



## DevConnect Program

---

# Application Notes for iNEMSOFT CLASSONE iCAS 6.0 with Avaya Aura® Application Enablement Services 10.1 and Avaya Aura® Session Manager 10.1 – Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for iNEMSOFT CLASSONE iCAS 6.0 to interoperate with Avaya Aura® Communication Manager 10.1 and Avaya Aura® Application Enablement Services 10.1.

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 Avaya DevConnect Program.

# 1. Introduction

These Application Notes contain instructions for iNEMSOFT CLASSONE iCAS (iCAS) with Avaya Aura® Session Manager (Session Manager), Avaya Aura® Communication Manager (Communication Manager) and Avaya Aura® Application Enablement Services (AES) to successfully interoperate.

The iCAS solution is a system-of-systems, enabling operators to take control of their communications network and manage multiple transactions from many types of devices.

The iCAS solution enables operators to handle inbound calls, connect with radio dispatch, bridge various radio talk groups and frequencies with each other and with back-office voice systems, collaborate and manage field operations regardless of the type of voice-enabled device, while maintaining the highest level of business continuity and interoperability. iCAS as a solution integrates with several interfaces provided by Avaya products. However, this document only contains instructions for iCAS Server and iCAS Dispatch Console with Session Manager. iCAS Dispatch Console registers to Session Manager as a SIP Endpoint and uses TSAPI via AES for inbound VDN call routing. Application notes related to other interfaces may be obtained via Avaya Support site.

- Application Notes for iNEMSOFT CLASSONE iCAS IP Radio Gateway with Avaya Aura® Session Manager

## 2. General Test Approach and Test Results

The feature test cases were performed manually. At startup the Dispatch Console registers with Session Manager as two SIP users via a non-encrypted connection and iCAS Server registers via TSAPI with a non-encrypted connection.

Incoming VDN calls were placed to iCAS Server from internal stations and external callers and outbound calls were placed from iCAS Server linking parties using radio devices and end-users on traditional hard and softphones.

The main objectives were to verify the following:

- Registration
- Codecs (G.711MU)
- Inbound PSTN calls
- Internal calls
- Outbound calls
- Call hold/unhold
- Call transfer

- Call conference
- Call termination (origination/destination)
- DTMF tone generation and detection
- Radio operation and push to talk for audio transmit
- Serviceability
- IP Shuffling and Encryption were not tested

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.

For the testing associated with these Application Notes, the interface between Avaya systems and iCAS 6.0 did not include use of any specific encryption features as requested by iNemsoft.

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.

## **2.1. Interoperability Compliance Testing**

The interoperability compliance test included features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on iCAS Dispatch Console. iCAS Dispatch Console operations such as inbound calls, outbound calls, transfer, conference, and hold/resume, and iCAS Dispatch Console interactions with Session Manager, Communication Manager, AES, and Avaya SIP, Avaya H.323 hardphones and Avaya Agent for Desktop softphones were verified. The serviceability testing introduced failure scenarios to see if iCAS Dispatch Console can recover from failures such as network and power failures of the iCAS Servers.

## **2.2. Test Results**

During compliance testing, iNEMSOFT CLASSONE Dispatch Console successfully registered with Avaya Aura® Session Manager, placed and received calls to and from Avaya endpoints.

## 2.3. Support

Technical support on iCAS can be obtained through the following:

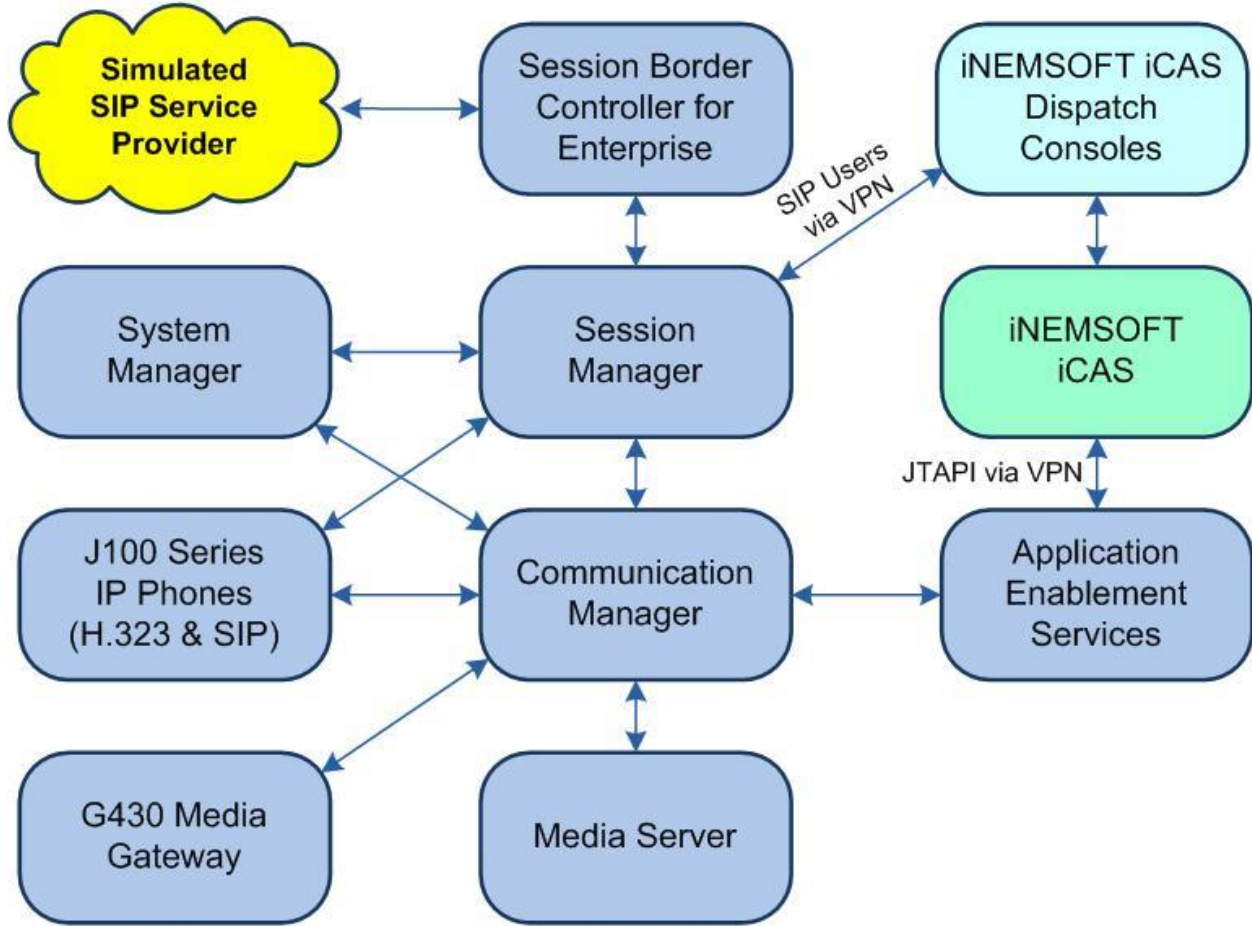
- **Phone:** (214) 423-2815
- **Email:** [rtisupport@inemsoft.com](mailto:rtisupport@inemsoft.com)

## 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, iCAS stations associated with the Station IDs shown in the table below.

Device Type	Extension
iCAS Stations	66006, 66007 (SIP)



**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	10.1.2

Virtual Environment	(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
iNEMSOFT CLASSONE iCAS	6.0
iNEMSOFT CLASSONE iCAS Dispatch Console	6.0

## 5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer CTI link
- Administer system parameters features
- Vector with adjunct routing step
- VDN

## 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**.

```
Change system-parameters features                               Page 13 of 19
                        FEATURE-RELATED SYSTEM PARAMETERS

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

  Reporting for PC Non-Predictive Calls? N

  Agent/Caller Disconnect Tones? N
  Interruptible Aux Notification Timer (sec): 3
  Zip Tone Burst for Callmaster Endpoints: double

ASAI
  Copy ASAI UII During Conference/Transfer? N
  Call Classification After Answer Supervision? 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. Configure a Vector with Adjunct Route Step

Use “**change vector n**” to configure a Vector, where “**n**” is an available Vector number. Add the step to adjunct route to the cti link created in **Section 5.2**.

```
change vector 1001                                     Page 1 of 6
                                                    CALL VECTOR
Number: 1001                                           Name: ClassOne
Multimedia? N      Attendant Vectoring? N      Meet-me Conf? n      Lock? N
  Basic? Y      EAS? Y      G3V4 Enhanced? Y      ANI/II-Digits? Y      ASAI Routing? Y
  Prompting? Y      LAI? Y      G3V4 Adv Route? Y      CINFO? Y      BSR? Y      Holidays? Y
  Variables? Y      3.0 Enhanced? Y
01 wait-time      2      secs hearing ringback
02 adjunct      routing link 1
03 wait-time      30      secs hearing ringback
04
```

## 5.5. Configure a VDN

Use “**add vdn n**” to add a VDN, where “**n**” is an available VDN extension. On **Page 1**:

1. In the **Name** field, enter a name
2. In the **Destination** field, set Vector Number to the vector configured earlier in **Section 5.4**

```
add vdn 41001                                         Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER
Extension: 41001                                       Unicode Name? n
  Name*: ClassOne VDN
  Destination: Vector Number      1001
  Attendant Vectoring? N
  Meet-me Conferencing? N
  Allow VDN Override? N
  COR: 1
  TN*: 2
  Measured: none      Report Adjunct Calls as ACD*? N
```

## 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 iNEMSOFT user
- Administer security database
- Restart service
- Obtain Tlink name

### 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 screenshot shows the Avaya Application Enablement Services Management Console login screen. At the top left is the Avaya logo. To its right, the text reads "Application Enablement Services" and "Management Console". A red horizontal bar spans the width of the page, with the word "Help" in the top right corner. In the center of the page, there is a light gray rectangular box containing the text "Please login here:" followed by "Username" and a text input field. Below the input field is a "Continue" button.

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

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User cust, Last login: Wed July 5 11:49:28 E.S.T. 2023 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 10.1.2.0.0.12-0, Server Date and Time: Wed Jul 26 17:11:51 EDT 2023, HA Status: Not Configured. The main content area is titled 'Welcome to OAM' and contains a list of administrative domains and their functions. A left-hand navigation menu is visible with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. A red navigation bar at the top contains 'Home | Help | Logout'.

Welcome: User cust  
Last login: Wed July 5 11:49:28 E.S.T. 2023 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.2.0.0.12-0  
Server Date and Time: Wed Jul 26 17:11:51 EDT 2023  
HA Status: Not Configured

Home | Help | Logout

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

### Welcome to OAM

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

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

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

## 6.2. Verify License

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

The screenshot shows the Avaya Application Enablement Services Management Console with the 'WebLM Server Access' page selected. The top right corner displays system information: Welcome: User cust, Last login: Wed July 5 11:49:28 E.S.T. 2023 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 10.1.2.0.0.12-0, Server Date and Time: Wed Jul 26 17:19:38 EDT 2023, HA Status: Not Configured. The main content area is titled 'WebLM Server Access' and contains a list of instructions for accessing the WebLM server. A left-hand navigation menu is visible with categories like AE Services, Communication Manager Interface, High Availability, Licensing, Maintenance, Networking, Security, Status, User Management, Utilities, and Help. The 'Licensing' category is expanded, showing 'WebLM Server Address', 'WebLM Server Access', and 'Reserved Licenses'. A red navigation bar at the top contains 'Licensing | WebLM Server Access | Home | Help | Logout'.

Welcome: User cust  
Last login: Wed July 5 11:49:28 E.S.T. 2023 from 192.168.200.20  
Number of prior failed login attempts: 0  
HostName/IP: aes/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.2.0.0.12-0  
Server Date and Time: Wed Jul 26 17:19:38 EDT 2023  
HA Status: Not Configured

Licensing | WebLM Server Access | Home | Help | Logout

**AE Services**  
Communication Manager Interface  
High Availability  
Licensing  
WebLM Server Address  
WebLM Server Access  
Reserved Licenses  
Maintenance  
Networking  
Security  
Status  
User Management  
Utilities  
Help

### 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.

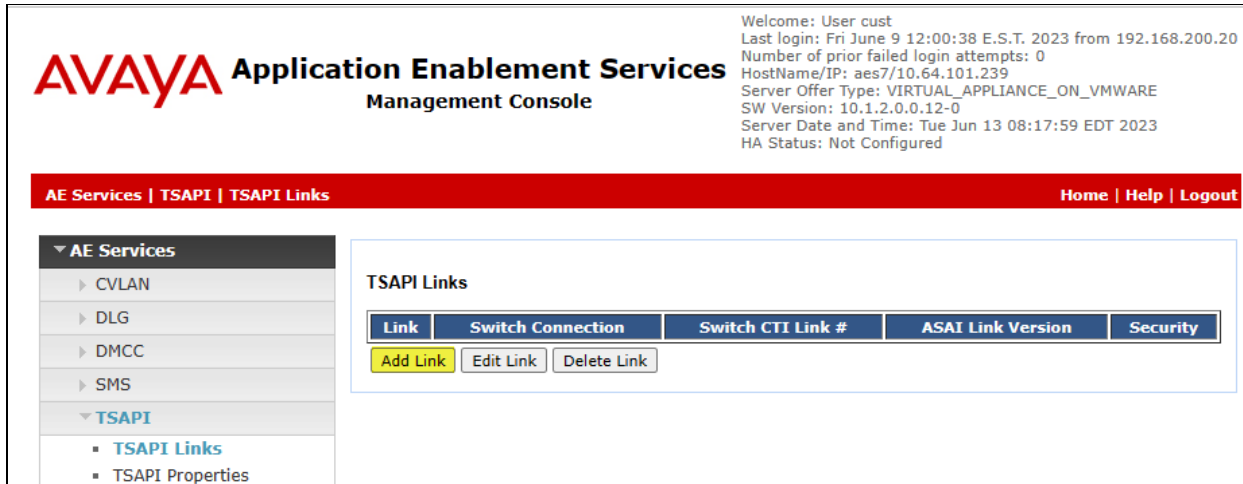
Verify that there are sufficient licenses for **TSAPI Simultaneous Users**, as shown below.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The left navigation pane is expanded to 'Application Enablement'. The main content area displays the 'Application Enablement (CTI) - Release: 10 - SID: 10503000(Enterprise license file)' page. The page includes a breadcrumb trail 'You are here: Licensed Products > Application Enablement > View by Feature', the license installation date 'License installed on: June 10, 2022 9:09:46 PM -04:00', and a 'License File Host IDs' field with the value 'V5-E1-B3-74-2B-9E-01'. Below this is a table of features and their capacities:

Feature (License Keyword)	License Capacity
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	1000
CVLAN ASA1 (VALUE_AES_CVLAN_ASA1)	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	

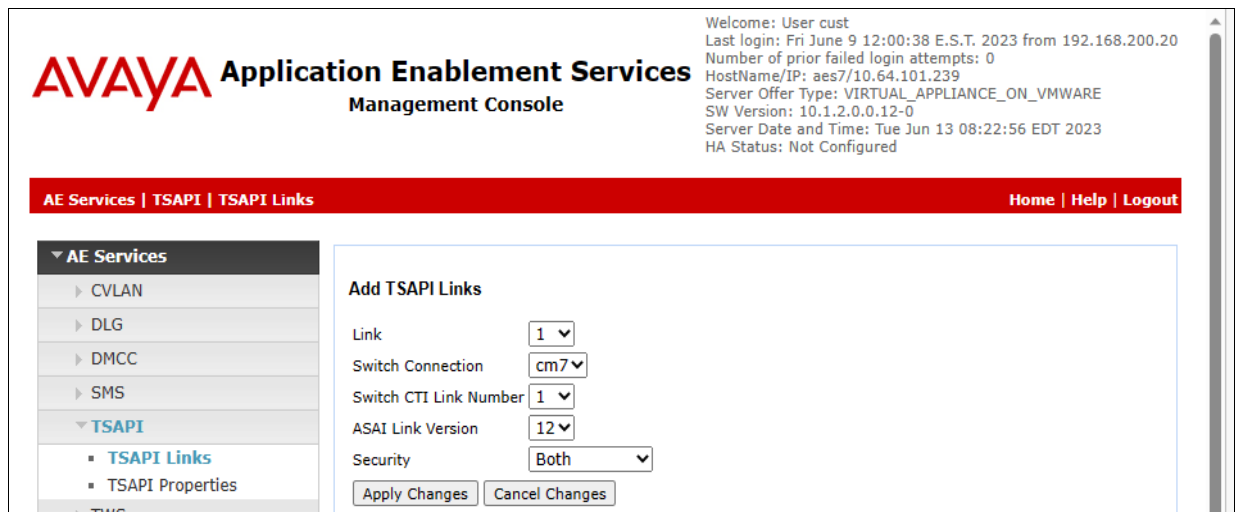
### 6.3. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane of the **Management Console**, to administer a TSAPI link. The **TSAPI Links** screen is displayed, as shown below. Click **Add Link**.



The **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.



## 6.4. Administer iNEMSOFT ClassOne iCAS CTI Users

There are three CTI Users configured for the iCAS application: **rtidrouter1**, **rtirouter1** and **rtitele**. For the purposes of this document only **rtitele** is displayed. All three are created with the same permission.

Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane.

Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password**, and **Confirm Password**. For **CT User**, select “**Yes**” from the drop-down list. Retain the default value in the remaining fields.

The screenshot displays the Avaya Application Enablement Services Management Console. The top right corner shows system information: Welcome: User cust, Last login: Wed Jul 5 11:49:28 E.S.T. 2023 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 10.1.2.0.0.12-0, Server Date and Time: Wed Jul 26 17:36:27 EDT 2023, HA Status: Not Configured. The breadcrumb navigation is **User Management | User Admin | Add User**. The left sidebar menu includes **AE Services**, **Communication Manager Interface**, **High Availability**, **Licensing**, **Maintenance**, **Networking**, **Security**, **Status**, **User Management** (expanded), **Service Admin**, **User Admin** (expanded), **Add User** (selected), **Change User Password**, **List All Users**, **Modify Default Users**, **Search Users**, **Utilities**, and **Help**. The main content area is titled **Add User** and contains the following fields: **User Id** (rtitele), **Common Name** (rtitele), **Surname** (rtitele), **User Password** (masked with dots), **Confirm Password** (masked with dots), **Admin Note** (empty), **Avaya Role** (None), **Business Category** (empty), **Car License** (empty), **CM Home** (empty), **Css Home** (empty), **CT User** (Yes), **Department Number** (empty), **Display Name** (empty), **Employee Number** (empty), and **Employee Type** (empty). A note at the top of the form states: "Fields marked with \* can not be empty."

## 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 iNEMSOFT user from **Section Error! Reference source not found.**

The screenshot displays the Avaya Application Enablement Services Management Console. The top left features the Avaya logo. The main header reads "Application Enablement Services Management Console". In the top right corner, system information is displayed: "Welcome: User cust", "Last login: Wed Jul 5 11:49:28 E.S.T. 2023 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 10.1.2.0.0.12-0", "Server Date and Time: Wed Jul 26 17:38:14 EDT 2023", and "HA Status: Not Configured".

A red navigation bar contains "Security | Security Database | Control" and "Home | Help | Logout". The left sidebar lists various service categories, with "Security" expanded to show "Security Database" and its sub-items: "Control", "CTI Users", "Devices", and "Device Groups".

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

## 6.6. 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**.

The screenshot shows the Avaya Application Enablement Services Management Console. The top right corner displays system information: Welcome: User cust, Last login: Wed Jul 5 11:49:28 E.S.T. 2023 from 192.168.200.20, Number of prior failed login attempts: 0, HostName/IP: aes/10.64.101.239, Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE, SW Version: 10.1.2.0.0.12-0, Server Date and Time: Wed Jul 26 17:39:33 EDT 2023, HA Status: Not Configured.

The main navigation bar includes "Maintenance | Service Controller" and "Home | Help | Logout". The left sidebar menu is expanded to "Maintenance", with "Service Controller" selected. The main content area displays the "Service Controller" page with a table of services:

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

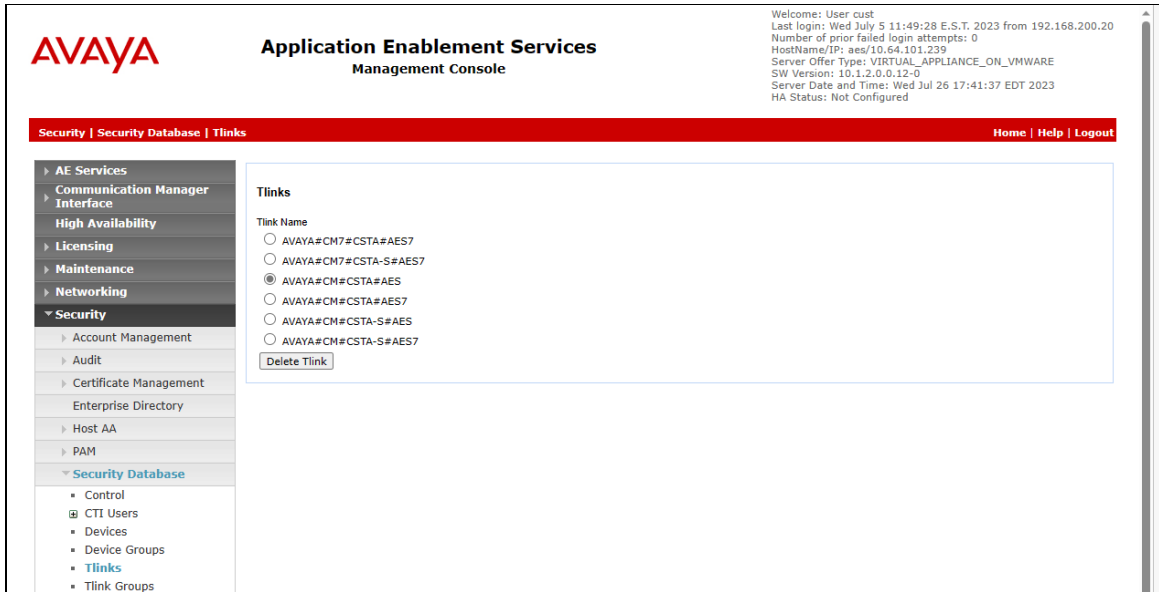
Below the table, a note states: "Note: DMCC Service must be restarted for WTI service changes to take effect. For status on actual services, please use [Status and Control](#)". At the bottom of the page, there are buttons for "Start", "Stop", "Restart Service", "Restart AE Server", "Restart Linux", and "Restart Web Server".



## 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 configure iCAS. In this case, the pertinent Tlink name for unencrypted connection is “**AVAYA#CM#CSTA#AES**”, as shown below.



The screenshot displays the Avaya Application Enablement Services Management Console. The top navigation bar includes the Avaya logo, the title "Application Enablement Services Management Console", and a user status area on the right with the following text: "Welcome: User cust", "Last login: Wed Jul 5 11:49:28 E.S.T. 2023 from 192.168.200.20", "Number of prior failed login attempts: 0", "HostName/IP: aes/10.64.101.239", "Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE", "SW Version: 10.1.2.0.0.12-0", "Server Date and Time: Wed Jul 26 17:41:37 EDT 2023", and "HA Status: Not Configured".

The main content area is titled "Tlinks" and contains a list of Tlink names with radio button selection options:

- AVAYA#CM7#CSTA#AES7
- AVAYA#CM7#CSTA-S#AES7
- AVAYA#CM#CSTA#AES
- AVAYA#CM#CSTA#AES7
- AVAYA#CM#CSTA-S#AES
- AVAYA#CM#CSTA-S#AES7

A "Delete Tlink" button is located below the list. The left-hand navigation pane shows a tree view with "Security Database" expanded to show "Tlinks" selected.

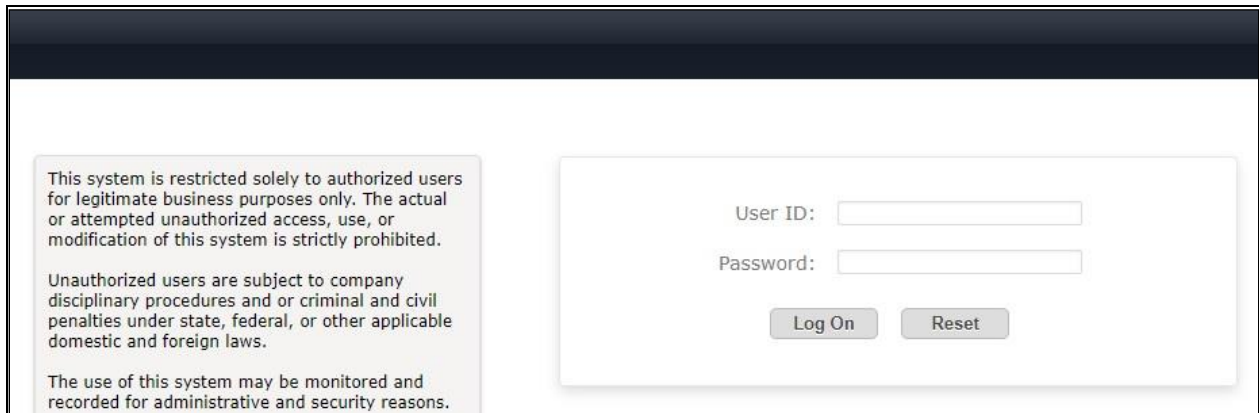
## 7. Configure Avaya Aura® Session Manager

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.

User ID:

Password:

## 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.

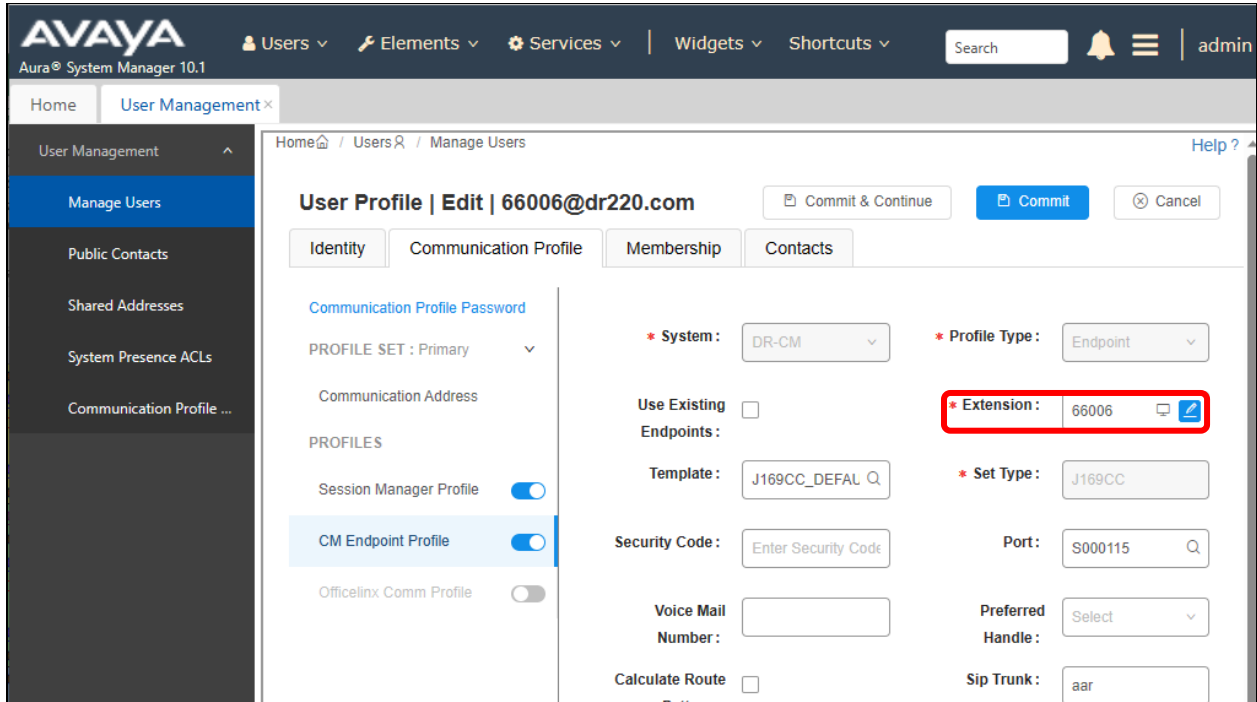
Select the entry associated with the first SIP agent station from **Section** Error! Reference source not found., in this case “66006”, and click **Edit**.

The screenshot shows the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, menu items (Users, Elements, Services, Widgets, Shortcuts), a search bar, and a user profile (admin). The left sidebar shows 'User Management' with 'Manage Users' selected. The main content area displays a table of users with columns for First Name, Surname, Display Name, Login Name, and SIP Handle. The user 'SIP 6' is selected.

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP 1	Avaya	Avaya, SIP 1	66001@dr220.com	66001
<input type="checkbox"/>	SIP 2	Avaya	Avaya, SIP 2	66002@dr220.com	66002
<input type="checkbox"/>	SIP 5	Avaya	Avaya, SIP 5	66005@dr220.com	66005
<input checked="" type="checkbox"/>	SIP 6	Avaya	Avaya, SIP 6	66006@dr220.com	66006

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.



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 Error! Reference source not found.** In the compliance testing, one SIP agent extension **66006** was configured.

The screenshot shows the 'Edit Endpoint' configuration interface. At the top, there are fields for System (DR-CM), Extension (66006), Template (J169CC\_DEFAULT\_CM\_8\_1), Port (S000115), and Name (Avaya, SIP 6). Below this is a tabbed interface with 'General Options (G)' selected. The 'General Options' section includes fields for Class of Restriction (COR) set to 2, Class of Service (COS) set to 1, Emergency Location Ext. set to 66006, Message Lamp Ext. set to 66006, Tenant Number set to 1, SIP Trunk set to aar, Coverage Path 1, Lock Message (unchecked), Multibyte Language set to Not Applicable, Localized Display Name set to Avaya, SIP 6, and Enable Reachability for Station Domain Control set to system. The 'Type of 3PCC Enabled' dropdown is highlighted with a red box and set to Avaya. A SIP URI field is at the bottom.

## 8. Configure iNEMSOFT ClassOne iCAS

Configuration of iNEMSOFT CLASSONE iCAS is done by designated iNEMSOFT engineers. Therefore, no configuration is provided in this document.

## 9. Verification Steps

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

### 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 Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Rcvd
1	12	no	aes	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 Error! Reference source not found.**, which for this application is “**2**”.

AVAYA Application Enablement Services Management Console

Welcome: User cust  
Last login: Wed Jul 26 17:10:56 E.S.T. 2023 from 192.168.120.42  
Number of prior failed login attempts: 0  
HostName/IP: aes/10.64.101.239  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 10.1.2.0.0.12-0  
Server Date and Time: Wed Jul 26 17:59:20 EDT 2023  
HA Status: Not Configured

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

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	cm	1	Talking	Mon Jul 10 14:14:52 2023	Online	20	0	1093	1093	30

Online Offline

For service-wide information, choose one of the following:  
[TSAPI Service Status](#) | [TLink Status](#) | [User Status](#)

### 9.3. Verify iNEMSOFT ClassOne iCAS Server

The following steps may be used to verify the configuration:

- Verify that iCAS Dispatch Console successfully registers with Session Manager server by following the **Session Manager → System Status → User Registrations** link on the System Manager Web Interface.

#### User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View	Default	Export	Force Unregister	AST Device Notifications:	Reboot	Reload	Failback	As of 1:06 PM
13 Items	Show	All						
<input type="checkbox"/> Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices
<input type="checkbox"/> Hide	70121@avaya.com	ClassOne	Station 1	DevConnect	10.64.10.47	<input type="checkbox"/>	<input type="checkbox"/>	1/1

User	Registration	Device	Simultaneous	History
First Name	ClassOne			
Last Name	Station 1			
Login Name	70121@avaya.com			
Registration Address	70121@avaya.com			
All Addresses	70121@avaya.com			
Home Location	DevConnect			
Actual Location	DevConnect			
Primary SM	sm81			
Secondary SM	---			
Survivable SM	---			
Simultaneous Devices	1/1			
ELIN Number	---			
ELIN Last Updated	---			

- Place calls to and from iCAS Dispatch Console and verify that the calls are successfully established with two-way talk path.

## 10. Conclusion

These Application Notes describe the configuration steps required for iNEMSOFT CLASSONE iCAS 6.0 Dispatch Console 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 Error! Reference source not found.**

## 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>.



---

**©2023 Avaya LLC All Rights Reserved.**

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

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