DevConnect Program

Application Notes for IntraNext Event Intelligence 11.2 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 for IntraNext Event Intelligence 11.2 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. IntraNext Event Intelligence is a contact center solution.

In the compliance testing, IntraNext Event Intelligence used the Telephony Services Application Programming Interface from Avaya Aura® Application Enablement Services to monitor agent stations on Avaya Aura® Communication Manager to provide screen pop and call control features from the agent desktops running the IntraNext OneCTI application.

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.

1. Introduction

These Application Notes describe the configuration steps required for IntraNext Event Intelligence 11.2 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. Event Intelligence is a contact center solution.

In the compliance testing, Event Intelligence used the Telephony Services Application Programming Interface (TSAPI) from Application Enablement Services to monitor agent stations on Communication Manager to provide screen pop and call control features from the agent desktops running the IntraNext OneCTI application.

2. General Test Approach and Test Results

The feature test cases were performed manually. Upon an agent log in, Event Intelligence used TSAPI to query and request monitoring on the agent station associated with the agent ID.

Incoming ACD calls were placed with available agents that have desktops running the OneCTI client application. Manual call controls from the OneCTI application were exercised to verify call control features such as answering and transferring of calls.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the Event Intelligence server and OneCTI client.

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 this Application Note, the interface between Avaya systems and IntraNext utilized encrypted TSAPI with Application Enablement Services.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on Event Intelligence:

- Use of TSAPI query services to query device information, name, agent state, and universal call ID.
- Use of TSAPI monitoring and event report services to monitor agent stations.
- Use of TSAPI set value services to set agent states, including log out, work mode changes with support for reason codes and pending aux work.
- Use of TSAPI snapshot services to obtain information on agent stations and existing calls.
- Use of TSAPI call control services to support call control actions initiated from OneCTI.
- Proper handling of call scenarios involving inbound, outbound, internal, external, ACD, non-ACD, screen pop, drop, hold/resume, multiple calls, multiple agents, transfer, conference, long duration, send DTMF, pending aux work, and reason codes.

The serviceability testing focused on verifying the ability of Event Intelligence to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Event Intelligence server and OneCTI client.

2.2. Test Results

All test cases were executed, and the following were observations on Event Intelligence:

- By design, agents are required to use the phone to log into the Avaya ACD at the start of each day. This is so that the association of agent ID with the used station extension can be established and be picked up by Event Intelligence via TSAPI queries.

- After the establishment of a three-party conference involving two agents, the agent phone bars did not reflect all other parties on the call nor get updated as other parties drop. IntraNext shared that in typical customer environments, there will be additional implementation of OneCare Transfer Tool and backend services that can provide and reflect all parties in conference and update accordingly as parties drop.

- Previous dialed digits can remain in the Touch Tone Keypad screen and may require manual clearing.

2.3. Support

Technical support on Event Intelligence can be obtained through the following:

- **Phone:** (800) 928-6398
- **Email :** support@intranext.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. 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, Event Intelligence monitored agent stations associated with the agent IDs shown in the table below.

Device Type	Extension
Agent Station	65001 (H.323), 66006 (SIP)
Agent ID	65881, 65882
Agent Password	65881, 65882

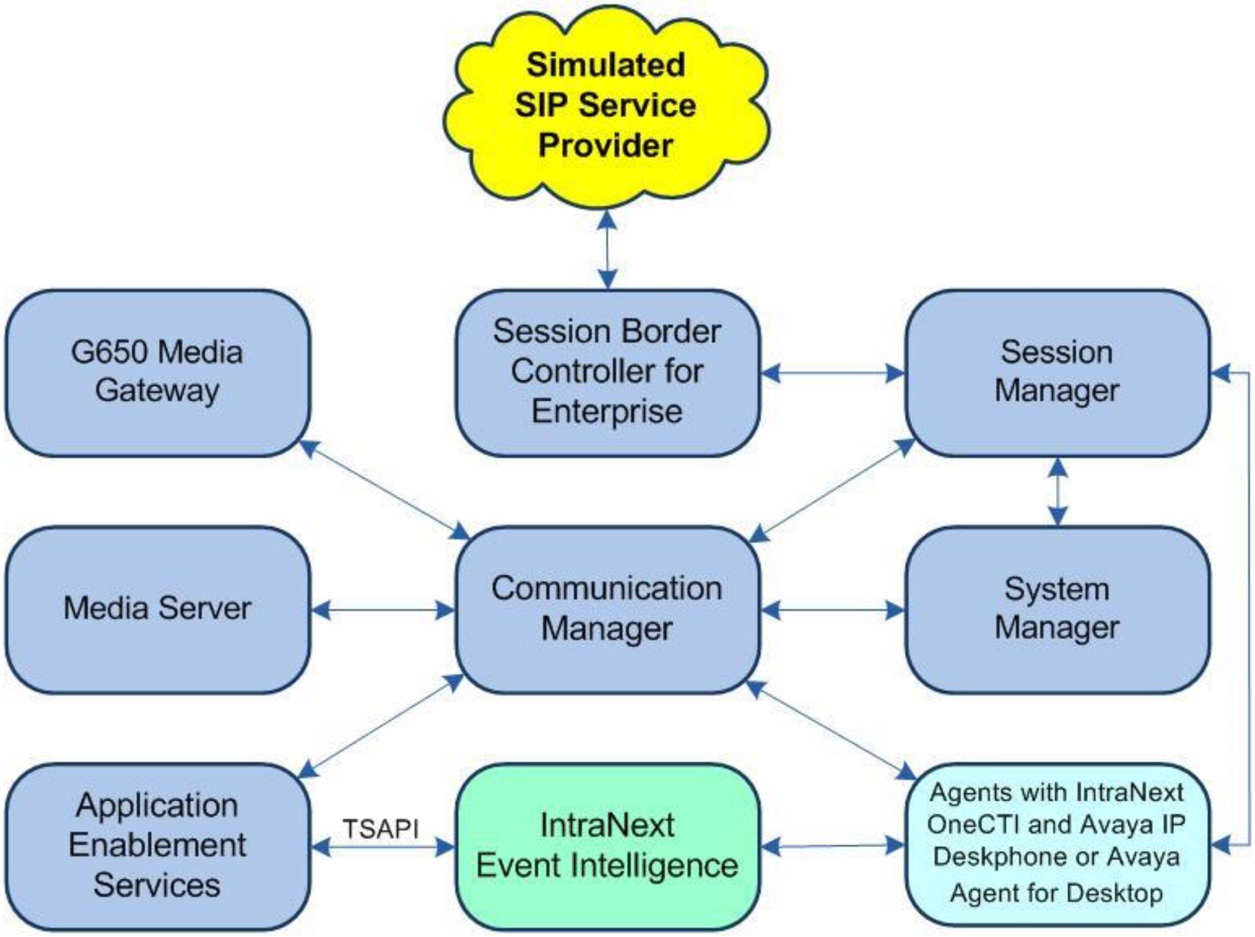

Simulated SIP Service Provider
G650 Media Gateway
Session Border Controller for Enterprise
Session Manager
Media Server
Communication Manager
System Manager
Application Enablement Services
TSAPI
IntraNext Event Intelligence
Agents with IntraNext OneCTI and Avaya IP Deskphone or Avaya Agent for Desktop

Figure 1: Compliance Testing Configuration

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 in Virtual Environment	10.1.2 (10.1.2.0.0.974.27783)
Avaya G430 Media Gateway	42.8.0
Avaya Aura® Media Server in Virtual Environment	10.1 (10.1.0.125)
Avaya Aura® Application Enablement Services in Virtual Environment	10.1.2 (10.1.2.0.0.12-0)
Avaya Aura® Session Manager in Virtual Environment	10.1.2 (10.1.2.0.101.2016)
Avaya Aura® System Manager in Virtual Environment	10.1.2 (10.1.2.0.0715476)
Avaya Session Border Controller for Enterprise in Virtual Environment	10.1 (10.1.0.0-32-21432)
Avaya Agent for Desktop (H.323 & SIP)	2.0.6.0.10
Avaya 9611G IP Desk phone (H.323)	6.8.5.3.2
Avaya J169 IP Desk phone (SIP)	4.0.13.0.6
Avaya J179 IP Desk phone (H.323)	6.8.5.3.2
IntraNext Event Intelligence on Windows Server 2019 • Avaya TSAPI Windows Client (csta32.dll)	11.2.17.0 Standard 8.1.3.25
IntraNext OneCTI on Windows 10	10.8.7 Pro

5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify License

Log in to the System Access Terminal to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the "**display system-parameters customer-options**" command to verify that the **Computer Telephony Adjunct Links** customer option is set to "**y**" on **Page 4**. If this option is not set to "**y**" then contact the Avaya sales team or business partner for a proper license file.

```
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? y                      DCS (Basic)? y
          ASAI Link Core Capabilities? y                DCS Call Coverage? y
          ASAI Link Plus Capabilities? y               DCS with Rerouting? y
```

5.2. Administer CTI Link

Add a CTI link using the "**add cti-link n**" command, where "**n**" is an available CTI link number. 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
```

5.3. Administer System Parameters Features

Log in to the System Access Terminal. 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.

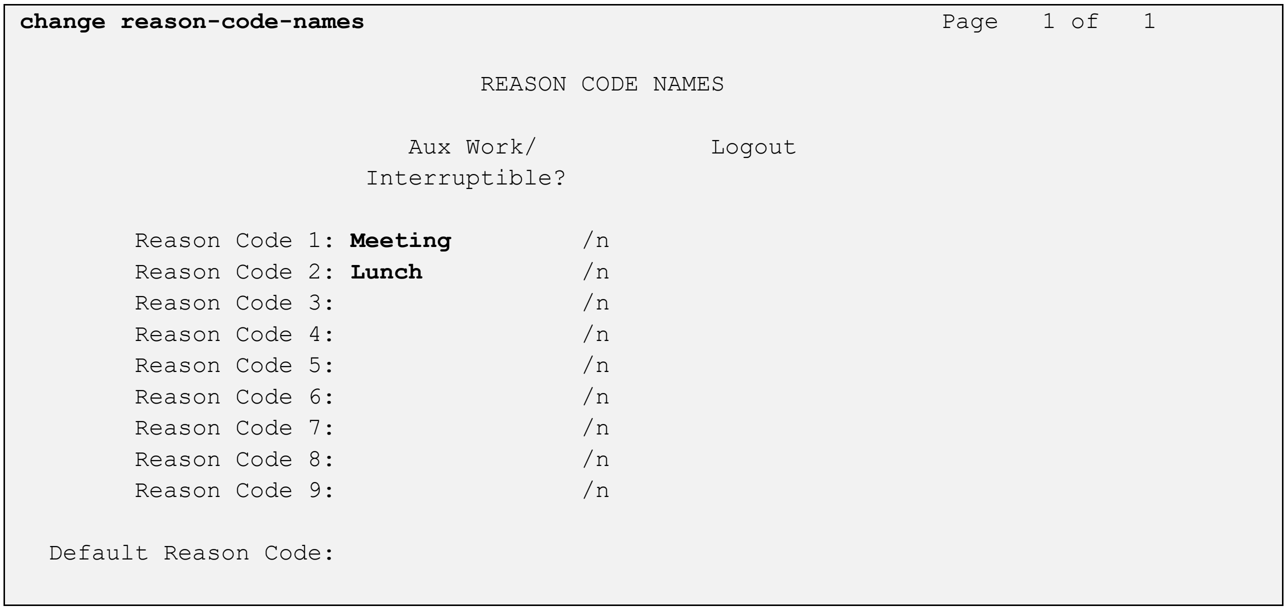
```
change system-parameters features                               Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

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 Event Intelligence.

```
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? y
                                           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
```

5.4. 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 **Aux Work** reason codes, which will be used later to configure Event Intelligence.



```
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:                 /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

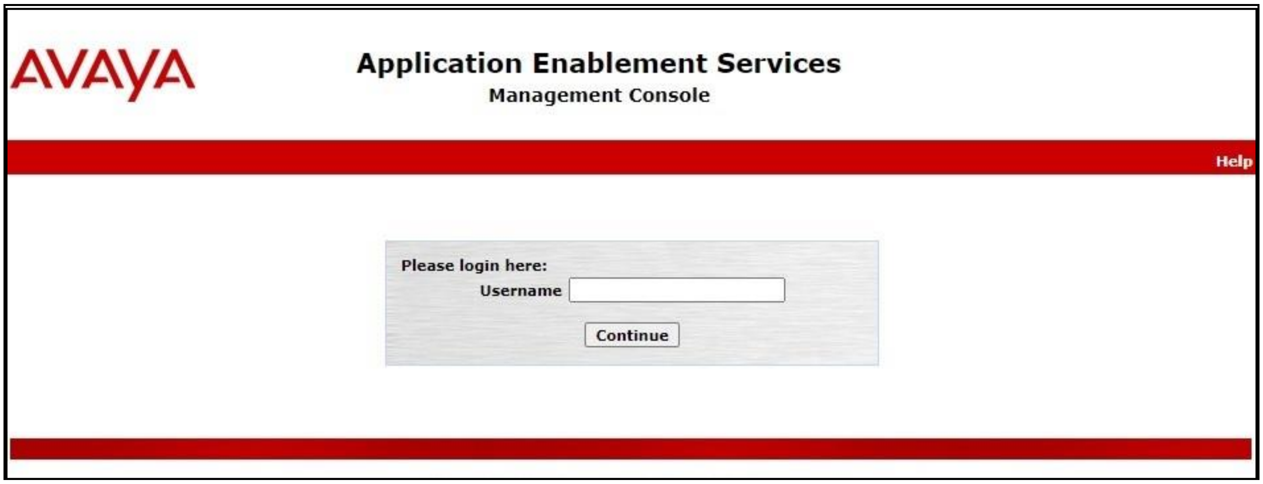
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Administer IntraNext user
- Administer security database
- Restart service
- Obtain Tlink name
- Export CA certificate

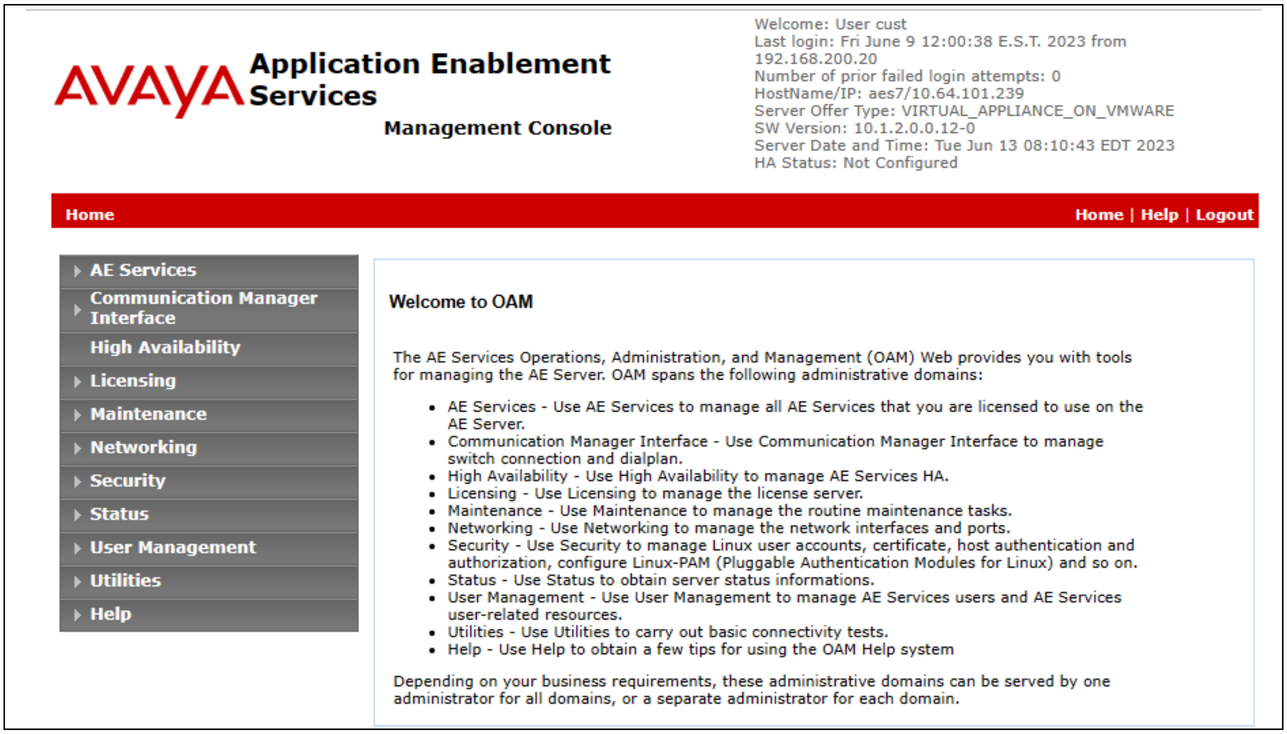
6.1. Launch OAM Interface

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 **Please login here** screen is displayed. Log in using the appropriate credentials.



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



Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:10:43 EDT 2023
HA Status: Not Configured

Welcome to OAM

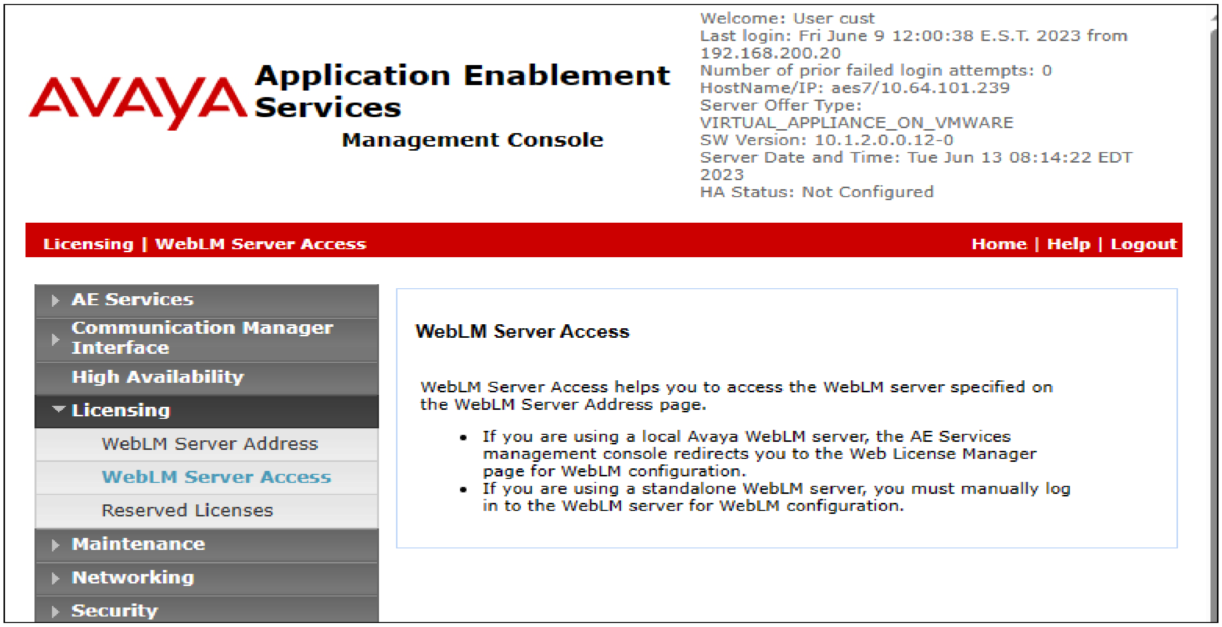
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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 Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials and navigate to display installed licenses (not shown).



Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:14:22 EDT 2023
HA Status: Not Configured

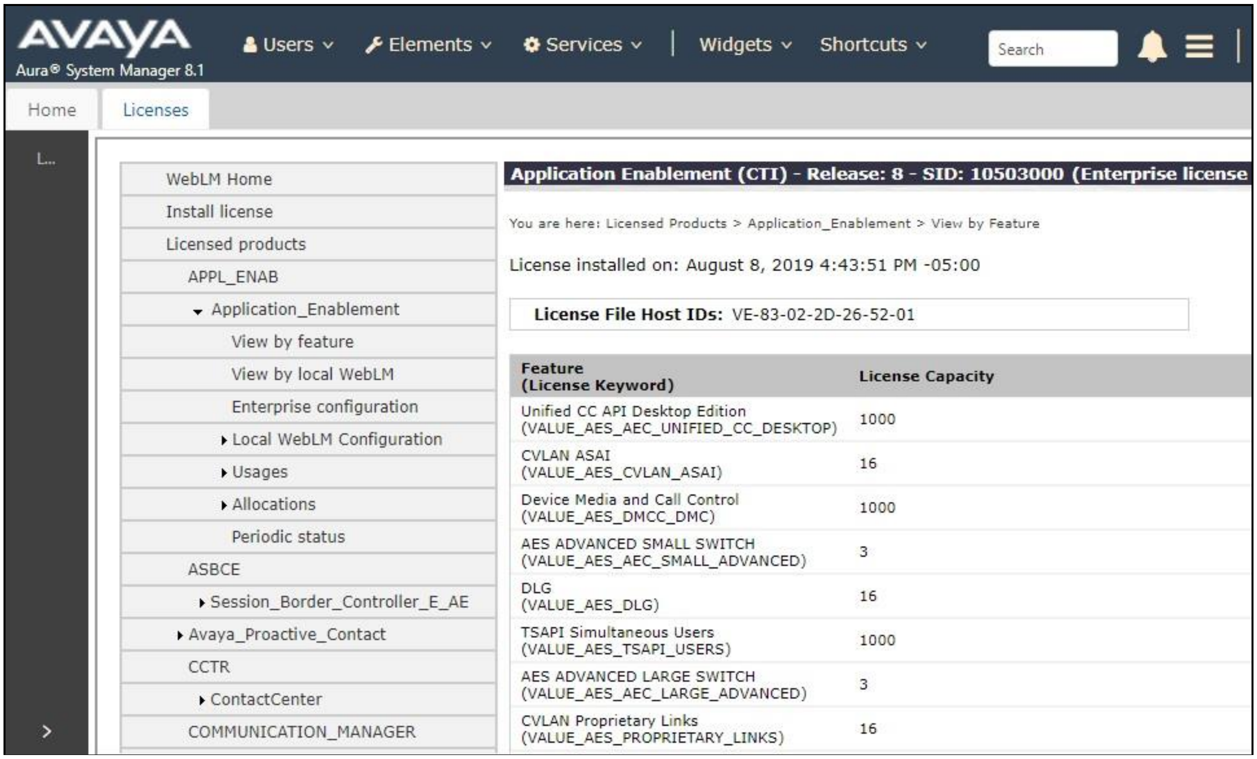
WebLM Server Access

WebLM Server Access helps you to access the WebLM server specified on the WebLM Server Address page.

- If you are using a local Avaya WebLM server, the AE Services management console redirects you to the Web License Manager page for WebLM configuration.
- If you are using a standalone WebLM server, you must manually log in to the WebLM server for WebLM configuration.

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.



Application Enablement (CTI) - Release: 8 - SID: 10503000 (Enterprise license

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

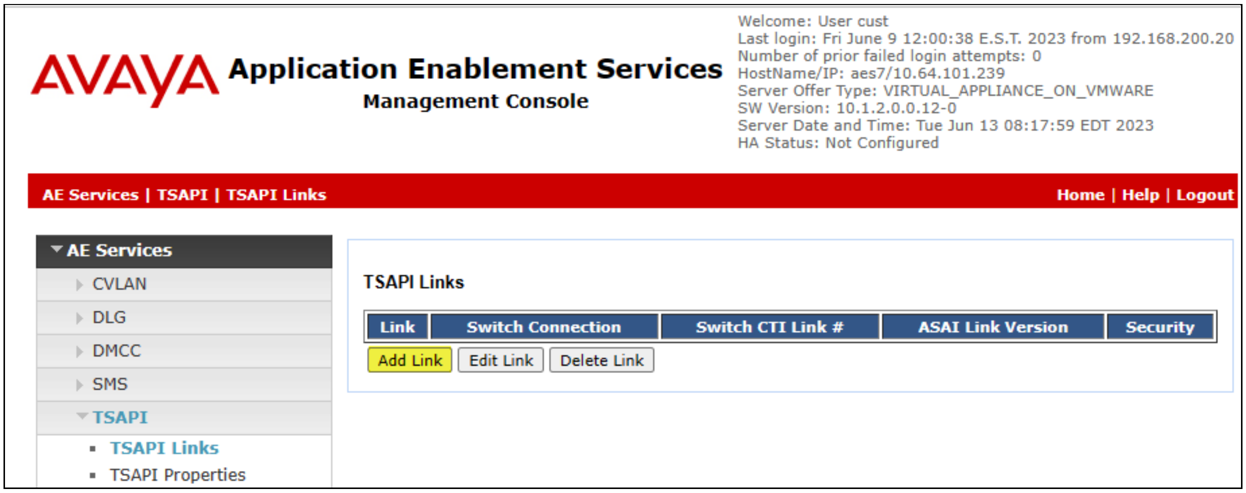
License installed on: August 8, 2019 4:43:51 PM -05:00

License File Host IDs: VE-83-02-2D-26-52-01

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	16
Device Media and Call Control (VALUE_AES_DMCC_DMC)	1000
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	3
DLG (VALUE_AES_DLG)	16
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	1000
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	3
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	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**.



AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:17:59 EDT 2023
HA Status: Not Configured

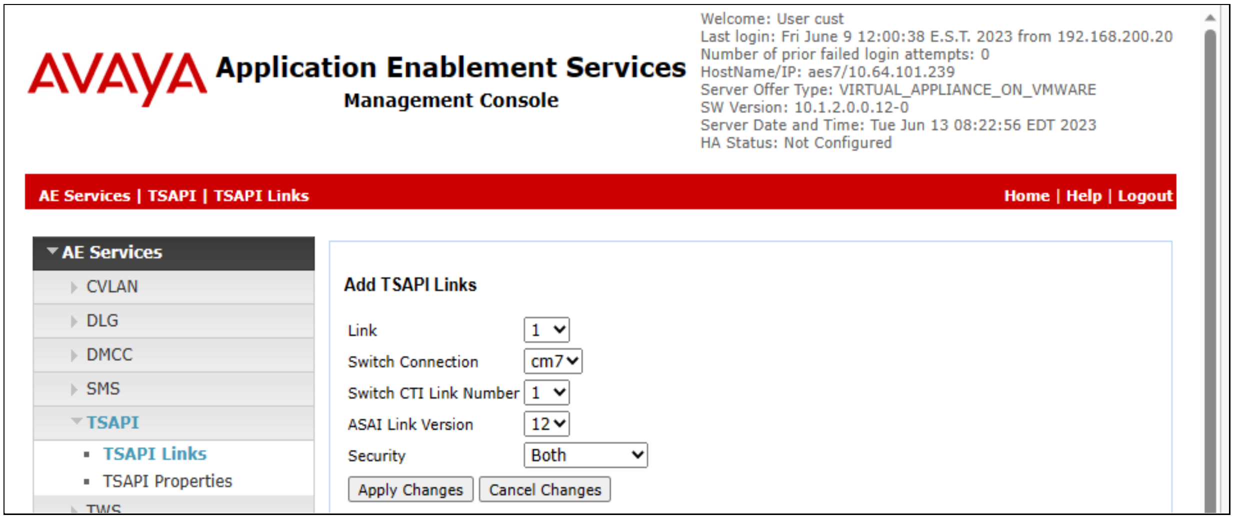
AE Services | TSAPI | TSAPI Links   Home | Help | Logout

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

The **Add TSAPI Links** screen is displayed next. Set the following values for the specified fields and retain the default values for the remaining fields.

- **Link:** An available link number.
- **Switch Connection:** The relevant switch connection, in this case “cm7”.
- **Switch CTI Link Number:** The CTI link number from **Section 5.2**.
- **Security:** “Encrypted” or “Both” to allow for encrypted connection.



AVAYA Application Enablement Services
Management Console

Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:22:56 EDT 2023
HA Status: Not Configured

AE Services | TSAPI | TSAPI Links   Home | Help | Logout

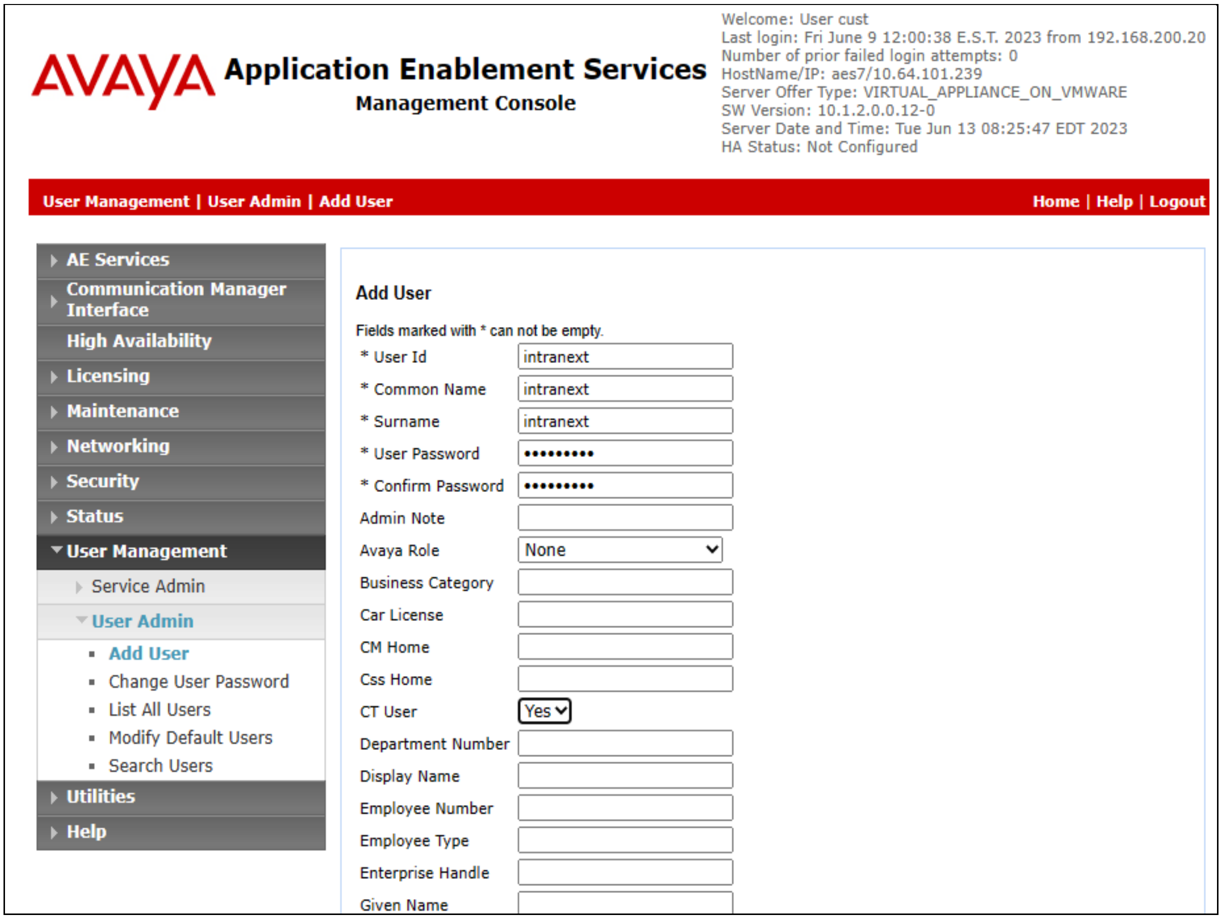
Add TSAPI Links

Link	1
Switch Connection	cm7
Switch CTI Link Number	1
ASAI Link Version	12
Security	Both

6.4. Administer IntraNext 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: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:25:47 EDT 2023
HA Status: Not Configured

Add User

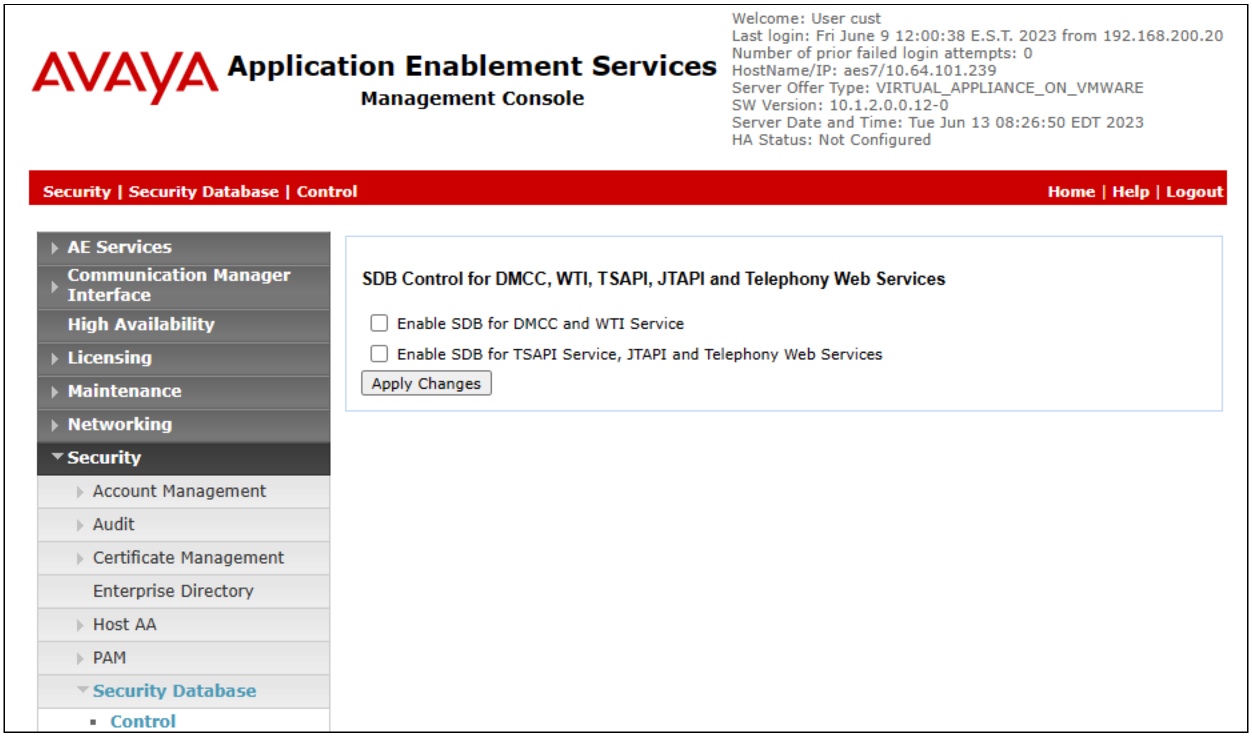
Fields marked with * can not be empty.

* User Id	intranext
* Common Name	intranext
* Surname	intranext
* 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	
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. Make certain that both parameters are unchecked, as shown below.

In the case that the security database is used by the customer with parameters already enabled, then follow reference [**2**] to configure access privileges for the IntraNext user from **Section 0**.



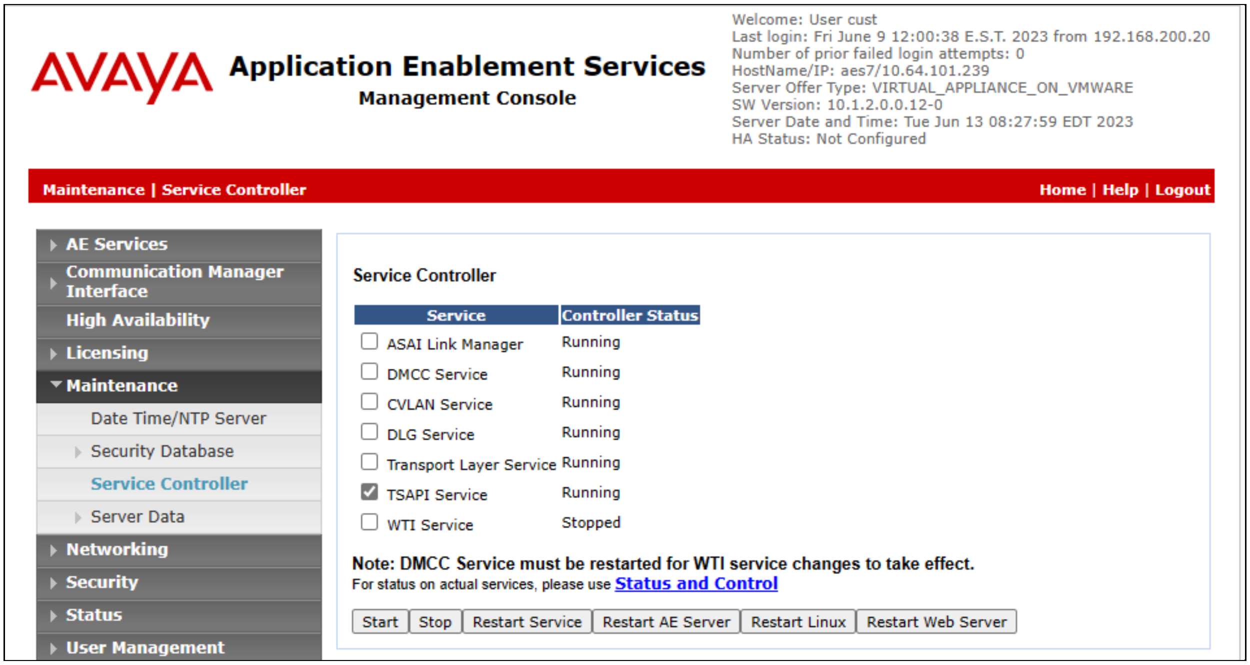
Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:26:50 EDT 2023
HA Status: Not Configured

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

☐ Enable SDB for DMCC and WTI Service
☐ Enable SDB for TSAPI Service, JTAPI and Telephony Web Services

6.6. Restart Service

Select **Maintenance → Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check **TSAPI Service** and click **Restart Service**.



Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:27:59 EDT 2023
HA Status: Not Configured

Service Controller

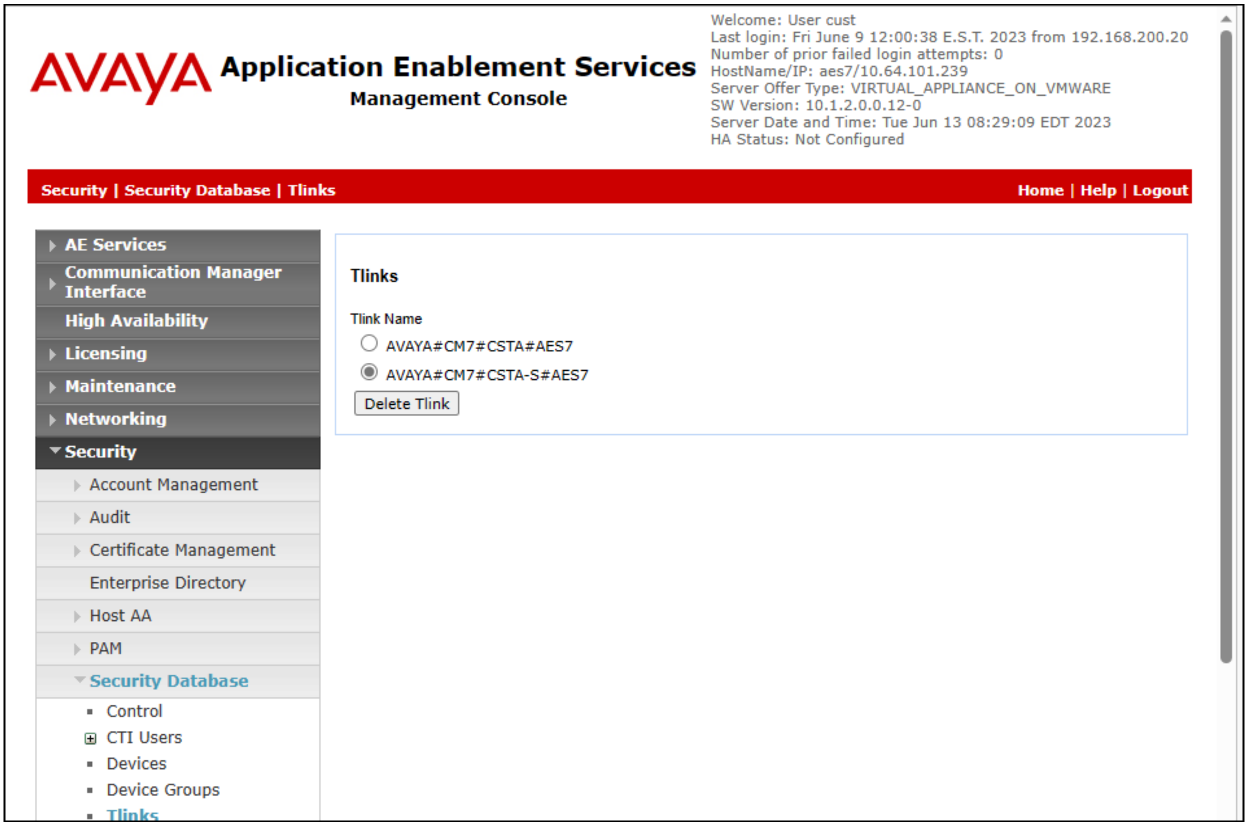
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running
□ WTI Service	Stopped

Note: DMCC Service must be restarted for WTI service changes to take effect.
For status on actual services, please use Status and Control

6.7. Obtain Tlink Name

Select **Security → Security Database → Tlinks** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name.

Make a note of the pertinent Tlink name, to be used later to share with Event Intelligence. In this case, the pertinent Tlink name for encrypted connection is "**AVAYA#CM7#CSTA-S#AES7**", as shown below.



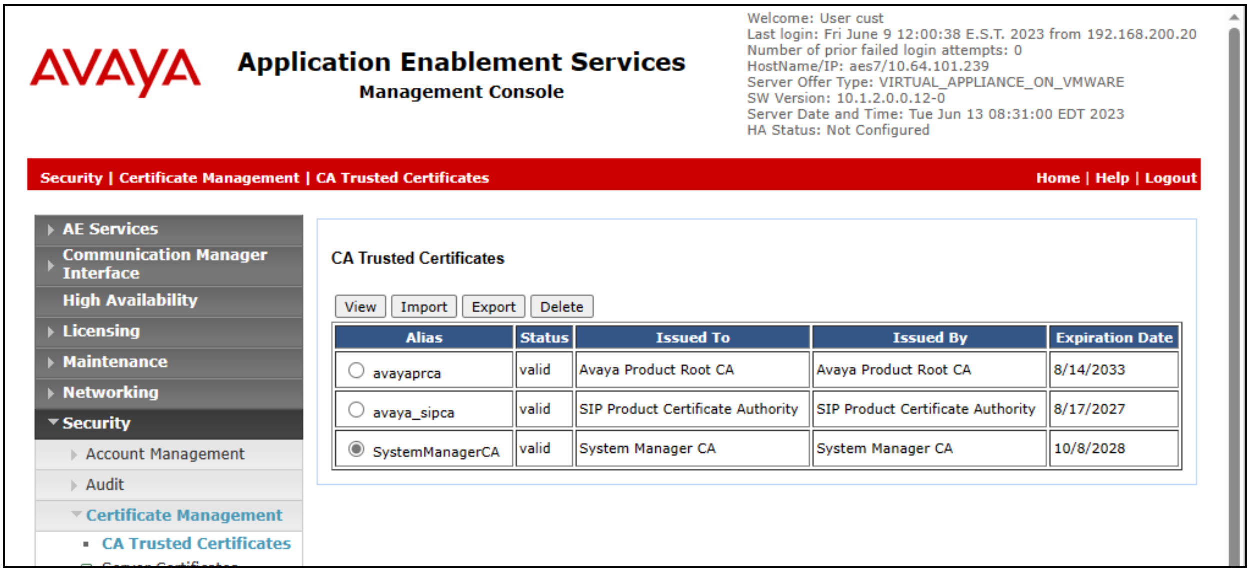
Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:29:09 EDT 2023
HA Status: Not Configured

Tlinks

Tlink Name
○ AVAYA#CM7#CSTA#AES7
● AVAYA#CM7#CSTA-S#AES7

6.8. Export CA Certificate

Select **Security → Certificate Management → CA Trusted Certificates** from the left pane, to display the **CA Trusted Certificates** screen. Select the pertinent CA certificate for secure connection with client applications, in this case "**SystemManagerCA**," and click **Export**.

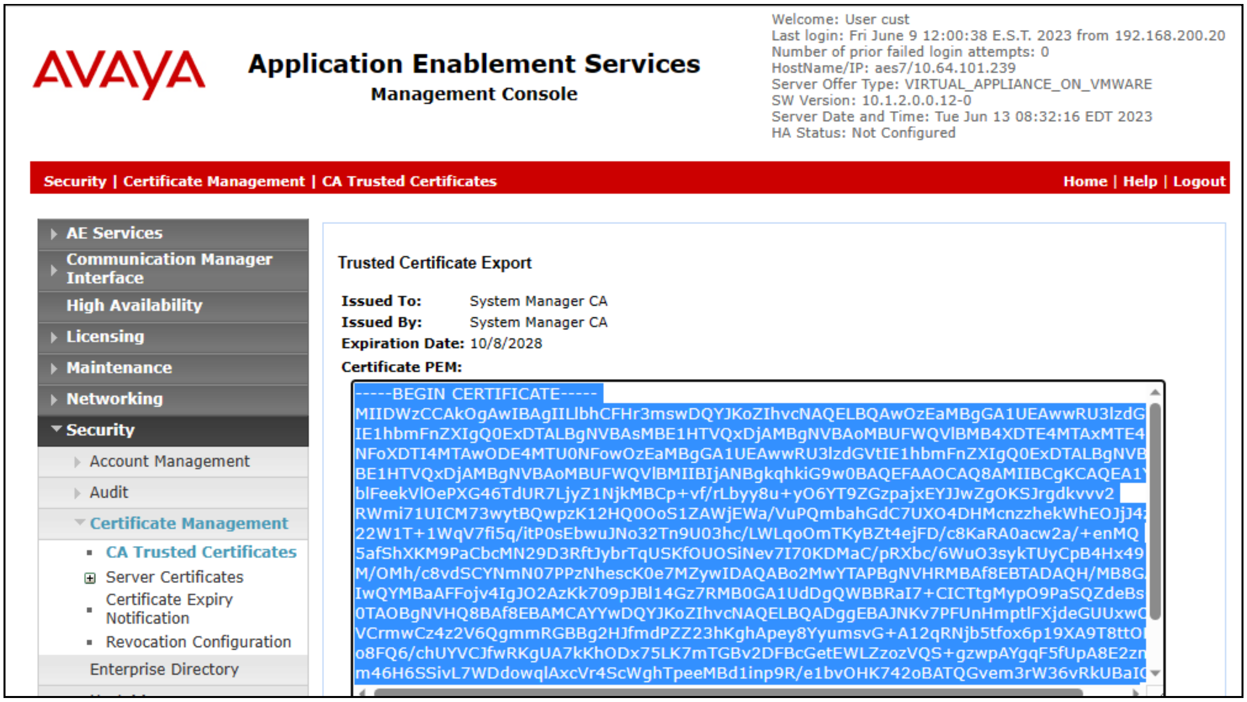


Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:31:00 EDT 2023
HA Status: Not Configured

CA Trusted Certificates

Alias	Status	Issued To	Issued By	Expiration Date
○ avayaprca	valid	Avaya Product Root CA	Avaya Product Root CA	8/14/2033
○ avaya_sipca	valid	SIP Product Certificate Authority	SIP Product Certificate Authority	8/17/2027
● SystemManagerCA	valid	System Manager CA	System Manager CA	10/8/2028

The **Trusted Certificate Export** screen is displayed next. Copy everything in the text box, including the **BEGIN CERTIFICATE** and **END CERTIFICATE** (not shown) lines.



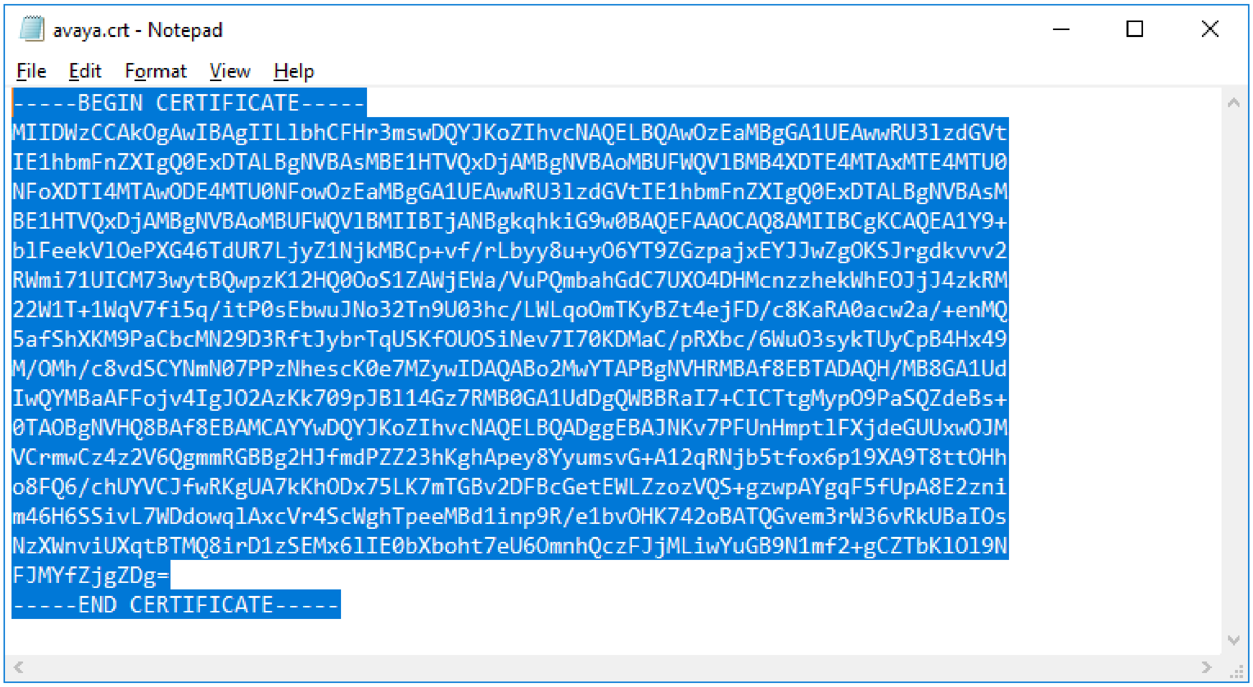
Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:32:16 EDT 2023
HA Status: Not Configured

Trusted Certificate Export

Issued To: System Manager CA
Issued By: System Manager CA
Expiration Date: 10/8/2028
Certificate PEM:

```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILlbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UEAwwRU3lzdG
IE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFWQVlBMB4XDTE4MTAxMTE4
NFoXDTI4MTAwODE4MTU0NFowOzEaMBgGA1UEAwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVB
BE1HTVQxDjAMBgNVBAoMBUFWQVlBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y
blFeekVlOePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpajxEYJJwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0OoS1ZAWjEWa/VuPQmbahGdC7UXO4DHMcnzzhekWhEOJjJ4
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8G
IwQYMBaAFFojv4IgJO2AzKk709pJBl14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwC
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttOI
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zn
m46H6SSivL7WDdowqlAxcVr4ScWghTpeeMBd1inp9R/e1bvOHK742oBATQGvem3rW36vRkUBaIC
```

Paste the copied content to a Notepad file and save with a desired file name using **.crt** as suffix, such as **avaya.crt** in the compliance testing.



```
-----BEGIN CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIILlbhCFHr3mswDQYJKoZIhvcNAQELBQAwOzEaMBgGA1UEAwwRU3lzdGVt
IE1hbmFnZXIgQ0ExDTALBgNVBAsMBE1HTVQxDjAMBgNVBAoMBUFWQVlBMB4XDTE4MTAxMTE4MTU0
NFoXDTI4MTAwODE4MTU0NFowOzEaMBgGA1UEAwwRU3lzdGVtIE1hbmFnZXIgQ0ExDTALBgNVBAsM
BE1HTVQxDjAMBgNVBAoMBUFWQVlBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1Y9+
blFeekVlOePXG46TdUR7LjyZ1NjkMBCp+vf/rLbyy8u+yO6YT9ZGzpajxEYJJwZgOKSJrgdkvvv2
RWmi71UICM73wytBQwpzK12HQ0OoS1ZAWjEWa/VuPQmbahGdC7UXO4DHMcnzzhekWhEOJjJ4zkRM
22W1T+1WqV7fi5q/itP0sEbwuJNo32Tn9U03hc/LWLqoOmTKyBZt4ejFD/c8KaRA0acw2a/+enMQ
5afShXKM9PaCbcMN29D3RftJybrTqUSKfOUOSiNev7I70KDMaC/pRXbc/6WuO3sykTUyCpB4Hx49
M/OMh/c8vdSCYNmN07PPzNhescK0e7MZywIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MB8GA1Ud
IwQYMBaAFFojv4IgJO2AzKk709pJBl14Gz7RMB0GA1UdDgQWBBRaI7+CICTtgMypO9PaSQZdeBs+
0TAOBgNVHQ8BAf8EBAMCAYYwDQYJKoZIhvcNAQELBQADggEBAJNKv7PFUnHmptlFXjdeGUUxwOJM
VCrmwCz4z2V6QgmmRGBBg2HJfmdPZZ23hKghApey8YyumsvG+A12qRNjb5tfox6p19XA9T8ttOHh
o8FQ6/chUYVCJfwRKgUA7kKhODx75LK7mTGBv2DFBcGetEWLZzozVQS+gzwpAYgqF5fUpA8E2zni
m46H6SSivL7WDdowqlAxcVr4ScWghTpeeMBd1inp9R/e1bvOHK742oBATQGvem3rW36vRkUBaIOs
NzXWnviUXqtBTMQ8irD1zSEMx6lIE0bXboht7eU6OmnhQczFJjMLiwYuGB9N1mf2+gCZTbK1O19N
FJMYfZjgZDg=
-----END CERTIFICATE-----
```

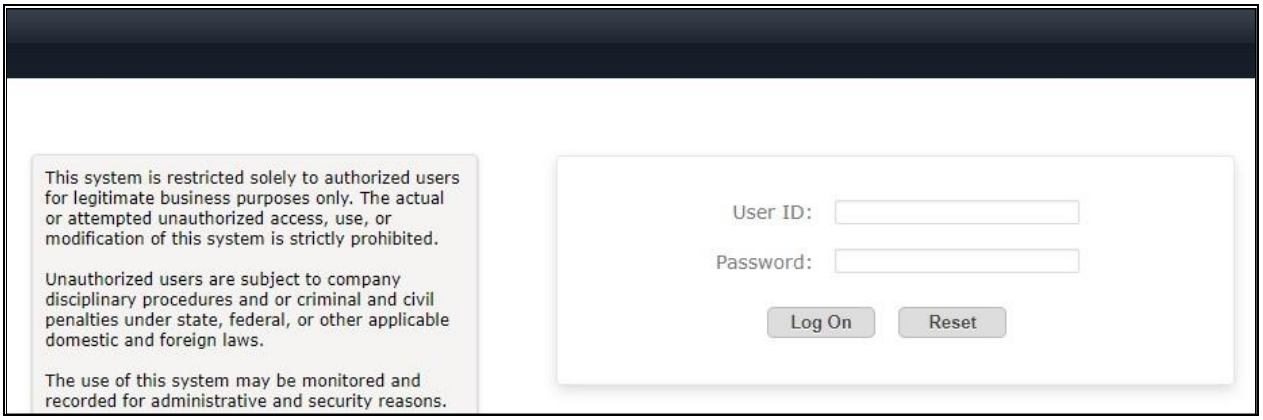
7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager, which is performed via the web interface of System Manager. The procedures include the following areas:

- Launch System Manager
- Administer users

7.1. Launch System Manager

Access the System Manager web interface by using the URL "**https://ip-address**" in an Internet browser window, where "**ip-address**" is the IP address of System Manager. Log in using the appropriate credentials.



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.

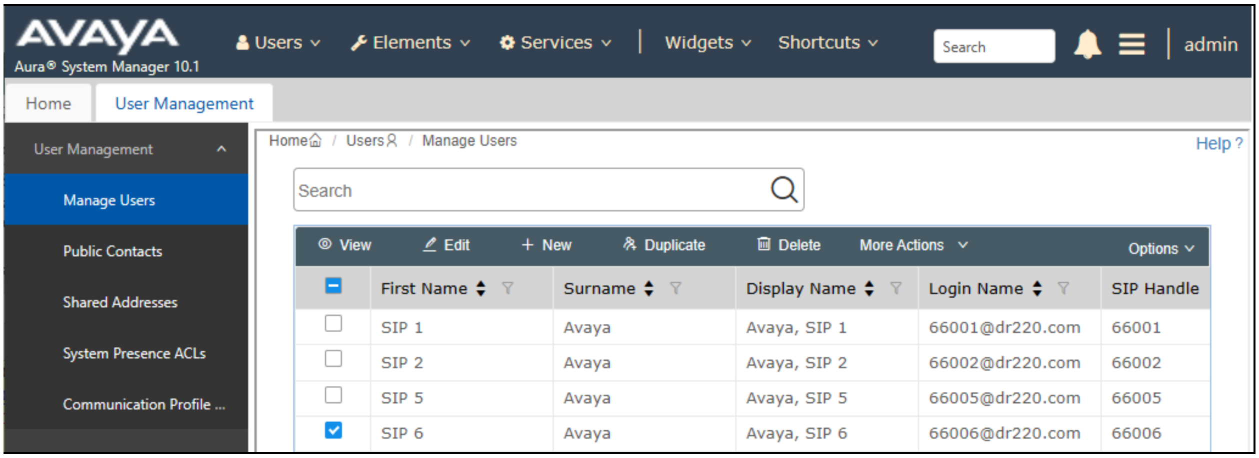
The use of this system may be monitored and recorded for administrative and security reasons.

7.2. Administer Users

NOTE: To ensure that TSAPI can successfully monitor the SIP Endpoints, this step must be performed on all SIP Endpoints. It is not required for H.323 Endpoints.

In the subsequent screen (not shown), select **Users → User Management** from the top menu. Select **User Management → Manage Users** (not shown) from the left pane to display the screen below.

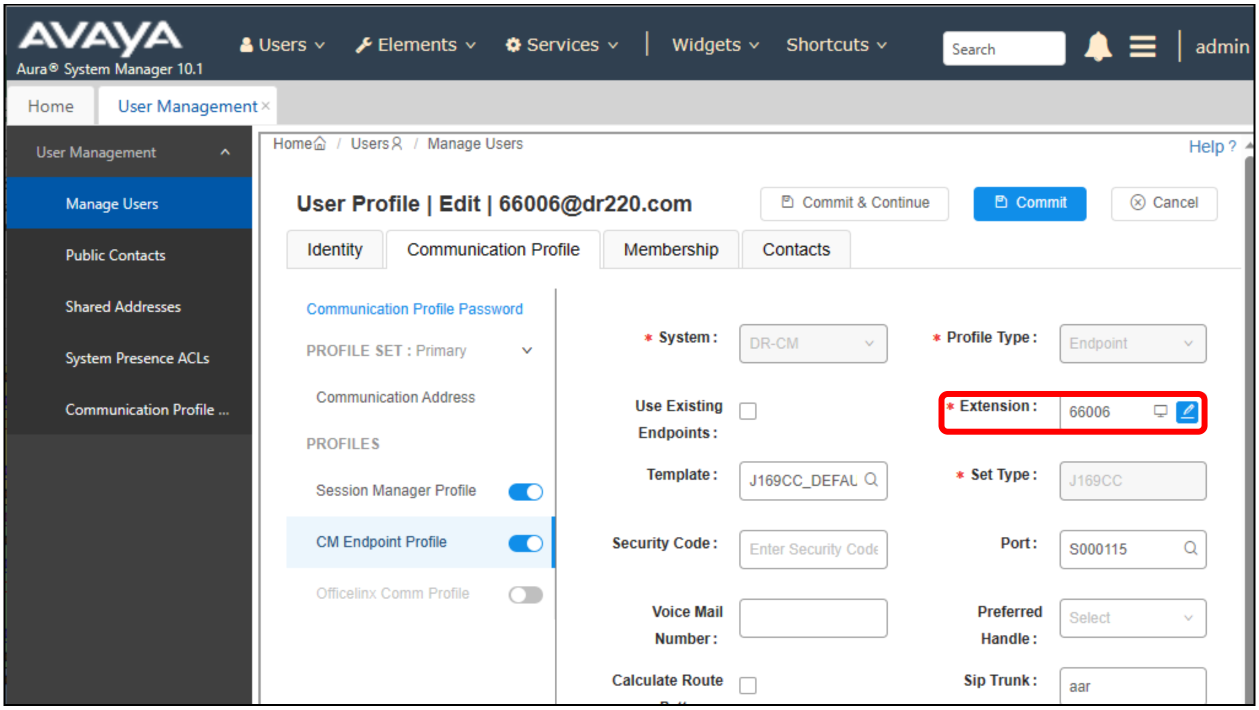
Select the entry associated with the first SIP agent station from **Section 3**, in this case "**66006**", and click **Edit**.



☐	First Name	Surname	Display Name	Login Name	SIP Handle
☐	SIP 1	Avaya	Avaya, SIP 1	66001@dr220.com	66001
☐	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
☐	SIP 5	Avaya	Avaya, SIP 5	66005@dr220.com	66005
☑	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006

The **User Profile | Edit** screen is displayed. Select the **Communication Profile** tab, followed by **CM Endpoint Profile** to display the screen below.

Click on the **Editor** icon shown below.

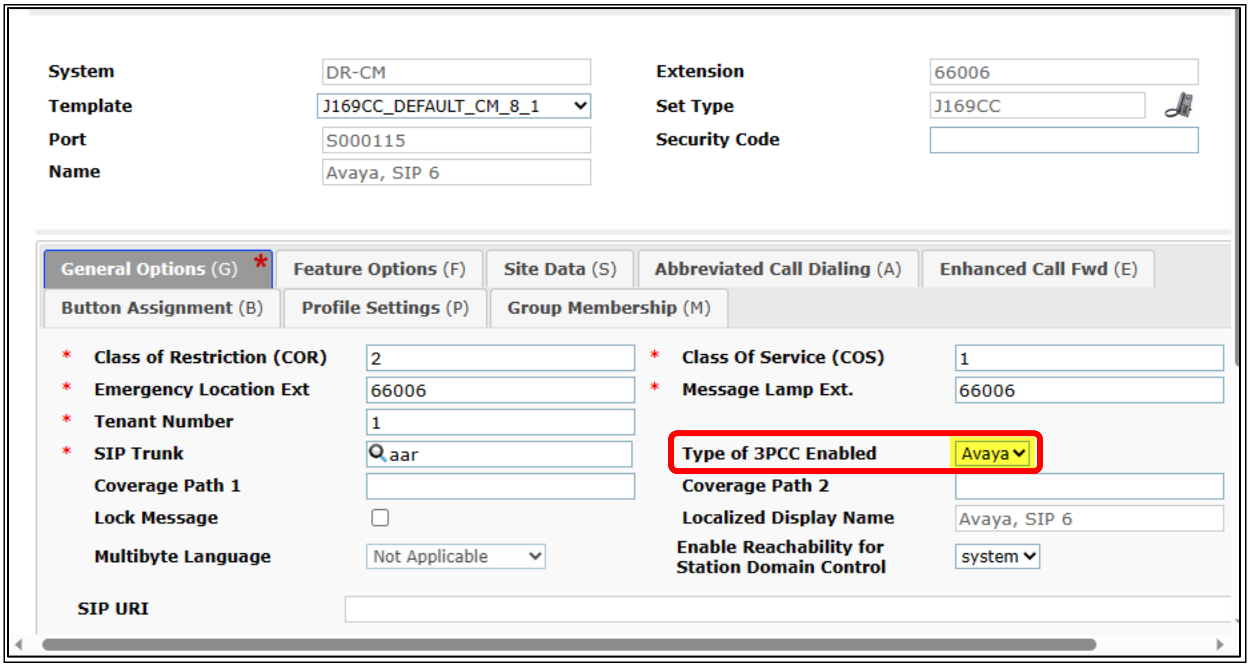


User Profile | Edit | 66006@dr220.com

* System :	DR-CM	* Profile Type :	Endpoint
Use Existing Endpoints :	□	* Extension :	66006
Template :	J169CC_DEFAL	* Set Type :	J169CC
Security Code :	Enter Security Code	Port :	S000115
Voice Mail Number :		Preferred Handle :	Select
Calculate Route	□	Sip Trunk :	aar

The **Edit Endpoint** pop-up screen is displayed. For **Type of 3PCC Enabled**, select "**Avaya**" as shown below.

Repeat this section for all SIP agent users from **Section 3**. In the compliance testing, one SIP agent extension **66006** was configured.



System	DR-CM	Extension	66006
Template	J169CC_DEFAULT_CM_8_1	Set Type	J169CC
Port	S000115	Security Code	
Name	Avaya, SIP 6		

* Class of Restriction (COR)	2	* Class Of Service (COS)	1
* Emergency Location Ext	66006	* Message Lamp Ext.	66006
* Tenant Number	1		
* SIP Trunk	aar	Type of 3PCC Enabled	Avaya
Coverage Path 1		Coverage Path 2	
Lock Message	□	Localized Display Name	Avaya, SIP 6
Multibyte Language	Not Applicable	Enable Reachability for Station Domain Control	system
SIP URI			

8. Configure IntraNext Event Intelligence

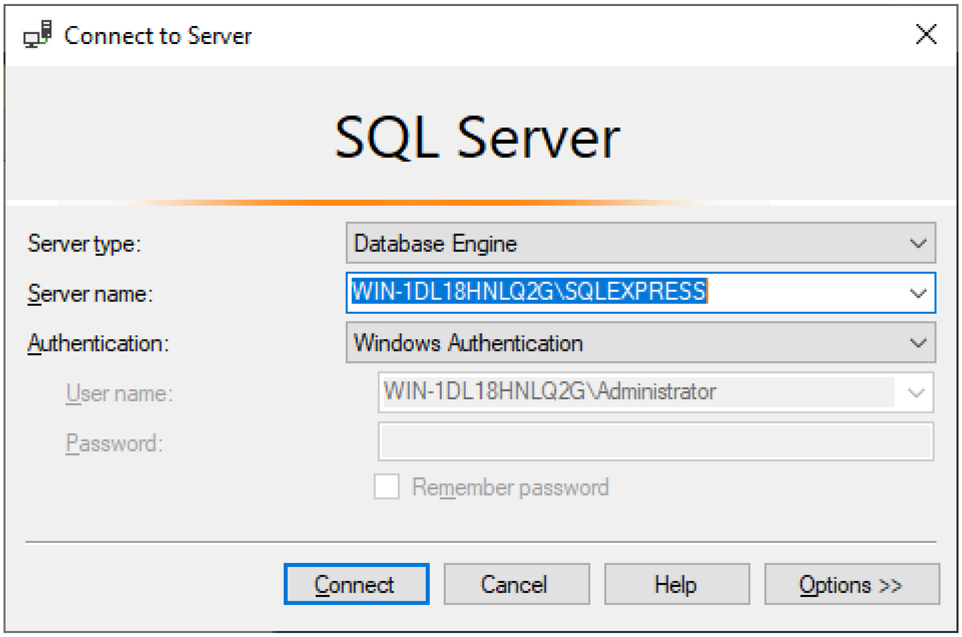
This section provides the procedures for configuring Event Intelligence. The procedures include the following areas:

- Administer agent logins
- Administer reason codes
- Administer CA certificate
- Administer TSLIB.INI
- Restart service

The configuration of Event Intelligence is performed by the IntraNext Support team and the procedural steps are presented in these Application Notes for information purposes only.

8.1. Administer Agent Logins

From the Event Intelligence server, navigate to **Start → Microsoft SQL Server Management Studio 18 → Microsoft SQL Server Management Studio 18** to launch and connect to the SQL server.



Connect to Server

SQL Server

Server type: Database Engine

Server name: WIN-1DL18HNLQ2G\SQLEXPRESS

Authentication: Windows Authentication

User name: WIN-1DL18HNLQ2G\Administrator

Password:

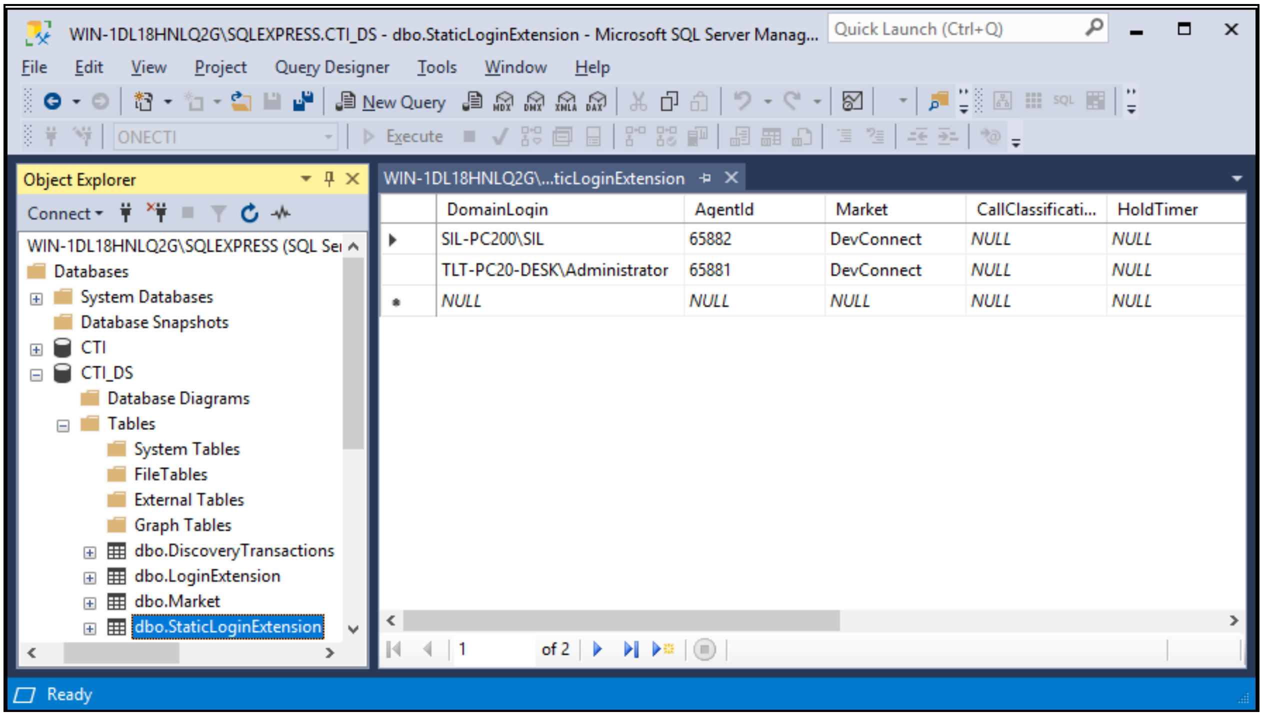
□ Remember password

Navigate to **Databases → CTI_DS → Tables → dbo.StaticLoginExtension** in the left pane, right click on the entry and select **Edit Top 200 Rows**.

Set the following values for the specified fields and retain the default values for the remaining fields.

- **DomainLogin:** The applicable domain and agent login name in the customer network.
- **AgentId:** The assigned agent ID from **Section 3** to this agent.
- **Market:** The applicable pre-existing market, in this case "DevConnect."

Repeat this section to create an entry for each agent from **Section 3**. In the compliance testing, two entries were created as shown below.

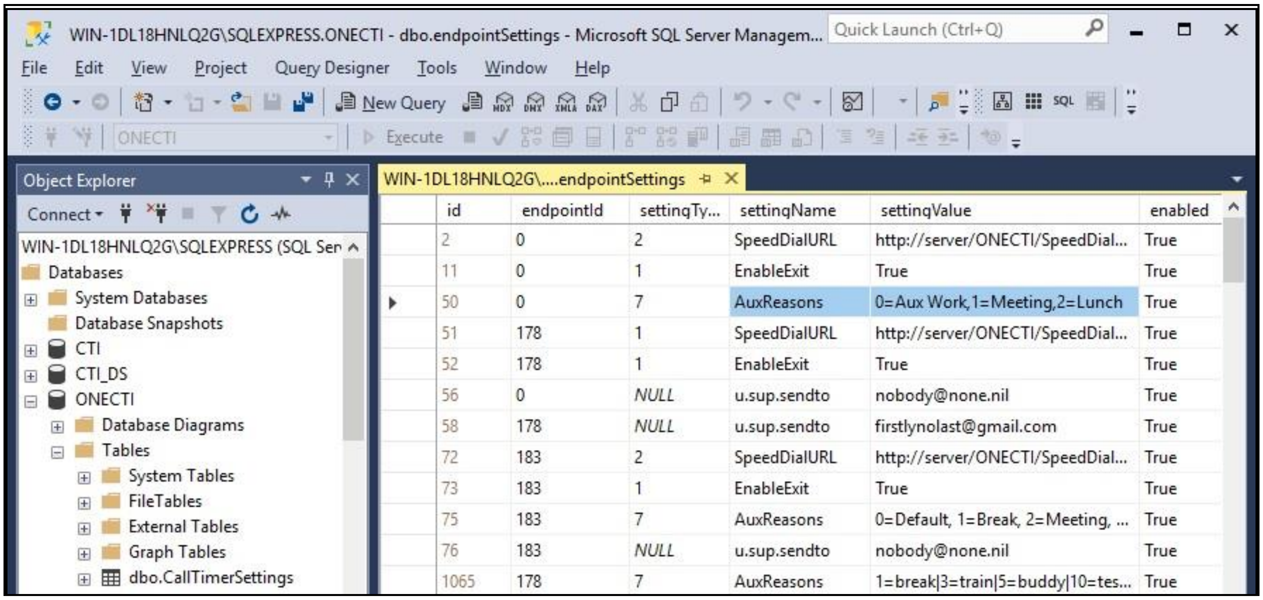


	DomainLogin	AgentId	Market	CallClassificati...	HoldTimer
▶	SIL-PC200\SIL	65882	DevConnect	NULL	NULL
	TLT-PC20-DESK\Administrator	65881	DevConnect	NULL	NULL
*	NULL	NULL	NULL	NULL	NULL

8.2. Administer Reason Codes

Navigate to **Databases → ONECTI → Tables → dbo.endpointSettings** (not shown) in the left pane, right click on the entry and select **Edit Top 200 Rows**.

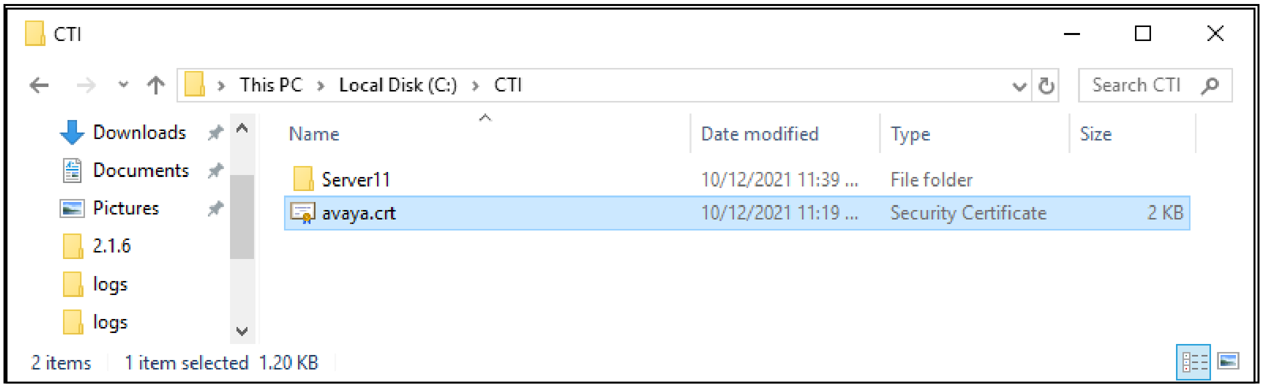
Locate the applicable **AuxReasons** entry and set **settingValue** to the reason code value and name from **Section 3**. Note that the setting also included the default reason code value of "**0**" and name "**Aux Work**" as shown below.



id	endpointId	settingTy...	settingName	settingValue	enabled
2	0	2	SpeedDialURL	http://server/ONECTI/SpeedDial...	True
11	0	1	EnableExit	True	True
50	0	7	AuxReasons	0=Aux Work,1=Meeting,2=Lunch	True
51	178	1	SpeedDialURL	http://server/ONECTI/SpeedDial...	True
52	178	1	EnableExit	True	True
56	0	*NULL*	u.sup.sendto	nobody@none.nil	True
58	178	*NULL*	u.sup.sendto	firstlynolast@gmail.com	True
72	183	2	SpeedDialURL	http://server/ONECTI/SpeedDial...	True
73	183	1	EnableExit	True	True
75	183	7	AuxReasons	0=Default, 1=Break, 2=Meeting, ...	True
76	183	*NULL*	u.sup.sendto	nobody@none.nil	True
1065	178	7	AuxReasons	1=break|3=train|5=buddy|10=tes...	True

8.3. Administer CA Certificate

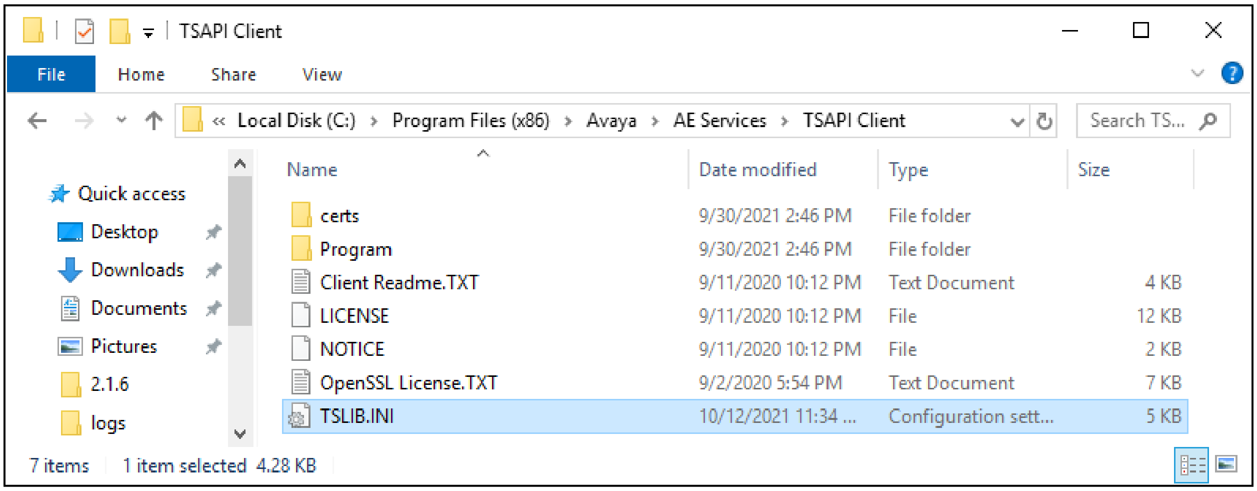
From the Event Intelligence server, copy the CA certificate **avaya.crt** from **Section 6.8** and place under a desired directory as shown below.



Name	Date modified	Type	Size
Server11	10/12/2021 11:39 ...	File folder	
avaya.crt	10/12/2021 11:19 ...	Security Certificate	2 KB

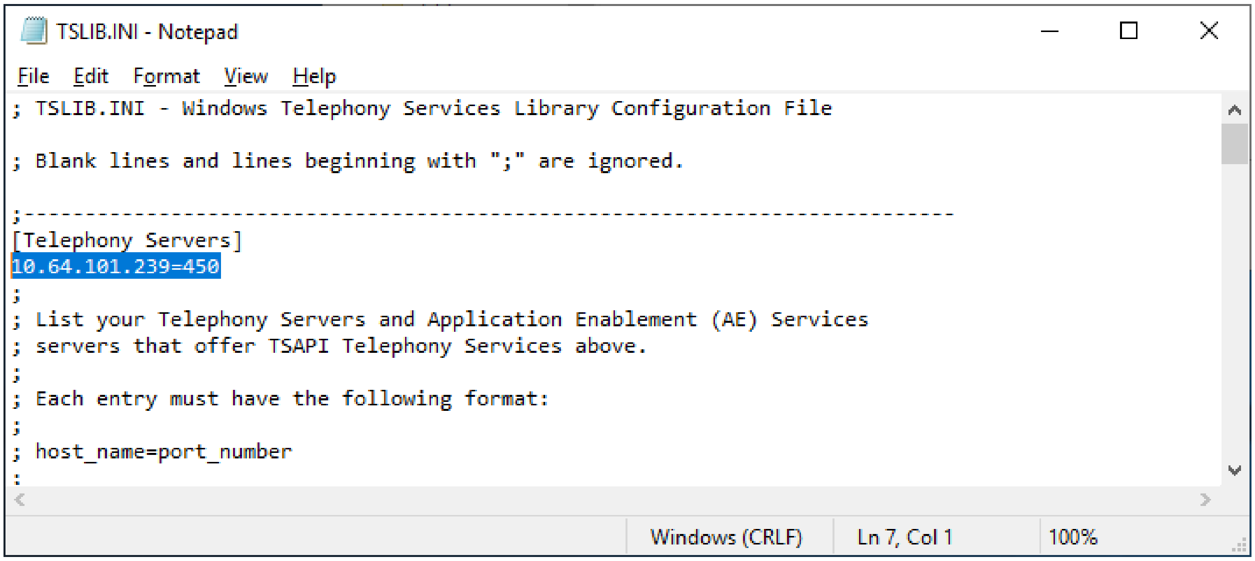
8.4. Administer TSLIB.INI

Navigate to the **C:\Program Files (x86)\Avaya\AE Services\TSAPI Client** directory to edit the **TSLIB.INI** file shown below.



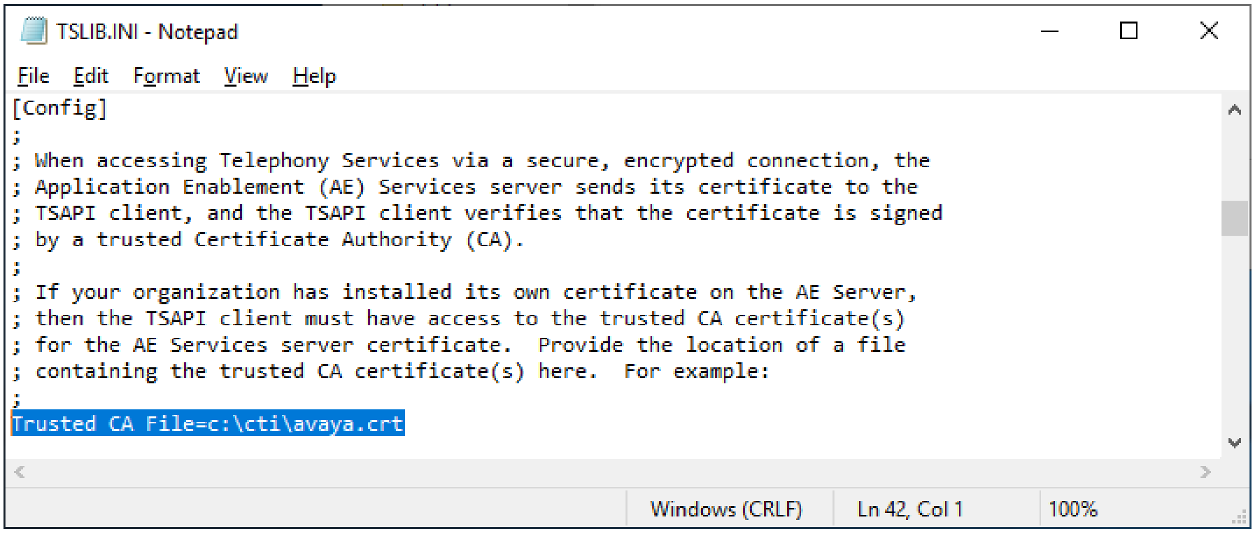
Name	Date modified	Type	Size
certs	9/30/2021 2:46 PM	File folder	
Program	9/30/2021 2:46 PM	File folder	
Client Readme.TXT	9/11/2020 10:12 PM	Text Document	4 KB
LICENSE	9/11/2020 10:12 PM	File	12 KB
NOTICE	9/11/2020 10:12 PM	File	2 KB
OpenSSL License.TXT	9/2/2020 5:54 PM	Text Document	7 KB
TSLIB.INI	10/12/2021 11:34 ...	Configuration sett...	5 KB

In the **Telephony Servers** sub-section, enter an entry shown below, where “**10.64.101.239=450**” is the IP address of Application Enablement Services and the default port number that the TSAPI Service is listening on.



```
; TSLIB.INI - Windows Telephony Services Library Configuration File

; Blank lines and lines beginning with ";" are ignored.

;----------------------------------------------------------------------------
[Telephony Servers]
10.64.101.239=450
;
; List your Telephony Servers and Application Enablement (AE) Services
; servers that offer TSAPI Telephony Services above.
;
; Each entry must have the following format:
;
; host_name=port_number
;
```

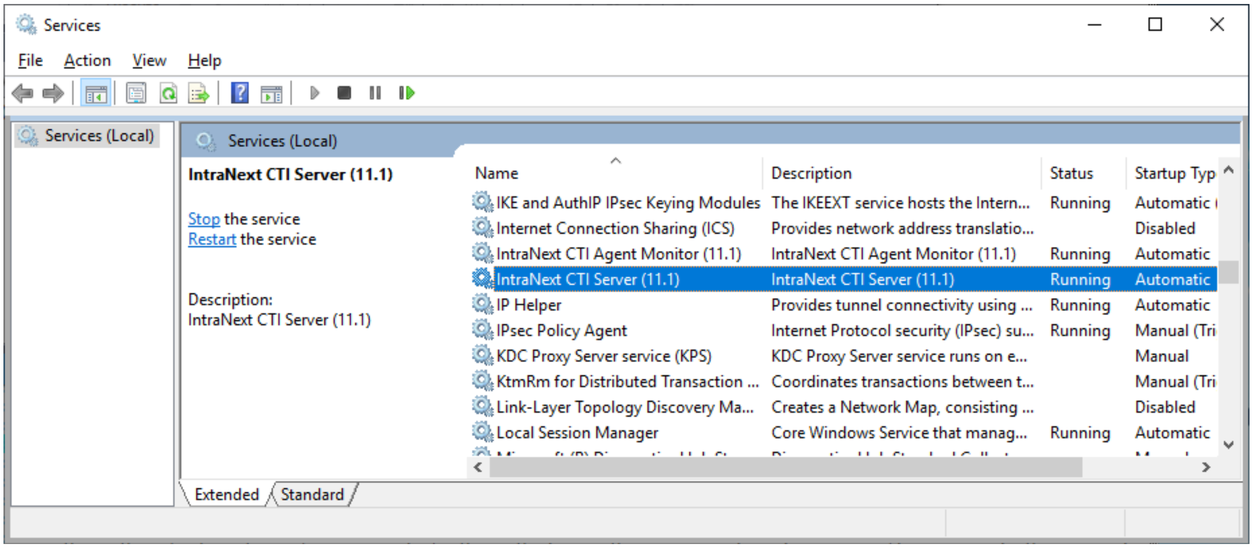
Scroll down to the **Config** sub-section, enter an entry shown below with the path and file name of the CA certificate from **Section 8.3**.



```
[Config]
;
; When accessing Telephony Services via a secure, encrypted connection, the
; Application Enablement (AE) Services server sends its certificate to the
; TSAPI client, and the TSAPI client verifies that the certificate is signed
; by a trusted Certificate Authority (CA).
;
; If your organization has installed its own certificate on the AE Server,
; then the TSAPI client must have access to the trusted CA certificate(s)
; for the AE Services server certificate.  Provide the location of a file
; containing the trusted CA certificate(s) here.  For example:
;
Trusted CA File=c:\cti\avaya.crt
```

8.5. Restart Service

From the Event Intelligence server, select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Restart the **IntraNext CTI Server (11.1)** service shown below.



IntraNext CTI Server (11.1)

Stop the service
Restart the service

Description:
IntraNext CTI Server (11.1)

Name	Description	Status	Startup Typ
IKE and AuthIP IPsec Keying Modules	The IKEEXT service hosts the Intern...	Running	Automatic (
Internet Connection Sharing (ICS)	Provides network address translatio...		Disabled
IntraNext CTI Agent Monitor (11.1)	IntraNext CTI Agent Monitor (11.1)	Running	Automatic
IntraNext CTI Server (11.1)	IntraNext CTI Server (11.1)	Running	Automatic
IP Helper	Provides tunnel connectivity using ...	Running	Automatic
IPsec Policy Agent	Internet Protocol security (IPsec) su...	Running	Manual (Tri
KDC Proxy Server service (KPS)	KDC Proxy Server service runs on e...		Manual
KtmRm for Distributed Transaction ...	Coordinates transactions between t...		Manual (Tri
Link-Layer Topology Discovery Ma...	Creates a Network Map, consisting ...		Disabled
Local Session Manager	Core Windows Service that manag...	Running	Automatic

9. Verification Steps

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

9.1. Verify Avaya Aura® Communication Manager

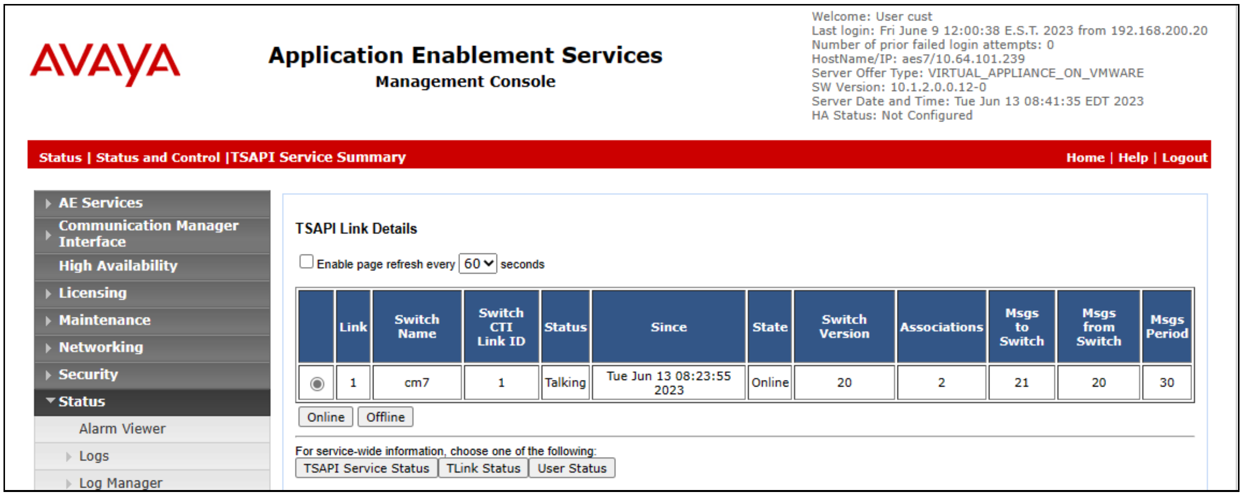
On Communication Manager, verify status of the administered CTI link by using the "**status aesvcs cti-link**" command. Verify that the **Service State** is "**established**" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1      12       no    aes7             established   49        49
```

9.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) 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 logged in agents from **Section 3**, in this case "**2**".



Welcome: User cust
Last login: Fri June 9 12:00:38 E.S.T. 2023 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 10.1.2.0.0.12-0
Server Date and Time: Tue Jun 13 08:41:35 EDT 2023
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	cm7	1	Talking	Tue Jun 13 08:23:55 2023	Online	20	2	21	20	30

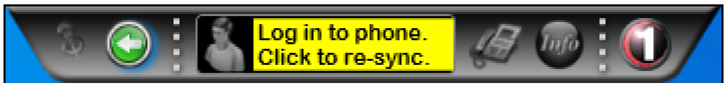
Online Offline

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

TSAPI Service Status TLink Status User Status

9.3. Verify IntraNext Event Intelligence

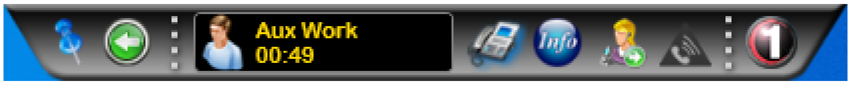
From an agent PC, select **Start → ONECTI** to launch the application. The OneCTI tool bar below is displayed.



Log in to phone.
Click to re-sync.

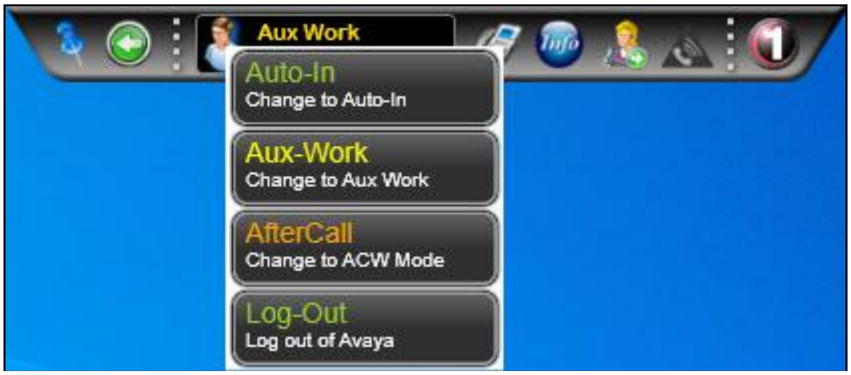
Use the agent's hard phone or soft phone to log the agent into the ACD on Communication Manager, followed by clicking on **Click to re-sync** shown above.

Verify that the OneCTI tool bar is updated to reflect the work mode the agent is in, in this case "**Aux Work**" as shown below.

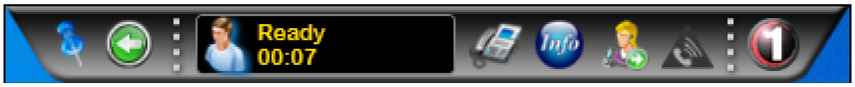


Aux Work
00:49

Select the **Change Work Mode** person icon and select **Auto-In** from the drop-down list.



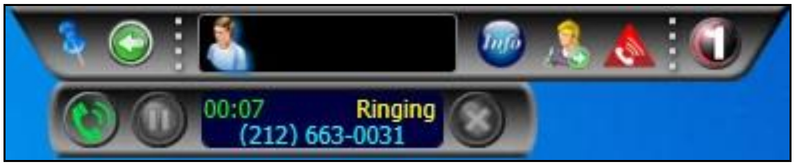
Verify that the OneCTI toolbar is updated to reflect **Ready** as shown below.



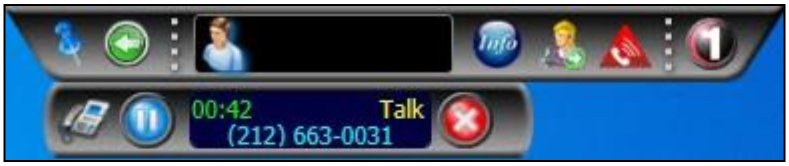
Ready
00:07

Make an incoming ACD call from the PSTN. Verify that a phone bar is displayed along with the PSTN caller number and **Ringing** as shown below.

Click on the green **Answer this call** icon to answer the call.



Verify that the agent is connected to the PSTN caller with a two-way talk path, and that the phone bar is updated to reflect **Talk** as shown below.



10. Conclusion

These Application Notes describe the configuration steps required for IntraNext Event Intelligence 11.2 to successfully interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1. 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.

4. *IntraNext Event Intelligence Computer Telephony Integration (CTI)*, available upon request to IntraNext Support.

5. *IntraNext Systems OneCTI User Guide*, available upon request to IntraNext 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.