Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the configuration steps for Protocol Systems FZC Imperium CRM Connect for Microsoft Dynamics CRM to interoperate with Avaya Aura® Application Enablement Services R6.3 and Avaya Aura® Communication Manager R6.3. Imperium CRM Connect for Microsoft Dynamics CRM integrates with Avaya Aura® Application Enablement Services using a TSAPI and DMCC connection 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 CRM Connect for Microsoft Dynamics CRM in order to interoperate with Avaya Aura® Application Enablement Services R6.3 and Avaya Aura® Communication Manager R6.3. Imperium CRM Connect for Microsoft Dynamics CRM integrates with Avaya Aura® Application Enablement Services using a Telephony Server Application Programming Interface (TSAPI) and Device, Media and Call Control (DMCC) API for call control.

Imperium CRM Connect for Microsoft Dynamics CRM presents to the user information such as caller name and company information retrieved from the CRM Database and offers "click to open" for CRM records related to a Caller ID, such as a contact record, opportunities/orders list or a notes/activity record containing information from previous calls with the customer. It provides call handling options including: answer incoming call, release call before or after answering, initiate call, place call on hold, retrieve held call, transfer call to another contact or telephone number, view call history and list of missed calls.

Imperium CRM Connect for Microsoft Dynamics CRM (IMCC for MSCRM) uses the DMCC interface on AES in order to gain full control of Communication Manager endpoints. IMCC for MSCRM Agent Desktop 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 IMCC for MSCRM with AES and covers the general test approach and the test results.

IMCC for MSCRM consists of a server component and client component. The Server component is a Solution file which will be imported to customer's MSCRM server which will enable dialling contacts in various forms from within the MSCRM webpage itself. Once the contact is dialled the client component, called IMCC for MSCRM Agent Desktop, is triggered and it provides all call control functionalities like Call Hold, Transfer, Conference, Call Drop, Open activity from the IMCC for MSCRM Agent Desktop itself. IMCC for MSCRM Agent Desktop has a client tool which runs on a user's PC. When there is an incoming call, based on CLID the corresponding customer details is matched in MSCRM and a "New Activity" or "New Lead window" is opened with in MSCRM itself and the IMCC for MSCRM Agent Desktop provides all call control functionalities. Each user/agent that is running IMCC for MSCRM 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 for MSCRM Agent Desktop to gain control of existing Communication Manager endpoints and focused on the handling of calls offered to

Communication Manager by IMCC for MSCRM Agent Desktop. The serviceability testing focused on the ability of IMCC for MSCRM 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 manually making and receiving calls to Communication Manager. The tests included:

- **Basic calls** – Basic incoming and outgoing calls using IMCC for MSCRM Agent Desktop.
- **Call Hold** – Tests held calls using IMCC for MSCRM Agent Desktop.
- **Call Transfer** Tests transferred calls using IMCC for MSCRM Agent Desktop.
- **Call Conference** Tests conferenced calls using IMCC for MSCRM Agent Desktop.
- **Failover/Service** – Tests the behaviour of IMCC for MSCRM 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 issue 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 for MSCRM 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 CRM Connect for Microsoft Dynamics CRM from the website http://imperiumapp.com/contact.aspx or from the following:

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 Imperium CRM Connect for Microsoft Dynamics CRM from Protocol Systems FZC with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Application Enablement R6.3 to gain call control of the various Avaya endpoints as shown below. IMCC for MSCRM consists of a server component and client component. The server component is a solution file which will be imported to customer's MSCRM server which will enable dialling contacts in various forms from within the MSCRM webpage itself. The client component consists of IMCC for MSCRM Agent Desktop software running on each user/agent that will have a unique connection to the AES using DMCC for call control and to monitor the caller's information.

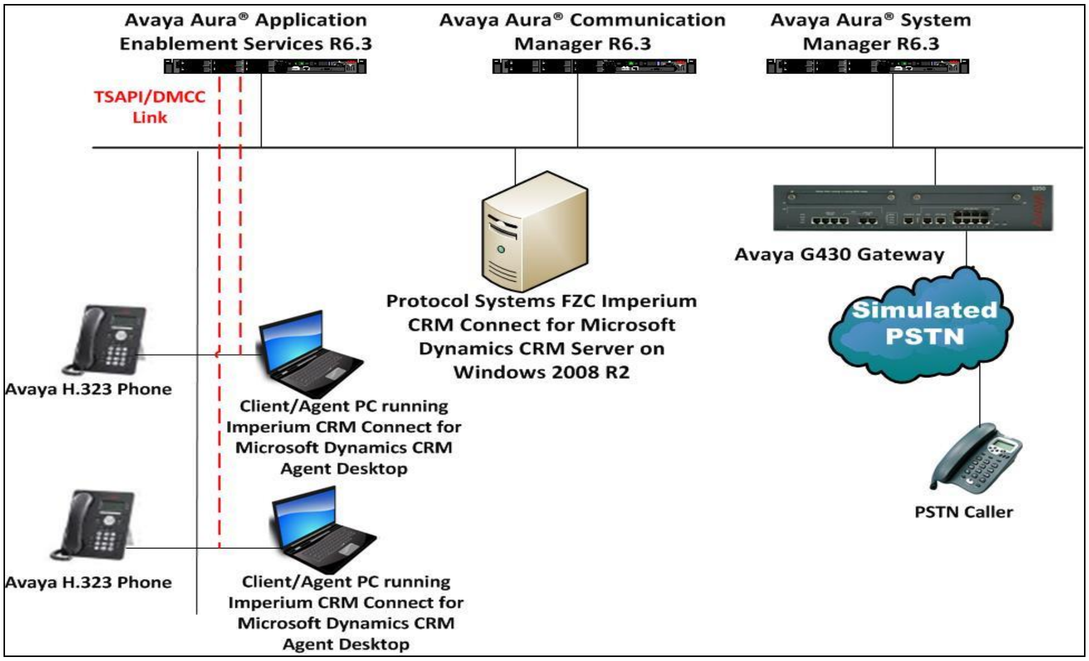

Avaya Aura® Application Enablement Services R6.3
Avaya Aura® Communication Manager R6.3
Avaya Aura® System Manager R6.3
TSAPI/DMCC Link
Avaya G430 Gateway
Simulated PSTN
Protocol Systems FZC Imperium CRM Connect for Microsoft Dynamics CRM Server on Windows 2008 R2
Avaya H.323 Phone
Client/Agent PC running Imperium CRM Connect for Microsoft Dynamics CRM Agent Desktop
PSTN Caller
Avaya H.323 Phone
Client/Agent PC running Imperium CRM Connect for Microsoft Dynamics CRM Agent Desktop

Figure 1: Connection of Imperium CRM Connect for Microsoft Dynamics CRM from Protocol Systems 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	96xx H.323 Release 6.4014U
Avaya 9620 H323 Deskphone	R3.186A
Windows 2008 Virtual Server Protocol Systems FZC Imperium CRM Connect for Microsoft Dynamics CRM **	Windows 2008 R2 R1.0
Windows 7 Client PC Imperium CRM Connect for Microsoft Dynamics CRM Agent Desktop	Windows 7 Enterprise R1.0

****Note:** IMCC Server Solution can be imported to the MSCRM Operating System: Depends on the Operating System being used by Customer. IMCC does not require separate server.

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                     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 **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, 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:         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 for MSCRM 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
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 1591
            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? n
                              Short/Prefixed Registration Allowed: default
```

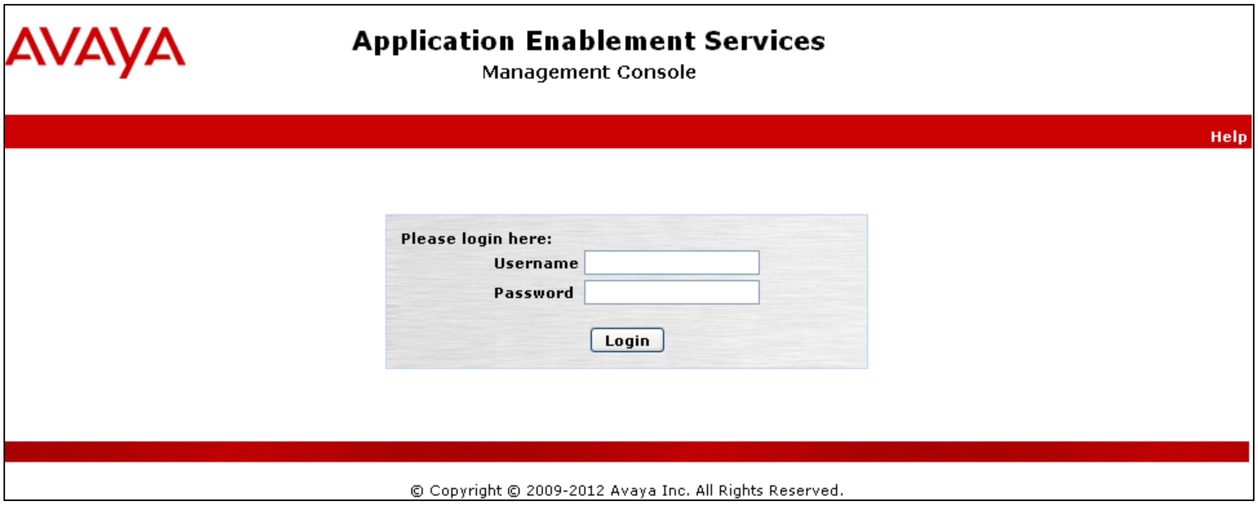
6. Configure Avaya Aura® Application Enablement Services

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

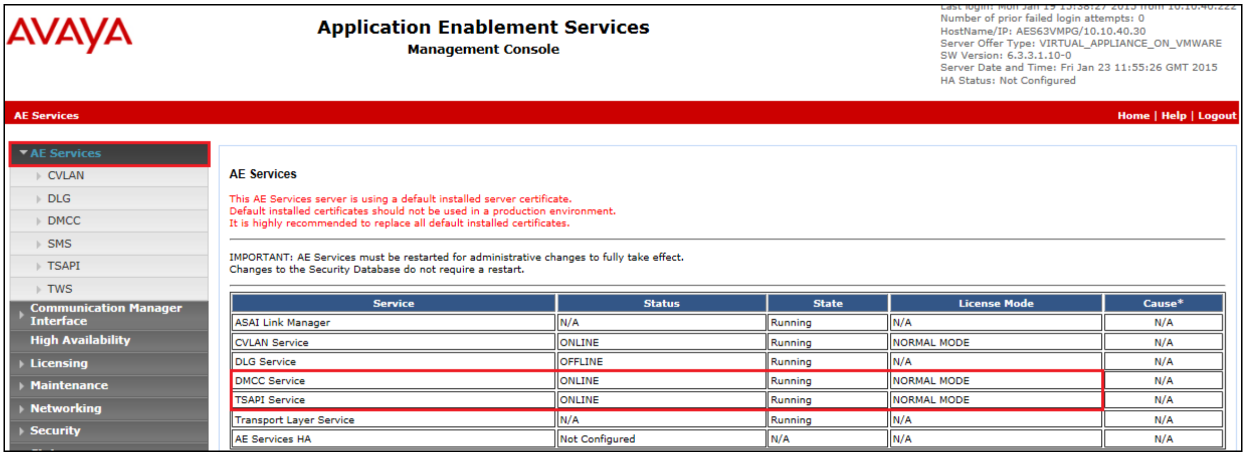
- Verify Licensing
- Create Switch Connection
- Administer TSAPI link
- Identify Tlinks
- Enable TSAPI & DMCC Ports
- Create CTI User
- Associate Devices with CTI User

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.


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Password
Login
© 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.



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 23 11:55:26 GMT 2015
HA Status: Not Configured

AE Services

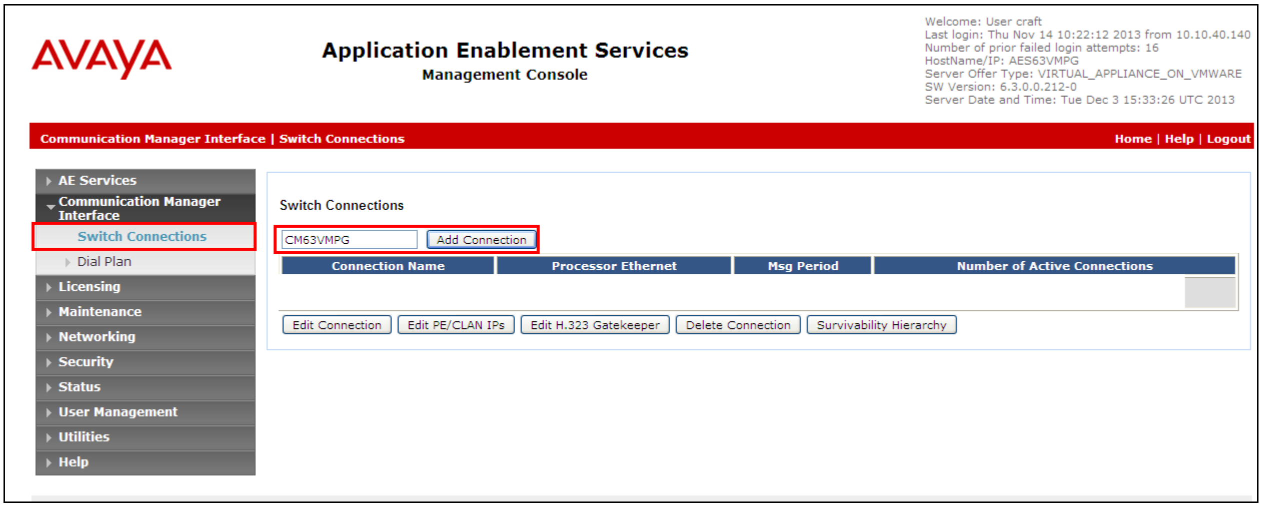
This AE Services server is using a default installed server certificate.
Default installed certificates should not be used in a production environment.
It is highly recommended to replace all default installed certificates.

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.



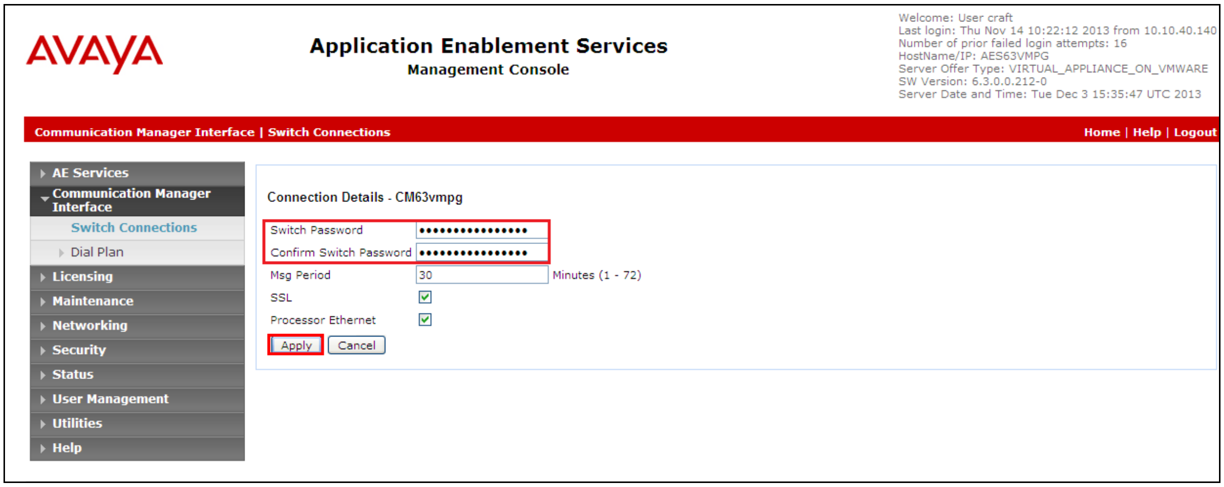
Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 3 15:33:26 UTC 2013

Switch Connections

CM63VMPG

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

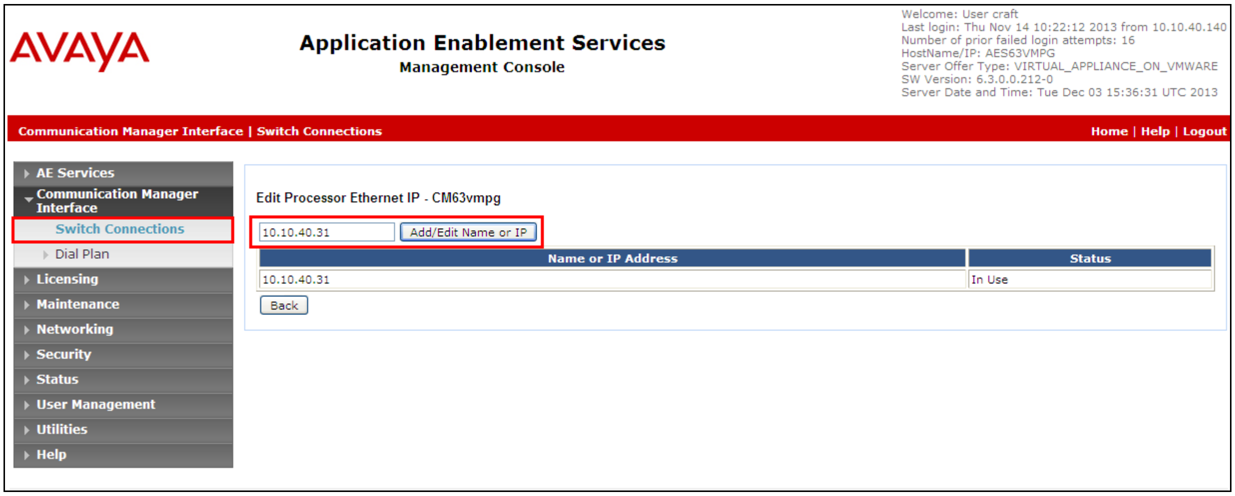


Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 3 15:35:47 UTC 2013

Connection Details - CM63vmpg

Switch Password	••••••••••••••••
Confirm Switch Password	••••••••••••••••
Msg Period	30 Minutes (1 - 72)
SSL	☑
Processor Ethernet	☑

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.



Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
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 15:36:31 UTC 2013

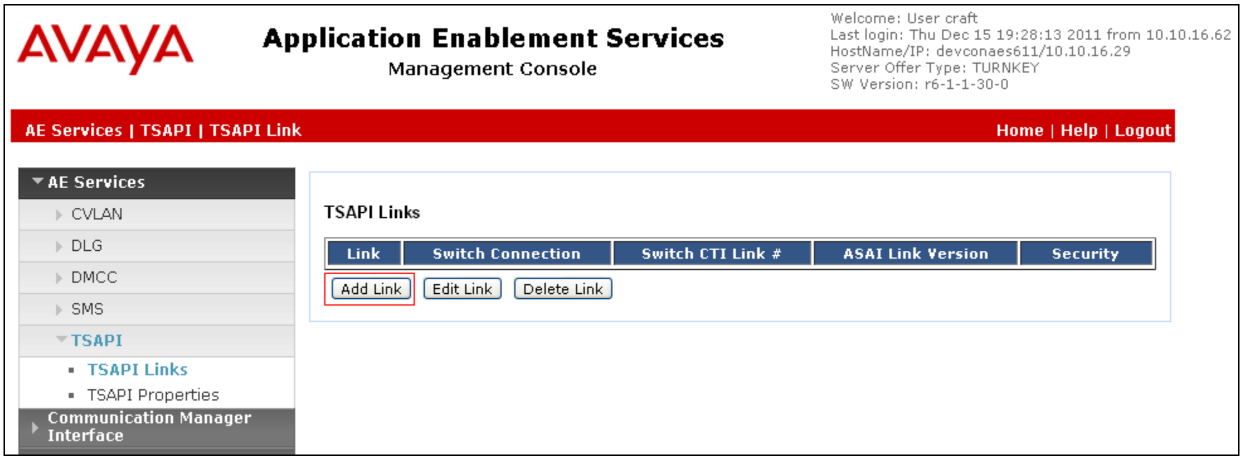
Edit Processor Ethernet IP - CM63vmpg

10.10.40.31

Name or IP Address	Status
10.10.40.31	In Use

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.



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

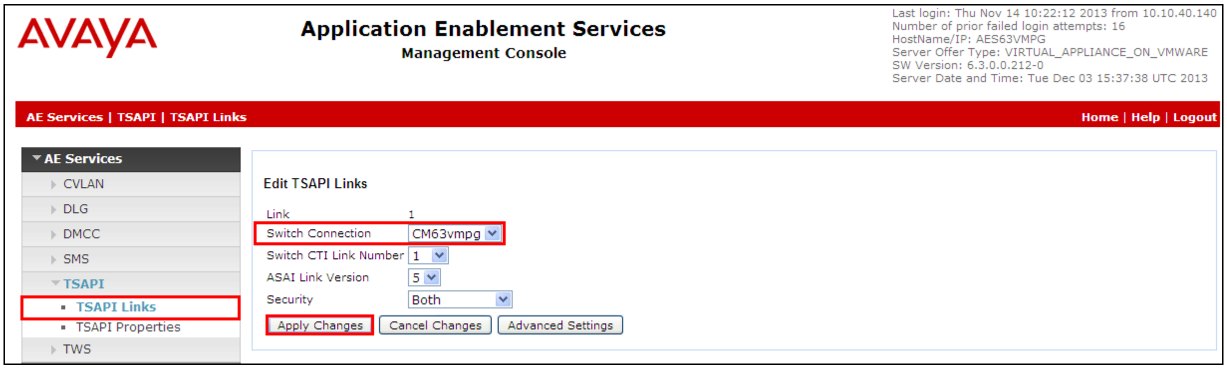
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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 **CM63VMPG**, 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**.

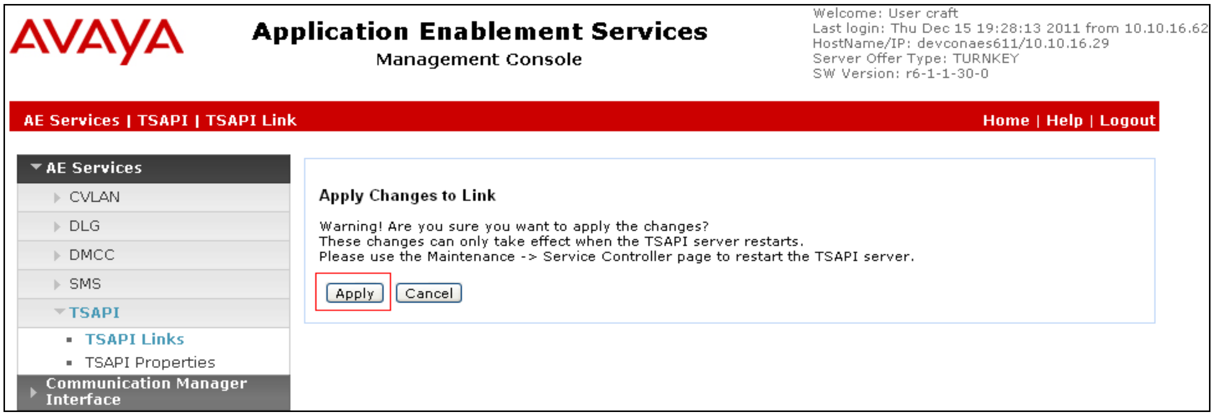


Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 15:37:38 UTC 2013

Edit TSAPI Links

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

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

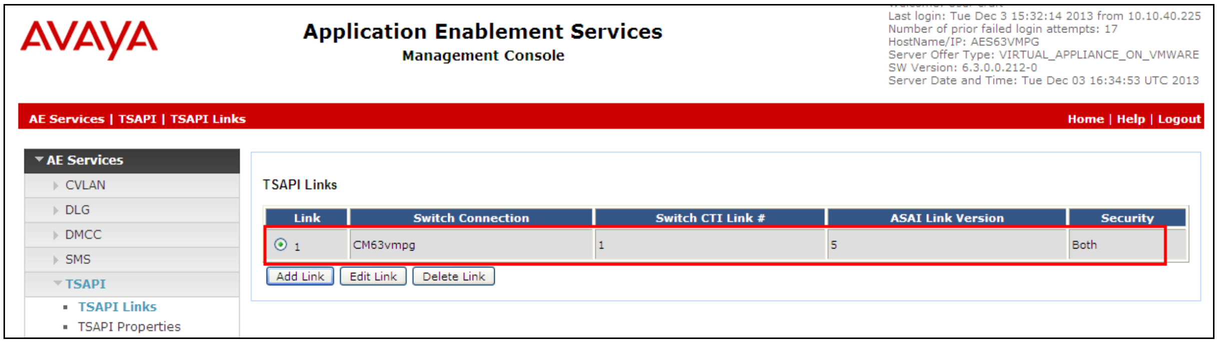


Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

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.

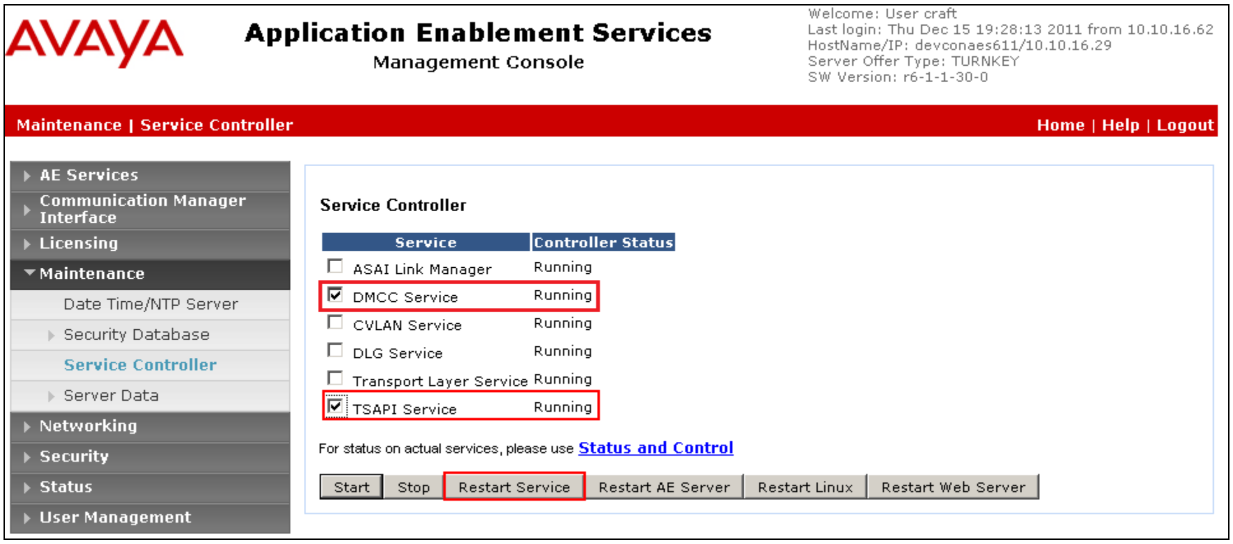


Last login: Tue Dec 3 15:32:14 2013 from 10.10.40.225
Number of prior failed login attempts: 17
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 16:34:53 UTC 2013

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**.



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

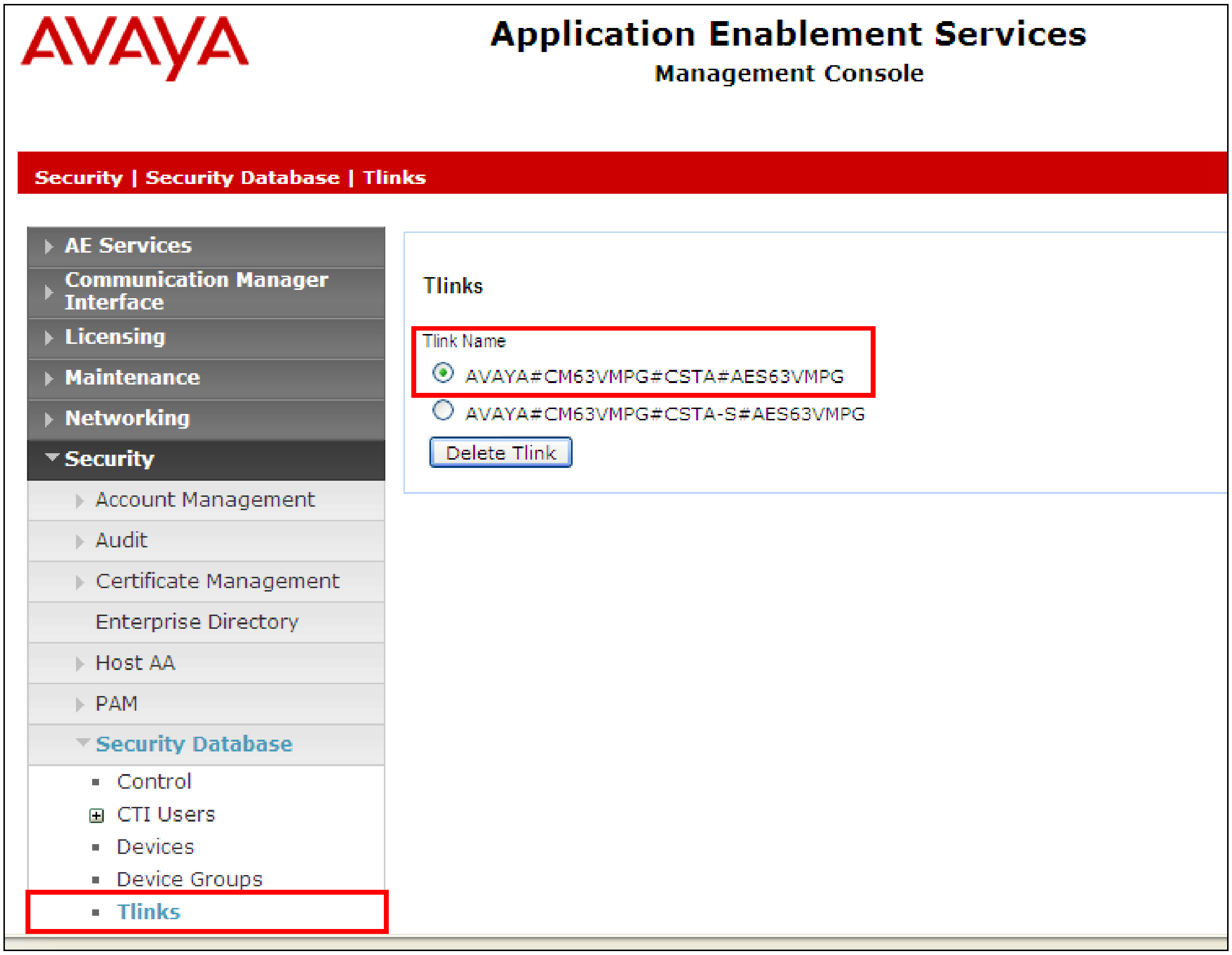
Service Controller

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**.



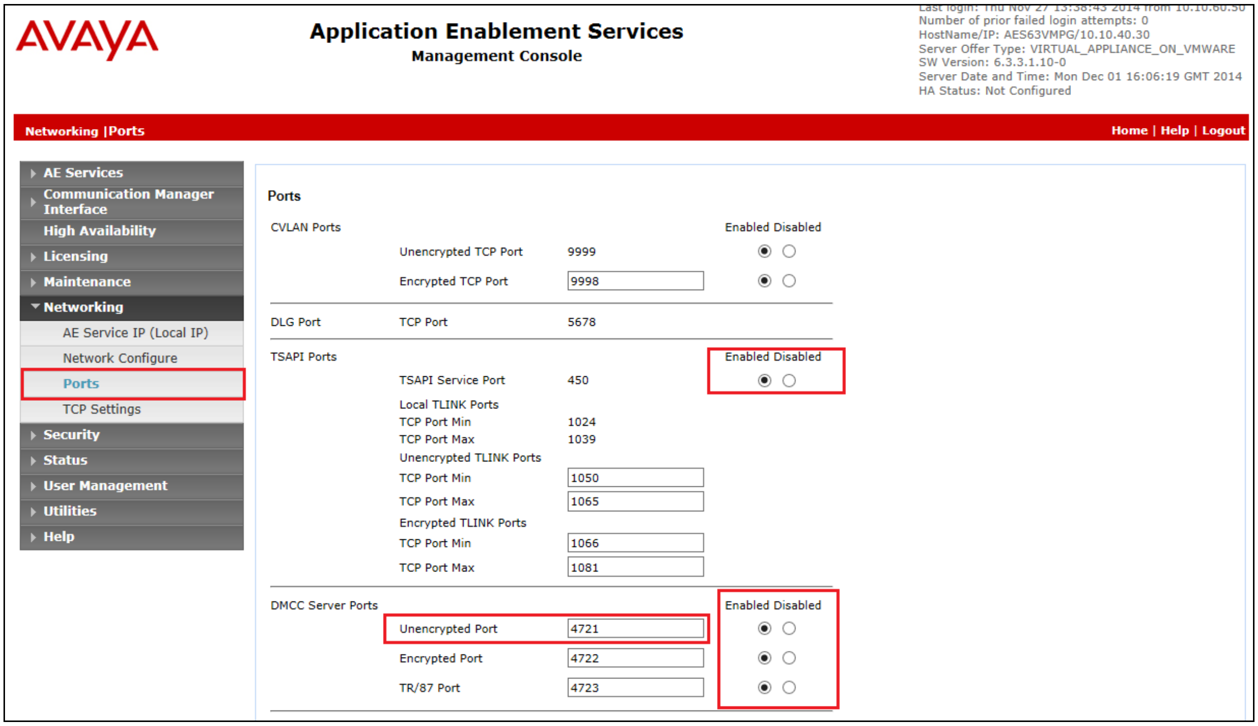
Tlink Name

● AVAYA#CM63VMPG#CSTA#AES63VMPG

○ AVAYA#CM63VMPG#CSTA-S#AES63VMPG

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**.



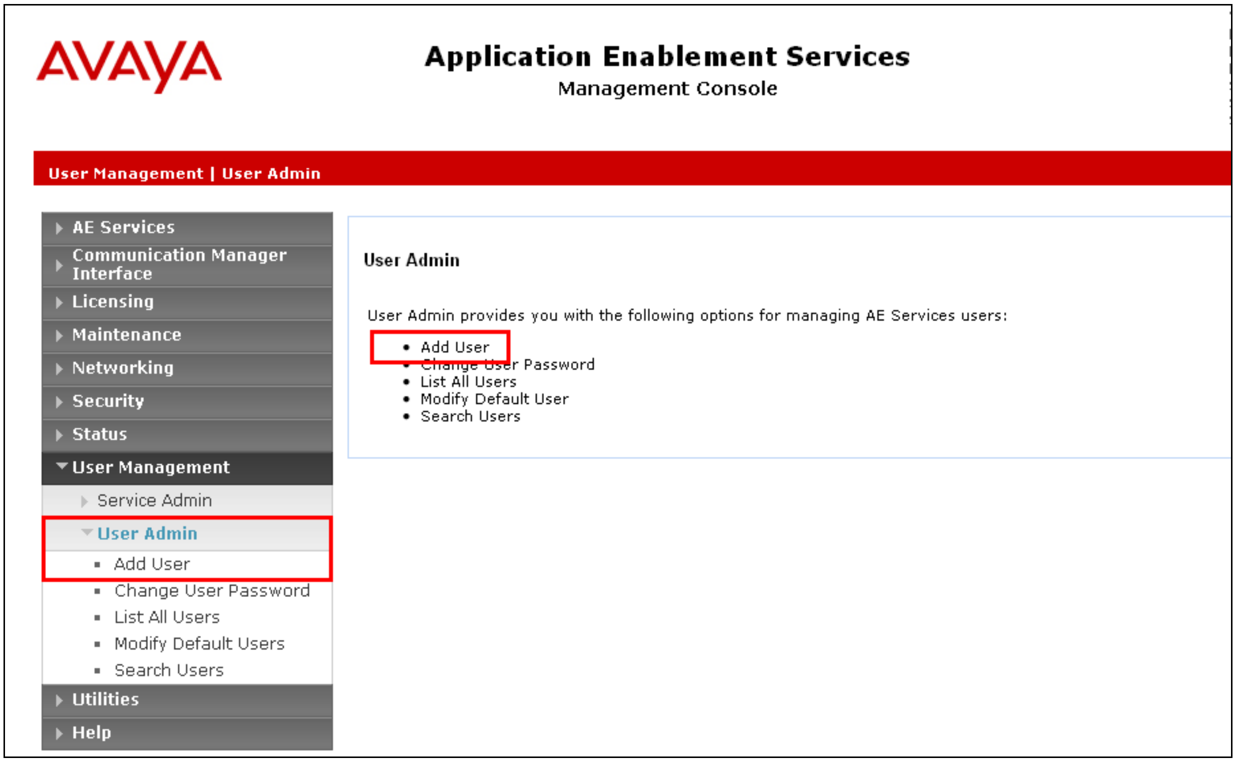
Last login: Thu Nov 27 13:38:43 2014 from 10.10.60.50
Number of prior failed login attempts: 0
HostName/IP: AES63VMPG/10.10.40.30
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.3.1.10-0
Server Date and Time: Mon Dec 01 16:06:19 GMT 2014
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports	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

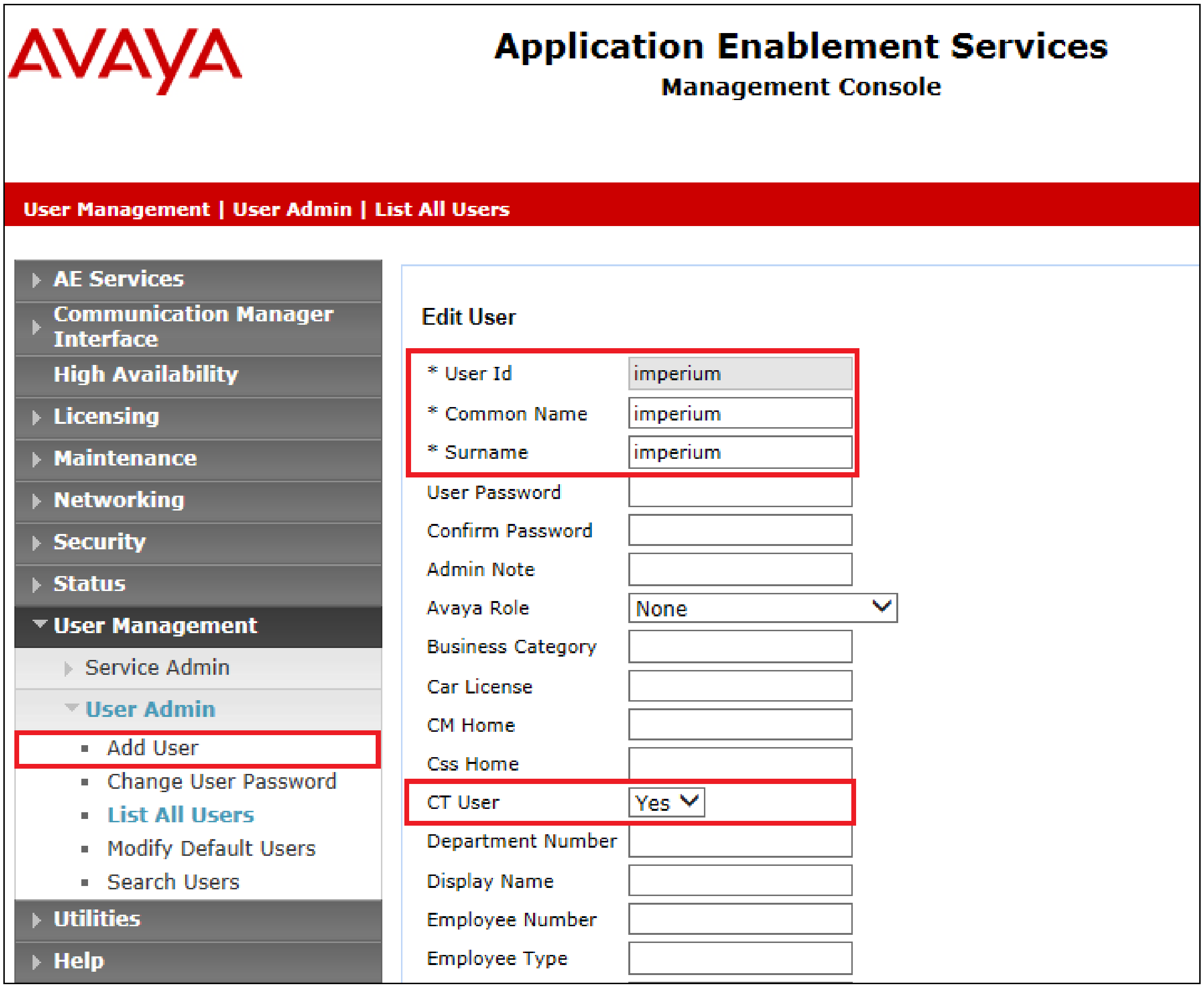
A User ID and password needs to be configured for IMCC for MSCRM Agent Desktop to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management** → **User Admin** screen then choose the **Add User** option.



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

- **User Id -** This will be used by the IMCC for MSCRM 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 the IMCC for MSCRM 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).



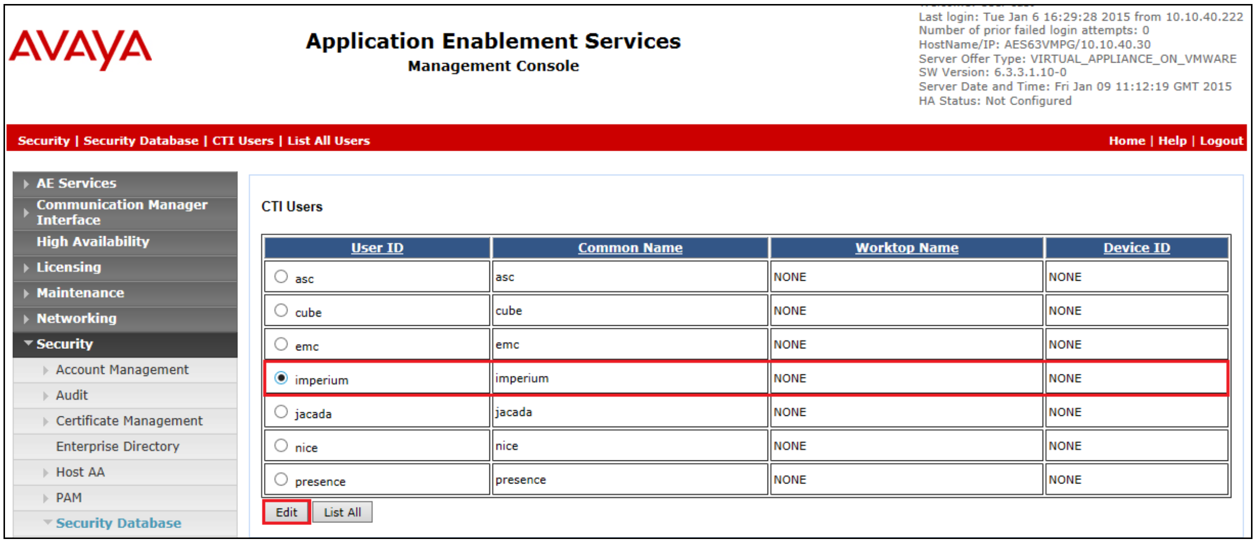
Edit User

* 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

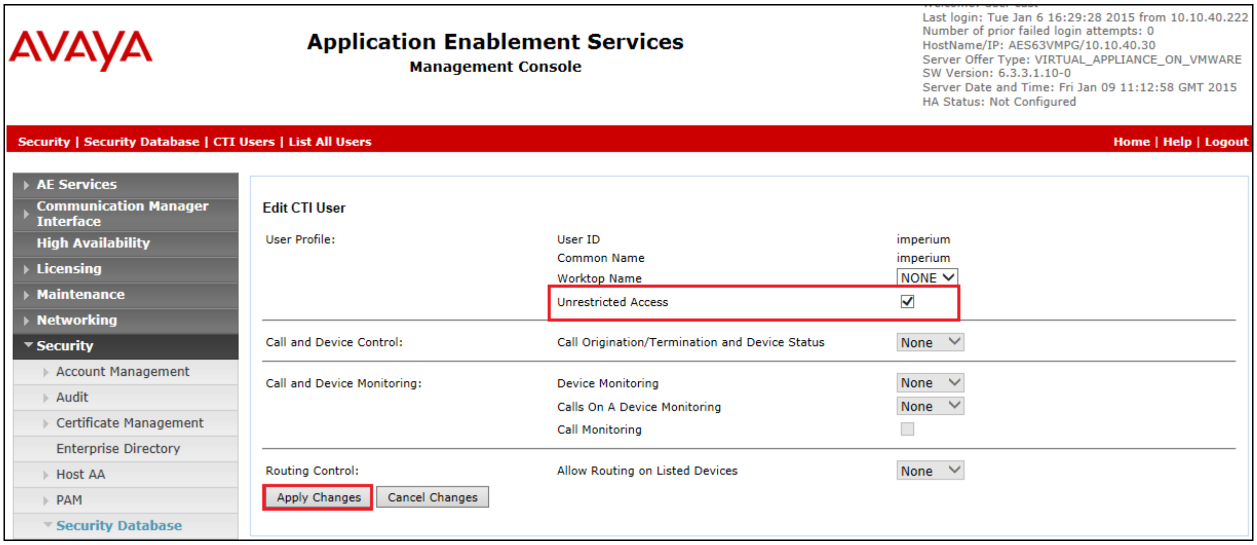
Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users** select the **imperium** user and click on **Edit**.



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

User ID	Common Name	Worktop Name	Device ID
○ asc	asc	NONE	NONE
○ cube	cube	NONE	NONE
○ emc	emc	NONE	NONE
● imperium	imperium	NONE	NONE
○ jacada	jacada	NONE	NONE
○ nice	nice	NONE	NONE
○ presence	presence	NONE	NONE

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



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

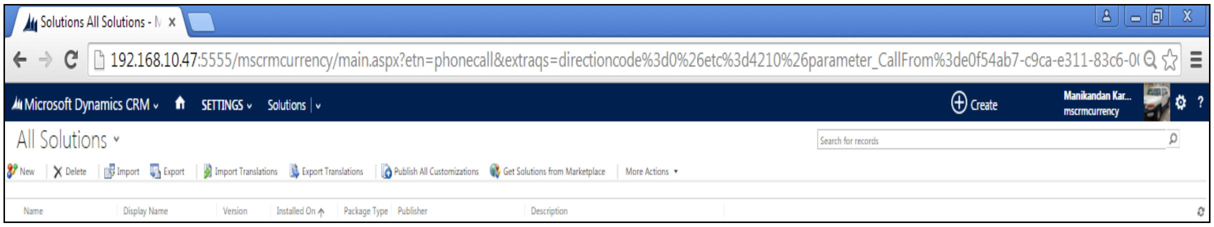
User Profile:	User ID	imperium
	Common Name	imperium
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	☐
Routing Control:	Allow Routing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

7. Configuration of Protocol Systems FZC Imperium CRM Connect for Microsoft Dynamics CRM

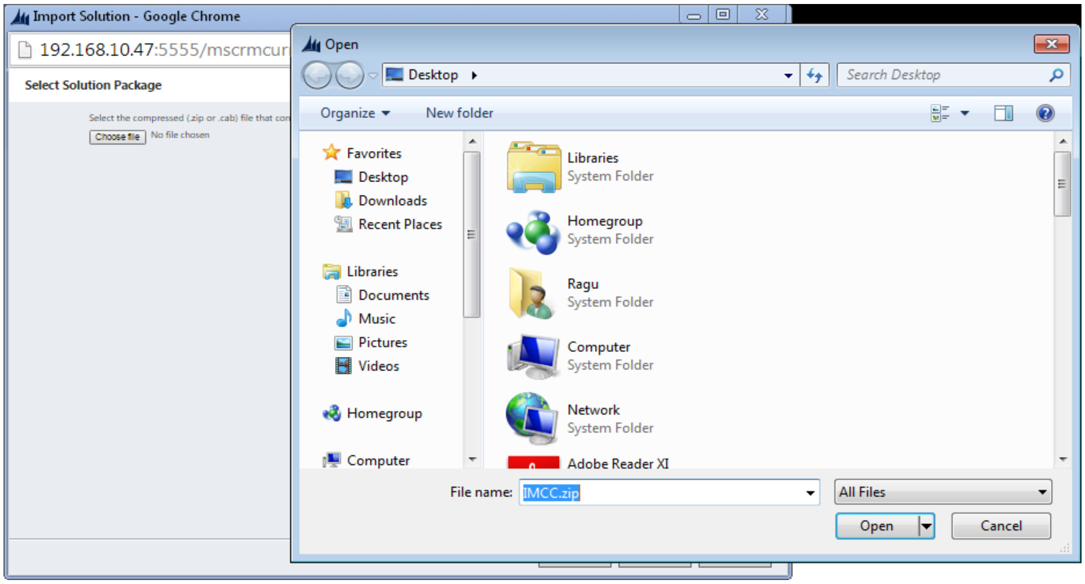
The IMCC for MSCRM Server Solution is imported to MSCRM which customer is already running and it does not require any separate server. IMCC for MSCRM Agent Desktop will connect to the IMCC for MSCRM Server in order to obtain information on each caller from a central database. Once a call is presented to an agent the IMCC for MSCRM Agent desktop can use the Call Line ID information obtained from Communication Manager to lookup the MSCRM and present to the agent all the customer information associated with that CLID. Each agent that is running IMCC for MSCRM Agent desktop will have a unique connection to the AES using DMCC for call control and to monitor the caller's information.

7.1. Importing Imperium CRM Connect for Microsoft Dynamics CRM Solution Template

The setup of the Imperium CRM Connect for Microsoft Dynamics CRM Solution is done by engineers from Protocol Systems FZC and is therefore outside the scope of these Application Notes. However a quick outline of the procedure is included in this section. Protocol Systems FZC will share a solution template which will be imported to the MSCRM as a Managed solution. Browse to **Settings → Solutions** in the MSCRM console.



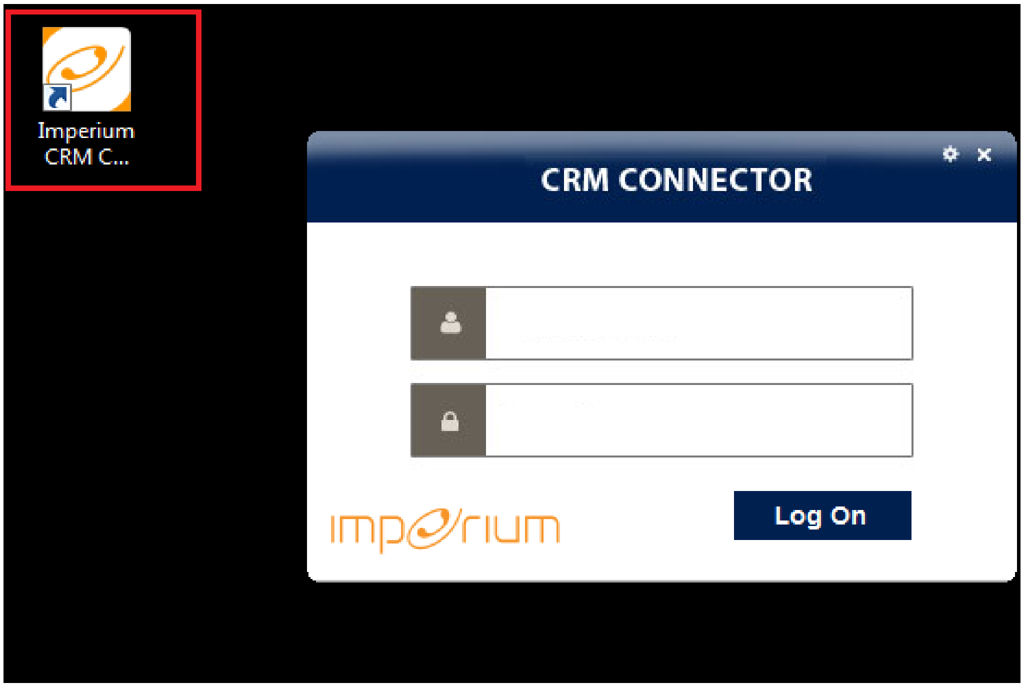
Select **Choose File** and browse to the provided solution template file which is in ZIP format.



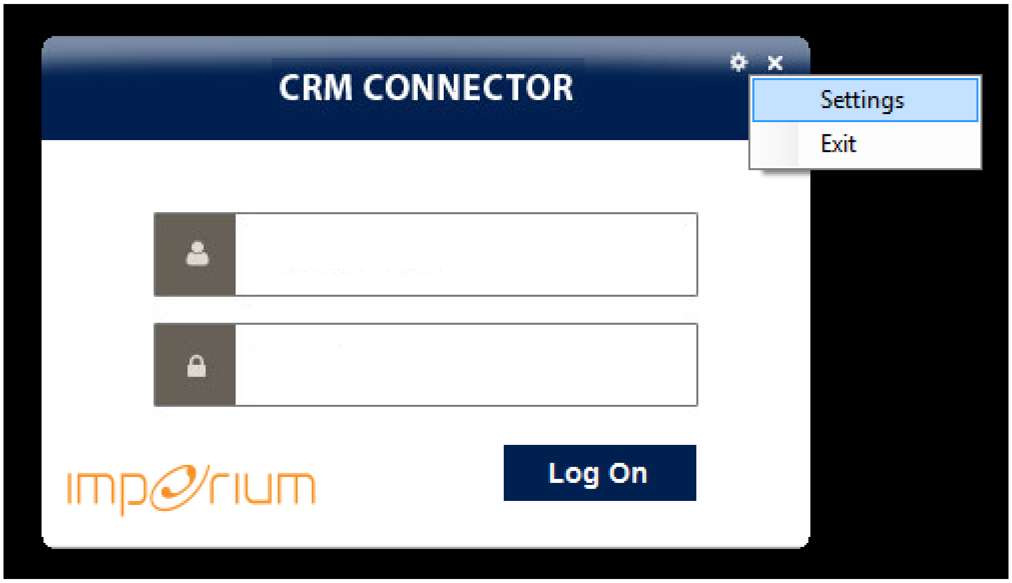
File name: IMCC.zip

7.2. Configure Imperium CRM Connect for Microsoft Dynamics CRM Agent Desktop connection to Avaya Aura® Application Enablement Services

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



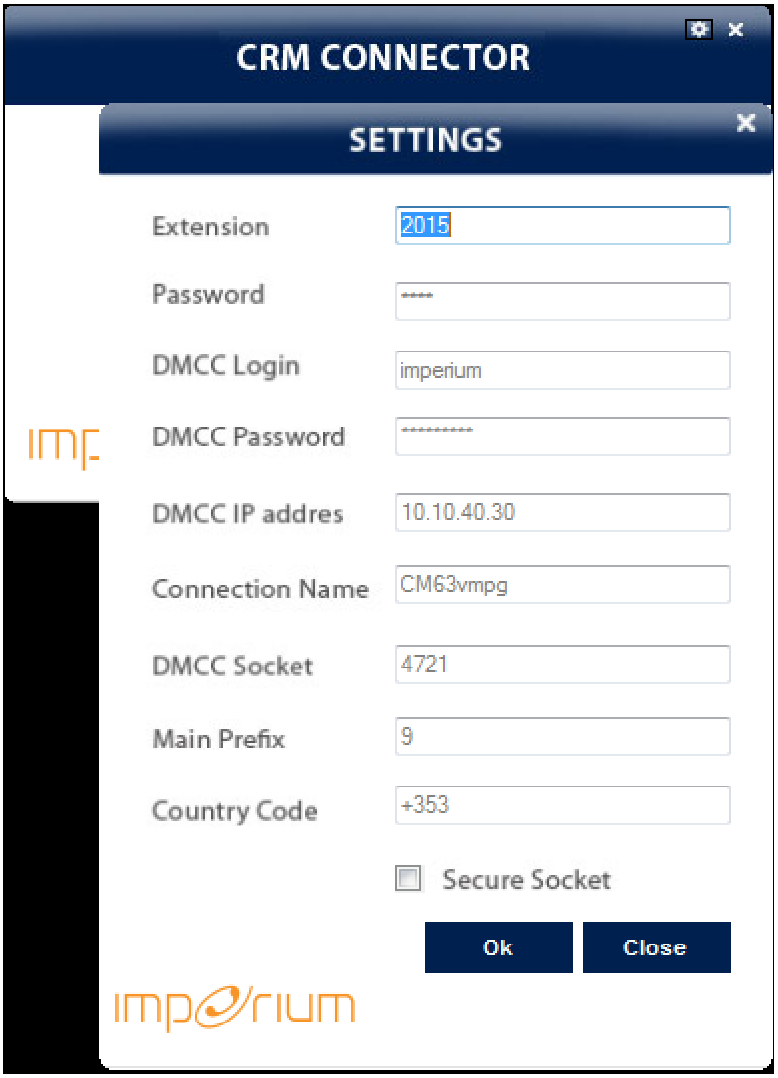
Click on the setting icon at the top of the window and select **Settings** as shown.



Enter the following information.

Extension	This is the Communication Manager station or extension 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.



Extension	2015
Password	*****
DMCC Login	imperium
DMCC Password	**********
DMCC IP addres	10.10.40.30
Connection Name	CM63vmpg
DMCC Socket	4721
Main Prefix	9
Country Code	+353

☐ Secure Socket

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 CRM Connect for Microsoft Dynamics CRM.

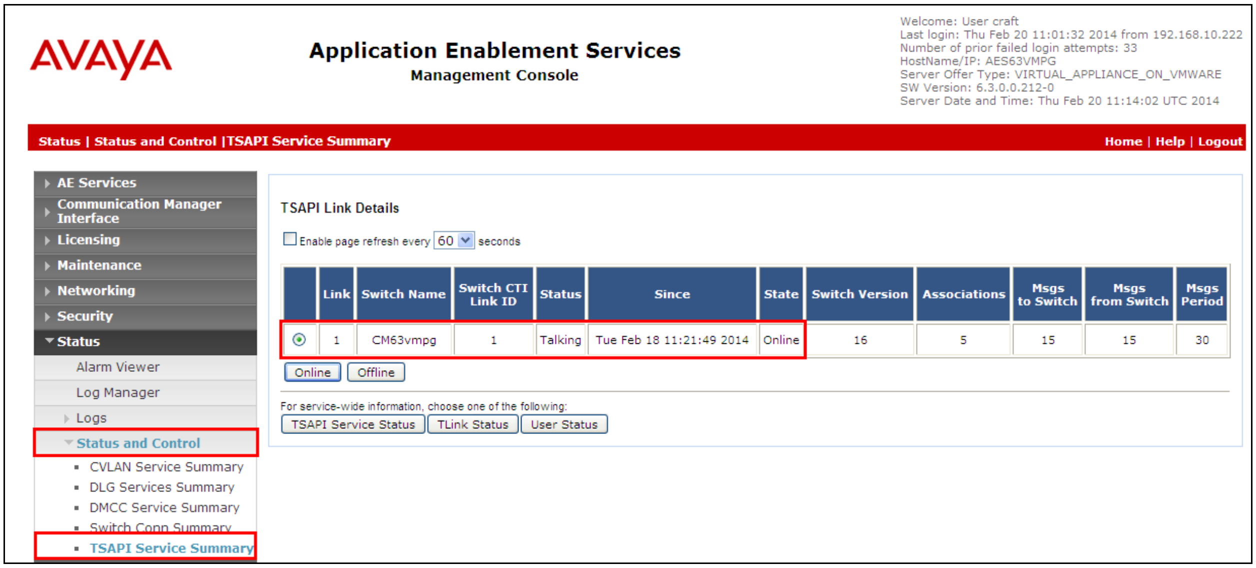
8.1. Verify Avaya Aura® Communication Manager CTI Service State

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

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:

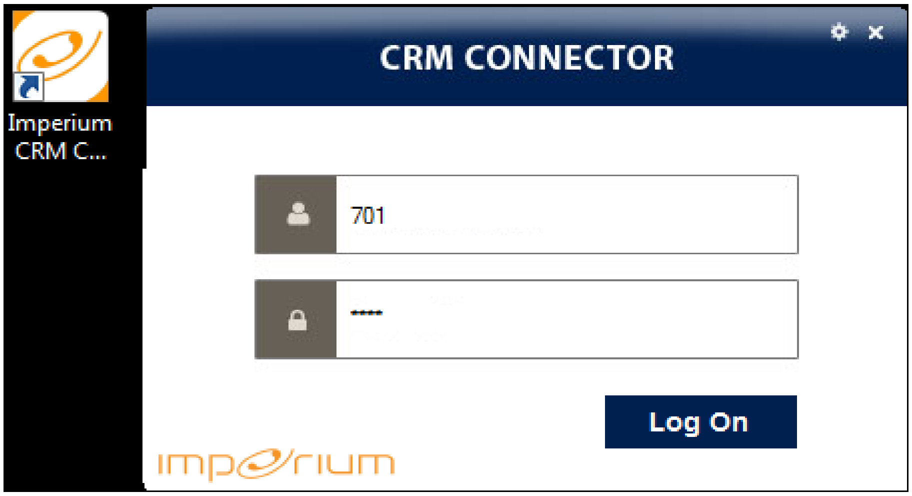
8.3. Verify 3rd Party Call Control using Imperium CRM Connect for Microsoft Dynamics CRM Agent Desktop

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

Note: The example calls shown below are not taken from the system tested during compliance testing. Rather these were taken from a fully working system connected to a Microsoft CRM database.

8.3.1. Log in to the Imperium CRM Connect for Microsoft Dynamics CRM Agent Desktop

Run the **Imperium CRM Connect** shortcut on the desktop. This will open the IMCC for MSCRM Agent Desktop window as shown. Enter the correct username and password i.e., the Communication Manager station number and password, and click on **Log On**.

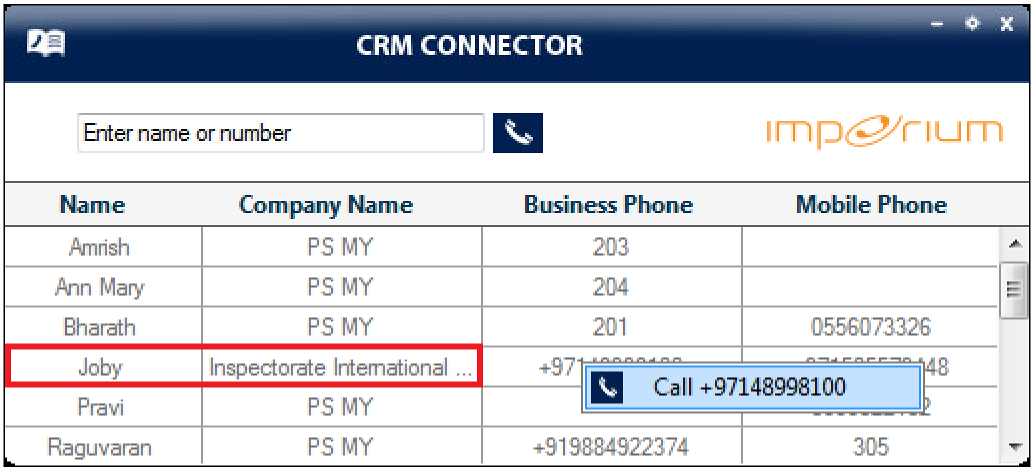


701

****

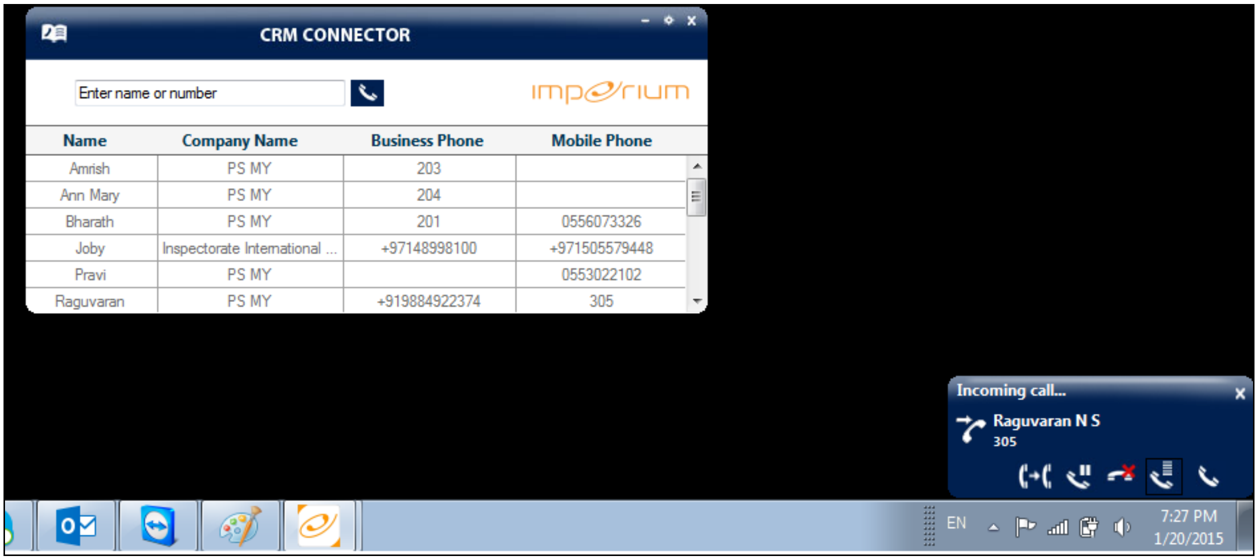
8.3.2. Make an outgoing call using Imperium CRM Connect for Microsoft Dynamics CRM Agent Desktop

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 right clicking on the name and selecting **Call** as is shown.



Name	Company Name	Business Phone	Mobile Phone
Amrish	PS MY	203	
Ann Mary	PS MY	204	
Bharath	PS MY	201	0556073326
Joby	Inspectorate International ...	+97	48
Pravi	PS MY		2
Raguvaran	PS MY	+919884922374	305

On the second agents PC this can be seen as an **Incoming call**.

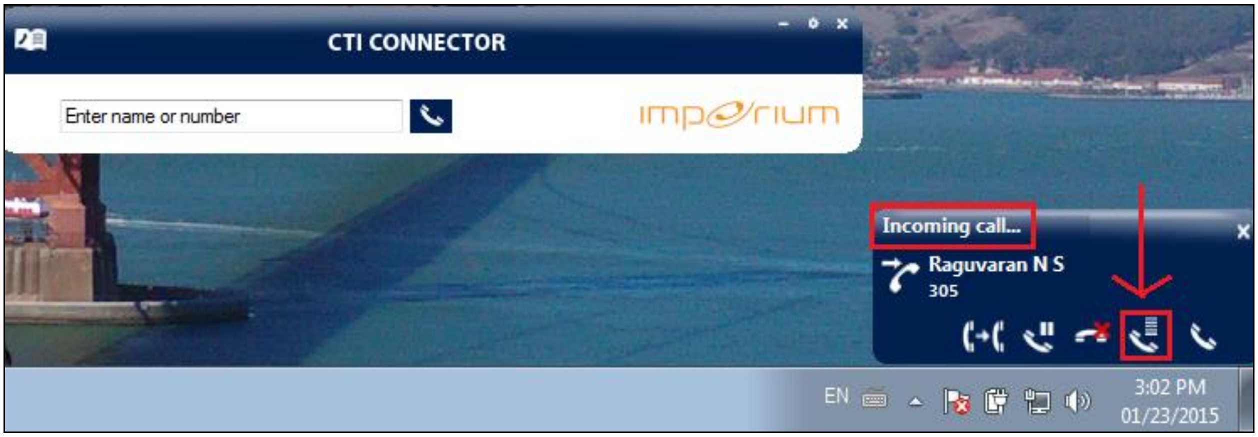


Name	Company Name	Business Phone	Mobile Phone
Amrish	PS MY	203	
Ann Mary	PS MY	204	
Bharath	PS MY	201	0556073326
Joby	Inspectorate International ...	+97148998100	+971505579448
Pravi	PS MY		0553022102
Raguvaran	PS MY	+919884922374	305

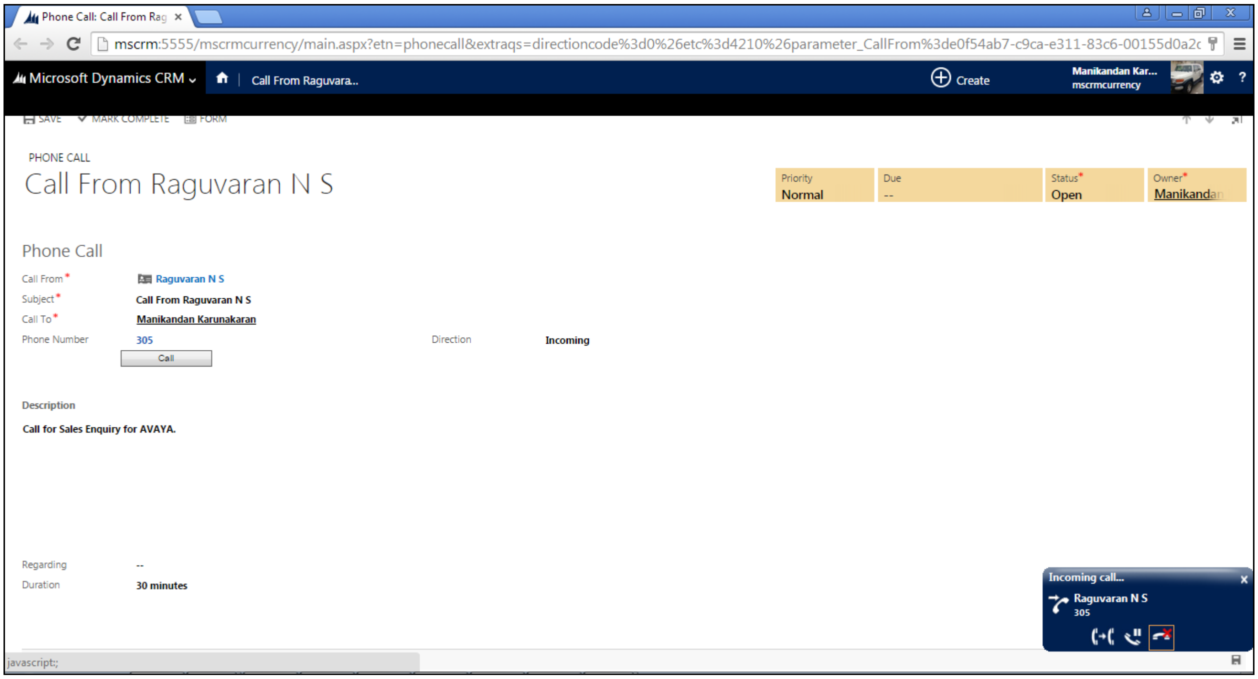
Incoming call...
Raguvaran N S
305

8.3.3. Answer an incoming call using Imperium CRM Connect for Microsoft Dynamics CRM 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.


Phone Call: Call From Rag
mscrm:5555/mscrmcurrency/main.aspx?etn=phonecall&extraqs=directioncode%3d0%26etc%3d4210%26parameter_CallFrom%3de0f54ab7-c9ca-e311-83c6-00155d0a2c
Microsoft Dynamics CRM
Call From Raguvara...
Create
Manikandan Kar...
mscrmcurrency
SAVE
MARK COMPLETE
FORM
Call
Incoming call...
Raguvaran N S
305
javascript:;

PHONE CALL

Call From Raguvaran N S

Priority	Due	Status*	Owner*
Normal	--	Open	Manikandan

Phone Call

Call From* Raguvaran N S

Subject* Call From Raguvaran N S

Call To* Manikandan Karunakaran

Phone Number 305

Direction Incoming

Description

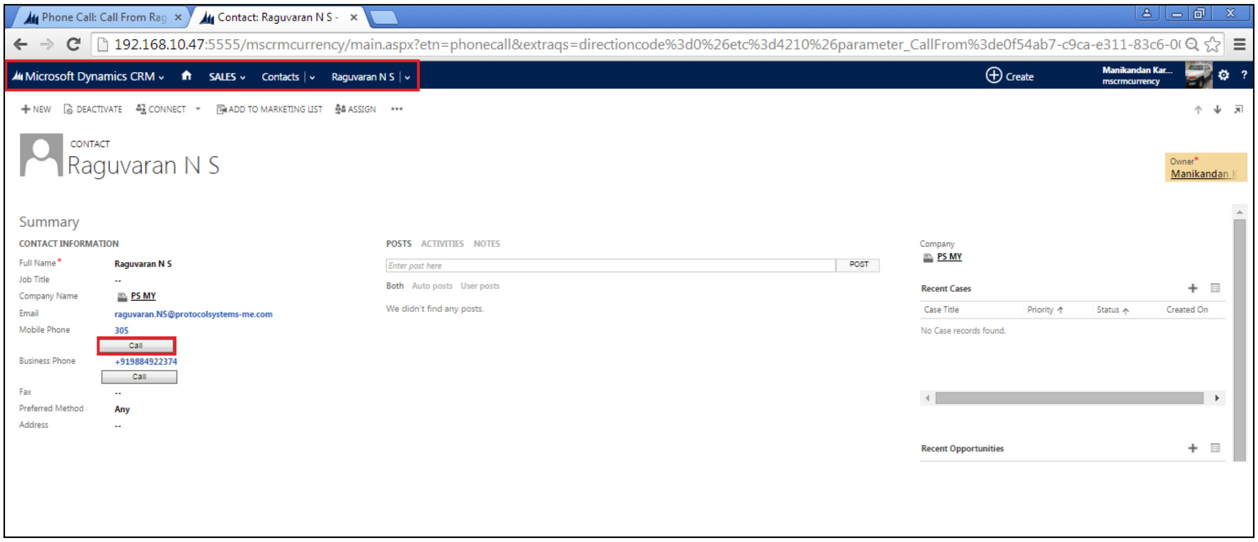
Call for Sales Enquiry for AVAYA.

Regarding --

Duration 30 minutes

8.4. Make an outgoing using Imperium CRM Connect for Microsoft Dynamics CRM to click to call

With IMCC for MSCRM users can make a call from within the MSCRM web interface itself from the Contacts page, Accounts Page, Phone Activity page, etc. In the example below of the MSCRM web interface, navigate to **Microsoft Dynamics CRM → Sales → Contacts** and click on a contact and press the **Call** button which will then make a call out.



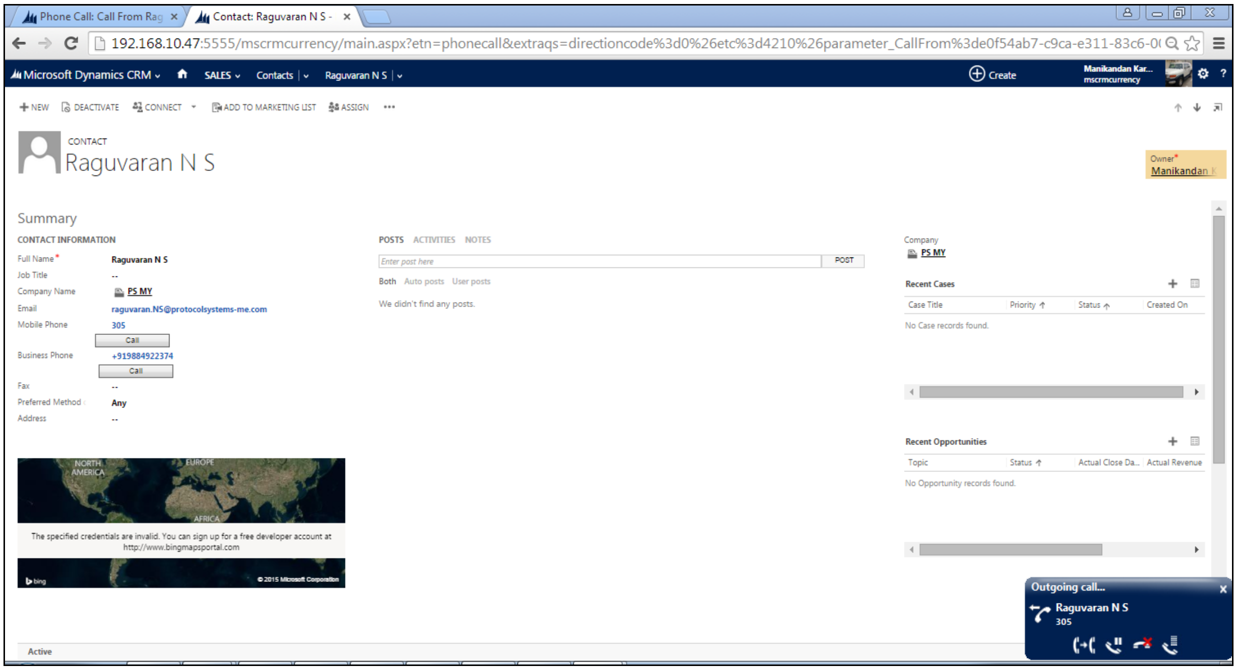
Full Name* Raguvaran N S
Job Title --
Company Name PS MY
Email raguvaran.NS@protocolsystems-me.com
Mobile Phone 305
Business Phone +919884922374
Fax --
Preferred Method Any
Address --

We didn't find any posts.

Company PS MY

No Case records found.

This call is then seen as on outgoing call as highlighted at the bottom right of the screen.



CONTACT

Raguvaran N S

Owner* Manikandan K

Summary

CONTACT INFORMATION

Full Name*: Raguvaran N S
Job Title: --
Company Name: PS MY
Email: raguvaran.NS@protocolsystems-me.com
Mobile Phone: 305 [Call]
Business Phone: +919884922374 [Call]
Fax: --
Preferred Method: Any
Address: --

Enter post here

We didn't find any posts.

The specified credentials are invalid. You can sign up for a free developer account at http://www.bingmapsportal.com

Company: PS MY

Recent Cases

Case Title	Priority ↑	Status ↑	Created On

No Case records found.

Recent Opportunities

Topic	Status ↑	Actual Close Da...	Actual Revenue

No Opportunity records found.

Active

Outgoing call...
Raguvaran N S
305

9. Conclusion

These Application Notes describe the configuration steps required for Protocol Systems FZC Imperium CRM Connect for Microsoft Dynamics CRM 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 any 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 CRM Connect for Microsoft Dynamics CRM from the website http://imperiumapp.com/

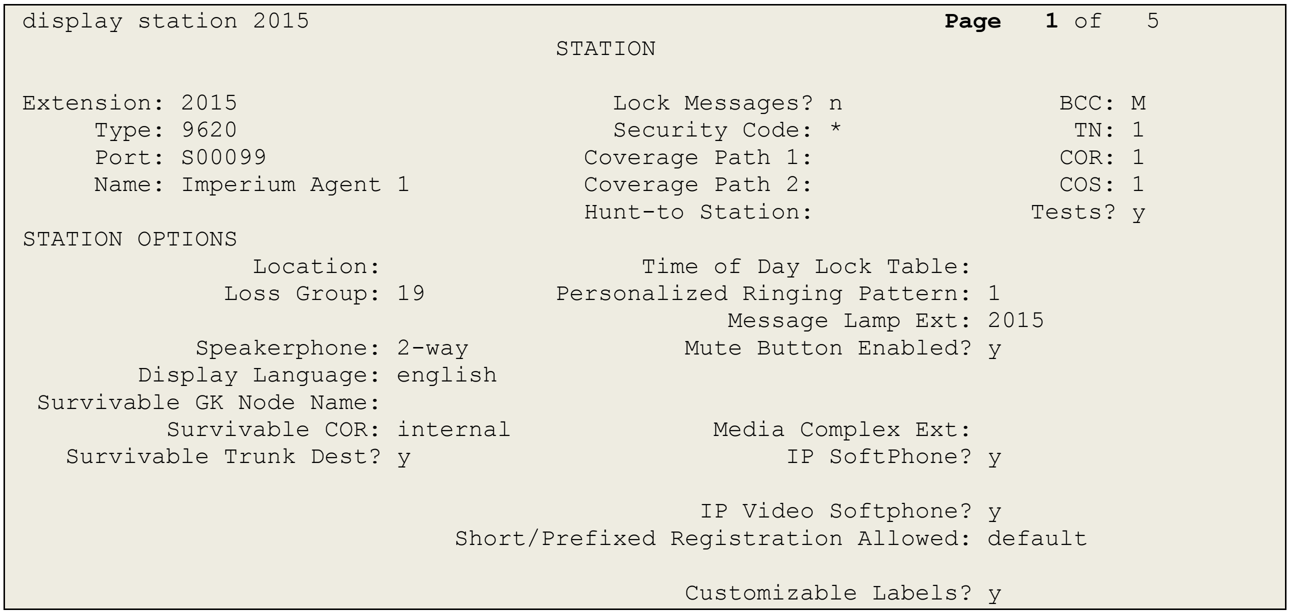
Support for Imperium Reporter can be found at:
Protocol Systems FZC
Tel: +9716 5578383
Fax: +9716 5578384
Email: support@protocolsystems-me.com

Appendix

Avaya H.323 Deskphone

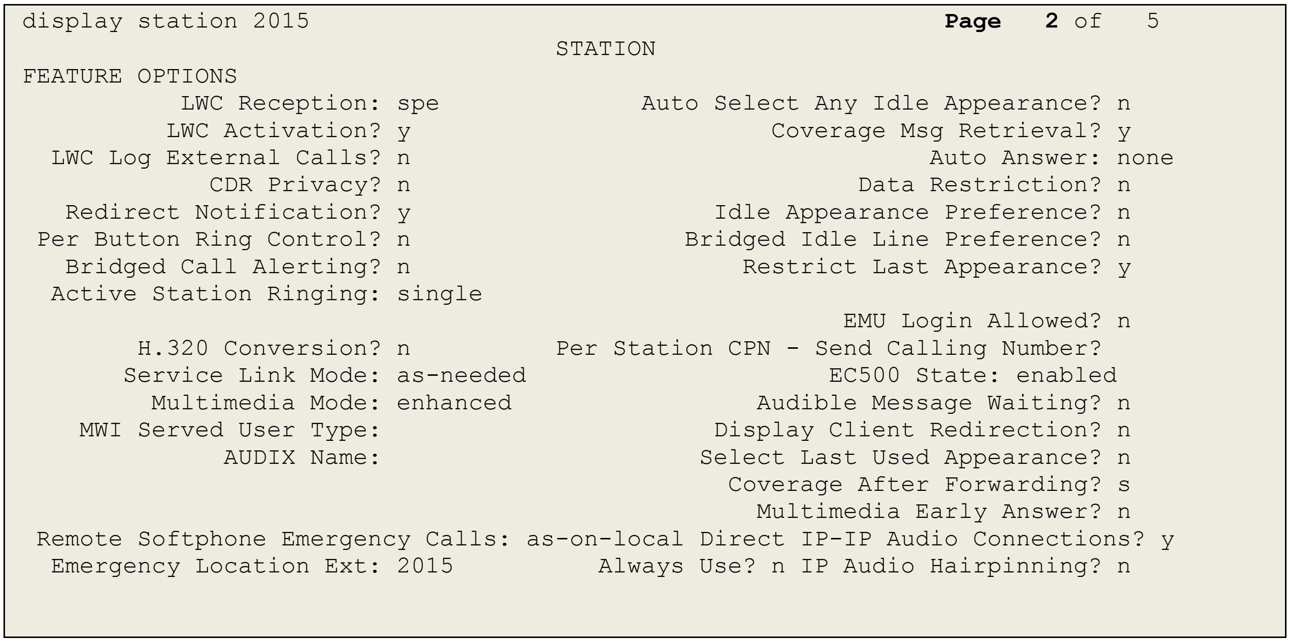
This is a printout of the Avaya 9620 H.323 Deskphone used during compliance testing.

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
```

Page 5.

```
display station 2015                                          Page   5 of   5
                                    STATION

BUTTON ASSIGNMENTS

 7:                                    10:
 8:                                    11:
 9:                                    12:
```

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.