DevConnect Program

Application Notes for Cyara Platform 23.11 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 using SIP Trunk and H.323 Endpoint Emulation – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Cyara Platform 23.11 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 using SIP trunk and H.323 endpoint 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 Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required for Cyara Platform 23.11 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 using SIP trunk and H.323 endpoint emulation.

The Cyara Platform is an automated testing product 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 hosts the Cyara Voice Call Engine and Cyara Voice Gateway. Cyara Virtual Endpoints are configured on the Cyara Endpoint Server and emulate H.323 endpoints on Avaya Aura® Communication Manager for incoming calls. Outbound calls originate from Cyara Call Engine via the SIP trunk to Avaya Aura® Session Manager to simulate inbound calls to the emulated H.323 endpoints.

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 are 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 endpoints. Outbound calls are made by Cyara Call Engine via the SIP Trunk to Session Manager for inbound calls to H.323 emulated endpoints.

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.
- Terminating calls through Communication Manager and Session 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.

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.

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), Avaya Aura® Media Server, Session Manager and Avaya Aura® System Manager. System Manager is the administration and management tool for Avaya Aura® products. Avaya Workplace Client, Avaya Communicator and Avaya Agent for Desktop are used as utility softphones for initiating calls. Cyara Virtual Endpoint Server provides the virtual H.323 endpoints. Cyara Platform Server (which includes the Cyara Virtual Agent component) was installed with Microsoft SQL 2017 as the database server. The Cyara Virtual Agent is detailed in another Application Note reference **[2]**. In the compliance test, both Cyara Platform and Virtual Endpoint Servers are installed on the same physical server. A SIP trunk is configured between Session Manager and Cyara Endpoint Server to allow outbound calls to be made. A personal computer was used for Cyara Web Portal access. Avaya Session Border Controller was used to complete a SIP trunk connection to simulate a PSTN connection to the enterprise solution.

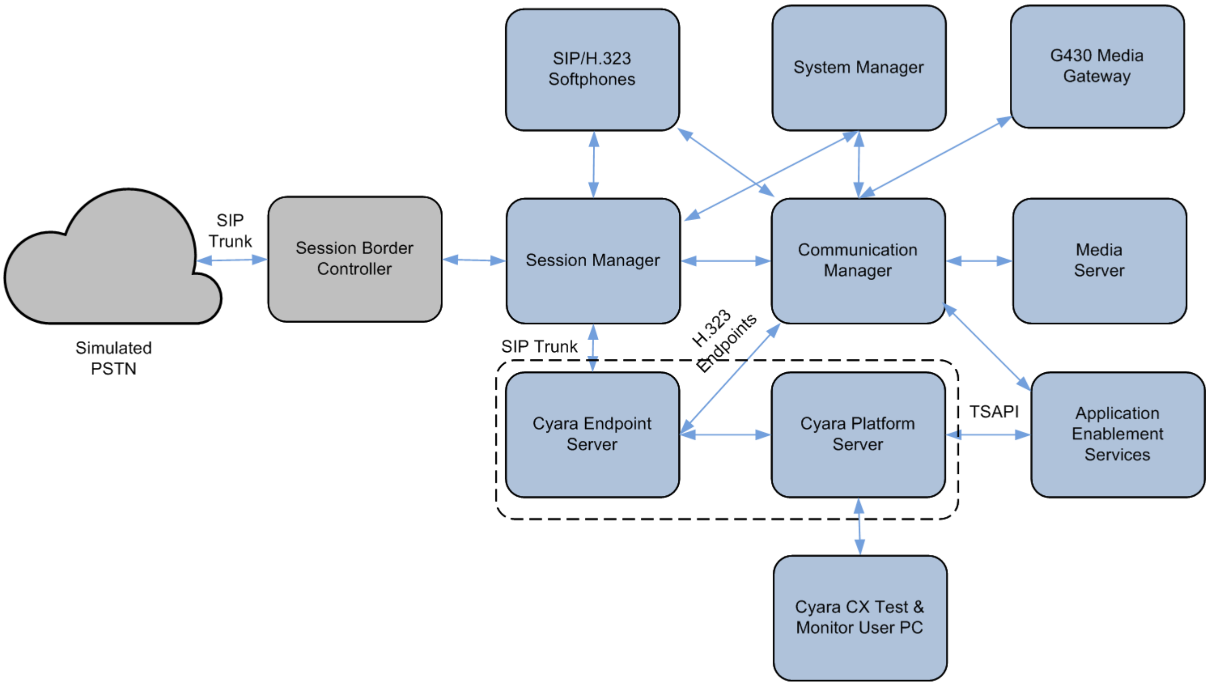


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Session Border Controller	10.1.0.0-32-21432
Avaya Aura® Communication Manager	10.1.3.1.0.974.27937
Avaya G430 Media Gateway	42.22.0
Avaya Aura® Application Enablement Services	10.1.3.1.0.49-0
Avaya Aura® Media Server	10.1.0.154
Avaya Aura® System Manager	System Manager 10.1 Build 10.1.0.0.537353 Feature Pack 3 Service Pack 1 Latest Build 10.1.3.1.0716418
Avaya Aura® Session Manager	10.1.3.1.1013103 patch 91698
Avaya Workplace Client (SIP)	3.34.1
Avaya Communicator (H.323/SIP)	6.2.14.4-SP14
Cyara Platform running on Windows Server with Microsoft SQL TSAPI Client	23.11.1.2 Microsoft Windows 2019 Microsoft SQL 2019 10.1.3.1
Cyara Endpoint Server running on Windows Server	23.11.1.2 Microsoft Windows 2019

Note: Avaya Aura® servers and Cyara server used in the test configuration were deployed in a virtualized environment. These servers ran as virtual machines on VMware®.

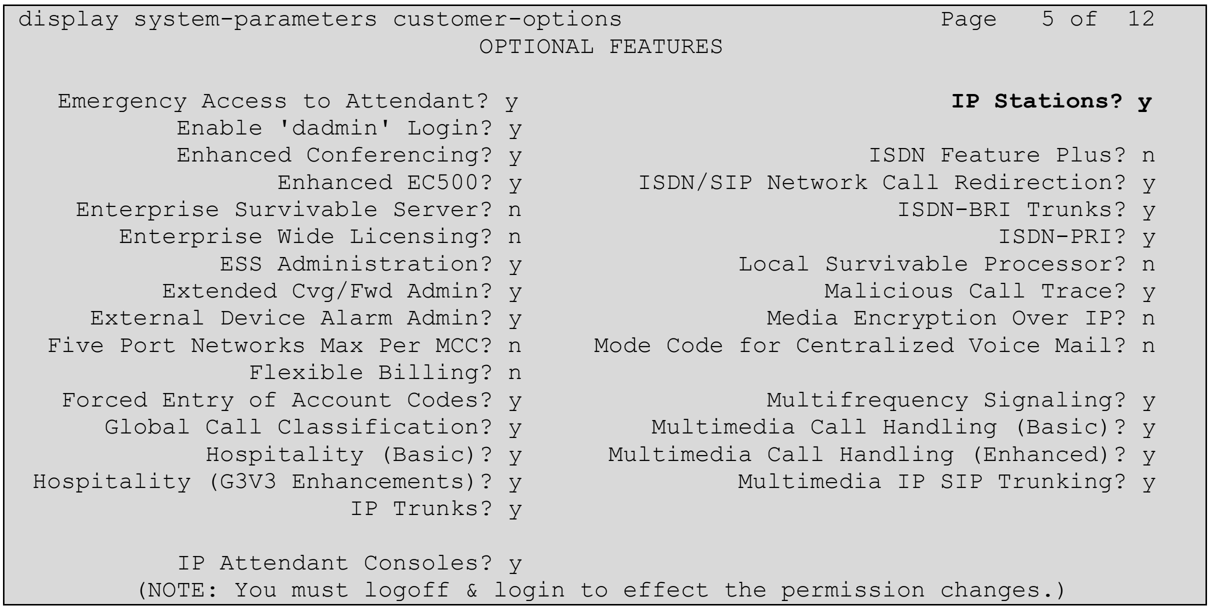
5. Configure Avaya Aura ® Communication Manager

This section provides the procedure for configuring Communication Manager.

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

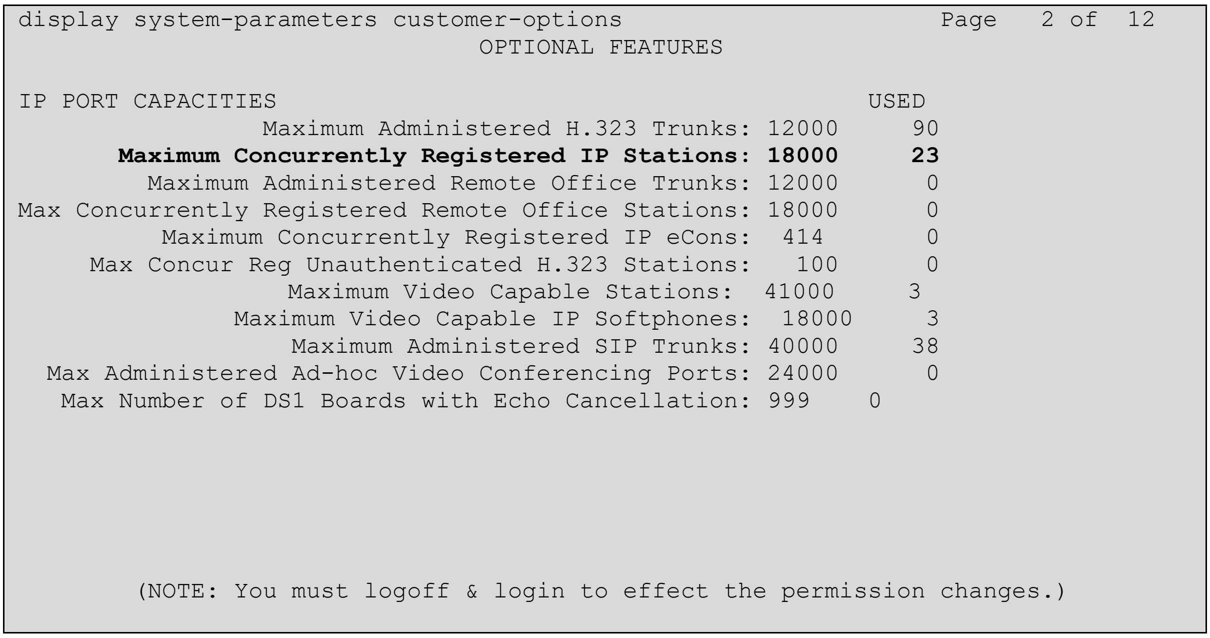
5.1. System Parameters Customer Options

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? 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.)
```

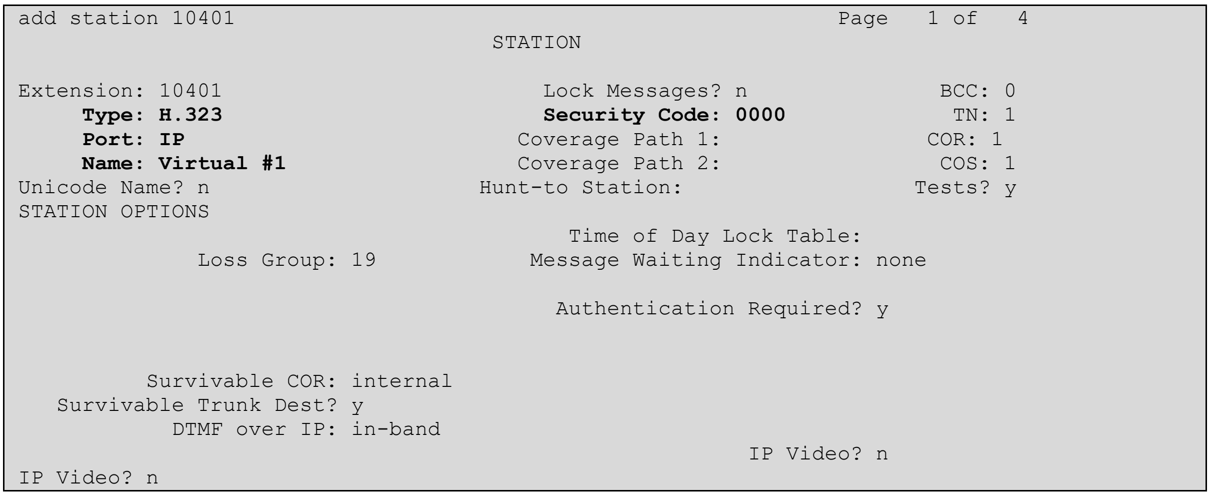
On **Page 2**, check the **Maximum Concurrently Registered IP Stations**. If the number is not sufficiently licensed, contact the Avaya sales team or business partner for a proper license file.



```
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     23
         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     3
               Maximum Video Capable IP Softphones:  18000     3
                   Maximum Administered SIP Trunks: 40000     38
  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.)
```

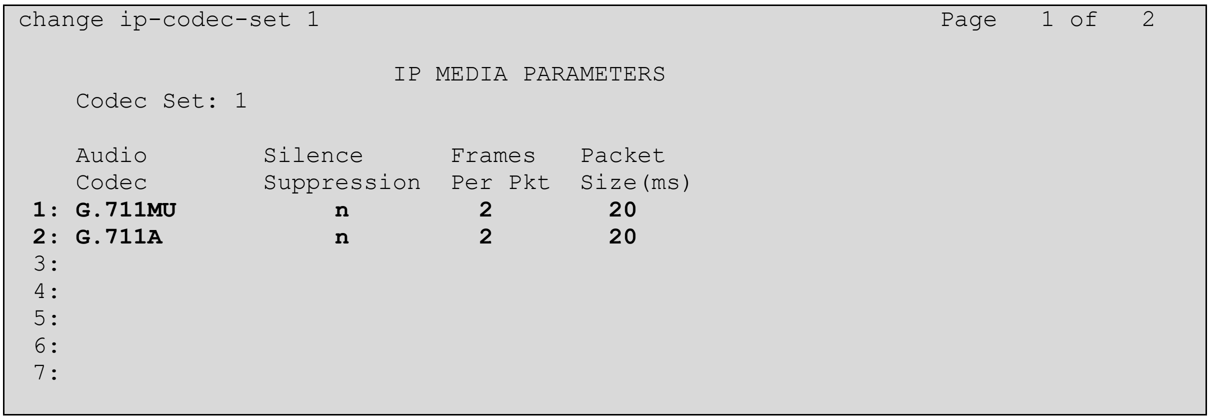
5.2. Configure Stations for Virtual Endpoint

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. 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. However, 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
Unicode Name? n                      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
IP Video? n
```

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

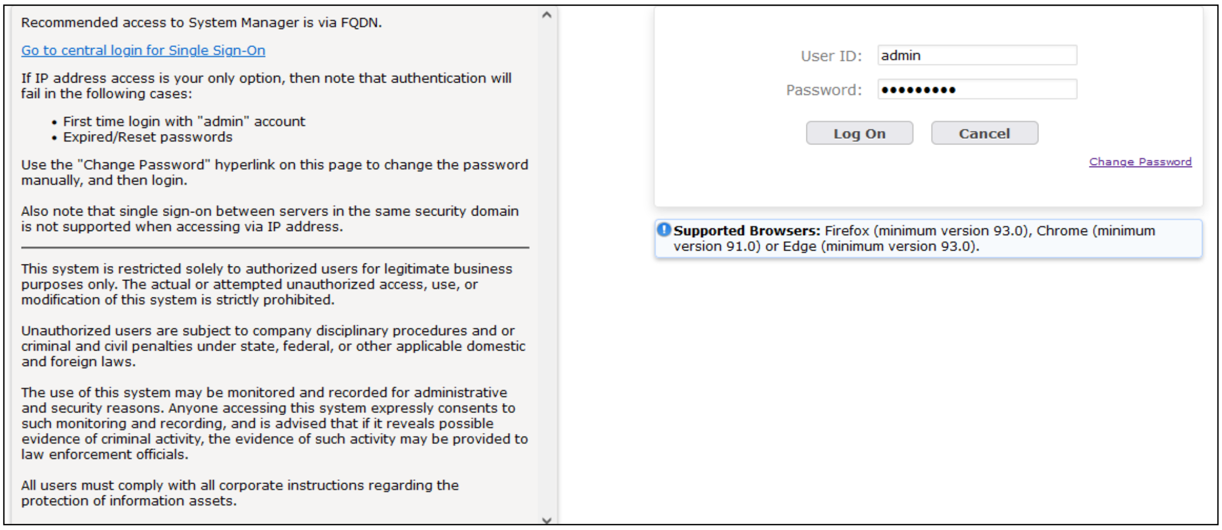


```
change ip-codec-set 1                                     Page   1 of   2

                          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:
```

6. Configure Avaya Aura® Session Manager

This section describes aspects of the Session Manager configuration required for the SIP trunk to Cyara Endpoint Server. It is assumed that the Domains, Locations, SIP Entities, Entity Links, Routing Policies, Dial Patterns and Application Sequences have been configured where appropriate for Communication Manager and Session Manager.

Session Manager is managed via System Manager. Using a web browser, access **https://<ip-addr of System Manager>/SMGR**. In the **Log On** screen, enter appropriate **User ID** and **Password** and click the **Log On** button.



Recommended access to System Manager is via FQDN.

Go to central login for Single Sign-On

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID: admin

Password: •••••••••

Supported Browsers: Firefox (minimum version 93.0), Chrome (minimum version 91.0) or Edge (minimum version 93.0).

6.1. Define SIP Entities

A SIP Entity must be added for Cyara Endpoint Server, in particular the Cyara Call Engine (CEN) component. To add a SIP Entity, expand **Elements** → **Routing** and select **SIP Entities** from the left navigation menu.

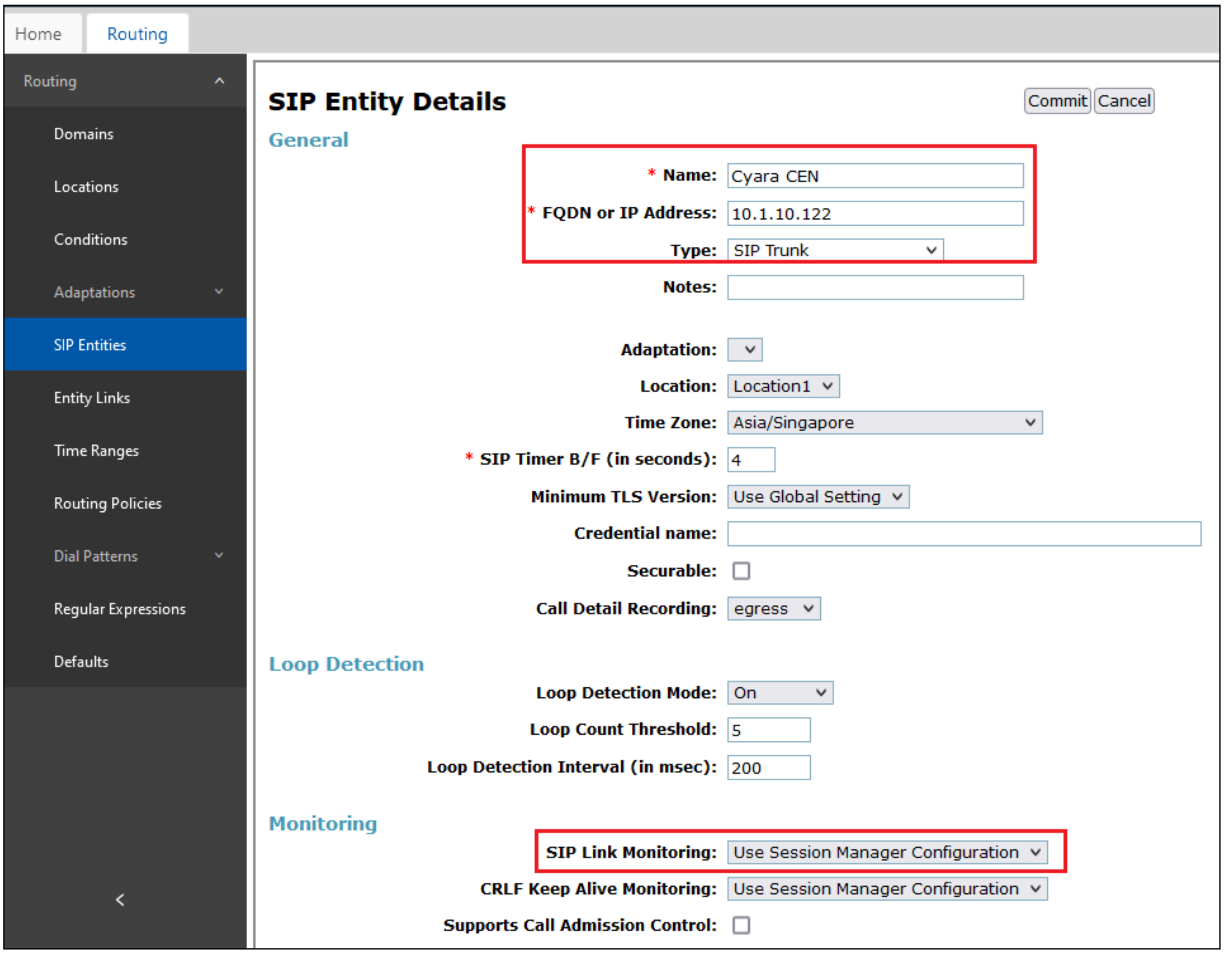
Click **New** (not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for new SIP Entity. In the sample configuration, *Cyara CEN* was used.
- **FQDN or IP Address:** Enter IP address such as *10.1.10.122.*
- **Type:** Select *SIP Trunk.*
- **Notes:** Enter a brief description. [Optional].
- **Location:** Select appropriate Location defined for Communication Manager.

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select *Link Monitoring Enabled*.

Click **Commit** to save SIP Entity definition. The following screen shows the SIP Entity defined for Cyara Endpoint Server.



SIP Entity Details

General

* Name: Cyara CEN
* FQDN or IP Address: 10.1.10.122
Type: SIP Trunk
Notes:
Adaptation:
Location: Location1
Time Zone: Asia/Singapore
* SIP Timer B/F (in seconds): 4
Minimum TLS Version: Use Global Setting
Credential name:
Securable: □
Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On
Loop Count Threshold: 5
Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration
CRLF Keep Alive Monitoring: Use Session Manager Configuration
Supports Call Admission Control: □

6.2. Define Entity Links

A SIP trunk between Cyara Endpoint Server and Session Manager is described by an Entity Link. In the sample configuration, a SIP Entity Link was added between Session Manager and Cyara Endpoint Server.

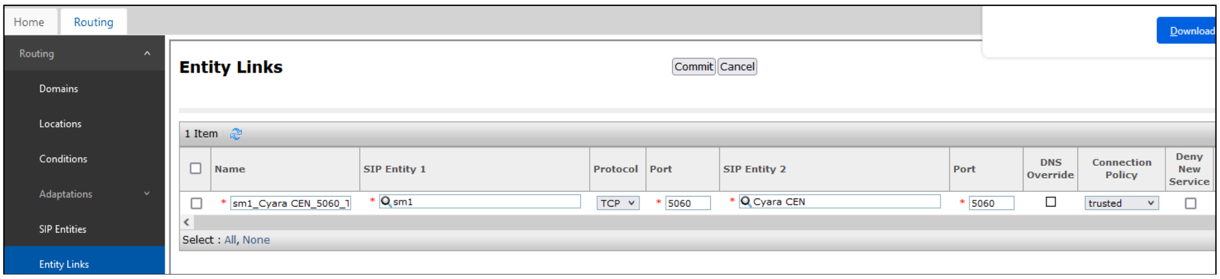
To add an Entity Link, expand **Elements→Routing** and select **Entity Links** from the left navigation menu.

Click **New** (not shown). Enter the following values**.**

- **Name:** Enter an identifier for the link to Session Manager.
- **SIP Entity 1:** Select existing Session Manager already configured.
- **SIP Entity 2:** Select the SIP Entity added in **Section 0** from drop-down menu.
- **Protocol:** After selecting both SIP Entities, enter the appropriate protocol configured for Cyara Endpoint Server. In the compliance testing, *TCP* was chosen.
- **Port:** Verify **Port** for both SIP entities is *5060*.
- **Connection Policy:** Select trusted.

Click **Commit** to save Entity Link definition.

The following screen shows the Entity Link defined between Cyara Endpoint Server and Session Manager.



Entity Links

1 Item

□	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy	Deny New Service
□	* sm1_Cyara CEN_5060_1	* sm1	TCP	* 5060	* Cyara CEN	* 5060	□	trusted	□

Select : All, None

6.3. Define Dial Pattern

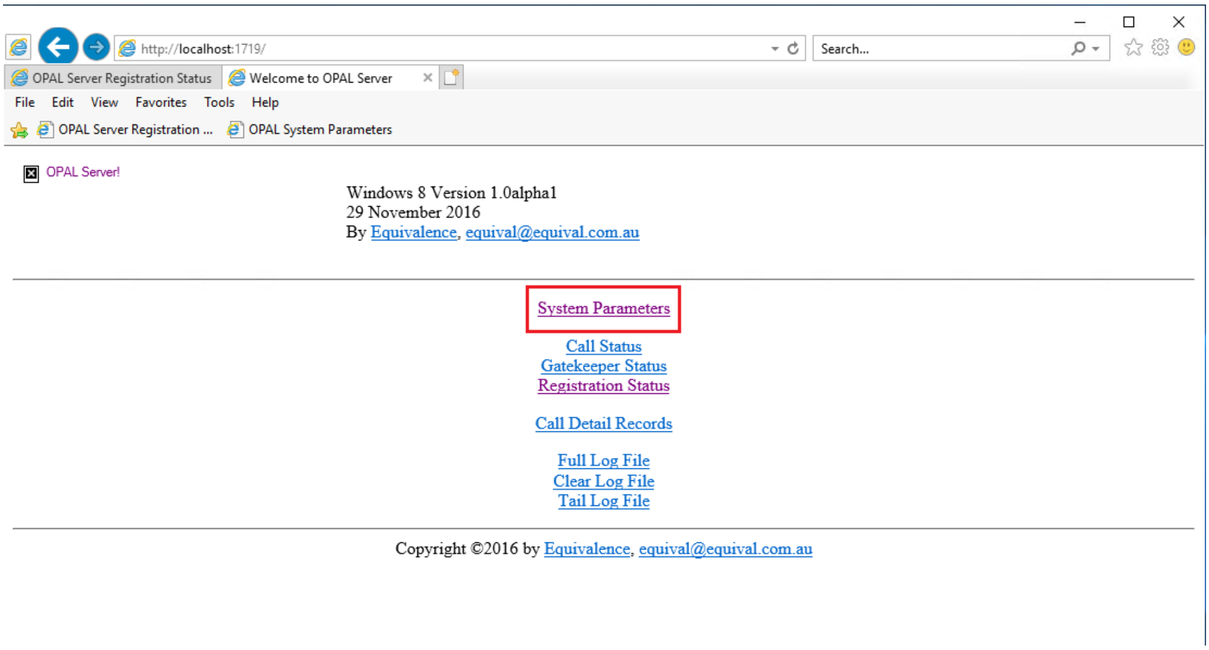
The dial pattern to route calls to Communication Manager is assumed to be defined for all extensions, VDNs and agent IDs on Communication Manager, including PSTN, and will not be detailed here.

7. Configure Cyara Endpoint Server

Setup of the Cyara Endpoint Server and Cyara Platform Server on Microsoft® Windows 2019 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 Internet Explorer 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 requires password access.



OPAL Server!

Windows 8 Version 1.0alpha1
29 November 2016
By Equivalence, equival@equival.com.au

System Parameters

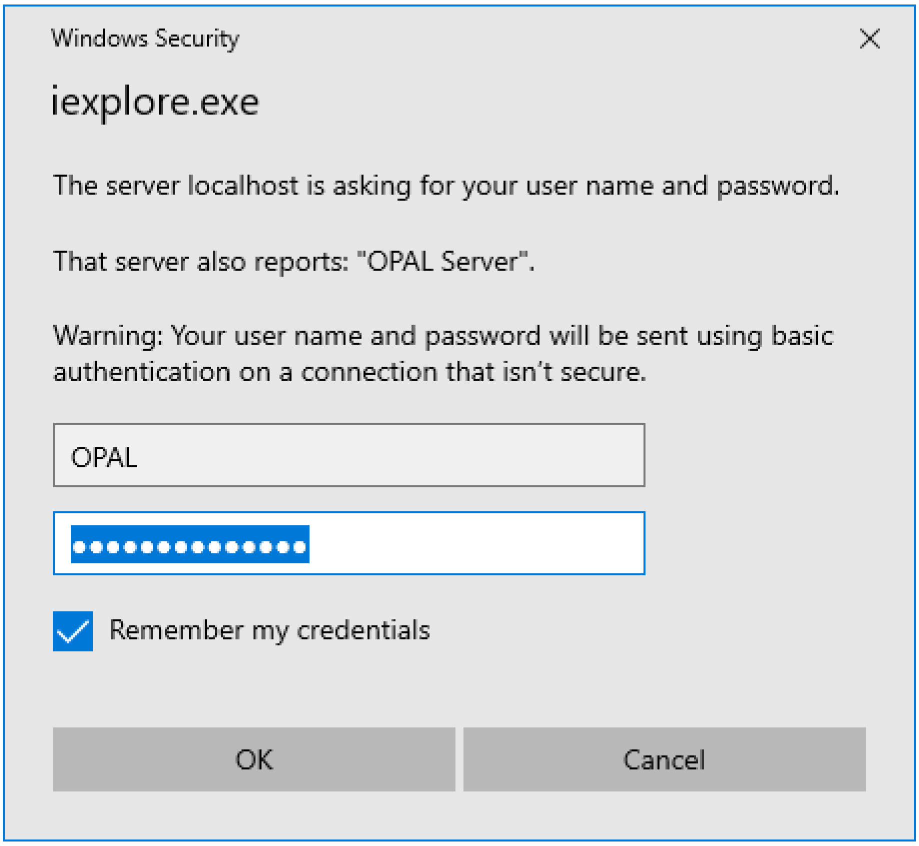
Call Status
Gatekeeper Status
Registration Status

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**. Then configure the relevant parameters in the next section.



Windows Security

iexplore.exe

The server localhost is asking for your user name and password.

That server also reports: "OPAL Server".

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

OPAL

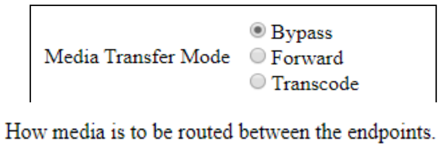
••••••••••••••

☑ Remember my credentials

7.1. Configure Cyara Endpoint

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

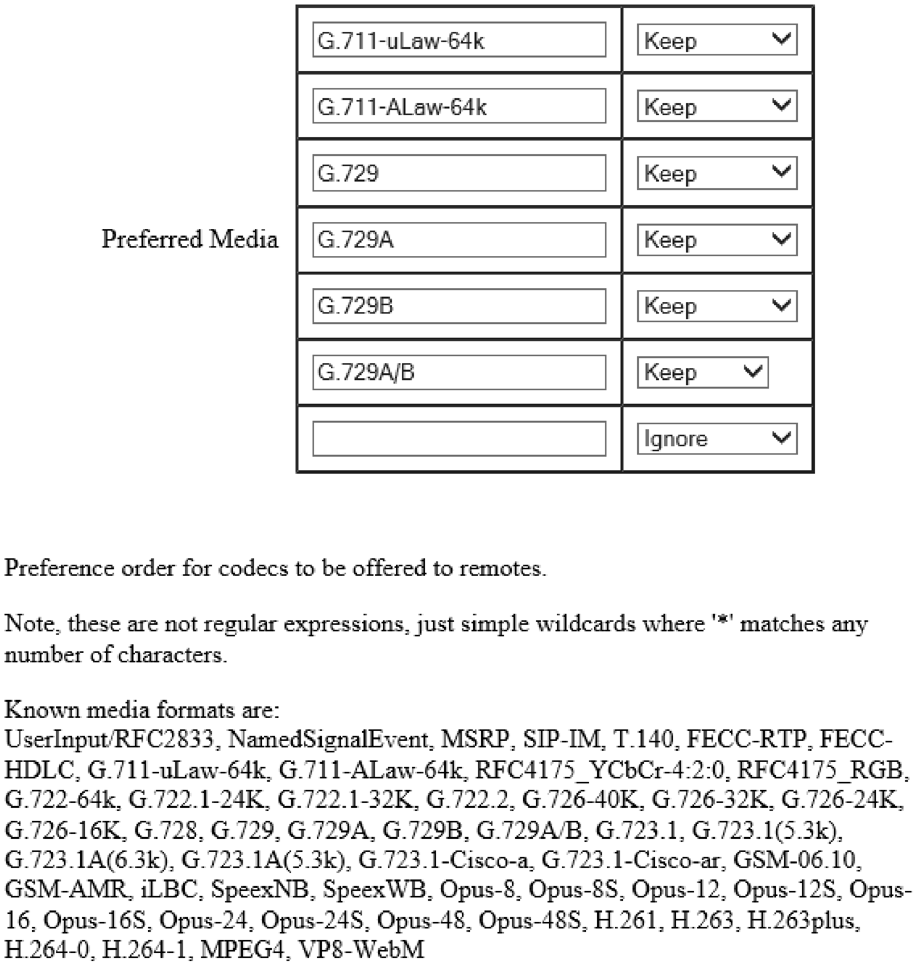
- Set the **Media Transfer Mode** to **Bypass** by selecting the button.



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 5.2**.



Preferred Media

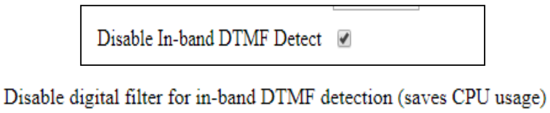
G.711-uLaw-64k	Keep
G.711-ALaw-64k	Keep
G.729	Keep
G.729A	Keep
G.729B	Keep
G.729A/B	Keep
	Ignore

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

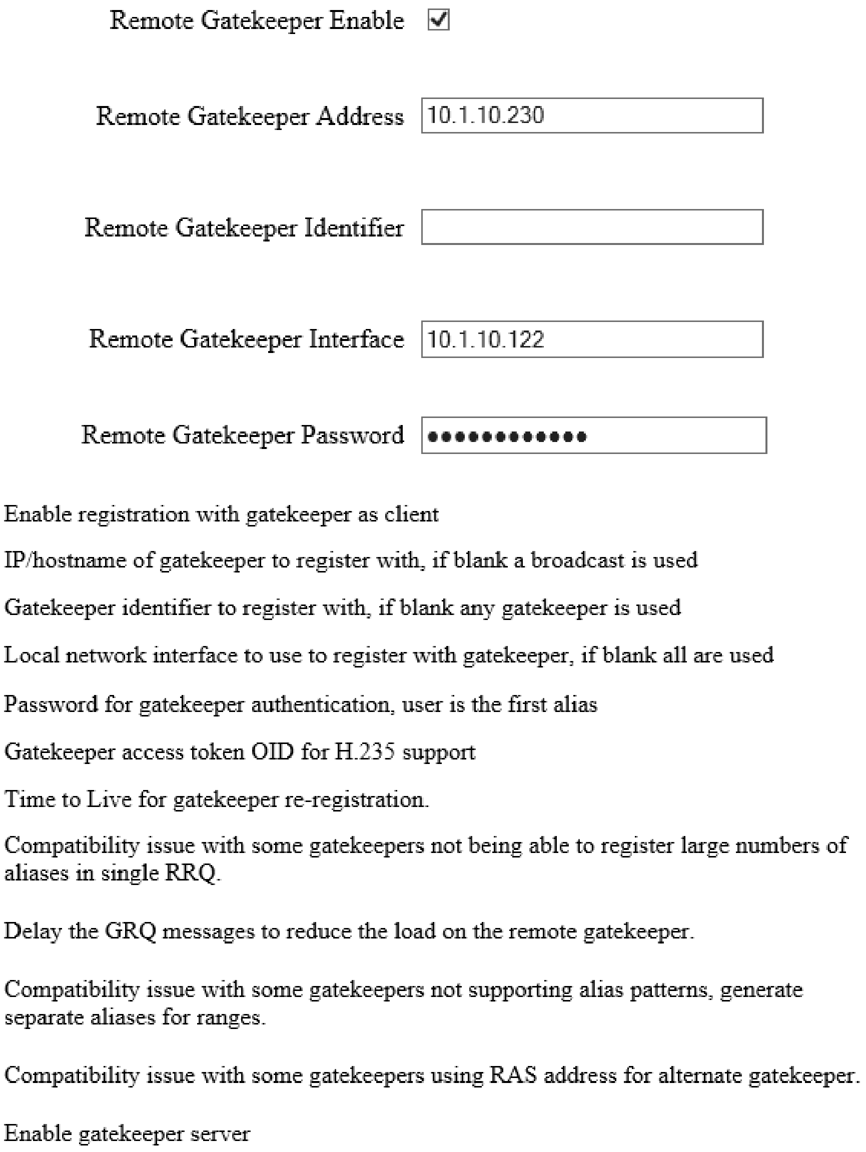
- Check the **Disable In-band DTMF Detect** to minimize the load on the system.



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 Server IP addresses. 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**.



Remote Gatekeeper Enable ☑

Remote Gatekeeper Address 10.1.10.230

Remote Gatekeeper Identifier

Remote Gatekeeper Interface 10.1.10.122

Remote Gatekeeper Password ●●●●●●●●●●●●

Enable registration with gatekeeper as client

IP/hostname of gatekeeper to register with, if blank a broadcast is used

Gatekeeper identifier to register with, if blank any gatekeeper is used

Local network interface to use to register with gatekeeper, if blank all are used

Password for gatekeeper authentication, user is the first alias

Gatekeeper access token OID for H.235 support

Time to Live for gatekeeper re-registration.

Compatibility issue with some gatekeepers not being able to register large numbers of aliases in single RRQ.

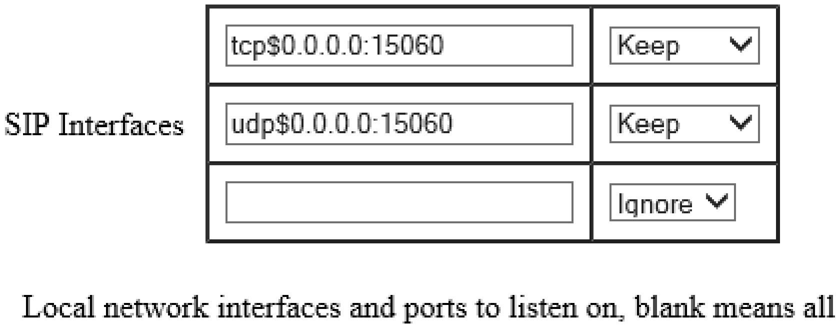
Delay the GRQ messages to reduce the load on the remote gatekeeper.

Compatibility issue with some gatekeepers not supporting alias patterns, generate separate aliases for ranges.

Compatibility issue with some gatekeepers using RAS address for alternate gatekeeper.

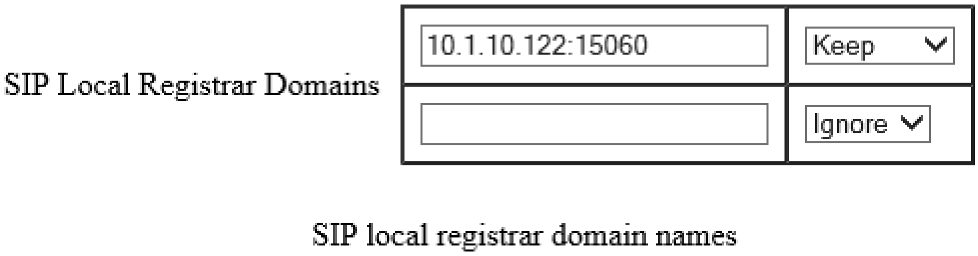
Enable gatekeeper server

- Because CEN is running on the same host as Voice Gateway, set the **SIP Interfaces Port** and set the **SIP Local Registrar Domains Port** to **15060**



SIP Interfaces		
	tcp$0.0.0.0:15060	Keep
	udp$0.0.0.0:15060	Keep
		Ignore

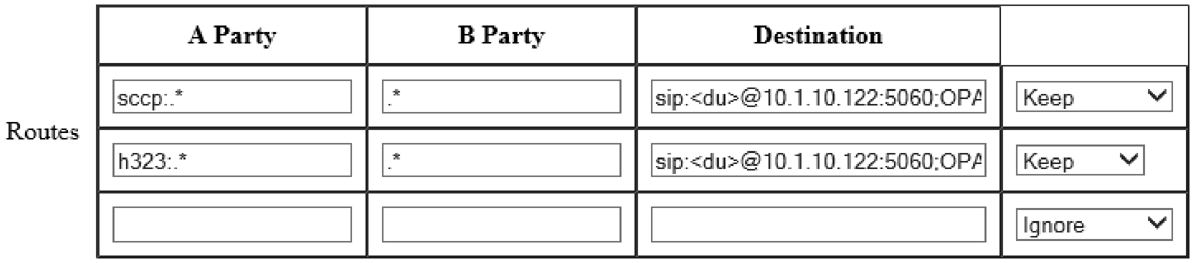
Local network interfaces and ports to listen on, blank means all



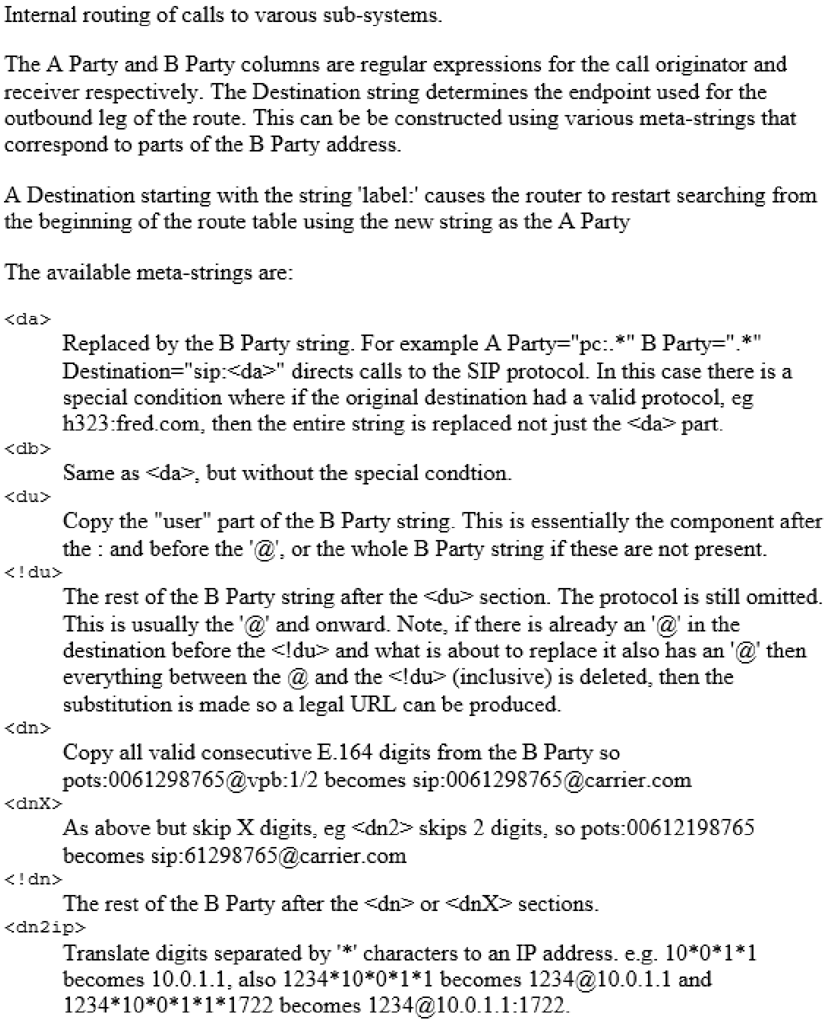
SIP Local Registrar Domains		
	10.1.10.122:15060	Keep
		Ignore

SIP local registrar domain names

- Set the **Routes** configuration for **A Party** to "**h323:.***" and **B Party** to "**.***" with **Destination** as "**sip:<du>@10.1.10.122;OPAL-Calling-Party-Number=<cu>**" and select **Keep** from the drop down menu.



Routes	A Party	B Party	Destination	
	sccp:.*	.*	sip:<du>@10.1.10.122:5060;OPA	Keep
	h323:.*	.*	sip:<du>@10.1.10.122:5060;OPA	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>`

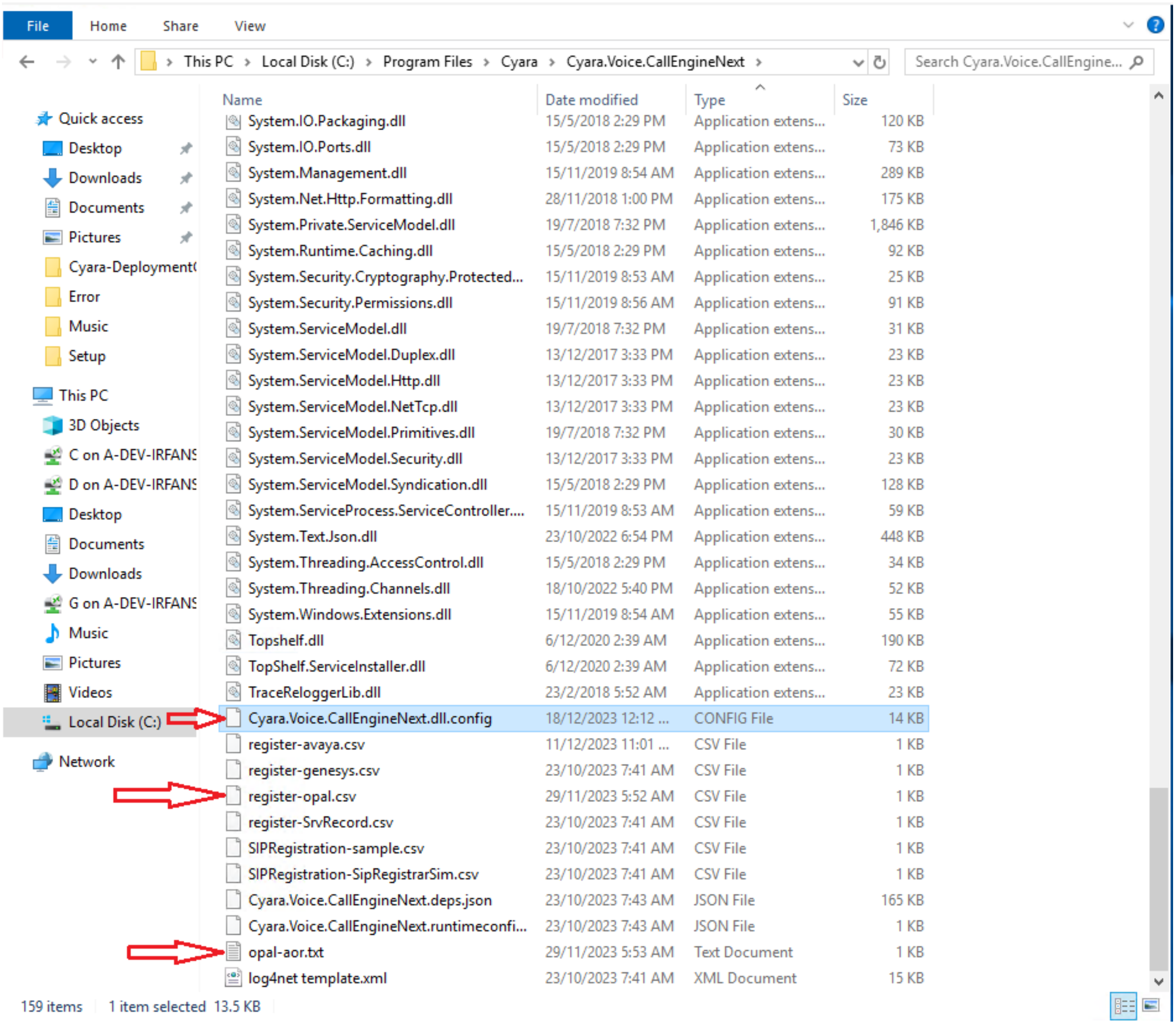
The rest of the B Party after the <dn> or <dnX> sections.

`<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.

7.2. Configure Cyara Call Engine

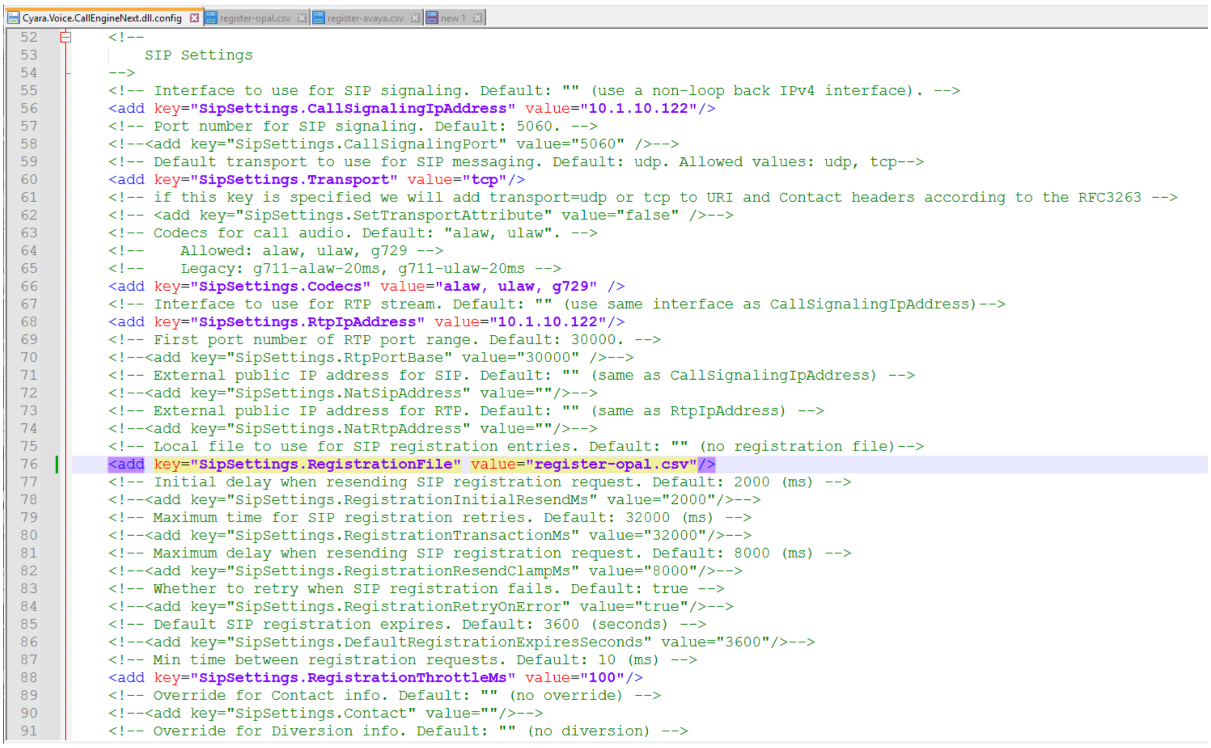
Cyara Call Engine resides as one of the components on the Cyara Platform. The configuration file needs to be configured. On the Cyara Platform Server, go to the location "**C:\Program Files\Cyara\Cyara.Voice.CallEngineNext**" below for the three files i.e., "Cyara.Voice.CallEngineNext.exe.config", "register-opal.csv"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



Name	Date modified	Type	Size
System.IO.Packaging.dll	15/5/2018 2:29 PM	Application extens...	120 KB
System.IO.Ports.dll	15/5/2018 2:29 PM	Application extens...	73 KB
System.Management.dll	15/11/2019 8:54 AM	Application extens...	289 KB
System.Net.Http.Formatting.dll	28/11/2018 1:00 PM	Application extens...	175 KB
System.Private.ServiceModel.dll	19/7/2018 7:32 PM	Application extens...	1,846 KB
System.Runtime.Caching.dll	15/5/2018 2:29 PM	Application extens...	92 KB
System.Security.Cryptography.Protected...	15/11/2019 8:53 AM	Application extens...	25 KB
System.Security.Permissions.dll	15/11/2019 8:56 AM	Application extens...	91 KB
System.ServiceModel.dll	19/7/2018 7:32 PM	Application extens...	31 KB
System.ServiceModel.Duplex.dll	13/12/2017 3:33 PM	Application extens...	23 KB
System.ServiceModel.Http.dll	13/12/2017 3:33 PM	Application extens...	23 KB
System.ServiceModel.NetTcp.dll	13/12/2017 3:33 PM	Application extens...	23 KB
System.ServiceModel.Primitives.dll	19/7/2018 7:32 PM	Application extens...	30 KB
System.ServiceModel.Security.dll	13/12/2017 3:33 PM	Application extens...	23 KB
System.ServiceModel.Syndication.dll	15/5/2018 2:29 PM	Application extens...	128 KB
System.ServiceProcess.ServiceController....	15/11/2019 8:53 AM	Application extens...	59 KB
System.Text.Json.dll	23/10/2022 6:54 PM	Application extens...	448 KB
System.Threading.AccessControl.dll	15/5/2018 2:29 PM	Application extens...	34 KB
System.Threading.Channels.dll	18/10/2022 5:40 PM	Application extens...	52 KB
System.Windows.Extensions.dll	15/11/2019 8:54 AM	Application extens...	55 KB
Topshelf.dll	6/12/2020 2:39 AM	Application extens...	190 KB
TopShelf.ServiceInstaller.dll	6/12/2020 2:39 AM	Application extens...	72 KB
TraceReloggerLib.dll	23/2/2018 5:52 AM	Application extens...	23 KB
Cyara.Voice.CallEngineNext.dll.config	18/12/2023 12:12 ...	CONFIG File	14 KB
register-avaya.csv	11/12/2023 11:01 ...	CSV File	1 KB
register-genesys.csv	23/10/2023 7:41 AM	CSV File	1 KB
register-opal.csv	29/11/2023 5:52 AM	CSV File	1 KB
register-SrvRecord.csv	23/10/2023 7:41 AM	CSV File	1 KB
SIPRegistration-sample.csv	23/10/2023 7:41 AM	CSV File	1 KB
SIPRegistration-SipRegistrarSim.csv	23/10/2023 7:41 AM	CSV File	1 KB
Cyara.Voice.CallEngineNext.deps.json	23/10/2023 7:43 AM	JSON File	165 KB
Cyara.Voice.CallEngineNext.runtimeconfi...	23/10/2023 7:43 AM	JSON File	1 KB
opal-aor.txt	29/11/2023 5:53 AM	Text Document	1 KB
log4net template.xml	23/10/2023 7:41 AM	XML Document	15 KB

7.2.1. 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. Note the **SipSettings.Tranport** value indicate the **tcp** protocol used which correspond to the SIP Entity links between Cyara Endpoint Server and Session Manager in **Section 6.2**.

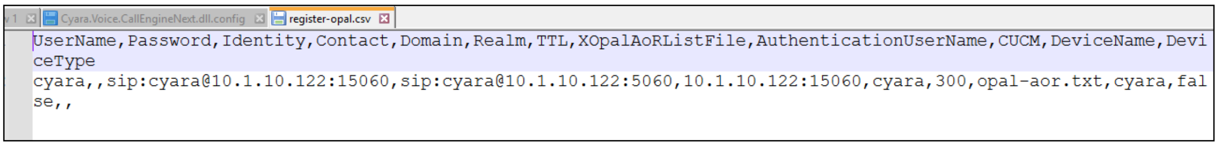


```
<!--
    SIP Settings
-->
<!-- Interface to use for SIP signaling. Default: "" (use a non-loop back IPv4 interface). -->
<add key="SipSettings.CallSignalingIpAddress" value="10.1.10.122"/>
<!-- Port number for SIP signaling. Default: 5060. -->
<!--<add key="SipSettings.CallSignalingPort" value="5060" />-->
<!-- Default transport to use for SIP messaging. Default: udp. Allowed values: udp, tcp-->
<add key="SipSettings.Transport" value="tcp"/>
<!-- if this key is specified we will add transport=udp or tcp to URI and Contact headers according to the RFC3263 -->
<!-- <add key="SipSettings.SetTransportAttribute" value="false" />-->
<!-- Codecs for call audio. Default: "alaw, ulaw". -->
<!--    Allowed: alaw, ulaw, g729 -->
<!--    Legacy: g711-alaw-20ms, g711-ulaw-20ms -->
<add key="SipSettings.Codecs" value="alaw, ulaw, g729" />
<!-- Interface to use for RTP stream. Default: "" (use same interface as CallSignalingIpAddress)-->
<add key="SipSettings.RtpIpAddress" value="10.1.10.122"/>
<!-- First port number of RTP port range. Default: 30000. -->
<!--<add key="SipSettings.RtpPortBase" value="30000" />-->
<!-- External public IP address for SIP. Default: "" (same as CallSignalingIpAddress) -->
<!--<add key="SipSettings.NatSipAddress" value=""/>-->
<!-- External public IP address for RTP. Default: "" (same as RtpIpAddress) -->
<!--<add key="SipSettings.NatRtpAddress" value=""/>-->
<!-- Local file to use for SIP registration entries. Default: "" (no registration file)-->
<add key="SipSettings.RegistrationFile" value="register-opal.csv"/>
<!-- Initial delay when resending SIP registration request. Default: 2000 (ms) -->
<!--<add key="SipSettings.RegistrationInitialResendMs" value="2000"/>-->
<!-- Maximum time for SIP registration retries. Default: 32000 (ms) -->
<!--<add key="SipSettings.RegistrationTransactionMs" value="32000"/>-->
<!-- Maximum delay when resending SIP registration request. Default: 8000 (ms) -->
<!--<add key="SipSettings.RegistrationResendClampMs" value="8000"/>-->
<!-- Whether to retry when SIP registration fails. Default: true -->
<!--<add key="SipSettings.RegistrationRetryOnError" value="true"/>-->
<!-- Default SIP registration expires. Default: 3600 (seconds) -->
<!--<add key="SipSettings.DefaultRegistrationExpiresSeconds" value="3600"/>-->
<!-- Min time between registration requests. Default: 10 (ms) -->
<add key="SipSettings.RegistrationThrottleMs" value="100"/>
<!-- Override for Contact info. Default: "" (no override) -->
<!--<add key="SipSettings.Contact" value=""/>-->
<!-- Override for Diversion info. Default: "" (no diversion) -->
```

7.2.2. register-opal.csv

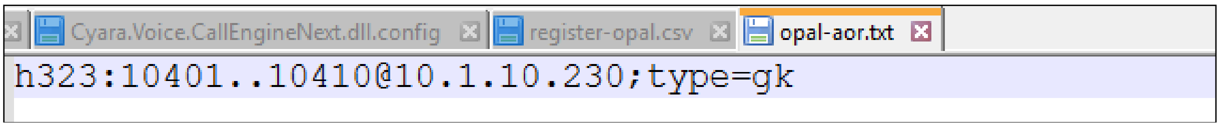
Configure the following for the csv file.

UserName	cyara
Password	
Identity	cyara@10.1.10.122:15060
Contact	cyara@10.1.10.122:5060
Domain	cyara@10.1.10.122:15060
Realm	cyara
TTL	300
XOpalAorListFile	opal-aor.txt



```
UserName,Password,Identity,Contact,Domain,Realm,TTL,XOpalAoRListFile,AuthenticationUserName,CUCM,DeviceName,Devi
ceType
cyara,,sip:cyara@10.1.10.122:15060,sip:cyara@10.1.10.122:5060,10.1.10.122:15060,cyara,300,opal-aor.txt,cyara,fal
se,,
```

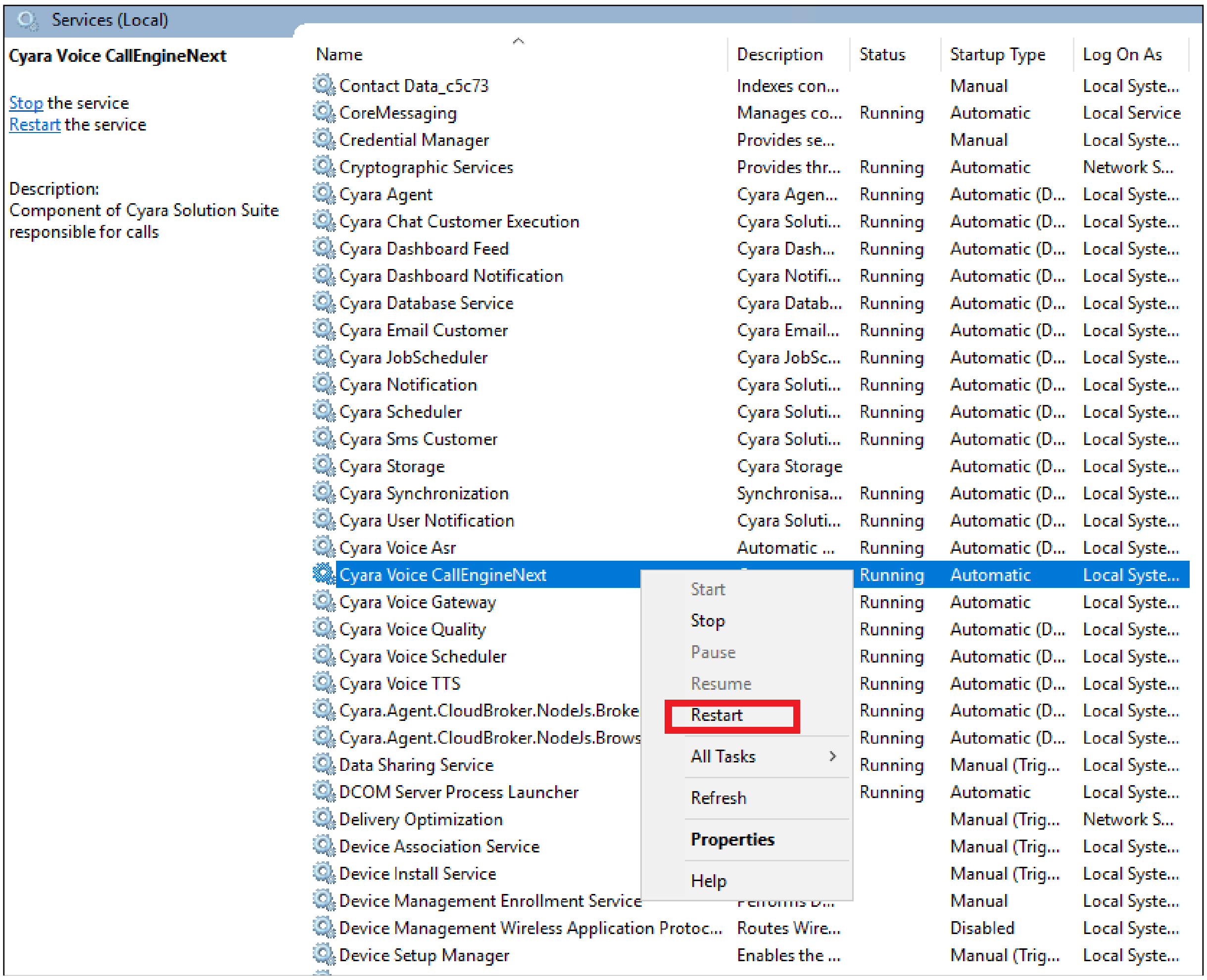
The **opal-aor.txt** file content specifies the range of extensions i.e., **10401** to **10410** to register with Communication Manager as the gatekeeper through the Cyara Endpoint Server which functions as the Cyara Voice Gateway. See below for the format. Note that the Communication Manager IP address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



```
h323:10401..10410@10.1.10.230;type=gk
```

7.2.3. 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.



Cyara Voice CallEngineNext

Stop the service
Restart the service

Description:
Component of Cyara Solution Suite responsible for calls

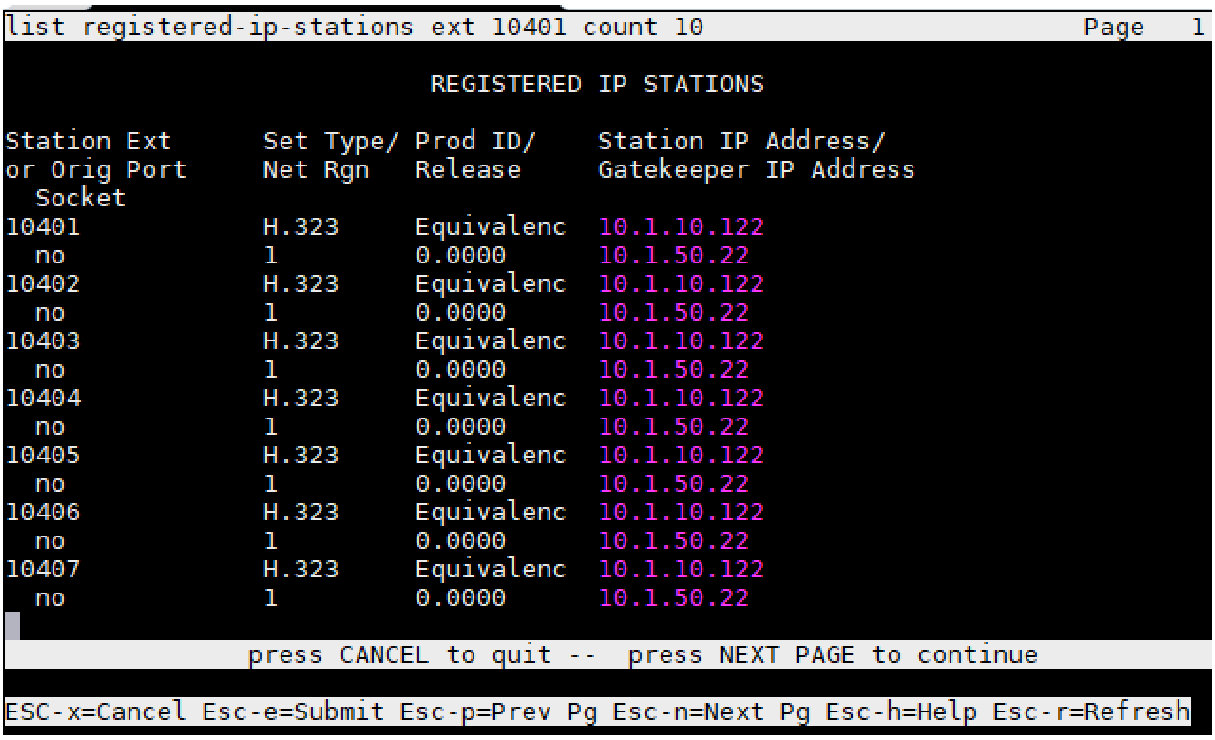
Name	Description	Status	Startup Type	Log On As
Contact Data_c5c73	Indexes con...		Manual	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...		Manual	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
Cyara Agent	Cyara Agen...	Running	Automatic (D...	Local Syste...
Cyara Chat Customer Execution	Cyara Soluti...	Running	Automatic (D...	Local Syste...
Cyara Dashboard Feed	Cyara Dash...	Running	Automatic (D...	Local Syste...
Cyara Dashboard Notification	Cyara Notifi...	Running	Automatic (D...	Local Syste...
Cyara Database Service	Cyara Datab...	Running	Automatic (D...	Local Syste...
Cyara Email Customer	Cyara Email...	Running	Automatic (D...	Local Syste...
Cyara JobScheduler	Cyara JobSc...	Running	Automatic (D...	Local Syste...
Cyara Notification	Cyara Soluti...	Running	Automatic (D...	Local Syste...
Cyara Scheduler	Cyara Soluti...	Running	Automatic (D...	Local Syste...
Cyara Sms Customer	Cyara Soluti...	Running	Automatic (D...	Local Syste...
Cyara Storage	Cyara Storage		Automatic (D...	Local Syste...
Cyara Synchronization	Synchronisa...	Running	Automatic (D...	Local Syste...
Cyara User Notification	Cyara Soluti...	Running	Automatic (D...	Local Syste...
Cyara Voice Asr	Automatic ...	Running	Automatic (D...	Local Syste...
Cyara Voice CallEngineNext		Running	Automatic	Local Syste...
Cyara Voice Gateway		Running	Automatic	Local Syste...
Cyara Voice Quality		Running	Automatic (D...	Local Syste...
Cyara Voice Scheduler		Running	Automatic (D...	Local Syste...
Cyara Voice TTS		Running	Automatic (D...	Local Syste...
Cyara.Agent.CloudBroker.NodeJs.Broke		Running	Automatic (D...	Local Syste...
Cyara.Agent.CloudBroker.NodeJs.Brows		Running	Automatic (D...	Local Syste...
Data Sharing Service		Running	Manual (Trig...	Local Syste...
DCOM Server Process Launcher		Running	Automatic	Local Syste...
Delivery Optimization			Manual (Trig...	Network S...
Device Association Service			Manual (Trig...	Local Syste...
Device Install Service			Manual (Trig...	Local Syste...
Device Management Enrollment Service	Performs D...		Manual	Local Syste...
Device Management Wireless Application Protoc...	Routes Wire...		Disabled	Local Syste...
Device Setup Manager	Enables the ...		Manual (Trig...	Local Syste...

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

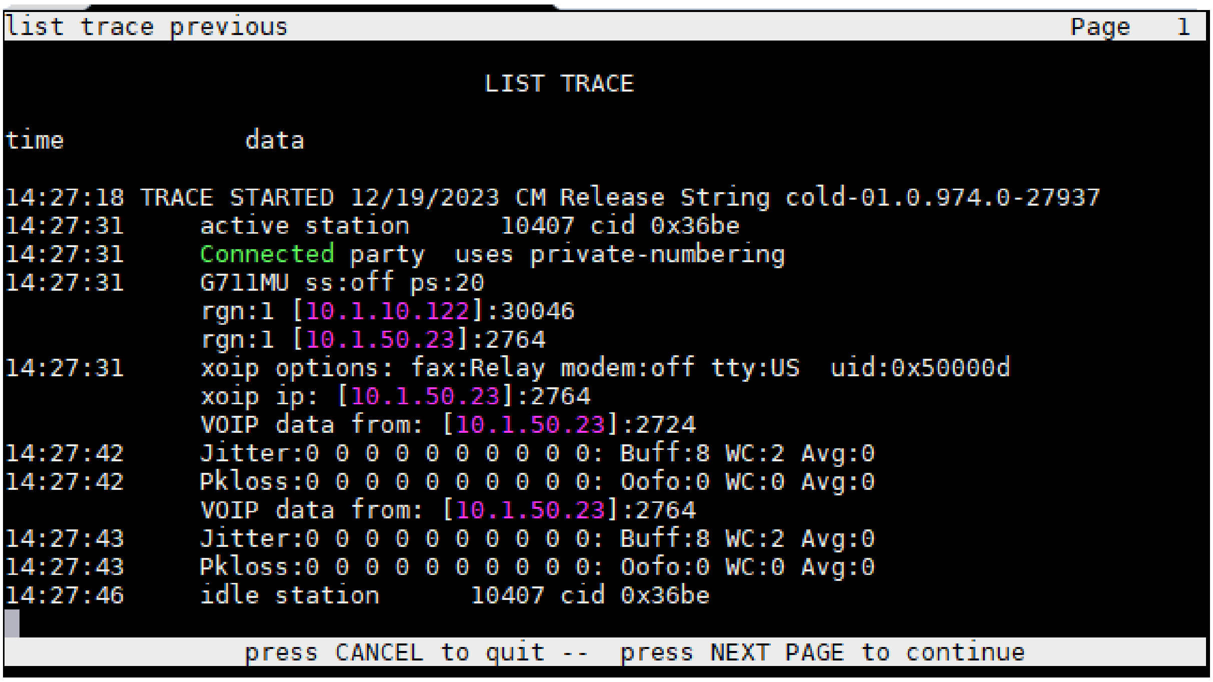
Verify the registration status of all the configured Cyara Virtual Endpoints by using the **list registered-ip-stations** command. The stations **10401 – 10410** should be listed as registered stations. Note the station IP address is the Cyara Endpoint Server with Communication Manager as the Gatekeeper.



```
list registered-ip-stations ext 10401 count 10                      Page   1

                            REGISTERED IP STATIONS

Station Ext      Set Type/ Prod ID/    Station IP Address/
or Orig Port     Net Rgn   Release     Gatekeeper IP Address
  Socket
10401            H.323     Equivalenc  10.1.10.122
  no             1         0.0000      10.1.50.22
10402            H.323     Equivalenc  10.1.10.122
  no             1         0.0000      10.1.50.22
10403            H.323     Equivalenc  10.1.10.122
  no             1         0.0000      10.1.50.22
10404            H.323     Equivalenc  10.1.10.122
  no             1         0.0000      10.1.50.22
10405            H.323     Equivalenc  10.1.10.122
  no             1         0.0000      10.1.50.22
10406            H.323     Equivalenc  10.1.10.122
  no             1         0.0000      10.1.50.22
10407            H.323     Equivalenc  10.1.10.122
  no             1         0.0000      10.1.50.22

                press CANCEL to quit --  press NEXT PAGE to continue

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

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

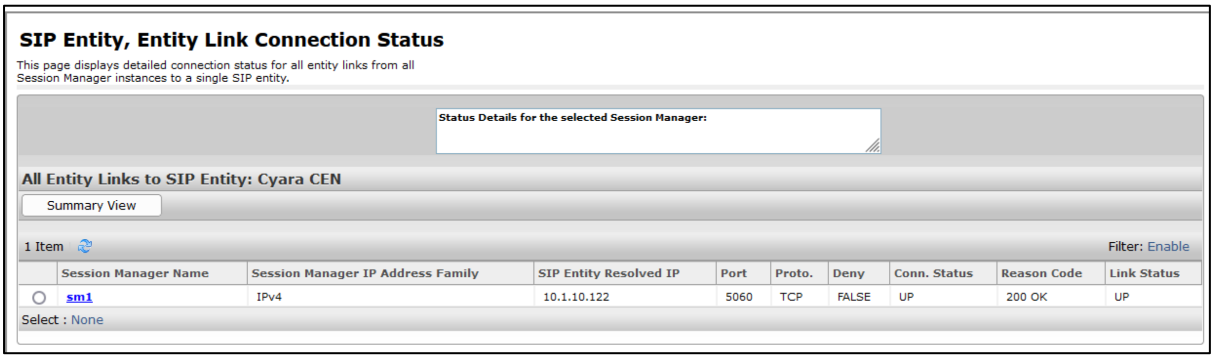
Verify with list trace stations such as an inbound call below:



```
list trace previous                                                    Page    1

                                    LIST TRACE

time            data

14:27:18 TRACE STARTED 12/19/2023 CM Release String cold-01.0.974.0-27937
14:27:31     active station      10407 cid 0x36be
14:27:31     Connected party  uses private-numbering
14:27:31     G711MU ss:off ps:20
             rgn:1 [10.1.10.122]:30046
             rgn:1 [10.1.50.23]:2764
14:27:31     xoip options: fax:Relay modem:off tty:US  uid:0x50000d
             xoip ip: [10.1.50.23]:2764
             VOIP data from: [10.1.50.23]:2724
14:27:42     Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 WC:2 Avg:0
14:27:42     Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 WC:0 Avg:0
             VOIP data from: [10.1.50.23]:2764
14:27:43     Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 WC:2 Avg:0
14:27:43     Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 WC:0 Avg:0
14:27:46     idle station      10407 cid 0x36be

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

8.2. Verify Avaya Aura® Session Manager

From the home page of System Manager in **Section 6**, navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown). Click under **SIP Entity Name** list **Cyara CEN** on the right pane. Verify that the **Link Status** is UP as shown below.



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: Cyara CEN

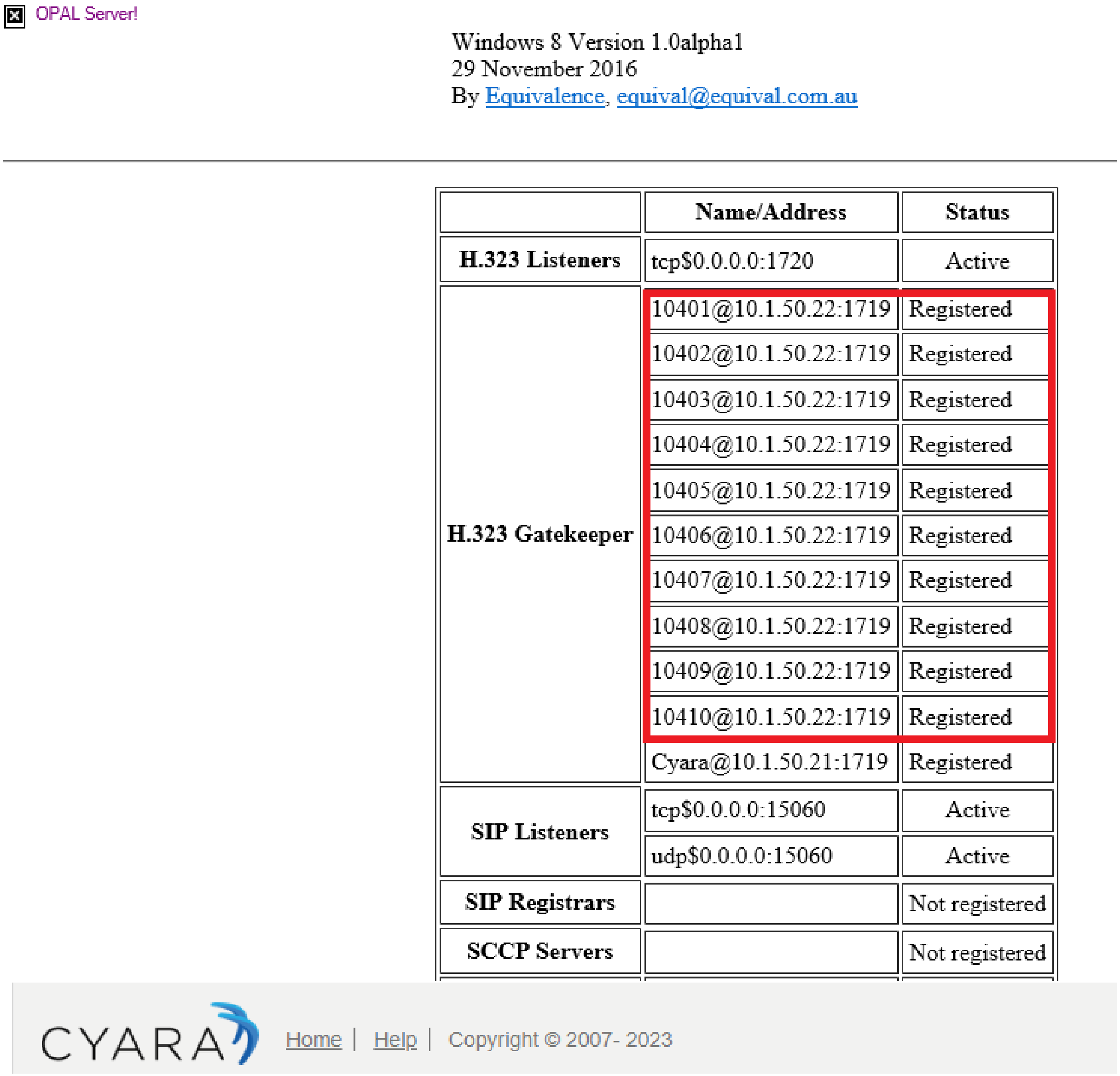
1 Item

	Session Manager Name	Session Manager IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	sm1	IPv4	10.1.10.122	5060	TCP	FALSE	UP	200 OK	UP

Select : None

8.3. 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**.



☒ OPAL Server!

Windows 8 Version 1.0alpha1
29 November 2016
By Equivalence, equival@equival.com.au

	Name/Address	Status
H.323 Listeners	tcp$0.0.0.0:1720	Active
H.323 Gatekeeper	10401@10.1.50.22:1719	Registered
	10402@10.1.50.22:1719	Registered
	10403@10.1.50.22:1719	Registered
	10404@10.1.50.22:1719	Registered
	10405@10.1.50.22:1719	Registered
	10406@10.1.50.22:1719	Registered
	10407@10.1.50.22:1719	Registered
	10408@10.1.50.22:1719	Registered
	10409@10.1.50.22:1719	Registered
	10410@10.1.50.22:1719	Registered
	Cyara@10.1.50.21:1719	Registered
SIP Listeners	tcp$0.0.0.0:15060	Active
	udp$0.0.0.0:15060	Active
SIP Registrars		Not registered
SCCP Servers		Not registered

9. Conclusion

These Application Notes describe the configuration steps required for Cyara Platform 23.11 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Session Manager 10.1 using SIP Trunk and H.323 Endpoints emulation. All feature test cases were successfully completed.

10. Additional References

This section references the Avaya and Cyara documentation 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 10.1, Issue 10, Oct 2023.
[2] *Application Notes for Cyara Platform Virtual Agent 23.11 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services*.

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

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.