



Avaya Application Enablement Services Configuration

10/29/2012

Americas Headquarters

OAISYS

7965 S. Priest Drive, Suite 105

Tempe, AZ 85284

USA

www.oaisys.com

(480) 496-9040



AVAYA APPLICATION ENABLEMENT SERVICES CONFIGURATION

ABOUT THIS GUIDE

This manual, *Avaya Application Enablement Services Configuration* explains how to set up devices and users for monitoring with the OAISYS recording solution. It enables people, teams, and organizations to capture greater insight into their phone-based interactions, providing more efficient management of their overall business operations.

INTENDED AUDIENCE

The information provided in this manual is written for experienced technical support representatives and IT/Networking administrators who install and configure the Avaya Application Enablement Services (AES) Security Database. Users should be familiar with Avaya terminology and programming procedures.

CONFIGURATION PROCEDURE

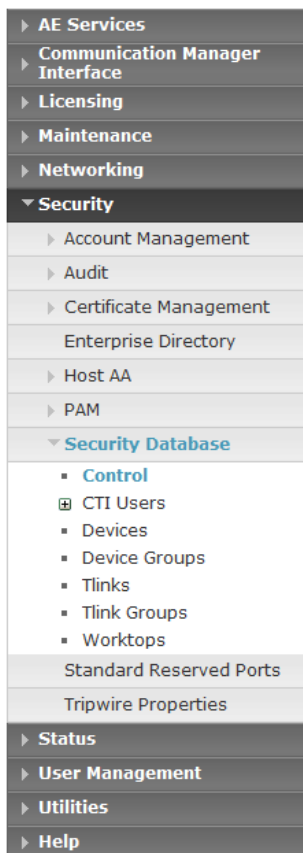
Use the information provided in the subsequent pages to configure the security database with AES.

1. Log on to the AES Operations Administration and Maintenance (OAM) utility.
2. From AES OAM → CTI OAM Administration → Administration → Security → Security Database → SDB Control, verify the checkbox for “Enable SDB TSAPI Service, JTAPI and Telephony Service” is selected.



Application Enablement Services Management Console

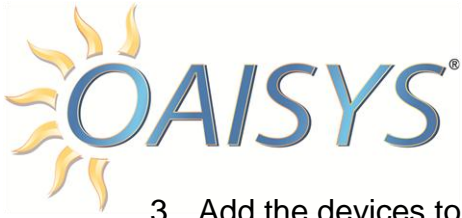
Security | Security Database | Control



SDB Control for DMCC and TSAPI

- Enable SDB for DMCC Service
- Enable SDB TSAPI Service, JTAPI and Telephony Service

Apply Changes



3. Add the devices to the security database for OAISYS to monitor.
 - a. From AES OAM → CTI Administration → Administration → Security → Security Database → Devices, verify the stations and ACD groups for OAISYS to monitor appear in the list.

If any stations or ACD groups are missing from the list, go to step 4.

If all stations and ACD groups appear, go to step 5.



Application Enablement Services Management Console

Security | Security Database | Devices

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
 - ▶ Account Management
 - ▶ Audit
 - ▶ Certificate Management
 - Enterprise Directory
 - ▶ Host AA
 - ▶ PAM
 - ▼ Security Database
 - Control
 - ▣ CTI Users
 - **Devices**
 - Device Groups
 - Tlinks
 - Tlink Groups
 - Worktops
 - Standard Reserved Ports
 - Tripwire Properties
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Devices

20004

Device ID	Tlink Group	Device
<input checked="" type="radio"/> 20001	Any	PHONE
<input type="radio"/> 20002	Any	PHONE
<input type="radio"/> 20003	Any	PHONE
<input type="radio"/> 22001	Any	ACD

NOTE: This does not affect the Communication Manager's database.



4. To add a station or ACD group to the list, enter the Device ID or extension number → select the appropriate “Device Type” from the drop list → select ‘Any’ for the T-Link group → click on “Apply Changes”
 - a. The other fields revert to default values, and can be left alone unless you want to specify a location.
 - b. Repeat these steps for additional devices.

NOTE: Account Code is not supported via AES (TSAPI)



Application Enablement Services Management Console

Security | Security Database | Devices

▶ AE Services
▶ Communication Manager Interface
▶ Licensing
▶ Maintenance
▶ Networking
▼ Security
▶ Account Management
▶ Audit
▶ Certificate Management
Enterprise Directory
▶ Host AA
▶ PAM
▼ Security Database
▪ Control
▣ CTI Users
▪ Devices
▪ Device Groups
▪ Tlinks
▪ Tlink Groups
▪ Worktops
Standard Reserved Ports

Add Device

Device ID	<input type="text" value="20004"/>
Location	<input type="text"/>
Device Type	<input type="text" value="PHONE"/>
Tlink Group	<input type="text" value="Any"/>
<input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/>	



5. Add a device group containing all the devices (stations and ACD groups) for OAISYS to monitor.
 - a. From AES OAM → CTI OAM Administration → Administration → Security → Security Database → Device Groups → enter “OAISYS Devices” in the text box → click the ‘Add Device Group’ button.



Application Enablement Services Management Console

Security | Security Database | Device Groups

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
 - ▶ Account Management
 - ▶ Audit
 - ▶ Certificate Management
 - ▶ Enterprise Directory
 - ▶ Host AA
 - ▶ PAM
 - ▼ Security Database
 - Control
 - ▣ CTI Users
 - Devices
 - **Device Groups**
 - Tlinks
 - Tlink Groups
 - Worktops
 - ▶ Standard Reserved Ports
 - ▶ Tripwire Properties
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Device Groups

OAISYS Devices

Device Group	
<input checked="" type="radio"/>	N



b. Select the devices you want OAISYS to monitor → click 'Apply Changes.'



Application Enablement Services Management Console

Security | Security Database | Device Groups

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
 - ▶ Account Management
 - ▶ Audit
 - ▶ Certificate Management
 - Enterprise Directory
 - ▶ Host AA
 - ▶ PAM
 - ▼ Security Database
 - Control
 - ▣ CTI Users
 - Devices
 - **Device Groups**
 - Tlinks
 - Tlink Groups
 - Worktops
 - Standard Reserved Ports
 - Tripwire Properties
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Edit Device Group

Device Group

Exception Group

Devices

20001

20002

20003

22001

NOTE: OAISYS will NOT be able to monitor any devices that are not selected.



6. Create a user for the TSAPI CTI service in OAISYS to log into the TSAPI service.
 - a. From AES OAM → User Management → User Admin → Add User
 - b. Verify the CT User field on the “Add User” page is set to ‘Yes.’



Application Enablement Services Management Console

User Management | User Admin | Add User

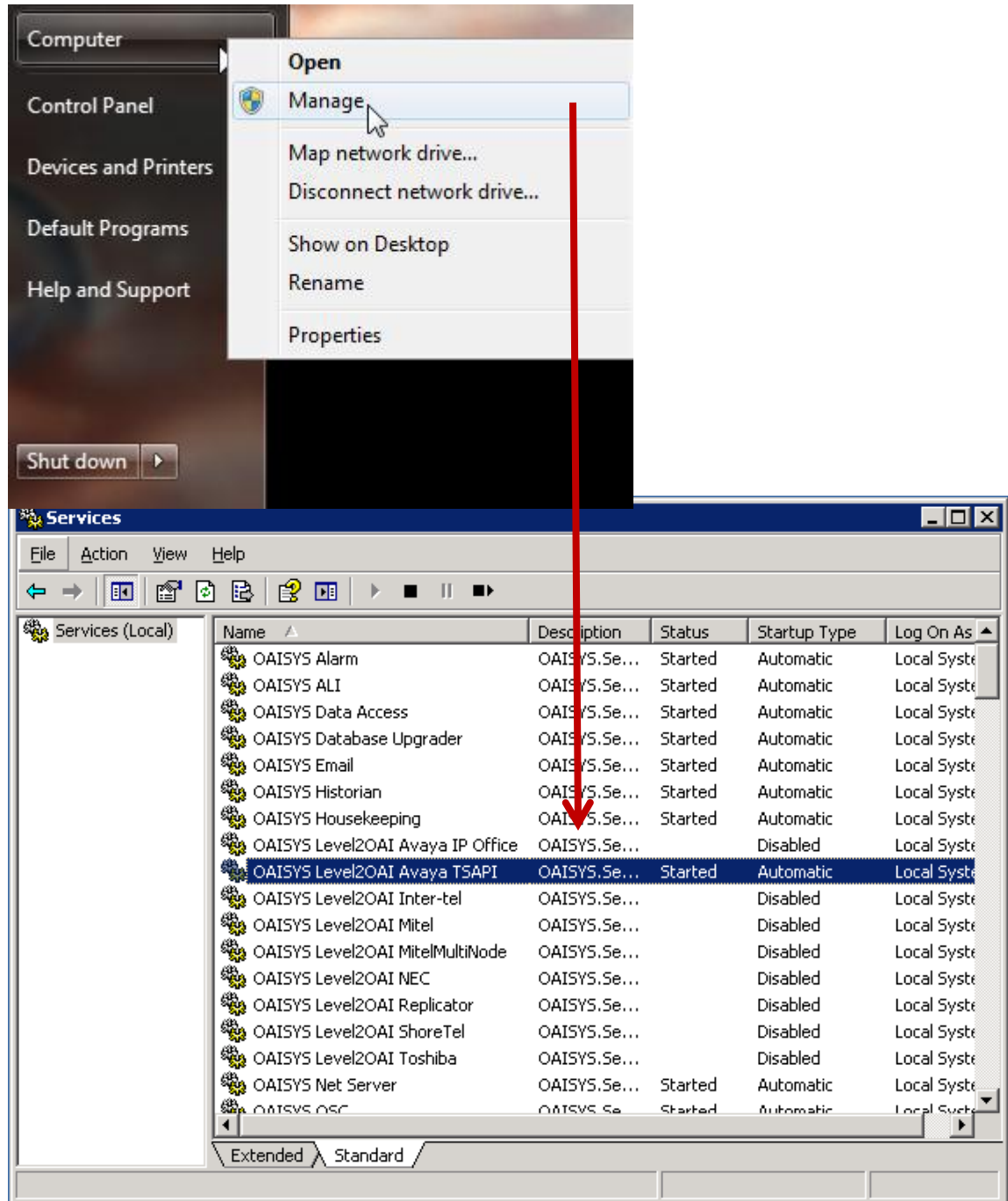
- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▼ User Management
 - ▶ Service Admin
 - ▼ User Admin
 - Add User
 - Change User Password
 - List All Users
 - Modify Default Users
 - Search Users
- ▶ Utilities
- ▶ Help

Add User

Fields marked with * can not be empty.

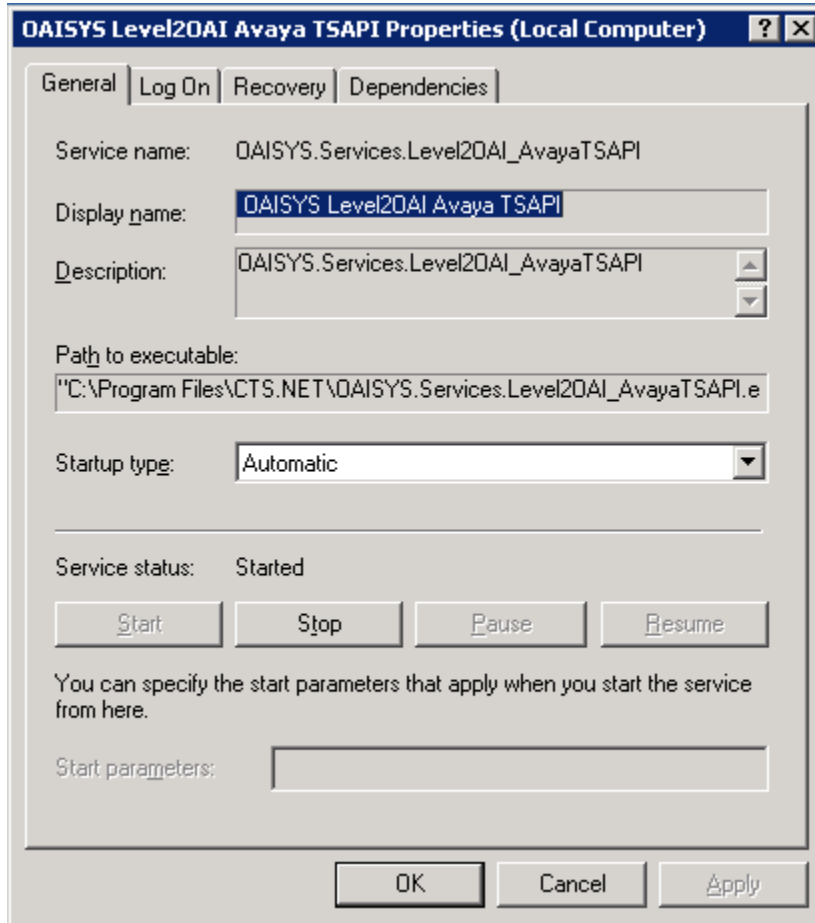
* User Id	<input type="text" value="oaisys"/>
* Common Name	<input type="text" value="oaisys"/>
* Surname	<input type="text" value="oaisys"/>
* User Password	<input type="password" value="••••••••"/>
* Confirm Password	<input type="password" value="••••••••"/>
Admin Note	<input type="text"/>
Avaya Role	<input type="text" value="None"/>
Business Category	<input type="text"/>
Car License	<input type="text"/>
CM Home	<input type="text"/>
Css Home	<input type="text"/>
CT User	<input type="text" value="Yes"/>
Department Number	<input type="text"/>
Display Name	<input type="text"/>
Employee Number	<input type="text"/>
Employee Type	<input type="text"/>
Enterprise Handle	<input type="text"/>
Given Name	<input type="text"/>
Home Phone	<input type="text"/>
Home Postal Address	<input type="text"/>
Initials	<input type="text"/>
Labeled URI	<input type="text"/>
Mail	<input type="text"/>
MM Home	<input type="text"/>
Mobile	<input type="text"/>
Organization	<input type="text"/>
Pager	<input type="text"/>
Preferred Language	<input type="text" value="English"/>
Room Number	<input type="text"/>
Telephone Number	<input type="text"/>

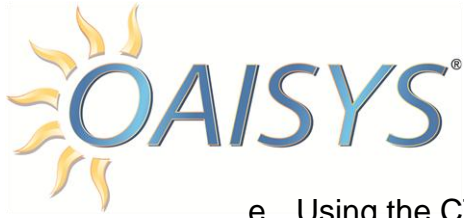
- c. Navigate to Services Manager → find the Level2 Avaya TSAPI service → right-click; select Properties



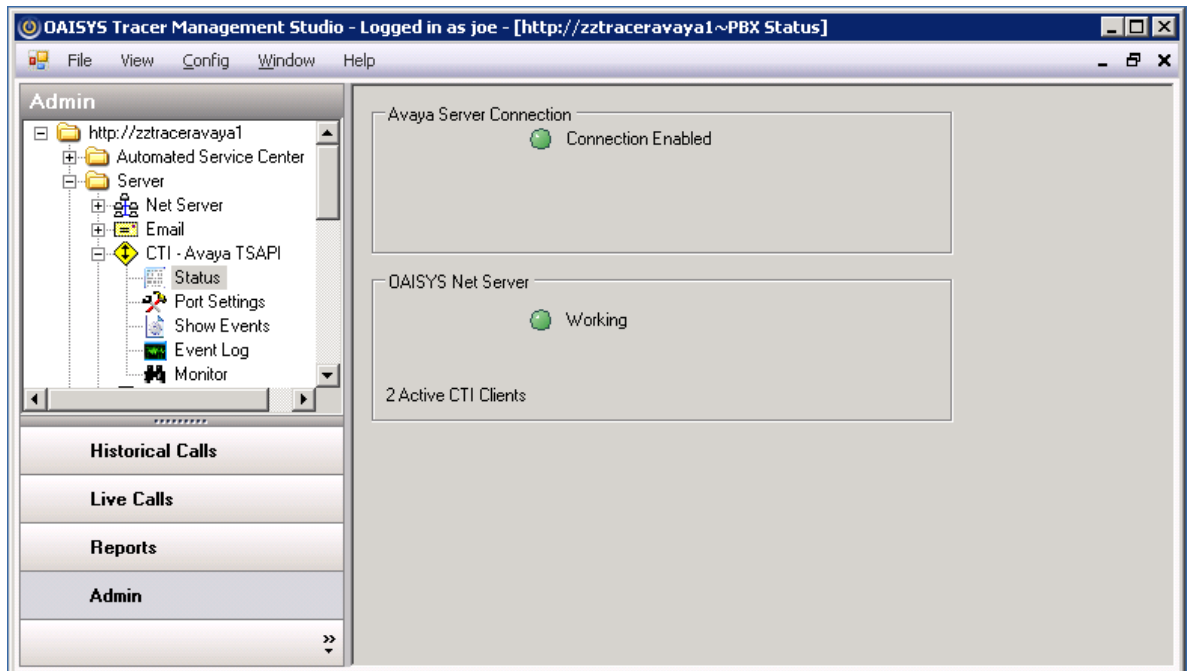
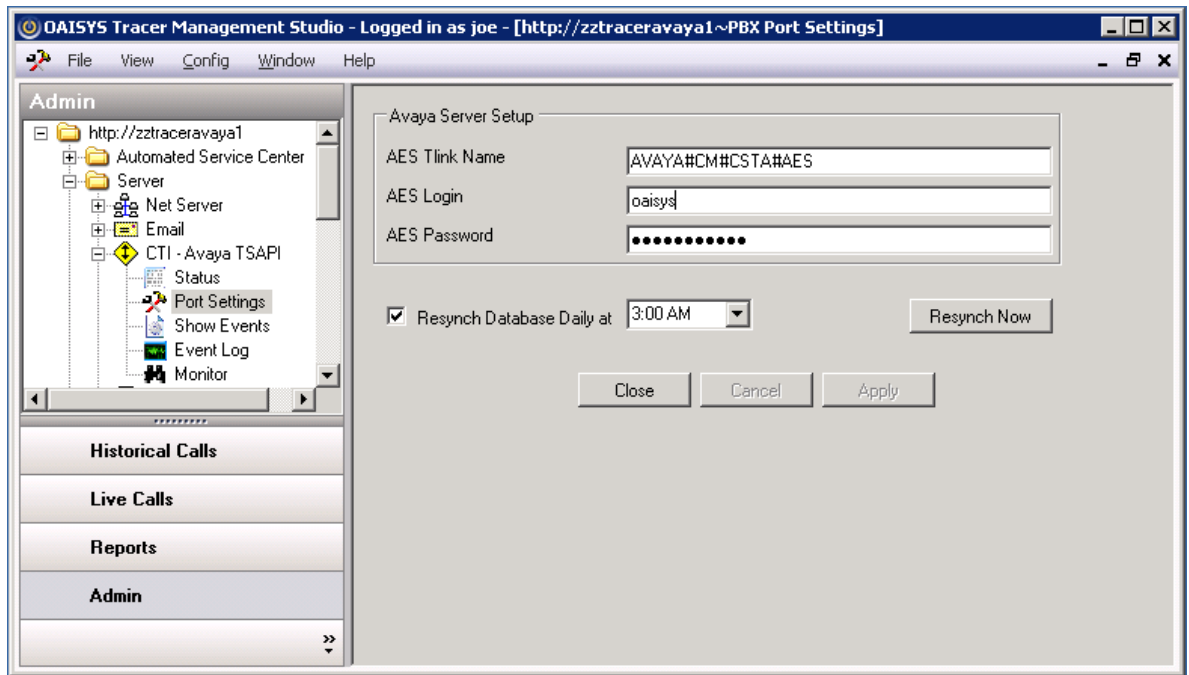


d. Change Startup tupe to “Automatic” Startup → press Start to begin running





- e. Using the CTI Service Port Settings form in OAISYS, enter the AES Login and AES Password.





7. Verify the user created in step 6 appears in the list.
 - a. From AES OAM → CTI OAM Administration → Administration → Security → Security Database → CTI Users → List All Users
 - b. If the user created is not in the list, go back to the Add User page to verify the CT User field is set to 'Yes.'



Application Enablement Services Management Console

Security | Security Database | CTI Users | List All Users

- ▶ 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
 - Tlinks
 - Tlink Groups
 - Worktops
 - Standard Reserved Ports
 - Tripwire Properties
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

CTI Users

User ID	Common Name	Worktop
<input checked="" type="radio"/> oaisys	oaisys	NONE



8. Assign the new device group to the OAISYS user.
 - a. From AES OAM → CTI OAM Administration → Administration → Security → Security Database → CTI Users → List All Users → select the OAISYS user → click on the 'Edit' button
 - i. The checkbox to the right of "Unrestricted Access" should not be selected. This means the user has restricted access.

NOTE: OAISYS can only monitor the devices put into the OAISYS Devices group.

- ii. Verify "Device" is set to the 'OAISYS Devices' group.
- iii. Verify "Call/Device" is set to 'OAISYS Devices.'
- iv. Verify "Call" checkbox is checked.
- v. All other fields revert to default values.



Application Enablement Services Management Console

Security | Security Database | CTI Users | List All Users

<ul style="list-style-type: none">▶ AE Services▶ Communication Manager Interface▶ Licensing▶ Maintenance▶ Networking▼ Security<ul style="list-style-type: none">▶ Account Management▶ Audit▶ Certificate ManagementEnterprise Directory▶ Host AA▶ PAM▼ Security Database<ul style="list-style-type: none">▪ Control▣ CTI Users<ul style="list-style-type: none">▪ List All Users▪ Search Users▪ Devices▪ Device Groups▪ Tlinks▪ Tlink Groups▪ Worktops	<h4>Edit CTI User</h4> <table><tr><td>User Profile:</td><td>User ID</td><td>oaisys</td></tr><tr><td></td><td>Common Name</td><td>oaisys</td></tr><tr><td></td><td>Worktop Name</td><td>NONE</td></tr><tr><td></td><td>Unrestricted Access</td><td><input type="checkbox"/></td></tr></table> <hr/> <table><tr><td>Call Origination and Termination / Device Status</td><td>OAISYS Devices</td></tr></table> <hr/> <table><tr><td>Call and Device Monitoring:</td><td>Device</td><td>OAISYS Devices</td></tr><tr><td></td><td>Call / Device</td><td>OAISYS Devices</td></tr><tr><td></td><td>Call</td><td><input checked="" type="checkbox"/></td></tr></table> <hr/> <table><tr><td>Routing Control:</td><td>Allow Routing on Listed Devices</td><td>None</td></tr></table> <p><input type="button" value="Apply Changes"/> <input type="button" value="Cancel Changes"/></p>	User Profile:	User ID	oaisys		Common Name	oaisys		Worktop Name	NONE		Unrestricted Access	<input type="checkbox"/>	Call Origination and Termination / Device Status	OAISYS Devices	Call and Device Monitoring:	Device	OAISYS Devices		Call / Device	OAISYS Devices		Call	<input checked="" type="checkbox"/>	Routing Control:	Allow Routing on Listed Devices	None
User Profile:	User ID	oaisys																									
	Common Name	oaisys																									
	Worktop Name	NONE																									
	Unrestricted Access	<input type="checkbox"/>																									
Call Origination and Termination / Device Status	OAISYS Devices																										
Call and Device Monitoring:	Device	OAISYS Devices																									
	Call / Device	OAISYS Devices																									
	Call	<input checked="" type="checkbox"/>																									
Routing Control:	Allow Routing on Listed Devices	None																									



9. Locate the name of the T-Link to use.

a. From AES OAM → CTI OAM Administration → Administration → Security → Security Database → TLinks

i. This will provide a list of available T-Links for use → enter this name on the CTI Service Port Settings form in OAISYS under “AES T-Link Name”.



Application Enablement Services Management Console

Security | Security Database | Tlinks

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▼ Security
 - ▶ Account Management
 - ▶ Audit
 - ▶ Certificate Management
 - Enterprise Directory
 - ▶ Host AA
 - ▶ PAM
 - ▼ Security Database
 - Control
 - CTI Users
 - Devices
 - Device Groups
 - **Tlinks**
 - Tlink Groups
 - Worktops
 - Standard Reserved Ports
 - Tripwire Properties
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Tlinks

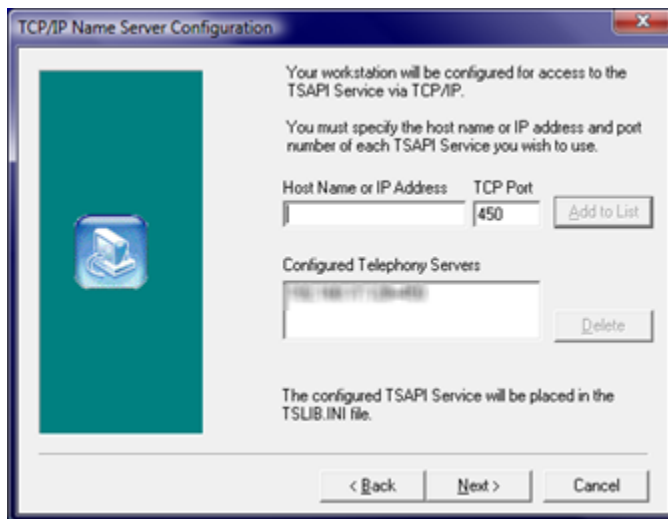
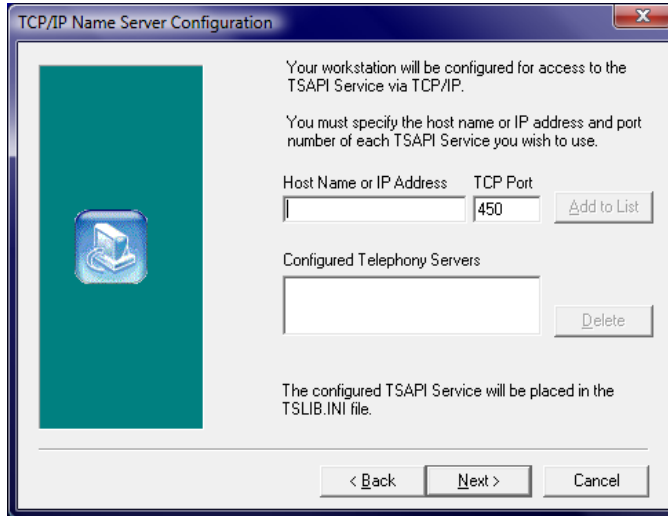
Tlink Name

AVAYA#CM#CSTA#AES



10. Run the TSAPI client on the OAISYS server.

- a. Enter the IP address of AVAYA AES Server → use default port 450 → select “Add to List”





11. After installing the TSAPI client on the OAISYS Server, edit the TSLIB.ini file so the TSAPI client knows where the AES Server is located.

- a. From All Programs → TSAPI Client → edit TSLIB.ini → add the IP address of the AES Server under 'Telephony Servers'

A screenshot of a Notepad window titled "TSLIB.INI - Notepad". The window contains the following text:

```
[Telephony Servers]
: This is a list of the servers offering Telephony Services via TCP/IP.
: Either domain name or IP address may be used; default port number is 450
: The form is: host_name=port_number For example:
: tserver.mydomain.com=450
:
[Config]
: When accessing Telephony Services via a secure, encrypted connection, the
: Application Enablement (AE) Services server sends its certificate to the
: TSAPI client, and the TSAPI client verifies that the certificate is signed
: by a trusted Certificate Authority (CA).
:
: If your organization has installed its own certificate on the AE Server,
: then the TSAPI client must have access to the trusted CA certificate(s)
: for the AE Services server certificate. Provide the location of a file
: containing the trusted CA certificate(s) here. For example:
: Trusted CA File=c:\certificates\verisign.cer
[Alternate Tlinks]
: Specify alternate TSAPI links (Tlinks) here.
: The format of each entry is:
: Alternates(preferred_Tlink)=alternate_Tlink_1:alternate_Tlink_2:...
: Each entry may specify between one and four alternate Tlinks for the
: preferred Tlink. Up to 16 entries are allowed.
: For example:
: Alternates(AVAYA#CML#CSTA#AES1)=AVAYA#CML#CSTA#AES2:AVAYA#CML#CSTA#AES3
[Shared Admin]
: Instead of each workstation maintaining its own list of servers, a shared
: tslib.ini file may be placed on a network file system, for example:
: tslib.ini=n:\csta\tslib.ini
: This entry overrides the [Telephony Servers] section, if any.
```