Integration Guide - Avaya ACM

Engage Voice Recorder

Release 5.5

Issue 1.0

1 Introduction to Avaya ACM Configurations

This document describes the configurations and procedures needed to successfully integrate an Engage Voice Recording system with an Avaya Aura Communication Manager (ACM) for voice and call event recording.

Engage Record provides auto or on-demand call recording, live monitoring, screen capture and playback, or live desktop monitoring synchronized to audio playback.

The majority of configurations performed on Engage and ACM systems are performed once and left alone. One-time configurations made to both the ACM and in Engage Record server include:

- Verifying system licenses.
- Creating an Application Enablement Service (AES) user with CTI functionality enabled.
- Device, Media and Call Control (DMCC) is enabled for soft phones.
- Associations of phone devices with CTI User for recording.
- Avaya's TSAPI software configured.
- Create consecutive (ex. 3100, 3101, 3103…) soft phones.
- Engage VoIP and Option configurations.
- Engage Port Mapping and Port Numbers assigned.

2 Network Architecture

The Engage Suite is compatible with and seamlessly integrates with Avaya'a Communication Manager (ACM) Release 3.0 and higher platforms.

Avaya's interoperability with Engage Record features include full support for audio conversation and call event data capture using Avaya's native Single Step Conference Recording or port spanning.

Both recording methods require an Avaya Application Enablement Service (AES) user.

The Engage Voice Recorder also integrates with the ACM's On-Demand recording feature set using a set of softkeys.

2.1 Avaya Single Step Conferencing Recording Method

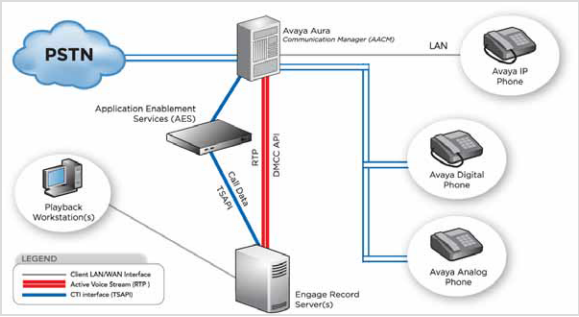
Using the Single Step Conference method, softphones are configured in the ACM for use by the Engage Recorder.

The Engage Recorder's assigned softphones are *conferenced* into recorded calls and the Device, Media, and Call Control API (DMCC) routes the voice packets to the Engage Record server.

Device, Media, and Call Control (DMCC) refers to the service that provides first party call control (Device and Media control or Device and Media Control with Call Information Services) as well as third party call control services which provides an extended set of third party call control services.

Call detail and control information is sent to the Engage Record server from the Avaya Telephony Server API (TSAPI).

Single Step Conference supports any VoIP, digital, or analog phone.

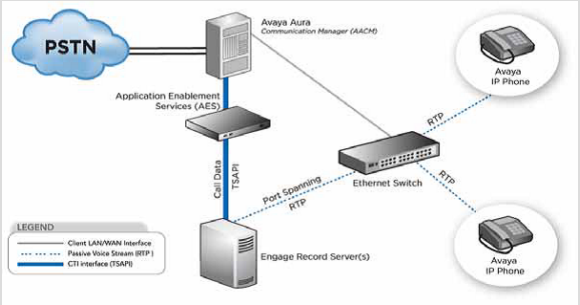


2.2 Port Spanning for TSAPI Method

For a lower licensing cost solution, Engage Record can record any IP station using the port spanning for TSAPI method.

All phone devices to be recorded are “spanned” to a single contact point (a NIC) on the network where the Engage Record server connects.

A second NIC in the Engage Record server is connected to the Avaya Telephony Server API (TSAPI) for call event information collection.



2.3 Mixed Phone Types Recorded on the Same Engage Server

Some customers may wish to use lower cost port spanning for their VoIP and Single Step Conferencing for their digital and analog phones.

Any phone types that are supported by the Communication Manager can be recorded by Engage.

Engage can record phones using different codecs and those different voice streams can be recorded on the same Engage Record Server.

Engage Record receives call events for any phone device through the TSAPI connection.

2.4 OnDemand Desktop Client Keys

To have OnDemand recording keys available as a push button on the phone, an Optional Avaya XML server is required.

Up to three functions can be push button activated on a per phone basis. These include:

- **RECORD**: This button toggles the Clickive recording of a conversation. When pressed, Engage starts recording the voice stream of the phone from that moment forward. When pressed again, Engage stops the recording. Only the voice data between the clicks of the Record button is recorded.
- **CONVERSATION SAVE**: This button causes Engage to record the entire call from start to finish, even if the button was activated midway or late in the call. Pressing the Conversation Save button anytime during the call will cause Engage to save the entire call.
- **DELETE**: Pressing this button prevents recording of a call (deletion of the recording). The conversation will be deleted even if the phone is automatically scheduled to record calls.

2.5 Avaya Server Considerations

The following is a list of Avaya server requirements:

- Avaya Aura Communication Manager 5.0 and higher acting as a central gateway compatible with the Engage Suite Server in different hardware environments.
- If the customer's configuration includes a contact center, then additional configurations are needed to supply Engage with various call center information as part of the call event data being collected.
- An *Application Enablement Services* (AES) Server will be created to provide administration for and call event data collection of associated phone devices.
- A set of consecutively numbered Soft Phones will be configured in the ACM. Under control of Engage, these devices will conference in on calls to provide conversation recording streams.
- If Avaya OnDemand recording is part of the customer configuration and phone recording keys are desired, then an optional XML server will need to be created. All phone device configurations come with OnDemand Desktop Client keys. These can be removed, if needed.
- It is imporntant to know what Avaya equipment the Engage Voice Recorder will be directly connecting with. Have the customer inform the install team of the type of equipment at the far-end. That information will be needed during TSAPI configuration. Types of equipment that Engage could connect with include:
    - S8xx Servers (S8730, S8720, S8710, S8500, S8400, S8300B/C).
    - G Series Media Gateways (G250, G350, G450, G600, G650, G700, G860).
    - IG550 Integrated Gateway, CMC1 Media Gateway, SCC1 Media Gateway, MCC1 Media Gateway, MultiTech MultiVOIP™Gateway.

2.6 Single Step Conferencing Licensing

Single step conferencing license requirements to consider are:

• All phone types are supported including VoIP, digital, or analog phones.

• Avaya Recording Licenses for each phone configured for recording:

- One (1) TSAPI license per Engage Server for the softphone conferencing
- One (1) TSAPI license per monitored phone
- One (1) TSAPI license for each concurrent voice stream
- One (1) DMCC license for each concurrent voice stream

For example, recording 100 stations would require 201 TSAPI plus 100 DMCC licenses.

2.7 Port Spanning for TAPI Licensing

Port spanning for TAPI considerations are:

- Any Avaya VoIP or remote phones can be recorded.
- Layer 2 Ethernet switch(es) with switch port analyzer (SPAN) capabilities are required
- Avaya Recording Licenses include:
    - One (1) TSAPI license per Engage Server
    - One (1) TSAPI license per monitored phone
- For example, recording 100 stations would require 101 TSAPI licenses.

3 Initial Configuration of the Avaya ACM for Recording

As with other kinds of systems, the initial configuration of the Avaya ACM with an Engage Voice Recorder is a one-time setup activity. All subsequent activities (adding and removing devices and users, setting recording schedules, individual ACD agent data manipulation, taking backups of databases, etc…) are administrative and maintenance related and are performed after system is in-service and functioning properly. Initial configuration of the Avaya ACMwill include:

- License verifications.
- Creating an Application Enablement Service (AES) User ID and Password.
- Enabling CTI functionality for the new AES User.
- Enabling Device, Media and Call Control (DMCC).
- Enable *unrestricted access* for the CTI User.
- Administer the H.323 Gatekeeper.
- Create a number of soft phones for Engage to use.
- Configuring phones for recording.
- Configure On-Demand recording, if part of the customer configuration.
- Configure contact center information for recording by Engage.

Avaya ports identify themselves through an auto-discovery process based on the devices assigned in the AES user configuration.

3.1 Avaya ACM System Management

The Avaya Communications Management system uses a web-based system manager to control all aspects of an ACM system. Implementation with an Engage Voice Recorder requires use of two components only:

- The ACM System Access Terminal (SAT) is a CLI based programming interface for the Communication Manager part of the ACM.
- The ACM Web License Manager (ACM WebLM) is a web-based application for ACM software license management.
- The ACM Application Enablement Server (ACM AES) is a web-based application used to configure, manage and control application servers.

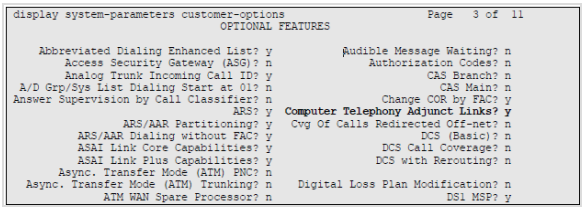
All can be accessed from the ACM administration console and will user names and passwords with appropriate permissions.

3.2 Verify Licensing on the ACM

Each ACM comes with sets of licenses for various aspects of its operation such as the Communication Manager and the Application Enablement Server. Check that these licenses are available:

Computer Telephony Adjunct Link License

The *Computer Telephony Adjunct Links* license parameter is a part of the Communication Manager license set of the ACM. This license allows the CM to configure and establish a CTI link to Engage. To check if CTI license is available:



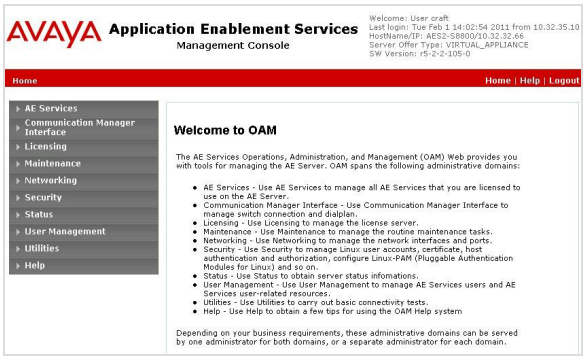
1. Log in to the System Access Terminal (SAT) and use the ***display system-parameters customer-options*** command. There are numerous pages of licensing and configuration for the ACM. Scroll down to page 3.
2. Verify that the Communication Manager license for **Computer Telephony Adjunct Links** customer option is set to ***y***.

NOTE: If this option is not set to *y*, have the customer contact the Avaya sales team or business partner to obtain a proper license file.

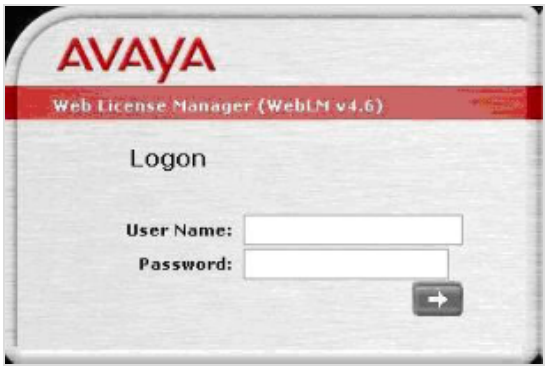
TSAPI and DMCC Licenses

The *Telephony Services Application Programming Interface* (TSAPI) license parameters are a part of the Application Enablement Services license set of the ACM. TSAPI is used to monitor and transport call data from the ACM to Engage using the CTI Link. DMCC is used for the IP softphones. Check that there are sufficient licenses to support tis deployment. To check this:

1. Start the **Application Enablement Services Management Console** and log in.

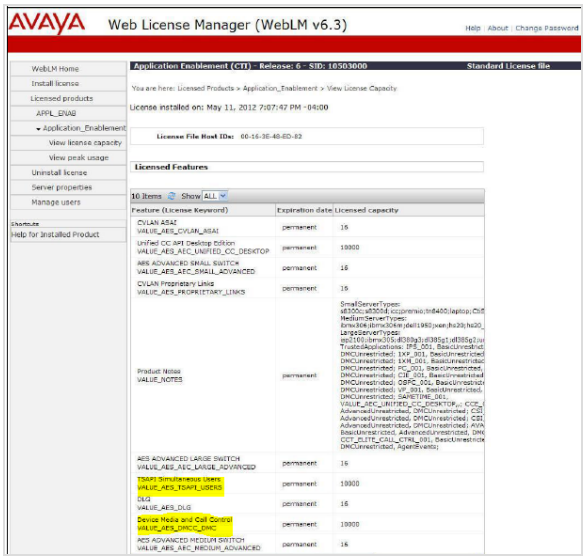


2. In the navigation pane, click ***Licensing***.

3. 

4. In the ***Licensing*** window, click ***Launch WebLM License Manager***.

5. When WebLM displays its Logon page, enter the user name and password for the WebLM.



1. The **Web License Manager** screen displays.
2. Check that TSAPI Simultaneous Users has sufficient licenses. TSAPI is used for device monitoring.
3. Check that Device Media and Call Control has sufficient licenses. DMCC is used with the virtual softphones.
4. Click ***Licensed Products » APPL_ENAB » Application_Enablement*** in the left pane, to display the Licensed Features screen in the right pane.
5. Verify that sufficient licenses for *TSAPI Simultaneous Users* are available then click ***Logoff***.

3.3 Add the CTI Link for Engage

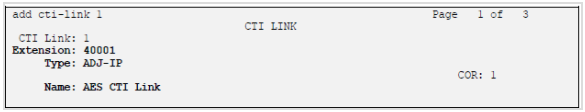
The CTI link is the path that call data is transported over. It will be used by the TSAPI link software. It must be configured in the CM system's parameters using the SAT. To do this:

Verify the CT Adjunct License

```
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
```

1. Log in to the System Access Terminal.
2. Enter the CLI command ***display system-parameters customer-options*** and verify that the **Computer Telephony Adjunct Links** optional feature is set to ***y*** on Page 3 of system-parameters.
3. If this option is not set to ***y***, have the customer contact the Avaya sales team or business partner for a proper license file.

Administer the CTI Link



1. On the SAT, enter the CLI command ***add cti-link n*** , where ***n*** is an available CTI link number.
2. Enter an available extension number (ex. ***40001***) in the **Extension** field.

NOTE: The CTI link number and extension number may vary.

3. In the **Type** field enter ***ADJ-IP*** and a descriptive name in the **Name** field.
4. Default values may be used in the remaining fields.

NOTE: The CTI link number and extension number may vary.

5. Enter ***ADJ-IP*** in the *Type* field, and a descriptive name in the *Name* field (ex. ***Engage CTI Link***). Default values may be used in the remaining fields.

3.4 Configure Avaya UCID

The Avaya Universal Call Identifier (UCID) is a unique code (up to 20 digits in length) generated in the ACM for each call. The UCID feature is a system parameter that must be enabled in the ACM. The feature must be enabled with its Node ID (switch node number) to generate per call UCIDs. An additional setting must be made to send the UCID along with other call details to Engage.

For call recording identification purposes, the UCID is sent along with other call details to Engage server. In the Engage web client, the UCID can be displayed with other call details in an assigned Generic field.

If the feature is not enabled in the ACM, then no UCID is generated or sent and the web client's Generic UCID field content will display all zeros (ex. 00000000000000000000).

To enable the UCID feature on the ACM, follow these steps:

1. Log in to the System Access Terminal (SAT).
2. Enter the CLI command: **change system-parameters features** to get to the system parameters features pages.
3. Change the following features in the system-parameters page (page 3):
   a. Create Universal Call ID (UCID): Set to y. Setting to y enables the ACM to generate a UCID for each call.
   b. UCID network Node ID: Set to 1 or any number between 1 and 32767 that is unique to this switch in the network of switches.
   c. Send UCID to ADAI: Set to y. This enables transmission of UCID information.
4. ***Save*** these settings.

3.5 Configuration for Unencrypted Data (default)

The default configuration for an Avaya ACM linked to an Engage voice recorder is using an unencrypted data and links. Use the following steps for the configuration.

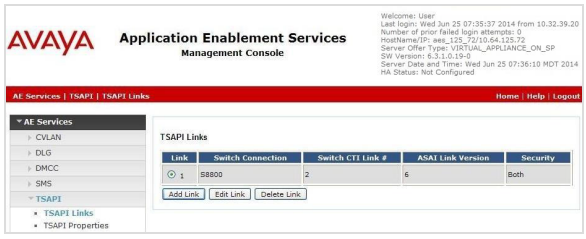
3.5.1 Add an Unencrypted TSAPI Link (Tlink)

The TSAPI link is a system software interface which provides device monitoring. TSAPI data is carried over the CTI Link. TSAPI Links (TLINKs) can be set up for *unencrypted (default) or encrypted (Clicked) data transport*.

Add an UNENCRYPTED TLINK

To add an unencrypted TSAPI Link for Engage:

1. Access the AES console and go to ***AE Services >> TSAPI >> TSAPI Links*** .



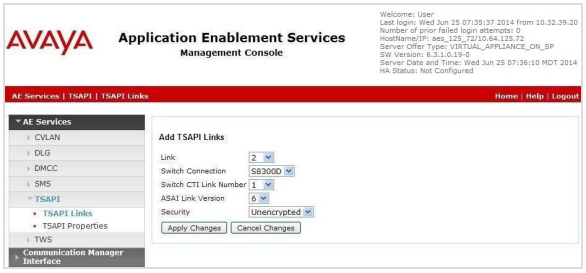
2. Click on the ***Add Link*** button to get the **Add TSAPI Links** window.
3. On the **ADD TSAPI Links** window, enter the following:
   a. **Link** field: Locally controlled and may be set to the next available number such as ***2***.
   b. **Switch Connection** dropdown: Click the correct Switch Connection (ex. ***S8300D***).

c. **Switch CTI Link Number** dropdown: Enter the ink number created with the CTI (ex. ***1***).

d. **ASAI Link Version** dropdown: Use the version inserted by the system (ex. ***6***).

e. **Security** dropdown: Leave the field set to default of ***Unencrypted***.

f. Click ***Apply Changes***.



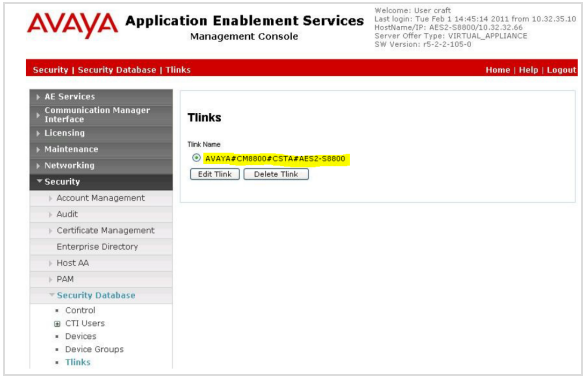
3.5.2 Obtain Unsecure AES to Engage TLINK Name

TSAPI links (Tlinks) are service identifiers (names) dynamically created by the TSAPI service. TLINK names can not be manually added or changed. They are machine-generated.

Unsecure Tlinks are the default.

To find the TLINK name:

1. Navigate to **Security » Security Database » Tlinks**.
2. The **Tlinks** window shows a listing of *Tlink names*. A **new Tlink name** is automatically generated for the new TSAPI service created.
3. Locate the **Tlink name** associated with the relevant switch connection (ex. ***CM8800***), using the name of the switch connection as part of the Tlink name.
4. Make note of the associated **Tlink name**, to be used later for configuring Engage.



NOTE: An example of a complete Tlink name is **AVAYA#CM8800#CSTA#AES2-S8800**.

3.6 Configuration Using Encrypted Data (if used)

The configurations for an Avaya ACM linked to an Engage voice recorder will use secure and encrypted data and links. Use the following steps for the configuration.

3.6.1 Add an Encrypted TLink

The TSAPI link is a system software interface which provides device monitoring. TSAPI data is carried over the CTI Link. TSAPI Links (TLINKs) can be set up for *unencrypted (default) or encrypted (Clicked) data transport*.

Add an ENCRYPTED Tlink

To add an encrypted TSAPI Link for Engage:

1. Access the AES console and go to ***AE Services >> TSAPI >> TSAPI Links*** .

2. Click on the ***Add Link*** button to get the **Add TSAPI Links** window.
3. On the **ADD TSAPI Links** window, enter the following:
    a. **Link** field: Locally controlled and may be set to the next available number such as ***2***.
    b. **Switch Connection** dropdown: Click the correct Switch Connection (ex. ***S8300D***).
    c. **Switch CTI Link Number** dropdown: Enter the ink number created with the CTI (ex. ***1***).
    d. **ASAI Link Version** dropdown: Use the version inserted by the system (ex. ***6***).
    e. **Security** dropdown: From the dropdown menu, Click ***Encrypted***.
    f. Click ***Apply Changes***.

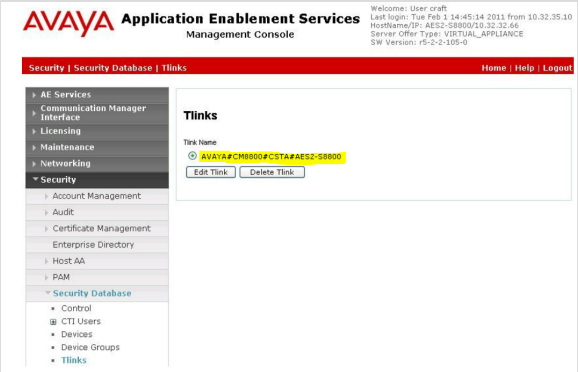
3.6.2 Obtain Secure AES to Engage Tlink

TSAPI links (Tlinks) are service identifiers (names) dynamically created by the TSAPI service. TLINK names can not be manually added or changed. They are machine-generated.

If implementing data encryption, be sure to find the associated SECURE TLINK name by looking for the secure link number in the Tlink name (ex. #AES2 is Tlink 2).

To find the secure TLINK name:

1. Navigate to **Security » Security Database » Tlinks**.
2. The **Tlinks** window shows a listing of *Tlink names*. A **new Tlink name** is automatically generated for the new TSAPI service created.
3. Locate the **Tlink name** associated with the relevant switch connection (ex. ***CM8800***) and data security implementation, using the name of the switch connection and link number as part of the Tlink name.
4. Make note of the associated **Tlink name**, to be used later for configuring Engage.



NOTE: An example of a complete Tlink name is **AVAYA#CM8800#CSTA#AES2-S8800**.

3.6.3 Export the CA Trusted Certificate

Because the Tlink will be secure, CA Trusted Certificates must be configured in both the AES and Engage. The CA Trusted Certificate, avayaprca, must be exported and placed on the Engage server.

Export the Certificate

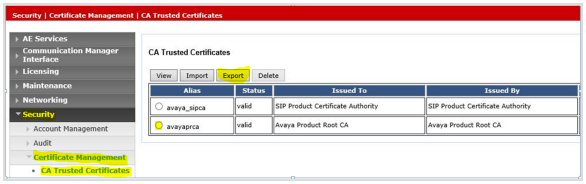
Export the avayaprca (Avaya Product Root CA) certificate from the AES server for installation to the Engage server. To do this:

1. Logon to AES.
2. Navigate to **Security » Certificate Management » CA trusted Certificates**.
3. In the **CA Trusted Certificates** window:
   a. Click the button to Click the ***avayaprca*** alias.
   b. Click the ***Export*** button.
   c. Click ALL certificate data and text (from the top line TO the bottom line) of new export dialog.

d. ***Copy*** and ***Paste*** this information into a new file.

e. Save this new file using ***Save As...*** with the filename ***avayaprca.crt*** .

f. Place this file onto the Engage server.



Import and installation of the CA Trusted Certificate is outlined in the section on Engage configuration.

3.7 Disable DMCC/TSAPI Security Database

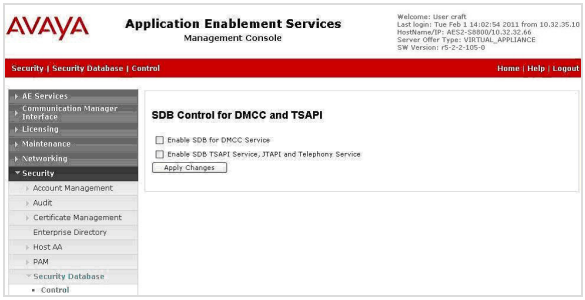
The Application Enablement Services Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control.

In the case of an AES linking to an Engage server for recording, one setting needs to be **disabled**. This procedure will affect two services, TSAPI and DMCC.

NOTE: When you change the security database settings of the AES, a restart of the affected services is required. In this case, the affected services are the DMCC Service and the TSAPI Service.

To do this:

1. Navigate to ***Security » Security Database » Control***.
2. The **SDB Control for DMCC and TSAPI** box appears.
3. *Uncheck* the ***Enable SDB TSAPI Service, JTAPI and Telephony Service*** box.
4. Click ***Apply Changes.***



5. Click ***Maintenance > Service Controller***

6. From the Service Controller page, Click the check box for the ***DMCC Service*** and click ***Restart Service***.
7. From the Restart Service page, click ***Restart***.
8. From the Service Controller page, Click the check box for the ***TSAPI Service*** and click ***Restart Service***.
9. From the Restart Service page, click ***Restart***.

3.8 Administer the H.323 Gatekeeper

H.323 is a standard that addresses call signaling and control, multimedia transport and control, and bandwidth control. IP phones require an H.323 gatekeeper to which they must register. The gatekeeper controls the connection of calls to and from the phone. The Gatekeeper needs to know what kind of equipment is on the far-end of the connection.

To set the connection:

1. Logon to the AES and go to ***Communication Manager Interface » Switch Connections*** . The **Switch Connections** screen will show a list of the existing switch connections..
2. Locate the connection name associated with the Communication Manager integrating with the Engage server ***ex. CM8800***, and Click the radio button. Click ***Edit H.323 Gatekeeper.***

3. On the **Edit H.323 Gatekeeper** page, enter the **IP address** of a *C-LAN circuit pack* or the *Processor C_LAN on the Communication Manager* to use as the **H.323 gatekeeper** (ex. 10.32.32.12) is a C-LAN.
4. Click ***Add Name or IP*** to complete the addition.

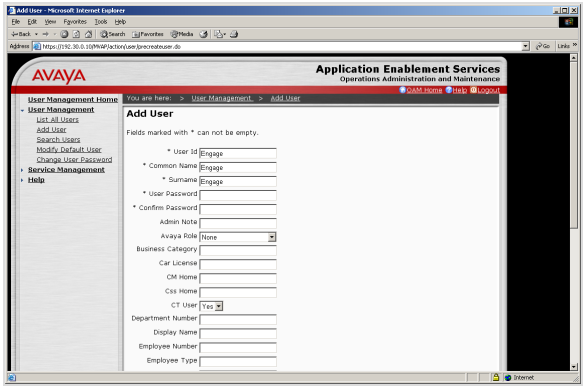
3.9 Create Application Enablement Services (AES) User

An Application Enablement Services (AES) user (with User ID and password) must be created on the Application Enablement Service (AES) server itslef. This user will have read-write access to AES User Management features and the AES Management Console.

This new user will also be configured with the CTI (TSAPI and DMCC) capabilities and associated phones to be recorded.

This AES user will be entered into the AES security database (SDB) where it is authorized and allowed to control the CTI services (DMCC and TSAPI) assigned to it.

To create and configure a new AES user:



1. Navigate to ***User Management*** and click on ***Add User***.
2. Enter desired values for: ***User Id, Common Name, Surname, User Password,*** and ***Confirm Password*** fields.

3. For **CT User**, Click ***Yes*** from the drop-down list.
4. Retain default values in the remaining fields and click ***Apply*** at the bottom of the screen (not shown).

3.10 Enable DMCC Unencrypted Port

The DMCC interface is used by Engage to register virtual IP softphones.

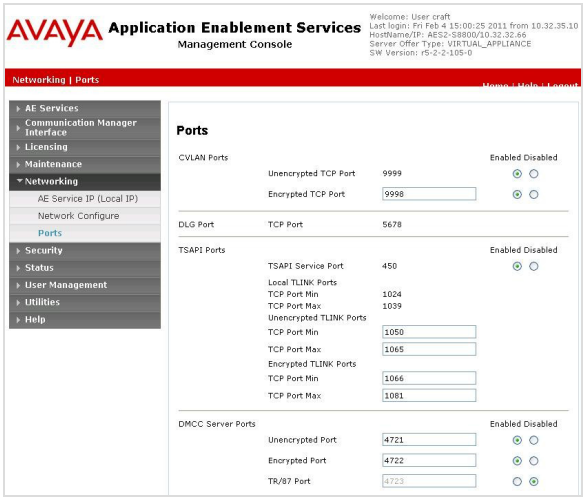
When there is an active call at the monitored agent, Engage is informed of the call via event reports from the TSAPI interface. Engage starts the call recording by using the Single Step Conference feature from the TSAPI interface to add a virtual IP soft phone to the active call to obtain the media. The event reports are also used to determine when to stop the call recordings.

DMCC service applications connect to two ports:

- Port 4721 is labeled the UNENCRYPTED port. It must be manually ***Enabled*** when deploying a default configuration.
- Port 4722 is labeled the ENCRYPTED port. The encrypted port is enabled by default.

To manually enable the Unencrypted Port, do this:

1. On the AES, navigate to ***Networking > Ports*** window.
2. In the **DMCC Server Ports** section, Click the ***Enabled*** radio button for ***Unencrypted Port***.
3. Do not change the ***Enabled*** Encrypted Port button.
4. Make note of the port numbers (unencrypted is 4721 and encrypted is 4722) for later use.
5. Click ***Apply.***

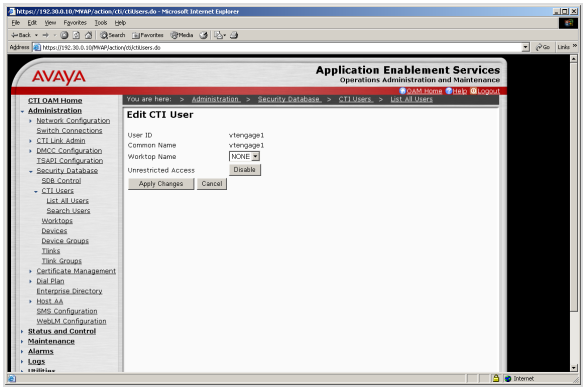


3.11 Enable Unrestricted Access to Phones for Recording

The AES user is created to manage the services and devices for recording of Avaya phone conversations. When created, it was added to the AES system's security database where it gained some CTI configurations and privileges.

Since the AES user has been added for Engage, it must be configured as a CTI user on the ACM to have unrestricted access to phone devices for recording.

Unrestricted Access is set to **Disable** by default in the ACM and must be changed. To do this:



1. On the AES, navigate to ***Administration » Security Database » CTI Users*** and click on the new AES User ID (ex. ***vtengage1*** or ***Engage***).
2. Locate the field**Unrestricted Access** and Click ***Enable*** .
3. Click ***Apply Changes***.

3.12 Add the IP Softphones for Engage

The Engage Recorder will need softphones added in the ACM for recording. These assigned (and sequential) softphones are conferenced into calls to be recorded and the Device, Media, and Call Control services (DMCC) routes the voice packets to the Engage Record server.

The number of softphones to be added depends on the system configuration. To add virtual softphones to the ACM, log in to the System Access Terminal:

```
add station next                                         Page 1 of X
                                  STATION

Extension:                        Lock Messages? n                       BCC: 0
     Type:                        Security Code:                          TN: 1
     Port:                   Coverage Path 1:                            COR: 1
     Name:                   Coverage Path 2:                            COS: 1
                             Hunt-to Station:

STATION OPTIONS
                                                  Time of Day Lock Table:
             Loss Group: 2                Personalized Ringing Pattern: 3
           Data Module? n                           Message Lamp Ext: 1014
         Speakerphone: 2-way                     Mute button enabled? y
      Display Language? English
                  Model:                            Expansion Module?

 Survivable GK Node Name:                          Media Complex Ext:
         Survivable COR:                                 IP Softphone? y
   Survivable Trunk Dest?                        Remote Office Phone? y
                                                  IP Video Softphone?
                                                               IP Video?

                                                 Customizable Labels?
```

```
change station nnnn                                      Page 2 of X
                                  STATION

FEATURE OPTIONS
          LWC Reception? spe              Auto Select Any Idle Appearance? n
         LWC Activation? y                        Coverage Msg Retrieval? y
  LWC Log External Calls? n                                  Auto Answer: none
            CDR Privacy? n                              Data Restriction? n
   Redirect Notification? y                       Call Waiting Indication:
 Per Button Ring Control? n                  Attd. Call Waiting Indication:
   Bridged Call Alerting? n                     Idle Appearance Preference? n
       Switchhook Flash? n                    Bridged Idle Line Preference? y
    Ignore Rotary Digits? n                         Restrict Last Appearance? y
  Active Station Ringing: single          Conf/Trans On Primary Appearance? n
                                                      EMU Login Allowed?
       H.320 Conversion? n          Per Station CPN - Send Calling Number? _
      Service Link Mode: as-needed       Busy Auto Callback without Flash? y
        Multimedia Mode: basic
    MWI Served User Type: _____               Display Client Redirection? n
          Automatic Moves:
               AUDIX Name:                     Select Last Used Appearance? n
                                                 Coverage After Forwarding? _
     Recall Rotary Digit? n                        Multimedia Early Answer? n

Remote Softphone Emergency Calls: as-on-local Direct IP-IP Audio Connections? n
Emergency Location Ext: 75001      Always use? n        IP Audio Hairpinning? n
Precedence Call Waiting? y
```

1. Enter the command ***add station n***, where ***n*** is an available extension number.

```
add station 45991                                        Page   1 of   5
                                  STATION

Extension: 45991                       Lock Messages? n                BCC: 0
     Type: 4620                        Security Code: 45991             TN: 1
     Port: IP                     Coverage Path 1:                     COR: 1
     Name: Engage Virtual 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: 45991
          Speakerphone: 2-way             Mute Button Enabled? y
       Display Language: english             Expansion Module? n
 Survivable GK Node Name:
         Survivable COR: internal            Media Complex Ext:
   Survivable Trunk Dest? y                        IP SoftPhone? y

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

                                       Customizable Labels? Y
```

2. Enter the following values for the specified fields and retain the default values for the remaining fields:

- **Extension**: Use an available extension number (ex. ***45991***).
- **Type**: Use any type of IP telephone. (ex. ***4620***).
- **Name**: Enter a descriptive name for the device (ex. ***Engage Virtual 1***).

- **Security Code**: Engage requires the Security Code to be the same as the Extension number (ex, ***45991***)
- **IP SoftPhone**: Set IP Softphone to ***Y***.

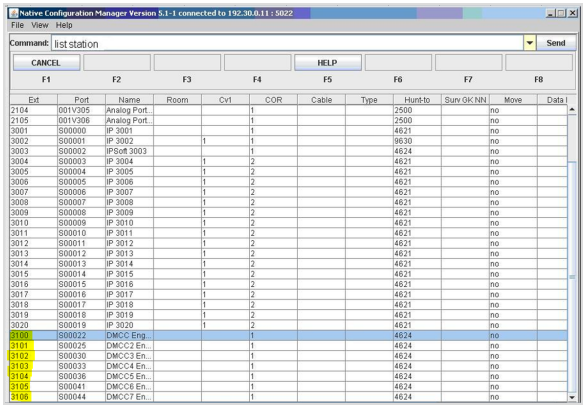
NOTE: When adding the softphones on the Avaya ACM, note that the security code for each DMCC soft phone could be anything from four to eight digits, however the security code must match the associated extension number for Engage. In other words, the Security Code of each soft phone should match the Extension number of that soft phone.

Repeat as needed to add the required number of virtual IP phones.

NOTE: Be sure that the Extension numbers are sequential.

3.13 Check that PBX Softphones Extensions are Consecutive

All of the softphones created for the Engage voice recorder need to be sequentially numbered.



On the SAT, use the ***List Station*** command to check that all softphones created for Engage recording are built in the PBX and are consecutive (ex. 3100, 3102, 3103, etc…).

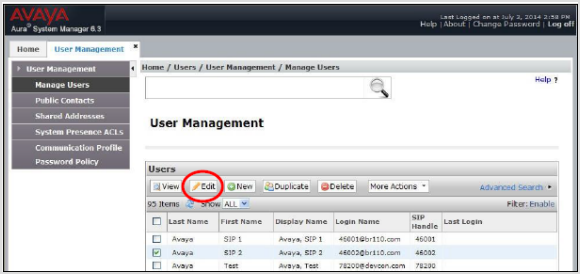
3.14 Configure Avaya Users for Recording

There are two ways to configure Avaya phones for recording.

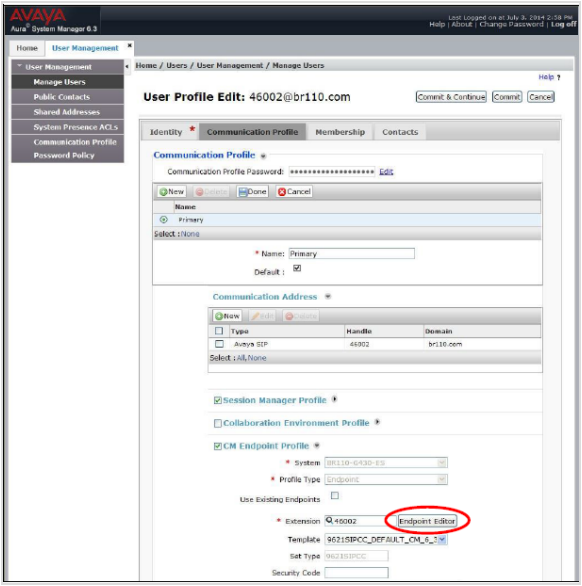
- Enable Unrestricted Access on the Engage AES user which grants unrestricted recording access to ALL phones on the ACM.

- Enable each device individually for recording.Gather MAC addresses of a Clickion of ACM phone devices for configuration for recording.

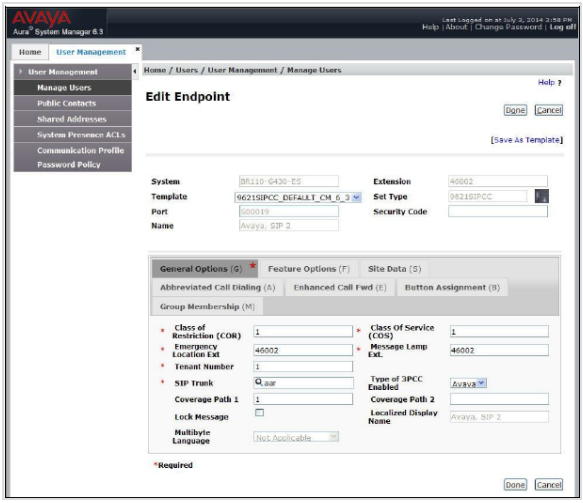
To administer users:



On the ACM system manager console, go to ***Users » User Management » Manage Users*** to display the **User Management** screen. Click the entry associated with the first SIP station to be administered and click ***Edit***.



The **User Profile Edit** screen is displayed. Click the **Communication Profile** tab and go to the **CM Endpoint Profile** and click on ***Endpoint Editor***.



The **Edit Endpoint** screen displays. Enter ***Avaya*** from the drop-down menu into the **Type of 3PCC Enabled** and retain the default values in the remaining fields. Click ***Done***.

Repeat for all phones to be recorded.

To configure the phone devices for recording:

It is necessary to obtain each device's MAC address. Gather MAC addresses of a Clickion of ACM phone devices for configuration for recording. The address will be used for port mapping in the Engage recorder. To get the IP addresses from all phones to be recorded:

1. From the Avaya IP Telephone, press the MENU button to display the Menu screen (not shown).
2. From the Menu screen, navigate to ***Network Information > Miscellaneous*** to display the Miscellaneous screen (not shown).
3. From the Miscellaneous screen, page down as necessary to display the ***MAC parameter*** (not shown).
4. Make a note of the MAC address, which will be used later to configure Engage.
5. Repeat for all Avaya IP phones to be recorded.

3.15 Configure On-Demand Recording via Softkeys for Avaya Phones

On-Demand Recording for Avaya phones is implemented by a set of softkey features that can be enabled through the ACM. When used, these keys tell the ACM to signal Engage to perform a recording request to either Clickively start and stop recording a call, record an entire call (even if the request is made sometime within the call) or to completely delete the recording a call.

These On-Demand softkeys (**Record, Conversation Save** and **Delete**) can be applied to Avaya phones. They can be removed from a phone. These push buttons, when activated, perform the following:

- **RECORD**: This button toggles the Clickive recording of a conversation. When pressed, Engage starts recording the voice stream of the phone from that moment forward. When pressed again, Engage stops the recording. *Only the voice conversation between the clicks of the Record button is recorded*.
- **CONVERSATION SAVE**: This button causes Engage to record the entire call from start to finish, even if the button was pushed mid-call. Pressing the Conversation Save button anytime during the call will cause Engage to save that entire call.
- **DELETE**: Pressing this button prevents recording of a call (deletion). The recording of the conversation will be deleted, even if the phone is automatically scheduled to record calls.

Implementation of On-Demand Softkey Recording for Avaya phones requires some configurations on both the ACM, Avaya IP Deskphones and the Engage Voice Recorder.

3.15.1 Check ACM Configuration

Most of the ACM configurations should have been completed earlier (ex. CTI link, AES user, etc) during the ACM configurations. However, use the **System Access Terminal (SAT)** and **Application Enablement Services** (AES) tool to check that the following items have been configured and started. If not, use these steps to perform the configurations as they are required for Avaya On-Demand softkeys:

1. Logon to the **ACM SAT** using credentials provided by the customer.
2. **Verify CT Adjunct Link Licensing**. Using the ***display system-parameters customer-options*** command, verify that the Computer Telephony Adjunct Links customer option is set to ***y***. If not set to ***y***, contact the Avaya sales team or business partner.

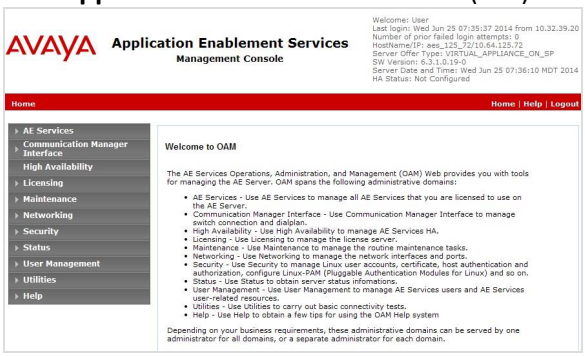
```
display system-parameters customer-options                    Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? n
        Access Security Gateway (ASG)? n               Authorization Codes? n
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? n                          CAS Main? n
Answer Supervision by Call Classifier? n                 Change COR by FAC? y
                                  ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? n
         ARS/AAR Dialing without FAC? y                        DCS (Basic)? n
         ASAI Link Core Capabilities? y                  DCS Call Coverage? n
         ASAI Link Plus Capabilities? y                 DCS with Rerouting? n
      Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? n
              ATM WAN Spare Processor? n                           DS1 MSP? y
```

3. **Administer the CTI Link**. If not already configured, add a CTI link using the ***add cti-link n*** command, where “n" is an available CTI link number. Enter an available extension number in the Extension field. Note that the CTI link number and extension number may vary. Enter ***ADJ-IP*** in the *Type* field, and a descriptive name in the *Name* field. Default values may be used in the remaining fields.

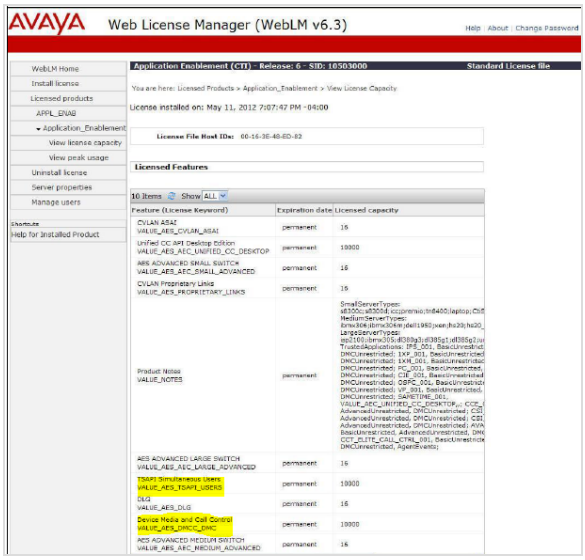
```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 40001
     Type: ADJ-IP
                                                               COR: 1
     Name: AES CTI Link
```

4. Access the OAM web-based interface by using the URL ***https://ip-address*** in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services (AES) server.

5. Launch the **Application Enablement Services** (AES) tool to perform these steps:

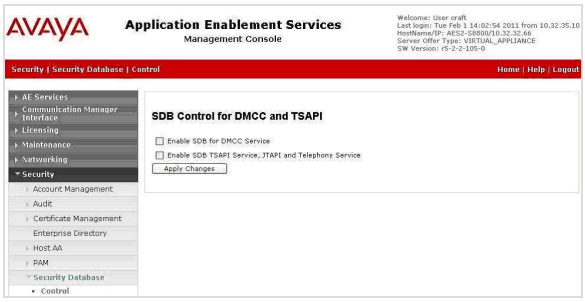


- **Verify Licensing** (TSAPI Simulaneous Users) by Clicking ***Licensing » WebLM Server Access*** in the left pane to display the Web License Manager pop-up screen and log in using the appropriate credentials. The **Web License Manager** screen is displayed. Click ***Licensed products » APPL_ENAB » Application_Enablement*** in the left pane, to display the Application Enablement (CTI) screen in the right pane. Verify that there are sufficient licenses for *TSAPI Simultaneous Users*.

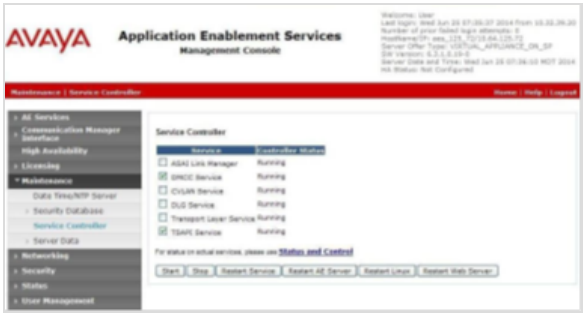


- **Administer TSAPI link**by Clicking ***AE Services » TSAPI » TSAPI Links*** from the left pane of the Management Console. The TSAPI Links screen is displayed. Click ***Add Link***. The **Add TSAPI Links** screen is displayed.
    - The *Link* field is only local to the Application Enablement Services server, and may be set to any available number.
    - For *Switch Connection*, Click the relevant switch connection from the drop-down list (ex. the existing switch connection “S8300D” is Clicked).
    - For *Switch CTI Link Number*, Click the CTI link number. Retain the default values in the remaining fields.

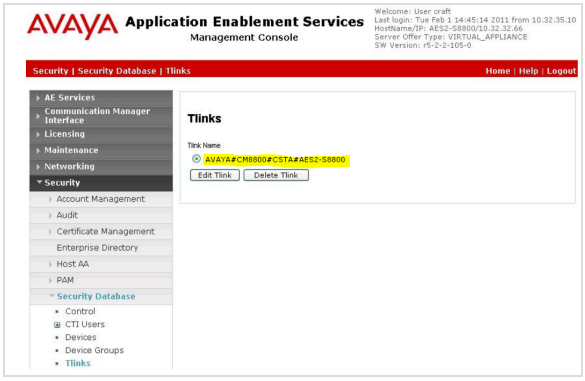
- **Disable Security Database**. Click ***Security » Security Database » Control*** from the left pane to display the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** window in the right pane.
    - Uncheck all fields.



- **Restart the TSAPI Service**. Click **Maintenance » Service Controller** from the left pane to display the Service Controller screen in the right pane. Check *TSAPI Service* and click on ***Restart Service***.



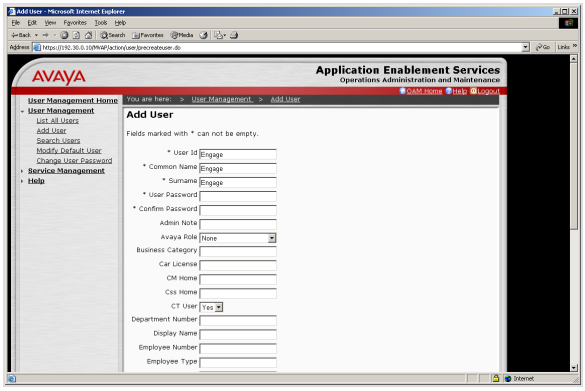
- **Obtain TLink name**. Click ***Security » Security Database » Tlinks*** from the left pane. The **Tlinks** screen shows a listing of the Tlink names. A new Tlink name is automatically generated for the TSAPI service. Locate the Tlink name associated with the relevant switch connection, which would use the name of the switch connection as part of the Tlink name. Make a note of the associated Tlink name, to be used later for configuring Engage. In this case, the associated Tlink name is "AVAYA#S8300D#CSTA#AES_125_72". Note the use of the switch connection "S8300D" from earlier configurations that is now part of the Tlink name.



- **Administer the Engage AES User**. Click ***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**.

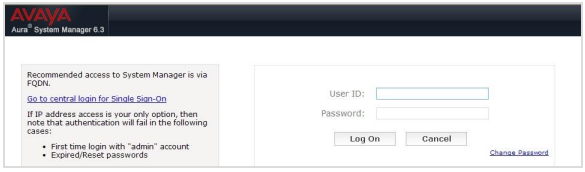
  For CT User, Click ***Yes*** from the drop-down list. Retain the default value in the remaining fields.



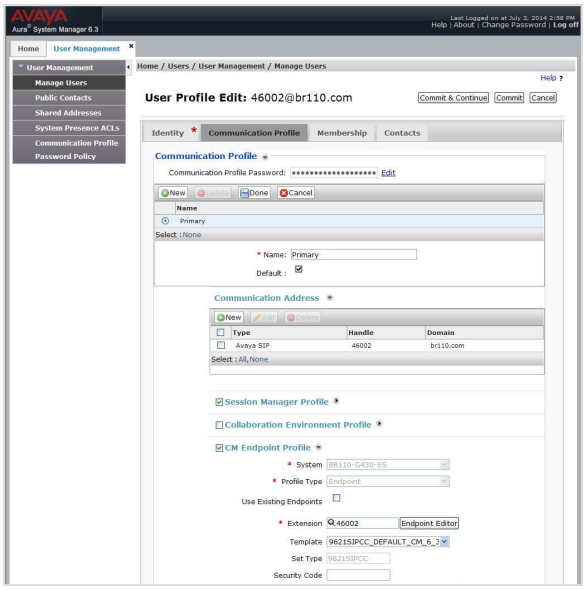
3.15.2 Configure The Session Manager

Use the **Session Manager** tool to administer the deskphones getting the on-demand softkeys.

Access the **System Manager** web interface by using the URL ***https://ip-address*** in an Internet browser window, where "ip-address" is the IP address of **System Manager**. Log in using the appropriate credentials.



- **Administer Users**. In the *System Manager* window, Click ***Users » User Management » Manage Users*** to display the *User Management* screen. Click the entry associated with the the SIP agent station (ex.***46002***), and click ***Edit***. The **User Profile Edit** screen is displayed. Click the **Communication Profile** tab.



- Scroll down to the *CM Endpoint Profile* sub-section and click ***Endpoint Editor***. In the *Type of 3PCC Enabled* field, Click ***Avaya*** from the drop-down list. Retain the default values in the remaining fields. Click ***Done***.

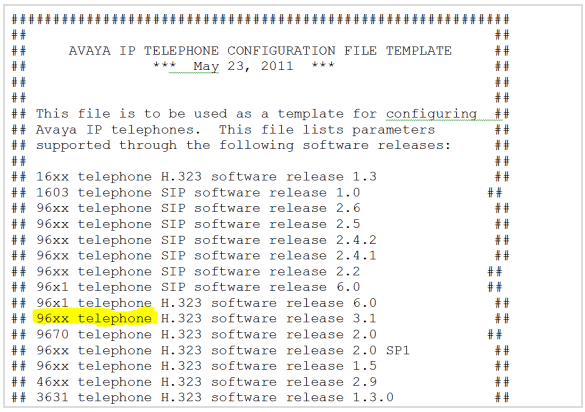
  Repeat these steps for all SIP agent users.

3.15.3 Configure the Avaya IP Deskphone Config File

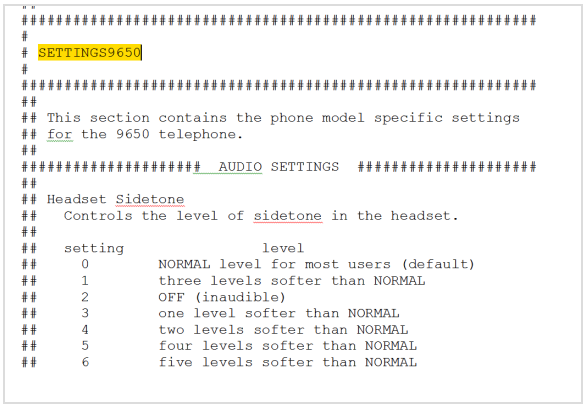
Avaya IP Deskphones use a downloaded .txt file to configure each type of phone served by the CM. Each type of phone that will be using the on-demand features will need its part (ex. the Avaya 9650 deskphone) of the .txt configuration file modified to interface the on-demand features and software. This .txt file contains elements of configuration for all types of Avaya deskphones supported by the ACM.

Using the *Avaya 9650 IP Deskphone* as an example, follow these steps to modify the .txt configuration file:

1. From the file server (the CM) serving **Avaya 96xx IP Deskphones**, locate the ***46xxsettings.txt*** file and open it with an application such as WordPad. Use the most current file.



2. Use the ***Find*** function to locate the specific phone parameters for, in this example, ***SETTINGS9650*** (the settings for an Avaya 9650 IP deskphone).



3. Scroll down the **SETTINGS9650** section of the file and locate the **WML BROWSER SETTINGS** section. In this subsection, set the ***PUSHCAP, TPSLIST, SUBSCRIBELIST, and WMLHOME*** parameters as shown below, where "10.32.39.180" will be the IP address of the Engage server running the Web Server component. ***SAVE*** the file.

Beginning of FILE EXAMPLE:

```
# SETTINGS9650

#

##############################################################

##
```

This section contains the phone model specific settings

for the 9650 telephone.

##

###################### AUDIO SETTINGS ######################

##

Headset Sidetone

Controls the level of sidetone in the headset.

##

setting level

0 NORMAL level for most users (default)

1 three levels softer than NORMAL

2 OFF (inaudible)

3 one level softer than NORMAL

4 two levels softer than NORMAL

5 four levels softer than NORMAL

6 five levels softer than NORMAL

7 six levels softer than NORMAL

8 one level louder than NORMAL

9 two levels louder than NORMAL

##

SET AUDIOSTHD 0

##

Handset Sidetone

Controls the level of sidetone in the handset.

##

setting level

0 NORMAL level for most users (default)

1 three levels softer than NORMAL

2 OFF (inaudible)

3 one level softer than NORMAL

4 two levels softer than NORMAL

5 four levels softer than NORMAL

6 five levels softer than NORMAL

7 six levels softer than NORMAL

8 one level louder than NORMAL

9 two levels louder than NORMAL

##

SET AUDIOSTHS 0

##

################ Authentication section ######################

##

CERTIFICATE SETTINGS

##

Authentication Certificates

List of trusted certificates to download to phone. This

parameter may contain one or more certificate filenames,

separated by commas without any intervening spaces.

Files may contain only PEM-formatted certificates.

SET TRUSTCERTS avayaprca.crt,sip_product_root.crt,avayacallserver.crt

##

################## WML BROWSER SETTINGS ###################

##

The WMLHOME setting is used to enable and

administer the 'Web' Application.

##

WMLIDLEURI may be used as an "idle screen" when the

phone has been idle for WMLIDLETIME minutes. By default

this URL is NULL ("") and this screen is not activated.

##

NOTES:

##

The WMLIDLEURI idle screen is different than the

Avaya screen saver activated by the SCREENSAVERON

timer. While it is possible to use WMLIDLEURI as an

"idle screen", it is recommended that the SCREENSAVERON

timer and the Avaya Screen Saver display be used for

screen saver purposes.

##

Avaya hosts a web site for IP Phones.

The WMLHOME and WMLIDLEURI parameters are set up

to point your IP telephones to this hosted site.

To enable access to this site, remove the "## "

from the SET WMLHOME ... and SET WMLIDLEURI ... lines.

To change the web site that your phones point to,

replace the provided URL in the SET WMLHOME .. and

SET WMLIDLEURI ...lines with the URL of your site.

##

SET PUSHCAP 2222

SET TPSLIST 10.32.39.180

SET SUBSCRIBELIST http://10.32.39.180/EngageOnDemand/AvayaPhoneServices/TelStratSuscribe.aspx

SET WMLHOME http://10.32.39.180/EngageOnDemandAvayaPhonesServices/TelStrat.aspxl

SET WMLIDLEURI http://www.mycompany.com/my_screen.wml

##

9650 H.323 Phone Multi-Language Administration

##

These settings are used to set the local display

language of your 9650 H.323 telephone.

##

First Language File Name

Contains the name of the first language file.

0 to 32 ASCII characters. File name must end in .txt

##

Note:

It is recommended you install the latest version of the

language files in all 96xx H.323 telephones, even if some

phones are running an earlier release of software.

##

SET LANG1FILE "mlf_s31_v49_russian.txt"

##

Second Language File Name

Contains the name of the second language file.

0 to 32 ASCII characters. File name must end in .txt

SET LANG2FILE "mlf_s31_v49_spanish.txt"

##

```
## Third Language File Name
## Contains the name of the third language file.
## 0 to 32 ASCII characters. File name must end in .txt
## SET LANG3FILE "mlf_s31_v49_french_paris.txt"
##
## Fourth Language File Name
## Contains the name of the fourth language file.
## 0 to 32 ASCII characters. File name must end in .txt
## SET LANG4FILE "mlf_s31_v49_german.txt"
##
## System-Wide Language
## Contains the name of the default system language file.
## 0 to 32 ASCII characters. File name must end in .txt
## SET LANGSYS "mlf_s31_v49_german.txt"
##
## Larger Text Font File name
## Specifies the loadable language file on the HTTP server
## for the Large Text Font. 0 to 32 ASCII characters.
##
## SET LANGLARGEFONT "mlf_s31_v49_english_large.txt"
GOTO END
############### END OF 9650 IP Phone Settings ################
#############################################################
```

End of FILE EXAMPLE

4. Repeat this programming for all Avaya 96xx IP Deskphone types that will get the On-Demand softkeys.

3.15.4 Obtain MAC Addresses

The MAC address of each deskphone that will be configured with on-demand recording softkeys will need to be recorded for later use in the Engage Port Mapping portion of the procedures. To get MAC addresses from Avaya deskphones:

1. On the Avaya IP deskphone, press the ***MENU*** or ***HOME*** button to display the *Menu* or *Home* screen.
2. From the *Menu* or *Home* screen, navigate to ***Network Information » Miscellaneous*** to display the *Miscellaneous* screen.
3. From the *Miscellaneous* screen, page ro scroll down the list to display the MAC parameter. Write down the MAC address, which will be used later to configure Engage.
4. Repeat these steps for all Avaya IP Deskphones used by the agents.

3.15.5 AFTER Engage has been Configured, Reboot the Deskphones

AFTER the Engage Voice Recorder has been configured for the On-Demand softkey feature, REBOOT all of the Avaya IP Deskphones. This will make them receive as part of their configuration, the .txt file that was changed.

4 Initial Configuration of Engage for Recording

Like the Avaya ACM, configuring the Engage Voice Recorder is a one-time configuration activity. When configuration is complete, the Engage Voice Recorder will integrate with the Avaya ACM to provide voice and call event recording services. All subsequent activities (adding and removing devices and users, setting recording schedules, individual ACD agent data manipulation, taking backups of databases, etc…) are administrative and maintenance related and are performed after system is in-service and functioning properly.

Configuring the Engage Record server requires:

Downloading and configuring Avaya TSAPI (TSP) software.

Configuring the CTI Option setting for Avaya ACM.

Configuring the VoIP and recording modes of the Engage server.

Port mapping all of the devices to be recorded in the Engage Recorder.

After installing the VoIP recording feature on the Engage Record server, the **VoIP Engine Configuration** utility is available from the Start menu. This utility includes general settings for the VoIP recording feature and is used to add specific stations to record or to delete stations from the recording configuration and to configure recording methods.

Engage supports an ability to *acquire port mapping*, en masse, but this requires that some of the per device settings, such as Dual Streaming/Mirroring and the OnDemand checkboxes for the newly acquired devices, will need updating. Updating these settings for newly acquired devices is required since not all of this information is provided by the ACM.

As lines and extensions to be recorded are added (or additional devices), the Device ID/DN combination must be entered into Engage Record for call recording.

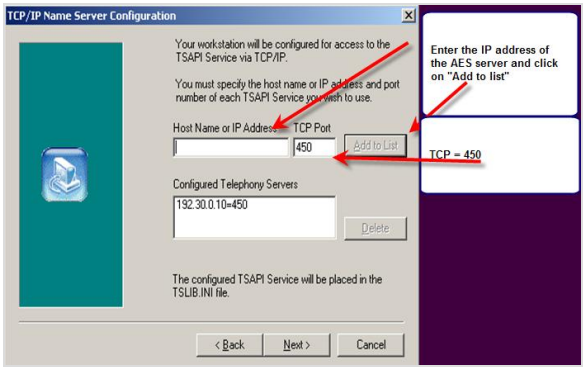
Engage Record uses a Port Number which consists of the recording board ID (ex. Avaya ACM is hard-coded as 2300) and a three-digit recording channel number (000 – 999), thus 2300:123 would be a port number. All phones to be recorded will get a port number which is used in the VoIP Configuration Utility and the WebClient.

4.1 Download/Configure Avaya ACM TSAPI

TSAPI software is an Avaya proprietary product and must be downloaded from the Avaya website to the Engage server for installation.

To do this, have the customer:

1. Go to the Avaya support site at http://support.avaya.com . They will need a login ID and password to logon to the site.
2. Once logged in, Click the TSAPI zip file version to be used and click to download to the Engage server.
3. When the folder of software is unzipped, locate and double-click on ***setup.exe*** to start the installation.
4. Click on the checkbox for I accept the terms of the license agreement and click Next.
5. Click ***Next*** to choose the default destination folder of *C:\Program Files\Avaya\AE Services\TSAPI Client* . 64-bit systems get the destination folder of *C:\Program Files (x86)\Avaya\AE Services\TSAPI Client*.



6. In the **Host Name or IP address** field, enter the ***IP address*** or valid host name of the AE server.
7. In the ***Port Number*** field, enter the default port number of ***450***.
8. Click ***Next***, then ***Install***, then ***Finish*** when the installation is complete.

NOTE: If there are other versions of TSAPI previously installed, they must be removed before the new TSAPI version can be installed.

4.2 Import CA Certificate for Encryption, If Used

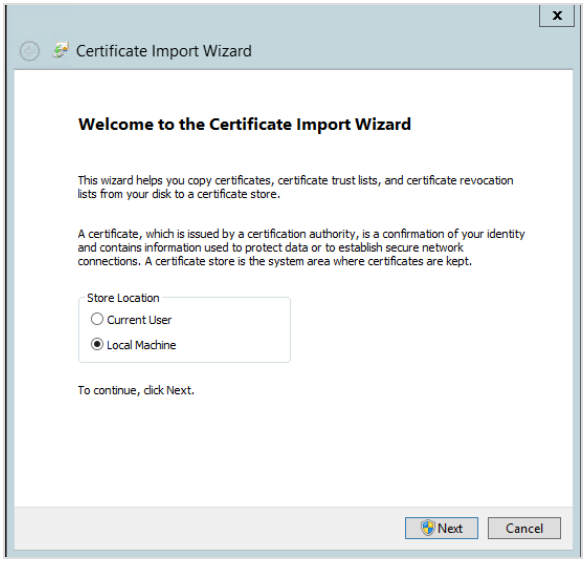
If this configuration requires encryption, the CA Trusted Certificate created on the AES and transferred to the Engage server system must be imported into Engage through the Certificate Import Wizard.

The certificate must be installed into a Personal Account repository of the Engage server. It must also be installed in the Trusted Root CA Repository of the Engage server.

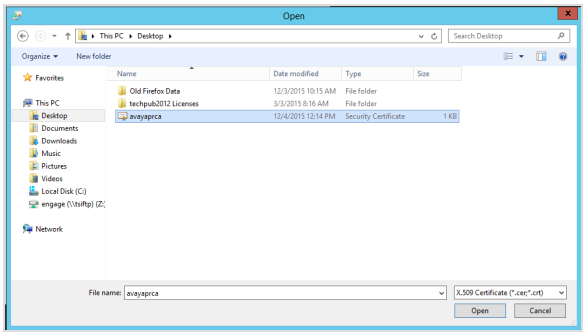
To do this:

1. Locate the file (filename is **avayaprca.crt**) that was created on the AES and sent to the Engage server.
2. Double-click on the file or right-click to get the pop-up menu and click on ***Install Certificate*** to launch the **Certificate Import Wizard**.

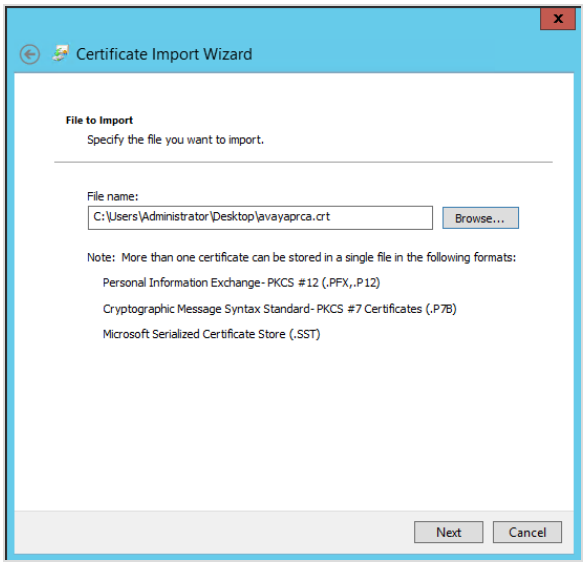
3. Click the ***Local Machine*** button and click ***Next***.



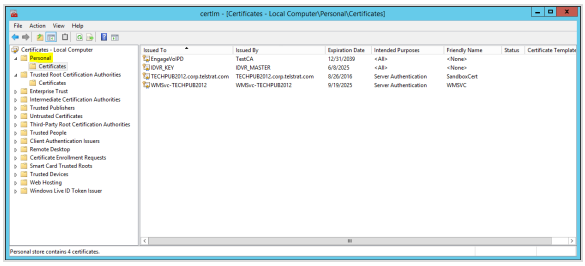
4. In the *File to Import* field, click ***Browse*** to locate the **avayaprca.crt** file.



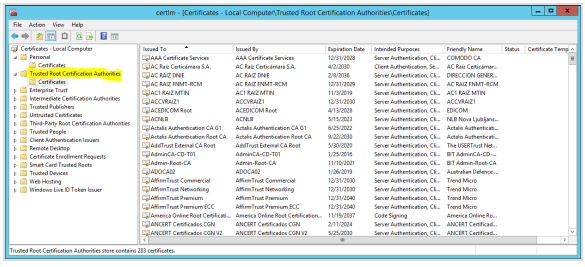
5. Click ***Next*** to continue to install the certificate.



6. The wizard will guide you through the imports. It must go to two places.
7. Install the Certificate into the Personal Certificates repository.



8. Install the Certificate into the Trusted Root Certification Authorities repository.



4.3 VoIP Configuration for Avaya ACM

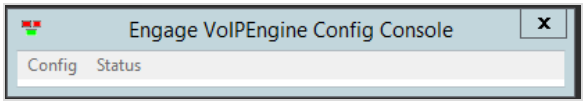
With the Avaya TSAPI software installed on the Engage server, the Engage VoIP CTI Option may now be configured for Avaya ACM.

There are TWO configurations that can be made here:

- **Unencrypted** Avaya ACM configuration (the default).
- **Encrypted** Avaya ACM configuration.

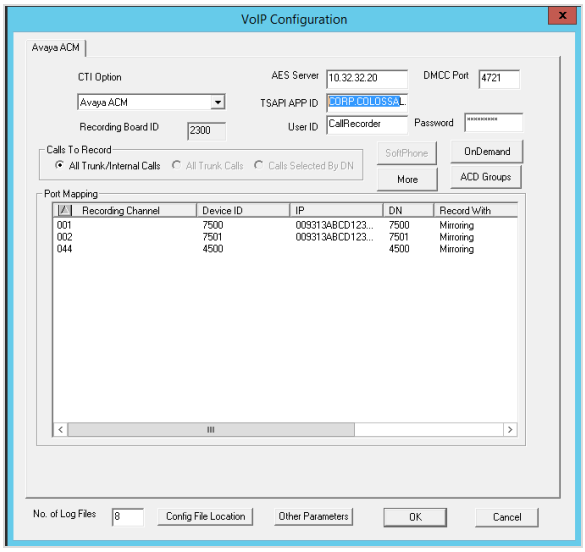
Configure an UNENCRYPTED Avaya ACM configuration (the default)

1. Launch the **VoIPEngine Config Console** and click ***Config***.



NOTE: The Recording Board ID for Avaya ACM is hard coded to 2300.

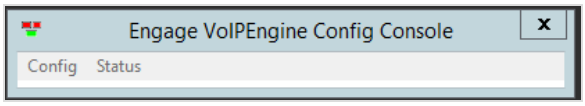
2. Enter the following Clickions into the VoIPEngine window fields:
   a. **CTI Option** drop-down menu: Click ***Avaya ACM***.
   b. **AES Server** field: Enter the ***IP address*** of the *Avaya Application Enablement Services (AES) server*.
   c. **DMCC Port** field: If using the *Single-Step Conference* recording method, enter ***4721***. Port 4721 is the Unencrypted DMCC Port. This is not required for the T-SPAN recording method.
   d. **TSAPI APP ID** field: Enter the ***TSAPI link name*** created earlier in the AES. This link is the UNSECURE lTlink created earlier in the AES.
   e. **User ID** field: Enter the AES CTI ***User ID*** (required to establish a link to the AES over TSAPI).
   f. **Password** field: Enter the ***Password*** (required to establish a link to AES over TSAPI).
   g. Click ***one*** of the following choices under **Calls to Record**:
      - **All trunk/internal calls**: To record all trunk and internal station to station call.Click
      - **All trunk calls**: To record only trunk calls.
      - **Calls Clicked by DN**: To record calls only on specific DNs.



3. Click ***OK***.

Configure an ENCRYPTED Avaya ACM configuration (IF USED)

1. Launch the **VoIPEngine Config Console** and click ***Config***.

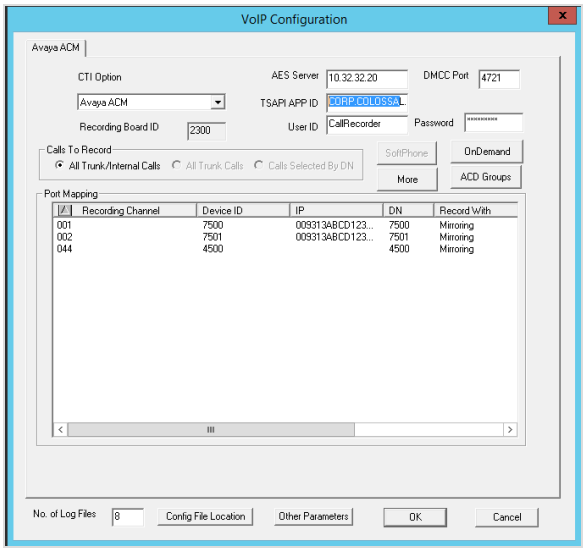


NOTE: The Recording Board ID for Avaya ACM is hard coded to 2300.

2. Enter the following Clickions into the VoIP Configuration window fields:
   a. **CTI Option** drop-down menu: Click ***Avaya ACM***.
   b. **AES Server** field: Enter the ***IP address*** of the *Avaya Application Enablement Services (AES) server*.
   c. **DMCC Port** field: If using the *Single-Step Conference* recording method, enter ***4722***. Port 4722 is the Encrypted DMCC Port.
   d. **TSAPI APP ID** field: Enter the ***TSAPI link name*** created earlier in the AES. This name is for the SECURE Tlink created in the AES.
   e. **User ID** field: Enter the AES CTI ***User ID*** (required to establish a link to the AES over TSAPI).
   f. **Password** field: Enter the ***Password*** (required to establish a link to AES over TSAPI).

g. Click one of the choices under **Calls to Record:**

- **All trunk/internal calls**: To record all trunk and internal station to station calls.
- **All trunk calls**: To record only trunk calls.
- **Calls Clicked by DN** : To Click only specific per station DNs to be recorded.



3. Click ***OK***.

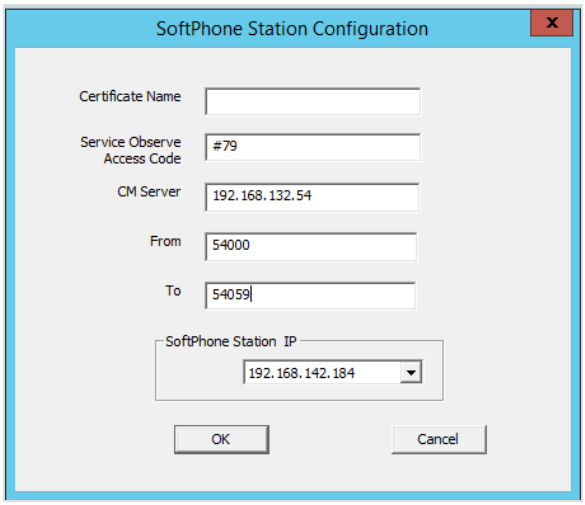
NOTE: VOIPInfo will show Keys rcvd when encrypted recording is in effect. Logs can be found here: C:\Program Files (x86)\TelStrat\Engage\VOIPEngine\Logs

4.4 Configure SoftPhones for Recording

The elements of this button are **required** for the Single-Step Conference recording method.

With Single Step Conference, Engage Record controls soft phones on the Avaya ACM. These soft phones are conferenced into calls that are recorded so that Engage Record receives the voice packets for the calls via DMCC control.

NOTE: The Engage T-SPAN recording method does not use DMCC and does not require this configuration.



1. Click the ***SoftPhone*** button on the Avaya ACM VoIP Configuration page and the **Softphone Station Configuration** window appears.
2. In the ***Certificate Name*** field: Not used.
3. In the ***Service Observe Access Code*** field, enter the code used (ex. #79) by the customer to initiate service observation.
4. In the ***CM Server*** field, enter the IP Address of the Avaya Communication Manager.
5. In the ***From*** field, enter the FIRST extension of the consecutive list of softphones with DMCC services.
6. In the ***To*** field, enter the last consecutive extension of the softphone list.
7. In the Softphone Station IP field, enter the drop-down menu to Click the IP address of the Engage NIC to use for recording calls.

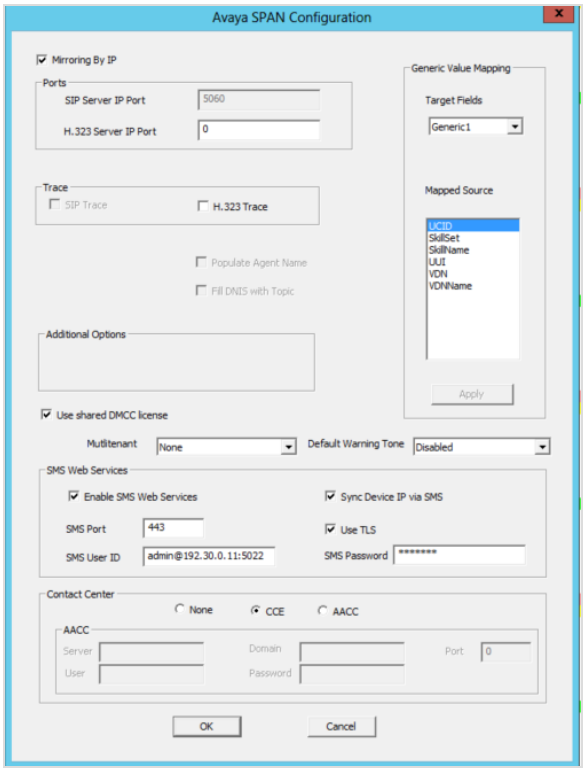
NOTE: These need to be CONSECUTIVE numbers (ex. **From** 3100 **To** 3150)

8. Use the **SoftPhone Station IP** drop-down box to Click the ***IP address*** of the **Engage Voice Recording server** NIC to be used for recording calls.
9. Click on the ***OK*** button.

NOTE: When performing configuration on the Avaya ACM, the security code for each DMCC soft phone must match its associated station. In other words, the Security Code of each softphone is the DN of that soft-phone.

4.5 More - Button - Avaya ACM SPAN Configuration

The **More** button provides the elements needed for the Avaya SPAN recording configuration. The elements of the **Avaya SPAN Configuration** window include:



- **Mirror by IP** checkbox: When checked, enables Engage to SPAN (mirror) all VoIP phones by IP address and enables *Sync Device IP by SMS* in the SMS Web Services configuration box.
- **Ports** box:
  - **SIP Server IP Port**: Enter the port (ex. ***5060*** for unencrypted) for this deployment.
  - **H.323 Server IP Port**: Enter the *port number of the H.323 gatekeeper* entity associated with the CM and Engage. H.323 gateways provide address translation, network access control and dial plans for IP virtual phones. They are optional but if a gatekeeper is present, endpoints must use the services provided.
- **Trace** box, in conjunction with the ***Ports*** box:
  - **SIP Trace**: If a SIP server is present, Clicking ***SIP Trace*** enables message tracing and troubleshooting of SIP messaging. *Do not Click this checkbox unless instructed to by TelStrat Support.*

- **H.323 Trace**: If an H.323 server is present, Clicking ***H.323 Trace*** enables message tracing and troubleshooting of H.323 messaging. *Do not Click this checkbox unless recommended to by TelStrat Support.*

- **Generic Value Mapping** box: Used to enhance the display of recorded call data on the Web Client.
  - **Target Fields** box: Sixteen target fields are available and labeled ***Generic1 through 16*** and can be found on the Web Client application on the ***Recordings tab » Playback*** display at the extreme right hand end of the columns.
  - **Mapped Source** box: The Mapped Source takes call related ACD data (ex. skillset) and populates the Clicked Generic# column fields with that data. Mapped Sources of data that can be used to fill generic columns in the web client include:
    - **UCID**: Unique Avaya Universal Call ID (UCID) value.
    - **SkillSet**: The skillset used.
    - **UUI**: User-to-User Interface data passed.
    - **VDN**: Vectored Directory Number used.
  - ***Apply*** button: Click this button when to complete the Generic Value Mapping process and save the settings.

  Working together, Target Fields and Mapped Source create a column of specific ACD/Agent type call-related information which is then displayed in the web client.

  For example, if the:

  - Target Field ***Generic1*** is Clicked (this is the column named Generic1 in the web client).
  - Mapped Source ***Skillset*** is chosen (this is the type of data to be displayed in the column).

  When a call is recorded that uses this mapped source, the information is made available to the Web Client in the Generic1 labeled column.

- **Populate Agent Name** checkbox - when available: When checked, causes the recorded agent's name to be placed in the Remark1 column of the web client.
- **Fill DNIS with Topic** checkbox - when available: When checked, Engage will populate the DNIS field of the Web Client in the ***Recordings tab » Playback*** display with a topic value.

- **Use shared DMCC license** checkbox (**required for ACM 7 only**): When checked, multiple Avaya DMCC licenses are required for conferencing, including supervised transfers, that involve multiple local extensions as well as extension-to-extension calls.

- **Multitenant** dropdown menu: Used to Click the multi-tenant configuration with an Avaya ACM. The Clickions are:
  - **None**: No multi-tenant setup is configured.
  - **Generic - Extension Mapped**: Choose this setting if Engage will be recording multiple tenants on the Avaya ACM.

- **Default Warning Tone** menu: Provides a global setting for Warning Tone use which can be managed by extension, if needed. The choices for the global setting are:
  - **Disabled**- default: When Clicked, the Warning Tone is disabled.
  - **Enabled**: When Clicked, the Warning Tone is enabled.
  - **Silent**: When Clicked, the Warning Tone is enabled but is silent.

- **SMS Web Services** box: Contains settings to support Avaya System Management Service or SMS. The SMS Web Service is hosted on the Avaya Aura® Application Enablement Services server which uses a plug-in to extend access to web-based services to a user of an ACCE system. The Clickions are:
  - **Enable SMS Web Services** checkbox: When checked, enables the SMS configurations within Engage.
  - **Sync Device IP via SMS** checkbox: When checked, enables Engage to use the SMS web services to "dynamically learn" Avaya ACM device IP addresses. If enabled, there is no need for entering the device IP during the port mapping process. Only available if **Mirroring by IP** is Clicked.
  - **SMS Port**: Must be a valid SMS Port number between 1024 and 65535 (not Zero - 0).
  - **Use TLS** checkbox: When checked, causes Engage to use TLS with the Avaya ACM SMS system.
  - **SMS User ID**: Enter the SMS user's ID.
  - **SMS Password**: Enter the SMS user's password.

- **Contact Center** box: Contains Clickions for Avaya Contact Centers.
  - **None** button: Default indicating NO contact center is configured.
  - **CCE** (Contact Center Express) button (default): When Clicked, indicates an Avaya Contact Center Express system is associated with the Avaya ACM.
  - **AACC** (Avaya Aura Contact Center) button: When Clicked, indicates an Avaya Aura Contact Center system is associated with the Avaya ACM. Additional configurations are needed, including:
    - **Server** box: Insert the server's name.
    - **Domain** box: Enter the domain name associated with the server.
    - **Port** box: Must be a valid number between 1024 and 65535 (not Zero - 0).
    - **User** box: Enter the username.
    - **Password** box: Enter the password of the user.

4.6 Other Parameters Button – Avaya ACM NICs - Port Spanning

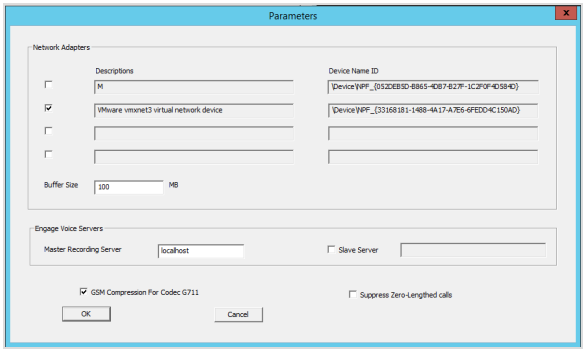
If the Port Spanning recording method is being used, click on the **Other Parameters** button. The **Parameters** window will list the Engage system's network interface cards (NIC) adapters. One of these will receive the port spanning stream from the network.

Elements of the **Other Parameters** Button window are:

- Network Adapters window is where server NIC information is listed. Select the network adapter being used for port spanning by checking the box to the left of the network adapter. Note the following information in records:
  - **Descriptions**: Contains specific descriptions for each available NIC listed.
  - **Device Name ID**: Contains specific identification information for each NIC listed.
  - **Buffer Size**: Default is 100MB.

- Engage Voice Servers box contains:
  - **Master Recording Server** text box: Enter ***localhost***.
  - **Slave Server** checkbox: If checked, enables the text box. Enter the name of the slave server here.

- **GSM Compression For Codec G711** checkbox: When checked, G.711 calls are compressed using GSM compression by default. This reduces the storage consumption by a factor of 10 (from 128kbps to 12.8kbps).
- **Suppress Zero-Lengthed calls** checkbox: If the customer is using two recorders and the Host2 recorder is a redundant/backup recorder only, there is an additional configuration parameter that needs to be checked. While Host2 is not receiving the bearer traffic, it is receiving TAPI call events. When selected, this setting prevents having 0K (zero-K) duration calls displayed in the backup recorder playback log when it's only receiving TAPI events and not the bearer traffic



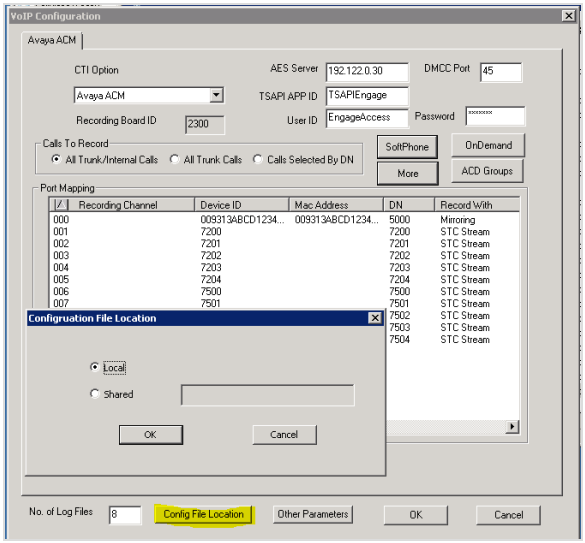
4.7 Config File Location Button

The Config Location button provides a choice on where to store the server's VoIP configuration, either locally or off the system.

The **Configuration File Location** button elements are:

1. ***Local*** radio button: When clicked, a copy of the VoIP configuration file is stored on the local host.
2. ***Shared*** radio button and window: When clicked, a copy of the VoIP configuration file is stored at this

shared location entered in the text box.

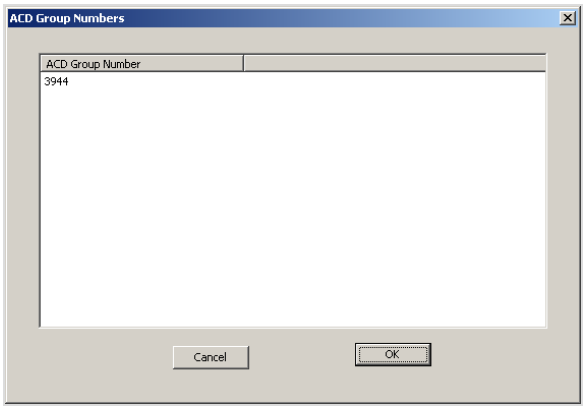


4.8 ACD Groups Button

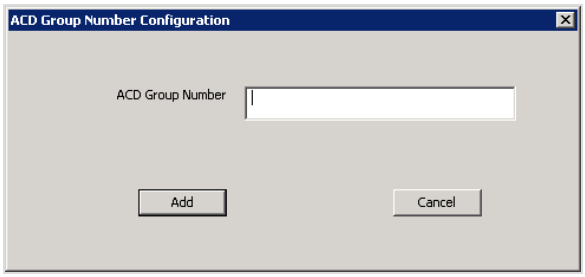
Engage Record can collect Agent Logon/Logoff events of acquired ACD agent IDs for agent calls. This requires that Engage Record is configured to monitor Avaya Hunt Groups.

To collect the agent logon/logoff events of an Avaya ACD Hunt Group, perform the following steps:

1. Click the **ACD Groups** button in the **Avaya ACM VoIP configuration** window.



2. Right-click in the **ACD Group Number Field** and then left-click on ***Add***. The following dialog box displays:



3. Enter the ***Hunt Group Extension*** of the group of Avaya devices to collect events, in the **ACD Group Number** field.
4. Click on the ***Add*** button.
5. Enter additional ***hunt group extensions***, as required, for the customer configuration and click on the ***Add*** button after each extension.
6. When finished entering hunt group extensions, click on the ***Cancel*** button to close the **ACD Group Number Configuration** window.
7. Click on the ***OK*** button to exit the **ACD Group Numbers** window.

4.9 Reconfigure for SMS

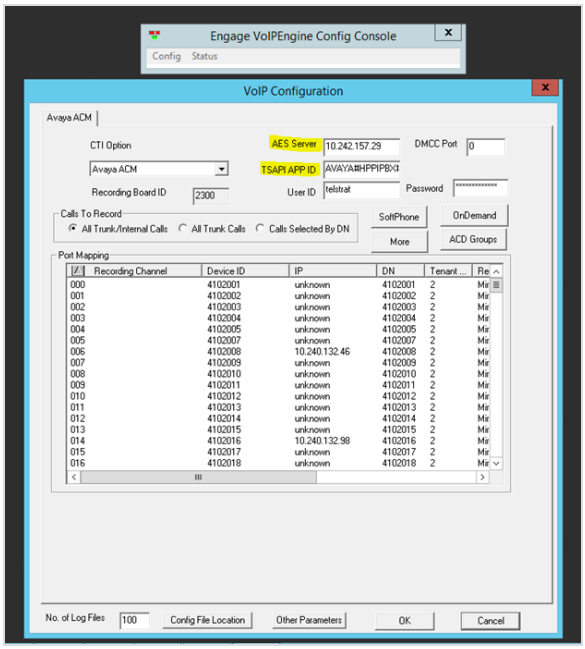
Some customers with an existing Engage-ACM integration may choose to reconfigure their systems to implement SMS features. This procedure uses customer supplied information to make changes to the Engage - AES connection supporting SMS.

Information needed to make this kind of change includes:

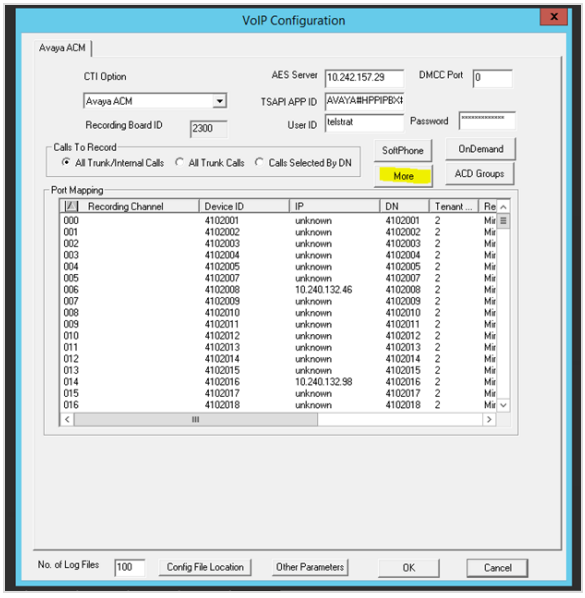
- AES Server IP Address: This is the address of the AES supporting SMS.
- TSAPI APP ID: This is the name of the TLINK created in the AES supporting SMS.
- SMS User ID and Password: This is the AES account created in the ACM supporting SMS.

Engage System Changes

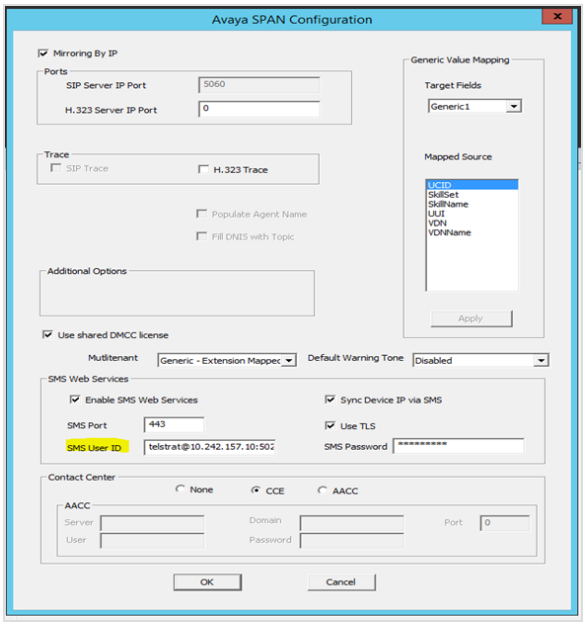
1. Log onto the Engage server and start the VoIPEngine Configuration Utility.
2. Change the following on the **VoIP Configuration** screen:
   - **AES Server**: Enter the IP address of the AES supporting SMS.
   - **TSAPI APP ID**: Enter the TLINK name of the TSAPI link used to support SMS.



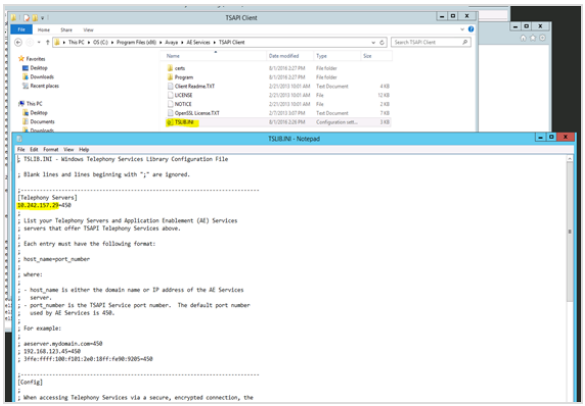
3. Click the ***More*** button and get the Avaya SPAN Configuration screen.



4. Change the following on the **Avaya SPAN Configuration** screen:
   - **SMS User ID**: Enter the AES user name for the account that supports SMS.
   - **SMS Password**: Enter this account's password.



5. Restart the TelStrat Engage VoIP Engine service using the Services tool. The restart will apply the new changes made in the VoIP Configuration.
6. When the restart is complete, use this general path to find the TSAPI Client folder: C:\Program Files (x86)\Avaya\AEServices\TSAPI Client
7. Using **Notepad**, open the script file named *TSLIB.ini*.
8. Find the *(Telephony Servers)* heading.
9. Highlight the IP address and change it to the IP address of the AES supporting SMS (ex. from 10.242.157.10 to 10.242.128.29).
10. Save this change.



Reboot the Engage server to apply this file change. After the reboot, verify that these changes took effect and are working.

Verify the Connection is Good

1. Start either Baretail or Notepad. Select ***File » Open*** and choose the path of the log file: C:\Program Files (x86)\TelStrat\Engage\VOIPEngine\Logs (AvayaSMSWS.log).
2. While viewing the log content, verify this type of entry (indicates Engage connected to the SMS service successfully): ***TelStrat.AvayaSMSWS:8: IsConnected::YES***
3. Close and exit the log file.

View Recorder Events for SMS

1. Use the web client's ***Recorder Admin Events*** tab and select the recorder that was reconfigured.
2. Verify that the most recent SMS event indicates *SMS Connected*.

Verify Test Calls Recorded Correctly

Use a test phone and the web client to verify that test calls are recording correctly.

1. Place a test call from a configured extension for that recorder. Call duration should be at least 60 seconds before release of the call.
2. Use the web client's ***Recordings » Playback*** tab and click on the ***Recent Calls*** button. The results should display the test call that was made.
3. Double click on the test call and play it back and verify audio was recorded in both directions.
4. Verify the call record does not contain a red exclamation point ! for duration. If it does, that means packets were not received for the call and the recording failed.

4.10 Configure OnDemand Recording Feature on Engage Server

Engage Record will collect supervisor/agent on-demand recording events (activated by softkey use) of acquired ACD agent IDs for agent calls.

Within the Avaya ACM, there will be ACD skill groups defined. Each group will have a ACD Group number (ex. 65555). Within the ACD skill Group will be members such as a supervisor and agent telephone extensions (ex. supervisor - 65000, agent1 - 65001, agent2 - 65002).

On-Demand softkeys are assigned to agent Avaya IP deskphones within the group. These phones are found in an Avaya Skill Group with a label such as ACD Group 65555. The group number will be needed later.

The following tasks need to be completed on the Engage Recording server to implement on-demand recording for Avaya phones with softkey buttons:

- Install the *Avaya Phone Support Features*oftware on the Engage Recording server.
- Configure the *Web.config* file on the Engage Recording server with the web server's IP address.
- Configure the *On-Demand Feature* in the VoIP configuration (VoIPEngine).
- Check the TSAPI settings in the VoIP Configuration.
- Administer ACD Skill Groups in the VoIP Configuration.
- Administer Device Port Mapping in the VoIP Configuration.

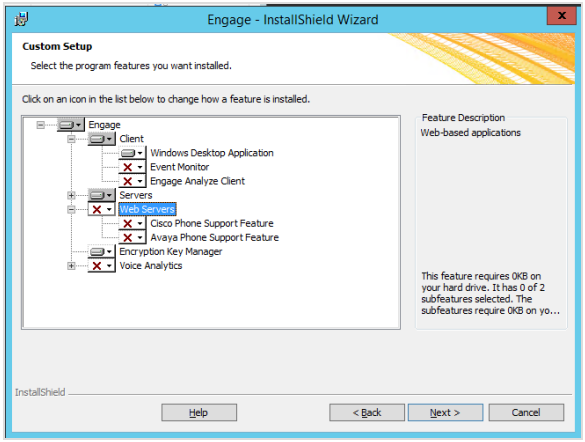
4.10.1 Install the *Avaya Phone Support Feature* in the Engage Recording server

This software is installed as part of the Engage Server software package. It creates a web server that will communicate with the ACM to manage the responses to on-demand recording softkey requests. The Engage Install Wizard is used to install the feature.

1. Launch the **Engage Install Wizard** from the folder containing Engage software.
    - *If this installation is the initial configuration* of a new Engage Recorder, follow the *Engage Server installation procedure* until arrival at the **Custom Setup** page. Add this step to the Engage Server Installation **Custom Setup** procedures.
    - *If this installation is an upgrade or change* to an existing Engage Recorder, the **Program Maintenance** window will ask what kind of change is requested. Click the ***Modify*** button and then ***Next*** which will bring up the **Custom Setup** window.

2. At the **Custom Setup** page, expand *Web Servers* and **Click** the ***Avaya Phone Support Feature*** and click ***This feature will be installed on the local hard drive***. Click ***Next***.

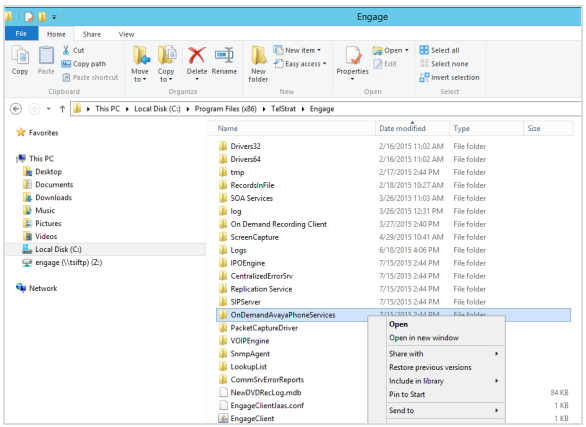
3. Click through the remaining windows until installation is complete. Close the install wizard.

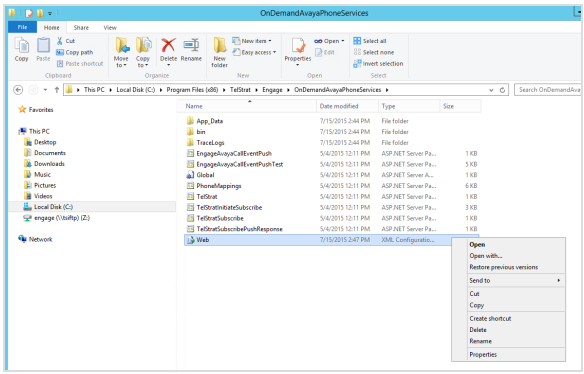


4.10.2 Configure the Web.Config file

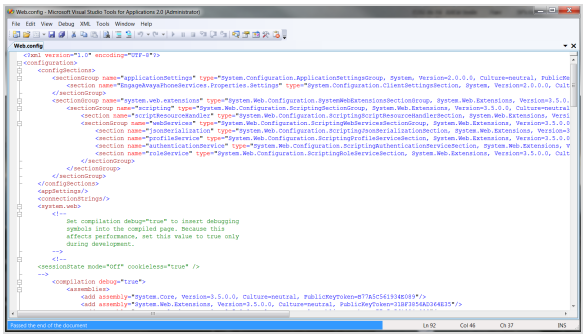
The Web.config file provides the configuration parameters of the Engage Web Server. A change is needed to set the correct web server IP address. Follow these steps:

1. On the Engage Recording server, navigate to the *Web.config* file by clicking through ***C:\ » Program Files (x86) » TelStrat » Engage » OnDemandAvayaPhoneServices*** and locating the filename ***Web*** or ***Web.-config***.

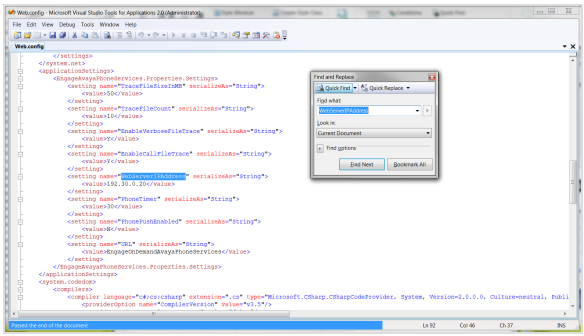




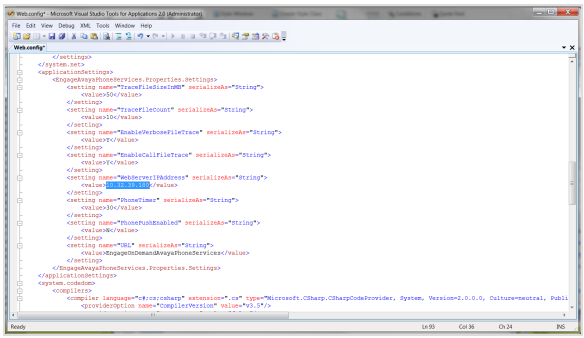
2. Double-click on the filename (ex. ***Web or Web.config***) to open it. It is an XML file and will use Microsoft Visual Studio to open the file.



3. Locate the *webserveripaddress* string and value field by clicking on ***cntl-f*** to get the **Find** window and entering ***webserveripaddress*** and clicking ***Find Next*** to get to the string.



4. Highlight the address and change the value in the value field to the IP address of the Engage web server (ex.***10.32.39.180***).

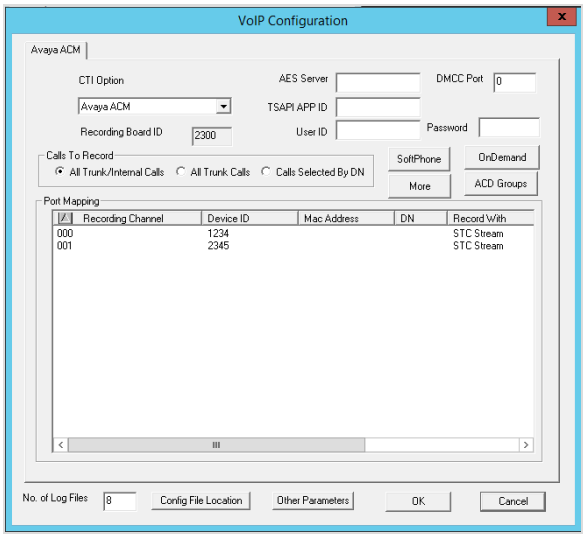


5. Click ***File » Save Web.config***.

4.10.3 Enable OnDemand in VoIP Configuration

This feature is activated by enabling it in the Avaya ACM VoIP configuration page of the Engage server.

1. Launch the **VoIPEngine utility** and click on ***Config***.
2. On the VoIP Configuration screen, click the ***OnDemand*** button.

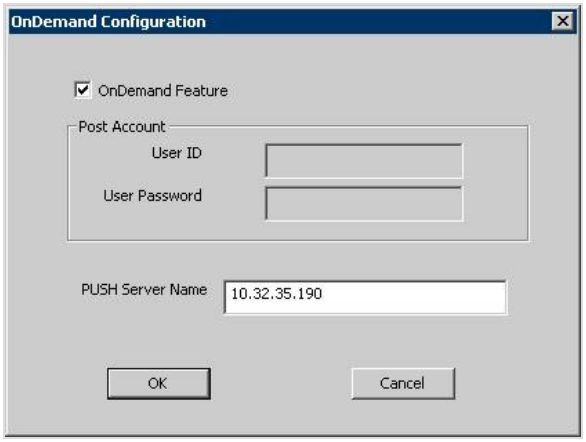


3. Check the **OnDemand Feature** checkbox.

> NOTE: **Do Not Use** the Post Account login area.

4. In the **PUSH Server Name**field, enter the ***name or IP address of the Engage Voice Recorder***, normally the C-LAN IP address of the server (***ex. 10.32.35.190***).
5. Click ***OK***

6. Since a change has been made to the Engage Configuration, a restart of the Engage Voice Recording Service is needed.
    - Go the **Services** tool on the Engage server.
    - Scroll to the *Telstrat Voice Recording Service* in the services list.
    - Right-click on the service and click ***Stop***.
    - Wait 10 seconds then right-click on the service and click ***Start***.
    - When the service starts, close the **Services** Tool.



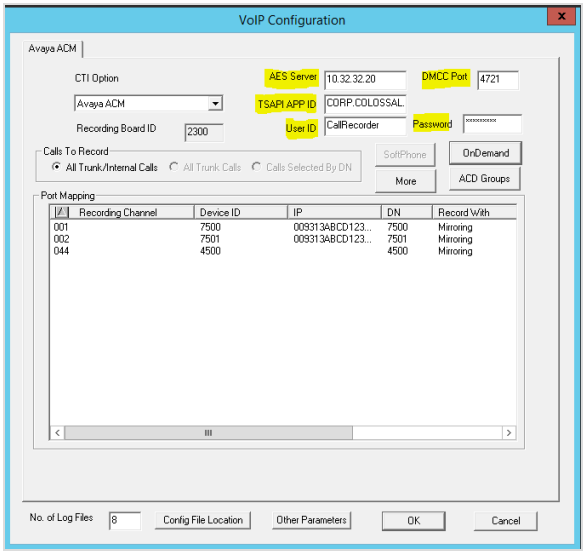
4.10.4 Check TSAPI Settings

With the VoIP Configuration screen still displayed, verify the following values have been entered in the specified fields, and retain the default values for the remaining fields.

This configuration should have been completed earlier in the Engage installation process. If not, make sure the following entries are set:

1. Launch the VoIPEngine Console Utility.
2. In the **AES Server** field, enter the ***IP address*** of the *Avaya Application Enablement Services (AES) server*.
3. If using the *Single-Step Conference* recording method, enter ***4721***in the **DMCC Port** field. This is not required for the T-SPAN recording method.
4. Enter the ***TSAPI link name*** created earlier in the **TSAPI APP ID** field.
5. Enter the AES CTI ***User ID*** in the **User ID** field (required to establish a link to the AES over TSAPI).

6. Enter the ***Password*** in the **Password** field (required to establish a link to AES over TSAPI).



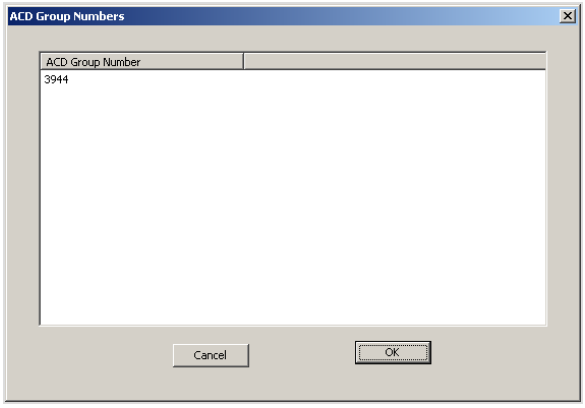
4.10.5 Administer ACD Groups

Engage Record will collect and respond to supervisor and agent on-demand recording events (softkey initiated) of acquired ACD agent IDs for agent calls. This requires that Engage Record is configured to monitor the Avaya ACM agent ACD Groups.

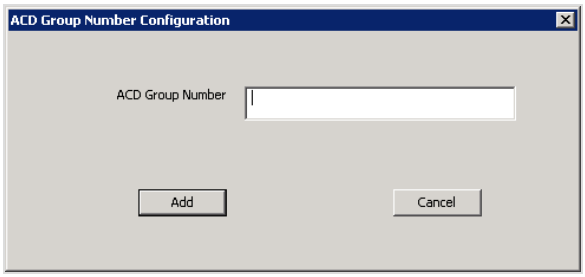
To collect the on-demand recording events of an Avaya ACD Group, perform the following steps:

While still in the VoIP Configuration window,

1. Click the **ACD Groups** button in the *Avaya ACM VoIP configuration*window.



2. Right-click in the **ACD Group Number Field** and then left-click on ***Add***. The following dialog box displays:

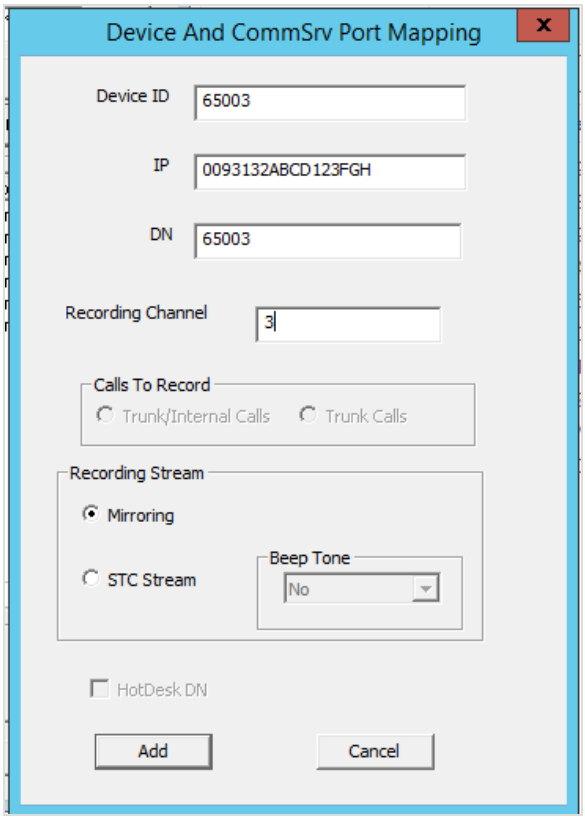


3. Enter the ***ACD Group number*** (ex. 65555) of the group of Avaya devices to collect on-demand events, in the **ACD Group Number** field.
4. Click on the ***Add*** button.
5. Enter additional***ACD Group numbers***, as required, for the customer configuration and click on the ***Add*** button after each extension.
6. When finished entering ACD Group numbers, click on the ***Cancel*** button to close the **ACD Group Number Configuration** window.
7. Click on the ***OK*** button to exit the **ACD Group Numbers** window.

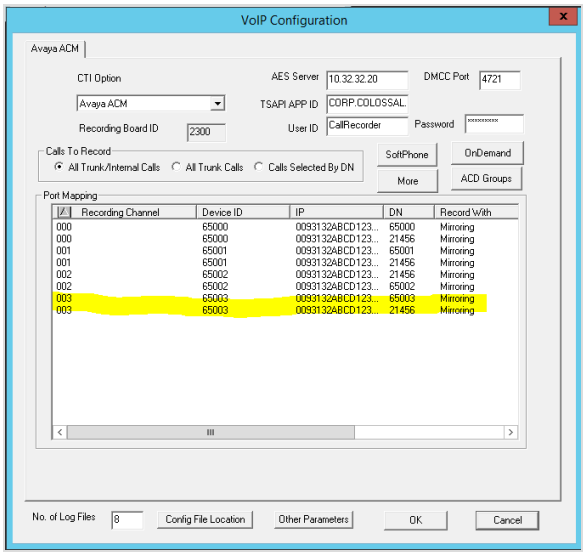
4.10.6 Port Mapping for Devices with On-Demand Recording

While still in the VoIP Configuration window:

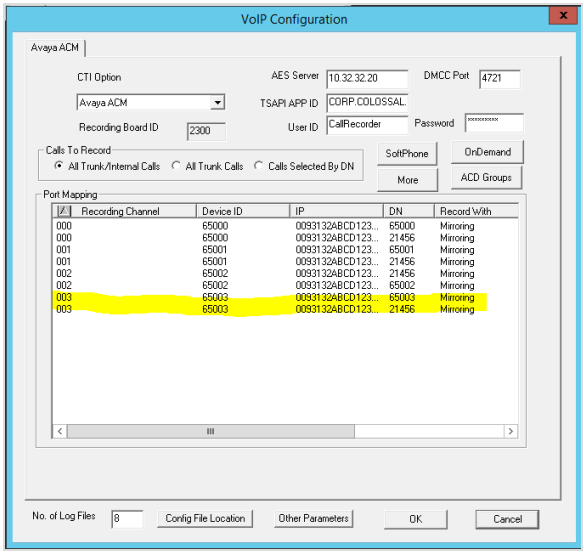
1. Right-click in the empty pane to get the popup menu and click ***ADD***. The Device And CommSrv Port Mapping screen is displayed.



2. For ***Device ID***, enter the first agent telephone extension of the ACD Group getting OnDemand.
3. Click the ***Mirroring*** button to enable the Mac Address field (it will be labeled IP but will hold the device's MAC address).
4. For ***Mac Address***, enter the MAC address of the first ACD group agent telephone.
5. For ***CommSrv Port Number***, enter an available port (ex. 000 through 999).
6. For ***DN***, enter the dialed number to reach the agent directly for personal calls (non-ACD). For calls originated inside the switch, this is usually the agent telephone extension, depending on the switch configuration. For calls originated outside the switch, the dialed number usually contains the dial plan prefix.
7. Note that a device port mapping needs to be created for every possible dialed number that can reach the agent directly.



Repeat these steps to create device port mappings for all agents in ACD Group. Depending on the numbering plan configuration, two entries may be created for each agent. In this example, the incoming trunk calls directly to the agent will have a prefix of 21456.



Internally, the agent is reached by dialing 65003.

Externally, the agent is reached by dialing 214-566-5003 (hence the prefix of 21456).

5 Engage Port Mapping

Port Mapping is the process of taking device data from the ACM and mapping it onto the Engage server's recording channels. All devices on the ACM that are to be recorded must be contained in the Port Mapping configuration.

Assigning Device IDs, DNs and Recording Methods will become tedious if hundreds of ports must be programmed. To speed the programming of port mapping, the Engage VoIP configuration supports importing the mapping information when it is entered as a comma separated file. Be aware that imported files will overwrite all existing port mapping information in Engage.

Use the **Bulk Data Import** method for initial and large changes to reduce installation time. Individual adds, deletes and modifications can be accomplished via the Web Client.

5.1 Bulk Port Mapping

Use the **bulk data import** method with a new deployment or a large configuration change. TelStrat recommends entering two ports of information into Engage and then exporting a CSV file (.txt or .xlt) to use as a starting point. This makes sure that the data entered into the file format is compatible with Engage Record and will be written into the port mapping area without issues. The imported file should contain all of the phones in the ACM that are to be recorded.

If creating new port mapping for a new Engage system:

- Enter two devices to be recorded into the port mapping area.
- Export the port mapping (with two entries) into a CSV .txt or .xlt file.
- Add all new port mapping data with a text editor or spreadsheet program (normally taken from customer completed text or spreadsheet files).
- Save the file.
- Import the new port mapping file into Engage (overwriting the old data with all new).

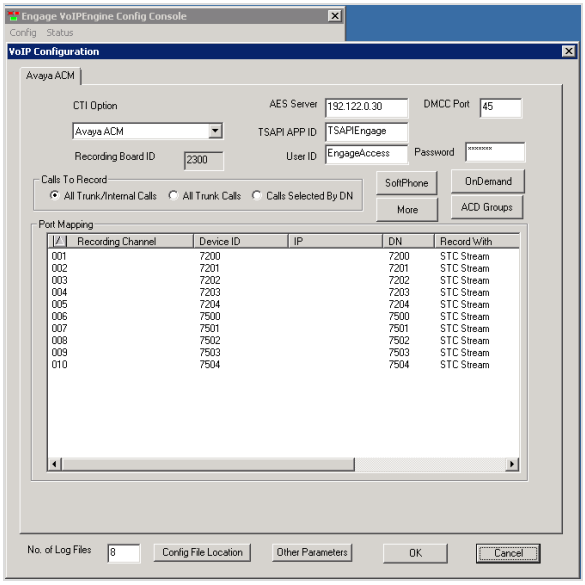
If changing current port mapping for an existing Engage system (ex. adding a few new phones for recording):

- Export all existing port mapping configuration data into a CSV .txt or .xlt file.
- Add / delete / modify the port mapping data with a text editor or spreadsheet program.
- Save the file.
- Import the newly updated port mapping file into Engage (overwriting the old data with new).

5.2 Export a port mapping configuration file

To *export* a port mapping configuration file (either to begin a new installation or change an existing port mapping configuration), perform the following:

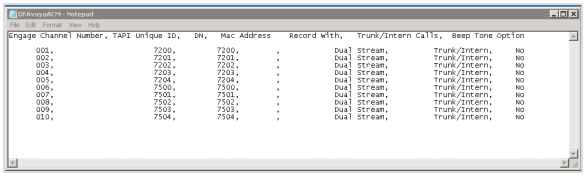
1. Right-click in the white area of **Port Mapping** section of the **ACM VoIP Configuration** page. A pop-up window appears.



2. Click ***Export File*** from the pop up menu.

3. An **Export File** dialog box displays. Create a filename (ex. ***VoIPConfig***) and Click a *directory* (ex. ***c:\Documents***) to store the file. Add the .txt extension to the filename to open it with the Windows text editor or .xlt to open the file with Microsoft Excel.

4. Click on the ***Save*** button.



5. Use a text editor such as Notepad or spreadsheet editor such as Excel to view and modify the contents of the file.

> **NOTE:** The field names for an ACM port mapping configuration are: Engage Channel Number and it must be a 3-digit number from 000, 001, 002 – 999), TAPI Unique ID, DN, Mac Address, Record With and Trunk/Intern Calls.

6. Click on ***Save*** when all entries to the file are completed.

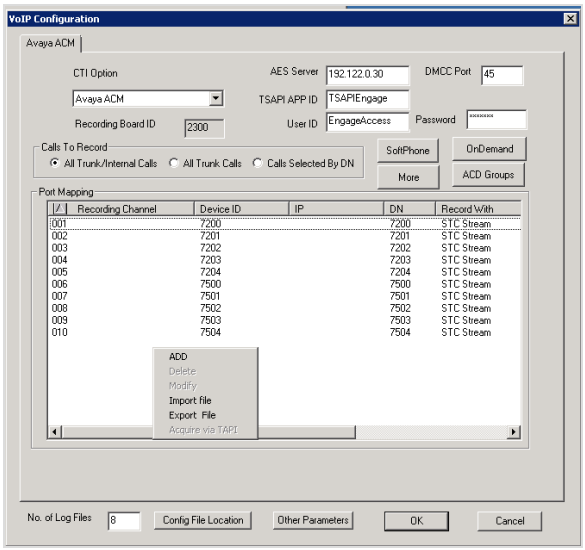
All devices that are to be recorded MUST have their data entered correctly into the port mapping file or there will be no recording of that device. Usually, this information is taken from customer files completed prior to the deployment.

5.3 Import a port mapping configuration file

Warning: Importing a VoIP configuration file (port mapping) will overwrite all of the current VoIP port mapping content in Engage with the new VoIP port mapping content. Be sure to have a backup of the current configuration before importing.

To **import** a new or modified port mapping configuration file, perform the following:

1. Right-click in the white area of **Port Mapping** section of the **ACM VoIP Configuration** page. A pop-up window appears.



2. Click ***Import File*** from the pop up menu.
3. A **Import File** dialog box displays.
4. Click on the **Browse** button and locate the name of the file (ex. c***:\Documents\VoIPConfig***) to import.
5. Click the file and click ***Open***.
6. The content of the import file will populate the port mapping area for the VoIP Configuration page, such as:

a. The Port (Recording Channel) located in column 1

b. The Station (Device ID) located in column 2

c. The MAC address located in column 3

d. The Extension (DN) located in column 4

e. The Record With Clickion is in column 5.

7. Click on the ***OK*** button.

8. Verify that ALL the information imported properly into Engage Port Mapping area before continuing.

Remember that whatever is NOT input into the Port Mapping area will not be recorded.

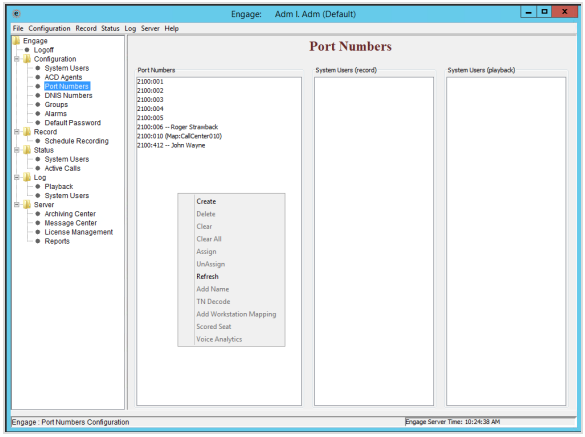
5.4 Assign Port Mapping to Engage Port Numbers

Once port mapping has been completed (by Bulk Port Mapping or individually), assign the contents of the **port mapping** in the**VoIP Configuration** to **Port Numbers** in the Engage Recorder.

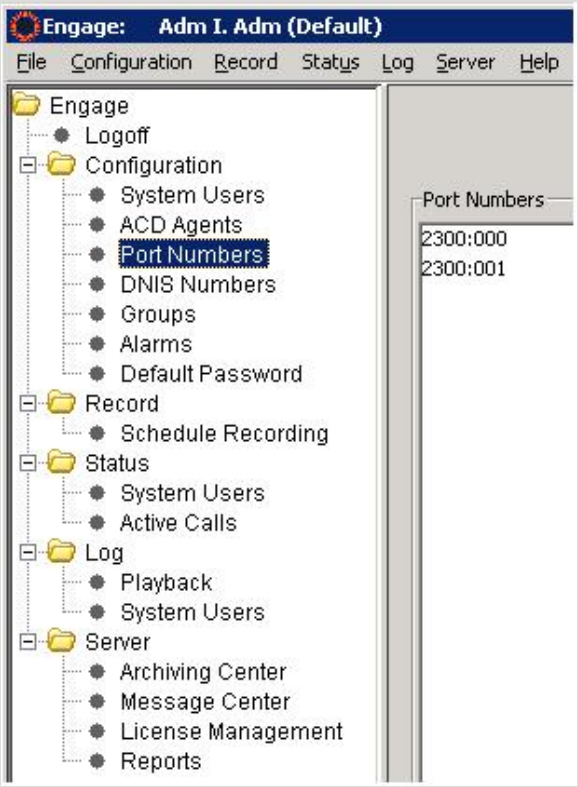
In Engage, **port numbers** consist of the Recording Board ID (2300 for ACM) and a Recording Channel number (000 – 999). An example would be Port Number 2300:001.

To assign Engage port numbers to VoIP port mapping, perform the following:

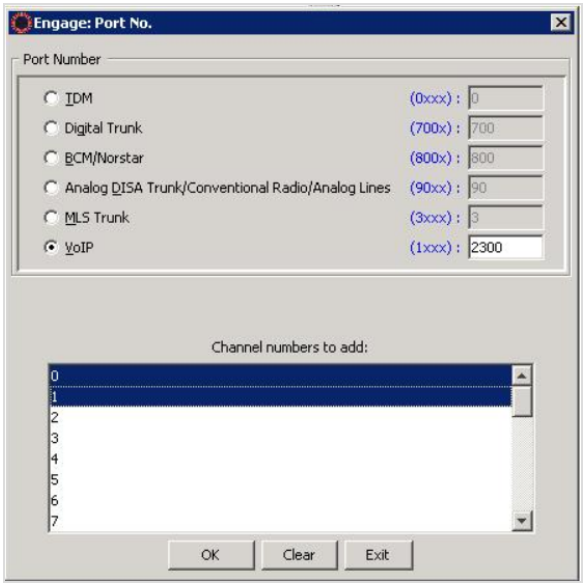
1. Launch the Engage JAVA Client



2. Click on **Port Numbers** and the **Port Numbers** window appears.

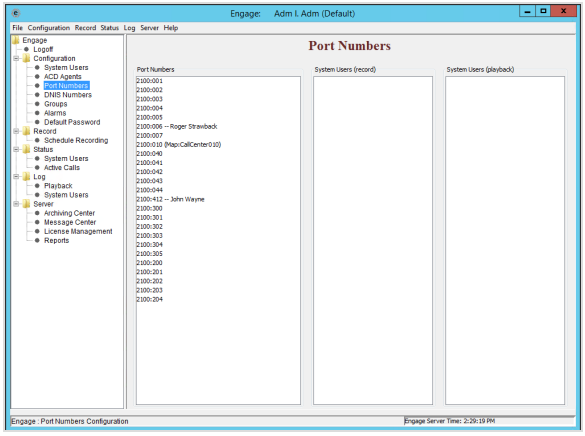


3. Right click in the **Port Numbers** column and the **Engage Port No.** Window appears.



4. In the **Engage: Port No**. window, click the ***VoIP*** radio button and the 2300 board ID populates.

5. Go to the **Channel numbers to add** box. Scroll down and highlight the first channel number to be used (by clicking on it) and press ctrl and click on ALL of the ports to be assigned. They will highlight, as well (ex. 0 through 1 are highlighted).
6. When done Clicking, click ***OK***. The **Add Port Number – Successful** box appears. Click ***Exit*** to close.

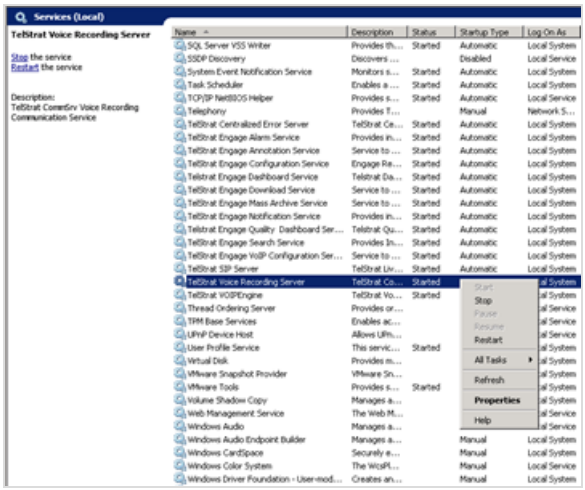


7. Go to the **Port Numbers** window and check that assigned ports are now listed in the Port Numbers area. Engage Port Numbers for an Avaya ACM deployment will always consists of Recording Board ID of 2300 and any number of channels, numbered 000 through 999.

6 When To Restart

After making major system configuration changes on the Engage Server, it is necessary to stop, then restart the Engage Server.

- When not to Restart: Adding, modifying, or deleting port mapping data can occur without restarting the server.
- When to Restart: System settings (CTI Option, CTI Server name, Calls to Record setting) require a restart of the server to take effect.



If a Restart of the Engage Voice Recorder server is needed, do the following:

1. Open **Services** on the Engage Voice Recording Server.
2. Scroll down to the *TelStrat Voice Recording Server Service*.
3. Right-click on *TelStrat Voice Recording Server Service* to get the pop-up menu and Click ***Stop***.
4. Wait 10 seconds, and then click on ***Start*** to start the service.

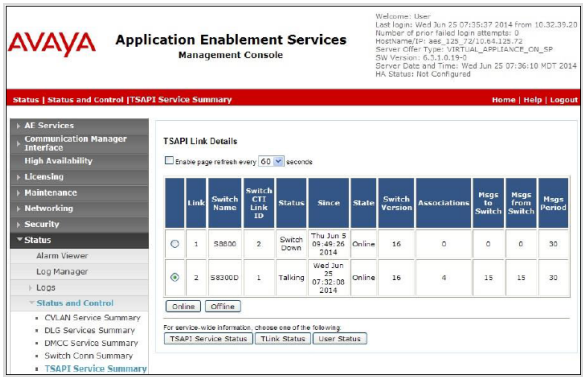
7 Review Status and Connections

To check the connection status of the ACM:

1. On the AES console, go to ***Status and Control >> TSAPI Services Summary***.
2. Click on the radio button next to the link number associated with Engage.

- Click ***TSAPI Service Status*** to view current status of the TSAPI service.
- Click ***Tlink Status*** to view status of the CTI link to the Engage server.
- Click ***User Status*** to view status of the Engage AES user.

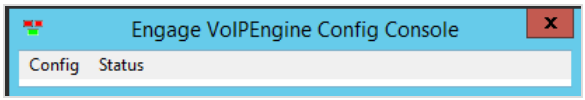
NOTE: If the services is any state but ONLINE, this could be a cause for Engage to not be recording.



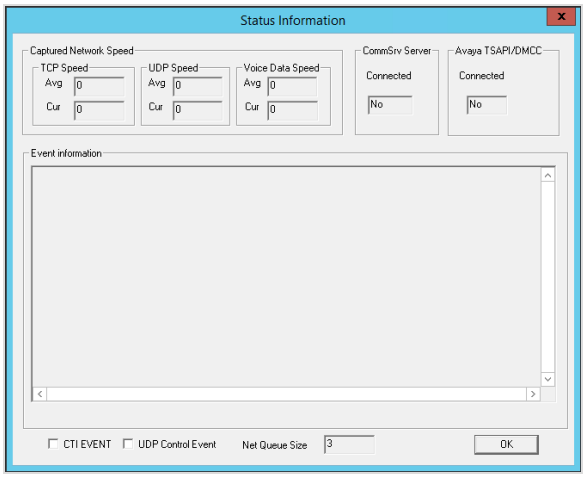
To check connection status on Engage:

To review the status of the Engage Voicer Recorder and its connection to the CS1000 system:

1. Logon to the Engage Voice Recorder server.
2. From the ***Start*** menu, launch the ***Engage VoIPEngine Console*** utility.



3. On the menu bar, click on the ***Status*** command and the **Status Information** window displays:



4. Review the following field descriptions:

Field	***Description***
Captured Network Speed Window	The following fields display the average and network speeds captured by the IP Telephone MLS Configuration application.
TCP Speed	This field displays the average and current speed of the Transmission Control Protocol (TCP).
UDP Speed	This field displays the average and current speed of the User Datagram Protocol (UDP).
Voice Data Speed	This field displays the average and current speed of the voice data.
CommSrv Server Connected Window	This field displays whether or not the Engage server is connected. Valid values are Yes and No.
Avaya TSAPI / DMCC Connected Window	This field displays whether or not the Avaya TSAPI or DMCC server is connected. Valid values are Yes and No.
Event Information Window	This window displays the events taking place. An example is *Successful Connect to CommSrv*.
CTI Event checkbox	Click the **CTI Event** checkbox to display CTI event information in the *Event Information* window.
UDP Control Event checkbox	Click the **UDP Control Event** check box to display the UDP control event information in the *Event Information* window.
Net Queue Size Win-	This field displays the network queue size.

dow	

END OF DOCUMENT