Avaya Solution & Interoperability Test Lab

Application Notes for Cyara Platform with Avaya Aura® Communication Manager using H.323 Endpoints Emulation– Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cyara Platform 20.1 to interoperate with Avaya Aura® Communication Manager 8.1 using H.323 Endpoints emulation.

Readers should pay attention to S**ection 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 Platform 20.1 to interoperate with Avaya Aura® Communication Manager 8.1 using H.323 Endpoints emulation.

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 Endpoint server is part of the Cyara Platform that host the Cyara Voice Call Engine and Cyara Voice Gateway. The Cyara Virtual Endpoints are configured on the Cyara Endpoint server that emulates as H.323 endpoints in 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 Cyara 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 reference [2]. In this testing, voice calls are answered by Cyara 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and the Cyara Platform did not include use of any specific encryption features as requested by Cyara.

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 interoperability compliance testing focused on verifying that the Cyara Virtual Endpoints can register with Communication Manager as H.323 endpoints, establish calls and send voice media.

The following features and functionality were covered:

- H.323 endpoint registration with Communication Manager.
- Originating and terminating calls through Communication Manager.
- Support of G.711 mu-law and G.711 a-law.
- Support of direct IP-to-IP media.
- DTMF support.
- Support for H.323 agent login to allow calls directly to a hunt/skill group to be routed to an available agent, which is a Cyara Virtual Agent.
- Originating calls from H.323 endpoints and terminating calls on H.323 endpoints and SIP trunks.

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

2.2. Test Results

All feature test cases were successfully completed with the following observation:

- Active campaigns have to be restarted after Communication Manager restarts.

2.3. Support

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

- Phone: +61-3-9093-0815 (Australia), +44-203-786-5070 (Europe/Middle East/Africa), +1-650-549-8522 (North America/Latin America)
- Email: support@cyara.com
- Web: http://support.cyara.com/

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Communication Manager, Avaya G430 Media Gateway, Application Enablement Services (AES) Server, Avaya Media Server, Session Manager and System Manager. The System Manager is the administration and management tool for the Avaya Aura® products. Avaya one-X® Communicator is used as utility softphone for initiating calls. Cyara Virtual Endpoint server is installed on Microsoft Windows 2016, provides the virtual H.323 endpoints. Cyara Platform server (which includes the Cyara Virtual Agent component) is also installed on Microsoft Windows 2016. Microsoft SQL 2016 was installed as the database on the same server which will be detailed in another Application Note reference **[2]**. A personal computer was used for Cyara Web Portal access. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution.

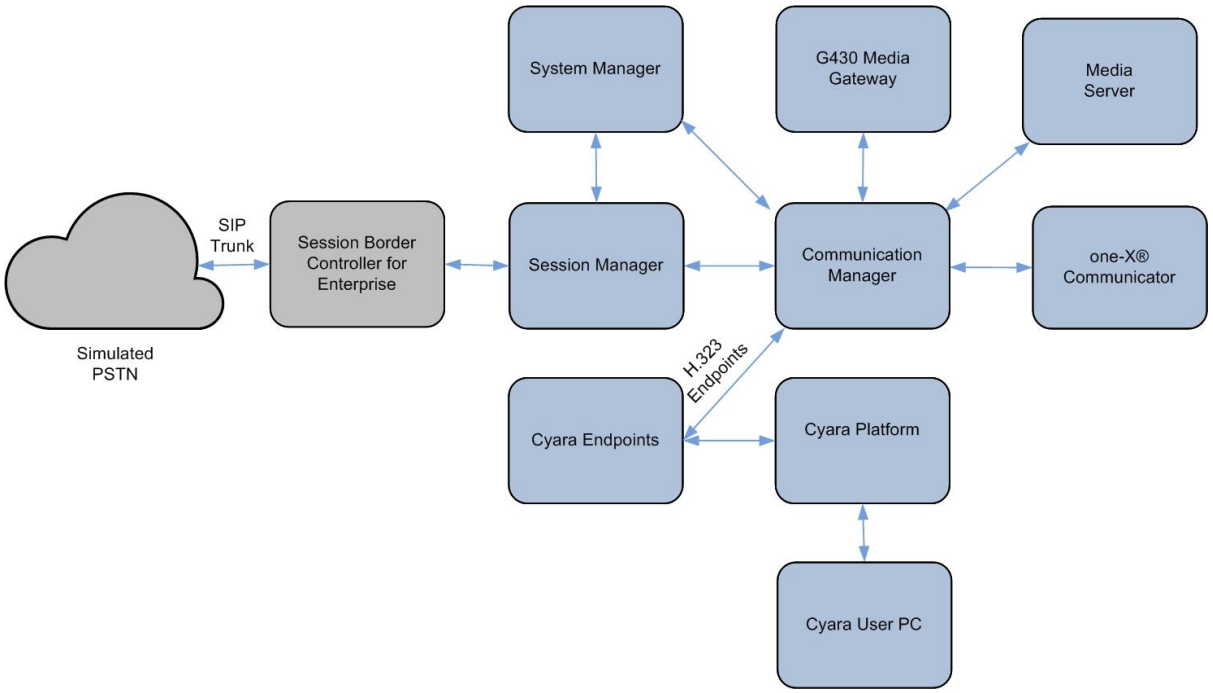


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager	8.1.2.0.0.890.26095
Avaya G430 Media Gateway • MGP	 41.16.0
Avaya Aura® Media Server	8.0.2.93
Avaya Aura® System Manager	8.1.2.0.0611167
Avaya Aura® Session Manager	8.1.2.0.812033
Avaya one-X® Communicator	6.2.14.4-SP14
Cyara Platform running on Microsoft Windows 2016	20.1.0
Cyara Endpoint running on Microsoft Windows 2016	20.1.0
Dell PC	Microsoft Windows 10 Pro

Table 1: Equipment/Software Validated

5. Configure Avaya Aura ® Communication Manager

This section provides the procedures for configuring 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. System Parameters Customer Options

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? y
  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.)
```

On **Page 2**, check the **Maximum Concurrently Registered IP Stations**. If the number is not sufficiently licensed, 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     90
       Maximum Concurrently Registered IP Stations: 18000     27
         Maximum Administered Remote Office Trunks: 12000      0
Max Concurrently Registered Remote Office Stations: 18000      0
          Maximum Concurrently Registered IP eCons:  414       0
     Max Concur Reg Unauthenticated H.323 Stations:   100      0
                   Maximum Video Capable Stations:  41000     0
               Maximum Video Capable IP Softphones:  18000     2
                   Maximum Administered SIP Trunks: 40000     28
  Max Administered Ad-hoc Video Conferencing Ports: 24000      0
   Max Number of DS1 Boards with Echo Cancellation: 999    0

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

5.2. Configure Stations for Virtual Endpoint

Cyara Virtual Endpoints are configured as generic H.323 stations 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 desired value **0000**. Repeat this for all the Cyara Virtual Endpoints required. In this compliance testing, extensions **10401** to **10410** are added and configured. It is required for the code to be the same but not required for the extension to be sequential as it saves time in the administration by defining the extensions as a range in Cyara later on.

```
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
```

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 MEDIA PARAMETERS
    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:

     Media Encryption                  Encrypted SRTCP: best-effort
 1: 1-srtp-aescm128-hmac80
 2: 2-srtp-aescm128-hmac32
 3: none
 4:
 5:
```

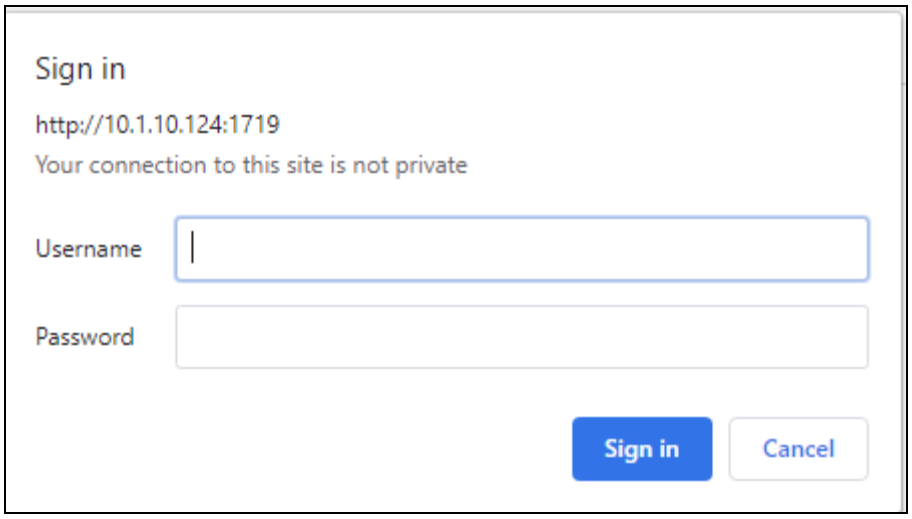
6. Configure Cyara Endpoint Server

Setup of the Cyara Endpoint server and Cyara Platform server on Microsoft® Windows 2016 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
- Configure Cyara Call Engine

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

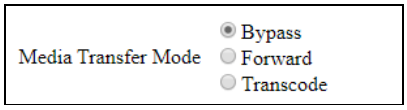
Select **System Parameters** and on the pop-up authentication window, log in with an appropriate **Username** and **Password**.



6.1. Configure Cyara Endpoint

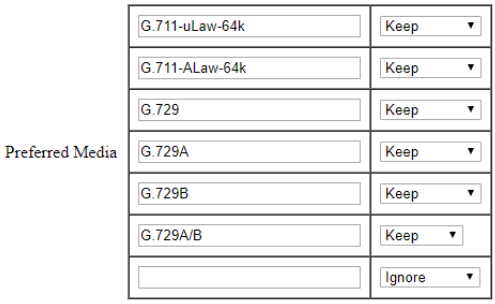
Leaving the rest as default, configure the following from the System Parameters page.

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



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 5.2**.

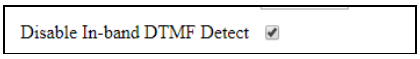


Preference order for codecs to be offered to remotes.

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

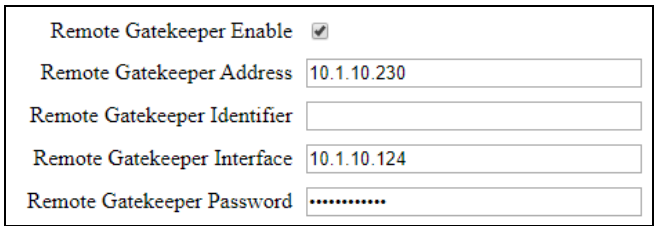
Known media formats are:
UserInput/RFC2833, NamedSignalEvent, MSRP, SIP-IM, T.140, FECC-RTP, FECC-HDLC, G.711-uLaw-64k, G.711-ALaw-64k, RFC4175_YCbCr-4:2:0, RFC4175_RGB, G.722-64k, G.722.1-24K, G.722.1-32K, G.722.2, G.726-40K, G.726-32K, G.726-24K, G.726-16K, G.728, G.729, G.729A, G.729B, G.729A/B, G.723.1, 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 Detect** to minimize the load on the system.

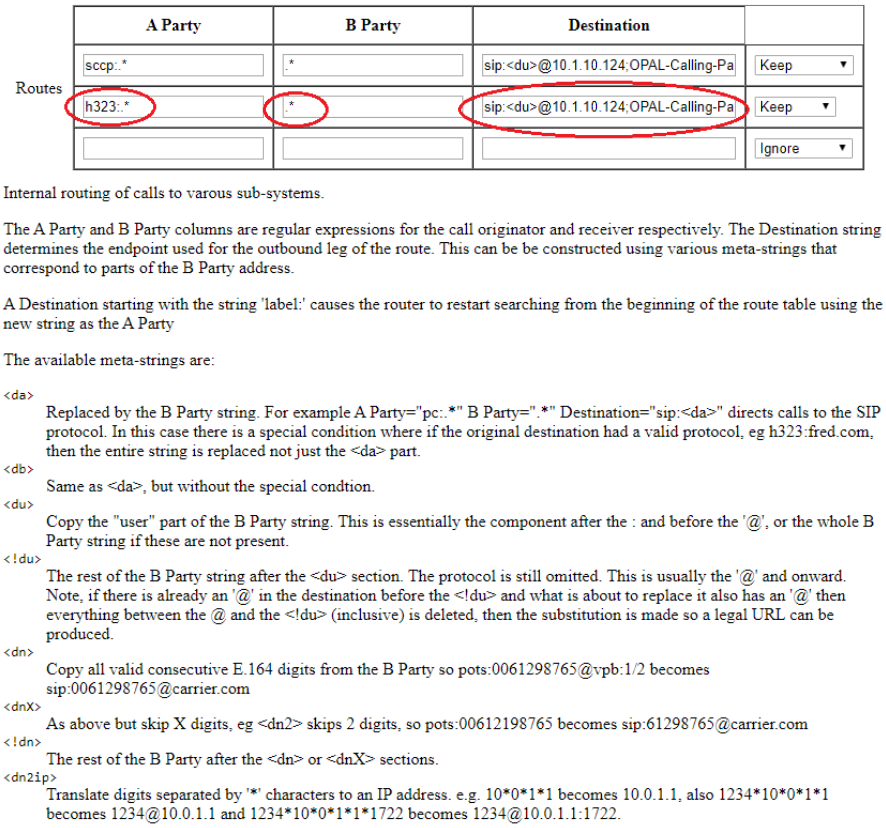


Disable digital filter for in-band DTMF detection (saves CPU usage)

- 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. The Remote Gatekeeper Interface IP address is the Cyara Endpoint server IP address where the password is the Virtual Endpoint security code administered in **Section 5.2**.

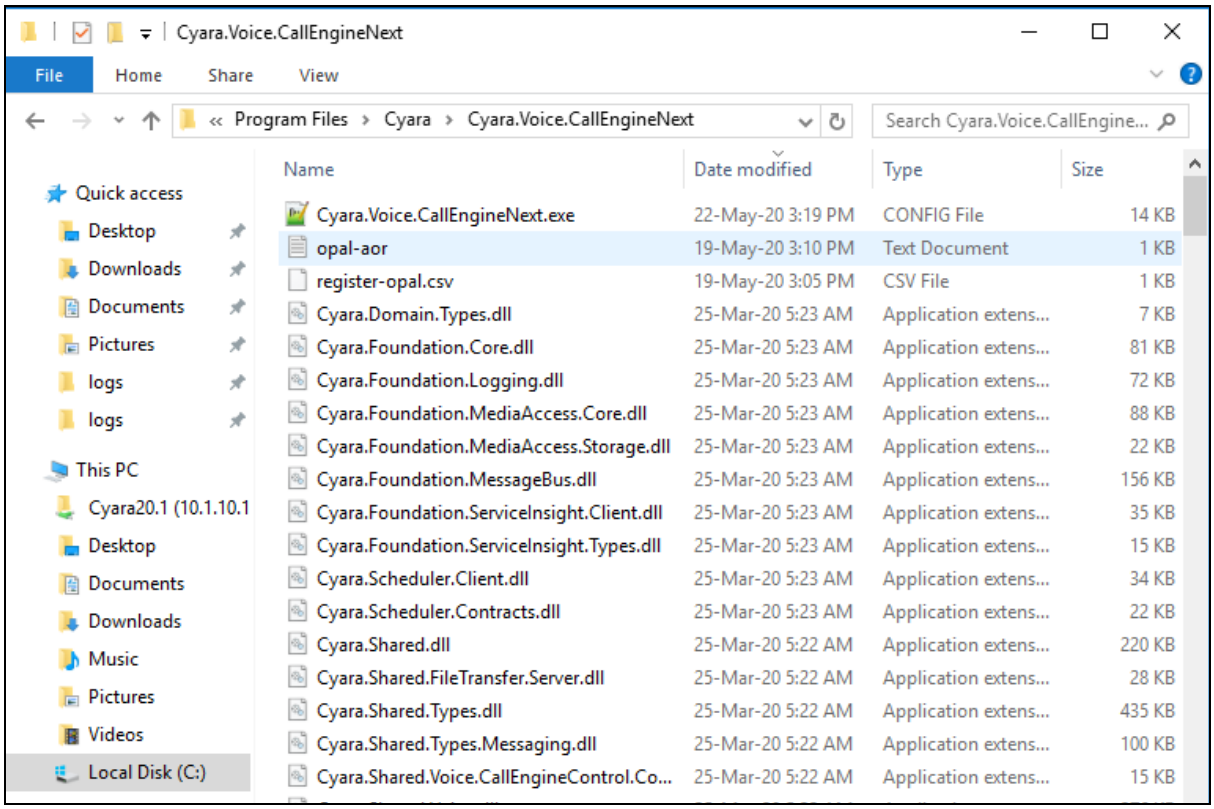


- Set the **Routes** configuration for **A Party** to "**h323:.***" and **B Party** to "**.***" with **Destination** as "**sip:<du>@10.1.10.124;OPAL-Calling-Party-Number=<cu>**" and select **Keep** from the drop down menu.



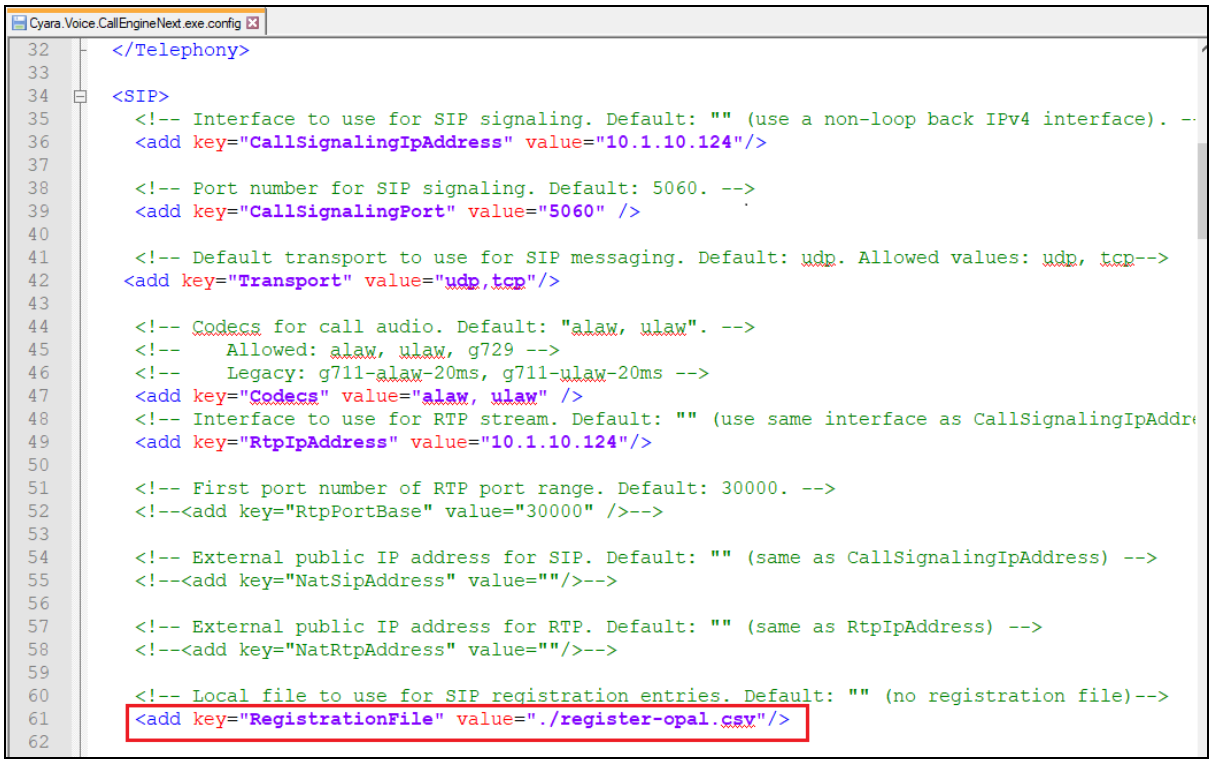
6.2. Configure Cyara Call Engine

Cyara Call Engine resides as one of the components on the Cyara Platform. The configuration file needs to be configured. On the Cyara Platform server, go to the location "**C:\Program Files\Cyara\Cyara.Voice.CallEngineNext**" below for the two files i.e., "Cyara.Voice.CallEngineNext.exe.config" and "register-opal.csv".



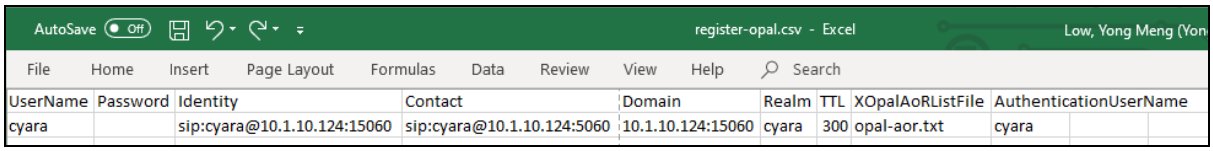
6.2.1. Cyara.Voice.CallEngineNext.exe.config

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

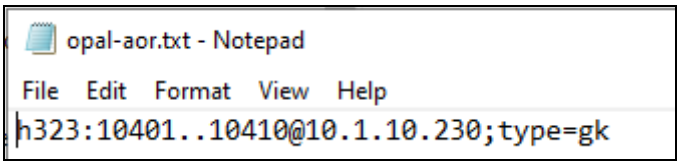


6.2.2. register-opal.csv

Configure the following for the csv file. The password is administered in **Section 6.1** as the **Remote Gatekeeper Password**.

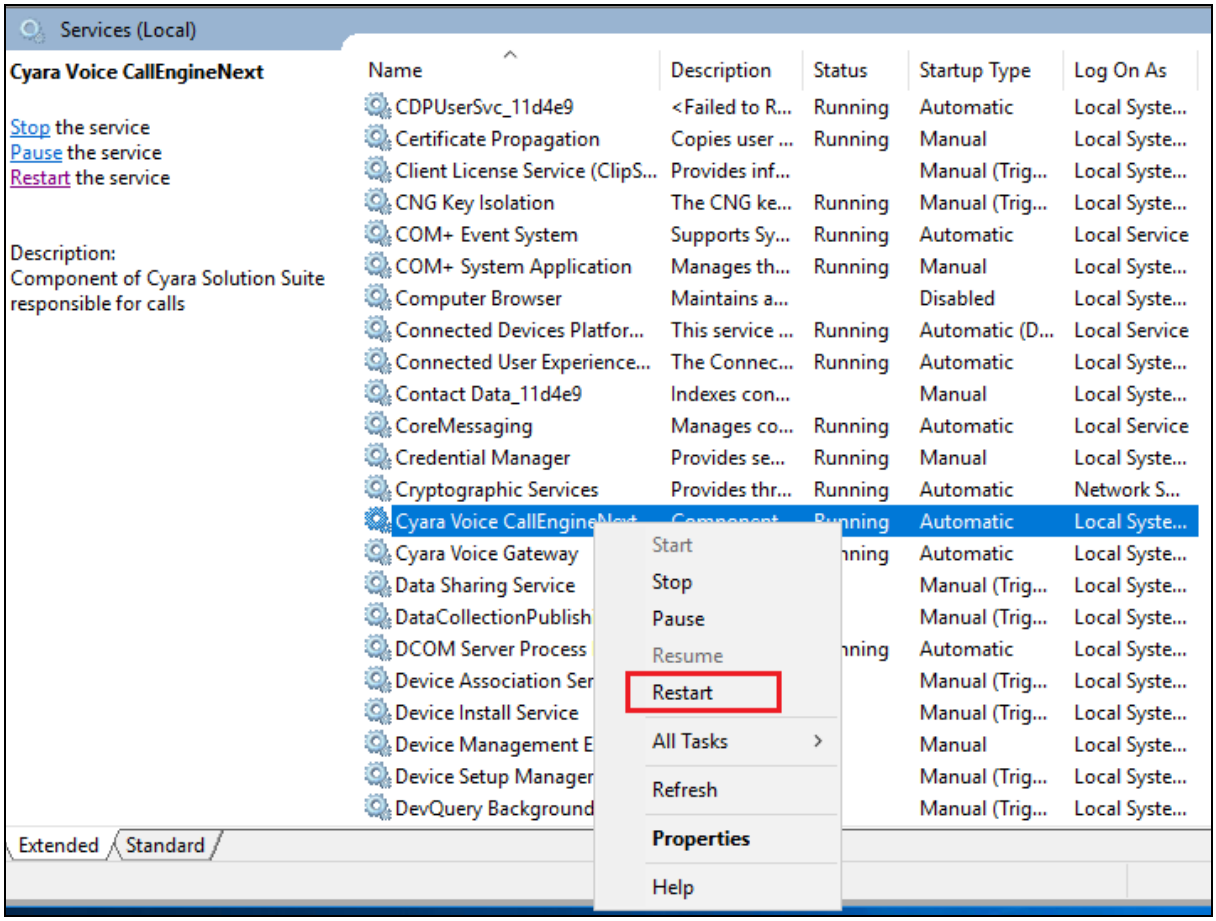


The **opal-aor.txt** file content specifies the range of extensions i.e., **10401** to **10410** register with Communication Manager as the gatekeeper through the Cyara Endpoint server which functions as the Cyara Voice Gateway. See below for the format. Note that the Communication Manager IP address is **10.1.10.230**.



6.2.3. Start Cyara Voice CallEngineNext Service

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

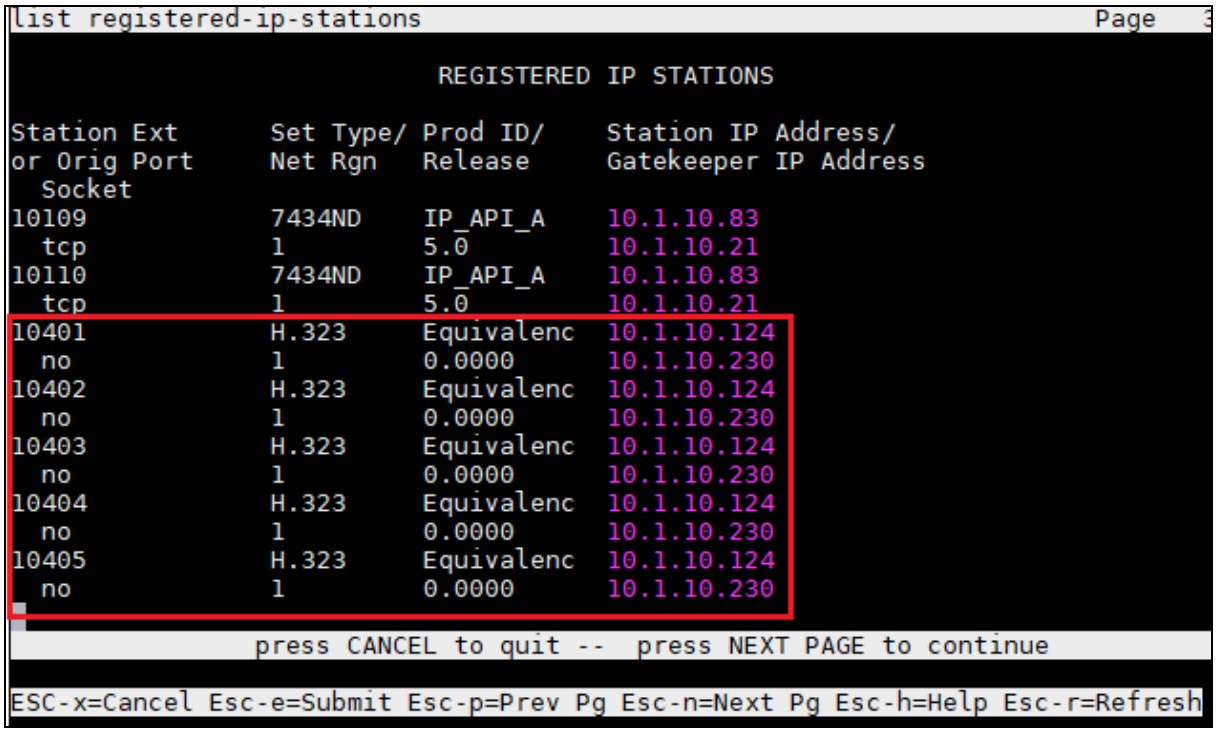


7. Verification Steps

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

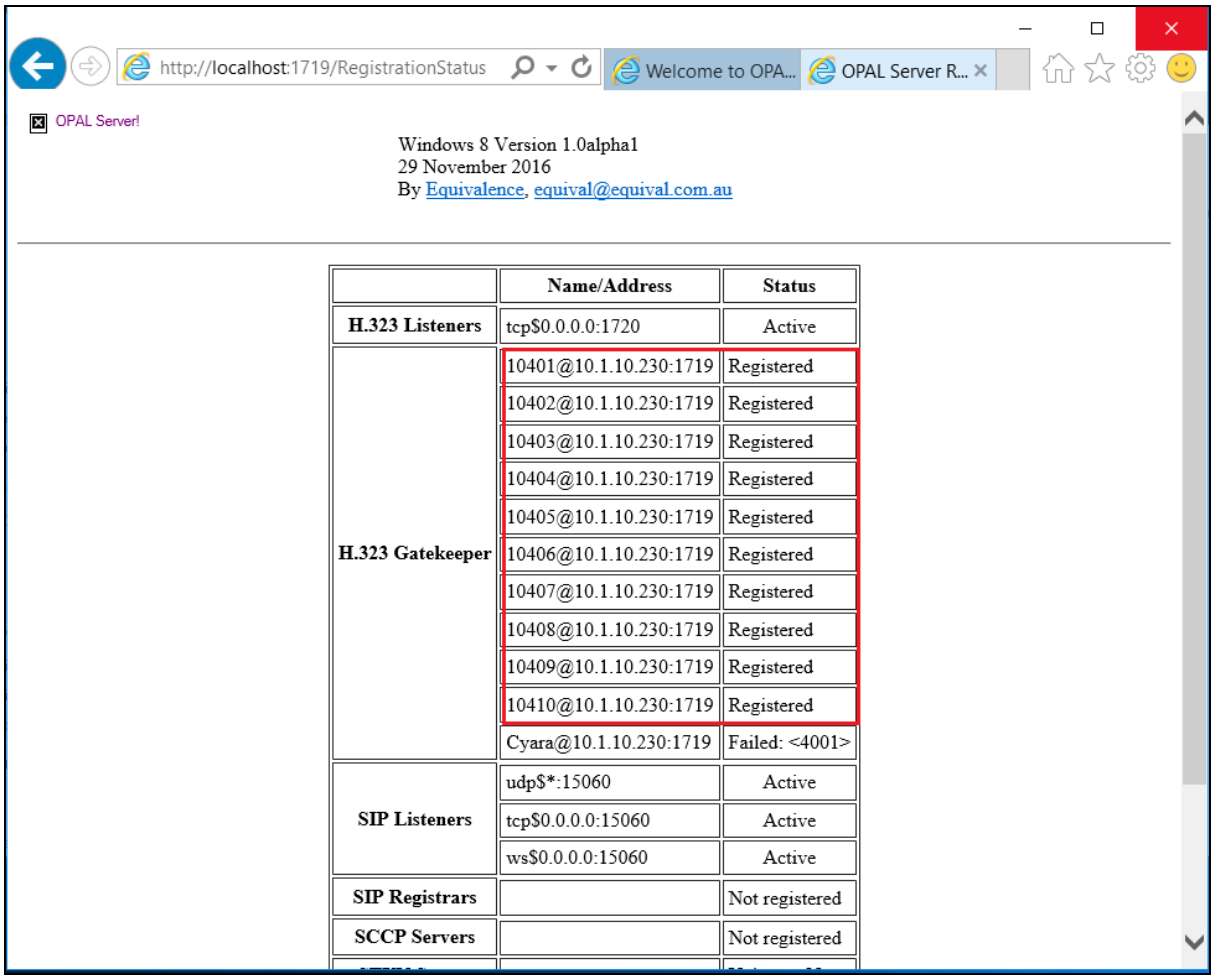
Verify the registration status of all the configured Cyara Virtual Endpoints by using the **list registered-ip-stations** command. The stations **10401 – 10410** should be listed as registered stations. Note the station IP address is the Cyara Endpoint server with Communication Manager as the Gatekeeper.



Make inbound and outbound calls by running the campaigns from Cyara Web Portal for handling calls.

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 (not shown). Verify that the **Status** of the Cyara Virtual Endpoints are all showing **Registered**.



	Name/Address	Status
H.323 Listeners	tcp$0.0.0.0:1720	Active
H.323 Gatekeeper	10401@10.1.10.230:1719	Registered
	10402@10.1.10.230:1719	Registered
	10403@10.1.10.230:1719	Registered
	10404@10.1.10.230:1719	Registered
	10405@10.1.10.230:1719	Registered
	10406@10.1.10.230:1719	Registered
	10407@10.1.10.230:1719	Registered
	10408@10.1.10.230:1719	Registered
	10409@10.1.10.230:1719	Registered
	10410@10.1.10.230:1719	Registered
	Cyara@10.1.10.230:1719	Failed: <4001>
SIP Listeners	udp$*:15060	Active
	tcp$0.0.0.0:15060	Active
	ws$0.0.0.0:15060	Active
SIP Registrars		Not registered
SCCP Servers		Not registered

8. Conclusion

These Application Notes describe the configuration steps required for Cyara Platform to interoperate with Avaya Aura® Communication Manager using H.323 Endpoints emulation. All feature test cases were completed successfully with observations in **Section 2.2**.

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*, Release 8.1.x, Issue 8, May 2020.
[2] *Application Notes for Cyara Platform Virtual Agent with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services*.

The following Cyara product documentation is obtained directly from member.
[3] *Cyara Platform Deployment Guide*.
[4] *Cyara User Guide*.