Application Notes for CTIntegrations CT Suite 3.0 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for Chat Integration – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for chat integration. CTIntegrations CT Suite is a contact center solution.

In the compliance testing, CTIntegrations CT Suite used the Device, Media, and Call Control interface from Avaya Aura® Application Enablement Services to monitor the chat VDN, along with use of the Administration Without Hardware feature on Communication Manager to support delivery of chat work items to agents.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.0 to interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for chat integration. CT Suite is a contact center solution.

In the compliance testing, CT Suite used the Device, Media, and Call Control (DMCC) .Net interface from Application Enablement Services to monitor the chat VDN, along with use of the Administration Without Hardware (AWOH) feature on Communication Manager to support delivery of chat work items to agents via the Open Queue component of CT Suite.

The Open Queue component of CT Suite initiates a phantom call for each chat work item, using an available AWOH station on Communication Manager as calling party and the applicable chat VDN on Communication Manager as destination. Once the phantom call is delivered to the agent desktop, subsequent call controls are supported by the Device Manager component of CT Suite.

These Application Notes focus on the integration between the Open Queue component of CT Suite with Application Enablement Services for support of chat work items, and assume the integration between the Device Manager component of CT Suite with Application Enablement Services for call control support is already in place as documented in reference [3].

2. General Test Approach and Test Results

The feature test cases were performed both automatically and manually. Upon start of the CT Suite application, the application automatically requests monitoring on the chat VDN.

For the manual part of the testing, incoming chats were placed with available agents that have web browser connections to the CT Suite server. All necessary chat actions by agents were initiated from the agent desktops.

The serviceability test cases were performed manually by disconnecting/reconnecting the Ethernet connection to the CT Suite server.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Application Enablement Services and CT Suite did not include use of any specific encryption features as requested by CTIntegrations.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following on CT Suite:

- Use of DMCC monitoring services to monitor the chat VDN.
- Use of DMCC call control services to support initiation and clearing of phantom calls.
- Proper handling of chat scenarios involving screen pop, drop, hold/resume, multiple agents, transfer, and long duration.

The serviceability testing focused on verifying the ability of CT Suite to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to the server and/or client components of CT Suite.

2.2. Test Results

All test cases were executed and verified.

2.3. Support

Technical support on CT Suite can be obtained through the following:

- **Phone:** (877) 449-6775
- **Email:** info@ctintegrations.com
- **Web:** http://www.ctintegrations.com

3. Reference Configuration

The configuration used for the compliance testing is shown in **Figure 1**. The detailed administration of basic connectivity between Communication Manager and Application Enablement Services, and of contact center resources are not the focus of these Application Notes and will not be described.

CT Suite can support chat requesters from the intranet or internet. For simplicity, all chats in the compliance testing were initiated from the intranet.

The contact center resources shown in the table below were used in the testing.

Device Type	Extension
Agent Station	65001, 66002
Agent ID	65881, 65882
Agent Password	65881, 65882

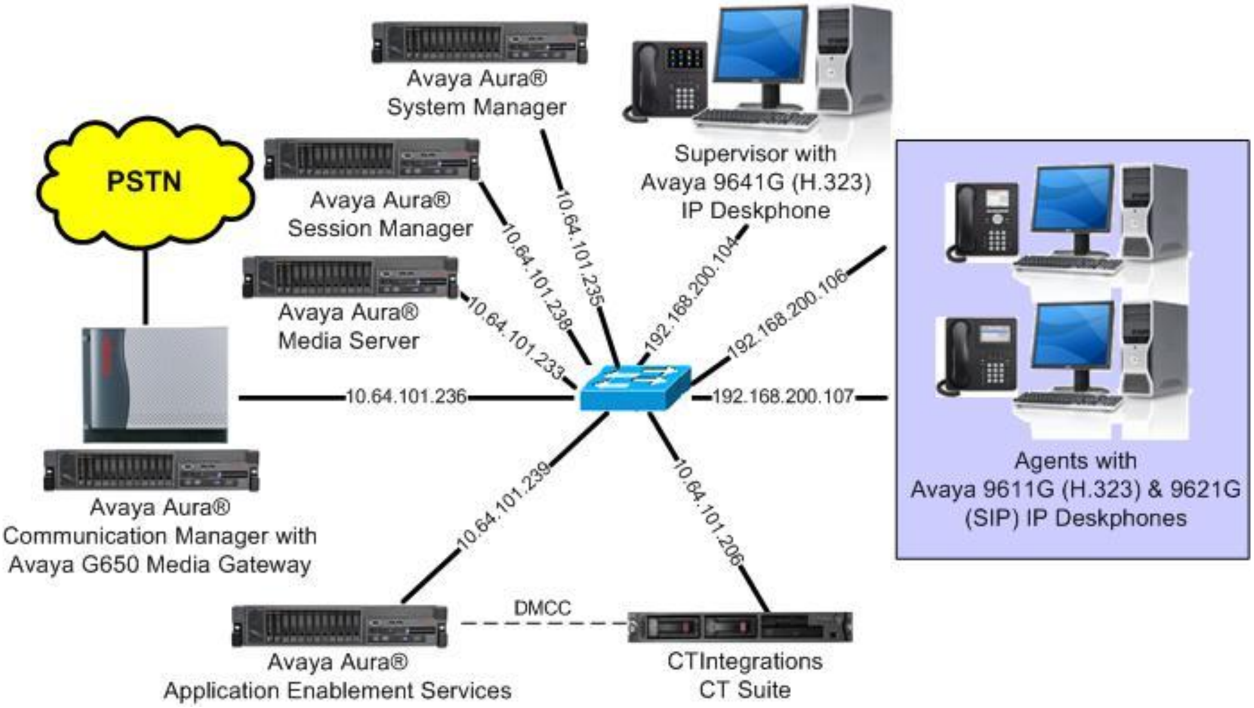


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.0.1.2 (7.0.1.2.0.441.23523)
Avaya G650 Media Gateway	NA
Avaya Aura® Media Server in Virtual Environment	7.7.0.375
Avaya Aura® Application Enablement Services in Virtual Environment	7.0.1 (7.0.1.0.4.15-0)
Avaya Aura® Session Manager in Virtual Environment	7.0.1.2 (7.0.1.2.701230)
Avaya Aura® System Manager in Virtual Environment	7.0.1.2 (7.0.1.2.086553)
Avaya 9611G and 9641G IP Deskphones (H.323)	6.6401
Avaya 9621G IP Deskphones (SIP)	7.0.1.4.6
CTIntegrations CT Suite on Microsoft Windows Server 2012 R2 • CT Admin • CT Web Client • CT Device Manager • CT Open Queue • Avaya DMCC .NET (ServiceProvider.dll)	3.0 Hotfix 1 Standard 3.0.6 3.0.3 3.0.12.17180 3.0.3.17132 7.0.0.38

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Administer AWOH stations
- Administer chat skill
- Administer chat vector and VDN
- Administer agent IDs

5.1. Administer AWOH Stations

Add an AWOH station using the "add station n" command, where "n" is an available extension number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Extension:** The available extension number.
- **Type:** "CTI"
- **Name:** A descriptive name.

```
add station 67771                                               Page   1 of   5
                                     STATION

Extension: 67771                         Lock Messages? n               BCC: 0
     Type: CTI                           Security Code:                  TN: 1
     Port: X                           Coverage Path 1:                 COR: 1
     Name: Chat AWOH 1                 Coverage Path 2:                 COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 1          Personalized Ringing Pattern: 1
             Data Module? n                      Message Lamp Ext: 67771
          Display Module: n
```

Repeat this section to administer the desired number of AWOH stations, to be used as originators of phantom calls for chat work items. The number of AWOH stations configured should correspond to the desired number of simultaneous chat work items. In the compliance testing, two AWOH stations with extensions 67771-67772 were configured, as shown below.

```
list station 67771 count 2

                                  STATIONS

Ext/          Port/   Name/                       Room/       Cv1/ COR/   Cable/
 Hunt-to       Type      Surv GK NN        Move    Data Ext    Cv2  COS TN Jack

67771         X       Chat AWOH 1                                  1
               CTI                         no                       1
67772         X       Chat AWOH 2                                  1
               CTI                         no                       1
```

5.2. Administer Chat Skill

Administer a skill group to be used for routing of chat work items to agents. Use the “add hunt-group n” command, where “n” is an available group number. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Number:** The available group number.
- **Group Name:** A descriptive name.
- **Group Extension:** An available extension number.
- **ACD:** “y”
- **Queue:** “y”
- **Vector:** “y”

```
add hunt-group 7                                                Page   1 of  4
                                  HUNT GROUP

            Group Number: 7                                ACD? y
              Group Name: Chat Skill                     Queue? y
         Group Extension: 67101                         Vector? y
              Group Type: ucd-mia
                      TN: 1
                     COR: 1                    MM Early Answer? n
           Security Code:               Local Agent Preference? n
 ISDN/SIP Caller Display:
```

Navigate to **Page 2**, and set **Skill** to “y” as shown below.

```
add hunt-group 7                                                Page   2 of  4
                                  HUNT GROUP

                    Skill? y      Expected Call Handling Time <sec>: 180
                      AAS? n
                 Measured: none
     Supervisor Extension:

      Controlling Adjunct: none
```

5.3. Administer Chat Vector and VDN

Modify a vector using the “change vector n” command, where “n” is an existing vector number. The vector will be used for routing of chat phantom calls to agents at medium priority. Note that the vector **Number**, **Name**, **queue-to-skill**, and **wait-time** steps may vary.

```
change vector 700                                               Page   1 of   6
                                  CALL VECTOR

    Number: 700             Name: CT Suite Chat
Multimedia? n      Attendant Vectoring? n    Meet-me Conf? n           Lock? n
     Basic? y   EAS? y   G3V4 Enhanced? y   ANI/II-Digits? y   ASAI Routing? y
 Prompting? y   LAI? n  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 queue-to     skill 7    pri m
02 wait-time    999 secs hearing ringback
03
04
```

Add a VDN using the “add vdn n” command, where “n” is an available extension number. Enter a descriptive name for the **Name** field, and enter the vector number from above for the **Vector Number** field. Retain the default values for all remaining fields.

```
add vdn 67000                                                  Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 67000
                                 Name*: CT Suite Chat
                         Vector Number: 700
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none
```

5.4. Administer Agent IDs

The newly created chat skill needs to be added to the applicable agents. Use the “change agent-loginID n” command, where “n” is the first agent ID from **Section 3**. Navigate to **Page 2**, and add the chat skill group number from **Section 5.2** to an available **SN**, and set the desired skill level under the corresponding **SL**, as shown below.

```
change agent-loginID 65881                                      Page   2 of   3
                                 AGENT LOGINID
      Direct Agent Skill:                               Service Objective? n
Call Handling Preference: skill-level               Local Call Preference? n

    SN   RL SL         SN   RL SL         SN   RL SL         SN   RL SL
 1: 1       1       16:                 31:                 46:
 2: 2       1       17:                 32:                 47:
 3: 7       1       18:                 33:                 48:
 4:                 19:                 34:                 49:
 5:                 20:                 35:                 50:
```

Repeat this section to add the chat skill to all desired agents. In the compliance testing, the chat skill was added to both agents from **Section 3**, as shown below.

```
list agent-loginID 65881 count 2
                               AGENT LOGINID
Login ID     Name          Extension     Dir Agt  AAS/AUD        COR Ag Pr SO
               Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv Skil/Lv

65881        CM Agent 1     unstaffed                              1   lvl
                  1/01    2/01    7/01     /       /       /       /       /
65882        CM Agent 2     unstaffed                              1   lvl
                  1/01    2/01    7/01     /       /       /       /       /
```

6. Configure Avaya Aura® Application Enablement Services

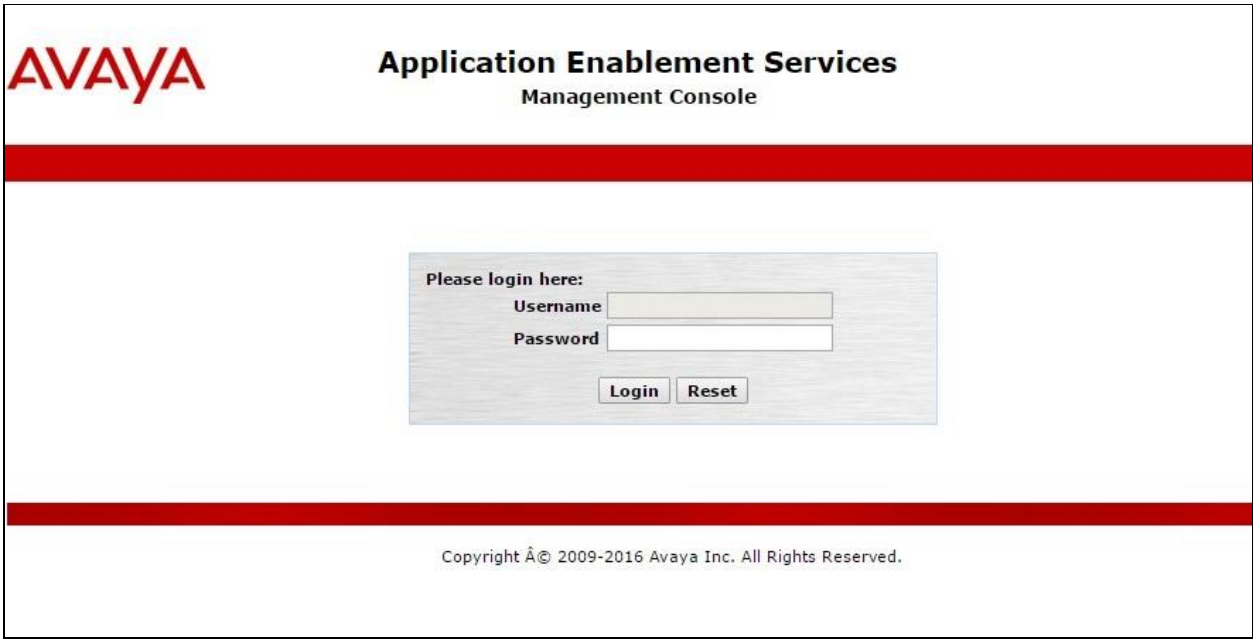
This section provides the procedures for configuring Application Enablement Services. The procedures include the following areas:

- Launch OAM interface
- Verify license
- Obtain CT Suite user credentials
- Obtain Tlink name

6.1. Launch OAM Interface

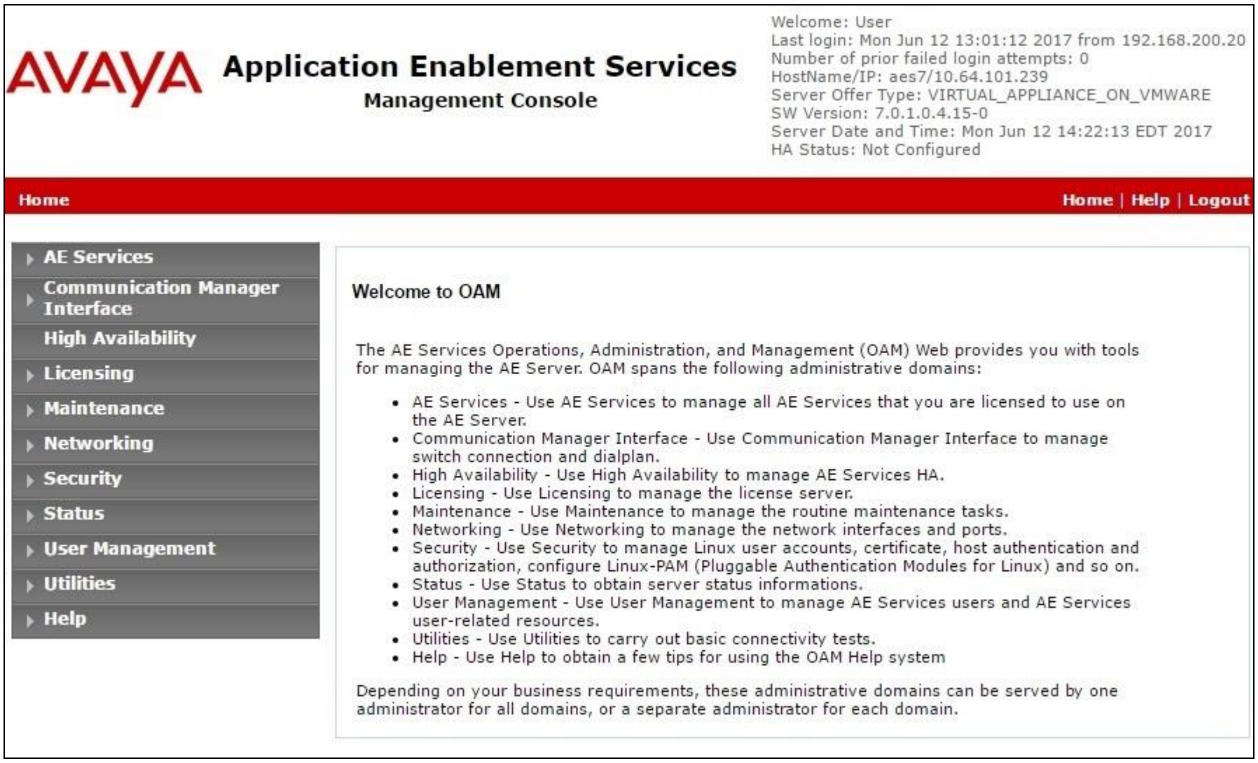
Access the OAM web-based interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of the Application Enablement Services server.

The **Please login here** screen is displayed. Log in using the appropriate credentials.



AVAYA
Application Enablement Services
Management Console
Please login here:
Username
Password
Login
Reset
Copyright Â© 2009-2016 Avaya Inc. All Rights Reserved.

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



Welcome: User
Last login: Mon Jun 12 13:01:12 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Welcome to OAM

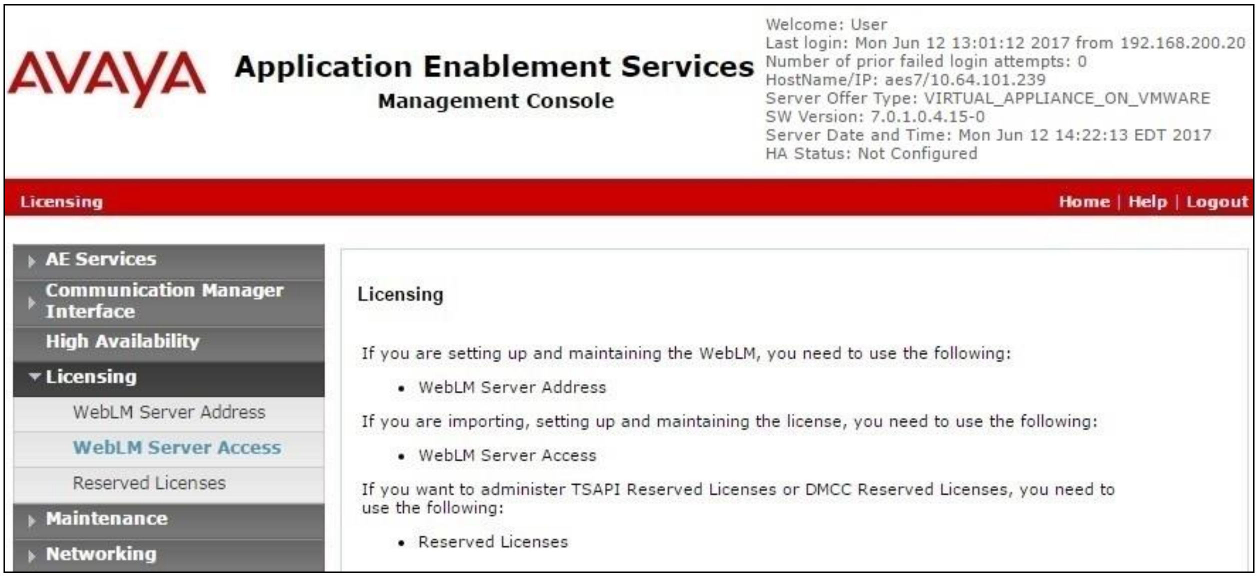
The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:

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

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

6.2. Verify License

Select **Licensing → WebLM Server Access** in the left pane, to display the applicable WebLM server log in screen (not shown). Log in using the appropriate credentials, and navigate to display installed licenses (not shown).



Welcome: User
Last login: Mon Jun 12 13:01:12 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

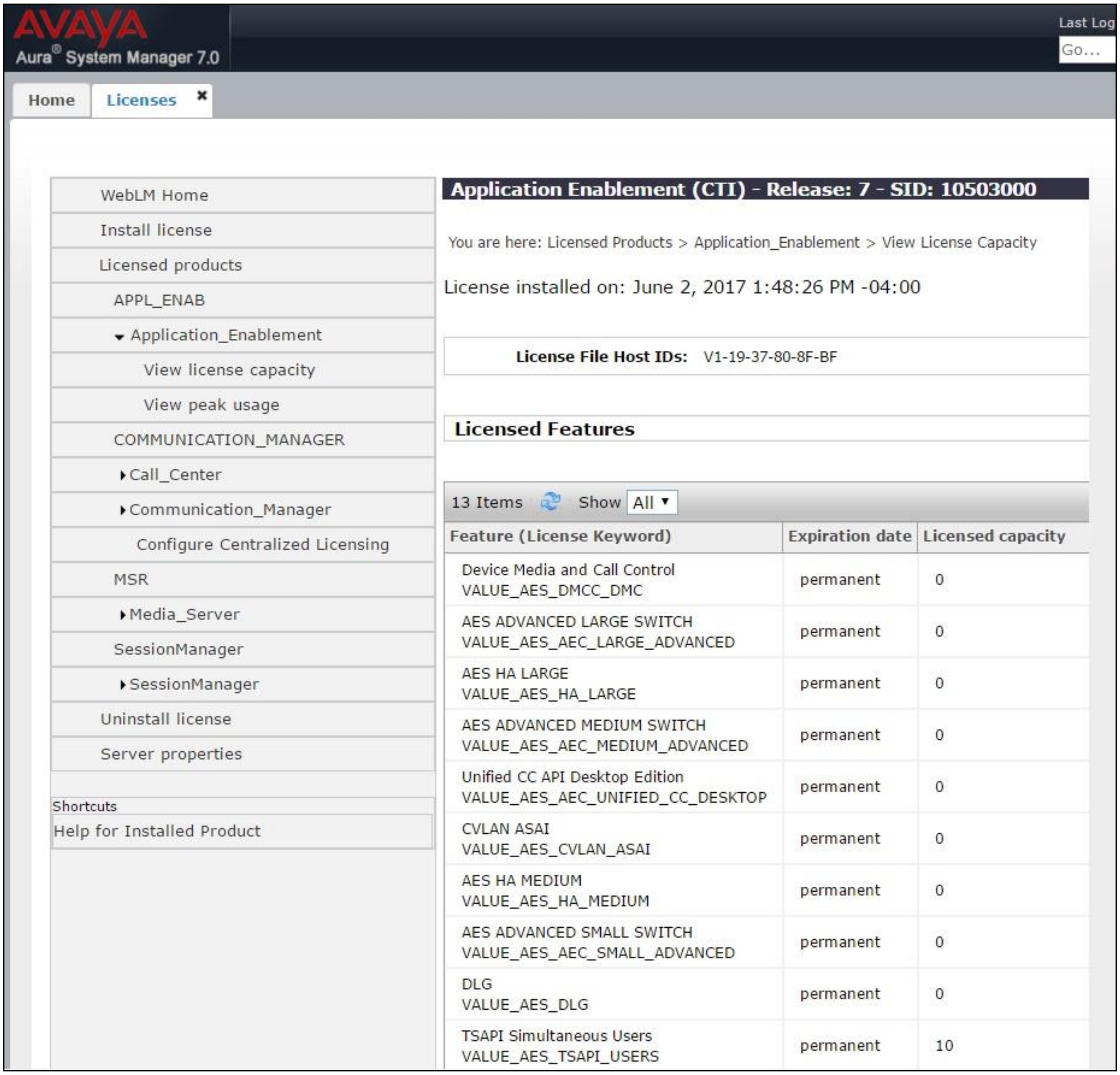
If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

Select **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**, as shown below. Note that the TSAPI license is used for phantom calls via DMCC.



Application Enablement (CTI) - Release: 7 - SID: 10503000

You are here: Licensed Products > Application_Enablement > View License Capacity

License installed on: June 2, 2017 1:48:26 PM -04:00

License File Host IDs: V1-19-37-80-8F-BF

Licensed Features

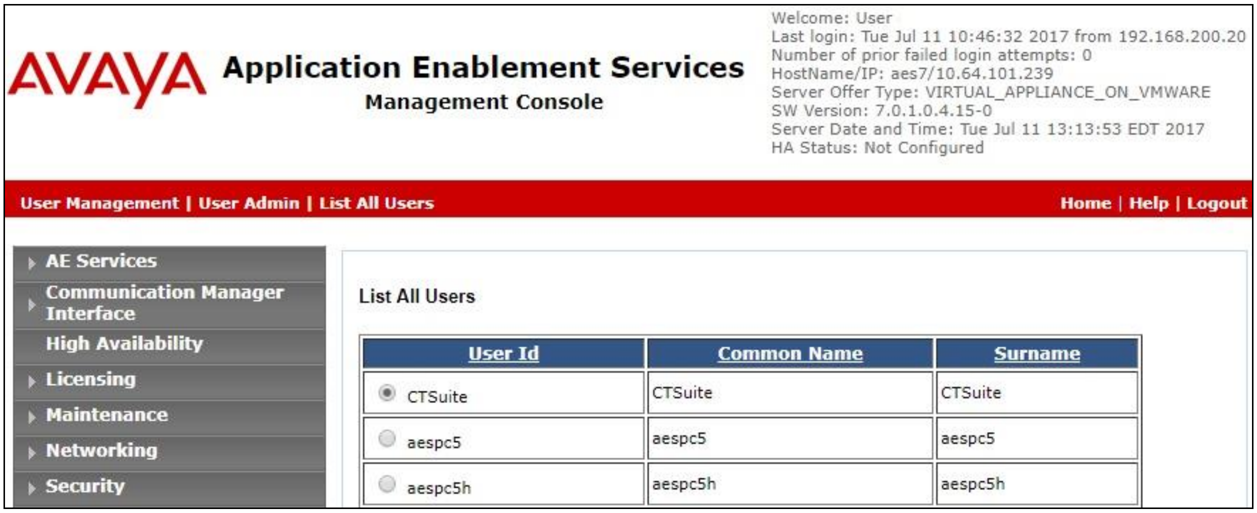
13 Items Show All

Feature (License Keyword)	Expiration date	Licensed capacity
Device Media and Call Control VALUE_AES_DMCC_DMC	permanent	0
AES ADVANCED LARGE SWITCH VALUE_AES_AEC_LARGE_ADVANCED	permanent	0
AES HA LARGE VALUE_AES_HA_LARGE	permanent	0
AES ADVANCED MEDIUM SWITCH VALUE_AES_AEC_MEDIUM_ADVANCED	permanent	0
Unified CC API Desktop Edition VALUE_AES_AEC_UNIFIED_CC_DESKTOP	permanent	0
CVLAN ASAI VALUE_AES_CVLAN_ASAI	permanent	0
AES HA MEDIUM VALUE_AES_HA_MEDIUM	permanent	0
AES ADVANCED SMALL SWITCH VALUE_AES_AEC_SMALL_ADVANCED	permanent	0
DLG VALUE_AES_DLG	permanent	0
TSAPI Simultaneous Users VALUE_AES_TSAPI_USERS	permanent	10

6.3. Obtain CT Suite User Credentials

Select **User Management → User Admin → List All Users** (not shown) from the left pane, to display the **List All Users** screen in the right pane.

Locate and note the CT Suite user credentials that was created as part of the voice channel integration as documented in reference [3].



Welcome: User
Last login: Tue Jul 11 10:46:32 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Tue Jul 11 13:13:53 EDT 2017
HA Status: Not Configured

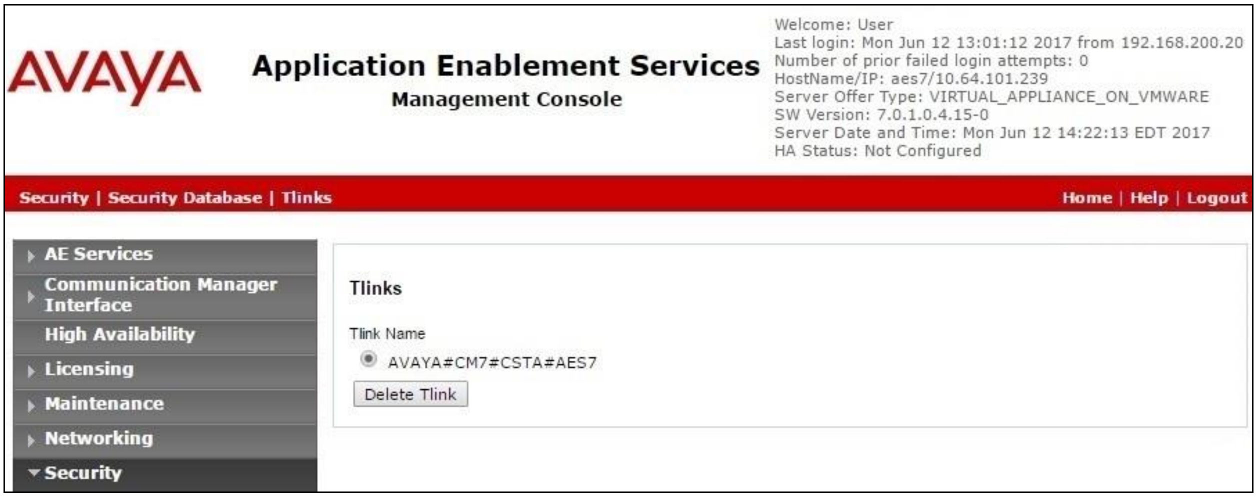
List All Users

User Id	Common Name	Surname
● CTSuite	CTSuite	CTSuite
○ aespc5	aespc5	aespc5
○ aespc5h	aespc5h	aespc5h

6.4. Obtain Tlink Name

Select **Security → Security Database → Tlinks** (not shown) from the left pane. The **Tlinks** screen shows a listing of Tlink names.

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. In the compliance testing, the relevant switch connection name is “cm7”, as shown below in caps.



Welcome: User
Last login: Mon Jun 12 13:01:12 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Mon Jun 12 14:22:13 EDT 2017
HA Status: Not Configured

Tlinks

Tlink Name

● AVAYA#CM7#CSTA#AES7

7. Configure CTIntegrations CT Suite

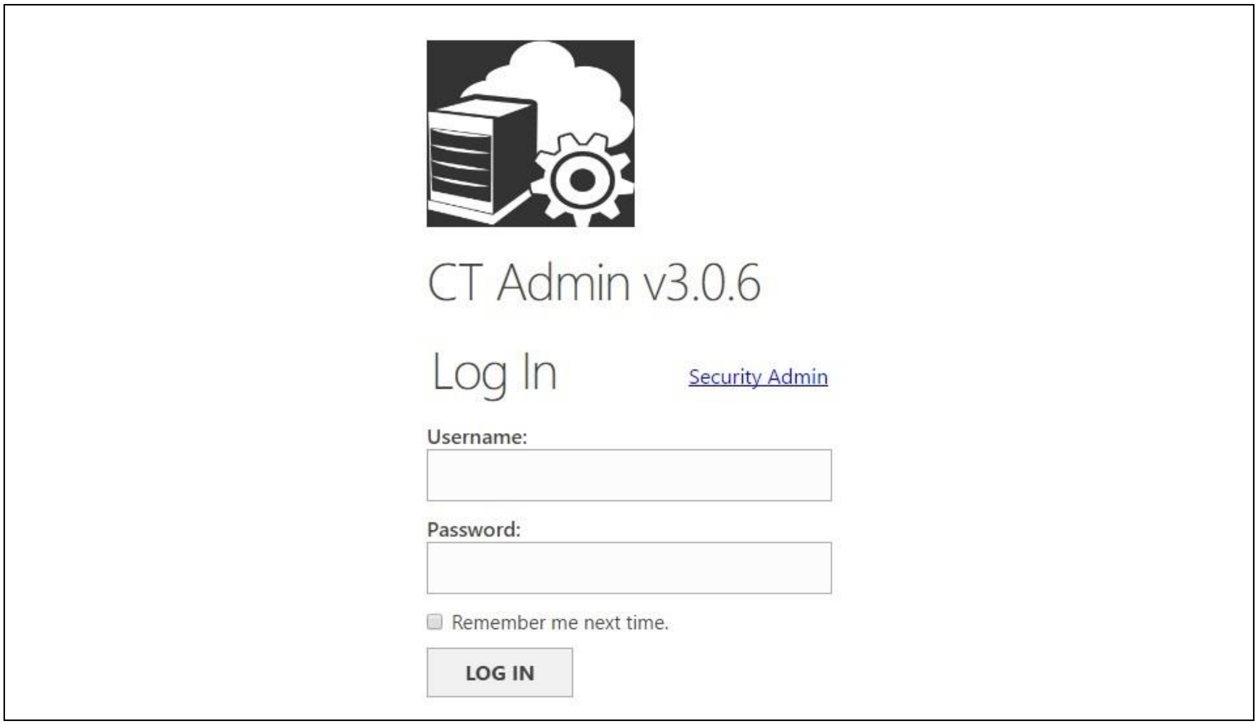
This section provides the procedures for configuring CT Suite. The procedures include the following areas:

- Launch CT Admin interface
- Administer CTI extensions
- Administer servers
- Restart service

The configuration of CT Suite is typically performed by CTIntegrations system integrators. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch CT Admin Interface

Access the CT Admin web interface by using the URL "http://ip-address/CTAdmin" in an Internet browser window, where "ip-address" is the IP address of the CT Suite server. The **CT Admin** screen below is displayed. Log in using the administrator credentials.

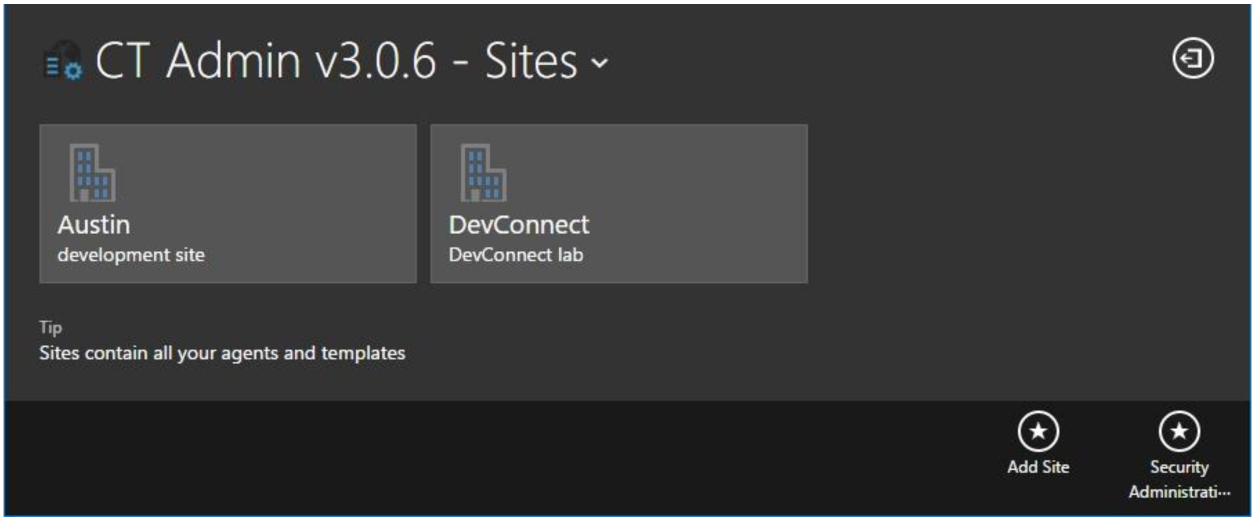


CT Admin v3.0.6

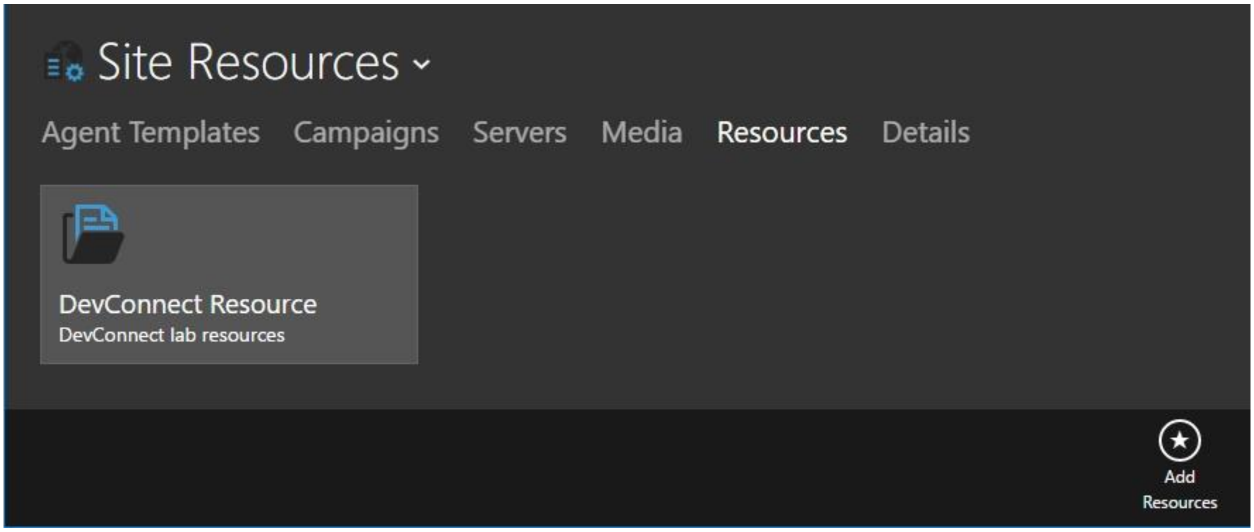
Log In

7.2. Administer CTI Extensions

The **Sites** screen below is displayed. Select the pertinent site, in this case "DevConnect".

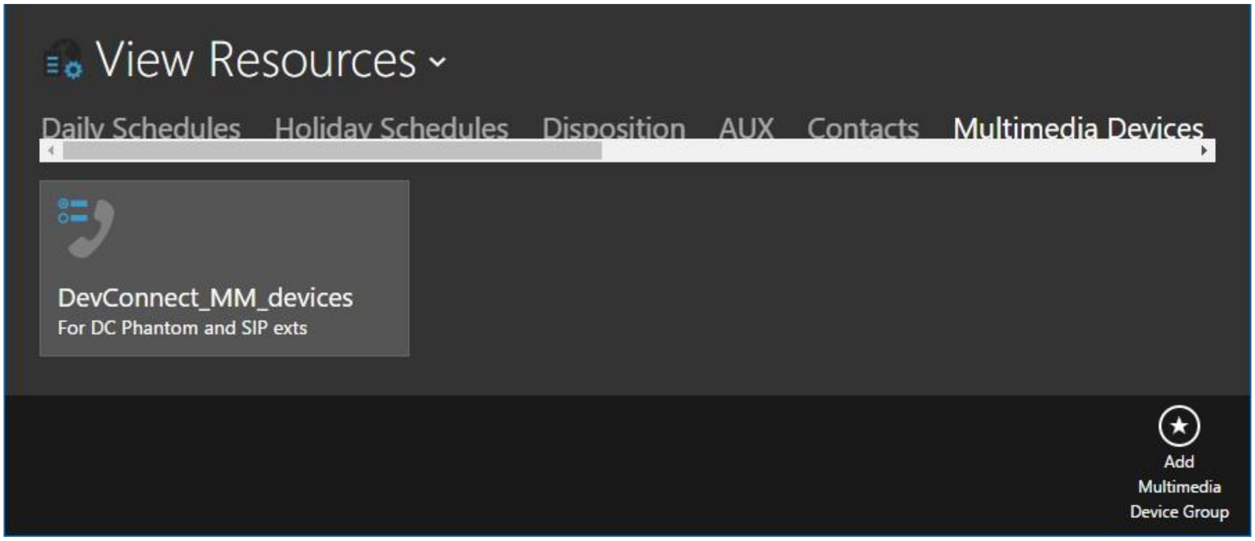


The **Site Resources** screen is displayed next. Select the pertinent logical resource group, in this case "DevConnect Resource".



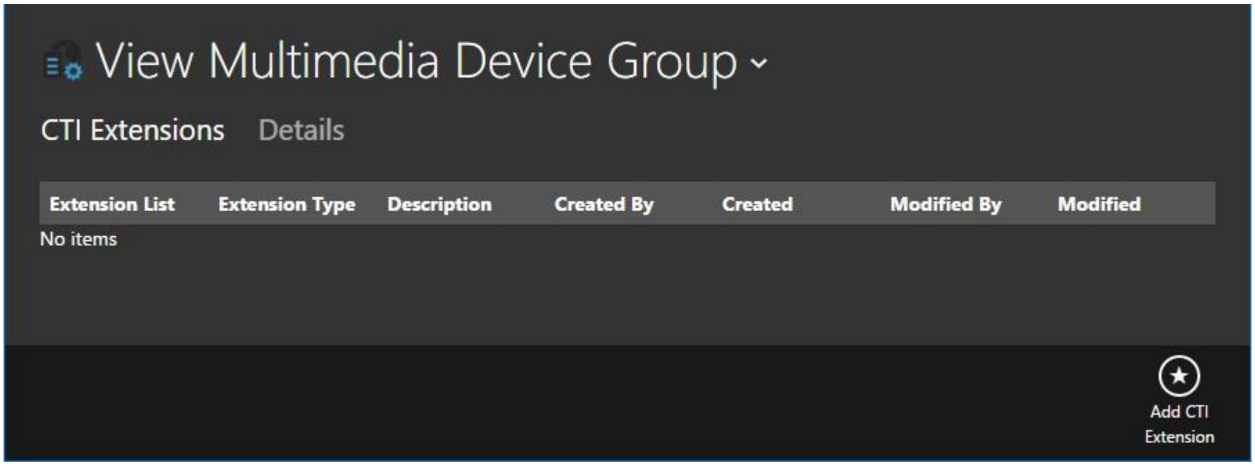
The **View Resources** screen is displayed. Scroll the top menu bar as necessary to locate and select **Multimedia Devices**, followed by **Add Multimedia Device Group** from bottom of screen to add a logical group for multimedia devices.

In the compliance testing, the “DevConnect_MM_devices” group was pre-configured. Select the newly added group.



DevConnect_MM_devices
For DC Phantom and SIP exts

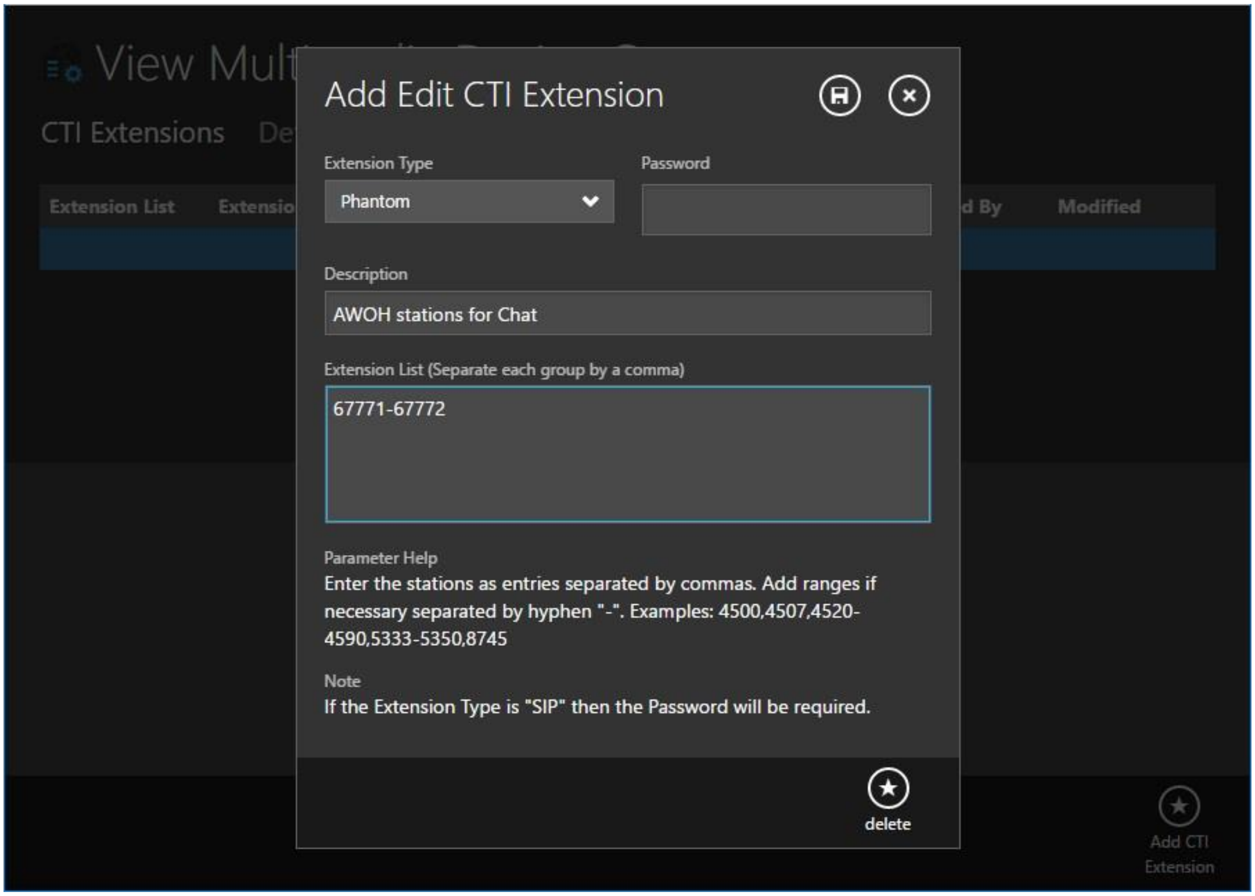
The **View Multimedia Device Group** screen is displayed next. Select the **CTI Extensions** tab, followed by **Add CTI Extension** from bottom of screen.



Extension List	Extension Type	Description	Created By	Created	Modified By	Modified
No items						

The **Add Edit CTI Extension** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **Extension Type:** "Phantom"
- **Description:** A desired description.
- **Extension List:** The AWOH station extensions from **Section 5.1**.



Add Edit CTI Extension

Extension Type: Phantom

Password:

Description: AWOH stations for Chat

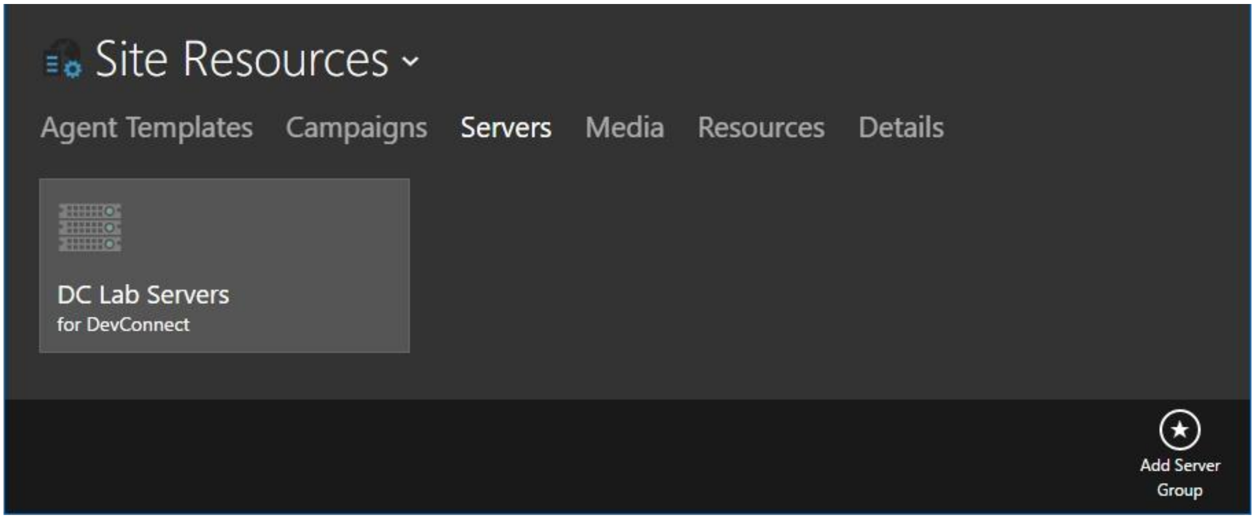
Extension List (Separate each group by a comma): 67771-67772

Parameter Help
Enter the stations as entries separated by commas. Add ranges if necessary separated by hyphen "-". Examples: 4500,4507,4520-4590,5333-5350,8745

Note
If the Extension Type is "SIP" then the Password will be required.

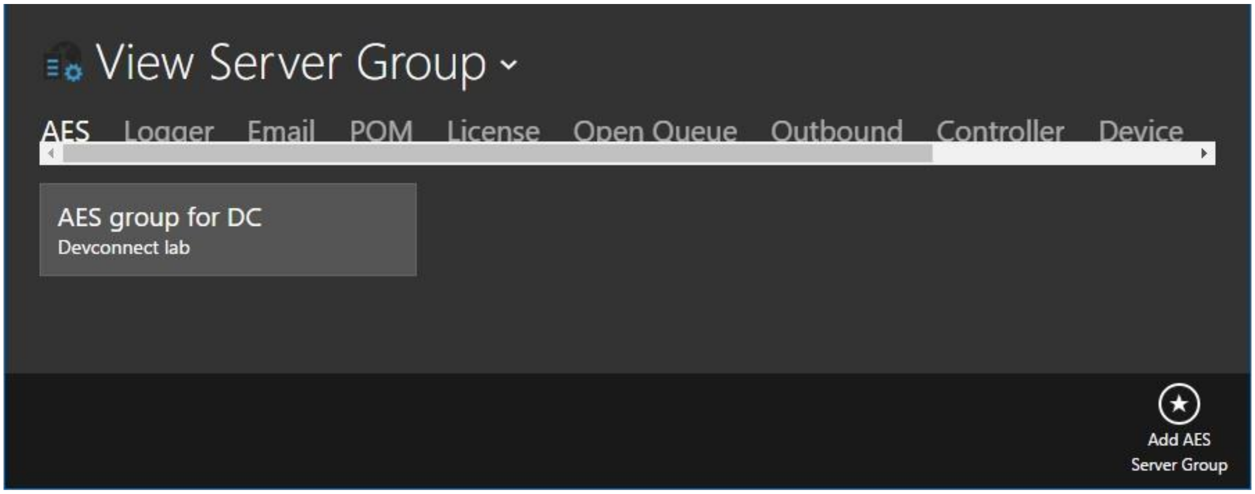
7.3. Administer Servers

Return to the **Site Resources** screen. Select **Servers** from the top menu, followed by the pertinent logical servers group, in this case "DC Lab Servers".



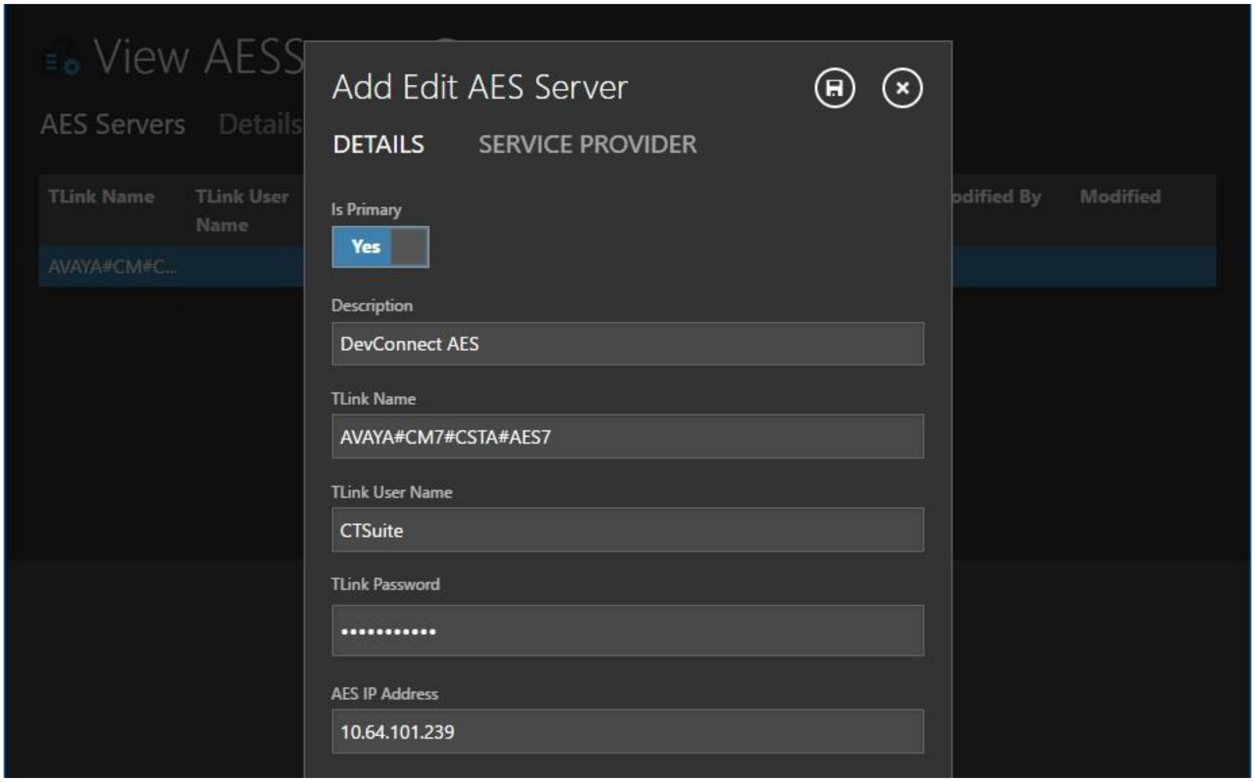
7.3.1. AES Server

The **View Server Group** screen is displayed next. Select **AES** from the top menu, followed by **Add AES Server Group** from bottom of screen to add a logical group. In the compliance testing, the "AES group for DC" group was pre-configured. Select the newly added group.



The **Add Edit AES Server** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **Is Primary:** "Yes"
- **Description:** A desired description.
- **TLink Name:** The Tlink name from **Section 6.4**.
- **TLink User Name:** The CT Suite user credentials from **Section 6.3**.
- **TLink Password:** The CT Suite user credentials from **Section 6.3**.
- **AES IP Address:** IP address of Application Enablement Services from **Section 3**.



Is Primary: Yes

Description: DevConnect AES

TLink Name: AVAYA#CM7#CSTA#AES7

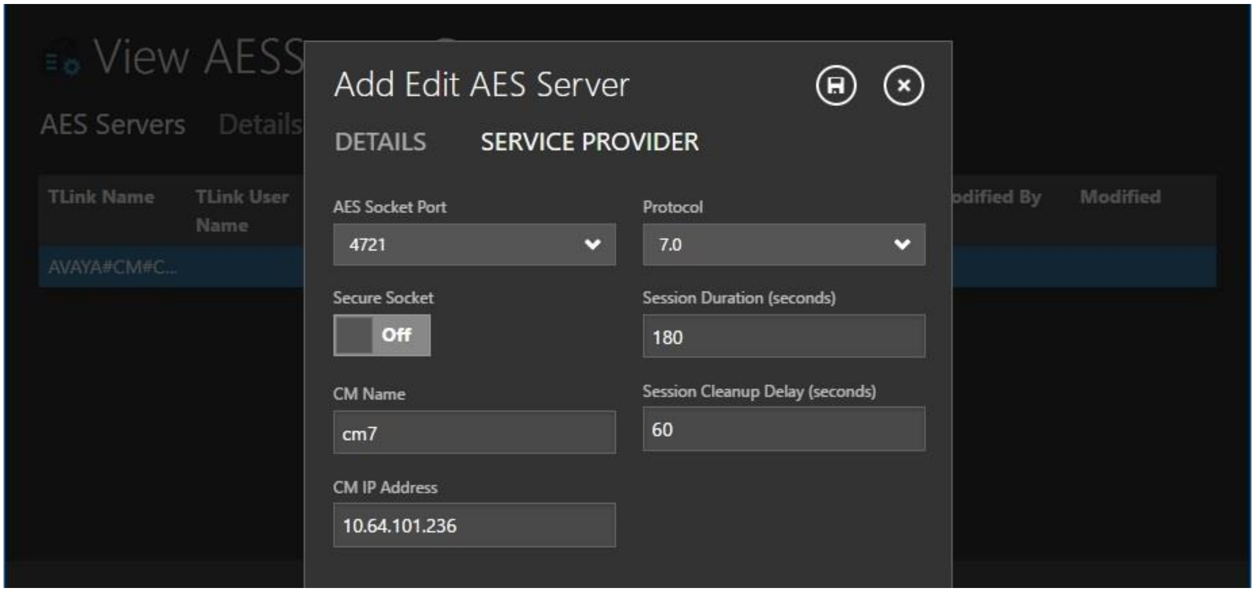
TLink User Name: CTSuite

TLink Password: •••••••••••

AES IP Address: 10.64.101.239

Select the **SERVICE PROVIDER** tab. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **Protocol:** "7.0"
- **CM Name:** The switch connection name from **Section 6.4**.
- **CM IP Address:** IP address of Communication Manager from **Section 3**.



Add Edit AES Server

DETAILS | SERVICE PROVIDER

AES Socket Port: 4721

Protocol: 7.0

Secure Socket: Off

Session Duration (seconds): 180

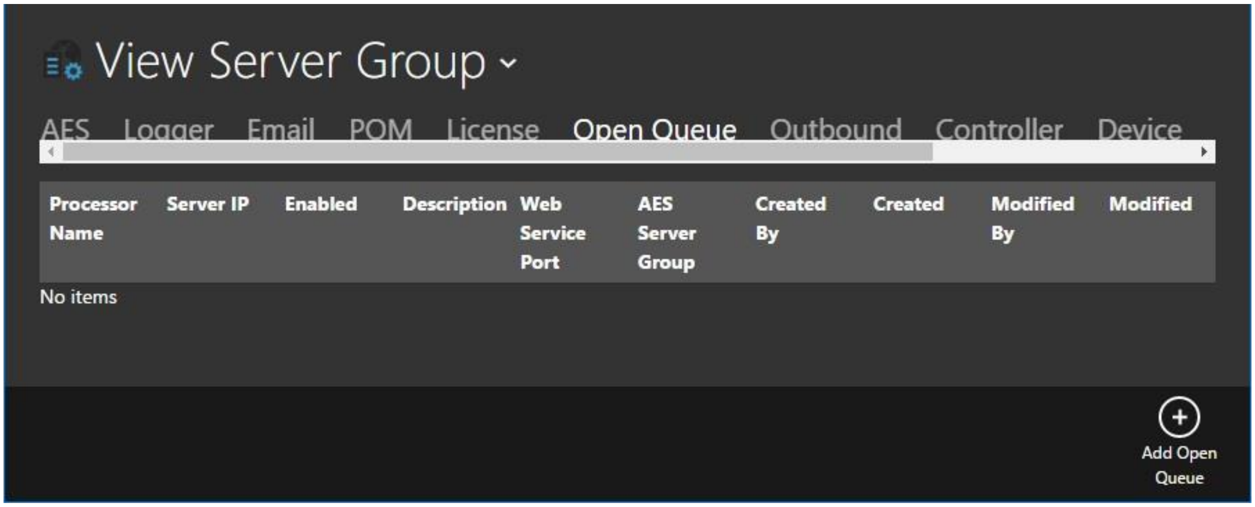
CM Name: cm7

Session Cleanup Delay (seconds): 60

CM IP Address: 10.64.101.236

7.3.2. Open Queue Server

Navigate back to the **View Server Group** screen below. Select **Open Queue** from the top menu, followed by **Add Open Queue** from bottom of screen.



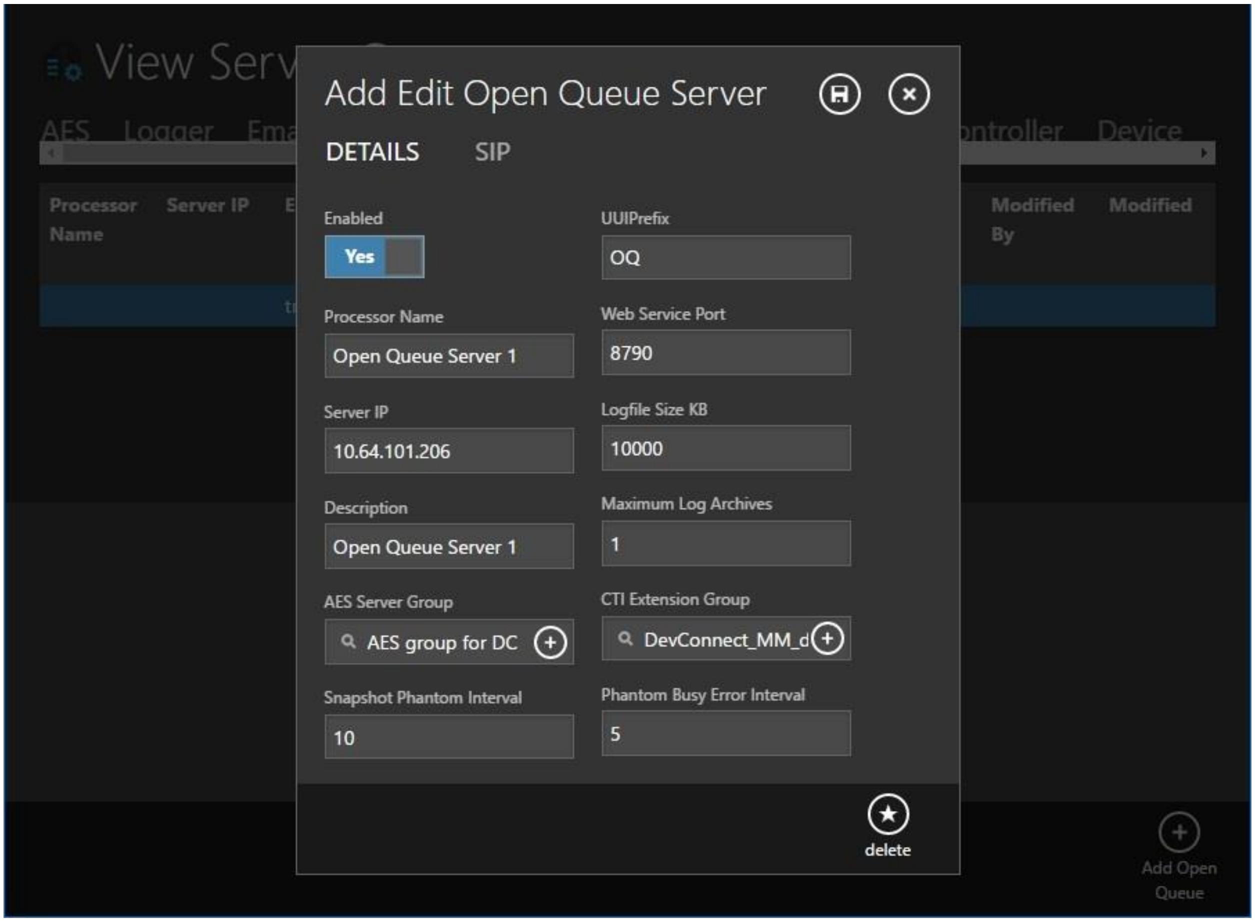
View Server Group

Processor Name	Server IP	Enabled	Description	Web Service Port	AES Server Group	Created By	Created	Modified By	Modified

No items

The **Add Edit Open Queue Server** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **Processor Name:** A descriptive name.
- **Web Service Port:** "8790"
- **Server IP:** IP address of CT Suite server.
- **Description:** A desired description.
- **AES Server Group:** Select the pertinent AES server group name from **Section 7.3.1**.
- **CTI Extension Group:** Select the multimedia device group name from **Section 7.2**.



Add Edit Open Queue Server

Enabled: Yes

UUIPrefix: OQ

Processor Name: Open Queue Server 1

Web Service Port: 8790

Server IP: 10.64.101.206

Logfile Size KB: 10000

Description: Open Queue Server 1

Maximum Log Archives: 1

AES Server Group: AES group for DC

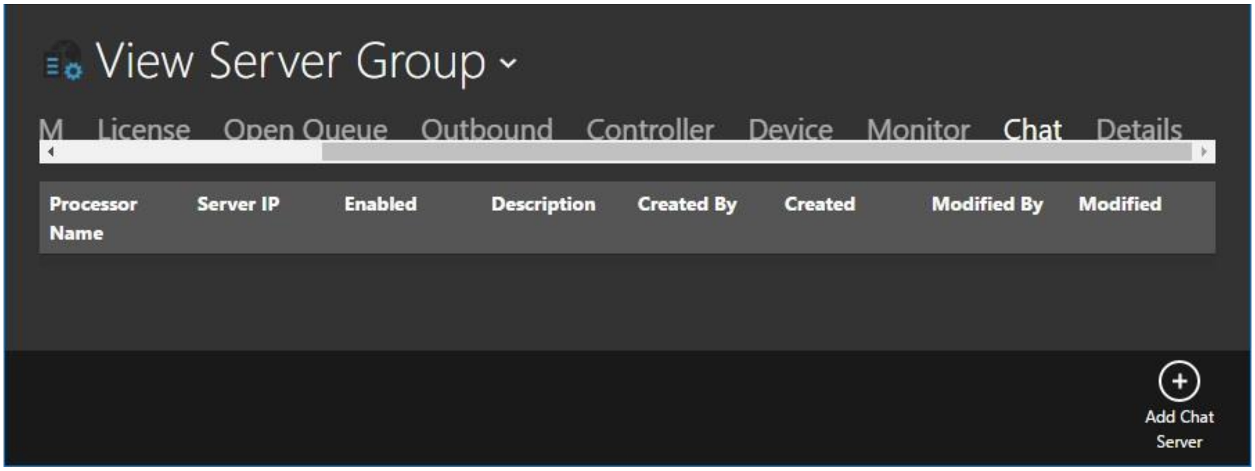
CTI Extension Group: DevConnect_MM_d

Snapshot Phantom Interval: 10

Phantom Busy Error Interval: 5

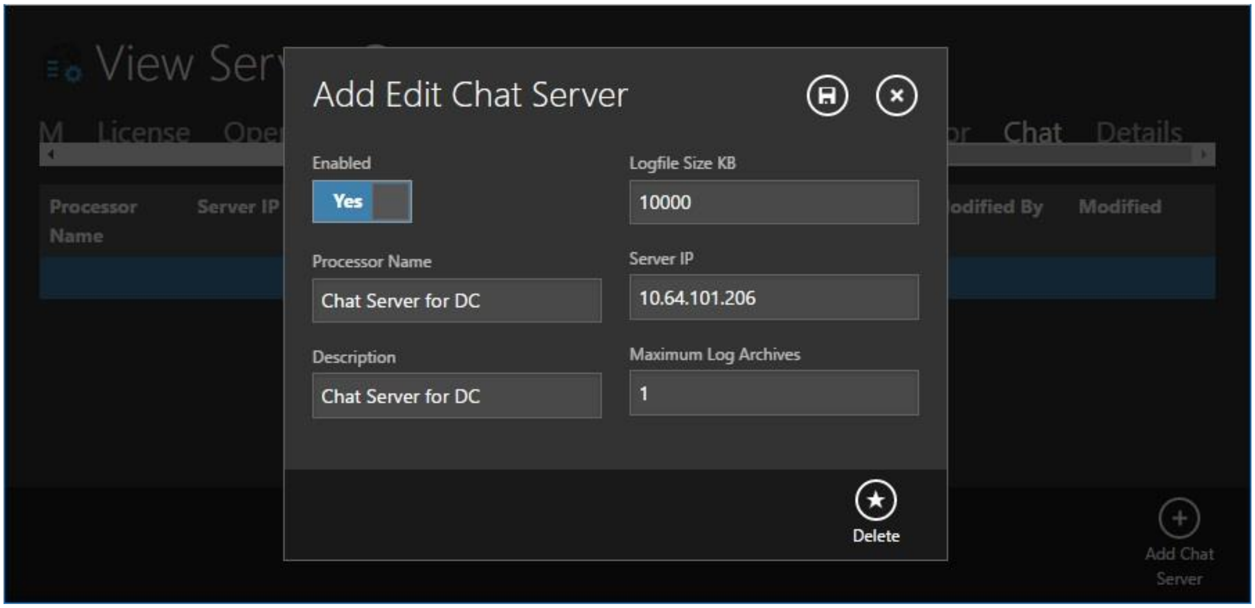
7.3.3. Chat Server

Navigate back to the **View Server Group** screen. Scroll the top menu bar as necessary to locate and select **Chat**, followed by **Add Chat Server** from bottom of screen.



The **Add Edit Chat Server** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **Processor Name:** A descriptive name.
- **Server IP:** IP address of CT Suite server.
- **Description:** A desired description.



Add Edit Chat Server

Enabled: Yes

Logfile Size KB: 10000

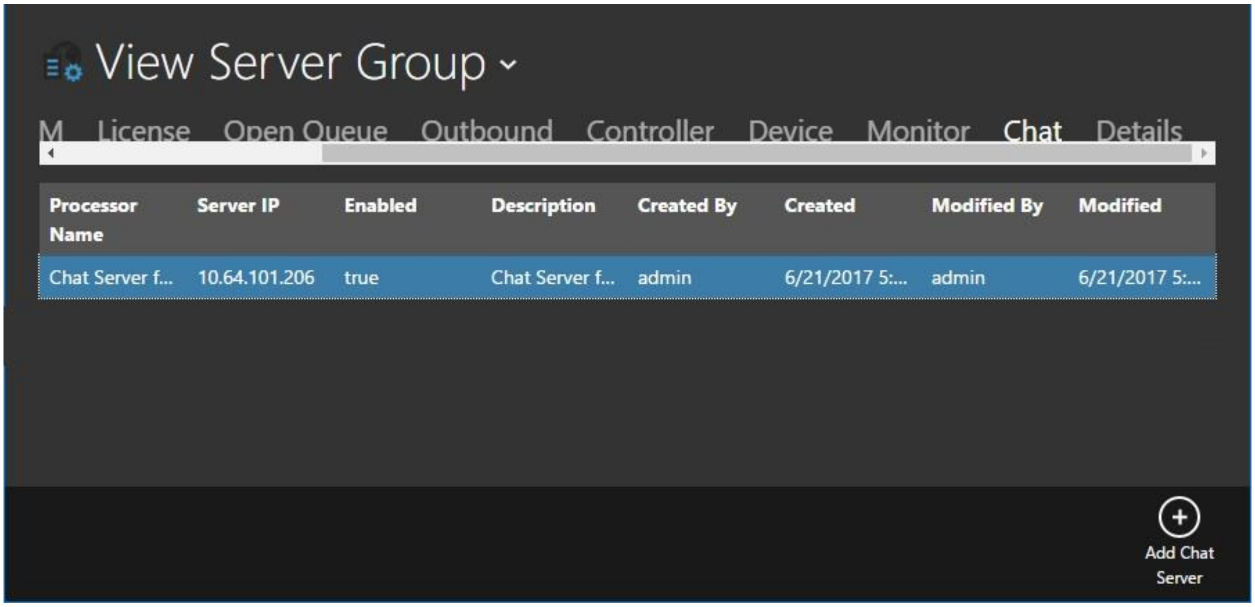
Processor Name: Chat Server for DC

Server IP: 10.64.101.206

Description: Chat Server for DC

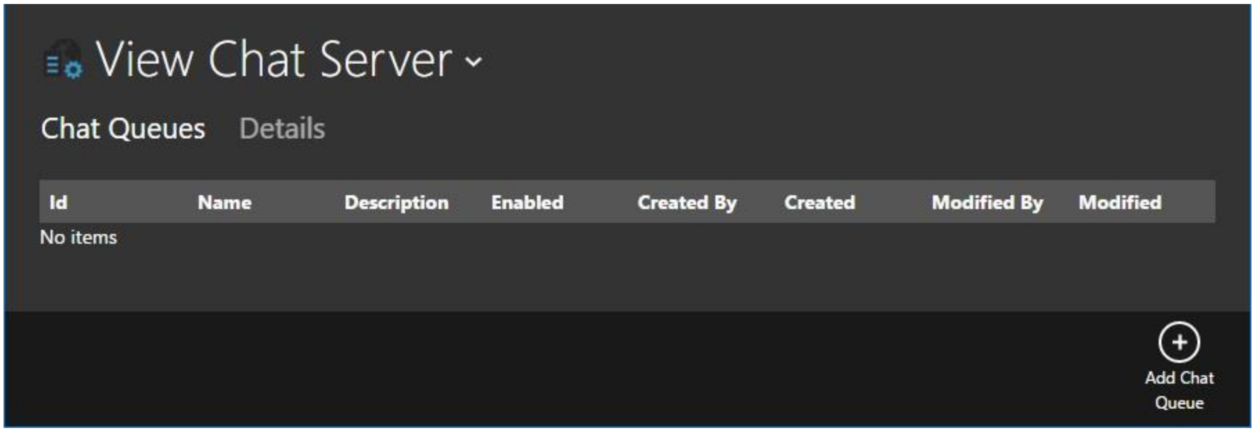
Maximum Log Archives: 1

The **View Server Group** screen is displayed again. Select the newly created chat server, as shown below.



Processor Name	Server IP	Enabled	Description	Created By	Created	Modified By	Modified
Chat Server f...	10.64.101.206	true	Chat Server f...	admin	6/21/2017 5:...	admin	6/21/2017 5:...

The **View Chat Server** screen is displayed next. Select **Add Chat Queue** from bottom of screen.

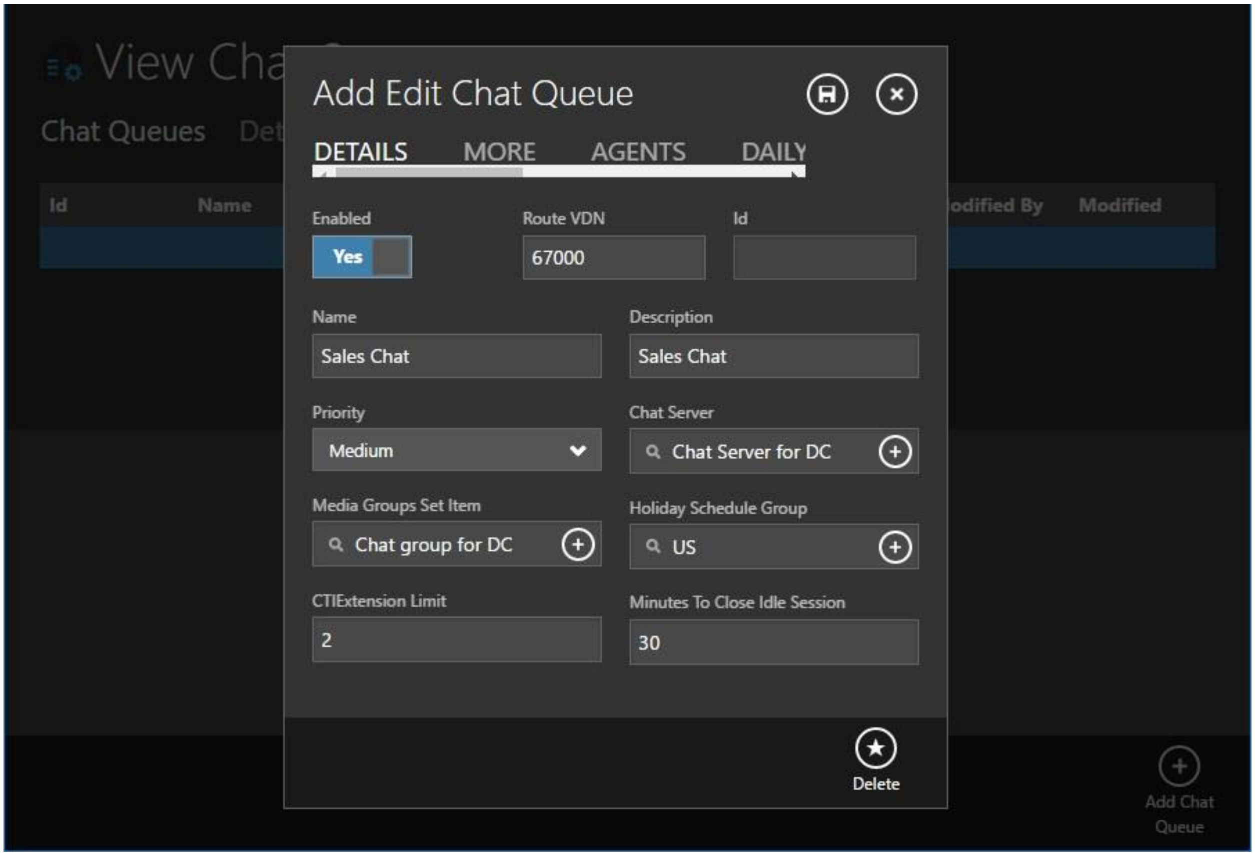


Id	Name	Description	Enabled	Created By	Created	Modified By	Modified

No items

The **Add Edit Chat Queue** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **Route VDN:** The Chat VDN extension number from **Section 5.3**.
- **Name:** A descriptive name.
- **Description:** A desired description.
- **Media Groups Set Item:** Select the pertinent pre-existing media group.
- **Holiday Schedule Group:** Select the pertinent pre-existing holiday schedule group.
- **CTIExtension Limit:** The number of CTI extensions from **Section 7.2**.
- **Minutes To Close Idle Session:** Enter the desired interval.



Add Edit Chat Queue

Enabled: Yes

Route VDN: 67000

Id:

Name: Sales Chat

Description: Sales Chat

Priority: Medium

Chat Server: Chat Server for DC

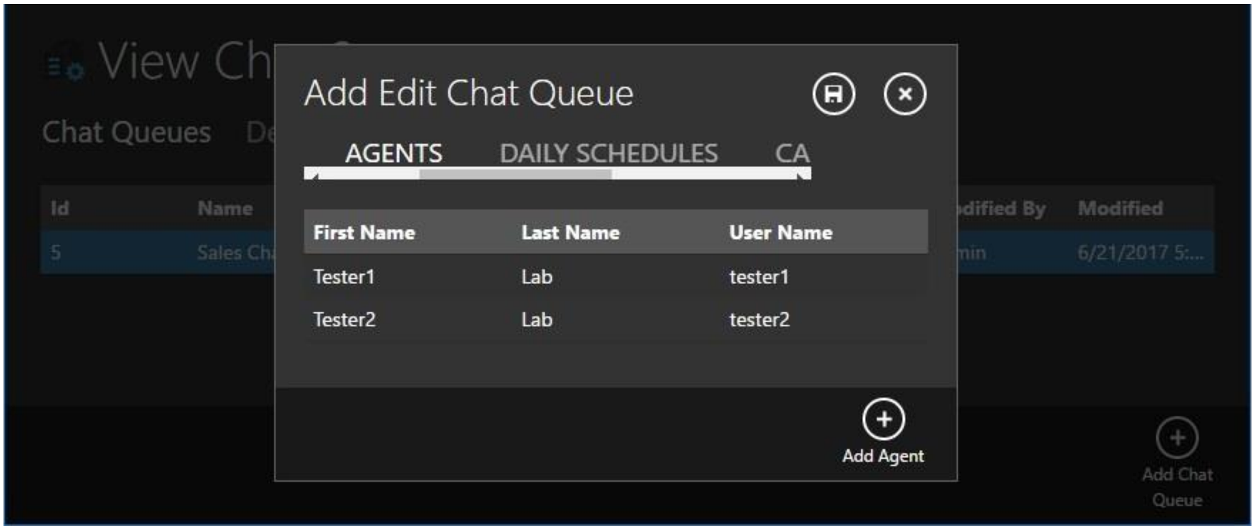
Media Groups Set Item: Chat group for DC

Holiday Schedule Group: US

CTIExtension Limit: 2

Minutes To Close Idle Session: 30

Select the **AGENTS** tab. Follow reference [4] to select the pertinent pre-existing agents. In the compliance testing, two agents below were selected.

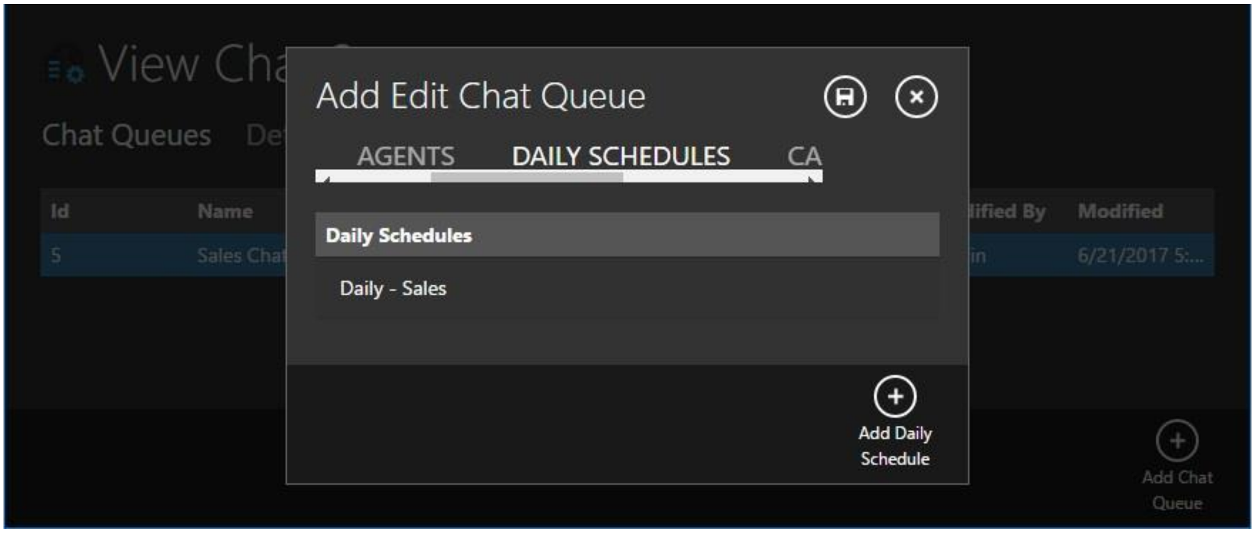


Add Edit Chat Queue

AGENTS | DAILY SCHEDULES | CA

First Name	Last Name	User Name
Tester1	Lab	tester1
Tester2	Lab	tester2

Select the **DAILY SCHEDULES** tab. Follow reference [4] to select the pertinent pre-existing daily schedule, in this case “Daily – Sales”.



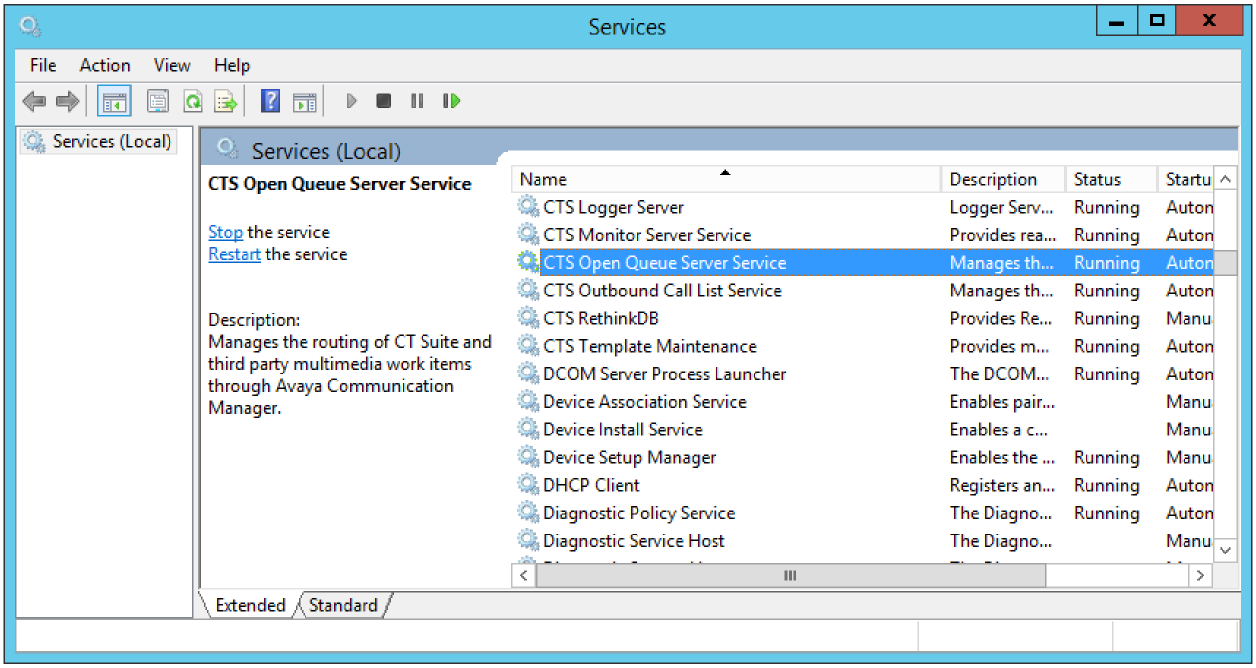
Add Edit Chat Queue

AGENTS | DAILY SCHEDULES | CA

Daily Schedules
Daily - Sales

7.4. Restart Service

From the CT Suite server, select **Start → Control Panel → Administrative Tools → Services** to display the **Services** screen. Locate and restart the **CTS Open Queue Server Service**, as shown below.



CTS Open Queue Server Service

Stop the service
Restart the service

Description:
Manages the routing of CT Suite and third party multimedia work items through Avaya Communication Manager.

Name	Description	Status	Startu
CTS Logger Server	Logger Serv...	Running	Auton
CTS Monitor Server Service	Provides rea...	Running	Auton
CTS Open Queue Server Service	Manages th...	Running	Auton
CTS Outbound Call List Service	Manages th...	Running	Auton
CTS RethinkDB	Provides Re...	Running	Manu
CTS Template Maintenance	Provides m...	Running	Auton
DCOM Server Process Launcher	The DCOM...	Running	Auton
Device Association Service	Enables pair...		Manu
Device Install Service	Enables a c...		Manu
Device Setup Manager	Enables the ...	Running	Manu
DHCP Client	Registers an...	Running	Auton
Diagnostic Policy Service	The Diagno...	Running	Auton
Diagnostic Service Host	The Diagno...		Manu

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Application Enablement Services, and CT Suite.

8.1. Verify Avaya Aura® Communication Manager

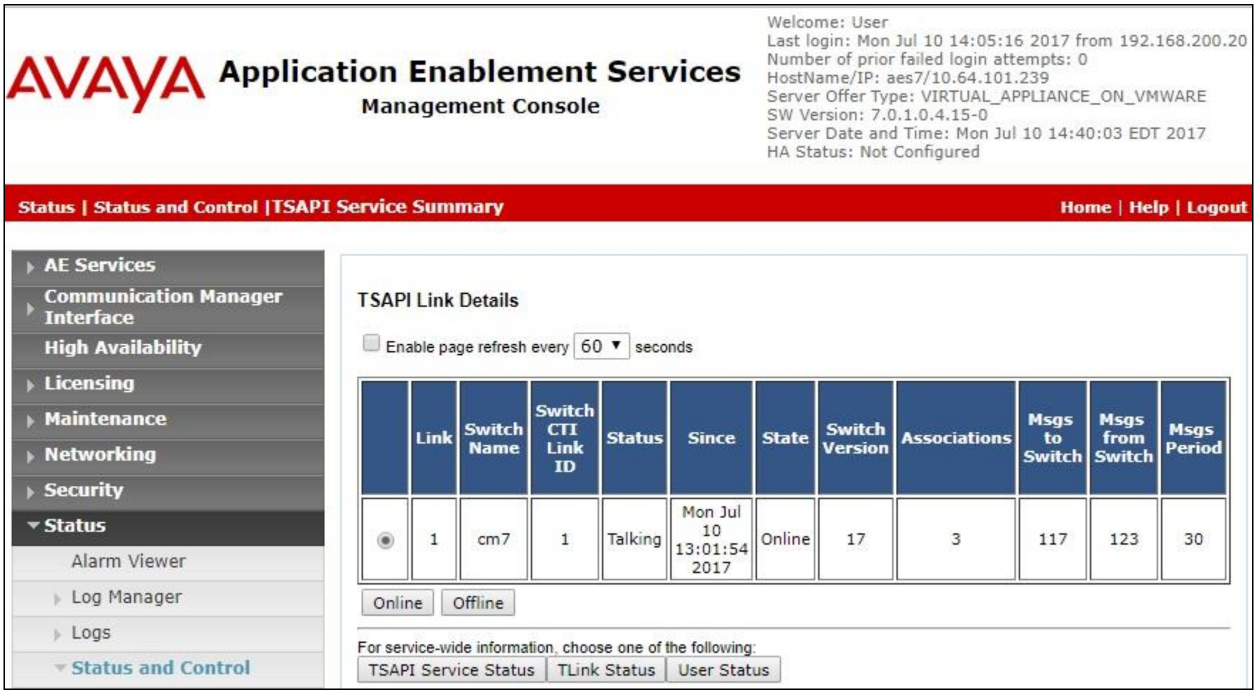
On Communication Manager, verify the status of the administered CTI link by using the “status aesvcs cti-link” command. Verify that the **Service State** is “established”, as shown below.

```
status aesvcs cti-link

                          AE SERVICES CTI LINK STATUS

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

1     7        no    aes7             established    118       112
```

8.2. Verify Avaya Aura® Application Enablement Services

On Application Enablement Services, verify the status of the TSAPI service by selecting **Status → Status and Control → TSAPI Service Summary** (not shown) from the left pane. The **TSAPI Link Details** screen is displayed.

Verify that the **Status** is “Talking”, and that the **Associations** column reflects the total number of agents that are logged in plus the chat VDN.



Welcome: User
Last login: Mon Jul 10 14:05:16 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Mon Jul 10 14:40:03 EDT 2017
HA Status: Not Configured

TSAPI Link Details

□ Enable page refresh every 60 ▼ seconds

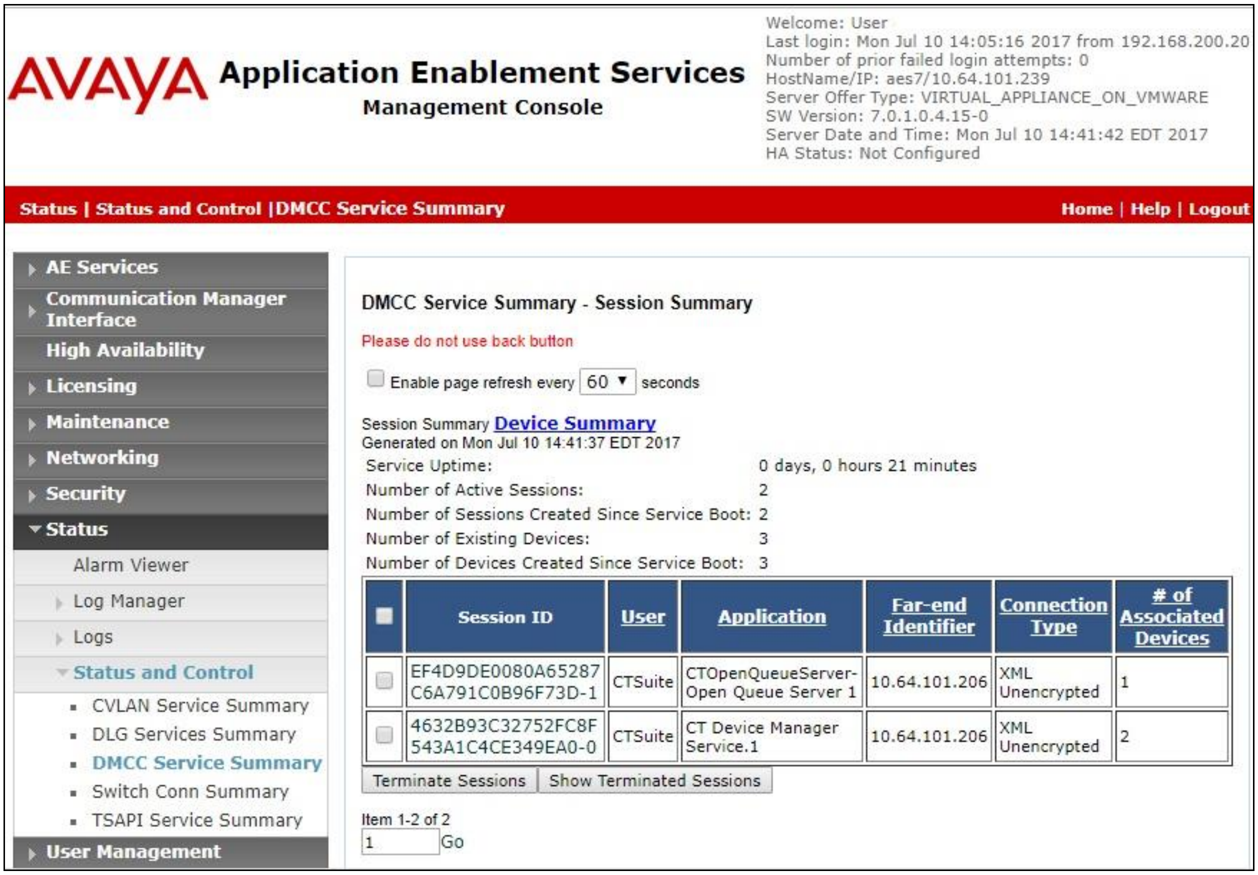
	Link	Switch Name	Switch CTI Link ID	Status	Since	State	Switch Version	Associations	Msgs to Switch	Msgs from Switch	Msgs Period
●	1	cm7	1	Talking	Mon Jul 10 13:01:54 2017	Online	17	3	117	123	30

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

Verify the status of the DMCC connections by selecting **Status → Status and Control → DMCC Service Summary** from the left pane. The **DMCC Service Summary – Session Summary** screen is displayed.

Verify there is an action session with "CTOpenQueueServer" as the **Application**, and with the CT Suite user name from **Section 6.3** as **User**. Also verify that the **# of Associated Devices** column reflects the total number of chat VDNs, in this case "1".

Note that the action session with "CT Device Manager" as the **Application** is used for voice integration with the Device Manager component of CT Suite, as documented in reference [3].



Welcome: User
Last login: Mon Jul 10 14:05:16 2017 from 192.168.200.20
Number of prior failed login attempts: 0
HostName/IP: aes7/10.64.101.239
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 7.0.1.0.4.15-0
Server Date and Time: Mon Jul 10 14:41:42 EDT 2017
HA Status: Not Configured

DMCC Service Summary - Session Summary

Please do not use back button

□ Enable page refresh every 60 ▾ seconds

Session Summary Device Summary
Generated on Mon Jul 10 14:41:37 EDT 2017

Service Uptime:	0 days, 0 hours 21 minutes
Number of Active Sessions:	2
Number of Sessions Created Since Service Boot:	2
Number of Existing Devices:	3
Number of Devices Created Since Service Boot:	3

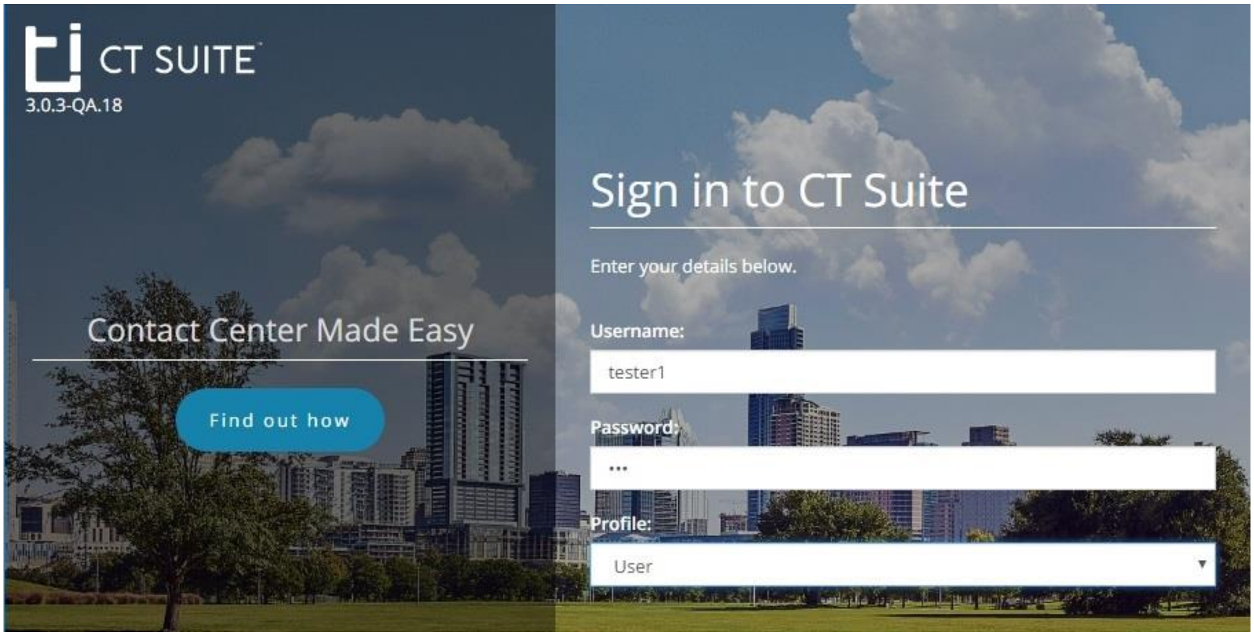
■	Session ID	User	Application	Far-end Identifier	Connection Type	# of Associated Devices
□	EF4D9DE0080A65287C6A791C0B96F73D-1	CTSuite	CTOpenQueueServer-Open Queue Server 1	10.64.101.206	XML Unencrypted	1
□	4632B93C32752FC8F543A1C4CE349EA0-0	CTSuite	CT Device Manager Service.1	10.64.101.206	XML Unencrypted	2

Item 1-2 of 2
1

8.3. Verify CTIntegrations CT Suite

From an agent PC, launch an Internet browser window and enter the URL "http://ip-address:8081", where "ip-address" is the IP address of the CT Suite server.

The **Sign in to CT Suite** screen is displayed. For **Username** and **Password**, enter an applicable agent credentials, and retain the default value in the remaining field.



Sign in to CT Suite

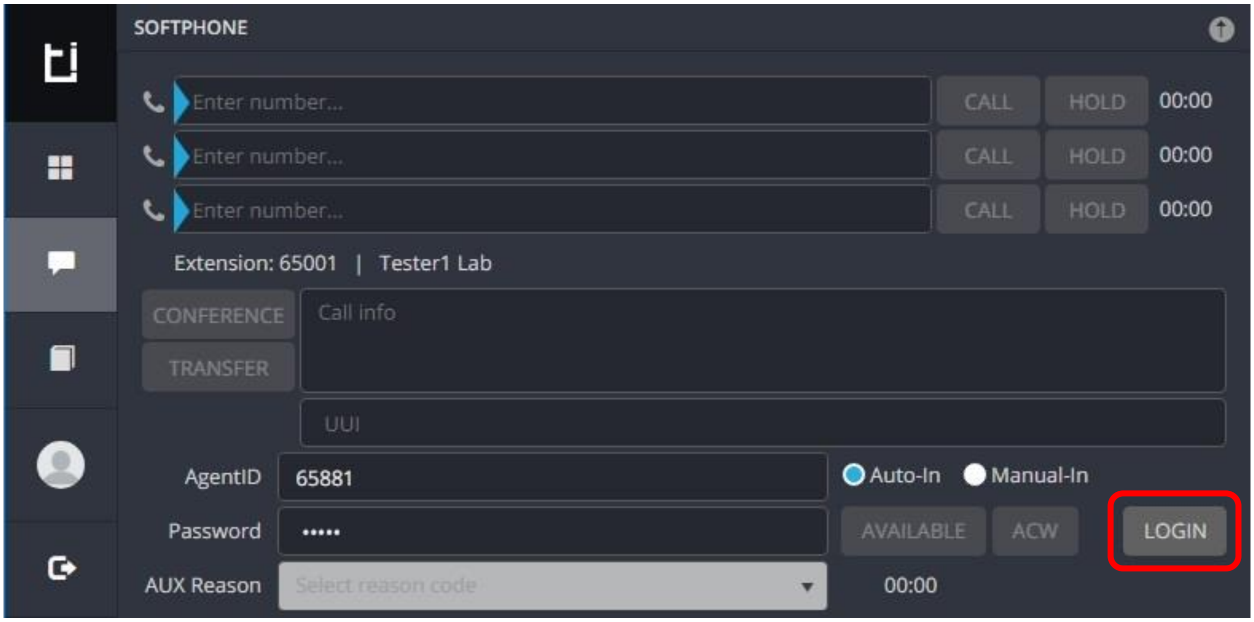
Enter your details below.

Username: tester1

Password: •••

Profile: User

The agent screen below is displayed next. Retain the default values, and select **LOGIN** to log the agent into Communication Manager.



Extension: 65001 | Tester1 Lab

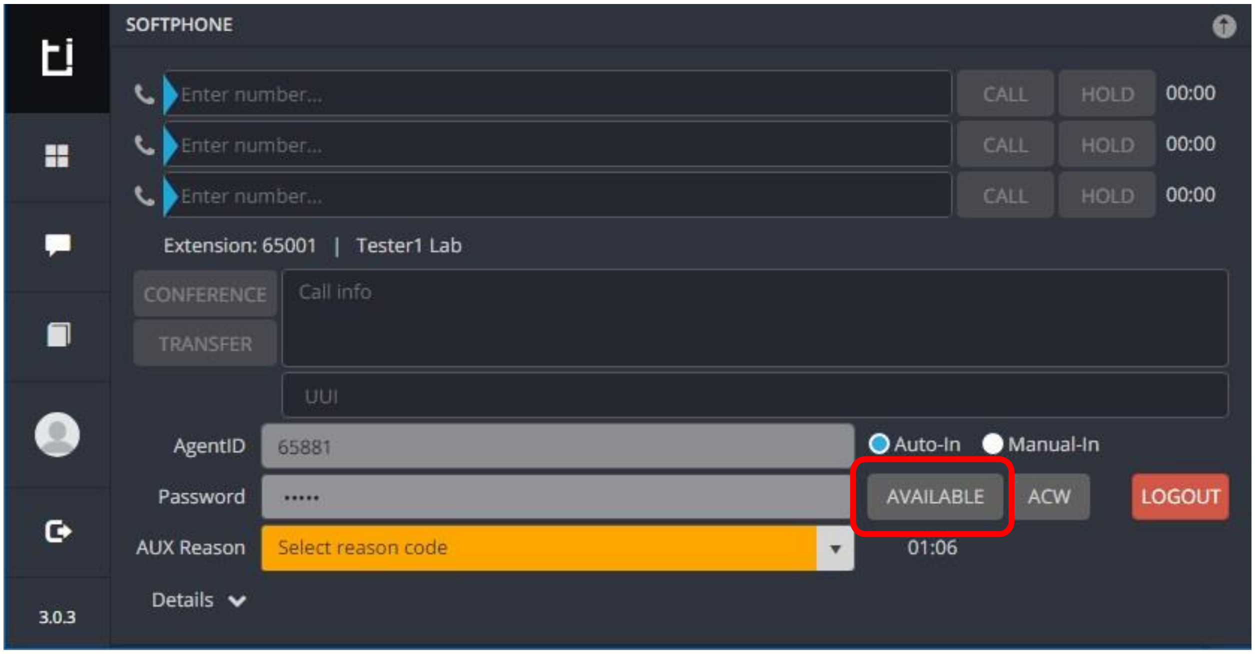
AgentID: 65881

● Auto-In ○ Manual-In

Password: •••••

AUX Reason: Select reason code

The agent screen is updated, as shown below. Click **AVAILABLE**.



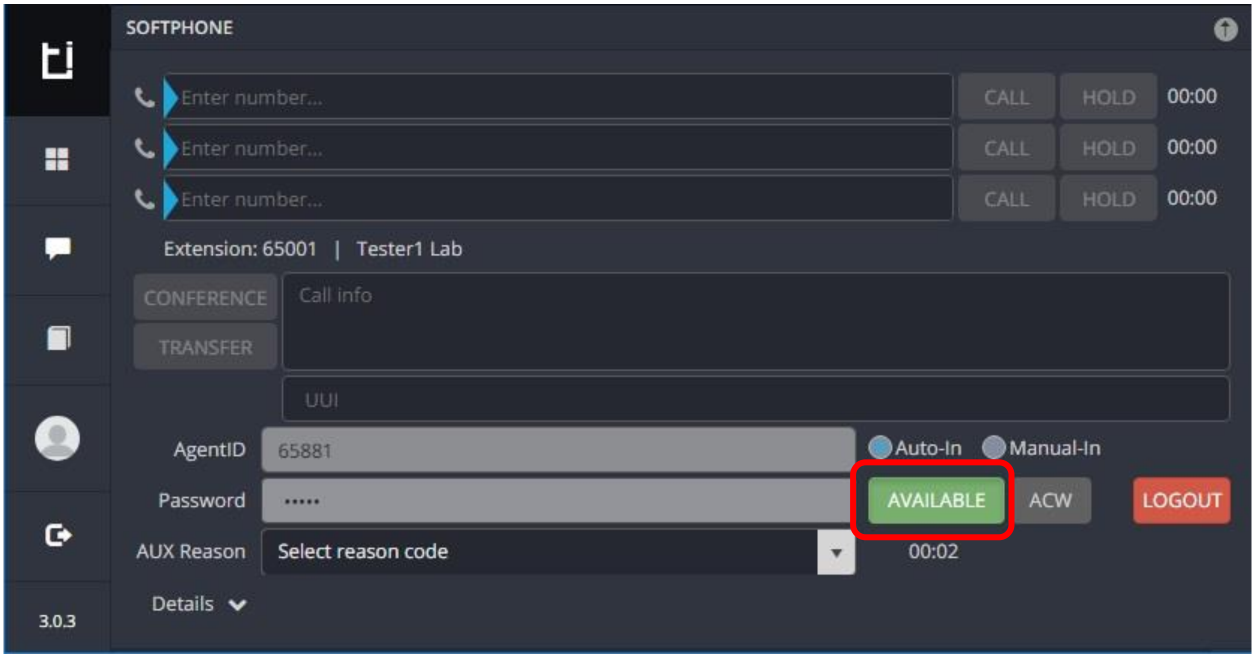
Extension: 65001 | Tester1 Lab

AgentID 65881

Password •••••

AUX Reason Select reason code

Verify that the agent screen is updated, with the **AVAILABLE** icon shown in green below.



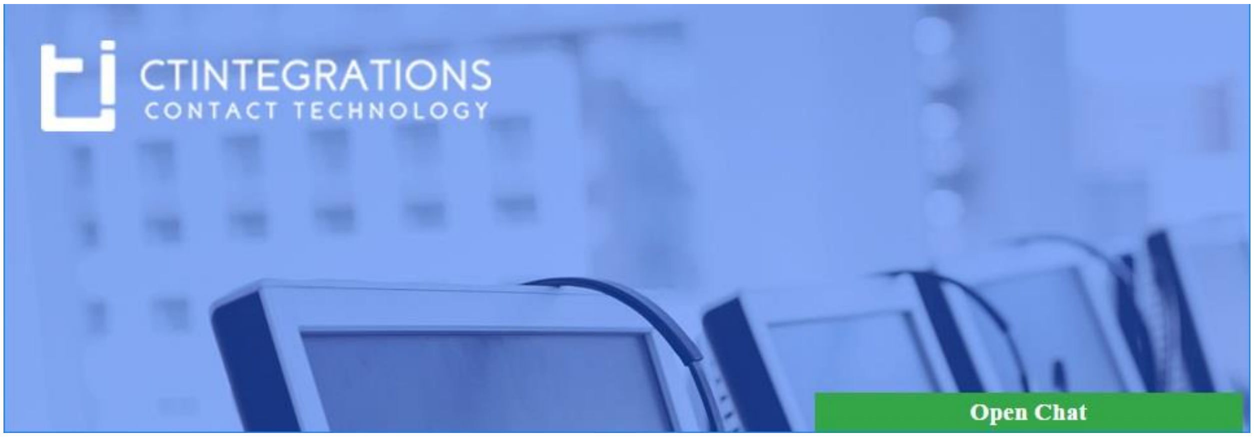
Extension: 65001 | Tester1 Lab

AgentID 65881

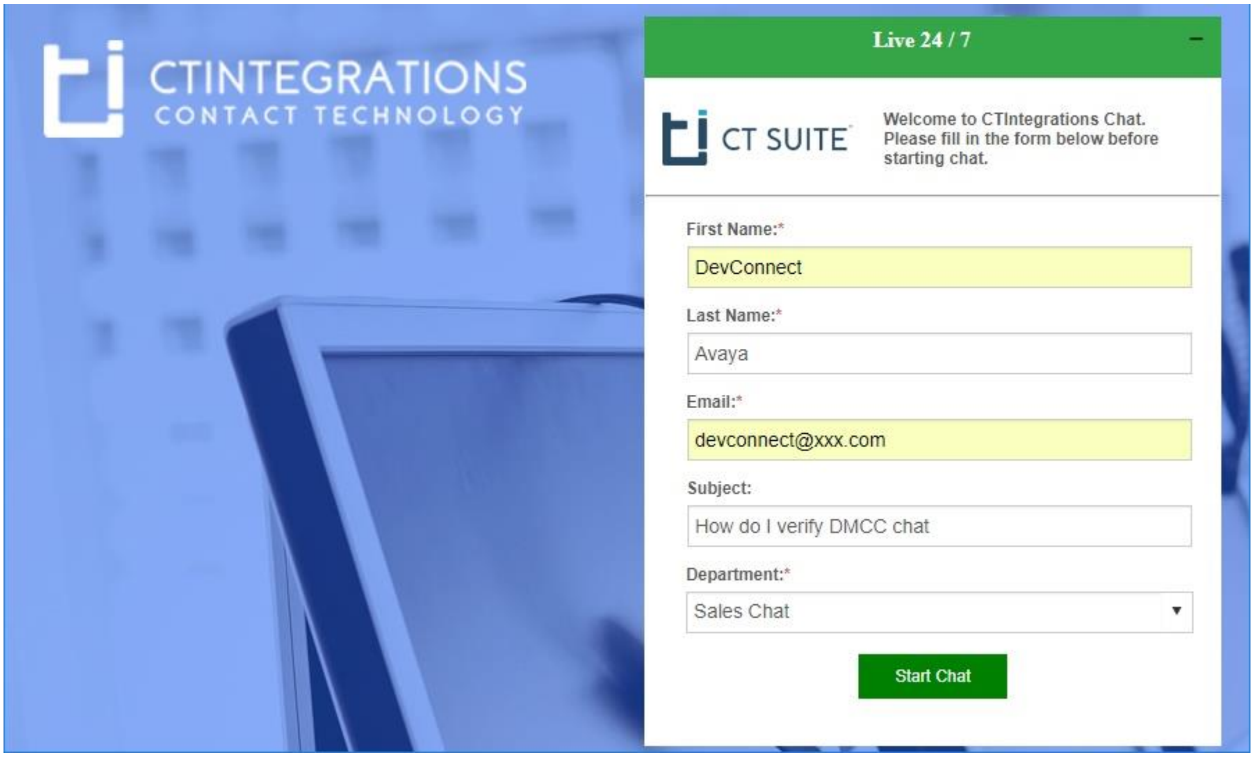
Password •••••

AUX Reason Select reason code

From a PC on the intranet, launch an Internet browser window and enter the URL http://ip-address:3000 to start a chat session, where "ip-address" is the IP address of the CT Suite server. The screen below is displayed, select **Open Chat**.



The screen is updated as shown below. Fill out the parameters as desired. For **Department**, select the chat queue name from **Section 7.3.3**. Click **Start Chat**.



Welcome to CTIntegrations Chat. Please fill in the form below before starting chat.

First Name:* DevConnect

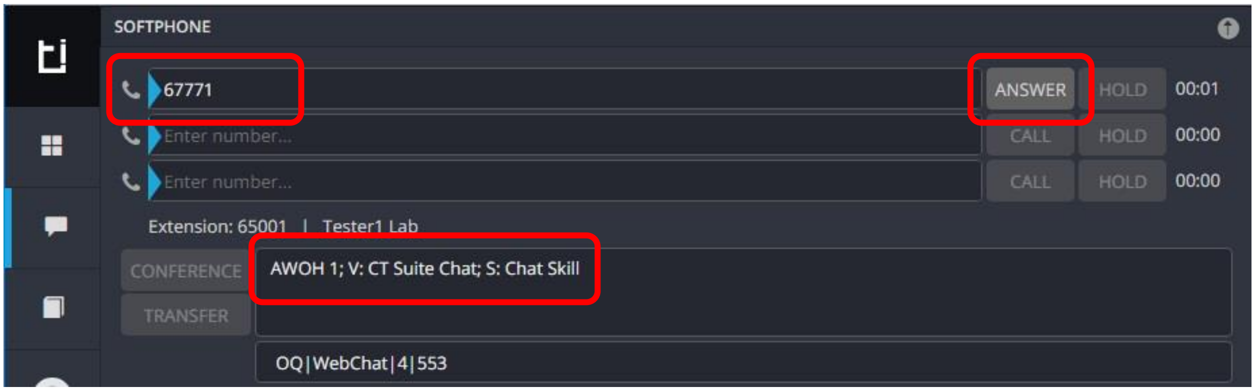
Last Name:* Avaya

Email:* devconnect@xxx.com

Subject: How do I verify DMCC chat

Department:* Sales Chat

Verify that the top section of the available agent's screen is updated to reflect a CTI extension from **Section 7.2** as calling party number, along with name of chat VDN from **Section 5.3**, as shown below. Click **ANSWER**.



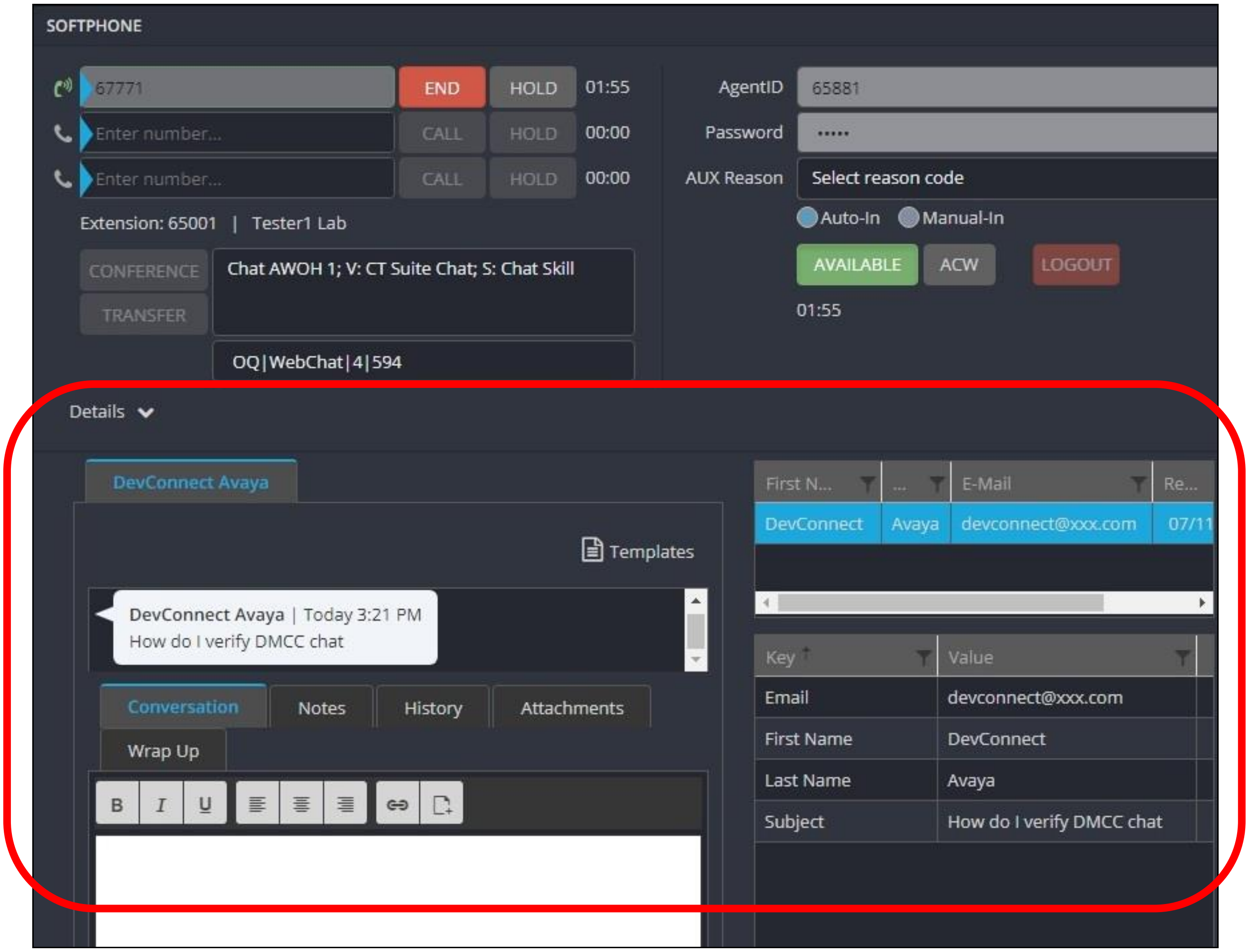
67771 — 00:01
Enter number... — 00:00
Enter number... — 00:00

Extension: 65001 | Tester1 Lab

AWOH 1; V: CT Suite Chat; S: Chat Skill

OQ|WebChat|4|553

Verify that the agent is connected to the phantom call, and that the **Details** sub-section of the agent screen is updated to reflect the content of the chat, as shown below.



67771 — 01:55
Enter number... — 00:00
Enter number... — 00:00

Extension: 65001 | Tester1 Lab

Chat AWOH 1; V: CT Suite Chat; S: Chat Skill

OQ|WebChat|4|594

AgentID: 65881
Password: •••••
AUX Reason: Select reason code
○ Auto-In ○ Manual-In

01:55

DevConnect Avaya | Today 3:21 PM
How do I verify DMCC chat

First N...	...	E-Mail	Re...
DevConnect	Avaya	devconnect@xxx.com	07/11

Key	Value
Email	devconnect@xxx.com
First Name	DevConnect
Last Name	Avaya
Subject	How do I verify DMCC chat

9. Conclusion

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.0 to successfully interoperate with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for chat integration. All feature and serviceability test cases were completed.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2.1, August 2016, available at http://support.avaya.com.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 7.0.1, Issue 2, August 2016, available at http://support.avaya.com.

3. *Application Notes for CTIntegrations CT Suite 3.0 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Application Enablement Services 7.0 for Voice Channel Integration*, Release 1.0, available at http://support.avaya.com.

4. *CT Admin Administrator's Guide*, CT Suite v3.0, 5/30/17, available at https://www.ctintegrations.com/docs.

5. *CT Suite Web Client*, Web Client User Guide, CT Suite R3.0, 5/30/17, available at https://www.ctintegrations.com/docs.

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.