Avaya Solution & Interoperability Test Lab

Application Notes for NEC Cortex with Avaya Aura® Contact Center and Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning NEC Cortex v8 to successfully interoperate with Avaya Aura® Contact Center R7.1.2.1 and Avaya Aura® Communication Manager R10.1. Cortex is an Agent Desktop GUI that connects to the Communications Control Toolkit (CCT) Application Programming Interface (API) on Avaya Aura® Contact Center to gain control of existing Avaya phonesets.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect Compliance Testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps for provisioning Cortex by NEC to successfully interoperate with Avaya Aura® Contact Center and Avaya Aura® Communication Manager.

Cortex is an integrated command and control system designed to help call operators identify and protect vulnerable people. It provides control room operators with a single interface, the Cortex GUI, that provides a number of key features, including:

- Radio Dispatch
- Telephone call handling
- Access Control
- CCTV monitoring

From a telephony standpoint, the focus for these Application Notes is on telephone call handling. Cortex, essentially, is an Agent Desktop GUI that connects to the Communications Control Toolkit (CCT) Application Programming Interface (API) on Avaya Aura® Contact Center to gain control of existing Avaya phonesets. This allows Cortex to log in agents into existing Avaya endpoints and take control of these endpoints to provide telephony functionality to the agent via their PC and the Cortex GUI. The Cortex Agent Desktop connects to Contact Center without the requirement of any Avaya desktops such as Avaya Aura® Agent Desktop.

Cortex makes use of the CCT .NET API which is implemented as a set of .NET types and interfaces that provides the user with a set of objects that can be used to develop communications applications. These applications communicate with the CCT server. This API uses the Microsoft .NET Framework to allow DevConnect members to quickly build and deploy robust applications that take advantage of the Microsoft common language runtime environment as well as security and connectivity features provided using the Windows Communication Foundation (WCF).

2. General Test Approach and Test Results

The interoperability compliance testing focused on verifying Cortex handling of CTI messages in the areas of call control and event notification. Compliance testing focused on the handling of calls presented to and made from the Cortex GUI. Basic calls were made to and from the Avaya phones associated with the Cortex GUI, as well as skillset calls that were made to Contact Center route points and delivered to Contact Center agents associated with those route points. A fully operational Contact Center was in place to facilitate the compliance testing. Agents were available to Cortex which had skillsets associated with them and calls routing correctly to those skillsets. The Cortex GUIs were verified by associating these agents to the Cortex users and making calls to the agents.

Two workstations running Windows 10 were added to a domain with three domain users. These domain users were associated with three CCT users, which in turn were associated with three Contact Center agents. These new operators/users/agents were then used to log into the Cortex GUI to make and receive calls as well as take skillset calls made to the route points. The Cortex database on an MS SQL 2019, which ran on Windows 2019 server stored the telephony configuration. The Cortex GUI is a client running on the Windows 10 PC's which opens and retrieves this telephony configuration through the Cortex Application server to connect directly to CCT using the .net API. This allows the Cortex GUI to make/receive calls using existing Avaya endpoints. Three operators/users/agents were used to allow testing with three different endpoints, see **Section 4** for a list of the endpoints used.

The agents/extensions that were used for compliance testing are as follows.

Domain User	CCT user	Agent ID	Extension/SIP URI	Phone Type
• agent1	agent1	3001	3001	J100 Series (H.323)
• agent2	agent2	3101	3101	J100 Series (SIP)
• agent3	agent3	3063	3063	9400 Series Digital

Note: agent1 was used with J100 Series H.323 phone and with a one-X® Communicator softphone on separate occasions.

The Cortex Application server ran on a Windows 2019 server running IIS. The purpose of this server is to provide a REST API to the clients for accessing information on the Cortex Database Server. The Cortex Database server ran on the same Windows 2019 sever running Microsoft SQL 2019. In addition to storing configuration, the database contains information such as contact details, conversation notes and audio recordings, testing of these features was not part of this particular compliance test. For known contacts, it can provide vulnerability markers and repeat caller counts.

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 Cortex did not include use of any specific encryption features as requested by NEC.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on various technical testing scenarios to verify Cortex with Avaya Aura® Contact Center. A fully operational Contact Center was in place with calls successfully routing to Contact Center agents. These agents were logged into Avaya endpoints and the Cortex GUI which had control of the same Avaya endpoints. The testing focused on the following types of calls.

- **Agent Login/Logout** – Logging in operators on workstations.
- **Agent Not Ready Reason Codes** – A pop up window was observed displaying a list of not ready reason codes when the agent was to be placed into Not Ready.
- **Inbound/Outbound** – Test inbound/outbound calls directly to the agent's extensions logged into the Cortex GUI.
- **Inbound Skillset calls** – Using Cortex to answer skillset calls.
- **Hold/Transfer** – Test the hold and transfer functions again on the agent's extensions logged into the Cortex GUI.
- **Caller Information** – Tests the logic for the inclusion of caller information.
- **Other Features** – Tests that include click to dial, presence and coloured line groups.
- **Serviceability tests** – Simulating various LAN failures and observing the response of the Cortex under these conditions.

2.2. Test Results

Most test cases passed successfully. The following issues and observations were noted during compliance testing.

1. When an Avaya **SIP phone** transfers a caller (using blind transfer only) into the phone associated with the Cortex GUI, the call is presented to the actual phone but does not get presented to the Cortex GUI, this is the same for both operators (associated with H.323 or SIP phones). This is not working on Reference Client and the CCT event is not being passed to the Ref Client. Avaya have stated that "In a SIP-enabled Contact Center, blind (single-step) transfers are not supported", so this is working as designed.
2. When a call is made from the agent desktop to a busy or invalid number, there is a different response from the SIP phone as opposed to the H.323 phone. The H.323 phone shows the call still active on the agent desktop and that call, although not a real call, can be ended as such, but on the SIP phone the call remains on the deskphone and cannot be ended unless ended manually on the phone, as there is no actual call on the desktop to end the call. This is the same on Reference Client. Avaya have stated that this is working as designed
3. When a caller is transferred into the phone associated with the agent desktop, the agent desktop is not updated with the CLID of the transferred caller although this is updated on the actual phone, this is the same issue for both operators (associated with H.323 or SIP phones). This issue only occurs on certain transfers, if the A party or B party are monitored by CCT then this issue does not occur. This behavior is the same on the Reference Client. Avaya is investigating the issue.
4. For the AES LAN disconnect on the "serviceability tests" where there is a breakdown of communication between the Avaya components that results in the agent desktop becoming in operable, the agent is not aware of any issues and may not understand that

there is some kind of failure on the system. This is only the case for an agent that is already on a call when the LAN cable is unplugged. NEC are aware of this observation.

2.3. Support

Technical support can be obtained for Cortex from NEC as follows:

- Email: pssd@necsws.com
- Website: https://www.necsws.com/iccs/
- Phone: + 44 1482 808 300

3. Reference Configuration

Figure 1 shows the network topology in place during compliance testing. Communication Manager, a Media Server and a G430 Media Gateway were used as the hosting PBX. SIP trunks are configured between Communication Manager, Session Manager and Contact Center to allow calls pass to the Contact Center agents. Cortex GUI was loaded onto Windows 10 PC's and using .net API they connected to CCT allowing the control of existing Contact Center phone sets and the ability to log Contact Center agents into those sets. A simulated PSTN using an Avaya Session Border Controller for Enterprise was used to initiate calls into the Contact Center. The Cortex server along with the Cortex desktop clients made up the hardware/software for Cortex.

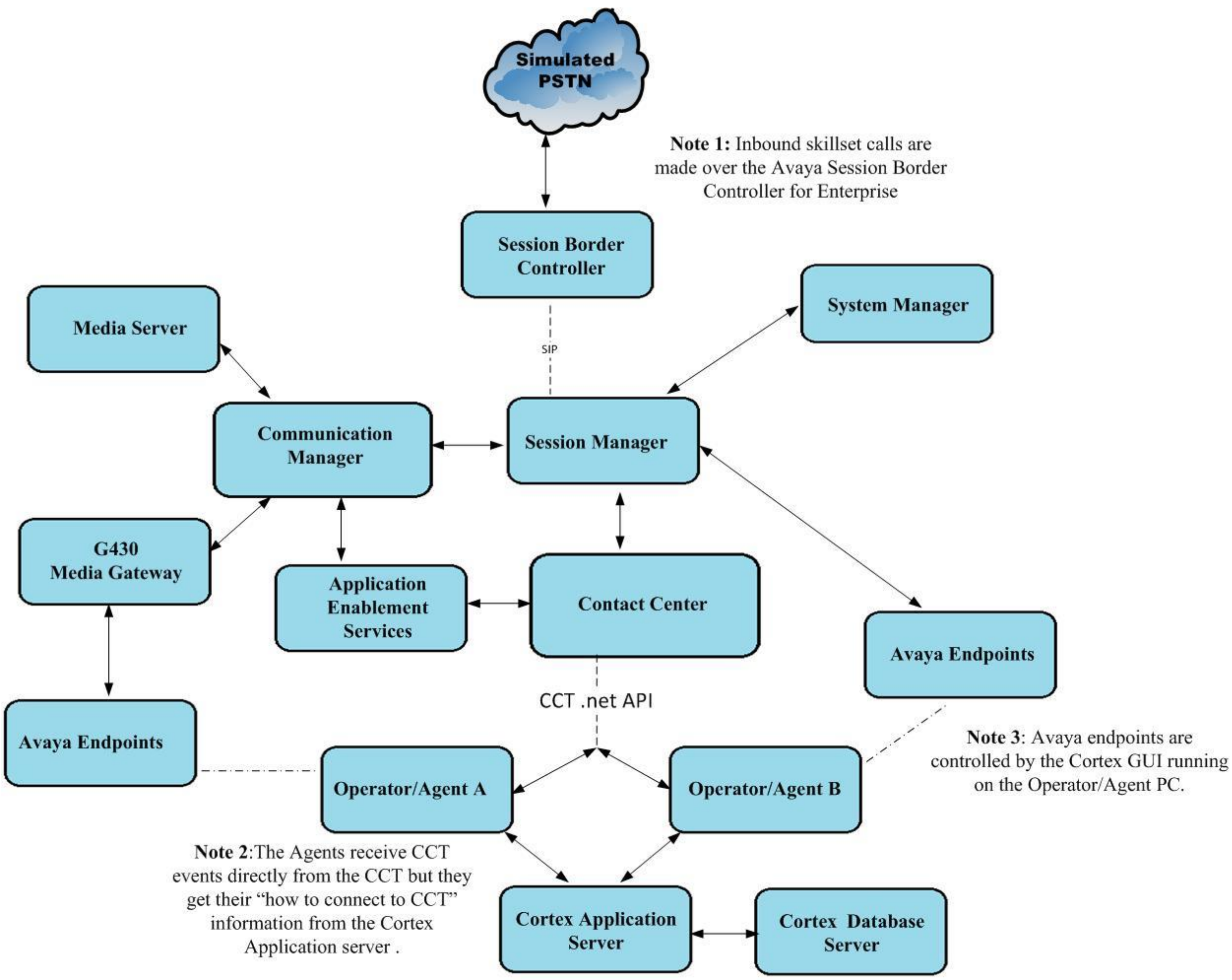


Figure 1: Network Topology used to test NEC Cortex with Avaya Aura® Contact Center R7.1 and Avaya Aura® Communication Manager R10.1

4. Equipment and Software Validated

All the hardware and associated software used in the compliance testing is listed below.

Avaya Equipment/Software	Firmware / Version
Avaya Aura® Contact Center running on Windows 2016 Server	R7.1.2.1 (See Appendix B [**12**])
Avaya Aura® System Manager	10.1.0.2 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.2.0715160 Service Pack 2
Avaya Aura® Session Manager	R10.1 Build No. – 10.1.0.2.1010219
Avaya Aura® Communication Manager	R10.1.0.2.0 – SP2 R020x.01.0.974.0 Update ID 01.0.974.0-27607
Avaya Aura® Application Enablement Services	10.1.0 Build 10.1.0.2.0.12-0
Avaya Aura® Media Server	10.1.0.101
Avaya Media Gateway G450	42.7.0 /2
Avaya 9404 Digital	17.0
Avaya J100 Series (SIP)	7.1.2.0.14
Avaya J100 Series (H323)	7.0.14.0.7
Avaya OneX® Communicator (H.323)	6.2.14.15 - SP14-Patch7
Avaya Session Border Controller for Enterprise (to facilitate simulated PSTN)	10.1.0
NEC Equipment /Software	**Firmware / Version**
NEC Cortex on Windows Server 2019 NEC Telephony Gateway	8.25.3.1 8.25.3.304

Table 1: Hardware and Software Version Numbers

Note: All equipment is running on Virtual machines on VMware.

5. Configure Avaya Aura® Communication Manager

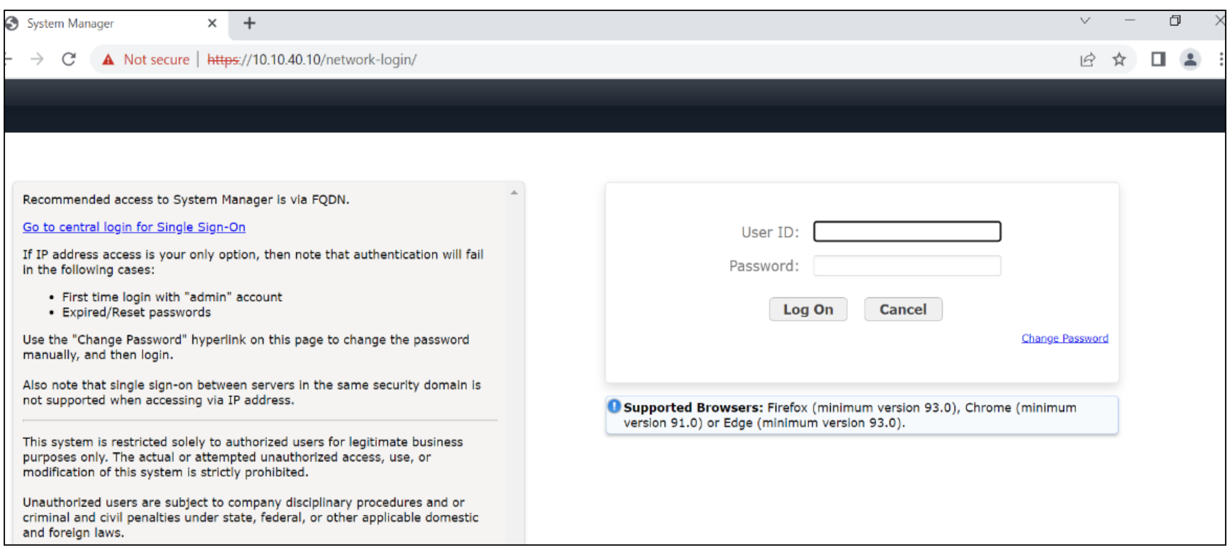
It is assumed that a fully functioning Communication Manager is already in place with all the necessary licenses. It is also assumed that the connections to Session Manager and Application Enablement Services are in place and therefore fall outside the scope of these Application Notes. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

Note: The configuration of the routing to Route Points 68xx and the SIP trunk configuration are included in **Appendix A** [**11**] of these Application Notes.

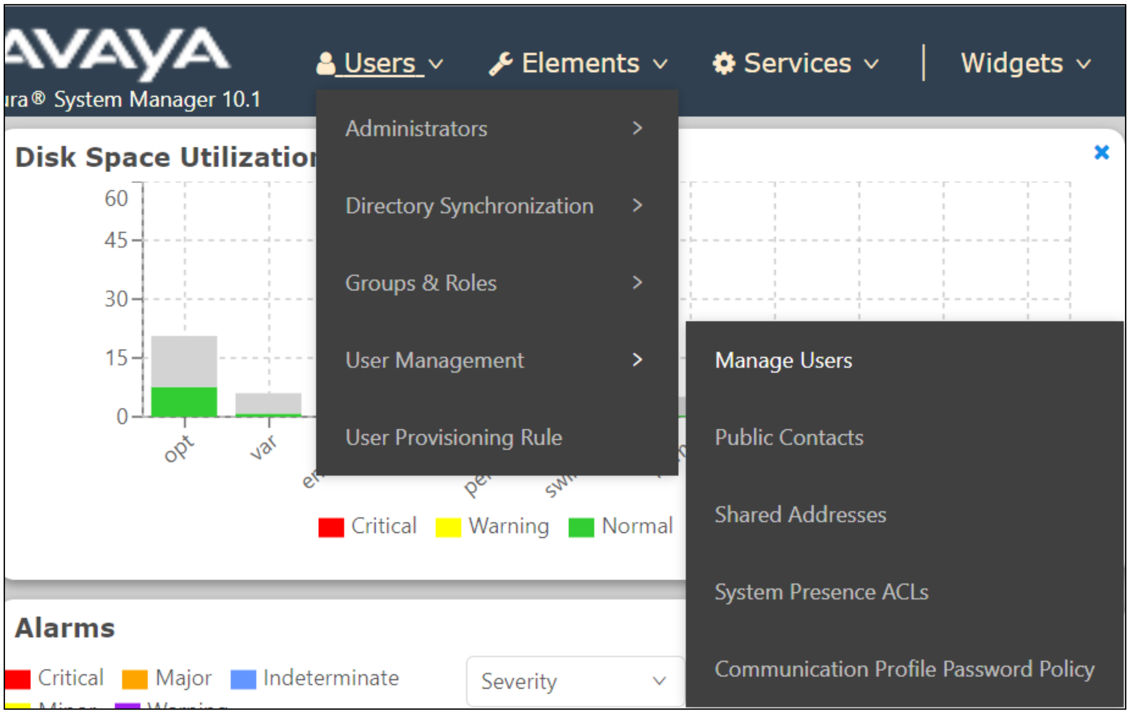
5.1. Configure Avaya SIP Endpoints for Third Party Call Control

Each Avaya SIP endpoint that needs to be monitored and used for 3rd party call control will need to have "Type of 3PCC Enabled" set to "Avaya". Changes to SIP phones on Communication Manager must be carried out from System Manager. Access the System Manager using a Web Browser by entering **http://<FQDN >/network-login**, where **<FQDN>** is the fully qualified domain name of System Manager or **http://<IP Address>/network-login**. Log in using appropriate credentials.

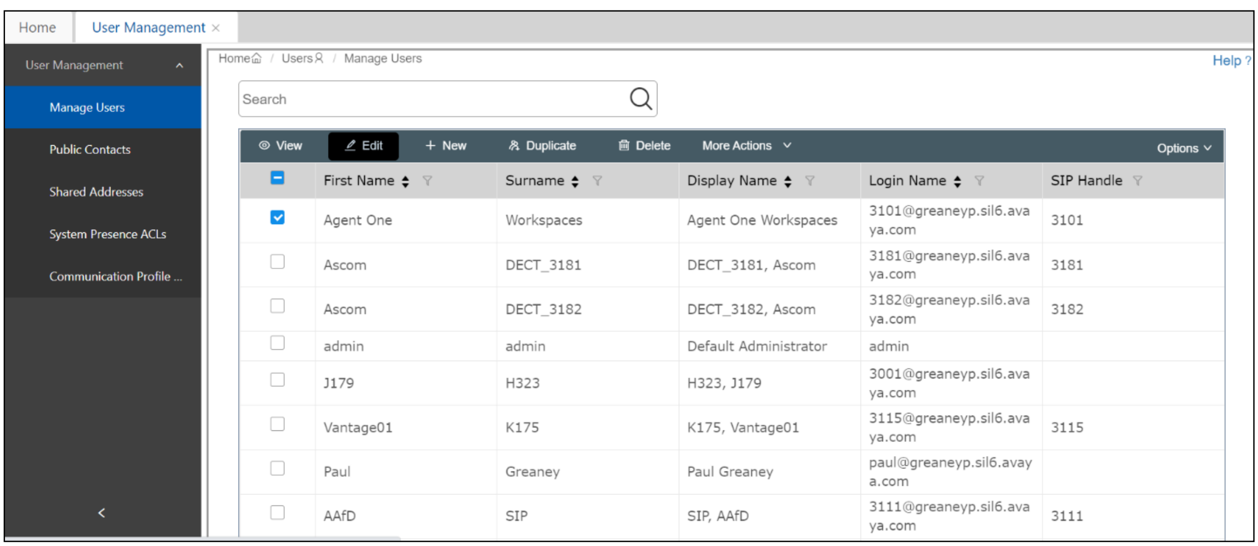
Note: The following shows changes a SIP extension and assumes that the SIP extension has been programmed correctly and is fully functioning.



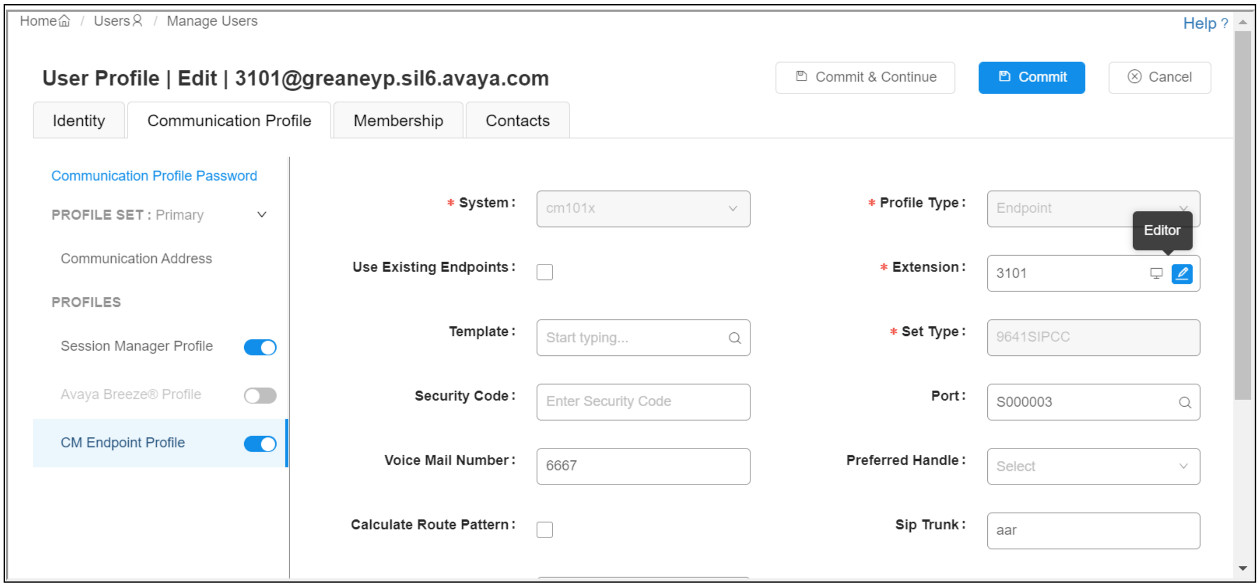
From the home page click on **Users → User Management → Manage Users** as highlighted below.



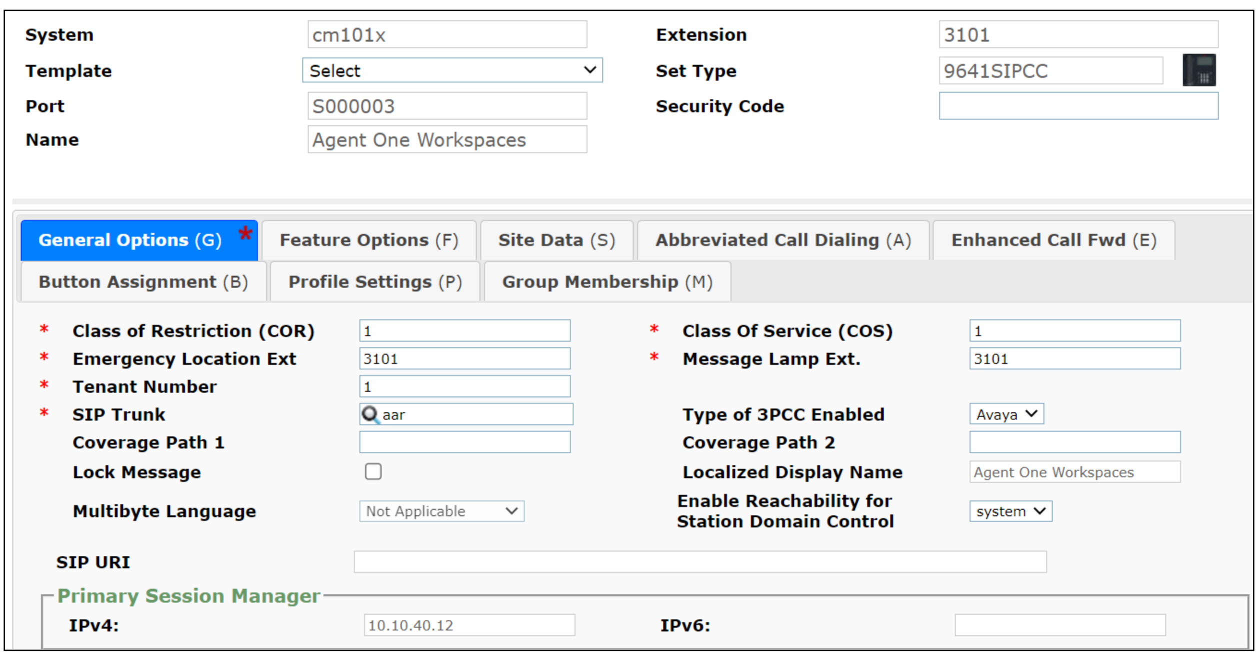
Select the station to be edited and click on **Edit**. The example below shows that SIP extension **3101** is selected.



Click on the **CM Endpoint Profile** tab in the left window. Click on **Endpoint Editor** to make changes to the SIP station.



In the **General Options** tab ensure that **Class of Restriction** is set correctly. Set **Type of 3PCC Enabled** to **Avaya**. Click on **Done**, at the bottom of the screen once this is set, (not shown).



Click on **Commit**, on the resulting page (not shown), to save the changes.

6. Configuring Avaya Aura® Contact Center

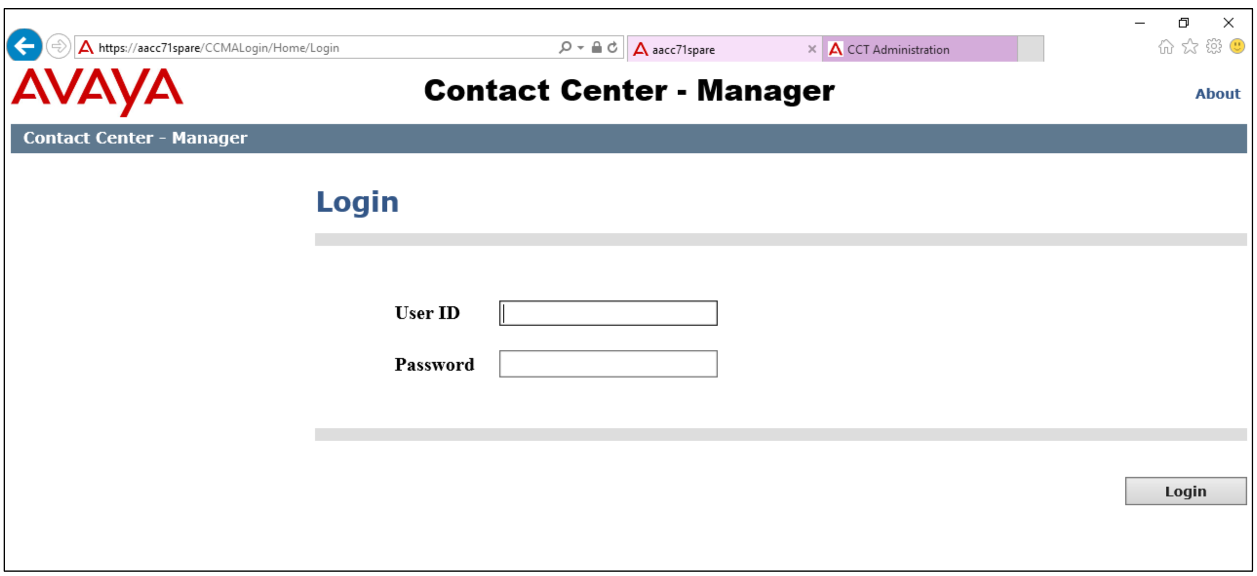
The Cortex GUI connects to an existing, fully functioning Contact Center. Each Contact Center that Cortex interfaces with may be setup and configured differently and there is no specific configuration of Contact Center required in order for Cortex to function correctly other than to have a fully working Contact Center with CCT agents available and taking skillset calls. However, certain information on the Contact Center is required by NEC to configure Cortex correctly. Such information includes:

- Communication Control Toolkit API Port Information
- Skillset Information
- Contact Center Agent Information
- Communication Control Toolkit User Information

Where this section does not include the installation and configuration of Contact Center, the steps to find the information listed above are listed to aid in outlining the configuration details for integration of Cortex with Contact Center.

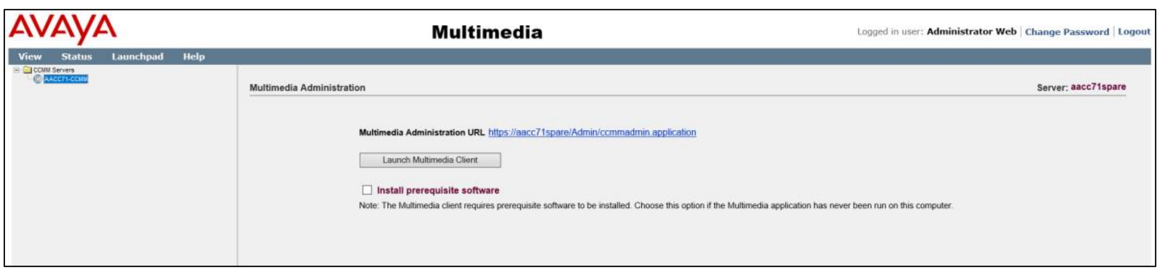
6.1. CCT API Port Information

The following steps can be taken to find the port of the CCT API. Open a URL to the Contact Center. Enter the appropriate credentials and click on **Login**.

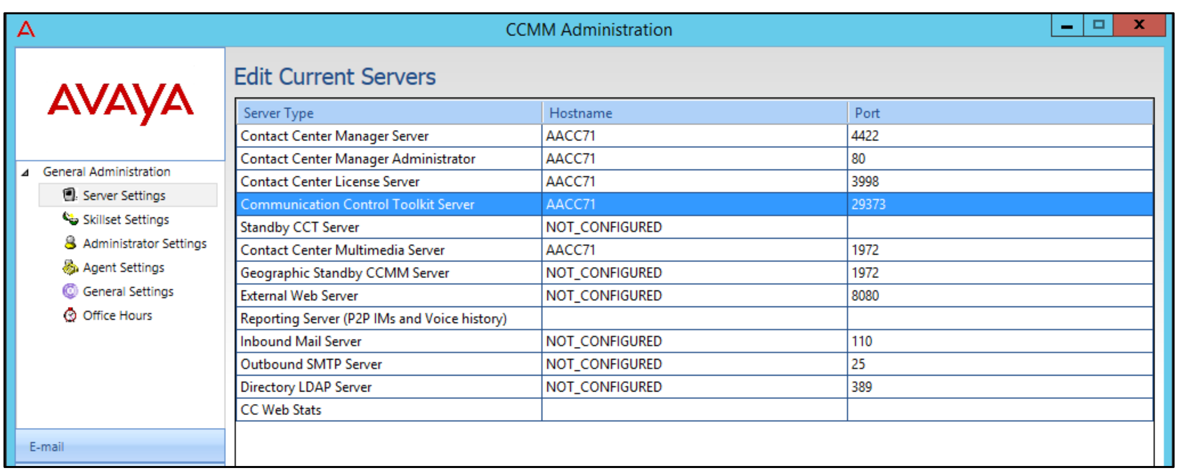


Once logged in select **Multimedia**, as shown.

Click on **Launch the Multimedia Client**. If this is being run for the first time, **Install prerequisite software** should also be ticked.



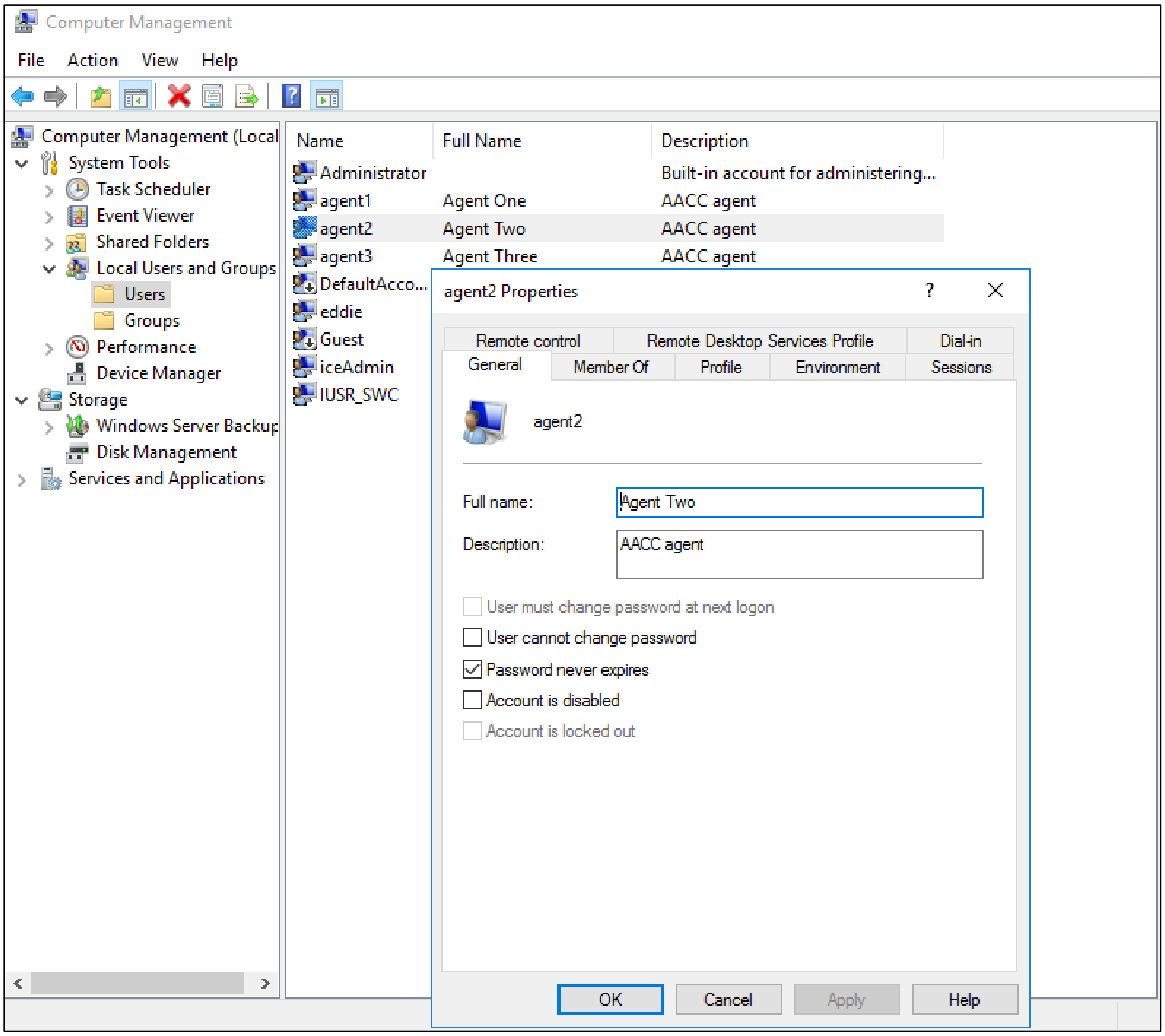
Under **General Administration →** Server Settings, information on the **Communication Control Toolkit Server** can be observed including the **Port** information which is displayed as **29373** below.



6.2. Observe Windows Domain Users

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 that can be used by the NEC engineers to configure the connection to Contact Center.

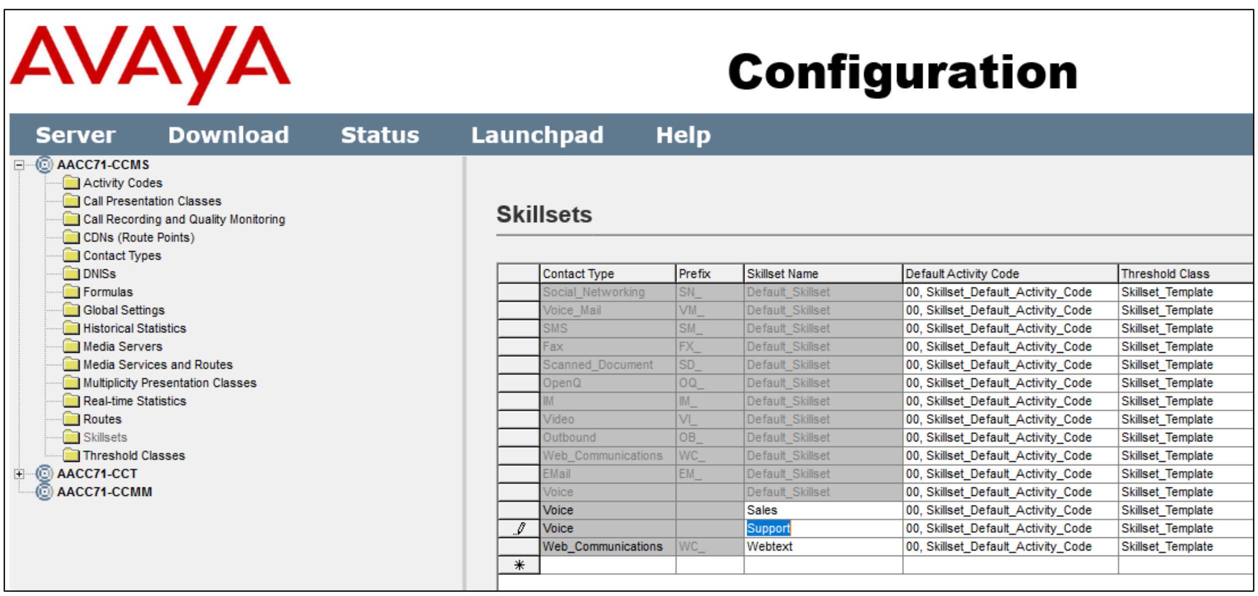
For compliance testing a domain was not configured, Contact Center was a standalone server in Workgroup and so each CCT user was added to the Contact Center server as a basic user. To add or display users, open Computer Management and select **Users**. The following window is opened where new users are added by right-clicking on **Users** and selecting **New → User** (not shown). Shown below is the information on a user called **agent2**. There are three users added as there were three agents that were tested as per the information outlined in **Section 2**.



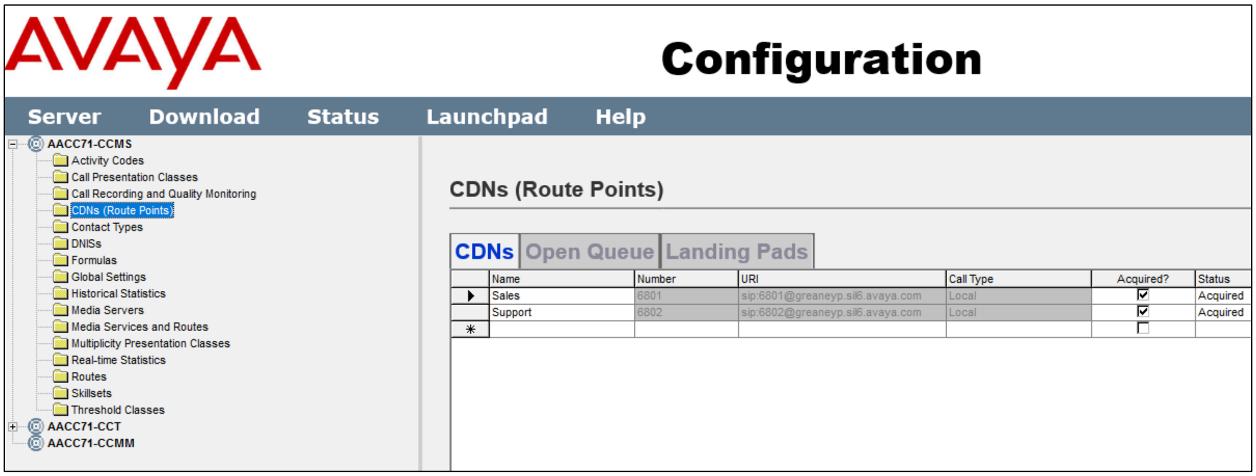
6.3. Skillset Information

Log into Contact Center as per **Section 6.1**. From the **Launchpad** click on **Configuration**.

Expand the AACC server in the left window and click on **Skillsets**. The **Skillset Name**s are highlighted, and these will be used in the Cortex setup in **Section 7.4**.



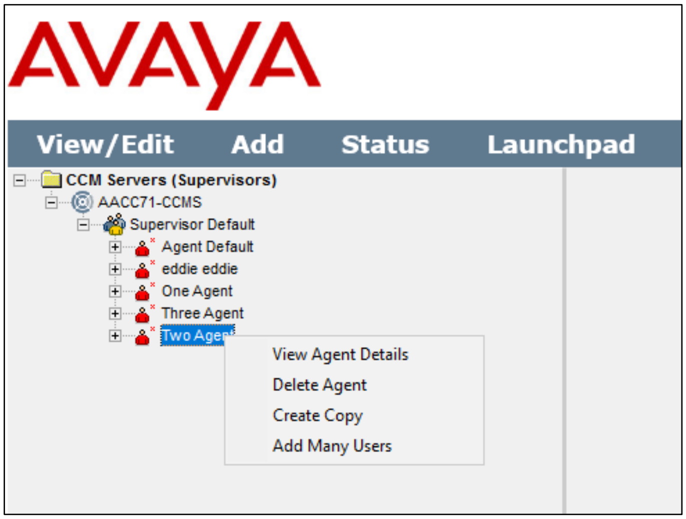
Click on **CDNs (Route Points)** to display the numbers that are to be dialed to reach the required skillsets. Note that **6801** and **6802** are used as the numbers associated with the Sales and Support skillsets. These numbers are routed to Contact Center as per **Section 11.3** in **Appendix A**.



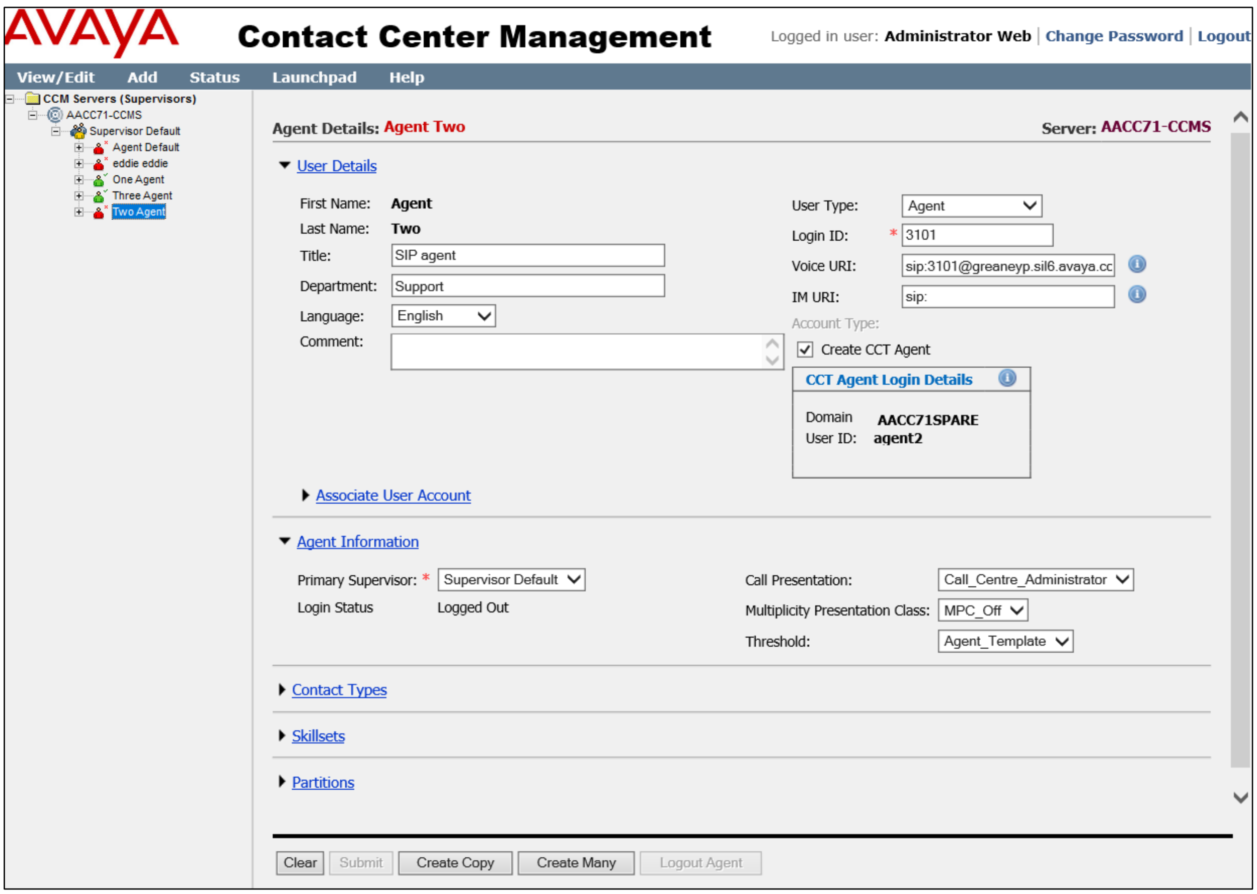
6.4. Contact Center Agent information

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

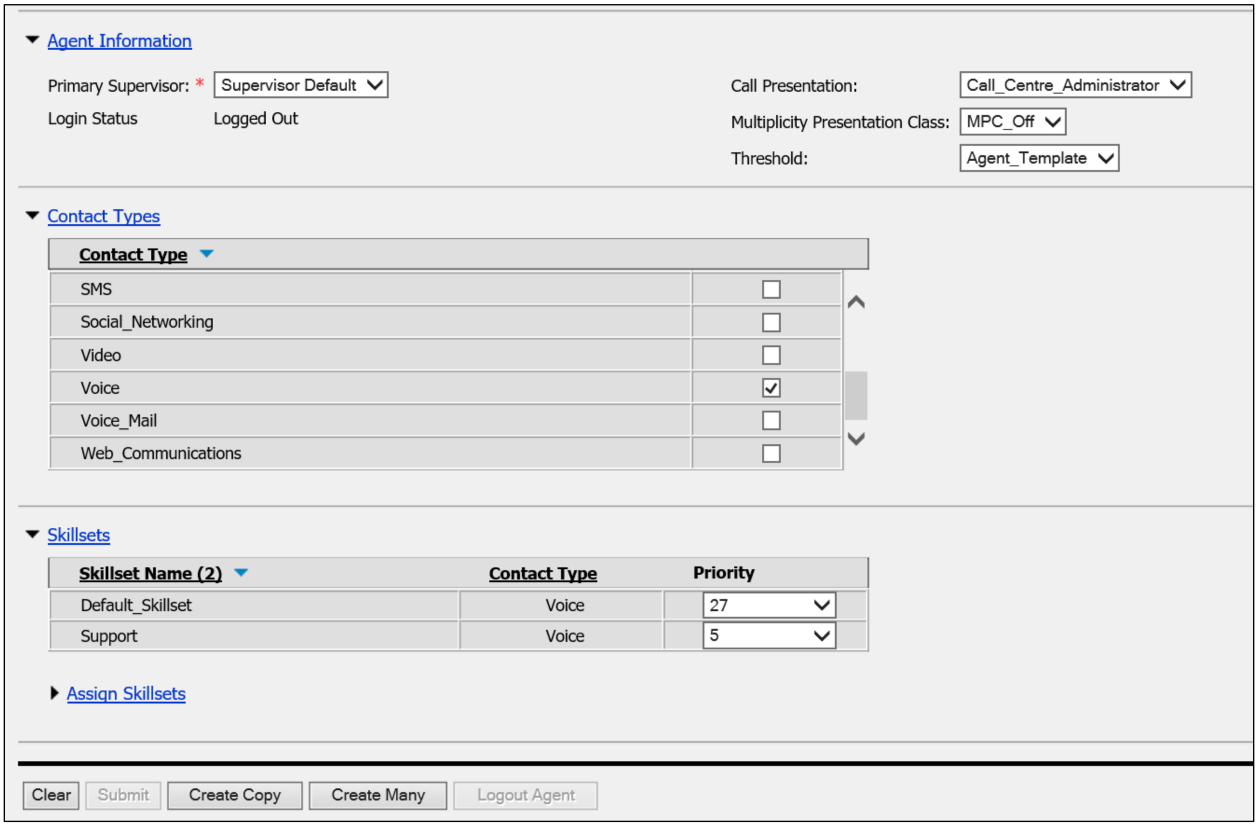
Information on existing agents can be observed by right-clicking on the desired agent and select **View Agent Details**.



Information such as the **Login ID** and **Voice URI** is useful for the Cortex configuration. Note that this agent is already configured and associated with the CCT user **agent2**.



Other information such as the **Contact Type** and assigned **Skillsets** are displayed and can be changed. Once all is complete, click on **Submit**.

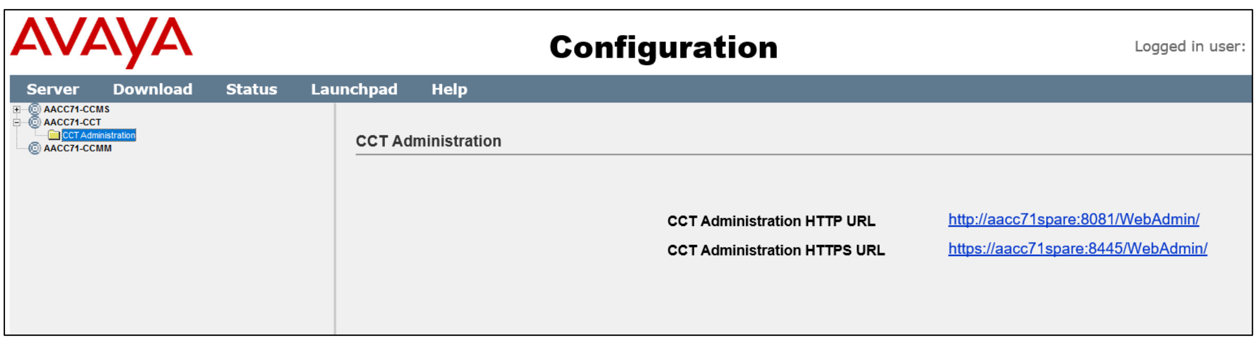


6.5. Communication Control Toolkit User Information

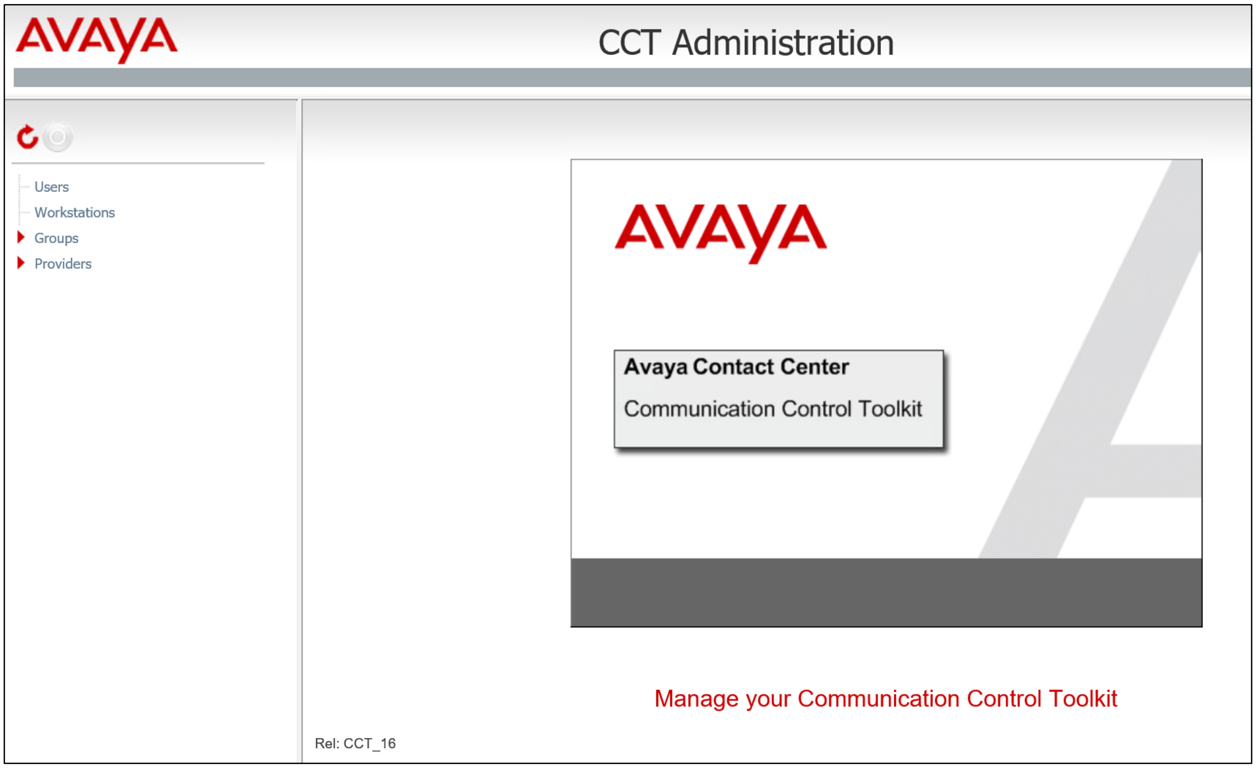
Cortex connects to Communication Control Toolkit (CCT) to enable the Cortex Agent Desktop to take control of Avaya phones and log in Contact Center agents. The CCT user must be present to allow Cortex to connect to CCT and log in that user on the Agent Desktop.

From the **Launchpad**, click on **Configuration**.

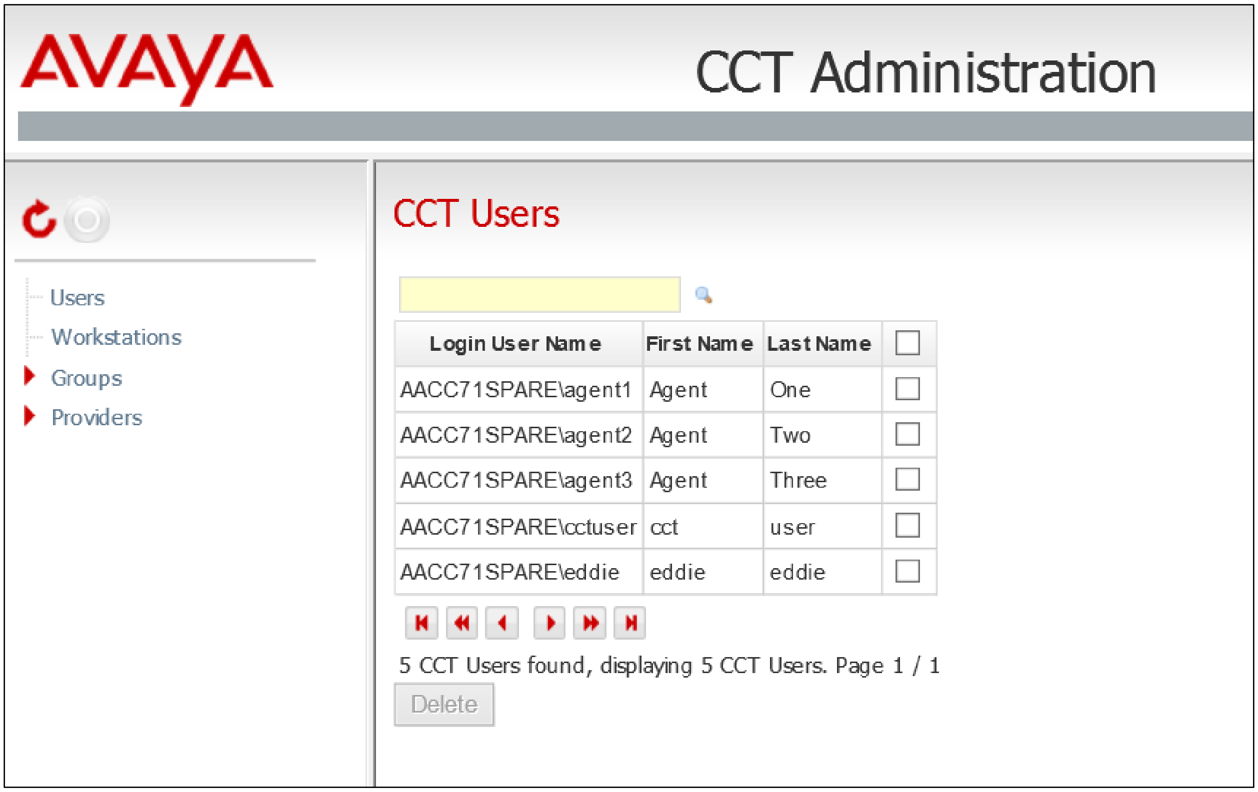
Expand the CCT server in the left window and click on the appropriate URL in the main window.



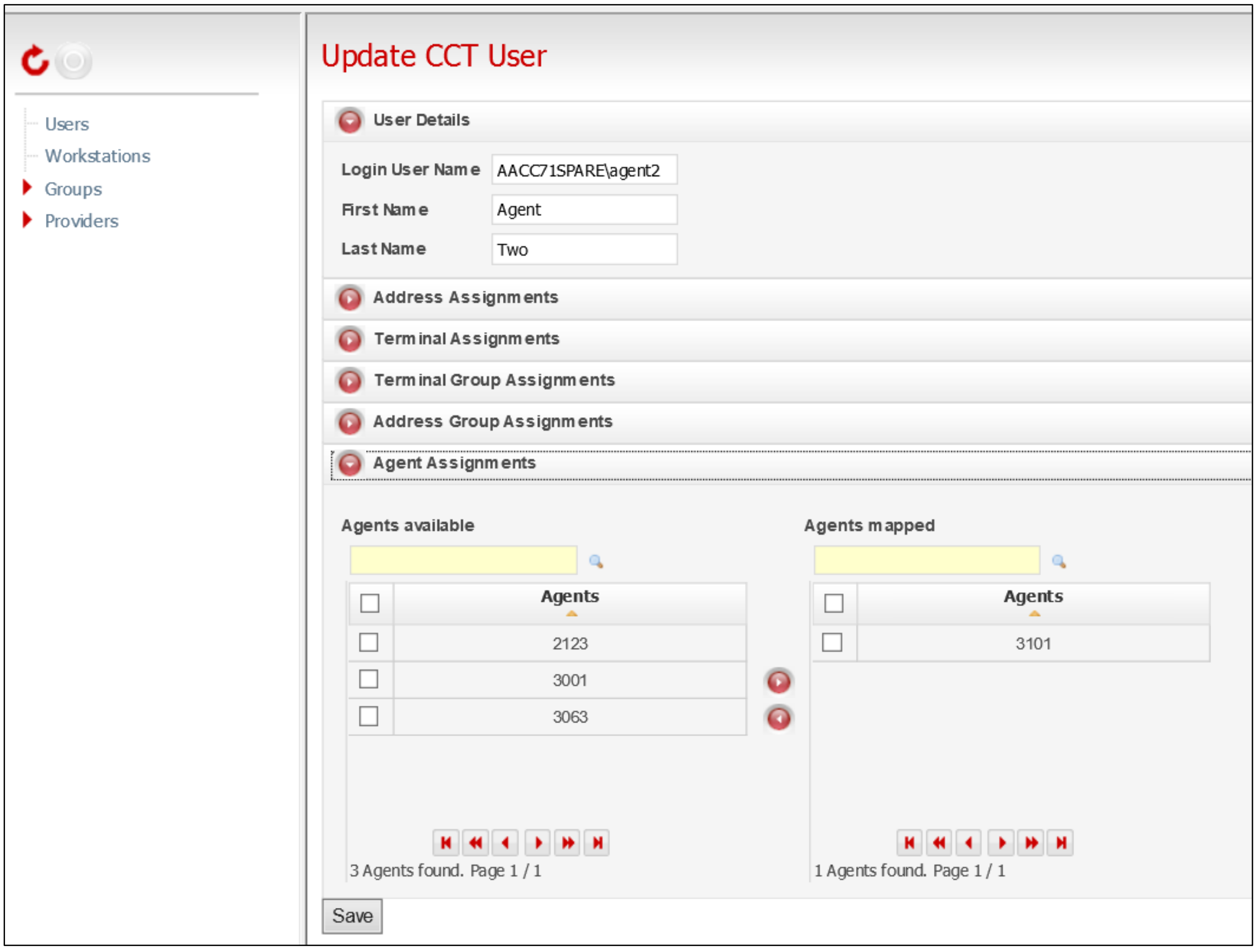
The following **CCT Administration** window is opened, where the CCT Users, Workstations, Groups and Providers can be administered. Click on **Users** in the left window.



The following CCT users are configured, including **agent1**, **agent2** and **agent3** that were all used for compliance testing.

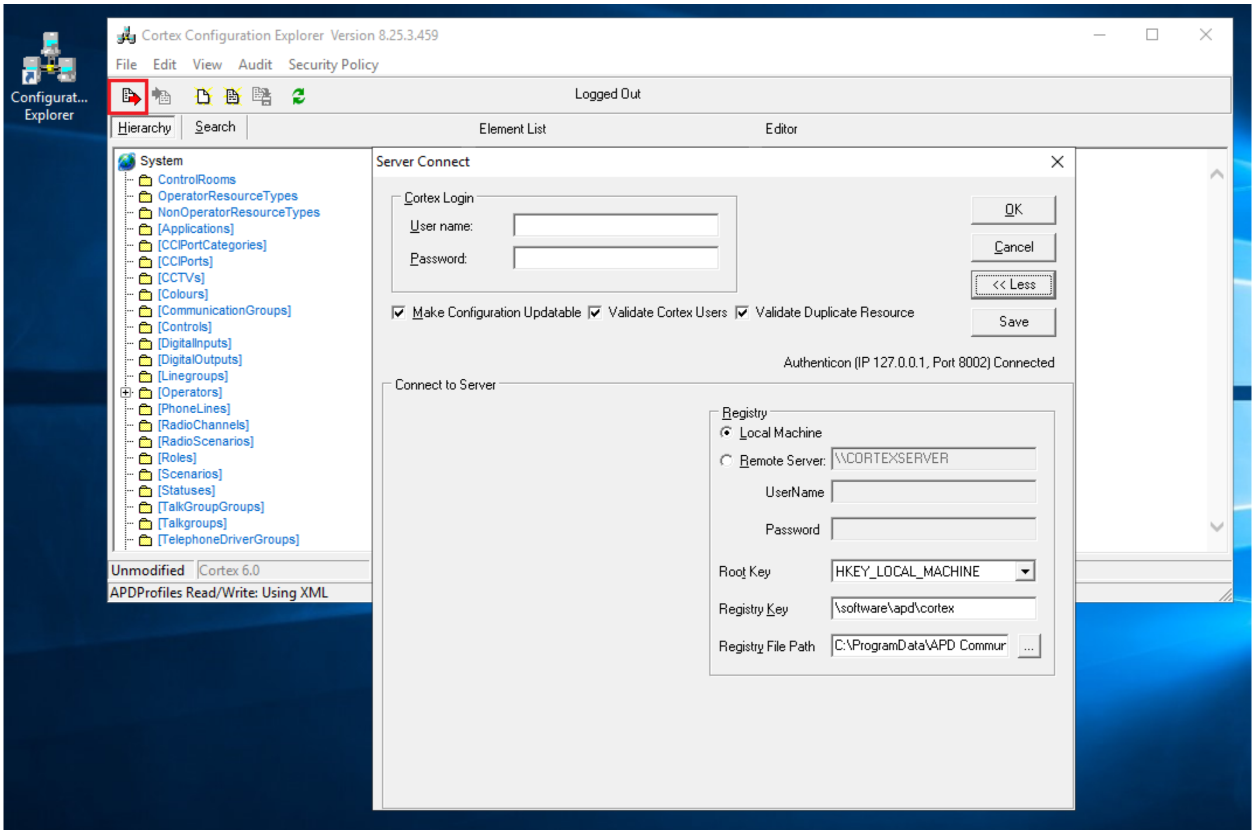


Clicking on **agent2** (from the previous page), shows the information below. As per the Contact Center user in **Section 6.4**, agent ID **3101** is associated with CCT user **agent2**.



7. Configure NEC Cortex

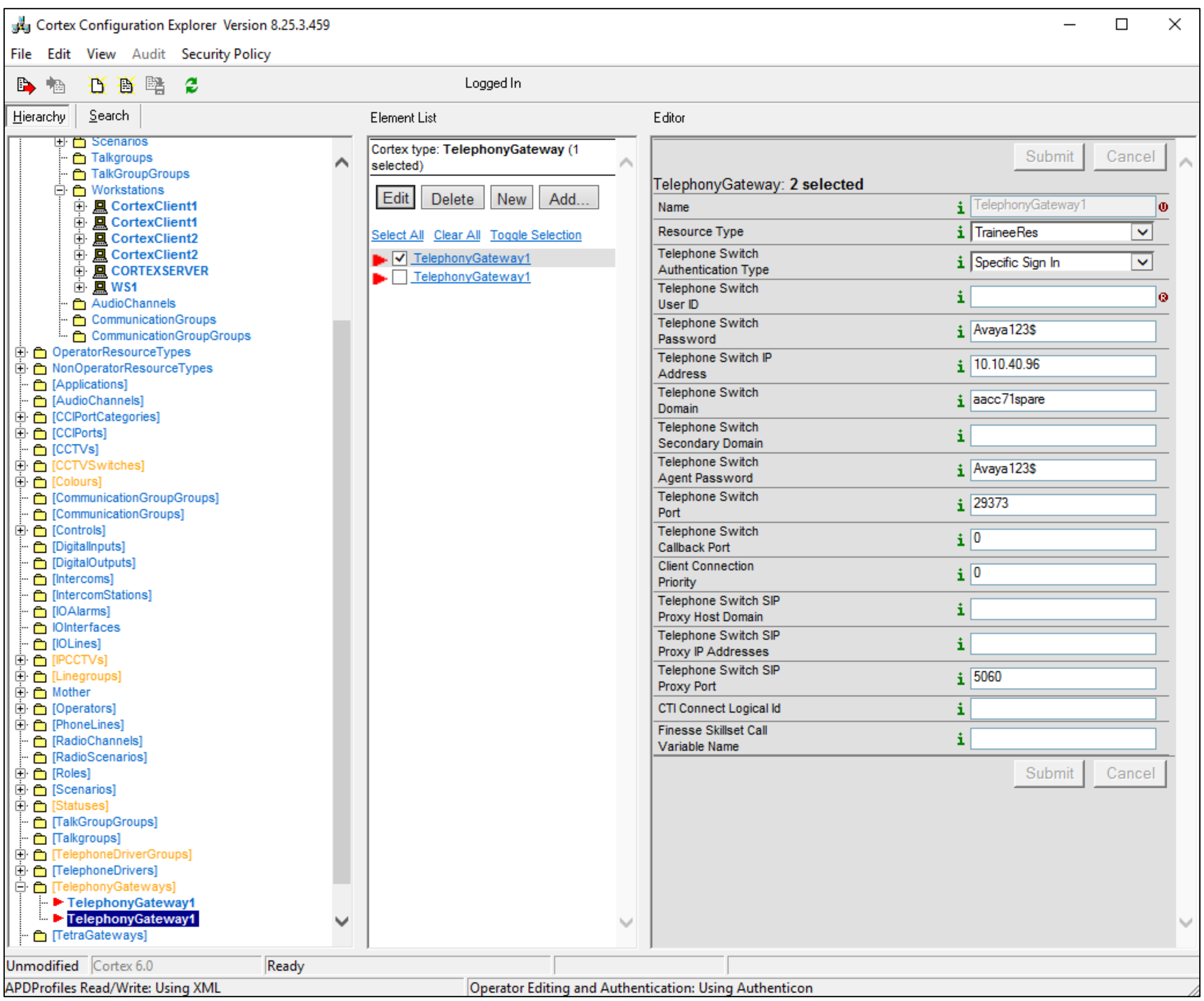
To configure the Cortex connection to CCT, open **Cortex Configuration Explorer** located on the Cortex server. Once opened, click on the icon highlighted which opens the **Server Connect** login screen shown. Enter the appropriate credentials and click on **OK**. The **Registry** information is automatically filled in and was expanded to show the connection details for compliance testing.



7.1. Configure CCT connection

Configure the connection to CCT by navigating to Telephony Gateways in the left window. The gateway that was created during the initial configuration is shown below. Note the following:

- **Telephone Switch User ID** – This was left blank as it was not used for compliance testing.
- **Telephone Switch Password** – This corresponds to the CCT password.
- **Telephone Switch IP** – This is the IP address of the CCT server which in this case is the IP address of the whole Avaya Aura® Contact Center
- **Telephone Switch Domain** – Because the Contact Center is not on a domain, the domain is the hostname of the Contact Center, but typically this is on a domain and so the name of the domain in question would be used.
- **Telephone Switch Agent Password** – this is the password that is used by the agents, for compliance testing all passwords were the same and so the password could be entered here.
- **Telephone Switch Port** – this is the same port as per **Section 6.1**.

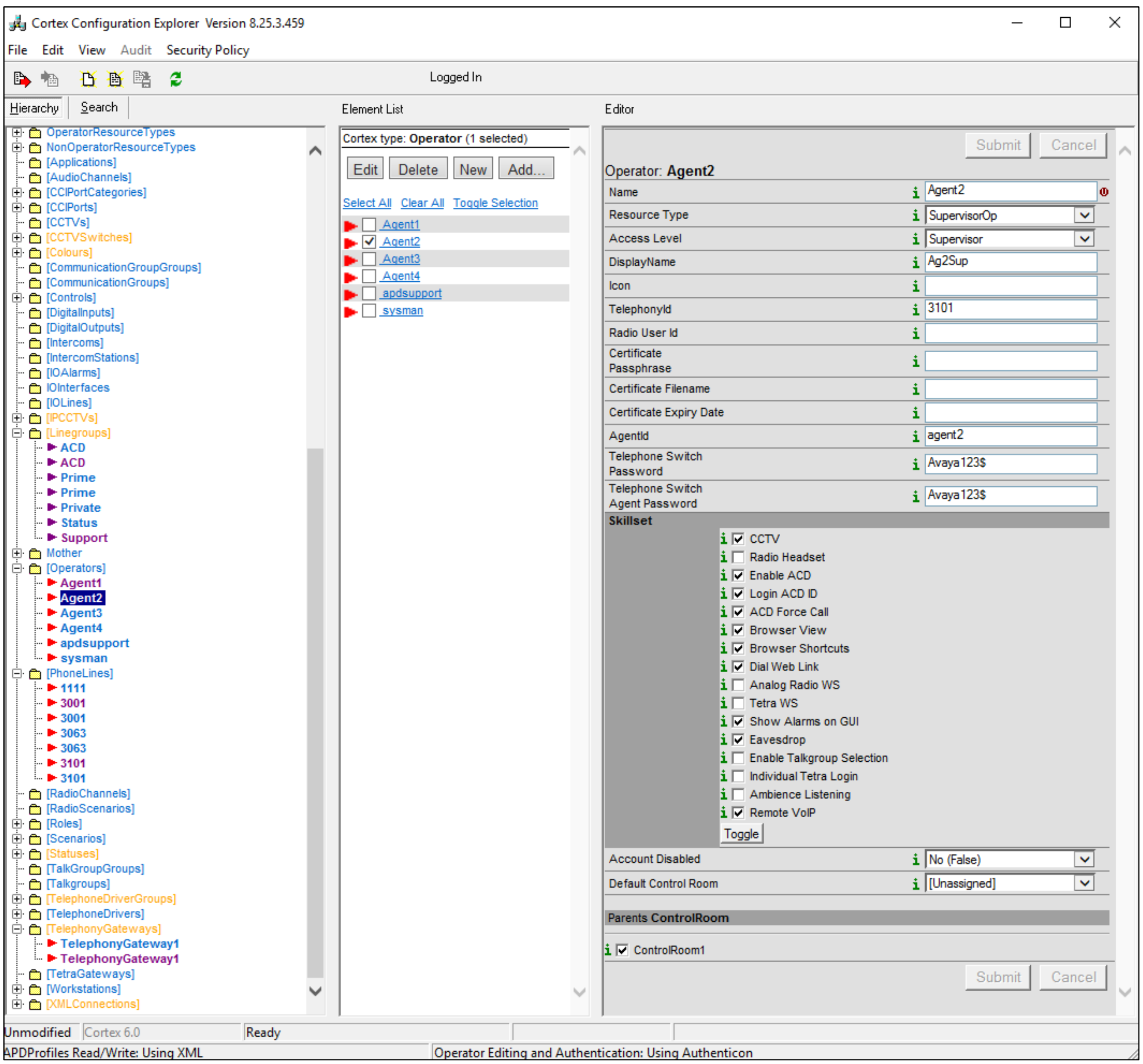


7.2. Configure Agent

Navigate to **Operators** in the left window. The list of operators or agents that are configured are shown here. A new operator can be added by selecting **Add** from the middle window. The example below shows **Agent2** that was added which is associated with telephone **3101** and agent **3101**. Please note the following:

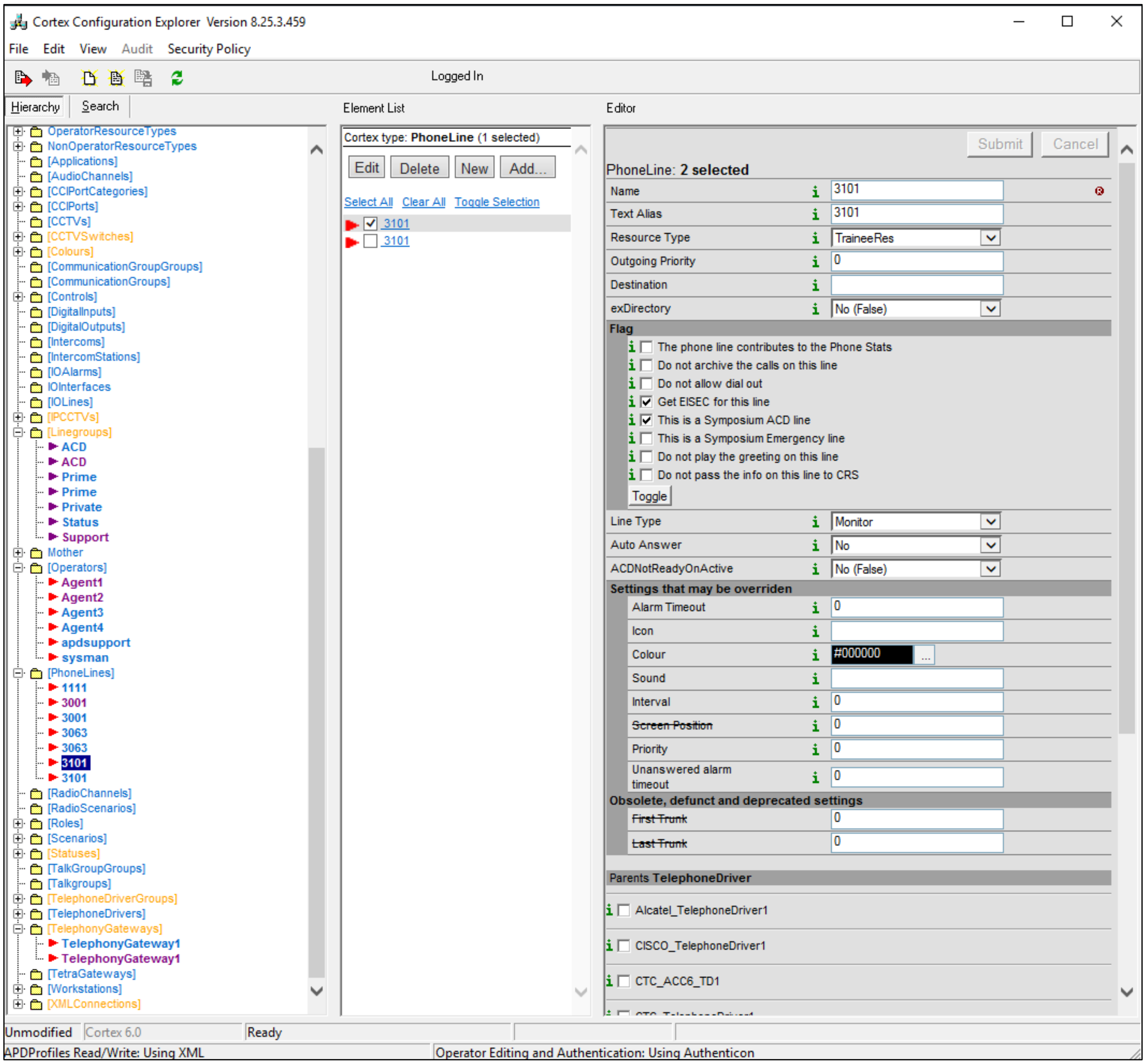
- **Name** below must correspond with the CCT username in **Section 6.5**.
- **TelephonyId** must match the SIP URI or telephone extension from **Section 6.4**.
- **AgentId** must match that of the Agent Login ID which in most cases is the same as the CCT user login ID.
- **Telephone Switch Password** is the CCT user password.
- **Telephone Switch Agent Password** is the Contact Center Agent password.

The other settings and tick boxes were all set as shown below.

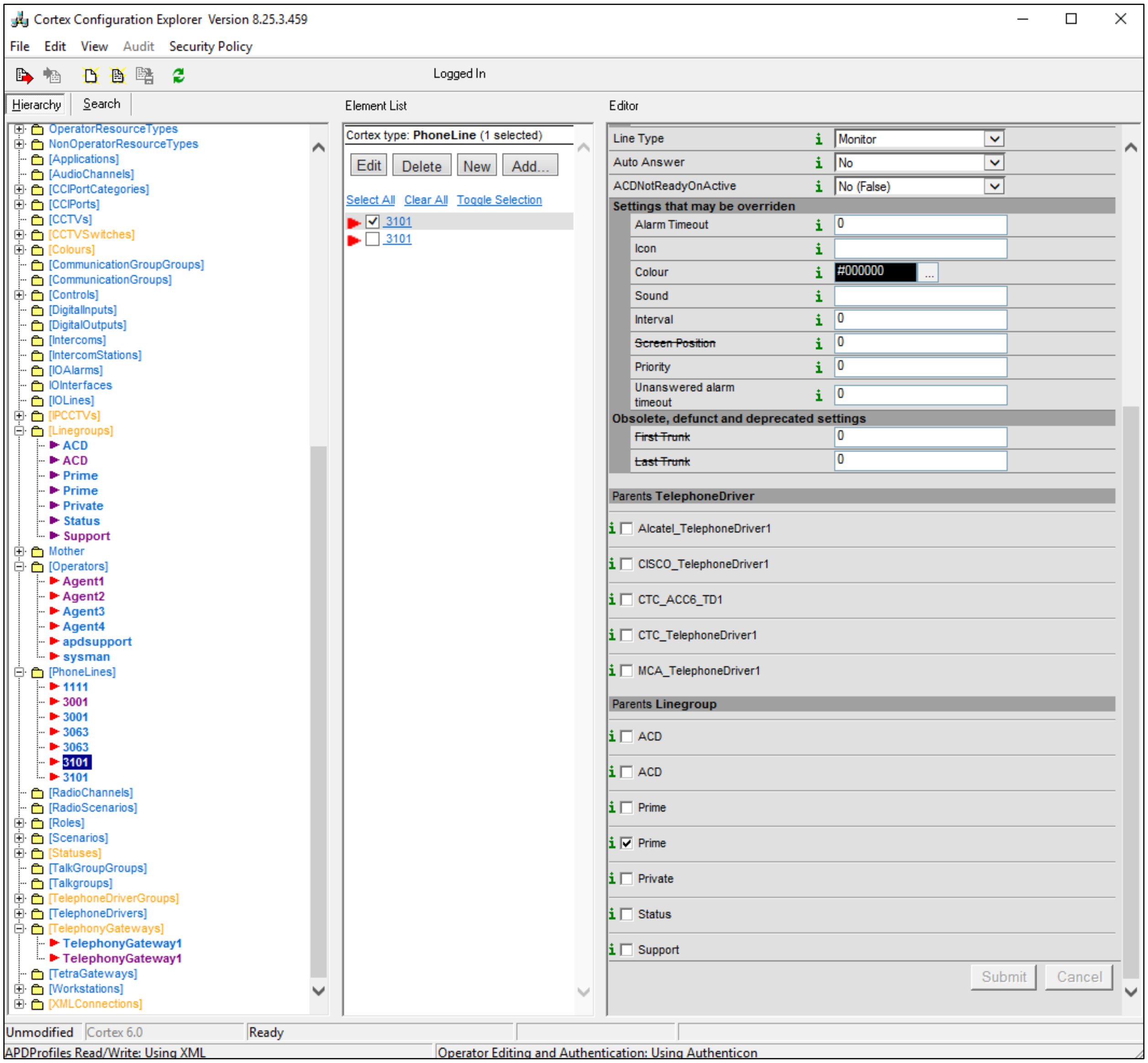


7.3. Configure Phone Lines

From the left window, navigate to **PhoneLines**. The list of configured phone lines is shown, and a new phone line can be added by selecting **Add** from the middle window. The phone line **3101** is displayed below, this corresponds to the phoneset 3101. Note that phonesets **3001**, **3063** and **3101** were all used for compliance testing, as outlined in **Section 2**. Note that **This is a Symposium ACD line** was ticked.



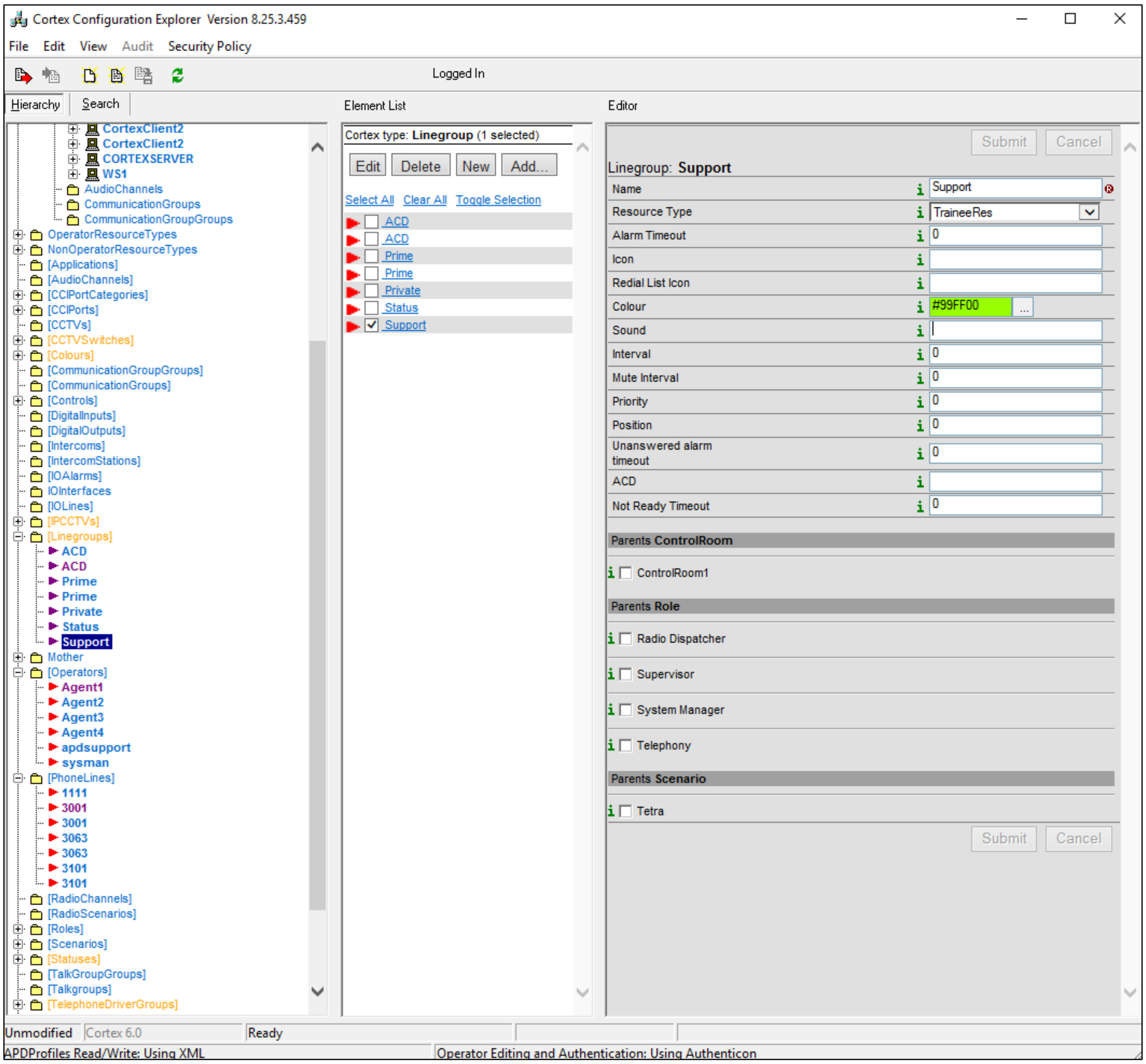
Scrolling down in the right window, the following were set for compliance testing. Note that **Prime** should be ticked, as shown below.



7.4. Configure Line Groups

The reason to create a line group would be to distinguish calls going to a certain skillset, this may be to highlight a "gold member" to the agent, or perhaps an emergency call. For compliance testing the skillset **Support** was chosen to be presented with a green border as shown below. Note that the Name of the line group must match exactly that of the Skillset name in **Section 6.3**.

From the left window, navigate to **Linegroups**. A list of configured line groups is shown, and a new line group can be added by selecting **Add** from the middle window. Below shows the configuration of the line group Support that was used for compliance testing.

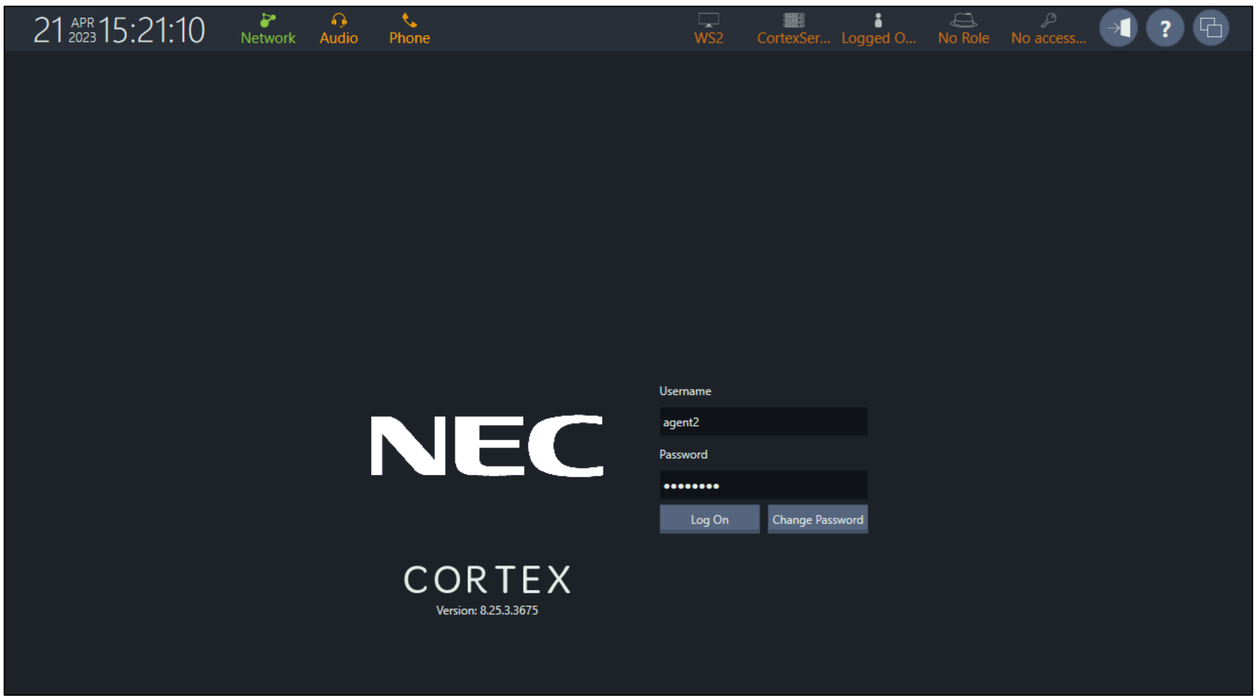


8. Verification Steps

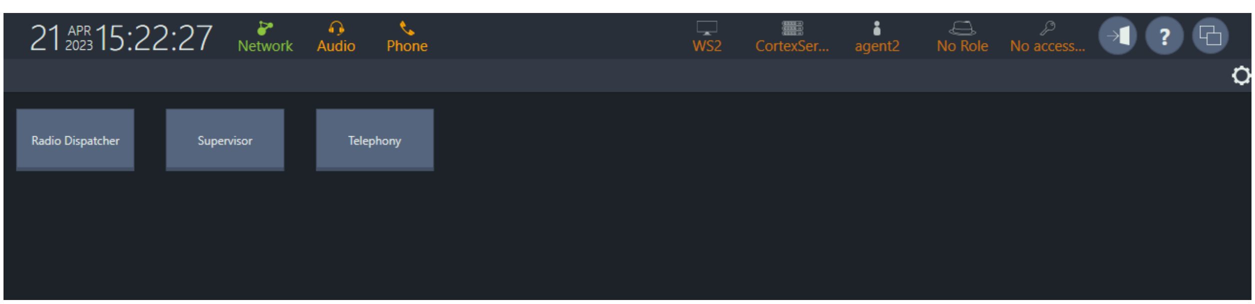
This section provides steps that may be performed to verify that the solution is configured correctly.

8.1. Verify NEC Cortex

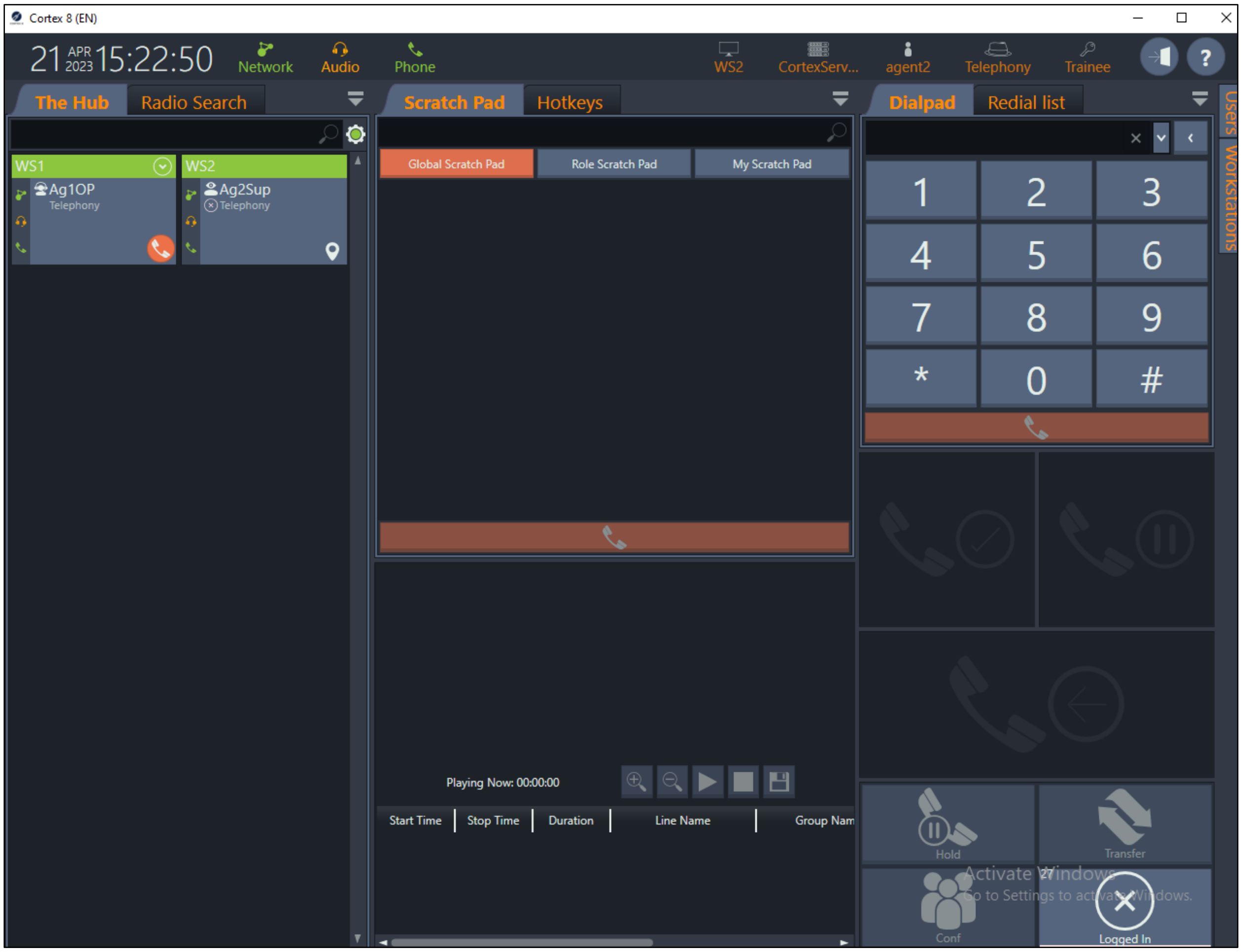
Once an agent can be logged in and a call answered using Cortex, this ultimately shows that the two products are connected and configured correctly. From an agent workstation that has Cortex installed, open the Cortex application (not shown) and the log into the resulting screen as shown below. Note that **agent2** is being logged in below to demonstrate the successful setup of the solution.



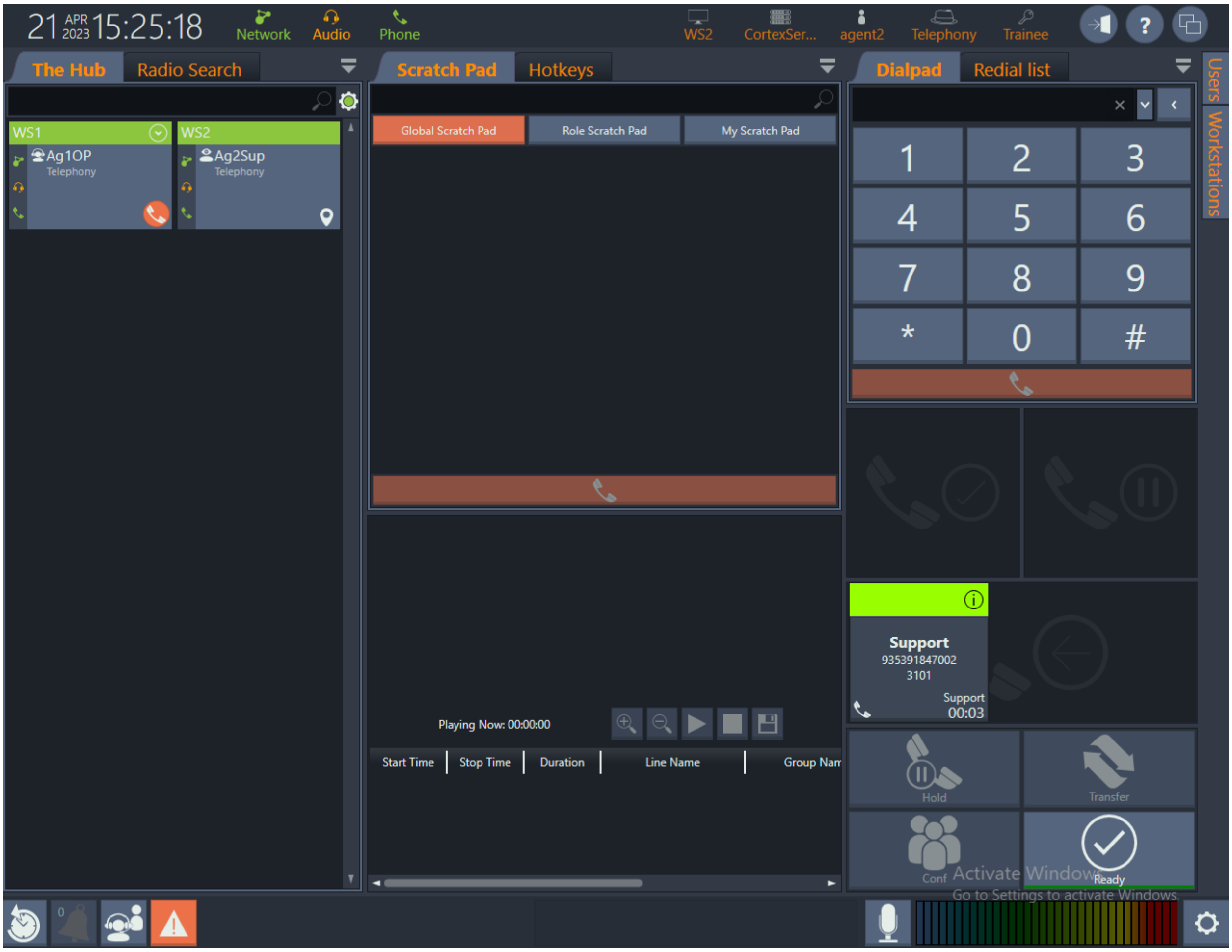
Once logged in above, the screen below is shown. For compliance testing, **Telephony** was chosen, and was clicked on.



Upon opening the Cortex GUI, the following screen is shown. Click on the icon at the bottom right of the screen to log in.

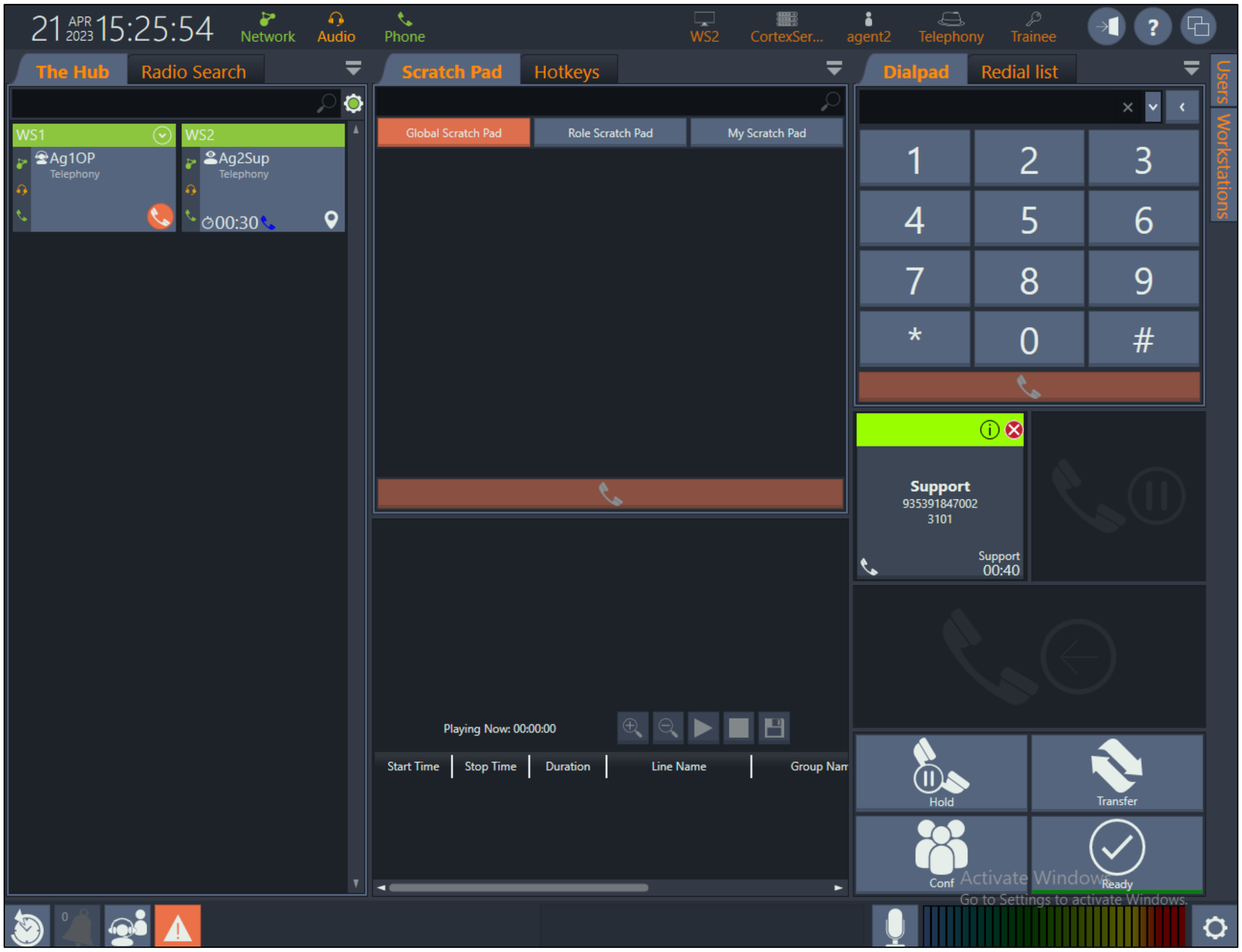


Once logged in, the agent is **Ready** to take a call. The **Support** skillset was called, and as per **Section 7.4**, the call is presented to the agent with a green border. To answer the call, the green icon is simply clicked on and that will transfer the icon into the window above where it is currently located, the call is then answered, and the agent is talking to the customer.



The call is now active, and the buttons located at the bottom right of the screen now become active allowing the agent to place the call on hold, transfer the call, or make a conference.

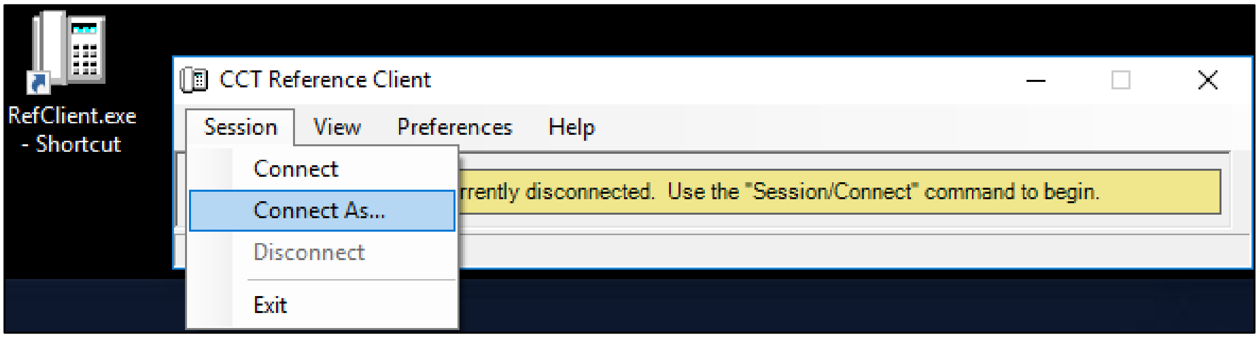
Information on that caller is presented to the agent from the database. In the example below, **35391847002** is calling into **Support**.



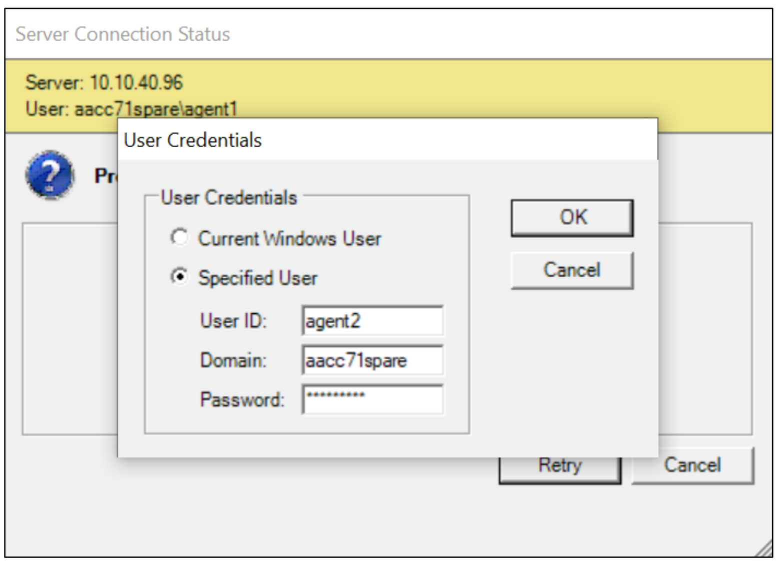
8.2. Verify CTI using Reference Client

In the event that there is some issue with the Cortex GUI, Ref Client is a very useful tool to ensure that the connection to CCT is running correctly and that the Contact Center is operating correctly.

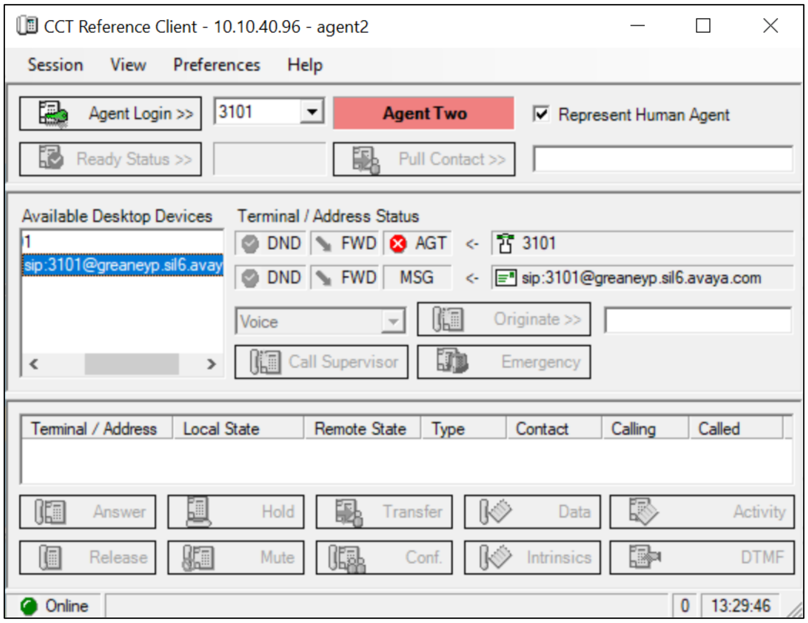
Open **CCT Reference Client** from any PC. From **Session** select **Connect As**.



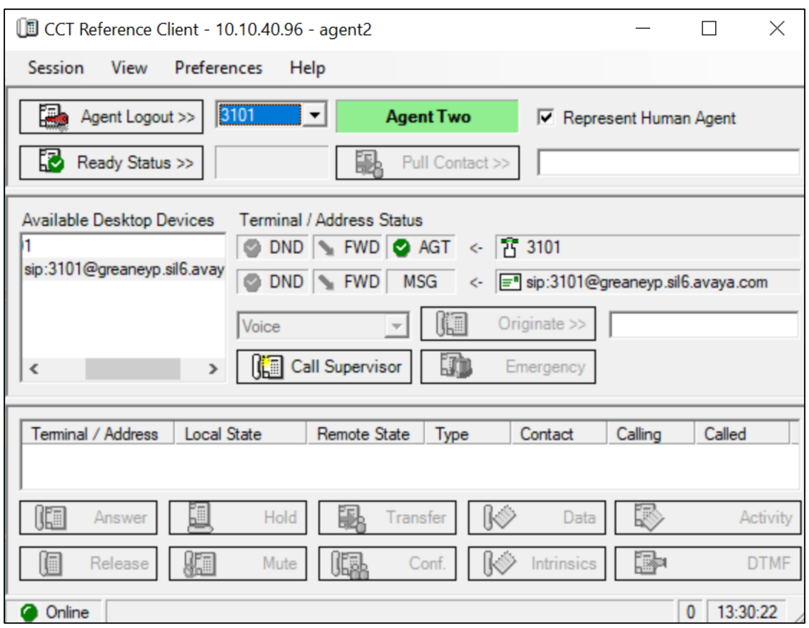
The example below shows the user **agent2** being logged in.



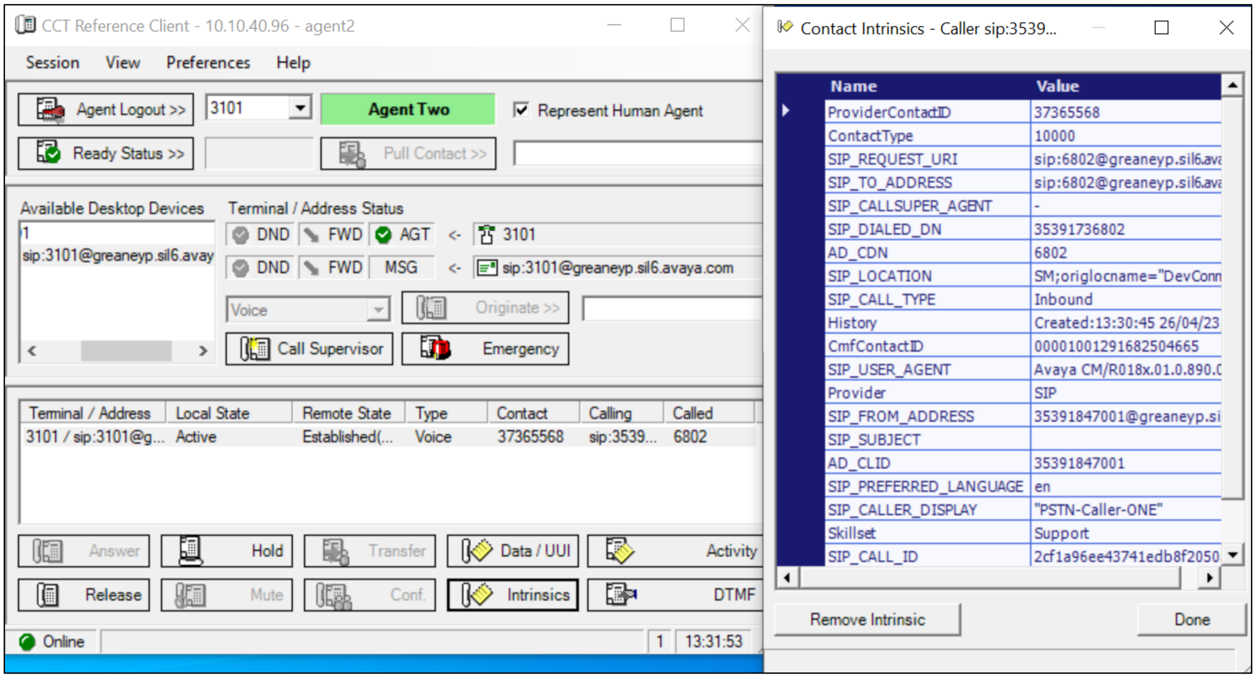
The user is now in control of phoneset **3101**. Note the icons are all green in color except for the AGT icon as the agent is not yet logged in. Click on **Agent Login**.



The agent will be logged in more than likely in the not ready state, but this will depend on what is setup on Contact Center. If the agent is not ready, then press **Ready Status** to ensure the agent is made ready to receive an incoming skillset call.

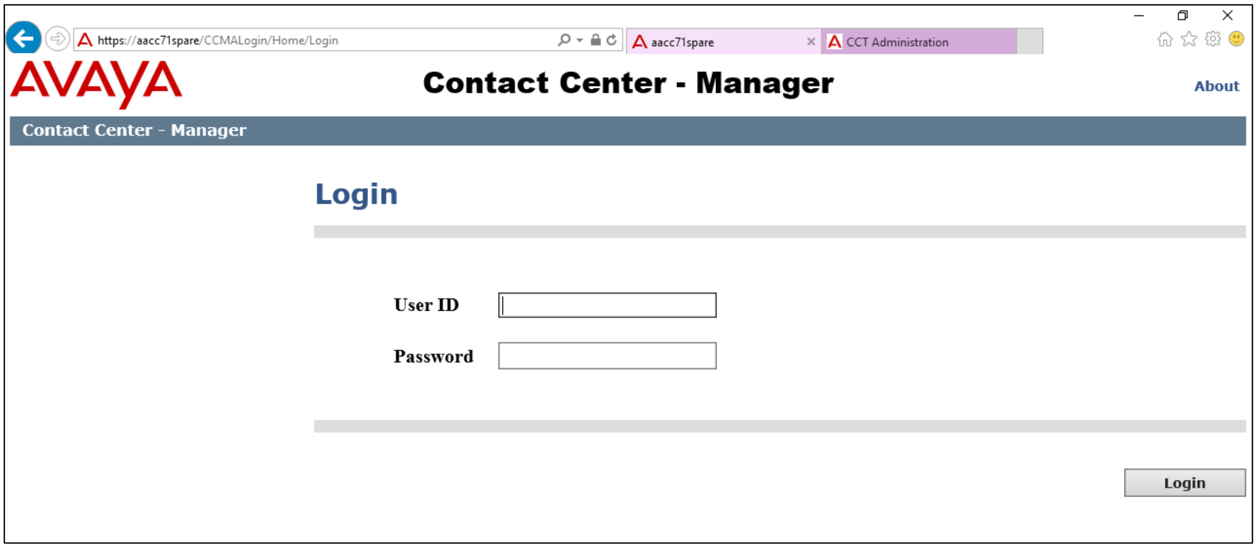


A call is made to the route point **6802** and should be presented to the agent as shown below. Once the call is answered the **Intrinsics** button can be pressed showing the call data.



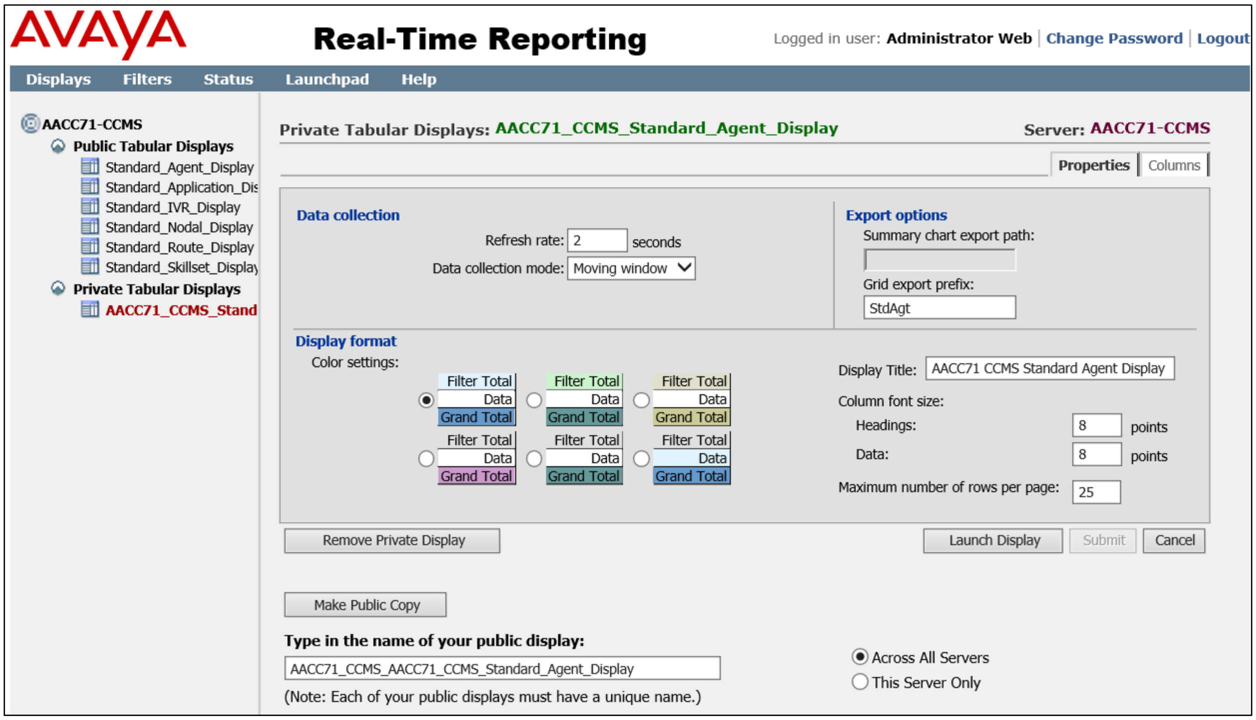
8.3. Verify Agent is logged in on Avaya Aura® Contact Center

Log into Contact Center as shown below.

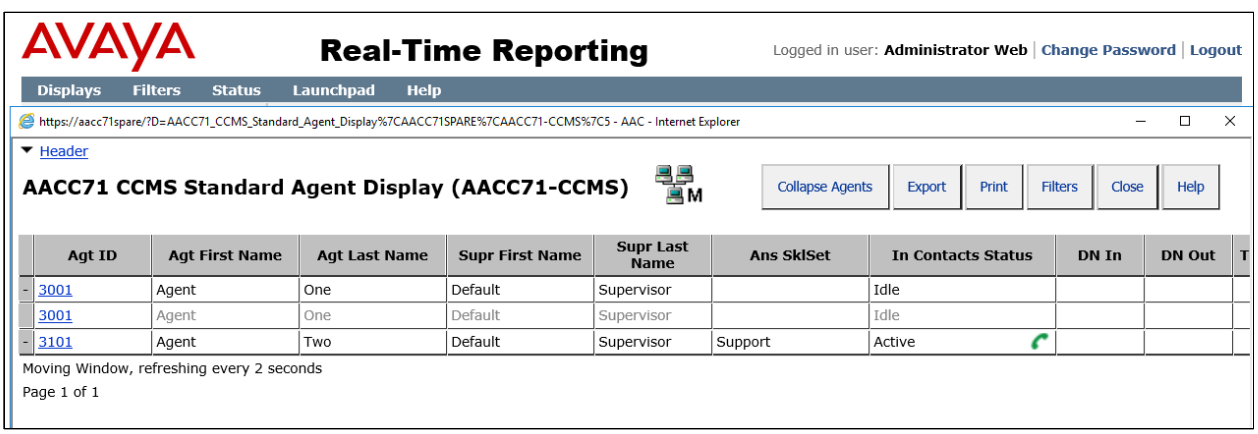


From the **Launchpad**, click on **Real-Time Reporting**.

Open an agent display. The display below was created as a **Private Tabular Display**, but the **Standard_Agent_Display** can also be chosen, that will give the necessary information on the agents that are logged in and, on a call, etc.

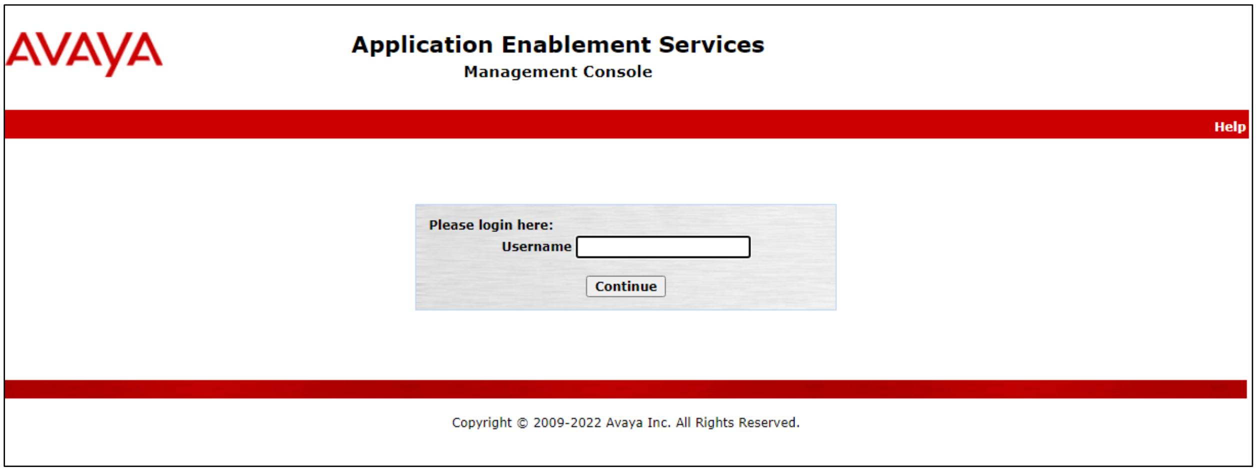


The display below shows that agent **3001** is currently logged in and **Idle** while agent **3101** is also logged in and, on a call, or **Active**. This corresponds to agent2 which is associated with agent ID 3101, being on a call as per **Section 8.1**.

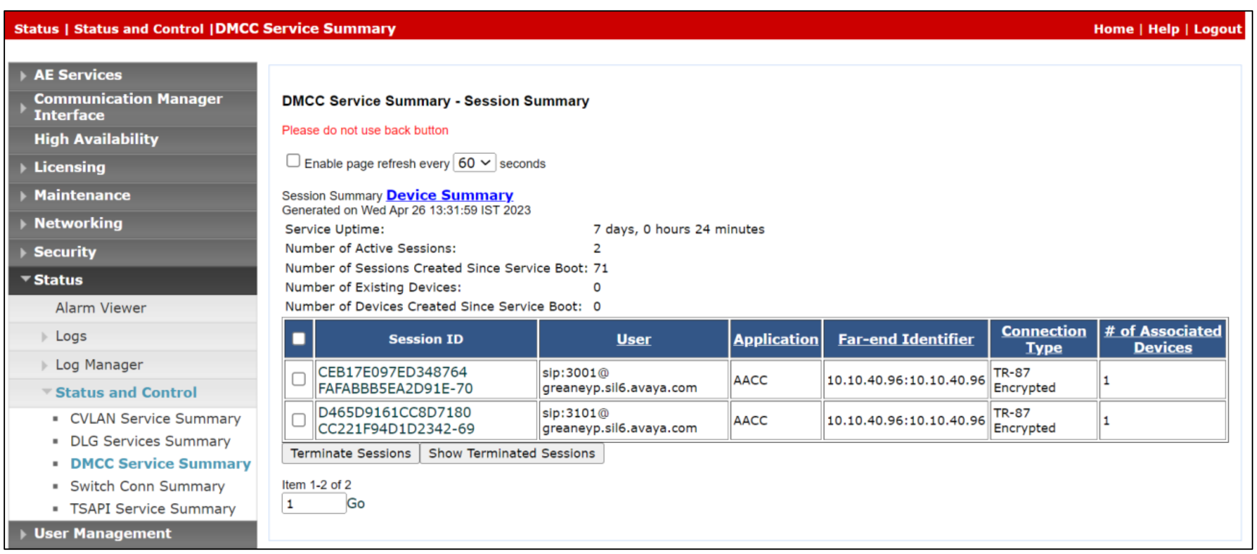


8.4. Verify connection between Avaya Aura® Contact Center and Avaya Aura® Application Enablement Services

If there is an issue with any of the connections that were being verified in this section, there may be some issue between the Contact Center and Communication Manager which is facilitated by Application Enablement Services. The TR87 connection can be checked on Application Enablement Services to see if this connection between Communication Manager and Contact Center is taking place. Log into Application Enablement Services, as shown below.



Navigate to **Status → Status and Control → DMCC Service Summary**, in the left window. A connection such as is shown below should be displayed in the main window. Note that two agents are currently logged in, that being **3001** and **3101**.



9. Conclusion

These Application Notes describe the configuration steps required for NEC Cortex v8 to successfully interoperate with Avaya Aura® Contact Center R7.1.2.1 and Avaya Aura® Communication Manager R10.1. Most test cases were completed successfully with all issues and observations listed in **Section 2.2**.

10. Additional References

This section references the Avaya and NEC product documentation 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 10.1

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 10.1

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 10.1

[4] *Administering Avaya Aura® Session Manager*, Release 10.1

[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

Support for Cortex can be obtained from NEC as follows:

- Email: pssd@necsws.com
- Website: https://www.necsws.com/iccs/
- Phone: + 44 1482 808 300

Appendix A

11. Call Routing to Contact Center

Each Communication Manager system will have its own setup with different System Parameters and Features configured depending on the requirement of the customer. Here is a snapshot of some of these values that were configured on the DevConnect lab for compliance testing. The configuration operations described in this section can be summarized as follows:

- Verify System Parameters and Features
- Configure SIP Trunk
- Configure Call Routing for Contact Center

Note: The configuration of PSTN trunks and routes are outside the scope of these Application Notes.

11.1. Verify System Parameters and Features

The license file installed on the system controls these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative. Use the **display system-parameters customer-options** command to determine these values. On **Page 2**, verify that **Maximum Administered SIP Trunks** has sufficient capacity. Each call answered by Contact Center uses a minimum of one SIP trunk. Calls that are routed back to stations on Communication Manager or calls that are routed back to Communication Manager to access the PSTN will use two SIP trunks.

```
display system-parameters customer-options                     Page   2 of  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 250
           Maximum Concurrently Registered IP Stations: 18000 2
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 18000 0
                       Maximum Administered SIP Trunks: 24000 319
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
```

On **Page 4**, ensure that both **ARS** and **ARS/AAR Partitioning** are set to **y**.

```
display system-parameters customer-options                        Page   4 of  12
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                       CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                         CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                      DCS (Basic)? y
```

On **Page 5**, ensure that **Uniform Dialing Plan** is set to **y**.

```
display system-parameters customer-options                       Page   6 of  12
                                OPTIONAL FEATURES

               Multinational Locations? n            Station and Trunk MSP? y
Multiple Level Precedence & Preemption? n     Station as Virtual Extension? y
                                           System Management Data Transfer? n
         Personal Station Access (PSA)? y              Tenant Partitioning? y
                       PNC Duplication? n      Terminal Trans. Init. (TTI)? y
                  Port Network Support? y              Time of Day Routing? y
                       Posted Messages? y      TN2501 VAL Maximum Capacity? y
                                                      Uniform Dialing Plan? y
                    Private Networking? y    Usage Allocation Enhancements? y
```

For compliance testing, **Trunk-to Trunk Transfer** was set to **all** on **Page 1** of the **system-parameters features** page. This is a system wide setting that allows calls to be routed from one trunk to another and is usually turned off to help prevent toll fraud. An alternative to enabling this feature on a system wide basis is to control it using COR (Class of Restriction).

```
display system-parameters features                                Page   1 of  19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y

              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n

             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

11.2. Configure SIP Trunk

In the **Node Names IP** form, note the IP Address of the processor interface of Communication Manager (**procr)** and the Session Manager (**sm101x**). The host names will be used throughout the other configuration screens of Communication Manager and Session Manager. Type **display node-names ip** to show all the necessary node names.

```
display node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
sm101x              10.10.40.12
aespri101x          10.10.40.16
aessec101x          10.10.40.46
g450                10.10.40.15
procr               10.10.40.13
```

In the **IP Codec Set** form, select the audio codecs supported for calls routed over the SIP trunk to Contact Center. The form is accessed via the **change ip-codec-set n** command. Multiple codecs may be specified in the **IP Codec Set** form in order of preference. Note the **Media Encryption** includes a setting of **none** to allow for unencrypted media. The media between Avaya endpoints are set to use Media Encryption as a preferred option.

```
change ip-codec-set 1                                        Page   1 of   2
                          IP MEDIA PARAMETERS
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: OPUS-SWB24K                 1        20
 2: G.722-64K         n         1        20
 3: G.722.2                     2        20
 4: G.711A            n         2        20
 5: G.711MU           n         2        20
 6: G.729             n         2        20
 7:
     Media Encryption                     Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: none
 3:
 4:
```

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**.
- Set the **Transport Method** to the appropriate setting, in this case it was set to **tls**.
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager.
- Specify the node names for the procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above.
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **sm101x**).
- Ensure that the recommended TLS port value of **5062** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- In the **Far-end Network Region** field, enter the IP Network Region configured above**.** This field logically establishes the **far-end** for calls using this signaling group as network region 1.
- **Far-end Domain** was set to the domain used during compliance testing.
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833.
- The **Direct IP-IP Audio Connections** field is set to **y**.
- **Initial IP-IP Direct Media** is set to **n**.
- The default values for the other fields may be used.

```
change signaling-group 1                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: sm101x
 Near-end Listen Port: 5062                 Far-end Listen Port: 5062
                                         Far-end Network Region: 1

Far-end Domain: greaneyp.sil6.avaya.com
                                              Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                   RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload             Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                      IP Audio Hairpinning? n
         Enable Layer 3 Test? Y                     Initial IP-IP Direct Media? n
                                                    Alternate Route Timer(sec): 6
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to and from Contact Center. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
change trunk-group 1                                            Page   1 of  4
                                TRUNK GROUP

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: SIP TRK                     COR: 1        TN: 1     TAC: *801
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 10
```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with the DevConnect member to prevent unnecessary SIP messages during call setup. Session refresh is used throughout the duration of the call, to check the other side has not gone away, for the compliance test a value of **600** was used.

```
change trunk-group 1                                            Page   2 of  4
      Group Type: sip

TRUNK PARAMETERS

     Unicode Name: auto

                                            Redirect On OPTIM Failure: 5000

            SCCAN? n                               Digital Loss Group: 18
                      Preferred Minimum Session Refresh Interval(sec): 600

 Disconnect Supervision - In? y  Out? y


           XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? n
```

Settings on **Page 3** can be left as default. However, the **Numbering Format** in the example below is set to **private**.

```
change trunk-group 1                                            Page   3 of  4
                                TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                             UUI Treatment: service-provider

                                               Replace Restricted Numbers? n
                                              Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

Settings on **Page 4** are as follows; ensure that the **Telephone Event Payload Type** is set to **101**. Ensure that **Support Request History** is set to **y**.

```
change trunk-group 1                                           Page   4 4
                              PROTOCOL VARIATIONS

                                       Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
                       Send Transferring Party Information? y
                                  Network Call Redirection? y
          Build Refer-To URI of REFER From Contact For NCR? n
                                     Send Diversion Header? n
                                   Support Request History? y
                              Telephone Event Payload Type: 101


                      Convert 180 to 183 for Early Media? n
                Always Use re-INVITE for Display Updates? n
                      Identity for Calling Party Display: P-Asserted-Identity
          Block Sending Calling Party Location in INVITE? n
               Accept Redirect to Blank User Destination? n
                                            Enable Q-SIP? n

        Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
                              Request URI Contents: may-have-extra-digits
```

11.3. Configure Call Routing to Contact Center

For compliance testing, all calls beginning with 68xx with a total length of 4 digits were to be sent across the SIP trunk to Session Manager and on to Contact Center. To achieve this, automatic alternate routing (aar) would be used to route the calls.

11.3.1. Administer Dial Plan

It was decided for compliance testing that all calls beginning with 68 with a total length of 4 digits were to be sent across the SIP trunk to Session Manager. Type **change dialplan analysis**, to make changes to the dial plan. Ensure that **68** is added with a **Total Length** of **4** and a **Call Type** of **udp**.

```
change dialplan analysis                                     Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 2

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   1           4   udp
   2           4   udp
   3           4   ext
   4           4   ext
   5           4   udp
   6           4   ext
   68          4   udp
   8           1   fac
   9           1   fac
   *8          4   dac
   *           3   fac
   #           3   fac
```

11.3.2. Administer Route Selection for calls to Contact Center

As digits **68**xx were defined in the dial plan as udp (**Section 11.3.1**), use the **change uniform-dialplan** command to configure the routing of the dialed digits. In the example below calls to numbers beginning with **68xx** that are **4** digits in length will be matched. No further digits are deleted or inserted. Calls are sent to **aar** for further processing.

```
change uniform-dialplan 6                                    Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 0

  Matching                    Insert              Node
  Pattern        Len Del      Digits      Net Conv Num
  68              4   0                   aar  n
                                               n
```

Use the **change aar analysis** x command to further configure the routing of the dialed digits. Calls to Contact Center begin with **68** and are matched with the AAR entry shown below. Calls are sent to **Route Pattern 1**, which contains the outbound SIP Trunk Group.

```
change aar analysis 6                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all            Percent Full: 1

    Dialed                  Total      Route     Call    Node  ANI
    String                 Min  Max   Pattern    Type    Num   Reqd
    68                     4    4      1         lev0          n
```

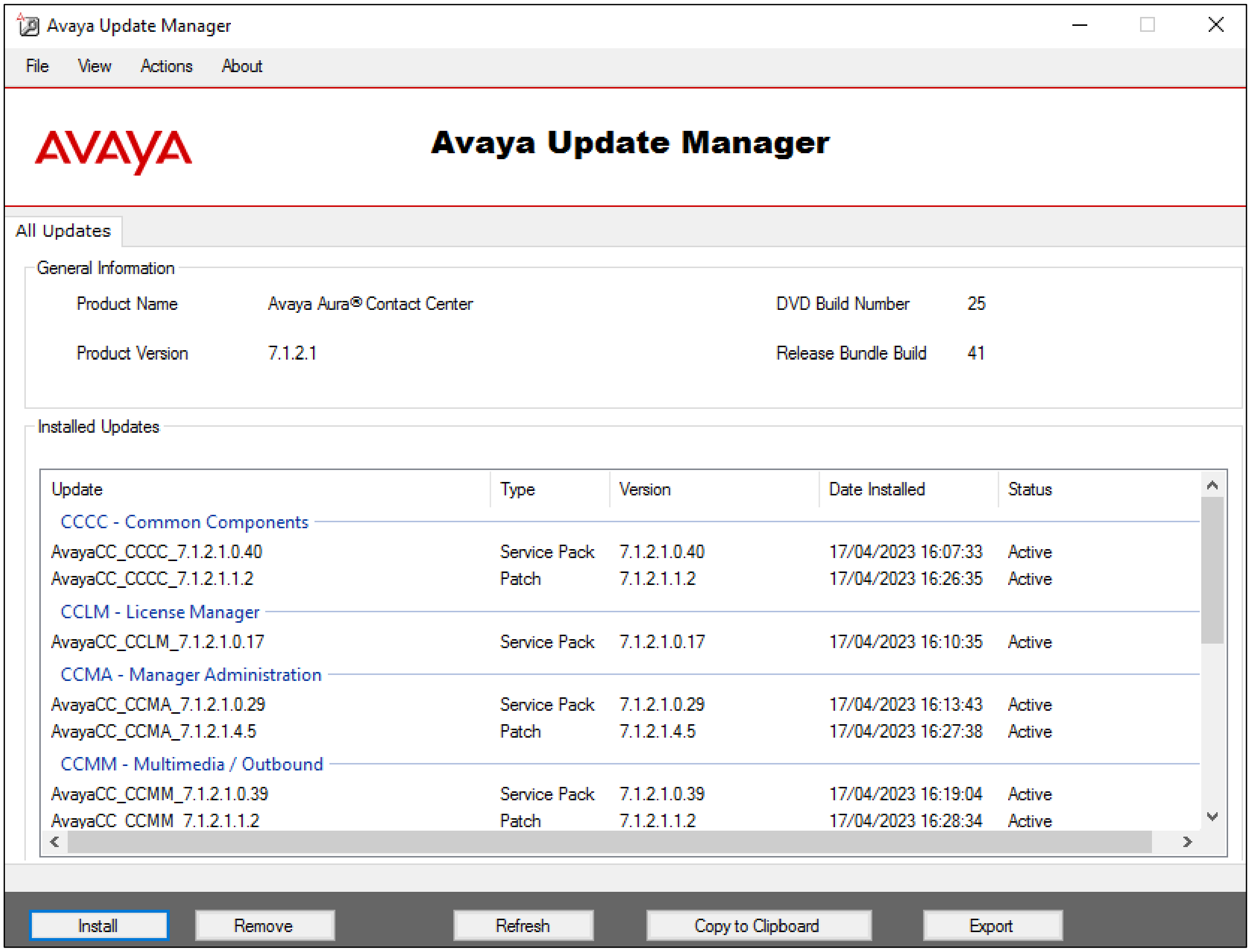
Use the **change route-pattern *n*** command to add the SIP trunk group to the route pattern that AAR selects. In this configuration, **Route Pattern Number 1** is used to route calls to trunk group (**Grp No**) **1**. This is the SIP Trunk configured in **Section 11.2**.

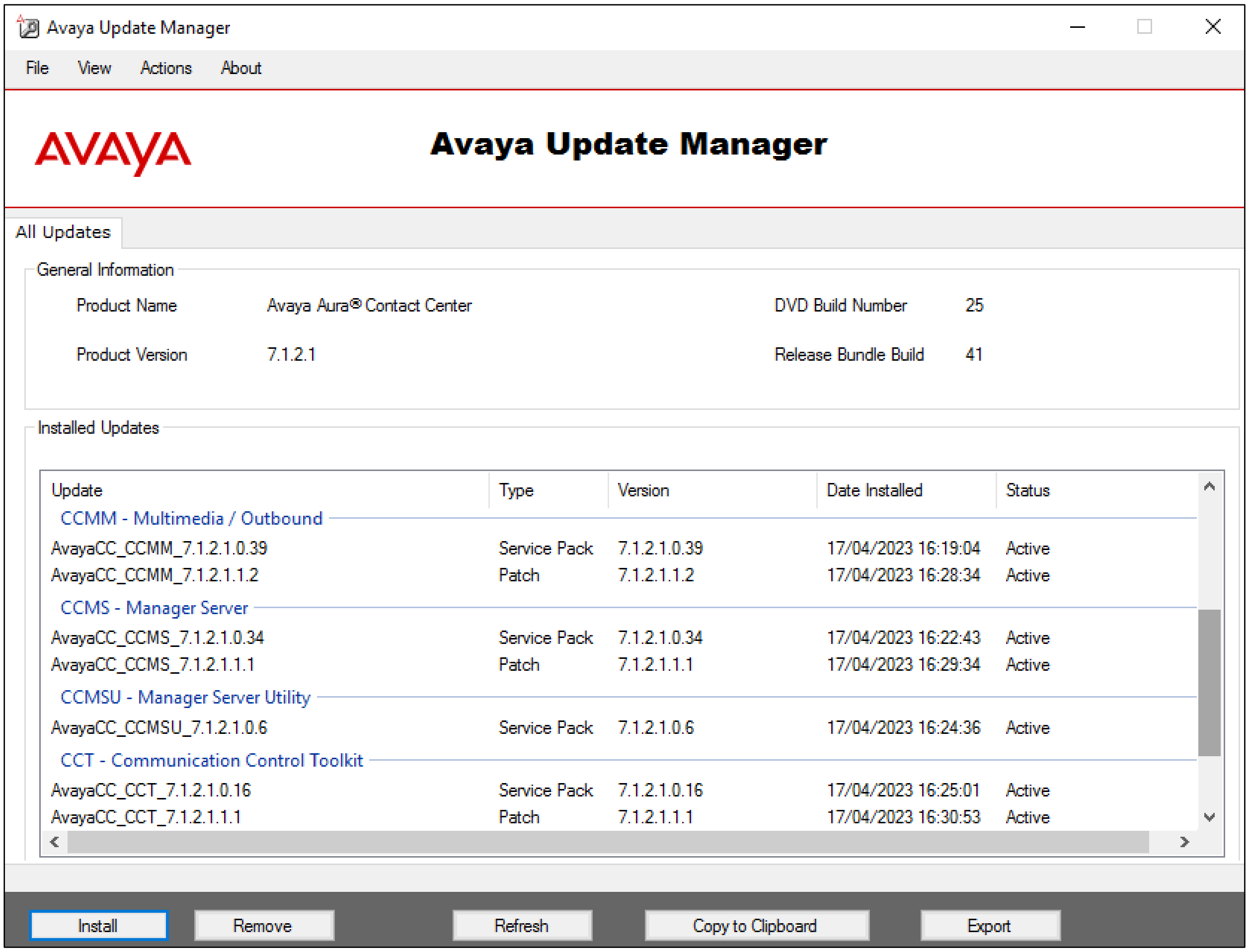
```
change route-pattern 1                                      Page   1 of   4
               Pattern Number: 1   Pattern Name: SIPTRK
           SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 1    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM   No.  Numbering  LAR
    0 1 2 M 4 W     Request                                  Dgts  Format
 1: y y y y y n  n            unre                                 lev0-pvt  none
 2: y y y y y n  n            rest                                           none
 3: y y y y y n  n            rest                                           none
 4: y y y y y n  n            rest                                           none
 5: y y y y y n  n            rest                                           none
 6: y y y y y n  n            rest                                           none
```

Appendix B

12. Contact Center Patches

The following two screen shots show the version of Contact Center that was tested with for compliance testing.




Avaya Update Manager
File View Actions About
AVAYA
Avaya Update Manager
All Updates
General Information
Product Name Avaya Aura® Contact Center
DVD Build Number 25
Product Version 7.1.2.1
Release Bundle Build 41
Installed Updates
Update Type Version Date Installed Status
CCMM - Multimedia / Outbound
AvayaCC_CCMM_7.1.2.1.0.39 Service Pack 7.1.2.1.0.39 17/04/2023 16:19:04 Active
AvayaCC_CCMM_7.1.2.1.1.2 Patch 7.1.2.1.1.2 17/04/2023 16:28:34 Active
CCMS - Manager Server
AvayaCC_CCMS_7.1.2.1.0.34 Service Pack 7.1.2.1.0.34 17/04/2023 16:22:43 Active
AvayaCC_CCMS_7.1.2.1.1.1 Patch 7.1.2.1.1.1 17/04/2023 16:29:34 Active
CCMSU - Manager Server Utility
AvayaCC_CCMSU_7.1.2.1.0.6 Service Pack 7.1.2.1.0.6 17/04/2023 16:24:36 Active
CCT - Communication Control Toolkit
AvayaCC_CCT_7.1.2.1.0.16 Service Pack 7.1.2.1.0.16 17/04/2023 16:25:01 Active
AvayaCC_CCT_7.1.2.1.1.1 Patch 7.1.2.1.1.1 17/04/2023 16:30:53 Active
Install
Remove
Refresh
Copy to Clipboard
Export

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.