Application Notes for Configuring esuits^2 AES Connector from Engelbart Software with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for the middleware solution esuits^2 AES Connector from Engelbart Software to interoperate with Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0. esuits^2 AES Connector utilizes the TS Links on Avaya Aura® Application Enablement Services to make administrative changes on 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 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 describe the configuration steps to integrate Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services with esuits^2 AES Connector.

esuits^2 AES Connector utilizes the TS Links on Avaya Aura® Application Enablement Services to make administrative changes on Avaya Aura® Communication Manager.

2. General Test Approach and Test Results

The general test approach was to configure the esuits^2 AES Connector to communicate with the Communication Manager (CM) via the Application Enablement Services (AES). A dedicated user was configured on esuits^2 AES Connector to allow changes to be made to Station, Hunt Groups and Pickup Groups. See **Figure 1** for a network diagram. The interoperability compliance test included both feature functionality and serviceability tests focusing on validating successful changes to CM.

esuits^2 AES Connector acts as a middleware TSAPI Client for various software solutions of Engelbart and was installed on an Ubuntu Linux virtual Machine. Changes are made using an internet browser that can access esuits^2 AES Connector.

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 both feature functionality and serviceability testing. The feature functionality testing focused on making changes to CM objects. The tests included:

- List existing Stations.
- Duplicate, Change and Remove Stations.
- List existing Hunt Groups.
- Modify non EAS hunt group members.
- List existing Pickup Groups.
- Modify Pickup Group members.

2.2. Test Results

All functionality and serviceability test cases were completed successfully.

3. Support

Paul Engelhardt
Engelbart Software GmbH
Goetheplatz 2
D-88214 Ravensburg
Tel.: +49 (0)751 76 424 311
www.engelbart-software.de

4. Reference Configuration

The configuration shown in **Figure 1** was used during the compliance test of esuits^2 AES Connector with AES and Communication Manager. esuits^2 AES Connector utilises AES to make administrative changes in Communication Manager.

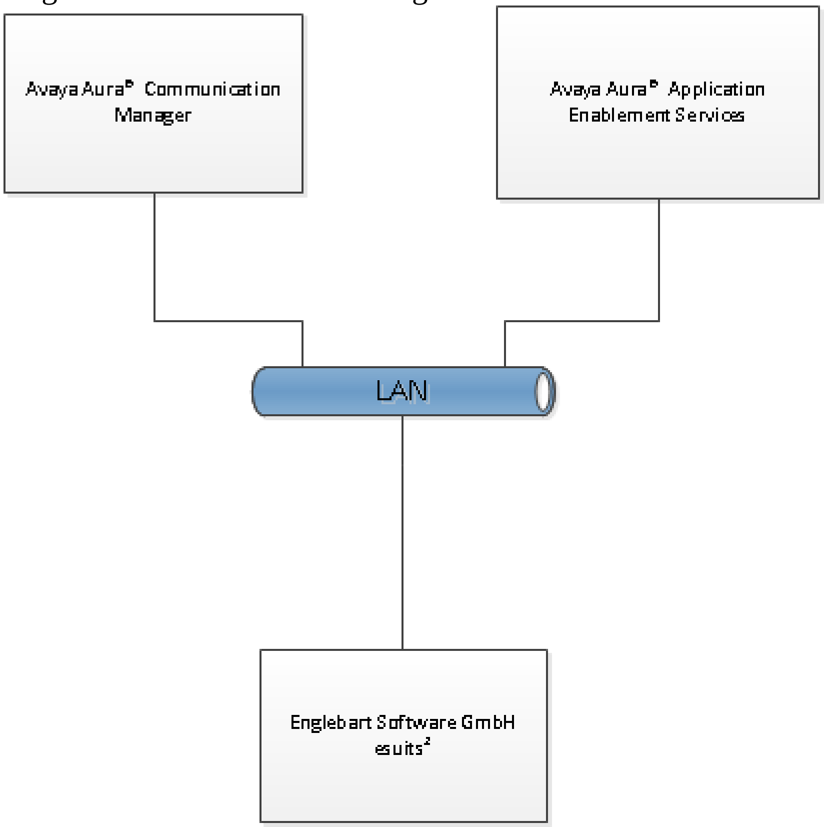

Avaya Aura® Communication Manager
Avaya Aura® Application Enablement Services
LAN
Englebart Software GmbH esuits²

Figure 1: Connection of Engelbart Software esuits^2 AES Connector with Avaya Aura® Application Enablement Services R7.0, Avaya Aura® Communication Manager R7.0

5. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on a virtual server	R7 SP1 R017.00.0.441.22438
Avaya Aura® Application Enablement Services running on a virtual server	7.0.0.0.0.13-0
Avaya G450 Gateway	37.19.0
esuits^2 AES Connector	R3

6. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

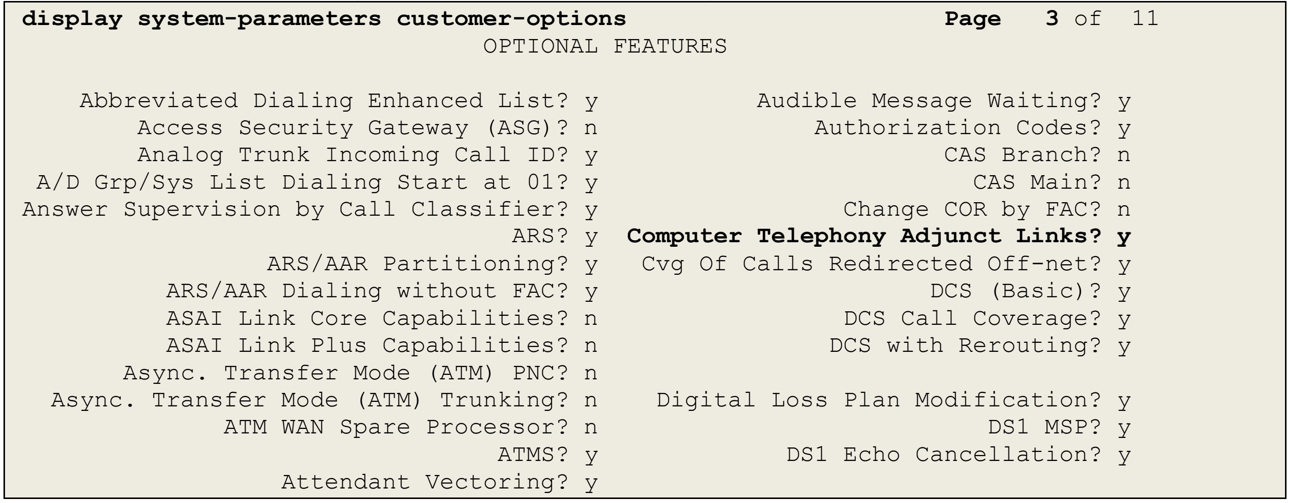
The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

6.1. Configure the Avaya Aura® Communication Manager Connection to Avaya Aura® Application Enablement Services

The connection between Communication Manager and AES is assumed to be already in place however the steps required to set this connection are listed in the sections below.

6.1.1. Verify System Features

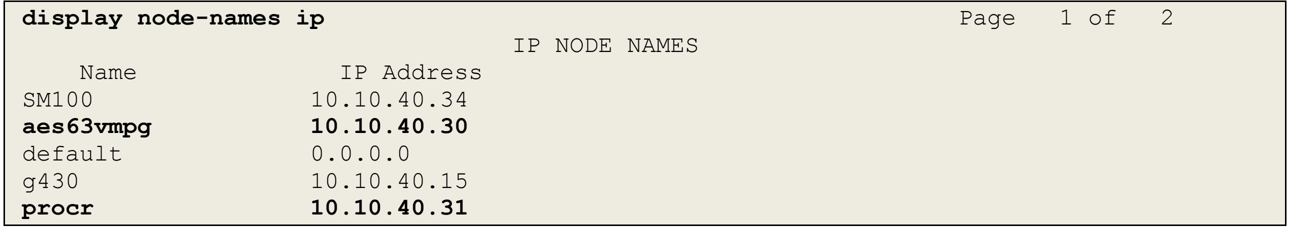
Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.



```
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? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               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
```

6.1.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aes63vmpg**).

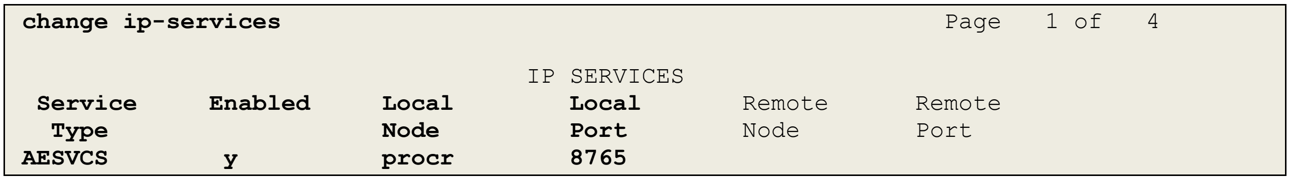


```
display node-names ip                                             Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM100               10.10.40.34
aes63vmpg           10.10.40.30
default             0.0.0.0
g430                10.10.40.15
procr               10.10.40.31
```

6.1.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 6.1.2**
- **Local Port:** Retain the default value of **8765**.

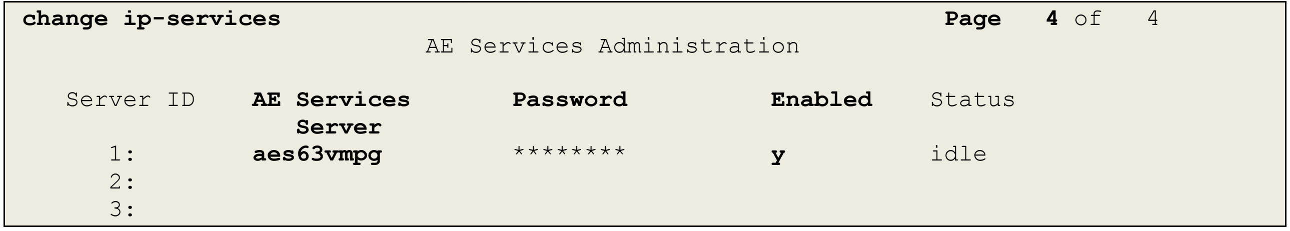


```
change ip-services                                            Page   1 of   4

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

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aes63vmpg**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

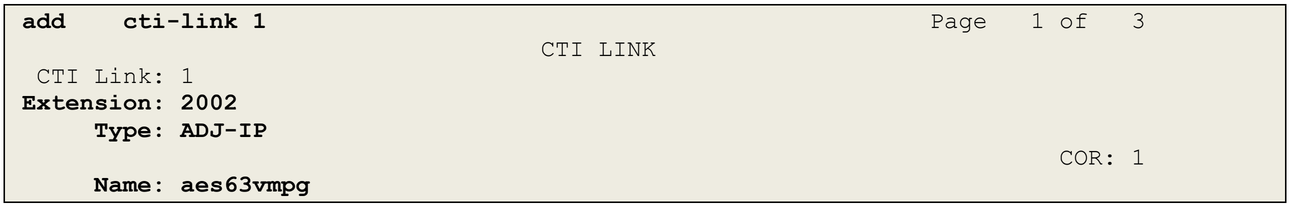
Note: The password entered for **Password** field must match the password on the AES server in **Section 7.2**. The **AE Services Server** must match the administered name for the AES server, this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.



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

   Server ID    AE Services      Password          Enabled    Status
                   Server
      1:        aes63vmpg        ********          y          idle
      2:
      3:
```

6.1.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

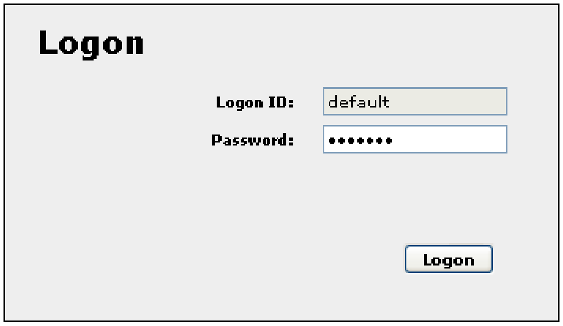


```
add    cti-link 1                                            Page   1 of   3
                                  CTI LINK
 CTI Link: 1
Extension: 2002
     Type: ADJ-IP
                                                                      COR: 1
     Name: aes63vmpg
```

6.1.5. Create Administrative User in Avaya Aura® Communication Manager

This section provides the procedure for administering a user with privileged administrator access in the Communication Manager web interface.

Browse to http://<CM IP Address> and login with the appropriate credentials.

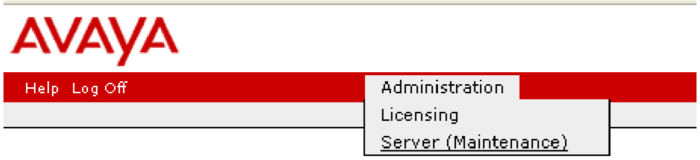


Logon

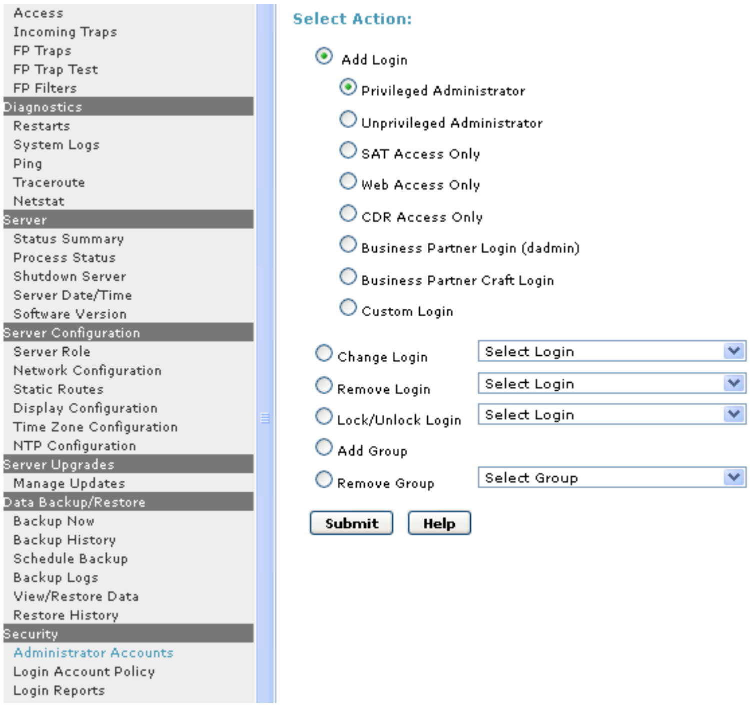
Logon ID: default

Password: •••••••

Select **Administration→Server (Maintenance)**



From the left hand menu select **Security→Administrative Accounts** and select Privileged Administrator.



Select Action:

● Add Login

- ● Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

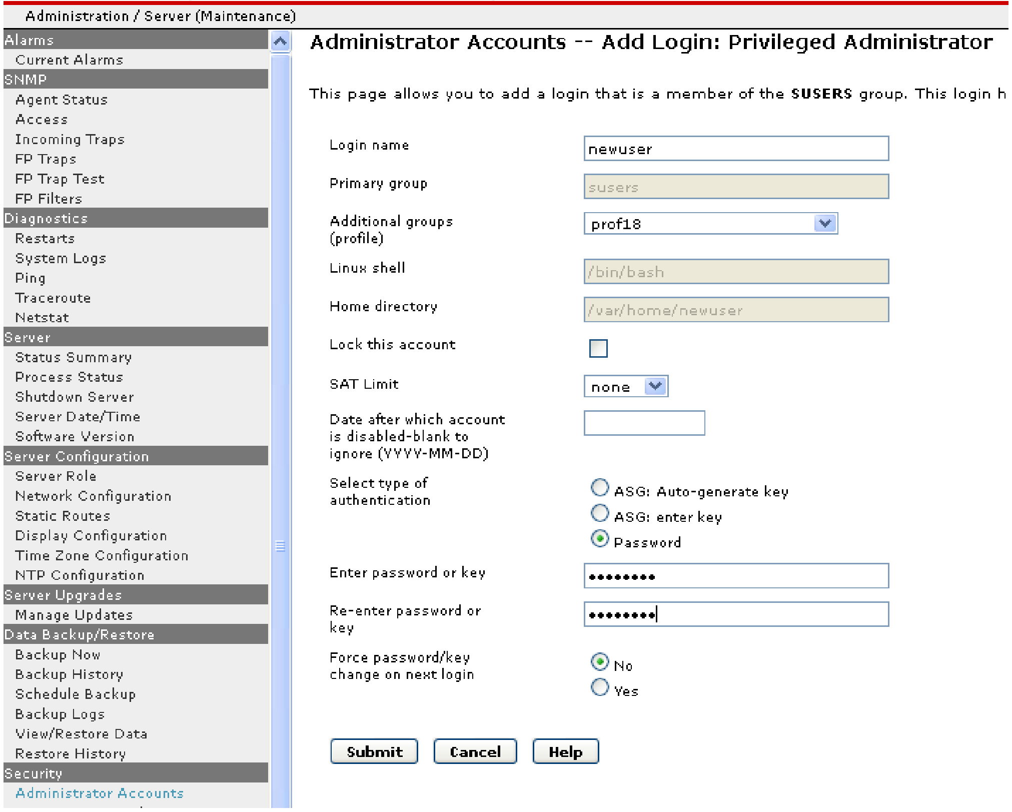
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

Give the user a unique **Login Name** and **Password**. Make sure that **Additional groups (profile)** is set to **prof18** allowing the user to make changes required.



Administrator Accounts -- Add Login: Privileged Administrator

This page allows you to add a login that is a member of the **SUSERS** group. This login h

Login name	newuser
Primary group	susers
Additional groups (profile)	prof18
Linux shell	/bin/bash
Home directory	/var/home/newuser
Lock this account	□
SAT Limit	none
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	
Select type of authentication	○ ASG: Auto-generate key ○ ASG: enter key ● Password
Enter password or key	••••••••
Re-enter password or key	••••••••
Force password/key change on next login	● No ○ Yes

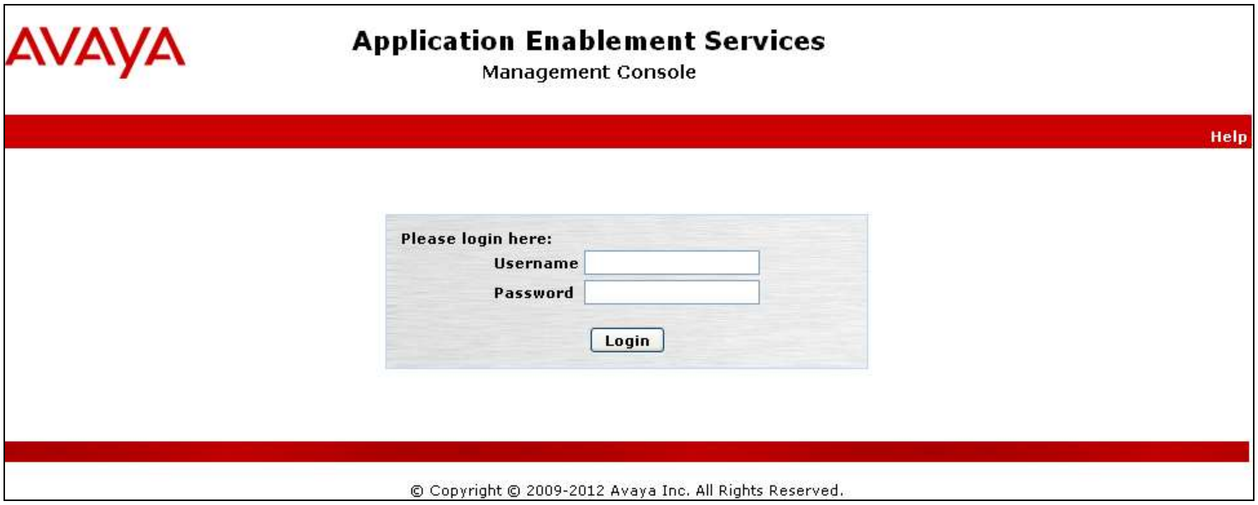
7. Configure Avaya Aura® Application Enablement Services

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

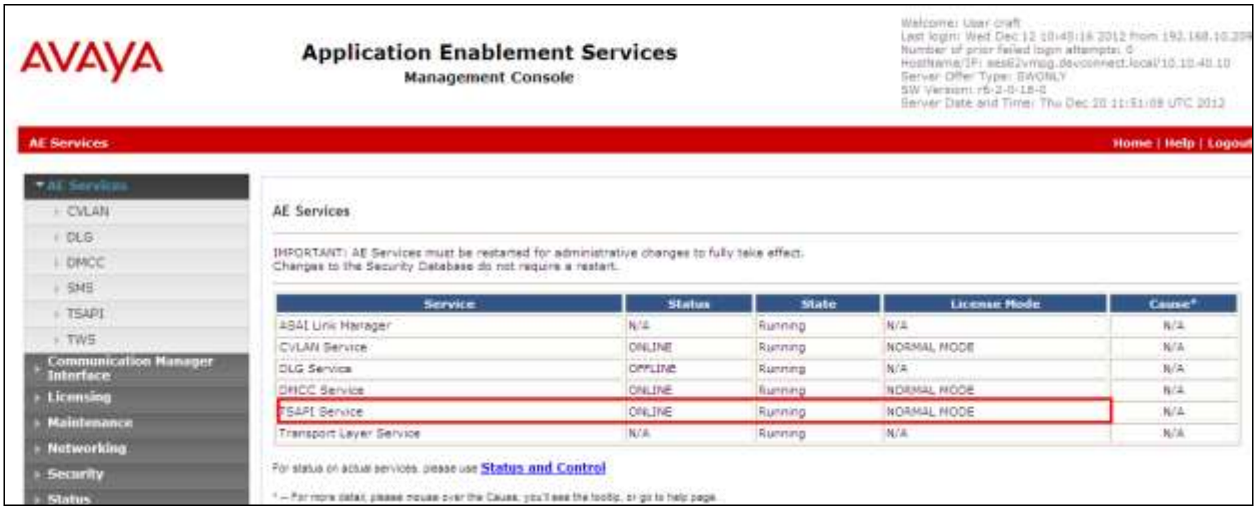
- Verify Licensing.
- Create Switch Connection.
- Administer TSAPI link.
- Enable DMCC Ports.
- Create CTI User.
- Associate Devices with CTI User.

7.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.


AVAYA
Application Enablement Services
Management Console
Help
Please login here:
Username
Password
Login
© Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI Service is licensed by ensuring that **TSAPI Service** is in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.



Welcome: User craft
Last login: Wed Dec 12 10:45:16 2012 from 192.168.10.239
Number of prior failed login attempts: 0
HostName/IP: aes62vmpg.devconnect.local/10.10.40.10
Server Offer Type: SWONLY
SW Version: r6-2-0-18-0
Server Date and Time: Thu Dec 20 11:51:08 UTC 2012

AE Services

IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.

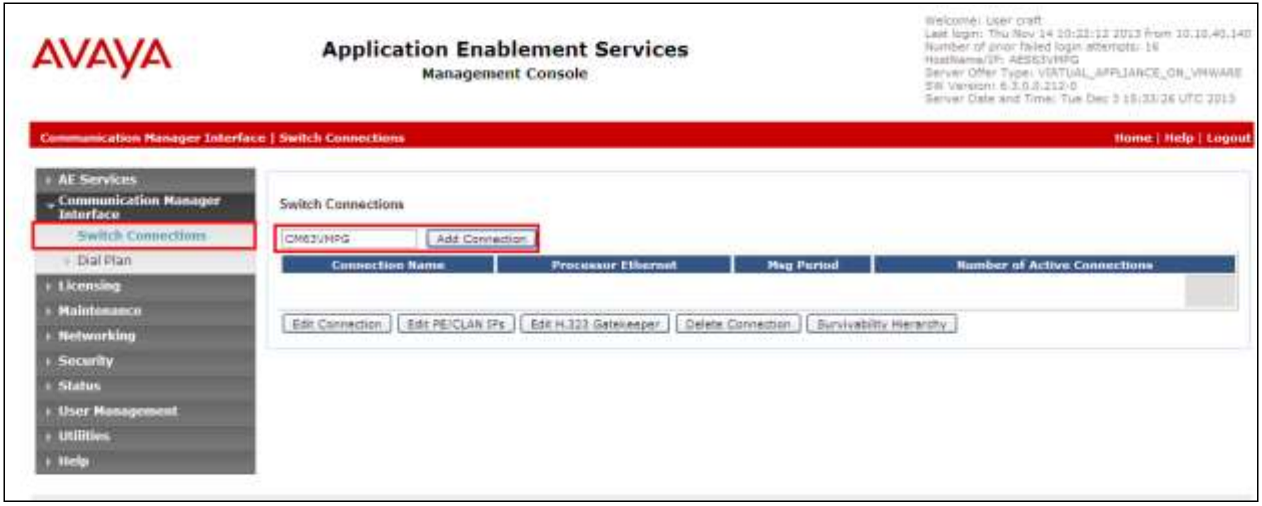
Service	Status	State	License Mode	Cause*
ASAI Link Manager	N/A	Running	N/A	N/A
CVLAN Service	ONLINE	Running	NORMAL MODE	N/A
DLG Service	OFFLINE	Running	N/A	N/A
DMCC Service	ONLINE	Running	NORMAL MODE	N/A
TSAPI Service	ONLINE	Running	NORMAL MODE	N/A
Transport Layer Service	N/A	Running	N/A	N/A

For status on actual services, please use **Status and Control**

* – For more detail, please mouse over the Cause, you'll see the tooltip, or go to help page.

7.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface → Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.



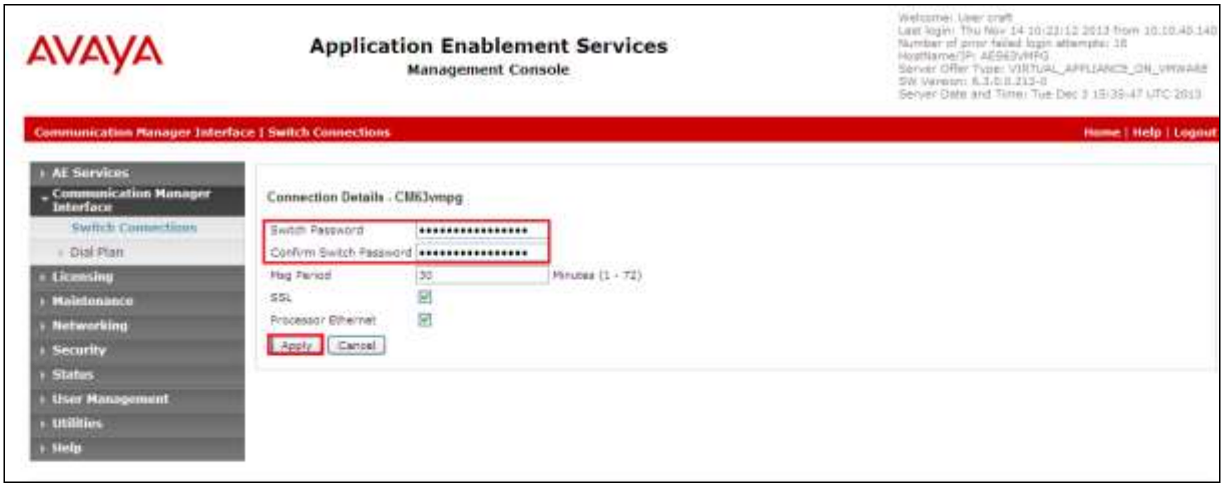
Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 3 15:33:26 UTC 2013

Switch Connections

CM63VMPG

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections

In the resulting screen enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 6.1.3**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.



Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 18
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 3 15:35:47 UTC 2013

Connection Details - CM63vmpg

Switch Password ••••••••••••••••

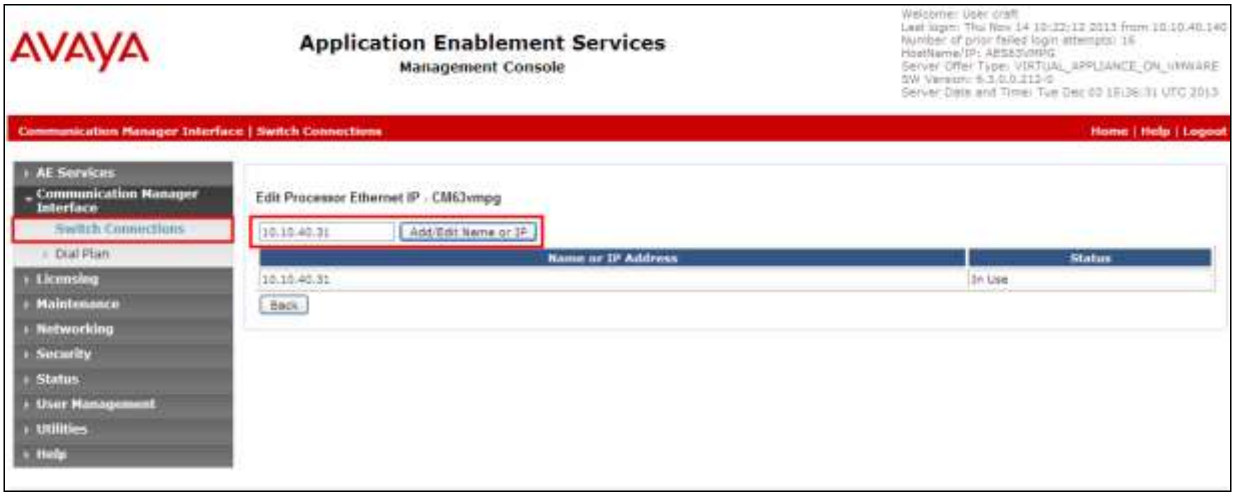
Confirm Switch Password ••••••••••••••••

Msg Period 30 Minutes (1 - 72)

SSL ☑

Processor Ethernet ☑

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown). In the resulting screen, enter the IP address of the procr as shown in **Section 6.1.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.



Welcome: User craft
Last login: Thu Nov 14 10:22:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 15:36:31 UTC 2013

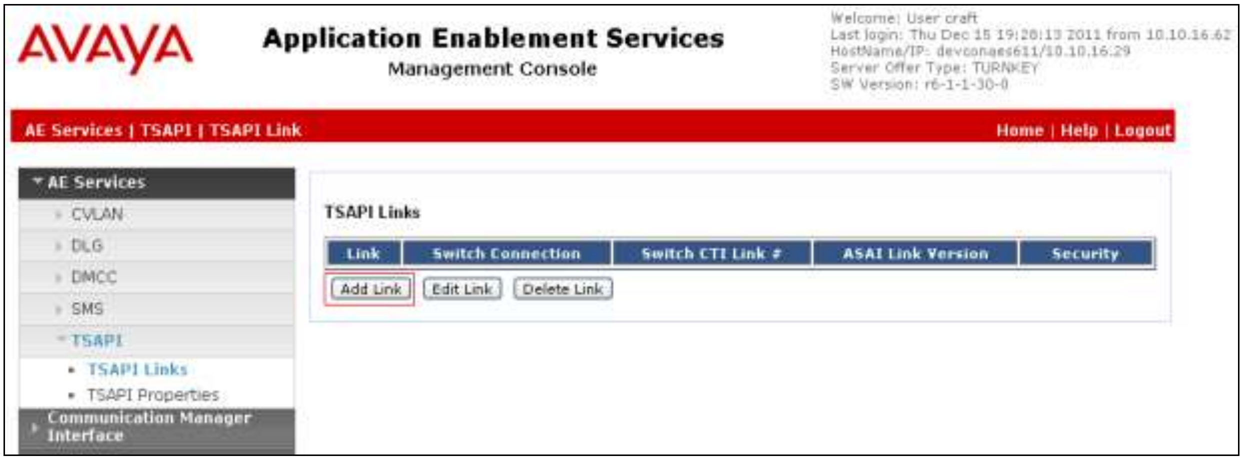
Edit Processor Ethernet IP - CM63vmpg

10.10.40.31

Name or IP Address	Status
10.10.40.31	In Use

7.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services → TSAPI → TSAPI Links**. Select **Add Link** button as shown in the screen below.



Welcome: User craft
Last login: Thu Dec 15 19:20:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

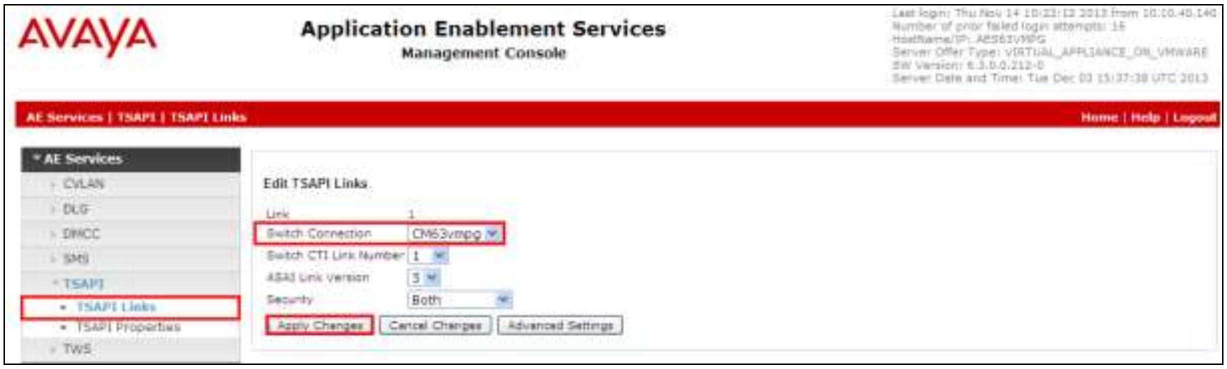
TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security

On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **CM63VMPG**, which has already been configured in **Section 7.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 6.1.4** which is **1**.
- **ASAI Link Version:** This can be left at the default value of **5**.
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.

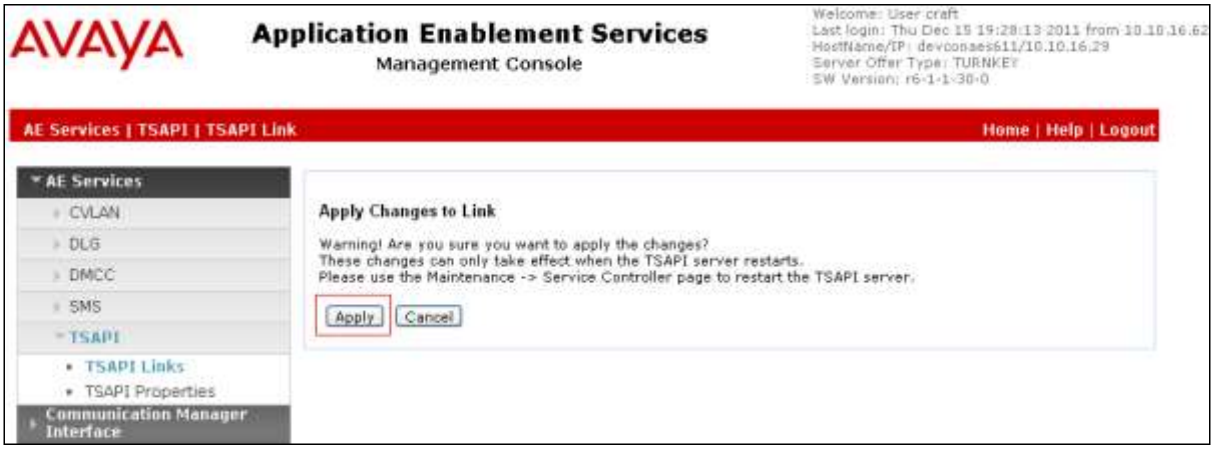


Last login: Thu Nov 14 10:23:12 2013 from 10.10.40.140
Number of prior failed login attempts: 16
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 15:37:38 UTC 2013

Edit TSAPI Links

Link 1
Switch Connection CM63vmpg
Switch CTI Link Number 1
ASAI Link Version 5
Security Both

Another screen appears for confirmation of the changes made. Choose **Apply**.

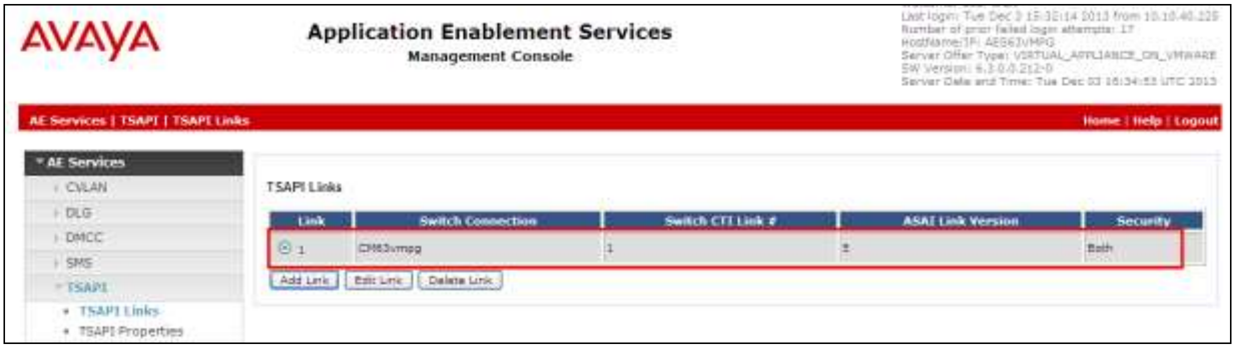


Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.
Please use the Maintenance -> Service Controller page to restart the TSAPI server.

When the TSAPI Link is completed, it should resemble the screen below.

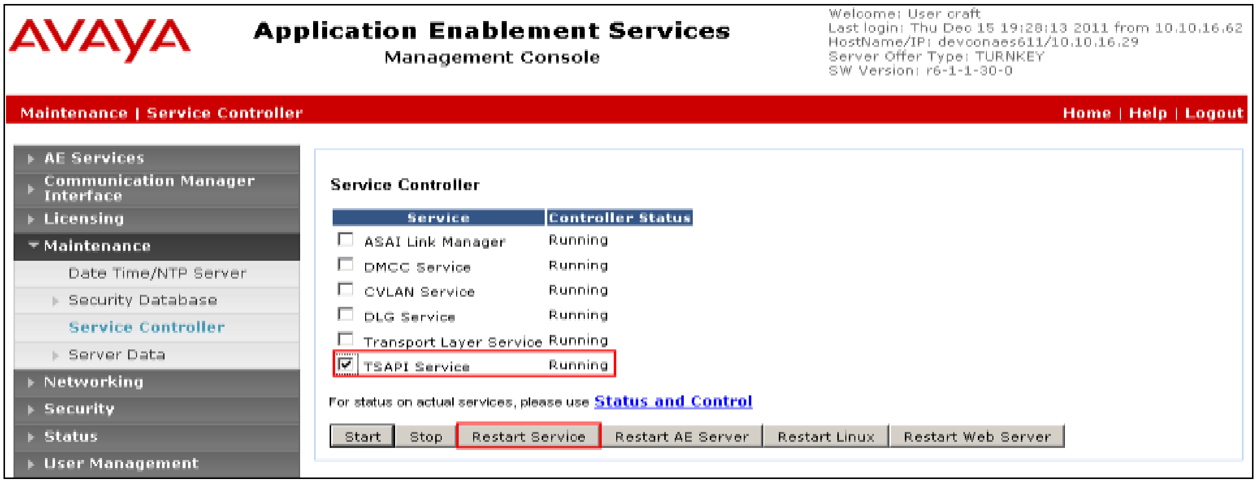


Last login: Tue Dec 3 15:32:14 2013 from 10.10.40.225
Number of prior failed login attempts: 17
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Tue Dec 03 16:34:55 UTC 2013

TSAPI Links

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
● 1	CM63vmpg	1	5	Both

The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.



Welcome: User craft
Last login: Thu Dec 15 19:28:13 2011 from 10.10.16.62
HostName/IP: devconaes611/10.10.16.29
Server Offer Type: TURNKEY
SW Version: r6-1-1-30-0

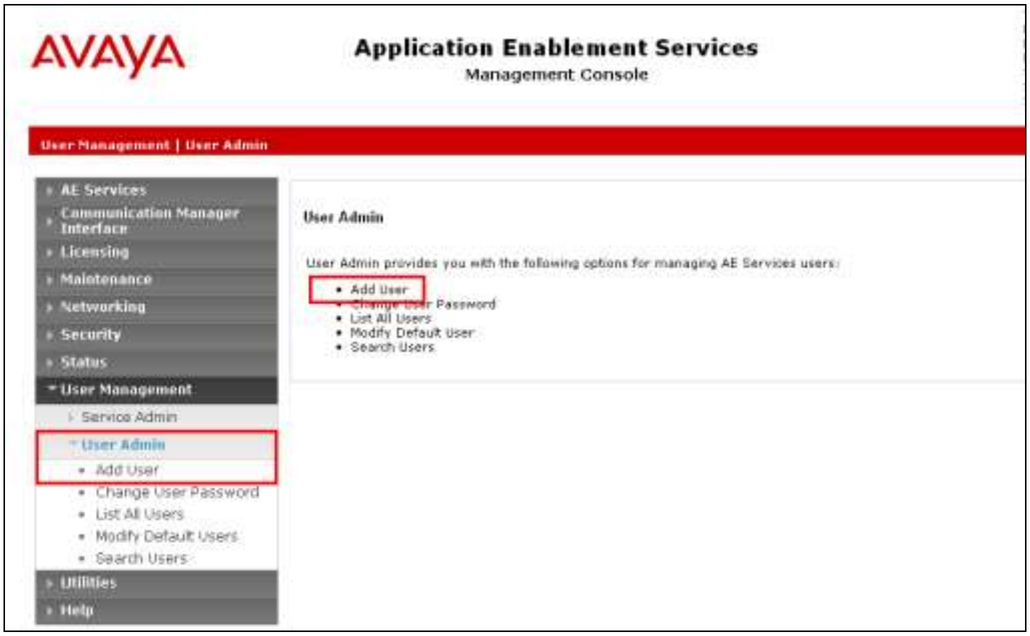
Service Controller

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

For status on actual services, please use Status and Control

7.4. Create CTI User

A User ID and password needs to be configured for the esuits^2 server to communicate as a TSAPI client with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.



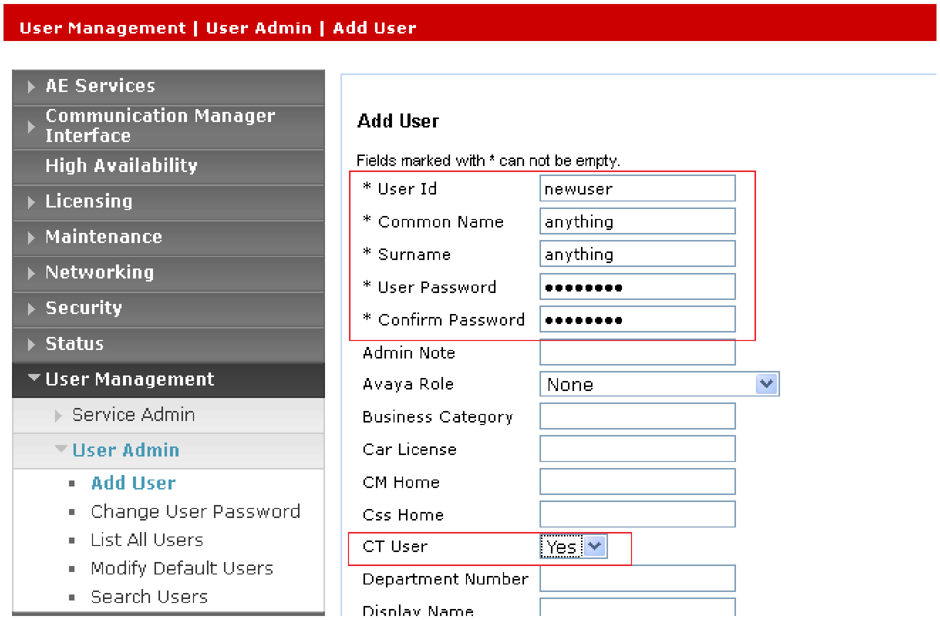
User Admin

User Admin provides you with the following options for managing AE Services users:

- Add User
- Change User Password
- List All Users
- Modify Default User
- Search Users

In the **Add User** screen shown below, enter the following values:

- **User Id -** This will be used by the Esuits^2 Server to connect to AES.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will again be used by the esuits^2 Server.
- **CT User -** Select **Yes** from the drop-down menu.

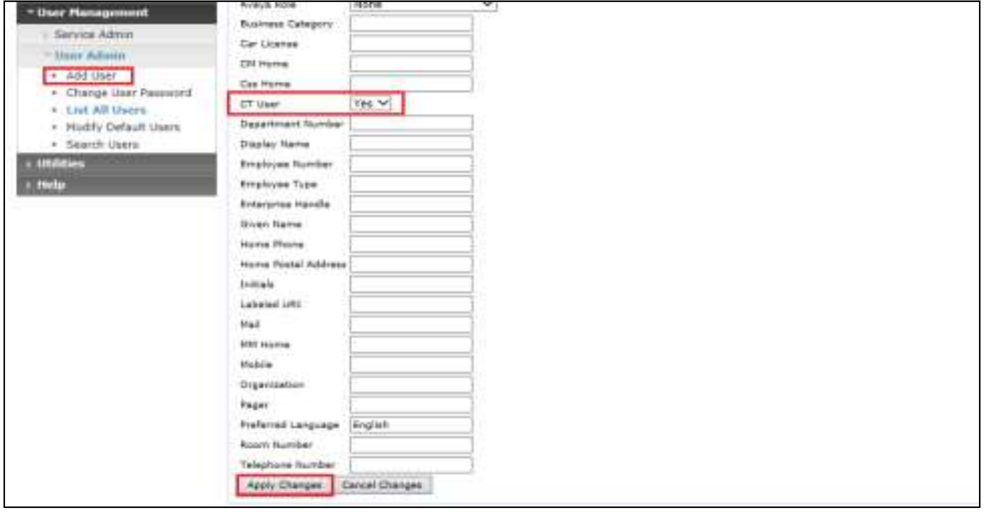


Add User

Fields marked with * can not be empty.

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

Complete the process by choosing **Apply** at the bottom of the screen.

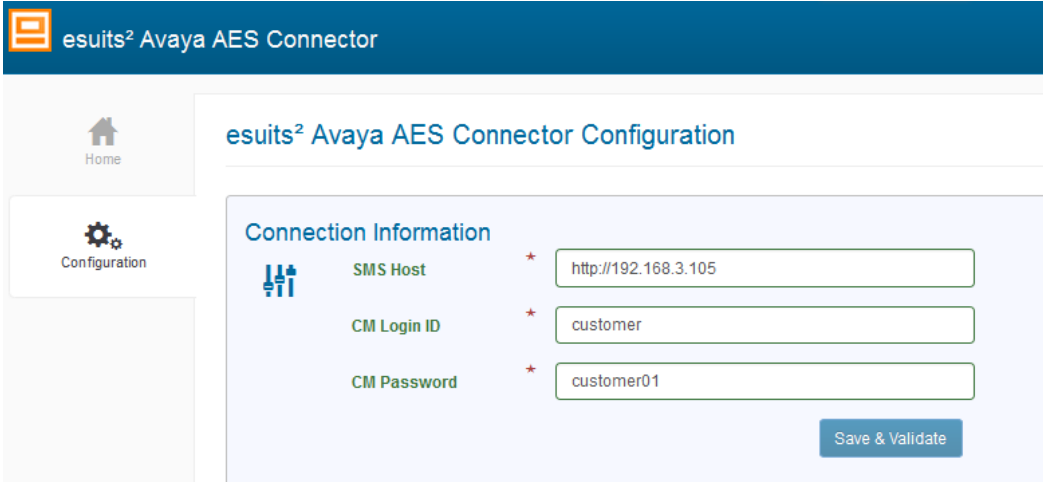


Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes
Department Number	
Display Name	
Employee Number	
Employee Type	
Enterprise Handle	
Given Name	
Home Phone	
Home Postal Address	
Initials	
Labeled URI	
Mail	
MM Home	
Mobile	
Organization	
Pager	
Preferred Language	English
Room Number	
Telephone Number	

The next screen will show a message indicating that the user was created successfully (not shown).

8. Configure esuits^2 AES Connector

To access the esuits^2 AES Connector, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of the esuits^2 AES Connector.
Define the parameters within section “Configuration”.

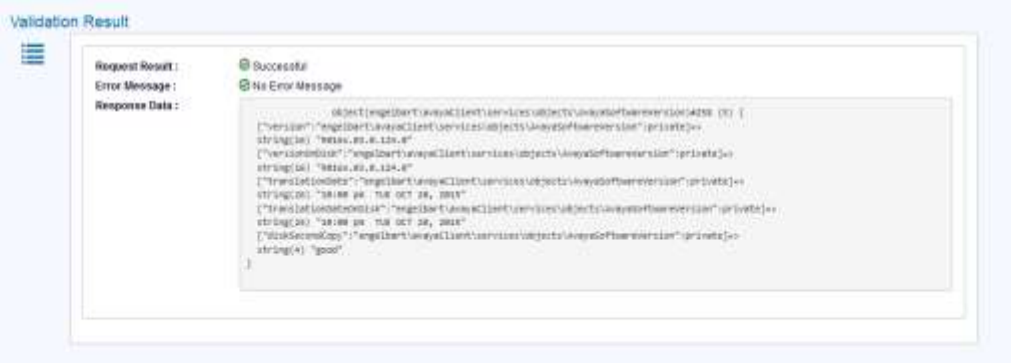


esuits² Avaya AES Connector Configuration

Connection Information

SMS Host *	http://192.168.3.105
CM Login ID *	customer
CM Password *	customer01

Press “Save & Validate” to store the configuration. With this the connection to the AES will be verified.
If the connection could be established the following response will be shown:

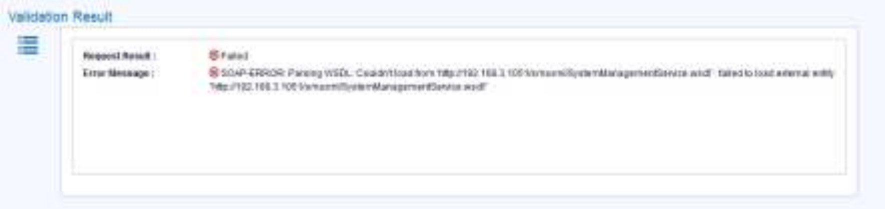


Validation Result

Request Result : Successful
Error Message : No Error Message
Response Data :

```
          object(engelbart\avayaClient\services\objects\AvayaSoftwareVersion)#258 (5) {
["version":"engelbart\avayaClient\services\objects\AvayaSoftwareVersion":private]=>
string(16) "R016x.03.0.124.0"
["versionOnDisk":"engelbart\avayaClient\services\objects\AvayaSoftwareVersion":private]=>
string(16) "R016x.03.0.124.0"
["translationDate":"engelbart\avayaClient\services\objects\AvayaSoftwareVersion":private]=>
string(26) "10:00 pm  TUE OCT 20, 2015"
["translationDateOnDisk":"engelbart\avayaClient\services\objects\AvayaSoftwareVersion":private]=>
string(26) "10:00 pm  TUE OCT 20, 2015"
["diskSecondCopy":"engelbart\avayaClient\services\objects\AvayaSoftwareVersion":private]=>
string(4) "good"
}
```

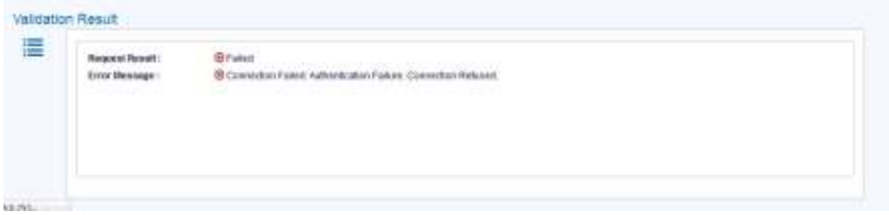
An invalid URL of the AVAYA AES will return the following error.



Validation Result

Request Result : Failed
Error Message : SOAP-ERROR: Parsing WSDL: Couldn't load from 'http://192.168.3.105/smsxml/SystemManagementService.wsdl' : failed to load external entity "http://192.168.3.105/smsxml/SystemManagementService.wsdl"

Invalid login credentials will return the following error.



Validation Result

Request Result : Failed
Error Message : Connection Failed: Authentication Failure. Connection Refused.

9. Verification Steps

This section provides the steps that can be taken to verify correct configuration of the Avaya solution and esuits^2 AES Connector server.

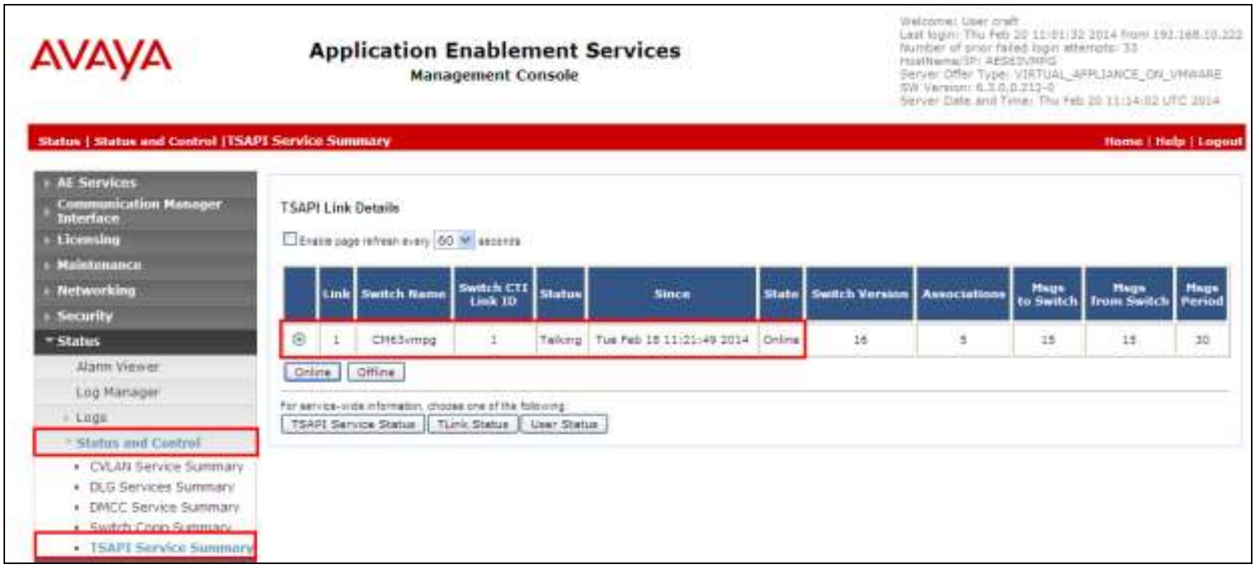
9.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can validate that the communication between Communication Manager and AES is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1         4       no      aes63vmpg      established   18        18
```

9.2. Verify TSAPI Link

On the AES Management Console verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.



Welcome: User craft
Last login: Thu Feb 20 11:01:32 2014 from 192.168.10.222
Number of prior failed login attempts: 33
HostName/IP: AES63VMPG
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Thu Feb 20 11:14:02 UTC 2014

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	CM63vmpg	1	Talking	Tue Feb 18 11:21:49 2014	Online	16	5	15	15	30

For service-wide information, choose one of the following:

9.3. esuits^2 AES Connector Connection

For verification of the connection please see **Section 8**.

10. Conclusion

These Application Notes describe the configuration steps required for Engelbart Software esuits^2 AES Connector to successfully interoperate with Avaya Aura® Avaya Aura® Communication Manager R7.0 and Avaya Aura® Application Enablement Services R7.0. All feature functionality and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

11. Additional References

This section references the Avaya and Engelbart Software product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Administering Avaya Aura® Communication Manager,* Document ID 03-300509.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Document ID 555-245-205.

[3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide Release 7.0.*

Technical documentation can be obtained for esuits^2 AES Connector by contacting Engelbart Software via info@engelbart-software.com.

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

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