



Avaya Solution & Interoperability Test Lab

Application notes for RMG Networks Intelligent Visual Solutions v12.0.2 with Avaya Aura® Contact Center's Contact Center Manager Server module Release 6.4 for Real Time Display – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for RMG Networks Intelligent Visual Solutions v12.0.2 to interoperate with Avaya Aura® Contact Center's Contact Center Manager Server (CCMS) 6.4, using Real Time Display (RTD). Intelligent Visual Solutions collects Real Time statistics from Contact Center Manager Server 6.4 and publishes this data to clients.

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

1. 1. Introduction

The purpose of this document is to explain the configuration steps required for Intelligent Visual Solutions (IVS) v12.0.2 to interoperate with Avaya Aura® Contact Center's Contact Center Manger Server (CCMS) 6.4. IVS interfaces with the CCMS and its internal database, collects and sorts the data, and prepares it for display on a variety of media using Real Time Data (RTD) display toolkit.

2. General Test Approach and Test Results

The General test approach was to verify that the IVS was able to integrate with Avaya Aura® Contact Center. IVS uses the Avaya Aura Collector (AAC) to connect to the Avaya Aura® Contact Center (Contact Center) RTD API to monitor a wide range of real time statistics that are available from Contact Center. The AAC is part of Portal Administrator, which is an application that is part of IVS and runs on the same server.

Once AAC is logged into Contact Center, all keys are extracted from the database including Application, Skillset, Agent, and IVR Queue statistics. All statistics can be viewed using a Portal Data Viewer, which is a debugging tool that is part of IVS.

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

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying IVS for the following:

- Connection to the CCMS is established and stays connected.
- Publishing all the available real-time data information based on the CCMS script.
- Making test calls to invoke changes in the values of the published statistics.
- Comparing the values with the CCMS statistics and making sure they match with the IVS published output.

2.2. Test Results

The objectives outlined in **Section 2.1** were verified and met. All tests were executed and passed.

2.3. Support

For technical support on IVS, please contact RMG Networks technical support team:

- **Telephone:** 1.877.789.8324 (North America)/+44 (0) 1442 275200 (International)
- **Email:** support@rmgnetworks.com
- **Web Site:** www.rmgnetworks.com/contact

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing between Avaya Contact Center Manager Server and IVS.

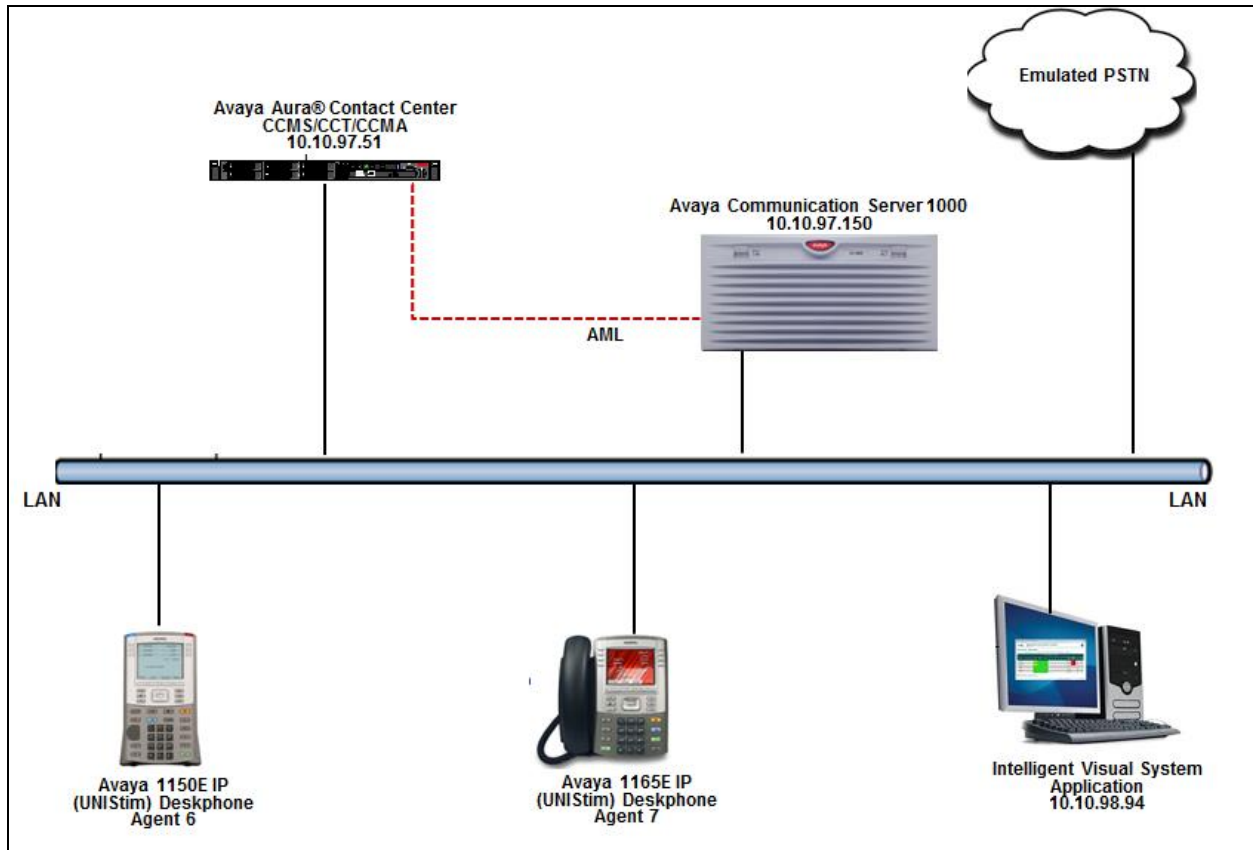


Figure 1: Test Solution Configuration.

4. Equipment and Software Validated

Equipment	Software/Firmware
Avaya Communication Server 1000	7.65
Avaya Contact Center Manager Server OS	Win2008 Server R2 Standard SP1
Avaya Aura® Contact Center Manager Server	6.4.212.0
Avaya Aura® RTD SDK	6.4
Avaya IP Deskphones as Agents: <ul style="list-style-type: none"> ○ 1150E (UNISTim) ○ 1165E (UNISTim) 	0x27C8V 0x25C8V
IVS Server OS IVS Application	Win2008 Server R2 Standard SP1 12.0.2

5. Configuring the Avaya Contact Center Manager Server

This section describes the steps to configure the CCMS so that the IVS is able to connect to it. Assumption is made that the CCMS is installed successfully and all the required scripts are running. Assumption is also made that the CCMS is interfaced and working successfully with the Avaya Communication Server 1000 (Communication Server 1000). For additional information on CCMS and Communication Server 1000 installation and configuration refer to **Section 9**.

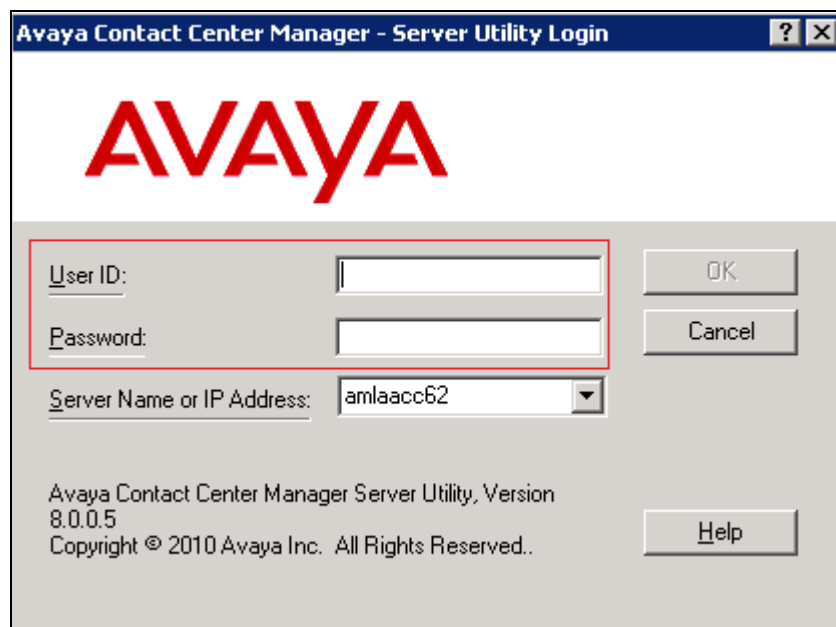
Here is a summary of CCMS Configuration:

- Creating new user to interface with IVS.

5.1. Configuring a New User

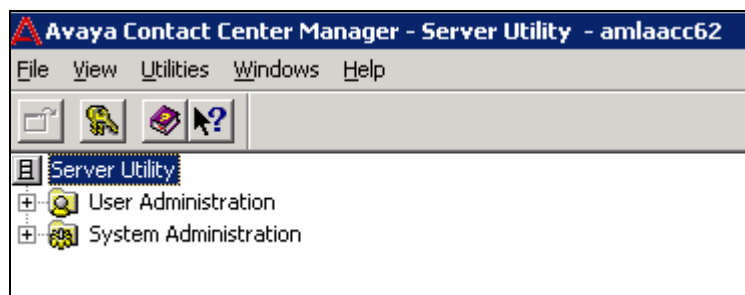
This section explains the steps to add a new user that is required to interface and connect to the IVS system. To add a new user, navigate through **Start → All Programs → Avaya → Server Utility** on the server the CCMS is installed on (not shown).

Screen below shows the **Server Utility Login** screen. Enter the administrator **User ID** and **Password**. Click on **OK** to continue.

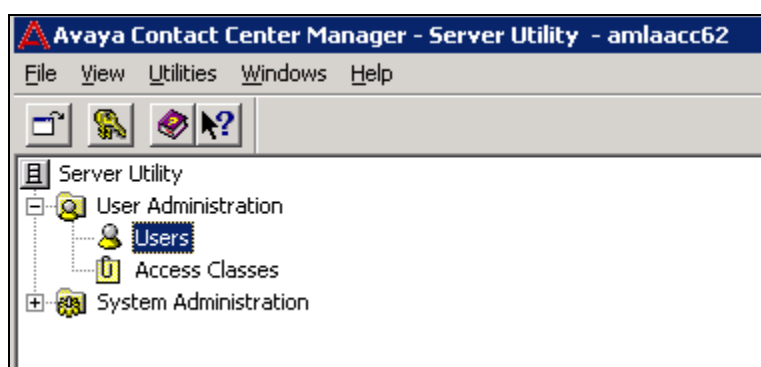


The image shows a Windows-style dialog box titled "Avaya Contact Center Manager - Server Utility Login". At the top center is the large red "AVAYA" logo. Below the logo, there are three input fields: "User ID:" with an empty text box, "Password:" with an empty text box, and "Server Name or IP Address:" with a dropdown menu showing "amlaacc62". A red rectangular box highlights the "User ID" and "Password" fields. To the right of the input fields are three buttons: "OK", "Cancel", and "Help". At the bottom left, there is text: "Avaya Contact Center Manager Server Utility, Version 8.0.0.5" and "Copyright © 2010 Avaya Inc. All Rights Reserved..".

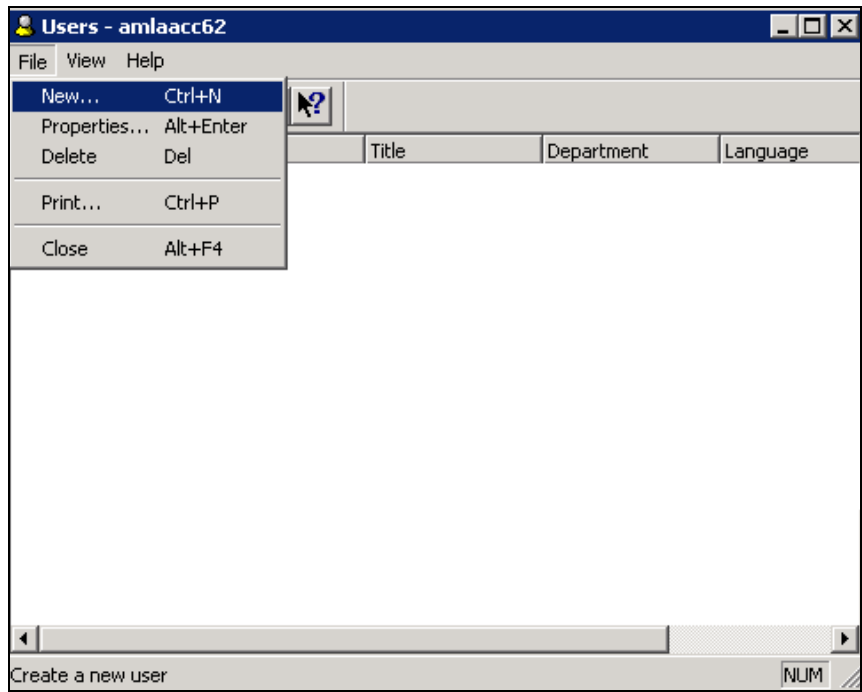
Screen below shows the **Server Utility** main screen.



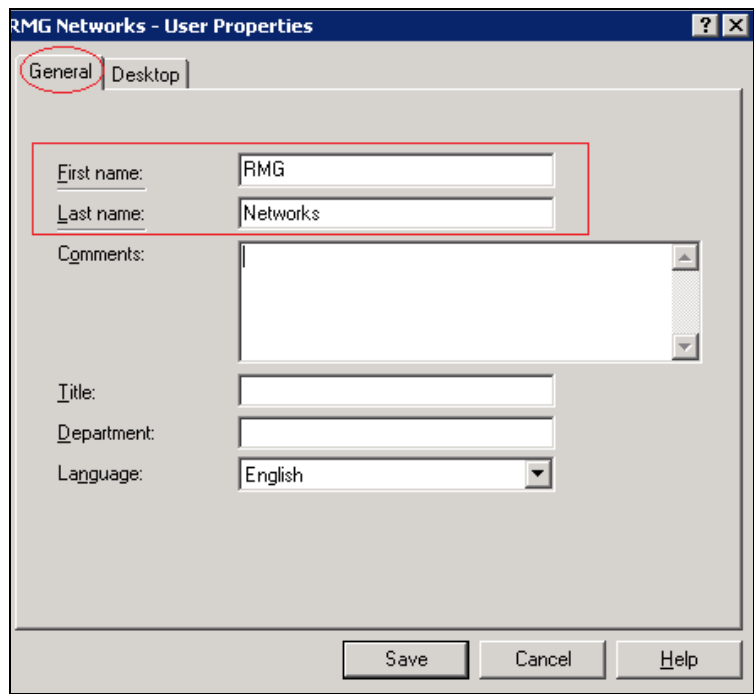
To add a new user, expand the **User Administration** tree and double-click on **Users** as shown in the screen below.



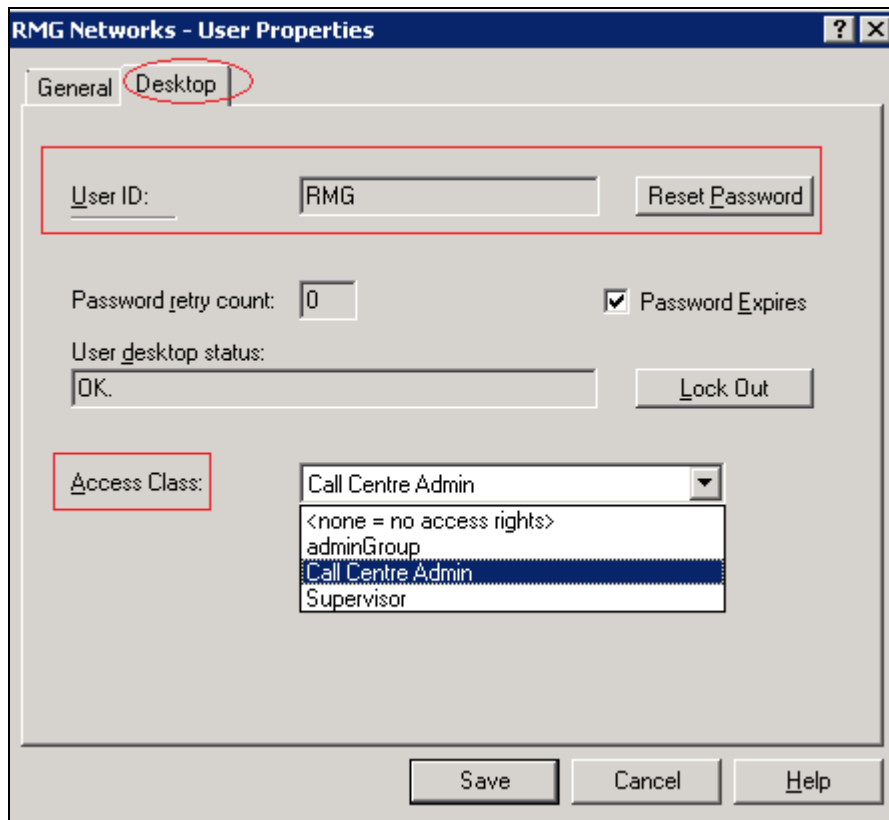
Screen below shows the **Users** screen. Click on **File** and select **New**.



Screen below shows the New User being configured. Populate the **First name** and **Last name** fields that is seen under the **General** tab.

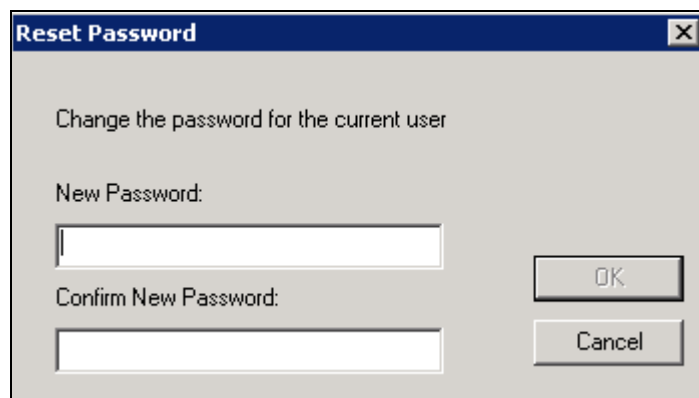


From the **Desktop** tab populate the **User ID** field and select **Call Centre Admin** under **Access Class** field as shown in the screen below. Click on **Reset Password** to continue.



The image shows a Windows-style dialog box titled "RMG Networks - User Properties". It has two tabs: "General" and "Desktop". The "Desktop" tab is selected and highlighted with a red circle. Inside the "Desktop" tab, there is a red rectangular box around the "User ID:" label, the text "RMG" in the input field, and the "Reset Password" button. Below this, there is a "Password retry count:" label with a value of "0" in a small box, and a checked checkbox labeled "Password Expires". Underneath, the "User desktop status:" label is followed by a text box containing "OK." and a "Lock Out" button. At the bottom of the tab, the "Access Class:" label is next to a dropdown menu. The dropdown menu is open, showing a list of options: "<none = no access rights>", "adminGroup", "Call Centre Admin" (which is highlighted in blue), and "Supervisor". At the very bottom of the dialog box, there are three buttons: "Save", "Cancel", and "Help".

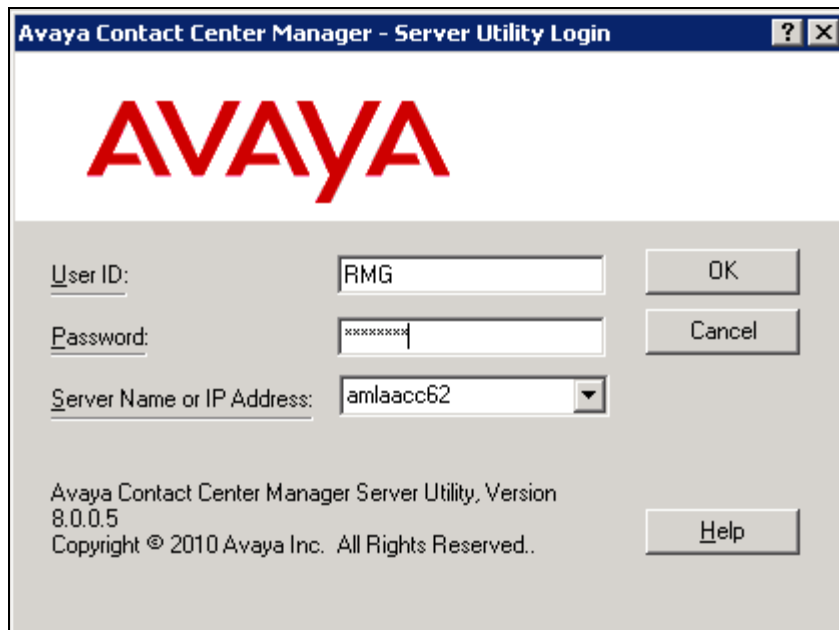
Configure the password and click on **OK** to continue as shown in below. Click on the **Save** button that is seen in the screen above to complete the configuration of New User.



The image shows a "Reset Password" dialog box. It contains the instruction "Change the password for the current user". Below this, there are two input fields. The first is labeled "New Password:" and the second is labeled "Confirm New Password:". To the right of these fields are two buttons: "OK" and "Cancel".

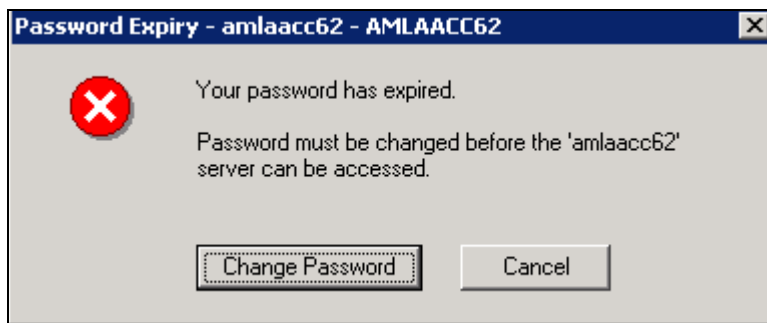
To confirm the configuration of the New User created, exit from the Server Utility application and navigate back to it as explained in **Section 5.1**.

Screen below shows the **Server Utility Login** screen. Populate the **User ID** and **Password** fields with the values that were configured above. Click on **OK** to continue.



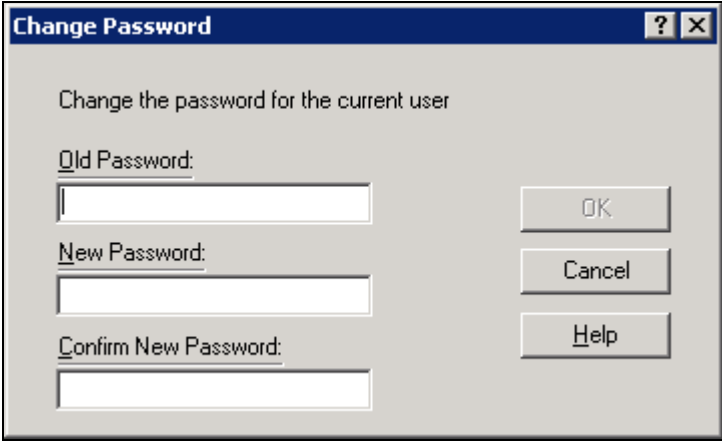
The image shows a Windows-style dialog box titled "Avaya Contact Center Manager - Server Utility Login". It features the Avaya logo in red at the top. Below the logo, there are three input fields: "User ID:" with the text "RMG", "Password:" with masked characters "xxxxxxx", and "Server Name or IP Address:" with a dropdown menu showing "amlaacc62". To the right of these fields are "OK" and "Cancel" buttons. At the bottom left, it says "Avaya Contact Center Manager Server Utility, Version 8.0.0.5" and "Copyright © 2010 Avaya Inc. All Rights Reserved..". A "Help" button is located at the bottom right.

While logging in for the first time using the new user, the system forces the password to be changed. Click on **Change Password** as shown in the screen below.



The image shows a Windows-style dialog box titled "Password Expiry - amlaacc62 - AMLAACC62". It has a red "X" icon in a circle on the left. The text inside says: "Your password has expired." followed by "Password must be changed before the 'amlaacc62' server can be accessed." At the bottom, there are two buttons: "Change Password" and "Cancel".

Configure the required fields and click on **OK** to complete the changing of the password as shown in the screen below.



A screenshot of a 'Change Password' dialog box. The title bar is blue with the text 'Change Password' and standard window controls. The main area is light gray and contains the instruction 'Change the password for the current user'. Below this are three input fields: 'Old Password:', 'New Password:', and 'Confirm New Password:'. To the right of these fields are three buttons: 'OK', 'Cancel', and 'Help'.

Change Password

Change the password for the current user

Old Password:

New Password:

Confirm New Password:

OK

Cancel

Help

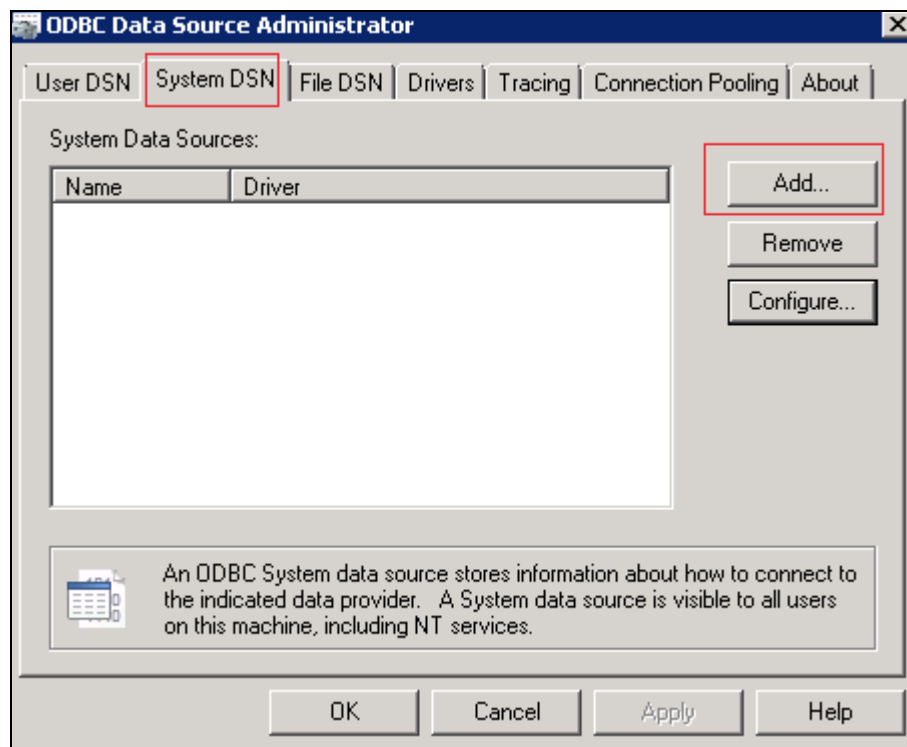
6. Configure Intelligent Visual Solutions Server

This document assumes that IVS server was properly installed and configured by a RMG Networks Engineer. This section provides steps on configuring the **IVS Portal Administrator** and **Portal Data Viewer** to work with Contact Center system.

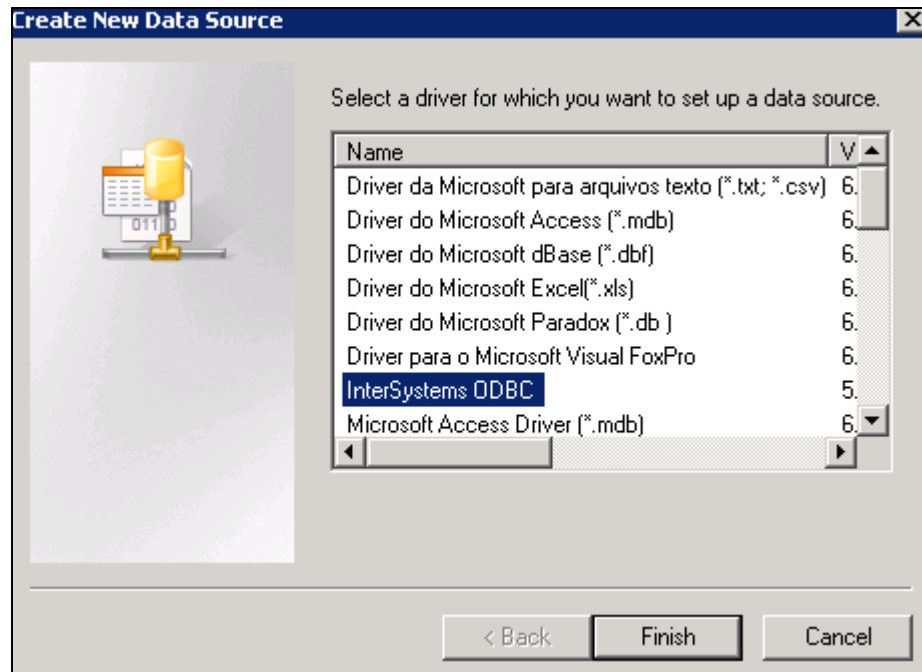
6.1. Creating a Data Source

To create a Data Source, run the **odbcad32.exe** file. During compliance testing this file was found under **C:\Windows\SysWOW64** path.

The **ODBC Data Source Administrator** window is seen as shown below. Select the **System DSN** tab and click on the **Add** button.



The **Create New Data Source** window is seen as shown below. Select **InterSystems ODBC** driver and click on the **Finish** button.



The **InterSystems Cache ODBC Data Source Setup** window is seen as shown below.

Configure the following values,

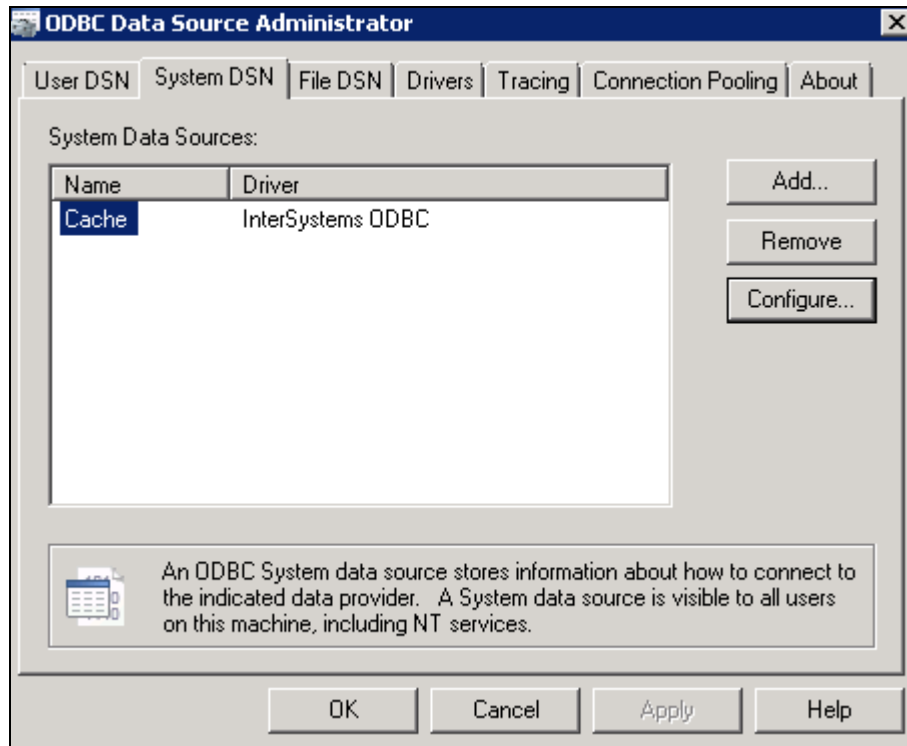
- In the **Name** field found under **Data Source**, type a name. During compliance testing **Cache** was used.
- Under the **Connection** section,
Host (IP Address): This is the IP address of the Contact Center Server
Port: 1972
Cache Namespace: During compliance testing **ccms_stat** was used. Note that this is the same name defined in the Contact Center Server (in CCMS module) and therefore using any other name would result in a failure of connecting to the CCMS database.
- Under the **Login** section,
User Name: Enter the User Name as configured in **Section 5.1**
Password: Enter the password as configured in **Section 5.1**

Retain default values for all other fields.

Before clicking on the **OK** button, click on the **Test Connection** button to verify the connectivity.

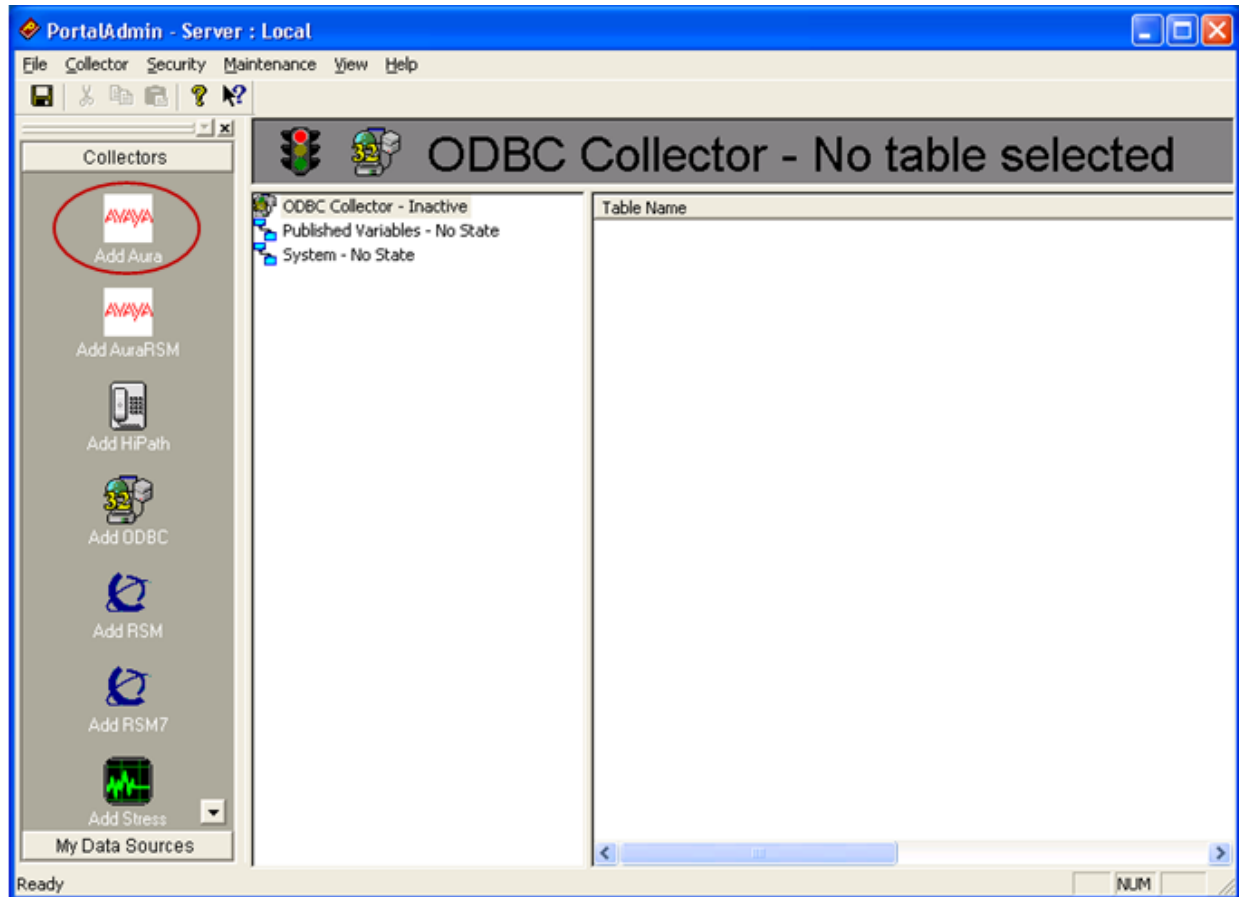
The screenshot shows the 'InterSystems Cache ODBC Data Source Setup' dialog box. It is divided into four main sections: 'Data Source', 'Connection', 'Login', and 'Misc'. In the 'Data Source' section, the 'Name' field contains 'Cache'. The 'Connection' section contains 'Host (IP Address)' as '10.10.97.51', 'Port' as '1972', and 'Cache Namespace' as 'ccms_stat'. The 'Login' section contains 'User Name' as 'RMG' and a masked 'Password' field. The 'Misc' section contains several unchecked checkboxes: 'ODBC Log', 'Static Cursors', 'Disable Query Timeout', 'Use Locale Decimal Symbol', and 'Unicode SQLTypes'. On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Test Connection', 'Ping', and a '# Times' field set to '1000', and a 'Help' button at the bottom.

Screen below shows the newly added Data Source. Click on OK button.



6.2. Configure IVS Portal Admin

To configure **PortalAdmin** log in to the IVS server as an administrator go to: **Start → All Programs → RMG Networks → IVS Portal Administrator**, the **PortalAdmin** window appears as shown below.



On the left hand side of the **PortalAdmin** window seen above, click on the **Add Aura** icon to add a Collector as shown below.

Enter a name in the name box as **Aura CCM** and click on the **Next** button to continue.

Add Aura/CCM Collector

AVAYA

Enter a descriptive name for the Aura/CCM collector. This will display on the collector for quick reference.

Aura CCM

Critical Information

Prior to adding the Aura/CCM collector, you should contact your Aura/CCM administrator and obtain login information, as well as the information about the associated Sybase database.

Without the appropriate login information, connection to the Aura/CCM cannot be made.

< Back Next > Cancel

In the window shown below, enter the credentials that were created in **Section 5.1** and the IP address of CCMS server. Click on the **Next** button to continue.

Add Aura/CCM Collector

AVAYA

Enter your login name and password for the Aura/CCM.

Login Name: RMG

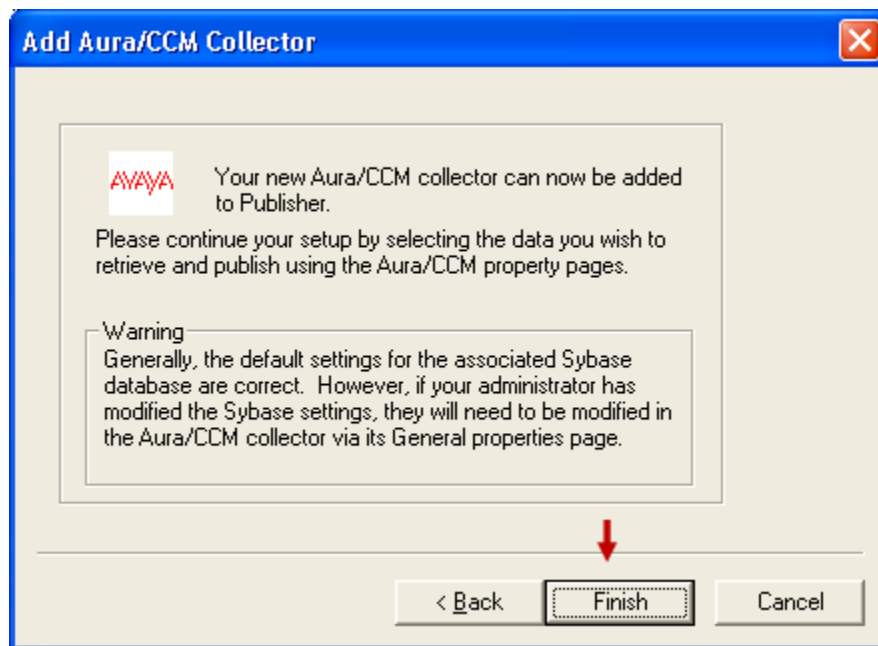
Password: xxxxxxx

Enter the IP Address for the Aura/CCM. This should have been provided by the Call Center Administrator

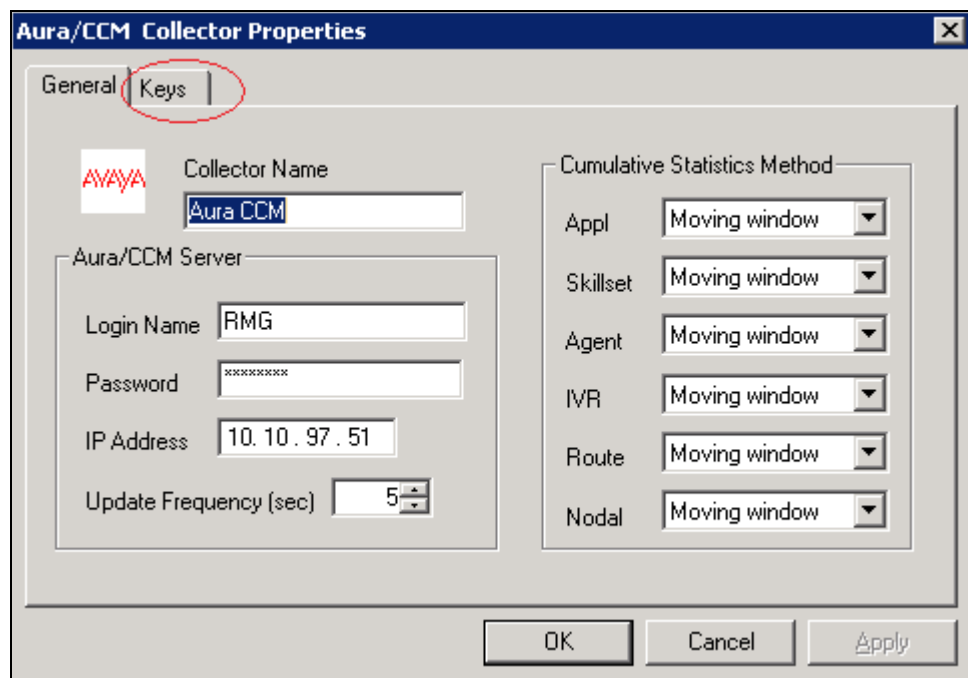
IP Address: 10.10.97.51

< Back Next > Cancel

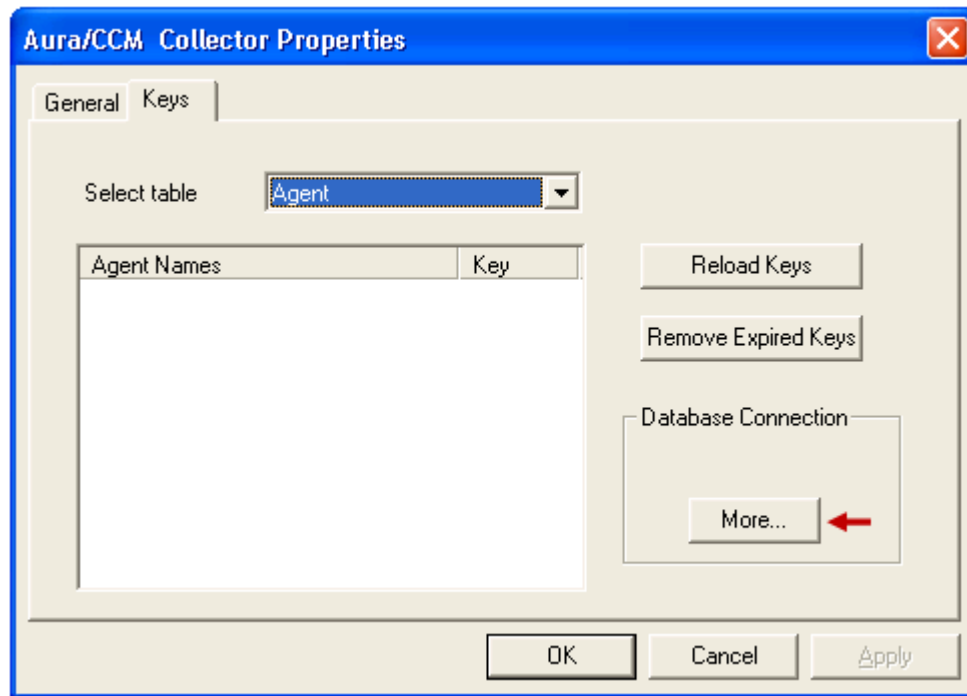
In the window shown below, click on the **Finish** button to complete adding a collector and go to the **Aura/CCM Collector Properties** window.



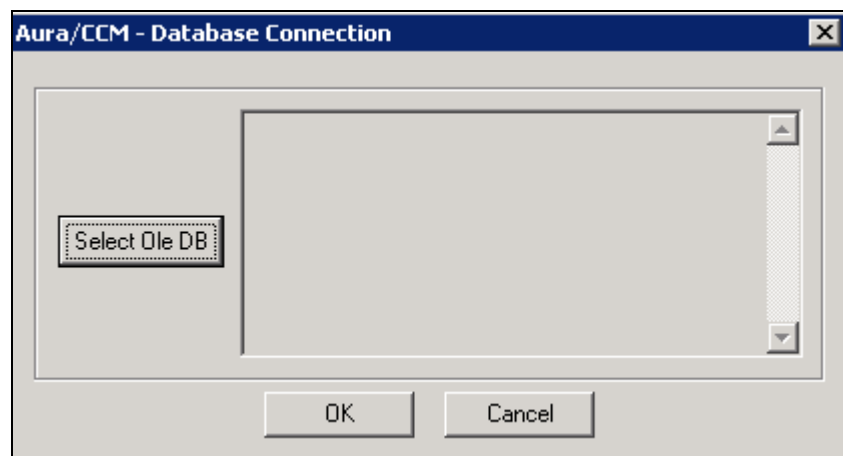
The **Aura/CCM Collector Properties** window appears as shown below.



Click on the **Keys** tab of the above window. Select **Agent** from the drop down menu for **Select table** field and click on the **More** button as shown below.



The **Aura/CCM – Database Connection** window is seen as shown below. Click on the **Select Ole DB** button to open the **Data Link Properties** window.

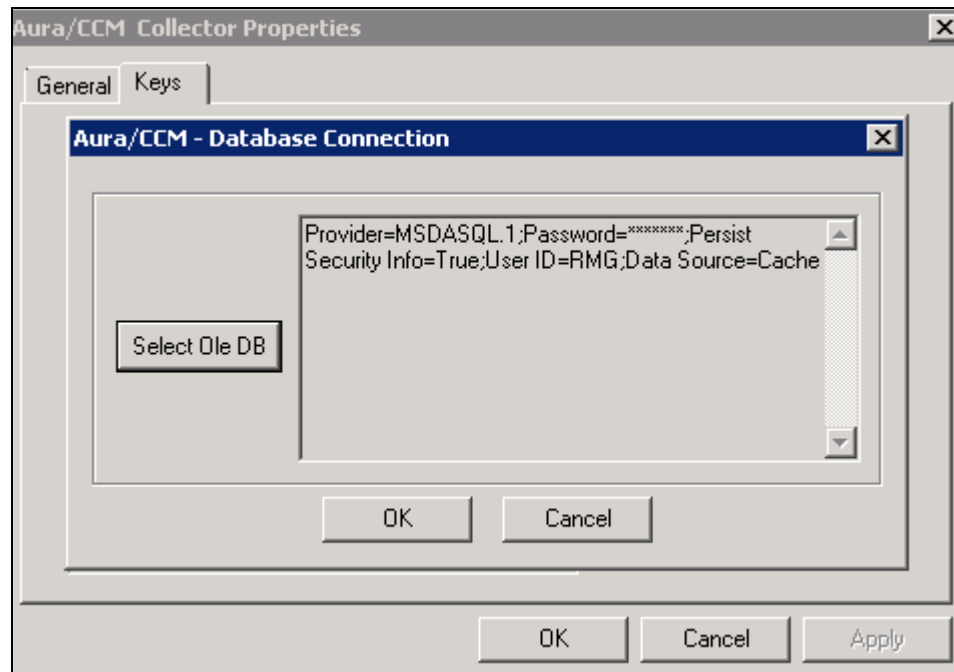


From the **Data Link Properties** window as shown below, select the **Connection** tab and configure the following,

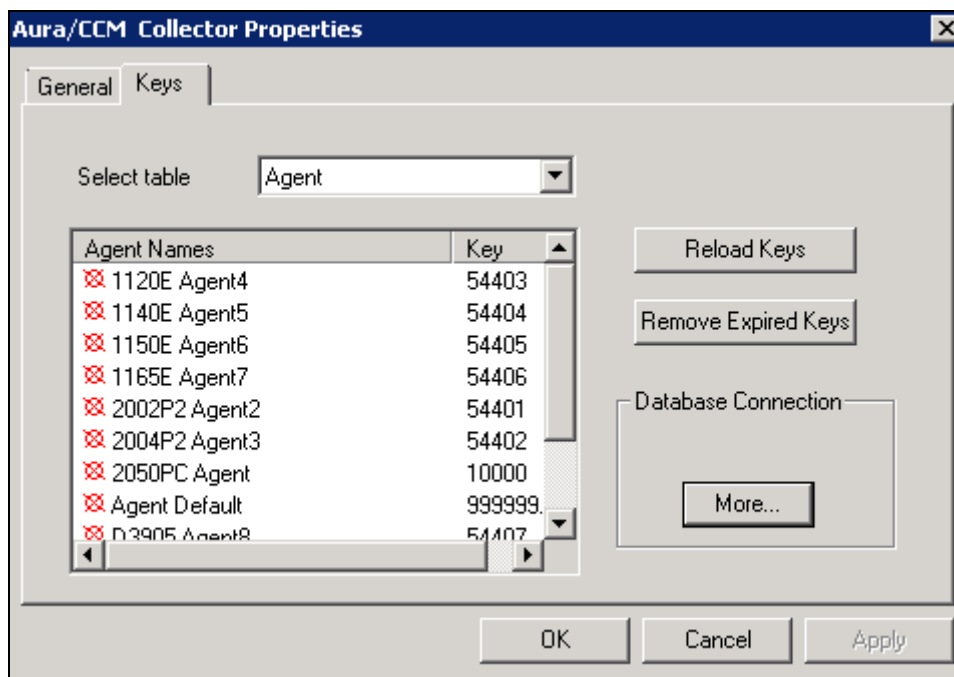
- Select the **Use data source name** radio button and from the drop down menu select the data source. During compliance testing **Cache** was selected and **Section 6.1** explains the creation of this data source.
- Enter the **User name** and **Password** information as configured in **Section 5.1**
- Check the **Allow saving password** box.
- Before clicking on **OK** to complete the configuration, click on the **Test Connection** button to verify the connectivity.

The screenshot shows the 'Data Link Properties' dialog box with the 'Connection' tab selected. The dialog is titled 'Data Link Properties' and has four tabs: 'Provider', 'Connection', 'Advanced', and 'All'. The 'Connection' tab is active. Below the tabs, the text 'Specify the following to connect to ODBC data:' is displayed. There are three numbered sections: 1. 'Specify the source of data:' with two radio buttons. The first, 'Use data source name', is selected and highlighted with a red box. Below it is a dropdown menu showing 'Cache' and a 'Refresh' button. The second radio button, 'Use connection string', is unselected. Below it is a 'Connection string:' label and a text box with a 'Build...' button. 2. 'Enter information to log on to the server' with two text boxes. The 'User name:' box contains 'RMG' and is highlighted with a red box. The 'Password:' box contains nine dots and is also highlighted with a red box. Below these are two checkboxes: 'Blank password' (unchecked) and 'Allow saving password' (checked, highlighted with a red box). 3. 'Enter the initial catalog to use:' with a dropdown menu. At the bottom right of the dialog is a 'Test Connection' button, highlighted with a red box. At the very bottom are three buttons: 'OK', 'Cancel', and 'Help'.

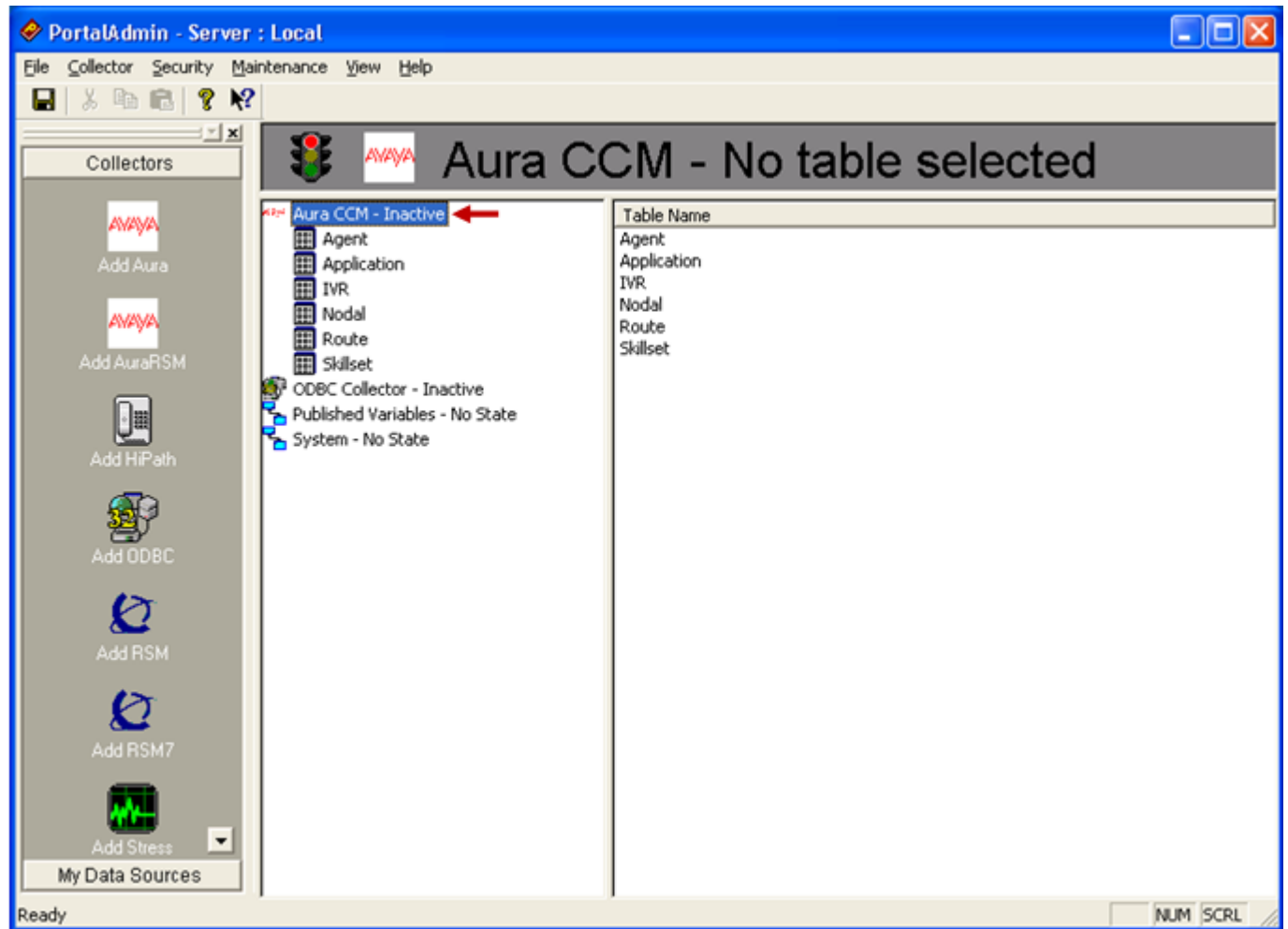
The **Aura/CCM - Database Connection** window is shown as below. Click on **OK** button to return to the **Aura/CCM Collector Properties** window.



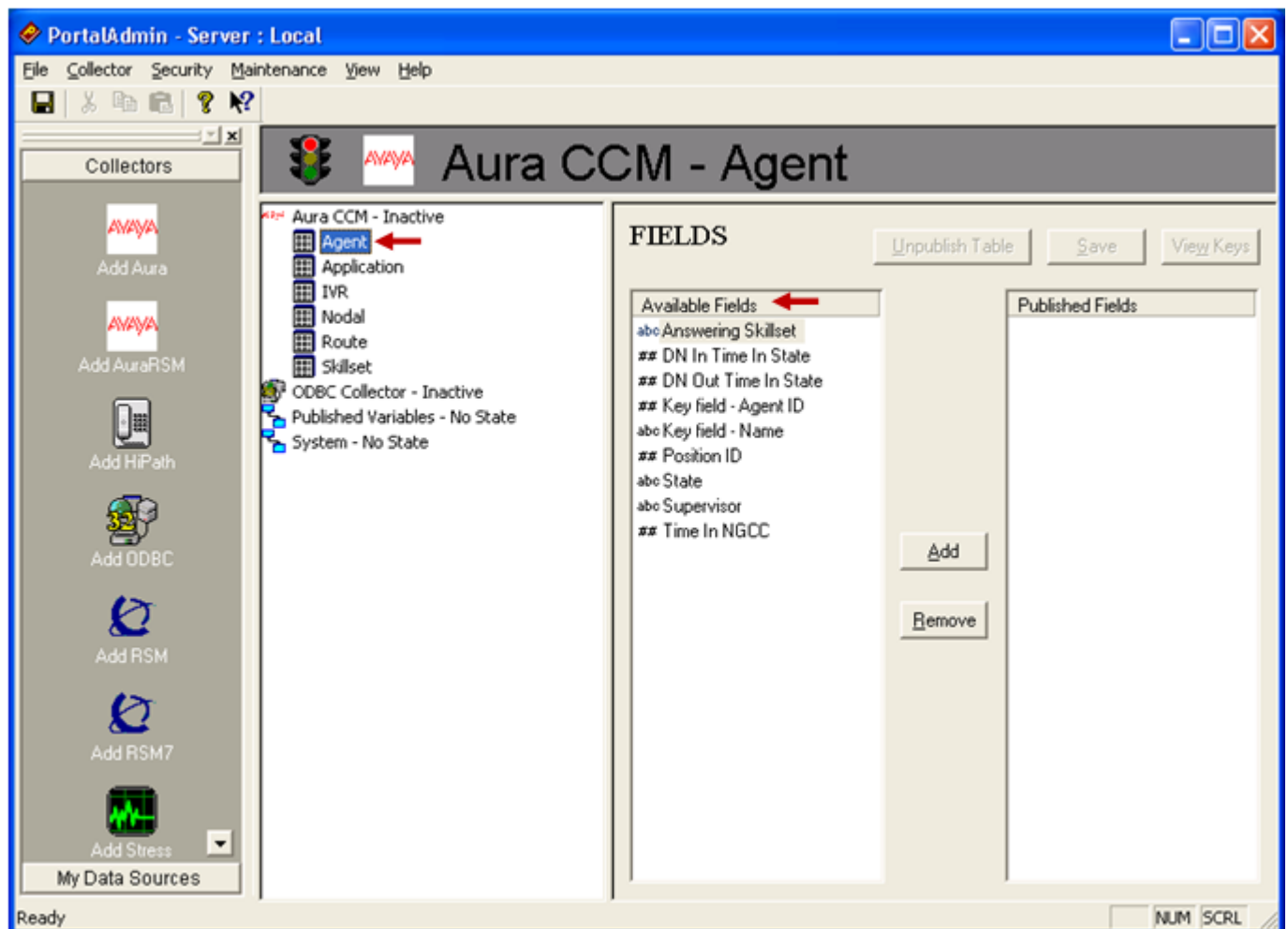
Screen below shows the **Aura/CCM Collector Properties** window with the Keys loaded. Click on the **OK** button to complete the configuration.



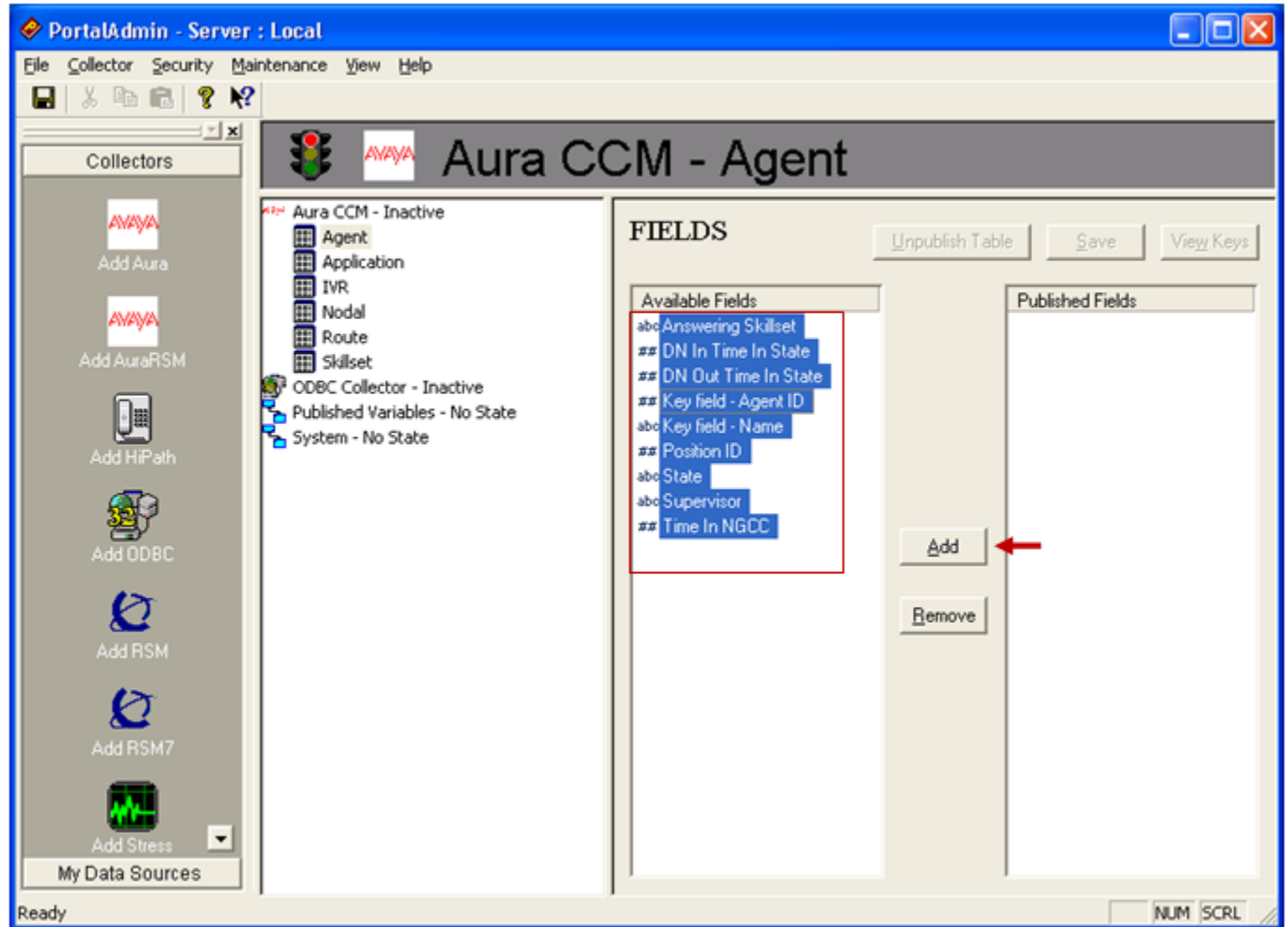
Screen below shows the **PortalAdmin** window with the **AuraCCM** collector created.



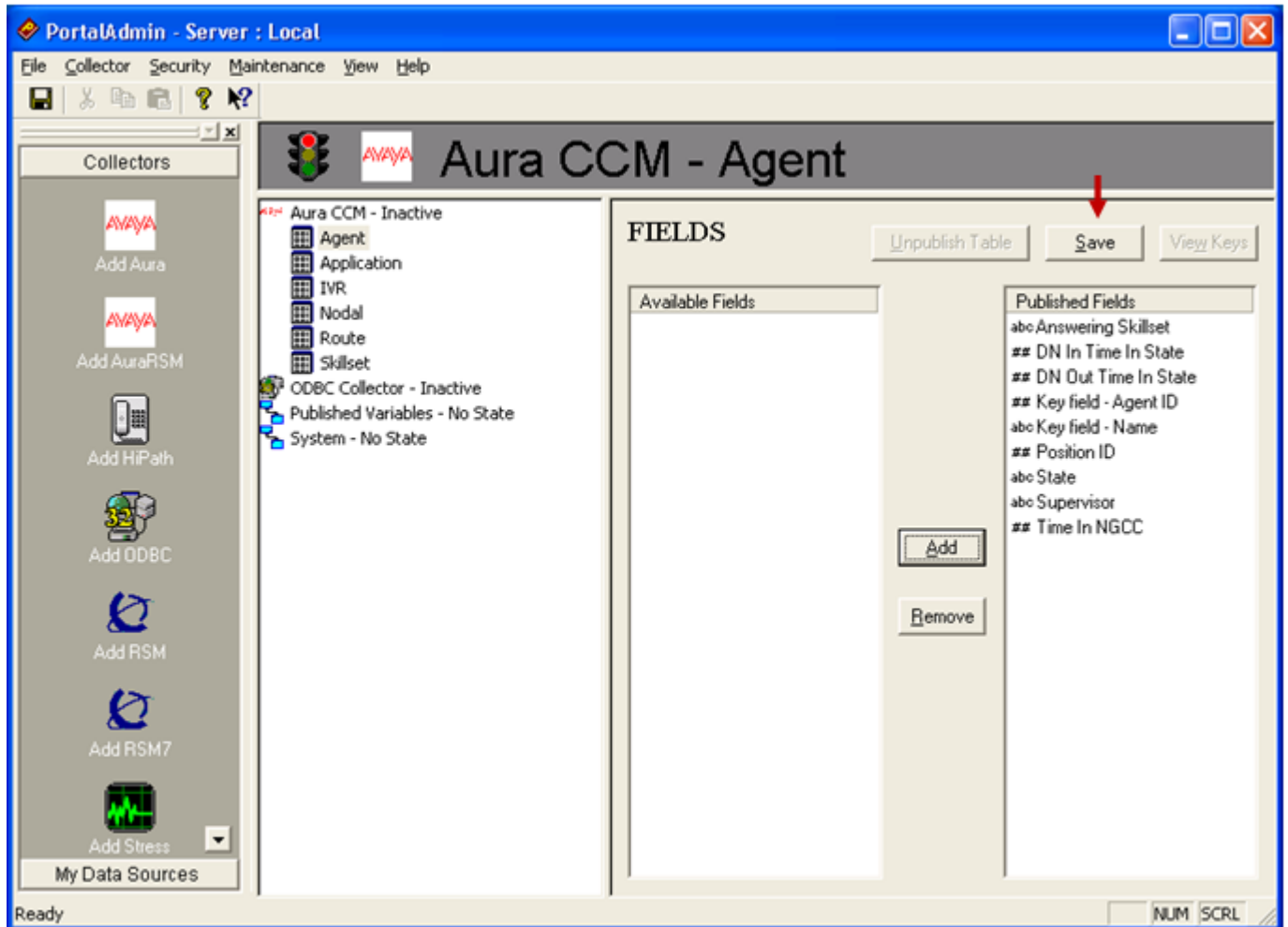
To publish the **Agent** application table, click on the **Agent** application tab under the **Aura CCM** collector that has been created. All keys of **Agent** application are listed under the **Available Fields** column of **Fields** window as shown below.



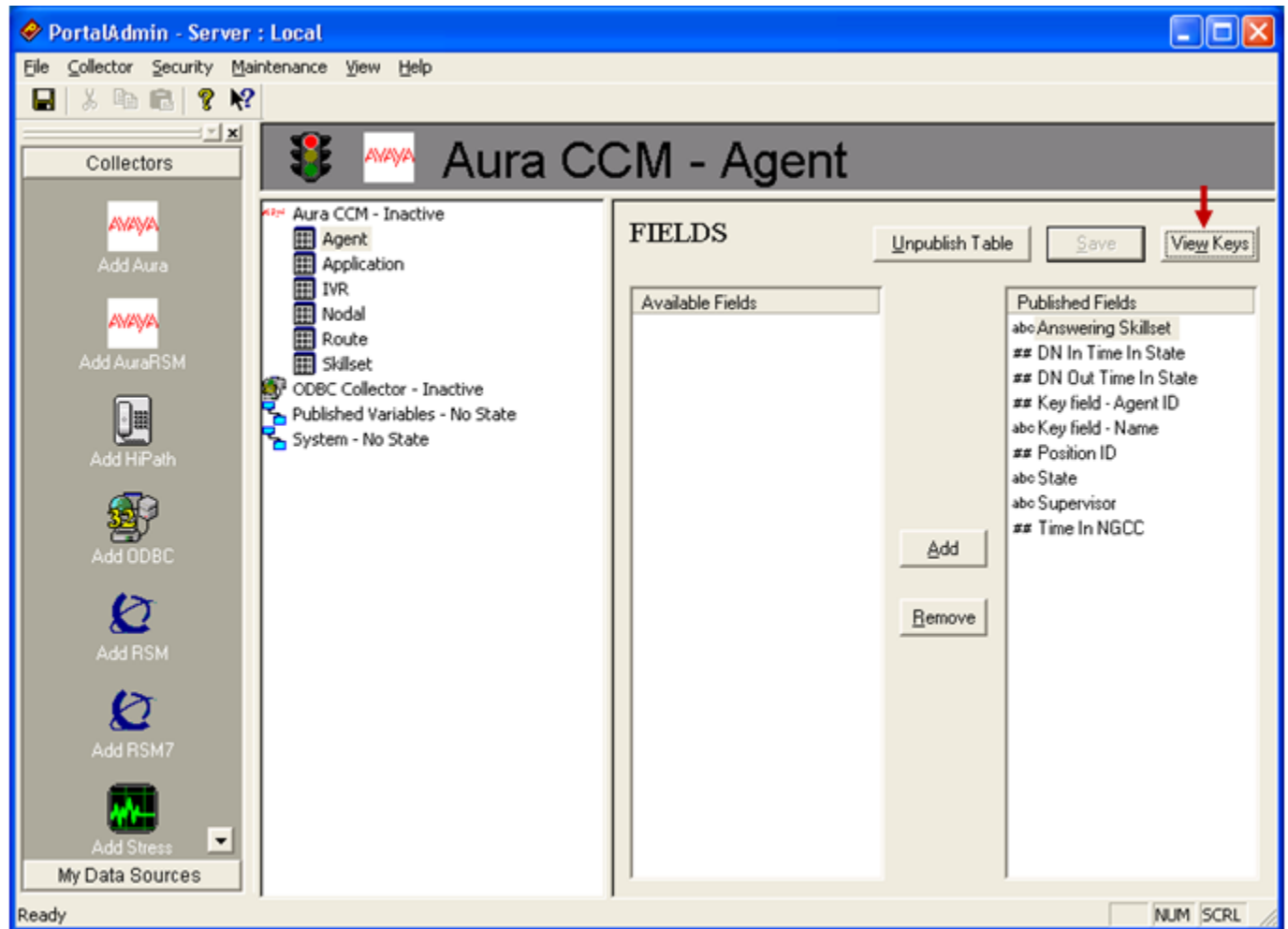
Select all fields of **Available Fields** column and click **Add** button as shown below.



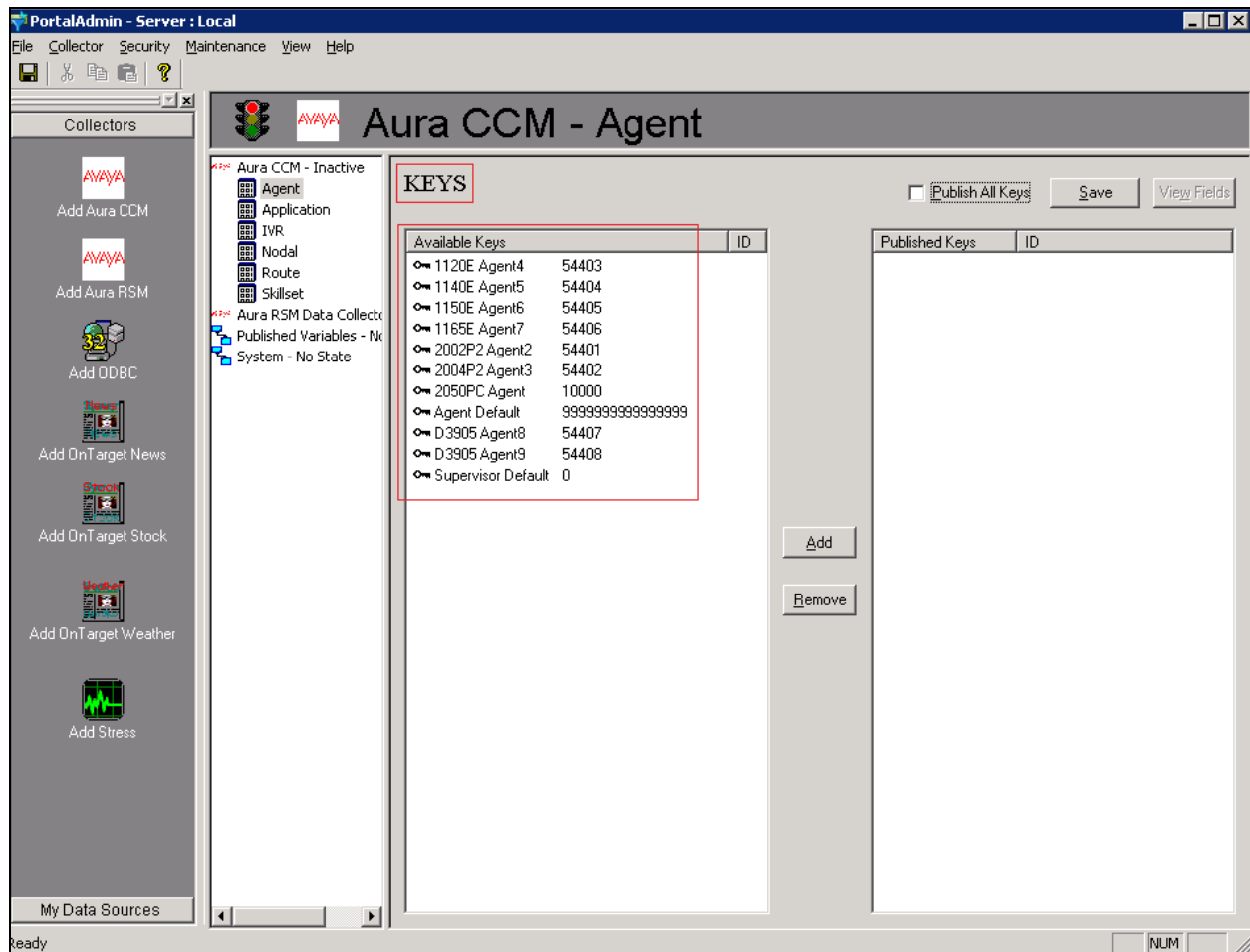
All fields are now moved to **Published Fields** column as shown below and then click on the **Save** button to save it.



The **View Keys** button now becomes available as shown below.



Click on the **View Keys** button, the Agent keys will display on the **Available Keys** column of **KEYS** window as shown below.

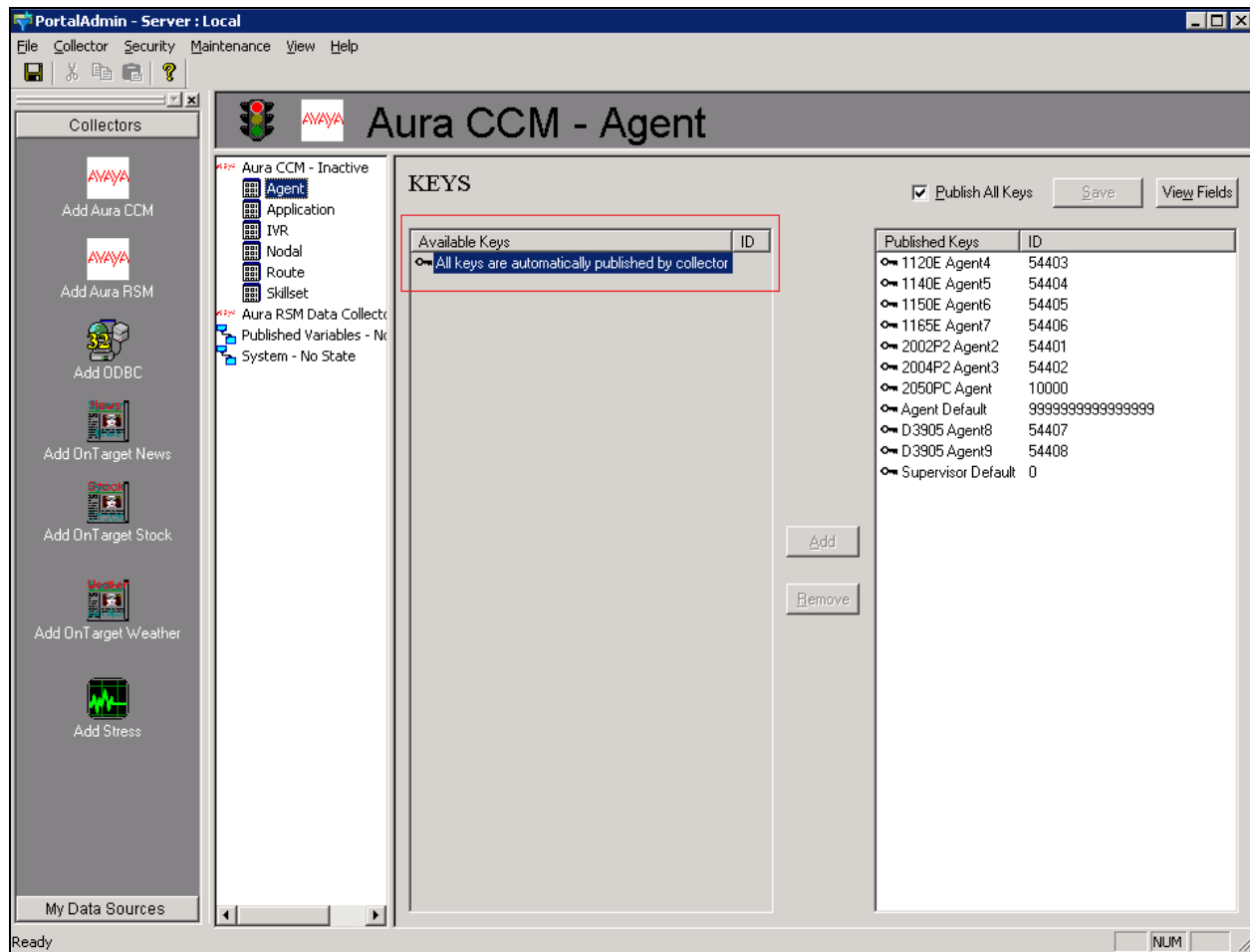


To publish all keys of **Agent** application, Check the **Publish All Keys** box and all keys will be published and moved to the **Published Keys** column as shown below.

The screenshot shows the PortalAdmin - Server : Local interface. The main window is titled 'Aura CCM - Agent'. On the left, there is a 'Collectors' sidebar with various options like 'Add Aura CCM', 'Add Aura RSM', 'Add ODBC', 'Add OnTarget News', 'Add OnTarget Stock', 'Add OnTarget Weather', and 'Add Stress'. The main area is divided into 'Available Keys' and 'Published Keys' columns. The 'Published All Keys' checkbox is checked, and a list of published keys is shown in the 'Published Keys' column.

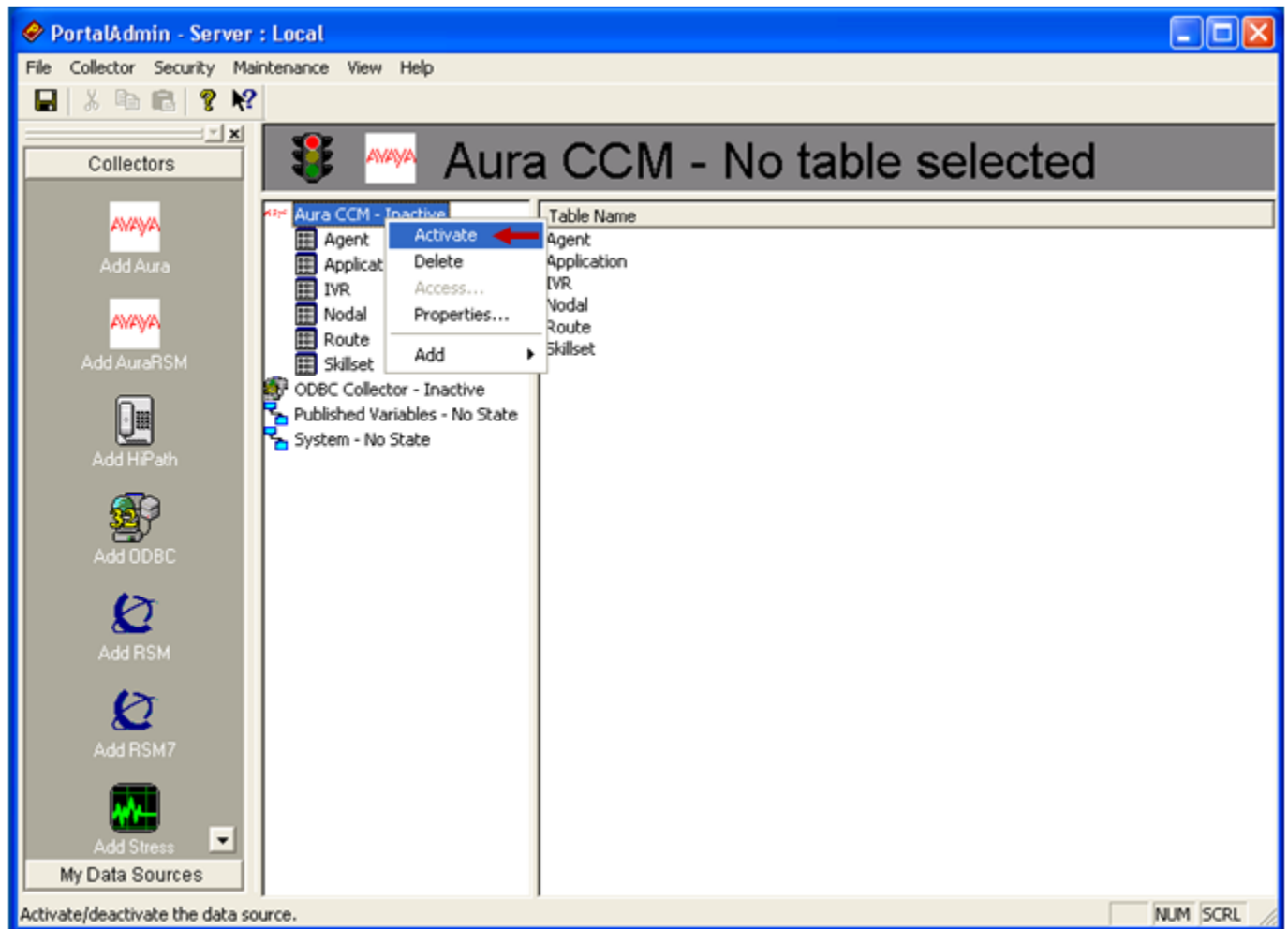
Published Keys	ID
1120E Agent4	54403
1140E Agent5	54404
1150E Agent6	54405
1165E Agent7	54406
2002P2 Agent2	54401
2004P2 Agent3	54402
2050PC Agent	10000
Agent Default	99999999999999999999
D3905 Agent8	54407
D3905 Agent9	54408
Supervisor Default	0

Click on the **Save** button to save the configuration and complete the publishing of all keys in the **Agent** application as shown below.

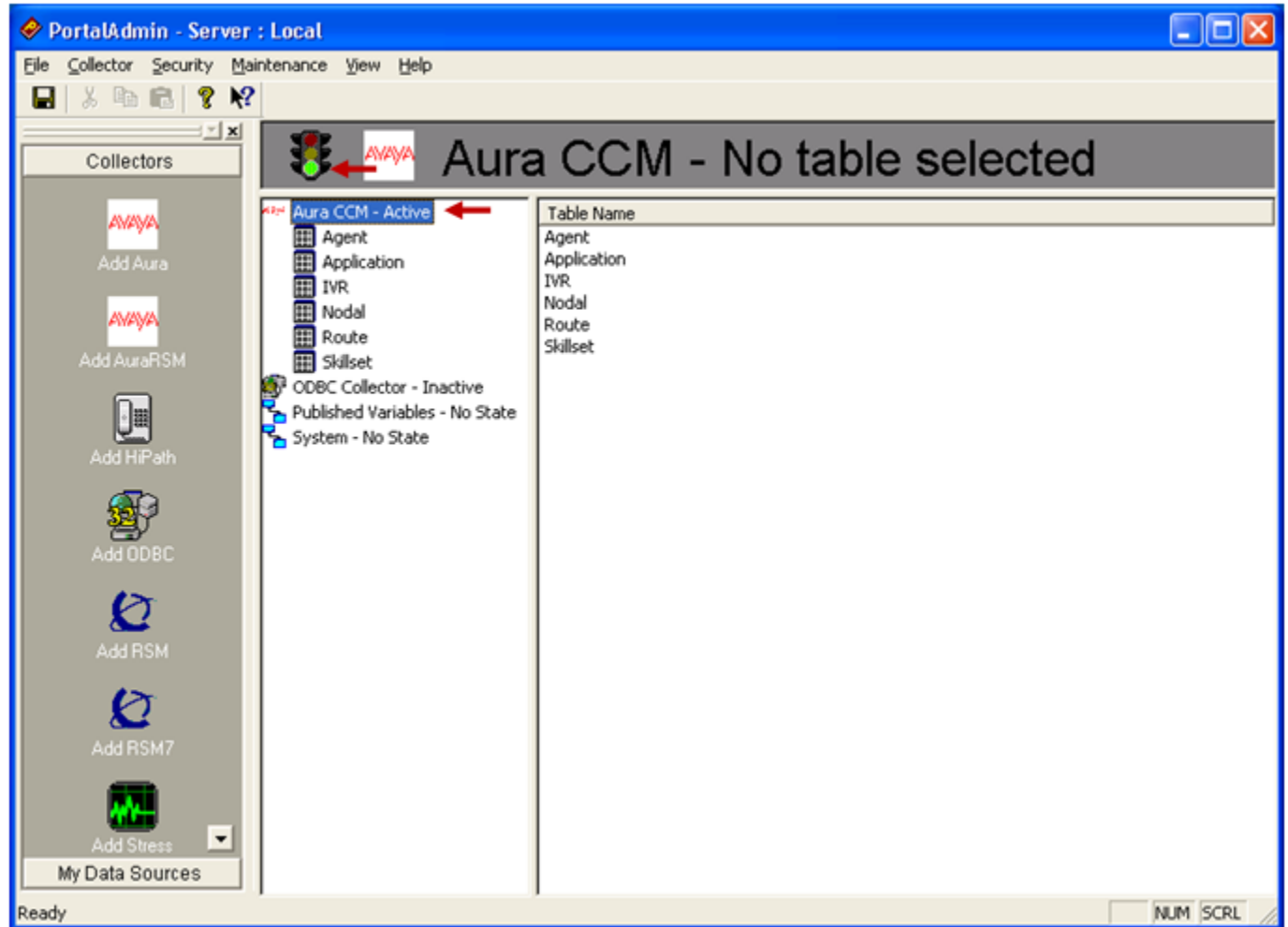


Apply the above steps of publishing **Agent** application for remaining applications of **Aura CCM** such as **Application**, **IVR**, **Nodal**, **Route** and **SkillSet**.

To activate the **AuraCCM** collector, right click on the **AuraCCM** and select the **Activate** option on the menu as shown below.

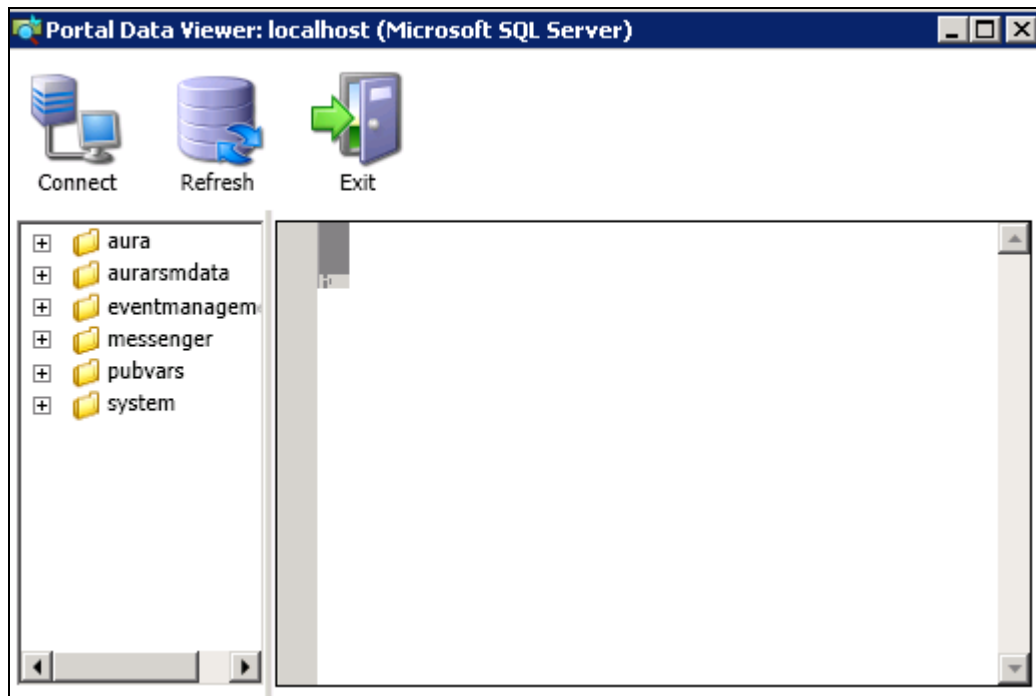


The **AuraCCM** collector is successfully activated as shown below.

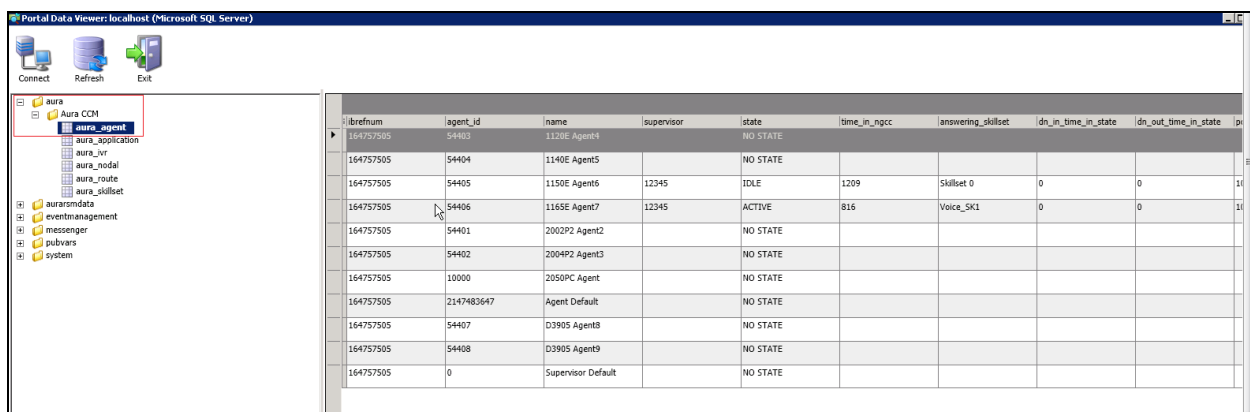


6.3. Configure IVS Portal Data Viewer

To open **Portal Data Viewer**, log in the IVS server as administrator and navigate to **Start → All Programs → RMG Networks → IVS Portal Data Viewer**, the **Portal Data Viewer** window appears as shown below.



Expand the **aura** folder and then expand the **Aura CCM** folder and click on **aura_agent** to display real time data of Agent application streamed from the Contact Center server as shown below.



Similarly click on the **aura_application**, **aura_ivr**, **aura_nodal**, **aura_route** and **aura_skillset** to display its real time data streamed from the Contact Center server.

7. Verification Steps

Real-time Displays were launched on Contact Center Manager Administrator to monitor real-time activity of calls being placed into the system. This was used to verify the data observed on the IVS Portal Data Viewer window as shown in the above screen.

8. Conclusion

All of the executed test cases have passed and met the objectives outlined in **Section 2**. RMG Networks Intelligent Visual Solutions v12.0.2 is considered compliant with Avaya Aura® Contact Center's Contact Center Manager Server Release 6.4 for Real Time Display.

9. Additional References

[1] Product documentation for Avaya products may be found at:

<https://support.avaya.com/css/Products/>

Avaya Aura® Contact Center Planning and Engineering (NN44400-210)

Avaya Aura® Contact Center Installation (NN44400-311)

Avaya Aura® Contact Center Server Administration (NN44400-610)

Avaya Aura® Contact Center Overview (NN44400-111)

Avaya Aura® Contact Center Fundamentals (NN44400-110)

Avaya Aura® Contact Center Manager Administration – Client Administration (NN44400-611)

[2] Product documentation for RMG Networks IVS may be found by contacting Customer Service.

©2014 Avaya Inc. All Rights Reserved.

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

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