



DevConnect Program

Application Notes for InGenius Connect 2023 R1.0 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate InGenius Connect with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. InGenius Connect is a CRM-VoIP integration tool that sits between the customer's phone system and a CRM application, such as Salesforce.

In the compliance test, InGenius Connect 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 Salesforce.

Readers should pay attention to **Section Error! Reference source not found.**, in particular the scope of testing as outlined in **Section Error! Reference source not found.** as well as any observations noted in **Section Error! Reference source not found.**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the Avaya DevConnect Program.

1. Introduction

These Application Notes describe the configuration steps required to integrate InGenius Connect with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. InGenius Connect is a CRM-VoIP integration tool that sits between the customer's phone system and a CRM application, such as Salesforce.

In the compliance test, InGenius Connect 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 Salesforce. InGenius Connect is comprised of the InGenius Telephony Gateway and InGenius Connect Apex Package .

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. Upon an agent log in, InGenius Connect used DMCC to query device information and agent state, log 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 Salesforce. 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 InGenius Telephony Gateway 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 InGenius Connect did not include use of any specific encryption features as requested by Upland Software.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on InGenius Connect:

- 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, redirect on no answer, auto answer, 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 InGenius Connect to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to InGenius Telephony Gateway.

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 InGenius Connect can be obtained through the following:

- **Phone:** +1 (613) 591-9002 x4000
- **Email:** ingenius-support@uplandsoftware.com
- **Web :** <https://support.uplandsoftware.com/portal/ss/login>

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, InGenius Connect monitored the agent stations shown in the table below.

Device Type	Extension
VDNs	60001
Skill Group	61001
Agent Stations	65000, 65001, 66006
Agent IDs	65881, 65882

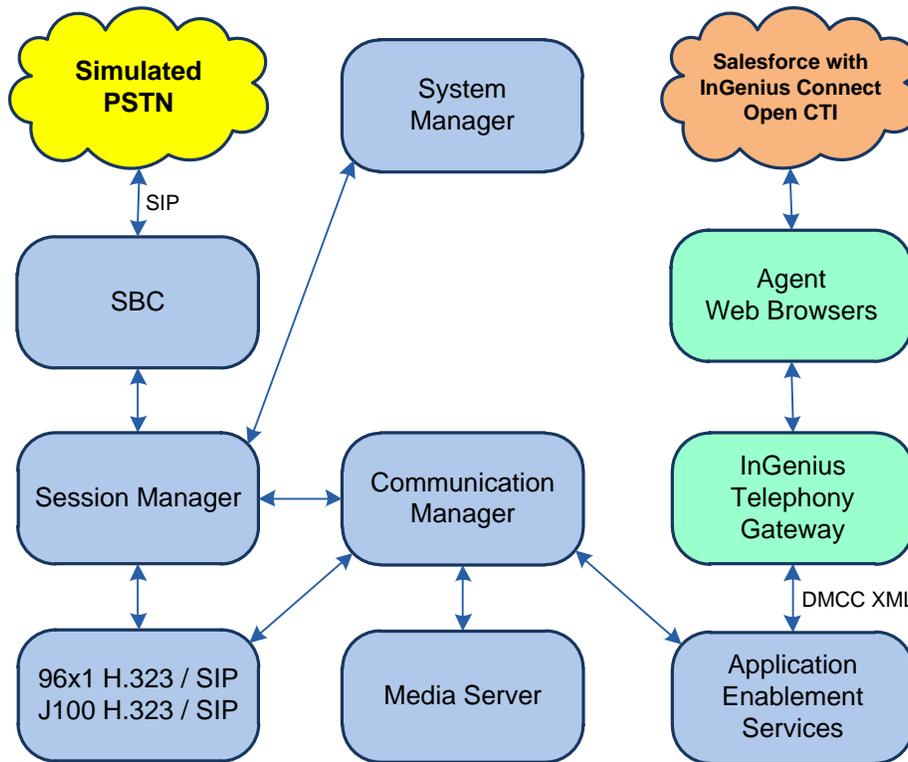


Figure 1: InGenius Connect with Avaya Aura® Suite

4. Equipment and Software Validated

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

Software Component	Version
Aura® Communication Manager	10.1.3.0.1.974.27893
Aura® Media Server	10.1.0.154
Aura® System Manager	10.1.3.0.0715713
Aura® Session Manager	10.1.3.0.1013007
Aura® Application Enablement Services	10.1.3.0.0.11-0
Session Border Controller	10.1.2.0-64-23285
96x1 Series Deskphones J179 Series Deskphones	6.8.5.3.2 (H.323)
J169 Series Deskphones	4.0.13.0.6 (SIP)
InGenius Connect , including: <ul style="list-style-type: none">▪ InGenius Telephony Gateway on Windows Server 2019▪ InGenius Connect Apex Package	2023 R1.0

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 InGenius Telephony Gateway.

```
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 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
```

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: 60111
  Type: ADJ-IP
                                                COR: 1
  Name: AES CTI 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 InGenius Connect.

```
change reason-code-names                          Page 1 of 1
                                                REASON CODE NAMES
                                                Aux Work/      Logout
                                                Interruptible?
Reason Code 1: Meeting           /n
Reason Code 2: Lunch             /n
Reason Code 3: Break             /n
Reason Code 4: Sleep             /n
Reason Code 5:                       /n
Reason Code 6:                       /n
Reason Code 7:                       /n      Other
Reason Code 8:                       /n
Reason Code 9:                       /n
Default Reason Code:
```

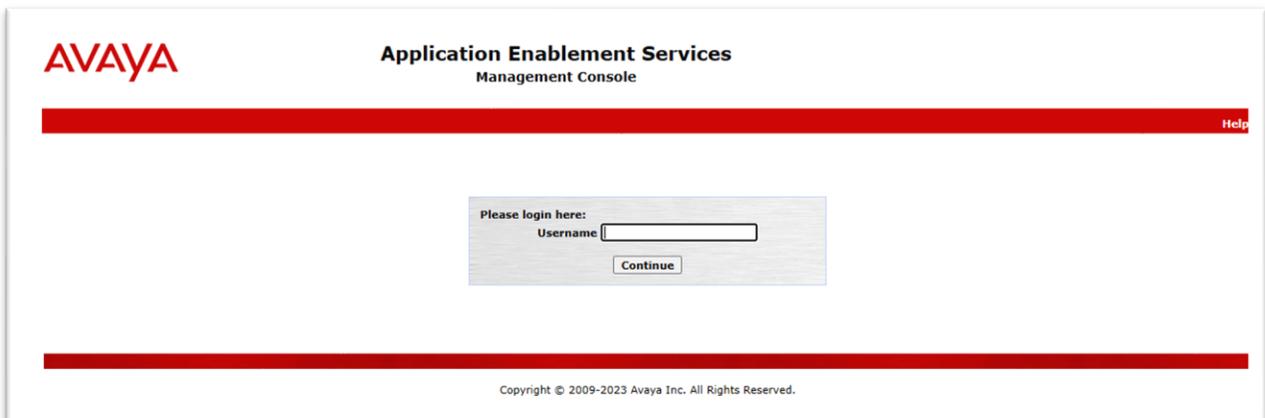
6. Configure Avaya Aura® Application Enablement Services

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

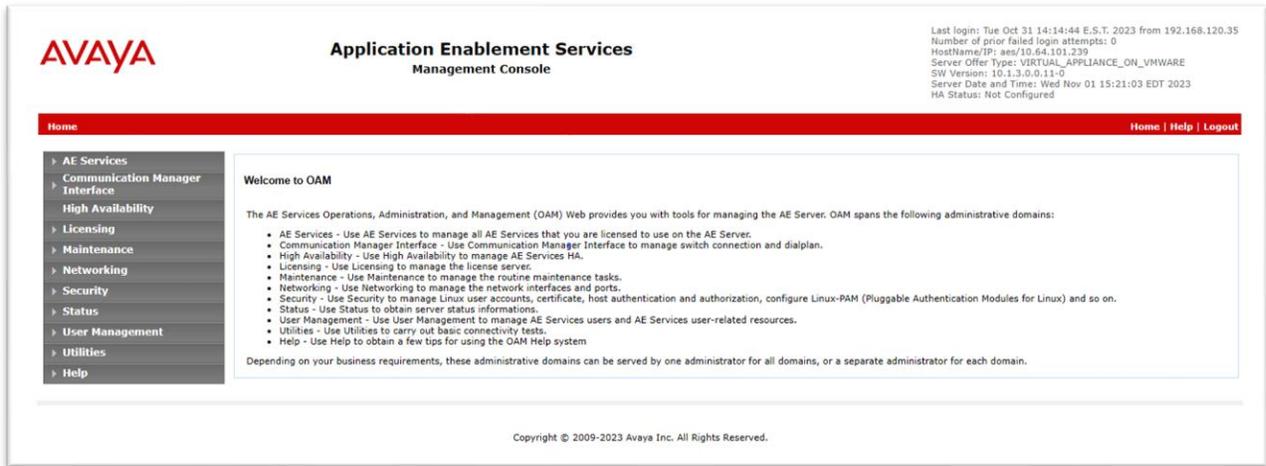
6.1. Launch OAM Interface

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 Application Enablement Services. The login screen is displayed. Log in using the appropriate credentials.



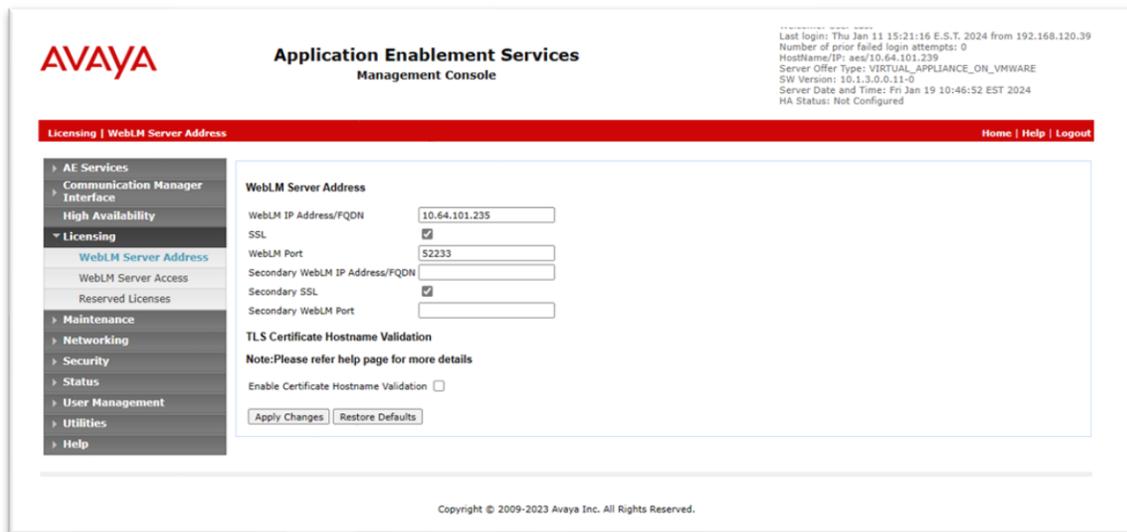
The screenshot shows the Avaya Application Enablement Services Management Console login interface. At the top left is the Avaya logo. The title "Application Enablement Services Management Console" is centered at the top. A red horizontal bar spans the width of the page, with a "Help" link on the right. Below this bar is a login form with the text "Please login here:" and a "Username" label next to a text input field. A "Continue" button is positioned below the input field. At the bottom of the page, a red horizontal bar is present, and the copyright notice "Copyright © 2009-2023 Avaya Inc. All Rights Reserved." is centered.

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



6.2. Verify License

Select **Licensing** → **WebLM Server Address** in the left pane to display the applicable WebLM IP address. Log into WebLM using the appropriate credentials.



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 InGenius Connect.

Application Enablement (CTI) - Release: 10 - SID: 10503000(Enterprise license file)

You are here: Licensed Products > Application_Enablement > View by Feature

License installed on: June 10, 2022 9:09:46 PM -04:00

License File Host IDs: V5-E1-B3-74-2B-9E-01

Feature (License Keyword)	Expiration date	License Capacity	Currently available
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	3
DLG (VALUE_AES_DLG)	permanent	16	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	16
Product Notes (VALUE_NOTES)	permanent		Not counted

SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;letpot;CtiSmallServer
MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer
LargeServerTypes: isp2100;ibmx305;d380g3;d385g1;d385g2;unknown;CtiLargeServer
TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; OSPC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted; CCT_ELITE_CALL_CTRL_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; ANAV_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; UNIFIED_DESKTOP_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; AACCC_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; CE_AGENT_STATES_001, BasicUnrestricted, AdvancedUnrestricted, DMCUnrestricted, AgentEvents; TP_CLIENT_001, BasicUnrestricted, , , AgentEvents; EXT_CLIENT_001, , ,

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**.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	cm	1	12	Both

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 **cm** is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.3**. Retain the default values in the remaining fields.

Link: 1
Switch Connection: cm
Switch CTI Link Number: 1
ASAI Link Version: 12
Security: Both

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The top center shows the title "Application Enablement Services Management Console". The top right contains system information: "Welcome: user user", "Last login: Thu Jan 11 15:21:16 E.S.T. 2024 from 192.168.120.39", "Number of prior failed login attempts: 0", "HostName/IP: aes/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.3.0.0.11-0", "Server Date and Time: Fri Jan 19 10:49:28 EST 2024", and "HA Status: Not Configured".

A red navigation bar at the top contains "User Management | User Admin | List All Users" on the left and "Home | Help | Logout" on the right. A left-hand navigation pane lists various services, with "User Management" expanded to show "User Admin" and its sub-items: "Add User", "Change User Password", "List All Users", "Modify Default Users", and "Search Users".

The main content area is titled "Edit User" and contains the following form fields:

- * User Id: ingenius
- * Common Name: ingenius
- * Surname: ingenius
- User Password: [masked]
- Confirm Password: [masked]
- Admin Note: [empty text area]
- Avaya Role: None (dropdown)
- Business Category: [empty text area]
- Car License: [empty text area]
- CM Home: [empty text area]
- Css Home: [empty text area]
- CT User: Yes (dropdown)
- Department Number: [empty text area]
- Display Name: [empty text area]
- Employee Number: [empty text area]
- Employee Type: [empty text area]

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, system information is provided: "welcome: user cust", "Last login: Fri Oct 27 14:14:39 E.S.T. 2023 from 192.168.120.19", "Number of prior failed login attempts: 1", "HostName/IP: aes/10.64.101.239", "Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE", "SW Version: 10.1.3.0.0.11-0", "Server Date and Time: Mon Oct 30 17:07:15 EDT 2023", and "HA Status: Not Configured".

A red navigation bar contains the breadcrumb "Security | Security Database | Control" on the left and "Home | Help | Logout" on the right. The left sidebar menu includes categories like "AE Services", "Communication Manager Interface", "High Availability", "Licensing", "Maintenance", "Networking", "Security", "Account Management", "Audit", "Certificate Management", "Enterprise Directory", "Host AA", "PAM", "Security Database", and "Control".

The main content area is titled "SDB Control for DMCC, WTI, TSAPI, JTAPI and Telephony Web Services" and contains two unchecked checkboxes: "Enable SDB for DMCC and WTI Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located below these options.

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User cust, Last login: Thu Jan 11 15:21:16 E.S.T. 2024 from 192.168.120.39, Number of prior failed login attempts: 0, HostName/IP: aes/10.64.101.239, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 10.1.3.0.0.11-0, Server Date and Time: Fri Jan 19 10:50:38 EST 2024, HA Status: Not Configured.

The main interface has a red header bar with "Networking | Ports" on the left and "Home | Help | Logout" on the right. A left-hand navigation pane lists various sections, with "Networking" expanded to show "Ports" selected.

The "Ports" configuration area is divided into three sections:

- CVLAN Ports:** Includes "Unencrypted TCP Port" (9999) and "Encrypted TCP Port" (9998), each with "Enabled" and "Disabled" radio buttons.
- DLG Port:** Includes "TCP Port" (5678).
- TSAPI Ports:** Includes "TSAPI Service Port" (450) with "Enabled" and "Disabled" radio buttons, and "Local TLINK Ports" with "TCP Port Min" (1024) and "TCP Port Max" (1039). Below this are "Unencrypted TLINK Ports" with "TCP Port Min" (1050) and "TCP Port Max" (1065), and "Encrypted TLINK Ports" with "TCP Port Min" (1066) and "TCP Port Max" (1081).
- DMCC Server Ports:** Includes "Unencrypted Port" (4721), "Encrypted Port" (4722), and "TR/87 Port" (4723), each with "Enabled" and "Disabled" radio buttons.

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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User cust, Last login: Thu Jan 11 15:21:16 E.S.T. 2024 from 192.168.120.39, Number of prior failed login attempts: 0, HostName/IP: aes10.64.101.239, Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE, SW Version: 10.1.3.0.0.11-0, Server Date and Time: Fri Jan 19 10:51:26 EST 2024, HA Status: Not Configured.

The main interface has a red header bar with "Maintenance | Service Controller" on the left and "Home | Help | Logout" on the right. A left-hand navigation pane lists various categories, with "Maintenance" expanded to show "Service Controller" selected.

The "Service Controller" section contains a table with the following data:

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
<input type="checkbox"/> WTI Service	Stopped

Below the table, a note states: "Note: DMCC Service must be restarted for WTI service changes to take effect. For status on actual services, please use [Status and Control](#)".

At the bottom of the service list, there are buttons for "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".

Copyright © 2008-2023 Avaya Inc. All Rights Reserved.

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.

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

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

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

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

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

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

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

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

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

User ID:

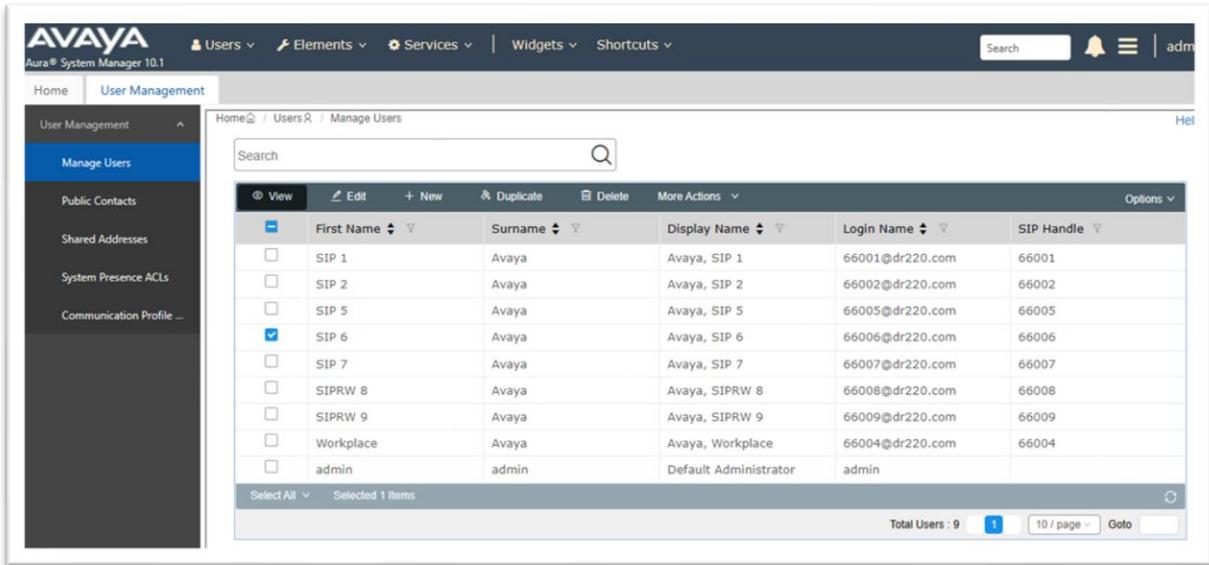
Password:

[Change Password](#)

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

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 SIP agent station from **Section Error! Reference source not found.**, in this case **66006**, and click **Edit**.

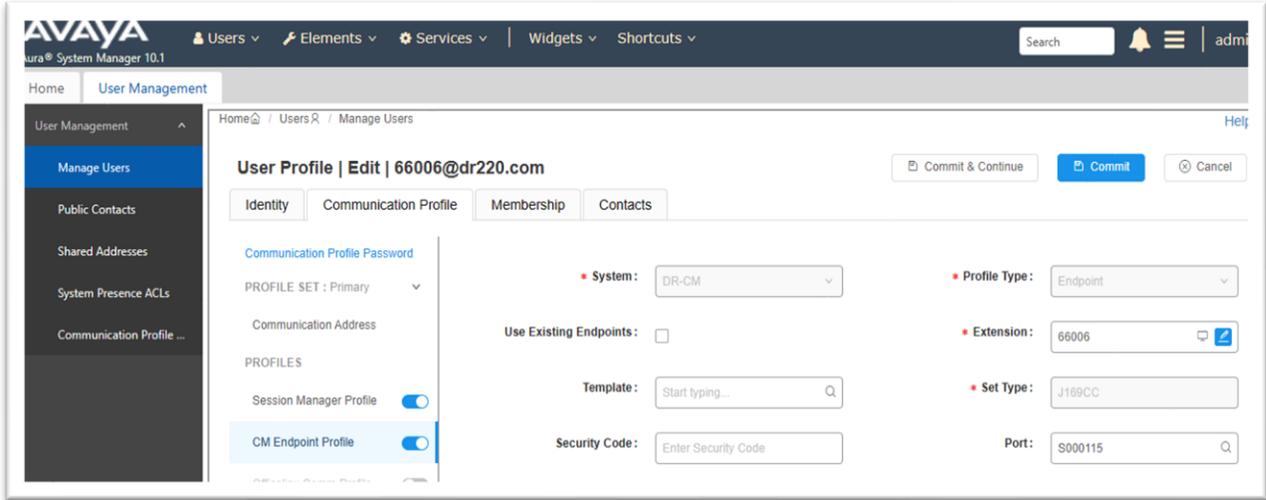


The screenshot displays the Avaya System Manager 10.1 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows 'User Management' with 'Manage Users' selected. The main content area shows a table of users with columns for First Name, Surname, Display Name, Login Name, and SIP Handle. The user 'SIP 6' is selected, and the status bar at the bottom indicates 'Total Users : 9' and 'Selected 1 Items'.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP 1	Avaya	Avaya, SIP 1	66001@dr220.com	66001
<input type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
<input type="checkbox"/>	SIP 5	Avaya	Avaya, SIP 5	66005@dr220.com	66005
<input checked="" type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006
<input type="checkbox"/>	SIP 7	Avaya	Avaya, SIP 7	66007@dr220.com	66007
<input type="checkbox"/>	SIPRW 8	Avaya	Avaya, SIPRW 8	66008@dr220.com	66008
<input type="checkbox"/>	SIPRW 9	Avaya	Avaya, SIPRW 9	66009@dr220.com	66009
<input type="checkbox"/>	Workplace	Avaya	Avaya, Workplace	66004@dr220.com	66004
<input type="checkbox"/>	admin	admin	Default Administrator	admin	

The **User Profile 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 **New 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.

Edit Endpoint Help ? x

Done

[Save As Template]

System	DR-CM	Extension	66006
Template	Select	Set Type	J169CC
Port	S000115	Security Code	
Name	Avaya, SIP 6		

General Options (G) *	Feature Options (F)	Site Data (S)	Abbreviated Call Dialing (A)	Enhanced Call Fwd (E)
Button Assignment (B)	Profile Settings (P)	Group Membership (M)		

* Class of Restriction (COR)	2	* Class Of Service (COS)	1
* Emergency Location Ext	66006	* Message Lamp Ext.	66006
* Tenant Number	1	Type of 3PCC Enabled	Avaya
* SIP Trunk	Qaar	Coverage Path 2	
Coverage Path 1		Localized Display Name	Avaya, SIP 6
Lock Message	<input type="checkbox"/>	Enable Reachability for Station Domain Control	system
Multibyte Language	Not Applicable		

SIP URI

Primary Session Manager

IPv4:	10.64.101.238	IPv6:	
--------------	---------------	--------------	--

Secondary Session Manager

8. Configure InGenius Connect

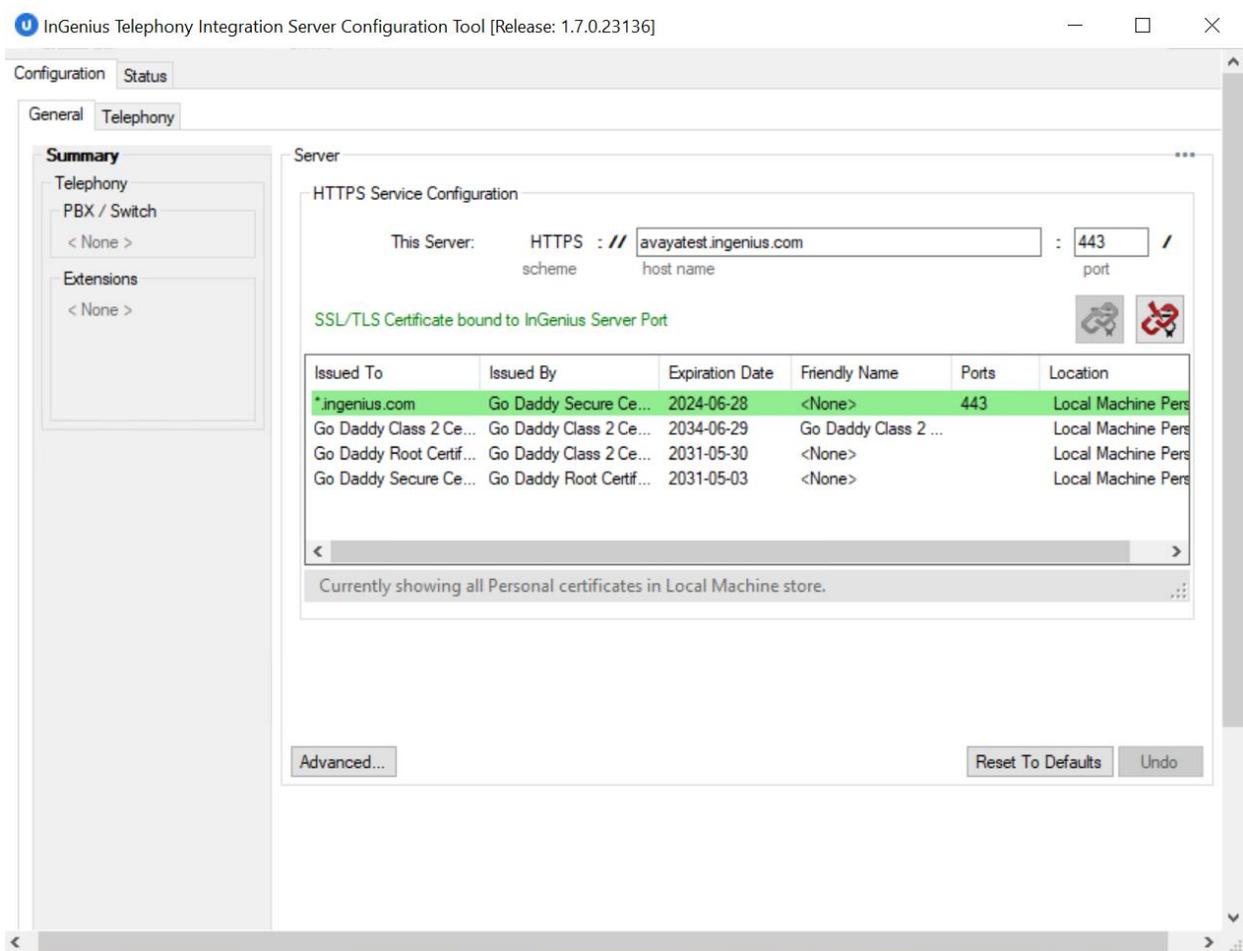
This section provides the procedures for configuring InGenius Connect. The procedures include the following areas:

- Launch InGenius Telephony Integration Server Configuration Tool
- 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 Telephony Integration Server Configuration Tool

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



8.2. Administer Telephony

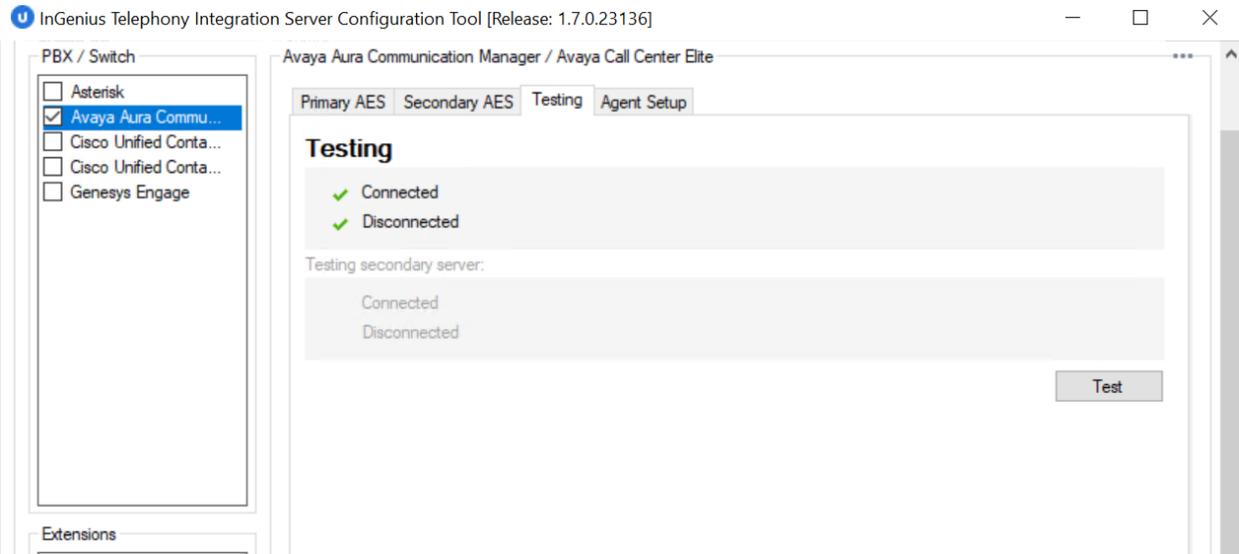
The **InGenius Telephony Integration Server Configuration Tool**, select **Configuration** → **Telephony** from the top menu, followed by the **Primary AES** tab in the right pane to display the screen below.

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.
- **Port:** The DMCC unencrypted port *4721*.
- **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 0**.

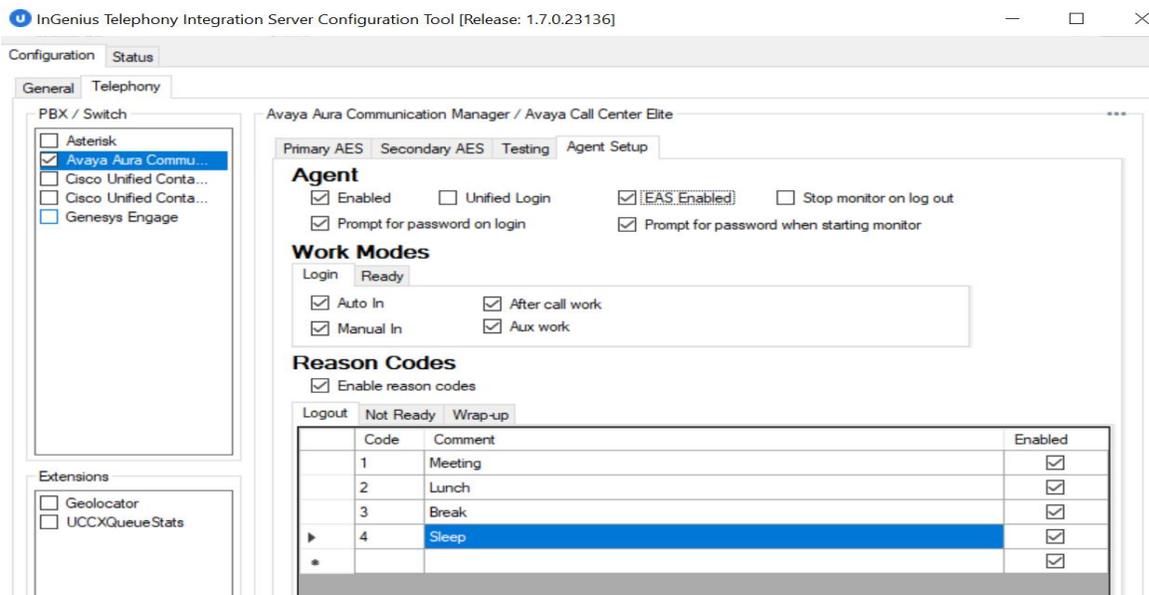
The screenshot shows the 'InGenius Telephony Integration Server Configuration Tool [Release: 1.7.0.23136]' window. The 'Configuration' tab is active, and the 'Telephony' sub-tab is selected. On the left, under 'PBX / Switch', the 'Avaya Aura Commu...' option is checked. The main area displays the 'Primary Application Enablement Services (AES)' configuration for 'Avaya Aura Communication Manager / Avaya Call Center Elite'. The 'Primary AES' tab is selected, showing fields for Address (10.64.101.239), Port (4721), Username (ingenius), Password (masked with asterisks), and Connection manager (CM) (cm). There is also a checkbox for 'Use secure connection' and a 'Server common name' field.

Select the **Testing** tab and click the **Test** button to verify connectivity to Application Enablement Services.

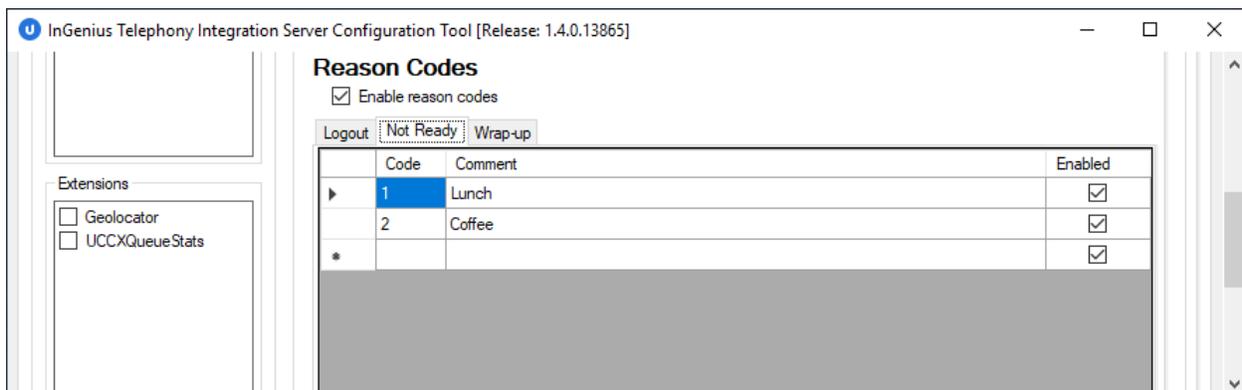


Select the **Agent Setup** tab in the right pane to display the screen below. Update parameters in the **Agent** and **Work Modes** sub-sections to the proper settings. The screenshot below shows the values used in the compliance testing.

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, four reason codes were created under the **Logout** tab.

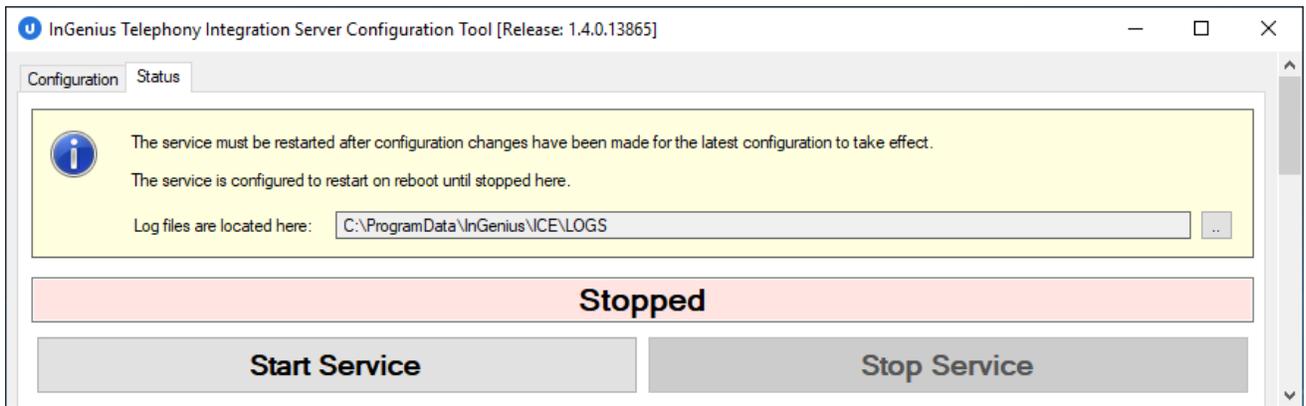


Two reason codes were created under the **Not Ready** tab.

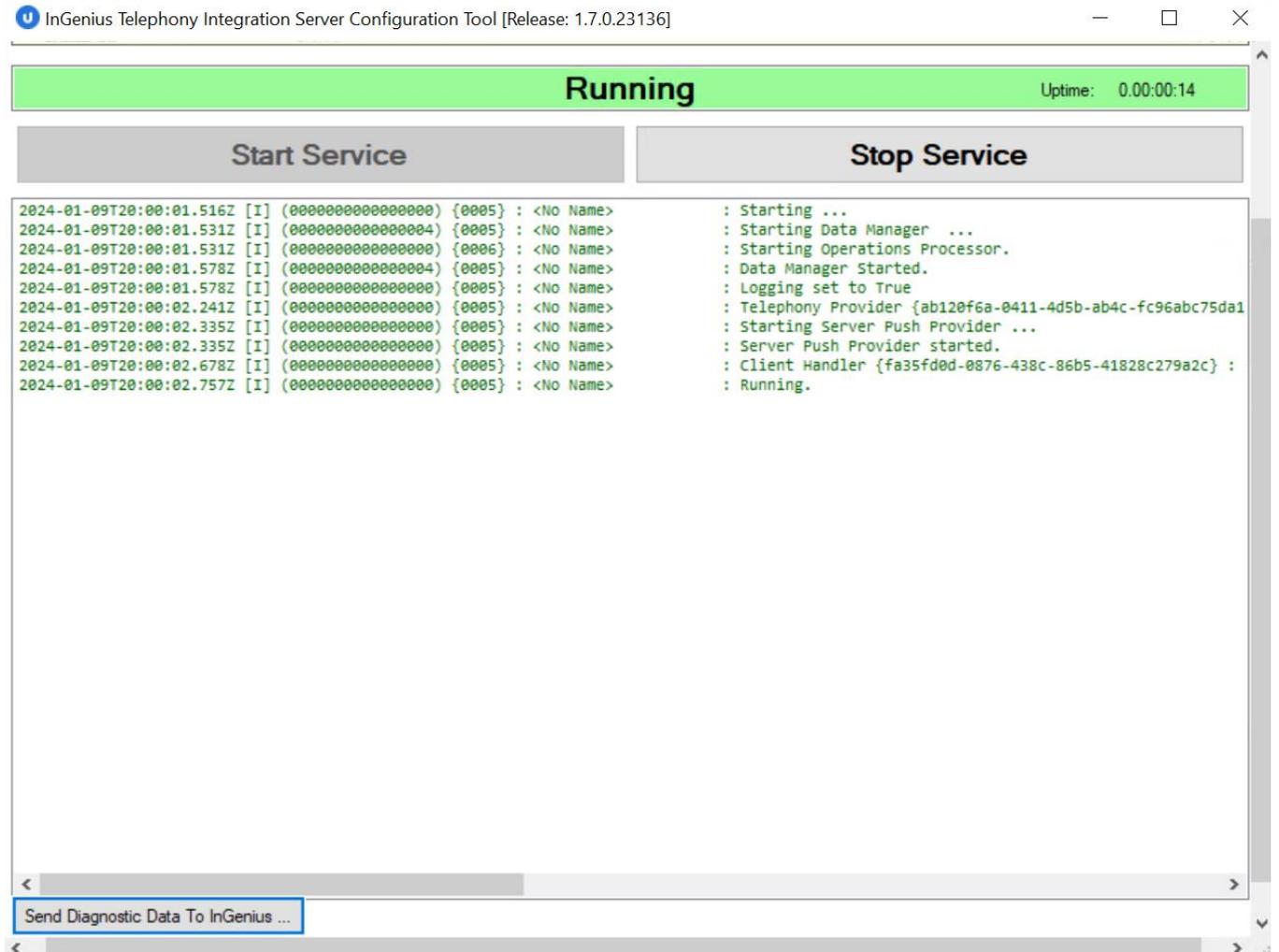


8.3. Start Service

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 InGenius Connect.

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	12	no	aes	established	3289	3289

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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The left navigation pane is expanded to 'Status and Control', with 'DMCC Service Summary' selected. The main content area displays the 'DMCC Service Summary - Session Summary' page. It includes a warning to not use the back button, an option to enable page refresh every 60 seconds, and session summary statistics: Service Uptime (13 days, 21 hours 11 minutes), Number of Active Sessions (1), Number of Sessions Created Since Service Boot (11), Number of Existing Devices (0), and Number of Devices Created Since Service Boot (4). A table lists the active session details:

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
86FDC9F4E6AEA0217 F4A4FE83859CBE6-13	ingenius	InGenius Avaya Plugin	10.64.101.207	XML Unencrypted	0

Below the table, there are buttons for 'Terminate Sessions' and 'Show Terminated Sessions', and a pagination control showing 'Item 1-1 of 1' and a 'Go' button.

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 0**, and that the **Associations** column reflects the number of agents from **Section Error!** Reference source not found. that are currently logged into InGenius Connect and connected to the agent stations on Communication Manager.

AVAYA Application Enablement Services Management Console

PREVIOUS: User Login
 Last login: Fri Jan 19 10:46:37 E.S.T. 2024 from 192.168.120.42
 Number of prior failed login attempts: 0
 HostName/IP: aes/10.64.101.239
 Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
 SW Version: 10.1.3.0.0.11-0
 Server Date and Time: Fri Jan 19 11:08:59 EST 2024
 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

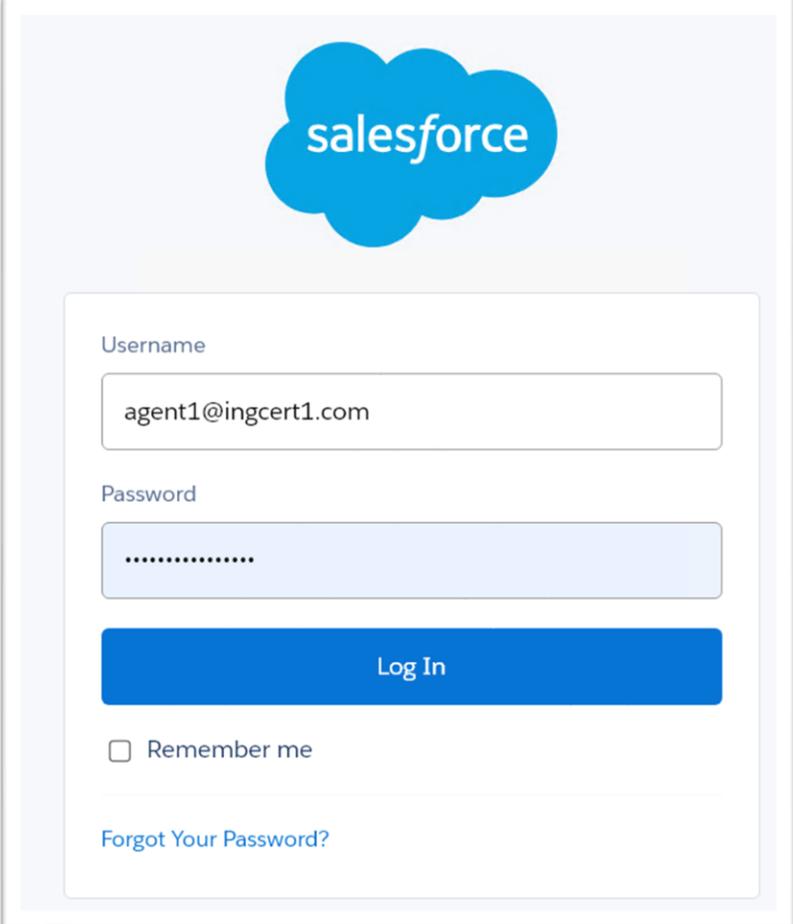
Enable page refresh every seconds

	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
Ⓢ	1	cm	1	Talking	Fri Jan 5 13:55:15 2024	Online	20	51	3326	3330	30

For service-wide information, choose one of the following:

9.3. Verify InGenius Connector Enterprise

From an agent PC, launch an Internet browser window and enter the Salesforce URL. Log in with the appropriate Salesforce user credentials.

A screenshot of the Salesforce login page. At the top center is the Salesforce logo, which consists of a blue cloud shape with the word "salesforce" in white lowercase letters. Below the logo is a white rectangular login form with a light gray border. Inside the form, there are two input fields: the first is labeled "Username" and contains the text "agent1@ingcert1.com"; the second is labeled "Password" and contains a series of black dots. Below the password field is a blue rectangular button with the text "Log In" in white. Underneath the button is a checkbox labeled "Remember me". At the bottom of the form is a link that says "Forgot Your Password?".

salesforce

Username

agent1@ingcert1.com

Password

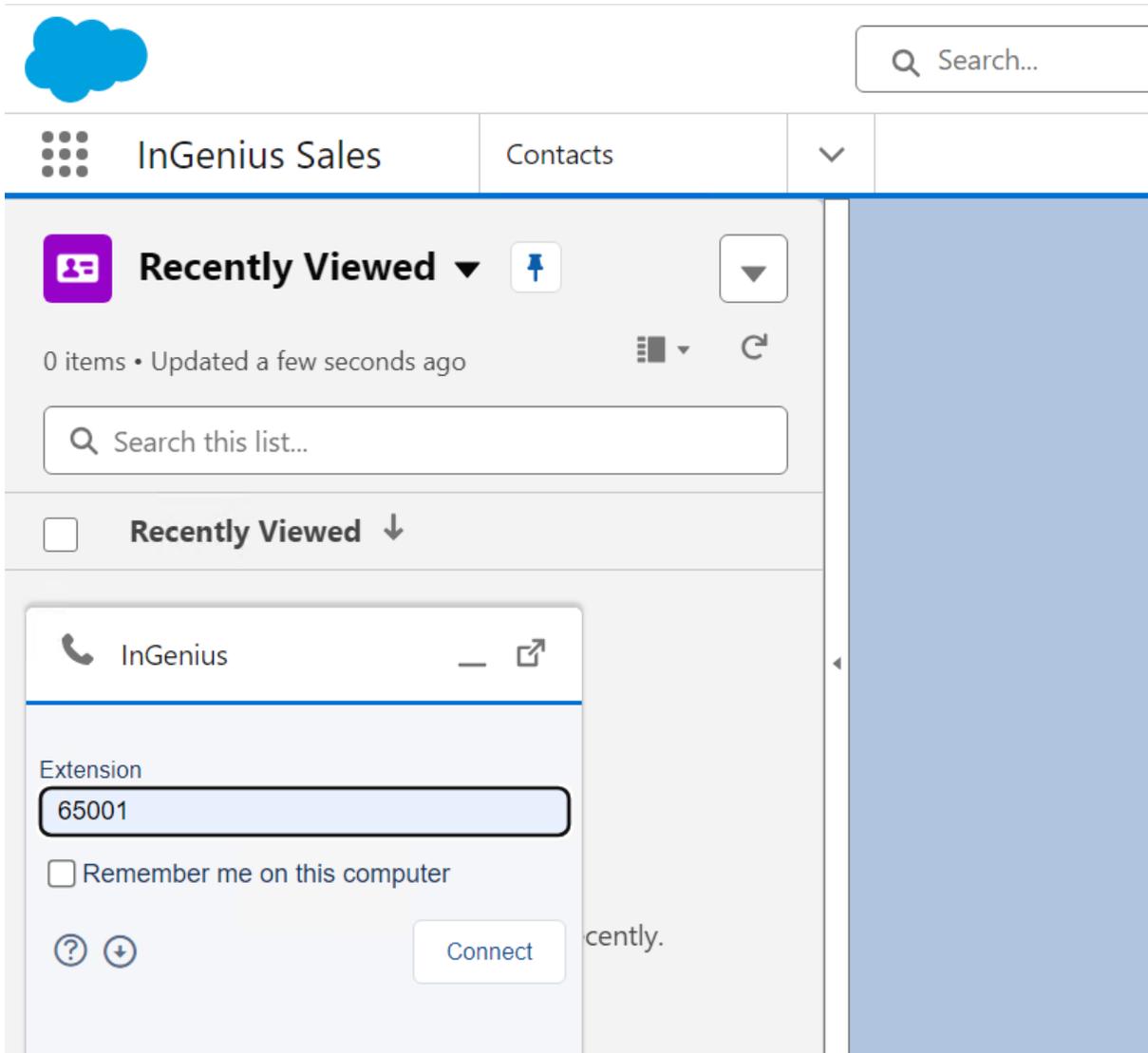
.....

Log In

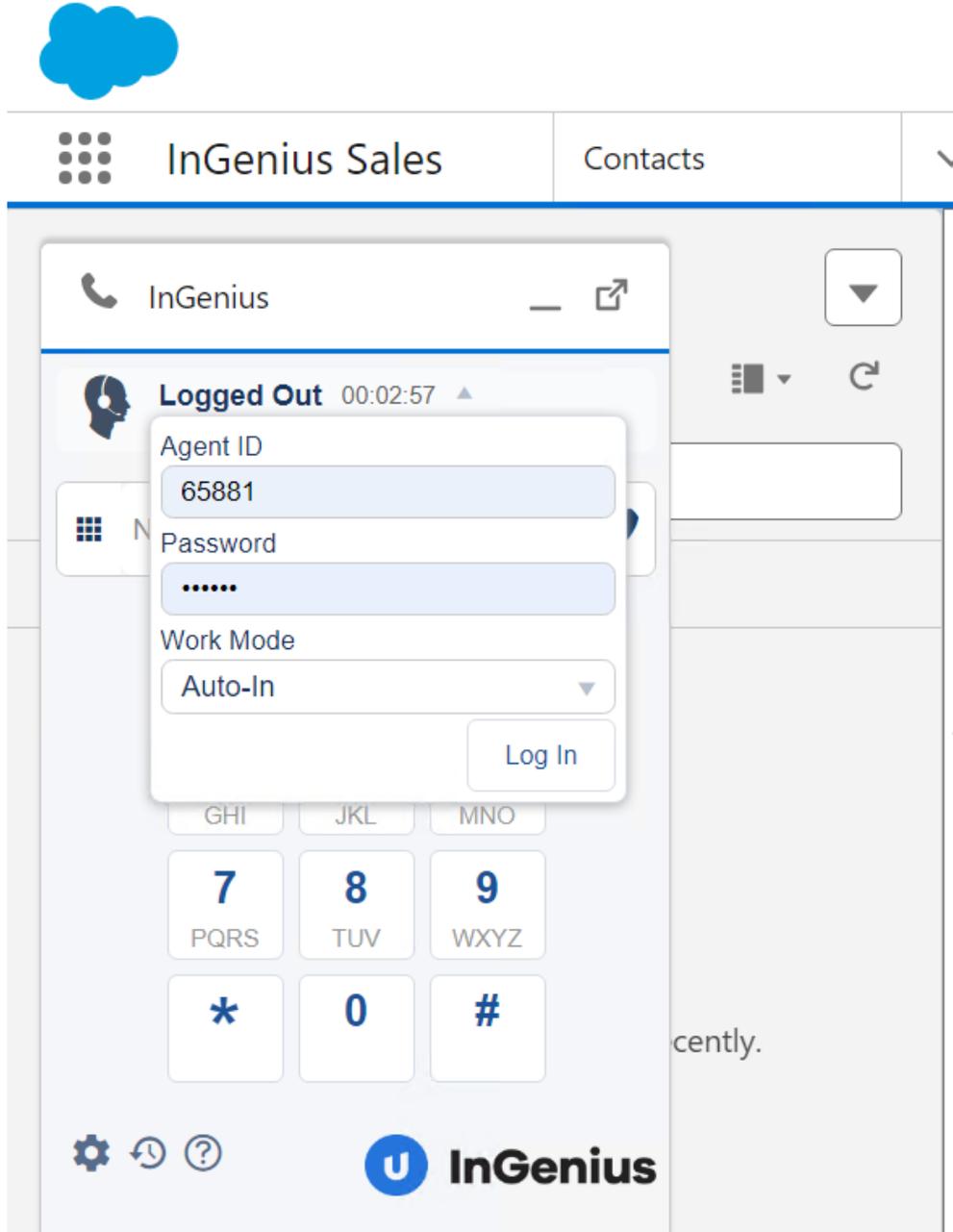
Remember me

[Forgot Your Password?](#)

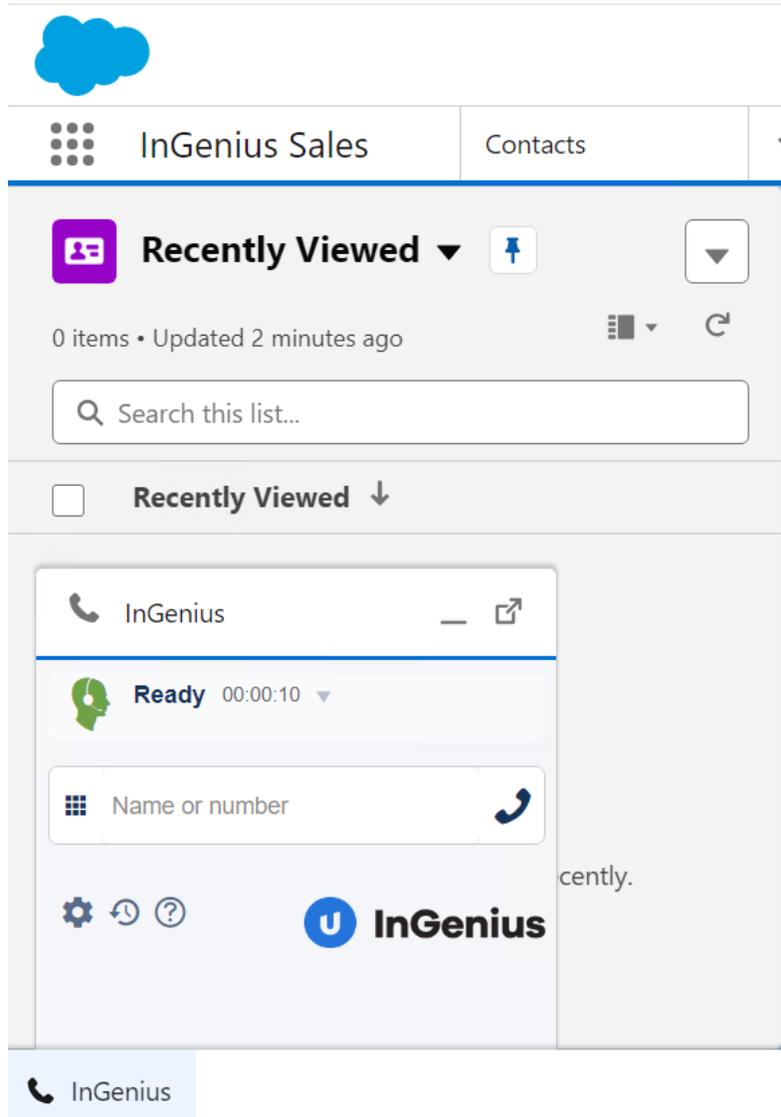
The screen below is displayed next. Select the phone icon from the top menu to display the **InGenius** floating screen shown below. Enter the relevant agent station extension from **Section Error! Reference source not found.**, and click **Connect**.



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 Error! Reference source not found.** For **Work Mode**, select the desired work mode, in this case *Auto-In*. Click **Log in**.

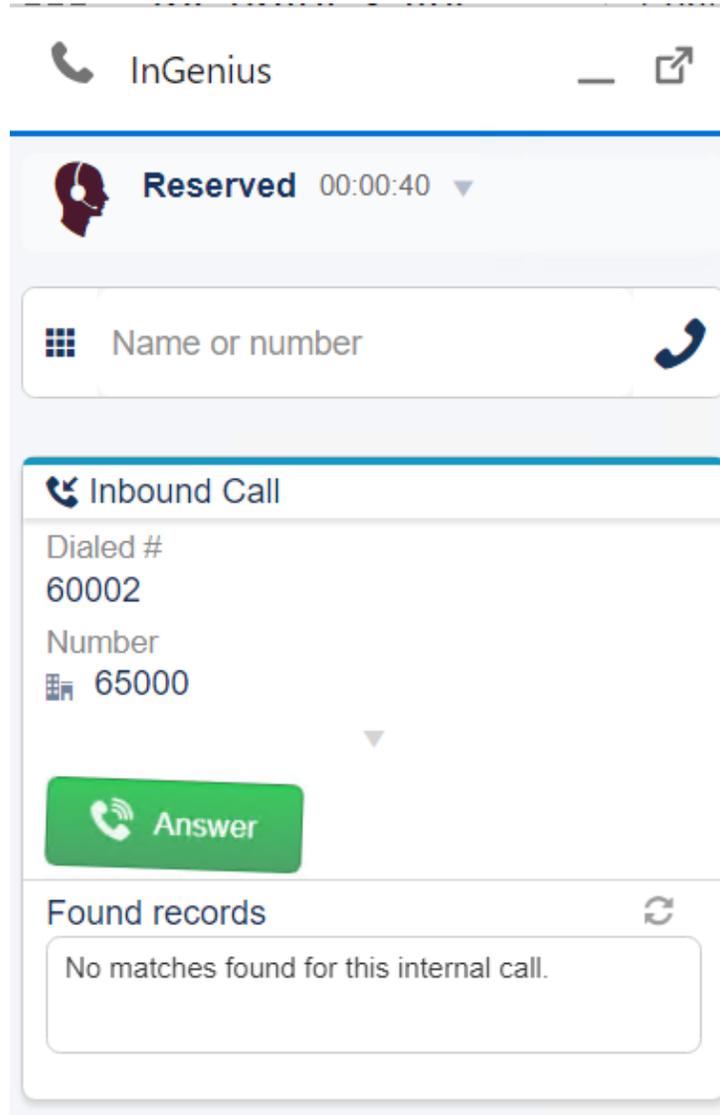


Verify that the **InGenius** screen is updated, showing the agent in the **Ready** state.

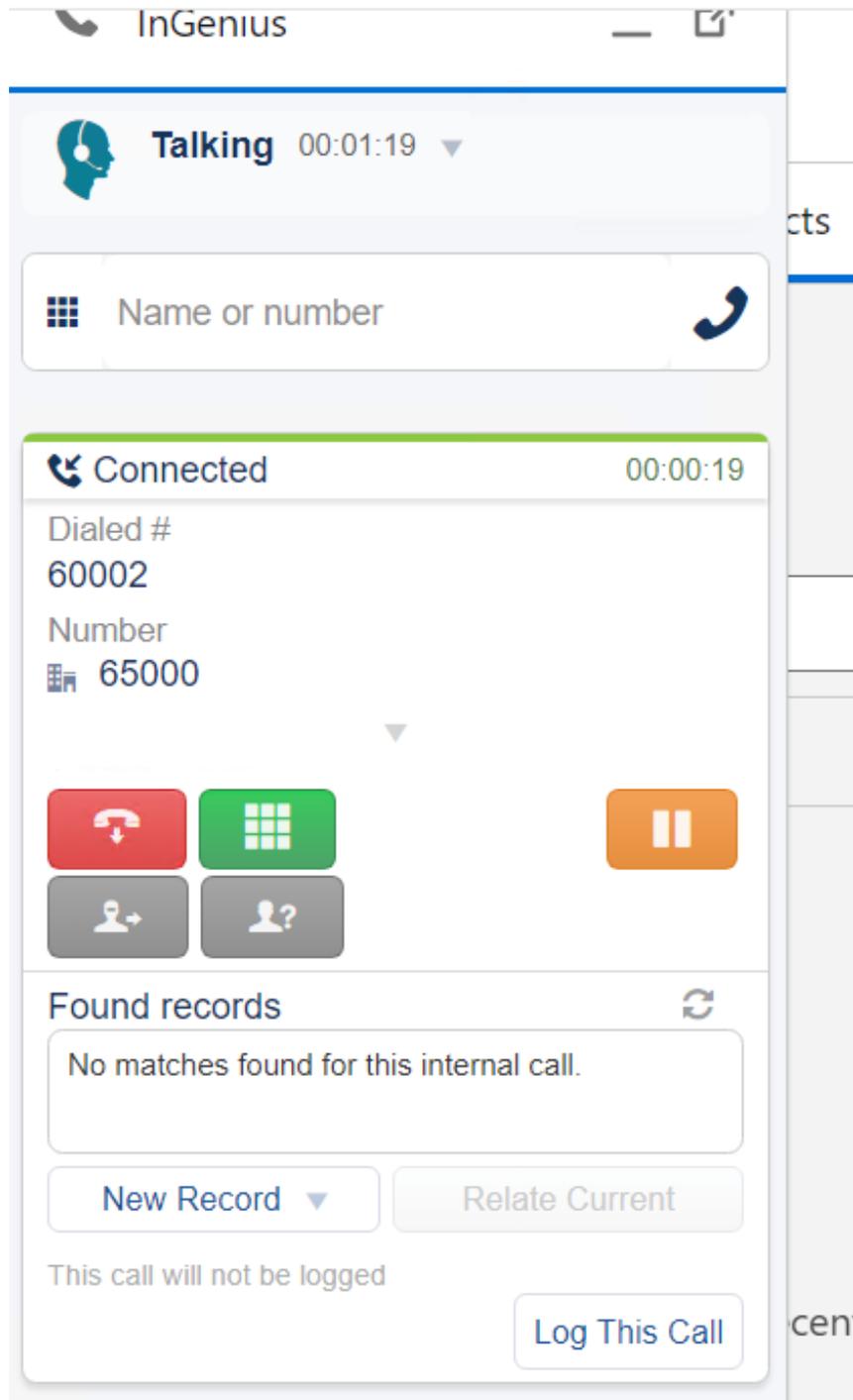


Make an incoming ACD call. Verify that the **InGenius** screen for the available agent is updated to reflect **Reserved** and **Inbound Call**, along with proper call information. Also verify that the background window is populated with the uniquely matching contact record associated with the caller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

Click **Answer** in the **InGenius** screen.



Verify that the agent is connected to the 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 Connect 2023 R1.0 with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. InGenius Connect 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 10.1.x, Issue 6, May 2023, available at <http://support.avaya.com>.
2. *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 7, May 2023, available at <http://support.avaya.com>.
3. *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 6, May 2023, available at <http://support.avaya.com>.

©2024 Avaya LLC All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya LLC. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya LLC. 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.