Avaya Solution & Interoperability Test Lab

Application Notes for Liquid Voice Assure Interaction Recording with Avaya Aura® Contact Center and Avaya Aura® Communication Manager using port mirroring of Avaya Session Border Controller for Enterprise to record trunk calls – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Liquid Voice Assure Interaction Recording V7.5 to interoperate with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Contact Center R7.1 using 'port mirroring' of Avaya Session Border Controller for Enterprise R8.1.1 to record trunk calls.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 Liquid Voice Assure Interaction Recording V7.5 to interoperate with Avaya Aura® Contact Center R7.1 and Avaya Aura® Communication Manager R8.1 using 'port mirroring' of Avaya Session Border Controller for Enterprise R8.1.1 to record trunk calls.

A PSTN is simulated using an Avaya Session Border Controller for Enterprise (ASBCE) connecting to another Avaya system. Calls are recorded by mirroring the external interface on the ASBCE. Recordings are started and stopped using SIP headers obtained from the mirrored port. Liquid Voice Assure Interaction Recording (Assure) connects to the Call Detail Recording (CDR) port on Communication Manager and to Communication Control Toolkit (CCT) Web Services to obtain both call and agent events to help provide the user with as much information as possible about each call recording.

On each of the agent's PCs the Liquid Voice PCI silencing client is installed, and this client has a connection in place with CCT to generate DTMF tones to the agent on call, pausing the recording when sensitive information is being exchanged.

This Liquid Voice system is fully integrated into a LAN (Local Area Network), and WAN (Wide Area Network) and includes easy-to-use Web based applications that works with .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. The Liquid Voice applications suite contains tools for audio retrieval, centralized system security authorization, system control, and system status monitoring. Also included is a call parameters database, search tools, a wide variety of Recording-on-Demand capabilities, and comprehensive long-term call database for immediate retrieval.

2. General Test Approach and Test Results

The general test approach was to validate the ability of Assure to correctly and successfully record telephone calls in a call center environment. Contact Center agents were logged into various Avaya endpoints (outlined in **Section 4**) and by mirroring the external port of the SBCE all RTP was sent to a dedicated Network Interface Card (NIC) on the Assure server. Recordings were made using the SIP headers from the packets received by Assure from the SBCE mirrored port.

The connection to CCT web services and to Communication Manager CDR are used to obtain information on each recording such as CLID, DNIS, agent ID and skillset information. The recordings can be made with or without these connections to CCT and Communication Manager. Both of these connections can be used individually or as a hybrid solution depending on what information is required to be displayed to the user, see *Application Notes for Liquid Voice Assure Interaction Recording with Avaya Aura® Communication Manager using port mirroring of Avaya Session Border Controller for Enterprise to record trunk calls*.

The Liquid Voice PCI silencing client is used to "pause" the recording when taking sensitive information on the customer. The PCI silencing client has a connection to CCT which allows the client to generate DTMF tones and send them down the line thus pausing the recording at that point. The PCI silencing client connects to the Pause Service for the configuration settings. The PCI silencing client uses the user's domain credentials on the client PC for Single Sign on to access the CCT service. When a pause request is generated, the PCI silencing client sends a request to the Avaya CCT service to generate DTMF tones on any of the user's terminals that are in a state that is capable of DTMF tone generation.

In total the Liquid Voice solution takes advantage of four separate connections to complete the full solution, that being:

1. CTI Call Detail connection to CCT to obtain agent events.
2. PCI silencing client to CCT to pause recordings.
3. CDR connection to Communication Manager to obtain call events.
4. Port Mirror connection to ASBCE to obtain the call recording itself.

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 interface between Avaya systems and Assure did not include use of any specific encryption features as requested by Liquid Voice.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on interacting with the Assure platform in different call scenarios. The tests included:

- **Inbound calls** – Test call recording for inbound calls to Communication Manager deskphones from the PSTN.
- **Outbound calls** – Test call recording for outbound calls from Communication Manager deskphones to the PSTN.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.

- **Contact Center Agent calls** – Call to CDN's answered by Agents, these calls include transfer and conference of other Agents.
- **PCI silencing client, DTMF testing** – Calls to agents using URL's to initiate DTMF tones to "pause" the recording.
- **Serviceability testing** - The behaviour of Liquid Voice Recording solution under different simulated failure conditions on the Avaya platform will also be observed.

2.2. Test Results

All test cases were executed successfully, with the following observations noted.

1. When a call is resumed from being placed on hold from a 9641G SIP phone, the recording breaks down at the time resume is pressed. This only seems to occur when the phone is dialed directly and not when the skillset is called. Looking at a trace of the RTP from the phone, it appears as though a burst of G.722 audio is being sent out from the 9641G SIP phone at the time resume is being pressed. At this point it is unknown why this is occurring as there is no G.722 programmed on the system as a usable CODEC. Avaya are investigating the issue and G.722 can be taken out of the 46xxsettings file to ensure that this will not occur (see Appendix for further information on this). Liquid Voice also have a workaround in place using a patch to accommodate the G.722 audio being sent.
2. If the PSTN calls to the extension and the Avaya deskphone places the PSTN caller on hold, all that is being recorded is the MOH coming from Communication Manager. However, if the same PSTN caller calls to the CDN/Skillset and is being answered by the same extension but this time on a skillset call and being placed on hold by the same Avaya deskphone now both the MOH and the PSTN caller are recorded. The PSTN caller can be heard shouting down the phone on top of the MOH but only when on a skillset call, not when a call is made directly to the agent's phone.

2.3. Support

Technical support can be obtained for Liquid Assure from:

- Website http://www.liquidvoice.com
- Telephone +44 (0) 113 200 2020
- Email support@liquidvoice.com

3. Reference Configuration

Figure 1 below shows Avaya Aura® Communication Manager serving Digital, H.323 and SIP endpoints with Avaya Aura® Contact Center used to receive skillset calls. Assure has three connections to Communication Manager to obtain CDR, to CCT web services to obtain agent events and to initiate DTMF and to Session Border Controller for Enterprise to obtain all IP packets through a mirroring of its external port.

Note: SIP, H.323 and Digital endpoints were used during compliance testing.

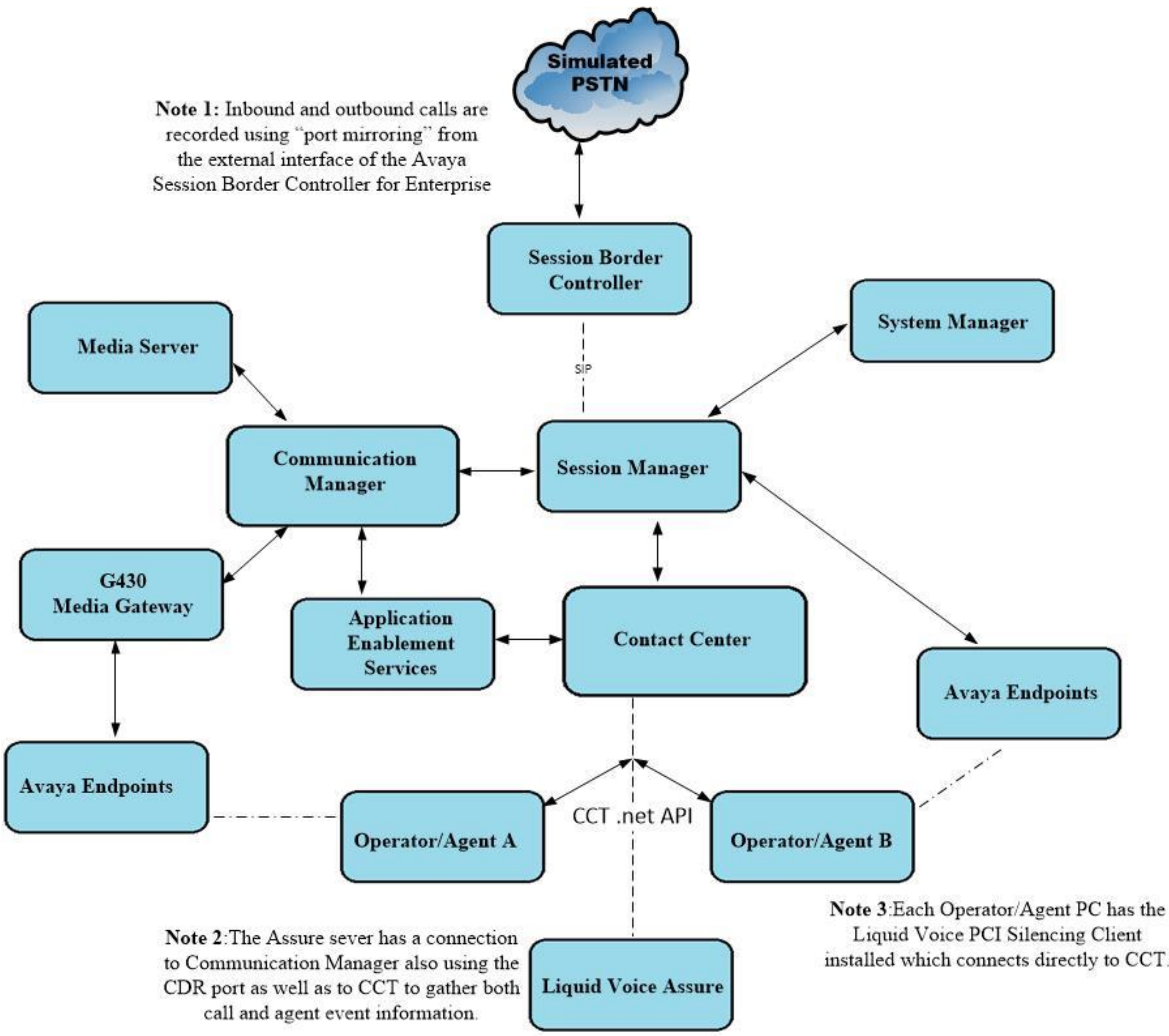


Figure 1: Connection of Liquid Voice Assure Interaction Recording with Avaya Aura® Communication Manager R8.1 and Avaya Aura® Contact Center R7.1

4. Equipment and Software Validated

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

Avaya Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 8.1.2.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.2.0.0611261 Feature Pack 2
Avaya Aura® Session Manager running on a virtual server	Session Manager R8.1.2 Build No. – 8.1.2.0.812039
Avaya Aura® Communication Manager running on a virtual server	R8.1.2.0 – FP2 R018x.00.0.890.0 Update ID 01.0.890.0-26095
Avaya Aura® Contact Center	7.1.0.3
Avaya Session Border Controller for Enterprise	8.1.1.0-26-19214
Avaya Aura® Application Enablement Services	8.1.2
Avaya Aura® Media Server	8.0.0.169
Avaya G430 Media Gateway	41.16.0/1
Avaya J179 H.323 Deskphone	6.8304
Avaya 96x1 SIP Deskphone	7.1.2.0.14
Avaya Digital 9408	2.00
Liquid Voice Equipment/Software	**Release/Version**
Liquid Voice Assure Interaction Recording - Interface version - Recording Service version - Cti Call Detail version - CDR Network Service	 7.5.1 8.3.4 3.1.1.3 7.1
Liquid Voice PCI silencing client running on Windows 10 PC	10.0.1.43

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**.

The following sections illustrate the steps required to allow CDR data to be sent to the Assure server. The first step is to add the Assure server as a name and IP address in the **IP NODE NAMES**. Use the command **change node-names ip** to add the Assure server. This was added using the name **LVoice** with IP address of **10.10.40.122**, as highlighted below.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
G430-Home           192.168.40.15
IP500V2             192.168.40.20
IPOffice            10.10.40.25
LVoice              10.10.40.122
aes81xvmpg          10.10.40.38
ams81vmpg           10.10.40.39
default             0.0.0.0
g430                10.10.40.15
procr               10.10.40.37
procr6              ::
sm81xvmpg           10.10.40.32






( 11 of 11   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Add the CDR service into IP Services by typing **change ip-services**. Note the following as this information may be needed when setting up the Assure server.

- **Local Node** is **procr**
- **Remote Node** is that of the **LVoice** entered as it was configured above
- **Service Type** is **CDR1**
- **Remote Port** number in this example shown as **9001** but can be any free port number

```
change ip-services                                          Page   1 of   3

                                    IP SERVICES
 Service     Enabled       Local       Local       Remote           Remote
  Type                     Node        Port        Node             Port
  CDR1                     procr          0        LVoice           9001
```

Use the command **change system-parameters cdr** to make changes to the way the CDR data is sent out. The following changes on **Page 1** were made specifically for this testing.

- Primary Output Endpoint is set to **CDR1**
- **Outg Trk Call Splitting** is set to **y**
- **Inc Trk Call Splitting** is set to **y**

```
change system-parameters cdr                               Page   1 of   2
                            CDR SYSTEM PARAMETERS
 Node Number (Local PBX ID):                       CDR Date Format: month/day
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
       CDR Retention (days): 20
           Use ISDN Layouts? n                 Enable CDR Storage on Disk? n
       Use Enhanced Formats? n     Condition Code 'T' For Redirected Calls? n
     Use Legacy CDR Formats? y                Remove # From Called Number? n
Modified Circuit ID Display? n                           Intra-switch CDR? n
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
 Suppress CDR for Ineffective Call Attempts? y        Outg Attd Call Record? y
     Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? y       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                  Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n          Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 15
Remove '+' from SIP Numbers? y
```

Page 2 of the system-parameters cdr shows the various fields and lengths that were set specifically for Liquid Voice Assure to obtain the records correctly.

```
change system-parameters cdr                                  Page   2 of   2
                            CDR SYSTEM PARAMETERS

     Data Item - Length          Data Item - Length          Data Item - Length
 1: date             - 6   17: in-trk-code      - 4   33: line-feed       - 1
 2: space            - 1   18: space            - 1   34:                  -
 3: time             - 4   19: in-crt-id        - 3   35:                  -
 4: space            - 1   20: space            - 1   36:                  -
 5: sec-dur          - 5   21: out-crt-id       - 3   37:                  -
 6: space            - 1   22: space            - 1   38:                  -
 7: cond-code        - 1   23: ppm              - 5   39:                  -
 8: space            - 1   24: space            - 1   40:                  -
 9: code-dial        - 4   25: isdn-cc          - 11  41:                  -
10: space            - 1   26: space            - 1   42:                  -
11: code-used        - 4   27: attd-console     - 2   43:                  -
12: space            - 1   28: space            - 1   44:                  -
13: dialed-num       - 18  29: vdn              - 5   45:                  -
14: space            - 1   30: space            - 1   46:                  -
15: clg-num/in-tac   - 10  31: acct-code        - 15  47:                  -
16: space            - 1   32: return           - 1   48:                  -

                              Record length = 117
```

6. Configure Avaya Aura® Contact Center

This section provides the procedures for configuring Contact Center. The procedures fall into the following areas:

- Add a Windows User for Liquid Voice
- Configure CCT Web Services
- Add a CCT User for Liquid Voice

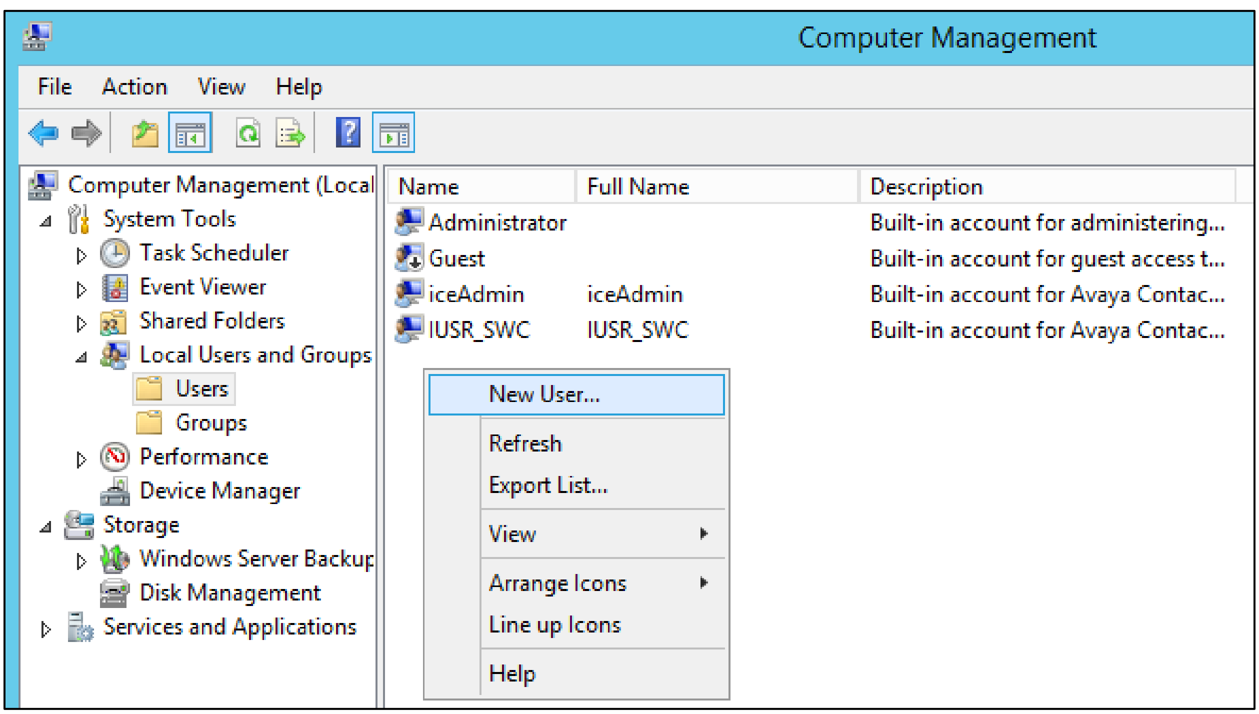
Note: The Contact Center and its workstations must be part of a domain. The Liquid Voice PCI silencing client uses the user's domain credentials on the client PC for Single Sign on to access the CCT service. When a pause request is generated, the PCI silencing client sends a request to the Avaya CCT service to generate DTMF tones on any of the user's terminals that are in a state that is capable of DTMF tone generation.

Note: It is assumed that a fully working Contact Center is already in place, with all the necessary agents configured and skillset routing in place. An overview of one agent that was used for compliance testing can be found in **Appendix 12**.

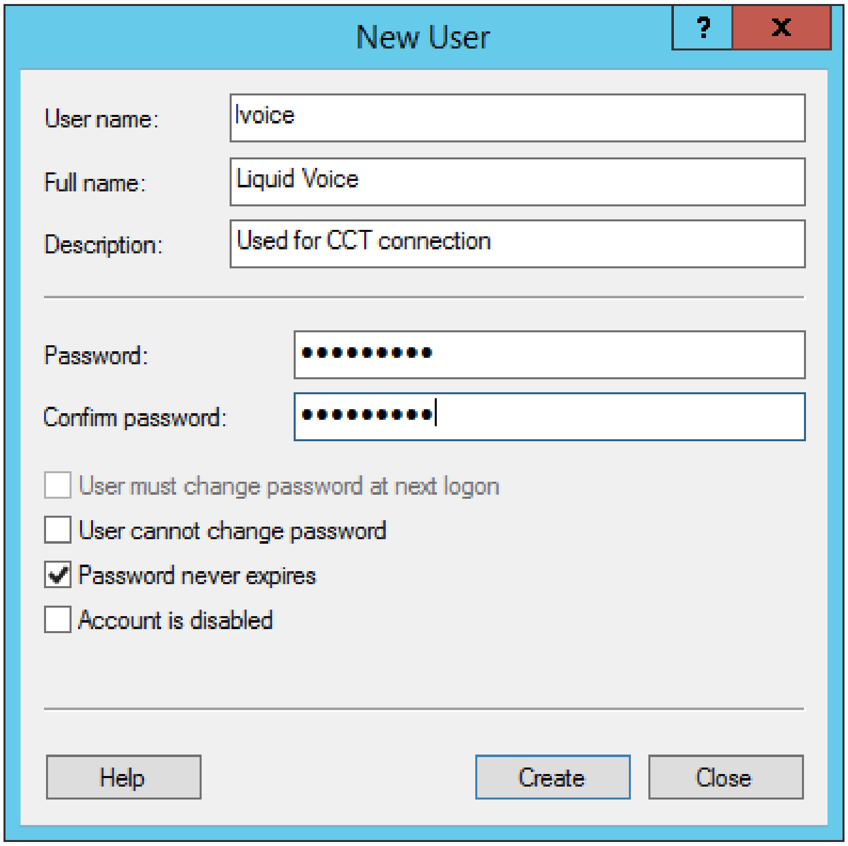
6.1. Add a Windows User for Liquid Voice

A user for Liquid Voice is added to the Contact Center server, this user will be used by Assure to connect to CCT as per **Section 7.1**. This user is also used to Enable SIP Call Recording on Web Services in **Section 6.2**.

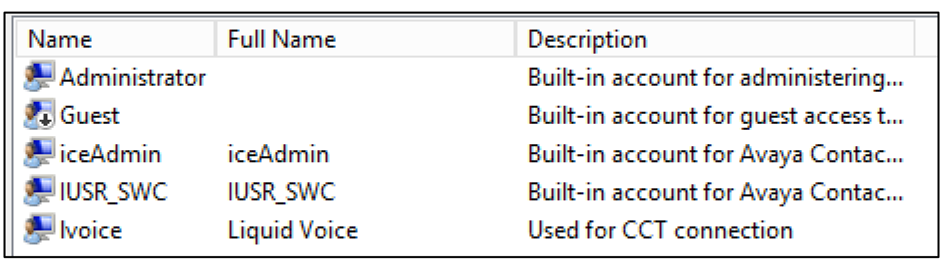
From **Computer Management**, navigate to **Local Users and Groups** in the left window and selected **Users**. From the main window, right click and select **New User**.



Enter a suitable **User name** and **Password**, and best to choose **Password never expires** as shown below. Click on **Create** to complete. This user will be used as part of the Assure configuration in **Section 7.1**.

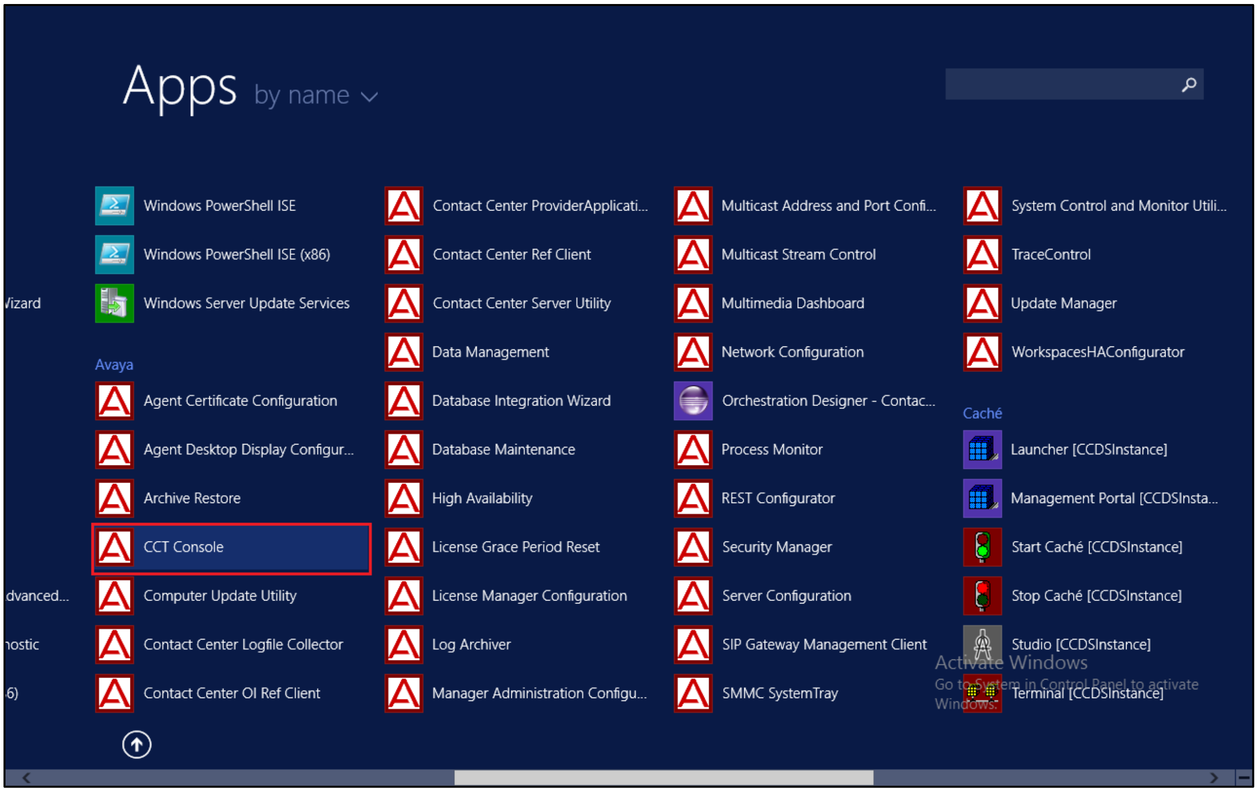


The new user is now visible at the bottom of the users' page, as shown.

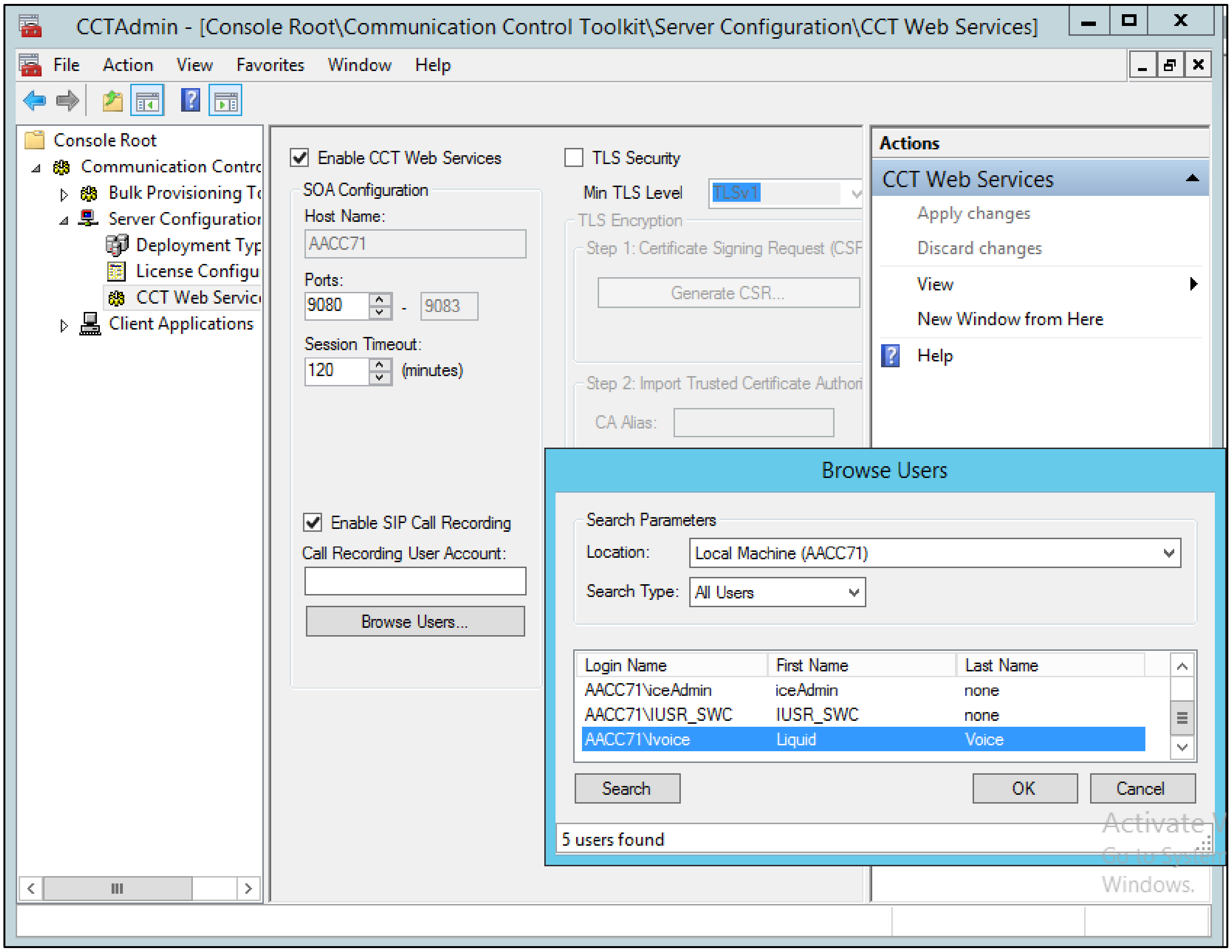


6.2. Configure CCT Web Services

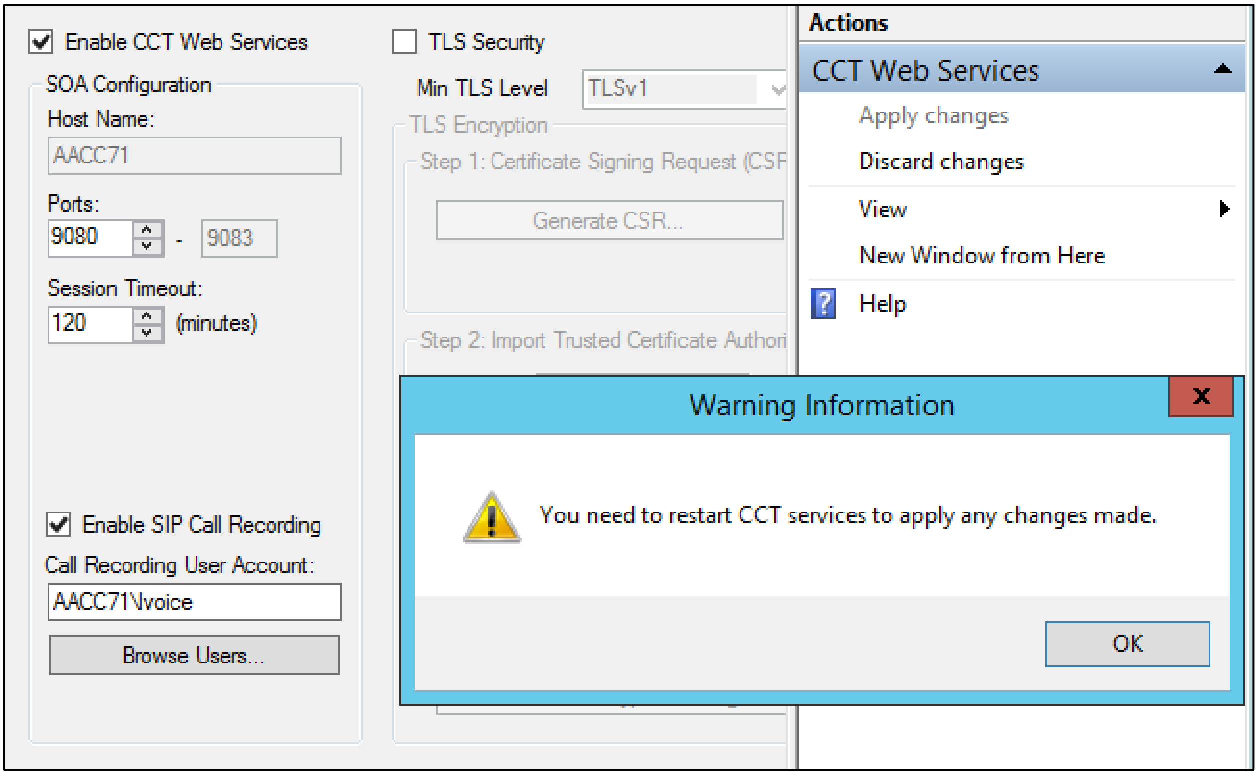
Open the **CCT Console** as shown below.



Navigate to **CCT Web Services** in the left window, this should be under **Server Configuration**. From the main window, ensure that **Enable CCT Web Services** box is **ticked**, note the port number shown. Ensure that **Enable SIP Call Recording** is also **ticked** and click on Browse Users. Select **Local Machine** as the **Location** and search for the user added in **Section 6.1**.

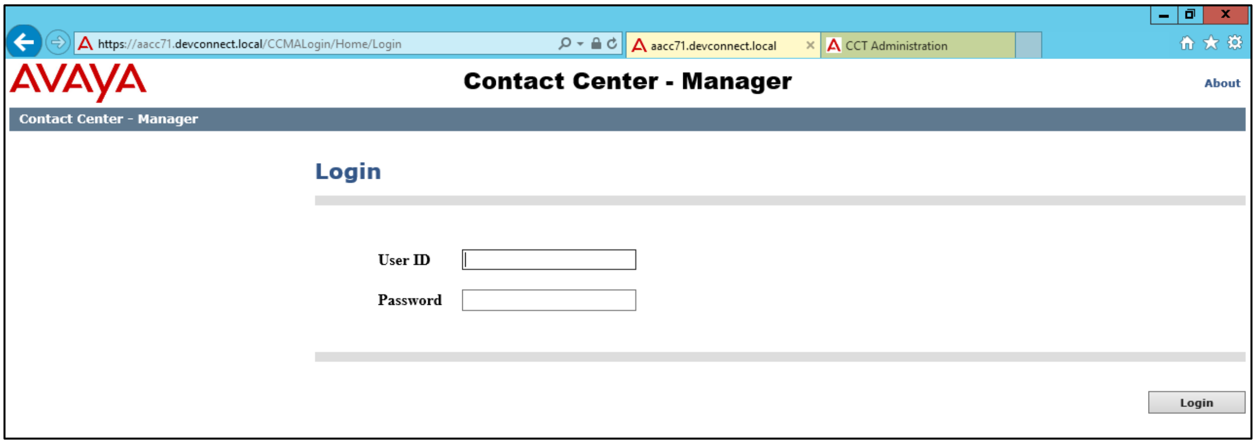


This message will appear and the CCT services will need to be shut down and started again.

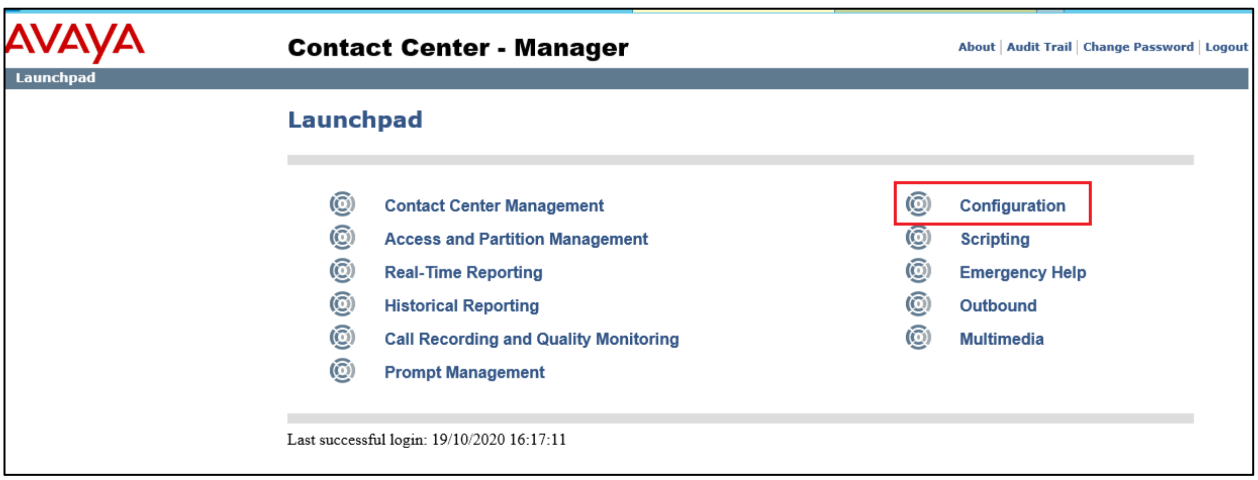


6.3. Add a Communication Control Toolkit User for Liquid Voice

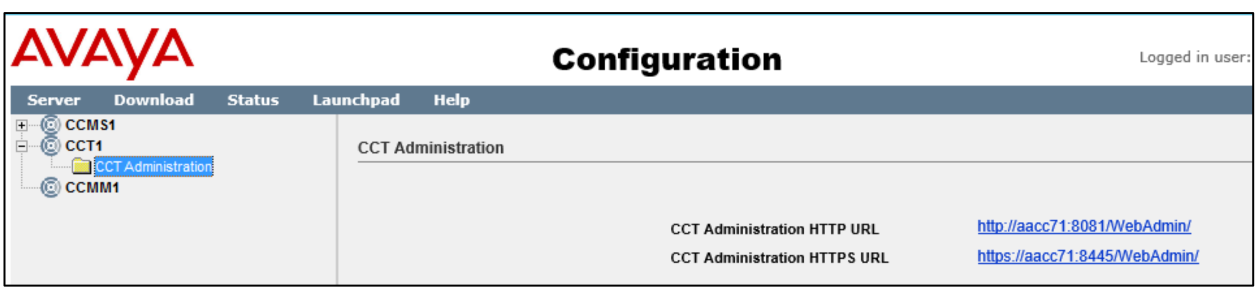
Log into **Contact Center Manager** by opening Internet Explorer and navigating to the Contact Center FQDN or IP address.



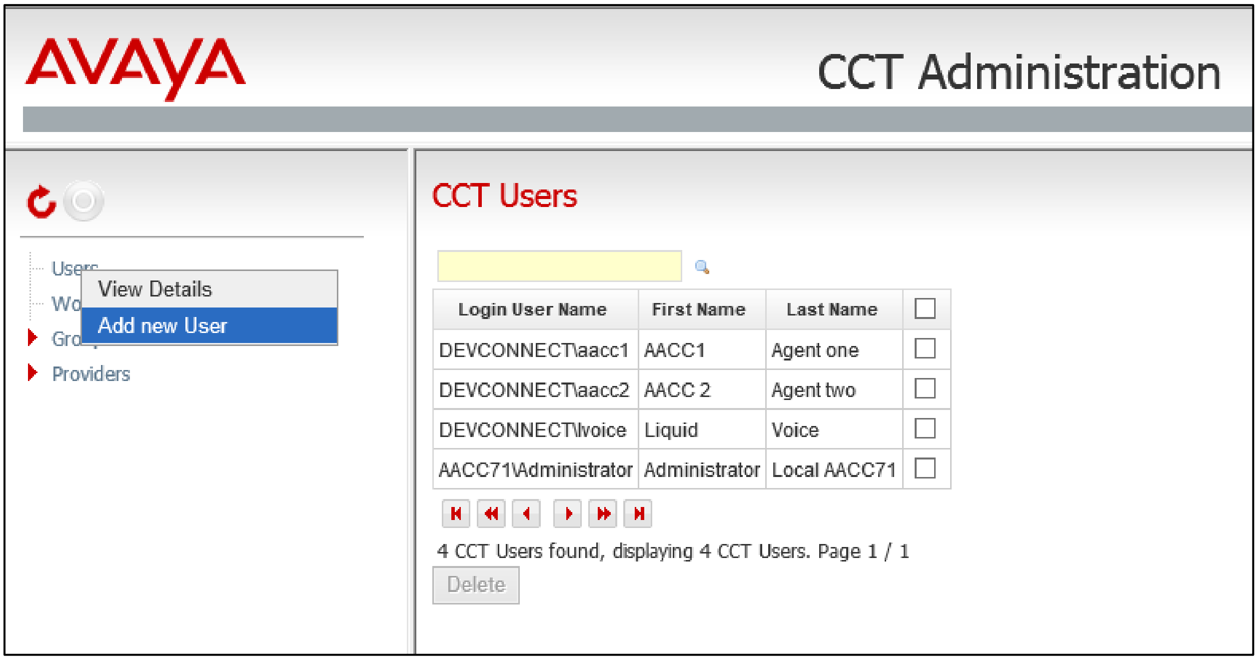
Click on **Configuration**.



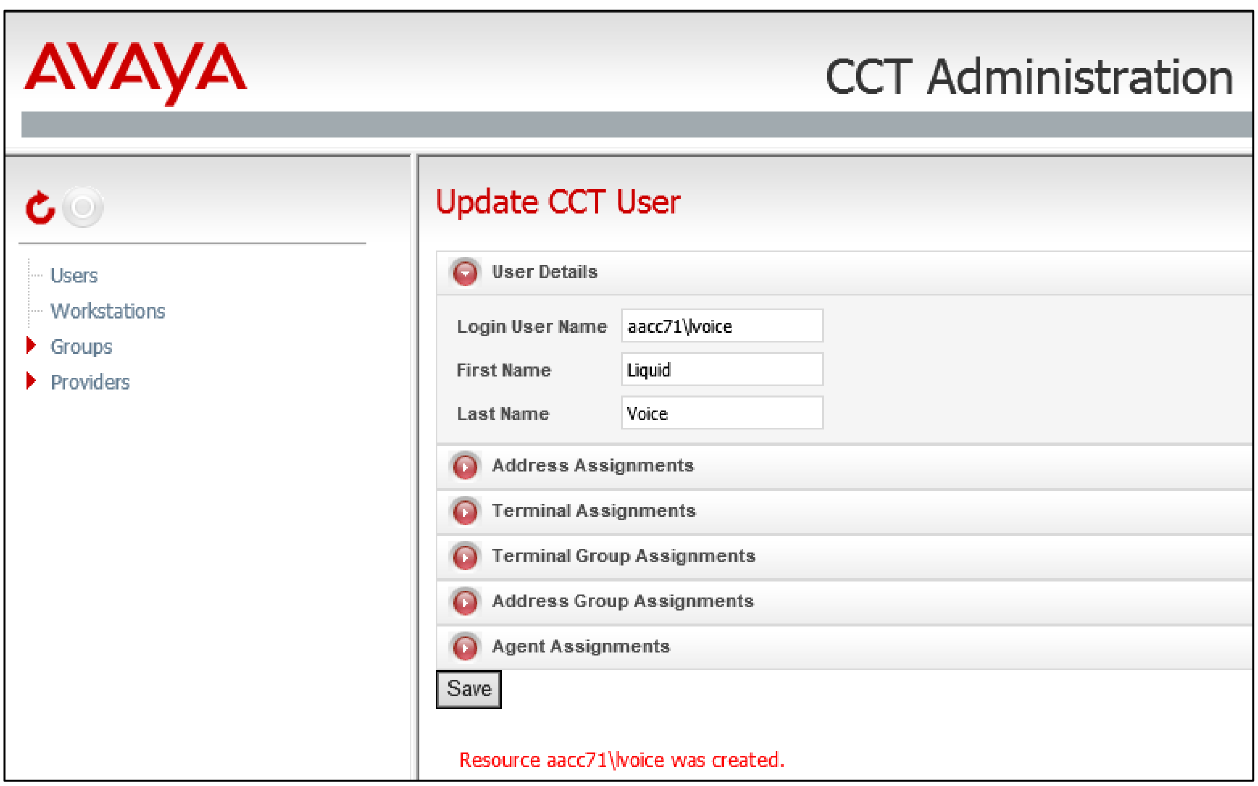
Open **CCT Administration** and select the secure or unsecure URL, whichever is preferred.



Right click on **Users** in the left window and select **Add new User**.



Enter the same user details as in **Section 6.1**. The configuration file in **Section 7.1** will use this username to obtain events from CCT.



7. Configure Liquid Voice Assure

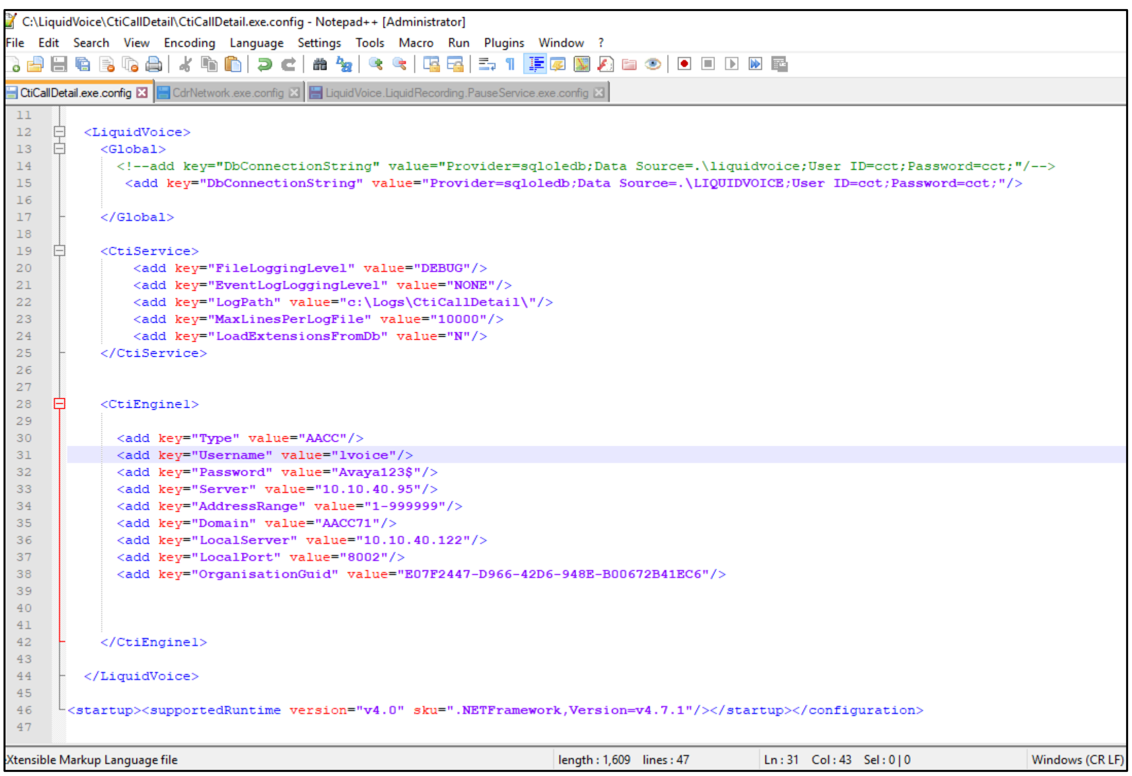
This section describes the steps required for Liquid Voice Assure Interaction Recording to interoperate with the Avaya solution. There are four connections to the Avaya solution required for this setup.

1. Liquid Voice Call Detail service connection to Avaya Aura® Contact Center, specifically to the Communication Control Toolkit (CCT) to gather events surrounding agent calls.
2. Connection to Avaya Aura® Contact Center, specifically to the Communication Control Toolkit (CCT) to allow Assure generate DTMF tones when a recording is being paused.
3. Connection to Avaya Aura® Communication Manager to collect CDR data.
4. Connection to Avaya Session Border Controller for Enterprise (ASBCE) via port mirror of the external interface on the ASBCE, to record all trunk calls.

Note: On most production setups the Assure server will have a separate connection to two different CCT servers in a geographical redundancy setup, however this was not tested during compliance testing and only one connection to one CCT server was configured.

7.1. Configure Liquid Voice Call Detail service connection to Avaya Aura® Contact Center

Assure connects to the CCT module of Contact Center. A user for CCT was setup in **Section 6.1** and **Section 6.3**, to allow Assure collect the necessary agent events from CCT. The location for the configuration file on the Assure server is shown in the top of the screen shot below. The file is named **CtiCallDetail.exe.config**.

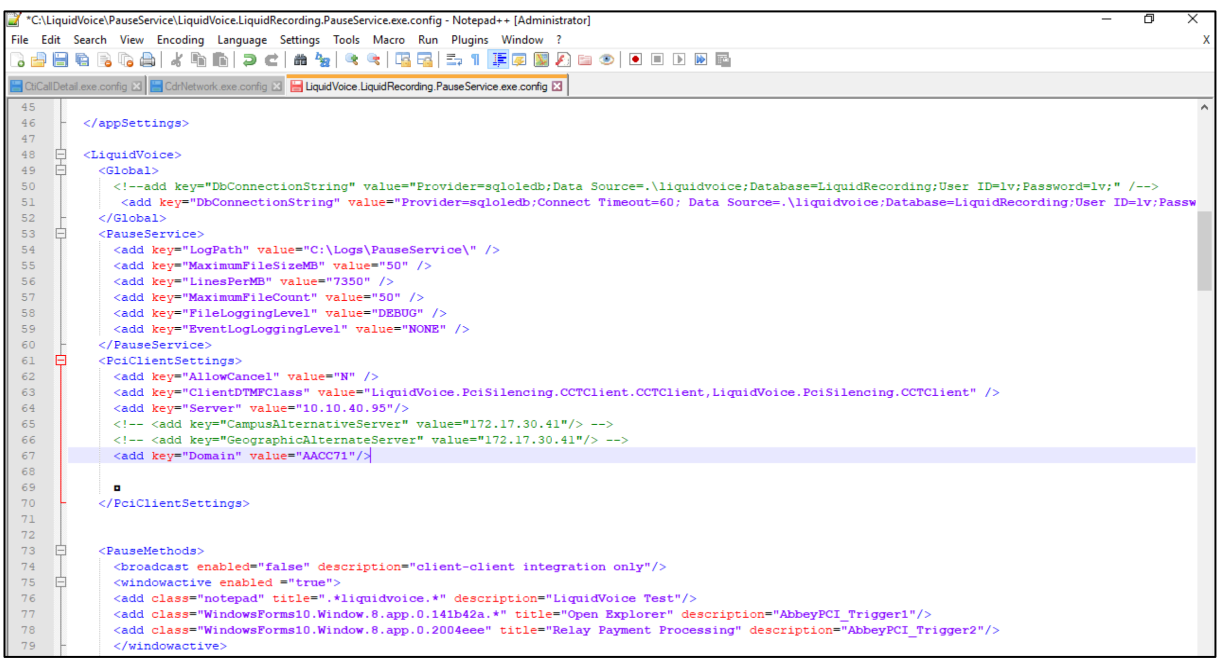


A closer examination of the **CtiEngine** section of the CtiCallDetail.exe.config configuration file shows the **Username** and **Password** that was used as per **Section 6.1**, as well as the IP address of the CCT server. The **Domain** entered should be the hostname of the CCT server. The **Server** address is the CCT server IP and the **LocalServer** is the Liquid Voice recorder IP.

```
<CtiEngine1>

  <add key="Type" value="AACC"/>
  <add key="Username" value="lvoice"/>
  <add key="Password" value="999999"/>
  <add key="Server" value="10.10.40.95"/>
  <add key="AddressRange" value="1-999999"/>
  <add key="Domain" value="AACC71"/>
  <add key="LocalServer" value="10.10.40.122"/>
  <add key="LocalPort" value="8002"/>
  <add key="OrganisationGuid" value="E07F2447-D966-42D6-948E-B00672B41EC6"/>



</CtiEngine1>
```

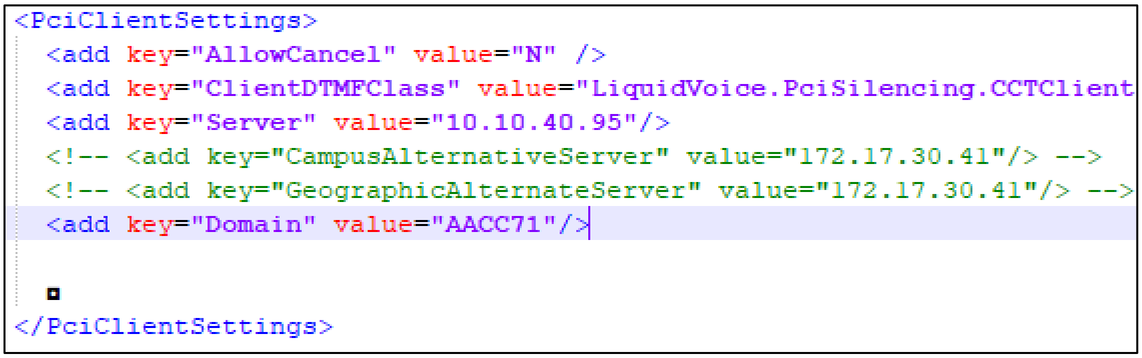
7.2. Liquid Voice Pause Solution connection to Avaya Aura® Contact Center

The pause solution is used to stop and start the recording automatically when an agent opens a certain URL. The Pause solution consist of two parts. The Pause Service and the PCI Clients. The PCI Clients take their configuration from the setting in the Pause Service configuration. When a pause request is received it is the client software that generates the DTMFs via the CCT connection. The Pause Service configuration file is used for that purpose. The location of this file is displayed at the top of the screen shot below.


*C:\LiquidVoice\PauseService\LiquidVoice.LiquidRecording.PauseService.exe.config - Notepad++ [Administrator]

```
</appSettings>

<LiquidVoice>
  <Global>
    <!--add key="DbConnectionString" value="Provider=sqloledb;Data Source=.\liquidvoice;Database=LiquidRecording;User ID=lv;Password=lv;" /-->
     <add key="DbConnectionString" value="Provider=sqloledb;Connect Timeout=60; Data Source=.\liquidvoice;Database=LiquidRecording;User ID=lv;Passw
  </Global>
  <PauseService>
    <add key="LogPath" value="C:\Logs\PauseService\" />
    <add key="MaximumFileSizeMB" value="50" />
    <add key="LinesPerMB" value="7350" />
    <add key="MaximumFileCount" value="50" />
    <add key="FileLoggingLevel" value="DEBUG" />
    <add key="EventLogLoggingLevel" value="NONE" />
  </PauseService>
  <PciClientSettings>
    <add key="AllowCancel" value="N" />
    <add key="ClientDTMFClass" value="LiquidVoice.PciSilencing.CCTClient.CCTClient,LiquidVoice.PciSilencing.CCTClient" />
    <add key="Server" value="10.10.40.95"/>
    <!-- <add key="CampusAlternativeServer" value="172.17.30.41"/> -->
    <!-- <add key="GeographicAlternateServer" value="172.17.30.41"/> -->
    <add key="Domain" value="AACC71"/>

  </PciClientSettings>


  <PauseMethods>
    <broadcast enabled="false" description="client-client integration only"/>
    <windowactive enabled ="true">
    <add class="notepad" title=".*liquidvoice.*" description="LiquidVoice Test"/>
    <add class="WindowsForms10.Window.8.app.0.141b42a.*" title="Open Explorer" description="AbbeyPCI_Trigger1"/>
    <add class="WindowsForms10.Window.8.app.0.2004eee" title="Relay Payment Processing" description="AbbeyPCI_Trigger2"/>
    </windowactive>
```

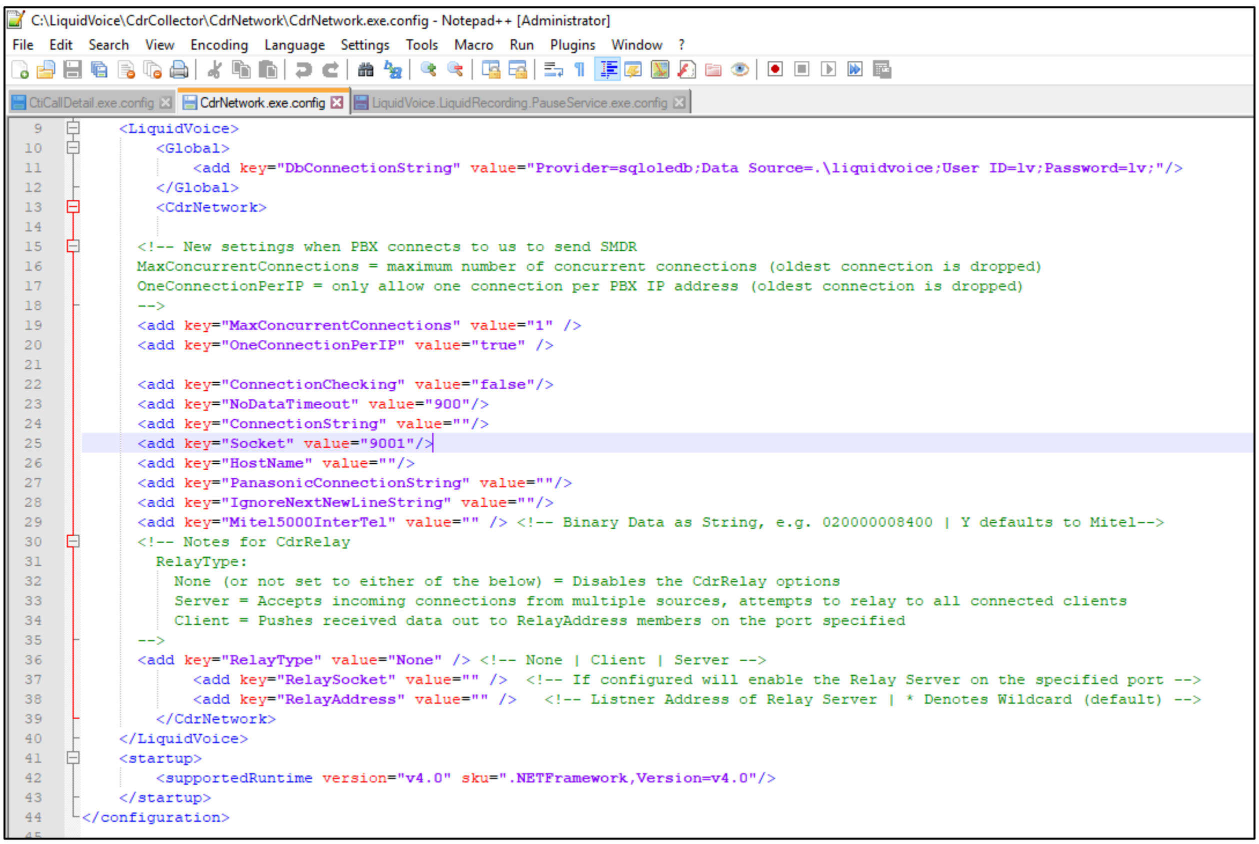
A closer look at the file will show the CCT servers IP address along with the **Domain,** which is the host name of the CCT server, in that case both being that of the Contact Center server also.



```
<PciClientSettings>
  <add key="AllowCancel" value="N" />
  <add key="ClientDTMFClass" value="LiquidVoice.PciSilencing.CCTClient
  <add key="Server" value="10.10.40.95"/>
  <!-- <add key="CampusAlternativeServer" value="172.17.30.41"/> -->
  <!-- <add key="GeographicAlternateServer" value="172.17.30.41"/> -->
  <add key="Domain" value="AACC71"/>

</PciClientSettings>
```

7.3. Configure connection to Avaya Aura® Communication Manager

Similarly, another configuration file is used to connect to Communication Manager. Again, the location of the file is displayed at the top of the screen shot below.



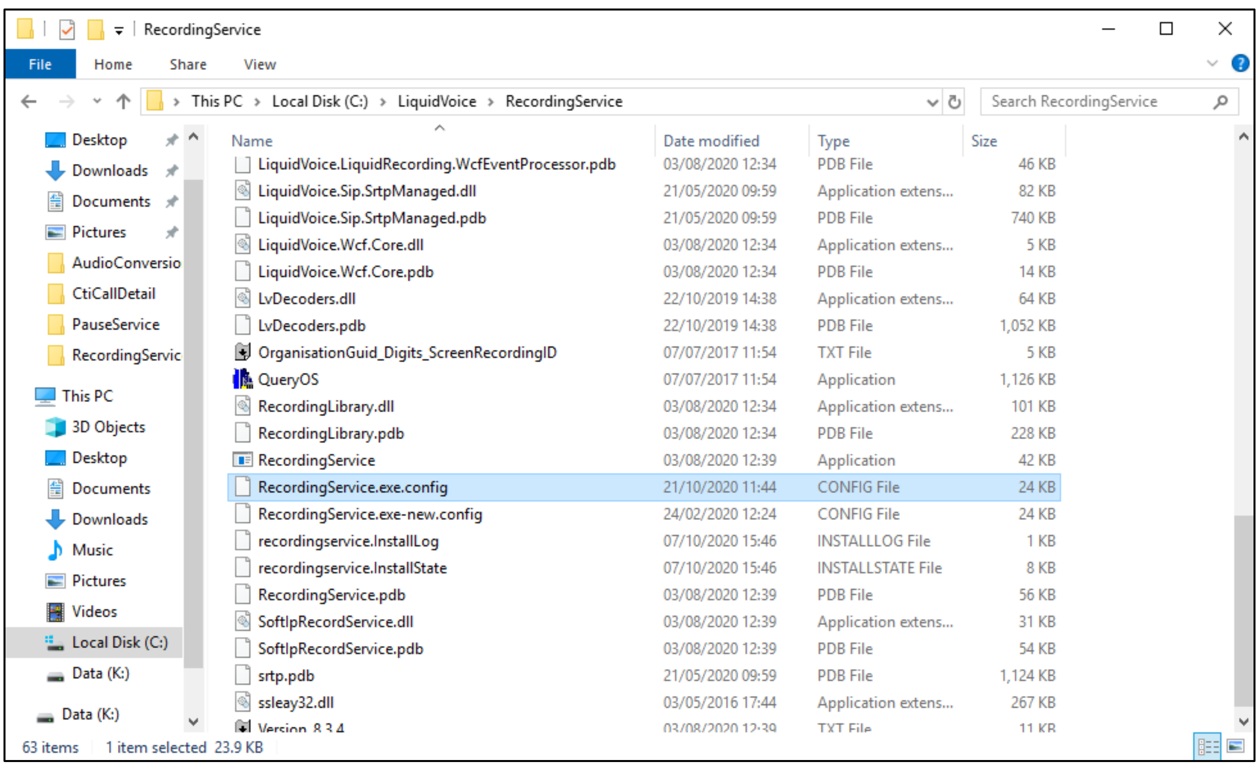

```
    <LiquidVoice>
        <Global>
            <add key="DbConnectionString" value="Provider=sqloledb;Data Source=.\liquidvoice;User ID=lv;Password=lv;"/>
        </Global>
        <CdrNetwork>

      <!-- New settings when PBX connects to us to send SMDR
      MaxConcurrentConnections = maximum number of concurrent connections (oldest connection is dropped)
      OneConnectionPerIP = only allow one connection per PBX IP address (oldest connection is dropped)
      -->
      <add key="MaxConcurrentConnections" value="1" />
      <add key="OneConnectionPerIP" value="true" />

      <add key="ConnectionChecking" value="false"/>
      <add key="NoDataTimeout" value="900"/>
      <add key="ConnectionString" value=""/>
      <add key="Socket" value="9001"/>
      <add key="HostName" value=""/>
      <add key="PanasonicConnectionString" value=""/>
      <add key="IgnoreNextNewLineString" value=""/>
      <add key="Mitel5000InterTel" value="" /> <!-- Binary Data as String, e.g. 020000008400 | Y defaults to Mitel-->
      <!-- Notes for CdrRelay
        RelayType:
          None (or not set to either of the below) = Disables the CdrRelay options
          Server = Accepts incoming connections from multiple sources, attempts to relay to all connected clients
          Client = Pushes received data out to RelayAddress members on the port specified
      -->
      <add key="RelayType" value="None" /> <!-- None | Client | Server -->
            <add key="RelaySocket" value="" />  <!-- If configured will enable the Relay Server on the specified port -->
            <add key="RelayAddress" value="" />   <!-- Listner Address of Relay Server | * Denotes Wildcard (default) -->
        </CdrNetwork>
    </LiquidVoice>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.0"/>
    </startup>
</configuration>
```

A closer look at the entry for the Socket will show the same port that was used in **Section 5.** Assure listen on port **9001** for the CDR output. If a host name or IP address is added to the **HostName** key the CDR service will connect to Communication Manager.

```
<add key="MaxConcurrentConnections" value="1" />
<add key="OneConnectionPerIP" value="true" />

<add key="ConnectionChecking" value="false"/>
<add key="NoDataTimeout" value="900"/>
<add key="ConnectionString" value=""/>
<add key="Socket" value="9001"/>
<add key="HostName" value=""/>
<add key="PanasonicConnectionString" value=""/>
<add key="IgnoreNextNewLineString" value=""/>
<add key="Mitel5000InterTel" value="" /> <!-- Binary Data
<!-- Notes for CdrRelay
```

7.4. Configure connection to Avaya Session Border Controller for Enterprise

A configuration file is used to connect to record the voice calls. These calls are recorded by mirroring the port on the Session Border Controller. The configuration file shows how this is setup. The location of the file is displayed at the top of the screen shot below i.e., **C:/LiquidVoice/RecordingService/** and the file is called **RecordingService.exe.config**.



In the config file, it is the **SoftIpRecorder** section that is configured for SIP.

The following in red are the important bits to observe.

- <add key="Enabled" value="Y"/> - turns on the Soft IP Recorder.
- <add key="SipPort1" value="5060"/> - Specifies the SIP port number.
- <add key="NetworkInterface1" value="10.10.40.121"/> - IP address or name of local NIC that the voice data is port mirrored to.
- <add key="IsTcpSipEnabled" value="Y"/> - Enables TCP SIP recording.
- <add key="IsUdpSipEnabled" value="N"/> - Enables UDP SIP recording.

```
<SoftIpRecorder>

    <add key="Enabled" value="Y"/>
    <add key="DisableJitterBuffer" value="N"/>
    <add key="DisableTimeStampResetting" value="N"/>
    <add key="RawRtpRecording" value="N"/>

    <!-- This adds silence to SoftIP Mitel recording -->
    <add key="AddSilentPadding" value="Y"/>
    <add key="IsAccurateTimeoutEnabled" value="Y" />
    <add key="LongTimeout" value="100"/>
    <add key="ShortTimeout" value="3"/>
    <add key="ReplayCaptureFile" value=""/>
    <add key="ReplayCaptureFile" value="c:/temp2"/>
    <add key="IsReplayCaptureFileProcessedRealtime" value="Y"/>
    <add key="CustomDtmfPayload" value="100" />
    <add key="StereoRecording" value="N"/>

    <!-- If mixing to Mono - use alternative mixing algorythmn-->
    <add key="AlternativeMixing" value="Y" />
    <add key="G72216KHZEnabled" value="Y" />

    <!-- Used for SIP recording -->
    <add key="PbxAddress" value=""/>
    <add key="PbxAddressRegex" value=""/>
    <add key="IpMappingFrom1" value=""/>
    <add key="IpMappingTo1" value=""/>
    <add key="SipPort1" value="5060"/>
    <add key="SipPort2" value=""/>
    <add key="SipPort3" value=""/>
    <add key="SipPort4" value=""/>
    <add key="SipPort5" value=""/>
    <add key="SipPort6" value=""/>
    <add key="CustomSipHeader1" value ="VIA" />
    <!--<add key="CustomSipHeader1" value="X-Asterisk-GUID"/>-->
```

```
<!-- For SoftIP this is the nic device name, or ip address we are listening for RTP on -->
<add key="NetworkInterface1" value="10.10.40.121"/>
<add key="NetworkInterface2" value="-1"/>
<add key="NetworkInterface3" value="-1"/>
<add key="NetworkInterface4" value="-1"/>
<add key="NetworkInterface5" value="-1"/>
<add key="InterfaceKernelBuffer" value="100000000"/>

<!-- an example of a rather complicated rtp filter to filter rtp -->
<!--<add key="PcapFilter" value="udp[8] &gt;&gt; 6 == 0x02 &amp;&amp; length &lt; 250
&amp;&amp; (udp[9] &amp; 0x7f == 0x0 || udp[9] &amp; 0x7f == 0x8 || udp[9] &amp; 0x7f == 0x9
|| udp[9] &amp; 0x7f == 0xd || udp[9] &amp; 0x7f == 0x67 || udp[9] &amp; 0x7f == 0x68)" />-->
<add key="PcapFilter" value="" />
<add key="PcapFilter1" value="" />
<add key="PcapFilter3" value="" />

<!-- Although SoftIP handlers can now be loaded dynamically, the following will load some defaults
<add key="IsTcpSipEnabled" value="Y"/>
<add key="IsUdpSipEnabled" value="N"/>
<add key="IsSkinnyEnabled" value="N"/>
<add key="IsLyncEnabled" value="N"/>
<add key="UseFullMacAddress" value="Y" />
<add key="UseIpForChannel" value="N" />

<!--<add key="MatchRule1" value="RtpRule"/>-->
<!--<add key="MatchRule2" value="IpAndPort"/>-->
<!--<add key="MatchRule3" value="IpAndNoDestinationPort"/>-->
<!--<add key="MatchRule4" value="IpAndSwapPort"/>-->
<!--<add key="MatchRule5" value="DestinationIpAndPort"/>-->

<!-- This is the softip engines load of extension. -->
<add key="LoadExtensionsFromDb" value="N"/>
<add key="CustomRtp1" value=""/>

<!-- We can silence pad using the timestamp. Only use if an IVR or other device is causing issues by
sending no RTP when 'silent' -->
<add key="TimeStampPadding" value="N"/>

</SoftIpRecorder>
```

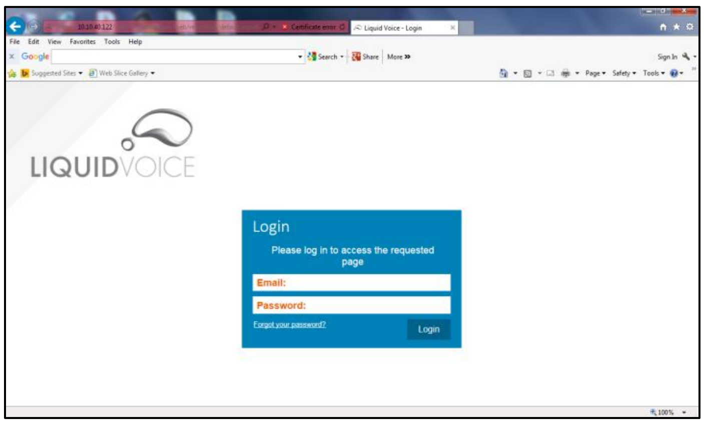
8. Verification Steps

The correct configuration of the solution can be verified as follows.

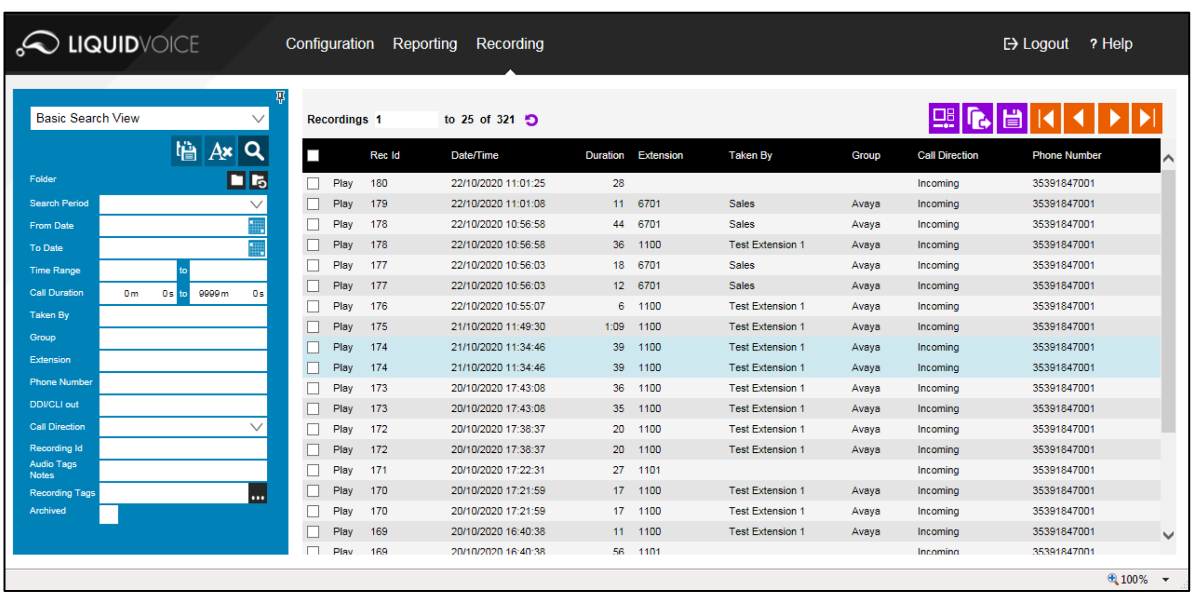
Note: Users can use any browser to access the interface and play back recordings. However, Assure uses Silverlight and so works best with Internet Explorer. If any other browser is used, the Liquid Voice Viewer will need to be downloaded. The Liquid Voice Viewer launches the Silverlight components out of browser enabling seamless use of the system in browsers that do not support Silverlight.

8.1. Verify Liquid Voice Assure

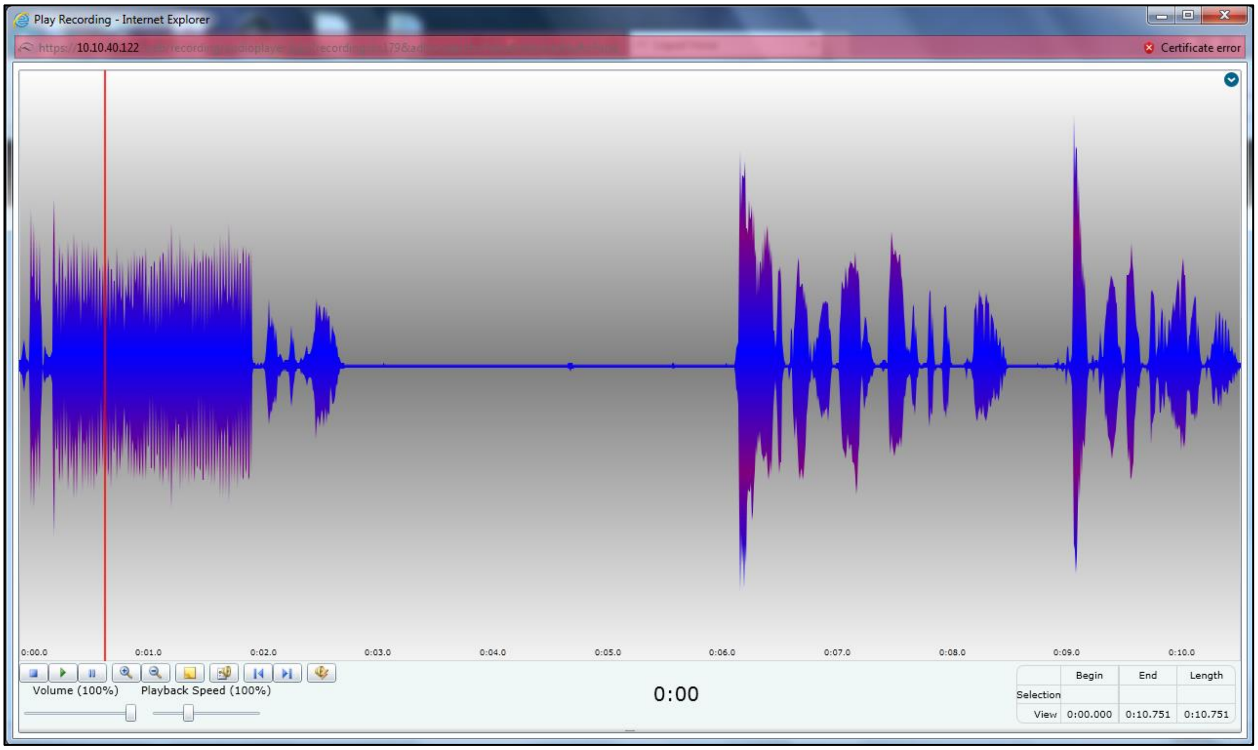
Open a URL to the Assure sever as shown below with Internet Explorer. Enter the appropriate credentials and click on **Login**.



A list of recordings is displayed and by clicking on **Play** at the beginning of any of the lines will open a new window containing the playback of that particular recording.



The following window shows the playing back of the recording that was chosen from the screen on the previous page.



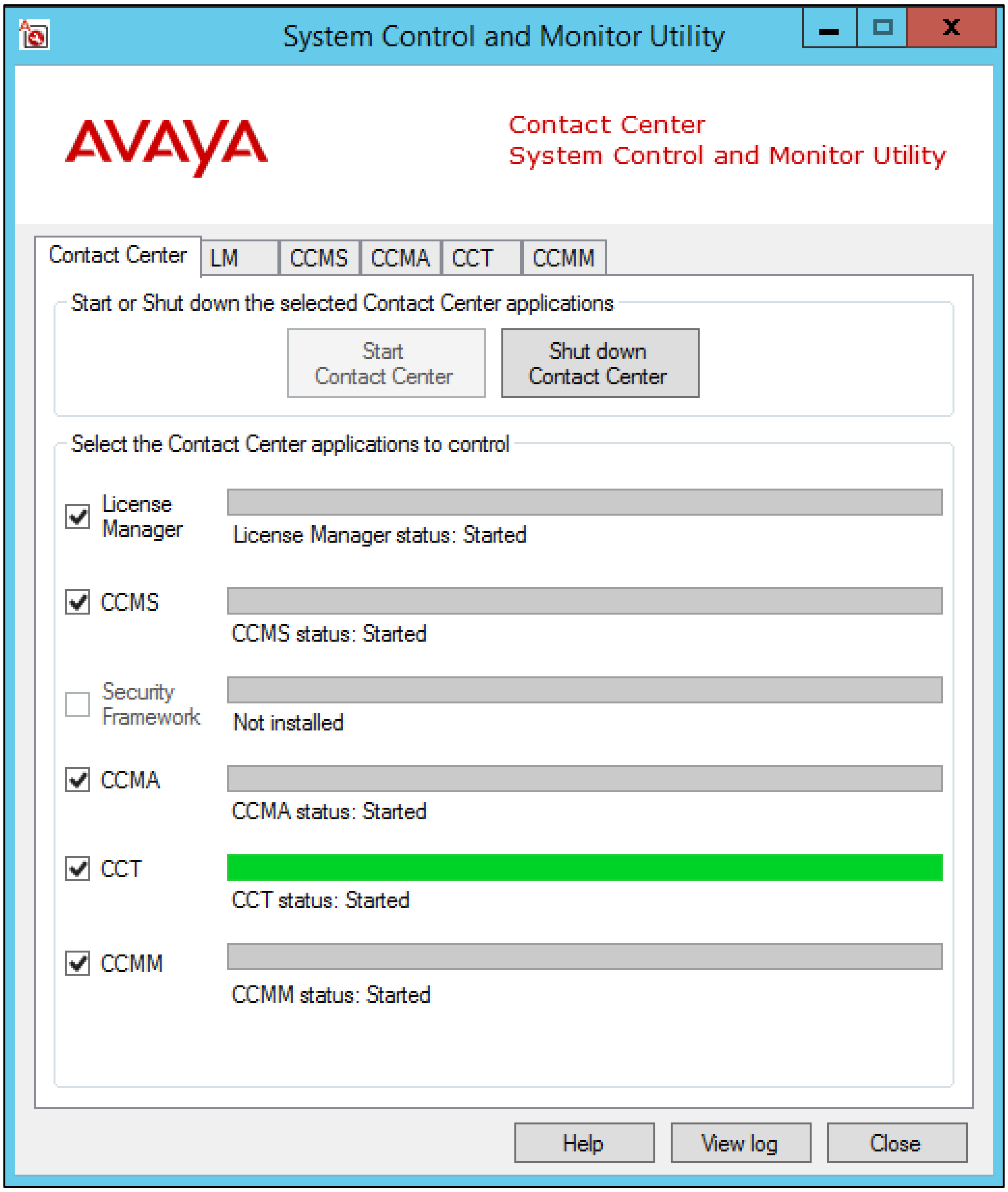
8.2. Verify CDR from Avaya Aura® Communication Manager

The **status cdr-link** command can be used to display the status of the CDR link from Communication Manager. The Primary **Link State** is shown as **up** below, which is good.

```
status cdr-link
                                CDR LINK STATUS
                   Primary                         Secondary

        Link State: up                             CDR not administered

       Date & Time: 2020/10/16 14:33:53            0000/00/00 00:00:00
   Forward Seq. No: 0                              0
  Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                            0.00
       Reason Code: OK
```

8.3. Verify Avaya Aura® Contact Center

From the Contact Center server, open the **System Control and Monitor Utility**. The following window should be displayed showing all applications as **Started**.



9. Conclusion

These Application Notes describe the compliance testing of Liquid Voice Assure Interaction Recording R7.5 with Avaya Aura® Contact Center R7.1 and Avaya Aura® Communication Manager R8.1. All test cases were executed successfully with any observations noted in **Section 2.2**.

10. Additional References

This section references the product documentations that are relevant to these Application Notes.

Product documentation for Avaya products may be found at *http://support.avaya.com*.

[1] *Administering Avaya Aura® Communication Manager,* Release 8.1

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 8.1

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide,* Release 8.1

[4] *Administering Avaya Aura® Session Manager*, Release 8.1

[5] *Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications Release 7.1* Issue 02.04 October 2020

[6] *Avaya Aura® Contact Center commissioning for Avaya Aura® Unified Communications* Release 7.1 Issue 02.04 December 2019

[7] *Avaya Aura® Contact Center Server Administration Release 7.1* Issue 07.05 October 2020

[8] *Administering Avaya Session Border Controller for Enterprise*, Release 8.1.x, Issue 3, August 2020

Product documentation for Assure can be found by contacting Liquid Voice as per **Section 2.3**.

11. Appendix A

To ensure a workaround is in place for the issue described in **Section 2.2** with the 9641G SIP phone, the 46xxsettings file for this SIP phone must be altered as shown below. Use the command **SET ENABLE_G722 0** to disable the use of G.722 from the phoneset in question.

```
##
## ENABLE_G722 specifies whether the G.722 codec is enabled.
## Value Operation
## 0 Disabled
## 1 Enabled
## This parameter is supported by:
## 96x1 SIP R6.2 and later; the default value is 1.
## 96x1 SIP R6.0.x; the default value is 0.
## 96x0 SIP R2.0 and later; the default value is
##  H1xx SIP R1.0 and later; the default value is 1.

SET  ENABLE_G722 0

##
```

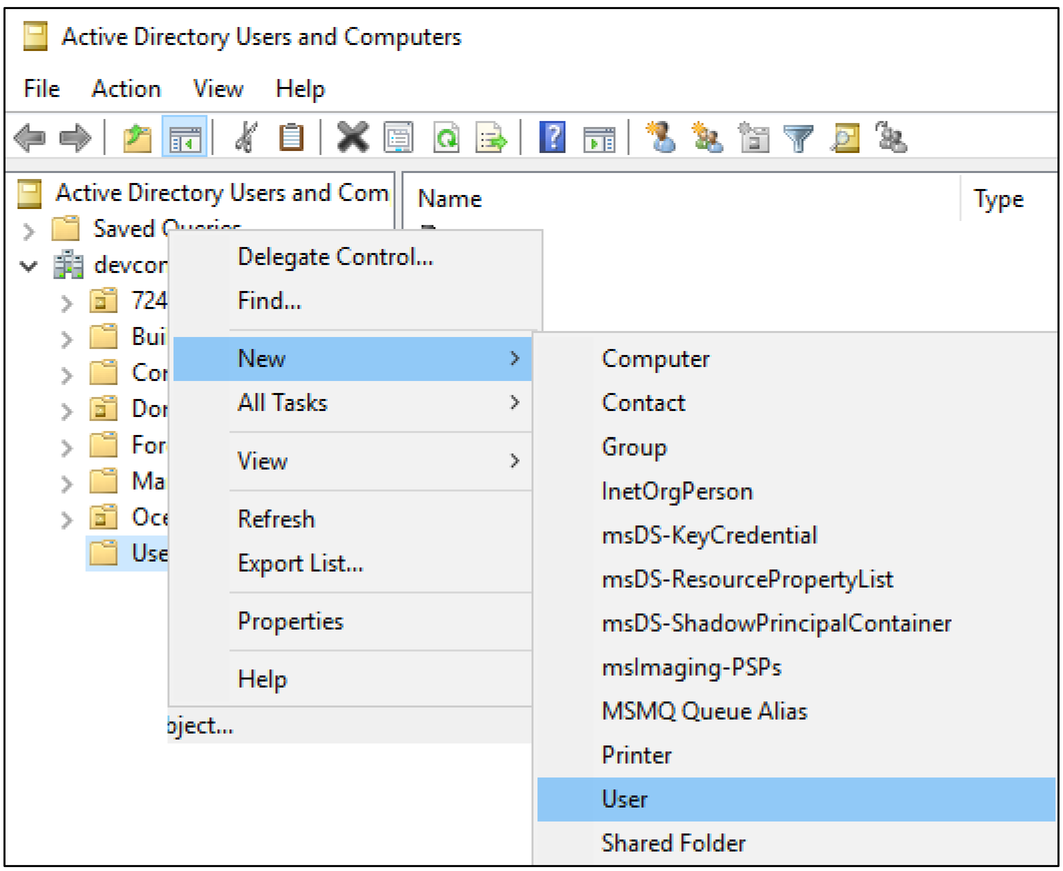
12. Appendix B

This section illustrates the Contact Center user setup that was used during compliance testing and how that user is added for CCT.

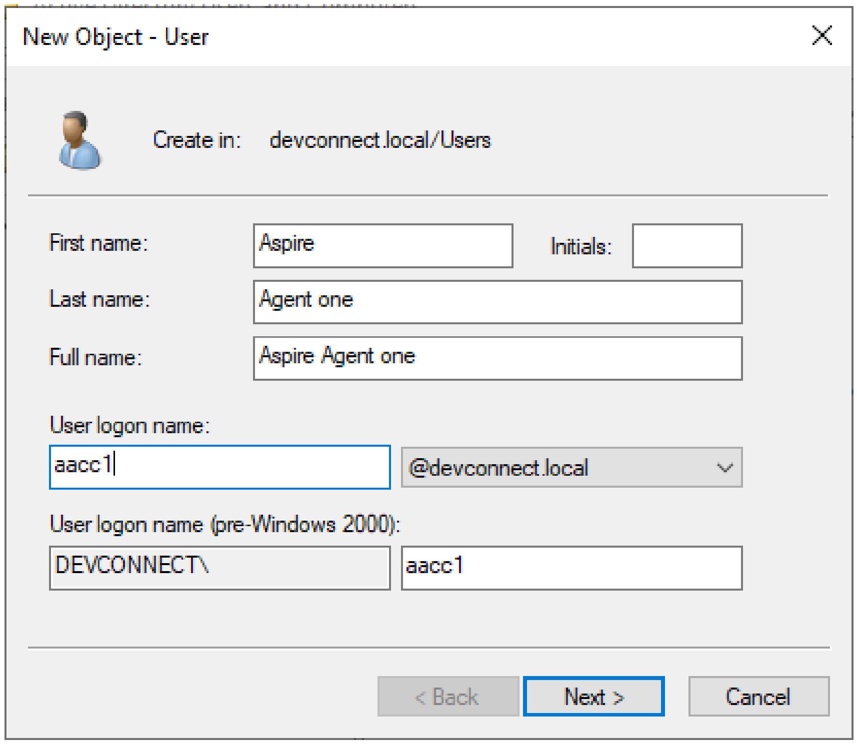
12.1. Add a Windows Domain User

On most sites running Contact Center, a domain will have been configured with an Active Directory containing windows users. A 'Domain Administrator' will be on hand to provide windows users information to configure the CCT user on Contact Center.

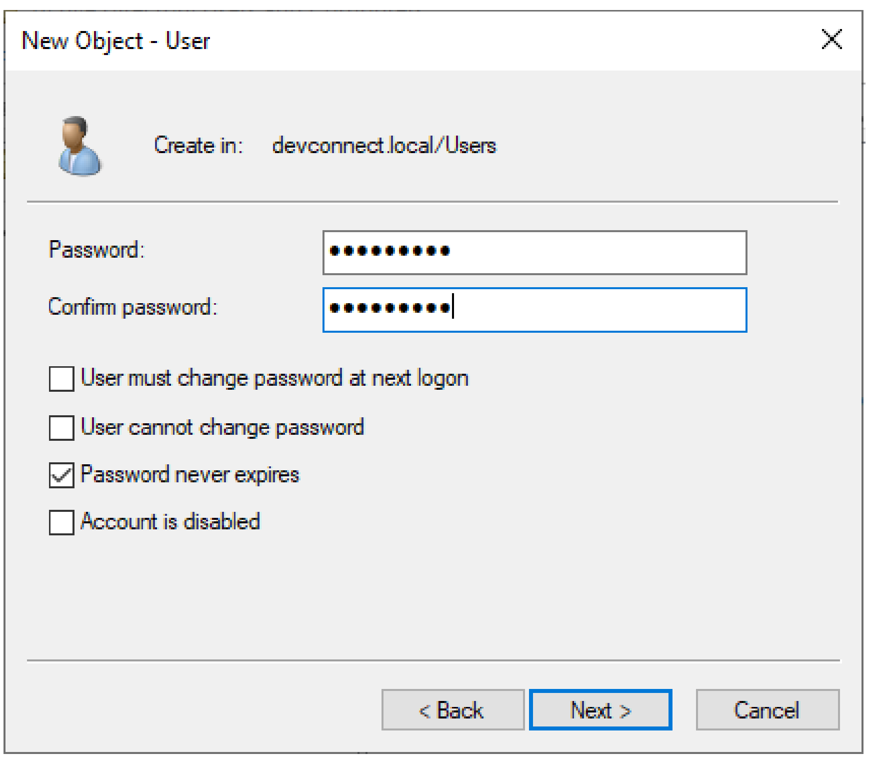
For compliance testing a domain was already in place with users previously added to this domain specifically for this solution test. To add or display users, open Computer Management and select **Active Directory Users and Computers** (not shown). The following window is opened where new users are added by right-clicking on **Users** and selecting **New → User** as shown below.



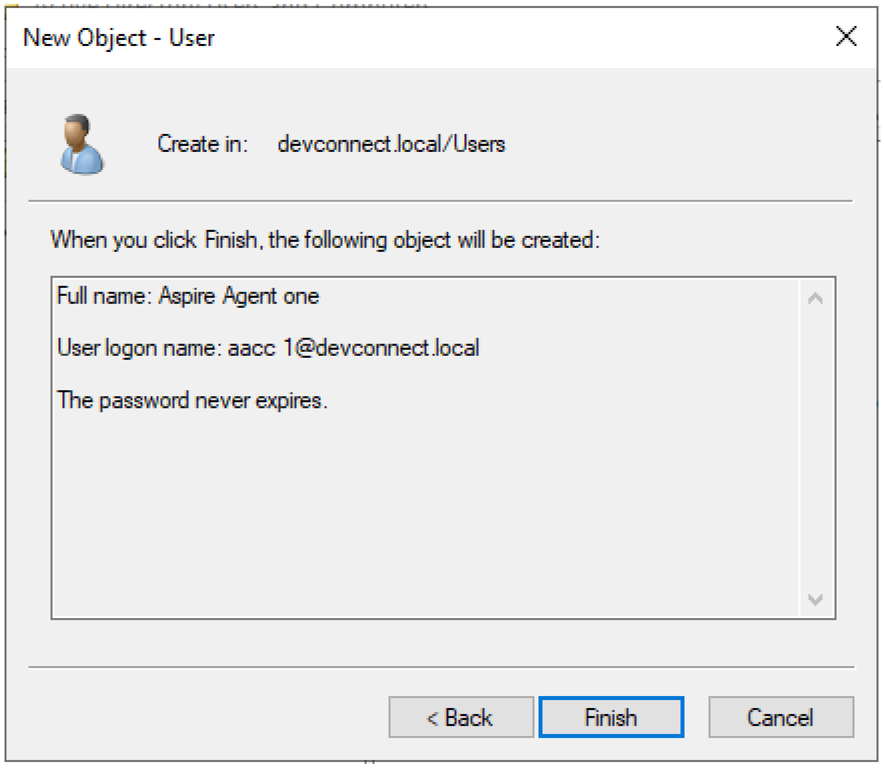
Enter the details as shown in the example below for **aacc1** and click on **Next**.



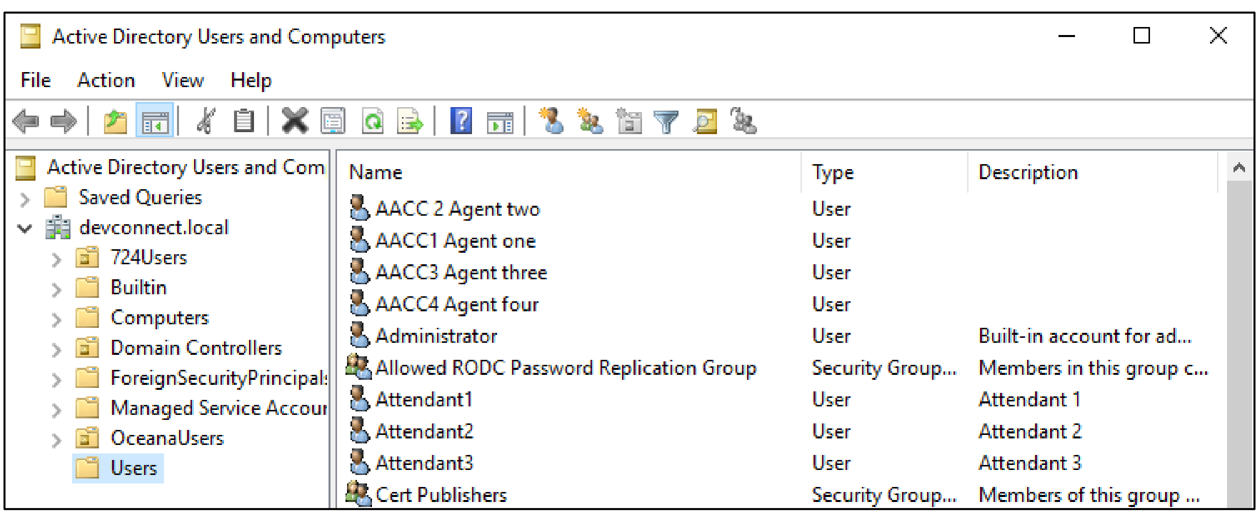
Enter the required **Password** and click on **Next** to continue.



Click on **Finish** to complete the addition of the new user that will be used for CCT.

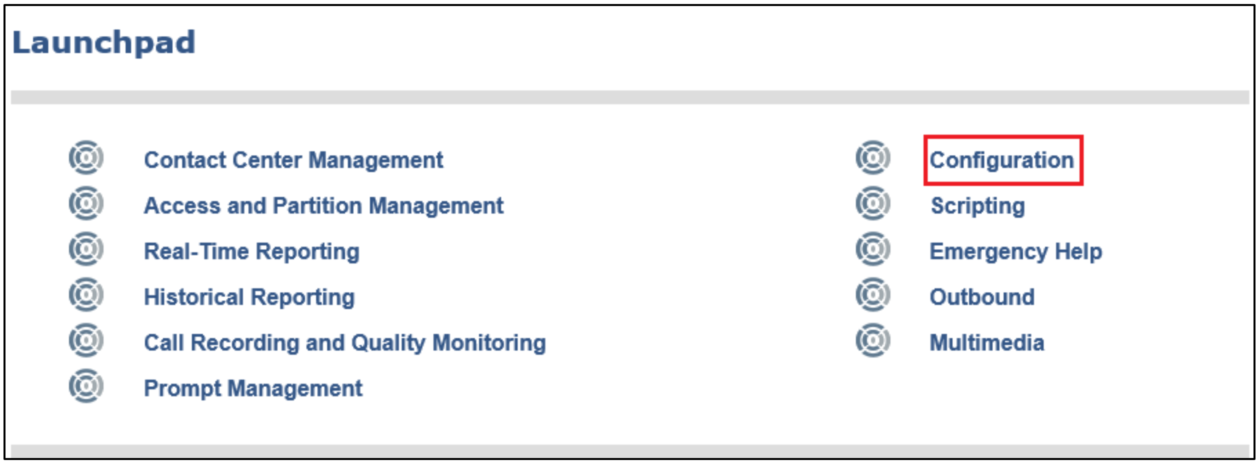


Four users were added specifically for compliance testing, these are **AACC1**, **AACC2**, **AACC3** and **AACC4**. These were added as there were four different phone set types used for the agent phones.

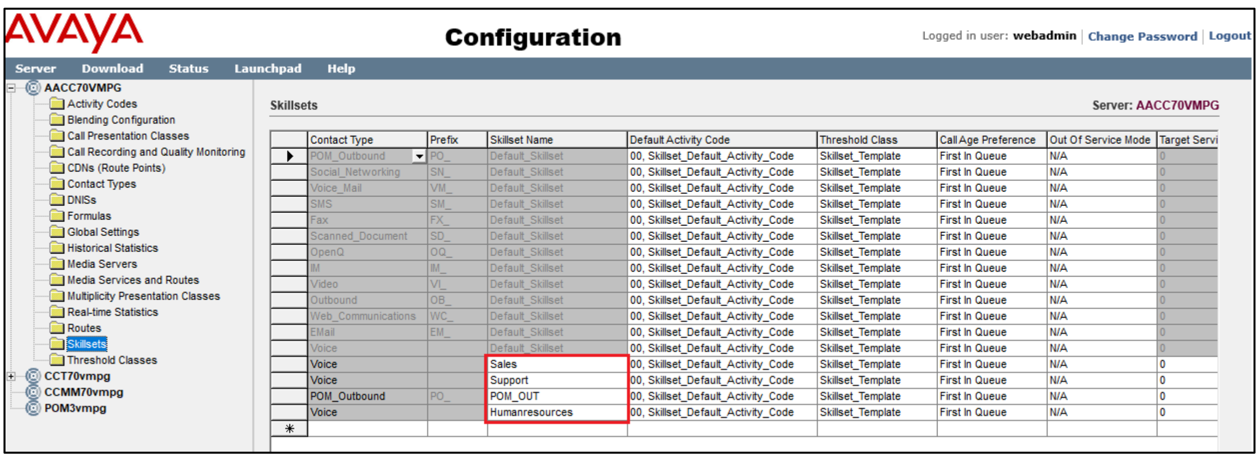


12.2. Skillset, Route Point and Call Presentation Information

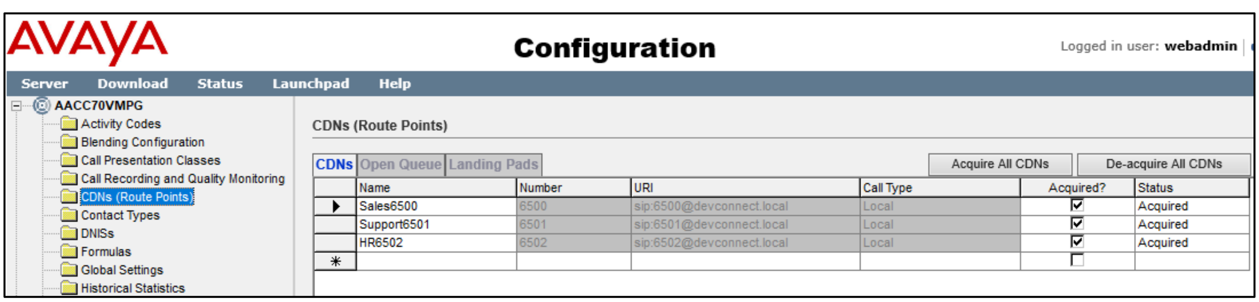
Log into Contact Center as per **Section 6.3**. From the **Launchpad** click on **Configuration**.



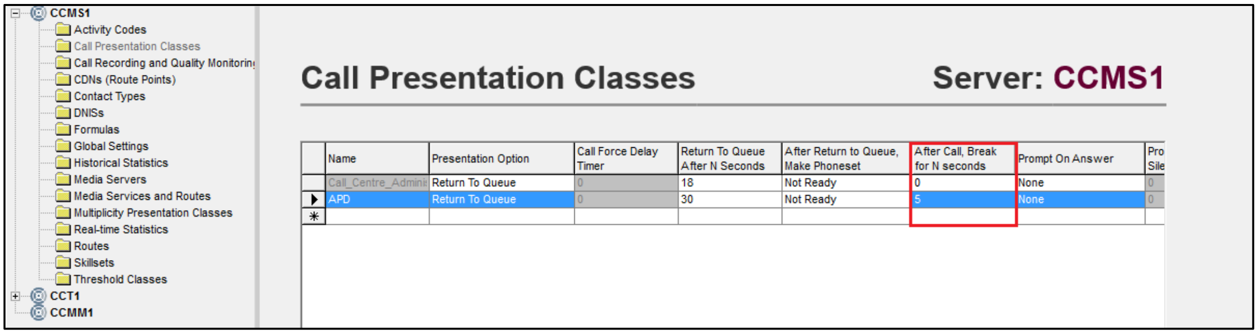
Expend the AACC server in the left window and click on **Skillsets**. The **Skillset Name**s are highlighted, and these will be assigned in **Section 12.3**.



Click on **CDNs (Route Points)** to display the numbers that are to be dialed to reach the required skillsets.

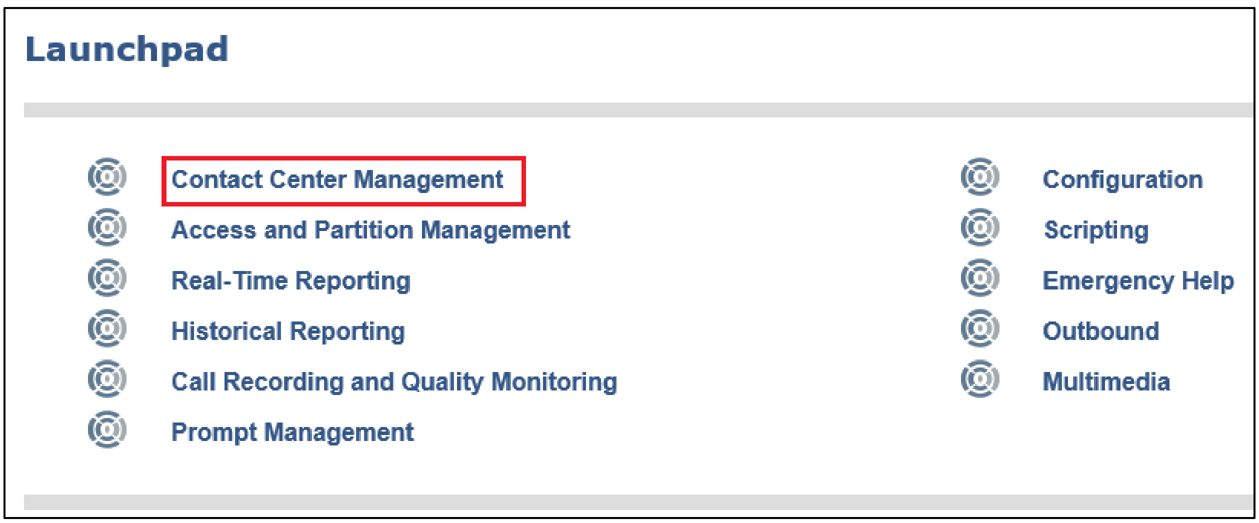


Click on **Call Presentation Classes** to show calls are presented to the agents. This can be used to force the call to the agent or to let the phone ring at the agents set or a set amount of time before returning the call to the queue. This Call Presentation Class will be assigned to the agent in **Section 12.3**.

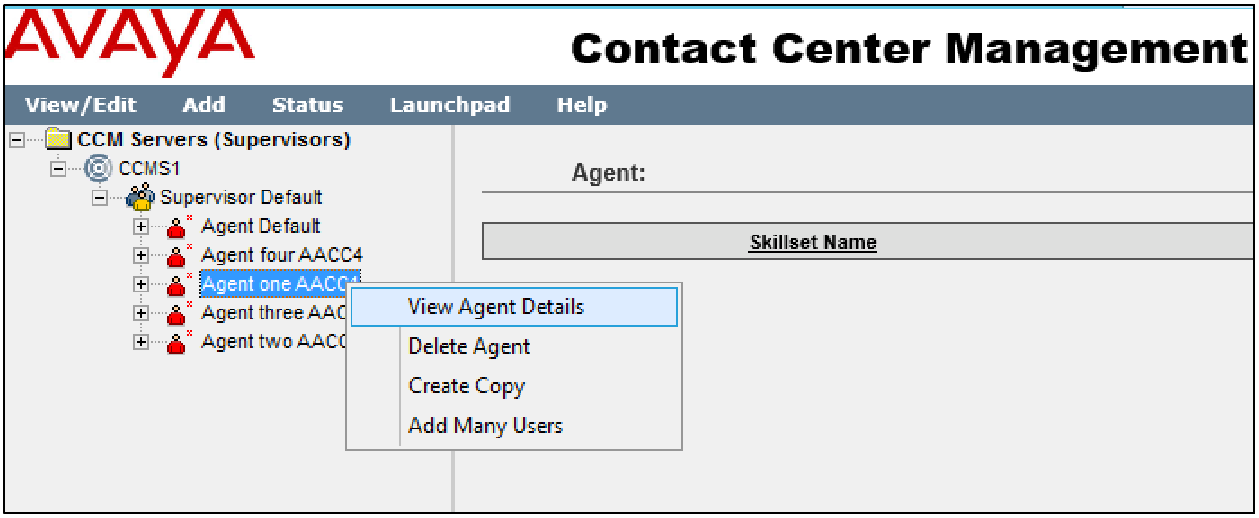


12.3. Contact Center Agent information

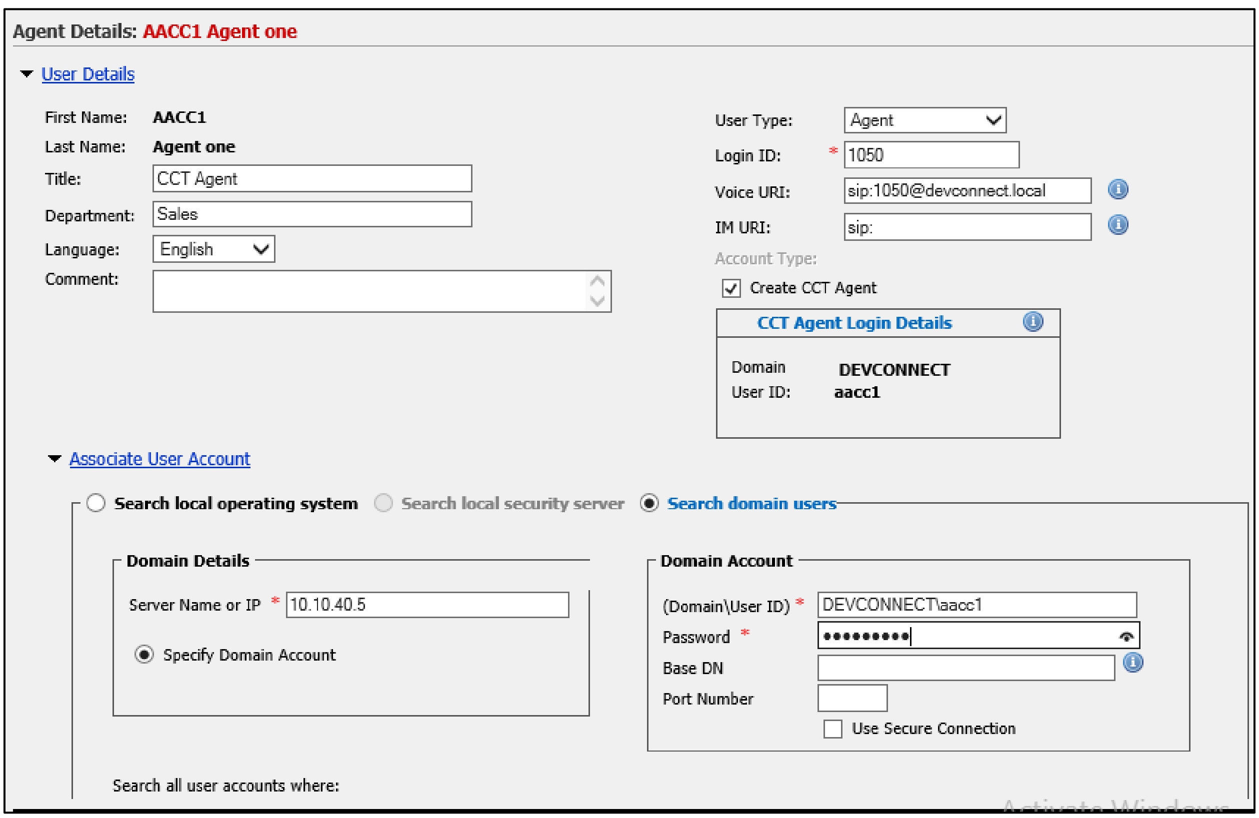
From the **Launchpad**, click on **Contact Center Management**.



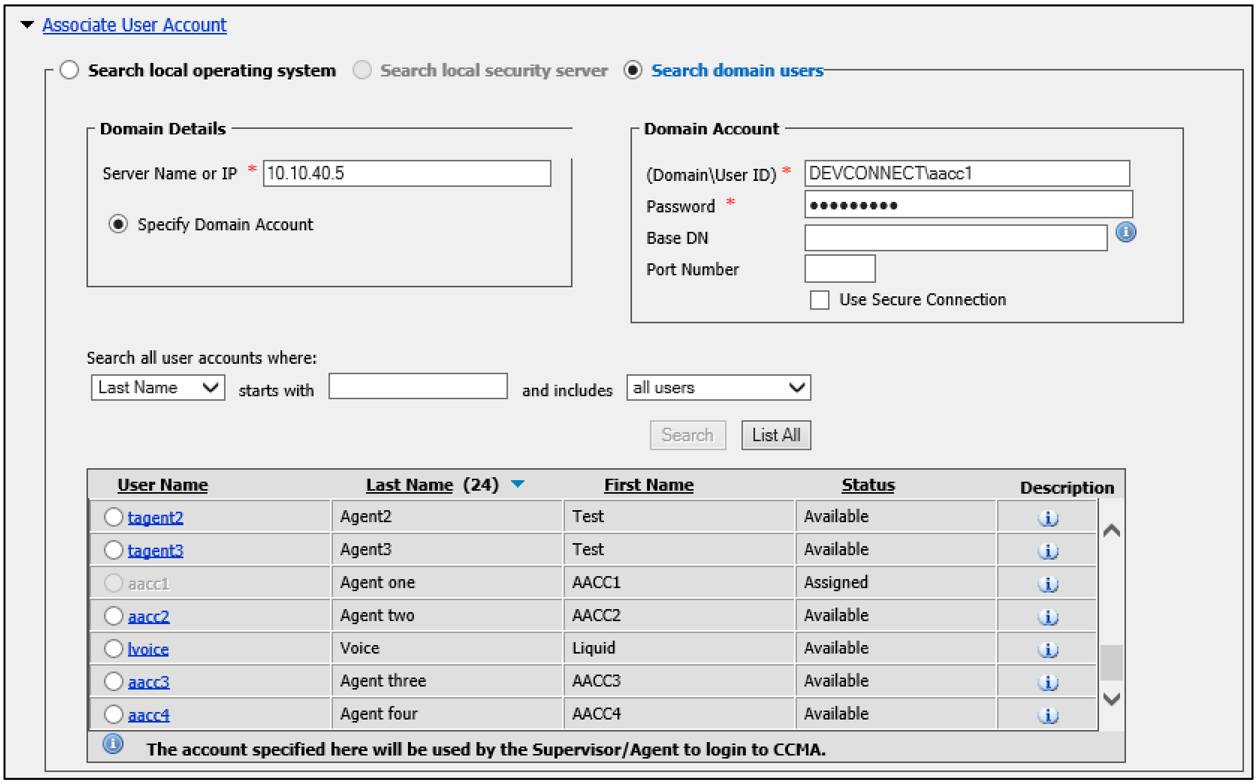
An existing agent can be associated with the domain user created in **Section 12.1**. Right-click on the desired user and select **View Agent Details**.



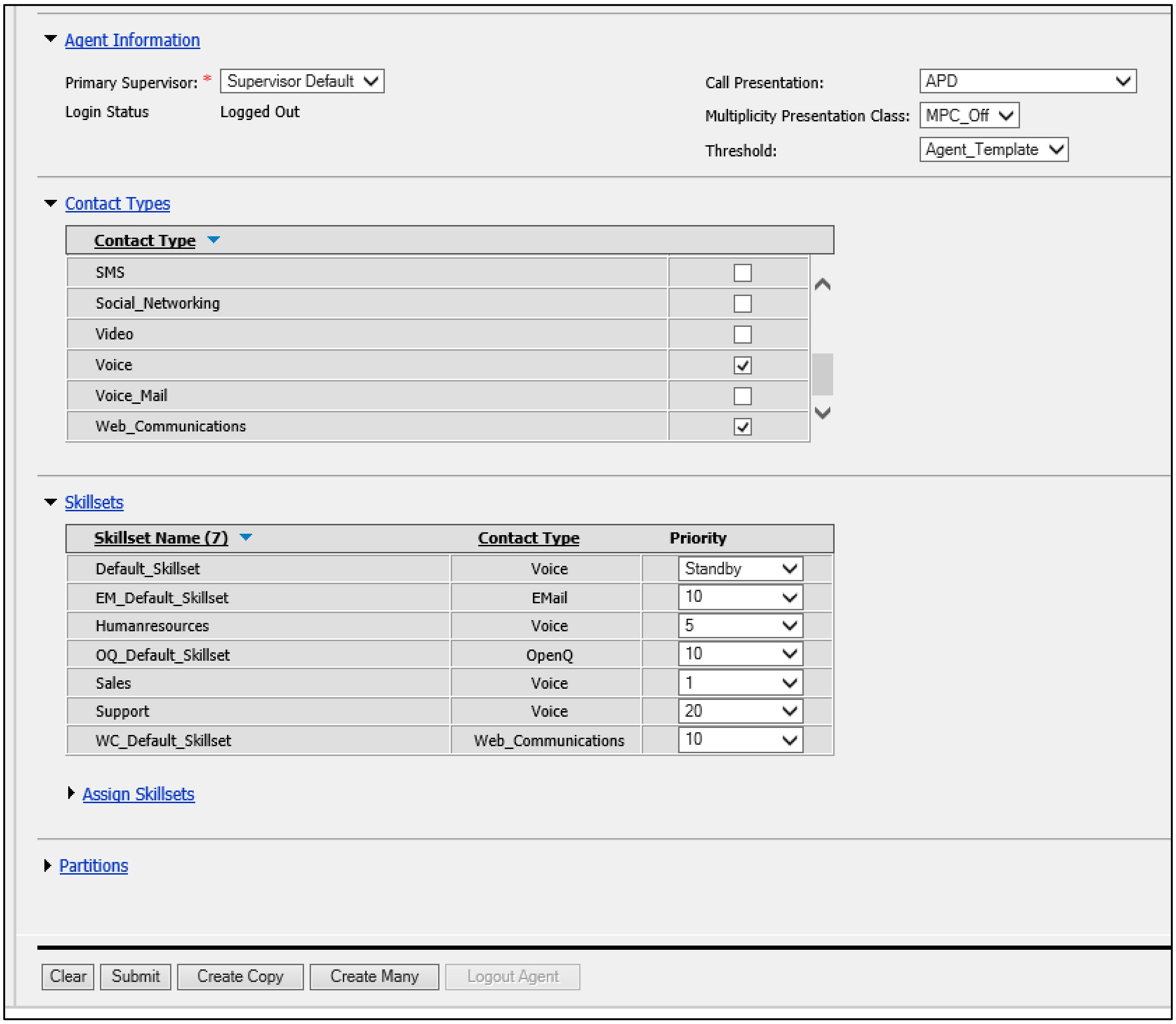
Tick the **Create CCT Agent** and expand the **Associate User Account** and selecting the **Search domain users**. Enter the domain user created in **Section 12.1** and click on list all (not shown). The **Login ID** and **Voice URI** were set to that of the Communication Manager extension that is associated with this agent.



The list of domain users is then displayed where the appropriate user can be selected as shown below.



Other information such as the **Call Presentation** (described in **Section 12.2**) and assigned **Skillsets** are displayed and can be changed. Once all is complete, click on **Submit**.



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.