Avaya Solution & Interoperability Test Lab

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

Abstract

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

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® Application Enablement Services (AES) and Avaya Aura® Communication Manager (Communication Manager) 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 AES. iCAS Dispatch Console registers to Communication Manager via AES as an H.323 end point. 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 Console with Avaya Aura® Session Manager
- Application Notes for iNEMSOFT CLASSONE® iCAS Dispatch Console with Avaya Aura® Session Manager

These Application Notes assume that Communication 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
- Inbound calls
- Outbound calls
- Hold/Resume
- Call termination (origination/destination)
- Three party conference (origination/destination)
- 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.

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 and hold/resume and iCAS Dispatch Console interactions with AES, Communication Manager, 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
Email:	rtisupport@inemsoft.com

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and iNEMSOFT CLASSONE® iCAS. Though this document only contains instructions for and iNEMSOFT CLASSONE® iCAS Dispatch Console with Avaya Aura® Application Enablement Services, the following diagram shows the entire solution that was tested during compliance testing.

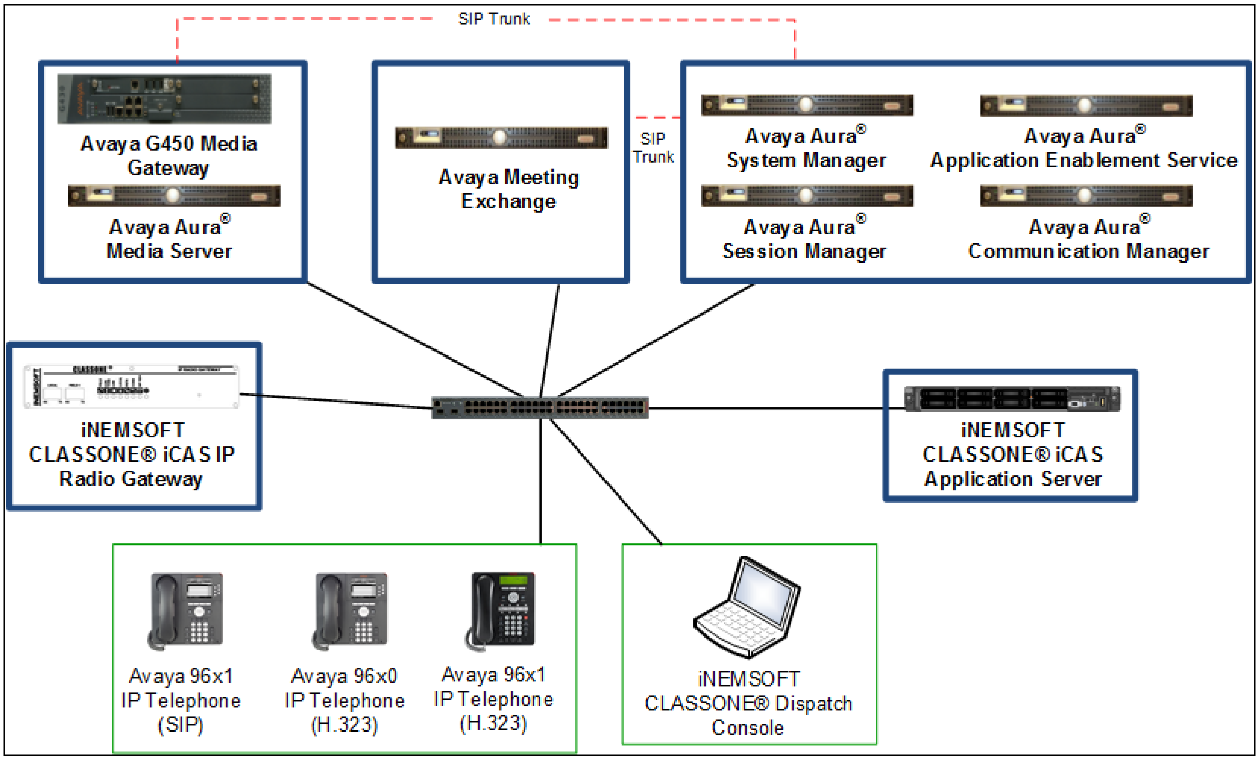

SIP Trunk
Avaya G450 Media Gateway
Avaya Aura® Media Server
Avaya Meeting Exchange
SIP Trunk
Avaya Aura® System Manager
Avaya Aura® Application Enablement Service
Avaya Aura® Session Manager
Avaya Aura® Communication Manager
iNEMSOFT CLASSONE® iCAS IP Radio Gateway
iNEMSOFT CLASSONE® iCAS Application Server
Avaya 96x1 IP Telephone (SIP)
Avaya 96x0 IP Telephone (H.323)
Avaya 96x1 IP Telephone (H.323)
iNEMSOFT CLASSONE® Dispatch Console

Figure 1: Test Configuration of CLASSONE® 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.

Equipment	Software/Firmware
Avaya Aura® Communication Manager	CM 7.0.1.2.0.441.23384
Avaya Aura® System Manager	7.0.1.1. 065378
Avaya Aura® Session Manager	7.0.1.1.701114
Avaya Aura® Application Enablement Services	7.0.1.0.0.15-0
Avaya G450 Media Gateway	37.19.0
iNEMSOFT CLASSONE® iCAS Dispatch Console	4.7

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure iCAS Dispatch Console to successfully 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   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
```

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.**

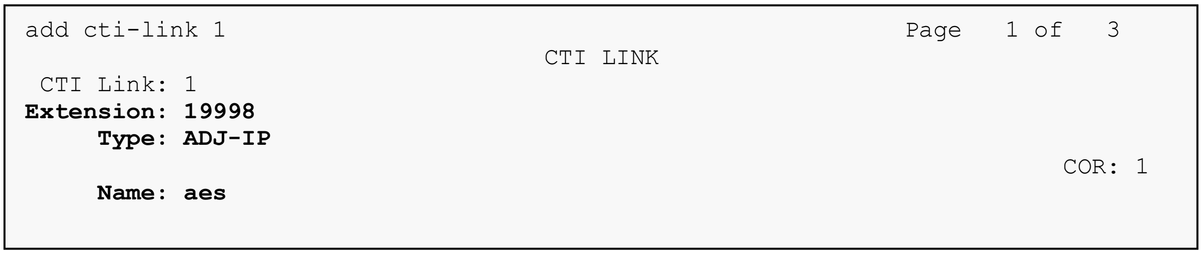
```
change ip-services                                              Page   4 of   4
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes               Interop123456789      y        in use
      2:
      3:
      4:
      5:
```

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.

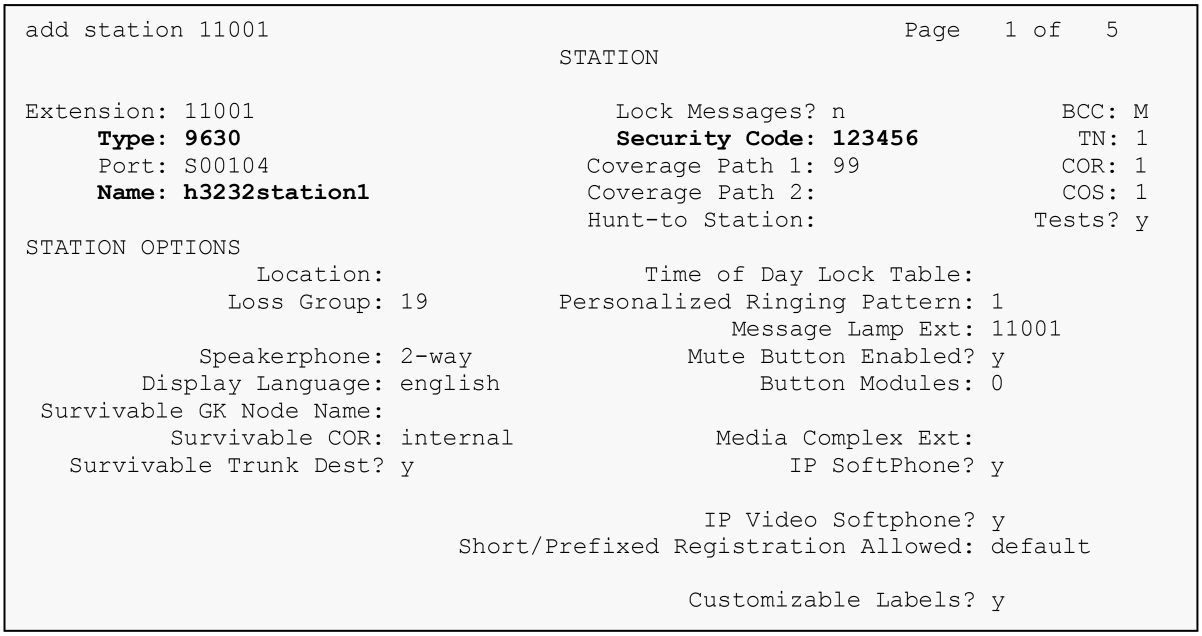


```
add cti-link 1                                               Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 19998
     Type: ADJ-IP
                                                                        COR: 1
     Name: aes
```

5.3. Administer Stations

Use **add station *n*** command, where ***n*** is an available extension number. iCAS Dispatch Console will use the information in this section to log in.

- Set **Type** to **9630**
- In the **Name** field, type a descriptive name
- In the **Security Code** field, type in a password that will be used by iCAS Dispatch Console



```
add station 11001                                            Page   1 of   5
                                     STATION

Extension: 11001                         Lock Messages? n               BCC: M
     Type: 9630                          Security Code: 123456           TN: 1
     Port: S00104                      Coverage Path 1: 99              COR: 1
     Name: h3232station1               Coverage Path 2:                 COS: 1
                                       Hunt-to Station:               Tests? y
STATION OPTIONS
                Location:                  Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 11001
            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

                                               IP Video Softphone? y
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

6. Configure Avaya Aura® Application Enablement Services

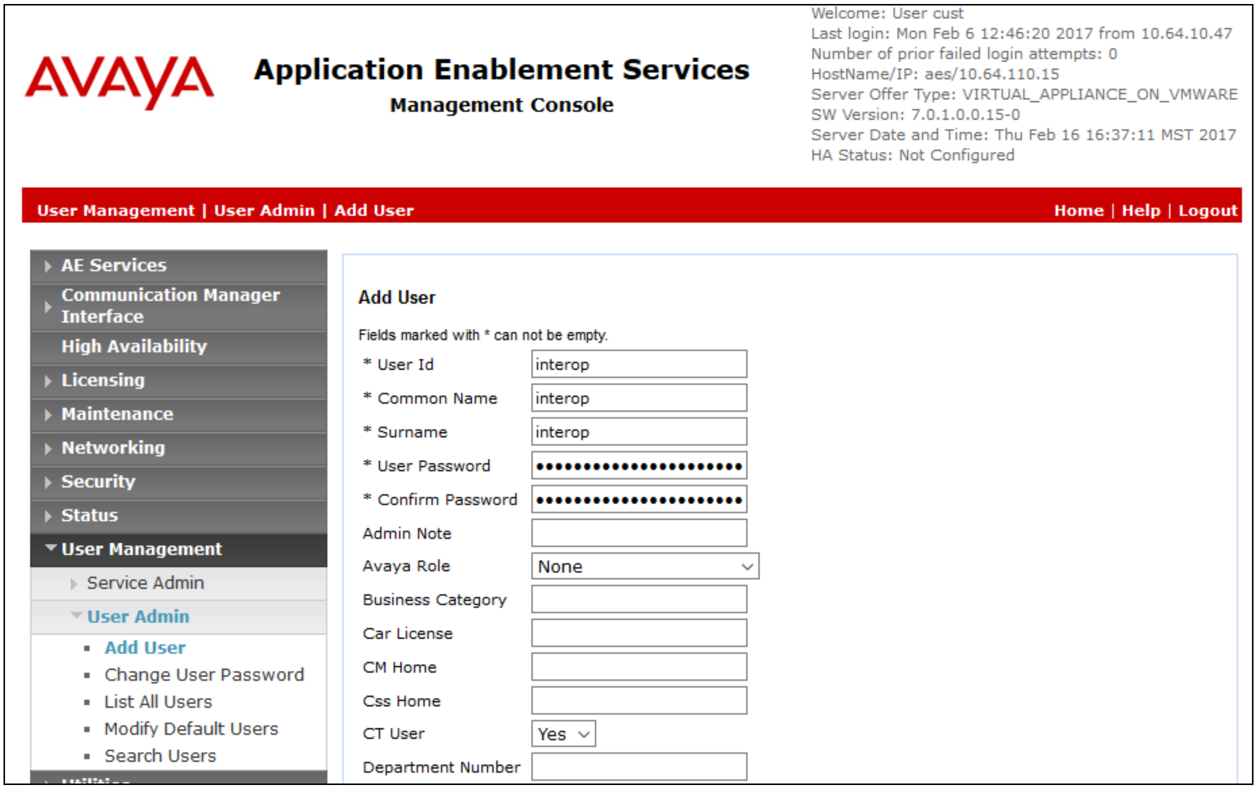
Configuration of Avaya Aura® Application Enablement Services requires a user account be configured for iCAS Dispatch Console.

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**.



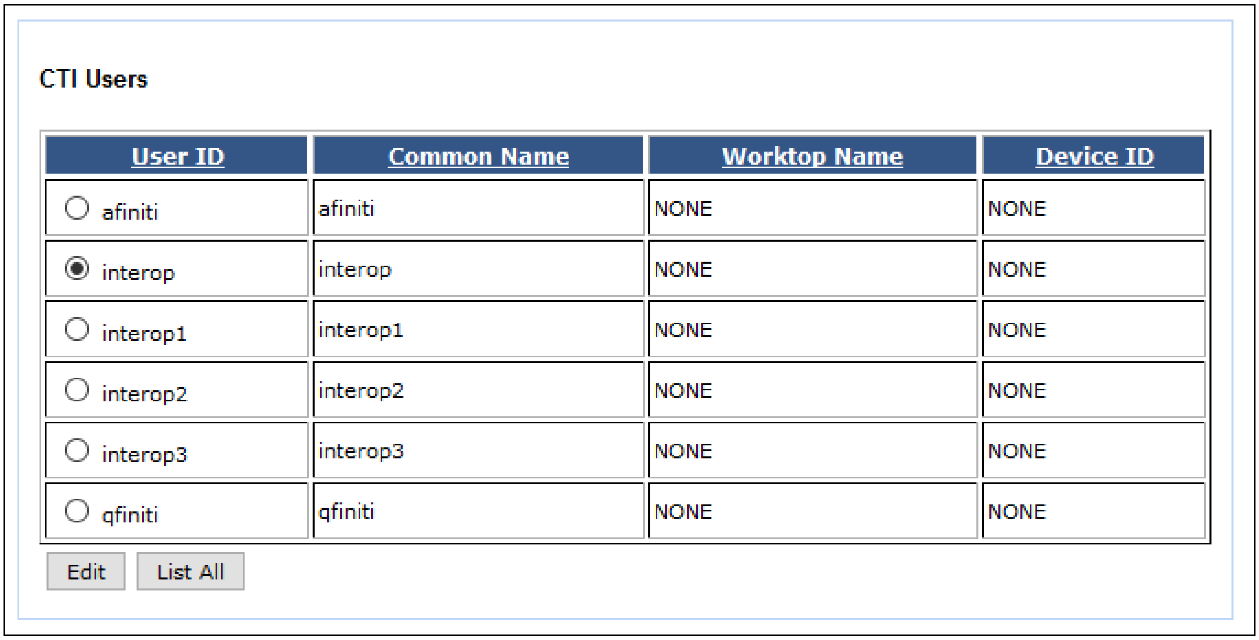
Welcome: User cust
Last login: Mon Feb 6 12:46:20 2017 from 10.64.10.47
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.0.15-0
Server Date and Time: Thu Feb 16 16:37:11 MST 2017
HA Status: Not Configured

Add User

Fields marked with * can not be empty.

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

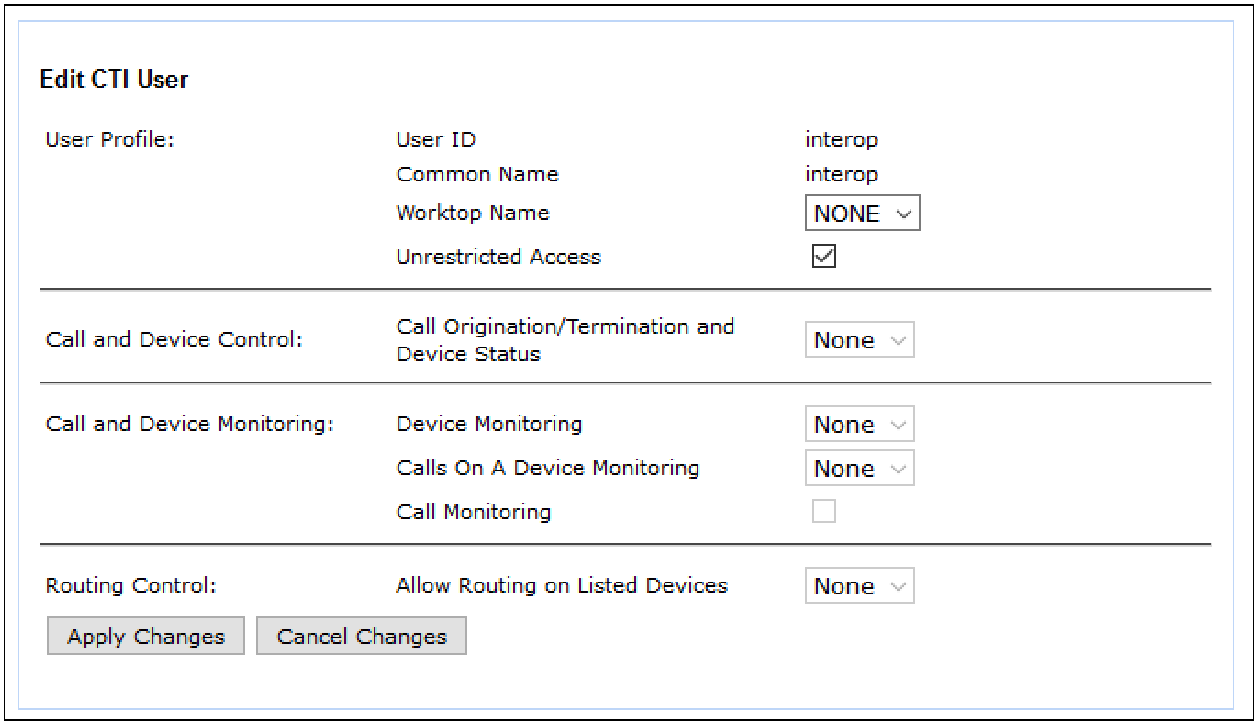
Navigate to **Security → Security Database → CTI Users → List All Users**.



CTI Users

User ID	Common Name	Worktop Name	Device ID
○ afiniti	afiniti	NONE	NONE
● interop	interop	NONE	NONE
○ interop1	interop1	NONE	NONE
○ interop2	interop2	NONE	NONE
○ interop3	interop3	NONE	NONE
○ qfiniti	qfiniti	NONE	NONE

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

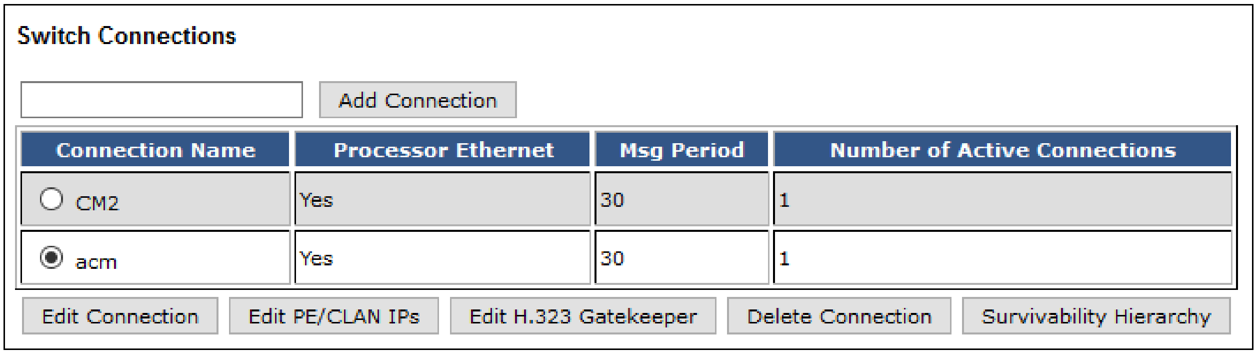


Edit CTI User

User Profile:	User ID	interop
	Common Name	interop
	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

6.2. Configure Communication Manager Switch Connections

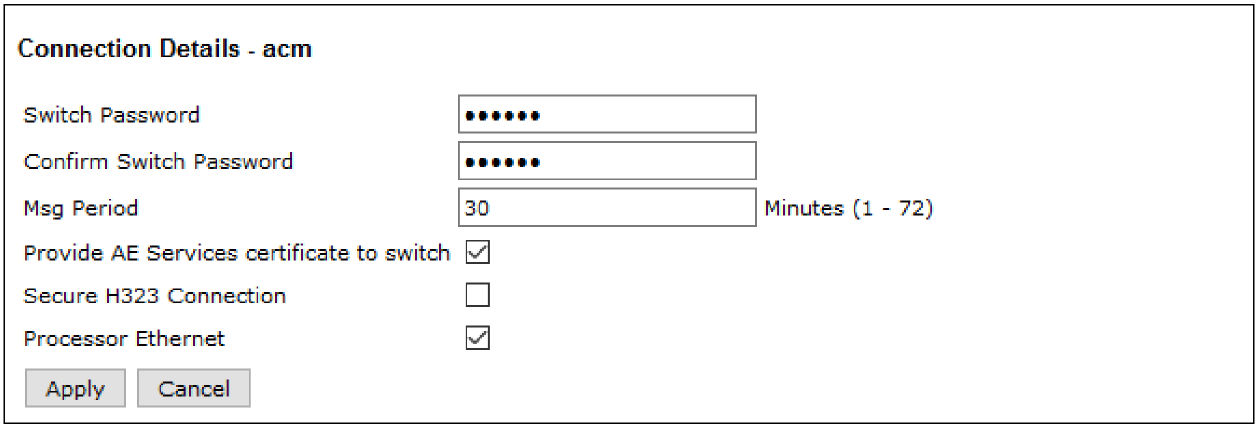
To add links to the Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection and click the **Add Connection** button. This was previously configured as **acm** for this test environment:



Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
○ CM2	Yes	30	1
● acm	Yes	30	1

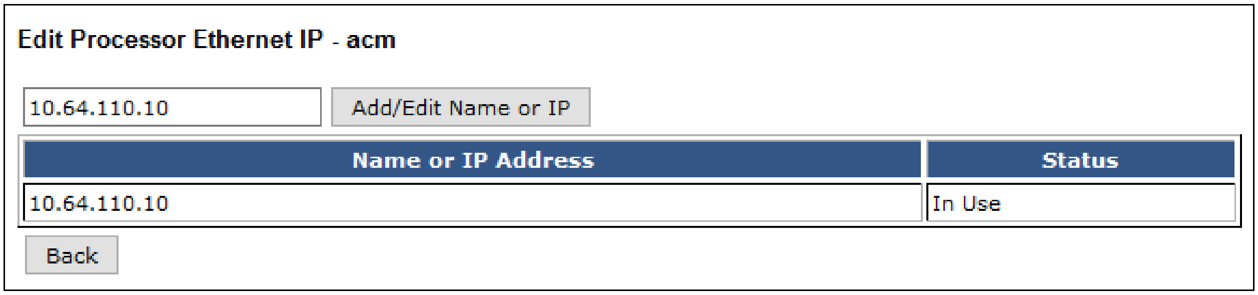
Use the **Edit Connection** button shown above to configure the connection. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below. This must match the password configured when adding AESVCS connection in Communication Manager.



Connection Details - acm

Switch Password	••••••
Confirm Switch Password	••••••
Msg Period	30 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.

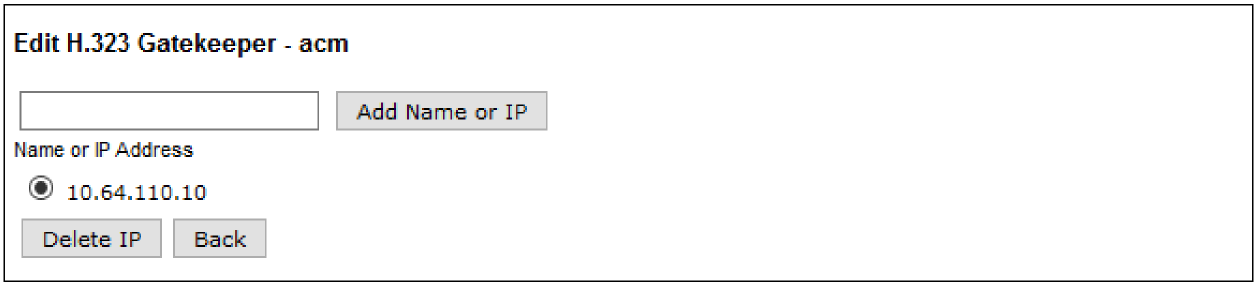


Edit Processor Ethernet IP - acm

10.64.110.10

Name or IP Address	Status
10.64.110.10	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).



Edit H.323 Gatekeeper - acm

Name or IP Address

● 10.64.110.10

6.3. Configure TSAPI Link

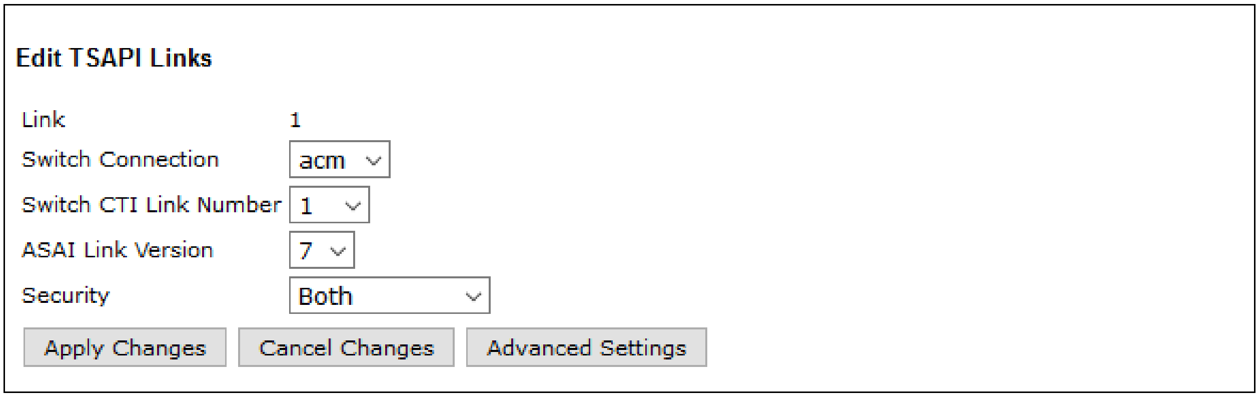
Navigate to the **AE Services → TSAPI → TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link** (not shown).

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**.

Configuration shown below was previously configured.



Edit TSAPI Links

Link	1
Switch Connection	acm
Switch CTI Link Number	1
ASAI Link Version	7
Security	Both

7. 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.

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify that iCAS Dispatch Console successfully registers with Communication Manager via AES. Via SAT, use the **list trace station** command to verify the registration is successful.

```
list trace station 11001                                              Page   3

                                LIST TRACE

time            data
10:49:35   TCP connected (fe)
                   endpt  [10.64.10.47]:25518
                   switch [10.64.110.10]:1720
10:49:35   Q.931 Setup received
                   endpt  [10.64.10.47]:25518
                   switch [10.64.110.10]:1720
10:49:35   Q.931 CallProc sent
                   endpt  [10.64.10.47]:25518
                   switch [10.64.110.10]:1720
10:49:35   Q.931 Connect sent
```

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

9. Conclusion

During compliance testing, iNEMSOFT CLASSONE® Dispatch Console successfully registered with Avaya Aura® Communication Manager via Avaya Aura® Application Enablement Services, placed and received calls to and from SIP and non-SIP telephones.

10. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, August 2016, Release 7.0.1, Document Number 03-300509.

[2] *Administering Avaya® Session Manager*, May 2016, Release 7.0.1, Issue 2

[3] *Administering Avaya® System Manager*, November 2016, Release 7.0.1,.Issue 2.2

Documentation related to iCAS can be directly obtained from iNEMSOFT.

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.