Abstract

These Application Notes describe the procedures for configuring Coordinated Systems Inc. Virtual Observer to monitor and record calls placed to and from stations, and to Vector Directory Numbers (VDN) on Avaya Communication Manager.

Coordinated Systems Inc. Virtual Observer is a monitoring solution for the contact center industry. Functionalities of CSI Virtual Observer include audio recording, screen recording, agent evaluation, e-Learning, data analytics and speech analytics and more. In the configuration discussed in these Application Notes, Coordinated Systems Inc. Virtual Observer employs Device, Media and Call Control Application Programming Interface (API) virtual stations as recording ports.

During compliance testing, Coordinated Systems Inc. Virtual Observer successfully recorded calls placed to and from stations, as well as calls placed to a VDN and then queued to an agent hunt/skill group.

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 a compliance-tested configuration comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) and Coordinated Systems Inc. (CSI) Virtual Observer. The Virtual Observer monitors, records, stores, and plays back phone calls for verification. The Virtual Observer uses the Device, Media and Call Control (DMCC) API (also known as CMAPI) with an Avaya AES server to monitor stations, and/or VDNs, i.e. to obtain recording triggers and call information. Coordinated Systems Inc. (CSI) Virtual Observer also uses DMCC with the Avaya AES server to register DMCC softphones that Virtual Observer uses as recording ports.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide a T1/ISDN-PRI trunk between two Avaya Communication Manager systems.

Figure 1: Sample Test Configuration for the CSI Virtual Observer Solution
2. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Software/Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya S8700 Server</td>
<td>Avaya Communication Manager 5.0 (R015x.00.0.825.4)</td>
</tr>
<tr>
<td>Avaya G650 Media Gateway</td>
<td>-</td>
</tr>
<tr>
<td>TN2312BP IP Server Interface</td>
<td>HW11 FW030</td>
</tr>
<tr>
<td>TN799DP C-LAN Interface</td>
<td>HW20 FW017</td>
</tr>
<tr>
<td>TN2302AP IP Media Processor</td>
<td>HW01 FW018</td>
</tr>
<tr>
<td>Avaya S8300 Server with Avaya G700 Media</td>
<td>Avaya Communication Manager 5.0 (R015x.00.0.825.4)</td>
</tr>
<tr>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td>Avaya Application Enablement Services Server</td>
<td>R4.1.31.2</td>
</tr>
<tr>
<td>Avaya 4600 Series IP Telephones</td>
<td>2.8</td>
</tr>
<tr>
<td>4620SW (H.323)</td>
<td></td>
</tr>
<tr>
<td>4625SW (H.323)</td>
<td></td>
</tr>
<tr>
<td>Avaya 9600 Series IP Telephones</td>
<td></td>
</tr>
<tr>
<td>9630 (H.323)</td>
<td>1.5</td>
</tr>
<tr>
<td>9650 (H.323)</td>
<td>1.5</td>
</tr>
<tr>
<td>Avaya 6408D+ Digital Telephone</td>
<td>-</td>
</tr>
<tr>
<td>Analog Telephones</td>
<td>-</td>
</tr>
<tr>
<td>Coordinated Systems Inc. Virtual Observer on</td>
<td>4.0</td>
</tr>
<tr>
<td>Windows Microsoft 2003 Server w/ SP1 or</td>
<td></td>
</tr>
<tr>
<td>higher.</td>
<td></td>
</tr>
</tbody>
</table>

3. Configure Avaya Communication Manager

This section provides the procedures for configuring an AES link, hunt/skill groups, vectors, Vector Directory Numbers (VDN), agents, agent login/logoff codes, and recording ports on Avaya Communication Manager. All the configuration changes in Avaya 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.

3.1. AES Link between Avaya Communication Manager and Avaya Application Enablement Services

The AES server communicates with Avaya Communication Manager over an AES link. The following steps demonstrate the configuration of the Avaya Communication Manager side of the AES link. See Section 4 for the details of configuring the AES side of the AES link.
Enter the `change node-names ip` command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoint (Avaya IP Telephones and IP Softphones, and AES Device, Media and Call Control API stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLAN</td>
<td>192.45.80.87</td>
</tr>
<tr>
<td>CLAN-AES</td>
<td>192.45.80.89</td>
</tr>
<tr>
<td>MEDPRO</td>
<td>192.45.80.88</td>
</tr>
<tr>
<td>MEDPRO2</td>
<td>192.45.80.161</td>
</tr>
<tr>
<td>S8300G700</td>
<td>192.45.87.11</td>
</tr>
<tr>
<td>default</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>procr</td>
<td>192.45.80.214</td>
</tr>
</tbody>
</table>

Enter the `change ip-services` command. On **Page 1**, configure the Service Type field to AESVCS and the Enabled field to y. The Local Node field should be pointed to the CLAN-AES board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was utilized for the Local Port field.

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Enabled</th>
<th>Local Node</th>
<th>Local Port</th>
<th>Remote Node</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>AESVCS</td>
<td>y</td>
<td>CLAN-AES</td>
<td>8765</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command `uname –a`. Enter an alphanumeric password for the Password field. Set the Enabled field to y. The same password will be configured on the AES server in Section 4.1.

<table>
<thead>
<tr>
<th>Server ID</th>
<th>AE Services Server</th>
<th>Password</th>
<th>Enabled</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>server1</td>
<td>xxxxxxxxxxxxxxxxxxx</td>
<td>y</td>
<td>idle</td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3.2. Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the `display system-parameters customer-options` command. On Page 6, verify that the ACD, Vectoring (Basic), and Expert Agent Selection (EAS) fields are set to `y`. If not, contact an authorized Avaya account representative to obtain these licenses.

```plaintext
<table>
<thead>
<tr>
<th>ACD? y</th>
<th>Reason Codes? n</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCMS (Basic)? y</td>
<td>Service Level Maximizer? n</td>
</tr>
<tr>
<td>BCMS/VuStats Service Level? n</td>
<td>Service Observing (Basic)? y</td>
</tr>
<tr>
<td>BSR Local Treatment for IP &amp; ISDN? n</td>
<td>Service Observing (Remote/By FAC)? y</td>
</tr>
<tr>
<td>Business Advocate? n</td>
<td>Service Observing (VDNs)? n</td>
</tr>
<tr>
<td>Call Work Codes? n</td>
<td>Timed ACW? N</td>
</tr>
<tr>
<td>DTMF Feedback Signals For VRU? n</td>
<td>Vectoring (Basic)? y</td>
</tr>
<tr>
<td>Dynamic Advocate? n</td>
<td>Vectoring (Prompting)? n</td>
</tr>
<tr>
<td><strong>Expert Agent Selection (EAS)? y</strong></td>
<td>Vectoring (G3V4 Enhanced)? n</td>
</tr>
<tr>
<td>EAS-PHD? n</td>
<td>Vectoring (3.0 Enhanced)? n</td>
</tr>
<tr>
<td>Forced ACD Calls? n</td>
<td>Vectoring (ANI/II-Digits Routing)? n</td>
</tr>
<tr>
<td>Least Occupied Agent? n</td>
<td>Vectoring (G3V4 Advanced Routing)? n</td>
</tr>
<tr>
<td>Lookahead Interflow (LAI)? n</td>
<td>Vectoring (CINFO)? n</td>
</tr>
<tr>
<td>Multiple Call Handling (On Request)? n</td>
<td>Vectoring (Best Service Routing)? n</td>
</tr>
<tr>
<td>Multiple Call Handling (Forced)? n</td>
<td>Vectoring (Holidays)? n</td>
</tr>
<tr>
<td>PASTE (Display PBX Data on Phone)? n</td>
<td>Vectoring (Variables)? n</td>
</tr>
</tbody>
</table>

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

Enter the `add hunt-group n` command, where `n` is an unused hunt group number. On Page 1 of the HUNT GROUP form, assign a descriptive Group Name and Group Extension that is valid in the provisioned dial plan. Set the ACD, Queue, and Vector fields to `y`. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.
On **Page 2**, set the Skill field to `y`, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

```plaintext
add hunt-group 1

HUNT GROUP

Skill? y
AAS? n
Measured: internal
Supervisor Extension:

Controlling Adjunct: none

VuStats Objective:

Redirect on No Answer (rings):
  Redirect to VDN:
Forced Entry of Stroke Counts or Call Work Codes? n
```

Enter the `add agent-loginID p` command, where `p` is a valid extension in the provisioned dial plan. On **Page 1** of the AGENT LOGINID form, enter a descriptive Name and Password.

```plaintext
add agent-loginID 50021

AGENT LOGINID

Login ID: 50021
  Name: Agent-1
TN: 1
COR: 1
Coverage Path:
Security Code:

AAS? n
AUDIX? n
LWC Reception: spe
LWC Log External Calls? n
AUDIX Name for Messaging:
LoginID for ISDN/SIP Display? n
Password:
Password (enter again):

Auto Answer: station
MIA Across Skills: system
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time: :

WARNING: Agent must log in again before changes take effect
```
On Page 2, set the Skill Number (SN) to the hunt group number previously created. The Skill Level (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.

```
add agent-loginID 50021
```

Enter the change vector q command, where q is an unused vector number. Enter a descriptive Name, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

```
change vector 1
```

Enter the add vdn r command, where r is an extension that is valid in the provisioned dial plan. Specify a descriptive Name for the VDN and the Vector Number configured in the previous step. In the example below, incoming calls to the extension 50000 will be routed to testVDN50000, which in turn will invoke the actions specified in vector 1.

```
add vdn 50000
```

Enter the **add abbreviated-dialing group g** command, where *g* is the number of an available abbreviated dialing group. In the DIAL CODE list, enter the Feature Access Codes, created previously, for ACD Login and Logout.

### 3.3. Recording Stations

The recording ports in this configuration are DMCC stations that essentially appear as IP Softphones, to Avaya Communication Manager. Each DMCC station requires an IP_API_A license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for AES DMCC stations. Enter the **display system-parameters customer-options** command and verify that there are sufficient IP_API_A licenses. If not, contact an authorized Avaya account representative to obtain these licenses.
Enter the `add station s` command, where `s` is an extension that is valid in the provisioned dial plan. On Page 1 of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, and specify the Security Code. During the compliance test, the set type 4620 was used for the recording stations. Repeat this as necessary, with the same Security Code, to configure additional DMCC stations. For the compliance test, stations from 23001 to 23046 were created for the purpose of recording. When multiple stations are involved, consider using the `duplicate station` command.

```
add station 23001
```

**STATION**

<table>
<thead>
<tr>
<th>Extension: 23001</th>
<th>Lock Messages? n</th>
<th>BCC: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type: 4620</strong></td>
<td>**Security Code: ***</td>
<td><strong>TN: 1</strong></td>
</tr>
<tr>
<td>Port: ip</td>
<td><strong>Coverage Path 1:</strong></td>
<td><strong>COR: 1</strong></td>
</tr>
<tr>
<td><strong>Name: DMCC -1</strong></td>
<td><strong>Coverage Path 2:</strong></td>
<td><strong>COS: 1</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Hunt-to Station:</strong></td>
<td></td>
</tr>
</tbody>
</table>

**STATION OPTIONS**

- Loss Group: 19
- Personalized Ringing Pattern: 1
- Message Lamp Ext: 23001
- Speakerphone: 2-way
- Mute Button Enabled? y
- Display Language: english
- Expansion Module? n
- Survivable GK Node Name:
- Survivable COR: internal
- Survivable Trunk Dest? y
- Media Complex Ext: 
- IP SoftPhone? y
- IP Video Softphone? n

3.4. Recorded Stations

Enter the `add station s` command, where `s` is an extension valid in the provisioned dial plan. On Page 1 of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, and specify the Security Code. For the compliance test, recorded stations from 22001 to 22009 were created.

```
add station 22001
```

**STATION**

<table>
<thead>
<tr>
<th>Extension: 22001</th>
<th>Lock Messages? n</th>
<th>BCC: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type: 4621</strong></td>
<td>**Security Code: ***</td>
<td><strong>TN: 1</strong></td>
</tr>
<tr>
<td>Port: S00142</td>
<td><strong>Coverage Path 1:</strong></td>
<td><strong>COR: 1</strong></td>
</tr>
<tr>
<td><strong>Name: 72001</strong></td>
<td><strong>Coverage Path 2:</strong></td>
<td><strong>COS: 1</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Hunt-to Station:</strong></td>
<td></td>
</tr>
</tbody>
</table>

**STATION OPTIONS**

- Loss Group: 19
- Personalized Ringing Pattern: 1
- Message Lamp Ext: 22001
- Speakerphone: 2-way
- Mute Button Enabled? y
- Display Language: english
- Expansion Module? n
- Survivable GK Node Name:
- Survivable COR: internal
- Survivable Trunk Dest? y
- Media Complex Ext: 
- IP SoftPhone? n
- Customizable Labels? y
On Page 3 of the STATION form, for ABBREVIATED DIALING List 2, enter the abbreviated dialing group configured in Section 3.2. Configure the following BUTTON ASSIGNMENTS in addition to the call-appr (call appearance) buttons:

- auto-in
- aux-work
- abrv-dial – for Login
- abrv-dial – for Logout.

4. Configure Avaya Application Enablement Services

The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, and a CMAPI port.
4.1. Configure Switch Connection

Launch a web browser, enter https://<IP address of AES server>:8443/MVAP in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

Select the CTI OAM Administration link from the left pane of the screen.
Click on Administration → Switch Connections in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on Add Connection.

The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in Section 3.1. Default values may be used in the remaining fields. Click on Apply.
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.

Enter the CLAN-AES IP address which was configured for AES connectivity in Section 3.1 and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.
4.2. Configure the CTI Users

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter https://<IP address of AES server>:8443/MVAP in the URL, and log in with the appropriate credentials to access the relevant administration pages.

The Welcome to OAM page is displayed next. Select User Management from the left pane.
From the Welcome to User Management page, navigate to the User Management ➔ Add User page to add a CTI user.

On the Add User page, provide the following information:

- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the CSI Server Configuration page in Section 5.

Select Yes using the drop down menu on the CT User field. This enables the user as a CTI user. Click the Apply button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.
Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Home** ➔ **Administration** ➔ **Security Database** ➔ **CTI Users** ➔ **List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.
Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.
Navigate to the CTI OAM Home → Administration → Network Configuration → Ports page to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to Enabled. Click the Apply Changes button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.
5. Configure Coordinated Systems Inc. Virtual Observer

Coordinated Systems Inc. installs, configures, and customizes the Virtual Observer application for their end customers. This section only describes the interface configuration for the Virtual Observer application to communicate with Avaya AES and Avaya Communication Manager. Refer to [3] for configuring the CSI Virtual Observer application.

Open the Virtual Observer Application Launcher by clicking the Virtual Observer – Application Launcher icon on the desktop of the server. Select the **Administration → Avaya DMCC Configuration**.

![Virtual Observer - Application Launcher](image)

From the Virtual Observer – Avaya DMCC Configuration page, provide the following information, to connect to Avaya AES:

- **AES Address** – Provide Avaya AES Client Connectivity IP address. The IP address can be obtained by navigating to the **Administration → Network Configuration → Local IP** page from the CTI OAM Home page in Avaya AES.
- **CLAN Address** - The CLAN IP address, which was utilized for registering AES DMCC stations. During the compliance test, the CLAN IP address was **192.45.80.87**.
- **Switch Link Name** – Provide the name of the Switch Connection created in **Section 4.1**.
- **Username** – Provide the User Id, created in **Section 4.2**.
- **Password** – Provide the User Password, created in **Section 4.2**.
- Provide the monitored station extensions, and click the **Add** button.
- Provide the recording station extensions, and click the **Add** button.

After the completion, save the file by click on the **disk icon**.
6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability, and performance testing. The feature testing evaluated the ability of the CSI Virtual Observer to monitor and record calls placed to and from stations and to a VDN. The serviceability testing introduced failure scenarios to see if the CSI Virtual Observer can resume recording after failure recovery. The performance testing stressed the CSI Virtual Observer by continuously placing calls over extended periods of time.
6.1. General Test Approach

The general approach was to place various types of calls to and from stations, agents, and to a VDN, monitor and record them using CSI Virtual Observer, and verify the recordings. For feature testing, the types of calls included internal calls, inbound and outbound trunk calls, transferred calls, bridged calls, and conferenced calls. Performance tests verified that the CSI Virtual Observer could record calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES.

7.1. Verify Avaya Communication Manager

Verify the status of the administered AES link by using the `status aesvcs link` command. The following shows a sample AE SERVICES LINK STATUS screen.

```
status aesvcs link

AE SERVICES LINK STATUS
Srvc/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
   Link   Server                           Port                    Sent    Rcvd
01/01  server1         192.45.80.102  36538   CLAN-AES        17      18
```

7.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services are ONLINE, by selecting Status and Control → Services Summary from the left pane. The following shows a sample Service Summary screen.

![Service Summary Screen](image-url)
7.3. Verify Recordings from CSI Virtual Observer

From the CSI Virtual Observer Application Launcher page, navigate to Features → Event Log → View → Record Server Status to go to the Virtual Observer – Record Server Status page to view the recording state. The following shows a sample Virtual Observer - Record Server Status page, which shows the channel is in a state of “Recording” and will stay that way until the monitored extension ends its current call.

![Virtual Observer - Record Server Status](image)

8. Support

Technical support for CSI Virtual Observer can be obtained by contacting Coordinated Systems Inc. via the support link at [http://www.csiworld.com/technical-support/index.php](http://www.csiworld.com/technical-support/index.php) or by calling the support telephone number at (860) 289-2151.

9. Conclusion

These Application Notes illustrate the procedures for configuring the Coordinated Systems Inc. Virtual Observer call recording solution to monitor and record calls placed to and from stations and agents, and to a VDN on an Avaya Communication Manager system. In the configuration described in these Application Notes, Coordinated Systems Inc. Virtual Observer employs DMCC Application Programming Interface virtual stations as recording ports. During compliance testing, Coordinated Systems Inc. Virtual Observer successfully monitored events and recorded calls placed to and from stations and agents, as well as calls placed to a VDN and then queued to an agent hunt/skill group. Coordinated Systems Inc. Virtual Observer was also able to record calls under continuous call volumes over extended periods of time.
10. Additional References

This section references the Avaya and Coordinated Systems Inc. documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com.


The following documentation was provided by Coordinated Systems Inc.
