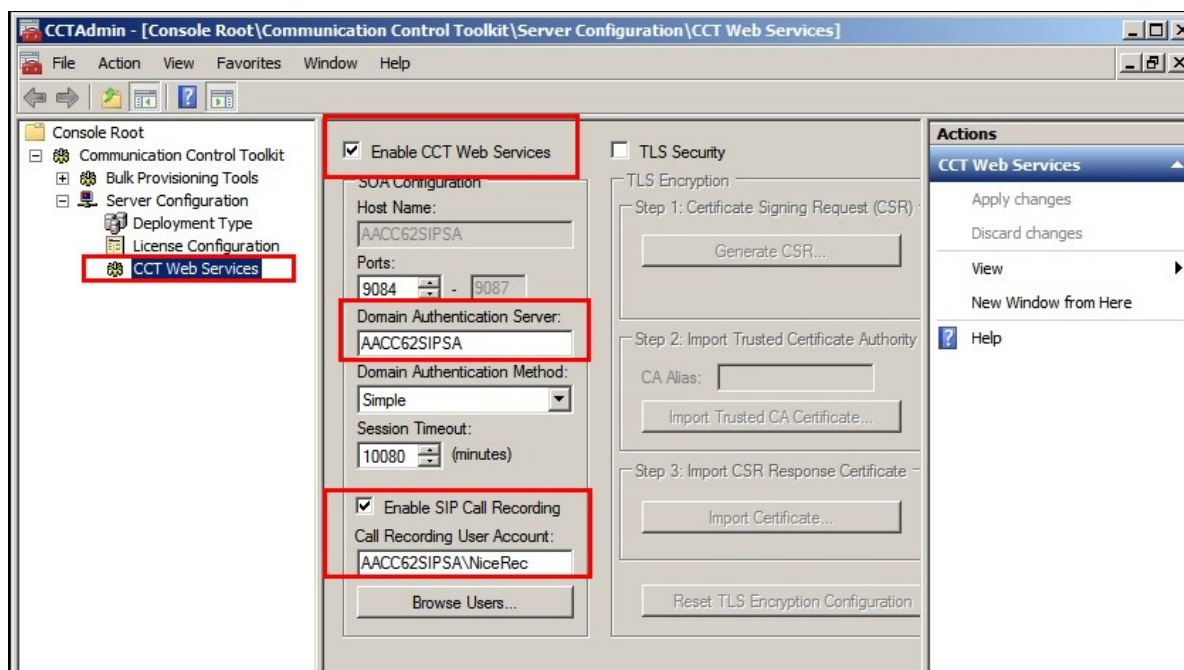
**Save**

## 7.2. Enabling CCT Web Services

On the Contact Centre server navigate to **Start → Programs → Avaya → CCT Console** as shown below.

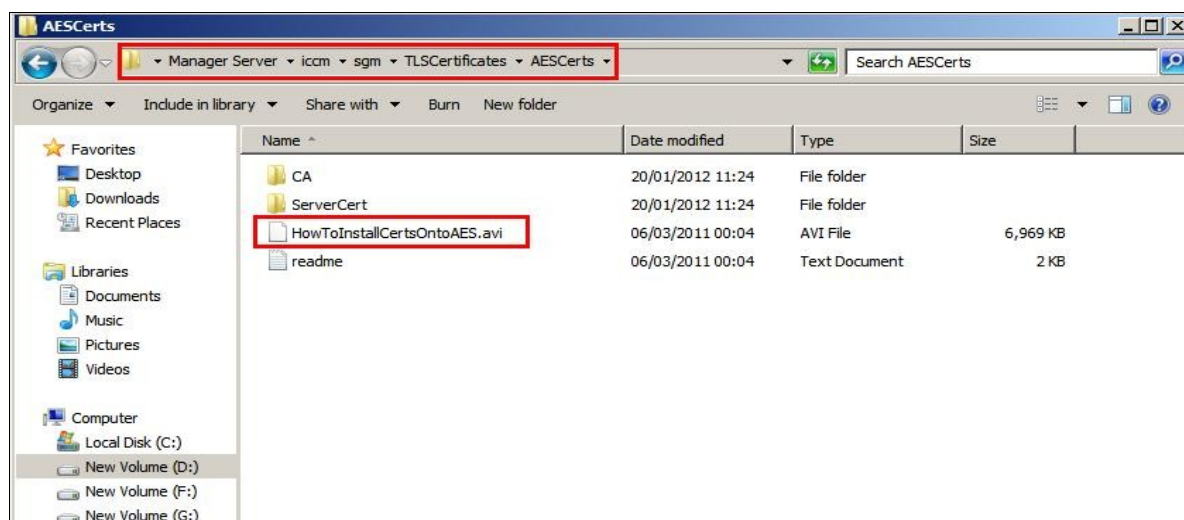


The **CCTAdmin** page is displayed as shown. Click on **CCT Web Services** in the left column and ensure that **Enable CCT Web Services** is ticked along with **Enable SIP Call Recording**. Enter the Contact Centre server name for **Domain Authentication Server** and the user configured in **Section 7.1** for the **Call Recording User Account**.



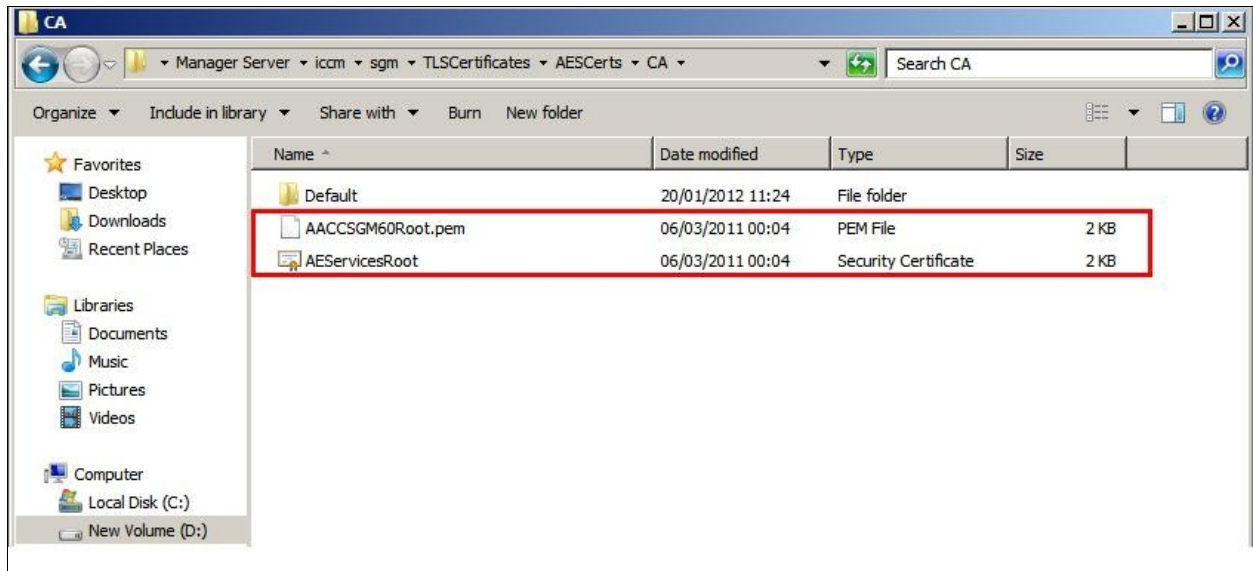
### 7.3. Locating Certificates for Avaya Aura® Application Enablement Services

Locate the certificates required for AES by navigating to **D: → Avaya → Manager Server → iccm → sgm → TLSCertificates → AESCerts**. Two CA Trusted Certificates are located in the CA folder and the Server certificate is located on the ServerCert as shown below. To assist in adding these certificates in **Section 6.3** open the **avi** named **HowToInstallCertsOntoAES**.

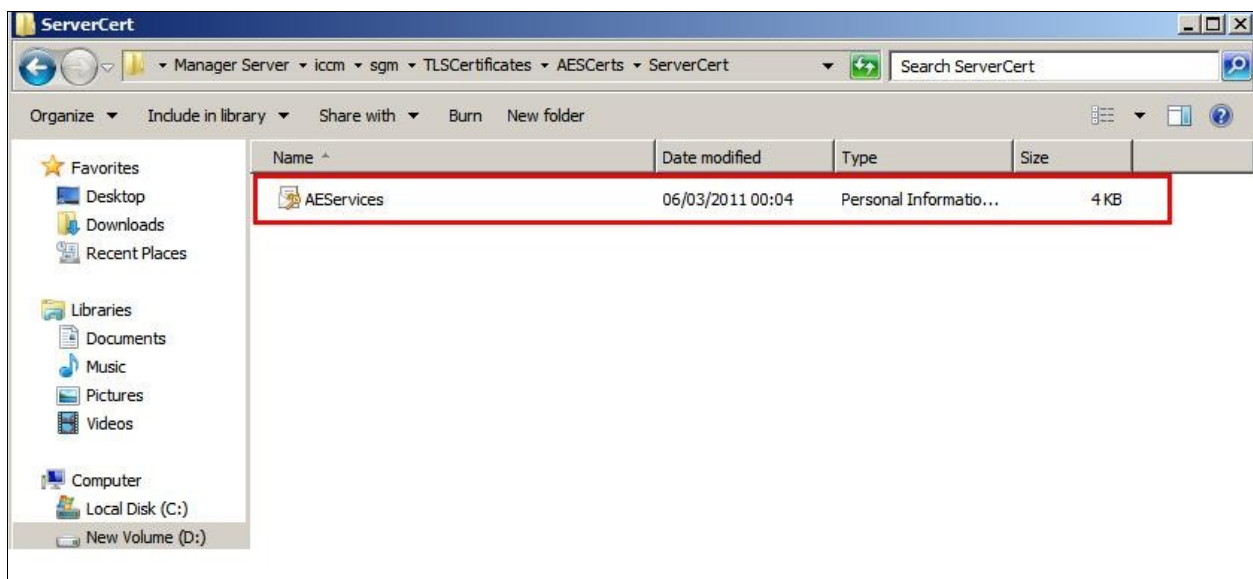




Open the folder above called CA, copy the two files highlighted below to a location for use in **Section 6.3**.

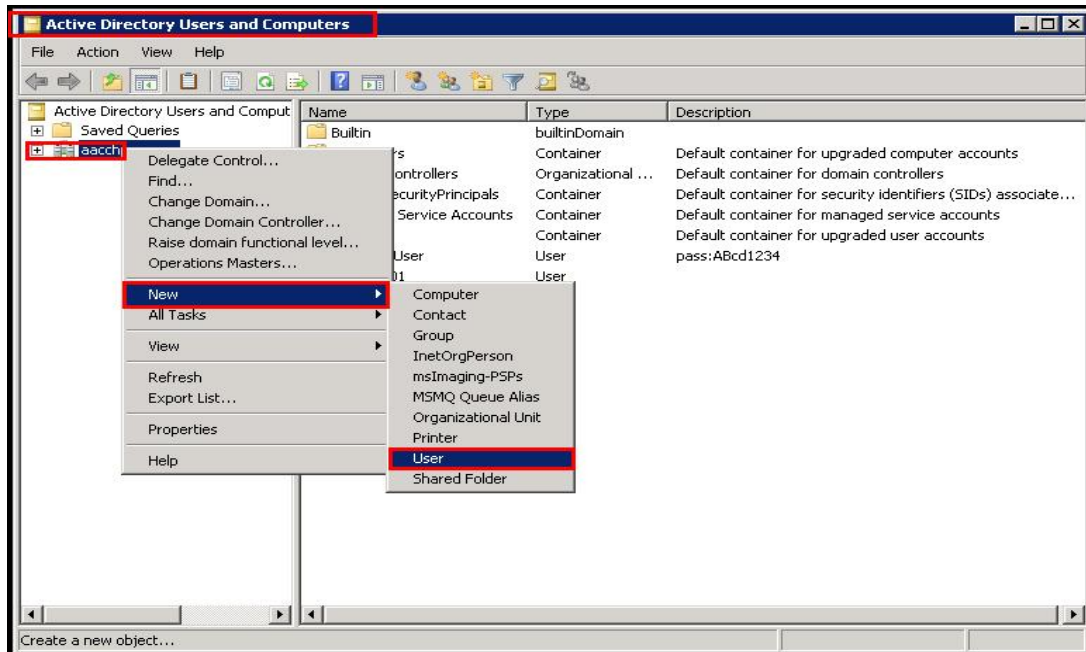


Open the folder **ServerCert** as shown in the previous page, copy the file highlighted below to a location for use in **Section 6.3**.

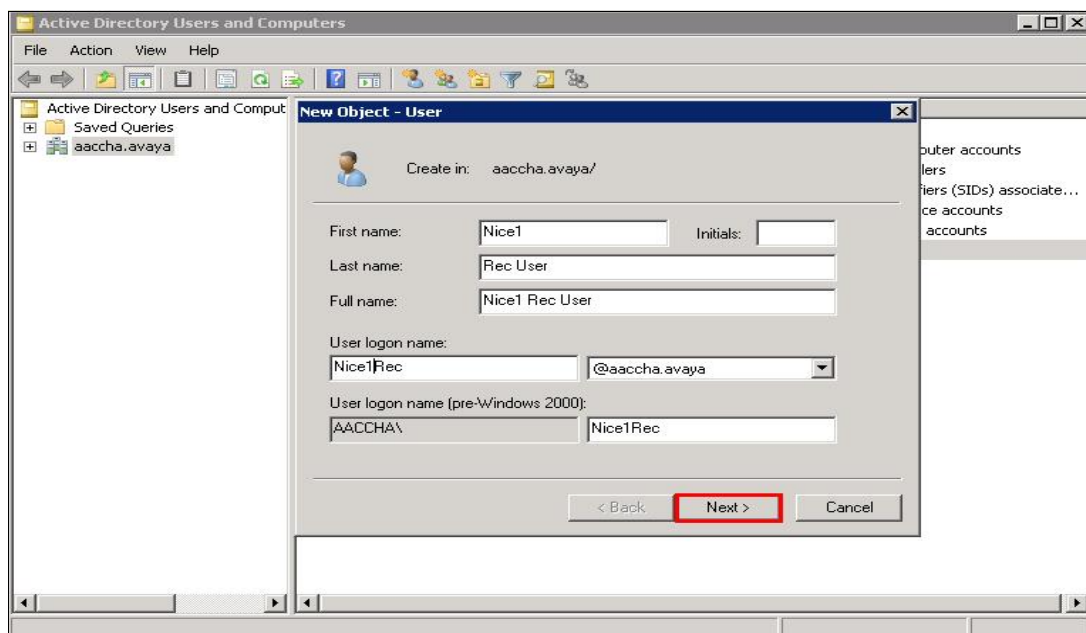


## 8. Configure Domain Controller

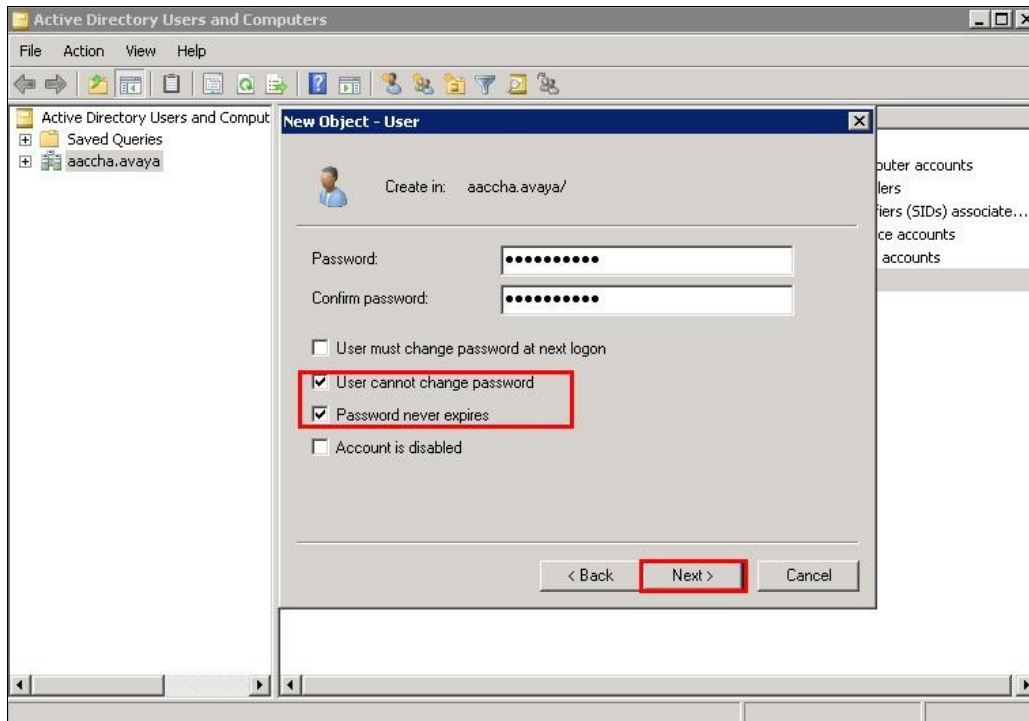
The CCT user configured in **Section 7.1** above must also be configured as a domain user on the Primary Domain Controller Server. Open **Active Directory Users and Computers** and right click on the server name, select **New** → **User**.



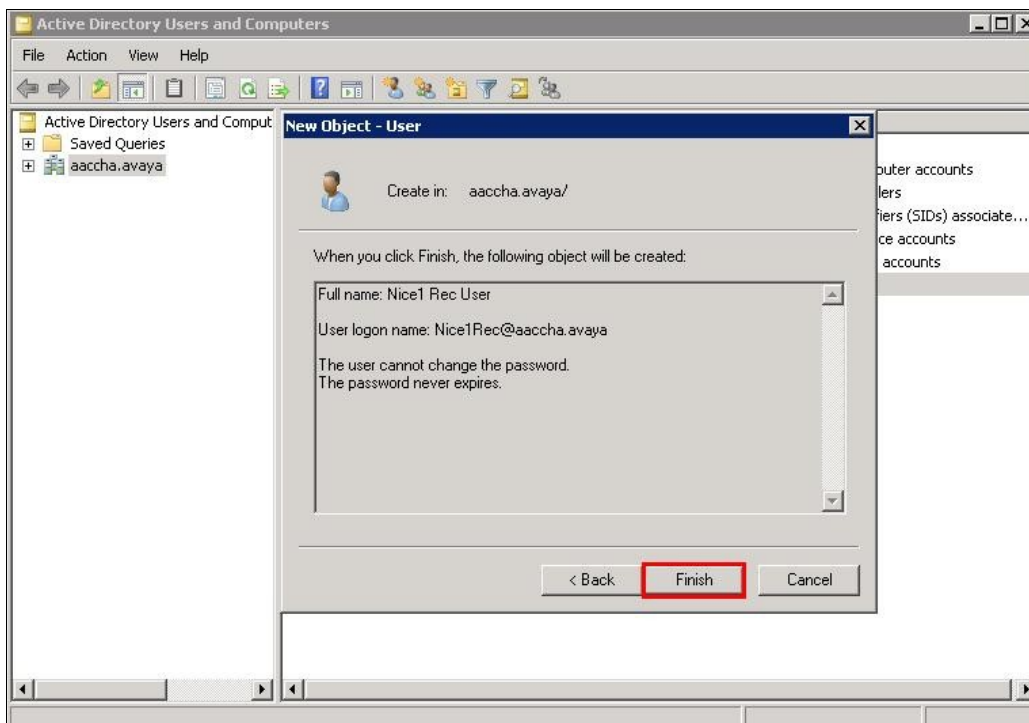
Fill in the **User login name** and other credentials as shown, click **Next** to continue.



Enter a suitable **Password** and ensure that **User cannot change password** and **Password never expires** are ticked. Click **Next** to continue.



Click **Finish** to complete adding the new user.



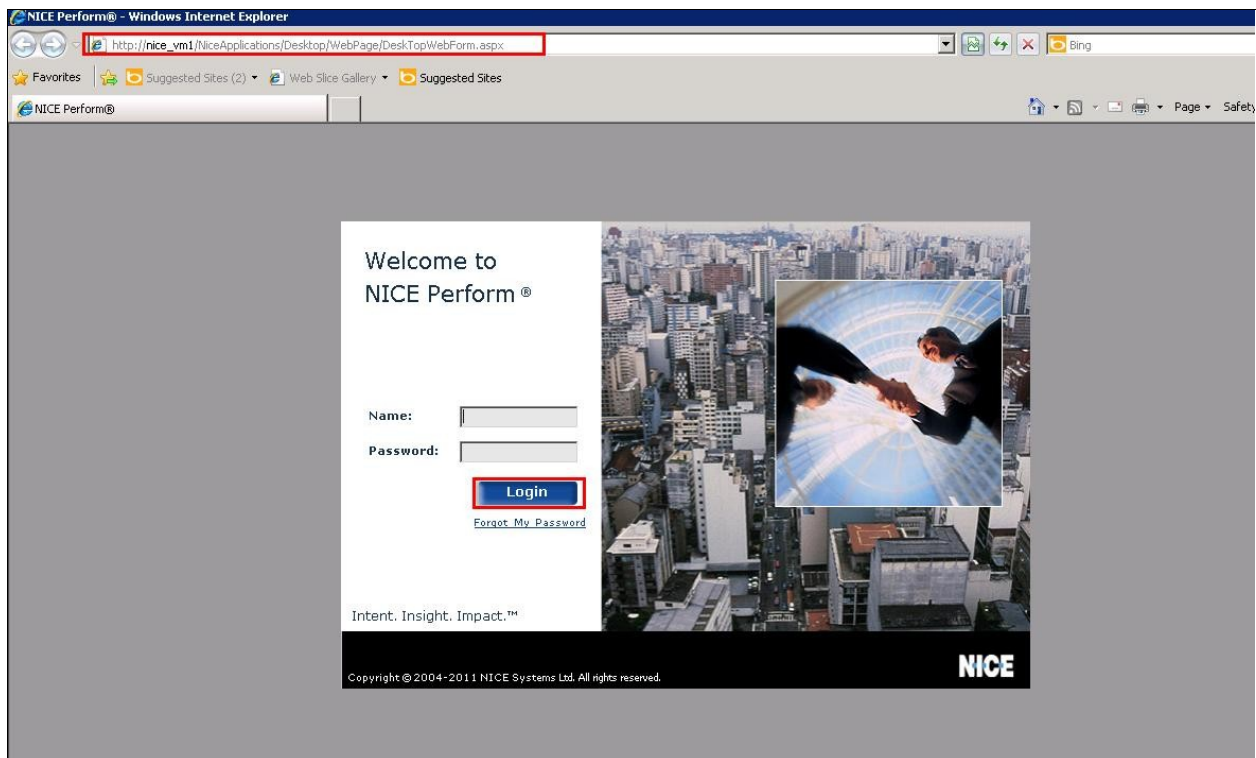
## 9. Configure NICE Integration Management

This section outlines the steps necessary to configure NICE Integration Management to connect successfully to the Avaya Solution outlined in **Section 3** of these Application Notes. The NICE Solution connects to the Communication Control Toolkit (CCT) module of Contact Centre as a CCT agent in order to receive events from the Contact Centre. These events are only passed to the NICE server when a Skillset call is being received by the agent. In order to receive events for calls made on the Avaya Deskphones an interface to the AES is configured to receive events via DMCC and TSAPI.

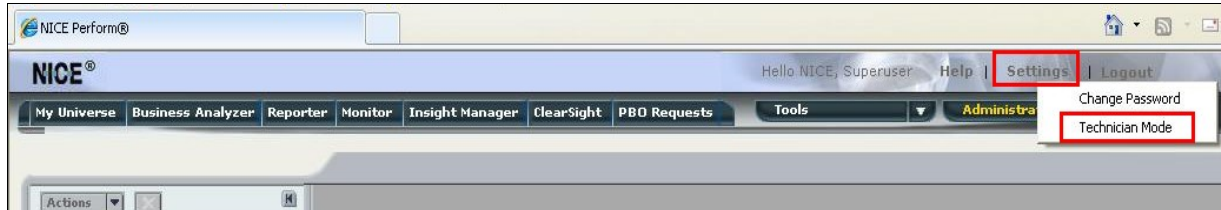
**Note:** In the case of a High Availability Contact Centre the NICE Interaction Management connects to a floating IP Address. This is common to both the active server and standby server and thus never changes regardless of the system that is active.

### 9.1. Configure NICE Interaction Management to connect to Communication Control Toolkit

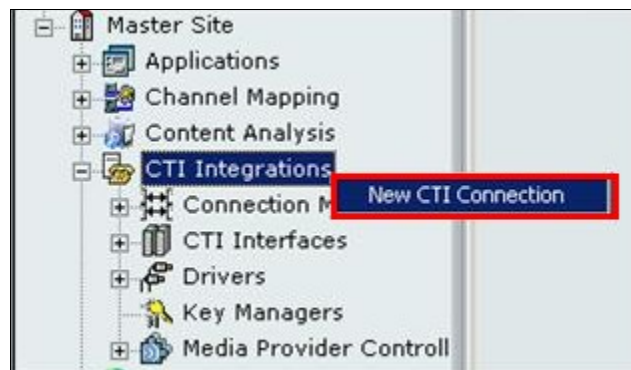
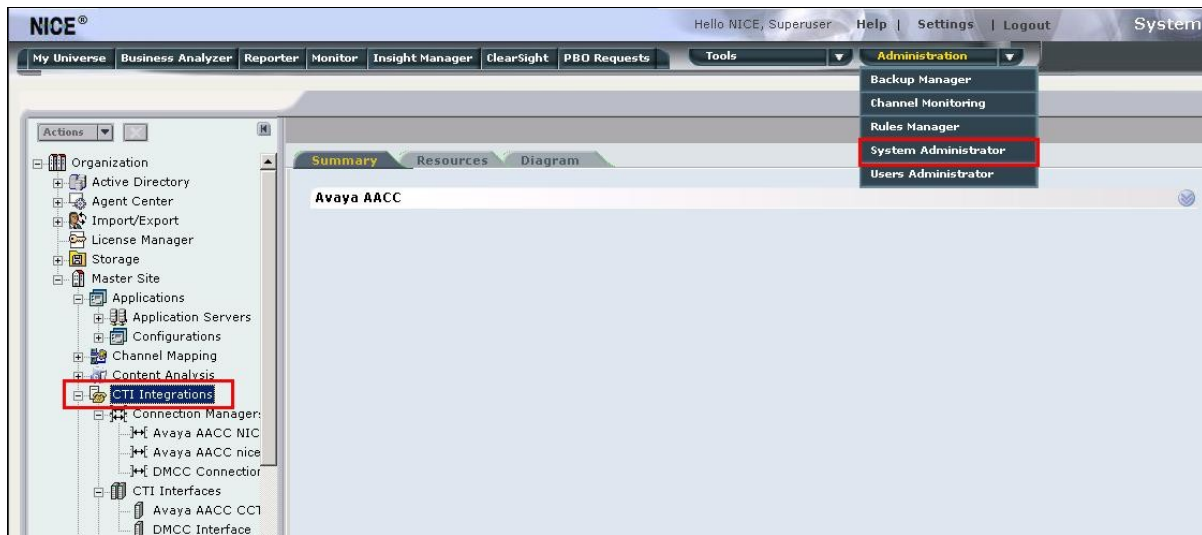
Open a web browser, navigate to `http://<NICE Interaction machine name>`. Enter the appropriate credentials and click **Login**.



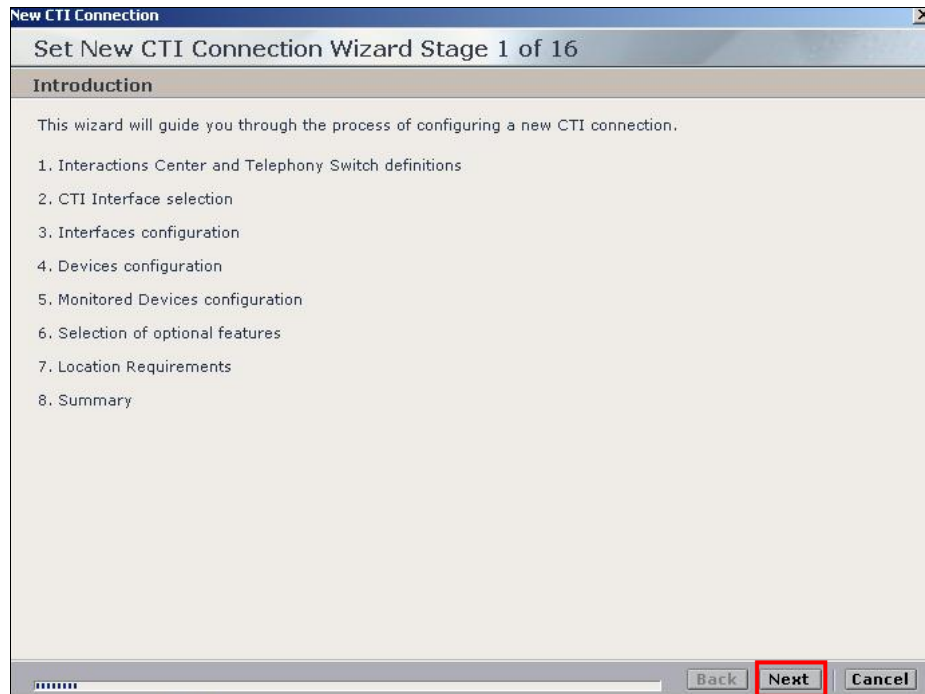
After logging in click on **Settings** highlighted below and choose **Technician Mode**.



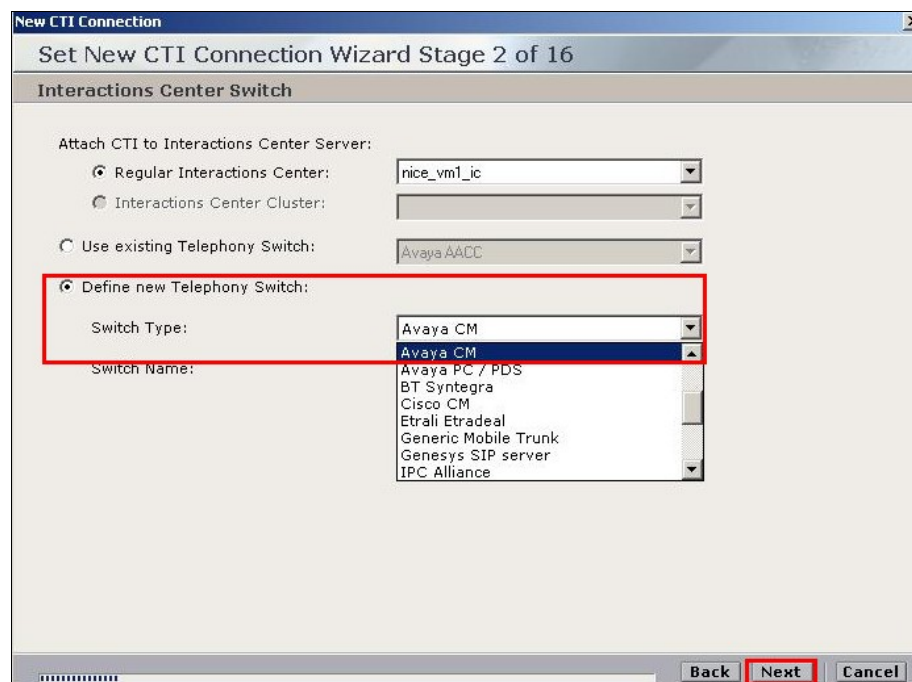
Under **Administration** at the top right select **System Administrator**. Right click on CTI integrations and select **add New CTI Connection** (see below).



The **New CTI Connection** window opens as shown below. Click **Next** to continue.



Select **Define new Telephony Switch** and ensure **Avaya CM** is picked from the drop-down menu. Click **Next** to continue.





Ensure **CCT** is chosen for both **Avaya CM CTI Interface** and **Active Recording** as shown below. Click **Next** to continue.

The screenshot shows the 'Set New CTI Connection Wizard Stage 3 of 16' window. The 'Interface Type' section is highlighted with a red box. It contains the following fields:

- CTI Interface Type:** A dropdown menu with 'CCT' selected. Below it, the text 'Avaya Communication Manager' and 'CCT' are visible.
- VolP Mapping:** A dropdown menu with 'AES SMS' selected.
- Additional VolP Mapping:** A dropdown menu with 'AES SMS' selected.
- Active Recording:** A checkbox is checked, and a dropdown menu with 'CCT' selected is next to it. Below it, the text 'Avaya Communication Manager' and 'CCT' are visible.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red box), and 'Cancel'.

Enter the connection details (**Username, Password, Domain** and **Address**) to the CCT as configured in **Section 7.1**. Click **Next** to continue.

The screenshot shows the 'Set New CTI Connection Wizard Stage 4 of 16' window. The 'Interface Parameters' section is highlighted with a red box. It contains the following fields:

- CTI Interface Details:** A section header.
- Interface Connection Details:** A section header.
- Mandatory fields are marked in bold:** A note.
- Parameter Value Table:** A table with two columns: 'Parameter' and 'Value'. The parameters are: Username, Password, Domain, Address, Port (9080), and Client Port ID (7070).
- Description:** A text field with the value 'CCT Server Username'.
- Additional Interface Parameters:** A section header.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red box), and 'Cancel'.

Enter the **Media Provider Controllers – Location**; this will be the IP address of the NICE logger server as shown in **Section 9.3**. Click **Next** to continue.

New CTI Connection

Set New CTI Connection Wizard Stage 8 of 16

Active Recording

**Media Provider Controllers - Location**

Media Provider Location

Server IP/Hostname: machinehost/ip

Connection Manager Port: 62094

Media Provider Controllers:

IP/Hostname	CM Port
machinehost/ip	62094

Back Next Cancel

Add **Telephony Switch Devices** in order to record private DN calls via DMCC. Each **Device** or extension can be added singly or in a **Range** of extensions. Click on **Add** highlighted below.

New CTI Connection

Set New CTI Connection Wizard Stage 10 of 16

Devices

**Available Devices**

Provide telephony switch available devices

0 devices

Add Add Range Add From Switch

Device Number	Type
---------------	------

Back Next Cancel



Enter a suitable **Name**, select **Extension** for **Device Type** and enter the extension number for each deskphone that is to be recorded for the **Device Number**. Click **OK** when finished.

**Available Device**

**Add Device**

Name

**Device Type:** \*

**Device Number:** \*

**Advanced Device Parameters**

☐ Display Read Only Information

Name	Value
------	-------

Description:

**OK** **Cancel**

Select **Create a new Connection Manager** and use a unique port. Click **Next** to pass to the summary window (shown below).

**New CTI Connection**

**Set New CTI Connection Wizard Stage 15 of 16**

**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:

☐ **Select available Connection Manager**

Ports in use:

- 62094
- 62095
- 62096

**Back** **Next** **Cancel**

**Summary** **Resources** **Diagram**

**Avaya AACC**

Component Type	Component Name	IP Address/Host Name
CTI Interface	Avaya AACC CCT Interface	
Connection Manager	Avaya AACC MPC Active Recording CM 1	AACCIC
Connection Manager	Avaya AACC AACCIC CM	AACCIC
Driver	Avaya AACC AACCIC Driver	AACCIC
Media Provider Controller	Avaya AACC AACCIC MPC	AACCIC

## 9.2. Configure NICE Interaction Management to connect to Application Enablement Services

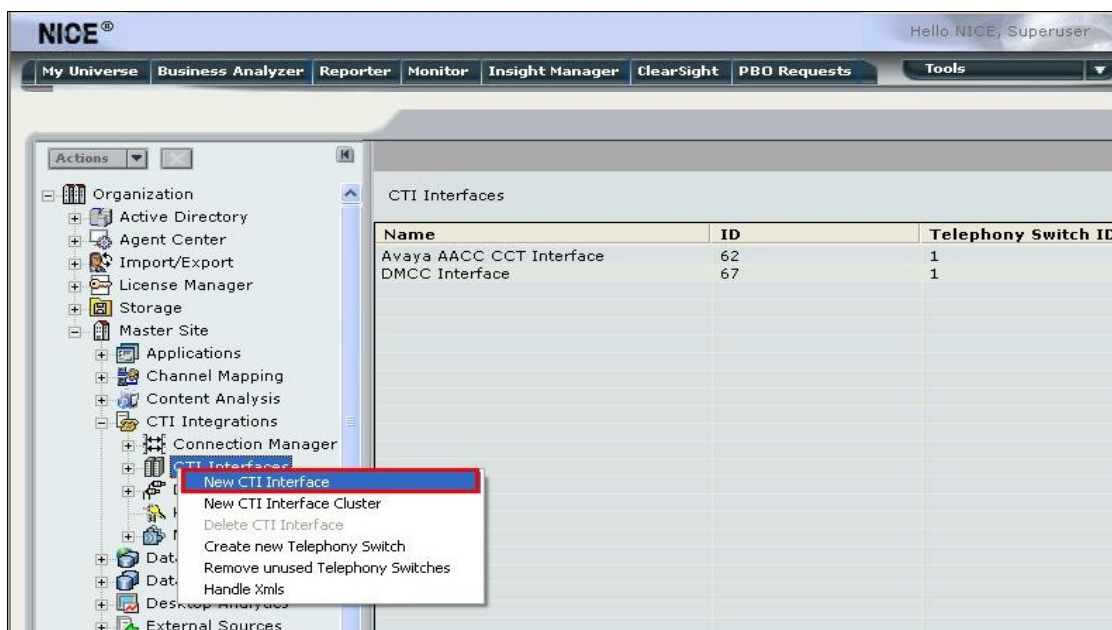
The previous section outlined the addition of a new CTI Connection which incorporates the setup of the following new configurations.

- **CTI Interface**
- **Connection Manager**
- **Media Provider Controller**

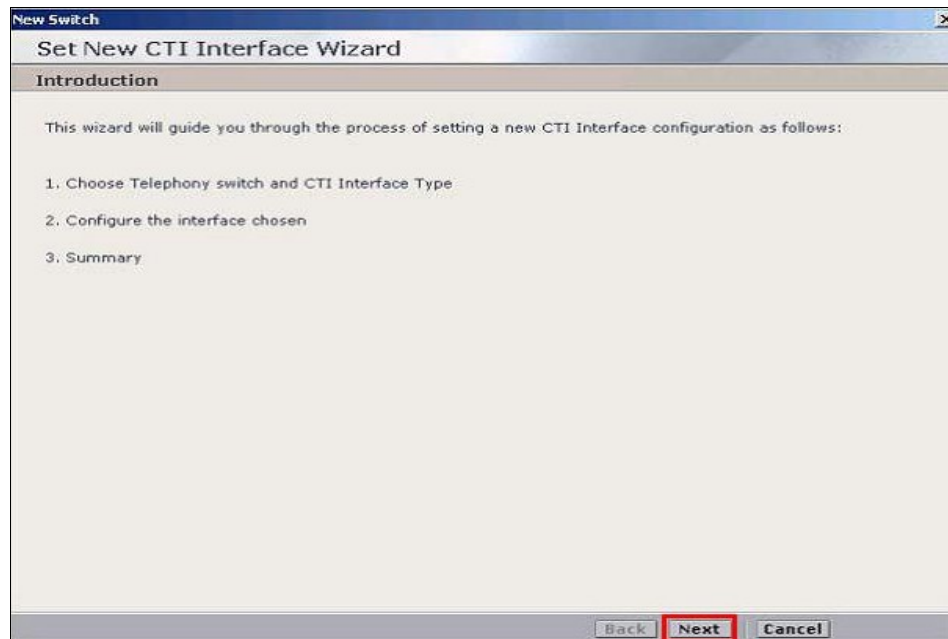
For Hybrid call recording or recording of non Contact Centre calls the DMCC must be configured to ensure that events from AES are being recorded. This means that a new CTI Interface, Connection Manager and Media Provider Controller must be setup.

### 9.2.1. Configure a new CTI Interface

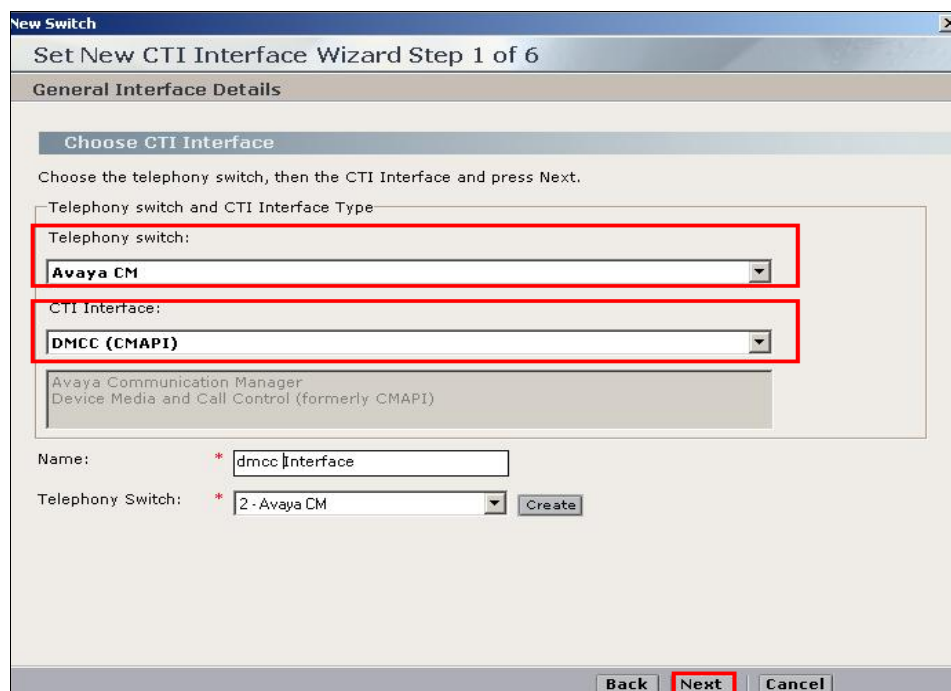
Navigate to **Master Site → CTI Integrations → CTI Interfaces**. Right click on **CTI Interfaces** and select **New CTI Interface**.



This brings up the window shown below. Click on **Next** to continue.



Ensure **Avaya CM** is selected for the **Telephony switch** and **DMCC (CMAPI)** for **CTI Interface** and click **Next**.



Enter the connection details for the AES (**Username**, **Password**, **Domain** and **Address**) to the AES as configured in **Section 6.2**.

New Switch

Set New CTI Interface Wizard Step 2 of 6

Switch Connection and Additional Details

General Interface Info

Interface Connection Details

☐ Display Read Only Information Mandatory fields are marked in bold

Parameter

Value

PrimaryAESServerAddress	
PrimaryAESMAPIPort	4722
PrimaryAESUserName	
PrimaryAESPassword	
PrimaryAESSecuredConnection	TRUE
UseAESWarmStandbyFeature	FALSE

Description:

Additional Interface Parameters

Back

Next

Cancel

Click on **Add** or **Add Range** if a group of extensions are to be configured.

The screenshot shows the "Set New CTI Interface Wizard Step 3 of 6" window, specifically the "Switch Devices Configuration" tab. The main area is titled "Set Devices". Underneath, it says "Available Devices" and "Provide telephony switch available devices". It indicates "0 devices" are currently listed. To the right of this text are three icons: a magnifying glass, a close button (X), and an edit button (pencil). Further right are three buttons: "Add", "Add Range", and "Add From Switch", all of which are highlighted with red rectangles. Below this is a table with two columns: "Device Number" and "Type". The table is currently empty. At the bottom of the window, there are three navigation buttons: "Back", "Next", and "Cancel". The "Next" button is also highlighted with a red rectangle.

Enter a suitable **Name**, select **Virtual Extension** for **Device Type** and enter the extension number configured in **Section 5.2** for the **Device Number**. Click **OK** when finished.

**Available Device**

**Add Device**

Name:

**Device Type:** \*

**Device Number:** \*

**Advanced Device Parameters**

☐ Display Read Only Information

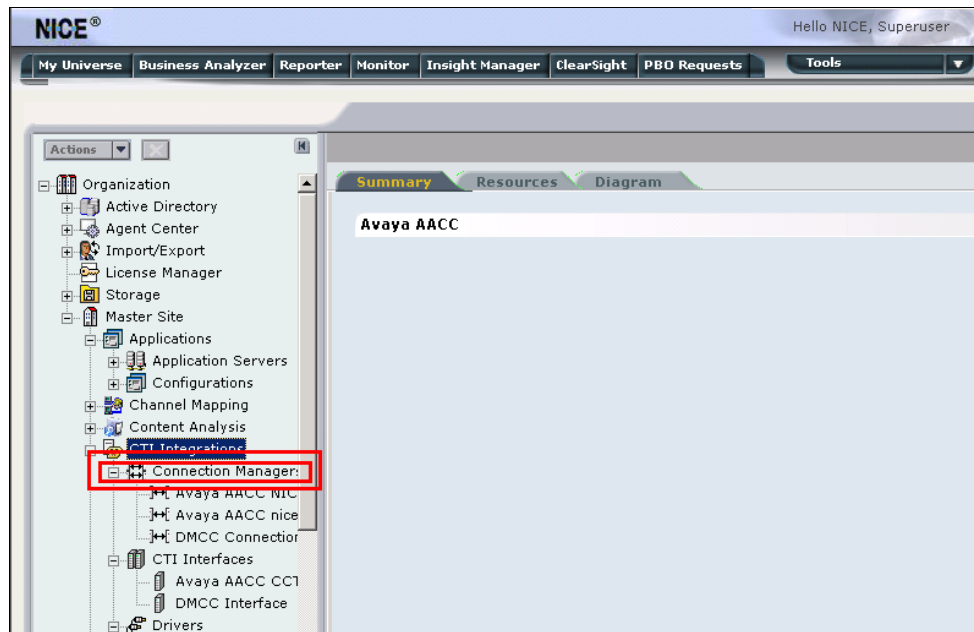
Name	Value
ObservationType	None
SymbolicName	
Password	
CodecsList	0
FncAlnlst	n

**Description:**

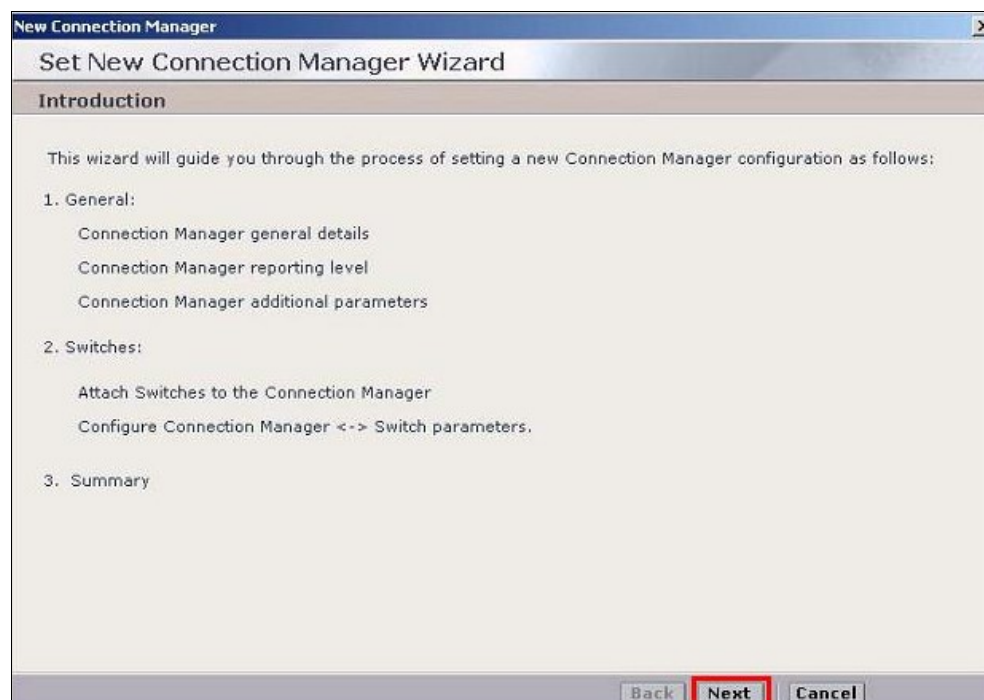
**OK** **Cancel**

### 9.2.2. Configure new Connection Manager

Navigate to **Master Site** → **CTI Integrations** → **Connection Manager**. Right click on **Connection Manager** and select **New Connection** (not shown).



This brings up the window shown below. Click on **Next** to continue.





Enter a suitable name for the new connection and enter the IP address of the NICE logger server (see **Section 9.3** for explanation of NICE Loggers) for **IP/Hostname**. Click on **Next** to continue.

New Connection Manager

Set New Connection Manager Wizard Step 1 of 3

General

Connection Manager Details

General Details

Name: \* New Connection Manager

\* Location

IP/HostName:

Port: 62094

Connection Manager Reporting Level

Additional Connection Manager Parameters

Back Next Cancel

Select the DMCC interface as previously configured in **Section 9.2.1**, under **Available Interfaces**. Click on **Next** to continue.

New Connection Manager

Set New Connection Manager Wizard Step 2 of 3

Switches

Attach CTI Interfaces

Available Interfaces

1 : AACC Interface

1 : DMCC Interface

2 : Lina Test Avaya AACC Interface

1 : CCS IMM Interface

Attached Interfaces

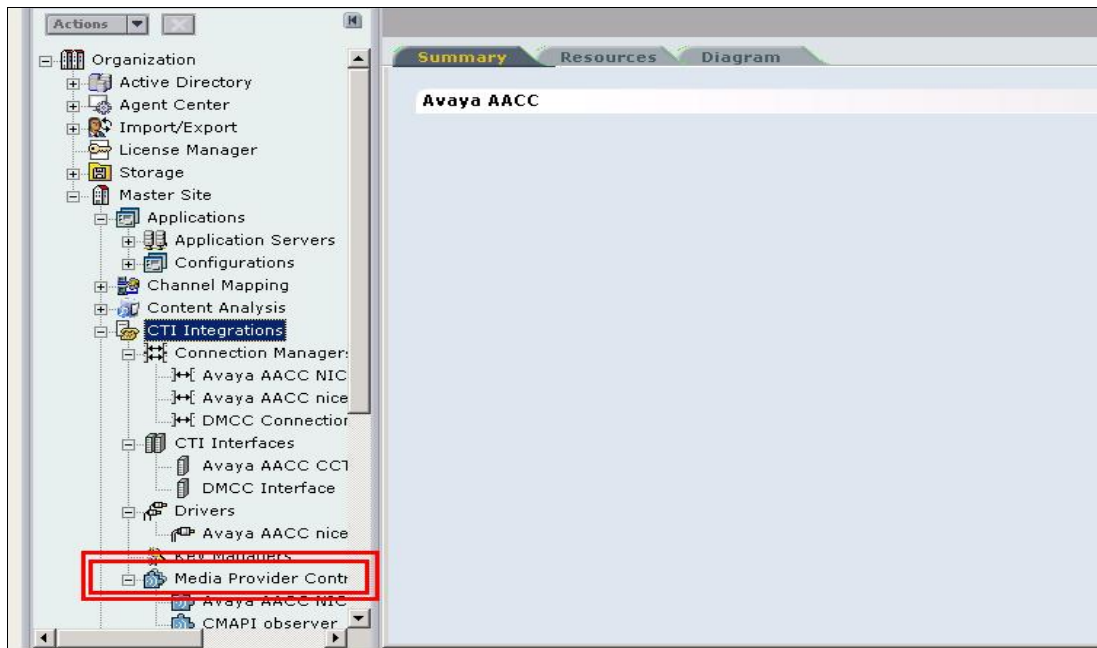
Configure Connection Manager - Interface Parameters

Back Next Cancel

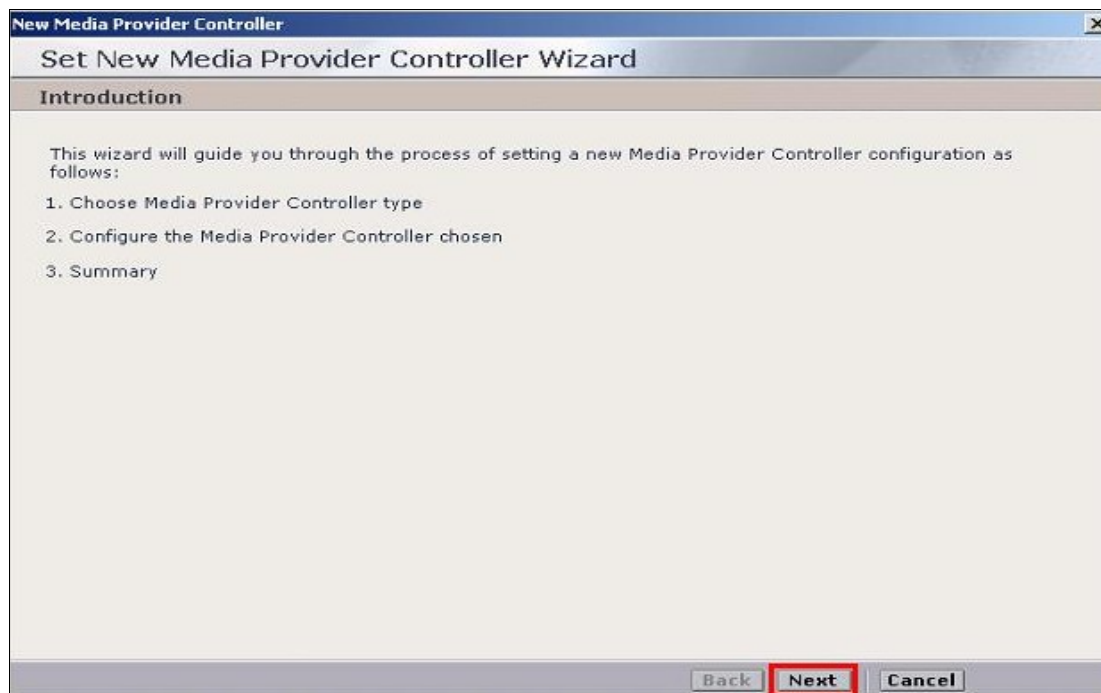


### 9.2.3. Configure a new Media Provider Controller

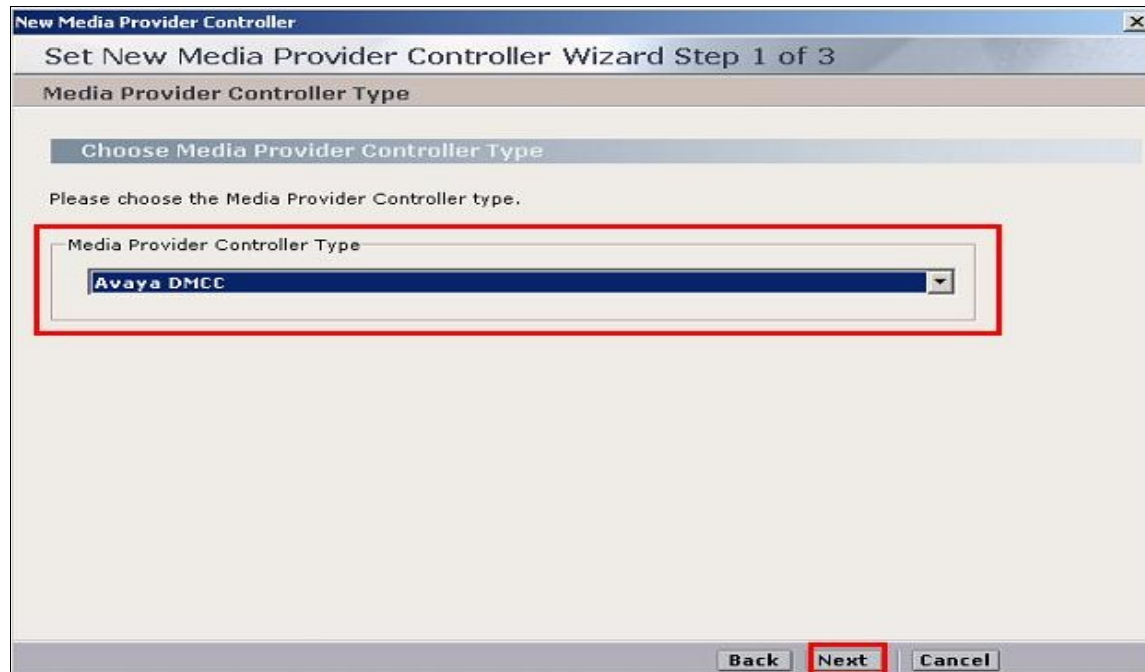
Navigate to **Master Site → Media Provider Controllers**. Right-click **Media Provider Controllers** and select New Media Provider Controller (not shown).



This brings up the window shown below. Click on **Next** to continue.



For the DMCC Media Provider Controller select **Avaya DMCC** for the **Media Provider Controller Type**. Click **Next** to continue.



New Media Provider Controller

Set New Media Provider Controller Wizard Step 1 of 3

Media Provider Controller Type

Choose Media Provider Controller type

Please choose the Media Provider Controller type.

Media Provider Controller Type

Avaya DMCC

Back Next Cancel

Enter a suitable **Name** and enter the IP Address of the NICE Logger Server for **IP/Hostname**. The DMCC loggers IP address will be filled in for the DMCC Controller (see **Section 9.3** for the DMCC Logger configuration). Click **Next** to continue.



New Media Provider Controller

Set New Media Provider Controller Wizard Step 2 of 3

General Information

Media Provider Controller General Information

Media Provider Controller Type

General Details

Name: \* New Media Provider

\* Location

IP/HostName:

Attach Connection Manager

Additional Media Provider Controller Parameters

Media Provider Controller Reporting Level

Back Next Cancel

Expand the **Attach Connection Manager** highlighted on the previous page. This brings up the page shown below. In the **Available Connection Managers** list select the appropriate Connection Manager. For the DMCC controller, add the DMCC Connection Manager configured in **Section 9.2.2**. Click on **Next** to continue.

The screenshot shows a Windows-style dialog box titled "New Media Provider Controller" with a subtitle "Set New Media Provider Controller Wizard Step 2 of 3". The "General Information" tab is selected. Under "Media Provider Controller General Information", the "Attach Connection Manager" section is expanded. It contains two panes: "Available Connection Managers" and "Attached Connection Manager". The "Available Connection Managers" list includes:

- 1 - AACC aaccvrsr Active Recording CM
- 2 - AACC AACCIC CM
- 3 - DMCC Connection Manager
- 4 - Lina Test CM
- 5 - FIVE941 OCS CM

A red box highlights the right arrow button between the two panes. The "Attached Connection Manager" pane is empty. At the bottom, the "Next" button is highlighted with a red box, along with "Back" and "Cancel" buttons.

### 9.3. Configure NICE Loggers

NICE Loggers are responsible for the recording of voice calls, using a SIP based Logger for the recording of Contact Centre agent calls with events from CCT and using a DMCC based Logger for recording all other calls from the Communication Manager deskphones with events from AES. For this compliance testing these loggers are installed on separate servers. Configuration of these loggers is performed from the same management console as used in **Sections 9.1 and 9.2**.

**Note:** The types of Loggers are defined as a part of the install of NICE Interaction Management and therefore will not be covered in these Application Notes. For more information on this install please refer to **Section 12** of these Application Notes. However the configuration of the installed NICE Loggers is required and is explained below.

Navigate to **Logger Servers → Nice Log**. Select the Logger that is to be configured. Under the general tab enter a suitable **Name** and enter the **Host Name/ IP Address** of the Logger server.

The screenshot displays the NICE Interaction Management console interface. The left-hand navigation pane shows a tree structure with 'Logger Servers' expanded, and 'NICE\_VM2 - DMCC logger' selected. The main content area is titled 'General' and contains the following configuration fields:

Logger Details	
Name	NICE_VM2 - DMC
Host Name/IP Address	192.168.10.72
Main Bus	IP
Logger ID	101

Capacity	
Logger Version	10.0
Number of Recording Channels	200
Online Capacity	5824 (ADPCM16) Hours

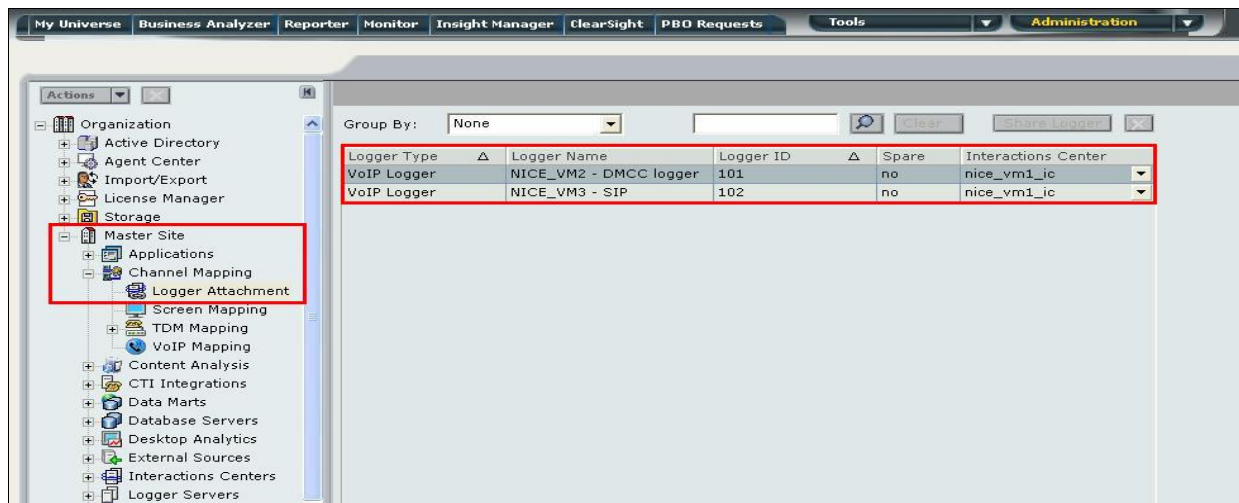
  

Advanced Configuration	
Cards	None
Compression Types	PCM, G729a, G723.6.3, G723.5.3

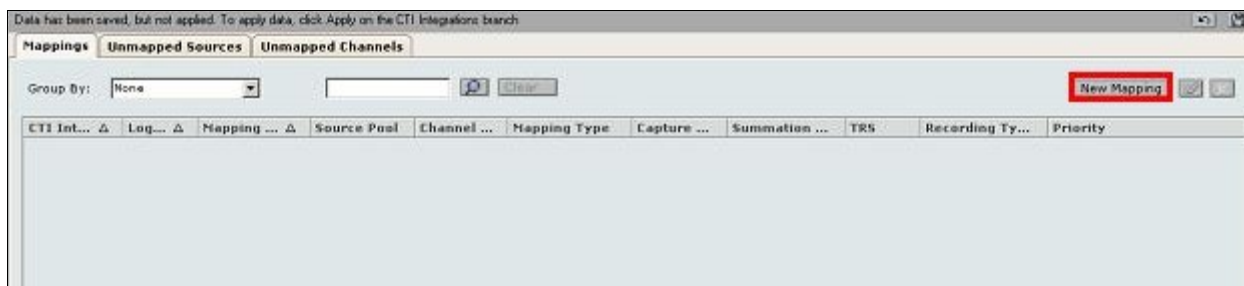
**Note:** Both the SIP and DMCC Loggers will need to be configured in order to successfully record both Contact Centre and Communication Manager calls.

## 9.4. Channel Mapping Configuration

The Loggers configured above must be associated with an **Interactions Center**. Navigate to **Master Site → Channel Mapping → Logger Attachment**. This brings up the page shown below with a list of Voice, VoIP and NICE Screen Loggers. To associate an interactions centre with a Logger simply select the interaction centre required from the **Interactions Center** drop-down menu. Both the SIP and DMCC Loggers configured in **Section 9.3** should be associated with an Interactions Center.

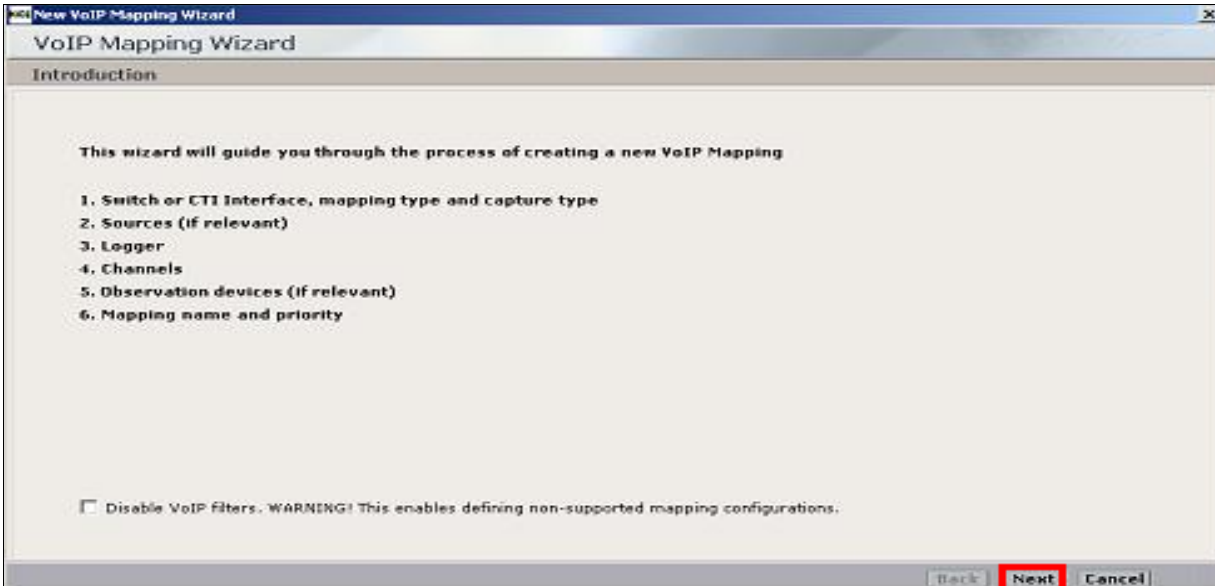


Navigate to **Master Site → Channel Mapping → VoIP Mapping**, which opens the window shown below. Click **New Mapping** highlighted to open the VoIP Mapping Wizard.

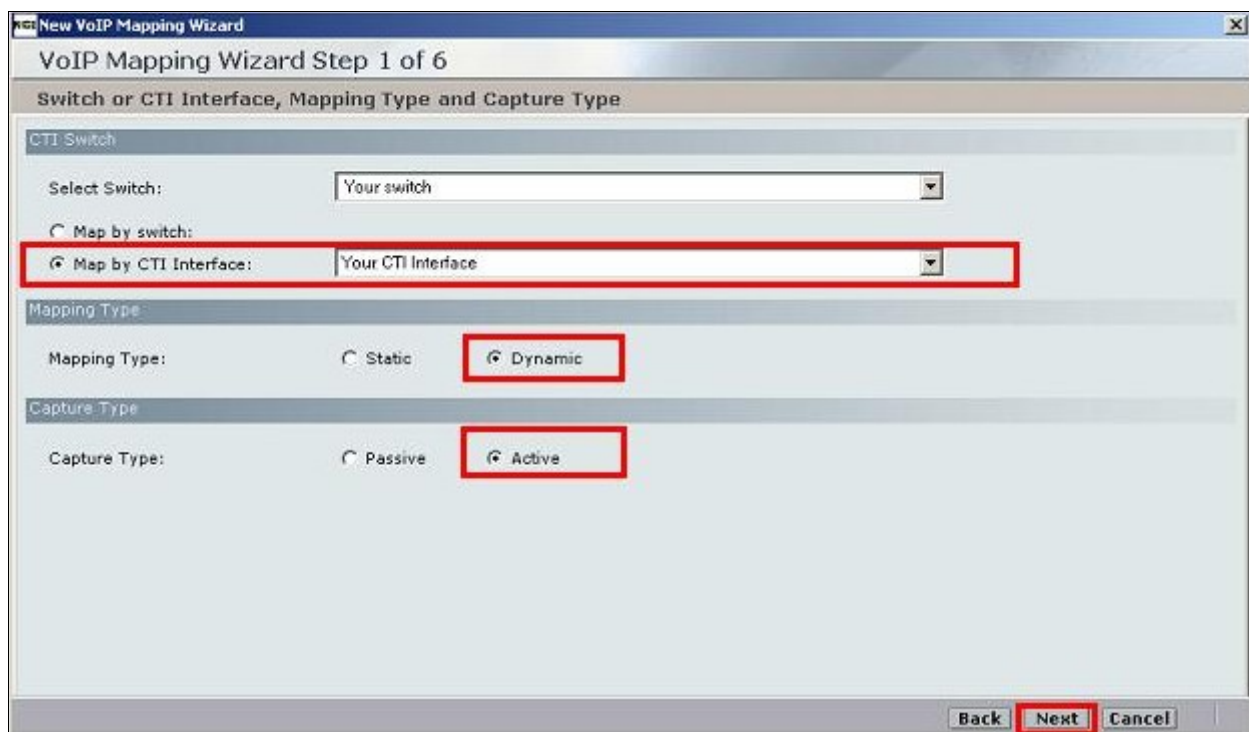




Click on **Next** to continue.



Ensure that **MAP by CTI Interface** is selected and that the relevant CTI Interface is chosen from the drop-down menu. For **Mapping Type**, select **Dynamic**. For **Capture Type**, select **Active**. Click **Next**. The Select Sources window appears.



Select **Create a new Source Pool**. Enter a Suitable name for the Source Pool. By default, all devices are selected, however not all devices may be relevant for channel mapping.

**VoIP Mapping Wizard Step 2 of 6**

**Sources for Source Pool**

**Sources**

☒ Create a new Source Pool ☐ Select an existing Source Pool

Create a Source Pool

Pool Name:

Group By:

Selected Sources: 2/2

	Source Name	Unique Device ...	IP Address	Port	Port Support	Device Number	Observation Type
<input checked="" type="checkbox"/>					Single Port	6223	NonResourceBased
<input checked="" type="checkbox"/>					Single Port	6253	NonResourceBased

Select the VoIP Logger for VoIP mapping. Click **Next** to continue.

**VoIP Mapping Wizard Step 3 of 6**

**Loggers**

Select a logger:

Logger ID	Logger Name	Type	Summation Mode	Capture Type	Is part of chain
101	NICE_VM2 - DMC...	VoIP Logger	Mono Recording	Active : CMAPI	no
102	NICE_VM3 - SIP	VoIP Logger	Mono Recording	Active : SIP	no



Select **Define Channels** and ensure that a suitable **Channel Pool Name** is chosen. In the **Number of Channels** field, enter the number of required channels for the pool, this determines the number of recordable devices in this Source Pool that can be simultaneously recorded. Click **Next** to continue.

New VoIP Mapping Wizard

VoIP Mapping Wizard Step 4 of 6

Channel Resources

Channels

☒ Define Channels ☐ Select an existing Channel Pool

Channel Pool Properties

This Logger is not part of an N+1 chain.

Channel Pool Name: ChannelPool 30001

Recording Type: Interaction Based By Call

Summation Mode: Mono Recording

Channels number: 1 of 24

Minimum number of channels for the pool is 1.  
Number of channels should not exceed number of available channels.  
Number of available channels is 24.

Back Next Cancel

In the **Mapping Name** field, enter a name for this channel mapping configuration. When necessary, set a **Priority**.

**Note:** Setting a **Priority** is a method of prioritizing recording resources for a specific mapping. This is relevant for site configurations in which one Source Pool is mapped to several Channel Pools or Loggers.

Click **Finish**. All of the devices in this defined Source Pool are mapped to VoIP Logger Recording channels.

The screenshot shows a window titled "New VoIP Mapping Wizard" with the subtitle "VoIP Mapping Wizard Step 6 of 6". The main heading is "Mapping Details and Summary".

Under "Mapping Name and Priority", there is a text field for "Mapping Name" containing "Mapping 30003" and a "Priority" dropdown menu set to "0".

Under "Mapping Summary", there is a table with the following data:

Mapping property name	Mapping property value
Switch	Avaya CM
CTI Interface	Avaya CM AACC Interface
Mapping type	Dynamic
Ratio of Sources to Channels	0 : 1

At the bottom right, there are three buttons: "Back", "Finish" (highlighted with a red box), and "Cancel".

**Note:** This configuration is required for both the SIP and DMCC Channel Mapping.

## 10. Verification Steps

The following steps can be taken to ensure that connections between Communication Manager, AES, Contact Centre and NICE Interaction Management are configured correctly.

### 10.1. Verify Avaya Aura® Communication Manager CTI link

Verify the status of the administered CTI link by using the **status aevcs cti-link** command. Verify the **Service State** is **established** for the CTI link number administered in **Section 5.1**, as shown below.

```
status aevcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	5	no	aes	established	15	15

### 10.2. Verify Avaya Aura® Application Enablement Services CTI link

From the Application Enablement Services Management Console web pages, verify the state of the TSAPI Service is set to **ONLINE** by selecting **Status** from the left pane.

**AVAYA** **Application Enablement Services**  
Management Console

Welcome: User craft  
Last login: Tue Sep 6 14:57:50 2011 from 10.64.44.2  
HostName/IP: aes.avaya.com/10.64.43.40  
Server Offer Type: VIRTUAL\_APPLIANCE  
SW Version: r6-1-0-20-0

StatusHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▼ Status

Alarm Viewer

▶ Logs

▶ Status and Control

▶ User Management

▶ Utilities

▶ Help

Services Summary

Service	State	Since	Cause
CVLAN Service	OFFLINE *	2011-08-30 16:01:21	NO_LICENSE_ACQUIRED
DLG Service	ONLINE	2011-08-30 16:01:18	NORMAL
DMCC Service	ONLINE	2011-08-30 16:01:22	NORMAL
TSAPI Service	ONLINE	2011-08-30 16:42:12	NORMAL

\* The state of the CVLAN and DLG services can either be ONLINE or OFFLINE. Also, the OFFLINE status would appear either until a link is administered or a valid license is acquired.

### 10.3. Verify that Web Services are running correctly

The following steps can be taken to ensure that Web Services are running correctly to allow NICE Interaction Management to receive call events to the API.

1. From any machine on the network, start Internet Explorer
2. Enter the following: <http://<ccmaservername>/supportutil/testwebservices.asp>
3. The web services that appear in green are running correctly

### 10.4. Verify NICE Interaction Management services are running

Go to Start → Services. Check the system services and make sure all NICE services are running. Highlighted below are a list of services that must be running to allow recording and playback of calls

NICE Coaching Server	Manages C...	Started	Automatic	.{Administ...
NICE Deployment Manager Agent	NICE Deplo...	Started	Automatic	.{Administ...
NICE Evaluation Forms Server	Manages E...	Started	Automatic	.{Administ...
NICE FTF Query Server	Performs q...	Started	Automatic	.{Administ...
NICE Integration Dispatch Service	Launches a...	Started	Automatic	.{Administ...
NICE Integration Log Services	Level Dum...	Started	Automatic	.{Administ...
NICE Interactions Center Core	Acts as the...	Started	Automatic	.{Administ...
NICE Interactions Center DBSrvr	Manages t...	Started	Automatic	.{Administ...
NICE Interactions Center Monitor	Report fail...	Started	Automatic	.{Administ...
NICE Interactions Center RCM	Responsibl...	Started	Automatic	.{Administ...
NICE Interactions Center TRS	Insert missi...	Started	Automatic	.{Administ...
NICE Investigations Server	Manages a...	Started	Automatic	.{Administ...
NICE IP Phone Applications	Performs I...	Started	Automatic	.{Administ...
NICE IPCapture	Controls a...	Starting	Automatic	.{Administ...
NICE Logging Service	A service d...	Started	Automatic	.{Administ...
NICE Media Provider Control Manager	An online r...	Started	Automatic	Local System
NICE Monitor Server	Performs ...	Started	Automatic	.{Administ...
NICE MyUniverse	Host for M...	Started	Automatic	.{Administ...
NICE NBA	Performs q...	Started	Automatic	.{Administ...
NICE Notification Service	Generates ...	Started	Automatic	.{Administ...
NICE Playback Administration	Manages A...	Started	Automatic	.{Administ...
NICE Playback Streaming	Manage M...	Started	Automatic	.{Administ...
NICE Reporter Engine	Nice Repor...	Started	Automatic	.{Administ...
NICE Reporter Scheduler	Nice Repor...	Started	Automatic	.{Administ...
NICE Retention Service	Performs r...	Started	Automatic	.{Administ...
NICE Rule Engine	Perform rul...	Started	Automatic	.{Administ...
NICE RulesManager Service	Manages w...	Started	Automatic	.{Administ...
NICE Storage Center Service	Nice Servic...	Started	Automatic	.{Administ...
NICE Storage Prepare	NICE Stora...	Started	Automatic	.{Administ...
NICE Storage Streaming Service	Responsibl...	Started	Automatic	.{Administ...
NICE SystemAdministrator	Perform Ni...	Started	Automatic	.{Administ...
NICE Text Capture	A service d...	Started	Automatic	.{Administ...
NICE VoIP Logger	Nice Syste...	Started	Automatic	.{Administ...
Offline Files	The Offline...	Disabled	Local System	
Performance Counter DLL Host	Enables re...	Manual	Local Service	

## 10.5. Verify calls are being recorded by NICE Interaction Management

Recordings are stored on the NICE Interaction Management server and can be replayed using **Business Analyzer** as shown below. Log in to NICE Interaction Management as shown in **Section 9.1**, click on the **Business Analyzer** tab. Select the Interactions tab on the left column and under **Queries** → **Public**, press on the query required.

The screenshot shows the NICE Business Analyzer interface. The top navigation bar includes 'My Universe', 'Business Analyzer' (highlighted with a red box), 'Reporter', 'Monitor', 'Insight Manager', 'ClearSight', 'PBO Requests', 'Tools', and 'Administration'. The left sidebar shows 'Interactions' (highlighted with a red box) and 'Queries' (highlighted with a red box). The main area displays a table of call records with columns: Type, Flag, Full Name, Complete Start, Complete Stop Time, Complete Duration, Score, Complete ID, Segments Compound ID, and Participants. The table shows 14 records found for the query 'Complete - Last 24 hours'.

Type	Flag	Full Name	Complete Start	Complete Stop Time	Complete Duration	Score	Complete ID	Segments Compound ID	Participants
2504, lyncuser5			27/03/2012 11:14:07	27/03/2012 11:14:23	00:00:16		5724502651937292333	5724502651937292333	
Unmapped, User			27/03/2012 10:58:32	27/03/2012 10:58:38	00:00:06		5724498679092543531	5724498679092543531	
Unmapped, User			27/03/2012 10:53:36	27/03/2012 10:56:46	00:03:11		5724497377717452840	5724497377717452840	
Unmapped, User			27/03/2012 10:53:06	27/03/2012 10:53:13	00:00:07		5724497235983532069	5724497235983532069	
Unmapped, User			27/03/2012 10:52:27	27/03/2012 10:52:31	00:00:03		5724497089954644002	5724497089954644002	
Unmapped, User			26/03/2012 15:06:02	26/03/2012 15:06:36	00:00:34		5724191369887547423	5724191369887547423	
Unmapped, User			26/03/2012 14:49:14	26/03/2012 14:49:34	00:00:20		5724187044855480348	5724187044855480348	
Unmapped, User			26/03/2012 14:41:36	26/03/2012 14:43:05	00:01:30		5724185073465491481	5724185073465491481	
Unmapped, User			26/03/2012 14:22:45	26/03/2012 14:23:07	00:00:22		5724180198677610518	5724180198677610518	
Unmapped, User			26/03/2012 14:09:50	26/03/2012 14:10:23	00:00:34		5724176887257825299	5724176887257825299	
Unmapped, User			26/03/2012 14:08:20	26/03/2012 14:08:25	00:00:04		5724176505005735952	5724176505005735952	
Unmapped, User			26/03/2012 13:47:16	26/03/2012 13:47:21	00:00:05		5724171071872106509	5724171071872106509	
Unmapped, User			26/03/2012 13:45:42	26/03/2012 13:45:50	00:00:08		5724170672440147978	5724170672440147978	
Unmapped, User			26/03/2012 13:42:45	26/03/2012 13:42:47	00:00:02		5724169890756100102	5724169890756100102	

Double click on any interaction in the table above to play it back. An example is shown below.

The screenshot shows the NICE Business Analyzer playback interface. The top bar displays 'Start: 27/03/2012 11:14:07', 'End: 11:14:23', 'Duration: 00:00:15', and 'Error occurred: Output allocated- pla'. The main area shows a timeline with a waveform and a list of participants: Customer and Agent. The timeline is marked with time intervals from 00:02 to 00:14. The participant list shows 'Customer' and '2504, lyncuser5'.

## 11. Conclusion

These Application Notes describe the configuration steps required for NICE Interaction Management R4.1 to successfully interoperate with Avaya Aura® Contact Centre and Avaya Aura® Application Enablement Services in a Mission Critical High Availability Environment. All test cases were completed successfully. Please refer to **Section 2.2** for test results and High Availability failover observations.

## 12. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com> where the following documents can be obtained.

- [1] *Administering Avaya Aura® Communication Manager, Document ID 03-300509*
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation, Document ID 555-245-205*
- [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 6.1 Issue 2*
- [4] *Avaya Aura ® Contact Centre SIP Commissioning, Doc # NN44400-511, Issue 3.02 Release 6.2*
- [5] *Avaya Aura ® Contact Centre Planning and Engineering, Doc # NN44400-210, Issue 3.03 Release 6.2*
- [6] *Avaya Aura ® Contact Centre Installation, Doc # NN44400-311, Issue 3.02 Release 6.2*

All information on the product installation and configuration of NICE Interaction Management can be found at <http://www.nice.com>

---

**©2012 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).