



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for iNEMSOFT CLASSONE® iCAS Dispatch Console with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

### Abstract

These Application Notes describe the procedures for configuring iNEMSOFT CLASSONE® iCAS Dispatch Console which were compliance tested with Avaya Aura® Session Manager, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

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 contain instructions for iNEMSOFT CLASSONE® iCAS (iCAS) Dispatch Console 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 is a system-of-systems, enabling operators to take control of their communications network and manage multiple transactions from many types of devices.

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 Dispatch Console with Session Manager. iCAS Dispatch Console registers to Session Manager as a SIP Endpoint and uses 3<sup>rd</sup> Party Call Control using TSAPI via AES. Application notes related to other interfaces may be obtained via Avaya Support site.

- Application Notes for iNEMSOFT CLASSONE® iCAS with Avaya Meeting Exchange
- Application Notes for iNEMSOFT CLASSONE® iCAS IP Radio Gateway with Avaya Aura® Session Manager
- Application Notes for iNEMSOFT CLASSONE® Endpoint Manager with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services

These Application Notes assume that Communication Manager, Session Manager and AES are already installed and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult references [1], [2], and [3].

## 2. General Test Approach and Test Results

The general test approach was to place calls to and from iCAS Dispatch Console and exercise basic telephone operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711MU)
- Inbound calls
- Outbound calls
- Hold/Resume
- Call termination (origination/destination)
- DTMF tone generation and detection
- VDN call handling
- Three party conference (origination/destination)
- Blind and Consultative transfers
- Agent work states
- Serviceability

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 this DevConnect Application Note 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 iNEMSOFT did not utilize encryption capabilities.

### 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, hold/resume and iCAS Dispatch Console interactions with Session Manager, Communication Manager, AES, and Avaya SIP, H.323, and digital telephones were verified. The

serviceability testing introduced failure scenarios to see if iCAS Dispatch Console can recover from failures.

## **2.2. Test Results**

The test objectives were verified. For serviceability testing, iCAS Dispatch Console operated properly after recovering from failures such as cable disconnects, and resets of iCAS Dispatch Console and Session Manager. iCAS Dispatch Console successfully negotiated the codec that was used. The features tested worked as expected.

## **2.3. Support**

iNEMSOFT CLASSONE® iCAS support can be obtained via following means:

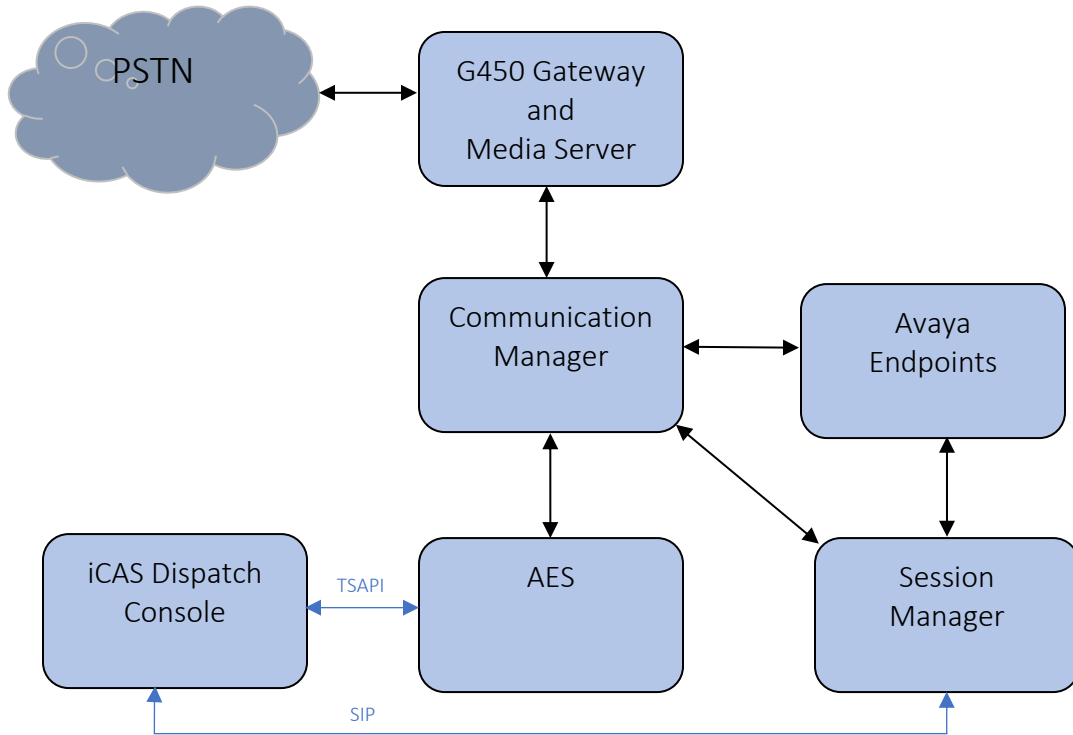
**Phone:** 214-423-2815

**Web:** [www.inemsoft.com](http://www.inemsoft.com)

**Email:** [rtisupport@inemsoft.com](mailto:rtisupport@inemsoft.com)

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration that consists of Avaya Products and iNEMSOFT CLASSONE® iCAS Dispatch Console.



**Figure 1: Test Configuration of CLASSONE® iCAS Dispatch Console by iNEMSOFT**

## 4. Equipment and Software Validated

The following equipment and software were used for the test configuration. With the exception of Avaya G450 Gateway, all other Avaya products were deployed on a Virtualization Environment.

<b>Equipment/Software</b>	<b>Release/Version</b>
Avaya Aura® Communication Manager	8.1.0.1.1.890.25517
Avaya G450 Media Gateway	FW 40.19.1
Avaya Aura® Media Server	8.0.1.121
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya Aura® System Manager	8.1.0.0.733078
Avaya Aura® Application Enablement Services	8.1.0.0.0.9-1
Avaya 9600 Series IP Deskphones	6.8.2 (H.323) 7.1.6.1 (SIP)
Avaya J100 Series IP Phones	6.8.2 (H.323) 4.0.2.1 (SIP)
iNEMSOFT CLASSONE® iCAS Dispatch Console	4.19

## 5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure iCAS Dispatch Console to successfully interoperate with Avaya Aura® Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

### 5.1. Configure AES connection

Use **change ip-services** command to add an entry for AES. On Page 1,

- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.

```
change ip-services                                     Page 1 of 3
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
<b>AESVCS</b>	<b>y</b>	<b>procr</b>	<b>8765</b>		

On Page 4 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the name obtained from the Application Enablement Services server.
- In the **Password** field, type a password to be administered on the Application Enablement Services server.
- In the **Enabled** field, type **y**.

```
change ip-services                                     Page 3 of 3
```

AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aes81	*	y	in use
2:				
3:				

## 5.2. Configure CTI Link

Use **add cti-link *n*** command, where *n* is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
add cti-link 1                                     Page 1 of 3
                                                    CTI LINK
CTI Link: 1
Extension: 77777
  Type: ADJ-IP
                                                    COR: 1
  Name: CTI Link 1
Unicode Name? n
```



## 6. Configure Avaya Aura® Application Enablement Services

Configuration of Avaya Aura® Application Enablement Services requires a user account to be configured for iCAS Dispatch Console.

### 6.1. Configure User

All administration is performed by web browser, <https://<aes-ip-address>> (not shown).

A user needs to be created for iCAS Dispatch Console to communicate with AES. Navigate to **User Management → User Admin → Add User**.

Fill in **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. Set the **CT User** to **Yes**, and **Apply**.



## Application Enablement Services Management Console

Welcome: User cust  
Last login: Thu Nov 14 17:05:31 2019 from 10.64.10.47  
Number of prior failed login attempts: 0  
HostName/IP: aes81/10.64.110.215  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.9-1  
Server Date and Time: Fri Nov 15 12:04:32 MST 2019  
HA Status: Not Configured

User Management | User Admin | Add User

Home | Help | Logout

<ul style="list-style-type: none"><li>▶ AE Services</li><li>▶ Communication Manager Interface</li><li>▶ High Availability</li><li>▶ Licensing</li><li>▶ Maintenance</li><li>▶ Networking</li><li>▶ Security</li><li>▶ Status</li><li>▼ User Management<ul style="list-style-type: none"><li>▶ Service Admin</li><li>▼ User Admin<ul style="list-style-type: none"><li>▪ <b>Add User</b></li><li>▪ Change User Password</li><li>▪ List All Users</li><li>▪ Modify Default Users</li></ul></li></ul></li></ul>	<h3>Add User</h3> <p>Fields marked with * can not be empty.</p> <p>* User Id <input type="text" value="rtitele1"/></p> <p>* Common Name <input type="text" value="rtitele1"/></p> <p>* Surname <input type="text" value="rtitele1"/></p> <p>* User Password <input type="password" value="....."/></p> <p>* Confirm Password <input type="password" value="....."/></p> <p>Admin Note <input type="text"/></p> <p>Avaya Role <input type="text" value="None"/></p> <p>Business Category <input type="text"/></p> <p>Car License <input type="text"/></p> <p>CM Home <input type="text"/></p> <p>Css Home <input type="text"/></p> <p>CT User <input type="text" value="Yes"/></p> <p>Department Number <input type="text"/></p>
--	---

Navigate to **Security** → **Security Database** → **CTI Users** → **List All Users**.



**Application Enablement Services  
Management Console**

Welcome: User cust  
Last login: Thu Nov 14 17:05:31 2019 from 10.64.10.47  
Number of prior failed login attempts: 0  
HostName/IP: aes81/10.64.110.215  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Fri Nov 15 12:05:38 MST 2019  
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ **Security**
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ **Security Database**

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> calabrio	calabrio	NONE	NONE
<input type="radio"/> intradiem	intradiem	NONE	NONE
<input type="radio"/> intranext	intranext	NONE	NONE
<input type="radio"/> rtirdrouter1	rtirdrouter1	NONE	NONE
<input type="radio"/> rtirouter1	rtirouter1	NONE	NONE
<input checked="" type="radio"/> rtitele1	rtitele1	NONE	NONE
<input type="radio"/> trio	trio	NONE	NONE

Select the recently added user and click **Edit**. Check the box for **Unrestricted Access** and click **Apply Changes**.



**Application Enablement Services  
Management Console**

Welcome: User cust  
Last login: Thu Nov 14 17:05:31 2019 from 10.64.10.47  
Number of prior failed login attempts: 0  
HostName/IP: aes81/10.64.110.215  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Fri Nov 15 12:06:04 MST 2019  
HA Status: Not Configured

Security | Security Database | CTI Users | List All Users Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ High Availability
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ **Security**
  - ▶ Account Management
  - ▶ Audit
  - ▶ Certificate Management
  - Enterprise Directory
  - ▶ Host AA
  - ▶ PAM
  - ▼ **Security Database**
    - Control

Edit CTI User

User Profile:

User ID	rtitele1
Common Name	rtitele1
Worktop Name	NONE ▼
Unrestricted Access	<input checked="" type="checkbox"/>

---

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	<input type="checkbox"/>

---

Routing Control:

Allow Routing on Listed Devices	None ▼
---------------------------------	--------

## 6.2. Configure Communication Manager Switch Connections

To add links to the Communication Manager, navigate to the **Communication Manager Interface** → **Switch Connections** page and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as **cm81** for this test environment:

Welcome: User cust  
Last login: Thu Nov 14 17:05:31 2019 from 10.64.10.47  
Number of prior failed login attempts: 0  
HostName/IP: aes81/10.64.110.215  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Fri Nov 15 12:06:42 MST 2019  
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

Navigation: AE Services, Communication Manager Interface, Switch Connections, Dial Plan, High Availability, Licensing, Maintenance

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> cm81	Yes	30	1

Use the **Edit Connection** button shown above to configure the connection. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below. This must match the password configured when adding AESVCS connection Type in Communication Manager.

Welcome: User cust  
Last login: Thu Nov 14 17:05:31 2019 from 10.64.10.47  
Number of prior failed login attempts: 0  
HostName/IP: aes81/10.64.110.215  
Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
SW Version: 8.1.0.0.0.9-1  
Server Date and Time: Fri Nov 15 12:07:11 MST 2019  
HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

Navigation: AE Services, Communication Manager Interface, Switch Connections, Dial Plan, High Availability, Licensing, Maintenance, Networking, Security, Status

Connection Details - cm81

Switch Password:

Confirm Switch Password:

Msg Period:  Minutes (1 - 72)

Provide AE Services certificate to switch:

Secure H323 Connection:

Processor Ethernet:

Use the **Edit PE/CLAN IPs** button (shown in this section’s first screen shot above) to configure the **procr** or **CLAN IP Address (es)** for TSAPI message traffic.

Welcome: User cust  
 Last login: Thu Nov 14 17:05:31 2019 from 10.64.10.47  
 Number of prior failed login attempts: 0  
 HostName/IP: aes81/10.64.110.215  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 8.1.0.0.0.9-1  
 Server Date and Time: Fri Nov 15 12:07:39 MST 2019  
 HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

> AE Services  
 > Communication Manager Interface  
   Switch Connections  
   > Dial Plan  
 High Availability  
 > Licensing  
 > Maintenance

**Edit Processor Ethernet IP - cm81**

Name or IP Address	Status
10.64.110.213	In Use

Use the **Edit H.323 Gatekeeper** button (shown in this section’s first screen capture above) to configure the **procr** or **CLAN IP Address(es)**.

Welcome: User cust  
 Last login: Thu Nov 14 17:05:31 2019 from 10.64.10.47  
 Number of prior failed login attempts: 0  
 HostName/IP: aes81/10.64.110.215  
 Server Offer Type: VIRTUAL\_APPLIANCE\_ON\_VMWARE  
 SW Version: 8.1.0.0.0.9-1  
 Server Date and Time: Fri Nov 15 12:08:04 MST 2019  
 HA Status: Not Configured

Communication Manager Interface | Switch Connections Home | Help | Logout

> AE Services  
 > Communication Manager Interface  
   Switch Connections  
   > Dial Plan  
 High Availability  
 > Licensing  
 > Maintenance

**Edit H.323 Gatekeeper - cm81**

Name or IP Address

10.64.110.213

### 6.3. Configure TSAPI Link

Navigate to the **AE Services** → **TSAPI** → **TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**.



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

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links

**TSAPI Links**

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
<input checked="" type="radio"/> 1	cm81	1	10	Both

Select a **Switch Connection** using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The **Switch CTI Link Number** must match the number configured in the **cti-link** form for Communication Manager.

If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box.

Click **Apply Changes**.

The configuration shown below was previously configured.



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

▼ AE Services

- ▶ CVLAN
- ▶ DLG
- ▶ DMCC
- ▶ SMS
- ▼ TSAPI
  - TSAPI Links
  - TSAPI Properties
- ▶ TWS

**Edit TSAPI Links**

Link: 1

Switch Connection:

Switch CTI Link Number:

ASAI Link Version:

Security:

## 7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager web console and is then downloaded into Session Manager. Log on to System Manager via a web browser.

Recommended access to System Manager is via FQDN.

[Go to central login for Single Sign-On](#)

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

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

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

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

---

This system is restricted solely to authorized users for legitimate business

User ID:

Password:

[Change Password](#)

**Supported Browsers:** Internet Explorer 11.x or Firefox 65.0, 66.0 and 67.0.

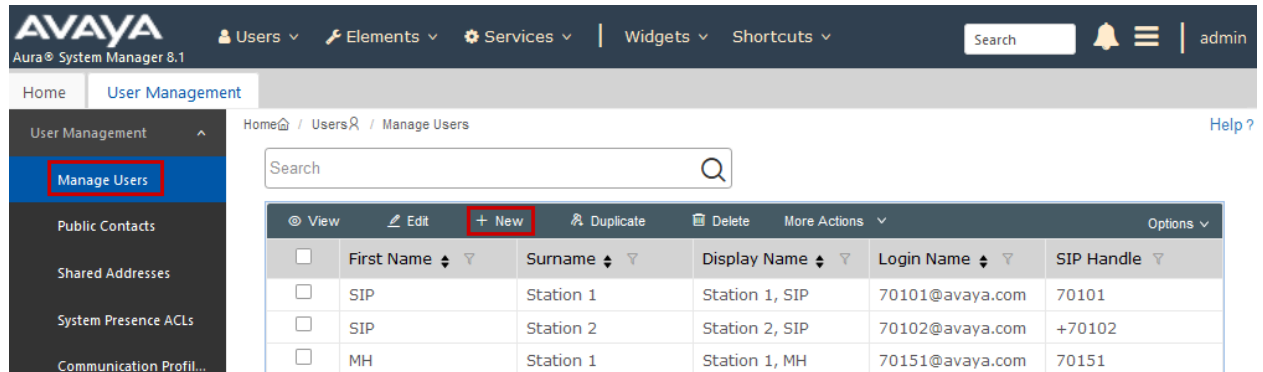
System Manager Dashboard is displayed.

## 7.1. Configure SIP Users

During the compliance test, no special users were created for this solution. However, the steps to configure a user are included.

Add a new SIP user for each iCAS Dispatch Console. During compliance testing SIP Users 70121, 70122, 70123 and 70124 were created for iCAS Dispatch Console.

To add new SIP users, Navigate to **Users → User Management → Manage Users**. Click **New**.



The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and menu items for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile icon labeled 'admin' are also present. The main content area is titled 'User Management' and 'Manage Users'. A sidebar on the left contains a 'Manage Users' button, which is highlighted with a red box. Below the sidebar, there is a search bar and a table of users. The table has columns for 'First Name', 'Surname', 'Display Name', 'Login Name', and 'SIP Handle'. The '+ New' button in the table's action bar is highlighted with a red box. The table contains three rows of user data:

	First Name	Surname	Display Name	Login Name	SIP Handle
<input type="checkbox"/>	SIP	Station 1	Station 1, SIP	70101@avaya.com	70101
<input type="checkbox"/>	SIP	Station 2	Station 2, SIP	70102@avaya.com	+70102
<input type="checkbox"/>	MH	Station 1	Station 1, MH	70151@avaya.com	70151

Configure the **Identity** tab as follows:

- **Last Name** – Enter last name of user.
- **First Name** – Enter first name of user.
- **Login Name** – Enter extension number@sip domain name.

User Profile | Edit | 70121@avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Basic Info

Address

LocalizedName

User Provisioning Rule: [v]

\* Last Name: Station 1 Last Name (Latin Translation): Station 1

\* First Name: ClassOne First Name (Latin Translation): ClassOne

\* Login Name: 70121@avaya.com Middle Name: Middle Name Of User

Select the **Communication Profile** tab followed by **Communication Profile Password** on the left pane and provide the following information:

- **Communication Profile Password** – Enter a numeric password
- **Confirm Password** – Repeat numeric password.

User Profile | Edit | 70121@avaya.com

Commit & Continue Commit Cancel

Identity Communication Profile Membership Contacts

Communication Profile Password

PROFILE SET : Primary

Communication Address

PROFILES

Session Manager Profile

Avaya Breeze® Profile

CM Endpoint Profile

Presence Profile

Comm-Profile Password

Comm-Profile Password: [.....]

\* Re-enter Comm-Profile Password: [.....] ✓

Generate Comm-Profile Password

Cancel OK

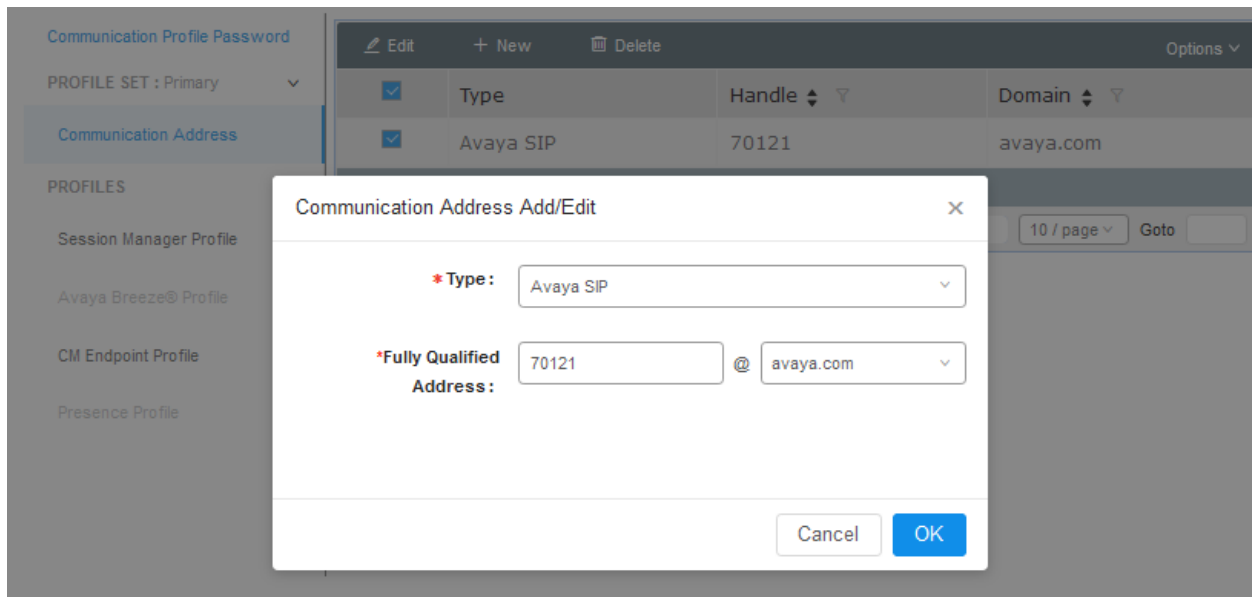
Type	Handle	Domain
Avaya SIP	70121	avaya.com



On the left pane, select **Communication Address** followed by **New** to define a **Communication Address** for the new SIP user, and provide the following information.

- Type – Select Avaya SIP using drop-down menu.
- Fully Qualified Address – Enter same extension number and domain used for Login Name, created previously.

Click the **Add** button to save the Communication Address for the new SIP user.



On the left pane, enable **Session Manager Profile** and configure as follows:

- **Primary Session Manager** – Select one of the Session Managers.
- **Origination Application Sequence** – Select Application Sequence defined (not shown) for Communication Manager.
- **Termination Application Sequence** – Select Application Sequence defined (not shown) for Communication Manager.
- **Home Location** – Select a predefined location.

The screenshot displays a configuration interface for SIP Registration. On the left, a sidebar shows 'PROFILE SET : Primary' and 'PROFILES' with 'Session Manager Profile' enabled. The main area is titled 'SIP Registration' and contains several sections:

- SIP Registration:**
  - \* Primary Session Manager: sm81
  - Secondary Session Manager: Start typing...
  - Survivability Server: Start typing...
  - Max. Simultaneous Devices: 1
  - Block New Registration When Maximum Registrations Active?:
- Application Sequences:**
  - Origination Sequence: cm81
  - Termination Sequence: cm81
- Emergency Calling Application Sequences:**
  - Emergency Calling Origination Sequence: Select
  - Emergency Calling Termination Sequence: Select
- Call Routing Settings:**
  - \* Home Location: DevConnect

On the left pane, enable **CM Endpoint Profile** and configure as follows:

- **System** – Select Managed Element defined in System Manager (not shown) for Communication Manager.
- **Use Existing Endpoints** - Leave unchecked to automatically create a new endpoint on Communication Manager when the new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
- **Extension** - Enter same extension number used in this section.
- **Template** – Select template for type of SIP phone. During the compliance test, 9641SIP\_DEFAULT\_CM\_8\_1 was selected.

Select **Commit** once done.

The screenshot shows the configuration page for a CM Endpoint Profile. On the left, a sidebar lists various profiles, with 'CM Endpoint Profile' selected and its toggle switch turned on. The main configuration area includes the following fields and options:

- System:** cm81
- Profile Type:** Endpoint
- Use Existing Endpoints:**
- Extension:** 70121
- Template:** 9641SIP\_DEFAULT\_CM\_8\_1
- Set Type:** 9641SIP
- Security Code:** Enter Security Code
- Port:** ip
- Voice Mail Number:** (empty)
- Preferred Handle:** Select
- Calculate Route Pattern:**
- SIP URI:** Select
- Enhanced Callr-Info Display for 1-line phones:**
- Delete on Unassign from User or on Delete User:**
- Override Endpoint Name and Localized Name:**
- Allow H.323 and SIP Endpoint Dual Registration:**
- Sip Trunk:** aar

Select the Endpoint Editor icon (not shown) and set **Type of 3PCC Enabled** to **Avaya**.

The screenshot shows the Endpoint Editor configuration page with several tabs: General Options (G), Feature Options (F), Site Data (S), Abbreviated Call Dialing (A), Enhanced Call Fwd (E), Button Assignment (B), Profile Settings (P), and Group Membership (M). The 'Profile Settings (P)' tab is active, showing the following configuration:

- Class of Restriction (COR):** 1
- Emergency Location Ext:** 70121
- Tenant Number:** 1
- SIP Trunk:** aar
- Class Of Service (COS):** 1
- Message Lamp Ext.:** 70121
- Type of 3PCC Enabled:** Avaya
- Coverage Path 1:** (empty)
- Coverage Path 2:** (empty)
- Localized Display Name:** Station 1, ClassOne
- Enable Reachability for Station Domain Control:** system
- Lock Message:**
- Multibyte Language:** Not Applicable

Select **Done** followed by **Commit** to save changes.

## 8. Configure iNEMSOFT CLASSONE® iCAS Dispatch Console

Installation and configuration of iCAS Dispatch Console is done by designated iNEMSOFT engineers. Hence, no configuration is provided in this document.

## 9. Verification Steps

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

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

## 11. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>

- [1] Administering Avaya Aura<sup>®</sup> Communication Manager, Release 8.1.x, Issue 4, November 2019.
- [2] Administering Avaya Aura<sup>®</sup> Application Enablement Services, Release 8.1.x, Issue 3, October 2019
- [3] Administering Avaya Aura<sup>®</sup> Session Manager, Release 8.1.1, Issue 2, October 2019

Documentation related to iCAS can be directly obtained from iNEMSOFT.

---

**©2019 Avaya Inc. All Rights Reserved.**

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