Avaya Solution & Interoperability Test Lab

Application Notes for IntraNext Event Intelligence and OneCTI desktop client with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for IntraNext Event Intelligence and OneCTI desktop client to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1.

The compliance testing focused on the telephony integration with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Telephony Services Application Programming Interface and Device Media and Call Control Application Programming Interface.

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 for IntraNext Event Intelligence (Event Intelligence) and OneCTI desktop client to interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1.

The compliance testing focused on the telephony integration with Avaya Aura® Communication Manager via the Avaya Aura® Application Enablement Services Telephony Services Application Programming Interface (TSAPI) and Device Media and Call Control (DMCC) Application Programming Interface.

Event Intelligence uses TSAPI and DMCC for providing screen synchronization and softphone telephony controls. OneCTI is a highly customized desktop client supporting enhanced call transfer, customer DTMF interaction, and various agent information interactions.

2. General Test Approach and Test Results

The general test approach was to verify the integration of TSAPI and DMCC events to trigger appropriate actions on OneCTI desktop client, and typical CTI functionality. Combination of only DMCC, only TSAPI, and both DMCC and TSAPI were tested. In addition, serviceability tests were also performed to assess the reliability and accuracy of the solution.

For the manual part of the testing, incoming ACD calls were placed with available agents logged on OneCTI desktop client. All necessary call actions were initiated from the OneCTI desktop client, whenever possible:

The serviceability test cases were performed manually by disconnecting and reconnecting the Ethernet connection to the Event Intelligence server and 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 these Application Notes, the interface between Avaya systems and Event Intelligence utilized enabled capabilities of secure connectivity of TSAPI and DMCC.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the:

- TSAPI and DMCC connectivity via secure interface.
- Incoming and outgoing PSTN calls via OneCTI desktop client and Avaya Deskphones.
- Incoming and outgoing intra-agent calls via OneCTI desktop client and Avaya Deskphones.
- Agent state changes via OneCTI desktop client and Avaya Deskphones; logon, logoff, aux-work, acw, etc.
- Call control features such as Hold, Conferences and Transfers via OneCTI desktop client and Avaya Deskphones.
- Adjunct routing incoming calls to Event Intelligence.
- DTMF detection by Event Intelligence.

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

2.2. Test Results

All test cases were executed and verified.

2.3. Support

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

- **Phone:** US 1-800-928-6398
- **Email:** support@intranext.com
- **Web:** http://www.intranext.com

3. Reference Configuration

Event Intelligence was can be deployed on a virtual machine running on a virtualization platform. OneCTI desktop client was installed on Windows 10 PC.

The detailed administration of basic connectivity between Communication Manager and Application Enablement Services is not the focus of these Application Notes and will not be described.

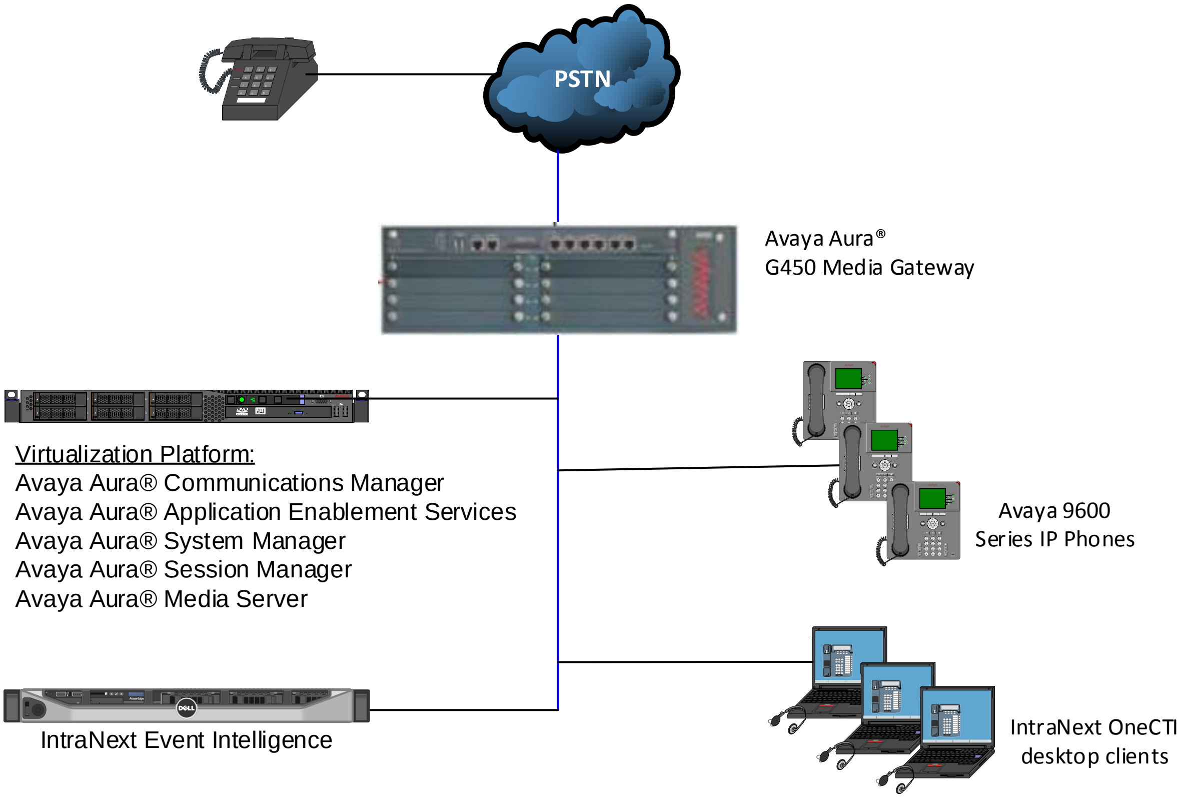

PSTN
Avaya Aura®
G450 Media Gateway
Virtualization Platform:
Avaya Aura® Communications Manager
Avaya Aura® Application Enablement Services
Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya Aura® Media Server
Avaya 9600
Series IP Phones
IntraNext Event Intelligence
IntraNext OneCTI
desktop clients

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 on a Virtual Machine	R017x.01.0.532.0 7.1.2.0.0-FP2
Avaya G450 Media Gateway	38.20.1/1
Avaya Aura® Media Server	7.8.0.309
Avaya Aura® Application Enablement Services	7.1.2.0.0.3
Avaya Aura® System Manager	7.1.2.0.07353
Avaya Aura® Session Manager	7.1.2.0.712004
Avaya 9611G IP Deskphone (SIP)	7.1.1.0
Avaya 9641G IP Deskphone (H.323)	6.6.6
IntraNext: • Event Intelligence running on Windows 2012 R2 server • OneCTI desktop client on Windows 10 PC	11.1.10.5 10.7.1.6

5. Configure Avaya Aura® Communication Manager

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

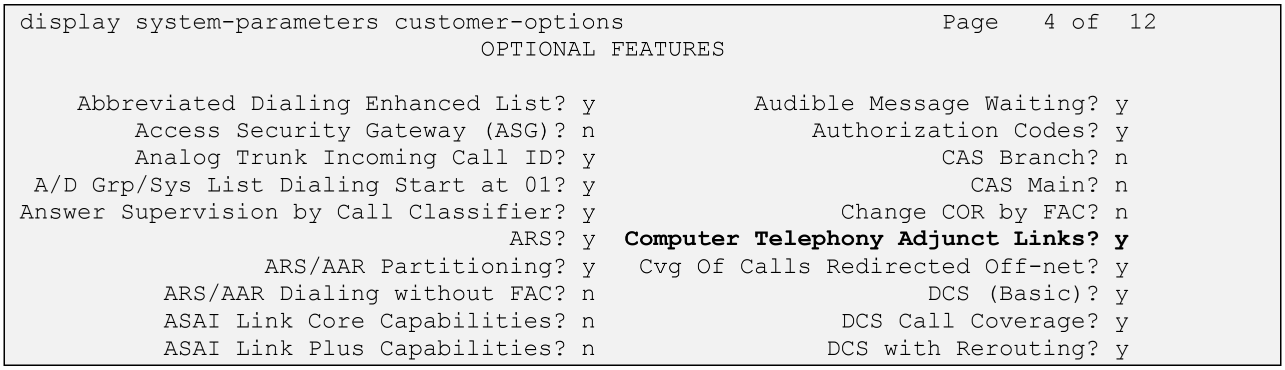
- Verify license
- Administer CTI link
- Administer system parameters features
- Obtain reason codes
- Administer DMCC Stations

The table below shows a sample call center data that was used during compliance testing.

Station	Agent	Hunt Group/Extension	VDN	Vector
50001	5001	1/23001	22001	1
50002	5002	2/23002	22002	2
50101	5003			

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? n                       DCS (Basic)? y
          ASAI Link Core Capabilities? n                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? n                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: 69999
     Type: ADJ-IP
                                                                        COR: 1
     Name: AES CTI Link
```

5.3. 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: 1
```

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? 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
```

5.4. Obtain Reason Codes

For contact centers 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 by OneCTI desktop client.

```
change reason-code-names                                        Page   1 of   1

                                REASON CODE NAMES

                           Aux Work/           Logout
                        Interruptible?

        Reason Code 1: Break           /n
        Reason Code 2: Support         /n
        Reason Code 3: Lunch           /n
        Reason Code 4: Training        /n
        Reason Code 5: Meeting         /n
        Reason Code 6:                 /n
        Reason Code 7:                 /n
        Reason Code 8:                 /n
        Reason Code 9:                 /n

  Default Reason Code:
```

5.5. Administer DMCC Stations

Add DMCC Stations as needed using the “add station n” command, where “n” is an available extension number. Enter “9641” in **Type** field. Enter a desired name in **Name** field. Set a security code in **Security Code** field. Set **IP Softphone** to “y.”

```
add station 55551                                           Page   1 of   5
                                     STATION

Extension: 55551                         Lock Messages? n               BCC: 0
     Type: 9641                          Security Code: *                TN: 1
     Port: S00037                      Coverage Path 1:                 COR: 1
     Name: DMCC Station 1              Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19        Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 55551
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y
```

6. Configure Avaya Aura® Application Enablement Services

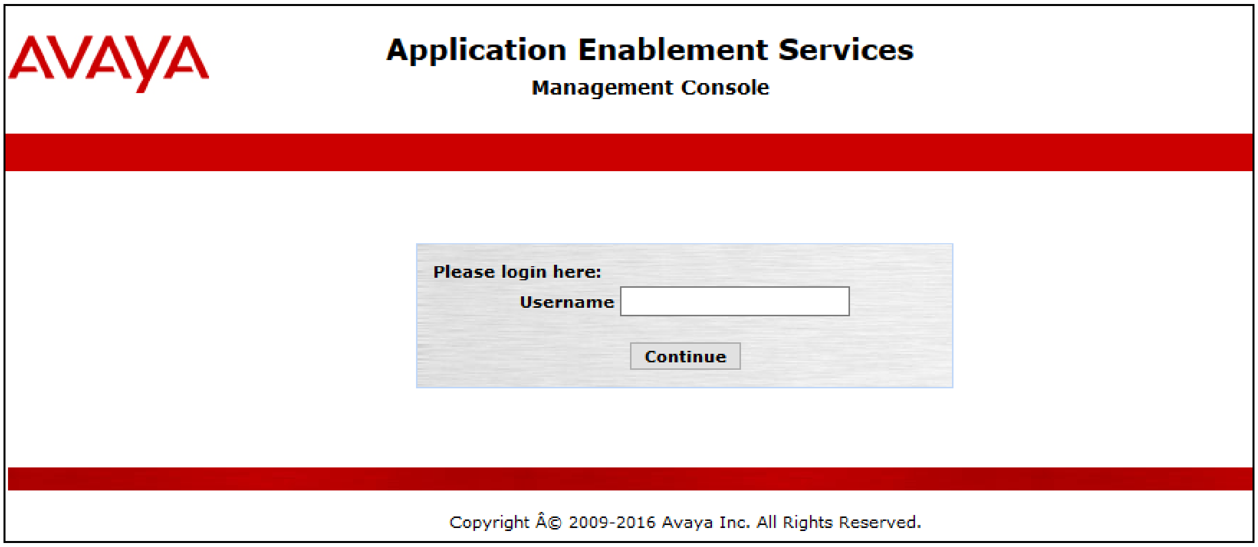
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Administer TSAPI link
- Restart service
- Obtain Tlink name
- Administer Event Intelligence user

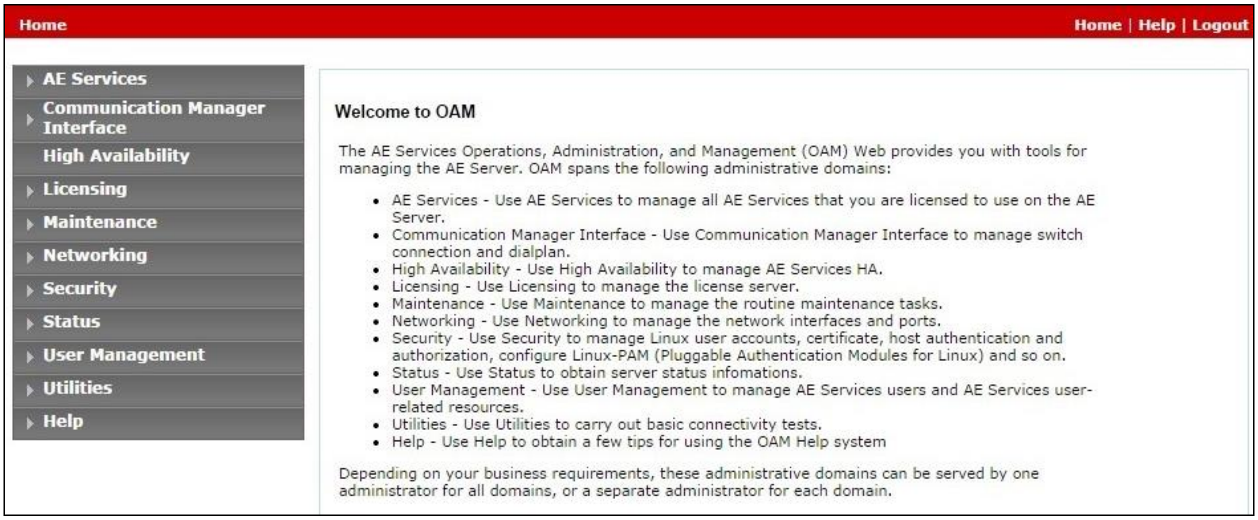
6.1. Launch OAM Interface

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.


AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Continue
Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

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



Welcome to OAM

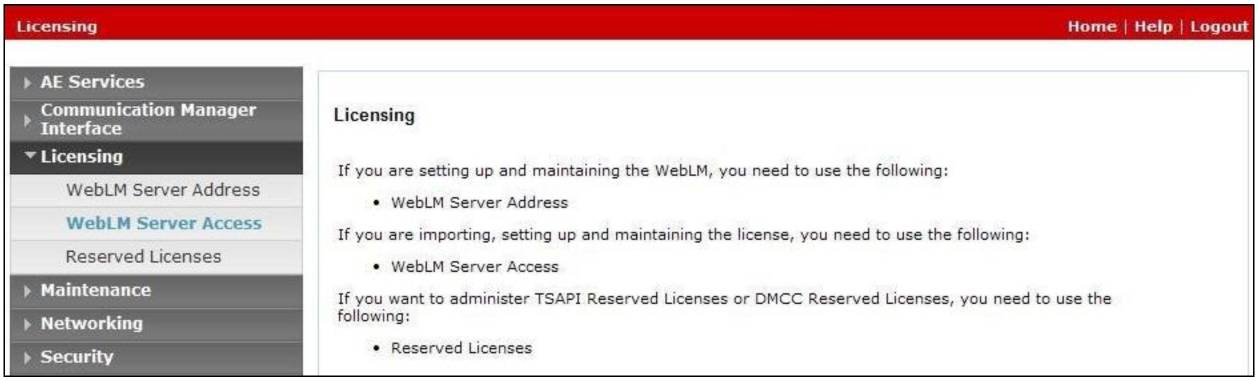
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

- 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 infomations.
- 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 **Web License Manager** pop-up screen (not shown), and log in using the appropriate credentials.



Licensing

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

- WebLM Server Address

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

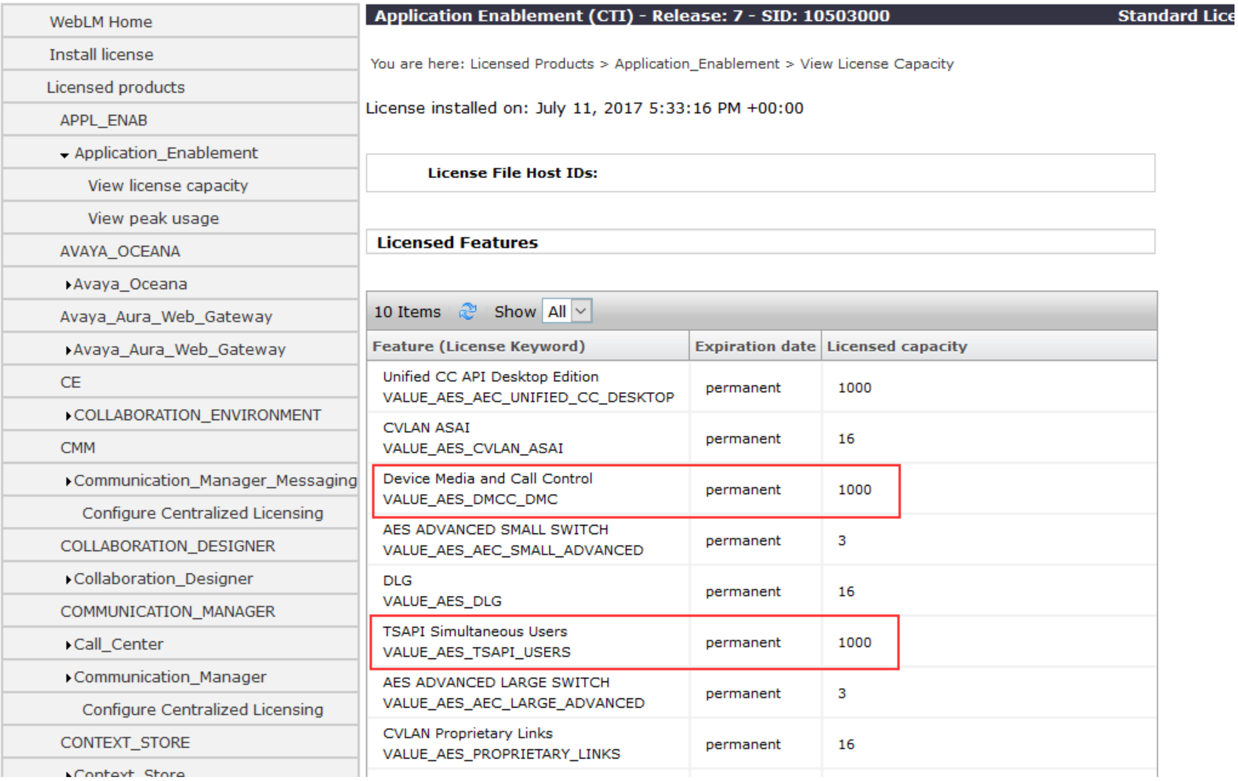
- WebLM Server Access

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

- Reserved Licenses

The **Web License Manager** 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 **Device Media and Call Control** for DMCC and **TSAPI Simultaneous Users** for TSAPI, as shown below.



Application Enablement (CTI) - Release: 7 - SID: 10503000 Standard Lice

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

License installed on: July 11, 2017 5:33:16 PM +00:00

License File Host IDs:

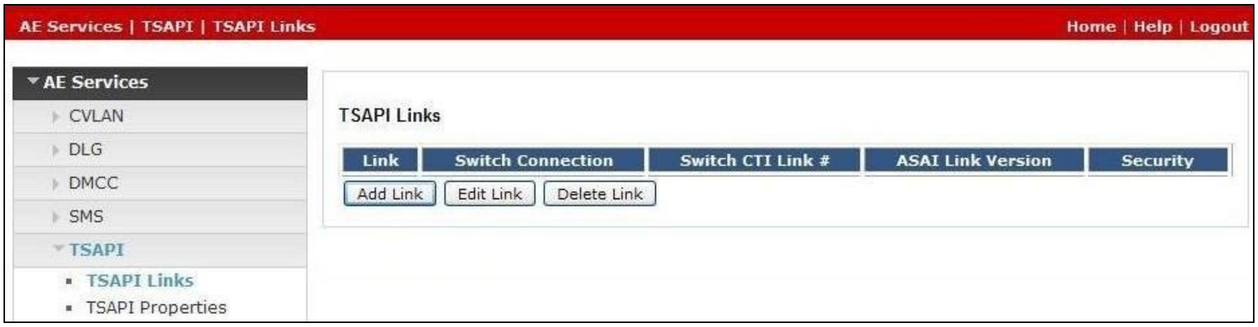
Licensed Features

10 Items Show All

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

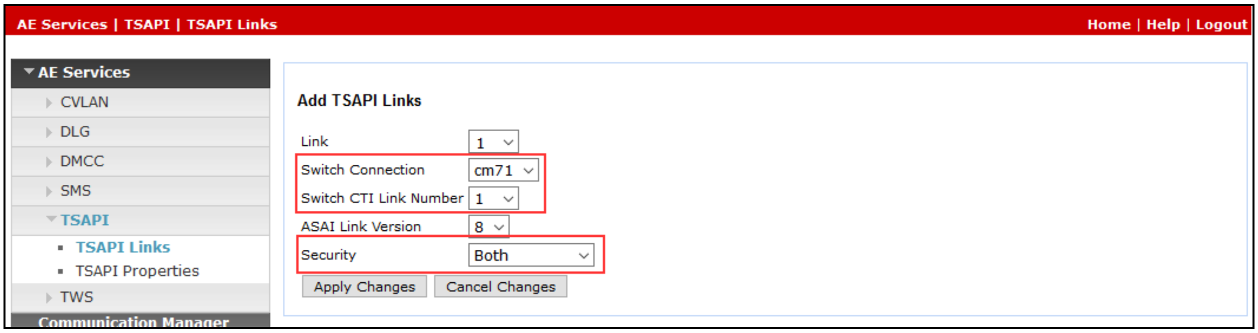


TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

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 “cm71” is selected. For **Switch CTI Link Number**, select the CTI link number from **Section 5.2**. For **Security,** select “Both.” Retain the default values in the remaining fields.

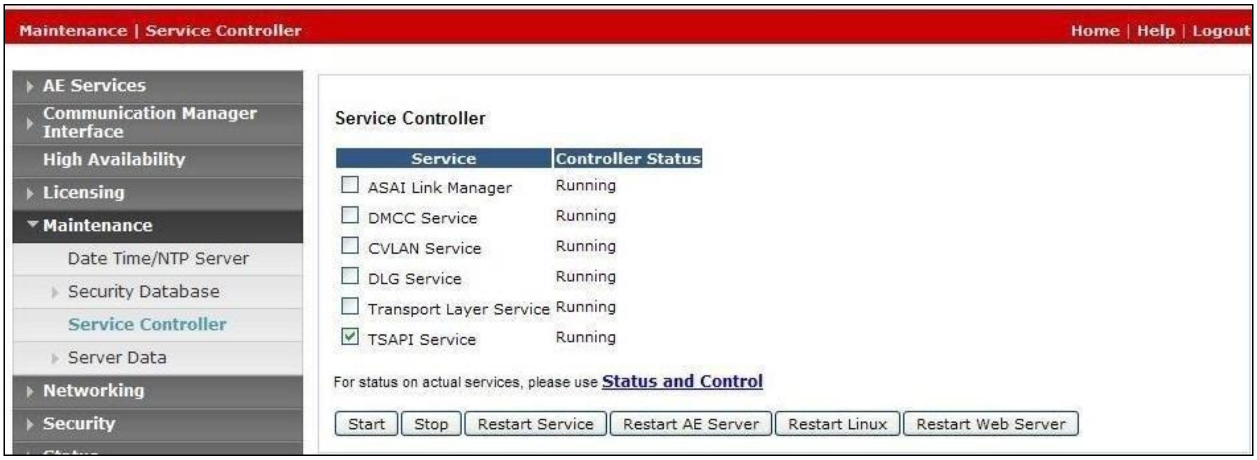


Add TSAPI Links

Link	1
Switch Connection	cm71
Switch CTI Link Number	1
ASAI Link Version	8
Security	Both

6.4. 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**.



Service Controller

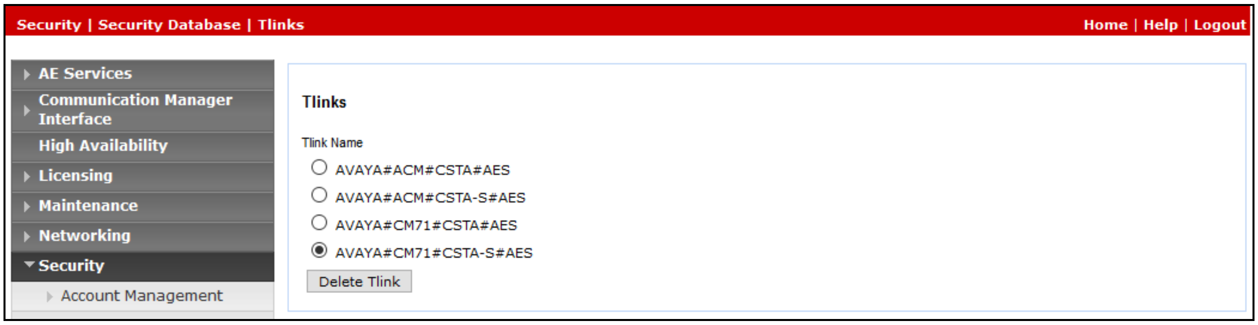
Service	Controller Status
□ ASAI Link Manager	Running
□ DMCC Service	Running
□ CVLAN Service	Running
□ DLG Service	Running
□ Transport Layer Service	Running
☑ TSAPI Service	Running

For status on actual services, please use Status and Control

6.5. 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 associated Tlink name, to be used for configuring Event Intelligence.

In this case, the associated Tlink name is "AVAYA#**CM71**#CSTA-S#AES". Note the use of the switch connection "CM71" from **Section 6.3** as part of the Tlink name.



Tlinks

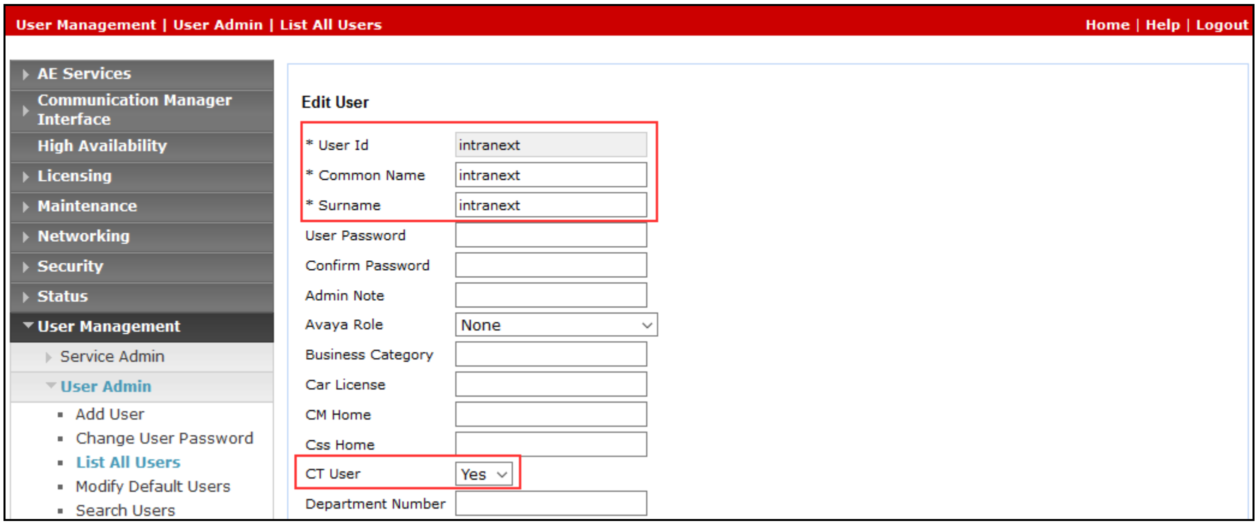
Tlink Name

○ AVAYA#ACM#CSTA#AES
○ AVAYA#ACM#CSTA-S#AES
○ AVAYA#CM71#CSTA#AES
● AVAYA#CM71#CSTA-S#AES

6.6. Administer Event Intelligence 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.

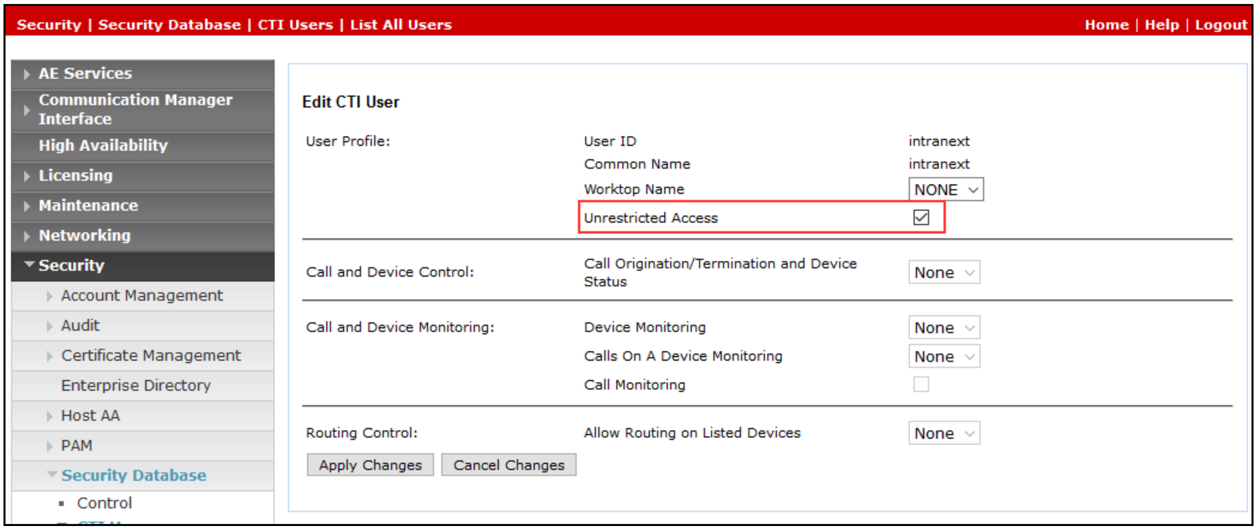


Edit User

* 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	

Select **Security → Security Database → CTI Users → List All User** from the left pane and Edit the user created above.

Check box for **Unrestricted Access** as shown below:



Edit CTI User

User Profile:	User ID	intranext
	Common Name	intranext
	Worktop Name	NONE
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	☐
Routing Control:	Allow Routing on Listed Devices	None

7. Configure IntraNext Event Intelligence and OneCTI desktop client.

All configurations related to Event Intelligence and OneCTI desktop client is performed by IntraNext engineers and, thus, is not documented.

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

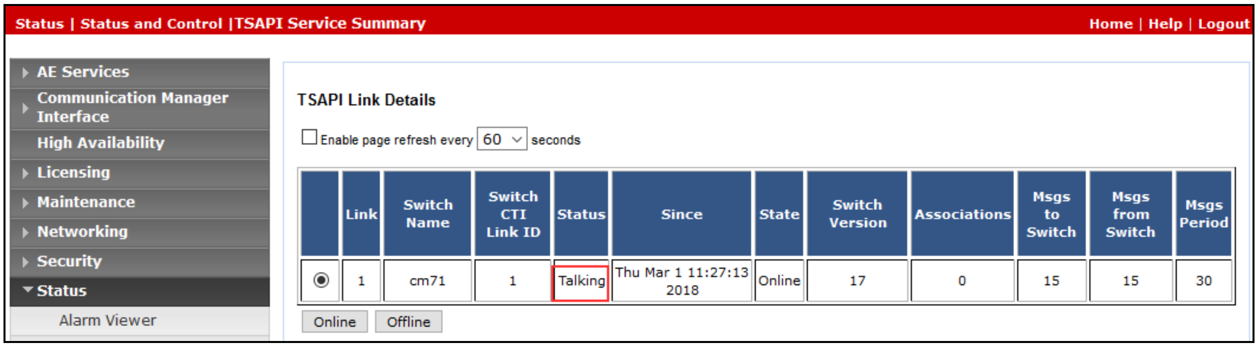
On Communication Manager, verify the status of the administered CTI link by using the "status aesvcs cti-link" command. Verify that the **Service State** is "established" for the CTI link number administered in **Section 5.2**, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     8        no    aes               established   15       15
```

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** from the left pane (not shown). The **TSAPI Link Details** screen is displayed.

Verify the **Status** is "Talking" for the TSAPI link administered in **Section 6.3**.



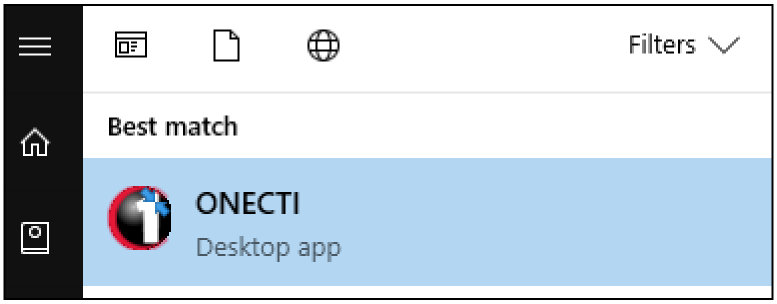
TSAPI Link Details

☐ Enable page refresh every 60 seconds

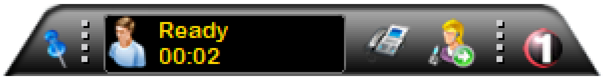
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
◉	1	cm71	1	Talking	Thu Mar 1 11:27:13 2018	Online	17	0	15	15	30

8.3. Verify OneCTI desktop client

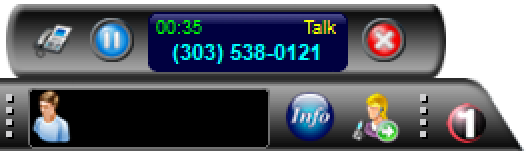
Ensure an agent is already logged onto Avaya Deskphone. From the agent desktop PC, launch ONECTI application.



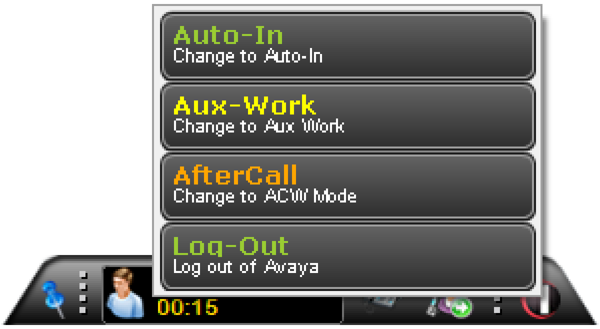
The ONECTI application automatically detects agent logon.



Place a call to the agent extension and answer the call via ONECTI application.



Chance various agent states and ensure, it gets updated on Communication Manager.



9. Conclusion

These Application Notes describe the configuration steps required for IntraNext Event Intelligence to successfully interoperate with Avaya Aura® Communication Manager 7.1 and Avaya Aura® Application Enablement Services 7.1. All feature and serviceability test cases were completed with observations noted in **Section 2.2**.

10. Additional References

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

1. *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 7.1, June 2017 available at http://support.avaya.com.

2. *Avaya Aura® Application Enablement Services Administration and Maintenance Guide*, Release 7.1, 02-300357, June 2017, available at http://support.avaya.com.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.