Avaya Solution & Interoperability Test Lab

Application Notes for Upland InGenius Connect for Salesforce 2022 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 Upland InGenius Connect for Salesforce with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Upland 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 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 Upland InGenius Connect for Salesforce 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 for Salesforce.

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	77550
Skill Group	77500
Agent Stations	78004, 77301
Agent IDs	76301, 76302

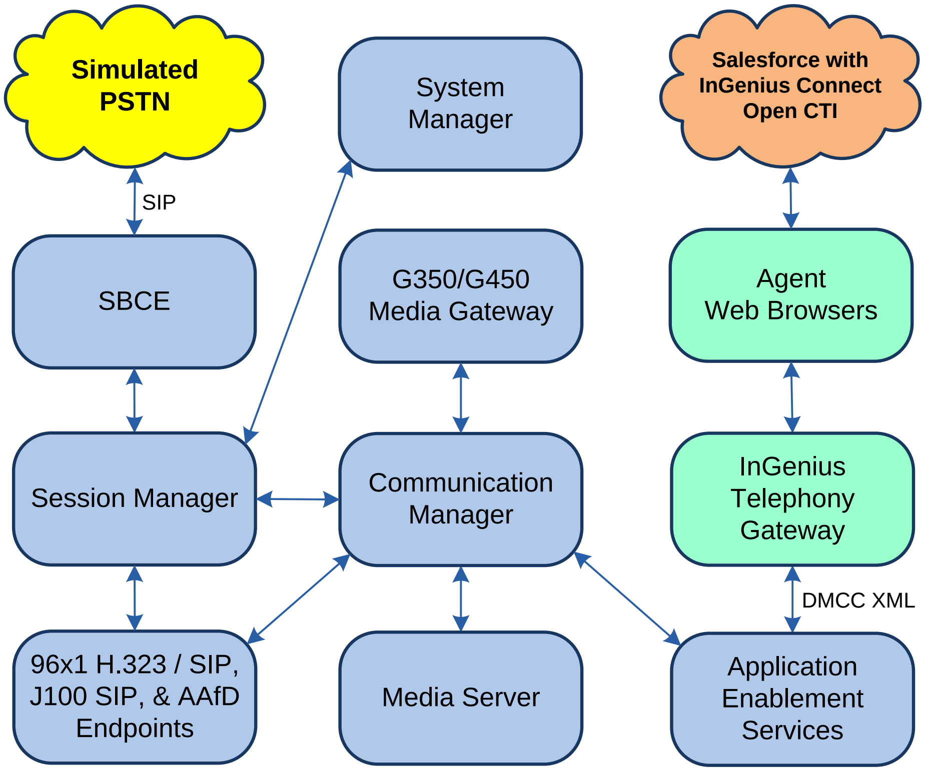

Simulated PSTN
System Manager
Salesforce with InGenius Connect Open CTI
SIP
SBCE
G350/G450 Media Gateway
Agent Web Browsers
Session Manager
Communication Manager
InGenius Telephony Gateway
DMCC XML
96x1 H.323 / SIP, J100 SIP, & AAfD Endpoints
Media Server
Application Enablement Services

Figure 1: Upland InGenius Connect for Salesforce 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	10.1.0.1.0-SP1
Avaya G350 Media Gateway	FW 42.4.0
Avaya G450 Media Gateway	FW 42.7.0
Avaya Aura® Media Server	10.1.0.77
Avaya Aura® Application Enablement Services	10.1.0.1.0.7-0
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.0614394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series Deskphones	6.8.5.3.2 (H.323) 7.1.13.0.4 (SIP)
Avaya J100 Series Deskphones	4.0.13.0.6
Avaya Agent for Desktop	2.0.6.0.10 (SIP)
Upland InGenius Connect for Salesforce, including: ▪ InGenius Telephony Gateway on Windows Server 2019 ▪ InGenius Connect Apex Package for Salesforce	2022 R1.0

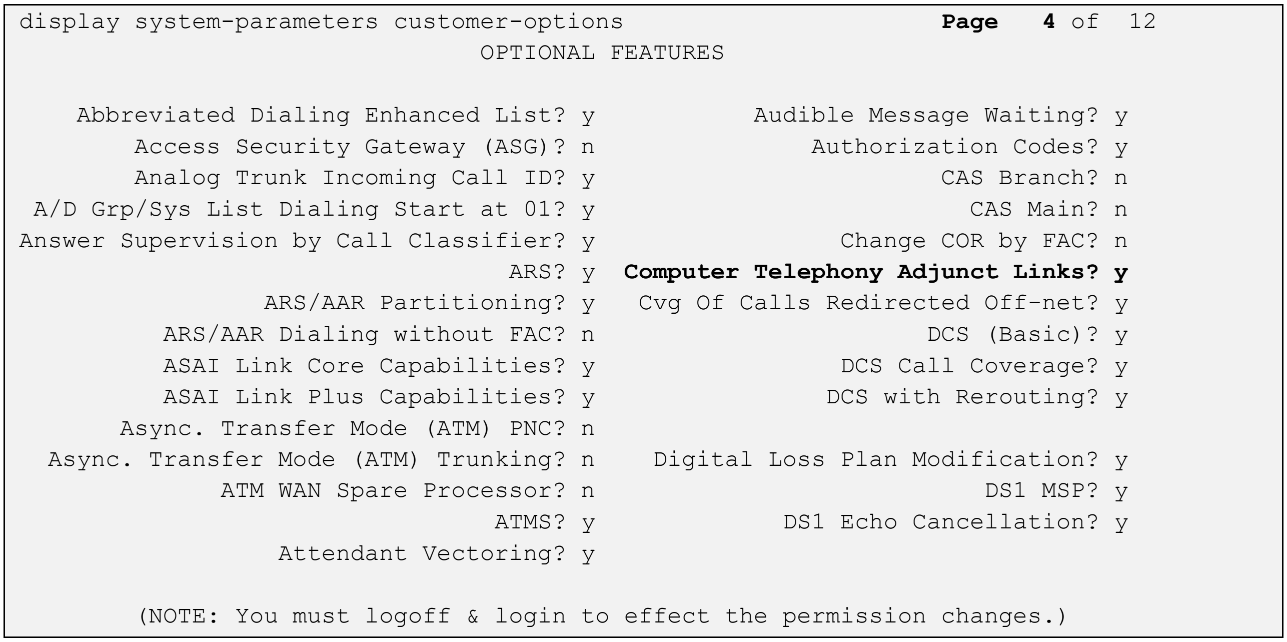
5. Configure Avaya Aura® Communication Manager

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: 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 InGenius Connect.

```
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:
```

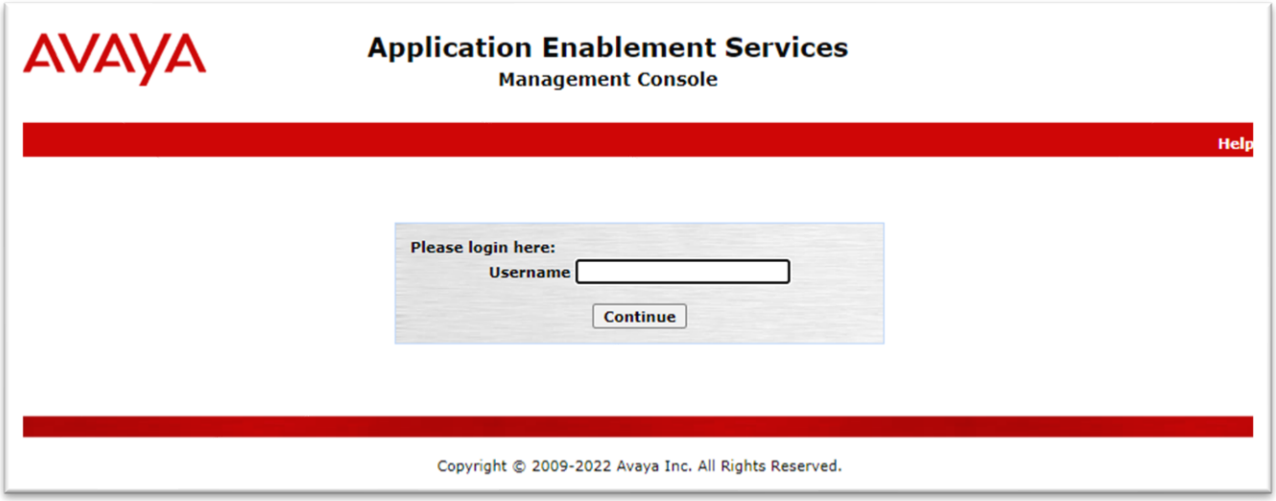
6. Configure Avaya Aura® Application Enablement Services

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

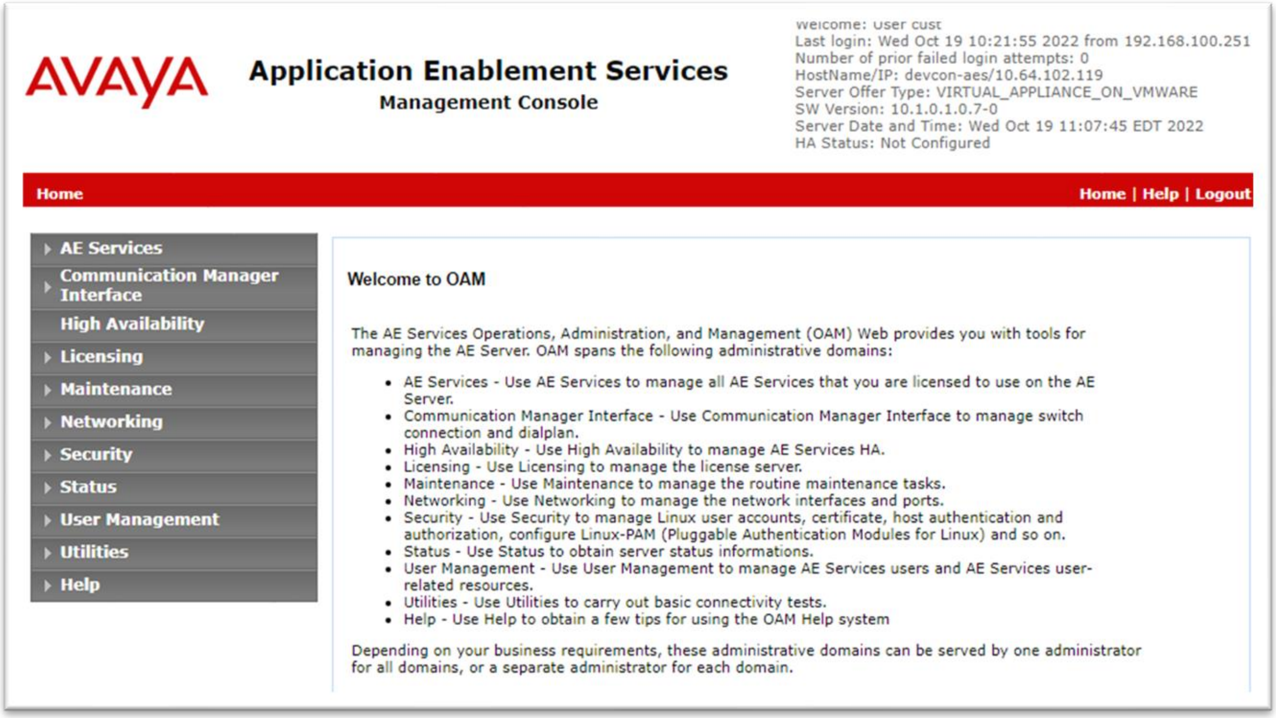
- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer InGenius user
- Administer security database
- Administer ports
- Restart services

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


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Continue
Copyright © 2009-2022 Avaya Inc. All Rights Reserved.

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



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:07:45 EDT 2022
HA Status: Not Configured

Welcome to OAM

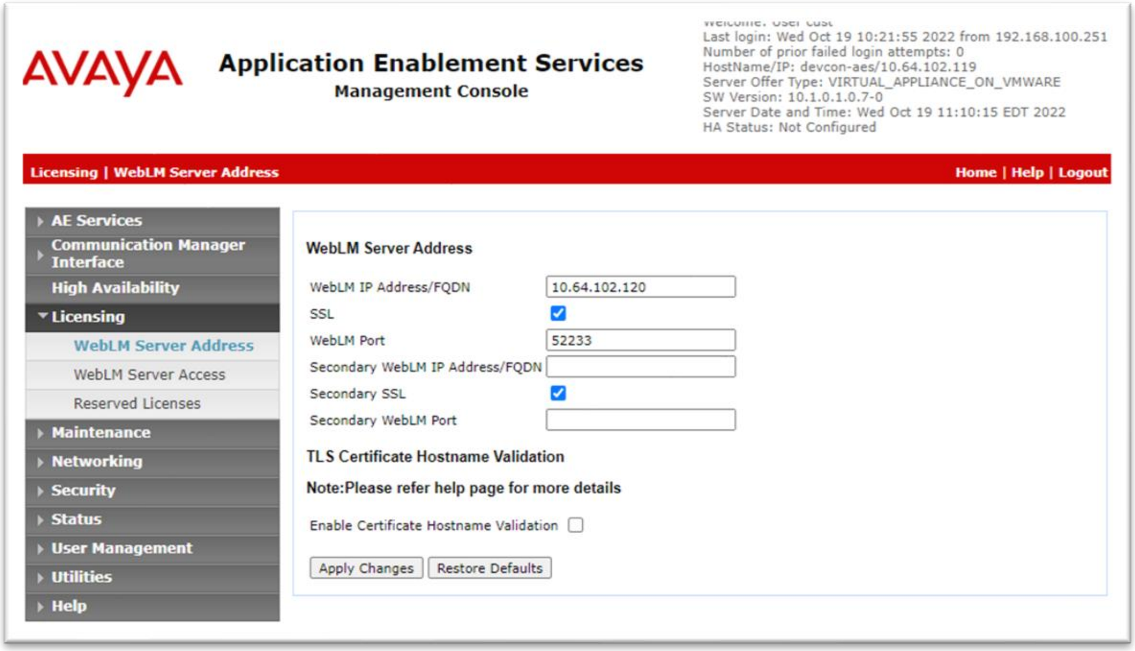
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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 Address** in the left pane to display the applicable WebLM IP address. Log into WebLM using the appropriate credentials.



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:10:15 EDT 2022
HA Status: Not Configured

WebLM Server Address

WebLM IP Address/FQDN	10.64.102.120
SSL	☑
WebLM Port	52233
Secondary WebLM IP Address/FQDN	
Secondary SSL	☑
Secondary WebLM Port	

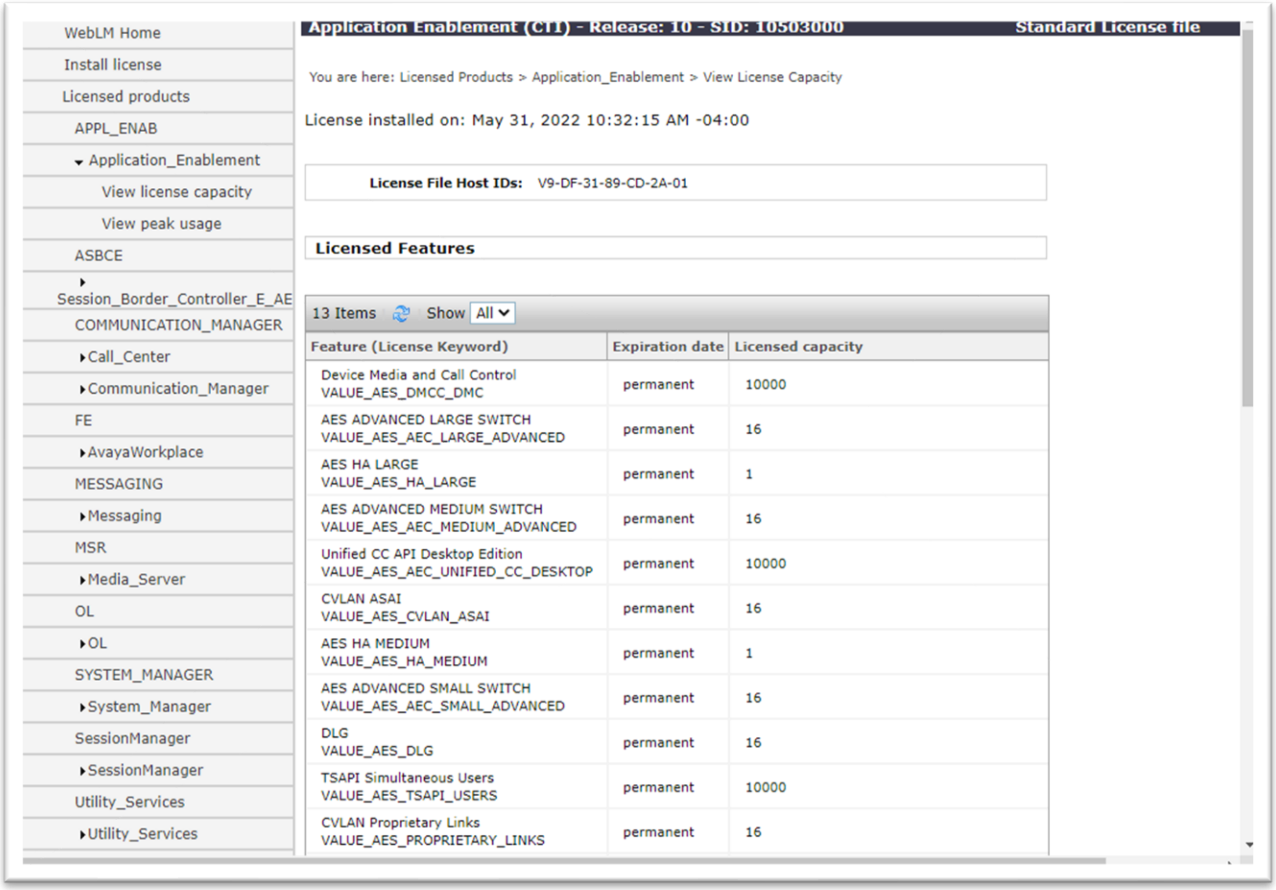
TLS Certificate Hostname Validation

Note:Please refer help page for more details

Enable Certificate Hostname Validation ☐

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 Standard License file

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

License installed on: May 31, 2022 10:32:15 AM -04:00

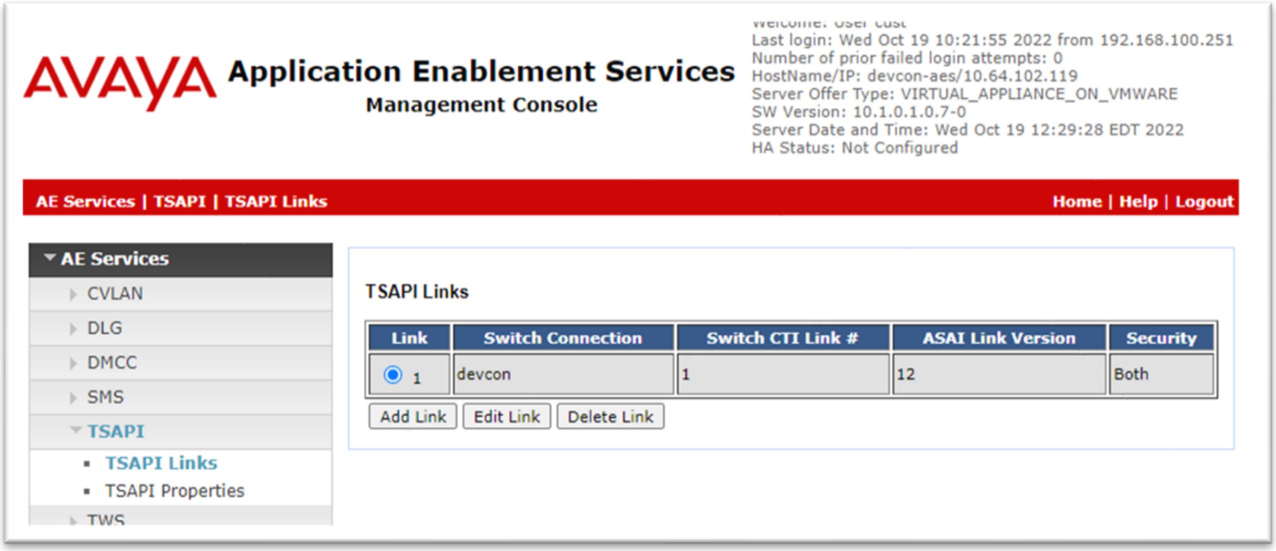
License File Host IDs: V9-DF-31-89-CD-2A-01

Licensed Features

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
CVLAN Proprietary Links VALUE_AES_PROPRIETARY_LINKS	permanent	16

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**.

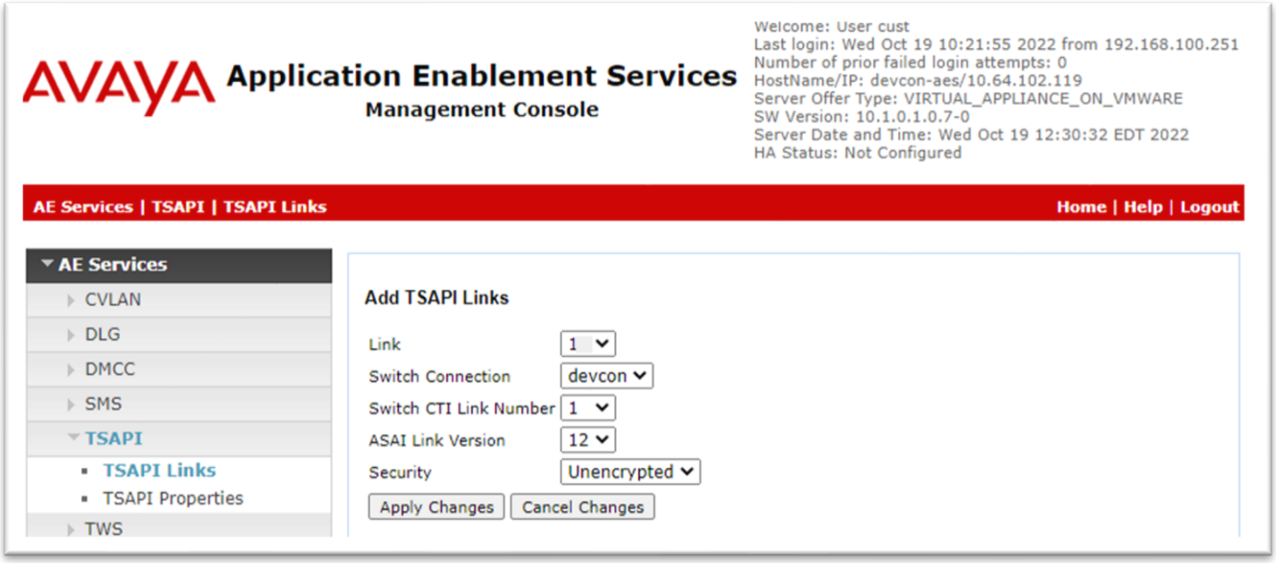


Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 12:29:28 EDT 2022
HA Status: Not Configured

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	devcon	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 *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.



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 12:30:32 EDT 2022
HA Status: Not Configured

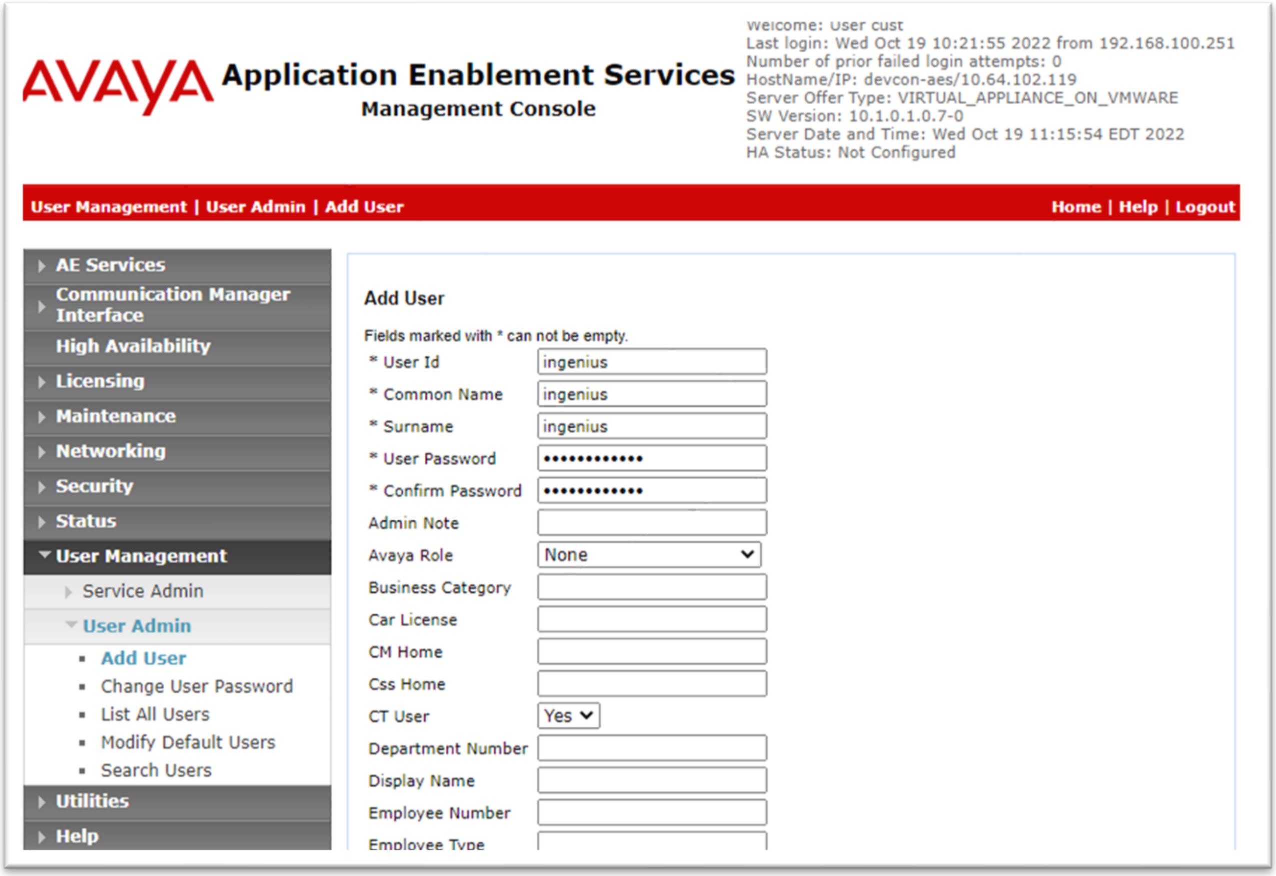
Add TSAPI Links

Link	1
Switch Connection	devcon
Switch CTI Link Number	1
ASAI Link Version	12
Security	Unencrypted

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.



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:15:54 EDT 2022
HA Status: Not Configured

Add User

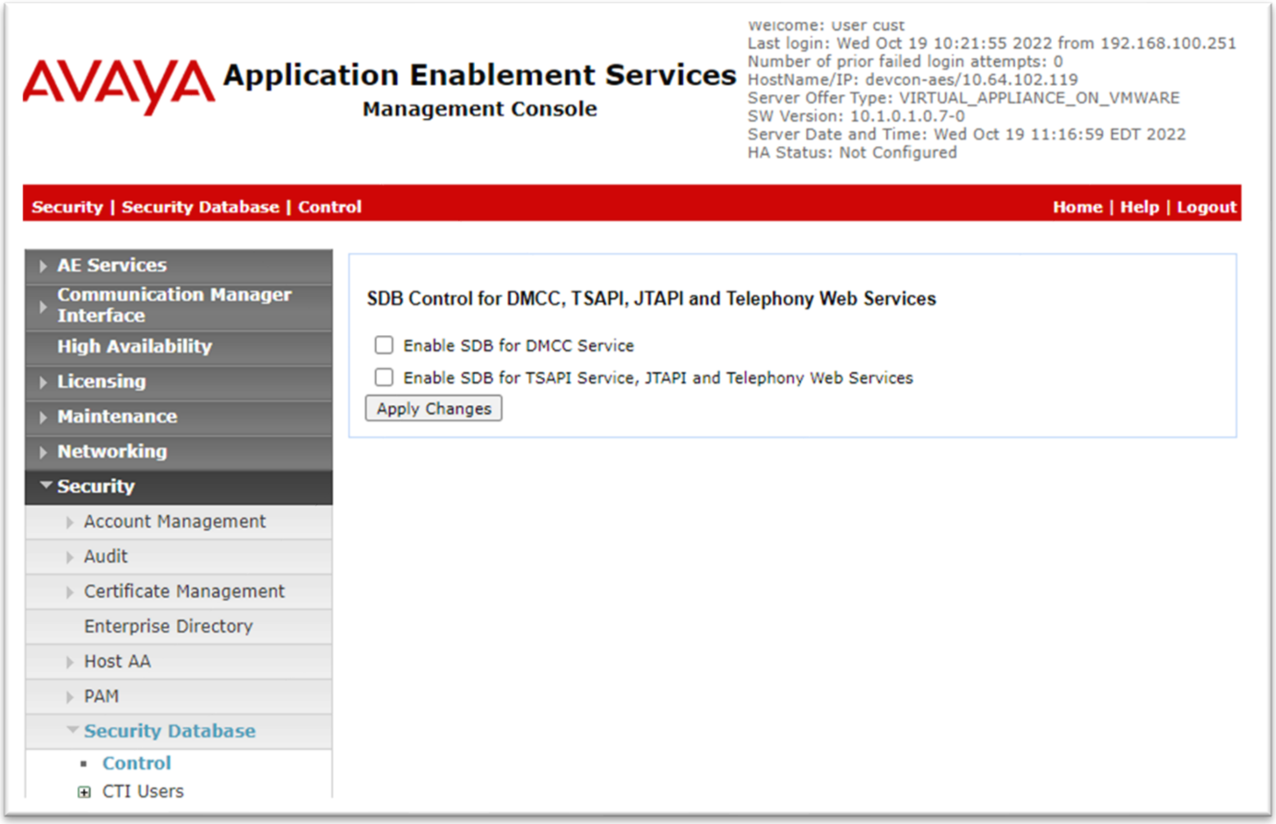
Fields marked with * can not be empty.

* User Id	ingenius
* Common Name	ingenius
* Surname	ingenius
* User Password	••••••••••••
* Confirm Password	••••••••••••
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	

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**.



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:16:59 EDT 2022
HA Status: Not Configured

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

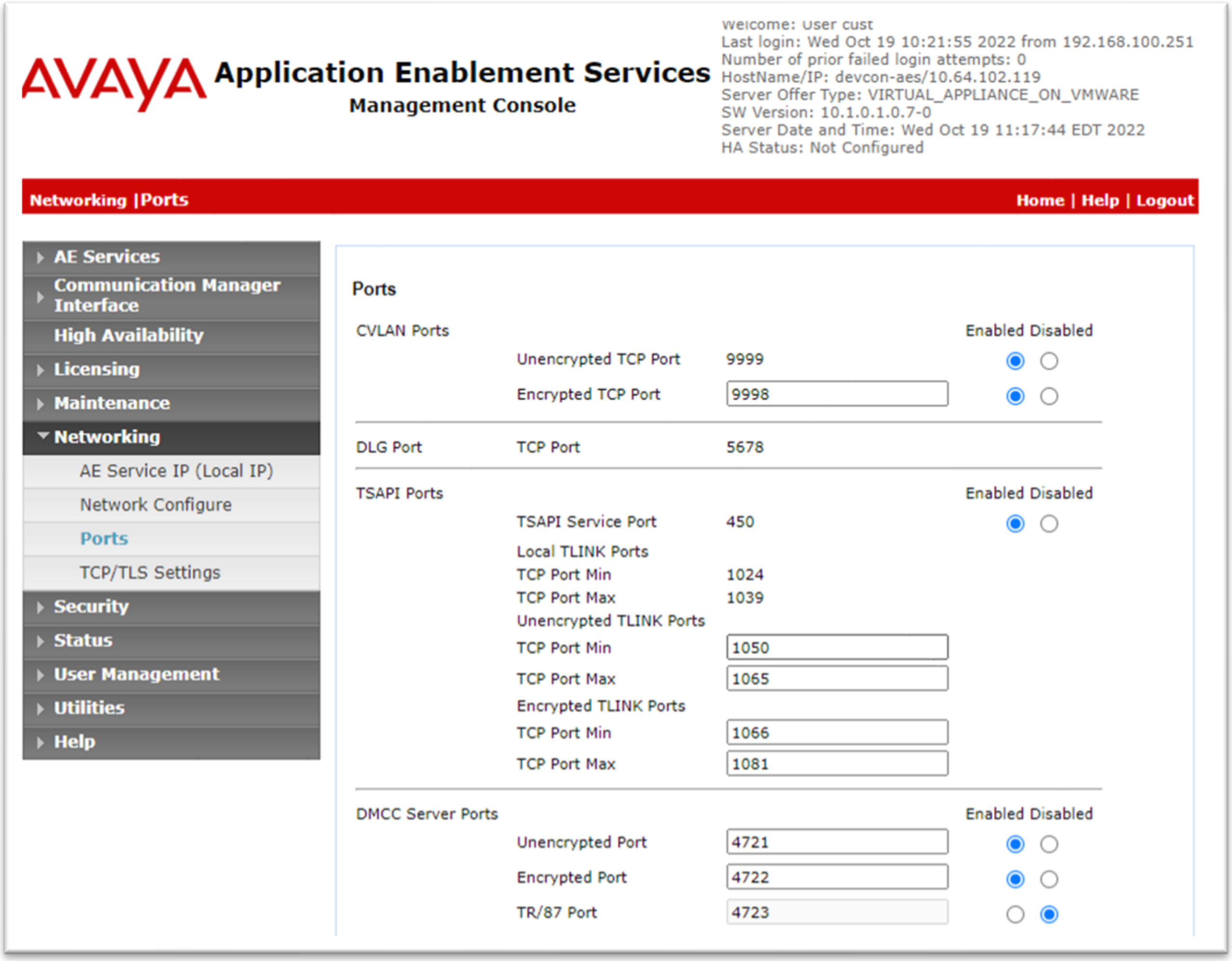
□ Enable SDB for DMCC Service

□ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

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.



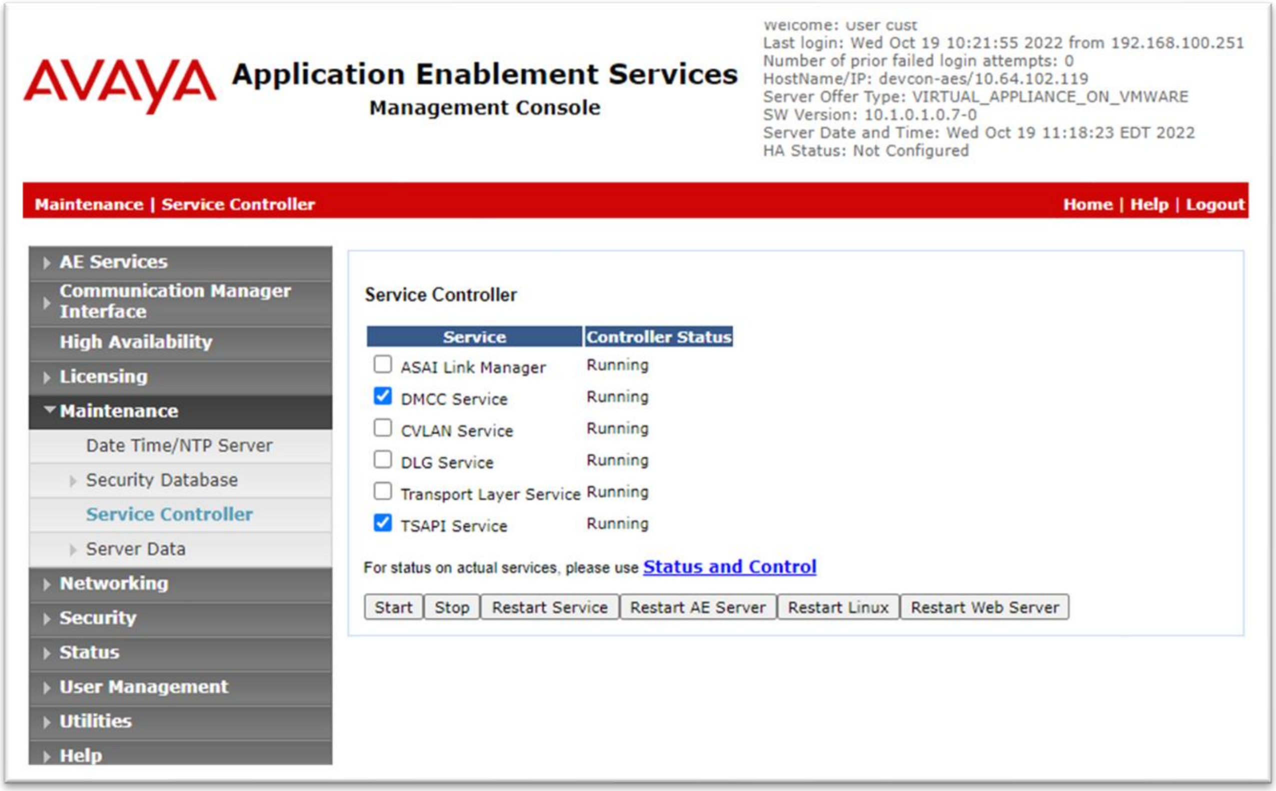
Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:17:44 EDT 2022
HA Status: Not Configured

Ports

			Enabled	Disabled
CVLAN Ports				
	Unencrypted TCP Port	9999	●	○
	Encrypted TCP Port	9998	●	○
DLG Port	TCP Port	5678		
TSAPI Ports				
	TSAPI Service Port	450	●	○
	Local TLINK Ports			
	TCP Port Min	1024		
	TCP Port Max	1039		
	Unencrypted TLINK Ports			
	TCP Port Min	1050		
	TCP Port Max	1065		
	Encrypted TLINK Ports			
	TCP Port Min	1066		
	TCP Port Max	1081		
DMCC Server Ports				
	Unencrypted Port	4721	●	○
	Encrypted Port	4722	●	○
	TR/87 Port	4723	○	●

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**.



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:18:23 EDT 2022
HA Status: Not Configured

Service Controller

Service	Controller Status
□ ASAI Link Manager	Running
☑ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

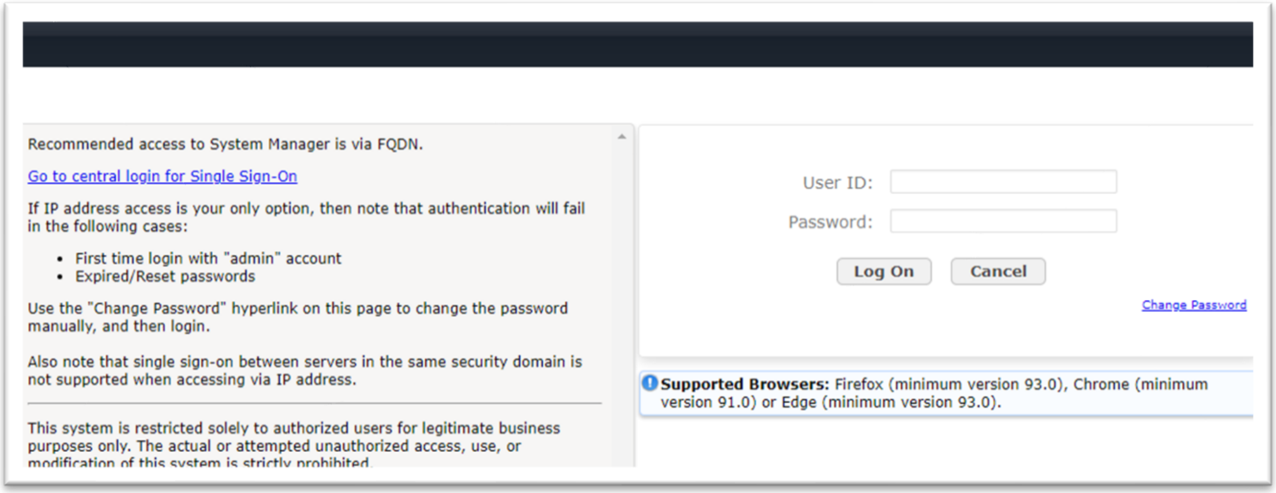
7. Configure Avaya Aura® Session Manager

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

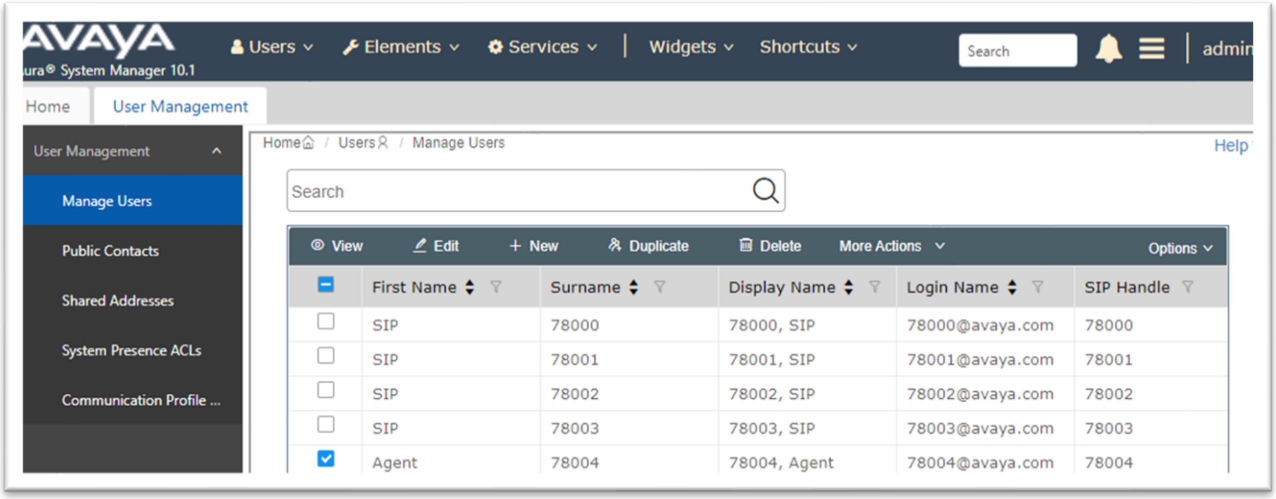
User ID:

Password:

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

7.2. Administer Users

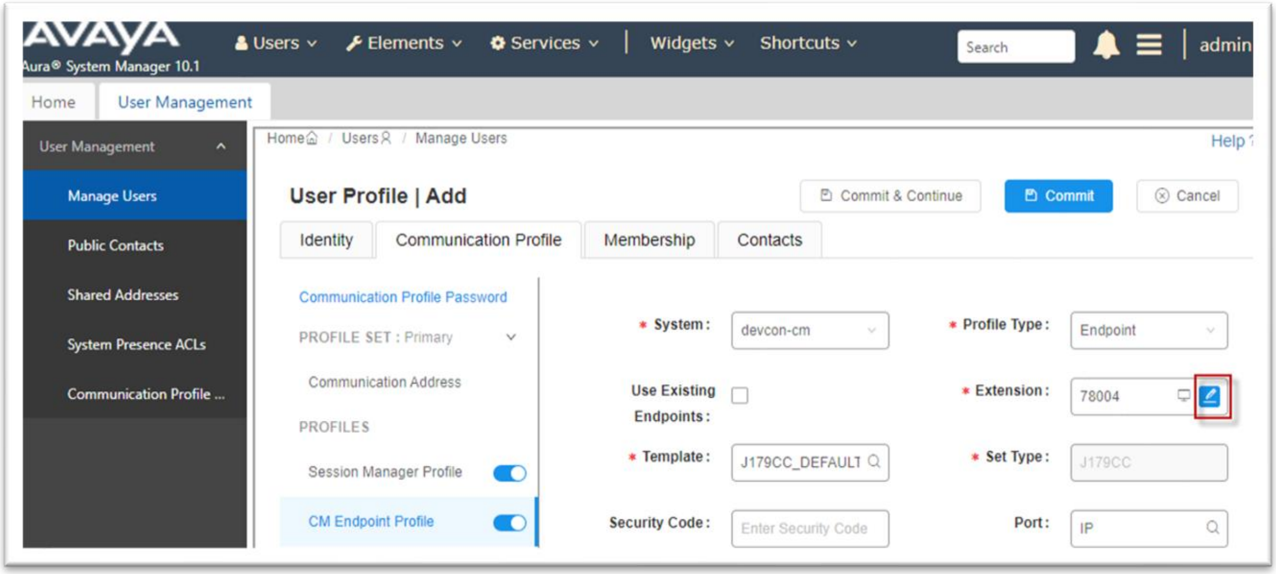
In the subsequent screen (not shown), select **Users → User Management**. Select **User Management → Manage Users** from the left pane to display the **User Management** screen below. Select the entry associated with the SIP agent station from **Section 3**, in this case *78004*, and click **Edit**.



	First Name	Surname	Display Name	Login Name	SIP Handle
□	SIP	78000	78000, SIP	78000@avaya.com	78000
□	SIP	78001	78001, SIP	78001@avaya.com	78001
□	SIP	78002	78002, SIP	78002@avaya.com	78002
□	SIP	78003	78003, SIP	78003@avaya.com	78003
☑	Agent	78004	78004, Agent	78004@avaya.com	78004

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**.



* System : devcon-cm

* Profile Type : Endpoint

Use Existing Endpoints : □

* Extension : 78004

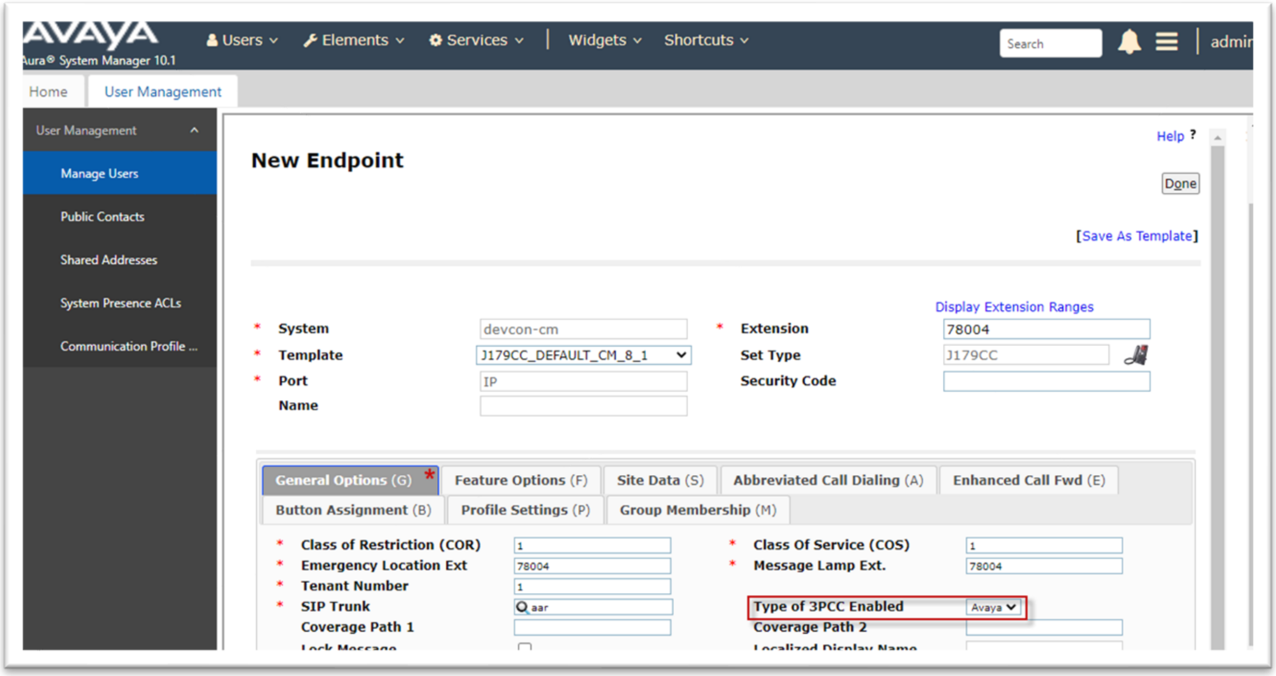
* Template : J179CC_DEFAULT

* Set Type : J179CC

Security Code : Enter Security Code

Port : IP

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.



New Endpoint

* System	devcon-cm	* Extension	78004
* Template	J179CC_DEFAULT_CM_8_1	Set Type	J179CC
* Port	IP	Security Code	
Name			

* Class of Restriction (COR)	1	* Class Of Service (COS)	1
* Emergency Location Ext	78004	* Message Lamp Ext.	78004
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	

8. Configure Upland InGenius Connect

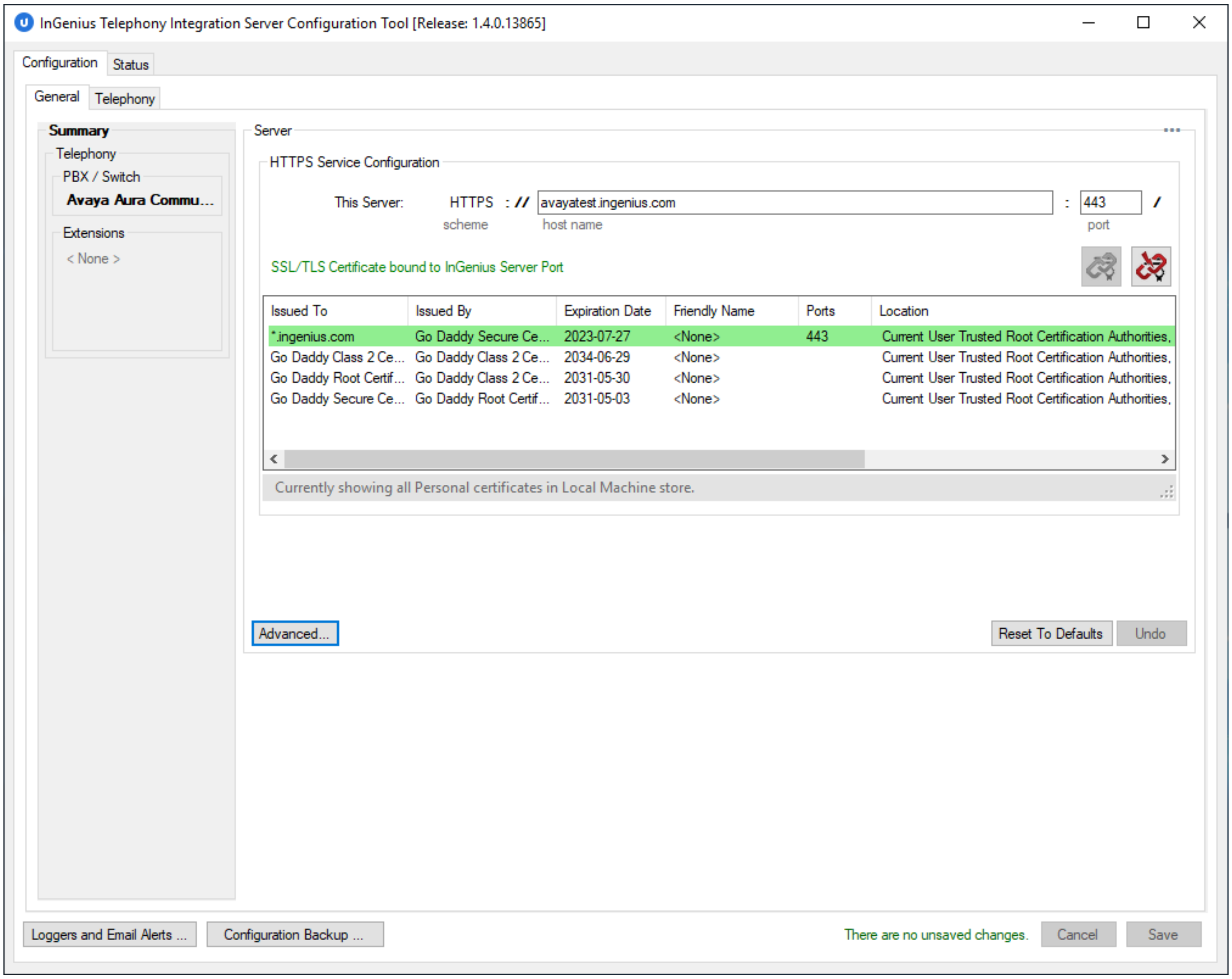
This section provides the procedures for configuring InGenius Connect. The procedures include the following areas:

- 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.



InGenius Telephony Integration Server Configuration Tool [Release: 1.4.0.13865]

This Server: HTTPS :// avayatest.ingenius.com : 443 /
scheme host name port

SSL/TLS Certificate bound to InGenius Server Port

Issued To	Issued By	Expiration Date	Friendly Name	Ports	Location
*.ingenius.com	Go Daddy Secure Ce...	2023-07-27	<None>	443	Current User Trusted Root Certification Authorities,
Go Daddy Class 2 Ce...	Go Daddy Class 2 Ce...	2034-06-29	<None>		Current User Trusted Root Certification Authorities,
Go Daddy Root Certif...	Go Daddy Class 2 Ce...	2031-05-30	<None>		Current User Trusted Root Certification Authorities,
Go Daddy Secure Ce...	Go Daddy Root Certif...	2031-05-03	<None>		Current User Trusted Root Certification Authorities,

Currently showing all Personal certificates in Local Machine store.

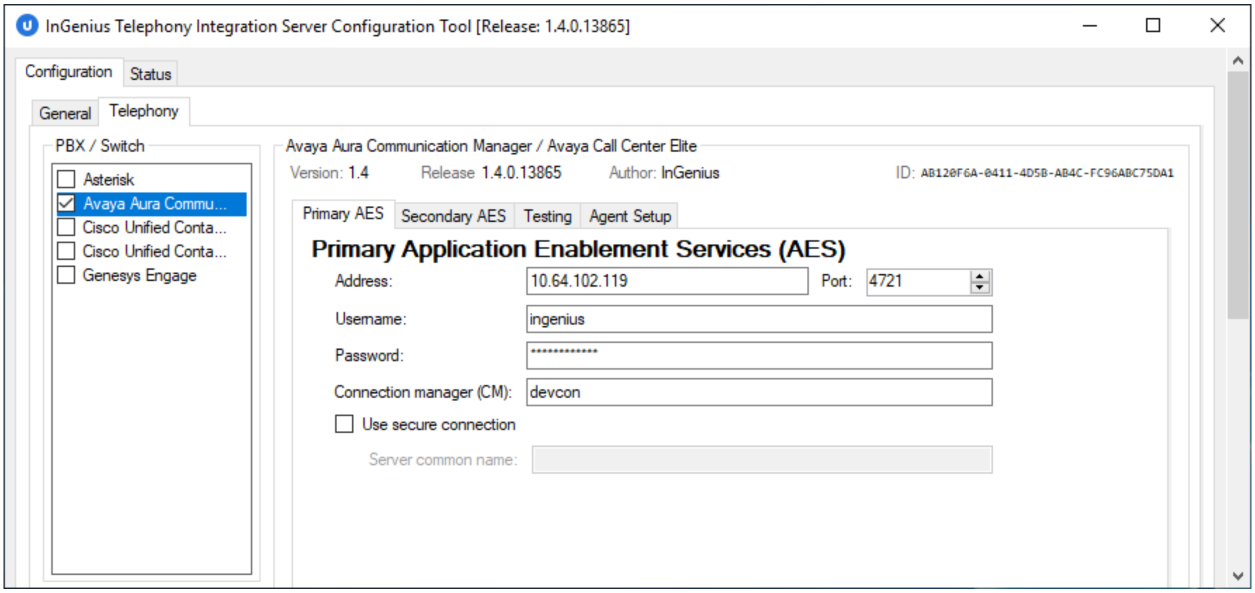
There are no unsaved changes.

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 6.3**.


InGenius Telephony Integration Server Configuration Tool [Release: 1.4.0.13865]

☐ Asterisk
☑ Avaya Aura Commu...
☐ Cisco Unified Conta...
☐ Cisco Unified Conta...
☐ Genesys Engage

Avaya Aura Communication Manager / Avaya Call Center Elite

Version: 1.4 Release 1.4.0.13865 Author: InGenius ID: AB120F6A-0411-4D5B-AB4C-FC96ABC75DA1

Primary Application Enablement Services (AES)

Address: 10.64.102.119 Port: 4721

Username: ingenius

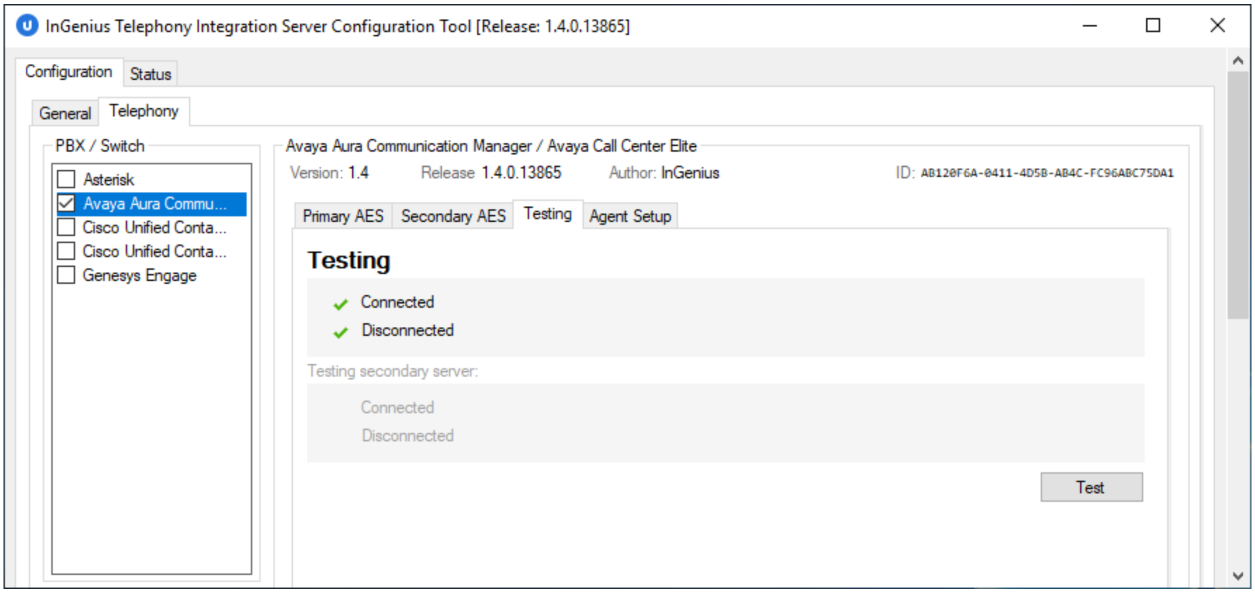
Password: ************

Connection manager (CM): devcon

☐ Use secure connection

Server common name:

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


InGenius Telephony Integration Server Configuration Tool [Release: 1.4.0.13865]
Configuration
Status
General
Telephony
PBX / Switch
Avaya Aura Communication Manager / Avaya Call Center Elite
Primary AES
Secondary AES
Testing
Agent Setup
Test

□ Asterisk
☑ Avaya Aura Commu...
□ Cisco Unified Conta...
□ Cisco Unified Conta...
□ Genesys Engage

Version: 1.4 Release 1.4.0.13865 Author: InGenius ID: AB120F6A-0411-4D5B-AB4C-FC96ABC75DA1

Testing

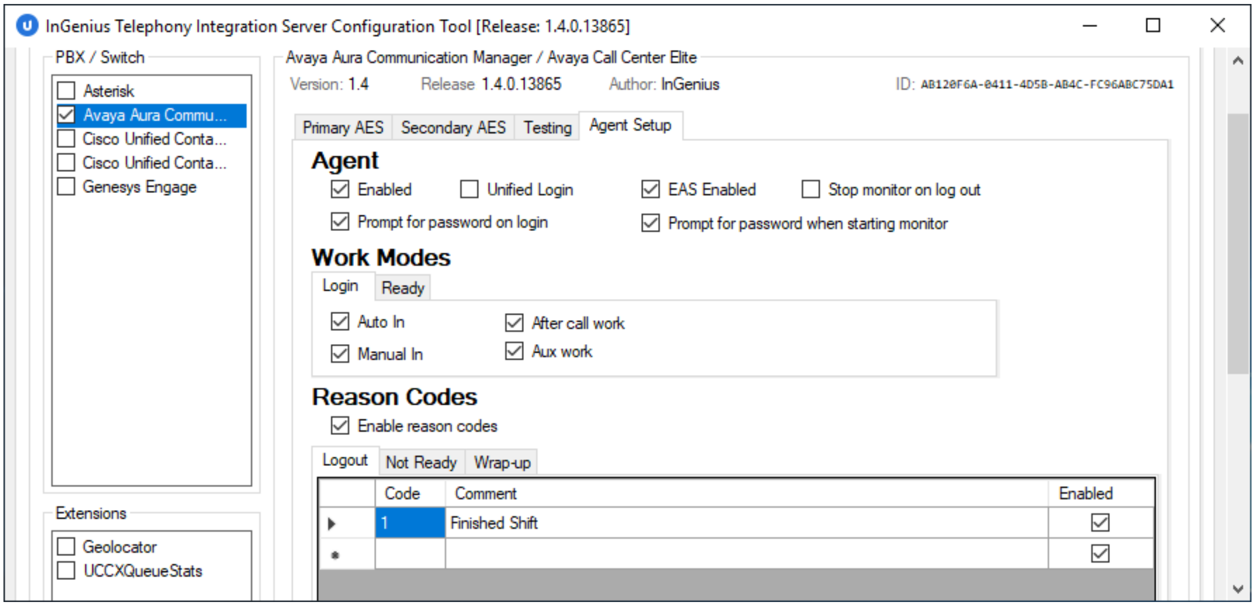
✓ Connected
✓ Disconnected

Testing secondary server:

Connected
Disconnected

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.


InGenius Telephony Integration Server Configuration Tool [Release: 1.4.0.13865]
PBX / Switch
Primary AES
Secondary AES
Testing
Agent Setup
Extensions

PBX / Switch:
☐ Asterisk
☑ Avaya Aura Commu...
☐ Cisco Unified Conta...
☐ Cisco Unified Conta...
☐ Genesys Engage

Extensions:
☐ Geolocator
☐ UCCXQueueStats

Avaya Aura Communication Manager / Avaya Call Center Elite
Version: 1.4 Release 1.4.0.13865 Author: InGenius ID: AB120F6A-0411-4D5B-AB4C-FC96ABC75DA1

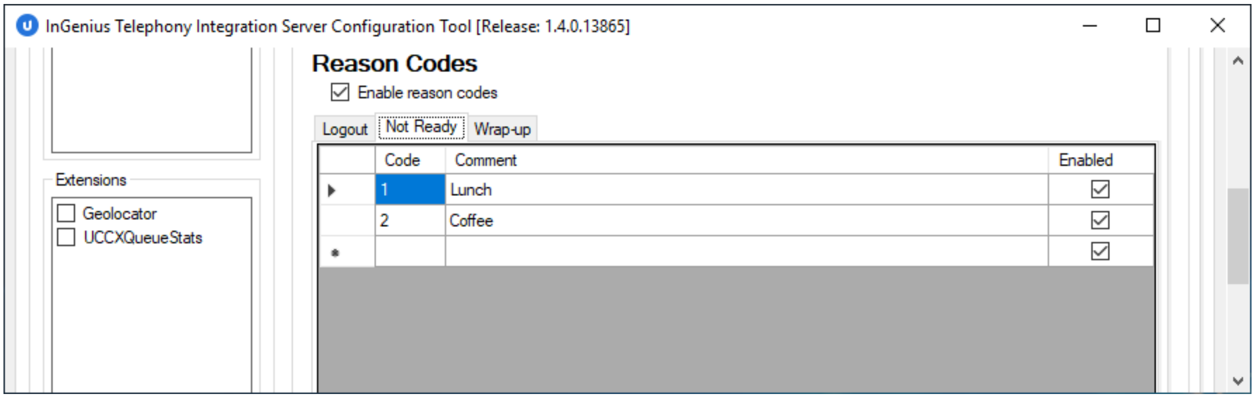
Agent
☑ Enabled ☐ Unified Login ☑ EAS Enabled ☐ Stop monitor on log out
☑ Prompt for password on login ☑ Prompt for password when starting monitor

Work Modes
Login | Ready
☑ Auto In ☑ After call work
☑ Manual In ☑ Aux work

Reason Codes
☑ Enable reason codes
Logout | Not Ready | Wrap-up

	Code	Comment	Enabled
▶	1	Finished Shift	☑
*			☑

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


InGenius Telephony Integration Server Configuration Tool [Release: 1.4.0.13865]
Extensions

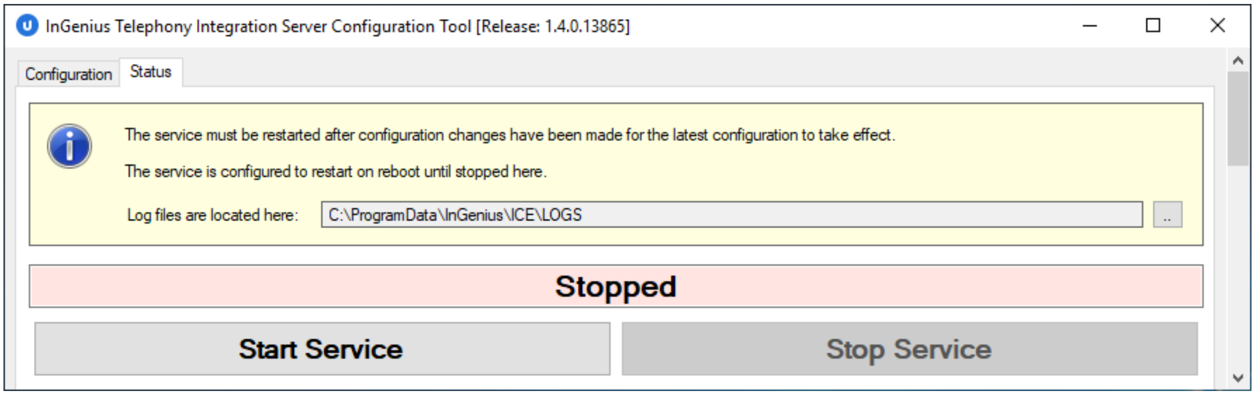
Extensions:
☐ Geolocator
☐ UCCXQueueStats

Reason Codes
☑ Enable reason codes
Logout | Not Ready | Wrap-up

	Code	Comment	Enabled
▶	1	Lunch	☑
	2	Coffee	☑
*			☑

8.3. Start Service

Select **Status** from the top menu to display the screen below, and click **Start Service**.


InGenius Telephony Integration Server Configuration Tool [Release: 1.4.0.13865]
Configuration
Status

The service must be restarted after configuration changes have been made for the latest configuration to take effect.

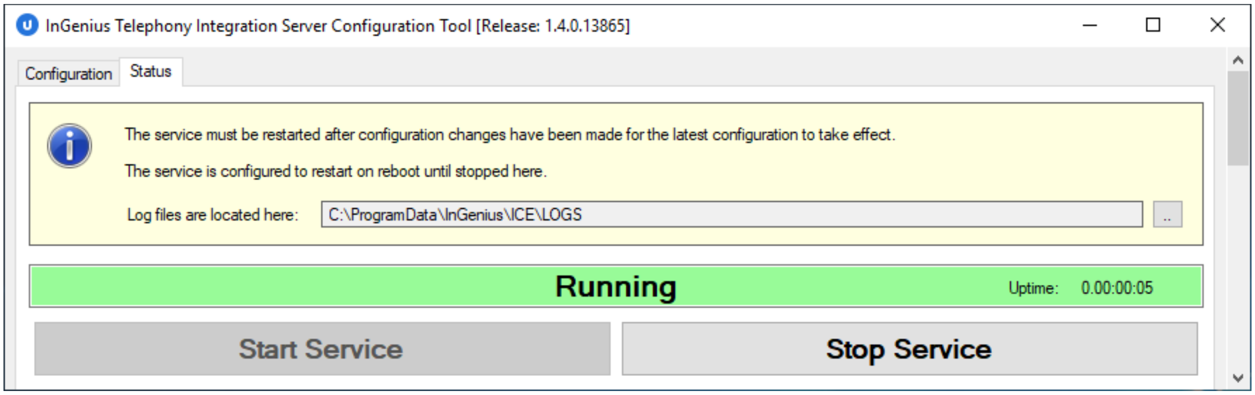
The service is configured to restart on reboot until stopped here.

Log files are located here: C:\ProgramData\InGenius\ICE\LOGS

Stopped

Start Service
Stop Service

The screen is updated, as shown below.


InGenius Telephony Integration Server Configuration Tool [Release: 1.4.0.13865]
Configuration
Status

The service must be restarted after configuration changes have been made for the latest configuration to take effect.

The service is configured to restart on reboot until stopped here.

Log files are located here: C:\ProgramData\InGenius\ICE\LOGS

Running Uptime: 0.00:00:05

Start Service
Stop Service

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.

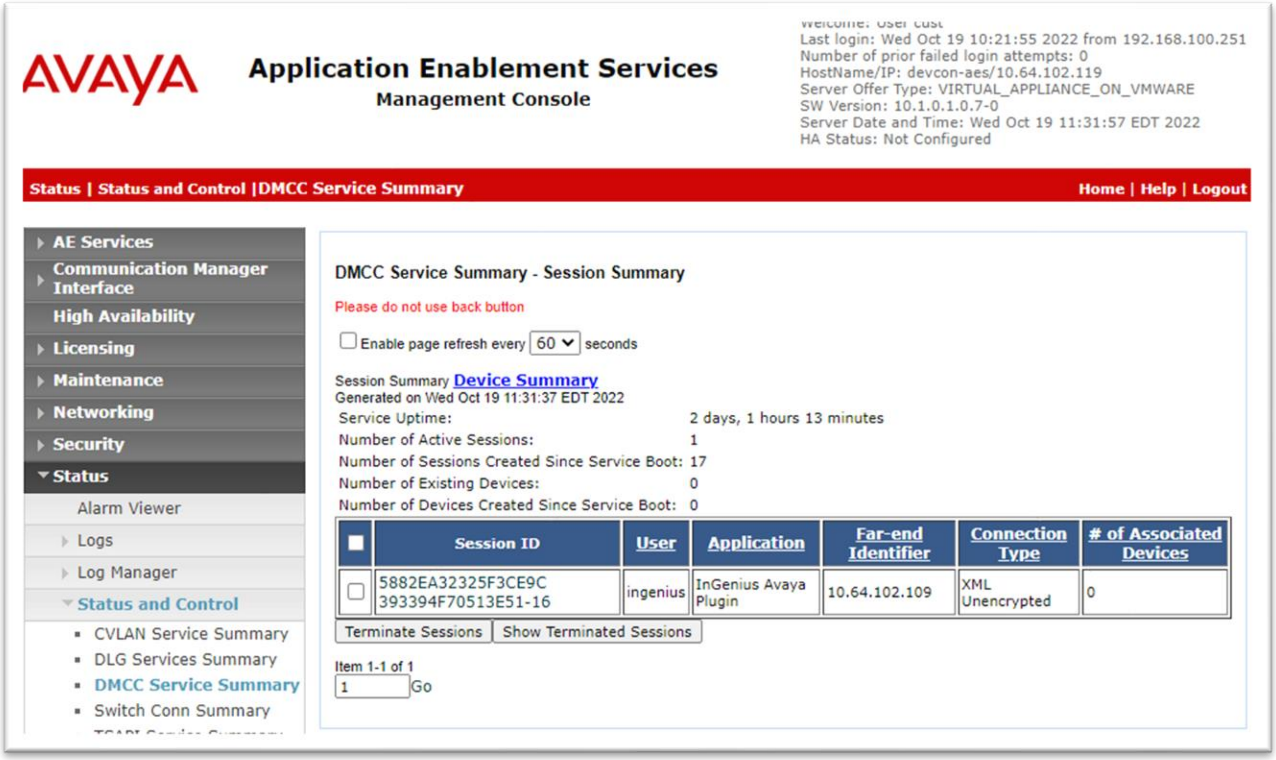
9.1. Verify Avaya Aura® Communication Manager

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    Version   Mnt   AE Services      Service       Msgs      Msgs
Link             Busy  Server           State         Sent      Rcvd

1      12        no    devcon-aes       established   860       861
```

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**.



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:31:57 EDT 2022
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

☐ Enable page refresh every 60 seconds

Session Summary Device Summary
Generated on Wed Oct 19 11:31:37 EDT 2022

Service Uptime:	2 days, 1 hours 13 minutes
Number of Active Sessions:	1
Number of Sessions Created Since Service Boot:	17
Number of Existing Devices:	0
Number of Devices Created Since Service Boot:	0

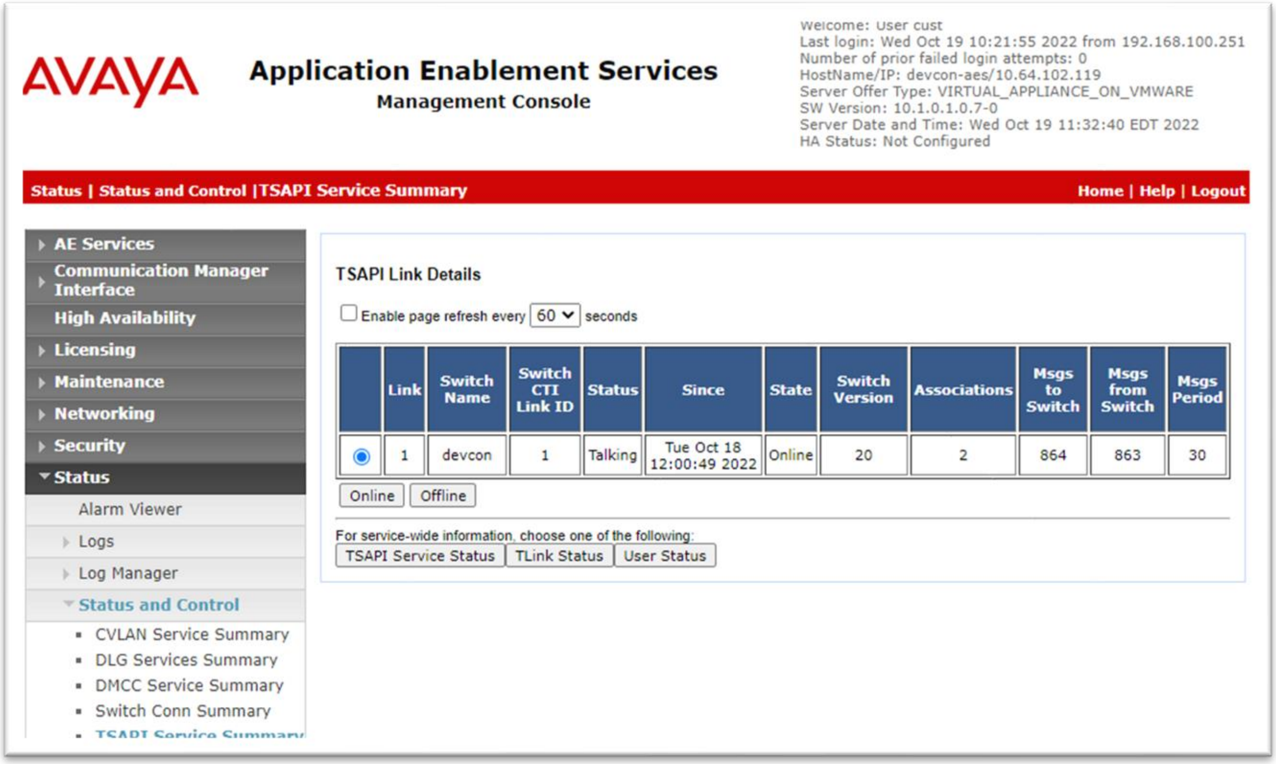
☐	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
☐	5882EA32325F3CE9C 393394F70513E51-16	ingenius	InGenius Avaya Plugin	10.64.102.109	XML Unencrypted	0

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 InGenius Connect and connected to the agent stations on Communication Manager.



Welcome: User cust
Last login: Wed Oct 19 10:21:55 2022 from 192.168.100.251
Number of prior failed login attempts: 0
HostName/IP: devcon-aes/10.64.102.119
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.0.1.0.7-0
Server Date and Time: Wed Oct 19 11:32:40 EDT 2022
HA Status: Not Configured

TSAPI Link Details

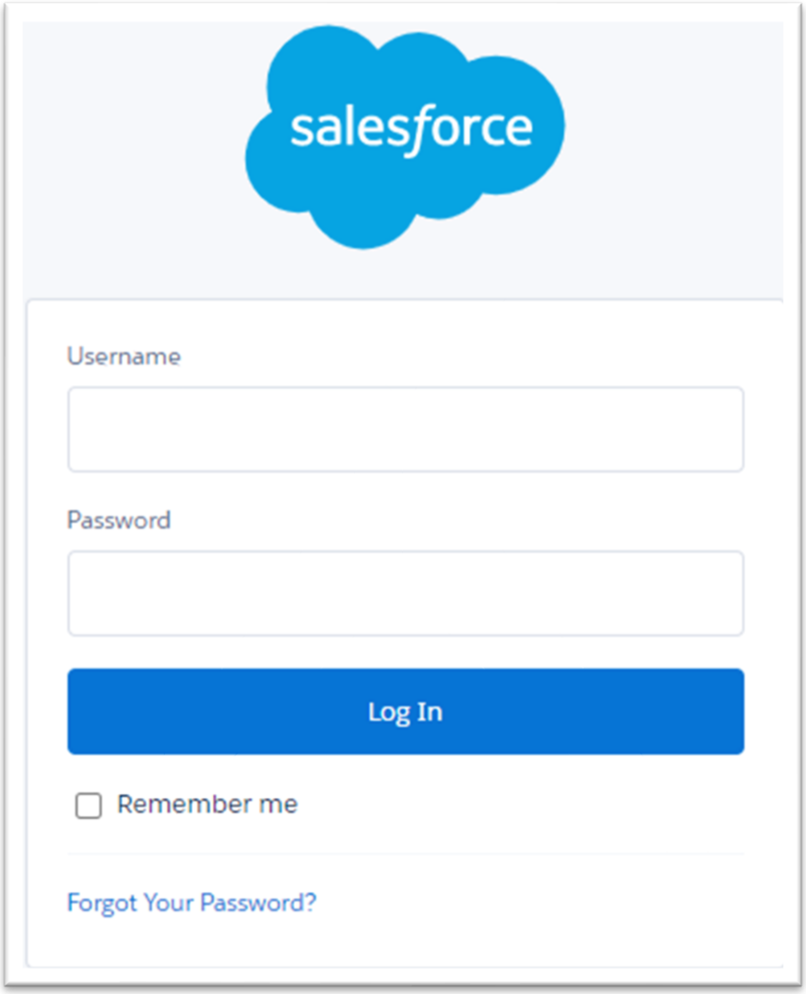
☐ Enable page refresh every 60 seconds

	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 Oct 18 12:00:49 2022	Online	20	2	864	863	30

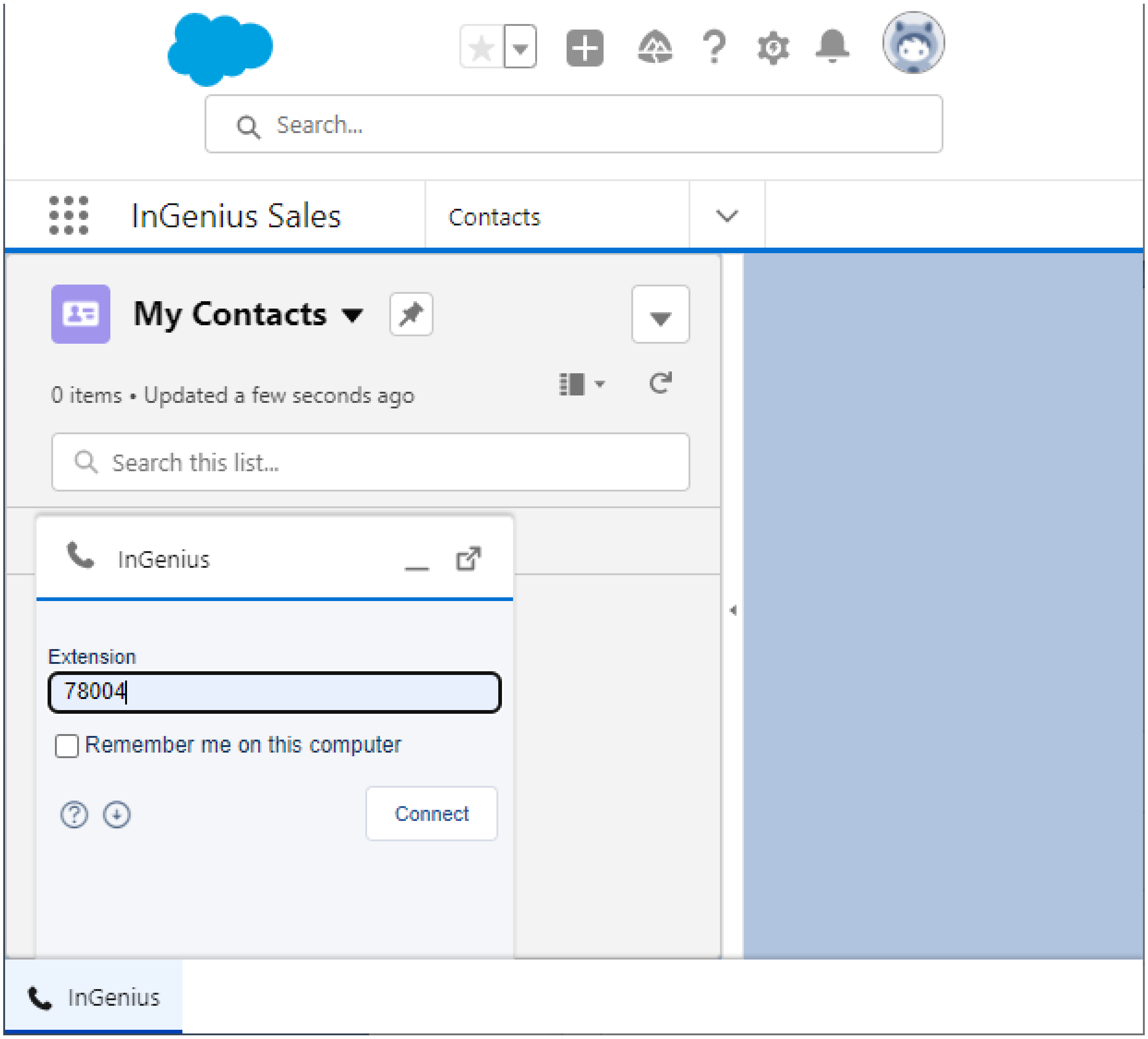
For service-wide information, choose one of the following:

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.



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**.

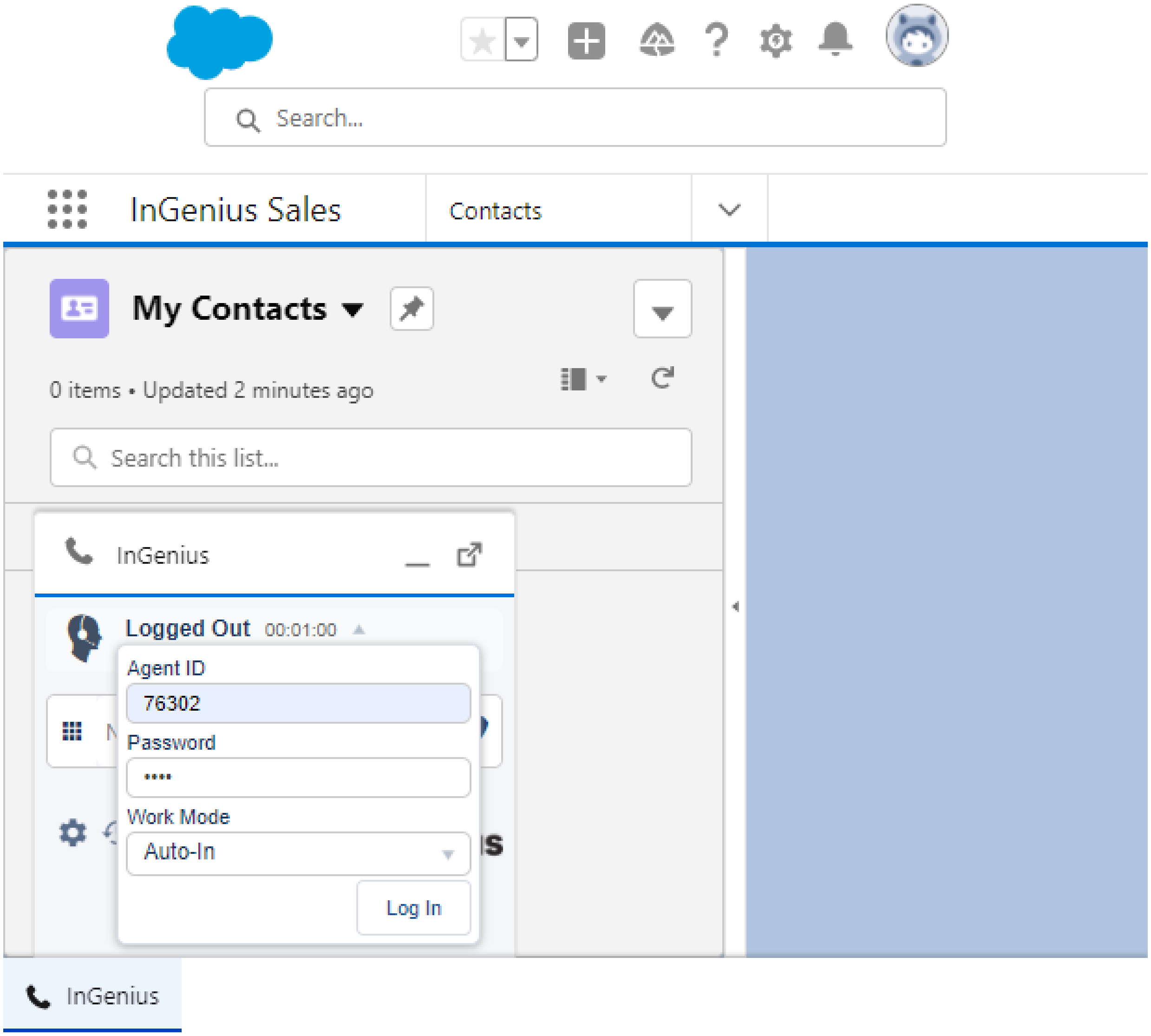


Extension

78004

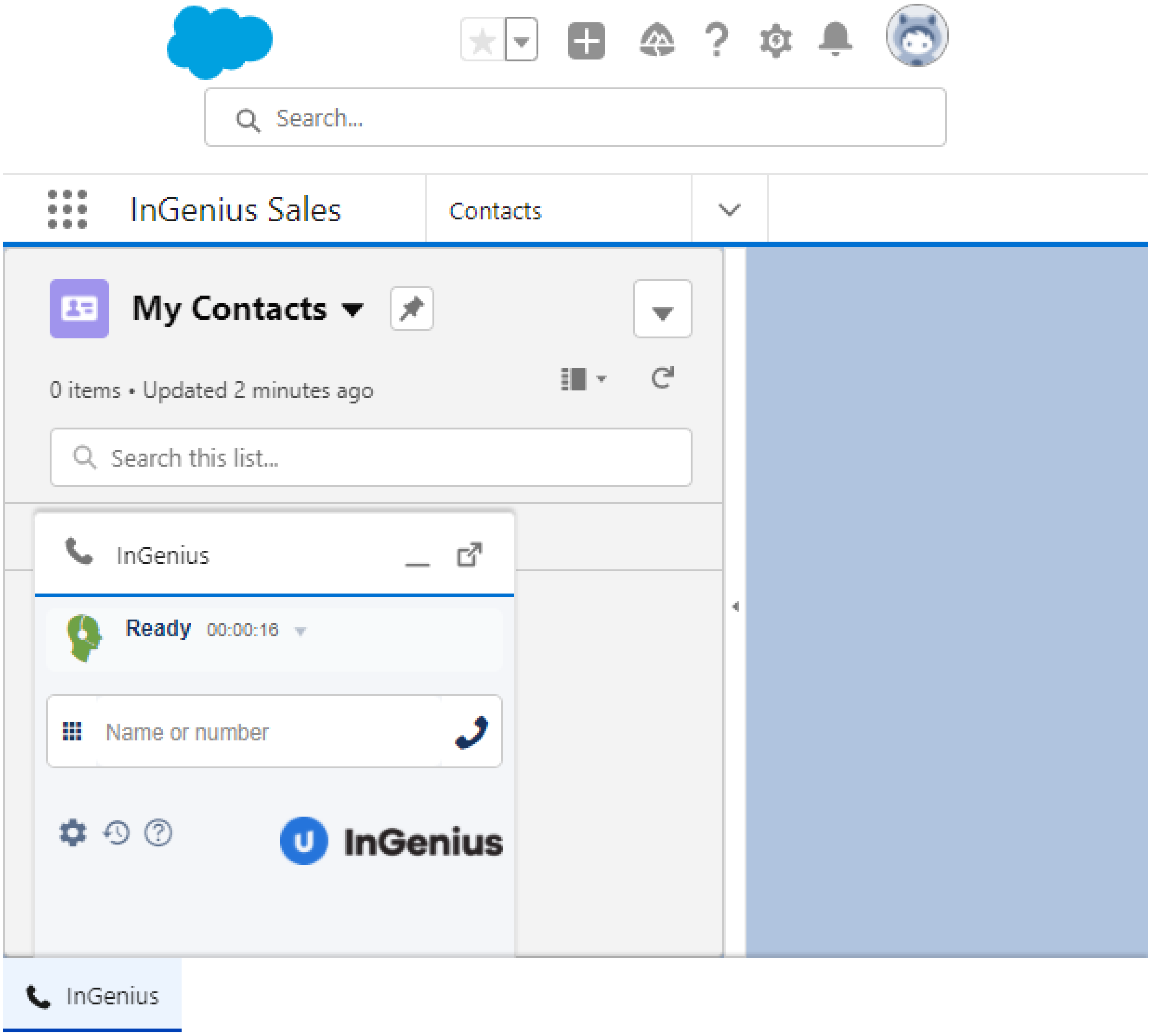
□ Remember me on this computer

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**.



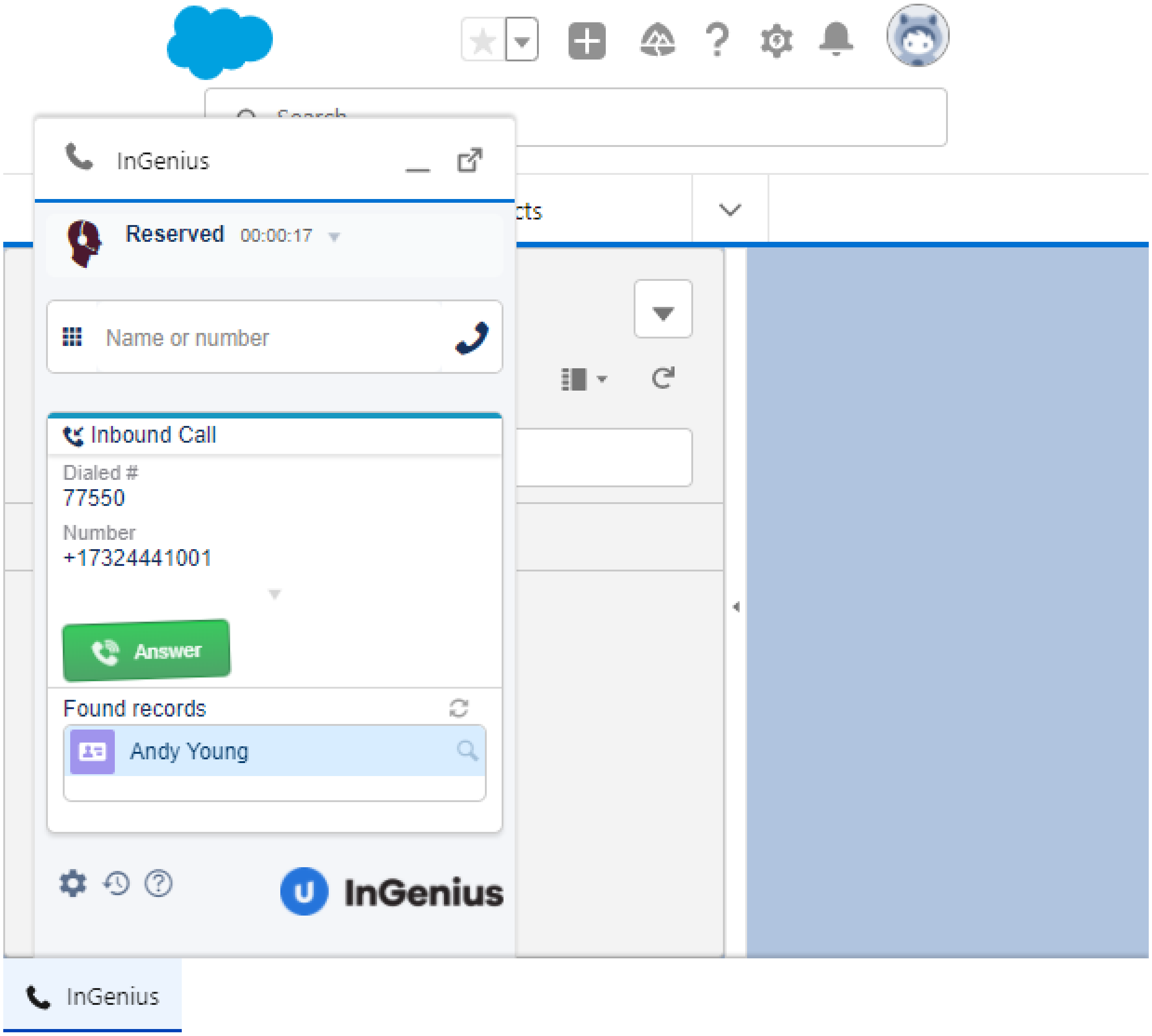
Agent ID: 76302
Password: ••••
Work Mode: Auto-In

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.



InGenius

Reserved 00:00:17

Name or number

Inbound Call

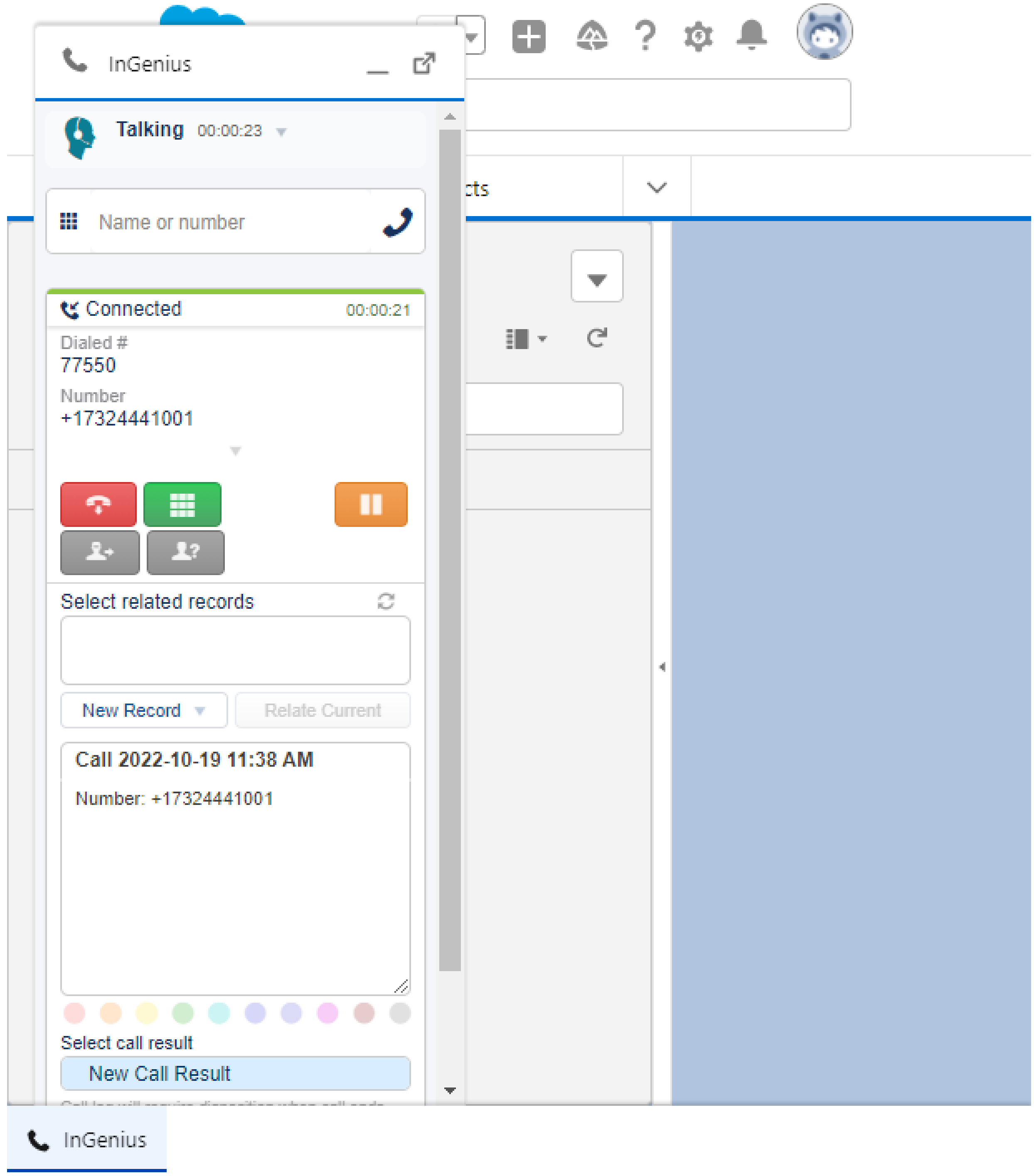
Dialed #
77550

Number
+17324441001

Found records

Andy Young

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.



InGenius

Talking 00:00:23

Name or number

Connected 00:00:21

Dialed #
77550

Number
+17324441001

Select related records

New Record

Relate Current

Call 2022-10-19 11:38 AM

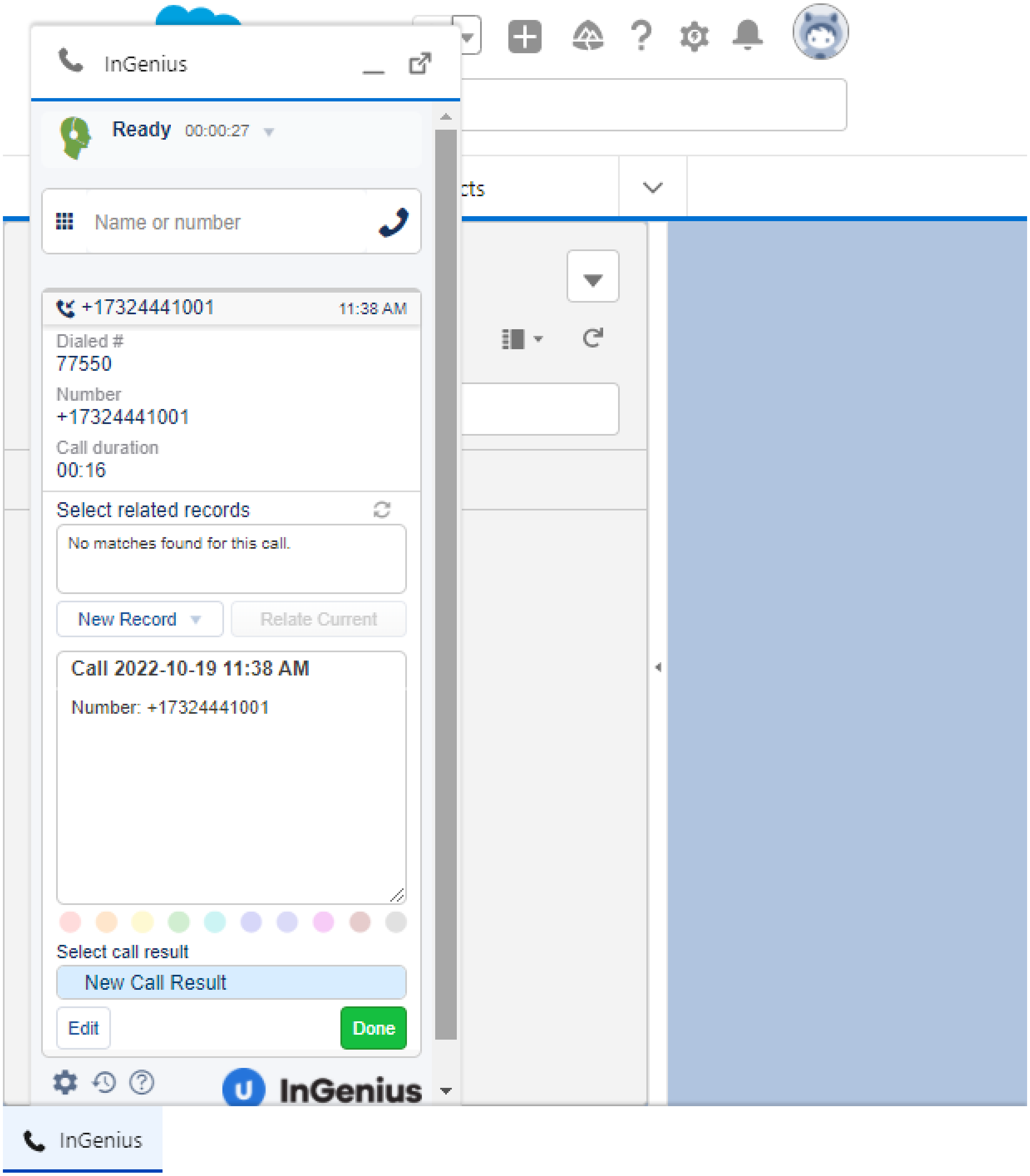
Number: +17324441001

Select call result

New Call Result

InGenius

When the ACD call is terminated, the following InGenius screen is displayed while the agent wraps up the call.



Ready 00:00:27

+17324441001 11:38 AM

Dialed #
77550

Number
+17324441001

Call duration
00:16

Select related records

No matches found for this call.

Call 2022-10-19 11:38 AM

Number: +17324441001

Select call result

New Call Result

10. Conclusion

These Application Notes describe the configuration steps required to integrate Upland InGenius Connect for Salesforce with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. Upland InGenius Connect for Salesforce 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 2, September 2022, available at http://support.avaya.com.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 10.1.x, Issue 5, September 2022, available at http://support.avaya.com.

3. *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 7, September 2022, available at http://support.avaya.com.

4. *Administering Avaya Aura® Session Manager*, Release 10.1, Issue 4, September 2022, available at http://support.avaya.com.

5. *InGenius Connect Administrator Guide*, Version 2022 R1.0, available upon request to InGenius Support.

6. *InGenius Connect User Guide*, Version 2022 R1.0, Telephony System: Avaya, available upon request to InGenius Support.

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.