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/](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.

Figure 1: Test Configuration
### 4. Equipment and Software Validated

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

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

Table 1: Equipment/Software Validated
5. Configure Avaya Aura ® Communication Manager

This section provides the procedures for configuring 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter <strong>display system-parameters customer-options</strong> command and on <strong>Page 5</strong>, check the <strong>IP Stations</strong> is set to y. If the feature is not licensed, then contact the Avaya sales team or business partner for a proper license file.</td>
</tr>
</tbody>
</table>

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

OPTIONAL FEATURES

Emergency Access to Attendant? y
Enable 'dadmin' Login? y
Enhanced Conferencing? y
Enhanced EC500? y
Enterprise Survivable Server? n
Enterprise Wide Licensing? n
BSS Administration? y
Extended Cvg/Fwd Admin? y
External Device Alarm Admin? y
Five Port Networks Max Per MCC? n
Flexible Billing? n
Forced Entry of Account Codes? y
Global Call Classification? y
Hospitality (Basic)? y
Hospitality (G3V3 Enhancements)? y
Flexible Billing? n
Forced Entry of Account Codes? y
Multifrequency Signaling? y
Multimedia Call Handling (Basic)? y
Multimedia Call Handling (Enhanced)? y
Multimedia IP SIP Trunking? y
IP Trunks? y
IP Attendant Consoles? y

(NO: You must logoff & login to effect the permission changes.)
```

| 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

Maximum Administered H.323 Trunks: 12000 70
Maximum Concurrently Registered H.323 Trunks: 70
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 DSL1 Boards with Echo Cancellation: 522 0

(NO: You must logoff & login to effect the permission changes.)
```
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.

<table>
<thead>
<tr>
<th>Extension: 10401</th>
<th>Lock Messages? n</th>
<th>BCC: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type: <strong>H.323</strong></td>
<td>Security Code: <strong>0000</strong></td>
<td>TN: 1</td>
</tr>
<tr>
<td>Port: IP</td>
<td>Coverage Path 1:</td>
<td>COR: 1</td>
</tr>
<tr>
<td>Name: <strong>Virtual #1</strong></td>
<td>Coverage Path 2:</td>
<td>COS: 1</td>
</tr>
<tr>
<td></td>
<td>Hunt-to Station:</td>
<td>Tests? y</td>
</tr>
</tbody>
</table>

**STATION OPTIONS**

- **Time of Day Lock Table:**
- **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.

<table>
<thead>
<tr>
<th>Codec Set: 1</th>
<th>IP CODEC SET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio Codec</td>
<td>Silence Suppression</td>
</tr>
<tr>
<td>1: <strong>G.711MU</strong></td>
<td>n</td>
</tr>
<tr>
<td>2: <strong>G.711A</strong></td>
<td>n</td>
</tr>
<tr>
<td>3:</td>
<td></td>
</tr>
<tr>
<td>4:</td>
<td></td>
</tr>
<tr>
<td>5:</td>
<td></td>
</tr>
<tr>
<td>6:</td>
<td></td>
</tr>
<tr>
<td>7:</td>
<td></td>
</tr>
</tbody>
</table>
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.

Select System Parameters and on the pop-up authentication window, log in with an appropriate User Name and 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](media/image1)

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

![Preferred Media](media/image2)

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

![Disable In-band DTMF](media/image3)

- 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](media/image4)
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.

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.

```
C:\Program Files (x86)\Cyara\CallEngine
```

- CallEngine.exe
- CallEngine.area.config
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.

6.2.2. register-opal.csv
Configure the following for the csv file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserName</td>
<td>cyara</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Identity</td>
<td>cyara@10.1.10.126:5060</td>
</tr>
<tr>
<td>Contact</td>
<td>cyara@10.1.10.123:5060</td>
</tr>
<tr>
<td>Domain</td>
<td>cyara@10.1.10.126:5060</td>
</tr>
<tr>
<td>Realm</td>
<td>cyara</td>
</tr>
<tr>
<td>TTL</td>
<td>300</td>
</tr>
<tr>
<td>XOpalAorListFile</td>
<td>opal-aor.txt</td>
</tr>
</tbody>
</table>

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.

```
323:10401..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.
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.

<table>
<thead>
<tr>
<th>Station Ext or Orig Port</th>
<th>Set Type/ Prod ID/ Release</th>
<th>Station IP Address/ Skt Gatekeeper IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10401</td>
<td>H.323</td>
<td>10.1.10.126</td>
</tr>
<tr>
<td>10402</td>
<td>H.323</td>
<td>10.1.10.126</td>
</tr>
<tr>
<td>10403</td>
<td>H.323</td>
<td>10.1.10.126</td>
</tr>
<tr>
<td>10404</td>
<td>H.323</td>
<td>10.1.10.126</td>
</tr>
<tr>
<td>10405</td>
<td>H.323</td>
<td>10.1.10.126</td>
</tr>
<tr>
<td>10406</td>
<td>H.323</td>
<td>10.1.10.126</td>
</tr>
<tr>
<td>10407</td>
<td>H.323</td>
<td>10.1.10.126</td>
</tr>
</tbody>
</table>

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.

![Cyara Endpoint Server screenshot](image)

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.
[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.