Avaya Solution & Interoperability Test Lab

Application Notes for Cyara CX Automated Test and Monitoring Virtual Endpoint with Avaya Aura® Communication Manager 7.0 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cyara CX Automated Test and Monitoring Virtual Endpoint to interoperate with Avaya Aura® Communication Manager.

The Cyara Platform is an automated testing products and services platform that provides scripting, reporting, administration, collaboration, and management portal for contact center testing. The Cyara Virtual Endpoints is configured on Cyara Endpoint Server that emulates as agent stations in order to simulate contact center operations. Virtual Agent logs the required agents using these Virtual Endpoints as stations into the CTI environment and performs the activities specified by the designated behaviors assigned to the agents.

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

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

1. Introduction

These Application Notes describe the configuration steps required for Cyara CX Automated Test and Monitoring Virtual Endpoints to interoperate with Avaya Aura® Communication Manager.

2. General Test Approach and Test Results

The feature test cases were performed manually. Campaigns are run from the Cyara Web Portal to handle inbound calls routed to the Virtual Endpoints as stations which are logged in as agents by Cyara Virtual Agents. Details of Cyara Virtual Agents will be covered in Application Notes **[2]**. In this testing, voice calls to Virtual Agents is answered by Virtual Endpoints registered to Communication Manager as generic H.323 endpoint.

The serviceability test cases were also performed manually by restarting the Cyara Endpoint Server as well as Communication Manager.

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.

This test was conducted in a lab environment simulating a basic customer enterprise network environment. The testing focused on the standards-based interface between the Avaya solution and the third party solution. The results of testing are therefore considered to be applicable to either a premise-based deployment or to a hosted or cloud deployment where some elements of the third party solution may reside beyond the boundaries of the enterprise network, or at a different physical location from the Avaya components.

Readers should be aware that network behaviors (e.g., jitter, packet loss, delay, speed, etc.) can vary significantly from one location to another, and may affect the reliability or performance of the overall solution. Different network elements (e.g., session border controllers, soft switches, firewalls, NAT appliances, etc.) can also affect how the solution performs.

If a customer is considering implementation of this solution in a cloud environment, the customer should evaluate and discuss the network characteristics with their cloud service provider and network organizations, and evaluate if the solution is viable to be deployed in the cloud.

The network characteristics required to support this solution are outside the scope of these Application Notes. Readers should consult the appropriate Avaya and third party documentation for the product network requirements. Avaya makes no guarantee that this solution will work in all potential deployment configurations.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying Cyara Virtual Agent login to the Virtual Endpoint.

- Agent in login mode, logout scenarios.
- Handling of incoming calls.
- Holding and resuming of calls.
- Consult and single step voice transfers including cancellation.
- Consult and single step voice conference including cancellation.
- Correct status of Agent reflected on the test user interface.
- Proper hang up of calls including call hold, transfer and conference.

The serviceability testing focused on verifying the ability of Cyara Endpoints to recover from adverse conditions such as restarting of the Cyara Endpoint Server and Communication Manager.

2.2. Test Results

All feature test cases were successfully completed.

2.3. Support

Technical support on Cyara Platform can be obtained through the following:

- Phone: +61-3-90930815 (Australia), +44-203-356-9775 (Europe/Middle East/Africa), +1-844-204-2359 (North America/Latin America)
- Email: support@cyarasolutions.com
- Web: http://cyara.com/services/support/

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of a duplex pair of Communication Manager, Avaya G430 Media Gateway, Avaya AES Server, Avaya Media Server and System Manager. The System Manager is the administration and management tool for the Avaya Aura® products. 96x1 H.323 IP Telephones are used as utility phones for initiating calls. Cyara Endpoint Server installed on Microsoft Windows 2012 R2, provides the virtual H.323 endpoint. Cyara Platform Server (which includes the Cyara Virtual Agent component) is also installed on Microsoft Windows 2012 R2 which communicates with the Telephony Services Application Programming Interface (TSAPI) Service on the Avaya AES Server and has the CallEngine component installed for H.323 registration. Microsoft SQL 2012 was installed as the database on the same server which will be detailed in another Application Note **[2]**. The Avaya 4548GT-PWR Converged Stackable Switch provides ethernet connectivity to the servers and IP telephones. A personal computer was used for Cyara Web Portal access.

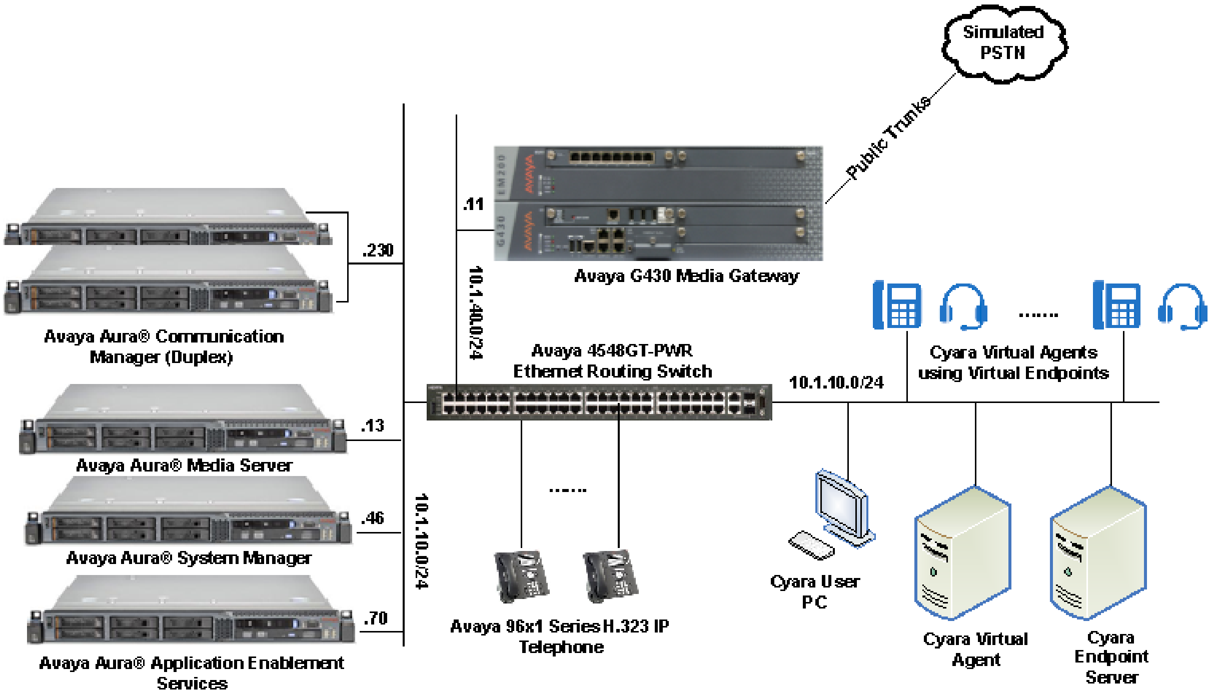

Simulated PSTN
Public Trunks
.11
Avaya G430 Media Gateway
.230
10.1.40.0/24
Avaya Aura® Communication Manager (Duplex)
Avaya 4548GT-PWR Ethernet Routing Switch
10.1.10.0/24
Cyara Virtual Agents using Virtual Endpoints
......
.13
Avaya Aura® Media Server
.46
Avaya Aura® System Manager
10.1.10.0/24
.70
Avaya Aura® Application Enablement Services
......
Avaya 96x1 Series H.323 IP Telephone
Cyara User PC
Cyara Virtual Agent
Cyara Endpoint Server

Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Version
Avaya Aura® Communication Manager Duplex Servers	7.0.1.0.0-FP1 (7.0.1.0.0.441.23012)
Avaya G430 Media Gateway • MGP	 37.38.0
Avaya Aura® Application Enablement Services	7.0.1.0.2.15-0
Avaya Aura® Media Server	7.7.0.19
Avaya Aura® System Manager	7.0.1.1.065378
96x1 Series (H.323) IP Telephones	6.6029
Cyara Platform Server running on Microsoft Windows 2012 R2	6.4
Cyara Endpoint Server running on Microsoft Windows 2012 R2	6.4
Dell PC	Microsoft Windows 10 Pro

Table 1: Equipment/Software Validated

5. Configure Avaya Aura ® Communication Manager

This section provides the procedures for configuring of Cyara Virtual Endpoints on Avaya Communication Manager.

All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

5.1. Configure Virtual Stations

Step	Description
1.	Enter **display system-parameters customer-options** command and on **Page 5**, check the **IP Stations** is set to **y**. If the feature is not licensed, then contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                      Page   5 of  12
                                OPTIONAL FEATURES

    Emergency Access to Attendant? y                              IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                        ISDN Feature Plus? n
                   Enhanced EC500? y       ISDN/SIP Network Call Redirection? y
     Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
        Enterprise Wide Licensing? n                                 ISDN-PRI? y
               ESS Administration? y            Local Survivable Processor? n
           Extended Cvg/Fwd Admin? y                  Malicious Call Trace? y
      External Device Alarm Admin? y              Media Encryption Over IP? n
   Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                 Flexible Billing? n
    Forced Entry of Account Codes? y                Multifrequency Signaling? y
       Global Call Classification? y         Multimedia Call Handling (Basic)? y
              Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
  Hospitality (G3V3 Enhancements)? y             Multimedia IP SIP Trunking? y
                        IP Trunks? y

            IP Attendant Consoles? y
         (NOTE: You must logoff & login to effect the permission changes.)
```

Step	Description
2.	On **Page 2**, check the **Maximum Concurrently Registered IP Stations** is sufficiently provisioned. If the number is not sufficiently licensed, then contact the Avaya sales team or business partner for a proper license file.

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

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 12000 70
           Maximum Concurrently Registered IP Stations: 18000 26
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 41000 0
                    Maximum Video Capable IP Softphones: 18000 3
                       Maximum Administered SIP Trunks: 24000 28
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0



         (NOTE: You must logoff & login to effect the permission changes.)
```

3. Cyara Virtual Endpoints are configured as generic H.323 station on Communication Manager. Enter the **add station m** command, where **m** is the desired extension. Enter **Type** as **H.323** with appropriate **Name** such as **Virtual #1**. Note that the **Port** will automatically be set as **IP** by Communication Manager. Set the **Security Code** to **0000**. Repeat this for all the Virtual Endpoints required. In this compliance testing, extensions **10401** to **10415** are added and configured.

```
add station 10401                                              Page   1 of   4
                                     STATION

Extension: 10401                         Lock Messages? n               BCC: 0
     Type: H.323                         Security Code: 0000             TN: 1
     Port: IP                          Coverage Path 1:                 COR: 1
     Name: Virtual #1                  Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19             Message Waiting Indicator: none

                                         Authentication Required? y



          Survivable COR: internal
   Survivable Trunk Dest? y
            DTMF over IP: in-band
                                                        IP Video? n
```

4. Enter the **change ip-codec n** command where **n** is a valid IP codec-set associated with the IP network region that is used by the Virtual Endpoint. Set Audio Codec to an appropriate value supported by Cyara Virtual Endpoint. In this configuration, the **G.711MU** and **G.711A** codec were configured.

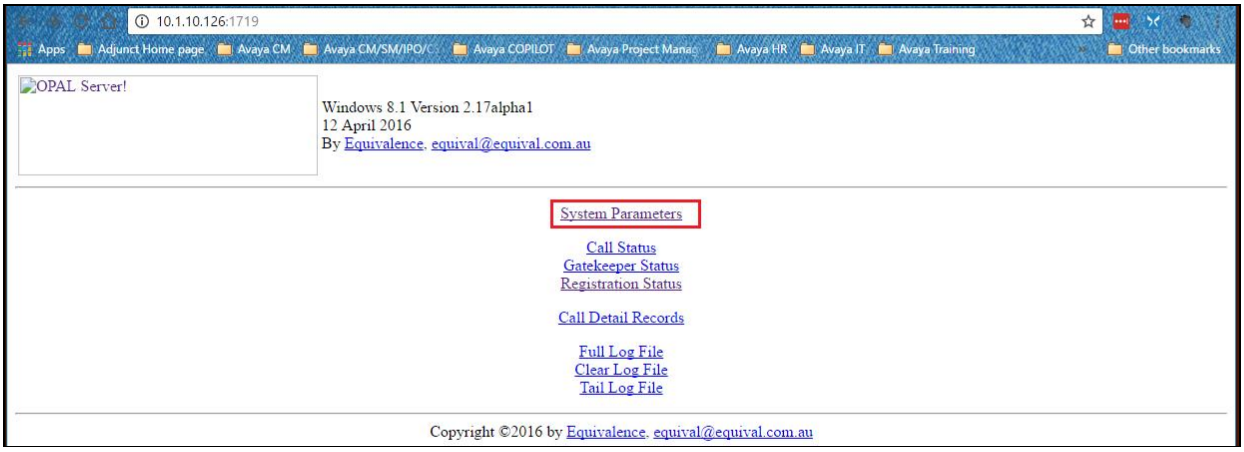
```
change ip-codec-set 1                                          Page   1 of   2

                          IP CODEC SET
    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.711A            n         2        20
 3:
 4:
 5:
 6:
 7:
```

6. Configure Cyara Endpoint Server

Setup of the Cyara Endpoint Server and Cyara Platform Server on Microsoft® Windows 2012 R2 will be done by Cyara engineers and will not be detailed here. This section highlights the configuration of Cyara Endpoint Server that interface with Communication Manager and it includes the following areas:

- Configure Cyara Endpoint Server
- Configure Cyara Call Engine

Enter on a web browser **http://<IP address of Cyara Endpoint Server>:1719/** to access the system. Clicking on any of the items on the list require password access.



Windows 8.1 Version 2.17alpha1
12 April 2016
By Equivalence, equival@equival.com.au

System Parameters

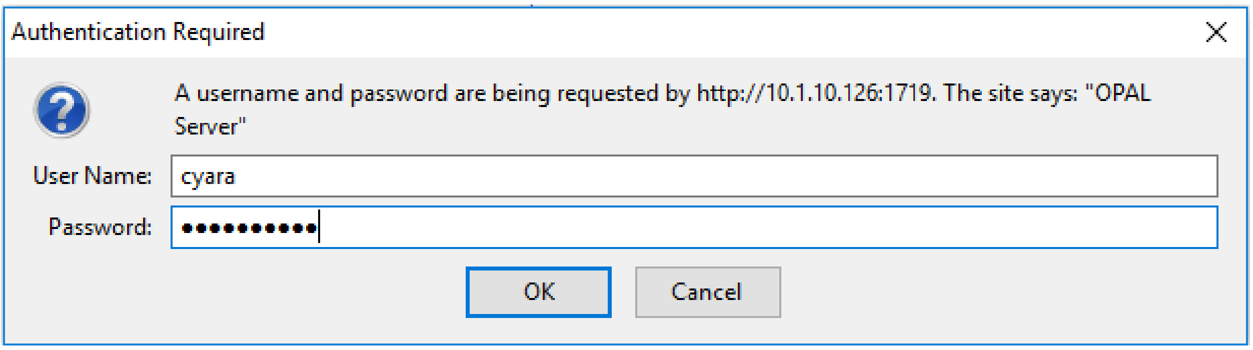
Call Status
Gatekeeper Status
Registration Status

Call Detail Records

Full Log File
Clear Log File
Tail Log File

Copyright ©2016 by Equivalence, equival@equival.com.au

Select System Parameters and on the pop-up authentication window, log in with an appropriate **User Name** and **Password**.



Authentication Required

A username and password are being requested by http://10.1.10.126:1719. The site says: "OPAL Server"

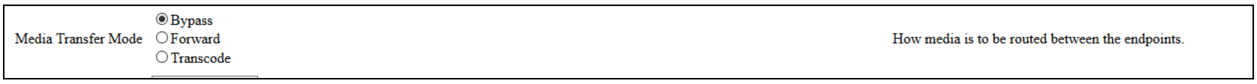
User Name: cyara

Password: ●●●●●●●●●●

6.1. Configure Cyara Endpoint Server

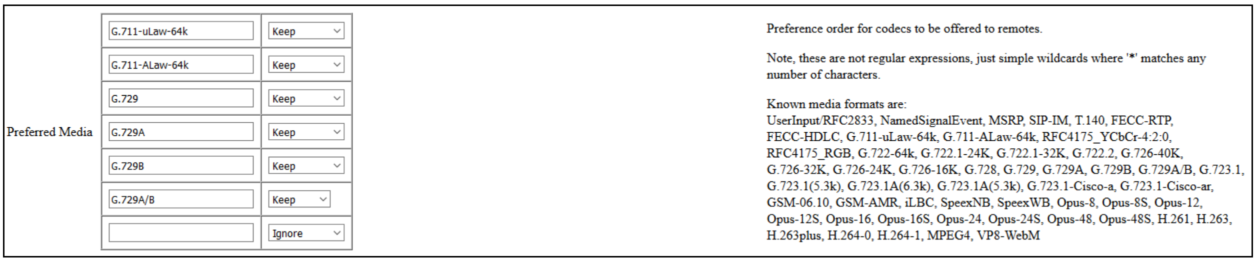
Leaving the rest as default, configure the following from the System Parameters page.

- Set the **Media Transfer Mode** to **Bypass** by selecting the button.



Media Transfer Mode ● Bypass ○ Forward ○ Transcode — How media is to be routed between the endpoints.

- Set the **Preferred Media** according to the supported codec configured on Communication Manager as in **Section 5.1 Step 4**.



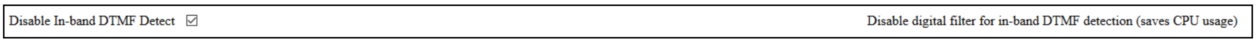
Preferred Media		
	G.711-uLaw-64k	Keep
	G.711-ALaw-64k	Keep
	G.729	Keep
	G.729A	Keep
	G.729B	Keep
	G.729A/B	Keep
		Ignore

Preference order for codecs to be offered to remotes.

Note, these are not regular expressions, just simple wildcards where '*' matches any number of characters.

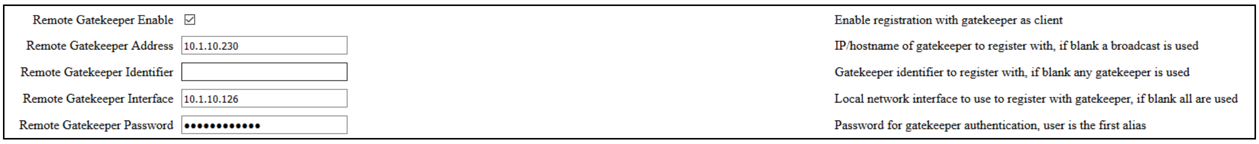
Known media formats are:
UserInput/RFC2833, NamedSignalEvent, MSRP, SIP-IM, T.140, FECC-RTP, FECC-HDLC, G.711-uLaw-64k, G.711-ALaw-64k, RFC4175_YCbCr-4:2:0, RFC4175_RGB, G.722-64k, G.722.1-24K, G.722.1-32K, G.722.2, G.726-40K, G.726-32K, G.726-24K, G.726-16K, G.728, G.729, G.729A, G.729B, G.729A/B, G.723.1, G.723.1(5.3k), G.723.1A(6.3k), G.723.1A(5.3k), G.723.1-Cisco-a, G.723.1-Cisco-ar, GSM-06.10, GSM-AMR, iLBC, SpeexNB, SpeexWB, Opus-8, Opus-8S, Opus-12, Opus-12S, Opus-16, Opus-16S, Opus-24, Opus-24S, Opus-48, Opus-48S, H.261, H.263, H.263plus, H.264-0, H.264-1, MPEG4, VP8-WebM

- Check the **Disable In-band DTMF** to minimize the load on the system.



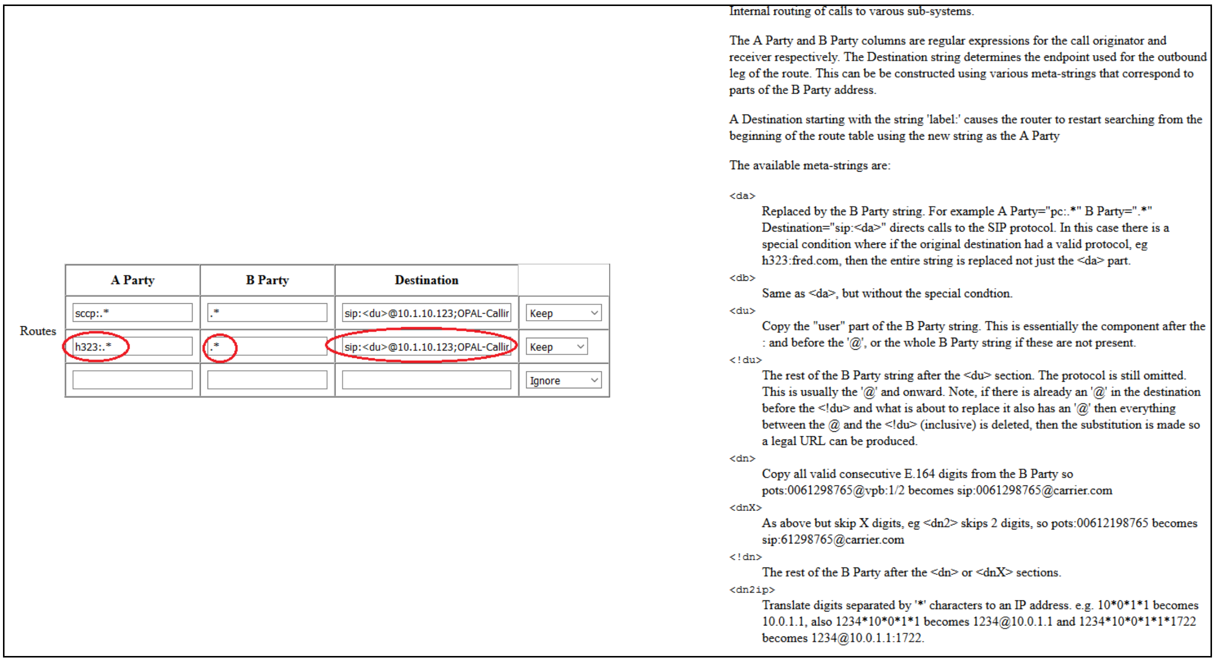
Disable In-band DTMF Detect ☑ — Disable digital filter for in-band DTMF detection (saves CPU usage)

- Check the **Remote Gatekeeper Enable** and set the Communication Manager ip address for the **Remote Gatekeeper Address**.
- Enter the **Remote Gatekeeper Interface** ip address for the Cyara Endpoint Server and provide the appropriate **Remote Gatekeeper Password**. This field can have a comma to separate list of Endpoint Servers ip address. This may be changed to wildcard to use all IPV4 interfaces on this machine.



Remote Gatekeeper Enable	☑	Enable registration with gatekeeper as client
Remote Gatekeeper Address	10.1.10.230	IP/hostname of gatekeeper to register with, if blank a broadcast is used
Remote Gatekeeper Identifier		Gatekeeper identifier to register with, if blank any gatekeeper is used
Remote Gatekeeper Interface	10.1.10.126	Local network interface to use to register with gatekeeper, if blank all are used
Remote Gatekeeper Password	••••••••••••	Password for gatekeeper authentication, user is the first alias

- Set the **Routes** configuration for **A Party** to "**h323:.***" and **B Party** to "**.***" with **Destination** as "**sip:<du>@10.1.10.123;OPAL-Calling-Party-Number=<cu>**" and select **Keep** from the drop down menu.



Routes

A Party	B Party	Destination	
sccp:.*	.*	sip:<du>@10.1.10.123;OPAL-Callir	Keep
h323:.*	.*	sip:<du>@10.1.10.123;OPAL-Callir	Keep
			Ignore

Internal routing of calls to varous sub-systems.

The A Party and B Party columns are regular expressions for the call originator and receiver respectively. The Destination string determines the endpoint used for the outbound leg of the route. This can be be constructed using various meta-strings that correspond to parts of the B Party address.

A Destination starting with the string 'label:' causes the router to restart searching from the beginning of the route table using the new string as the A Party

The available meta-strings are:

`<da>`
Replaced by the B Party string. For example A Party="pc:.*" B Party=".*" Destination="sip:<da>" directs calls to the SIP protocol. In this case there is a special condition where if the original destination had a valid protocol, eg h323:fred.com, then the entire string is replaced not just the <da> part.

`<db>`
Same as <da>, but without the special condtion.

`<du>`
Copy the "user" part of the B Party string. This is essentially the component after the : and before the '@', or the whole B Party string if these are not present.

`<!du>`
The rest of the B Party string after the <du> section. The protocol is still omitted. This is usually the '@' and onward. Note, if there is already an '@' in the destination before the <!du> and what is about to replace it also has an '@' then everything between the @ and the <!du> (inclusive) is deleted, then the substitution is made so a legal URL can be produced.

`<dn>`
Copy all valid consecutive E.164 digits from the B Party so pots:0061298765@vpb:1/2 becomes sip:0061298765@carrier.com

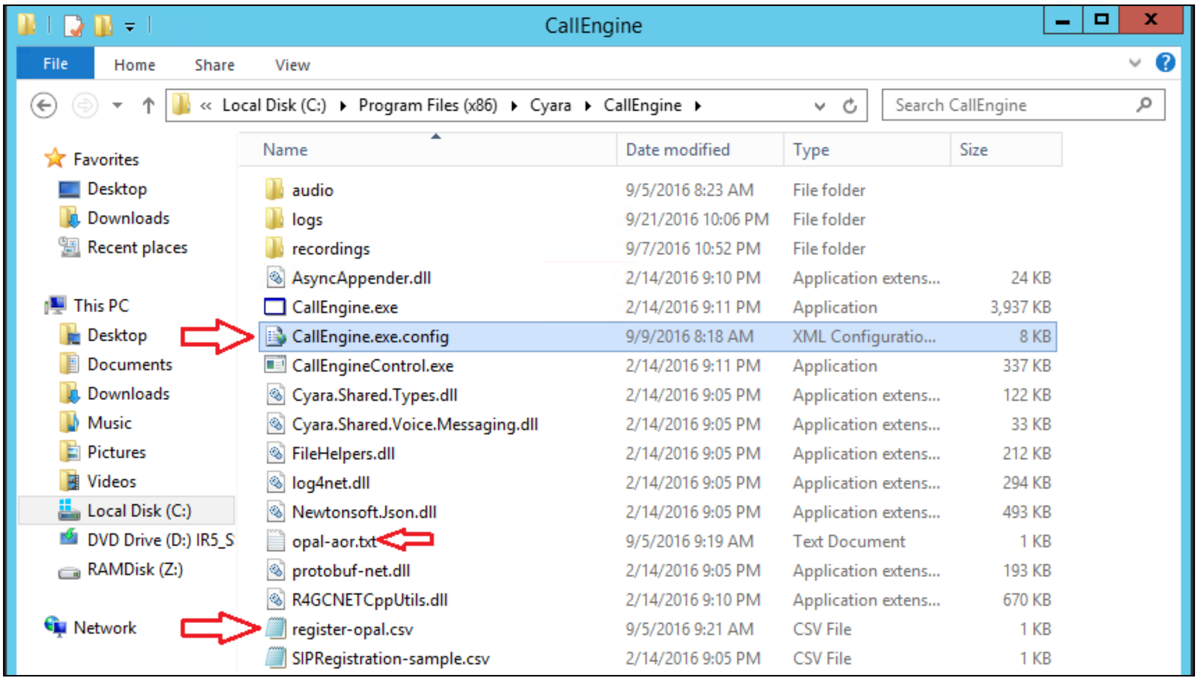
`<dnX>`
As above but skip X digits, eg <dn2> skips 2 digits, so pots:00612198765 becomes sip:61298765@carrier.com

`<!dn>`
The rest of the B Party after the <dn> or <dnX> sections.

`<dn2ip>`
Translate digits separated by '*' characters to an IP address. e.g. 10*0*1*1 becomes 10.0.1.1, also 1234*10*0*1*1 becomes 1234@10.0.1.1 and 1234*10*0*1*1*1722 becomes 1234@10.0.1.1:1722.

6.2. Configure Cyara Call Engine

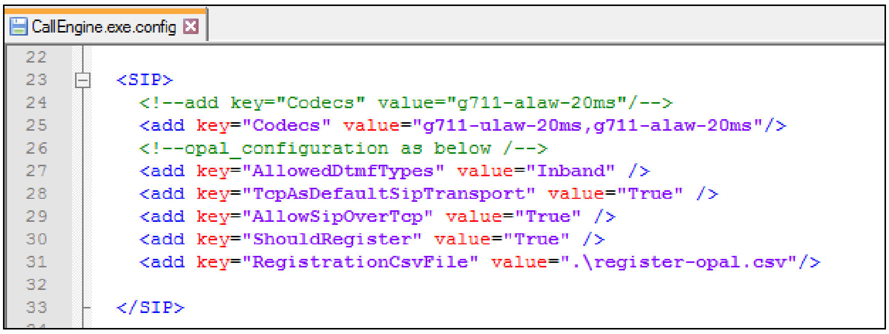
Cyara Call Engine resides as one of the component on the Cyara Platform Server. The configuration file needs to be configured. On the Cyara Platform Server, go to the location "**C:\Program Files (x86)\Cyara\CallEngine**" below for the 2 files.



Name	Date modified	Type	Size
audio	9/5/2016 8:23 AM	File folder	
logs	9/21/2016 10:06 PM	File folder	
recordings	9/7/2016 10:52 PM	File folder	
AsyncAppender.dll	2/14/2016 9:10 PM	Application extens...	24 KB
CallEngine.exe	2/14/2016 9:11 PM	Application	3,937 KB
CallEngine.exe.config	9/9/2016 8:18 AM	XML Configuratio...	8 KB
CallEngineControl.exe	2/14/2016 9:11 PM	Application	337 KB
Cyara.Shared.Types.dll	2/14/2016 9:05 PM	Application extens...	122 KB
Cyara.Shared.Voice.Messaging.dll	2/14/2016 9:05 PM	Application extens...	33 KB
FileHelpers.dll	2/14/2016 9:05 PM	Application extens...	212 KB
log4net.dll	2/14/2016 9:05 PM	Application extens...	294 KB
Newtonsoft.Json.dll	2/14/2016 9:05 PM	Application extens...	493 KB
opal-aor.txt	9/5/2016 9:19 AM	Text Document	1 KB
protobuf-net.dll	2/14/2016 9:05 PM	Application extens...	193 KB
R4GCNETCppUtils.dll	2/14/2016 9:10 PM	Application extens...	670 KB
register-opal.csv	9/5/2016 9:21 AM	CSV File	1 KB
SIPRegistration-sample.csv	2/14/2016 9:05 PM	CSV File	1 KB

6.2.1. CallEngine.exe.config

Set the parameters below with the **RegistrationCsvFile** name as “**register-opal.csv**” which will be configured on the next section.

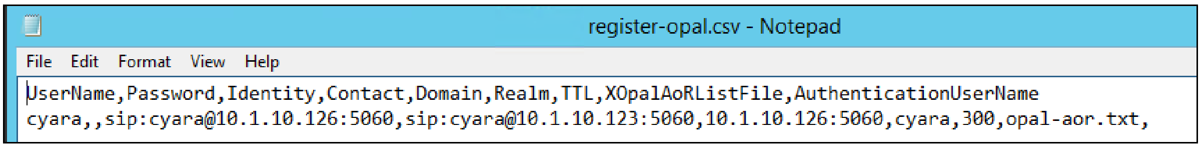


```
<SIP>
  <!--add key="Codecs" value="g711-alaw-20ms"/-->
  <add key="Codecs" value="g711-ulaw-20ms,g711-alaw-20ms"/>
  <!--opal_configuration as below /-->
  <add key="AllowedDtmfTypes" value="Inband" />
  <add key="TcpAsDefaultSipTransport" value="True" />
  <add key="AllowSipOverTcp" value="True" />
  <add key="ShouldRegister" value="True" />
  <add key="RegistrationCsvFile" value=".\register-opal.csv"/>

</SIP>
```

6.2.2. register-opal.csv

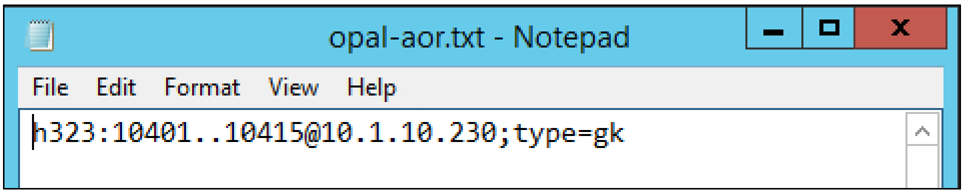
Configure the following for the csv file.

UserName	cyara
Password	
Identity	cyara@10.1.10.126:5060
Contact	cyara@10.1.10.123:5060
Domain	cyara@10.1.10.126:5060
Realm	cyara
TTL	300
XOpalAorListFile	opal-aor.txt



```
UserName,Password,Identity,Contact,Domain,Realm,TTL,XOpalAoRListFile,AuthenticationUserName
cyara,,sip:cyara@10.1.10.126:5060,sip:cyara@10.1.10.123:5060,10.1.10.126:5060,cyara,300,opal-aor.txt,
```

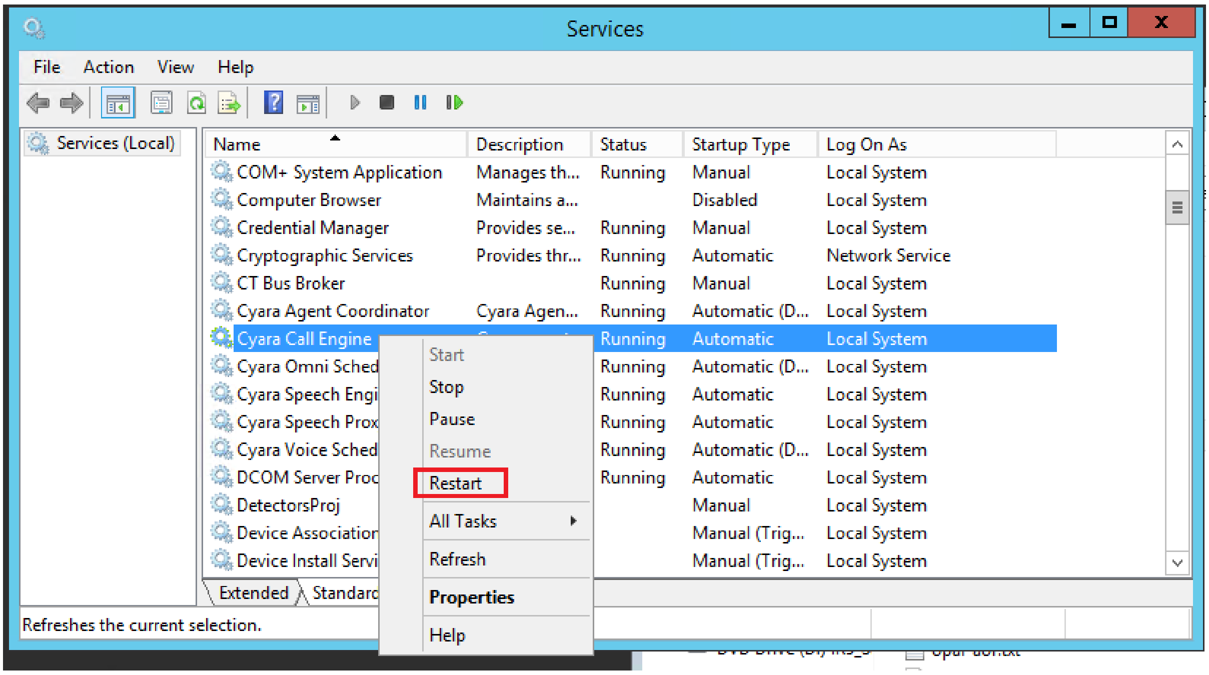
The **opal-aor.txt** file content specifies the range of extensions i.e., **10401** to **10415** register with Communication Manager as the gatekeeper through the Cyara Endpoint Server which functions as the Cyara Voice Gateway. See below for the format.



```
h323:10401..10415@10.1.10.230;type=gk
```

6.2.3. Start the CallEngine Service

From the Cyara Platform server, right-click on the Windows logo, select run and enter **services.msc**. Right-click on **Cyara Call Engine** and restart the service to kick off the registration.



Name	Description	Status	Startup Type	Log On As
COM+ System Application	Manages th...	Running	Manual	Local System
Computer Browser	Maintains a...		Disabled	Local System
Credential Manager	Provides se...	Running	Manual	Local System
Cryptographic Services	Provides thr...	Running	Automatic	Network Service
CT Bus Broker		Running	Manual	Local System
Cyara Agent Coordinator	Cyara Agen...	Running	Automatic (D...	Local System
Cyara Call Engine		Running	Automatic	Local System
Cyara Omni Sched		Running	Automatic (D...	Local System
Cyara Speech Engi		Running	Automatic	Local System
Cyara Speech Prox		Running	Automatic	Local System
Cyara Voice Sched		Running	Automatic (D...	Local System
DCOM Server Proc		Running	Automatic	Local System
DetectorsProj			Manual	Local System
Device Associatior			Manual (Trig...	Local System
Device Install Servi			Manual (Trig...	Local System

Refreshes the current selection.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and Cyara Endpoint Server.

7.1. Verify Avaya Aura® Communication Manager

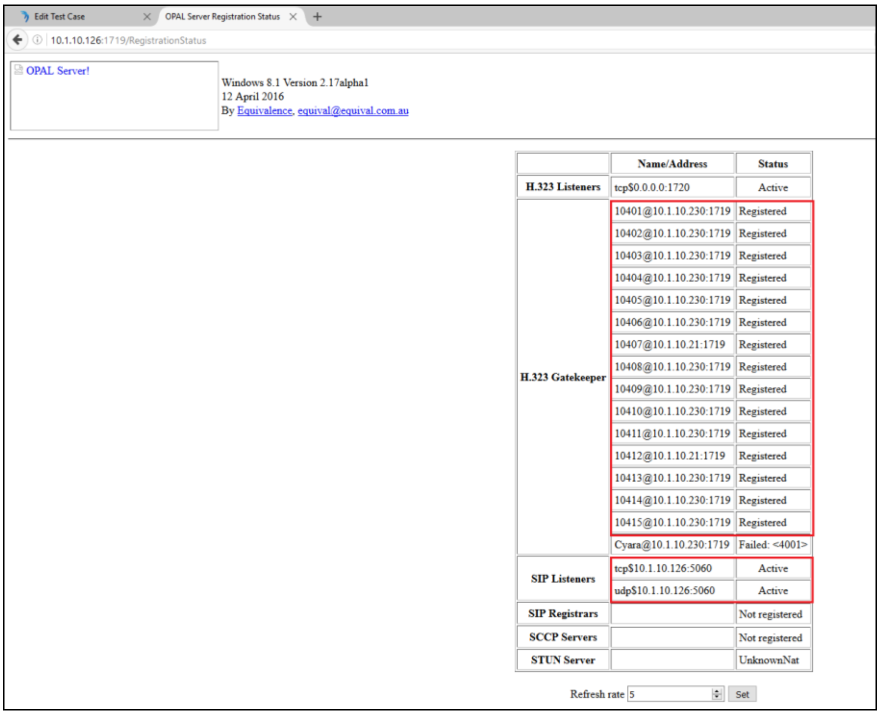
Verify the registration status of all the configured Virtual Endpoints by using the **list registered-ip-stations ext 10401 count 15** command. These stations should be listed as below. Note the station ip address is the Cyara Endpoint Server.

```
list registered-ip-stations ext 10401 count 15                        Page   1

                            REGISTERED IP STATIONS

Station Ext   Set Type/ Prod ID/       Station IP Address/
or Orig Port  Net Rgn   Release    Skt Gatekeeper IP Address
------------- --------- ---------- --- ---------------------------------------
10401         H.323     Equivalenc no  10.1.10.126
              1         0.0000         10.1.10.22
10402         H.323     Equivalenc no  10.1.10.126
              1         0.0000         10.1.10.22
10403         H.323     Equivalenc no  10.1.10.126
              1         0.0000         10.1.10.22
10404         H.323     Equivalenc no  10.1.10.126
              1         0.0000         10.1.10.22
10405         H.323     Equivalenc no  10.1.10.126
              1         0.0000         10.1.10.22
10406         H.323     Equivalenc no  10.1.10.126
              1         0.0000         10.1.10.22
10407         H.323     Equivalenc no  10.1.10.126
              1         0.0000         10.1.10.22

                press CANCEL to quit --  press NEXT PAGE to continue
```

Make inbound and outbound calls by running the campaigns from Cyara Web Portal for handling inbound calls and agent features which will not be detailed here. Refer to Application Notes **[2]** for details.

7.2. Verify Cyara Endpoint Server

Log in to the Cyara Endpoint Server as in **Section 6**. Click on **Registration Status** on the home page. Verify that the **Status** of the Virtual Stations are all showing **Registered** and the server is listening to the default SIP port 5060.


Edit Test Case
OPAL Server Registration Status
10.1.10.126:1719/RegistrationStatus
OPAL Server!

Windows 8.1 Version 2.17alpha1
12 April 2016
By Equivalence, equival@equival.com.au

	Name/Address	Status
H.323 Listeners	tcp$0.0.0.0:1720	Active
H.323 Gatekeeper	10401@10.1.10.230:1719	Registered
	10402@10.1.10.230:1719	Registered
	10403@10.1.10.230:1719	Registered
	10404@10.1.10.230:1719	Registered
	10405@10.1.10.230:1719	Registered
	10406@10.1.10.230:1719	Registered
	10407@10.1.10.21:1719	Registered
	10408@10.1.10.230:1719	Registered
	10409@10.1.10.230:1719	Registered
	10410@10.1.10.230:1719	Registered
	10411@10.1.10.230:1719	Registered
	10412@10.1.10.21:1719	Registered
	10413@10.1.10.230:1719	Registered
	10414@10.1.10.230:1719	Registered
	10415@10.1.10.230:1719	Registered
	Cyara@10.1.10.230:1719	Failed: <4001>
SIP Listeners	tcp$10.1.10.126:5060	Active
	udp$10.1.10.126:5060	Active
SIP Registrars		Not registered
SCCP Servers		Not registered
STUN Server		UnknownNat

Refresh rate 5 Set

8. Conclusion

These Application Notes describe the configuration steps required for Cyara Platform Virtual Endpoint to interoperate with Avaya Aura® Communication Manager. All feature test cases were completed successfully.

9. Additional References

This section references the Avaya and Cyara documentations that are relevant to these Application Notes.

The following Avaya product documentations can be found at http://support.avaya.com.
[1] *Avaya Aura® Avaya Communication Manager Feature Description and Implementation,* Document Number 555-245-205, Release 7.0.1, Issue 3, Sep 2016
[2] *Application Notes for Cyara CX Automated Test and Monitoring Virtual Agent with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0*

The following Cyara product documentation is either obtained directly from member or available online.
[3] Cyara Platform Deployment Guide
[4] Cyara User Guide available online at https://www.cyaraportal.com/CyaraWebPortal.

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.