



Application Notes for configuring Imperium CTI Connect from Protocol Systems FZC with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager R6.3 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for Protocol Systems FZC Imperium CTI Connect to interoperate with Avaya Aura® Application Enablement Services R6.3 and Avaya Aura® Communication Manager R6.3. Imperium CTI Connect integrates with Avaya Aura® Application Enablement Services using TSAPI and DMCC connections for call control.

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 Protocol Systems FZC Imperium CTI Connect to interoperate with Avaya Aura® Application Enablement Services R6.3 and Avaya Aura® Communication Manager R6.3. Imperium CTI Connect integrates with Avaya Aura® Application Enablement Services using Telephony Server Application Programming Interface (TSAPI) and Device, Media and Call Control (DMCC) API for call control.

Imperium CTI Connect provides the user with single interface, single system and media control functionalities such as call control, caller number identification, screen pop, call answer, transfer and hold, all required by the agent/users for effectively and efficiently completing a customer interaction. Imperium CTI Connect offers businesses a client based agent desktop program that works alongside existing systems, or a fully integrated CTI solution that combines existing systems into one unified desktop interface. Able to integrate with Communication Manager via a TSAPI DMCC connection through AES, and extract and update caller information, the CTI application helps ensure customers are served effectively and efficiently.

2. General Test Approach and Test Results

This section describes the compliance testing used to verify interoperability of Imperium CTI Connect (IMCC) with Avaya AES and covers the general test approach and the test results.

IMCC Server is installed on a Windows 2008 Server R2 running Microsoft SQL 2008 database. Each client or Imperium CTI Connect Agent Desktop (IMCC Agent Desktop) connects to the IMCC Server in order to obtain information on each caller from a central database. Once a call is presented to an agent the IMCC can use the Call Line ID information obtained from Communication Manager to lookup the database on the IMCC Server and present to the agent all the customer information associated with that CLID. Each agent that is running IMCC Agent Desktop will have a unique connection to the AES using DMCC for call control and to monitor the caller's information.

Feature testing covered the ability of IMCC to gain control of existing Communication Manager endpoints and focused on the handling of calls offered to Communication Manager by the IMCC Agent Desktop application. The serviceability testing focused on the ability of IMCC to recover from adverse conditions such as loss of network connectivity.

Note: During compliance testing, SIP endpoints were not included. SIP phones are not supported in this configuration.

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 placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Basic Calls** – Basic incoming and outgoing calls using IMCC Agent Desktop.
- **Call Hold** – Tests held calls using IMCC Agent Desktop.
- **Call Transfer** Tests transferred calls using IMCC Agent Desktop.
- **Call Conference** Tests conferenced calls using IMCC Agent Desktop.
- **Failover/Service** – Tests the behaviour of both the IMCC Server IMCC Agent Desktop when there are certain failed conditions.

2.2. Test Results

All functionality and serviceability test cases were completed successfully. The following issues and observation were noted during the compliance testing.

1. When a transfer takes place from Agent 1 to Agent 2 no CLID or CRM data is passed onto the second agent. The call is transferred successfully but there is no accompanying data. This feature will be available in the next release.
2. When an agent dials a busy or unobtainable number and then presses disconnect on the screen the call does not hang up on the phone.
3. Blind Transfer to a busy/unobtainable number. When an agent dials a busy or unobtainable number and then presses disconnect on the screen the call does not hang up on the phone. This is the similar and resulting from point 2 above. The Application should understand that this number is busy or unoccupied and not allow the completion of the transfer, because once completed the call cannot be retrieved.
4. Supervised Transfer to a busy/unobtainable number. When an agent dials a busy or unobtainable number they must wait for the Communication Manager's default timer to run and disconnect the consult call before they can retrieve the initial caller.
5. Call Park cannot be used successfully and can therefore not be supported using the IMCC Agent Desktop but still can be achieved from Avaya deskphone directly.
6. SIP endpoints were not included. SIP phones are not supported in this configuration.

2.3. Support

Technical support can be obtained for Imperium CTI Connect from the website <http://imperiumapp.com/contact.aspx>

Protocol Systems FZC
Q3-133, SAIF Zone,
Sharjah, UAE.
Tel: +9716 5578383
Fax: +9716 5578384
Email: support@protocolsystems-me.com

3. Reference Configuration

The configuration in **Figure 1** is used to compliance test Protocol Systems FZC Imperium CTI Connect with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3 to gain call control of the various Avaya endpoints as shown below. Imperium CTI Connect Server is installed on a Windows 2008 Server R2 running Microsoft SQL 2008 database. Each client or Imperium CTI Connect Agent Desktop connects to the Imperium CTI Connect Server in order to obtain information on each caller from a central database.

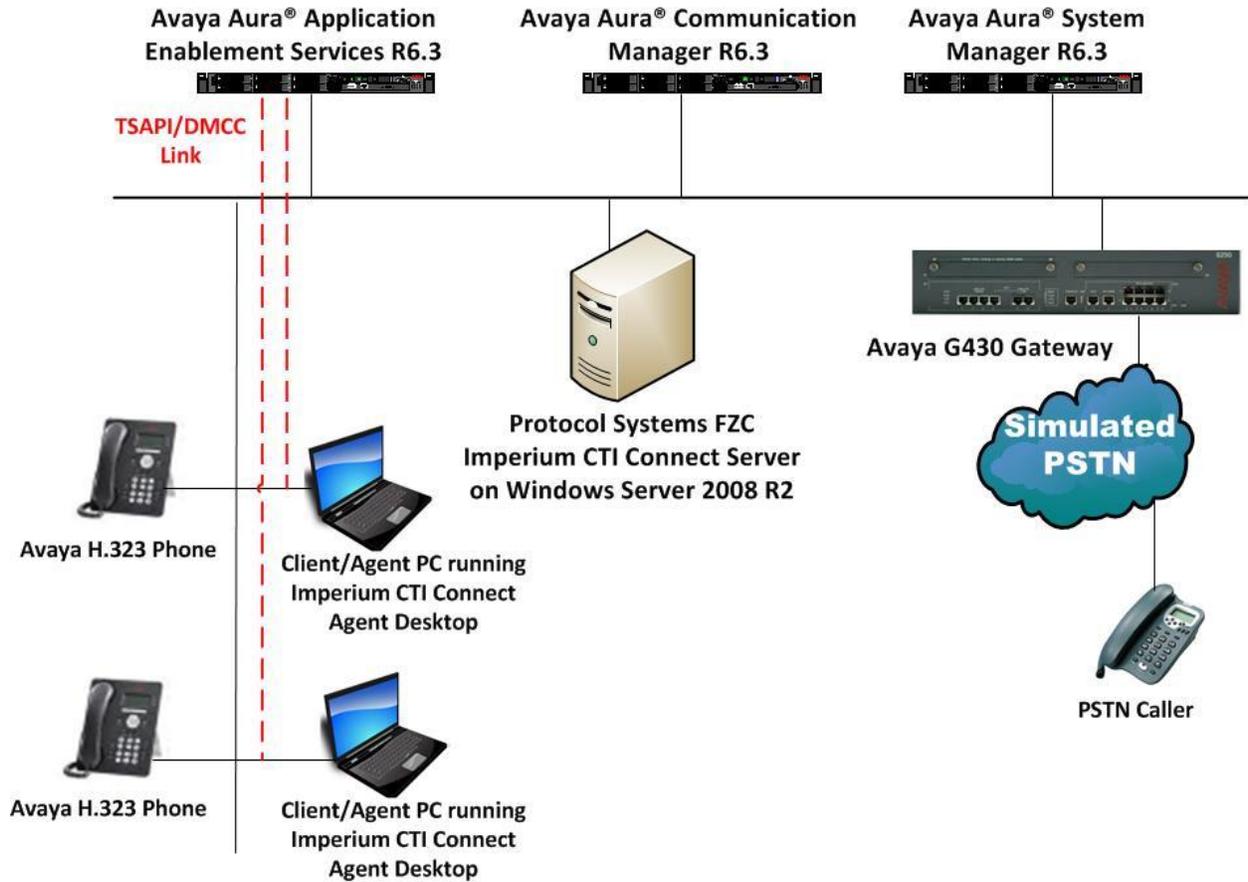


Figure 1: Connection of Imperium CTI Connect from Protocol System FZC with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement Services R6.3.

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 Virtual Server	R6.3.10 [Build 6.3.0.8.5682-6.3.8.4514] [SW Update Rev 6.3.10.7.2656]
Avaya Aura® Communication Manager running on Virtual Server	R6.3 SP8 R016x.03.0.124.0 03.0.124.0-21588
Avaya Aura® Application Enablement Services running on Virtual Server	R6.3 Build No - 6.3.3.1.10-0
Avaya G430 Gateway	33.12.0 /1
Avaya 9608 H323 Deskphone	Release 6.4014U
Avaya 9620 H323 Deskphone	Release 3.186A
Protocol Systems FZC Imperium CTI Connect Server running on Virtual Server Imperium CTI Connect Server	Windows Server 2008 R2 & MSSQL 2008 R1.0
Windows 7 Client PC Imperium CTI Connect Agent Desktop	Windows 7 Enterprise R1.0

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 (**aes63vmpg**).

```

display node-names ip                                     Page 1 of 2
                                     IP NODE NAMES
Name                                IP Address
SM100                               10.10.40.34
aes63vmpg                          10.10.40.30
default                             0.0.0.0
g430                                10.10.40.15
procr                               10.10.40.31

```

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      y Node  Port Node  Port
AESVCS

```

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 **aes63vmpg**.
- **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** should match the administered name for the AES server, that 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:        aes63vmpg *****    y      idle
2:
3:

```

5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. 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: 2002
    Type: ADJ-IP
                                           COR: 1
Name: aes63vmpg
```

5.5. Configure Stations

All endpoints that are to be monitored by IMCC will need to have IP Softphone set to Y. IP Softphone must be enabled for the DMCC connection. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required in **Section 7.1**. Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

```
change station x                               Page 1 of 6
                                           STATION
Extension: x                                  Lock Messages? n          BCC: 0
    Type: 9630                                Security Code: 1234      TN: 1
    Port: S00101                              Coverage Path 1:          COR: 1
    Name: IMCC Agent Desktop A                 Coverage Path 2:          COS: 1
                                           Hunt-to Station:
STATION OPTIONS
    Loss Group: 19                            Time of Day Lock Table:
    Speakerphone: 2-way                       Personalized Ringing Pattern: 1
    Display Language: english                  Message Lamp Ext: 1591
    Survivable GK Node Name:                  Mute Button Enabled? y
    Survivable COR: internal                   Media Complex Ext:
    Survivable Trunk Dest? y                  IP SoftPhone? y
                                           IP Video Softphone? n
                                           Short/Prefixed Registration Allowed: default
```

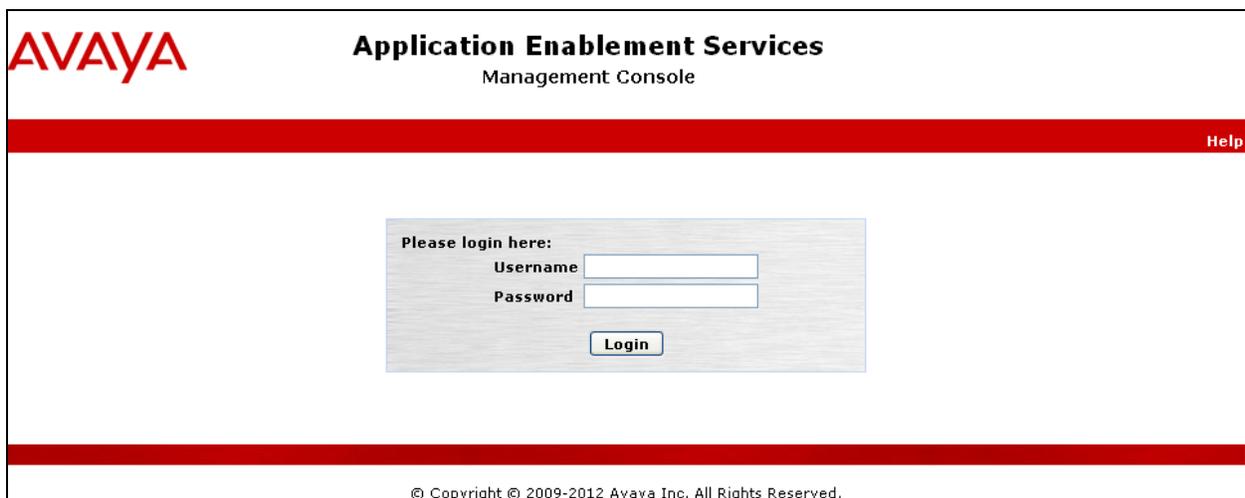
6. Configure Avaya Aura® Application Enablement Services

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 & DMCC 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, log in with the appropriate credentials and then select the **Login** button.



The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. The page title is "Application Enablement Services Management Console". A red horizontal bar spans the width of the page, with a "Help" link on the right. The main content area contains a login form with the text "Please login here:" followed by "Username" and "Password" labels, each with a corresponding text input field. Below the input fields is a "Login" button. At the bottom of the page, a red horizontal bar contains the copyright notice: "© Copyright © 2009-2012 Avaya Inc. All Rights Reserved."

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** from the left window and verify that both the TSAPI and DMCC services are licensed by ensuring that both services are 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 for your solution.

AVAYA Application Enablement Services Management Console

AE Services | Home | Help | Logout

AE Services

This AE Services server is using a default installed server certificate. Default installed certificates should not be used in a production environment. It is highly recommended to replace all default installed certificates.

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	ONLINE	Running	NORMAL MODE	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

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.

AVAYA Application Enablement Services Management Console

Communication Manager Interface | Switch Connections | Home | Help | Logout

Switch Connections

CM63VMPPG Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

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

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**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'Switch Connections' selected. The main content area is titled 'Connection Details - CM63vmpg' and contains the following fields:

- Switch Password: [Redacted]
- Confirm Switch Password: [Redacted]
- Msg Period: 30 Minutes (1 - 72)
- SSL:
- Processor Ethernet:

Buttons for 'Apply' and 'Cancel' are visible at the bottom of the form.

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). 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.

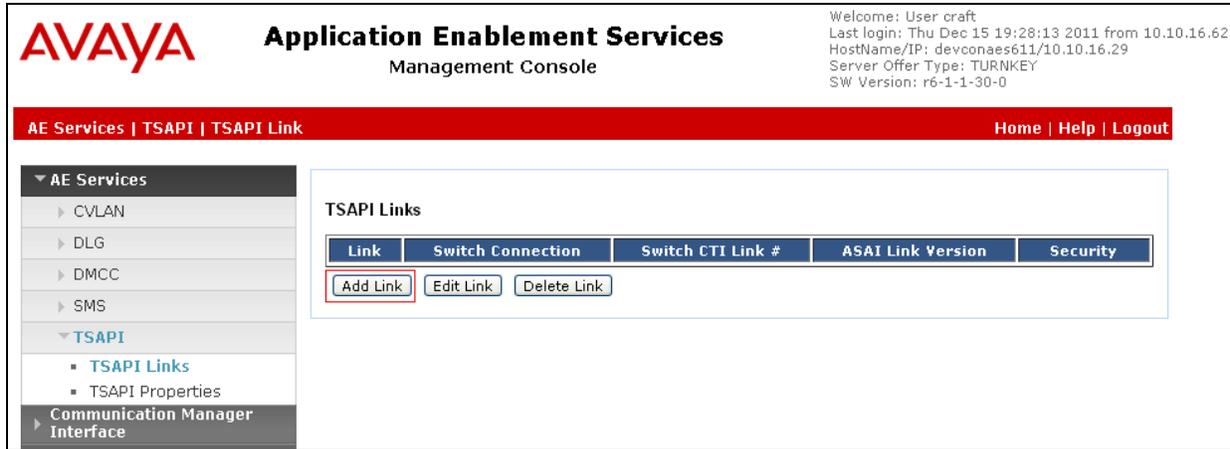
The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with 'Switch Connections' selected. The main content area is titled 'Edit Processor Ethernet IP - CM63vmpg' and contains the following elements:

- Input field for IP address: 10.10.40.31
- Button: Add/Edit Name or IP
- Table with columns 'Name or IP Address' and 'Status':

Name or IP Address	Status
10.10.40.31	In Use
- Button: Back

6.3. Administer TSAPI link

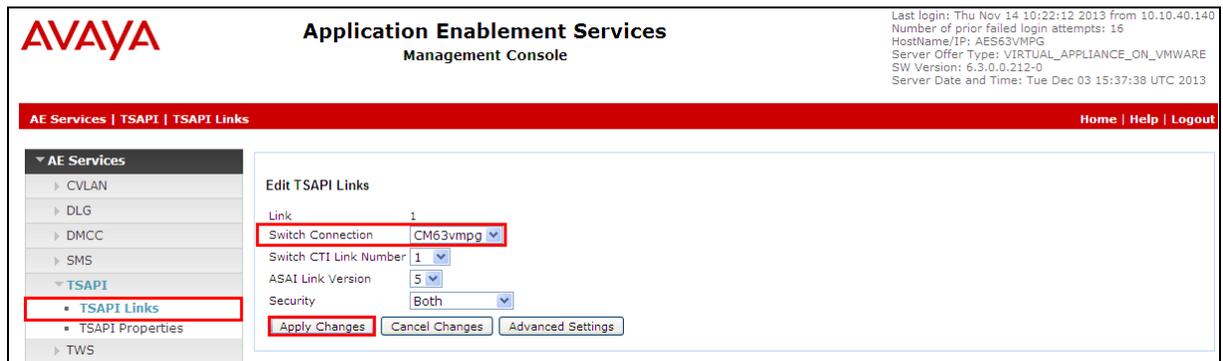
From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.



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 **CM63VMPPG**, 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 **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.



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

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

AE Services | TSAPI | TSAPI Link Home | Help | Logout

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.

AVAYA Application Enablement Services Management Console

Last login: Tue Dec 3 15:32:14 2013 from 10.10.40.225
Number of prior failed login attempts: 17
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 16:34:53 UTC 2013

AE Services | TSAPI | TSAPI Links Home | Help | Logout

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM63vmpg	1	5	Both

Both the TSAPI and DMCC services 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** & **DMCC Service** and select **Restart Service**.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

Maintenance | Service Controller Home | Help | Logout

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> 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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo, and the top right shows the title "Application Enablement Services Management Console". A red navigation bar contains the text "Security | Security Database | Tlinks". On the left is a sidebar menu with categories: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, and Security. The Security section is expanded, showing sub-items like Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database, Control, CTI Users, Devices, Device Groups, and Tlinks. The Tlinks item is highlighted with a red box. The main content area is titled "Tlinks" and contains a "Tlink Name" field with two radio button options: "AVAYA#CM63VMPPG#CSTA#AES63VMPPG" (selected) and "AVAYA#CM63VMPPG#CSTA-S#AES63VMPPG". A "Delete Tlink" button is located below the options.

6.5. Enable TSAPI and DMCC Ports

To ensure that TSAPI and DMCC ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7**.

The screenshot displays the Avaya Application Enablement Services Management Console. The interface includes a navigation menu on the left with 'Ports' highlighted under the 'Networking' section. The main content area is titled 'Ports' and is divided into three sections: CVLAN Ports, TSAPI Ports, and DMCC Server Ports. In the CVLAN Ports section, the Unencrypted TCP Port is 9999 and the Encrypted TCP Port is 9998, both with 'Enabled' radio buttons selected. The DLG Port section shows the TCP Port as 5678. The TSAPI Ports section includes the TSAPI Service Port (450) with an 'Enabled' radio button selected, and Local TLINK Ports (TCP Port Min: 1024, TCP Port Max: 1039) and Unencrypted TLINK Ports (TCP Port Min: 1050, TCP Port Max: 1065). The Encrypted TLINK Ports section shows TCP Port Min: 1066 and TCP Port Max: 1081. The DMCC Server Ports section includes the Unencrypted Port (4721) with an 'Enabled' radio button selected, the Encrypted Port (4722), and the TR/87 Port (4723) with an 'Enabled' radio button selected. Red boxes highlight the 'Ports' menu item, the 'Enabled' radio buttons for the TSAPI and DMCC Unencrypted ports, and the '4721' value in the DMCC Unencrypted Port field.

AVAYA Application Enablement Services Management Console

Last login: Thu Nov 27 15:58:43 2014 from 10.10.60.30
Number of prior failed login attempts: 0
HostName/IP: AES63VMPPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Dec 01 16:06:19 GMT 2014
HA Status: Not Configured

Networking | Ports Home | Help | Logout

Ports

CVLAN Ports

Unencrypted TCP Port	9999	Enabled Disabled
Encrypted TCP Port	9998	Enabled Disabled

DLG Port

TCP Port	5678
----------	------

TSAPI Ports

TSAPI Service Port	450	Enabled Disabled
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

Unencrypted Port	4721	Enabled Disabled
Encrypted Port	4722	Enabled Disabled
TR/87 Port	4723	Enabled Disabled

6.6. Create CTI User

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

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the AVAYA logo. The main title is "Application Enablement Services Management Console". A red navigation bar at the top contains the text "User Management | User Admin". On the left is a vertical navigation menu with the following items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security, Status, User Management (expanded), Service Admin, User Admin (expanded), Utilities, and Help. The "User Admin" sub-menu is highlighted with a red box and contains: Add User, Change User Password, List All Users, Modify Default Users, and Search Users. The main content area on the right is titled "User Admin" and contains the text: "User Admin provides you with the following options for managing AE Services users:". Below this text is a bulleted list of options: Add User, Change User Password, List All Users, Modify Default User, and Search Users. The "Add User" option in this list is also highlighted with a red box.

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

- **User Id** - This will be used by the each IMCC Agent Desktop to connect to AES.
- **Common Name** and **Surname** - Descriptive names need to be entered.
- **User Password** and **Confirm Password** - This will again be used by each IMCC Agent Desktop.
- **CT User** - Select **Yes** from the drop-down menu.

Complete the process by choosing **Apply** at the bottom of the screen (not shown).

AVAYA **Application Enablement Services**
Management Console

User Management | User Admin | List All Users

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Service Admin
User Admin
Add User
Change User Password
List All Users
Modify Default Users
Search Users
Utilities
Help

Edit User

* User Id	imperium
* Common Name	imperium
* Surname	imperium
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	

The next screen will show a message indicating that the user was created successfully (not shown).

6.7. Associate Devices with CTI User

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users** select the **imperium** user and click on **Edit**.

AVAYA Application Enablement Services Management Console

Last login: Tue Jan 6 16:29:28 2015 from 10.10.40.222
 Number of prior failed login attempts: 0
 HostName/IP: AES63VMPG/10.10.40.30
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 6.3.3.1.10-0
 Server Date and Time: Fri Jan 09 11:12:19 GMT 2015
 HA Status: Not Configured

Security | Security Database | CTI Users | List All Users Home | Help | Logout

Navigation menu: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database).

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> asc	asc	NONE	NONE
<input type="radio"/> cube	cube	NONE	NONE
<input type="radio"/> emc	emc	NONE	NONE
<input checked="" type="radio"/> imperium	imperium	NONE	NONE
<input type="radio"/> jacada	jacada	NONE	NONE
<input type="radio"/> nice	nice	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE

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

AVAYA Application Enablement Services Management Console

Last login: Tue Jan 6 16:29:28 2015 from 10.10.40.222
 Number of prior failed login attempts: 0
 HostName/IP: AES63VMPG/10.10.40.30
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 6.3.3.1.10-0
 Server Date and Time: Fri Jan 09 11:12:58 GMT 2015
 HA Status: Not Configured

Security | Security Database | CTI Users | List All Users Home | Help | Logout

Navigation menu: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security (Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database).

Edit CTI User

User Profile: User ID: imperium, Common Name: imperium, 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:

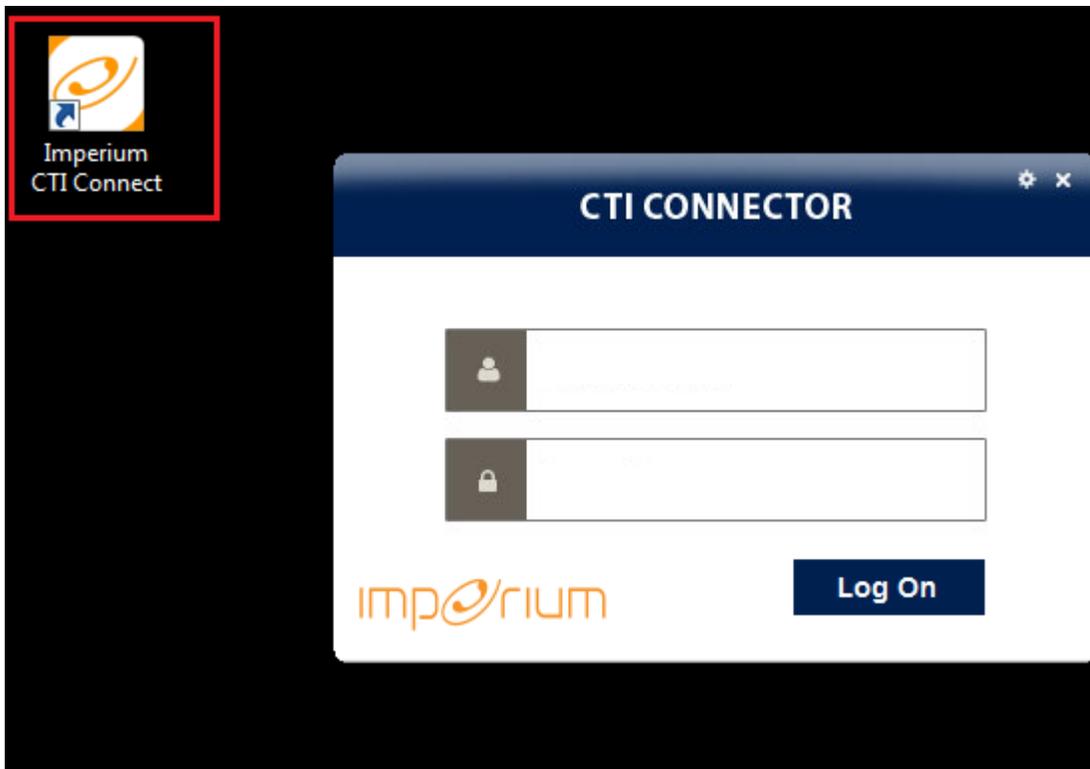
Routing Control: Allow Routing on Listed Devices: None

7. Configuration of Protocol Systems FZC Imperium CTI Connect Server

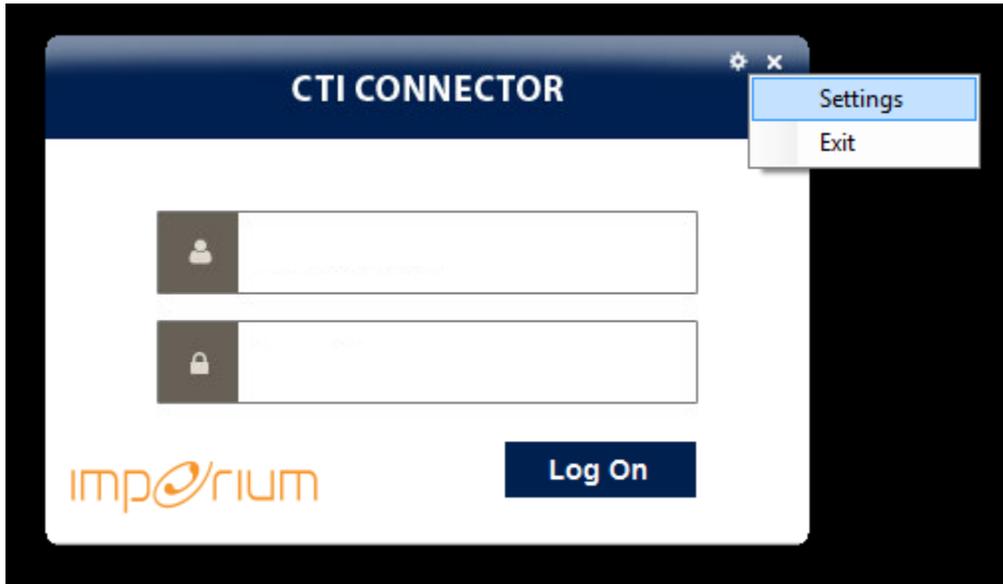
IMCC Server is installed on a Windows 2008 Server R2 running Microsoft SQL 2008 database. Each client connects to the IMCC Server in order to obtain information on each caller from a central database. Once a call is presented to an agent, the IMCC Agent Desktop can use the Call Line ID information obtained from Communication Manager to lookup the database on the IMCC Server and present to the agent all the customer information, including call history and case history associated with that CLID. Each agent that is running IMCC Agent Desktop will have a unique connection to the AES using DMCC for call control and to monitor the caller's information.

7.1. Configure Imperium CTI Connect Agent Desktop connection to Avaya Aura® Application Enablement Services

The connection of the IMCC Agent Desktop running on the client PC is configured as follows. Run the **Imperium CTI Connect** shortcut on the desktop. This will open the **CTI Connector** window as shown.



Click on the setting icon at the top of the window and select **Settings** as shown.



Enter the following information.

- **Extension** This is the Communication Manager's station number that is to be monitored.
- **Password** This is the password (Security Code) of the Communication Manager station as per **Section 5.5**.
- **DMCC Login** This is the username created in AES as per **Section 6.6**.
- **DMCC Password** This is the password of the AES user created in **Section 6.6**.
- **DMCC IP Address** This is the IP address of the AES server.
- **Connection Name** This is the switch connection name configured in AES as per **Section 6.3**.
- **DMCC Socket** This is the port that DMCC uses as per **Section 6.5**.
- **Main Prefix** This is the number used to dial out from the PBX.
- **Country Code** This is the country code for example **353** for Ireland.

Click on **OK** at the bottom of the screen once the information is filled in correctly.

The screenshot shows a 'CTI CONNECTOR' window with a 'SETTINGS' sub-window. The settings are as follows:

Field	Value
Extension	2015
Password	****
DMCC Login	imperium
DMCC Password	*****
DMCC IP address	10.10.40.30
Connection Name	CM63vmpg
DMCC Socket	4721
Main Prefix	9
Country Code	+353
Secure Socket	<input type="checkbox"/>

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the Avaya solution and Protocol Systems FZC Imperium CTI Connect.

8.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES 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 Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	aes63vmpg	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**.

Welcome: User craft
Last login: Thu Feb 20 11:01:32 2014 from 192.168.10.222
Number of prior failed login attempts: 33
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Thu Feb 20 11:14:02 UTC 2014

AVAYA Application Enablement Services Management Console

Status | Status and Control | TSAPI Service Summary Home | Help | Logout

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	CM63vmpg	1	Talking	Tue Feb 18 11:21:49 2014	Online	16	5	15	15	30

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

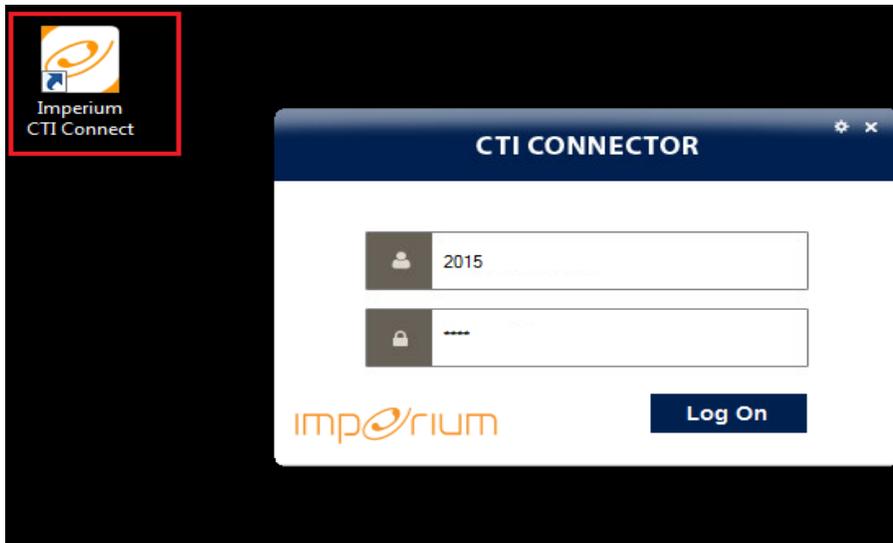
- AE Services
- Communication Manager Interface
- Licensing
- Maintenance
- Networking
- Security
- Status
 - Alarm Viewer
 - Log Manager
 - Logs
 - Status and Control
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - TSAPI Service Summary**

8.3. Verify 3rd Party Call Control using Imperium CTI Connect

The section will show the full working solution by demonstrating a call being made and answered from the IMCC Agent Desktop.

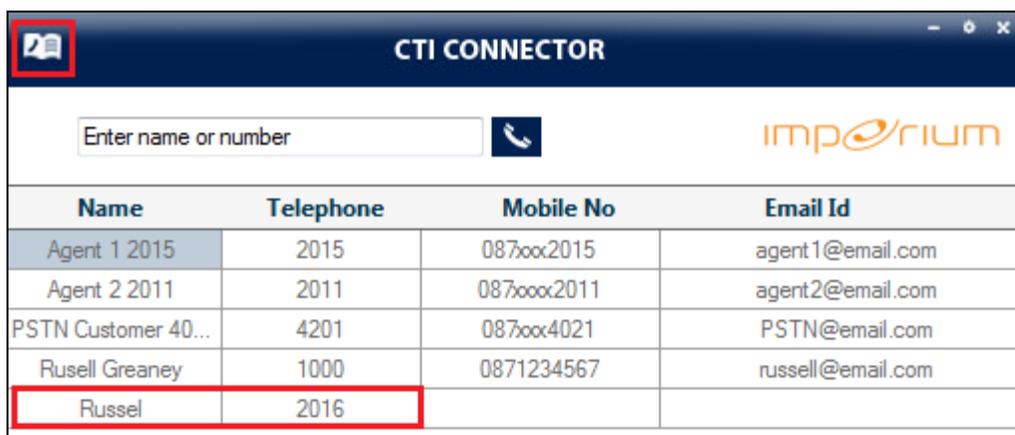
8.3.1. Log in to the Imperium CTI Connect Agent Desktop

Run the **Imperium CTI Connect** shortcut on the desktop. This will open the **CTI Connector** window as shown. Enter the correct username and password i.e., the Communication Manager station number and password, and click on **Log On**.

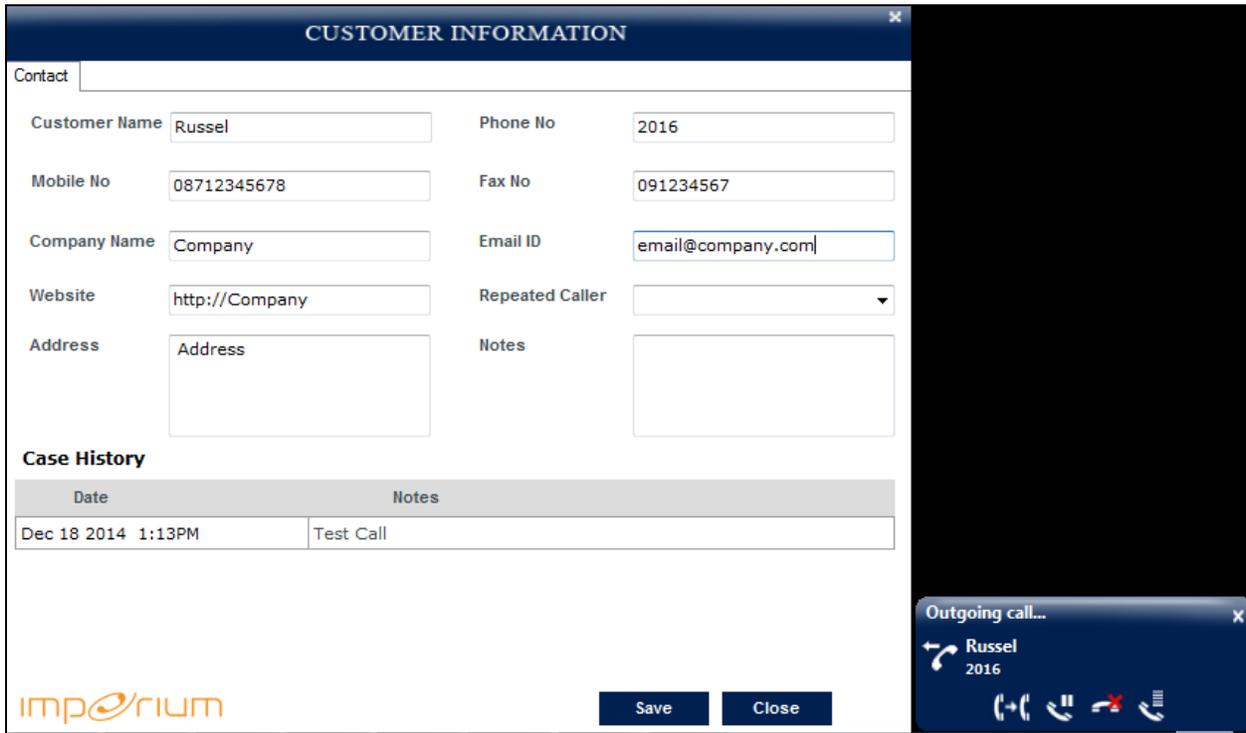


8.3.2. Make an outgoing call using Imperium CTI Connect Agent Desktop

Once logged in click on the phonebook icon at the top left to show the list of contacts and each of these contacts can be dialled by clicking on.



Clicking on the contact **Russel** above will initiate a new call from 2015 to **2016** as shown below. Note that a screen pop showing the customer information is presented to the agents screen.

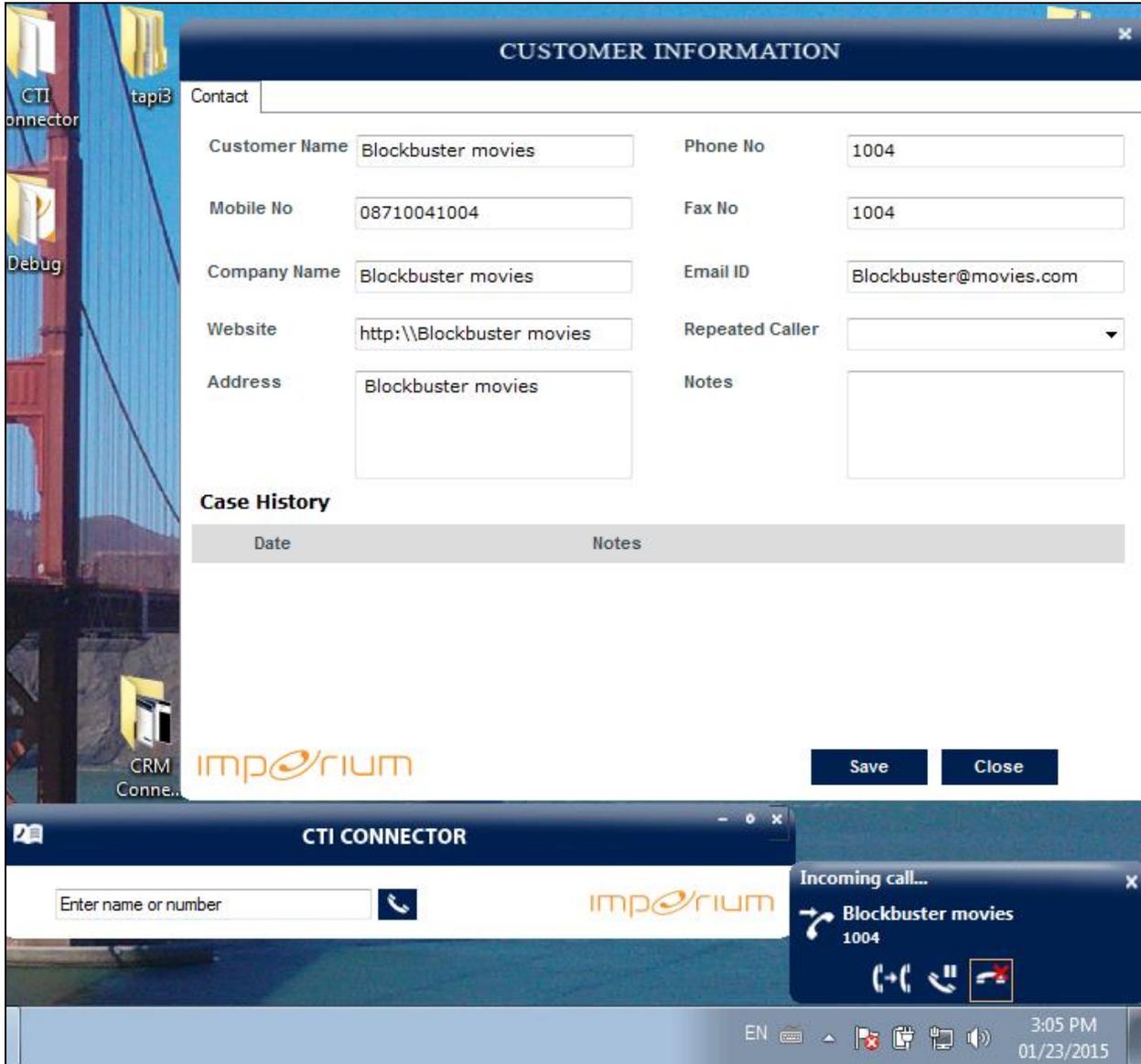


8.3.3. Answer an incoming call using Imperium CTI Connect Agent Desktop

An incoming call is presented to the agent as shown below. Click on the icon highlighted to answer the call with a screen pop of the customer's information.



A screen pop showing the customers information is shown. The call is ended by clicking on the icon highlighted at the bottom of the screen.



9. Conclusion

These Application Notes describe the configuration steps required for Protocol Systems FZC Imperium CTI Connect to successfully interoperate with Avaya Aura® Application Enablement Services R6.3 and Avaya Aura® Communication Manager R6.3. All feature functionality and serviceability test cases were completed successfully with all issues and observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and Protocol Systems FZC 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 6.3*

Technical documentation can be obtained for Imperium CTI Connect from the website <http://imperiumapp.com>

Support for Imperium CTI Connect can be reached at:
Protocol Systems FZC
Tel: +9716 5578383
Fax: +9716 5578384
Email: support@protocolsystems-me.com

Appendix

Avaya H.323 Deskphone

This is a printout of the Avaya 9620 H.323 Deskphone used during compliance testing.

Page 1.

```
display station 2015                                     Page 1 of 5
                                                    STATION
Extension: 2015                                         Lock Messages? n          BCC: M
  Type: 9620                                           Security Code: *         TN: 1
  Port: S00099                                         Coverage Path 1:        COR: 1
  Name: Imperium Agent 1                               Coverage Path 2:        COS: 1
                                                    Hunt-to Station:        Tests? y
STATION OPTIONS
  Location:                                           Time of Day Lock Table:
  Loss Group: 19                                     Personalized Ringing Pattern: 1
                                                    Message Lamp Ext: 2015
  Speakerphone: 2-way                                Mute Button Enabled? y
  Display Language: english
  Survivable GK Node Name:
  Survivable COR: internal                           Media Complex Ext:
  Survivable Trunk Dest? y                           IP SoftPhone? y
                                                    IP Video Softphone? y
                                                    Short/Prefixed Registration Allowed: default
                                                    Customizable Labels? y
```

Page 2.

```
display station 2015                                     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:                             Display Client Redirection? n
  AUDIX Name:                                        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: 2015                       Always Use? n IP Audio Hairpinning? n
```

Page 3.

```
display station 2015                                     Page 3 of 5
                                                    STATION
      Conf/Trans on Primary Appearance? n
      Bridged Appearance Origination Restriction? n      Offline Call Logging? y

      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: 2016              n
      External Calls To: 2016              n
      Busy For Internal Calls To: 2016              n
      External Calls To: 2016              n
      No Reply For Internal Calls To: 2016           n
      External Calls To: 2016              n

      SAC/CF Override: n
```

Page 4.

```
display station 2015                                     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              4:
  2: call-appr              5:
  3: call-appr              6:

  voice-mail
```

display station 2015		Page 5 of 5
	STATION	
BUTTON ASSIGNMENTS		
7:	10:	
8:	11:	
9:	12:	

©2015 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.