Application Notes for IntraNext iGuard with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes contain instructions for IntraNext iGuard with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager to successfully interoperate.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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 IntraNext iGuard with Avaya Aura® Application Enablement Services and Avaya Aura® Communication Manager to successfully interoperate.

The iGuard solution offers an innovative way to protect customers' personally identifiable information (PII) during calls with contact center agents. When customers input data such as credit card or social security numbers during a call, iGuard prevents the customer service representative (CSR) from seeing the data.

iGuard is a Dual Tone Multi Frequency (DTMF) capturing solution. In the compliance testing, iGuard used the Telephony Services Application Programming interface (TSAPI) and Device, Media, and Call Control (DMCC) interface from Avaya Aura® Application Enablement Services to monitor agent stations on Avaya Aura® Communication Manager and to capture the media associated with the monitored stations for DTMF collection.

2. General Test Approach and Test Results

The feature test cases were performed manually. Each test call was handled manually on the agent station with generation of unique media (DTMF) content for the recordings. Necessary user actions such as hold and reconnect were performed from the agent telephones to test the different call scenarios.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet cable to iGuard.

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 feature and serviceability testing.

The feature testing focused on verifying the following on iGuard:

- Handling of TSAPI messages in the areas of event notification and value queries.
- Proper capture of DTMF of calls for scenarios involving inbound, outbound, internal, external, ACD, non-ACD, hold, reconnect, conference, and transfer.

The serviceability testing focused on verifying the ability of iGuard to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to iGuard.

2.2. Test Results

All planned test cases were passed with one observation as mention below:
When a cti-link is placed in busy state and then released, iGuard does not re-connect automatically. iGuard services need to be manually restarted in order for the monitors to re-connect.

2.3. Support

Technical support on IntraNext iGuard can be obtained through the following:

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

3. Reference Configuration

Figure 1 illustrates a sample configuration that consists of Avaya Products and IntraNext iGuard.

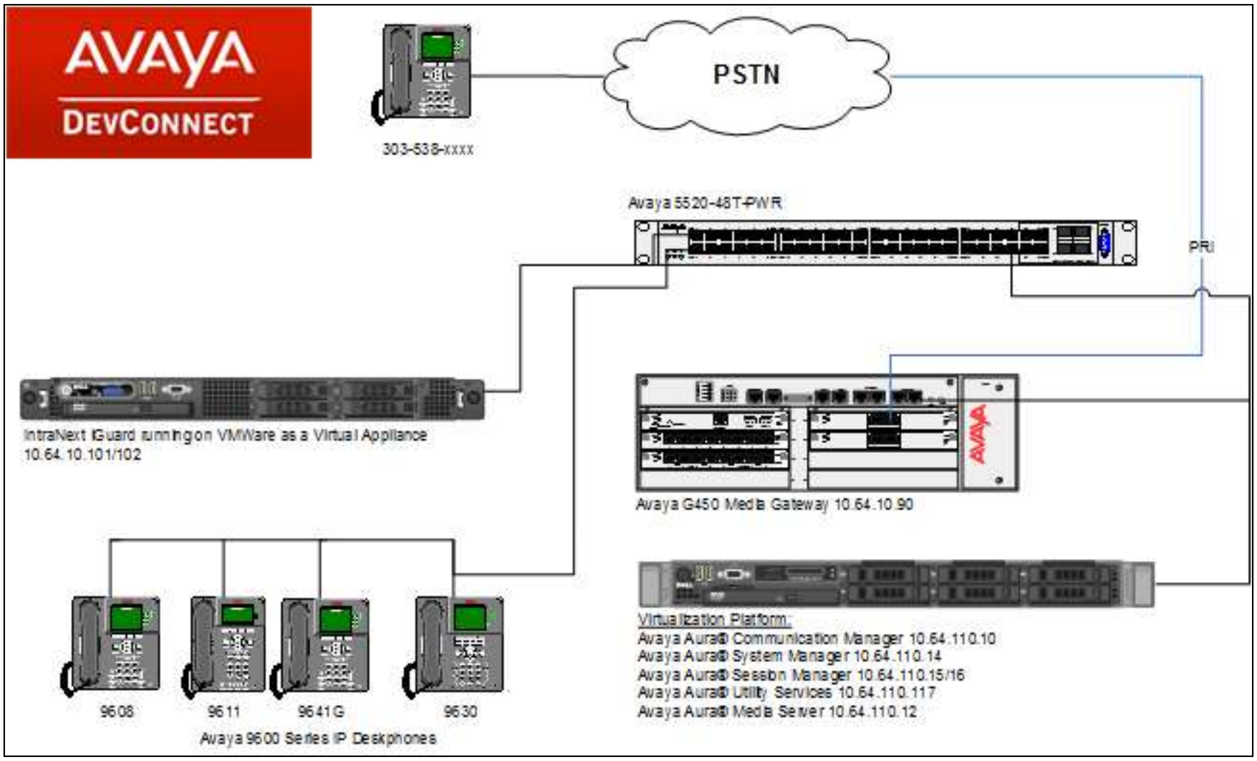

AVAYA
DEVCONNECT
PSTN
303-538-xxxx
Avaya 5520-48T-PWR
PRI
IntraNext iGuard running on VMWare as a Virtual Appliance
10.64.10.101/102
Avaya G450 Media Gateway 10.64.10.90
Virtualization Platform:
Avaya Aura® Communication Manager 10.64.110.10
Avaya Aura® System Manager 10.64.110.14
Avaya Aura® Session Manager 10.64.110.15/16
Avaya Aura® Utility Services 10.64.110.117
Avaya Aura® Media Server 10.64.110.12
9608
9611
9641G
9630
Avaya 9600 Series IP Deskphones

Figure 1: Test Configuration for IntraNext iGuard

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	7.0 Service Pack 1
Avaya Aura® Session Manager	7.0
Avaya Aura® System Manager	7.0
Avaya 9600 Series IP Deskphones	6.6.0 (SIP) 3.2.6 (H.323)
Avaya G450 Media Gateway	39.17.0
Avaya Aura® Application Enablement Services	7.0
Avaya TSAPI Client	7.0
IntraNext iGuard	10.3

5. Configure Avaya Aura® Communication Manager

This section contains steps necessary to configure iGuard successfully with Avaya Aura® Communication Manager.

All configurations in Communication Manager were performed via SAT terminal.

5.1. Verify Feature and License

Enter the **display system-parameters customer-options** command and ensure that the following features are enabled.

One Page 3, verify **Computer Telephone Adjunct Links** is set to **y.**

```
display system-parameters customer-options                      Page   3 of  11
                                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
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                           DS1 MSP? y
                                 ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

5.2. Configure Stations

Use **add station *n*** command to add virtual stations that will be used by iGuard to perform single step conference, where ***n*** is an available station extension. Configure the station as follows, on Page 1:

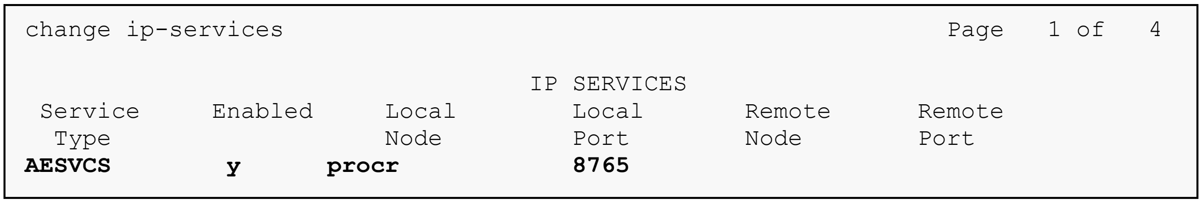
- In **Name** field, enter a descriptive name
- Set **Type** to the type of the telephones
- Enter a **Security Code**
- Set **IP Softphone** to **y**

```
                               STATION

Extension: 11551                         Lock Messages? n               BCC: M
     Type: 9630                          Security Code: 123456           TN: 1
     Port: S00019                      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: 11551
            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
```

5.3. Configure IP Services

Add an IP-Services entry, using the **change ip-services** command, for Application Enablement Services as described below. On Page 1:

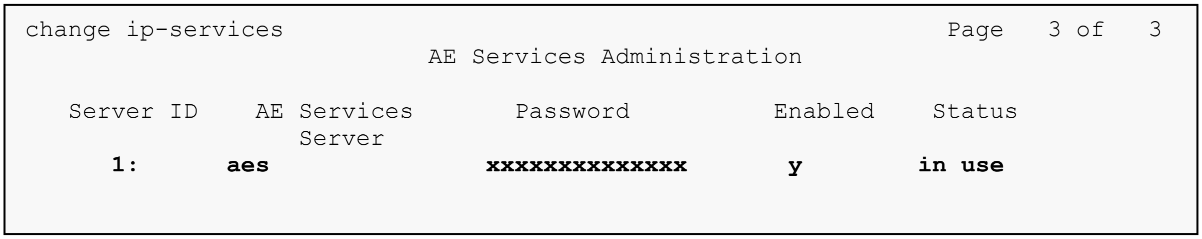
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.



```
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 host name of the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server in **Section 6**, **Step 1**.
- In the **Enabled** field, type **y**.



```
change ip-services                                              Page   3 of   3
                            AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:      aes              xxxxxxxxxxxxxx       y        in use
```

5.4. Configure CTI Link

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type 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: 19999
     Type: ADJ-IP
                                                                        COR: 1
     Name: aes
```

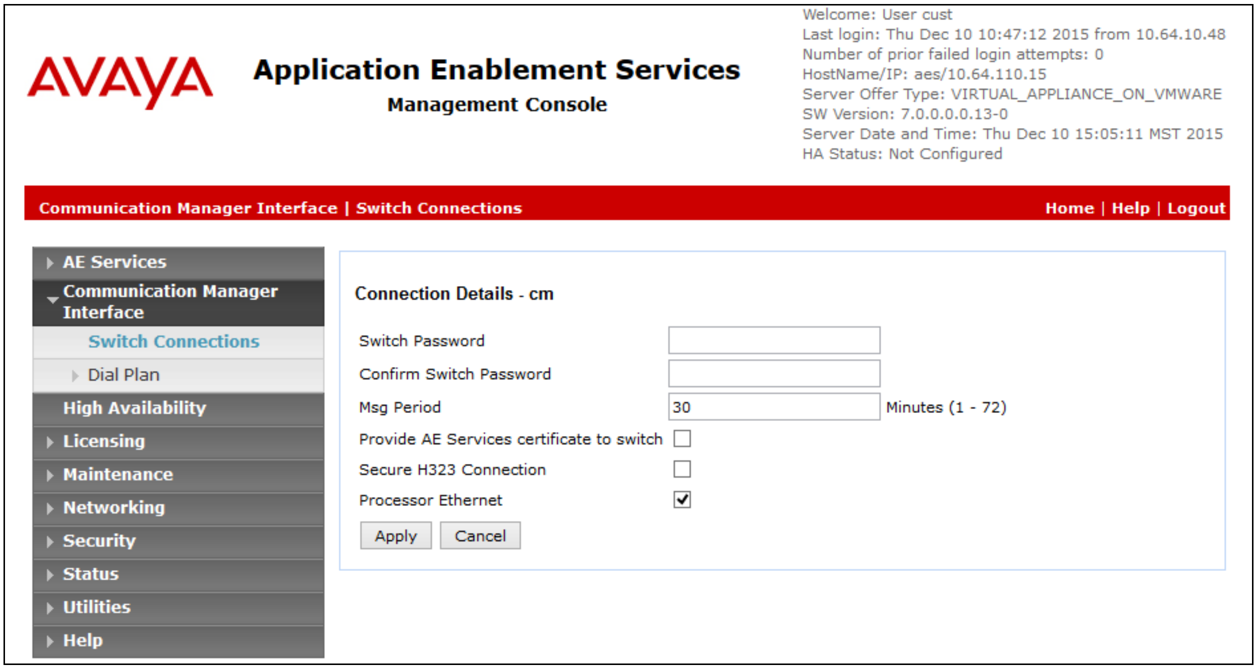
6. Configure Avaya Aura® Application Enablement Services

Configuration of Avaya Aura® Application Enablement Services requires a user account be configured for iGuard and CTI/TSAPI configuration for Communication Manager.

All administration is performed by web browser, https://<aes-ip-address>/

6.1. Configure Communication Manager Switch Connections

To add links to Communication Manager, navigate to the **Communication Manager Interface → Switch Connections** page and enter a name for the new switch connection (e.g. **cm**) and click the **Add Connection** button (not shown). The **Connection Details** screen is shown. Enter the **Switch Password** configured in **Section 5.3** and check the **Processor Ethernet** box if using the **procr** interface. Click **Apply**.

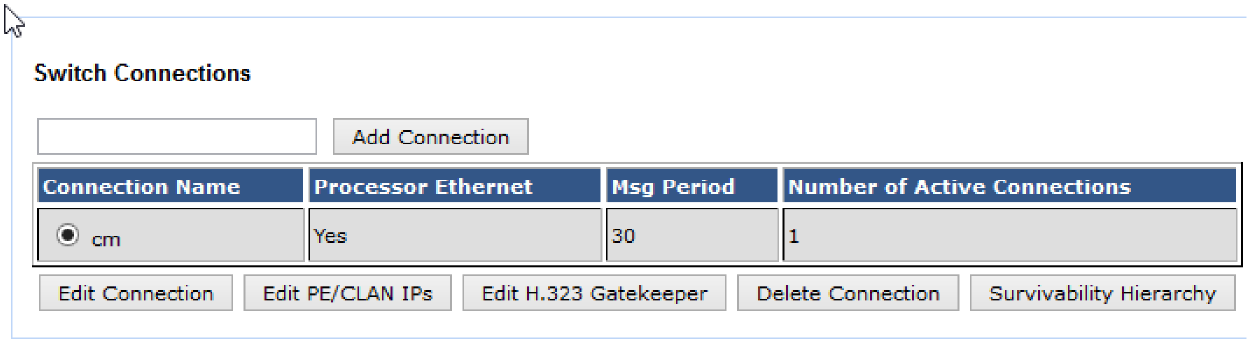


Welcome: User cust
Last login: Thu Dec 10 10:47:12 2015 from 10.64.10.48
Number of prior failed login attempts: 0
HostName/IP: aes/10.64.110.15
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.0.0.0.13-0
Server Date and Time: Thu Dec 10 15:05:11 MST 2015
HA Status: Not Configured

Connection Details - cm

Switch Password		
Confirm Switch Password		
Msg Period	30	Minutes (1 - 72)
Provide AE Services certificate to switch	□	
Secure H323 Connection	□	
Processor Ethernet	☑	

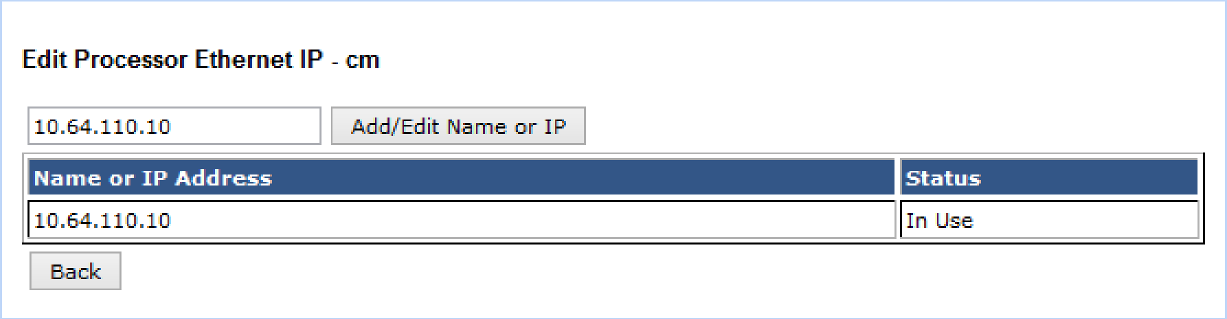
The display returns to the **Switch Connections** screen which shows that the **cm** switch connection has been added.



Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
● cm	Yes	30	1

Click the **Edit PE/CLAN IPs** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic. The **Edit Processor Ethernet IP** screen is displayed. Enter the IP address of the **procr** interface and click the **Add/Edit Name or IP** button.

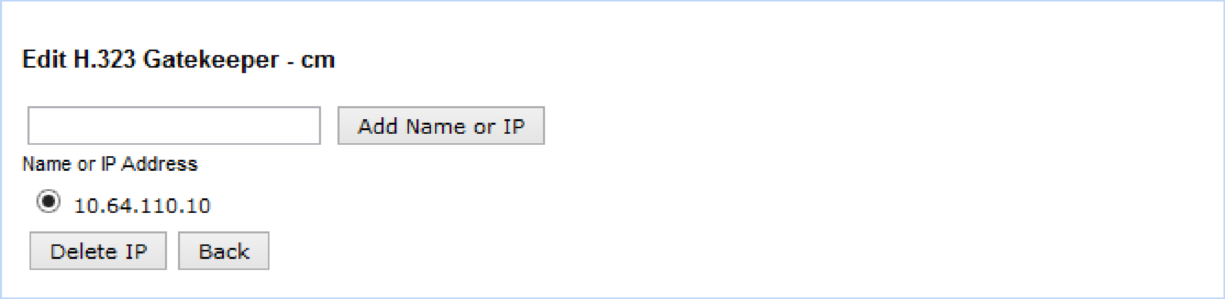


Edit Processor Ethernet IP - cm

10.64.110.10

Name or IP Address	Status
10.64.110.10	In Use

Click the **Edit H.323 Gatekeeper** button on the **Switch Connections** screen to configure the **procr** or **CLAN** IP Address(es) for DMCC registrations. The **Edit H.323 Gatekeeper** screen is displayed. Enter the IP address of the **procr** interface and click the **Add Name or IP** button.



Edit H.323 Gatekeeper - cm

Name or IP Address

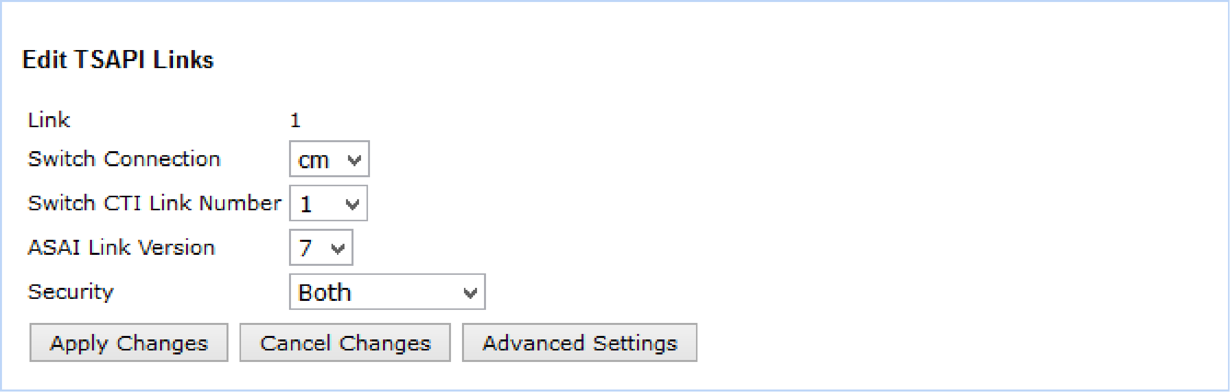
● 10.64.110.10

6.2. Add TSAPI Link

Navigate to the **AE Services** →**TSAPI** → **TSAPI Links** page to add a 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 in **Section 5**. **4**. Select **Both** in the **Security** field.

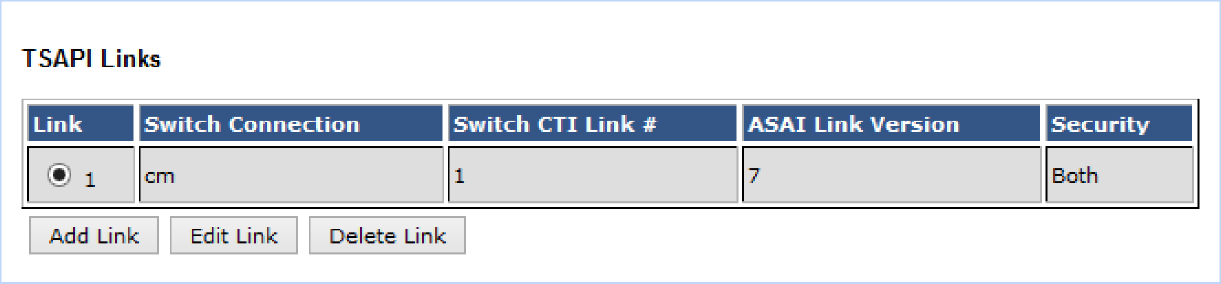
Click **Apply Changes**.



Edit TSAPI Links

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

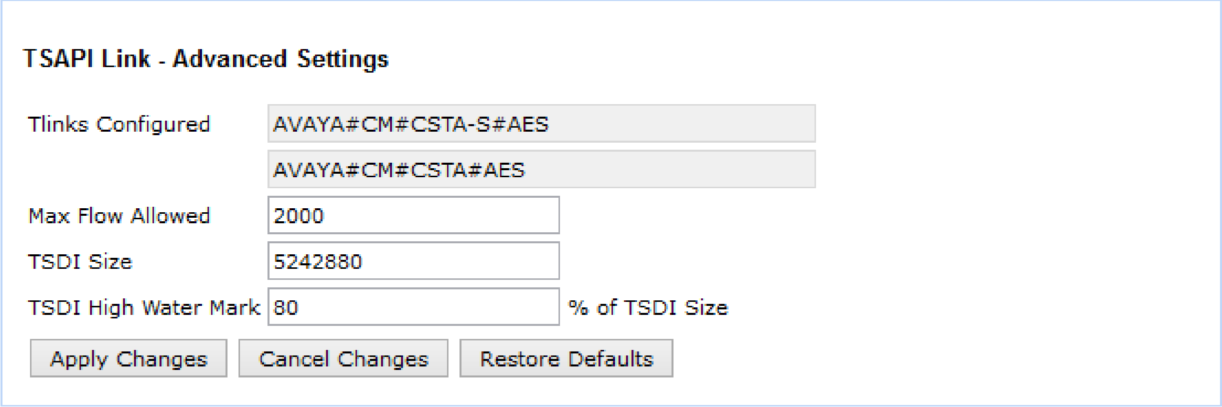
It returns to the **TSAPI Links** screen which shows that the **cm** link has been added.



TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	cm	1	7	Both

Click **Edit Link →Advanced Setting** to obtain the TSAPI Link that will be used by iGuard.



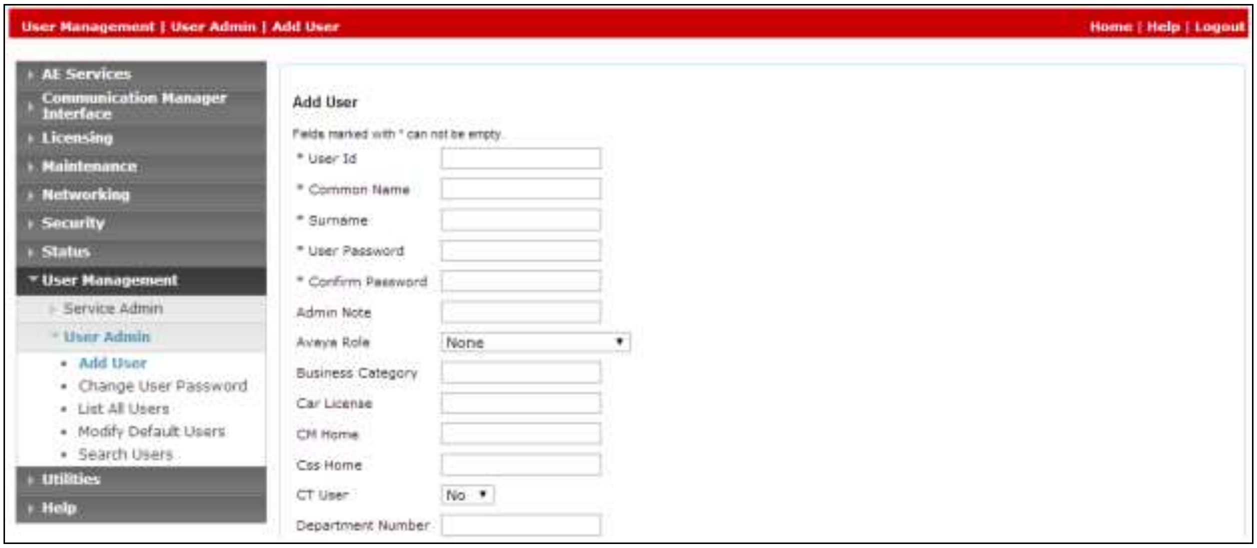
TSAPI Link - Advanced Settings

Tlinks Configured	AVAYA#CM#CSTA-S#AES AVAYA#CM#CSTA#AES
Max Flow Allowed	2000
TSDI Size	5242880
TSDI High Water Mark	80 % of TSDI Size

6.3. Configure User

A user needs to be created for iGuard 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**.

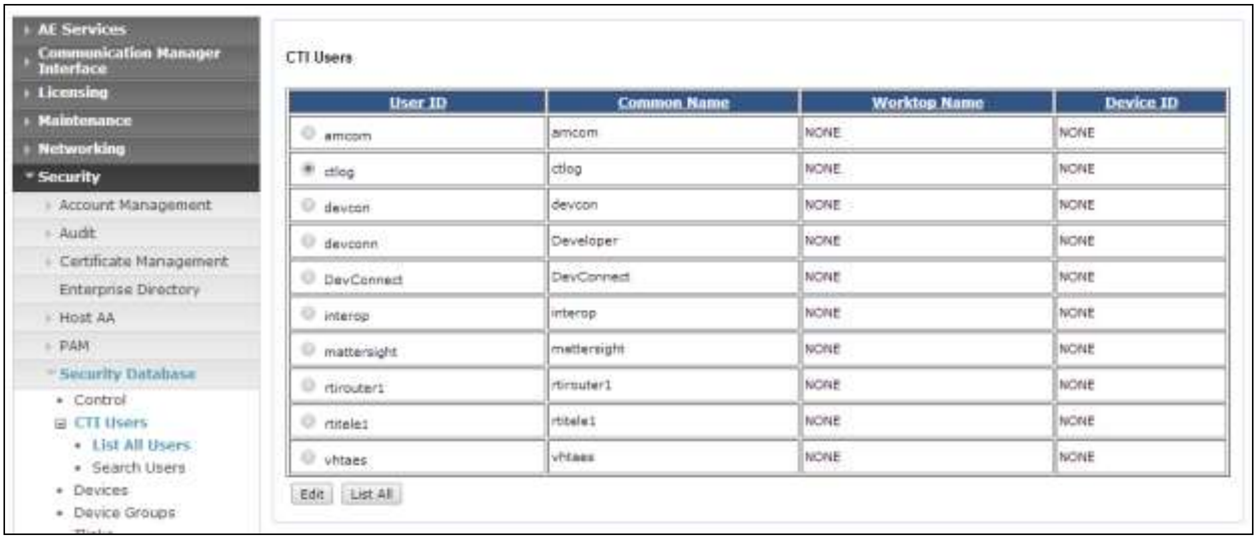


Add User

Fields marked with * can not be empty.

* User Id	
* Common Name	
* Surname	
* User Password	
* Confirm Password	
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	No
Department Number	

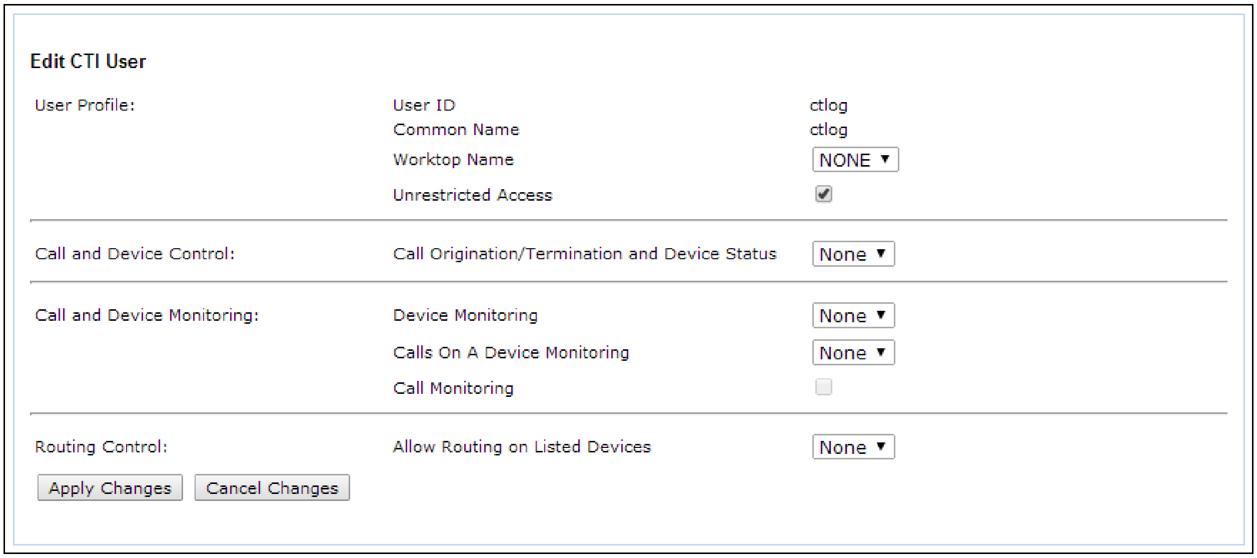
Navigate to **Security → Security Database → CTI Users → List All Users**.



CTI Users

	User ID	Common Name	Worktop Name	Device ID
○	amcom	amcom	NONE	NONE
●	ctlog	ctlog	NONE	NONE
○	devcon	devcon	NONE	NONE
○	devconn	Developer	NONE	NONE
○	DevConnect	DevConnect	NONE	NONE
○	interop	interop	NONE	NONE
○	mattersight	mattersight	NONE	NONE
○	rtirouter1	rtirouter1	NONE	NONE
○	rtitele1	rtitele1	NONE	NONE
○	vhtaes	vhtaes	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	ctlog
	Common Name	ctlog
	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 iGuard

All configuration related to iGuard is performed by IntraNext engineers and, thus, is not documented.

8. Verification Steps

To verify the status CTI Links to AES , via SAT, use the **status aesvcs cti-link**. The **Service State** of **established** indicates that the trunk is in an operational state.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     7        no    aes              established   15       15
```

To verify iGuard is able to monitor the stations correctly, use the **list monitored-station** command. All the stations that are being monitored by iGuard are as shown below:

```
list monitored-station

                            MONITORED STATION

  Station     Association 1    Association 2    Association 3    Association 4
  Ext         CTI Link  CRV    CTI Link  CRV    CTI Link  CRV    CTI Link  CRV
  -------     -------------    -------------    -------------    -------------
11551          1          27
11552          1          25
```

9. Conclusion

IntraNext iGuard was able to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

10. Additional References

Documentation related to Avaya can be obtained from https://support.avaya.com.

[1] *Administering Avaya Aura® Communication Manager, Release 7.0, July 2015*

[2] *Avaya Aura® Application Enablement Service Administration and Maintenance Guide, Release 7.0, August 2015*

[3] *IntraNext iGuard Version 10.1 Implementation Guide (PA-DSS), Avaya version 5.4*

©2016 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.