



Avaya Solution & Interoperability Test Lab

Application Notes for configuring Avaya Aura® Communication Manager R6.0.1 and Avaya Aura® Application Enablement Services R6.1 to interoperate with ESTOS ECSTA – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for ESTOS ECSTA to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. ESTOS ECSTA provides users with a TAPI to perform a variety of call handling scenarios.

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 required for ESTOS ECSTA to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services (AES). ESTOS ECSTA is a Telephony Service Provider (TSP) for Microsoft TAPI 2.1, 2.2 and 3.0. This TAPI driver implements central communication between a PC and Avaya Aura® Communication Manager using CTI provided by AES. ESTOS Ephone is a test application which is used to verify successful communication between ESTOS ECSTA and AES and ensures call handling is completed as intended. ESTOS Ephone is a test tool provided by ESTOS for the purposes of demonstrating the abilities of ESTOS ECSTA only. The connection to AES is established by ESTOS ECSTA over the CSTA Phase III XML protocol using DMCC.

2. General Test Approach and Test Results

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on a variety of inbound and outbound call handling scenarios to verify successful call control using the ECSTA TSP. The serviceability testing focused on verifying the ability of the ECSTA service to recover from disconnection and reconnection to the Avaya solution.

2.1. Interoperability Compliance Testing

Feature functionality testing included

- Conferencing.
- Consultative transfer.
- Blind transfer.
- Forwarding.
- DND (Do Not Disturb).
- SAC (Send All Calls).
- Call waiting.
- Toggling between held calls.
- Activation/deactivation of the above features.

These calls were placed and received using the Ephone test tool. Serviceability testing verified the ability of the solution to recover from simulated power and network failure.

2.2. Test Results

All tests were executed successfully.

2.3. Support

Technical Support can be obtained for ESTOS products as follows:

- Email: support@estos.de
- Phone: + 49 (8151) 36856-177

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of an Avaya S8800 Server running Communication Manager with Avaya G650 Media Gateway as the PBX. An Avaya S8800 Server hosts the Application Enablement Services software. Avaya 9600 series, 1600 series IP telephones and 2400 series Digital telephones are connected to the PBX and used in the testing. The ESTOS client is running on a Windows 2008 64bit server in a VMWare environment.

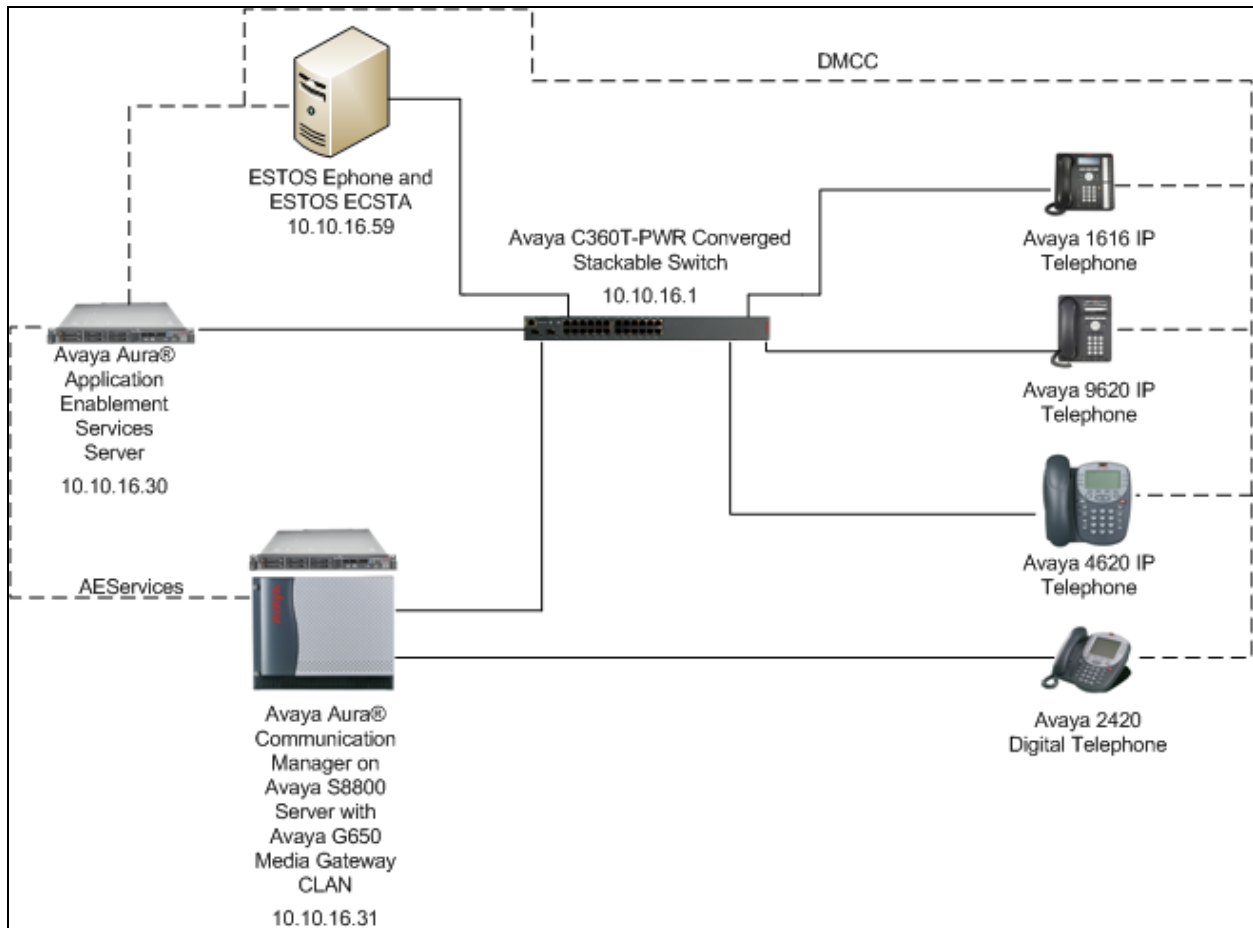


Figure 1: Avaya Aura® Communication Manager with Avaya Aura® Application Enablement Services Server and ESTOS Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Communication Manager R6.0.1 R16.00.1.510.1-19100
Avaya G650- Media Gateway Avaya TN799DP C-LAN Circuit Pack Avaya TN2602AP Media Processor Circuit Pack	HW1 FW40 HW8 FW58
Avaya S8800 Server	Avaya Aura® Application Enablement Services R6.1
Avaya 9620C IP Telephone	3.110b
Avaya 1616 IP Telephone	1_3000
Avaya 4620 IP Telephone	2.3
Avaya 2420 Digital Telephone	REL 4.00 HWV 1 FWV 4
Generic VMWare Server	Microsoft Windows 2008 Server R2 64bit ECSTA Avaya ACM 3.0.0.133uk Ephone X64 3.0.0.135 (64 bit)

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using Communication Manager System Administration Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure Coverage Path
- Configure Station Button Assignments
- Configure the Interface to AES

5.1. Configure Coverage Path

In order to test DND, a cover path must be configured. Enter the command **add coverage-path next**, set **DND/SAC/Goto Cover** to **y**, configure **Point 1** as a station to which calls will be sent when DND is activated, in this case **1350**. Take a note of the **Coverage Path Number**.

add coverage path next		Page 1 of 1	
COVERAGE PATH			
Coverage Path Number: 1			
Cvg Enabled for VDN Route-To Party? n		Hunt after Coverage? n	
Next Path Number:		Linkage	
COVERAGE CRITERIA			
Station/Group Status	Inside Call	Outside Call	
Active?	n	n	
Busy?	y	y	
Don't Answer?	y	y	Number of Rings: 2
All?	n	n	
DND/SAC/Goto Cover?	y	y	
Holiday Coverage?	n	n	
COVERAGE POINTS			
Terminate to Coverage Pts. with Bridged Appearances? n			
Point1: 1350	Rng:	Point2:	
Point3:		Point4:	
Point5:		Point6:	

5.2. Configure Station Button Assignments

The application note assumes stations used are already configured on Communication Manager. Enter the command **change station x**, where **x** is the extension number to be controlled by the Ephone test tool. On **Page 1** configure **Coverage Path 1** with the coverage path created in **Section 5.1**, in this case **1**.

change station 4000		Page 1 of 5
STATION		
Extension: 4000	Lock Messages? n	BCC: 0
Type: 2420	Security Code: 1234	TN: 1
Port: 01A0701	Coverage Path 1: 1	COR: 1
Name: Extn,4000	Coverage Path 2:	COS: 1
Hunt-to Station:		
STATION OPTIONS		
Time of Day Lock Table:		
Loss Group: 2	Personalized Ringing Pattern: 1	
Data Option: none	Message Lamp Ext: 4000	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english	Expansion Module? n	
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	Remote Office Phone? n	
	IP Video Softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

Navigate to **Page 4** and configure **send-calls** and **dn-dst** as button assignments, this will provide a visual indicator of when the Send All Calls and DND features are activated.

change station 4000		Page 4 of 5
STATION		
SITE DATA		
Room:	Headset? n	
Jack:	Speaker? n	
Cable:	Mounting: d	
Floor:	Cord Length: 0	
Building:	Set Color:	
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3: send-calls Ext:	7:	
4: dn-dst	8:	
voice-mail		

5.3. Configure Interface to Avaya Aura® Application Enablement Services

Enter the node **Name** and **IP Address** for the Application Enablement Server, in this case **devconaes61** and **10.10.16.31** respectively. Take a note of the **CLAN** node **Name** and **IP Address** as it is used later in this section.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
CLAN	10.10.16.31	
CM521	10.10.16.23	
Gateway	10.10.16.1	
IPbuffer	10.10.16.184	
Intuition	10.10.16.51	
MedPro	10.10.16.32	
Presence	10.10.16.83	
RDTT	10.10.16.185	
SESMNGR	10.10.16.44	
SM1	10.10.16.43	
SM61	10.10.16.201	
default	0.0.0.0	
devconaes61	10.10.16.30	

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link as shown below. Specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

add cti-link 1		Page 1 of 3
CTI LINK		
CTI Link: 1		
Extension: 1111		
Type: ADJ-IP		
Name: devconaes61		COR: 1

Configure IP-Services for the AESVCS service using the **change ip-services** command. Using the C-LAN node name as noted above i.e. **CLAN**

change ip-services					Page	1 of	4
IP SERVICES							
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		
CDR1		CLAN	0	IPbuffer	9000		
CDR2		CLAN	0	RDTT	9001		
AESVCS	y	CLAN	8765				

Navigate to **Page 4**, set the **AE Services Server** node-name and the **Password** the AES Server will use to authenticate with Communication Manager.

change ip-services					Page	4 of	4
AE Services Administration							
Server ID	AE Services Server	Password	Enabled	Status			
1:	devconaes61	Avayapassword1	y	in use			

6. Configuration of Avaya Aura® Application Enablement Services

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

- Create Switch Connection
- Create CTI User
- Enable CTI User
- Configure DMCC Port
- Enable Security Database

6.1. Create Switch Connection

Access the OAM web-based interface of the Application Enablement Services Server, in this instance using the URL <https://10.10.16.30>. The Management console is displayed. Log in using the appropriate credentials.

The screenshot shows the Avaya Application Enablement Services Management Console login page. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. A red horizontal bar spans the width of the page, with a "Help" link on the right. In the center, there is a login box with the text "Please login here:" followed by "Username" and "Password" labels, each with an adjacent input field. Below these fields is a "Login" button. At the bottom of the page, a red horizontal bar contains the copyright notice: "© Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

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

The screenshot shows the Avaya Application Enablement Services Management Console "Welcome to OAM" screen. At the top left is the Avaya logo. To its right, the text "Application Enablement Services" and "Management Console" is displayed. In the top right corner, a welcome message is shown: "Welcome: User craft", "Last login: Tue May 24 15:45:54 2011 from 10.10.16.62", "HostName/IP: devconaes61/10.10.16.30", "Server Offer Type: TURNKEY", and "SW Version: r6-1-0-20-0". A red horizontal bar spans the width of the page, with "Home" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with the following items: "AE Services", "Communication Manager Interface", "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area is titled "Welcome to OAM" and contains the following text: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:" followed by a bulleted list of domains and their uses. At the bottom of the page, a red horizontal bar contains the copyright notice: "Copyright © 2009-2010 Avaya Inc. All Rights Reserved."

Welcome to OAM

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

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

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

To establish the connection between Communication Manager and the Application Enablement Services Server, click **Communication Manager Interface** → **Switch Connections**. In the field next to next to **Add Connection**, enter **CM** and click on **Add Connection** (not shown), the following screen will be displayed. Complete the configuration as shown and enter the password specified in **Section 5.3** when configuring AESVCS in ip-services. In this instance **Avayapassword1**, click **Apply** when done.

AVAYA **Application Enablement Services** Management Console

Welcome: User craft
Last login: Tue Jun 7 16:03:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Connection Details - CM

Switch Password
Confirm Switch Password

Msg Period Minutes (1 - 72)
SSL ☒
Processor Ethernet ☐

Apply **Cancel**

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

The following screen will be displayed. Click on **Edit PE/CLAN IPs** in order to specify the IP address of the C-CLAN, as noted in **Section 5.3**

AVAYA **Application Enablement Services** Management Console

Welcome: User craft
Last login: Tue Jun 7 16:03:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURNKEY
SW Version: r6-1-0-20-0

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Switch Connections

Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
CM	No	30	1

Edit Connection **Edit PE/CLAN IPs** **Edit H.323 Gatekeeper** **Delete Connection** **Survivability Hierarchy**

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

Next to the **Add Name or IP** button, enter the IP address of the C-LAN and click on **Add Name or IP**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Tue Jun 7 16:03:19 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURKEY
SW Version: r6-1-0-20-0

Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit CLAN IPs - CM


Add Name or IP

Name or IP Address	Status
10.10.16.31	In Use

Delete IP
Back

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

Select **AE Services** on the left pane and verify that the **DMCC Service** is licensed by ensuring that **DMCC Service** is in the list of services and that the **License Mode** is showing **NORMAL MODE**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Fri Jun 3 13:34:08 2011 from 10.10.16.62
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURKEY
SW Version: r6-1-0-20-0

AE Services
Home | Help | Logout

AE Services
CVLAN
DLG
DMCC
SMS
TSAPI
TWS
Communication Manager Interface
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

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	OFFLINE	Running	N/A	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.

License Information
You are licensed to run Application Enablement (CTI) version 6.0

Copyright © 2009-2010 Avaya Inc. All Rights Reserved.

6.2. Create CTI User

A user ID and password needs to be configured for ECSTA to communicate as a DMCC client with Application Enablement Services. Select **User Management** → **User Admin** → **Add User** from the left pane, to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown below).

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for 'User craft' with login details. A red navigation bar contains 'User Management | User Admin | Add User' and links for 'Home | Help | Logout'. The left sidebar lists various system components, with 'User Management' expanded to show 'User Admin' and 'Add User' selected. The main content area is titled 'Add User' and contains a form with the following fields: 'User Id' (text), 'Common Name' (text), 'Surname' (text), 'User Password' (password), 'Confirm Password' (password), 'Admin Note' (text), 'Avaya Role' (dropdown menu), 'Business Category' (text), 'Car License' (text), 'CM Home' (text), 'Css Home' (text), 'CT User' (dropdown menu), and 'Department Number' (text). A red box highlights the 'User Id', 'Common Name', 'Surname', 'User Password', and 'Confirm Password' fields, with a note stating 'Fields marked with * can not be empty.' Another red box highlights the 'CT User' dropdown menu, which is set to 'Yes'.

6.3. Enable CTI User

Navigate to the users screen by selecting **Security → Security Database → CTI Users → List All Users**. In the **CTI Users** window, select the user that was set up in **Section 6.2** and select the **Edit** option.

AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Wed Nov 9 17:59:57 2011 from 10.255.255.120
HostName/IP: devconaes61/10.10.16.30
Server Offer Type: TURKEY
SW Version: r6-1-0-20-0

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

- AE Services
 - Communication Manager Interface
 - Licensing
 - Maintenance
 - Networking
 - Security**
 - Account Management
 - Audit
 - Certificate Management
 - Enterprise Directory
 - Host AA
 - PAM
 - Security Database**
 - Control
 - CTI Users**
 - List All Users
 - Search Users
 - Devices
 - Device Groups

CTI Users

User ID	Common Name	Worktop Name	Device ID
<input type="radio"/> ciboodle	ciboodle	NONE	NONE
<input checked="" type="radio"/> estosAES	estosAES	NONE	NONE
<input type="radio"/> John	John	NONE	NONE
<input type="radio"/> pcS	pcS	NONE	NONE
<input type="radio"/> pcShd	pcShd	NONE	NONE
<input type="radio"/> presence	presence	NONE	NONE
<input type="radio"/> redboxAES	redboxAES	NONE	NONE
<input type="radio"/> scantalk	Scantalk	NONE	NONE
<input type="radio"/> smartloggerAES	smartloggerAES	NONE	NONE
<input type="radio"/> synAES	synAES	NONE	NONE

Edit **List All**

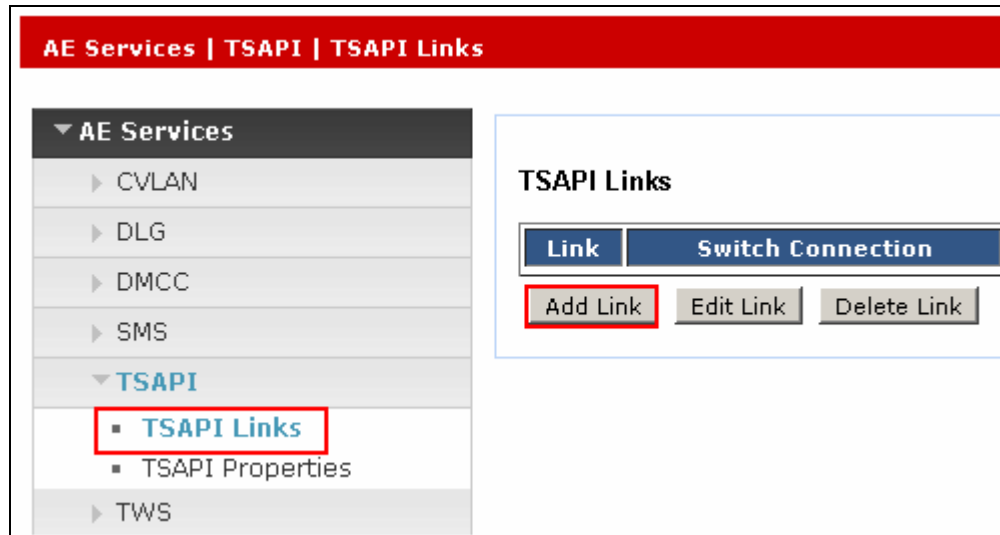
The **Edit CTI User** screen appears. Tick the **Unrestricted Access** box and **Apply Changes** at the bottom of the screen.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for 'User craft' with login details. A red navigation bar contains links for 'Security', 'Security Database', 'CTI Users', and 'List All Users', along with 'Home', 'Help', and 'Logout' links. A left sidebar lists various services, with 'Security' expanded to show 'CTI Users' and 'List All Users'. The main content area is titled 'Edit CTI User' and contains a form for user configuration. The 'User Profile' section includes fields for 'User ID', 'Common Name', 'Worktop Name', and a checked 'Unrestricted Access' checkbox. Below this, the 'Call and Device Control' section has a 'Call Origination/Termination and Device Status' dropdown set to 'None'. The 'Call and Device Monitoring' section includes 'Device Monitoring', 'Calls On A Device Monitoring', and 'Call Monitoring' dropdowns, all set to 'None'. The 'Routing Control' section has an 'Allow Routing on Listed Devices' dropdown set to 'None'. At the bottom of the form, the 'Apply Changes' button is highlighted with a red box, next to a 'Cancel Changes' button.

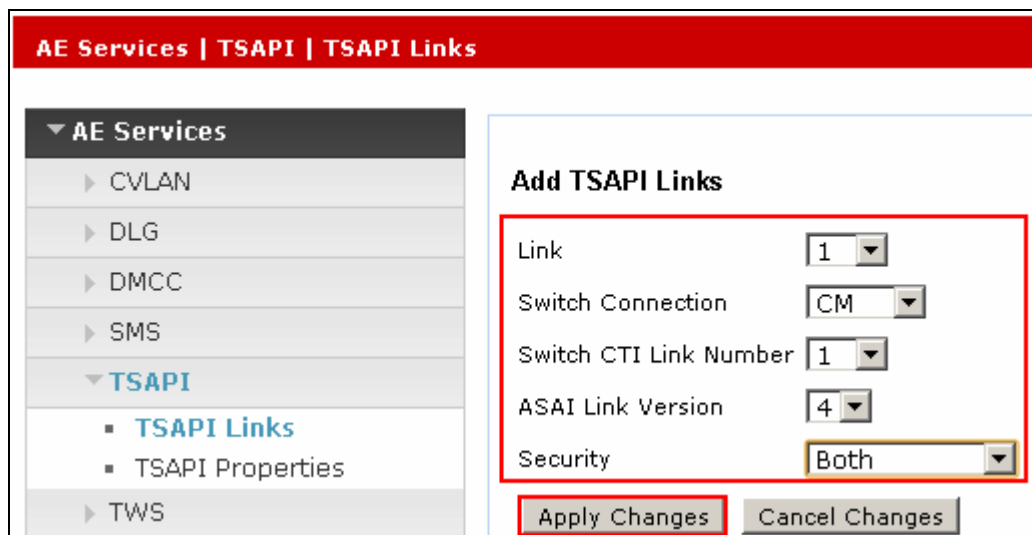
Edit CTI User		
User Profile:		
User ID	estosAES	
Common Name	estosAES	
Worktop Name	NONE	
Unrestricted Access	<input checked="" type="checkbox"/>	
<hr/>		
Call and Device Control:	Call Origination/Termination and Device Status	None
<hr/>		
Call and Device Monitoring:	Device Monitoring	None
	Calls On A Device Monitoring	None
	Call Monitoring	<input type="checkbox"/>
<hr/>		
Routing Control:	Allow Routing on Listed Devices	None
<hr/>		
Apply Changes Cancel Changes		

6.4. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, click **Add Link**.



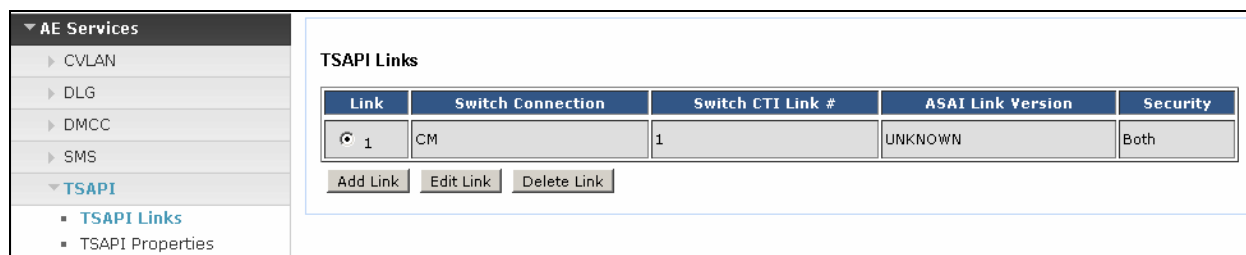
Configure the TSAPI Link using the newly configured **Switch Connection** as shown below and click **Apply Changes**.



The screen below will be displayed with instructions to restart the TSAPI Server. Click **Apply** taking note of the instructions given.



The screen below will appear displaying the newly added TSAPI link.



6.5. Restart TSAPI Service


Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service** box, and click **Restart Service**.



6.6. Configure DMCC Port

On the AES Management Console navigate to **Networking** → **Ports** to set the DMCC server port. During the compliance test, the **Unencrypted Port** set to **4721** was **Enabled** as shown in

the screen below. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



Application Enablement Services
 Management Console

Welcome: User craft
 Last login: Fri Jun 3 13:34:08 2011 from 10.10.16.62
 HostName/IP: devconaes61/10.10.16.30
 Server Offer Type: TURNKEY
 SW Version: r6-1-0-20-0

Networking | Ports
Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▼ Networking
- AE Service IP (Local IP)
- Network Configure
- Ports
- TCP Settings
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Ports

CVLAN Ports			Enabled Disabled
Unencrypted TCP Port	9999		<input checked="" type="radio"/> <input type="radio"/>
Encrypted TCP Port	<input type="text" value="9998"/>		<input checked="" type="radio"/> <input type="radio"/>
<hr/>			
DLG Port	TCP Port	5678	
<hr/>			
TSAPI Ports			Enabled Disabled
TSAPI Service Port	450		<input checked="" type="radio"/> <input type="radio"/>
<hr/>			
Local TLINK Ports			
TCP Port Min	1024		
TCP Port Max	1039		
<hr/>			
Unencrypted TLINK Ports			
TCP Port Min	<input type="text" value="1050"/>		
TCP Port Max	<input type="text" value="1065"/>		
<hr/>			
Encrypted TLINK Ports			
TCP Port Min	<input type="text" value="1066"/>		
TCP Port Max	<input type="text" value="1081"/>		
<hr/>			
DMCC Server Ports			Enabled Disabled
Unencrypted Port	<input type="text" value="4721"/>		<input checked="" type="radio"/> <input type="radio"/>
Encrypted Port	<input type="text" value="4722"/>		<input checked="" type="radio"/> <input type="radio"/>
TR/87 Port	<input type="text" value="4723"/>		<input type="radio"/> <input checked="" type="radio"/>
<hr/>			
H.323 Ports			
TCP Port Min	<input type="text" value="20000"/>		
TCP Port Max	<input type="text" value="23999"/>		
Local UDP Port Min	<input type="text" value="30000"/>		
Local UDP Port Max	<input type="text" value="33999"/>		
<hr/>			
Server Media			Enabled Disabled
RTP Local UDP Port Min*	<input type="text" value="40000"/>		<input checked="" type="radio"/> <input type="radio"/>
RTP Local UDP Port Max*	<input type="text" value="47999"/>		

* Note: The number of RTP ports needs to be double the number of extensions using server media.

6.7. Enable Security Database

Select **Security** → **Security Database** → **Control** from the left pane, to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen in the right pane. Uncheck **Enable SDB for DMCC Service** and click **Apply Changes**.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with login details. A red navigation bar contains "Security | Security Database | Control" and links for "Home | Help | Logout". The left sidebar lists various services, with "Security" expanded to show "Security Database" and "Control" selected. The main content area, titled "SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services", contains two unchecked checkboxes: "Enable SDB for DMCC Service" and "Enable SDB for TSAPI Service, JTAPI and Telephony Web Services". An "Apply Changes" button is located at the bottom of this section.

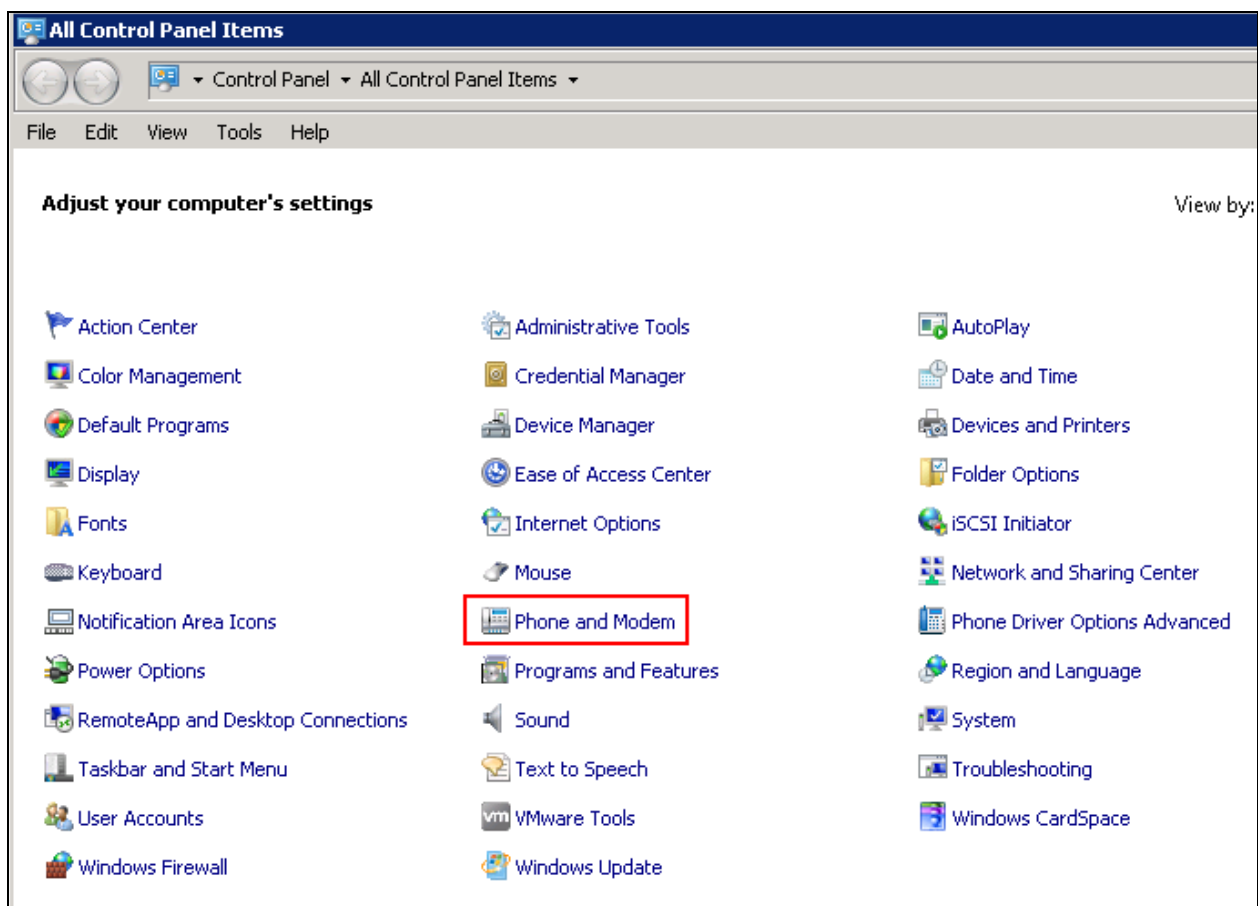
7. Configure ESTOS ECSTA

ESTOS ECSTA is installed using a Microsoft Installer package. These Application Notes assume installation of ECSTA has been completed, the subsequent configuration of ECSTA can be summarized as follows:

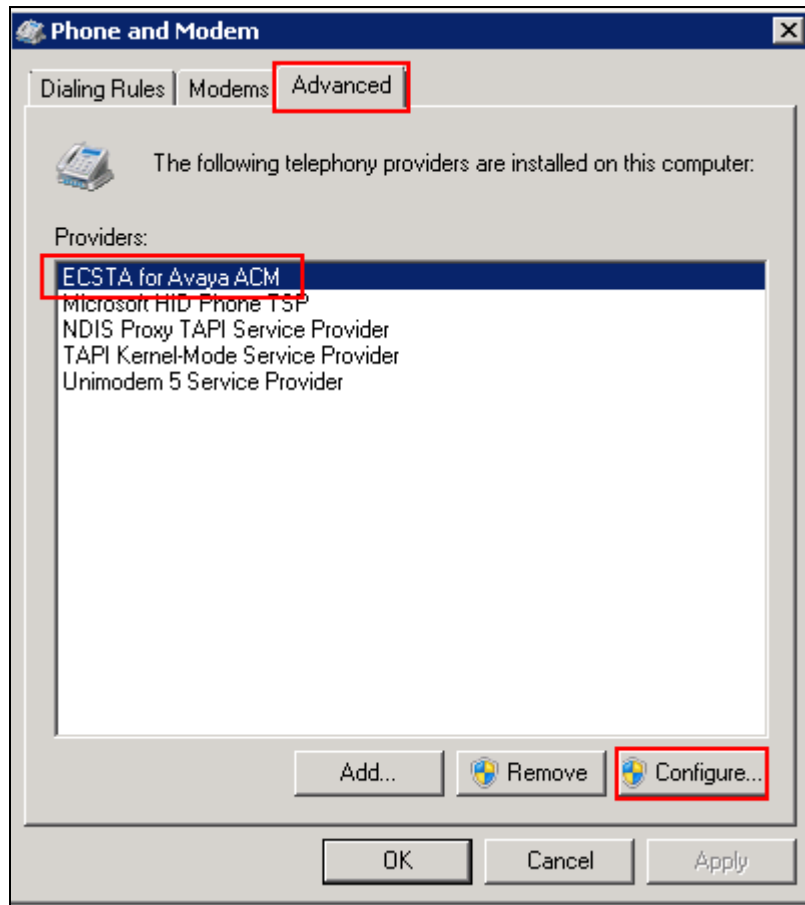
- Configure CTI Parameters
- Configure Extensions to be Controlled

7.1. Configure CTI Parameters

In order to establish connectivity to the AES, ECSTA must be configured with the appropriate settings. On the PC hosting the ECSTA client, access the Windows Control Panel and double click on **Phone and Modem**.



Click the **Advanced** tab, select **ECSTA for Avaya ACM** and click **Configure**.



The ECSTA configuration screen will appear, in the **AES Connection** section configure the **Hostname or IP – Port** with the AES IP Address and the DMCC port configured in **Section 6.6**. Click the radio button next to **TCP Connection (not encrypted)**. In the **Login** section specify the **CTI User** and **Password** configured in **Section 6.2**, in the **Communication Manager Name** field enter the name of the switch connection created in **Section 6.1**.

ECSTA for Avaya ACM

Connection | Lines | Location | Advanced | Licenses | Info

AES Connection

Host Name or IP - Port: 10.10.16.30 4721

☒ TCP Connection (not encrypted)
☐ TLS Connection (encrypted)

Login

User: estosAES
Password: *****
Communication Manager Name: CM

Comments for this connection:

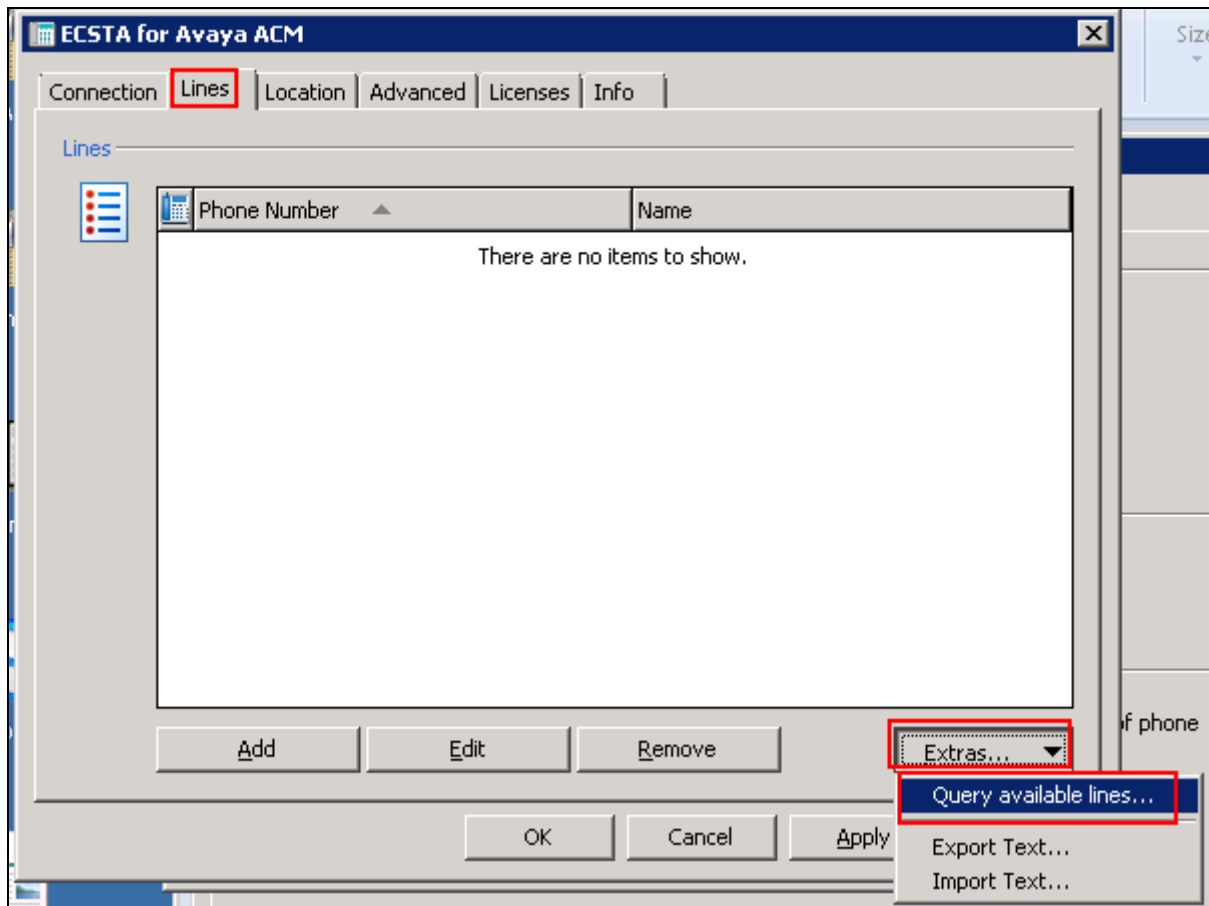
OK Cancel Apply Help

Click on the **Locations** tab, in the **First Extension (Phone Number)** and **Last Extension (Phone Number)** fields enter the first and last extension numbers for the range of extensions to be controlled.

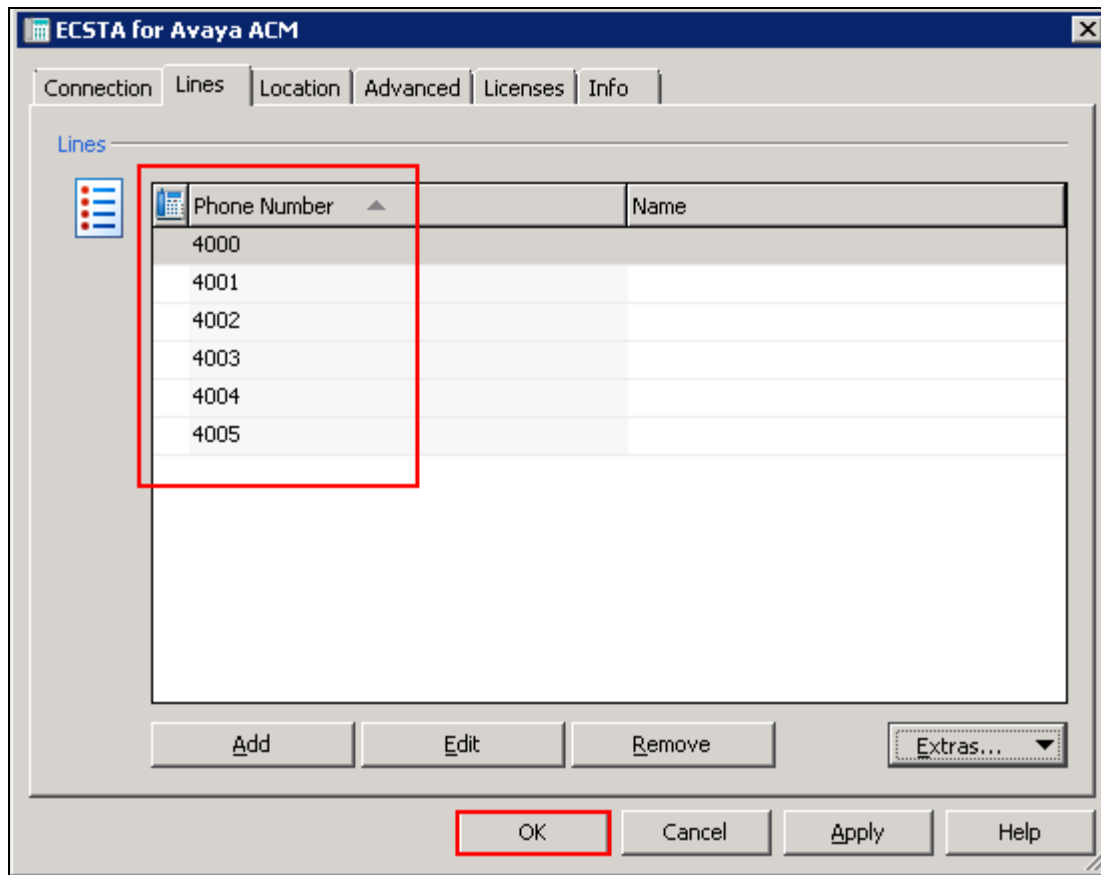
The screenshot shows the 'ECSTA for Avaya ACM' dialog box with the 'Location' tab selected. The 'Location' section includes a globe icon with a red arrow, a 'Use Location' checkbox, and three input fields for 'Country Code' (1 for USA), 'Area Code' (212 NY City), and 'Local Office Code' (1234 for Company). The 'Phone Number Range' section has two input fields: 'First Extension (Phone Number)' with the value '4000' and 'Last Extension (Phone Number)' with the value '4005'. The 'Phone Number Format' section includes an 'Edit Format...' button and a note: 'You may apply rules for formatting of phone numbers.' The dialog box has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

Location		
<input type="checkbox"/> Use Location		
Country Code	<input type="text" value="1"/>	1 for USA
Area Code	<input type="text" value="212"/>	212 NY City
Local Office Code	<input type="text" value="1234"/>	1234 for Company
Phone Number Range		
First Extension (Phone Number)	<input type="text" value="4000"/>	e.g. 10
Last Extension (Phone Number)	<input type="text" value="4005"/>	e.g. 350
Phone Number Format		
<input type="button" value="Edit Format..."/>	You may apply rules for formatting of phone numbers.	

Click the **Lines** tab and click **Extras**, from the menu which appears, click **Query Available Lines**. This will interrogate Communication Manager for all extensions available in the range defined in the Location tab.



The following screen will be displayed showing the extensions available from Communication Manager. Click on **OK** when done.

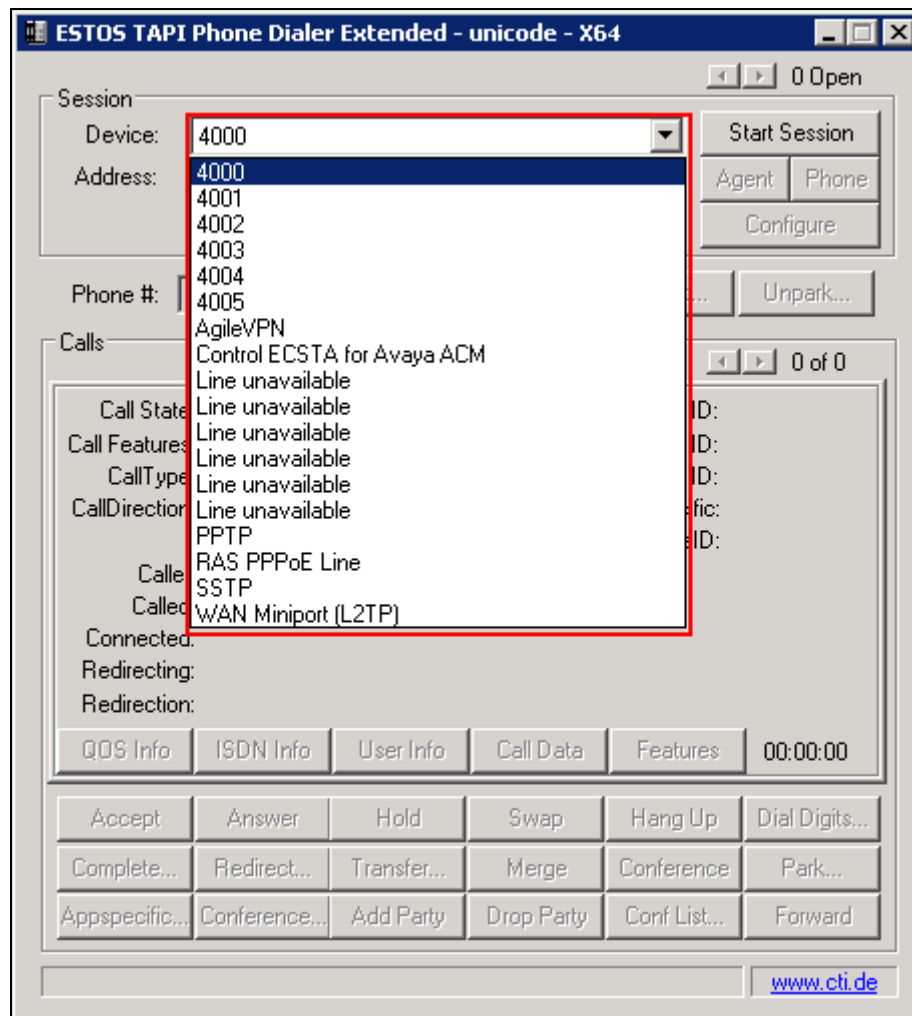


8. Configure ESTOS Ephone Test Tool

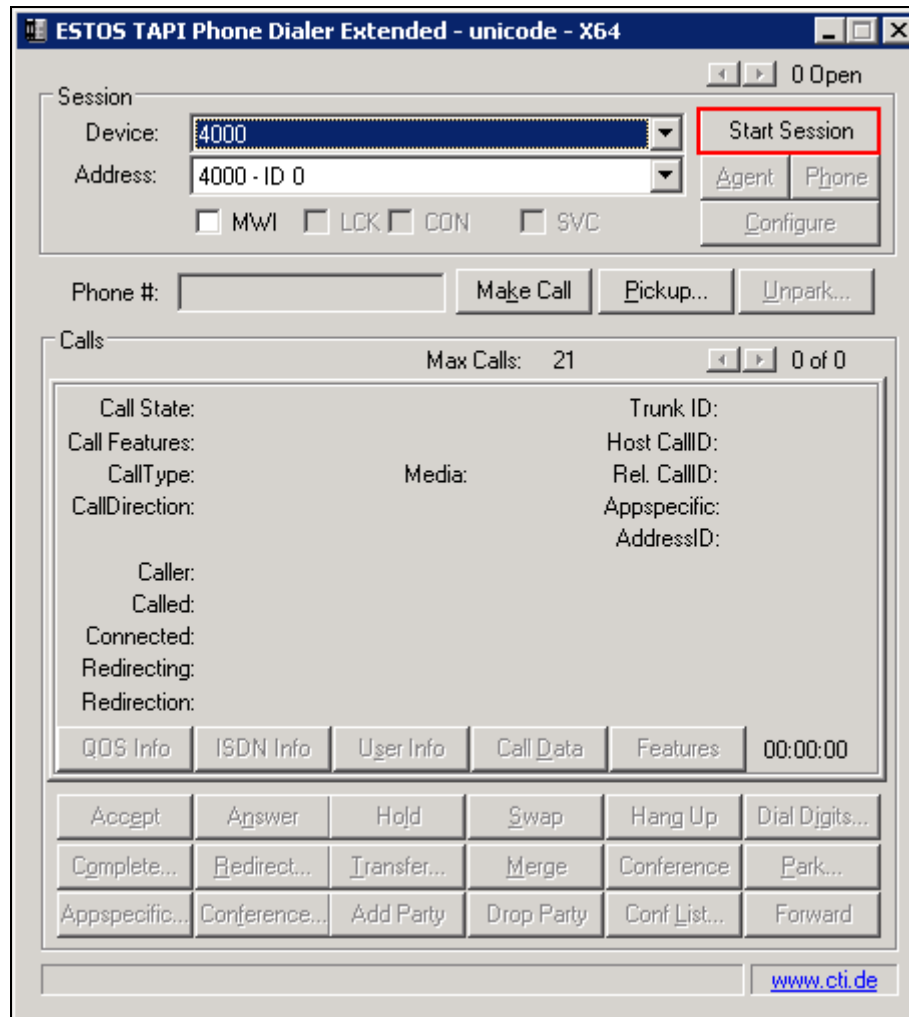
ESTOS Ephone is a test tool provided by ESTOS for the purposes of demonstrating the abilities of ESTOS ECSTA only, and is not a product available for purchase. The Ephone test tool used to verify connectivity and call control to Communication Manager using CTI provided by AES through the ECSTA connection. Double click on the EPhoneX64 icon on the desktop.



The application will load. Select the extension to be controlled from the drop down list.



Click on **Start Session** in order to begin control of the selected extension.



The screen shown below will be displayed. Note that it is now possible to enter a number in the **Phone #** field.

ESTOS TAPI Phone Dialer Extended - unicode - X64

Session 1 of 1

Device: 4000

Address: 4000 - ID 0

☐ MWI ☐ LCK ☒ CON ☒ SVC

End Session

Agent Phone

Configure

Phone #:

Make Call Pickup... Unpark...

Calls Max Calls: 21 0 of 0

Call State: Trunk ID:

Call Features: Host CallID:

CallType: Media: Rel. CallID:

CallDirection: Appspecific:

AddressID:

Caller:

Called:

Connected:

Redirecting:

Redirection:

QOS Info ISDN Info User Info Call Data Features 00:00:00

Accept Answer Hold Swap Hang Up Dial Digits...

Complete... Redirect... Transfer... Merge Conference Park...

Appspecific... Conference... Add Party Drop Party Conf List... Forward

www.cti.de

9. Verification Steps

This section provides tests that can be performed to verify correct configuration of the Avaya and ESTOS solution.

9.1. Verify Avaya Aura® Communication Manager CTI Service State

The following steps can ensure that the communication between Communication Manager and the Application Enablement Services server is functioning correctly. Check the AESVCS link status with Application Enablement Services by using the command **status aesvcs cti-link**. The CTI link is 1. Verify the **Service State** of the CTI link is **established**.

status aesvcs cti-link						
AE SERVICES CTI LINK STATUS						
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd
1	4	no	devconaes61	established	18	18

9.2. Verify Avaya Aura® Application Enablement Services DMCC Service

The following steps are carried out on the Application Enablement Services to ensure that the communication link between ECSTA and the Application Enablement Services server is functioning correctly. Verify the status of the DMCC service by selecting **Status → Status and Control → DMCC Service Summary**. The **DMCC Service Summary – Session Summary** screen is displayed as shown below. It shows a connection to the ESTOS client, IP address **10.10.16.59**. The **Application** is set to **Avaya DMCC Source** and the **Far-end Identifier** is given as the IP address **10.10.16.59** as expected.

The screenshot shows the Avaya Application Enablement Services Management Console. The left sidebar contains a navigation menu with options like AE Services, Communication Manager, Interface, Licensing, Maintenance, Networking, Security, and Status. The main content area displays the 'DMCC Service Summary - Session Summary' page. It includes a session summary table with columns for Session ID, User, Application, Far-end Identifier, Connection Type, and # of Associated Devices. The table shows one session with Session ID 781AE5AEE18FBF538 F82DDC06F486333-7, User estosAES, Application ECSTA for Avaya ACM, Far-end Identifier 10.10.16.59, Connection Type XML Unencrypted, and 0 associated devices. There are also buttons for 'Terminate Sessions' and 'Show Terminated Sessions'.

Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
781AE5AEE18FBF538 F82DDC06F486333-7	estosAES	ECSTA for Avaya ACM	10.10.16.59	XML Unencrypted	0

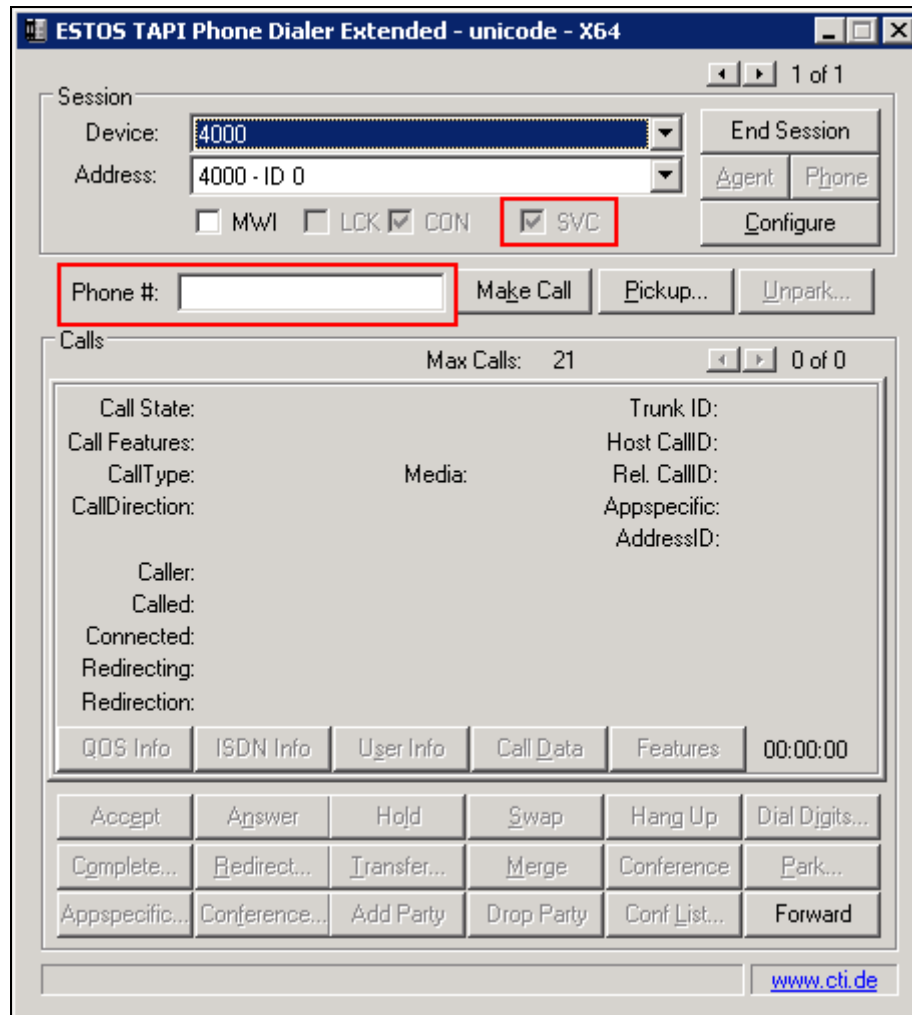
9.3. Verify Connection of ESTOS ECSTA to Avaya Aura® Application Enablement Services

Navigate to the ESTOS log files contained in **c:\ecstaACM** and open **general5_0.txt**. Verify connectivity with the AES (**10.10.16.30**) on port **4721** by the Ephone test tool controlling extension **4000** via ECSTA, as shown in the log extract below. **LineOpen** confirms successful connection.

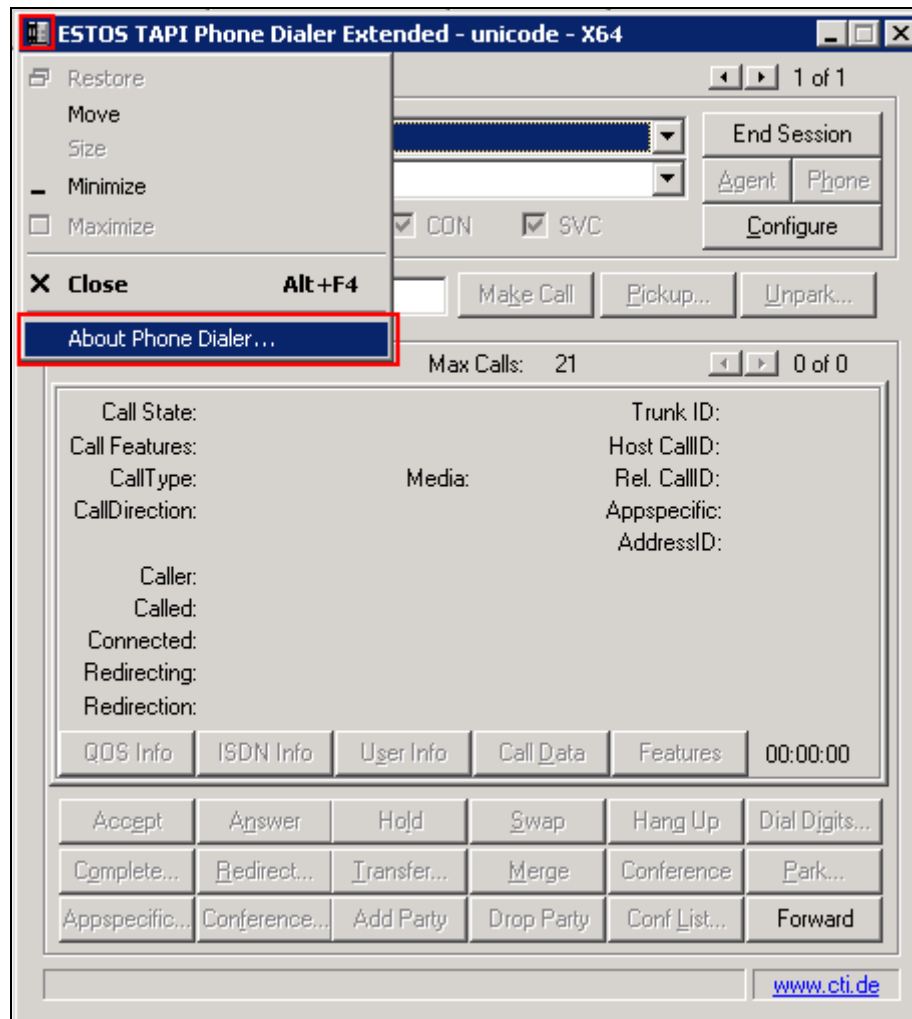
```
09.11.2011 18:40:09:023;32;4000;TSPI_lineOpen begin
09.11.2011 18:40:09:023;32;4000;TSPI_lineOpen success
09.11.2011 18:40:09:023;32;TSPI_lineSetDefaultMediaDetection;4000 MediaModes 00000004
09.11.2011 18:40:09:023;32;ETspBase::ConnectionWatchFunction;PBX Connect is required
09.11.2011 18:40:09:023;32;ETspBase::Connect;ETspBase::Connect TCP: Host 10.10.16.30,
Port 4721
09.11.2011 18:40:09:055;32;ETspBase::ConnectionWatchFunction;Connect result: 00000000
09.11.2011 18:40:09:242;32;4000;LineOpen 00000000
```

9.4. Verify Connectivity of ESTOS Ephone test tool to the Avaya Solution

Select the extension to be controlled from the drop down list and click **Start Session**. Verify that the EPhone test tool is connected with the presence of a tick in the **SVC** box and the availability of the **Phone #** field, highlighted in the screen shot below



Click on the top left corner of the Ephone test tool and select **About Phone Dialer** from the menu that appears.



Verify the version is as expected.



10. Conclusion

These Application Notes describe the configuration steps required for ESTOS ECSTA to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services. All functionality and serviceability test cases were completed successfully.

11. Additional References

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

[1] Avaya Aura® Application Enablement Services Administration and Maintenance Guide – Release 6.1, Issue 2, February 2011

[2] Administering Avaya Aura® Communication Manager – Release 6.0, Issue 6.0, June 2010

Product documentation for ESTOS products can be found at <http://www.estos.de>

©2013 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.