



Avaya Solution & Interoperability Test Lab

Application Notes for Startel Call Manager Center with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Startel Call Manager Center (CMC) to monitor and control calls placed to and from stations and agents on Avaya Communication Manager.

Startel CMC is a Call Center selective and compliance call control and monitoring system. As the call comes into agent phone, the agent can control the phone for transfer, conference, and hold. The system interfaces with Avaya Communication Manager through Avaya Application Enablement Services (AES), using the Telephony Services Application Programming Interface (TSAPI) to collect important Computer Telephony Integration (CTI) information like agent events and user data.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) and Startel CMC. Startel CMC uses TSAPI with an Avaya AES server to monitor stations and/or agents, and call information.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide a T1/ISDN-PRI trunk between two Avaya Communication Manager systems.

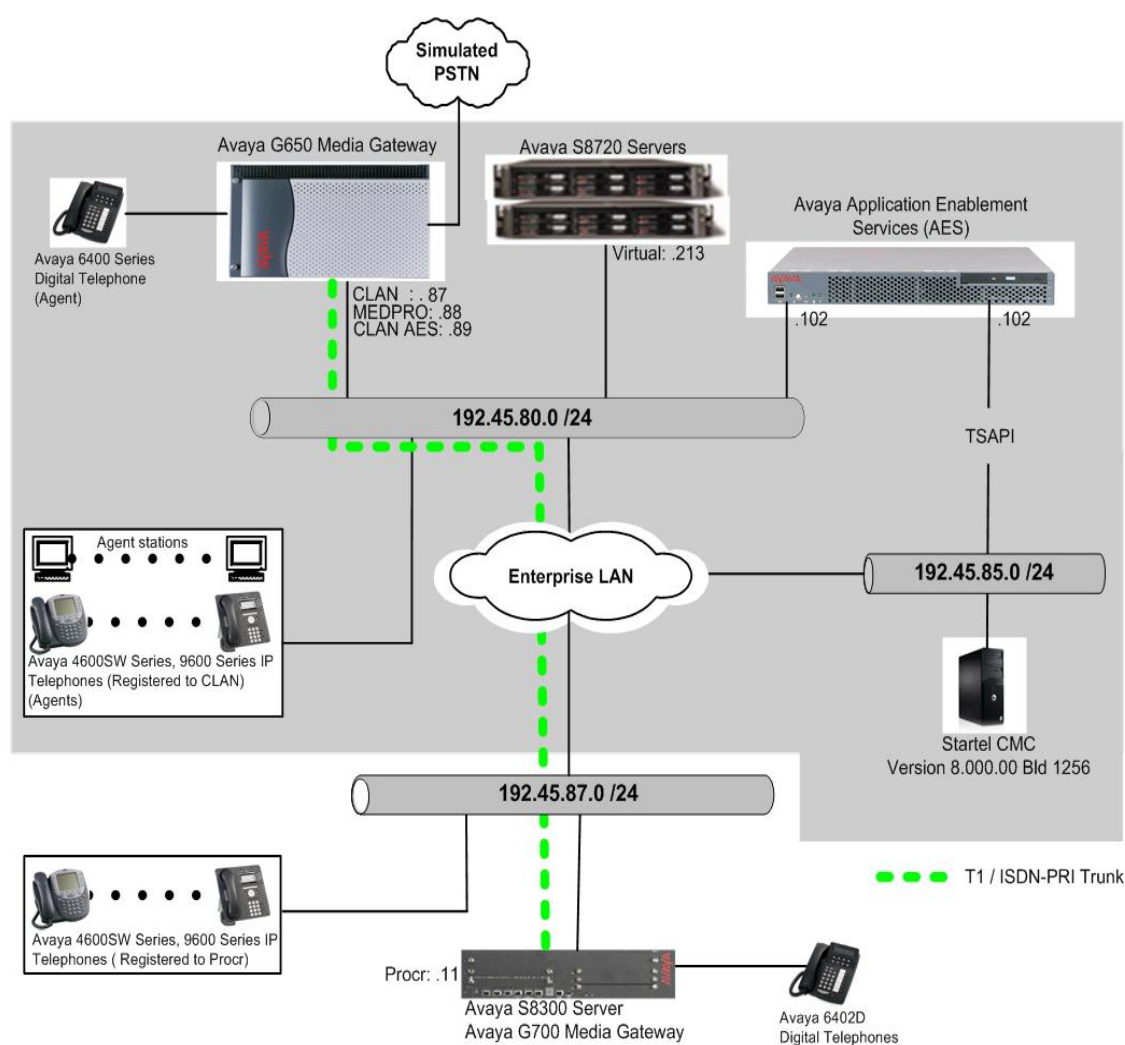


Figure 1: Sample Test Configuration for the Startel CMC Solution

2. Equipment and Software Validated

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

| Equipment | | Software/Firmware |
|---|------------------------------|--|
| Avaya S8720 Server | | Avaya Communication Manager 5.0 (R015x.00.0.825.4) |
| Avaya G650 Media Gateway | | - |
| | TN2312BP IP Server Interface | HW11 FW030 |
| | TN799DP C-LAN Interface | HW20 FW017 |
| | TN2302AP IP Media Processor | HW01 FW108 |
| Avaya S8300 Server with Avaya G700 Media Gateway | | Avaya Communication Manager 5.0 (R015x.00.0.825.4) |
| Avaya Application Enablement Services Server | | R4.1.31.2 |
| Avaya 4600 Series IP Telephones | | |
| | 4620SW (H.323) | 2.8 |
| | 4625SW (H.323) | 2.8 |
| Avaya 9600 Series IP Telephones | | |
| | 9630 (H.323) | 1.5 |
| | 9650 (H.323) | 1.5 |
| Avaya IP Agent | | 7.0.15.86 |
| Avaya 6408D+ Digital Telephone | | - |
| Startel CMC Server on Windows Microsoft 2003 Server with Service Pack 2 | | 8.000.00 Bld 1256 |

3. Configure Avaya Communication Manager

This section provides the procedures for configuring a switch connection and Computer Telephony Integration (CTI) links, hunt/skill groups, vectors, Vector Directory Numbers (VDN), agents, agent login/logoff codes, and monitored stations on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

3.1. Configure Switch Connection and CTI Links between Avaya Communication Manager and Avaya Application Enablement Services

The Avaya AES server forwards CTI requests, responses, and events between Startel CMC and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over a switch connection link. Within the switch connection link, CTI links may be configured to provide CTI services to CTI applications such as Startel CMC. The following steps demonstrate the configuration of the Avaya Communication Manager side of the switch connection and CTI links. See **Section 4** for the details of configuring the AES side of the switch connection and CTI links.

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid Extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to **ADJ-IP**, and assign a descriptive Name to the CTI link.

| add cti-link 4 | | Page 1 of 2 |
|------------------|--|-------------|
| CTI Link: 4 | | CTI LINK |
| Extension: 20006 | | |
| Type: ADJ-IP | | |
| Name: TSAPI | | COR: 1 |

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoint (Avaya IP Telephones and IP Softphones, and AES monitored stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

| change node-names ip | | Page 1 of 2 |
|----------------------|---------------|---------------|
| | | IP NODE NAMES |
| Name | IP Address | |
| CLAN | 192.45.80.87 | |
| CLAN-AES | 192.45.80.89 | |
| MEDPRO | 192.45.80.88 | |
| MEDPRO2 | 192.45.80.161 | |
| S8300G700 | 192.45.87.11 | |
| default | 0.0.0.0 | |
| procr | 192.45.80.214 | |

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was utilized for the Local Port field.

| change ip-services | | | | | | Page 1 of 4 |
|--------------------|---------|------------|------------|-------------|-------------|-------------|
| | | | | | | IP SERVICES |
| Service Type | Enabled | Local Node | Local Port | Remote Node | Remote Port | |
| AESVCS | y | CLAN-AES | 8765 | | | |

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname -a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 4.1**.

| change ip-services | | | | | Page 4 of 4 |
|--------------------|--------------------|--------------------|---------|--------|----------------------------|
| | | | | | AE Services Administration |
| Server ID | AE Services Server | Password | Enabled | Status | |
| 1: | AES | xxxxxxxxxxxxxxxxxx | y | idle | |
| 2: | | | | | |
| 3: | | | | | |

3.2. Hunt/Skill Groups, Agent Logins, and Call Vectoring

Enter the **display system-parameters customer-options** command. On **Page 6**, verify that the ACD, Expert Agent Selection (EAS) and Vectoring (Basic) fields are set to **y**. If not, contact an authorized Avaya account representative to obtain these licenses.

```
display system-parameters customer-options                               Page 6 of 11
CALL CENTER OPTIONAL FEATURES

Call Center Release: 3.0

ACD? y                                                                    Reason Codes? n
BCMS (Basic)? y                                                            Service Level Maximizer? n
BCMS/VuStats Service Level? n                                              Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? n   Service Observing (Remote/By FAC)? y
Business Advocate? n                                                         Service Observing (VDNs)? n
Call Work Codes? n                                                         Timed ACW? N

DTMF Feedback Signals For VRU? n                                           Vectoring (Basic)? y
Dynamic Advocate? n                                                         Vectoring (Prompting)? n
Expert Agent Selection (EAS)? y      Vectoring (G3V4 Enhanced)? n
EAS-PHD? n                                                                Vectoring (3.0 Enhanced)? n
Forced ACD Calls? n                                                         Vectoring (ANI/II-Digits Routing)? n
Least Occupied Agent? n                                                     Vectoring (G3V4 Advanced Routing)? n
Lookahead Interflow (LAI)? n                                               Vectoring (CINFO)? n
Multiple Call Handling (On Request)? n   Vectoring (Best Service Routing)? n
Multiple Call Handling (Forced)? n      Vectoring (Holidays)? n
PASTE (Display PBX Data on Phone)? n   Vectoring (Variables)? n
(NOTE: You must logoff & login to effect the permission changes.)
```

Once the Expert Agent Selection (EAS) field is set to **y**, from the previous step, enter the **change system-parameters features** command. On **Page 11**, verify that the Expert Agent Selection (EAS) Enabled field is set to **y**. To enable the EAS feature, the Expert Agent Selection field in both system-parameters customer-options and system-parameters features pages should be set to **y**.

```
change system-parameters features                                       Page 11 of 18
FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
EAS
Expert Agent Selection (EAS) Enabled? y
Minimum Agent-LoginID Password Length:
Direct Agent Announcement Extension: Delay:
Message Waiting Lamp Indicates Status For: station

VECTORIZING
Converse First Data Delay: 0 Second Data Delay: 2
Converse Signaling Tone (msec): 100 Pause (msec): 30
Prompting Timeout (secs): 10

Reverse Star/Pound Digit For Collect Step? n

Store VDN Name in Station's Local Call Log? y
SERVICE OBSERVING
Service Observing: Warning Tone? y or Conference Tone? n
Service Observing Allowed with Exclusion? n
Allow Two Observers in Same Call? y
```

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the HUNT GROUP form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan. Set the ACD, Queue, and Vector fields to **y**. When ACD is enabled, hunt group members serve as ACD agents and must log in to receive ACD split/skill calls. When Queue is enabled, calls to the hunt group will be served by a queue. When Vector is enabled, the hunt group will be vector controlled.

| | | | |
|--------------------------|-------|---------------------------|--|
| add hunt-group 1 | | Page 1 of 3 | |
| HUNT GROUP | | | |
| Group Number: 1 | | ACD? y | |
| Group Name: test | | Queue? y | |
| Group Extension: 50011 | | Vector? y | |
| Group Type: ucd-mia | | | |
| TN: 1 | | | |
| COR: 1 | | MM Early Answer? n | |
| Security Code: | | Local Agent Preference? n | |
| ISDN/SIP Caller Display: | | | |
| Queue Limit: unlimited | | | |
| Calls Warning Threshold: | Port: | | |
| Time Warning Threshold: | Port: | | |

On **Page 2**, set the Skill field to **y**, which means that agent membership in the hunt group is based on skills, rather than pre-programmed assignment to the hunt group.

| | | | |
|---|--|-------------|--|
| add hunt-group 1 | | Page 2 of 3 | |
| HUNT GROUP | | | |
| Skill? y | | | |
| AAS? n | | | |
| Measured: internal | | | |
| Supervisor Extension: | | | |
| Controlling Adjunct: none | | | |
| VuStats Objective: | | | |
| Redirect on No Answer (rings): | | | |
| Redirect to VDN: | | | |
| Forced Entry of Stroke Counts or Call Work Codes? n | | | |

Enter the **add agent-loginID p** command, where **p** is a valid extension in the provisioned dial plan. On **Page 1** of the agent-loginID form, enter a descriptive Name and Password.

| add agent-loginID 50021 | | Page 1 of 2 | |
|---|---|-------------|--|
| AGENT LOGINID | | | |
| Login ID: 50021 | AAS? n | | |
| Name: Agent-1 | AUDIX? n | | |
| TN: 1 | LWC Reception: spe | | |
| COR: 1 | LWC Log External Calls? n | | |
| Coverage Path: | AUDIX Name for Messaging: | | |
| Security Code: | LoginID for ISDN/SIP Display? n | | |
| | Password: | | |
| | Password (enter again): | | |
| | Auto Answer: station | | |
| | MIA Across Skills: system | | |
| | ACW Agent Considered Idle: system | | |
| | Aux Work Reason Code Type: system | | |
| | Logout Reason Code Type: system | | |
| | Maximum time agent in ACW before logout (sec): system | | |
| | Forced Agent Logout Time: : | | |
| WARNING: Agent must log in again before changes take effect | | | |

On **Page 2**, set the Skill Number (SN) to the hunt group number previously created. The Skill Level (SL) may be set according to customer requirements.

Repeat this step as necessary to configure additional agent extensions.

| add agent-loginID 50021 | | Page 2 of 2 | |
|---------------------------------------|----|--------------------------|-----|
| AGENT LOGINID | | | |
| Direct Agent Skill: | | | |
| Call Handling Preference: skill-level | | Local Call Preference? n | |
| SN | SL | SN | SL |
| 1: 1 | 1 | 16: | |
| 2: | | 31: | 46: |
| | | 32: | 47: |

Enter the **change vector q** command, where **q** is an unused vector number. Enter a descriptive Name, and program the vector to deliver calls to the hunt/skill group number. Agents that are logged into the hunt/skill group will be able to answer calls queued to the hunt/skill group.

| change vector 1 | | Page 1 of 3 | |
|-----------------|-----------------------|-------------------|------------------|
| CALL VECTOR | | | |
| Number: 1 | Name: Queue to skill1 | | |
| Basic? y | EAS? y | G3V4 Enhanced? n | Meet-me Conf? n |
| Prompting? n | LAI? n | G3V4 Adv Route? n | ANI/II-Digits? n |
| Variables? n | 3.0 Enhanced? n | CINFO? n | BSR? n |
| 01 wait-time | 2 secs | hearing ringback | Lock? n |
| 02 queue-to | skill 1 | pri m | ASAI Routing? y |
| 03 | | | Holidays? n |

Enter the **add vdn r** command, where **r** is an extension valid in the provisioned dial plan. Specify a descriptive Name for the VDN and the **Vector Number** configured in the previous step. In the example below, incoming calls to extension 50000 will be routed to testVDN50000, which in turn will invoke the actions specified in vector 1.

```

add vdn 50000                                     Page 1 of 2
                                         VECTOR DIRECTORY NUMBER

                                         Extension: 50000
                                         Name*: testVDN50000
                                         Vector Number: 1

Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none

1st Skill*:
2nd Skill*:
3rd Skill*:

```

Enter the **change feature-access-codes** command. Define the Auto-In Access Code, Login Access Code, Logout Access Code, and Aux Work Access Code.

```

change feature-access-codes                       Page 5 of 6
                                         FEATURE ACCESS CODE (FAC)

                                         Automatic Call Distribution Features

                                         After Call Work Access Code: 120
                                         Assist Access Code: 121
                                         Auto-In Access Code: 122
                                         Aux Work Access Code: 123
                                         Login Access Code: 124
                                         Logout Access Code: 125
                                         Manual-in Access Code: 126
                                         Service Observing Listen Only Access Code: 127
                                         Service Observing Listen/Talk Access Code: 128
                                         Add Agent Skill Access Code: 130

```

Enter the **add abbreviated-dialing group g** command, where **g** is the number of an available abbreviated dialing group. In the DIAL CODE list, enter the Feature Access Codes, created previously, for ACD Login and Logout.

```

add abbreviated-dialing group 1                 Page 1 of 1
                                         ABBREVIATED DIALING LIST

                                         Group List: 1          Group Name: Call Center
                                         Size (multiple of 5): 5    Program Ext:          Privileged? n

DIAL CODE
11: 124
12: 125
13:

```


3.3. Configure Stations

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, specify the Security Code, and make sure that the IP Softphone field is set to **y**. For the compliance test, stations from 22001 to 22009 were utilized for monitoring purpose.

| | | | |
|---------------------------|------------------|---------------------------------|--|
| add station 22001 | | Page 1 of 5 | |
| STATION | | | |
| Extension: 22001 | Lock Messages? n | BCC: 0 | |
| Type: 4620 | Security Code: * | TN: 1 | |
| Port: IP | Coverage Path 1: | COR: 1 | |
| Name: Record-1 | Coverage Path 2: | COS: 1 | |
| Hunt-to Station: | | | |
| STATION OPTIONS | | | |
| Loss Group: 19 | | Time of Day Lock Table: | |
| | | Personalized Ringing Pattern: 1 | |
| Speakerphone: 2-way | | Message Lamp Ext: 22001 | |
| Display Language: english | | Mute Button Enabled? y | |
| Survivable GK Node Name: | | Expansion Module? n | |
| Survivable COR: internal | | Media Complex Ext: | |
| Survivable Trunk Dest? y | | IP SoftPhone? y | |
| | | IP Video Softphone? n | |
| | | Customizable Labels? y | |

On **Page 4** of the STATION form, for ABBREVIATED DIALING List 2, enter the abbreviated dialing group configured in **Section 3.3**. Configure the following **BUTTON ASSIGNMENTS**:

- auto-in
- aux-work
- abrv-dial – for Login
- abrv-dial – for Logout.

| | | | |
|---------------------|----------------|----------------|--|
| add station 22001 | | Page 4 of 5 | |
| STATION | | | |
| SITE DATA | | | |
| Room: change sta | | Headset? n | |
| Jack: | | Speaker? n | |
| Cable: SITE | | Mounting: d | |
| Floor: | | Cord Length: 1 | |
| Building: | | Set Color: | |
| ABBREVIATED DIALING | | | |
| List1: personal 1 | List2: group 1 | List3: system | |
| BUTTON ASSIGNMENTS | | | |
| 1: call-appr | 5: auto-in | Grp: 1 | |
| 2: call-appr | 6: aux-work | RC: Grp: 1 | |
| 3: call-appr | 7: abrv-dial | List: 2 DC: 11 | |
| 4: | 8: abrv-dial | List: 2 DC: 12 | |

4. Configure Avaya Application Enablement Services

The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

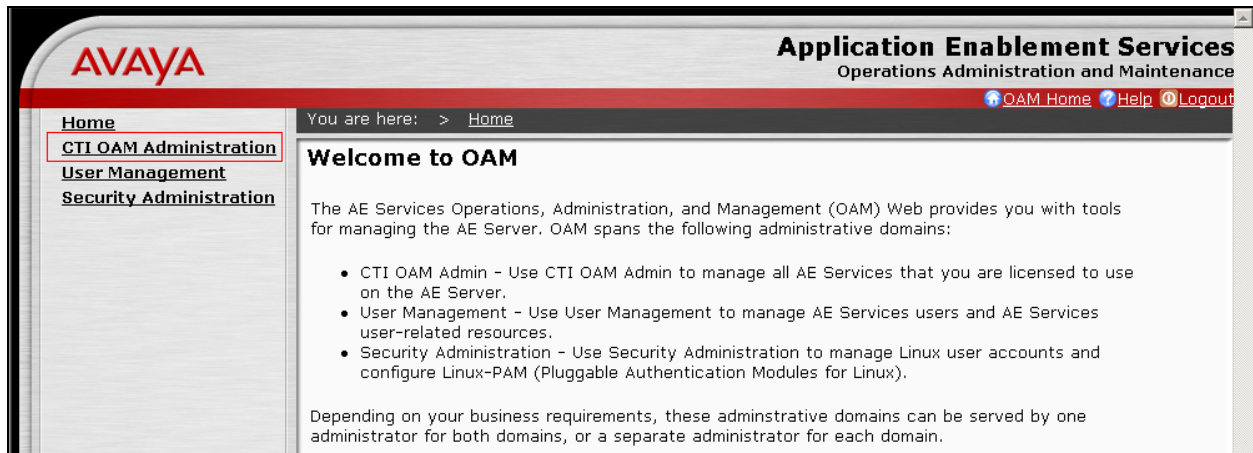
This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, and creating a CTI link for TSAPI.

4.1. Configure Switch Connection

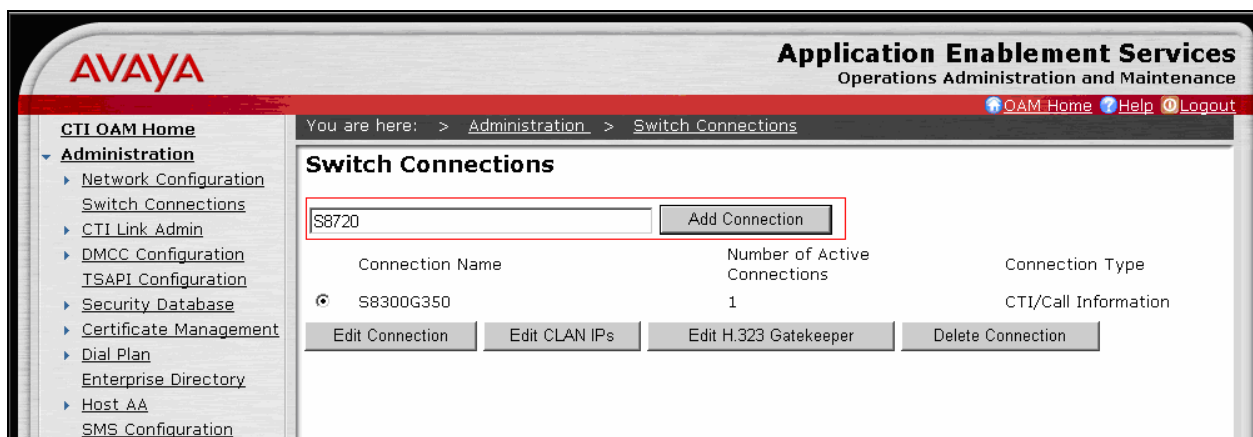
Launch a web browser, enter <https://<IP address of AES server>:8443/MVAP> in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.



Select the **CTI OAM Administration** link from the left pane of the screen.



Click on **Administration** → **Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 3.1**. Default values may be used in the remaining fields. Click on **Apply**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

Set Password - S8720

Please note the following:
 * A password is not required for a H323 Gatekeeper Connection.
 * Changing the password affects only new connections, not open connections.

Switch Connection Type: CTI/Call Information

Switch Password: [Redacted]

Confirm Switch Password: [Redacted]

SSL: ☒

Apply Cancel

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.

AVAYA Application Enablement Services
Operations Administration and Maintenance

You are here: > Administration > Switch Connections

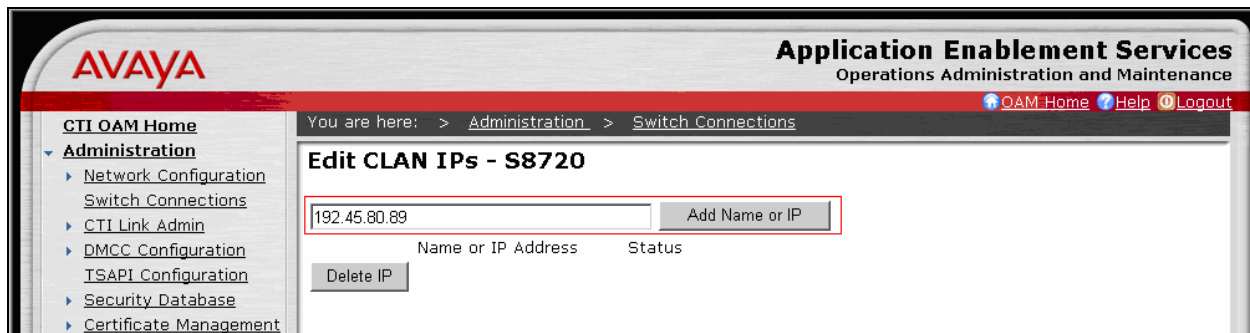
Switch Connections

[Add Connection]

| Connection Name | Number of Active Connections | Connection Type |
|--|------------------------------|----------------------|
| <input type="radio"/> S8300G350 | 1 | CTI/Call Information |
| <input checked="" type="radio"/> S8720 | 0 | CTI/Call Information |

Edit CLAN IPs Edit Connection Edit H.323 Gatekeeper Delete Connection

Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 3.1** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

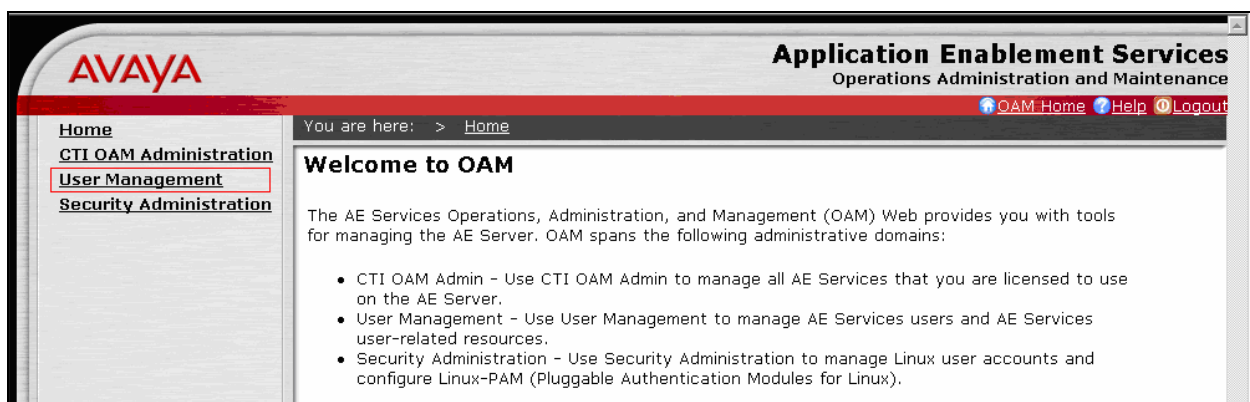


4.2. Configure the CTI Users

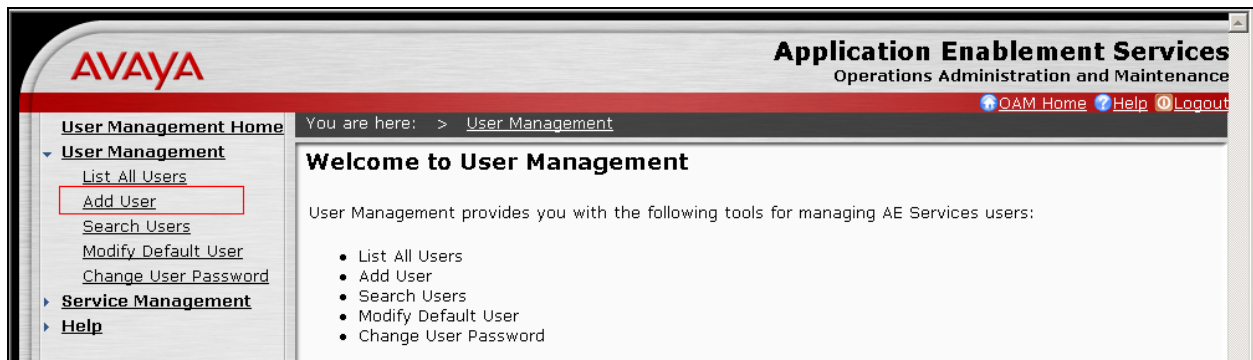
The steps in this section describe the configuration of a CTI user. Launch a web browser, enter <https://<IP address of AES server>:8443/MVAP> in the URL, and log in with the appropriate credentials to access the relevant administration pages.



The Welcome to OAM page is displayed next. Select **User Management** from the left pane.



From the Welcome to User Management page, navigate to the **User Management → Add User** page to add a CTI user.



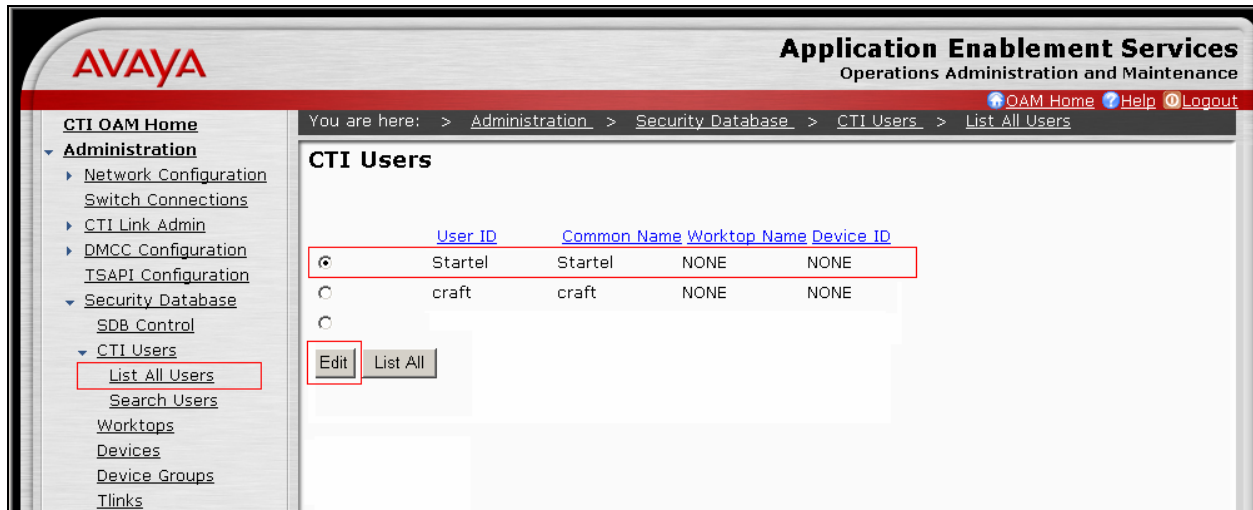
On the Add User page, provide the following information:

- User Id
- Common Name
- Surname
- User Password
- Confirm Password

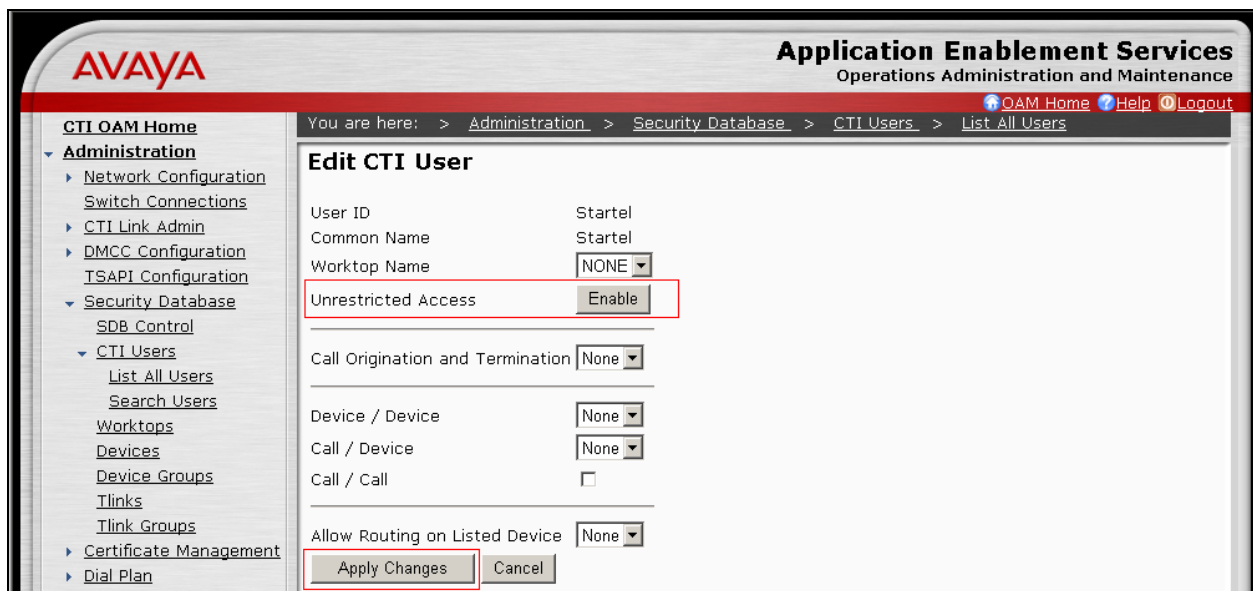
The above information (User ID and User Password) must match with the information configured in Startel CMC Configuration page in **Section 5**.

Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Click the **Apply** button (not shown) at the bottom of the screen to complete the process. Default values may be used in the remaining fields.

Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Administration → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.

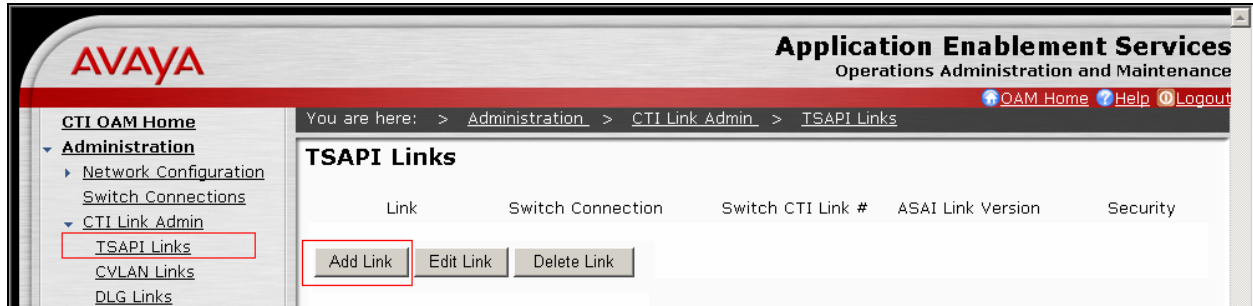


Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.

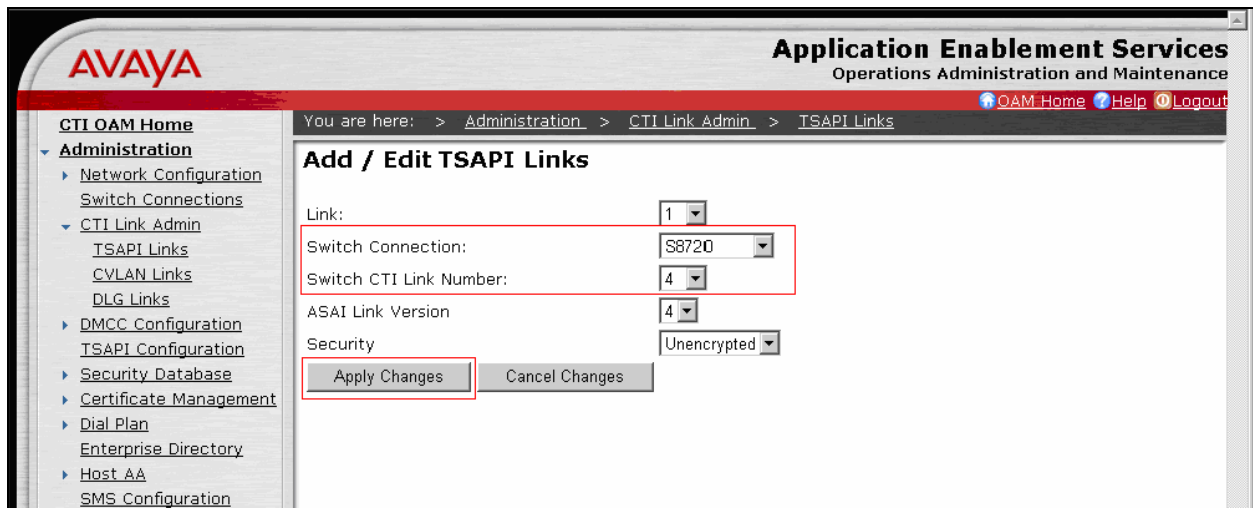


4.3. Configure the TSAPI CTI Link

Navigate to the **OAM Home** → **CTI OAM Admin** → **Administration** → **CTI Link Admin** → **TSAPI Links** page to set the TSAPI CTI Link. Click on **Add Link**.



Select a Switch Connection using the drop down menu. The Switch Connection is configured in **Section 4.1**. Select the Switch CTI Link Number using the drop down menu. Switch CTI Link Number should match with the number configured in the cti-link form in **Section 3.1**. Click the **Apply Changes** button. Default values may be used in the remaining fields.



5. Configure Startel CMC

Startel installs, configures, and customizes the Startel CMC application for their end customers. This section only describes the interface configuration for the Startel CMC application to communicate with Avaya AES and Avaya Communication Manager.


Refer to [3] for configuring the Startel CMC application. For more information on the Startel CMC configuration, contact Startel Technical Support.

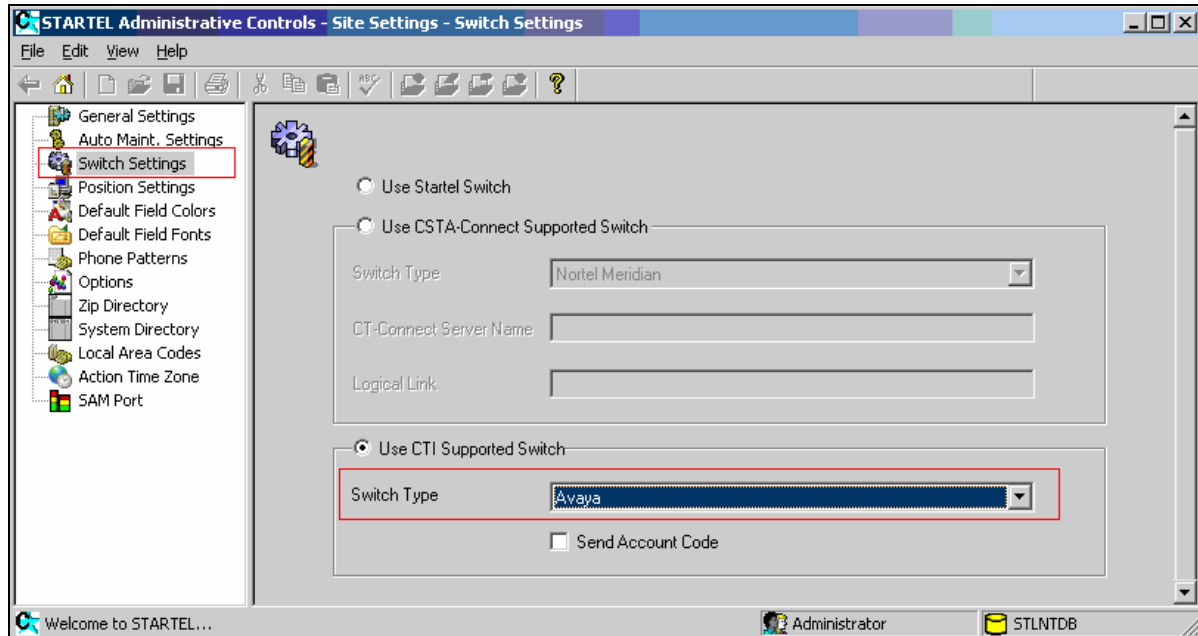
The following screen shows the tslib.ini file in the C:\WINNT directory. In this file, the Avaya AES server IP address and TSAPI port is configured.

```
-----  
[Telephony Servers]  
192.45.85.102=450  
  
; This is a list of the servers offering Telephony Services via TCP/IP.  
; Either domain name or IP address may be used; default port number is 450  
; The form is: host_name=port_number For example:  
;  
;  
; tserver.mydomain.com=450  
; 127.0.0.1=450  
;  
;  
[Shared Admin]  
  
; Instead of each workstation maintaining its own list of servers, a shared  
; tslib.ini file may be placed on a network file system, for example:  
;  
;  
; tslib.ini=n:\csta\tslib.ini
```

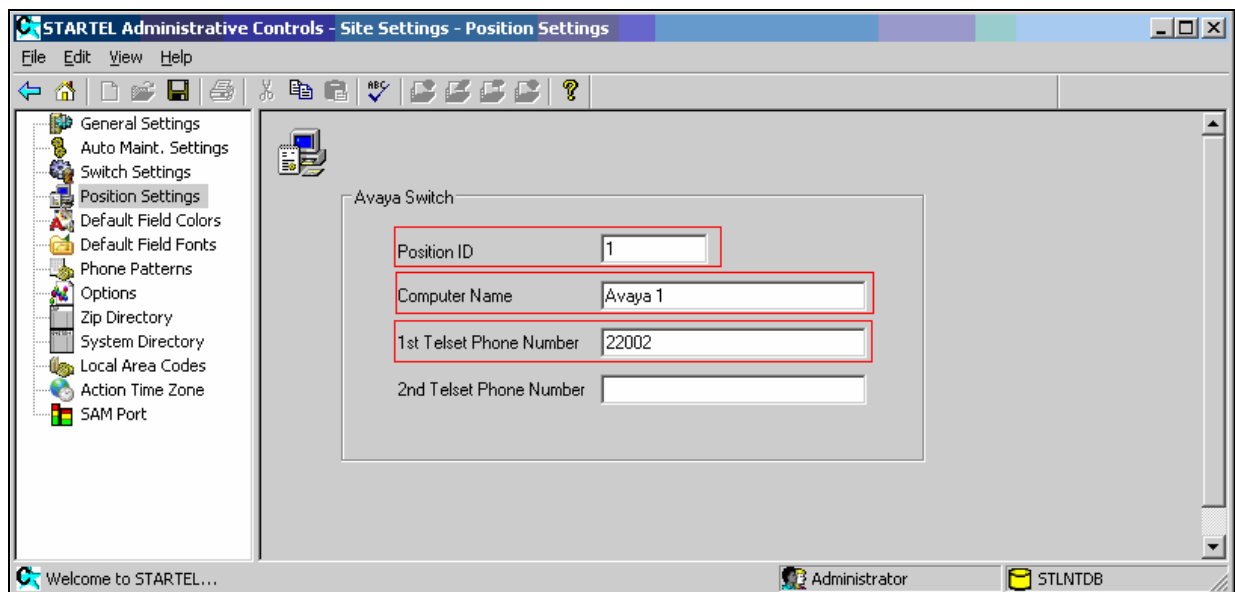
The following screen shows the STLCTISvc.cfg file in the c:\Startel\CTI Srv directory. In this file, the Tlink name (SERVERID) and credentials (USER and PASSWORD) are configured. The Tlink name can be obtained by navigating to **CTI OAM Home → Administration → Security Database → Tlinks** in Avaya AES.

```
[ODBC]  
DSN = STLNTDB  
USER = startelopr  
PASSWORD = 1letrats  
  
[TSERVER]  
SERVERID = AVAYA#S8720#CSTA#AES  
USER = Startel  
PASSWORD = Startel123&  
  
[CHARGEACCOUNT]  
ACCESSCODE = *50  
OUTDIALACCESSCODE =  
  
[INITIALMONITORDEVICES]  
50011  
  
Startel Administrative Controls  
  
Logon Credentials  
Logon---Administrator  
P/W---ADMIN
```

Click the **Startel Administrative Console** icon,  from the Windows Desktop Console to start the application. In the Startel Administrative Console, navigate to **Site Settings → Switch Settings**. Ensure the **Use CTI Supported Switch** option button is selected, and **Avaya** is selected in the Switch Type drop-down list. Save any change.

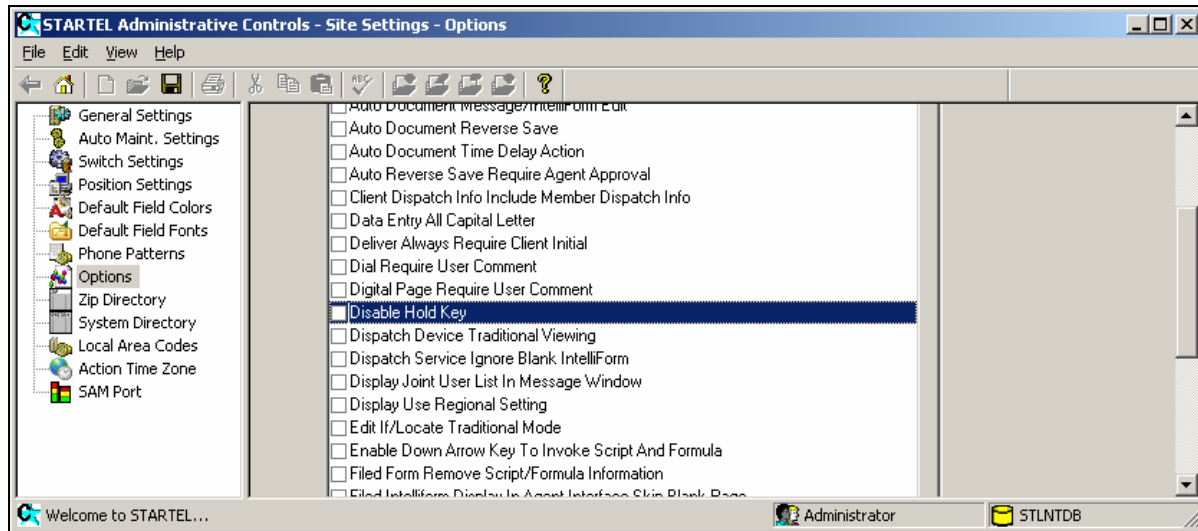


In the Site Settings window, select **Position Settings**, and provide PositionID, a descriptive name for the Computer Name field, and monitored extension for the 1st Telset Phone Number field. The 1st Telset Phone number is the Avaya extension number for the device on the agent's station. Save the entry. This step will map between the monitored extension, and the Position ID. Repeat this step configure additional Mapping between monitored extensions, and Position IDs



In the Site Settings window, select **Options**. Ensure the **Disable Hold Key** is not checked.

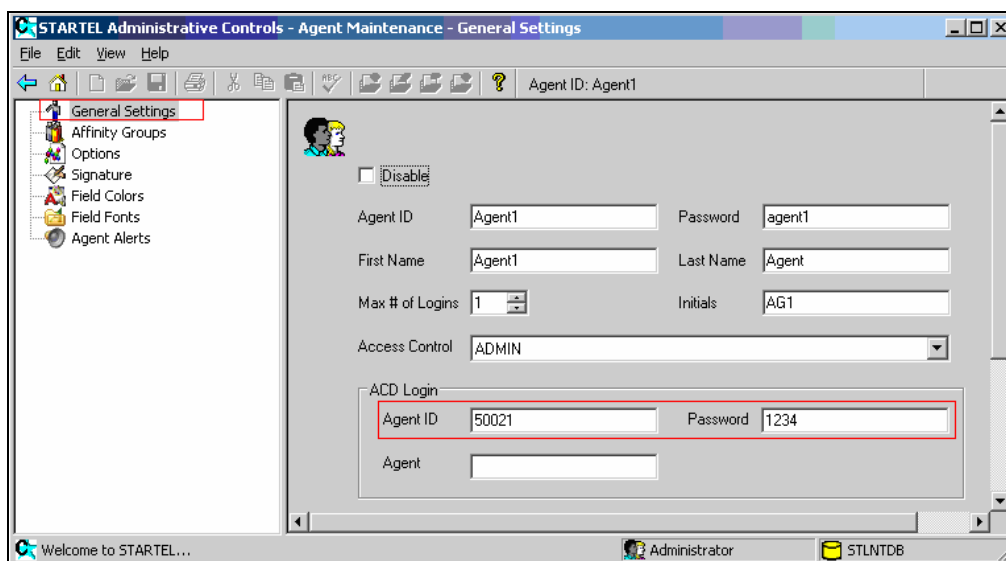
NOTE: If the key is checked, the agent may not be able to place a call on hold, conference calls, and transfer calls. Save your entries.




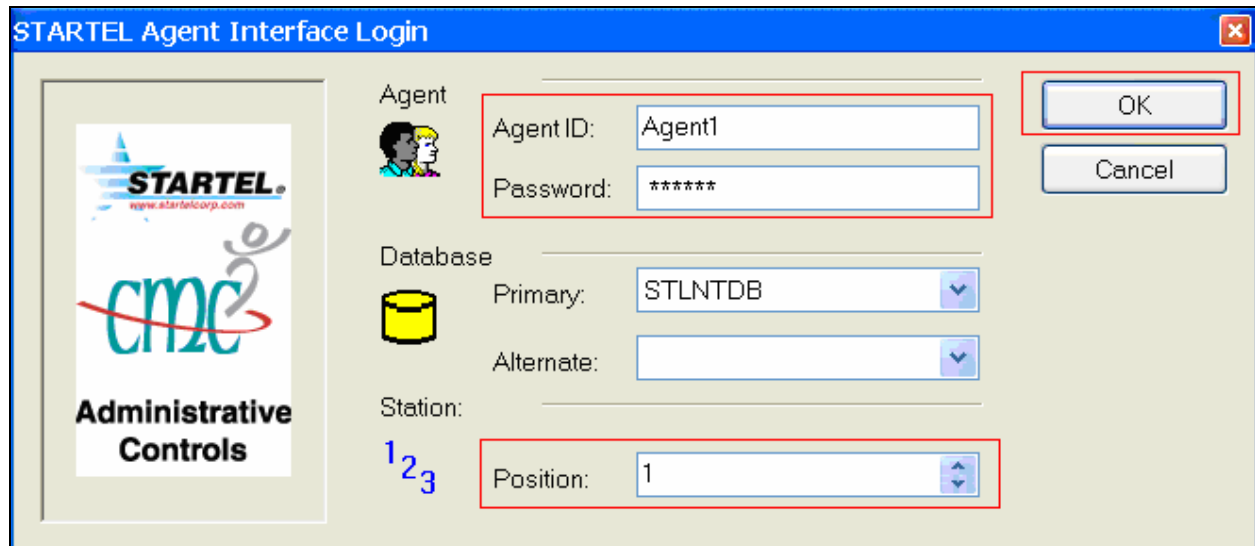
In the Startel Administrative Console, navigate to **Agent Maintenance → General Settings**, and provide the following information in the ACD Login section:

- In the Agent ID field under the ACD Login section, enter Avaya Agent ID created in **Section 3.2**.
- In the Password field under the ACD Login section, enter the Avaya password associated with the Agent ID created in **Section 3.2**.

NOTE: The Agent ID and Password in the upper section are for the Startel CMC login. The Agent ID and Password in the lower section are for the Avaya ACD login.



Click the **Startel Agent Interface** icon,  from the Windows Desktop Console to access Startel Agent Interface Login window. In the Startel Agent Interface Login window, provide **Agent ID**, **Password** (CMC password), and **Position**. Click on the **OK** button. This step will map between the Startel CMC agent ID, and the position.



The image shows the 'STARTEL Agent Interface Login' window. On the left is a logo for 'STARTEL Administrative Controls' with the website 'www.startelcorp.com'. The main area has three sections: 'Agent' with fields for 'Agent ID' (containing 'Agent1') and 'Password' (containing '*****'); 'Database' with 'Primary' set to 'STLNTDB' and an empty 'Alternate' field; and 'Station' with a 'Position' dropdown set to '1'. There are 'OK' and 'Cancel' buttons on the right. Red boxes highlight the Agent ID/Password fields, the Position dropdown, and the OK/Cancel buttons.

6. Interoperability Compliance Testing

The interoperability compliance test included feature, serviceability, and performance testing. The feature testing evaluated the ability of Startel CMC to control and monitor calls placed to and from stations and agents. The serviceability testing introduced failure scenarios to see if Startel CMC can resume monitoring after failure recovery. The performance testing stressed Startel CMC by continuously placing calls over extended periods of time.

6.1. General Test Approach

The general approach was to place various types of calls to and from stations, agents, and to a VDN, and control and monitor them using Startel CMC. For feature testing, the types of calls included internal calls, inbound and outbound trunk calls, transferred calls, hold calls, and conferenced calls. Performance tests verified that Startel CMC could monitor calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES. In the Startel CMC application, the TSAPI log was utilized for verification

7.1. Verify Avaya Communication Manager

Verify the status of the administered AES link by using the **status aesvcs link** command.

```
status aesvcs link
```

| AE SERVICES LINK STATUS | | | | | | |
|-------------------------|-----------------------|-----------------|----------------|------------|--------------|--------------|
| Srvr/ Link | AE Services Server | Remote IP | Remote Port | Local Node | Msgs Sent | Msgs Rcvd |
| 01/01 | AES | 192. 45. 80.102 | 36538 | CLAN-AES | 17 | 18 |

Verify the Service State field of the administered TSAPI CTI link is in **established** state, by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link
```

| AE SERVICES CTI LINK STATUS | | | | | | |
|-----------------------------|---------|-------------|-----------------------|------------------|--------------|--------------|
| CTI Link | Version | Mnt Busy | AE Services Server | Service State | Msgs Sent | Msgs Rcvd |
| 2 | | no | AES | restarting | 15 | 15 |
| 4 | 4 | no | AES | established | 15 | 15 |

7.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify that the status of the TSAPI service is ONLINE, by selecting **Status and Control** → **Services Summary** from the left pane. The following screen shows a sample Services Summary.

| Service | Status | Since | Cause |
|---------------|--------|---------------------|--------|
| CVLAN Service | ONLINE | 2007-12-12 20:47:41 | NORMAL |
| DLG Service | ONLINE | 2007-12-12 20:47:36 | NORMAL |
| TSAPI Service | ONLINE | 2007-12-12 20:47:43 | NORMAL |
| DMCC Service | ONLINE | 2007-12-12 20:47:44 | NORMAL |

8. Support

Technical support on Startel CMC can be obtained through the following:

Phone: (800) 344-4909

Email: techsupport@startelcorp.com

9. Conclusion

These Application Notes illustrate the procedures for configuring Startel CMC to control and monitor calls placed to and from stations and agents on Avaya Communication Manager. In the configuration described in these Application Notes, Startel CMC employs TSAPI to collect important CTI information like agent event and user data. During compliance testing, Startel CMC successfully monitored events and controlled calls placed to and from stations, as well as calls placed to VDNs and then queued to an agent hunt/skill group. Startel CMC was also able to monitor calls under continuous call volumes over extended periods of time.

10. Additional References

This section references the Avaya and Startel documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Feature Description and Implementation for Avaya Communication Manager*, Issue 5, February 2007, Document Number 555-245-205.

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 4.1, Issue 9, February 2008, Document Number 02-300357

The following documentation was provided by Startel

[3] *Setting Up the Startel CTI Service*, 2007.

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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