



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.

Device Type	Extension
VDNs	77550
Skill Group	77500
Agent Stations	78030, 77301
Agent IDs	76301, 76302

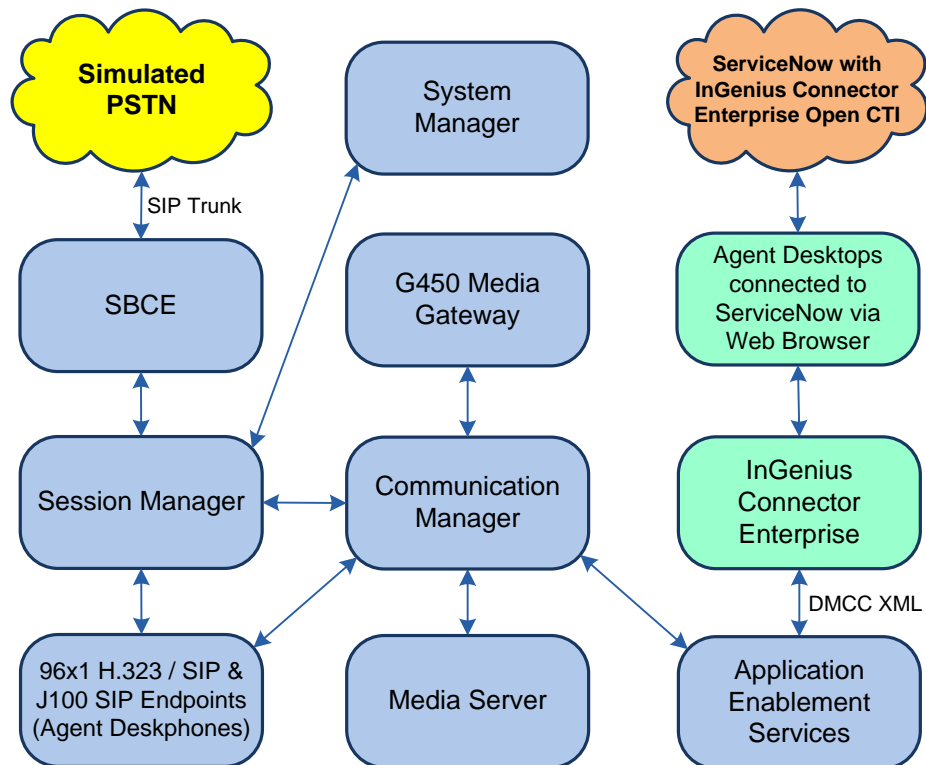


Figure 1: InGenius Connector Enterprise for ServiceNow with Avaya Aura® Suite

4. Equipment and Software Validated

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

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

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                                Page 4 of 12
                                OPTIONAL FEATURES

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

(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                                     Page 5 of 19
                                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                                     Page 13 of 19
                                FEATURE-RELATED SYSTEM PARAMETERS

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

                                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 UII 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
```

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.

```
add cti-link 1                                     Page 1 of 3
                                                    CTI LINK
CTI Link: 1
Extension: 77700
Type: ADJ-IP
                                                    COR: 1
Name: AES TSAPI Link
Unicode Name? n
```

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.

```
change reason-code-names                          Page 1 of 1
                                                    REASON CODE NAMES
                                                    Aux Work/      Logout
                                                    Interruptible?
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:
```

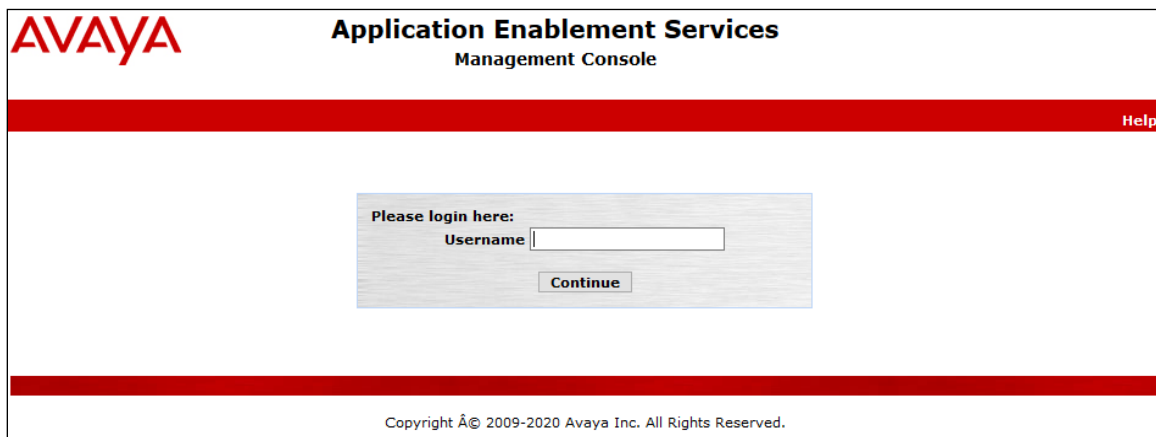

6. Configure Avaya Aura® Application Enablement Services

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 screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" is displayed in bold, with "Management Console" underneath it. A red horizontal bar spans the width of the page, with a "Help" link on the right side. In the center of the page is a login box with the text "Please login here:" followed by a "Username" label and a text input field. Below the input field is a "Continue" button. At the bottom of the page, a red horizontal bar is present, and below it, the copyright notice "Copyright © 2009-2020 Avaya Inc. All Rights Reserved." is displayed.

The **Welcome to OAM** screen is displayed next.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". A red navigation bar at the top contains "Home", "Help", and "Logout" links. On the left, a sidebar lists various services: AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The main content area is titled "Welcome to OAM" and provides an overview of the OAM Web interface, listing administrative domains and their functions. A welcome message is displayed in the top right corner.

Welcome: User cust
Last login: Wed Sep 23 12:35:00 2020 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Fri Oct 02 13:03:35 EDT 2020
HA Status: Not Configured

Home | [Home](#) | [Help](#) | [Logout](#)

AE Services
Communication Manager Interface
High Availability
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Welcome to OAM

The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.
- Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.
- High Availability - Use High Availability to manage AE Services HA.
- Licensing - Use Licensing to manage the license server.
- Maintenance - Use Maintenance to manage the routine maintenance tasks.
- Networking - Use Networking to manage the network interfaces and ports.
- Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.
- Status - Use Status to obtain server status informations.
- User Management - Use User Management to manage AE Services users and AE Services user-related resources.
- Utilities - Use Utilities to carry out basic connectivity tests.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

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.

The screenshot displays the Avaya Application Enablement Services Management Console with the "Licensing" section selected. The top header and navigation bar are identical to the previous screenshot. The sidebar on the left shows "Licensing" expanded, with sub-items: WebLM Server Address, WebLM Server Access (highlighted in blue), and Reserved Licenses. The main content area is titled "Licensing" and provides instructions for setting up and maintaining the WebLM, including a note about disabling pop-up blockers. A welcome message is displayed in the top right corner.

Welcome: User cust
Last login: Fri Oct 2 13:03:04 2020 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Fri Oct 02 13:07:48 EDT 2020
HA Status: Not Configured

Licensing | [Home](#) | [Help](#) | [Logout](#)

AE Services
Communication Manager Interface
High Availability
Licensing
WebLM Server Address
WebLM Server Access
Reserved Licenses
Maintenance
Networking
Security
Status

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

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.

AVAYA Aura® System Manager 8.1

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search 🔍 admin

Home Licenses

WebLM Home

Install license

Licensed products

APPL_ENAB

Application_Enablement

View license capacity

View peak usage

ASBCE

Session_Border_Controller_E_AE

COMMUNICATION_MANAGER

Call_Center

Communication_Manager

MESSAGING

Messaging

MSR

Media_Server

OL

OL

SYSTEM_MANAGER

System_Manager

SessionManager

SessionManager

VDIA

VDIA

VSS

Application Enablement (CTI) - Release: 8 - SID: 10503000 Stand

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: June 28, 2019 12:26:36 PM -04:00

License File Host IDs: V7-94-F5-41-87-5E-01

Licensed Features

13 Items Show All ▾

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	10000
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	16
AES HA LARGE VALUE_AES_HA_LARGE	permanent	1
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	16
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	10000
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	16
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	1
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	16
DLG VALUE_AES_DLG	permanent	16
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10000

6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **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 screenshot shows the AVAYA Application Enablement Services Management Console. The top right corner displays system information: Welcome: User cust, Last login: Fri Oct 2 13:03:04 2020 from 192.168.100.250, Number of prior failed login attempts: 0, HostName/IP: devcon-aes/10.64.102.119, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 8.1.2.1.1.6-0, Server Date and Time: Fri Oct 02 13:12:22 EDT 2020, HA Status: Not Configured. The left navigation pane shows 'AE Services' expanded, with 'TSAPI' selected and 'TSAPI Links' highlighted. The main content area is titled 'TSAPI Links' and contains a table with one link:

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	devcon	1	10	Unencrypted

Below the table are buttons for 'Add Link', 'Edit Link', and 'Delete 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.

The screenshot shows the AVAYA Application Enablement Services Management Console with the 'Add TSAPI Links' screen. The left navigation pane is the same as the previous screenshot. The main content area is titled 'Add TSAPI Links' and contains the following fields:

- Link: 1
- Switch Connection: devcon
- Switch CTI Link Number: 1
- ASAI Link Version: 10
- Security: Unencrypted

At the bottom are buttons for 'Apply Changes' and 'Cancel Changes'.

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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User cust
Last login: Fri Oct 2 13:03:04 2020 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Fri Oct 02 13:16:42 EDT 2020
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▶ Maintenance

▶ Networking

▶ Security

▶ Status

▼ User Management

▶ Service Admin

▼ User Admin

▪ Add User

▪ Change User Password

▪ List All Users

▪ Modify Default Users

▪ Search Users

▶ Utilities

▶ Help

Add User

Fields marked with * can not be empty.

* User Id

* Common Name

* Surname

* User Password

* Confirm Password

Admin Note

Avaya Role

Business Category

Car License

CM Home

Css Home

CT User

Department Number

Display Name

Employee Number

Employee Type

Enterprise Handle

Given Name

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**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo and the text "Application Enablement Services Management Console". On the right, a welcome message for user "cust" is shown, along with login details and system status. A red navigation bar contains "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services", followed by an "Apply Changes" button.

Welcome: User cust
Last login: Fri Oct 2 13:03:04 2020 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Fri Oct 02 13:18:30 EDT 2020
HA Status: Not Configured

Security | Security Database | Control [Home](#) | [Help](#) | [Logout](#)

▶ AE Services
▶ Communication Manager Interface
▶ High Availability
▶ Licensing
▶ Maintenance
▶ Networking
▼ **Security**
 ▶ Account Management
 ▶ Audit
 ▶ Certificate Management
 Enterprise Directory
 ▶ Host AA
 ▶ PAM
 ▼ **Security Database**
 ▪ **Control**


SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services

☐ Enable SDB for DMCC Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services
[Apply Changes](#)

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.



Application Enablement Services

Management Console

Welcome: User cust
 Last login: Fri Oct 2 13:03:04 2020 from 192.168.100.250
 Number of prior failed login attempts: 0
 HostName/IP: devcon-aes/10.64.102.119
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 8.1.2.1.1.6-0
 Server Date and Time: Fri Oct 02 13:19:12 EDT 2020
 HA Status: Not Configured

Networking | Ports
[Home](#) | [Help](#) | [Logout](#)

- [▶ AE Services](#)
- [▶ Communication Manager Interface](#)
- [High Availability](#)
- [▶ Licensing](#)
- [▶ Maintenance](#)
- [▼ Networking](#)
- [AE Service IP \(Local IP\)](#)
- [Network Configure](#)
- [Ports](#)
- [TCP/TLS Settings](#)
- [▶ Security](#)
- [▶ Status](#)
- [▶ User Management](#)
- [▶ Utilities](#)
- [▶ Help](#)

Ports

			Enabled	Disabled
CVLAN Ports				
Unencrypted TCP Port	9999		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/>	<input type="radio"/>
<hr/>				
DLG Port	TCP Port	5678		
<hr/>				
TSAPI Ports			Enabled	Disabled
TSAPI Service Port	450		<input checked="" type="radio"/>	<input type="radio"/>
Local TLINK Ports				
TCP Port Min	1024			
TCP Port Max	1039			
Unencrypted TLINK Ports				
TCP Port Min	<input type="text" value="1050"/>			
TCP Port Max	<input type="text" value="1065"/>			
Encrypted TLINK Ports				
TCP Port Min	<input type="text" value="1066"/>			
TCP Port Max	<input type="text" value="1081"/>			
<hr/>				
DMCC Server Ports			Enabled	Disabled
Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/>	<input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input checked="" type="radio"/>	<input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>		<input type="radio"/>	<input checked="" type="radio"/>

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**.

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Oct 2 13:03:04 2020 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.1.6-0
Server Date and Time: Fri Oct 02 13:20:30 EDT 2020
HA Status: Not Configured

Maintenance | Service ControllerHome | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ High Availability

▶ Licensing

▼ Maintenance

▶ Date Time/NTP Server

▶ Security Database

▶ Service Controller

▶ Server Data

▶ Networking

▶ Security

▶ Status

Service Controller

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input checked="" type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

For status on actual services, please use [Status and Control](#)

StartStopRestart ServiceRestart AE ServerRestart LinuxRestart Web Server

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 a 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 screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar has 'User Management' expanded, with 'Manage Users' selected. The main content area shows a search bar and a table of users.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	78000	78000, SIP	78000@avaya.com	78000
<input type="checkbox"/>	SIP	78001	78001, SIP	78001@avaya.com	78001
<input type="checkbox"/>	SIP	78002	78002, SIP	78002@avaya.com	78002
<input type="checkbox"/>	SIP	78003	78003, SIP	78003@avaya.com	78003

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 screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 8.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are on the right. The left sidebar shows 'User Management' with sub-items: Manage Users (selected), Public Contacts, Shared Addresses, System Presence ACLs, and Communication Profile... The main content area is titled 'User Profile | Add' and has tabs for Identity, Communication Profile (selected), Membership, and Contacts. At the top right of the main area are buttons for 'Commit & Continue', 'Commit', and 'Cancel'. The 'Communication Profile' tab is active, showing a 'Communication Profile Password' section with a dropdown for 'PROFILE SET : Primary' and a 'Communication Address' field. Below this is a 'PROFILES' section with two toggle switches: 'Session Manager Profile' (off) and 'CM Endpoint Profile' (on). The right side of the form contains several fields: '* System:' (dropdown set to 'devcon-cm'), '* Profile Type:' (dropdown set to 'Endpoint'), '* Extension:' (text field with '78030' and a red square icon to its right), '* Template:' (text field with '9641SIPCC_DEFAULT' and a search icon), '* Set Type:' (text field with '9641SIPCC'), 'Security Code:' (text field with placeholder 'Enter Security Code'), and 'Port:' (text field with 'IP' and a search icon).

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.

The screenshot shows the 'New Endpoint' configuration page in the Avaya Aura System Manager 8.1 interface. The page is divided into a left sidebar with navigation options like 'Manage Users', 'Public Contacts', and 'System Presence ACLs'. The main content area is titled 'New Endpoint' and contains several configuration sections. The 'General Options (G)' section is active, showing fields for System, Template, Port, Name, Extension, Set Type, and Security Code. Below this, there are tabs for 'General Options (G)', 'Feature Options (F)', 'Site Data (S)', 'Abbreviated Call Dialing (A)', and 'Enhanced Call Fwd (E)'. The 'General Options (G)' tab is selected, displaying a grid of settings. The 'Type of 3PCC Enabled' dropdown is highlighted with a red box and set to 'Avaya'. Other settings include Class of Restriction (COR), Emergency Location Ext, Tenant Number, SIP Trunk, Coverage Path 1, Lock Message, Multibyte Language, Class Of Service (COS), Message Lamp Ext, Coverage Path 2, Localized Display Name, and Enable Reachability for Station Domain Control.

Field	Value
System	devcon-cm
Extension	78030
Template	9641SIPCC_DEFAULT_CM_8_1
Set Type	9641SIPCC
Port	IP
Security Code	
Name	
Class of Restriction (COR)	1
Emergency Location Ext	78030
Tenant Number	1
SIP Trunk	Qaar
Coverage Path 1	
Lock Message	<input type="checkbox"/>
Multibyte Language	Not Applicable
Class Of Service (COS)	1
Message Lamp Ext.	78030
Coverage Path 2	
Localized Display Name	
Enable Reachability for Station Domain Control	system
Type of 3PCC Enabled	Avaya

8. Configure InGenius Connector Enterprise

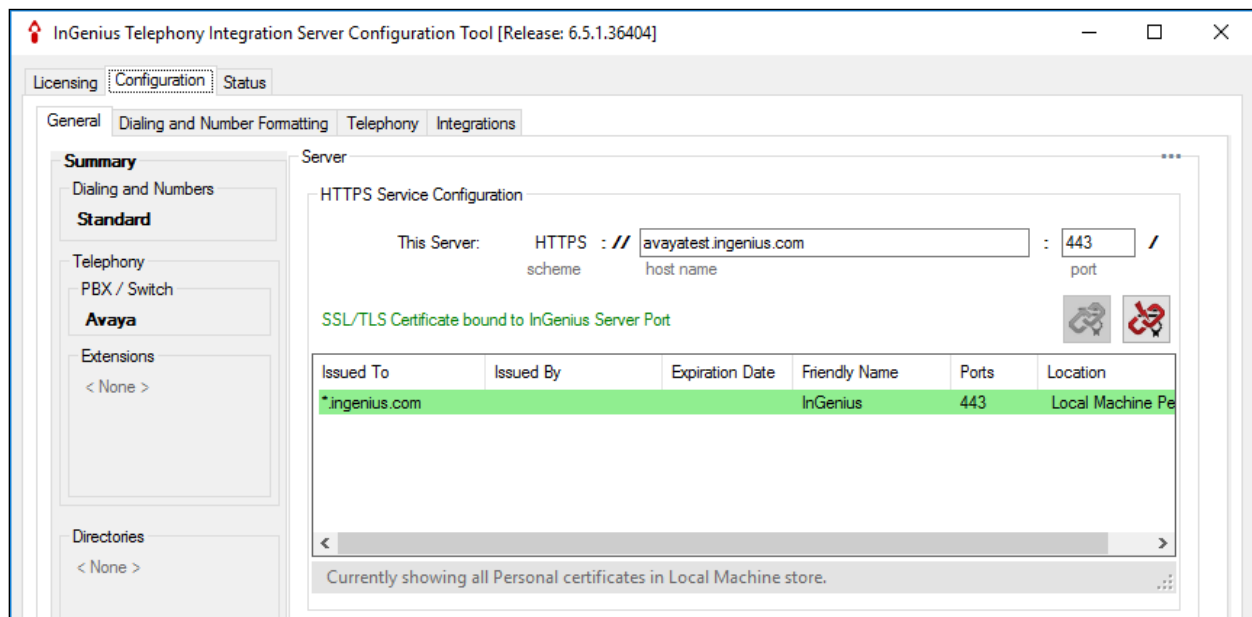
This section provides the procedures for configuring ICE. The procedures include the following areas:

- 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.

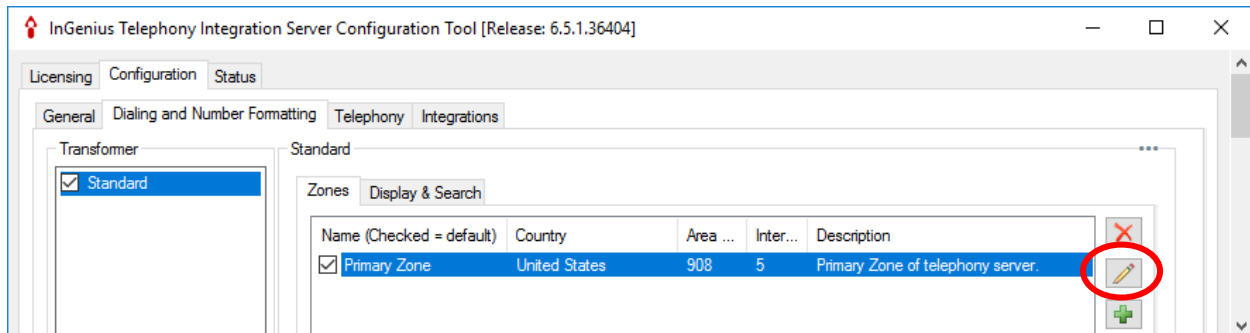
8.1. Launch InGenius Server Configuration

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



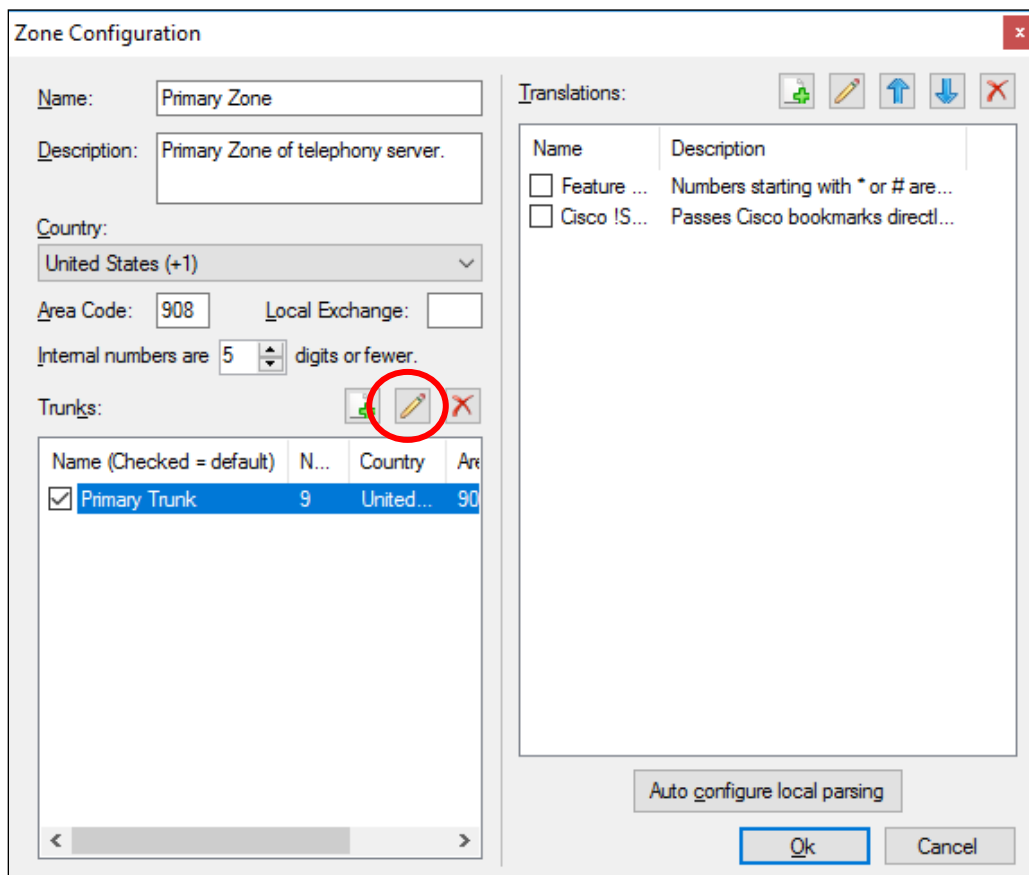
8.2. Administer Dialing and Number Formatting

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.

The screenshot shows a 'Trunk' configuration window. On the left, there are fields for Name (Primary Trunk), Description (Primary trunk of telephony server), Prefix (9), Country (United States (+1)), Area Code (908), and Local Exchange. Below these are checkboxes for Allowed calls: Local, Dial area code for local calls, Long Distance, and International. Further down are fields for Long distance carrier code and International carrier code. At the bottom left is a 'Test dialing' section with fields for Enter number to dial, Expanded to, and Dialable. On the right, there is a 'Translations to dialable' section with a table containing two entries: Argentina and Mexican. At the bottom right are buttons for 'Auto configure local dialing', 'OK', and 'Cancel'.

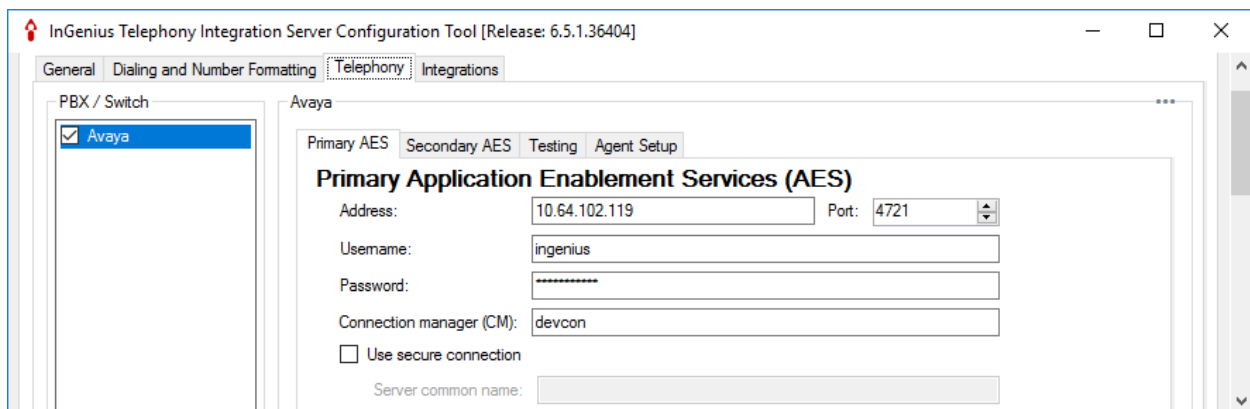
Name	Description
<input type="checkbox"/> Argentina ...	International call from North A...
<input type="checkbox"/> Mexican ...	International calls to Mexican ...

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**.

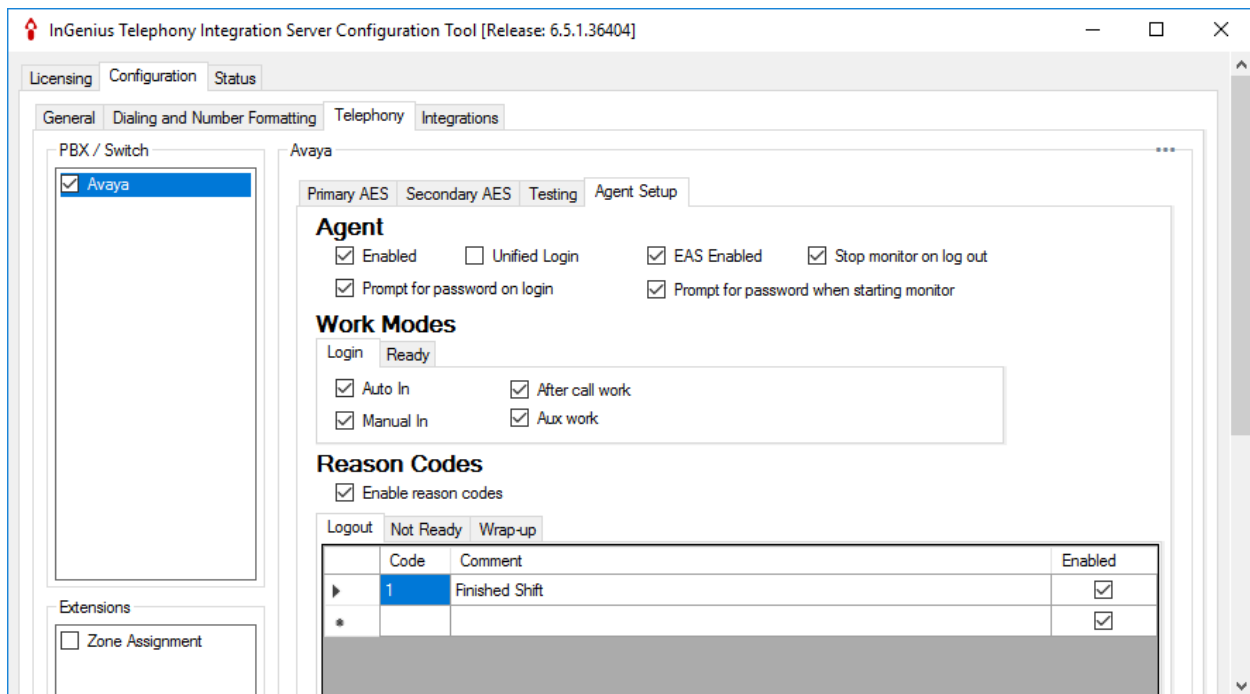


The screenshot shows the 'InGenius Telephony Integration Server Configuration Tool' window. The 'Telephony' tab is selected in the top menu. On the left, under 'PBX / Switch', 'Avaya' is selected. The main area shows the 'Primary AES' configuration for 'Avaya'. The 'Primary Application Enablement Services (AES)' section contains the following fields:

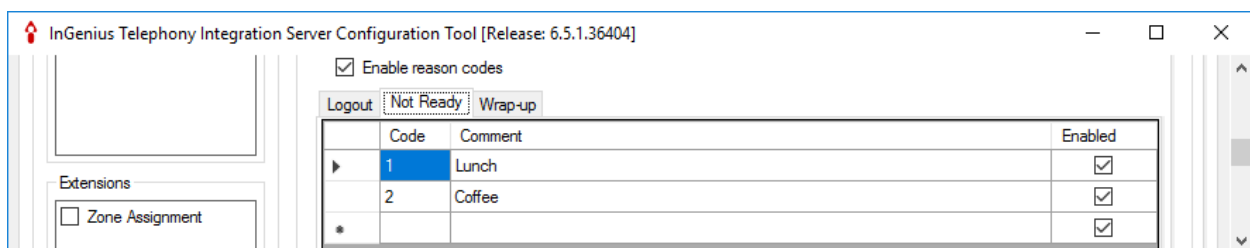
- Address:** 10.64.102.119
- Port:** 4721
- Username:** ingenius
- Password:** (masked with asterisks)
- Connection manager (CM):** devcon
- ☐ Use secure connection
- Server common name:** (empty field)

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.

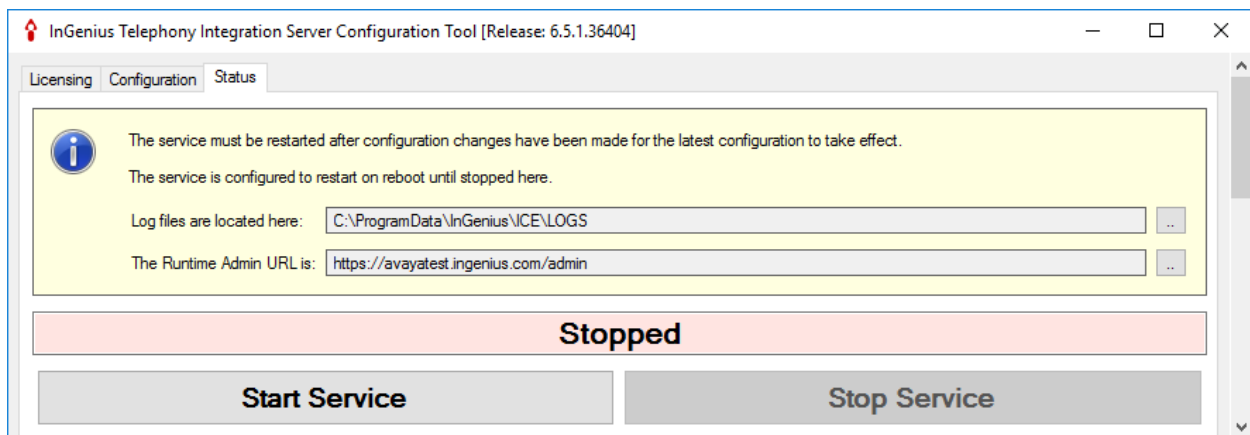


Two reason codes were created under the **Not Ready** tab.

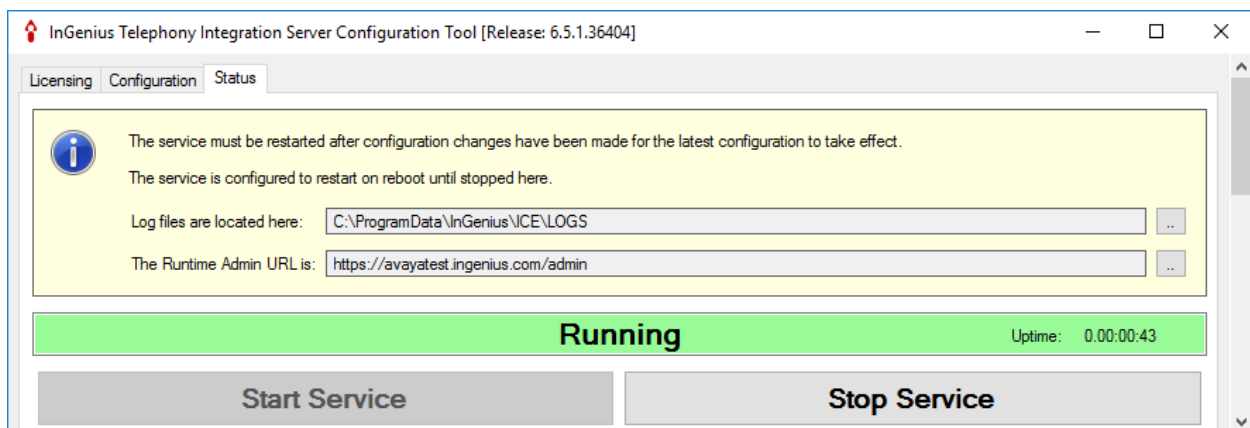


8.4. Start Service

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 aesvcs cti-link** command. Verify that the **Service State** is *established* for the CTI link number administered in **Section 5.3**, as shown below.

```
status aesvcs cti-link
```

AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs 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**.

AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri Oct 2 13:07:03 2020 from 192.168.100.250
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 8.1.2.1.6-0
Server Date and Time: Fri Oct 02 13:38:39 EDT 2020
HA Status: Not Configured

Status | Status and Control | DMCC Service Summary

AE Services

Communication Manager Interface

High Availability

Licensing

Maintenance

Networking

Security

Status

Alarm Viewer

Logs

Log Manager

Status and Control

CVLAN Service Summary

DLG Services Summary

DMCC Service Summary

Switch Conn Summary

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary [Device Summary](#)
Generated on Fri Oct 02 13:38:04 EDT 2020

Service Uptime: 16 days, 1 hours 45 minutes

Number of Active Sessions: 1

Number of Sessions Created Since Service Boot: 12

Number of Existing Devices: 0

Number of Devices Created Since Service Boot: 0


	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
<input type="checkbox"/>	3C4583D046938E4F D21EF6677D7E50B-11	ingenius	InGenius Avaya Plugin	10.64.102.104	XML Unencrypted	0

Terminate Sessions Show Terminated Sessions

Item 1-1 of 1
1 Go

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.



Application Enablement Services
Management Console

Welcome: User cust
 Last login: Fri Oct 2 13:07:03 2020 from 192.168.100.250
 Number of prior failed login attempts: 0
 HostName/IP: devcon-aes/10.64.102.119
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 8.1.2.1.1.6-0
 Server Date and Time: Fri Oct 02 13:39:27 EDT 2020
 HA Status: Not Configured

Status | Status and Control | TSAPI Service Summary
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▼ **Status**
 - Alarm Viewer
 - ▶ Logs
 - ▶ Log Manager
 - ▼ **Status and Control**
 - CVLAN Service Summary
 - DLG Services Summary
 - DMCC Service Summary
 - Switch Conn Summary
 - **TSAPI Service Summary**

TSAPI Link Details

☐ Enable page refresh every 60 seconds

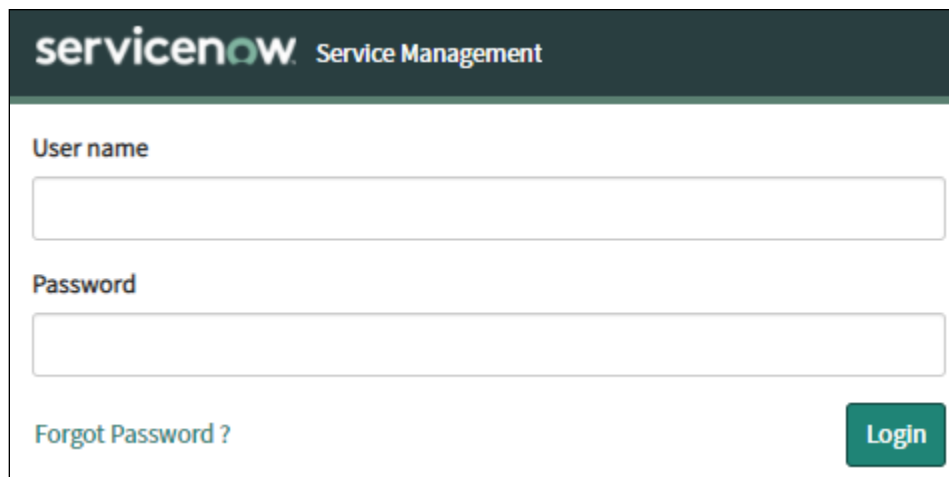
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	devcon	1	Talking	Tue Sep 22 14:11:50 2020	Online	18	1	15	15	30

Online
Offline

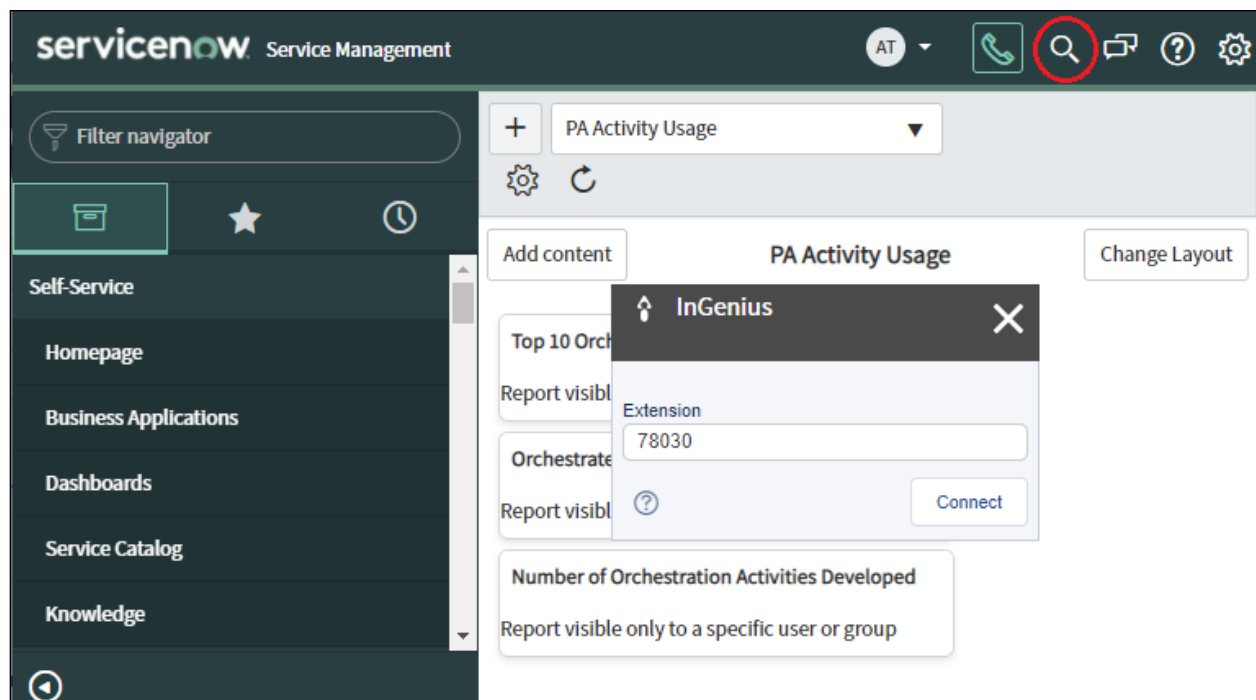
For service-wide information, choose one of the following:
TSAPI Service Status
TLink Status
User Status

9.3. Verify InGenius Connector Enterprise

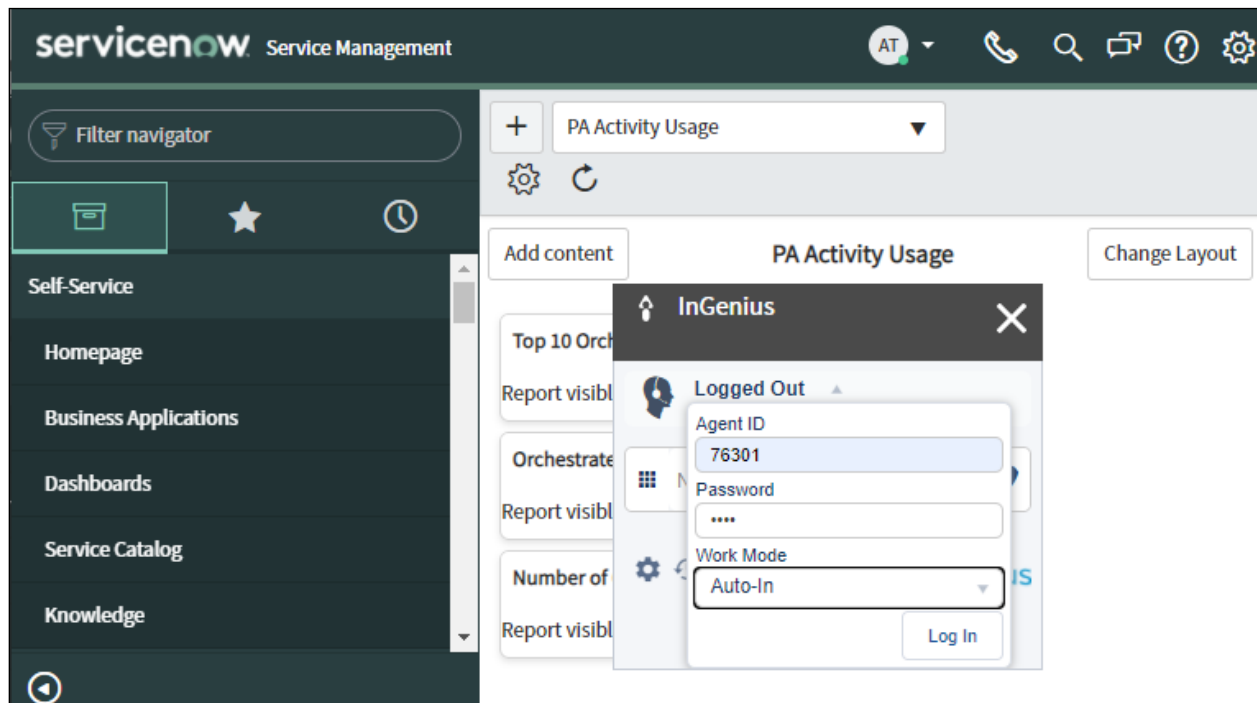
From an agent PC, launch an Internet browser window and enter the URL provided by the end customer for ServiceNow. Log in with the relevant user credentials provided by InGenius.

The image shows the ServiceNow login page. At the top, the ServiceNow logo is followed by the text "Service Management". Below this, there are two input fields: "User name" and "Password". To the right of the "Password" field is a green "Login" button. Below the "User name" field is a link that says "Forgot Password?".

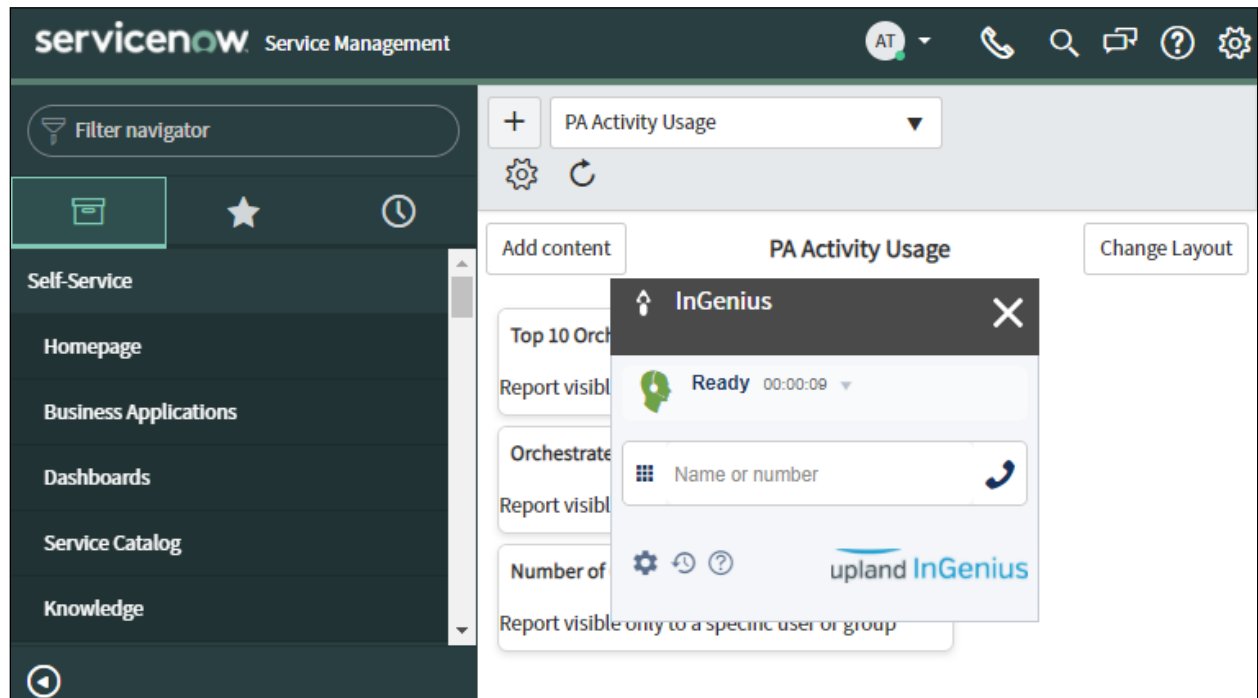
The screen below is displayed next. Select the phone icon from the top menu to display the **InGenius** floating screen shown below. Enter the relevant agent station extension from **Section 3**, and click **Connect**.

The image shows the ServiceNow interface. On the left is a dark sidebar with a "Filter navigator" at the top and a list of menu items: "Self-Service", "Homepage", "Business Applications", "Dashboards", "Service Catalog", and "Knowledge". At the bottom of the sidebar is a circular arrow icon. The main area has a header with the ServiceNow logo and "Service Management", followed by a user profile icon labeled "AT" and several utility icons. One of these icons, a magnifying glass, is circled in red. Below the header, there's a section titled "PA Activity Usage" with a dropdown menu. Below this, there's a "Top 10 Orch" report visible. An "InGenius" floating screen is overlaid on the main content. It has a title bar with an up arrow icon and a close button. Inside the floating screen, there's an "Extension" input field with the value "78030" and a "Connect" button. Below the floating screen, there's a "Number of Orchestration Activities Developed" report visible, with a note that it's "Report visible only to a specific user or group".

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**.

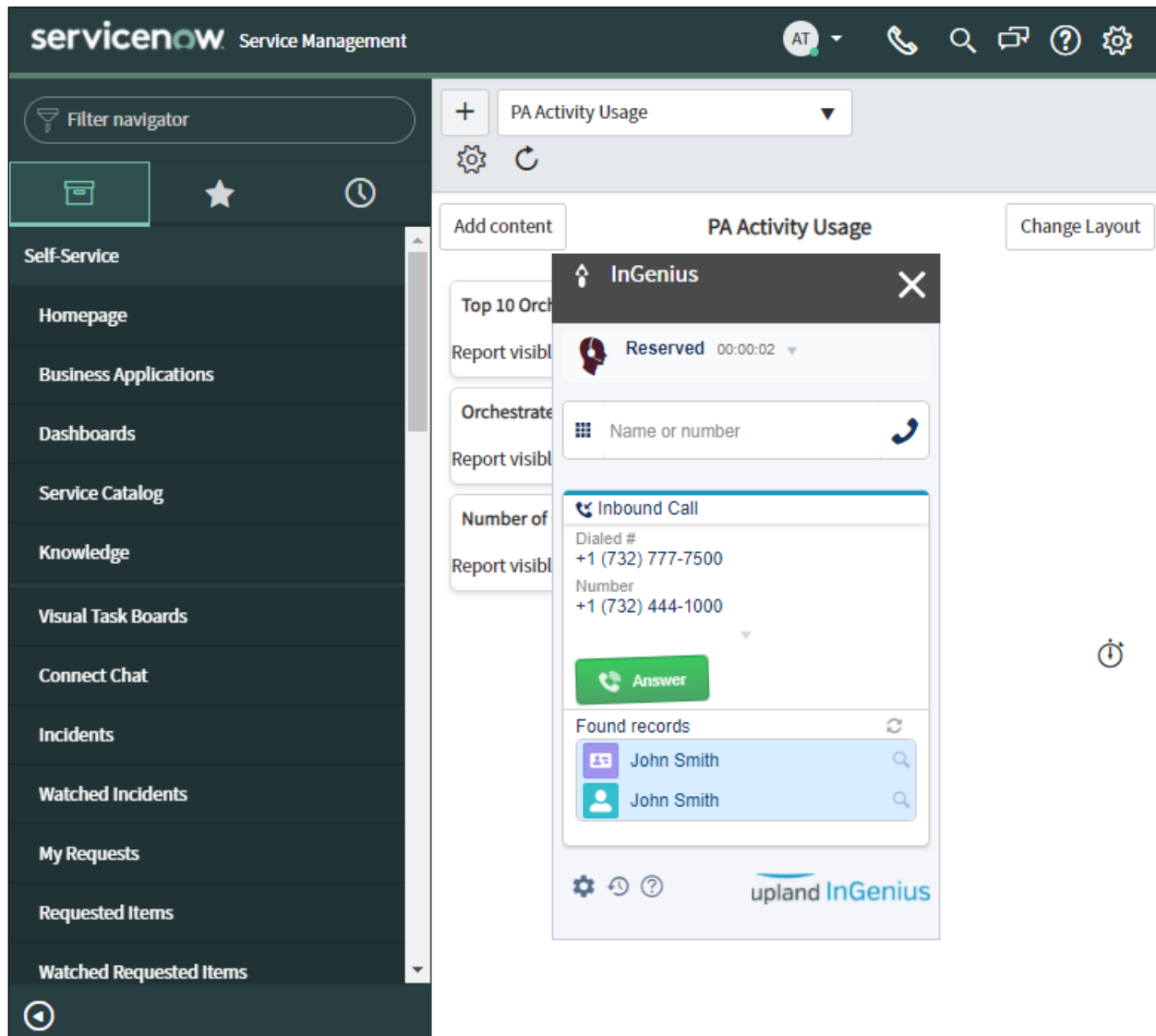


Verify that the **InGenius** screen is updated, showing the agent in the **Ready** state.

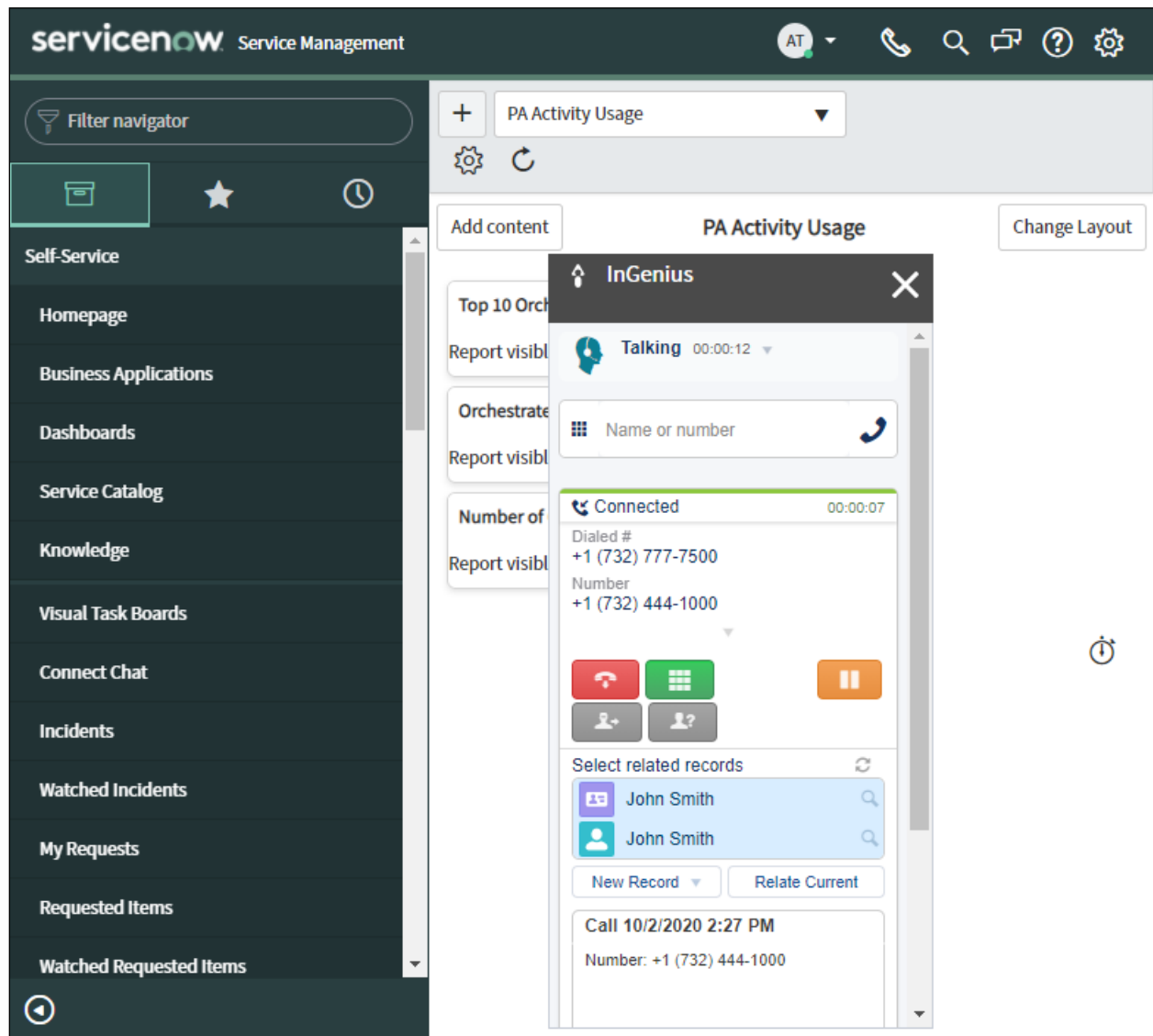


Make an incoming ACD call. Verify that the **InGenius** screen for the available agent is updated to reflect **Reserved** and **Inbound Call**, along with proper call information. Also verify that the background window is populated with the uniquely matching contact record associated with the PSTN caller 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.

1. *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 6, March 2020, available at <http://support.avaya.com>.
2. *Administering and Maintaining Aura® Application Enablement Services*, Release 8.1.x, Issue 7, July 2020, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® System Manager*, Release 8.1.x, Issue 6, April 2020, available at <http://support.avaya.com>.
4. *Administering Avaya Aura® Session Manager*, Release 8.1.x, Issue 6, August 2020, available at <http://support.avaya.com>.
5. *InGenius Connector Enterprise for ServiceNow Readiness Guide*, Version 6.5, CRM: ServiceNow, Phone System: Avaya, available upon request to InGenius Support.
6. *InGenius Connector Enterprise for ServiceNow Administrator Guide*, Version 6.5, CRM: ServiceNow, Phone System: Avaya, available upon request to InGenius Support.
7. *InGenius Connector Enterprise for ServiceNow User Guide*, Version 6.5, CRM: ServiceNow, Phone System: Avaya, available upon request to InGenius Support.

©2020 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.