Avaya Solution & Interoperability Test Lab

Application Notes for InGenius Connector Enterprise 6.5 for ServiceNow with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate InGenius Connector Enterprise 6.5 for ServiceNow with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. InGenius Connector Enterprise is a CRM-VoIP integration tool that sits between the customer’s phone system and a CRM application, such as ServiceNow.

In the compliance testing, InGenius Connector Enterprise used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor agents on Avaya Aura® Communication Manager, to provide screen pop, call control, and click-to-dial features from the agent desktops connected to ServiceNow.

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 to integrate InGenius Connector Enterprise (ICE) 6.5 for ServiceNow with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. InGenius Connector Enterprise is a CRM-VoIP integration tool that sits between the customer’s phone system and a CRM application, such as ServiceNow.

In the compliance testing, ICE used the Device, Media, and Call Control (DMCC) XML interface from Application Enablement Services to monitor agents on Communication Manager, to provide screen pop, call control, and click-to-dial features from the agent desktops. The agent desktop uses a web browser to connect to the ICE server and to the ICE Update Set running on ServiceNow.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. Upon an agent log in, ICE used DMCC to query device information and agent state, logged the agent into the ACD on Communication Manager, if needed, and requested device monitoring.

During the feature testing, incoming ACD calls were placed to available agents that have web browser connections to ServiceNow. All necessary call actions were initiated from the agent desktops and/or telephones. The click-to-dial calls were initiated by clicking on the contact phone number displayed on the agent desktops.

The serviceability testing focused on verifying that the ICE server recovered after restoring network connectivity and the CTI link to Application Enablement Services.

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 Application Enablement Services and ICE did not include use of any specific encryption features as requested by InGenius.

2.1. Interoperability Compliance Testing
The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on ICE:

- Use of DMCC logical device services to set agent states, including log in, log out, and work mode changes with support for reason codes and pending aux work.
- Use of DMCC snapshot services to obtain information on agent stations and existing calls.
- Use of DMCC monitoring services to monitor agent stations and existing calls.
- Use of DMCC call control services to support call control and click-to-dial features.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, conference, transfer, long duration, send DTMF, click-to-dial from contact phone number, pending aux work, and reason codes.

The serviceability testing focused on verifying the ability of ICE to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to ICE.

2.2. Test Results
All test cases passed with the following observation:

- By design, the agent desktop does not support initiation of unattended conference.

2.3. Support
Technical support on ICE can be obtained through the following:

- **Phone:** +1 (613) 591-9002 x4000
- **Email:** ingenius_support@uplandsoftware.com
- **Web:** http://uplandsoftware.com/ingenius/contact-us
3. Reference Configuration

Figure 1 illustrates the configuration used for the compliance testing. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of call center devices are not the focus of these Application Notes and will not be described.

In the compliance testing, ICE monitored the agent stations shown in the table below.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDNs</td>
<td>77550</td>
</tr>
<tr>
<td>Skill Group</td>
<td>77500</td>
</tr>
<tr>
<td>Agent Stations</td>
<td>78030, 77301</td>
</tr>
<tr>
<td>Agent IDs</td>
<td>76301, 76302</td>
</tr>
</tbody>
</table>

Figure 1: InGenius Connector Enterprise for ServiceNow with Avaya Aura® Suite
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>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>8.1.2.0.0-FP2</td>
</tr>
<tr>
<td>Avaya G450 Media Gateway</td>
<td>FW 41.24.0</td>
</tr>
<tr>
<td>Avaya Aura® Media Server</td>
<td>v.8.0.2.93</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services</td>
<td>8.1.2.1.1.6-0</td>
</tr>
<tr>
<td>Avaya Aura® System Manager</td>
<td>8.1.2.0 Build No. – 8.1.0.0.733078</td>
</tr>
<tr>
<td></td>
<td>Software Update Revision No: 8.1.2.0.0611167</td>
</tr>
<tr>
<td></td>
<td>Feature Pack 2</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>8.1.2.0.812039</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise</td>
<td>8.1.0.014-18490</td>
</tr>
<tr>
<td>Avaya 96x1 Series Deskphones</td>
<td>6.8304 (H.323)</td>
</tr>
<tr>
<td></td>
<td>7.1.9.0.8 (SIP)</td>
</tr>
<tr>
<td>Avaya J100 Series Deskphones</td>
<td>4.0.5.0.10 (SIP)</td>
</tr>
<tr>
<td>InGenius Connector Enterprise for ServiceNow on Windows Server 2016</td>
<td>6.5.1.36404</td>
</tr>
<tr>
<td>InGenius Update Set and OpenFrame Configuration on ServiceNow</td>
<td>6.5.1.36404</td>
</tr>
</tbody>
</table>
5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify license
- Administer system parameters features
- Administer CTI link
- Obtain reason codes

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license allows the features illustrated in these Application Notes. Use the `display system-parameters customer-options` command to verify that the Computer Telephony Adjunct Links option is enabled on Page 4. If this option is not enabled, then contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options

Optional Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviated Dialing Enhanced List?</td>
<td>y</td>
</tr>
<tr>
<td>Access Security Gateway (ASG)?</td>
<td>n</td>
</tr>
<tr>
<td>Analog Trunk Incoming Call ID?</td>
<td>y</td>
</tr>
<tr>
<td>A/D Grp/Sys List Dialing Start at 01?</td>
<td>y</td>
</tr>
<tr>
<td>Answer Supervision by Call Classifier?</td>
<td>y</td>
</tr>
<tr>
<td>ARS?</td>
<td>y</td>
</tr>
<tr>
<td>ARS/AAR Partitioning?</td>
<td>y</td>
</tr>
<tr>
<td>ARS/AAR Dialing without FAC?</td>
<td>n</td>
</tr>
<tr>
<td>ASAI Link Core Capabilities?</td>
<td>y</td>
</tr>
<tr>
<td>ASAI Link Plus Capabilities?</td>
<td>y</td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) PNC?</td>
<td>n</td>
</tr>
<tr>
<td>Async. Transfer Mode (ATM) Trunking?</td>
<td>n</td>
</tr>
<tr>
<td>ATM WAN Spare Processor?</td>
<td>n</td>
</tr>
<tr>
<td>ATMS?</td>
<td>y</td>
</tr>
<tr>
<td>Attendant Vectoring?</td>
<td>y</td>
</tr>
<tr>
<td>Audible Message Waiting?</td>
<td>y</td>
</tr>
<tr>
<td>Authorization Codes?</td>
<td>y</td>
</tr>
<tr>
<td>CAS Branch?</td>
<td>n</td>
</tr>
<tr>
<td>CAS Main?</td>
<td>n</td>
</tr>
<tr>
<td>Change COR by FAC?</td>
<td>n</td>
</tr>
<tr>
<td>Cvg Of Calls Redirected Off-net?</td>
<td>y</td>
</tr>
<tr>
<td>DCS (Basic)?</td>
<td>y</td>
</tr>
<tr>
<td>DCS Call Coverage?</td>
<td>y</td>
</tr>
<tr>
<td>DCS with Rerouting?</td>
<td>y</td>
</tr>
<tr>
<td>Digital Loss Plan Modification?</td>
<td>y</td>
</tr>
<tr>
<td>DS1 MSP?</td>
<td>y</td>
</tr>
<tr>
<td>DS1 Echo Cancellation?</td>
<td>y</td>
</tr>
</tbody>
</table>

(Note: You must logoff & login to effect the permission changes.)
```
5.2. Administer System Parameters Features

Use the `change system-parameters features` command to enable Create Universal Call ID (UCID), which is located on Page 5. For UCID Network Node ID, enter an available node ID.

```
change system-parameters features
FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
  Switch Name:
  Emergency Extension Forwarding (min): 10
  Enable Inter-Gateway Alternate Routing? n
  Enable Dial Plan Transparency in Survivable Mode? n
  COR to Use for DPT: station
  EC500 Routing in Survivable Mode: dpt-then-ec500

MALICIOUS CALL TRACE PARAMETERS
  Apply MCT Warning Tone? n
  MCT Voice Recorder Trunk Group:
  Delay Sending RELEASE (seconds): 0

SEND ALL CALLS OPTIONS
  Send All Calls Applies to: station
  Auto Inspect on Send All Calls? n
  Preserve previous AUX Work button states after deactivation? n

UNIVERSAL CALL ID
  Create Universal Call ID (UCID)? y
  UCID Network Node ID: 27
```

Navigate to Page 13 and enable Send UCID to ASAI. This parameter allows for the universal call ID to be sent to ICE.

```
change system-parameters features
FEATURE-RELATED SYSTEM PARAMETERS

CALL CENTER MISCELLANEOUS
  Callr-info Display Timer (sec): 10
  Allow Ringer-off with Auto-Answer? n
  Clear Callr-info: next-call
  Reporting for PC Non-Predictive Calls? n

  Agent/Caller Disconnect Tones? n
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UUI During Conference/Transfer? n
  Call Classification After Answer Supervision? n
  Send UCID to ASAI? y
  For ASAI Send DTMF Tone to Call Originator? y
  Send Connect Event to ASAI For Announcement Answer? n
  Prefer H.323 Over SIP For Dual-Reg Station 3PCC Make Call? n
```

Navigate to Page 13 and enable Send UCID to ASAI. This parameter allows for the universal call ID to be sent to ICE.
5.3. Administer CTI Link

Add a CTI link using the `add cti-link` command. Enter an available extension number in the Extension field. Note that the CTI link number and extension number may vary. Enter ADJ-IP in the Type field, and a descriptive name in the Name field. Default values may be used in the remaining fields.

```plaintext
add cti-link 1
CTI Link: 1
Extension: 77700
Type: ADJ-IP
Name: AES TSAPI Link
```

5.4. Obtain Reason Codes

For customers that use reason codes, enter the `change reason-code-names` command to display the configured reason codes. Make a note of the reason codes, which will be used later to configure ICE.

```plaintext
change reason-code-names
Reason Code 1: Lunch /n Finished Shift
Reason Code 2: Coffee /n
Reason Code 3: /n
Reason Code 4: /n
Reason Code 5: /n
Reason Code 6: /n
Reason Code 7: /n
Reason Code 8: /n
Reason Code 9: /n
Default Reason Code:
```
6. **Configure Avaya Aura® Application Enablement Services**

This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer InGenius user
- Administer security database
- Administer ports
- Restart services

### 6.1. Launch OAM Interface

Access the OAM web-based interface by using the URL “https://<ip-address>” in an Internet browser window, where `<ip-address>` is the IP address of the Application Enablement Services server. The login screen is displayed. Log in using the appropriate credentials.
The **Welcome to OAM** screen is displayed next.

![Welcome to OAM Screen](AVAYA.png)

6.2. **Verify License**

Select **Licensing → WebLM Server Access** in the left pane to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials.

![WebLM Server Access](AVAYA.png)

**NOTE:** Please disable your pop-up blocker if you are having difficulty with opening this page.
The WebLM screen below is displayed. Select **Licensed products → APPL_ENAB → Application_Enablement** in the left pane to display the **Application Enablement (CTI)** screen in the right pane.

Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below. Note that the TSAPI license is used for device monitoring and call control via DMCC, and that no specific DMCC license is required for the integration with ICE.
6.3. Administer TSAPI Link

Select AE Services \(\rightarrow\) TSAPI \(\rightarrow\) TSAPI Links from the left pane of the Management Console to administer a TSAPI link. The TSAPI Links screen is displayed, as shown below. Click Add Link.

The Add TSAPI Links screen is displayed next. The Link field is only local to the Application Enablement Services server and may be set to any available number. For Switch Connection, select the relevant switch connection from the drop-down list. In this case, the existing switch connection `devcon` is selected. For Switch CTI Link Number, select the CTI link number from Section 5.3. Retain the default values in the remaining fields.
6.4. Administer InGenius User

Select User Management → User Admin → Add User from the left pane to display the Add User screen in the right pane.

Enter desired values for User Id, Common Name, Surname, User Password, and Confirm Password. For CT User, select Yes from the drop-down list. Retain the default value in the remaining fields.
6.5. Administer Security Database

Select Security → Security Database → Control from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Ensure that both parameters are unchecked as shown below.

In the event that the security database is being used by the customer with parameters already enabled, then follow reference [2] to configure access privileges for the InGenius user from Section 6.4.
6.6. Administer Ports

Select Networking → Ports from the left pane to display the Ports screen in the right pane.

In the DMCC Server Ports section, select the radio button for Unencrypted Port under the Enabled column as shown below. Retain the default values in the remaining fields.
6.7. Restart Services
Select **Maintenance → Service Controller** from the left pane to display the **Service Controller** screen in the right pane. Check **DMCC Service** and **TSAPI Service** and click **Restart Service**.
7. Configure Avaya Aura® Session Manager

This section provides the procedure for configuring a SIP agent on Session Manager, which is performed via the web interface of System Manager. The procedure includes the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

Access the System Manager web interface by using the URL “https://<ip-address>” in an web browser window, where <ip-address> is the System Manager IP address. Log in using the appropriate credentials.
7.2. Administer Users

In the subsequent screen (not shown), select Users → User Management. Select User Management → Manage Users from the left pane to display the User Management screen below. Select the entry associated with the first SIP agent station from Section 3, in this case 78030, and click Edit.
The **User Profile** Edit-Add screen is displayed. Select the **Communication Profile** tab to display the screen below.

Navigate to the **CM Endpoint Profile** sub-section and click **Endpoint Editor**.
The **Edit Endpoint** screen is displayed next. For **Type of 3PCC Enabled**, select *Avaya* from the drop-down list as shown below. Retain the default values in the remaining fields.
8. Configure InGenius Connector Enterprise

This section provides the procedures for configuring ICE. The procedures include the following areas:

- Launch InGenius Server Configuration
- Administer dialing and number formatting
- Administer telephony
- Start service

This section assumes the InGenius Connector Enterprise package has been imported and published, with the appropriate Security Role created, and users created and assigned to the Security Role.

8.1. Launch InGenius Server Configuration

Launch the InGenius Server Configuration application. The InGenius Telephony Integration Server Configuration Tool screen is displayed.

![InGenius Telephony Integration Server Configuration Tool](image_url)
8.2. Administer Dialing and Number Formatting

Navigate to **Configuration → Dialing and Number Formatting** followed by the **Zones** tab in the right pane. Select the default entry, and click the **Edit translation** icon shown below.

The **Zone Configuration** screen is displayed next. For **Country**, **Area Code**, and **Internal numbers**, select and enter values to match the network configuration. Retain the default values in the remaining fields.

Select the default entry in the **Trunks** sub-section, and click on the **Edit Trunk** icon shown below.
The **Trunk** screen is displayed. Update trunk parameter values to match the network configuration. The screenshot below shows the values used in the compliance testing.
8.3. Administer Telephony

The InGenius Telephony Integration Server Configuration Tool screen is displayed again. Select Configuration → Telephony from the top menu, followed by the Primary AES tab in the right pane to display the screen below.

Enter the following values for the specified fields, and retain the default values in the remaining fields.

- **Address:** The IP address of Application Enablement Services.
- **Username:** The InGenius user credentials from Section 6.4.
- **Password:** The InGenius user credentials from Section 6.4.
- **Connection manager:** The relevant switch connection name from Section 6.3.
Select the Agent Setup tab in the right pane to display the screen below. Update parameters in the Agent and Work Modes sub-sections to the proper settings. The screenshot below shows the values used in the compliance testing.

For customers that use reason codes, check Enable reason codes in the Reason Codes sub-section and create reason code entries to match Section 5.4. In the compliance testing, one reason code was created under the Logout tab.

Two reason codes were created under the Not Ready tab.
8.4. Start Service
Select Status from the top menu to display the screen below, and click Start Service.

The screen is updated, as shown below.
9. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and ICE.

9.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the administered CTI link by using the `status aescvcs cti-link` command. Verify that the Service State is *established* for the CTI link number administered in Section 5.3, as shown below.

```
status aescvcs cti-link
AE SERVICES CTI LINK STATUS
CTI  Version  Mnt  AE Services       Service       Msgs     Msgs
     Link     Busy  Server           State         Sent     Rcvd
1     10       no    devcon-aes       established   15       15
```

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the DMCC service by selecting *Status → Status and Control → DMCC Service Summary* from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed. Verify the User column shows an active session with the InGenius user name from Section 6.4.
Verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is *Talking* for the TSAPI link administered in **Section 6.3**, and that the **Associations** column reflects the number of agents from **Section 3** that are currently logged into ICE and connected to the agent stations on Communication Manager.
9.3. Verify InGenius Connector Enterprise
From an agent PC, launch an Internet browser window and enter the URL provided by the end customer for ServiceNow. Log in with the relevant user credentials provided by InGenius.

The screen below is displayed next. Select the phone icon from the top menu to display the InGenius floating screen shown below. Enter the relevant agent station extension from Section 3, and click Connect.
The InGenius screen is updated, as shown below. Click on the Log in drop-down to display additional parameters. For Agent ID and Password, enter the relevant credentials from Section 3. For Work Mode, select the desired work mode, in this case “Auto-In”. Click Log in.
Verify that the **InGenius** screen is updated, showing the agent in the **Ready** state.
Make an incoming ACD call. Verify that the InGenius screen for the available agent is updated to reflect **Reserved** and **Inbound Call**, along with proper call information. Also verify that the background window is populated with the uniquely matching contact record associated with the PSTN caller number, as shown below.

Click **Answer** in the InGenius screen.
Verify that the agent is connected to the PSTN caller with two-way talk path, and that the InGenius screen is updated to reflect **Talking** and **Connected**, as shown below.
10. Conclusion

These Application Notes describe the configuration steps required to integrate InGenius Connector Enterprise 6.5 for ServiceNow with Avaya Aura® Communication Manager 8.1 and Avaya Aura® Application Enablement Services 8.1. InGenius Connector Enterprise for ServiceNow was able to change and monitor agent states, place and answer calls, and perform call transfers and conferences. All feature and serviceability test cases were completed with observations noted in Section 2.2.

11. Additional References

This section references the product documentation relevant to these Application Notes.


