Avaya Solution & Interoperability Test Lab

Application Notes for configuring Kana Enterprise from Verint Systems Inc. with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for Kana Enterprise to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0.

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 for Kana Enterprise 14R1 SP4 from Verint Systems Inc. to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0.

Kana Enterprise is a server based, thin client, agent desktop solution that provides call control and monitoring functionality to Avaya Aura® Communication Manager end users via a JTAPI connection to Avaya Aura® Application Enablement Services. The design time modelling and runtime process execution and workflow engines run within a standard J2EE application server. A typical deployment will include integration to a number of back end systems and databases. Many deployments also incorporate full agent and call state control via a range of CTI integration options.

When an agent logs into their Kana Enterprise desktop thin client their desktop client is connected (via initial load balancing) to a KE process kernel session held within the J2EE application server. The process kernel makes use of a channel provider to interact with the telephony subsystem. There are a number of Kana Enterprise channel providers available including the Avaya AES version. This channel provider connects and communicates to/from Avaya AES via the Avaya Aura AE Services JTAPI SDK. The channel provider is a pluggable interface and channel providers can be changed without affecting the application.

During the agent's login to Kana Enterprise, the process kernel issues instructions via the channel provider to log the agent into telephony and make them available for calls (mappings are kept of extensions to desktop hosts and agent usernames to agent numbers (agent logins)).

After login the agent has a CTI toolbar available within the desktop application which allows them to perform functions such as drop a call, transfer or conference a call and request a break. Whenever the agent performs any action via this toolbar the request is routed via the channel provider and subsequently via the AES.

2. General Test Approach and Test Results

The general test approach was to validate successful handling of inbound skillset/VDN calls using Kana Enterprise desktop client. This was performed by calling inbound to a VDN and/or outbound from the elite call center using Kana Enterprise desktop client to answer calls.

Kana Enterprise has a Client/Server relationship and Kana Enterprise server was installed on a Windows 2012 Server R2 running an MS SQL 2012 database. Tables are created on this database specifically for Kana Enterprise and contained in these tables is the configuration information required for the connection to AES. The database has also many other tables utilised by the Kana Enterprise desktop client such as contact and customer database information but these are not the focus of these Application Notes. The primary concern is the connection to the AES in order to gain call control of the endpoints on Communication Manager.

There is no software is installed on any client PC utilised by an agent, a web browser is opened to the Kana Enterprise servers IP and the agent can then log into the Kana Enterprise system and receive calls.

Only Avaya H.323 endpoints were included in the compliance testing and SIP endpoints are not supported by Kana Enterprise.

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 test included both feature functionality and serviceability testing. The feature functionality testing focused on the handling of inbound skillset/VDN calls using Kana Enterprise desktop client.

- **Agent state change**– Make agent Ready/Not Ready using Kana Enterprise desktop client.
- **Inbound Calls** – Answer calls Kana Enterprise desktop client.
- **Outbound Calls** – Make calls using Kana Enterprise desktop client.
- **Call Hold** – Place calls on hold and retrieve calls using Kana Enterprise desktop client.
- **Blind Transfer** – Transfer callers using Kana Enterprise desktop client.
- **Consultative Transfer** - Transfer callers using Kana Enterprise desktop client.
- **Inbound Skillset Calls** – Answer skillset/VDN calls using Kana Enterprise desktop client.
- **Serviceability Testing** - Verify the ability of Kana Enterprise desktop client to recover from disconnection and reconnection to the Avaya solution

2.2. Test Results

All functionality and serviceability test cases were completed successfully, the following was noted. SIP phones are not supported by Kana Enterprise.

2.3. Support

Technical support for Kana Enterprise can be obtained from:

Website	http://www.kana.com/contact-form
Telephone	NA: +1-800-737-8738 EMEA: +44 (0)1932 839500 APAC: +61 2 8907 0300 Sales: +1-866-672-3791
Email	info@kana.com

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Kana Enterprise server is placed on the Avaya Telephony LAN. Kana Enterprise server connects to AES in order to gain call control of Communication Manager phonesets using a JTAPI client to communicate with AES services using TSAPI. An agent PC using a web browser is used to log in to the Kana Enterprise server in order to make and receive calls.

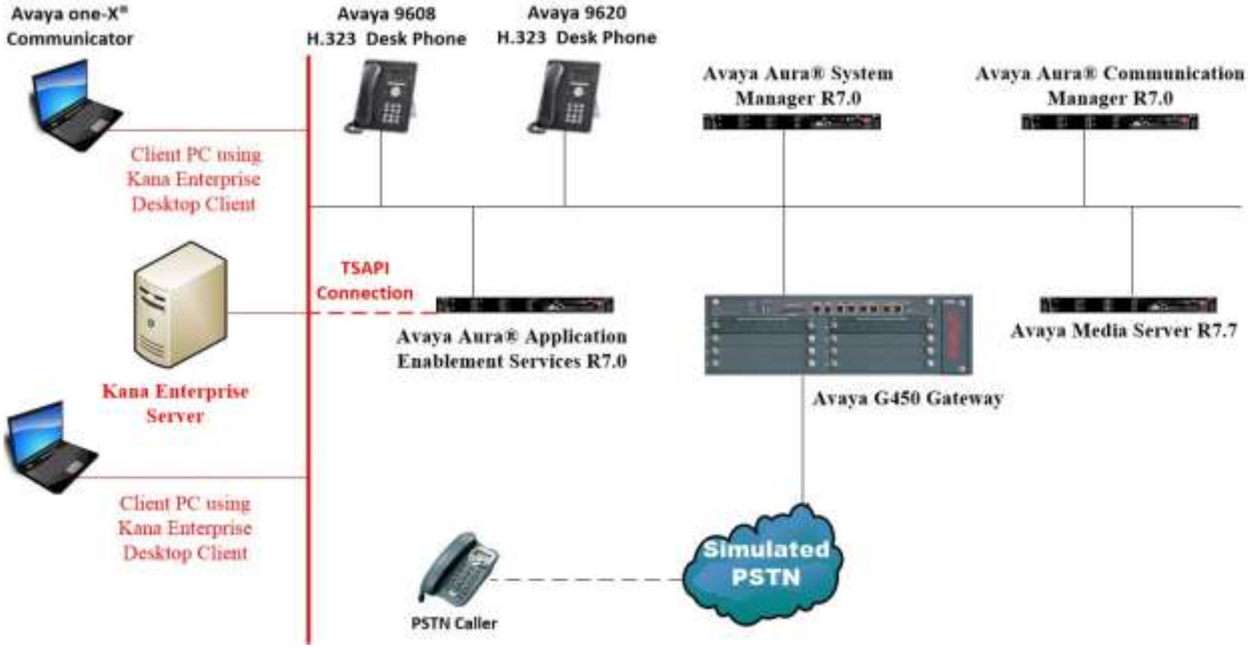

Avaya one-X® Communicator
Avaya 9608 H.323 Desk Phone
Avaya 9620 H.323 Desk Phone
Avaya Aura® System Manager R7.0
Avaya Aura® Communication Manager R7.0
Client PC using Kana Enterprise Desktop Client
TSAPI Connection
Avaya Aura® Application Enablement Services R7.0
Avaya Media Server R7.7
Kana Enterprise Server
Avaya G450 Gateway
Client PC using Kana Enterprise Desktop Client
Simulated PSTN
PSTN Caller

Figure 1: Network solution of Kana Enterprise with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.0.1.0 Build No. - 7.0.0.0.16266 Software Update Revision No: 7.0.1.0.064859 Feature Pack 1
Avaya Aura® Communication Manager running on a virtual server	R7.0 R017x.00.0.441.0 00.0.441.0-23012
Avaya Aura® Application Enablement Services running on a virtual server	R7.0 Build No – 7.0.0.0.1.13
Avaya Media Server running on a virtual server	R7.7
Avaya G450 Gateway	37.19.0 /1
Avaya 9608 H323 Deskphone	96x1 H323 Release 6.6.028
Avaya 9620 H323 Deskphone	96xx H323 Release S3.220A
Avaya one-X® Communicator H.323	R6.2.4.07-FP4
Kana Enterprise Server	14R1 SP4 HFR9
Avaya Aura AE Services JTAPI SDK used by Kana Enterprise Server	7.0.0.64
Kana Enterprise Desktop Client on Windows 7 PC using Web Browser - Chrome - Internet Explorer	 V51.0.2704.103 V11.0.9600.18349

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

```
display system-parameters customer-options                    Page   3 of  11
                                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
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                ATMS? y              DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

5.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

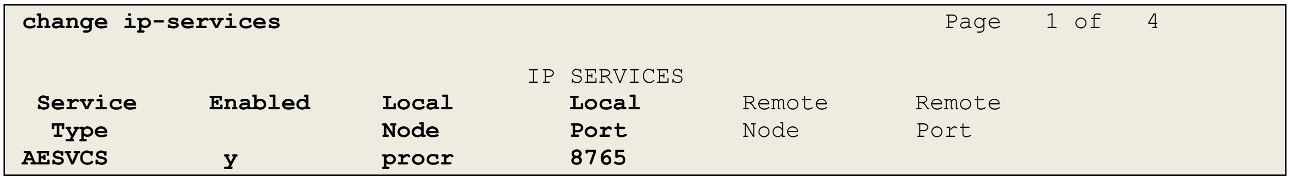
Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes70vmpg**).

```
display node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.40.12
aes70vmpg           10.10.40.16
default             0.0.0.0
G450                10.10.40.15
procr               10.10.40.13
```

5.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 5.2**.
- **Local Port:** Retain the default value of **8765**.

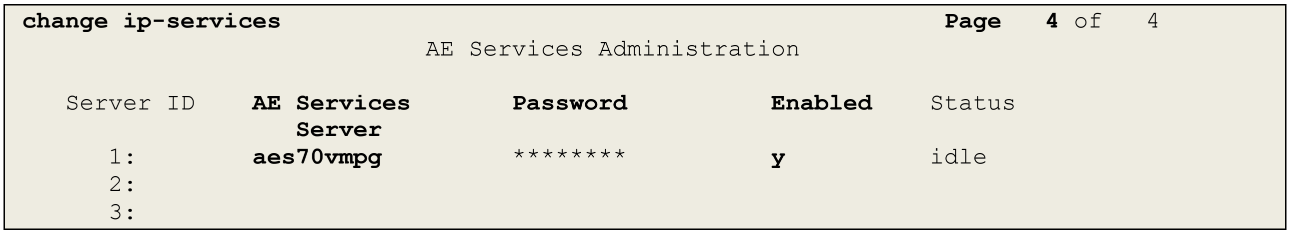


```
change ip-services                                            Page   1 of   4

                                  IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS         y         procr        8765
```

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes70vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

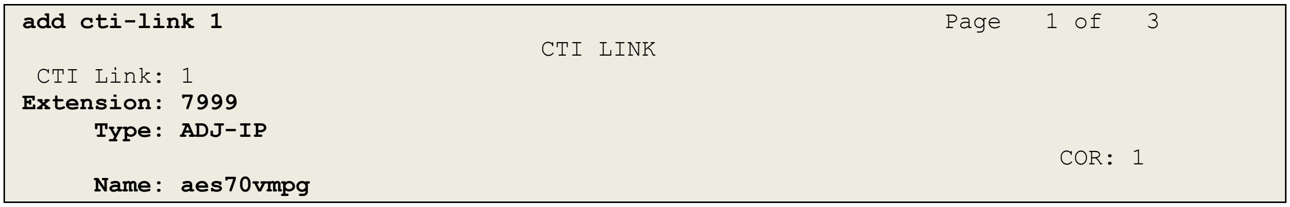
Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** must match the administered name for the AES server; this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.



```
change ip-services                                            Page   4 of   4
                           AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:        aes70vmpg         ********          y          idle
      2:
      3:
```

5.4. Configure CTI Link for TSAPI Service

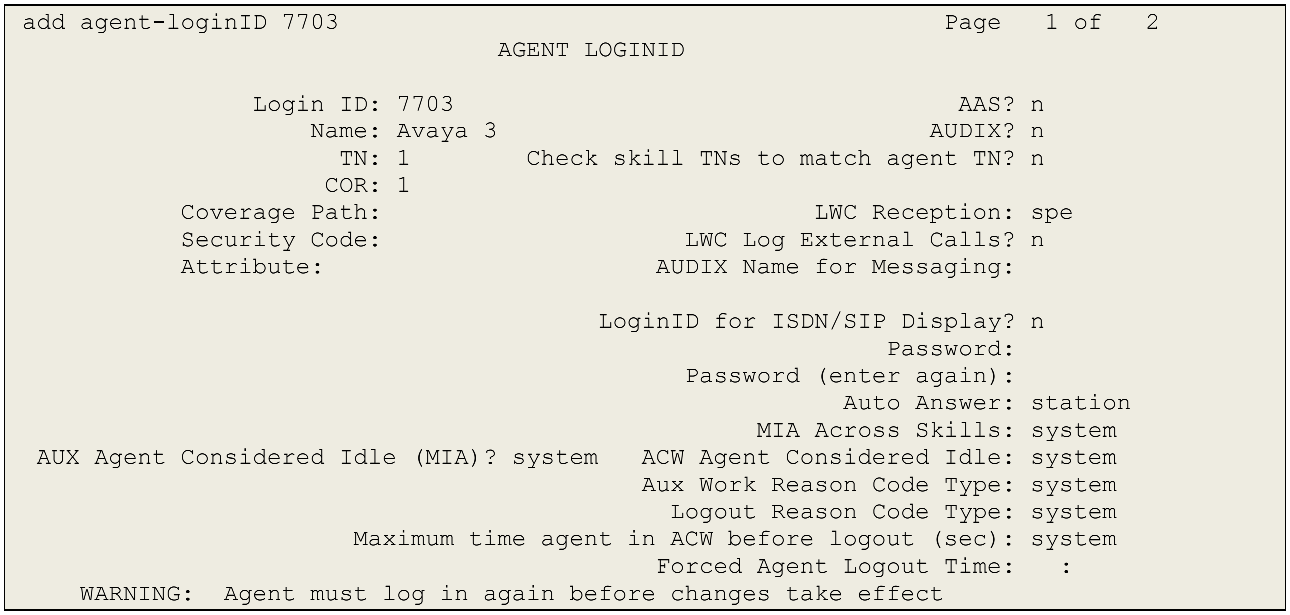
Add a CTI link using the **add cti-link n** command, where n is the n is the cti-link number as shown in the example below this is **1**. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.



```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 7999
     Type: ADJ-IP
                                                                     COR: 1

     Name: aes70vmpg
```

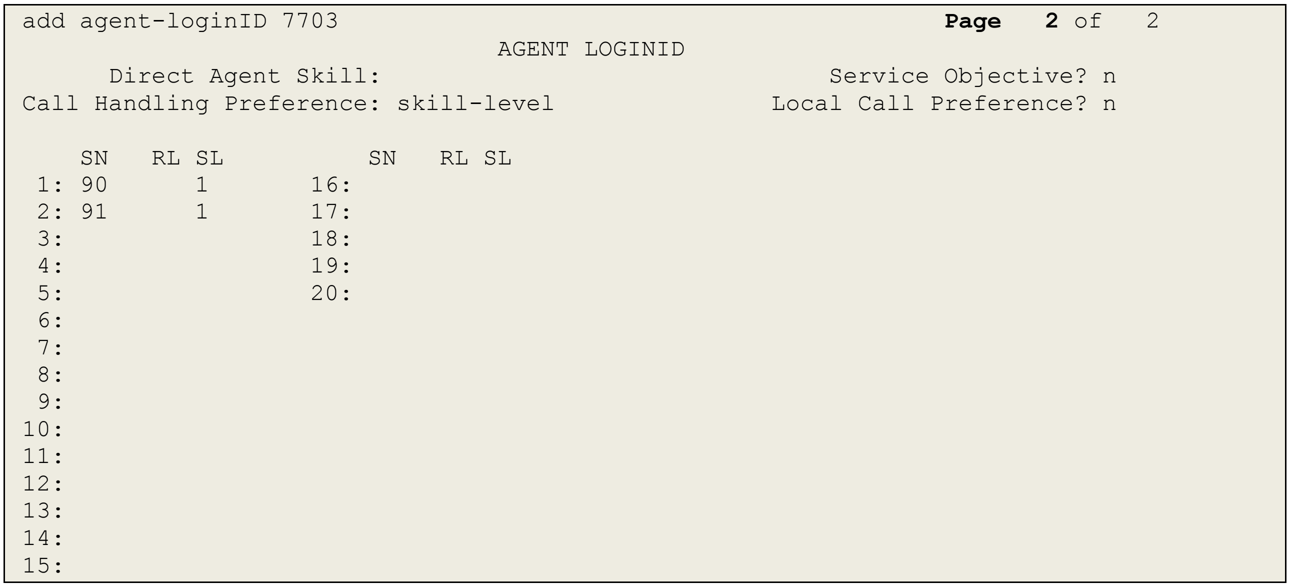
5.5. Add new Agent LoginID

To add a new agent ID type **add agent-LoginID x** where x is the agent's login ID. Enter a suitable **Name** and **Password** these values will be required again in **Section 7.1**.



```
add agent-loginID 7703                                          Page   1 of   2
                                 AGENT LOGINID

                Login ID: 7703                                     AAS? n
                    Name: Avaya 3                                AUDIX? n
                      TN: 1       Check skill TNs to match agent TN? n
                     COR: 1
           Coverage Path:                              LWC Reception: spe
           Security Code:                     LWC Log External Calls? n
           Attribute:                       AUDIX Name for Messaging:

                                        LoginID for ISDN/SIP Display? n
                                                            Password:
                                              Password (enter again):
                                                         Auto Answer: station
                                                   MIA Across Skills: system
 AUX Agent Considered Idle (MIA)? system   ACW Agent Considered Idle: system
                                           Aux Work Reason Code Type: system
                                             Logout Reason Code Type: system
                       Maximum time agent in ACW before logout (sec): system
                                            Forced Agent Logout Time:   :
    WARNING:  Agent must log in again before changes take effect
```

On **Page 2**, add the appropriate skillsets/hunt groups for **SN**.



```
add agent-loginID 7703                                          Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill:                                  Service Objective? n
Call Handling Preference: skill-level                  Local Call Preference? n

    SN   RL SL          SN   RL SL
 1: 90      1       16:
 2: 91      1       17:
 3:                 18:
 4:                 19:
 5:                 20:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
```

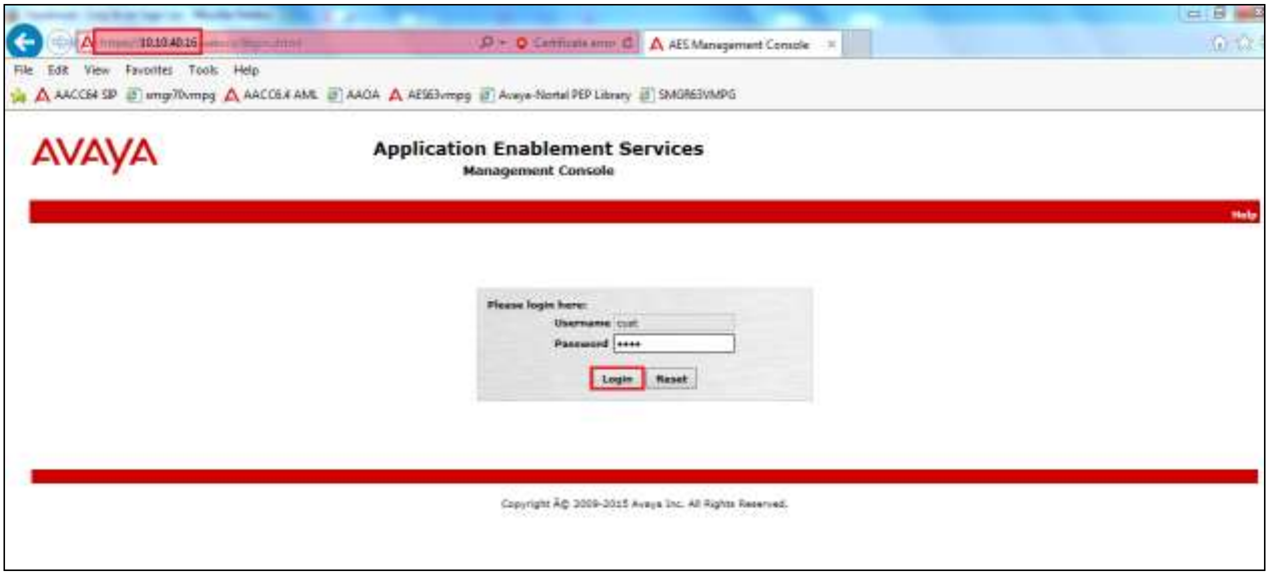
6. Configure Avaya Aura® Application Enablement Services

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

- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI Ports
- Create CTI User
- Associate Devices with CTI User

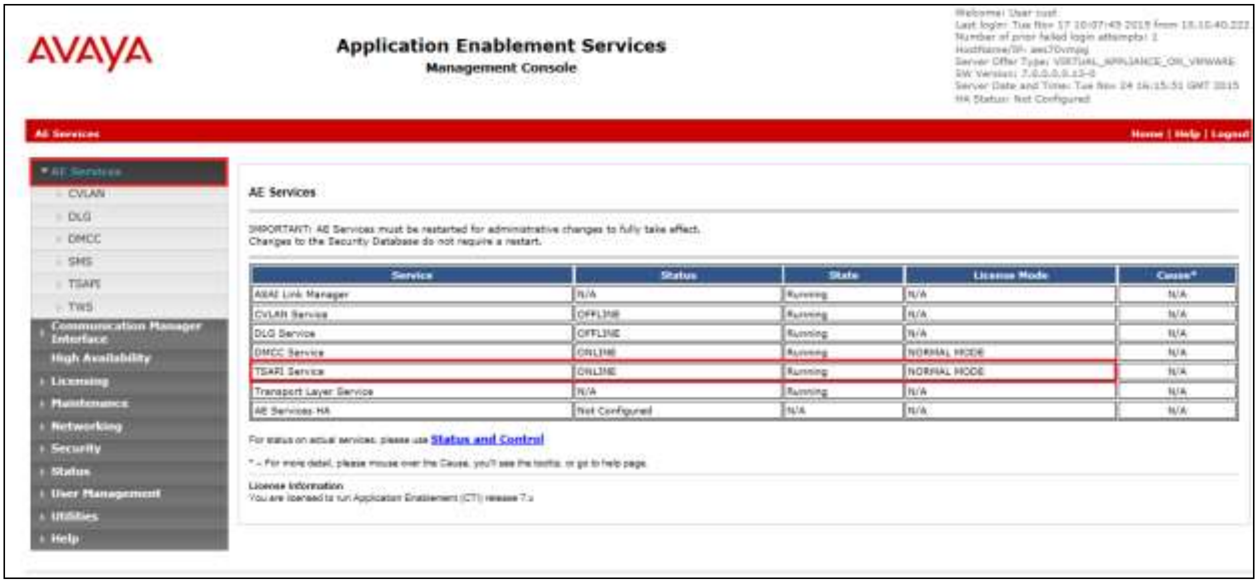
6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, enter the appropriate credentials and then select the **Login** button.



Please login here:
Username cust
Password ****

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license.



AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	OFFLINE	Running	N/A	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A
AE Services HA	Not Configured	N/A	N/A	N/A

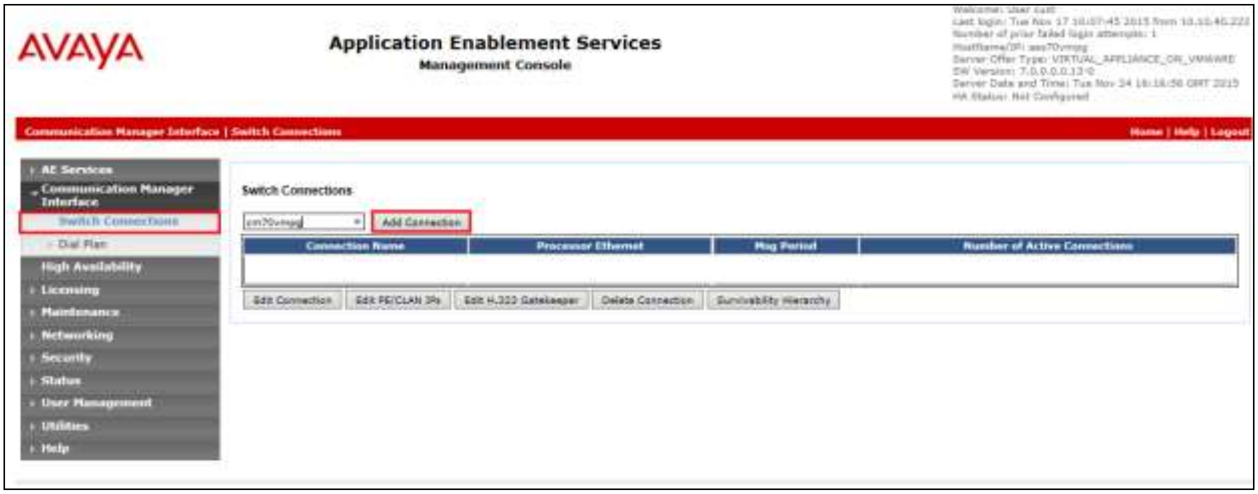
For status on actual services, please use Status and Control

* - For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

License Information
You are licensed to run Application Enablement (CTI) release 7.x

6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface → Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

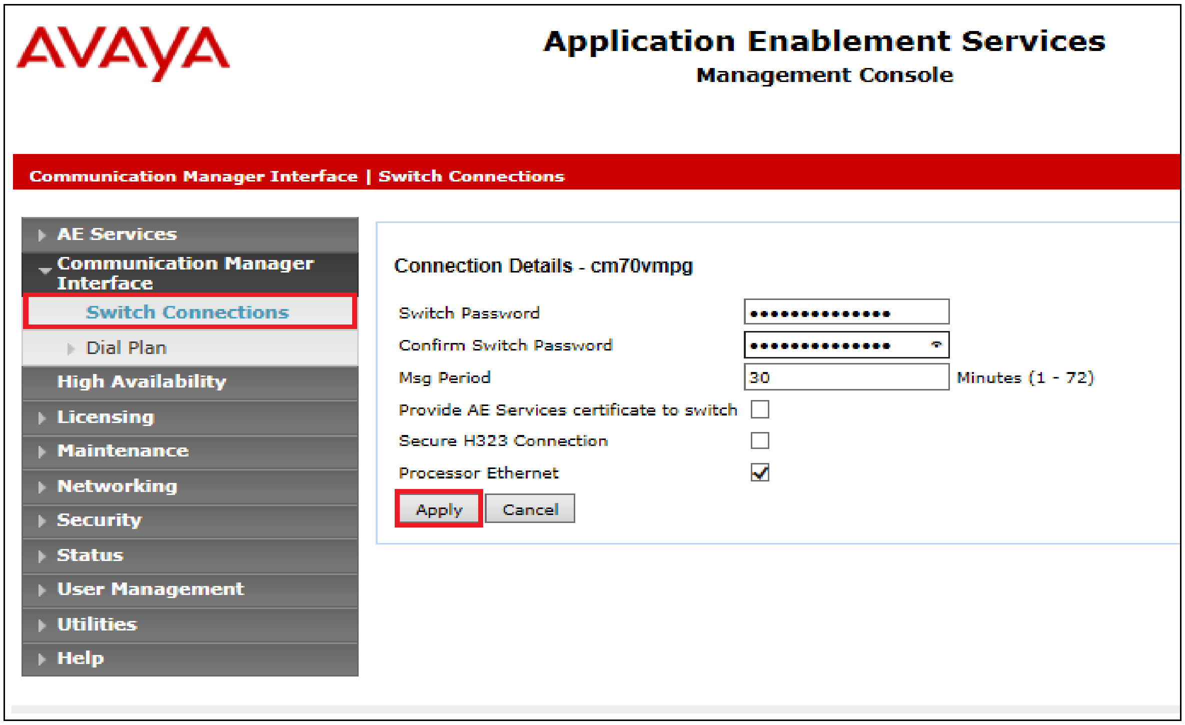


Switch Connections

cm70vmpg

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. The remaining fields should show as below. Click **Apply** to save changes.

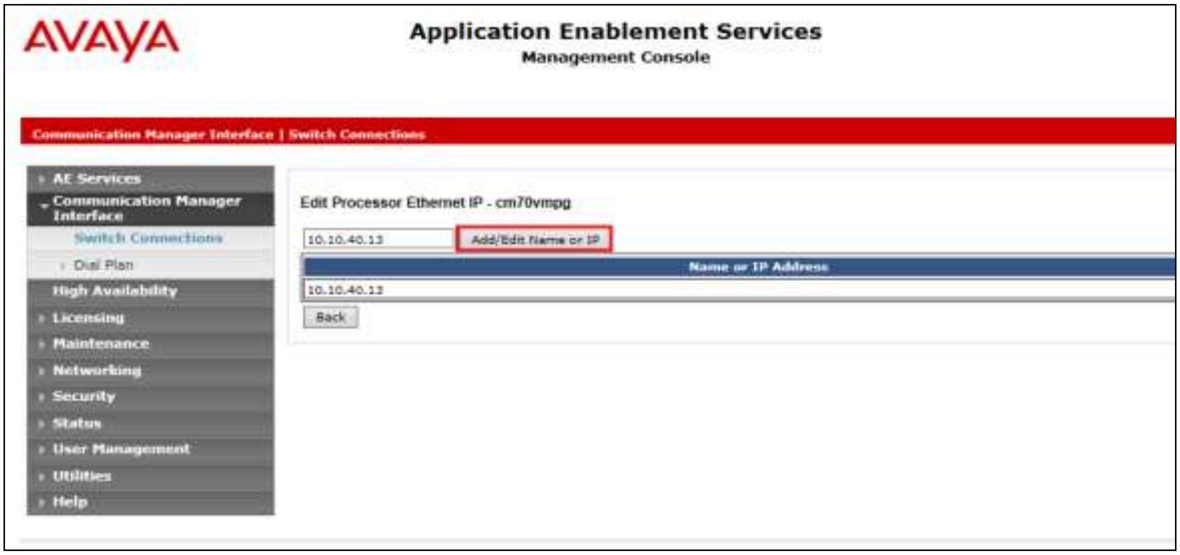


Connection Details - cm70vmpg

Switch Password	••••••••••••••
Confirm Switch Password	••••••••••••••
Msg Period	30 Minutes (1 - 72)
Provide AE Services certificate to switch	□
Secure H323 Connection	□
Processor Ethernet	☑

Apply Cancel

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown, see screen at the bottom of the previous page. In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.



Edit Processor Ethernet IP - cm70vmpg

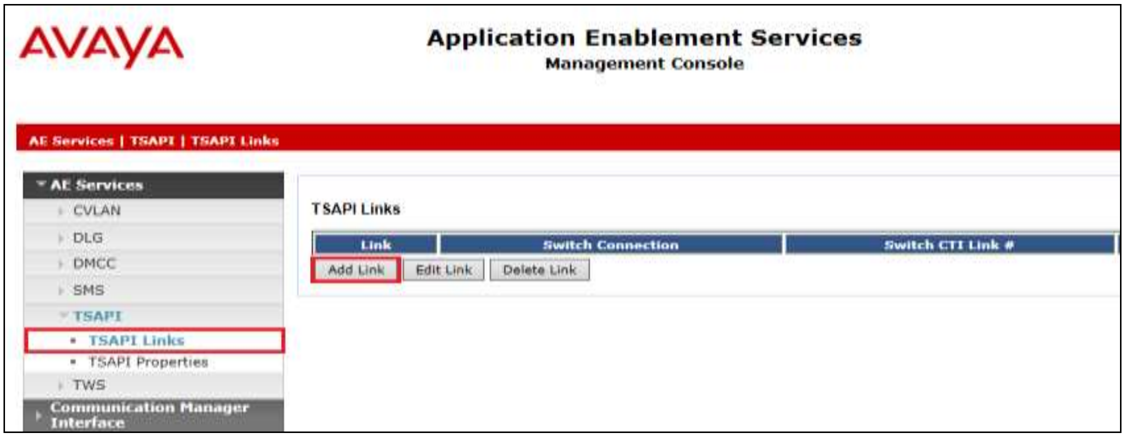
10.10.40.13 Add/Edit Name or IP

Name or IP Address
10.10.40.13

Back

6.3. Administer TSAPI link

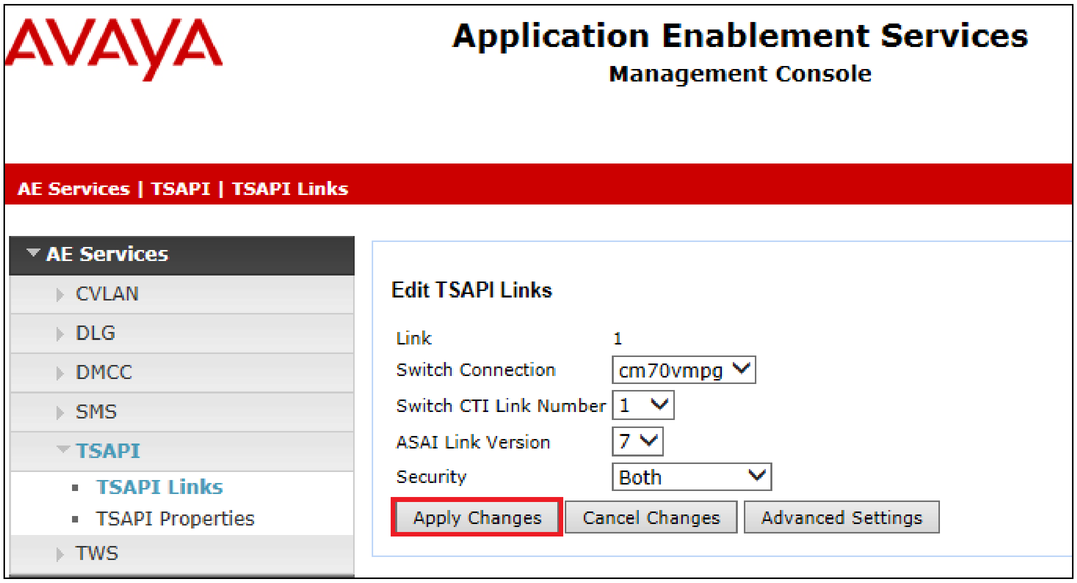
From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm70vmpg**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **7**.
- **Security:** This can be left at the default value of **both**.

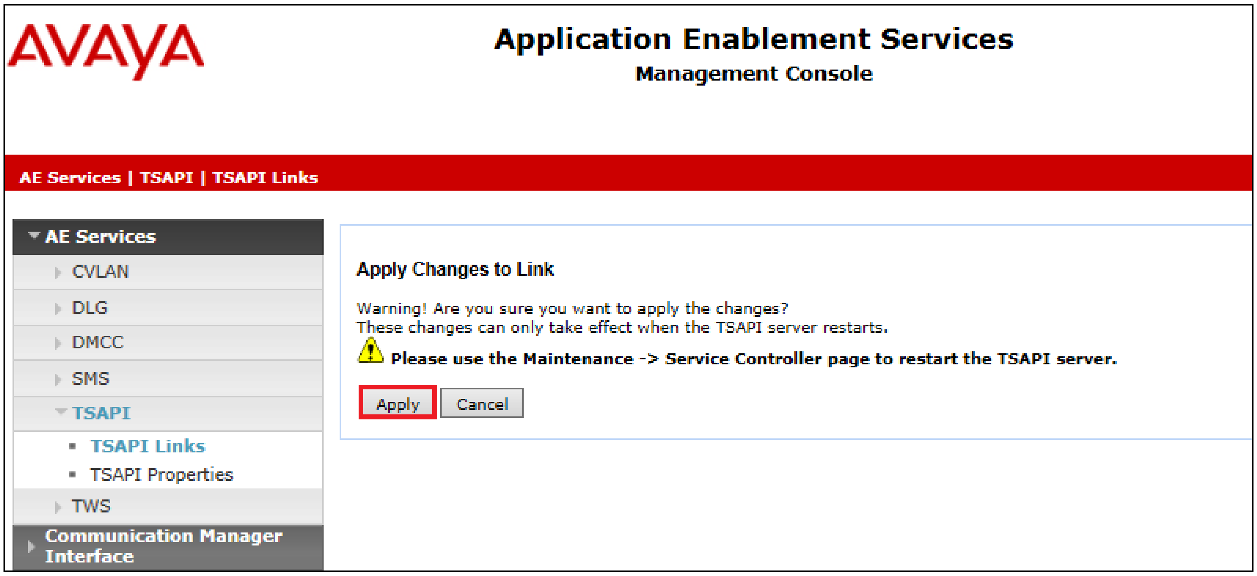
Once completed, select **Apply Changes**.



Edit TSAPI Links

Link	1
Switch Connection	cm70vmpg
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

Another screen appears for confirmation of the changes made. Choose **Apply**.

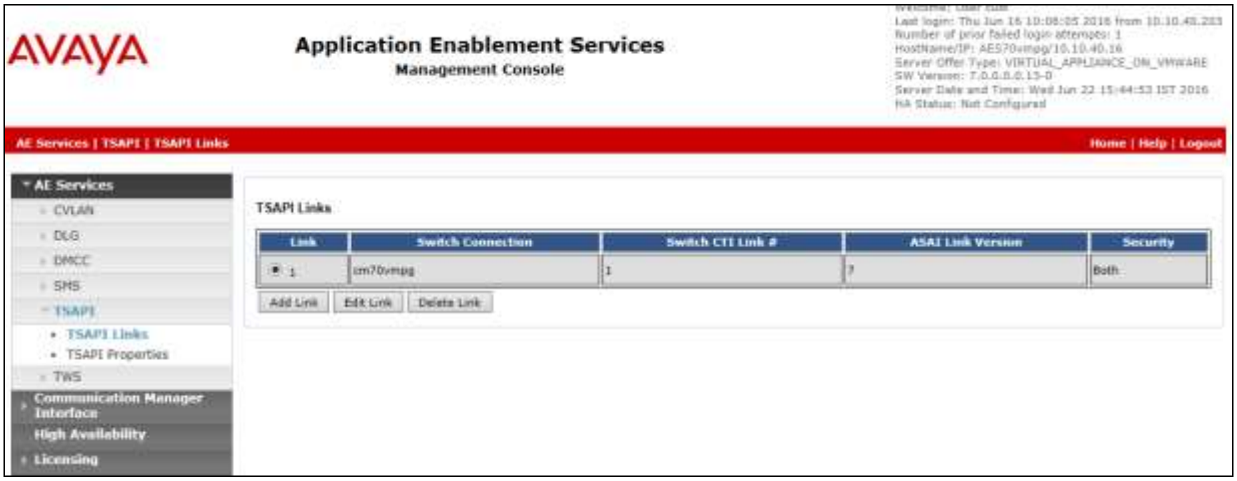


AVAYA
Application Enablement Services
Management Console
AE Services | TSAPI | TSAPI Links
AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TSAPI Links
TSAPI Properties
TWS
Communication Manager Interface

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
⚠ Please use the Maintenance -> Service Controller page to restart the TSAPI server.

When the TSAPI Link is completed, it should resemble the screen below.

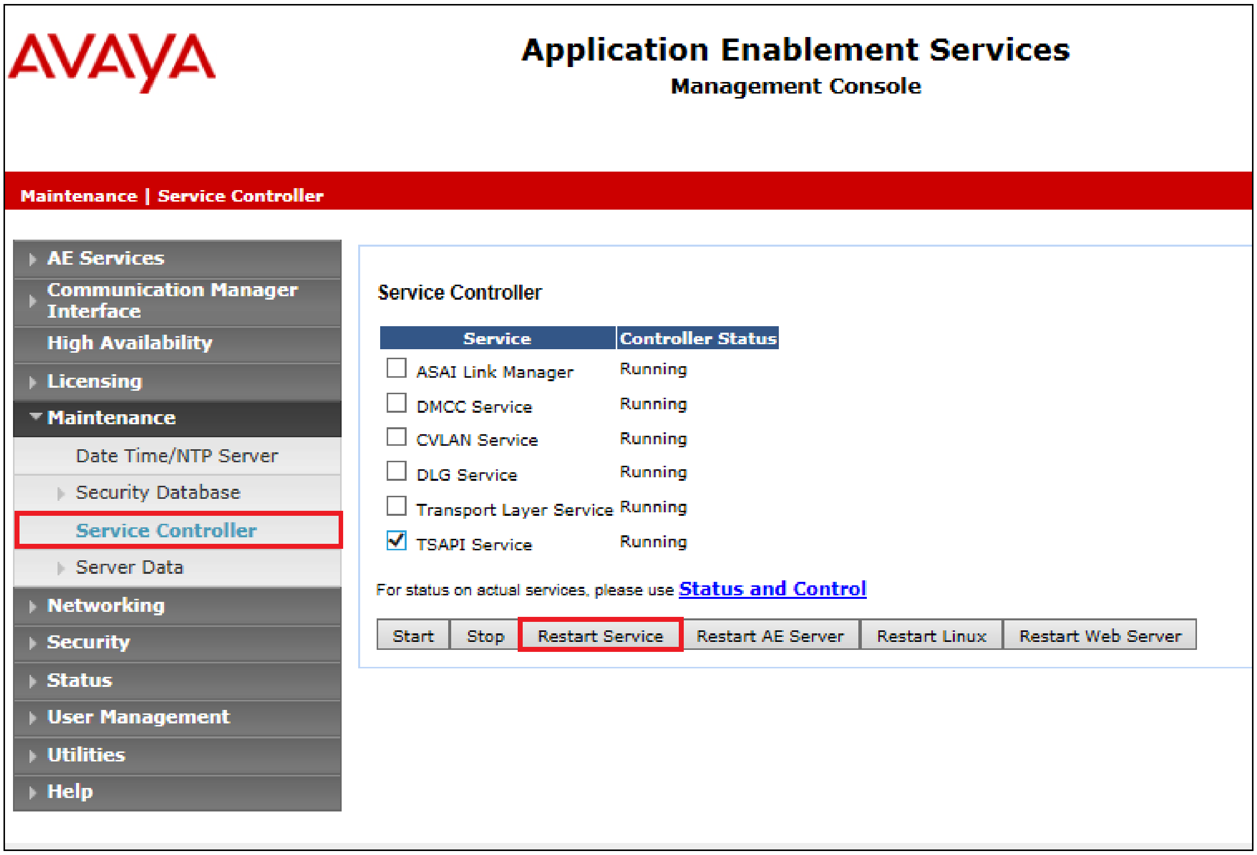


Welcome: User cust
Last login: Thu Jun 16 10:08:05 2016 from 10.10.40.203
Number of prior failed login attempts: 1
HostName/IP: AES70vmpg/10.10.40.16
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-0
Server Date and Time: Wed Jun 22 15:44:53 IST 2016
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	cm70vmpg	1	7	Both

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



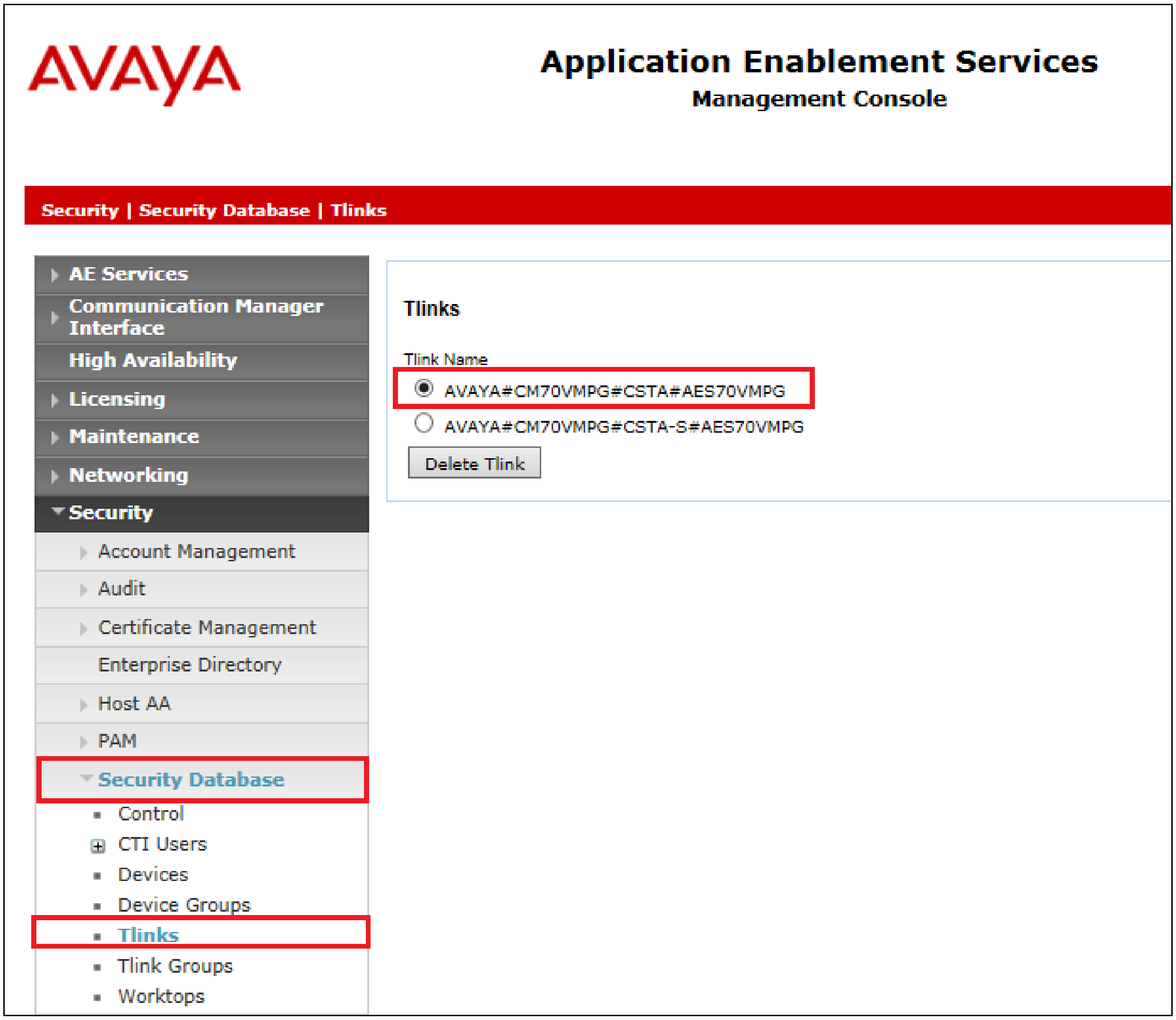
Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.4. Identify Tlinks

Navigate to **Security** → **Security Database** → **Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure Kana Enterprise in **Section 7.4**. Note the insecure link is chosen below, this is because security was not enabled on the link between Kana Enterprise and the AES.



Tlinks

Tlink Name

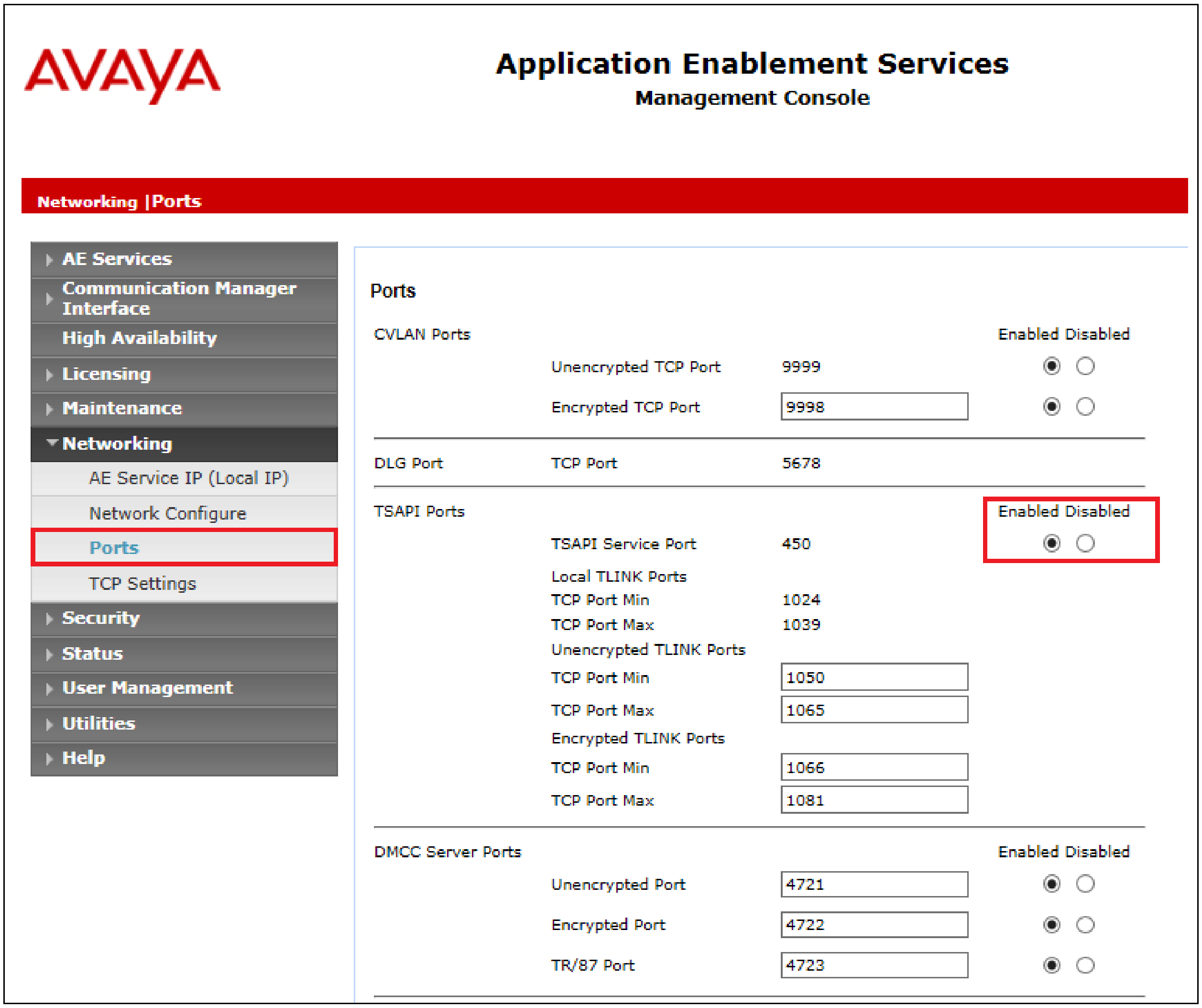
● AVAYA#CM70VMPG#CSTA#AES70VMPG

○ AVAYA#CM70VMPG#CSTA-S#AES70VMPG

Delete Tlink

6.5. Enable TSAPI and DMCC Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below.

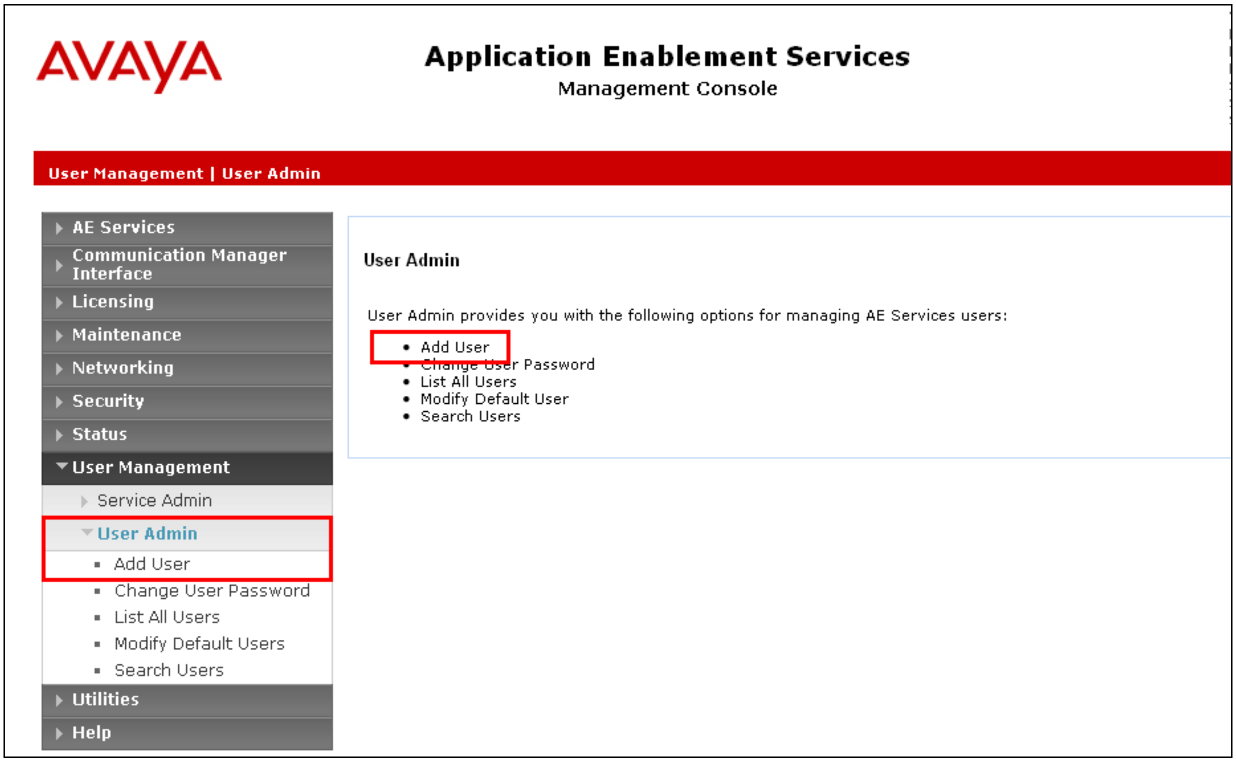


Ports

			Enabled	Disabled
CVLAN Ports			Enabled	Disabled
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports			Enabled	Disabled
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports			Enabled	Disabled
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	●	○

6.6. Create CTI User

A User ID and password needs to be configured for the Kana Enterprise to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



User Admin

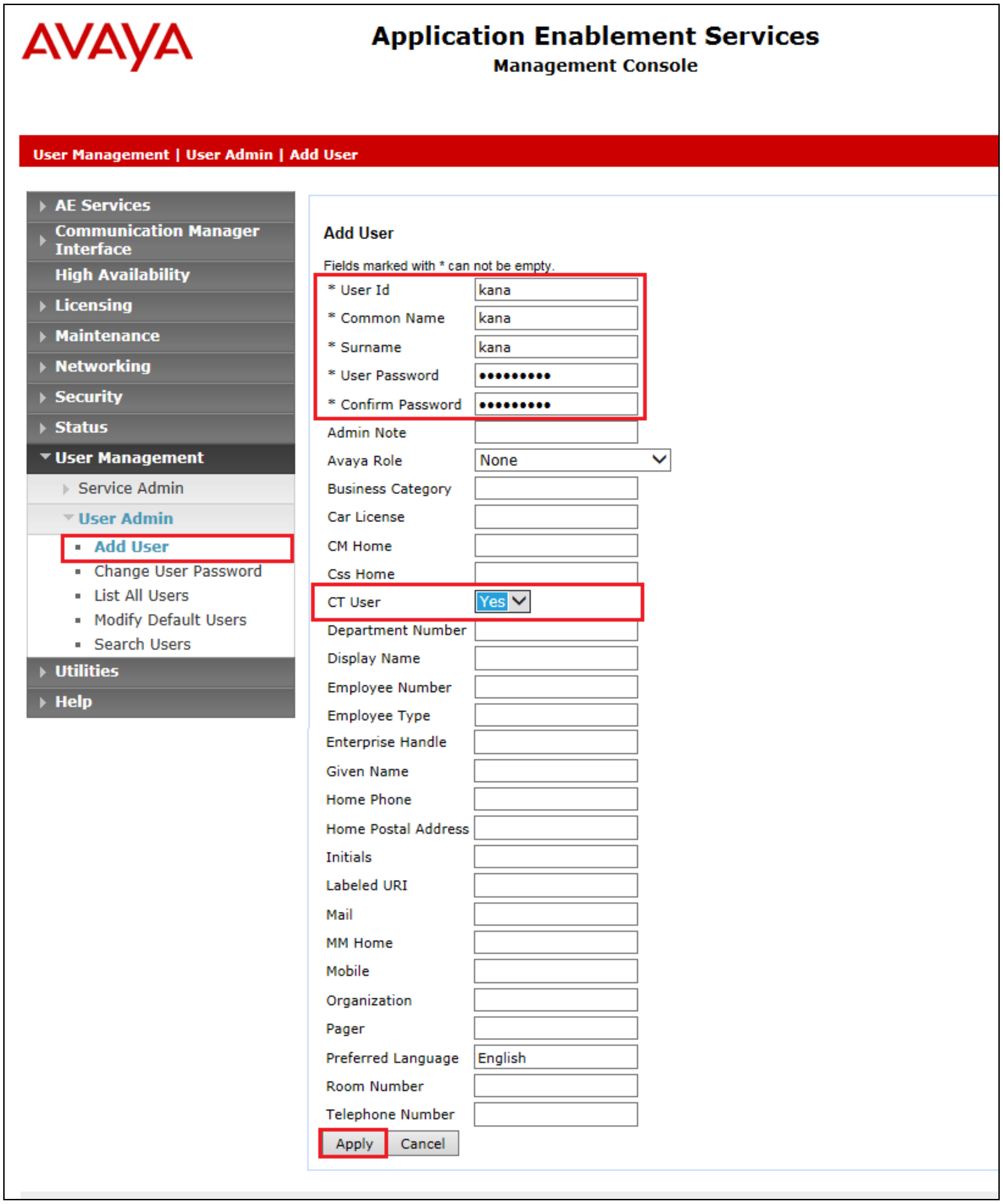
User Admin provides you with the following options for managing AE Services users:

- Add User
- Change User Password
- List All Users
- Modify Default User
- Search Users

In the **Add User** screen shown below, enter the following values:

- **User Id -** This will be used by the Kana Enterprise setup in **Section 7.4**.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with Kana Enterprise setup in **Section 7.4**.
- **CT User -** Select **Yes** from the drop-down menu.

Click on **Apply Changes** at the bottom of the screen.



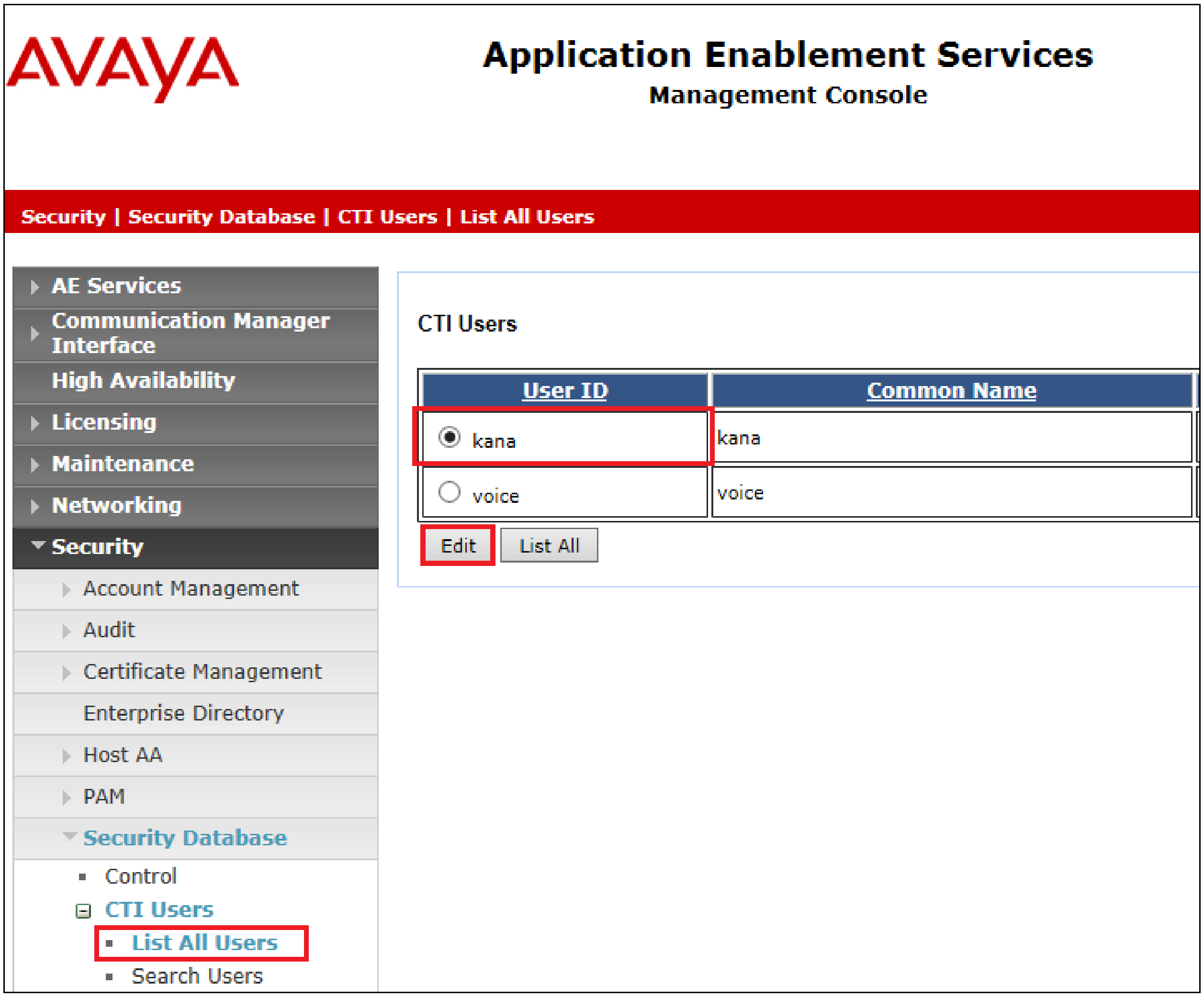
Add User

Fields marked with * can not be empty.

* User Id	kana
* Common Name	kana
* Surname	kana
* User Password	•••••••••
* Confirm Password	•••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	
Mail	
MM Home	
Mobile	
Organization	
Pager	
Preferred Language	English
Room Number	
Telephone Number	

6.7. Associate Devices with CTI User

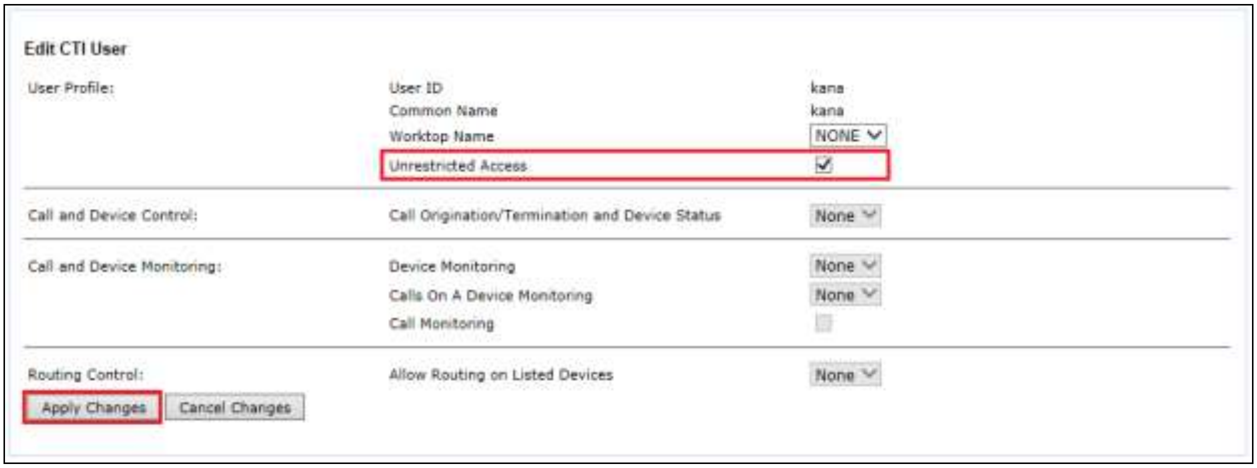
Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit**.



CTI Users

User ID	Common Name
● kana	kana
○ voice	voice

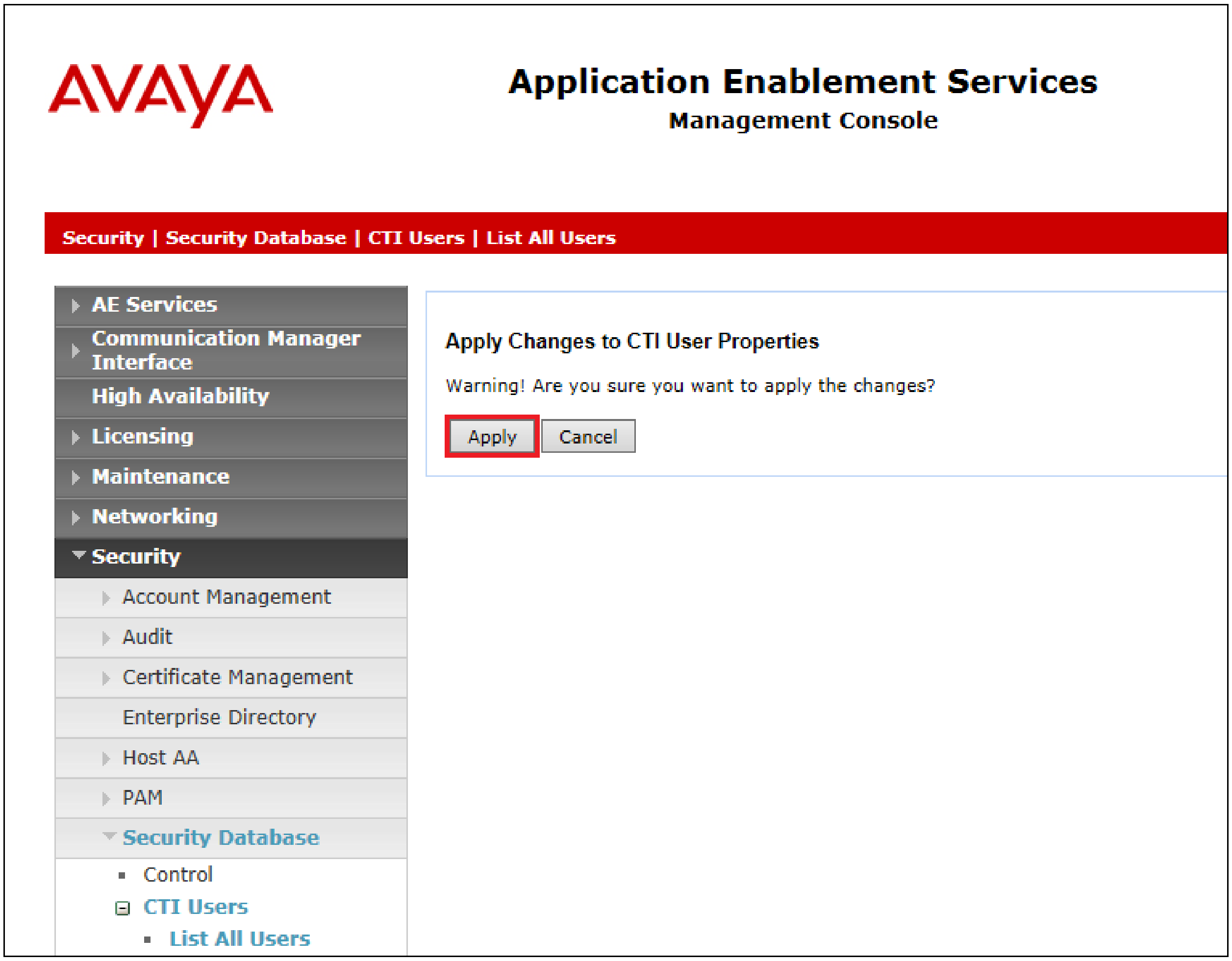
In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.



Edit CTI User

User Profile:	User ID	kana
	Common Name	kana
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	□
Routing Control:	Allow Routing on Listed Devices	None

Click on **Apply** when asked again to **Apply Changes**.



Application Enablement Services
Management Console

Security | Security Database | CTI Users | List All Users

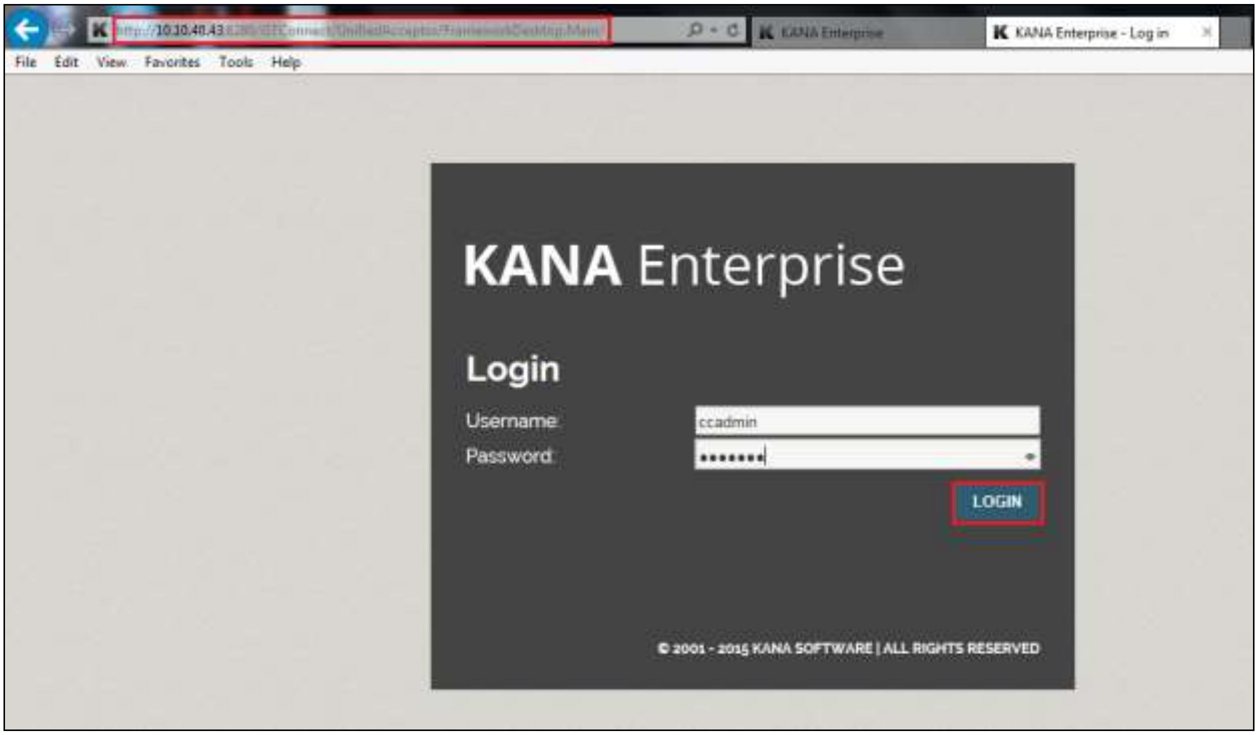
Apply Changes to CTI User Properties

Warning! Are you sure you want to apply the changes?

7. Configure Kana Enterprise

The installation of Kana Enterprise is typically carried out by a Verint certified engineer and is outside the scope of these Application Notes. For information on the installation of Kana Enterprise contact Verint as per the information provided in **Section 2.3**.

The following sections will outline the process involved in connecting Kana Enterprise to the Avaya solution. All configuration of Kana Enterprise for connection with the AES is performed using by opening a web session to **http://<KanaEnterpriseServer>:8280/GTConnect/UnifiedAcceptor/FrameworkDesktop.Main/**. Enter the proper credentials and click on **LOGIN**.


http://10.10.40.43:8280/GTConnect/UnifiedAcceptor/FrameworkDesktop.Main
KANA Enterprise
KANA Enterprise - Log in
File Edit View Favorites Tools Help
KANA Enterprise
Login

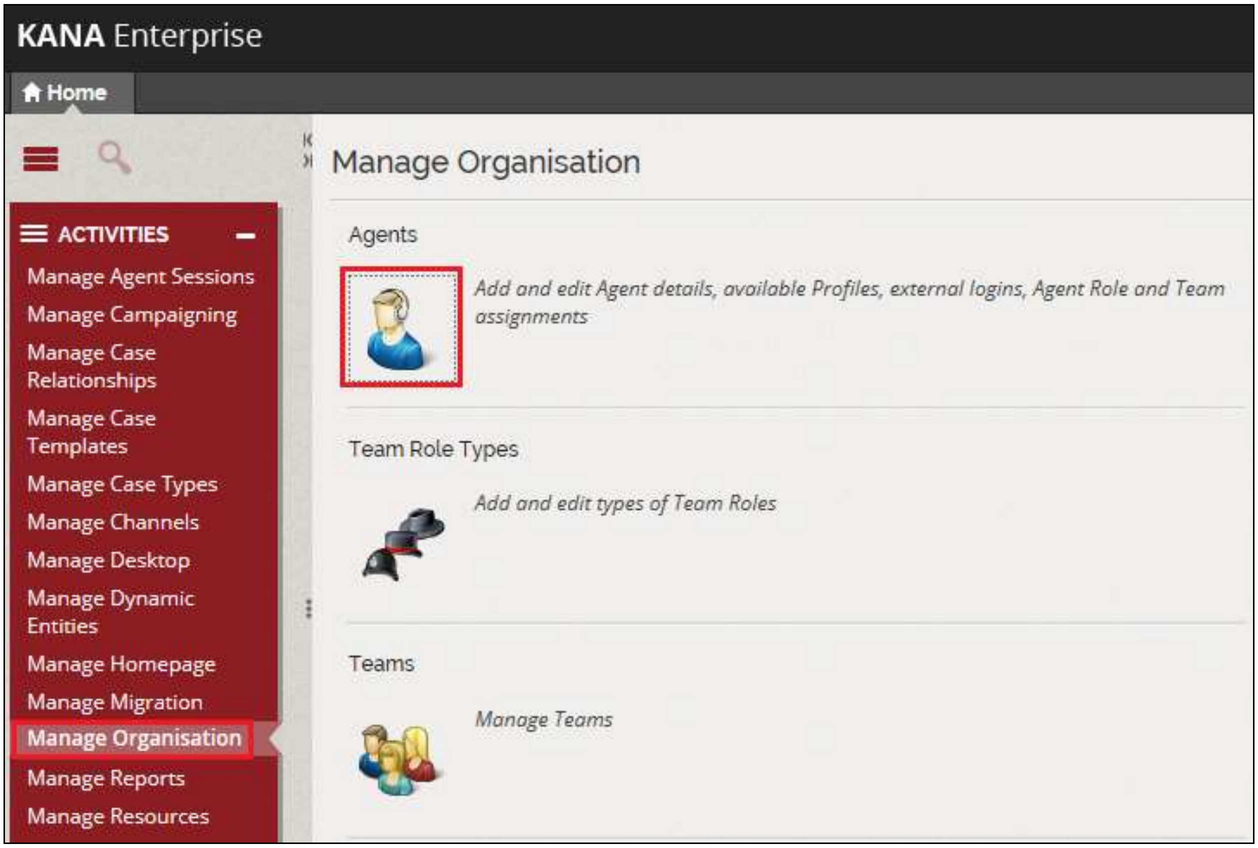
Username: ccadmin

Password: •••••••

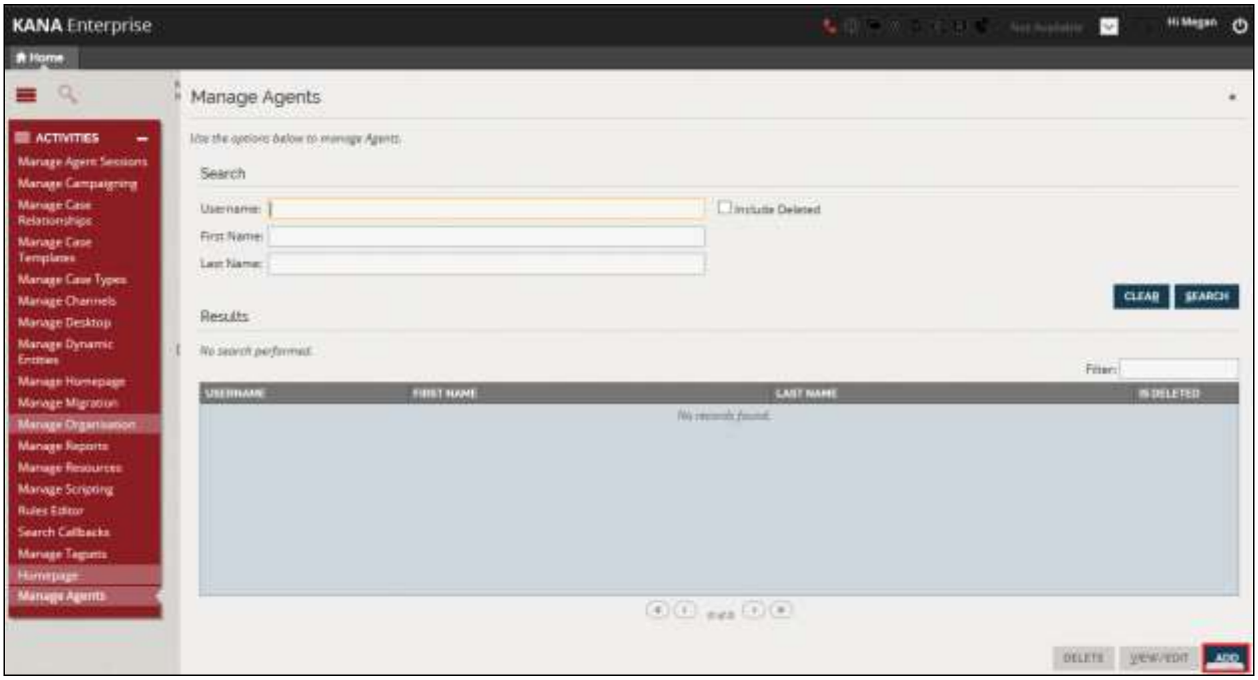
LOGIN
© 2001 - 2015 KANA SOFTWARE | ALL RIGHTS RESERVED

7.1. Manage Agents

Select **Manage Organisation** in the left tab and **Agents** in the main window.



Select **ADD** at the bottom right of the screen.



Manage Agents

Use the options below to manage Agents.

Search

Username:

□ Include Deleted

First Name:

Last Name:

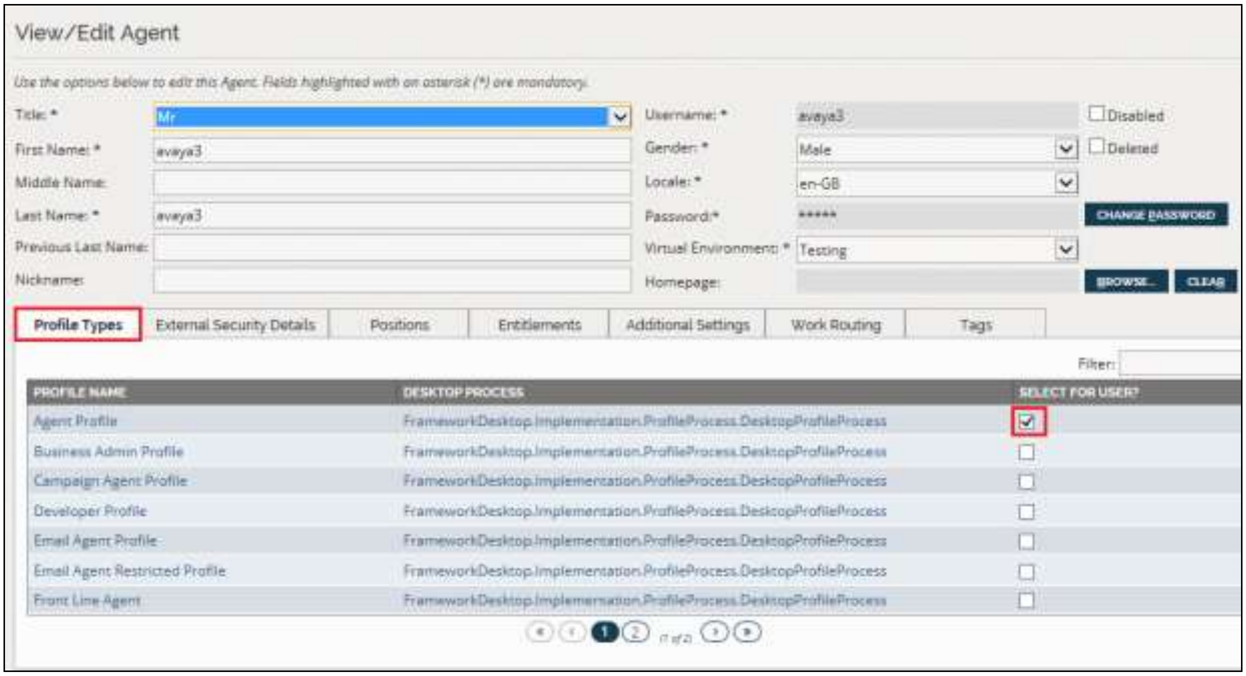
Results

No search performed.

Filter:

USERNAME	FIRST NAME	LAST NAME	IS DELETED
No records found.			

Enter the agent’s details such as name, password and click on the **Profile Types** tab and select the appropriate **Agent Profile** – the exact profile type may vary depending on the customer site.



View/Edit Agent

Use the options below to edit this Agent. Fields highlighted with an asterisk (*) are mandatory.

Title: * Mr

First Name: * avaya3

Middle Name:

Last Name: * avaya3

Previous Last Name:

Nickname:

Username: * avaya3

□ Disabled

Gender: * Male

□ Deleted

Locale: * en-GB

Password:* *****

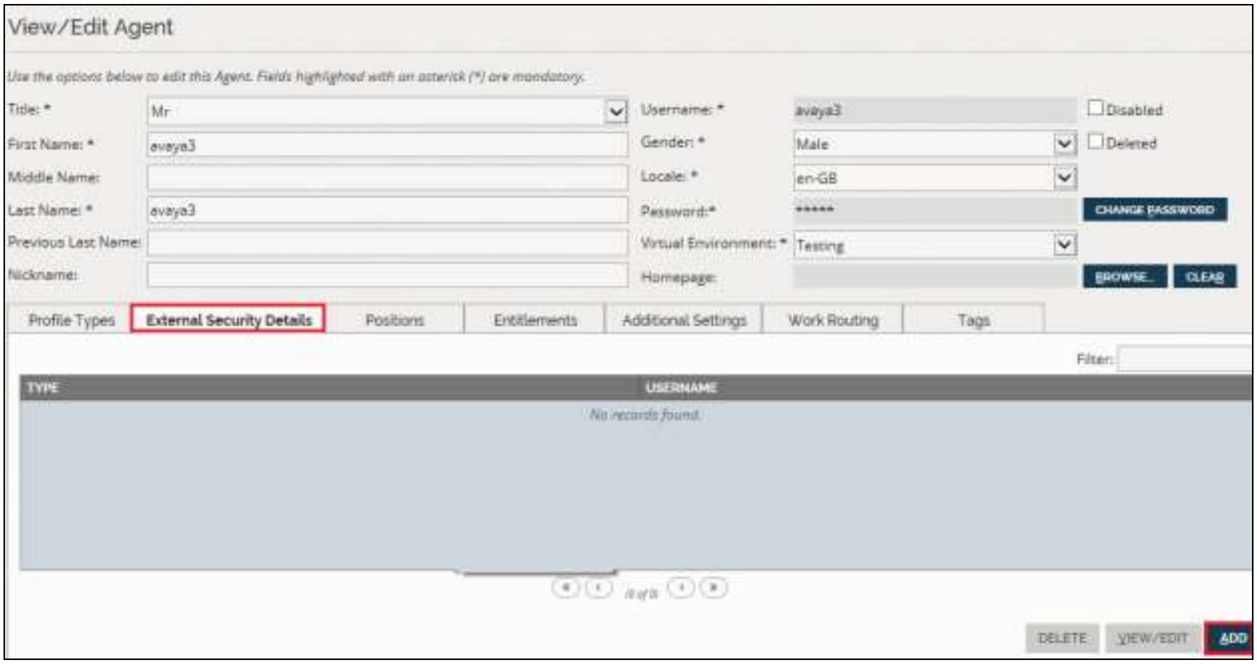
Virtual Environment: * Testing

Homepage:

Filter:

PROFILE NAME	DESKTOP PROCESS	SELECT FOR USER?
Agent Profile	FrameworkDesktop.Implementation.ProfileProcess.DesktopProfileProcess	☑
Business Admin Profile	FrameworkDesktop.Implementation.ProfileProcess.DesktopProfileProcess	□
Campaign Agent Profile	FrameworkDesktop.Implementation.ProfileProcess.DesktopProfileProcess	□
Developer Profile	FrameworkDesktop.Implementation.ProfileProcess.DesktopProfileProcess	□
Email Agent Profile	FrameworkDesktop.Implementation.ProfileProcess.DesktopProfileProcess	□
Email Agent Restricted Profile	FrameworkDesktop.Implementation.ProfileProcess.DesktopProfileProcess	□
Front Line Agent	FrameworkDesktop.Implementation.ProfileProcess.DesktopProfileProcess	□

Click on the **External Security Details** tab and click on **ADD** at the bottom right of the screen.



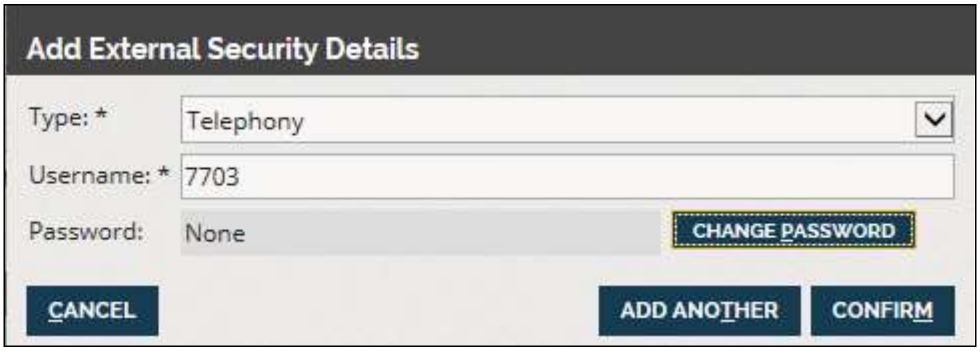
View/Edit Agent

Use the options below to edit this Agent. Fields highlighted with an asterisk (*) are mandatory.

Title: *	Mr	Username: *	avaya3	□ Disabled
First Name: *	avaya3	Gender: *	Male	□ Deleted
Middle Name:		Locale: *	en-GB	
Last Name: *	avaya3	Password:*	*****	CHANGE PASSWORD
Previous Last Name:		Virtual Environment: *	Testing	
Nickname:		Homepage:		BROWSE... CLEAR

TYPE	USERNAME
	No records found.

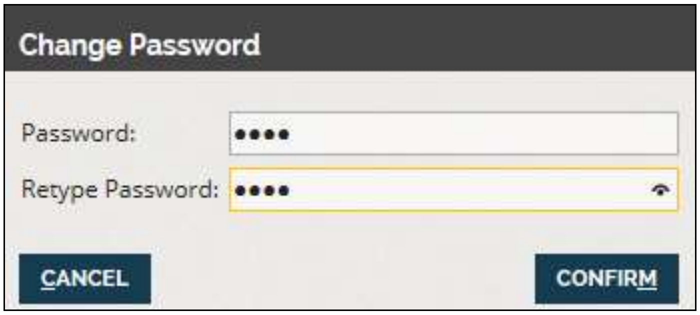
Type should be set to **Telephony** and the **Username** will be the agent ID that was setup in **Section 5.5**. Click on **CHANGE PASSWORD** once finished.



Add External Security Details

Type: *	Telephony
Username: *	7703
Password:	None

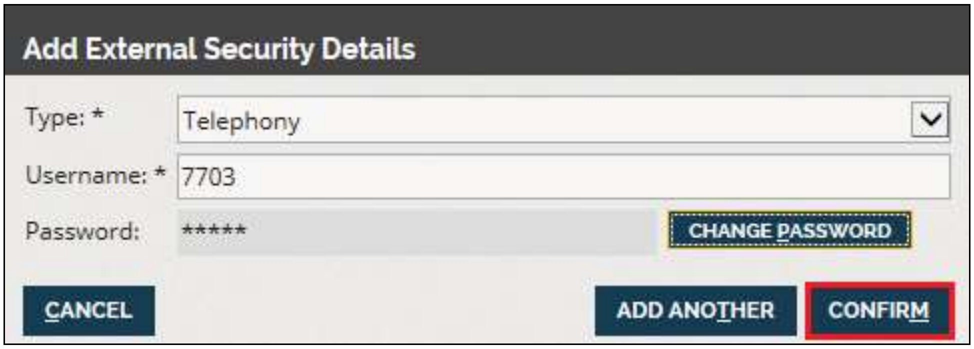
Enter the Agents password as per **Section 5.5**.



Change Password

Password:	••••
Retype Password:	••••

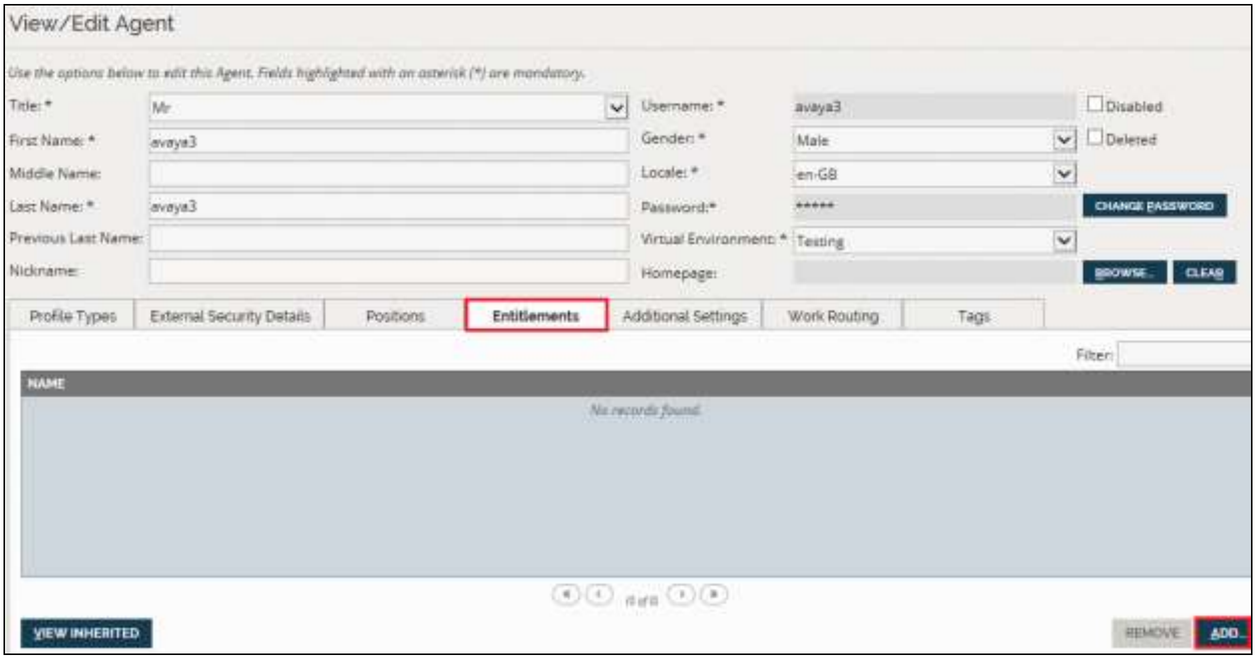
Click on **CONFIRM** once this is completed to save the **Security Details**.



Add External Security Details

Type: *	Telephony
Username: *	7703
Password:	*****

Click on the **Entitlements** tab and click on **ADD** at the bottom right of the screen.



View/Edit Agent

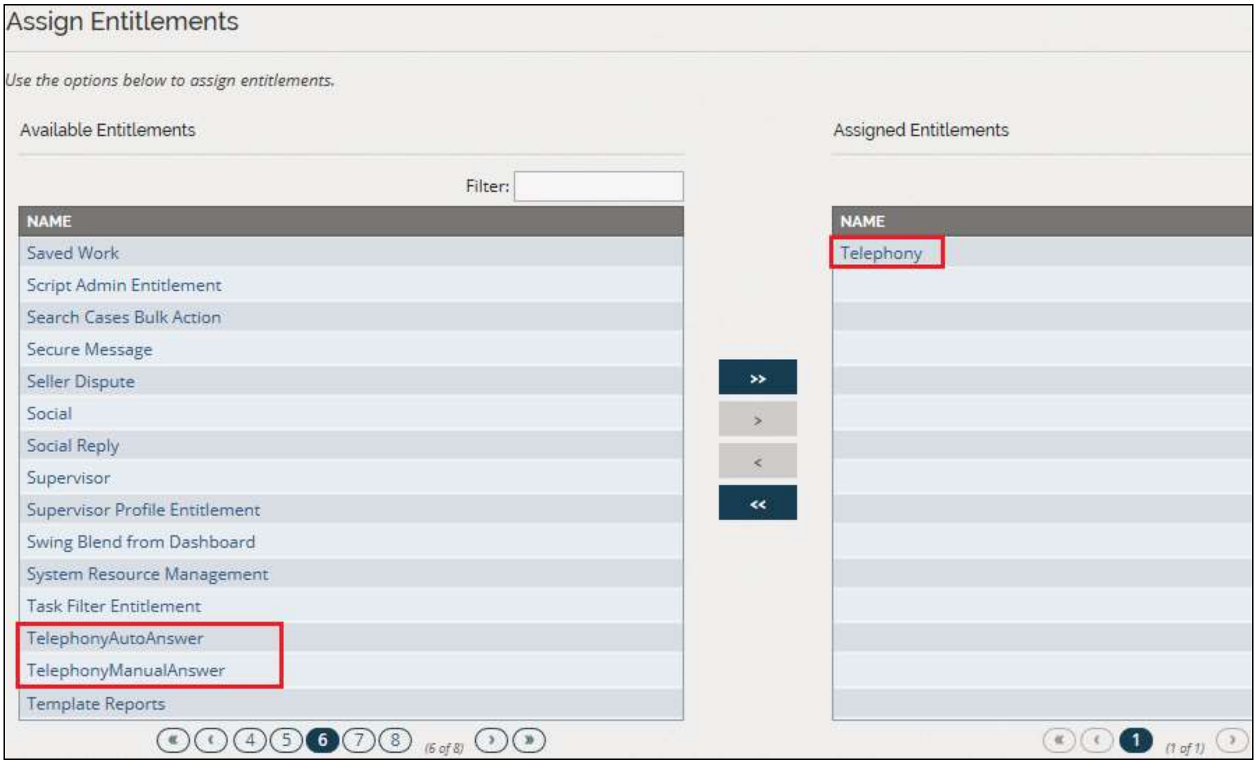
Use the options below to edit this Agent. Fields highlighted with an asterisk (*) are mandatory.

Title: *	Mr	Username: *	avaya3
First Name: *	avaya3	Gender: *	Male
Middle Name:		Locale: *	en-GB
Last Name: *	avaya3	Password:*	*****
Previous Last Name:		Virtual Environment: *	Testing
Nickname:		Homepage:	

☐ Disabled
☐ Deleted

NAME
No records found.

The **Telephony** Entitlement must be selected as shown below. Either **TelephonyAutoAnswer** or **TelephonyManualAnswer** can also be selected depending on whether Kana Enterprise will answer the call automatically or if it will send a pop up answer button to allow the agent manually answer the call.



Assign Entitlements

Use the options below to assign entitlements.

Available Entitlements

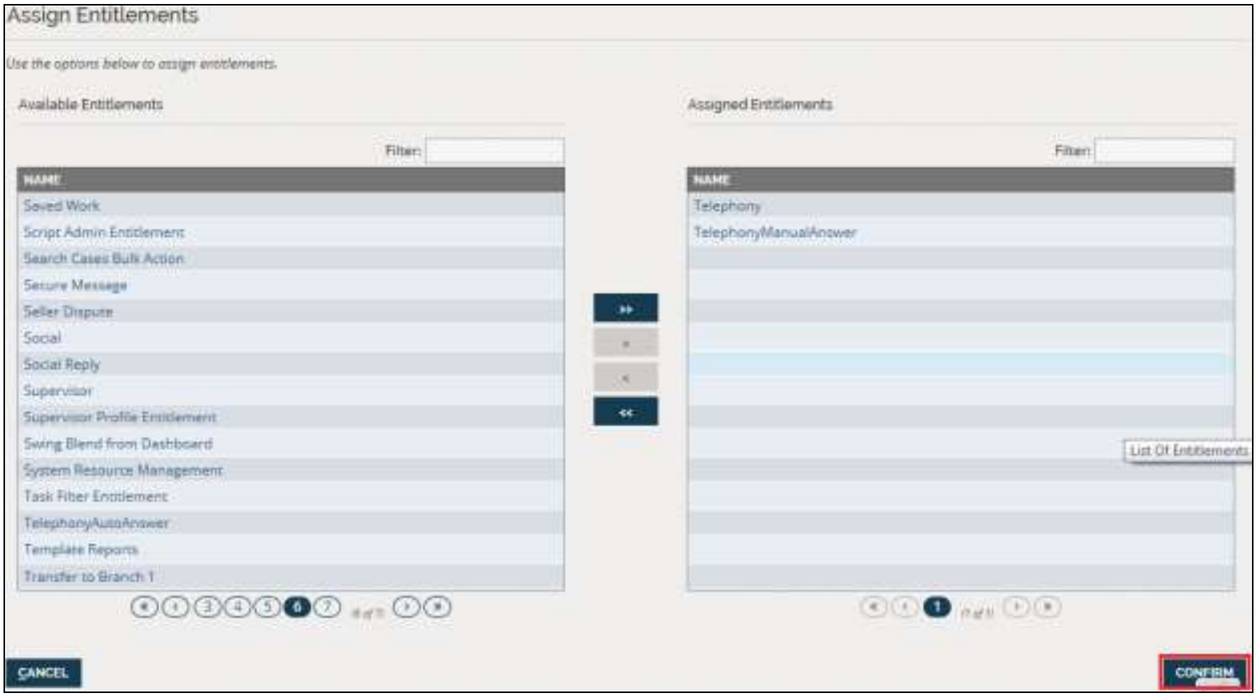
Filter:

NAME
Saved Work
Script Admin Entitlement
Search Cases Bulk Action
Secure Message
Seller Dispute
Social
Social Reply
Supervisor
Supervisor Profile Entitlement
Swing Blend from Dashboard
System Resource Management
Task Filter Entitlement
TelephonyAutoAnswer
TelephonyManualAnswer
Template Reports

Assigned Entitlements

NAME
Telephony

The **Telephony** and **TelephonyManualAnswer** entitlements are selected and click on **CONFIRM** at the bottom right of the screen.



Assign Entitlements

Use the options below to assign entitlements.

Available Entitlements

Filter:

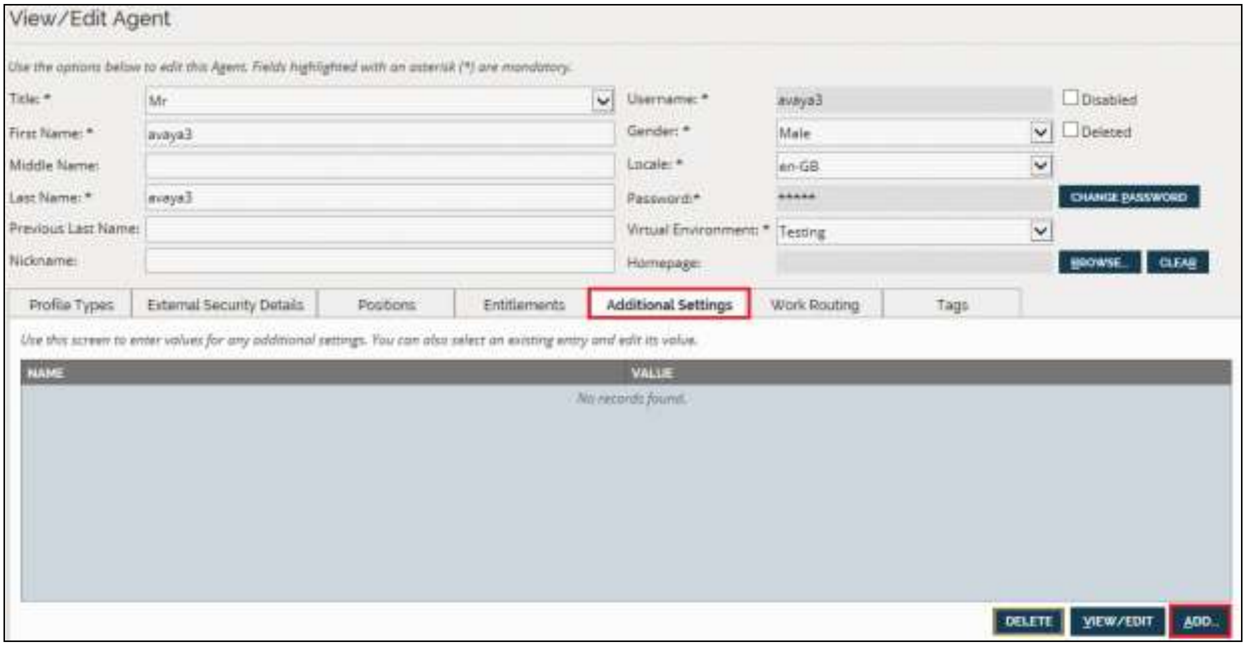
NAME
Saved Work
Script Admin Entitlement
Search Cases Bulk Action
Secure Message
Seller Dispute
Social
Social Reply
Supervisor
Supervisor Profile Entitlement
Swing Blend from Dashboard
System Resource Management
Task Filter Entitlement
TelephonyAutoAnswer
Template Reports
Transfer to Branch 1

Assigned Entitlements

Filter:

NAME
Telephony
TelephonyManualAnswer

Click on the **Additional Settings** tab and **ADD** at the bottom right of the screen.



View/Edit Agent

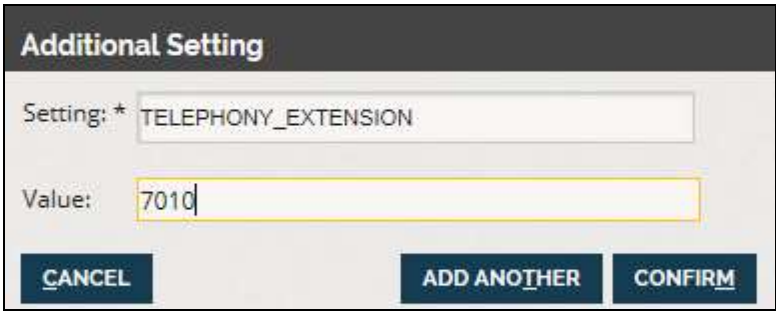
Use the options below to edit this Agent. Fields highlighted with an asterisk (*) are mandatory.

Title: *	Mr	Username: *	avaya3	□ Disabled
First Name: *	avaya3	Gender: *	Male	□ Deleted
Middle Name:		Locale: *	en-GB	
Last Name: *	avaya3	Password:*	*****	CHANGE PASSWORD
Previous Last Name:		Virtual Environment: *	Testing	
Nickname:		Homepage:		BROWSE... CLEAR

Use this screen to enter values for any additional settings. You can also select an existing entry and edit its value.

NAME	VALUE
No records found.	

Enter the extension number associated with the agent. This is the Communication Manager station that this agent will be logging in to. Click on **CONFIRM** once this is completed.

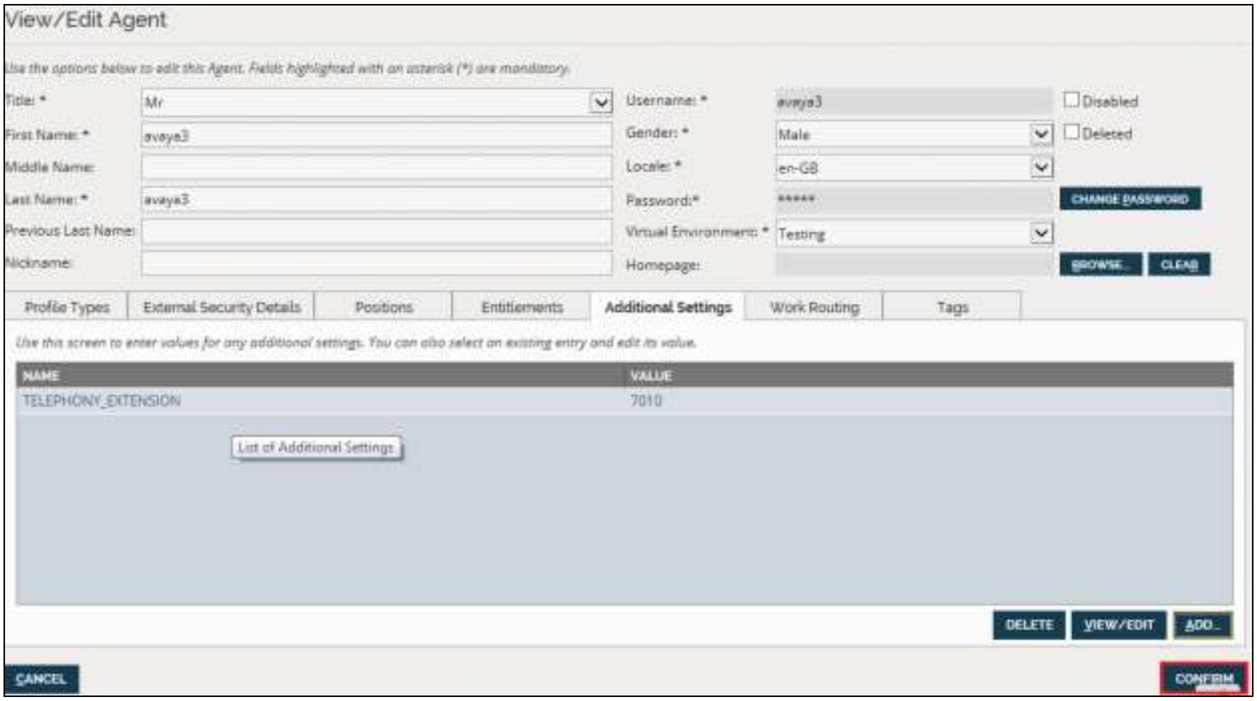


Additional Setting

Setting: * TELEPHONY_EXTENSION

Value: 7010

Click on **CONFIRM** at the bottom of the screen to compete the agent setup.



View/Edit Agent

Use the options below to edit this Agent. Fields highlighted with an asterisk (*) are mandatory.

Title: * Mr

First Name: * avaya3

Middle Name:

Last Name: * avaya3

Previous Last Name:

Nickname:

Username: * avaya3

Gender: * Male

Locale: * en-GB

Password:* *****

Virtual Environment: * Testing

Homepage:

□ Disabled

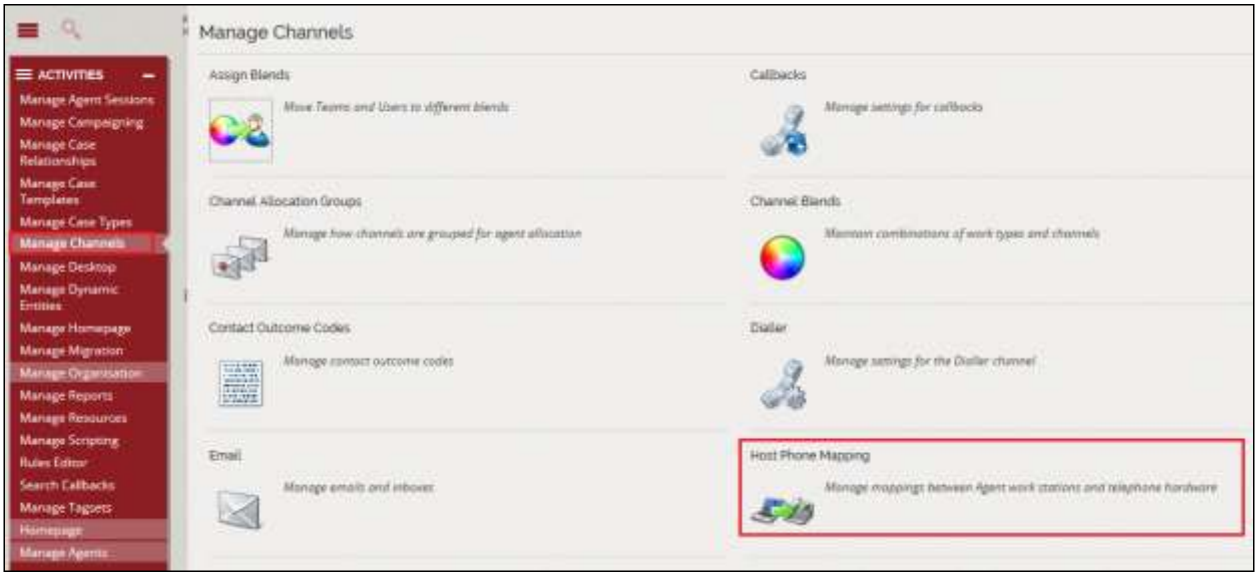
□ Deleted

Use this screen to enter values for any additional settings. You can also select an existing entry and edit its value.

NAME	VALUE
TELEPHONY_EXTENSION	7010

7.2. Host Phone Mapping

Click on **Manage Channels** in the left window and **Host Phone Mapping** in the main window.



Manage Channels

Assign Blends

Move Teams and Users to different blends

Callbacks

Manage settings for callbacks

Channel Allocation Groups

Manage how channels are grouped for agent allocation

Channel Blends

Maintain combinations of work types and channels

Contact Outcome Codes

Manage contact outcome codes

Dialler

Manage settings for the Dialler channel

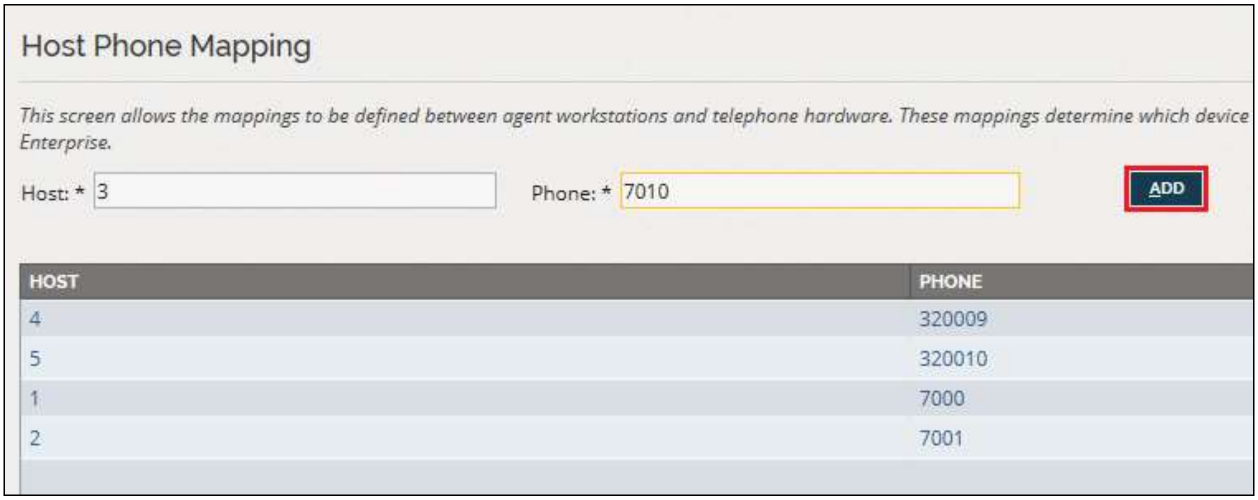
Email

Manage emails and inboxes

Host Phone Mapping

Manage mappings between Agent work stations and telephone hardware

Enter the **Host** number and the phoneset associated with that host and click on **ADD**.



Host Phone Mapping

This screen allows the mappings to be defined between agent workstations and telephone hardware. These mappings determine which device Enterprise.

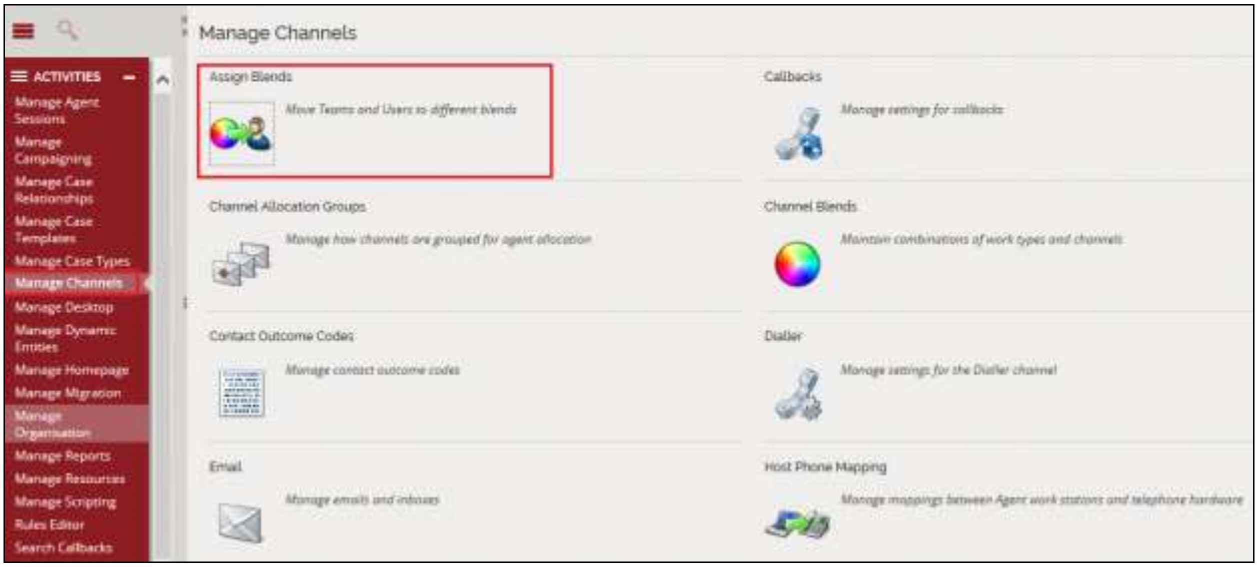
Host: * 3

Phone: * 7010

HOST	PHONE
4	320009
5	320010
1	7000
2	7001

7.3. Assign Blends

Staying within **Manage Channels** click on **Assign Blends** in the main window.



Manage Channels

Assign Blends – *Move Teams and Users to different blends*

Callbacks – *Manage settings for callbacks*

Channel Allocation Groups – *Manage how channels are grouped for agent allocation*

Channel Blends – *Maintain combinations of work types and channels*

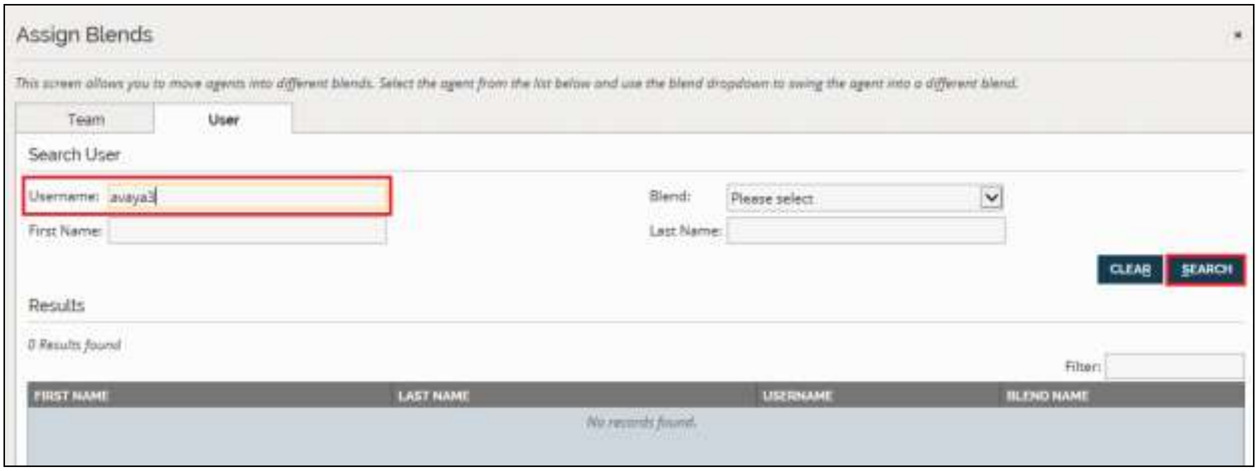
Contact Outcome Codes – *Manage contact outcome codes*

Dialler – *Manage settings for the Dialler channel*

Email – *Manage emails and inboxes*

Host Phone Mapping – *Manage mappings between Agent work stations and telephone hardware*

Search for the new user added in **Section 7.1**.



Assign Blends

This screen allows you to move agents into different blends. Select the agent from the list below and use the blend dropdown to swing the agent into a different blend.

Search User

Username: avaya3

Blend: Please select

First Name:

Last Name:

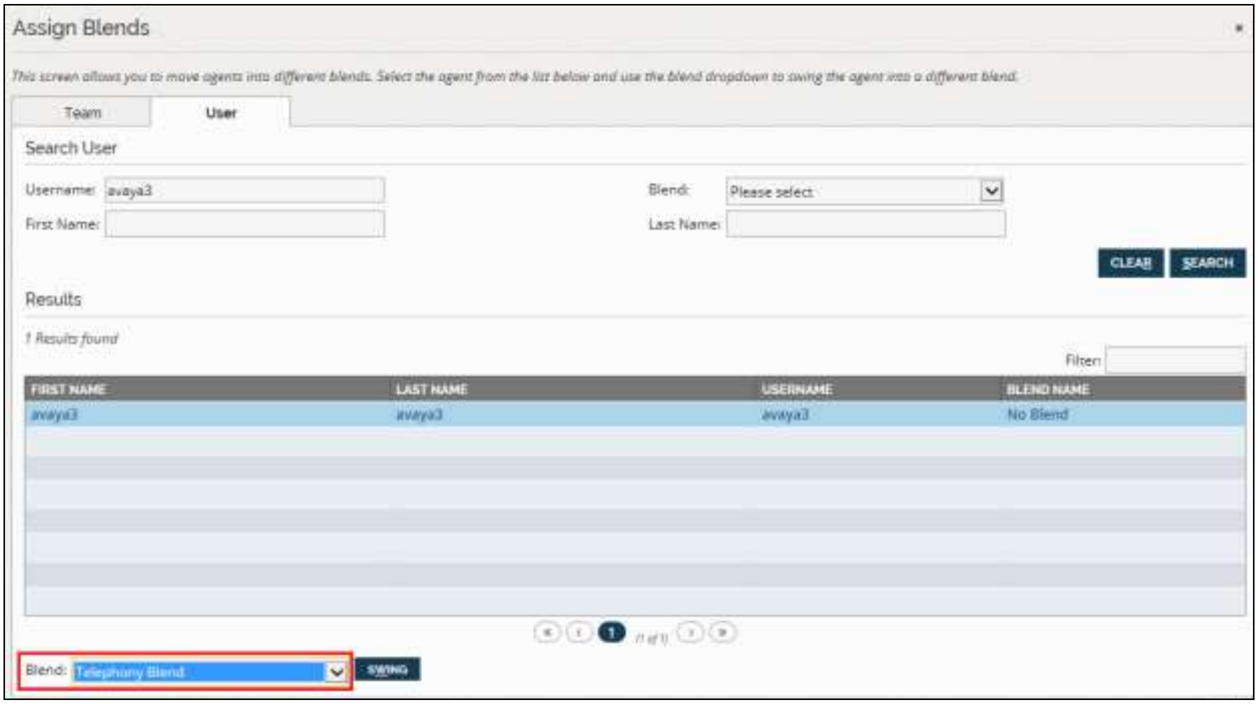
Results

0 Results found

Filter:

FIRST NAME	LAST NAME	USERNAME	BLEND NAME
No records found.			

Highlight the user and select the **Telephony Blend** from the drop-down box at the bottom of the screen and click on the **SWING** button beside the drop-down box.



Assign Blends

This screen allows you to move agents into different blends. Select the agent from the list below and use the blend dropdown to swing the agent into a different blend.

Search User

Username: avaya3

First Name:

Blend: Please select

Last Name:

Results

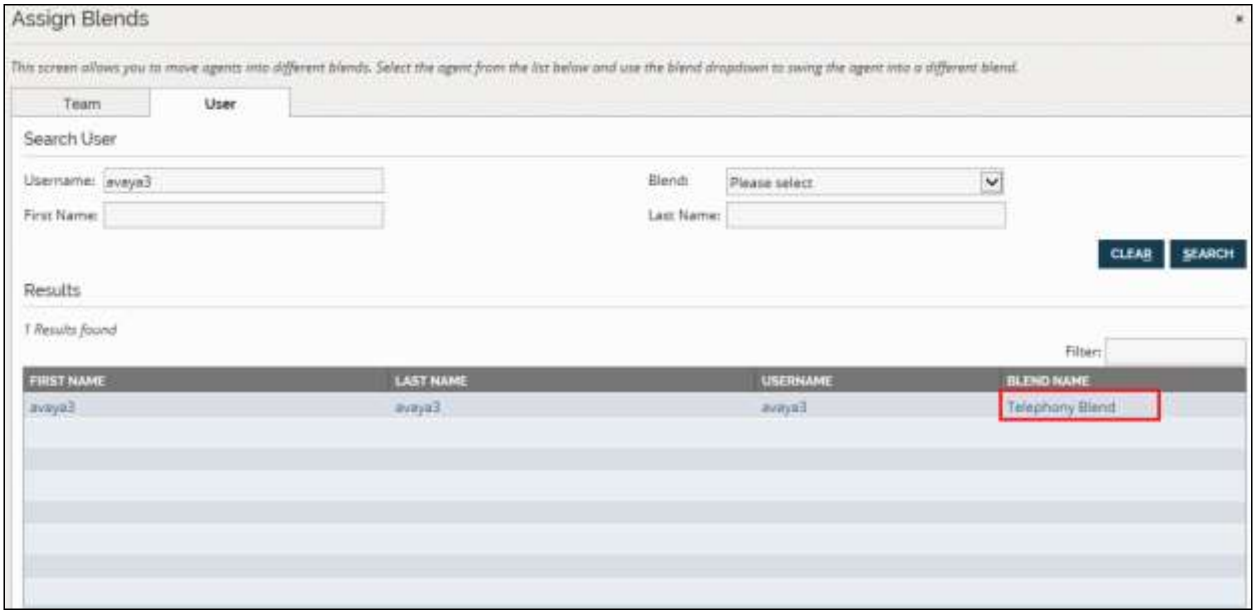
1 Results found

Filter:

FIRST NAME	LAST NAME	USERNAME	BLEND NAME
avaya3	avaya3	avaya3	No Blend

Blend: Telephony Blend

The new blend is now associated with the Avaya user.



Assign Blends

This screen allows you to move agents into different blends. Select the agent from the list below and use the blend dropdown to swing the agent into a different blend.

Search User

Username: avaya3

First Name:

Blend: Please select

Last Name:

Results

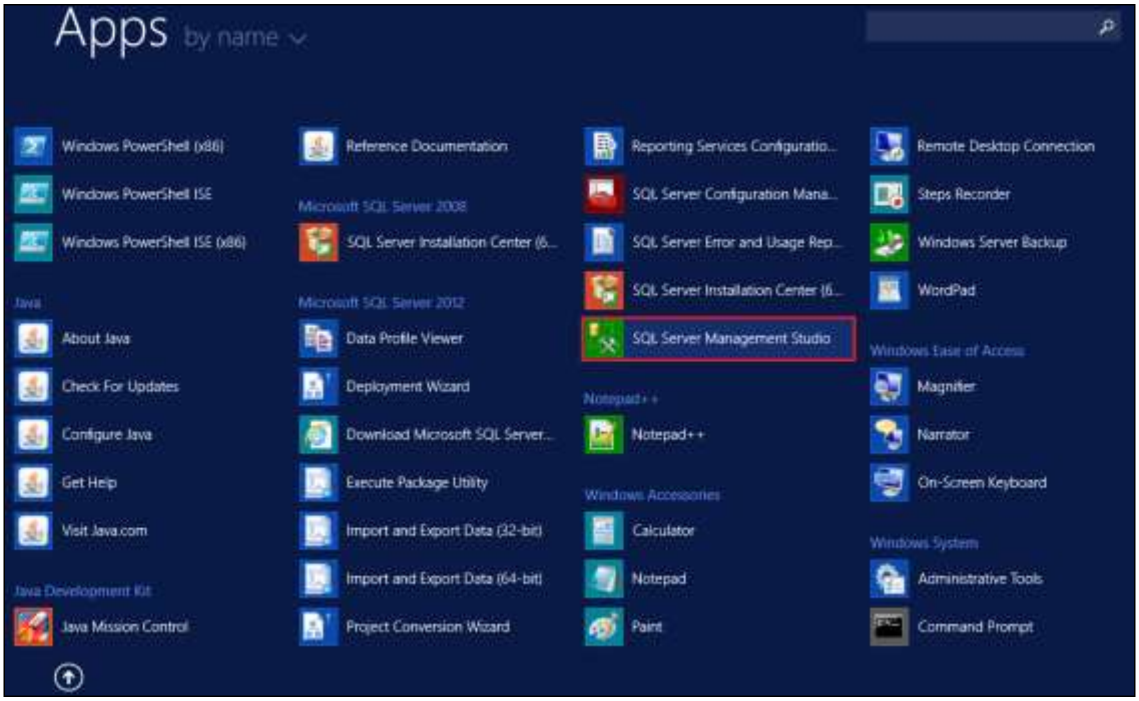
1 Results found

Filter:

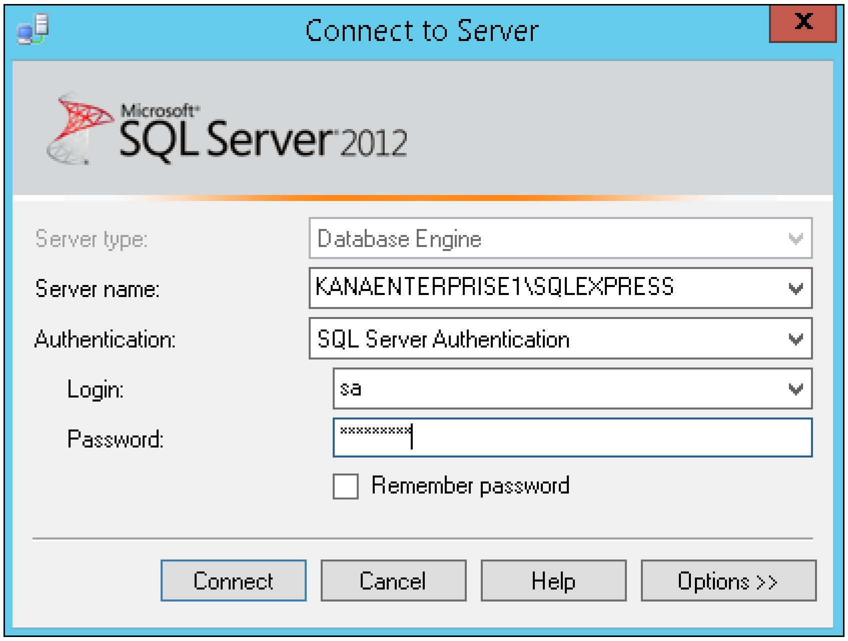
FIRST NAME	LAST NAME	USERNAME	BLEND NAME
avaya3	avaya3	avaya3	Telephony Blend

7.4. Configure connection to AES

The connection to AES is configured by updating the SQL database on the Kana Enterprise server. To update the database open the **SQL Server Management Studio** which can be located on the **Apps** page as shown below.



Enter the proper credentials to connect to the database and click on **Connect.**



Server type: Database Engine

Server name: KANAENTERPRISE1\SQLEXPRESS

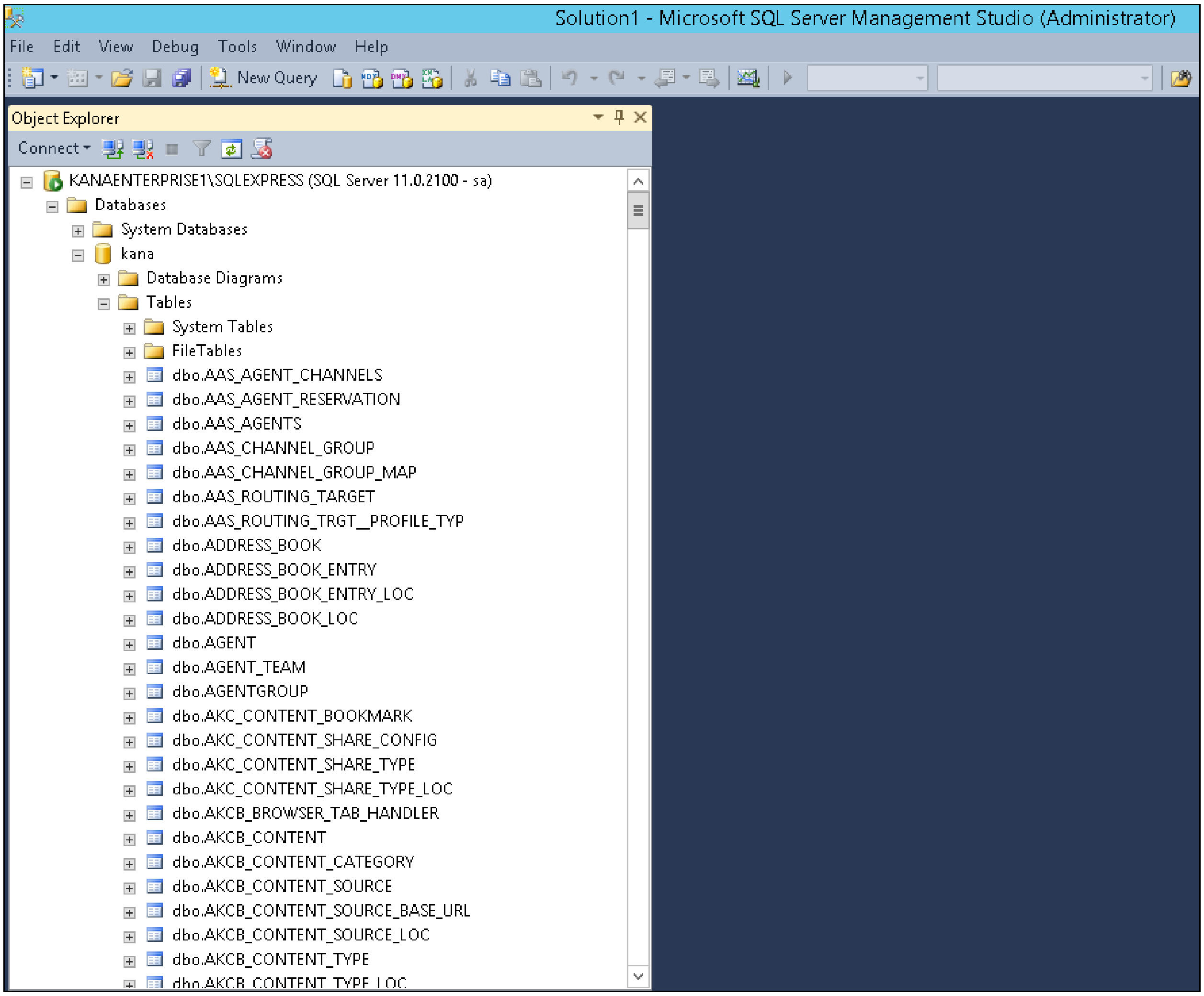
Authentication: SQL Server Authentication

Login: sa

Password: *********

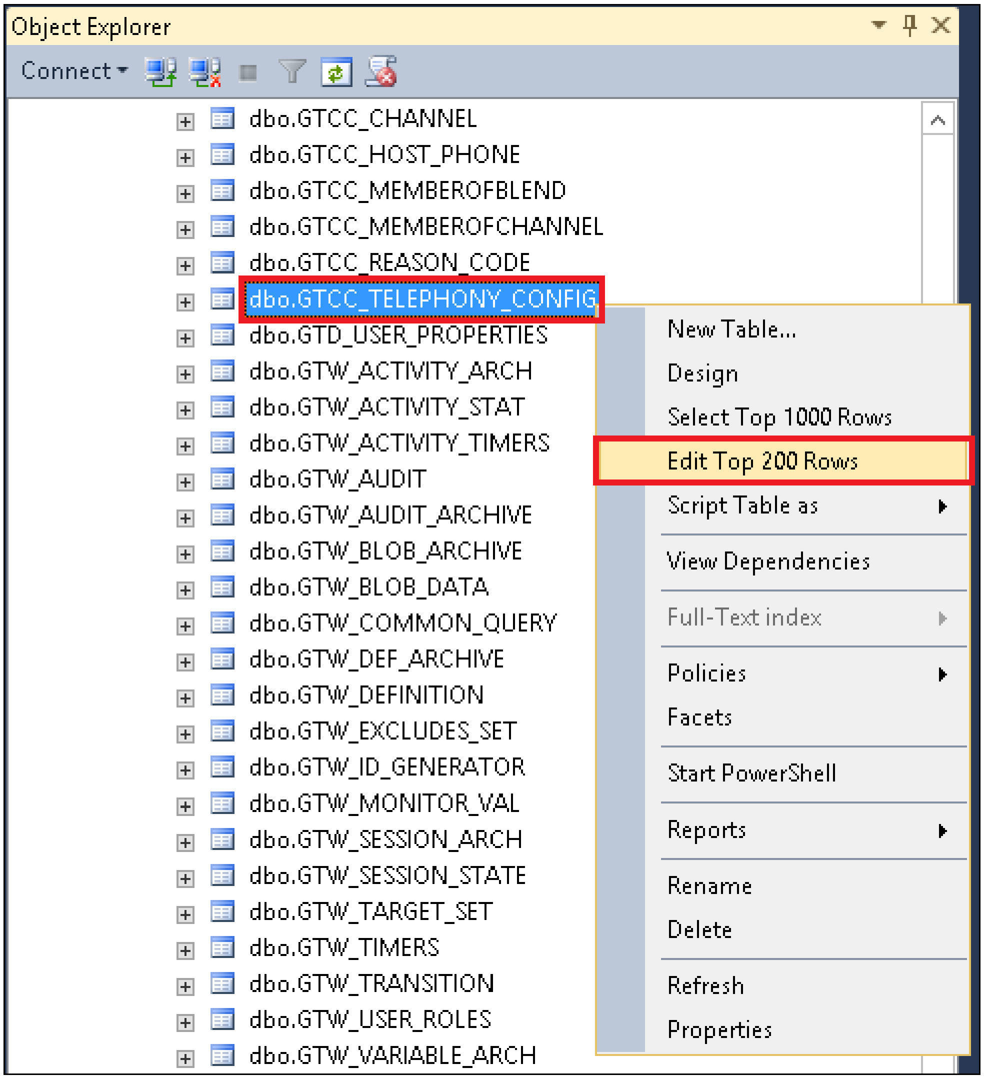
□ Remember password

Open the **Tables** by opening **<Server>\SQLEXPRESS → Databases → kana → Tables**.

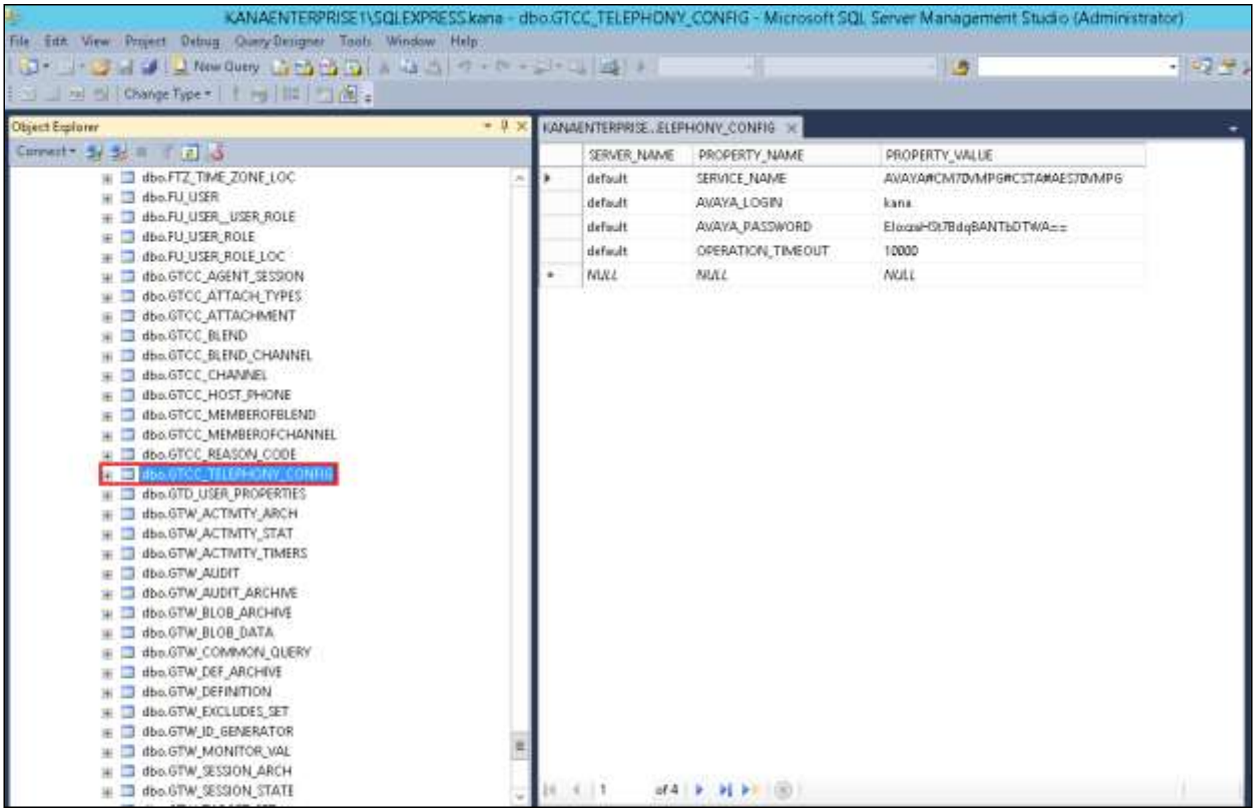

Solution1 - Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect

KANAENTERPRISE1\SQLEXPRESS (SQL Server 11.0.2100 - sa)
Databases
System Databases
kana
Database Diagrams
Tables
System Tables
FileTables
dbo.AAS_AGENT_CHANNELS
dbo.AAS_AGENT_RESERVATION
dbo.AAS_AGENTS
dbo.AAS_CHANNEL_GROUP
dbo.AAS_CHANNEL_GROUP_MAP
dbo.AAS_ROUTING_TARGET
dbo.AAS_ROUTING_TRGT__PROFILE_TYP
dbo.ADDRESS_BOOK
dbo.ADDRESS_BOOK_ENTRY
dbo.ADDRESS_BOOK_ENTRY_LOC
dbo.ADDRESS_BOOK_LOC
dbo.AGENT
dbo.AGENT_TEAM
dbo.AGENTGROUP
dbo.AKC_CONTENT_BOOKMARK
dbo.AKC_CONTENT_SHARE_CONFIG
dbo.AKC_CONTENT_SHARE_TYPE
dbo.AKC_CONTENT_SHARE_TYPE_LOC
dbo.AKCB_BROWSER_TAB_HANDLER
dbo.AKCB_CONTENT
dbo.AKCB_CONTENT_CATEGORY
dbo.AKCB_CONTENT_SOURCE
dbo.AKCB_CONTENT_SOURCE_BASE_URL
dbo.AKCB_CONTENT_SOURCE_LOC
dbo.AKCB_CONTENT_TYPE
dbo.AKCB_CONTENT_TYPE_LOC

Right-click on the **dbo.GTCC_TELEPHONY_CONFIG** table and select **Edit Top 200 Rows**.

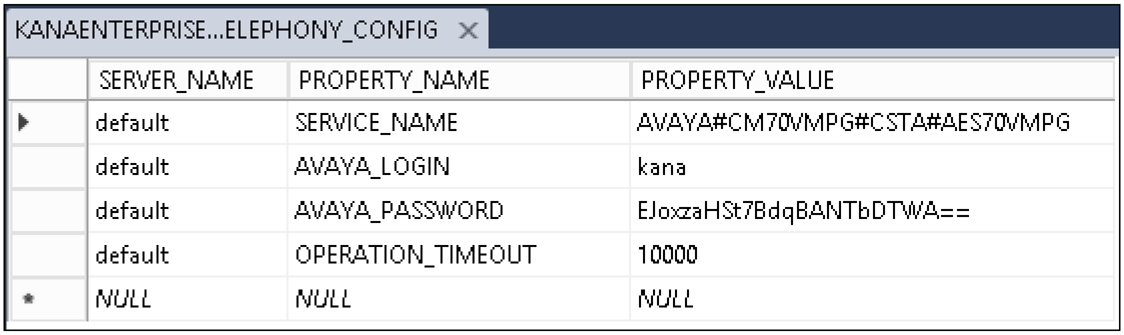


The following information is then displayed.



This information close up shows the Tlink information obtained from **Section 6.4** entered for the **SERVICE_NAME** and the username/password obtained from **Section 6.6** are entered as **AVAYA_LOGIN** and **AVAYA_PASSWORD**.

Note: The **AVAYA_PASSWORD** requires to be an encrypted version, this however is outside the scope of these Application Notes,for more details on encrypting this please refer to the Kana Enterprise documentation in **Section 10**.



	SERVER_NAME	PROPERTY_NAME	PROPERTY_VALUE
▶	default	SERVICE_NAME	AVAYA#CM70VMPG#CSTA#AES70VMPG
	default	AVAYA_LOGIN	kana
	default	AVAYA_PASSWORD	EJoxzaHSt7BdqBANTbDTWA==
	default	OPERATION_TIMEOUT	10000
*	NULL	NULL	NULL

Note: The IP address of the AES server is entered as part of the TSAPI Client installation on the Kana Enterprise server and this is outside the scope of these Application Notes, for more information on this installation please refer to **Section 10**.

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the Kana Enterprise and Avaya Aura® Application Enablement Services.

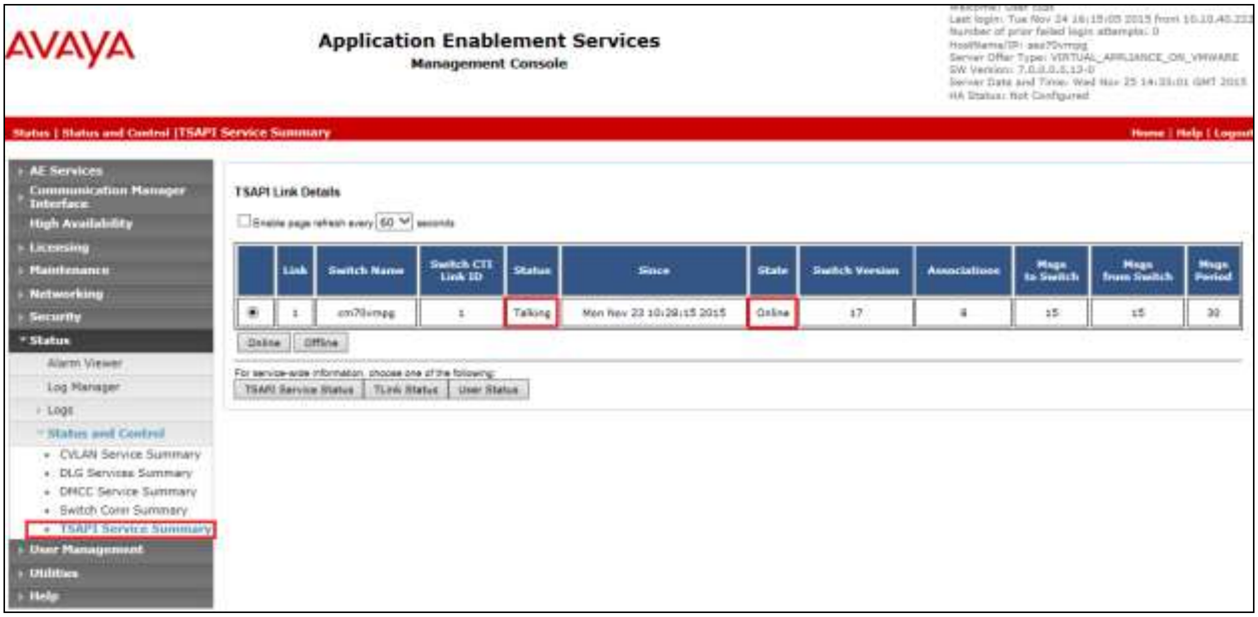
8.1. Verify Avaya Aura® Communication Manager CTI Service State

Before checking the connection between the Kana Enterprise and AES, check the connection between Communication Manager and AES to ensure it is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

CTI   Version      Mnt   AE Services       Service       Msgs      Msgs
Link               Busy     Server          State        Sent      Rcvd

1         5        no      aes70vmpg       established   18        18
```

8.2. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.



TSAPI Link Details

☐ Enable page refresh every 60 seconds

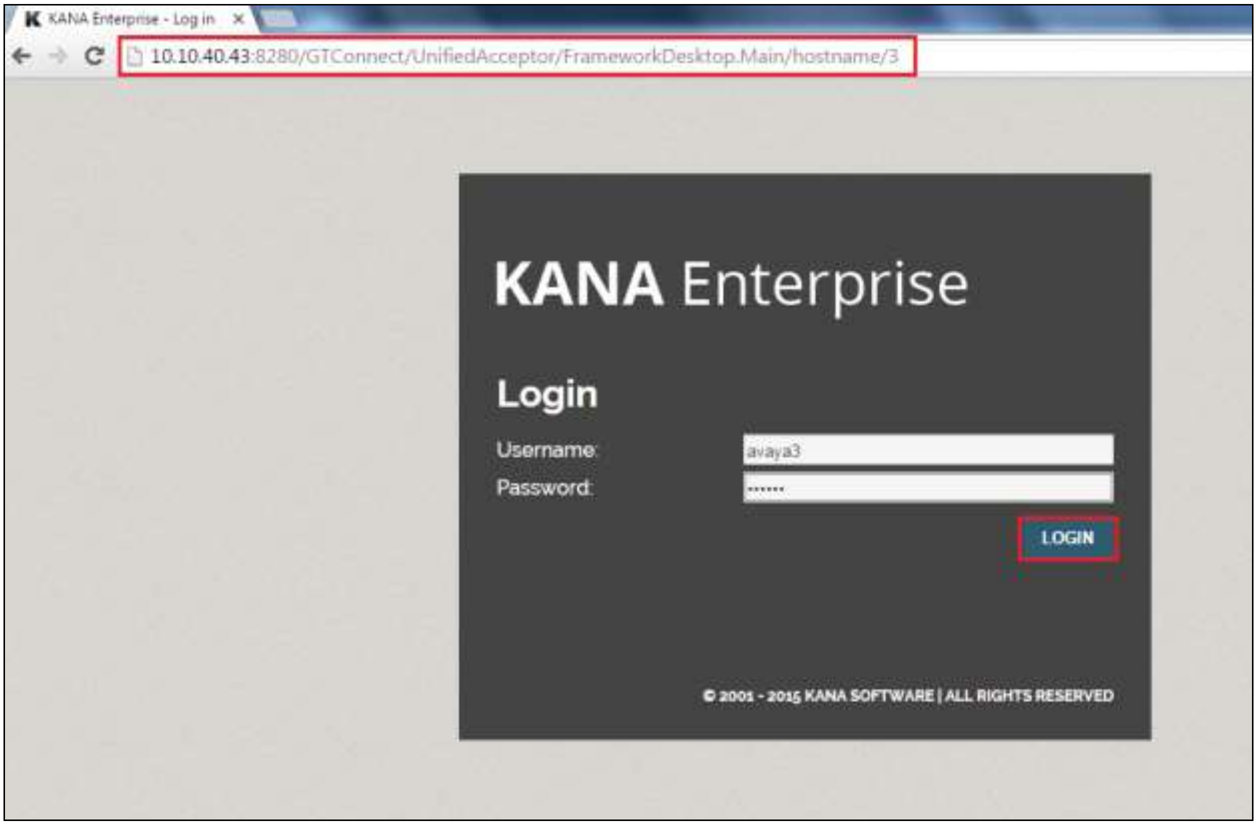
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm70vmpg	1	Talking	Mon Nov 23 10:29:15 2015	Online	17	8	15	15	30

For service-wide information, choose one of the following:

8.3. Verify Kana Enterprise

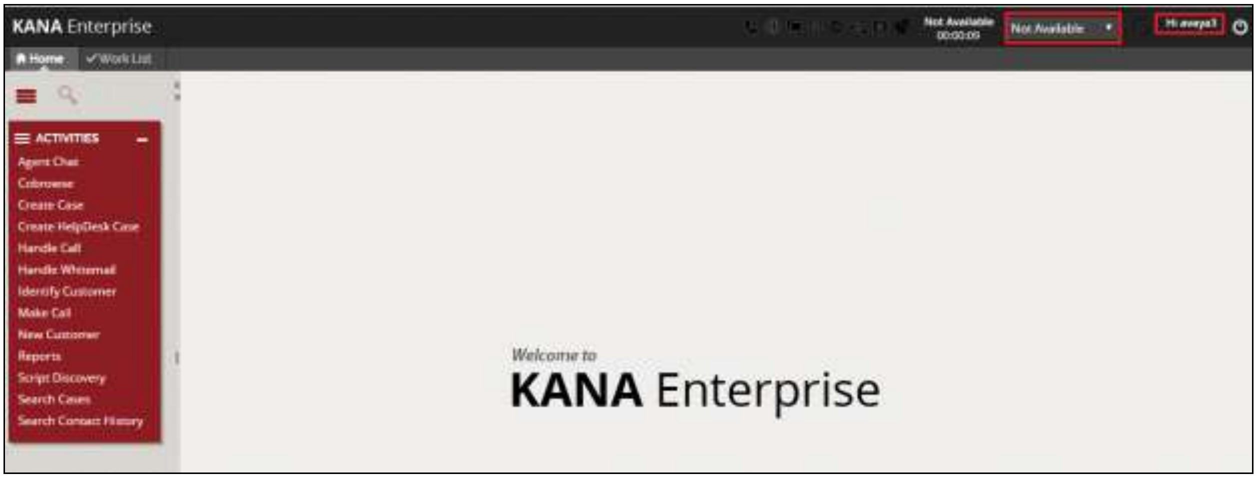
Open a web session to the Kana Enterprise server with a URI of **http://<KanaEnterpriseServer>:8280/GTConnect/UnifiedAcceptor/FrameworkDesktop.Main/hostname/3**. Note the "3" at the end of the link which constitutes the host configured in **Section 7.2**. This host "3" was associated with a phoneset and agent in the configuration of Kana Enterprise in **Section 7.1**.

Enter appropriate login credentials which will be that of the agent configured in **Section 7.1** and click on **LOGIN**.

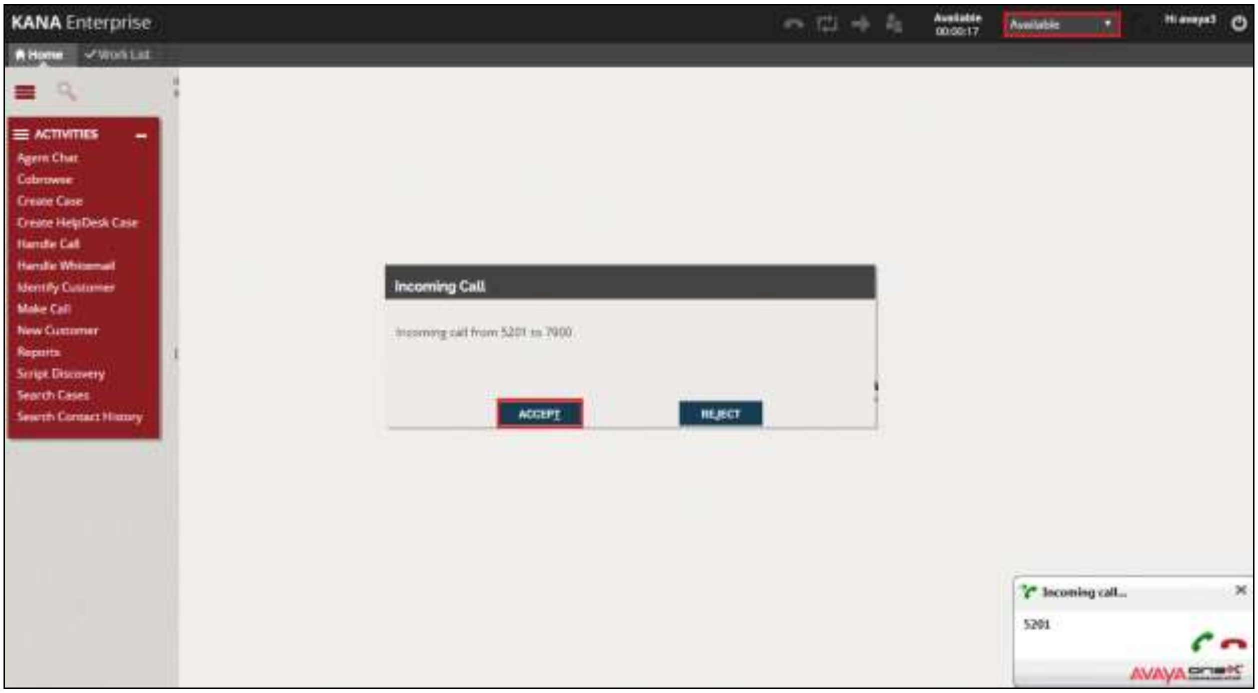

KANA Enterprise - Log in
10.10.40.43:8280/GTConnect/UnifiedAcceptor/FrameworkDesktop.Main/hostname/3
KANA Enterprise
Login
LOGIN
© 2001 - 2015 KANA SOFTWARE | ALL RIGHTS RESERVED

Username: avaya3
Password: ••••••

Once logged in the following window is automatically displayed. By default the system places the agent into not ready or **Not Available.**



By changing the agent to **Available** using the drop-down box at the top of the screen and sending a new call to the VDN **7900** a pop-up window displaying an Incoming Call allows the agent answer the call by pressing **ACCEPT** as shown below.



Incoming call from 5201 to 7900

9. Conclusion

These Application Notes describe the configuration steps required for Kana Enterprise 14R1 SP4 from Verint Systems Inc. to successfully interoperate with Avaya Aura® Communication Manager R7.0 using Avaya Aura® Application Enablement Services R7.0 to gain 3rd party call control of the Communication Manager phones and agents. All feature functionality and serviceability test cases were completed successfully with any observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Kana Enterprise 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*, Document ID 03-300509

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 7.0

Product documentation for Kana Enterprise can be downloaded or requested via the secure customer portal at http://kanacommunity.verint.com.

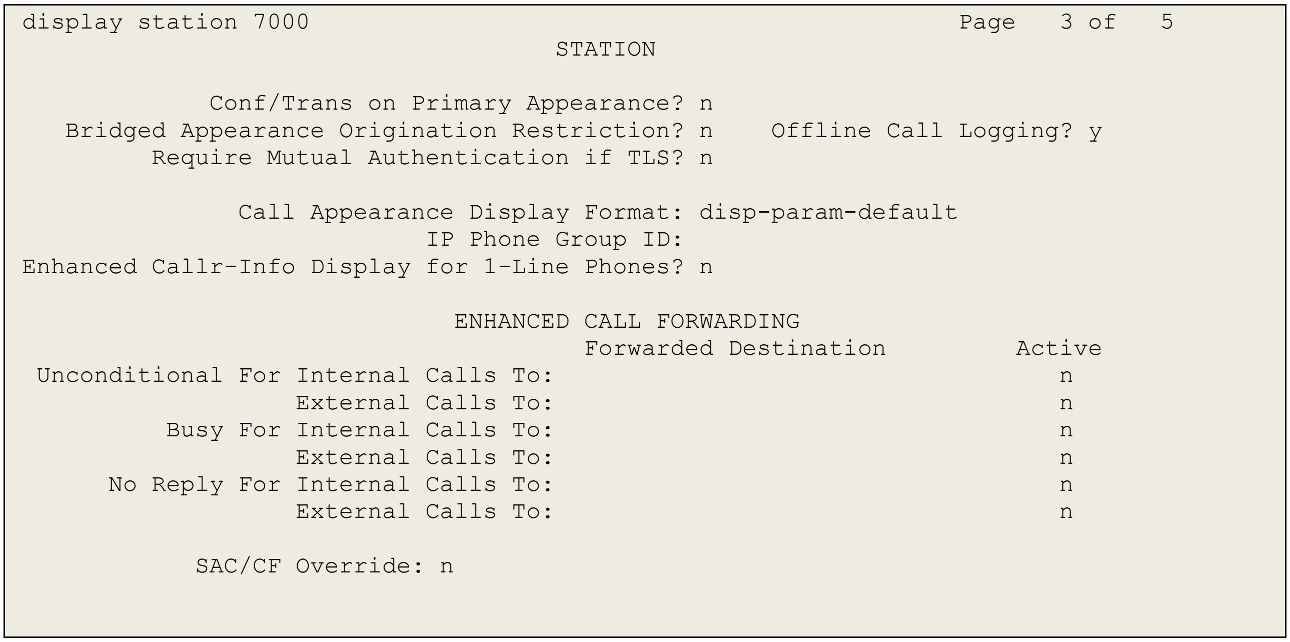
Appendix

Avaya 9608 H.323 Deskphone

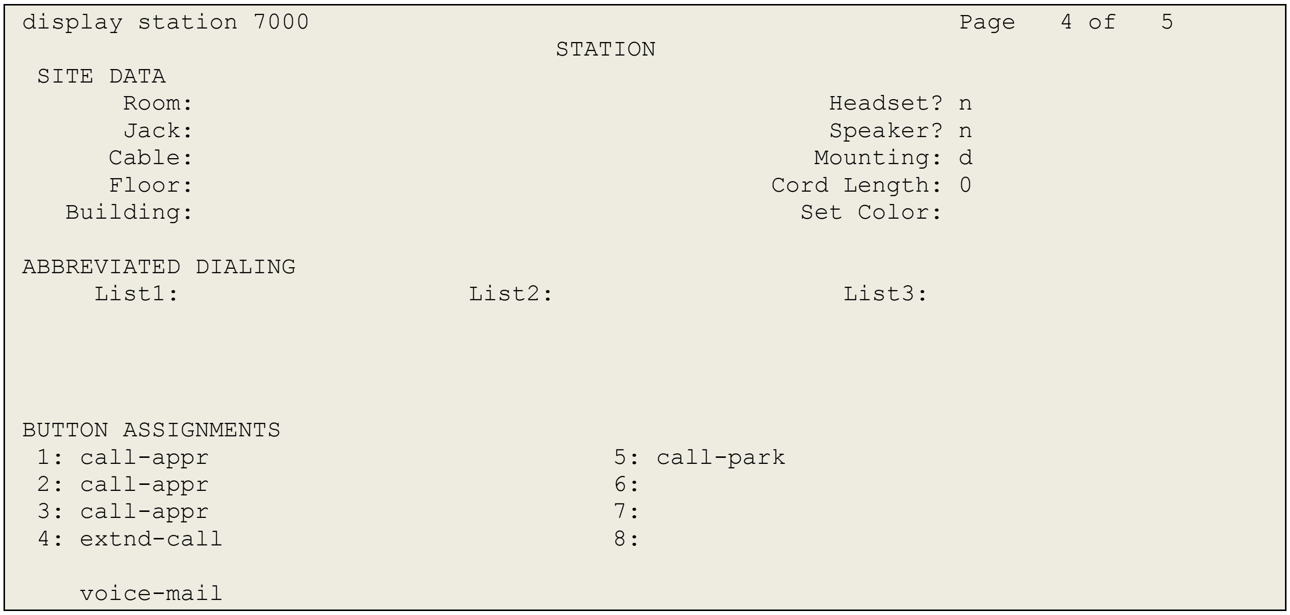
This is a printout of one of the Avaya 9608 H.323 desk phones used during compliance testing.

```
display station 7000                                             Page   1 of   5
                                     STATION

Extension: 7000                          Lock Messages? n                BCC: 0
     Type: 9608                          Security Code: *                 TN: 1
     Port: S00000                      Coverage Path 1: 1                COR: 1
     Name: Ext2000                     Coverage Path 2:                  COS: 1
                                       Hunt-to Station:                Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 7000
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? y

                                               IP Video Softphone? n
                              Short/Prefixed Registration Allowed: yes

                                              Customizable Labels? y
```

```
display station 7000                                             Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe              Auto Select Any Idle Appearance? n
          LWC Activation? y                         Coverage Msg Retrieval? y
  LWC Log External Calls? n                                    Auto Answer: none
             CDR Privacy? n                               Data Restriction? n
   Redirect Notification? y                     Idle Appearance Preference? n
 Per Button Ring Control? n                   Bridged Idle Line Preference? n
   Bridged Call Alerting? n                       Restrict Last Appearance? y
  Active Station Ringing: single
                                                         EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                    EC500 State: enabled
         Multimedia Mode: enhanced                 Audible Message Waiting? n
    MWI Served User Type: sip-adjunct           Display Client Redirection? n
                                               Select Last Used Appearance? n
                                                 Coverage After Forwarding? s
                                                   Multimedia Early Answer? n
 Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? y
  Emergency Location Ext: 7000          Always Use? n IP Audio Hairpinning? n
```



```
display station 7000                                             Page   3 of   5
                                     STATION

             Conf/Trans on Primary Appearance? n
   Bridged Appearance Origination Restriction? n    Offline Call Logging? y
         Require Mutual Authentication if TLS? n

               Call Appearance Display Format: disp-param-default
                            IP Phone Group ID:
Enhanced Callr-Info Display for 1-Line Phones? n

                              ENHANCED CALL FORWARDING
                                       Forwarded Destination         Active
 Unconditional For Internal Calls To:                                   n
                   External Calls To:                                   n
          Busy For Internal Calls To:                                   n
                   External Calls To:                                   n
      No Reply For Internal Calls To:                                   n
                   External Calls To:                                   n

            SAC/CF Override: n
```



```
display station 7000                                             Page   4 of   5
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                        Cord Length: 0
   Building:                                          Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                            5: call-park
 2: call-appr                            6:
 3: call-appr                            7:
 4: extnd-call                           8:

    voice-mail
```

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.