



Avaya Solution & Interoperability Test Lab

Application Notes for CTIntegrations CT Suite 3.0 with Avaya Aura® Communication Manager 7.0 and Avaya Aura® Session Manager 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® Session Manager 7.0 for chat integration. CTIntegrations CT Suite is a contact center solution.

In the compliance testing, CTIntegrations CT Suite used the SIP trunks interface from Avaya Aura® Session 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® Session Manager 7.0 for chat integration. CT Suite is a contact center solution.

In the compliance testing, CT Suite used the SIP trunks interface from Session Manager to support delivery of chat work items to agents. The CT Suite solution consists of a CT Suite server with Open Queue and Device Manager components, and a CT Suite Communication Server.

The CT Suite Communication Server connects to Session Manager via SIP trunks, and consists of the FreeSWITCH open source application server component acting as a SIP gateway, and the FusionPBX open source application component providing a graphical user interface for FreeSWITCH.

The Open Queue component of CT Suite initiates a SIP call for each chat work item, using an available local SIP extension on CT Suite Communication Server as calling party and the applicable chat VDN on Communication Manager as destination. Once the SIP 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 CT Suite Communication Server and the Open Queue component of CT Suite with Session Manager for support of chat work items, and assume the integration between the Device Manager component of CT Suite with Application Enablement Services for screen pop and call control is already in place as documented in reference [5].

2. General Test Approach and Test Results

The feature test cases were performed both manually. 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 and CT Suite Communication 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 Session Manager 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 included chat scenarios involving G.711, media shuffling, screen pop, hold/resume, drop, 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 CT Suite server and CT Suite Communication Server.

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

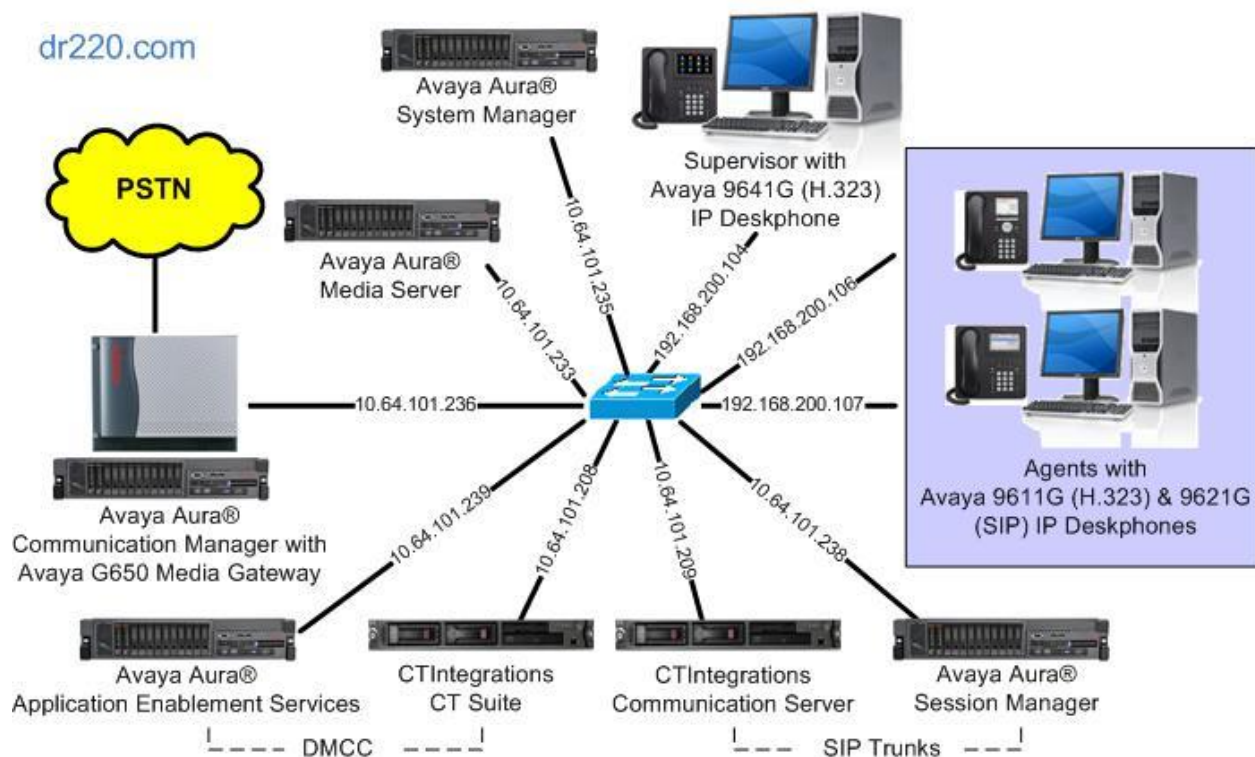


Figure 1: Compliance Testing Configuration

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 <ul style="list-style-type: none">CT AdminCT Web ClientCT Device ManagerCT Open QueueAvaya 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
CTIntegrations CT Suite Communication Server on Debian <ul style="list-style-type: none">FreeSWITCHFusionPBX	NA 8.6 1.6.13 4.2.0

5. Configure Avaya Aura® Communication Manager

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

- Verify license
- Administer SIP trunk group
- Administer SIP signaling group
- Administer SIP trunk group members
- Administer IP network region
- Administer IP codec set
- Administer chat skill
- Administer chat vector and VDN
- Administer agent IDs

In the compliance testing, a separate set of codec set, network region, trunk group, and signaling group were used for integration with CT Suite.

5.1. Verify License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column.

The license file installed on the system controls the maximum permitted. If there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

display system-parameters customer-options		Page 2 of 12
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	12000	10
Maximum Concurrently Registered IP Stations:	18000	4
Maximum Administered Remote Office Trunks:	12000	0
Maximum Concurrently Registered Remote Office Stations:	18000	0
Maximum Concurrently Registered IP eCons:	414	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	41000	0
Maximum Video Capable IP Softphones:	18000	0
Maximum Administered SIP Trunks:	24000	30
Maximum Administered Ad-hoc Video Conferencing Ports:	24000	0
Maximum Number of DS1 Boards with Echo Cancellation:	522	0

5.2. Administer SIP Trunk Group

Use the “add trunk-group n” command, where “n” is an available trunk group number, in this case “53”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Group Name:** A descriptive name.
- **TAC:** An available trunk access code.
- **Service Type:** “public-ntwrk”

add trunk-group 53		Page 1 of 22	
TRUNK GROUP			
Group Number: 53	Group Type: sip	CDR Reports: y	
Group Name: CT Suite Chat	COR: 1	TN: 1	TAC: 1053
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
	Member Assignment Method: auto		
	Signaling Group:		
	Number of Members: 0		

Navigate to **Page 3**. Enter “private” for **Numbering Format**, and “shared” for **UUI Treatment**.

add trunk-group 53		Page 3 of 22	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Suppress # Outpulsing? n	Numbering Format: private		
	UUI Treatment: shared		
	Replace Restricted Numbers? n		
	Replace Unavailable Numbers? n		
	Hold/Unhold Notifications? y		
	Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y			

5.3. Administer SIP Signaling Group

Use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “53”. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Group Type:** “sip”
- **Near-end Node Name:** An existing C-LAN node name or “procr” in this case.
- **Far-end Node Name:** The existing Session Manager node name.
- **Near-end Listen Port:** An available port for integration with CT Suite.
- **Far-end Listen Port:** The same port number as in **Near-end Listen Port**.
- **Far-end Network Region:** An existing network region to use with CT Suite.
- **Far-end Domain:** The applicable domain name for the network.

```
add signaling-group 53                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 53                Group Type: sip
IMS Enabled? n                  Transport Method: tls
Q-SIP? n
IP Video? n                    Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: Others
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? n
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? y
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                Far-end Node Name: sm7-sig
Near-end Listen Port: 5053              Far-end Listen Port: 5053
                                     Far-end Network Region: 3
Far-end Domain: dr220.com
```

5.4. Administer SIP Trunk Group Members

Use the “change trunk-group n” command, where “n” is the trunk group number from **Section 5.2**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Signaling Group:** The signaling group number from **Section 5.3**.
- **Number of Members:** The desired number of members, in this case “10”.

```
change trunk-group 53                                     Page 1 of 22
                                     TRUNK GROUP

Group Number: 53                Group Type: sip                CDR Reports: y
Group Name: CT Suite Chat        COR: 1                TN: 1                TAC: 1053
Direction: two-way              Outgoing Display? n
Dial Access? n                  Night Service:
Queue Length: 0
Service Type: public-ntwrk      Auth Code? n
                                     Member Assignment Method: auto
                                     Signaling Group: 53
                                     Number of Members: 10
```


5.5. Administer IP Network Region

Use the “change ip-network-region n” command, where “n” is the existing far-end network region number used by the SIP signaling group from **Section 5.3**.

For **Authoritative Domain**, enter the applicable domain for the network. Enter a descriptive **Name**. Enter “yes” for **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio**, as shown below. For **Codec Set**, enter an available codec set number for integration with CT Suite.

change ip-network-region 3		Page 1 of 20	
IP NETWORK REGION			
Region: 3			
Location:		Authoritative Domain: dr220.com	
Name: CT Suite		Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 3		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048		IP Audio Hairpinning? n	
UDP Port Max: 3329			
DIFFSERV/TOS PARAMETERS			
Call Control PHB Value: 46			
Audio PHB Value: 46			
Video PHB Value: 26			

Navigate to **Page 4**, and specify this codec set to be used for calls with the network region used by the Avaya endpoints. In the compliance testing, network region “1” was used by the Avaya endpoints.

change ip-network-region 3										Page 4 of 20			
Source Region: 3 Inter Network Region Connection Management										I	M		
										G	A	t	
dst codec direct	WAN-BW-limits			Video		Intervening			Dyn	A	G	c	
rgn set	WAN	Units	Total	Norm	Prio	Shr	Regions			CAC	R	L	e
1	3	y	NoLimit								n	t	
2													

5.6. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from **Section 5.5**. Update the audio codec types in the **Audio Codec** fields as necessary. Note that CT Suite supports the G.711 and G.729 codec variants, with G.729 requiring special configuration on CT Suite. The compliance testing only covered the G.711 codec.

change ip-codec-set 5				Page 1 of 2	
IP Codec Set					
Codec Set: 5					
Audio		Silence		Frames	
Codec		Suppression		Per Pkt	
1: G.711MU		n		2	
2:				20	

5.7. 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			
Security Code:		MM Early Answer? n	
ISDN/SIP Caller Display:		Local Agent Preference? n	

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			

5.8. 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	

5.9. 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 5.7** 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	/	/	/	/	/	/

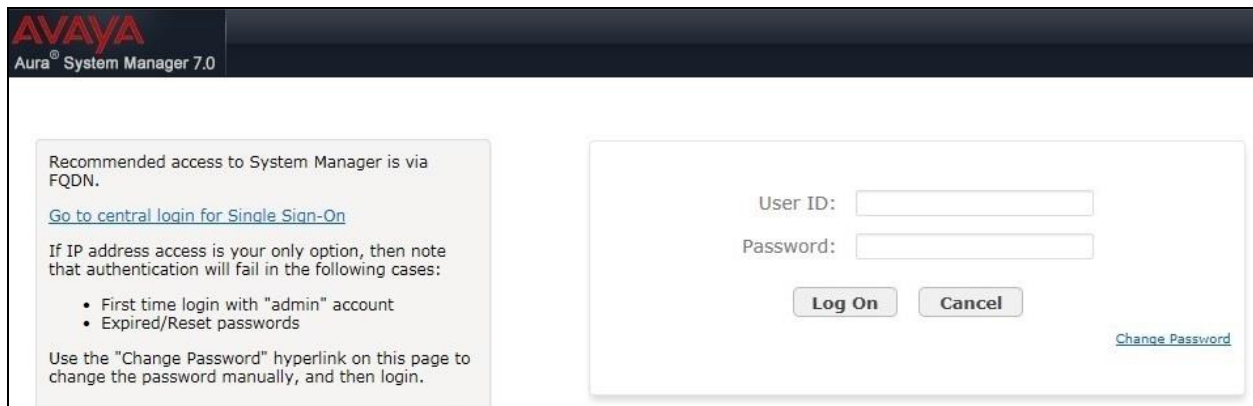
6. Configure Avaya Aura® Session Manager

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

- Launch System Manager
- Administer locations
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

6.1. Launch System Manager

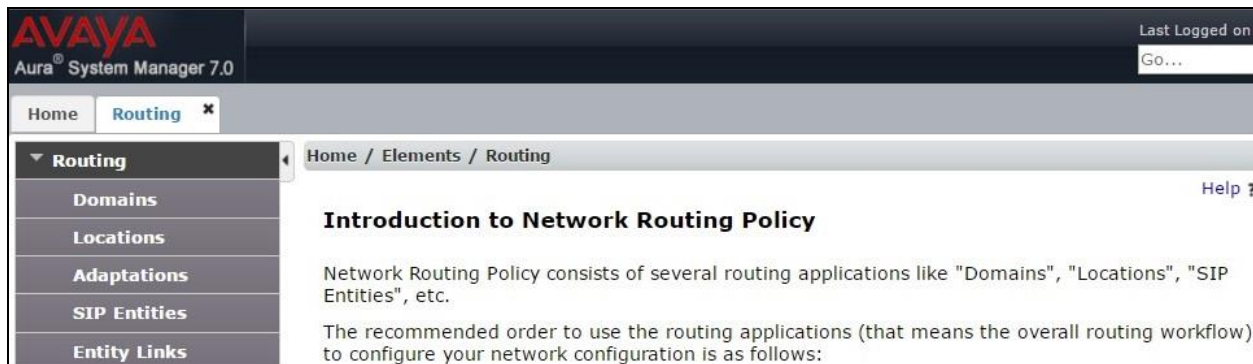
Access the System Manager web interface by using the URL “https://ip-address” in an Internet browser window, where “ip-address” is the IP address of System Manager. Log in using the appropriate credentials.



The screenshot shows the Avaya Aura System Manager 7.0 login interface. The header includes the Avaya logo and the text 'Aura® System Manager 7.0'. The main content area is divided into two sections. The left section contains instructions: 'Recommended access to System Manager is via FQDN.' with a link 'Go to central login for Single Sign-On', and 'If IP address access is your only option, then note that authentication will fail in the following cases:' followed by a bulleted list: 'First time login with "admin" account' and 'Expired/Reset passwords'. It also mentions using the 'Change Password' hyperlink. The right section is a login form with fields for 'User ID:' and 'Password:', and buttons for 'Log On' and 'Cancel'. A 'Change Password' link is located at the bottom right of the login form.

6.2. Administer Locations

In the subsequent screen (not shown), select **Elements** → **Routing** to display the **Introduction to Network Routing Policy** screen below. Select **Routing** → **Locations** from the left pane, and click **New** in the subsequent screen (not shown) to add a new location for CT Suite.



The screenshot shows the Avaya Aura System Manager 7.0 interface after navigating to the Routing section. The header includes the Avaya logo and the text 'Aura® System Manager 7.0'. The top navigation bar shows 'Home' and 'Routing' (selected). The left pane shows a tree view with 'Routing' expanded, containing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', and 'Entity Links'. The main content area displays the 'Introduction to Network Routing Policy' screen. It includes a breadcrumb trail 'Home / Elements / Routing' and a 'Help ?' link. The text on the screen states: 'Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.' and 'The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:'.

The **Location Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name** and optional **Notes**. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.0

Home Routing

Home / Elements / Routing / Locations

Location Details

General

* Name: CTI-Loc

Notes: CTIntegrations CT Suite

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Scroll down to the **Location Pattern** sub-section, click **Add** and enter the IP address of the CT Suite Communication Server in **IP Address Pattern**, as shown below. Retain the default values in the remaining fields.

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

1 Item Filter: Enable

IP Address Pattern	Notes
* 10.64.101.207	CT Suite

Select : All, None

6.3. Administer SIP Entities

Add two new SIP entities, one for CT Suite and one for the new SIP trunks with Communication Manager.

6.3.1. SIP Entity for CT Suite

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for CT Suite.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the CT Suite Communication Server.
- **Type:** “SIP Trunk”
- **Location:** Select the CT Suite location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a 'Routing' menu with options: Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form fields are as follows:

- Name:** CTSuite
- FQDN or IP Address:** 10.64.101.207
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** CTI-Loc
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** egress
- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DR-SM7”.
- **Protocol:** “UDP”
- **Port:** “5060”
- **SIP Entity 2:** The CT Suite entity name from this section.
- **Port:** “5060”
- **Connection Policy:** “trusted”

Note that CT Suite can support UDP and TCP, and the compliance testing used the UDP protocol.

Entity Links

Override Port & Transport with DNS ☐ SRV: ☐

Add Remove

1 Item
Filter: Enable

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* DR-SM7_CTSuite_5060	DR-SM7	UDP	* 5060	CTSuite	* 5060	trusted

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items
Filter: Enable

	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--	-------------------------------	---------------------	-------

Commit Cancel

6.3.2. SIP Entity for Communication Manager

Select **Routing** → **SIP Entities** from the left pane, and click **New** in the subsequent screen (not shown) to add a new SIP entity for Communication Manager. Note that this SIP entity is used for integration with CT Suite.

The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of an existing CLAN or the processor interface.
- **Type:** “CM”
- **Notes:** Any desired notes.
- **Adaptation:** Select the applicable adaptation for Communication Manager.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.

AVAYA
Aura® System Manager 7.0

Last Logged on: Go...

Home Routing x

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit

General

* Name: DR-CM7-5053

* FQDN or IP Address: 10.64.101.236

Type: CM

Notes: CM Port 5053 (CTIntegrations CT Suite)

Adaptation: DR-CM7-Adaptation

Location: DR-Loc

Time Zone: America/New_York

* SIP Timer B/F (in seconds): 4

Credential name:

Securable: ☐

Call Detail Recording: none

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

Scroll down to the **Entity Links** sub-section, and click **Add** to add an entity link. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Name:** A descriptive name.
- **SIP Entity 1:** The Session Manager entity name, in this case “DR-SM7”.
- **Protocol:** The signaling group transport method from **Section 5.3**.
- **Port:** The signaling group far-end listen port number from **Section 5.3**.
- **SIP Entity 2:** The Communication Manager entity name from this section.
- **Port:** The signaling group near-end listen port number from **Section 5.3**.
- **Connection Policy:** “trusted”

Entity Links

Override Port & Transport with DNS ☐
SRV: ☐

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	* DR-SM7_DR-CM7-5053	DR-SM7 ▼	TLS ▼	* 5053	DR-CM7-5053 ▼	* 5053	trusted ▼

Select : All, None

SIP Responses to an OPTIONS Request

Add Remove

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

6.4. Administer Routing Policies

Add a new routing policy for routing of chat calls from CT Suite to Communication Manager.

Select **Routing → Routing Policies** from the left pane, and click **New** in the subsequent screen (not shown) to add a new routing policy to Communication Manager.

The **Routing Policy Details** screen is displayed. In the **General** sub-section, enter a descriptive **Name**. Enter optional **Notes**, and retain the default values in the remaining fields.

In the **SIP Entity as Destination** sub-section, click **Select** and select the Communication Manager entity name from **Section 6.3.2**. The screen below shows the result of the selection.

AVAYA
Aura® System Manager 7.0

Last Logged
Go...

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit

General

* Name: To-CM7-5053

Disabled: ☐

* Retries: 0

Notes: To CM7 port 5053 from CT Suite

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
DR-CM7-5053	10.64.101.236	CM	CM Port 5053 (CTIntegrations CT Suite)

6.5. Administer Dial Patterns

Update existing dial patterns for Communication Manager to allow calls from CT Suite.

Select **Routing → Dial Patterns** from the left pane, and click on the applicable dial pattern for Communication Manager in the subsequent screen, in this case dial pattern “6” (not shown). The **Dial Pattern Details** screen is displayed.

In the **Originating Locations and Routing Policies** sub-section, click **Add** and create a new entry as necessary for calls from CT Suite. In the compliance testing, the new entry allowed for call origination from the CT Suite location from **Section 6.2**, and the Communication Manager routing policy from **Section 6.4** was selected as shown below. Retain the default values in the remaining fields.

AVAYA
Aura® System Manager 7.0

Last Logged on at
Go...

Home Routing *
Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Ca

General

* Pattern: 6

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes: To CM7

Originating Locations and Routing Policies

Add Remove

3 Items

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	CTI-Loc	CTIntegrations CT Suite	To-CM7- 5053	0	<input type="checkbox"/>	DR-CM7-5053
<input type="checkbox"/>	DR-Loc	TLT DR Network	To-CM7	0	<input type="checkbox"/>	DR-CM7
<input type="checkbox"/>	NJ-Loc	TLT NJ Network	To-CM7	0	<input type="checkbox"/>	DR-CM7

Select : All, None

7. Configure CTIntegrations CT Suite

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

- Launch FusionPBX
- Administer gateways
- Administer destinations
- Administer outbound routes
- Administer SIP extensions
- 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.

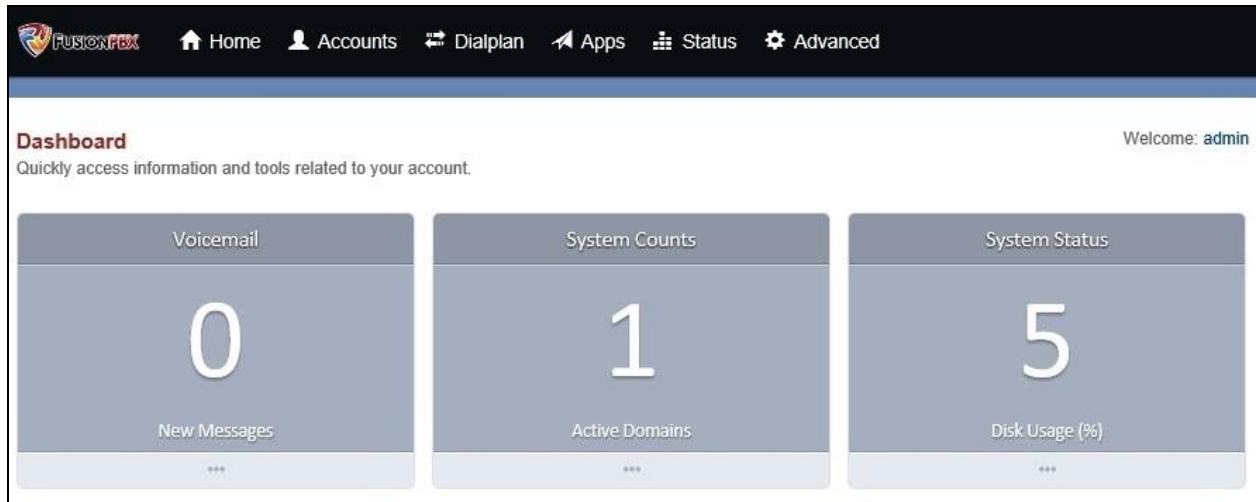
7.1. Launch FusionPBX

Access the FusionPBX web interface by using the URL “http://ip-address” in an Internet browser window, where “ip-address” is the IP address of the CT Suite Communication Server. The **FUSIONPBX** screen below is displayed. Log in using the administrator credentials.



7.2. Administer Gateways

The **Dashboard** screen below is displayed. Select **Accounts** → **Gateways** from the top menu.



The **Gateways** screen is displayed next. Select the add icon shown below.



The **Gateway** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

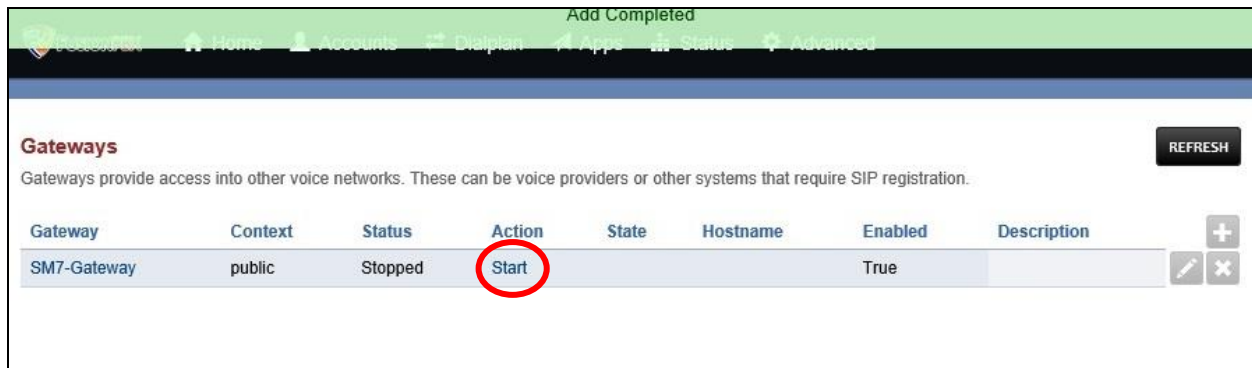
- **Gateway:** A descriptive name.
- **Username:** A desired value.
- **Password:** A desired value.
- **From Domain:** The applicable domain name from **Section 3**.
- **Proxy:** IP address of the Session Manager signaling interface.
- **Realm:** The applicable domain name from **Section 3**.
- **Register:** “False”
- **Profile:** “Internal”

Gateway BACK SAVE

Defines a connections to a SIP Provider or another SIP server.

Gateway	<input type="text" value="SM7-Gateway"/>	Enter the gateway name here.
Username	<input type="text" value="CTI"/>	Enter the username here.
Password	<input type="password" value="••"/>	Enter the password here.
From User	<input type="text"/>	Enter the from-user here.
From Domain	<input type="text" value="dr220.com"/>	Enter the from-domain here.
Proxy	<input type="text" value="10.64.101.238"/>	Enter the domain or IP address of the proxy.
Realm	<input type="text" value="dr220.com"/>	Enter the realm here.
Expire Seconds	<input type="text" value="800"/>	Enter the expire-seconds here.
Register	<input type="text" value="False"/>	Choose whether to register.
Retry Seconds	<input type="text" value="30"/>	Enter the retry-seconds here.
	ADVANCED	
Context	<input type="text" value="public"/>	Enter the context here.
Profile	<input type="text" value="internal"/>	Enter the profile here.

The **Gateways** screen is displayed again, showing the newly added gateway entry. Click **Start** to start the gateway.

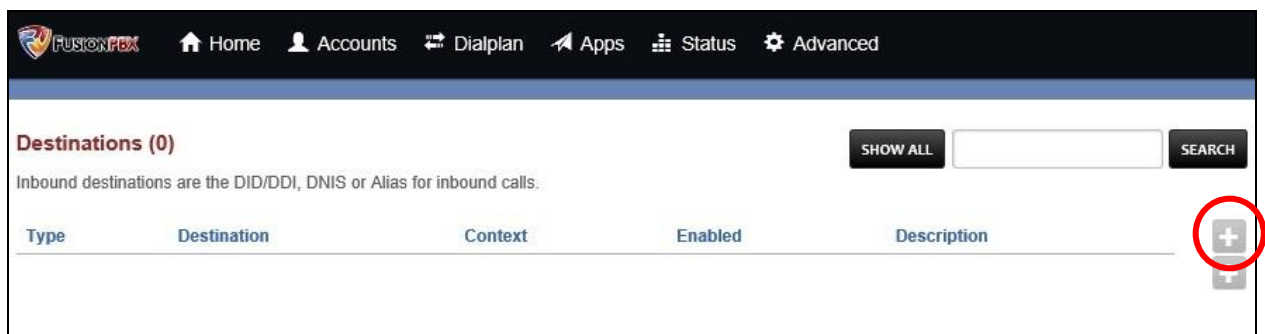


The screenshot shows the 'Gateways' management interface. At the top, a green banner indicates 'Add Completed'. The navigation bar includes Home, Accounts, Dialplan, Apps, Status, and Advanced. The main heading is 'Gateways' with a 'REFRESH' button. A descriptive text states: 'Gateways provide access into other voice networks. These can be voice providers or other systems that require SIP registration.' Below this is a table with columns: Gateway, Context, Status, Action, State, Hostname, Enabled, and Description. A single entry, 'SM7-Gateway', is listed with Context 'public' and Status 'Stopped'. The 'Action' column for this entry contains a 'Start' button, which is circled in red. To the right of the table are icons for adding (+), editing (pencil), and deleting (X) a gateway.

Gateway	Context	Status	Action	State	Hostname	Enabled	Description
SM7-Gateway	public	Stopped	Start			True	

7.3. Administer Destinations

Select **Dialplan** → **Destinations** from the top menu, to display the **Destinations** screen. Select the add icon shown below.

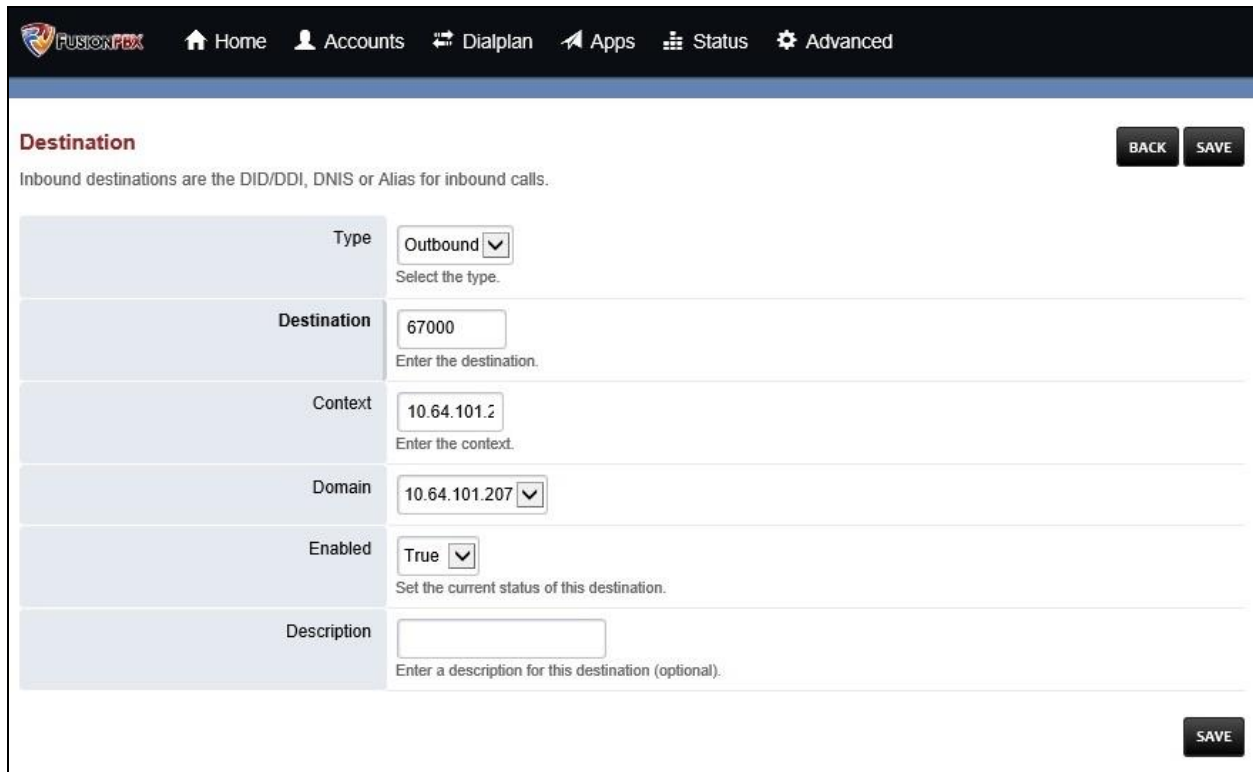


The screenshot shows the 'Destinations' management interface. The navigation bar is the same as the previous screen. The main heading is 'Destinations (0)' with a 'SHOW ALL' button and a search bar. A descriptive text states: 'Inbound destinations are the DID/DDI, DNIS or Alias for inbound calls.' Below this is a table with columns: Type, Destination, Context, Enabled, and Description. To the right of the table is a red circle highlighting the add icon (+).

Type	Destination	Context	Enabled	Description
------	-------------	---------	---------	-------------

The **Destination** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Type:** “Outbound”
- **Destination:** The chat VDN extension number from **Section 5.8**.



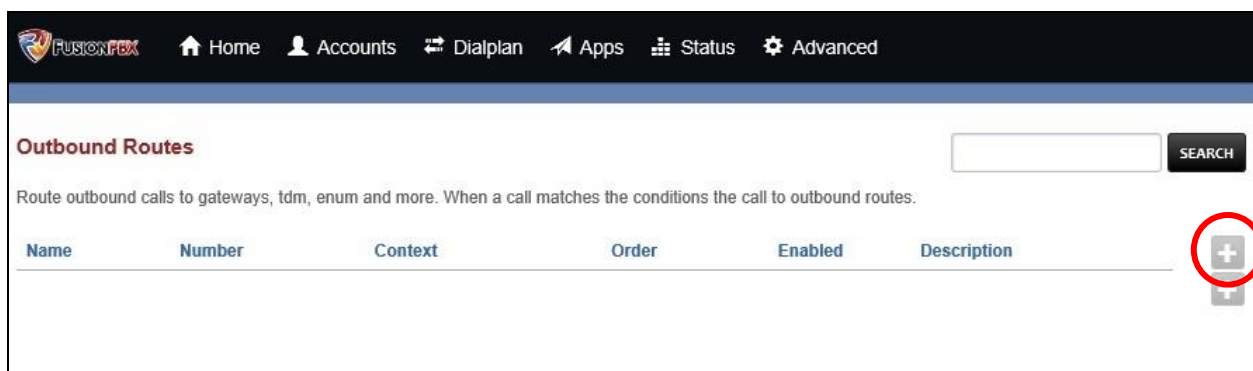
The screenshot shows the 'Destination' configuration page in FusionPBX. The top navigation bar includes 'Home', 'Accounts', 'Dialplan', 'Apps', 'Status', and 'Advanced'. The page title is 'Destination' with 'BACK' and 'SAVE' buttons. A note states: 'Inbound destinations are the DID/DDI, DNIS or Alias for inbound calls.' The form contains the following fields:

Type	Outbound	Select the type.
Destination	67000	Enter the destination.
Context	10.64.101.2	Enter the context.
Domain	10.64.101.207	
Enabled	True	Set the current status of this destination.
Description		Enter a description for this destination (optional).

A 'SAVE' button is located at the bottom right of the form.

7.4. Administer Outbound Routes

Select **Dialplan** → **Outbound Routes** from the top menu, to display the **Outbound Routes** screen. Select the add icon shown below.



The screenshot shows the 'Outbound Routes' page in FusionPBX. The top navigation bar is the same as the previous screen. The page title is 'Outbound Routes' with a search bar and 'SEARCH' button. A note states: 'Route outbound calls to gateways, tdm, enum and more. When a call matches the conditions the call to outbound routes.' Below the note is a table with the following columns: Name, Number, Context, Order, Enabled, and Description. A red circle highlights a '+' icon in the bottom right corner, which is used to add a new outbound route.

The **Outbound Routes** screen is updated. Enter the following values for the specified fields, and retain the default values for the remaining fields.

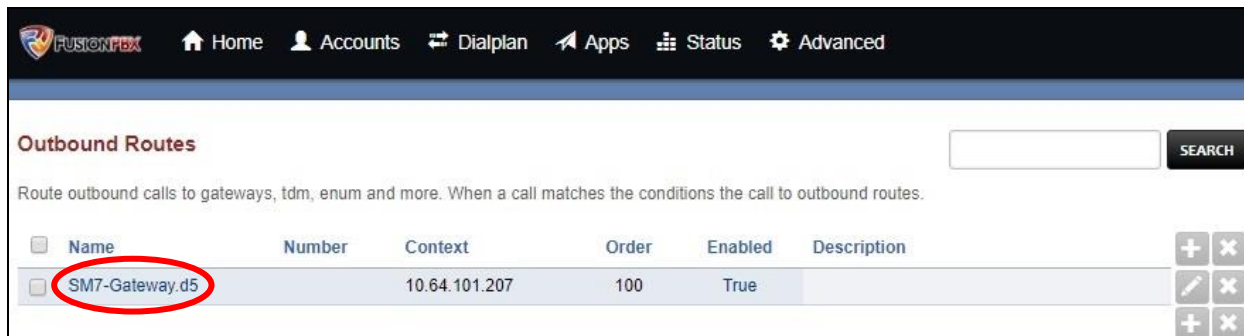
- **Gateway:** Select the pertinent gateway name from **Section 7.2**.
- **Dialplan Express:** Select the length of internal extensions, in this case “5 Digits”.

The screenshot shows the 'Outbound Routes' configuration page in FusionPBX. The page has a dark header with navigation links: Home, Accounts, Dialplan, Apps, Status, and Advanced. The main content area is titled 'Outbound Routes' and includes a 'BACK' button and a 'SAVE' button. Below the title, a descriptive text states: 'Outbound dialplans have one or more conditions that are matched to attributes of a call. When a call matches the conditions the call is then routed to the gateway.'

The configuration form consists of several fields:

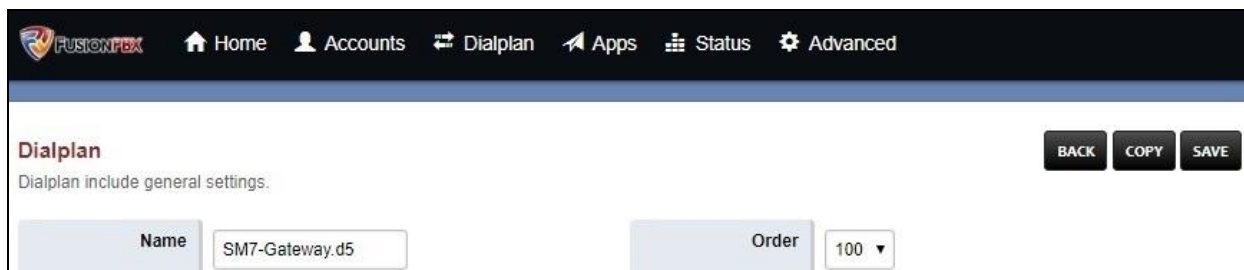
- Gateway:** A text input field containing '51292375-241e-4e07-9999-00bd1f75db8d:SM7-Gateway' and a dropdown arrow button. Below the field is the instruction: 'Select the gateway to use with this outbound route.'
- Alternate 1:** A dropdown menu with a downward arrow. Below it is the instruction: 'Select another gateway as an alternative to use if the first one fails.'
- Alternate 2:** A dropdown menu with a downward arrow. Below it is the instruction: 'Select another gateway as an alternative to use if the second one fails.'
- Dialplan Expression:** A large text input field containing '^(\d{5})\$'. Below the field is a dropdown menu with '5 Digits' selected and a downward arrow. Below this is the instruction: 'Shortcut to create the outbound dialplan entries for this Gateway.'
- Prefix:** A text input field. Below it is the instruction: 'Enter a prefix number to add to the beginning of the destination number.'
- Limit:** A text input field. Below it is the instruction: 'Enter limit to restrict the number of outbound calls.'
- Account Code:** A text input field. Below it is the instruction: 'Enter the accountcode.'
- Order:** A dropdown menu with '100' selected and a downward arrow. Below it is the instruction: 'Select the order number. The order number determines the order of the outbound routes when there is more than one.'
- Enabled:** A dropdown menu with 'True' selected and a downward arrow. Below it is the instruction: 'Choose to enable or disable the outbound route.'
- Description:** A text input field. Below it is the instruction: 'Enter the description.'

The **Outbound Routes** screen is updated, showing the newly added entry. Click on the **Name** of the new entry.



Name	Number	Context	Order	Enabled	Description
SM7-Gateway.d5		10.64.101.207	100	True	

The **Dialplan** screen is displayed, as shown below.



Dialplan

Dialplan include general settings.

BACK COPY SAVE

Name: SM7-Gateway.d5 Order: 100

Scroll to the bottom of the screen, add an entry for the call timeout parameter and set to the desired value. The default timeout for the SIP chat calls is three minutes. In the compliance testing, the call timeout was set to 999 minutes, as shown below.

Tag	Type	Data	Break	Inline	Group	Order
condition	destination_number	^\d{5}\$			0	5
action	set	sip_h_X-accountcode=\${accountcode}			0	10
action	set	call_direction=outbound			0	20
action	set	hangup_after_bridge=true			0	25
action	set	effective_caller_id_name=\${outbound_caller_id_			0	30
action	set	effective_caller_id_number=\${outbound_caller_			0	35
action	set	inherit_codec=true			0	40
action	set	ignore_display_updates=true			0	42
action	set	callee_id_number=\$1			0	43
action	set	continue_on_fail=true			0	45
action	bridge	sofia/gateway/SM7-Gateway/\$1			0	70
Action	set	call_timeout=999			0	80

7.5. Administer SIP Extensions

Select **Accounts** → **Extensions** from the top menu, to display the **Extensions** screen. Select the add icon shown below, to add an extension by following reference [6], the extension will be used as originator of calls for chat work items.

Repeat this section to create desired number of extensions with the same password. The number of extensions configured should correspond to the desired number of simultaneous chat work items. In the compliance testing, the two extensions 200-201 shown below were pre-configured.




The screenshot shows the FusionPBX web interface. The top navigation bar includes links for Home, Accounts, Dialplan, Apps, Status, and Advanced. The main content area is titled "Extensions (2)" and includes an "EXPORT" button and a "SEARCH" input field. Below this, a table lists the configured extensions:

<input type="checkbox"/>	Extension	Call Group	Context	Enabled	Description	
<input type="checkbox"/>	200		10.64.101.207	True		  
<input type="checkbox"/>	201		10.64.101.207	True		  

A red circle highlights the "Add" icon (a plus sign) in the top right corner of the table.

7.6. Launch CT Admin Interface

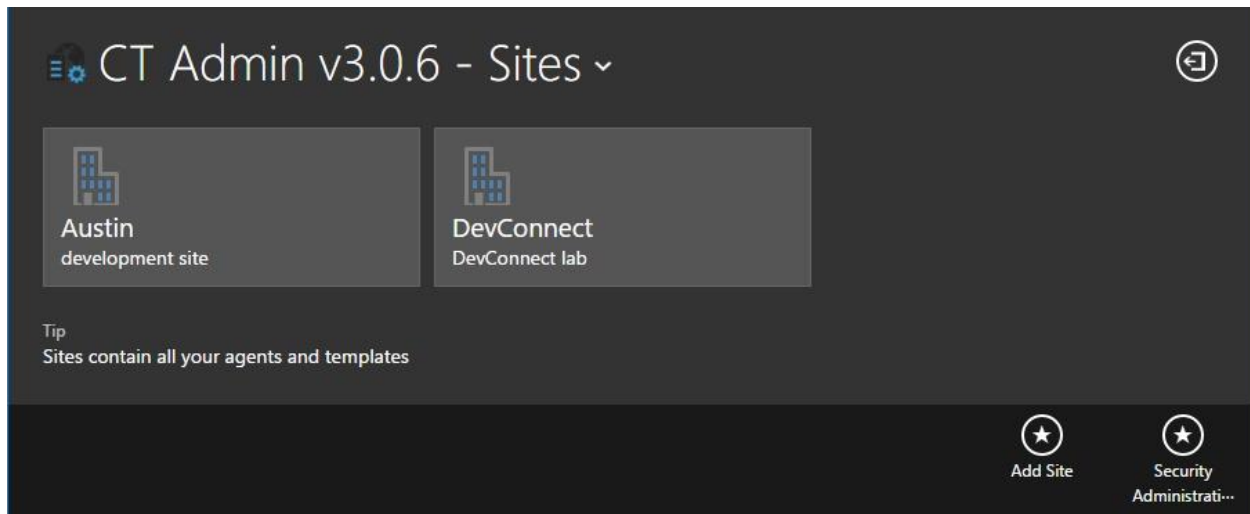
Access the CT Admin web interface by using the URL “http://ip-address/CTAdmin” in an Internet browser window, where “ip-address” is the IP address of the CT Suite server. The **CT Admin** screen below is displayed. Log in using the administrator credentials.



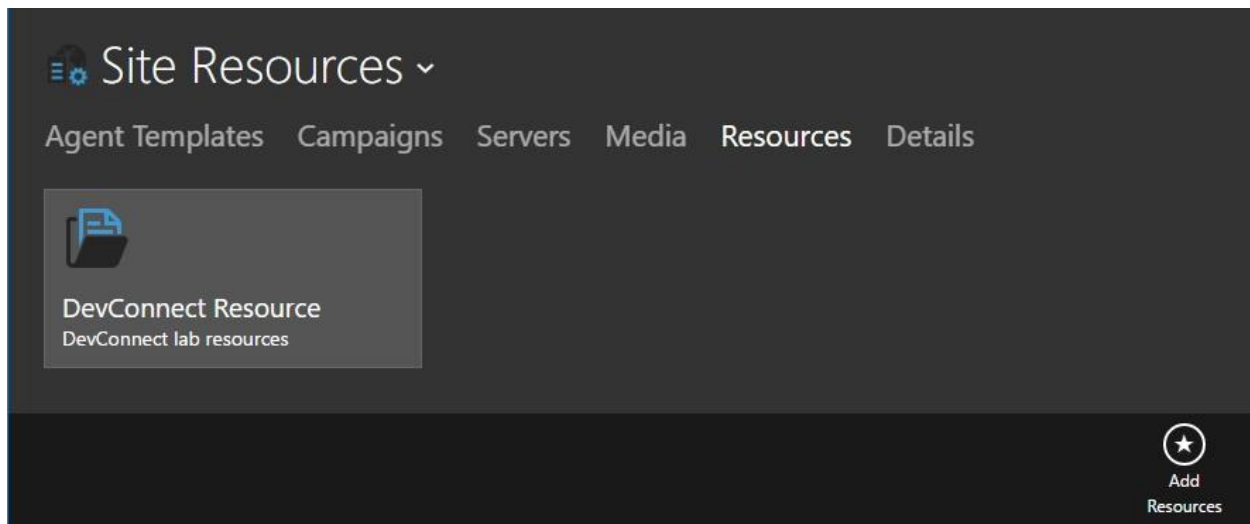
The screenshot shows the CT Admin v3.0.6 login page. It features a logo with a server and a gear. Below the logo, the text "CT Admin v3.0.6" is displayed. The "Log In" section includes a "Username:" label and a text input field, a "Password:" label and a text input field, and a "Remember me next time." checkbox. A "LOG IN" button is located at the bottom of the login section. A link for "Security Admin" is also visible.

7.7. Administer CTI Extensions

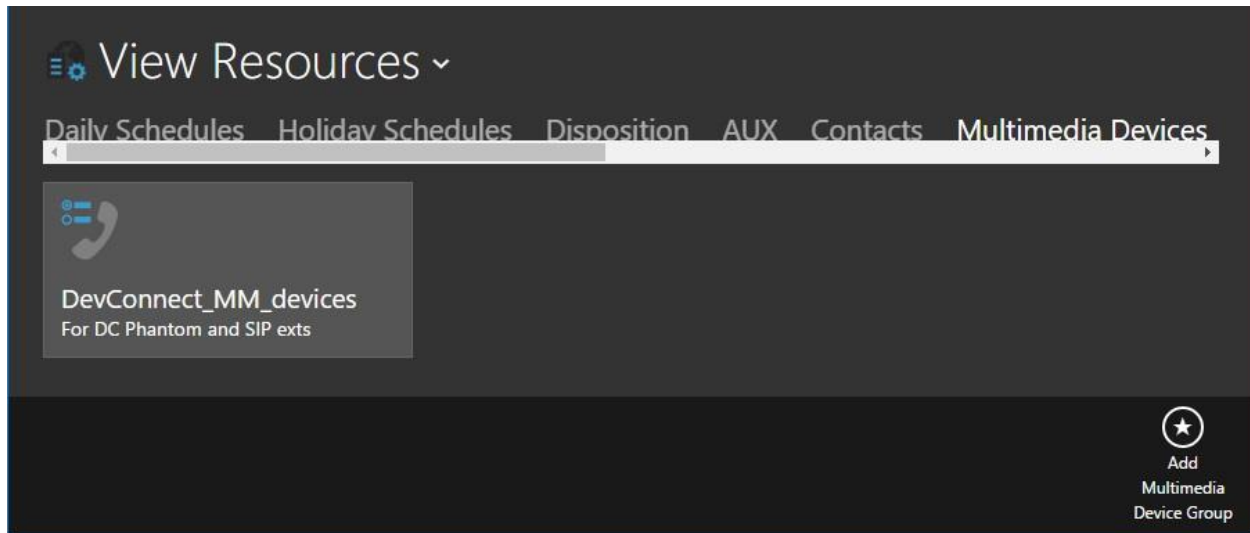
The **Sites** screen below is displayed. Select the pertinent site, in this case “DevConnect”.



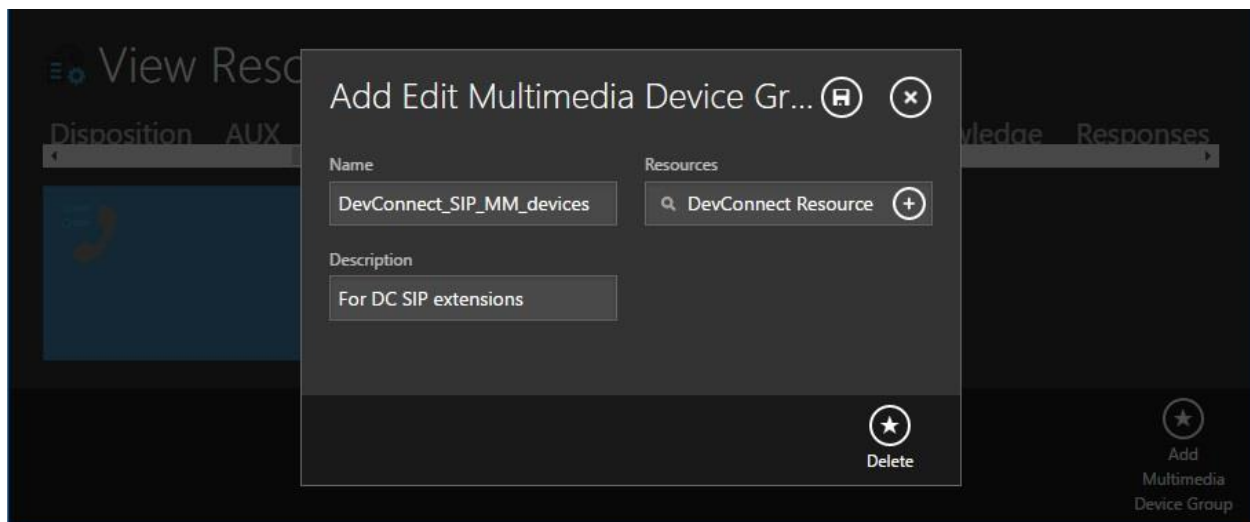
The **Site Resources** screen is displayed next. Select the pertinent logical resource group, in this case “DevConnect Resource”.



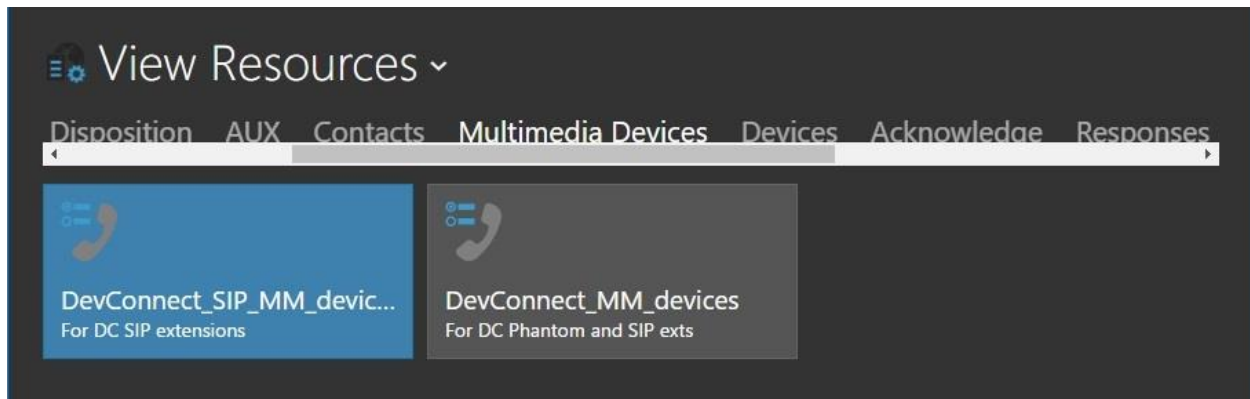
The **View Resources** screen is displayed. Scroll the top menu bar as necessary to locate and select **Multimedia Devices**, followed by **Add Multimedia Device Group** from bottom of screen to add a logical group for multimedia devices.



The **Add Edit Multimedia Device Group** screen is displayed next. Enter a descriptive **Name** and **Description**. For **Resources**, select the pertinent logical resource group shown earlier in this section.



The **View Resources** screen is displayed again. Select the newly added group, in this case “DevConnect_SIP_MM_devices”.



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



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:** “SIP”
- **Password:** Enter the common password for the SIP extensions from **Section 7.5**.
- **Description:** A desired description.
- **Extension List:** The SIP extensions from **Section 7.5**.

Add Edit CTI Extension

Extension Type: SIP

Password: ...

Description: SIP extensions

Extension List (Separate each group by a comma): 200-201

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

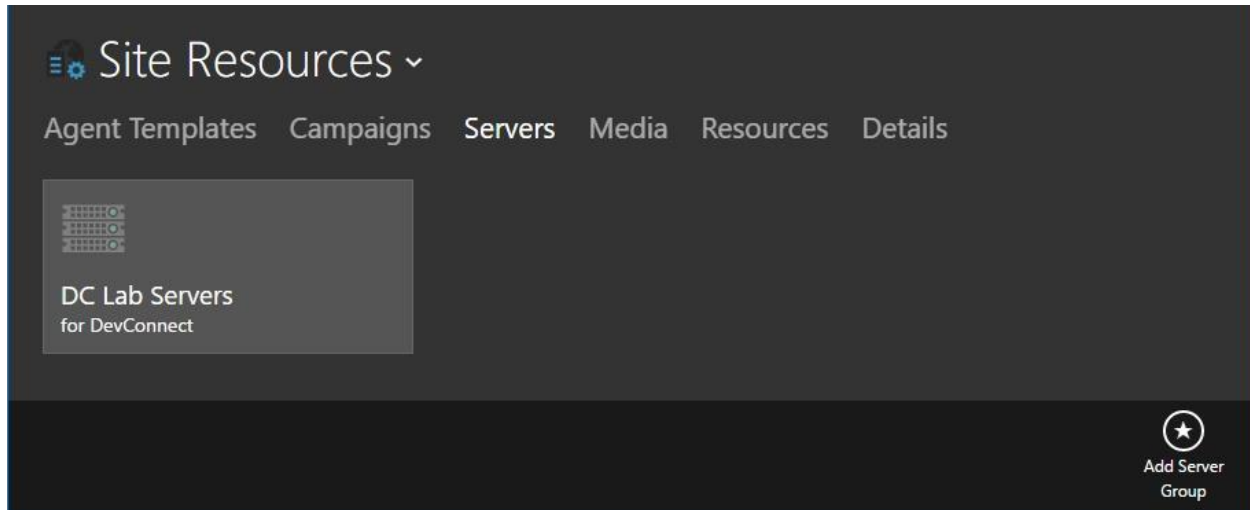
Note
If the Extension Type is "SIP" then the Password will be required.

delete

Add CTI Extension

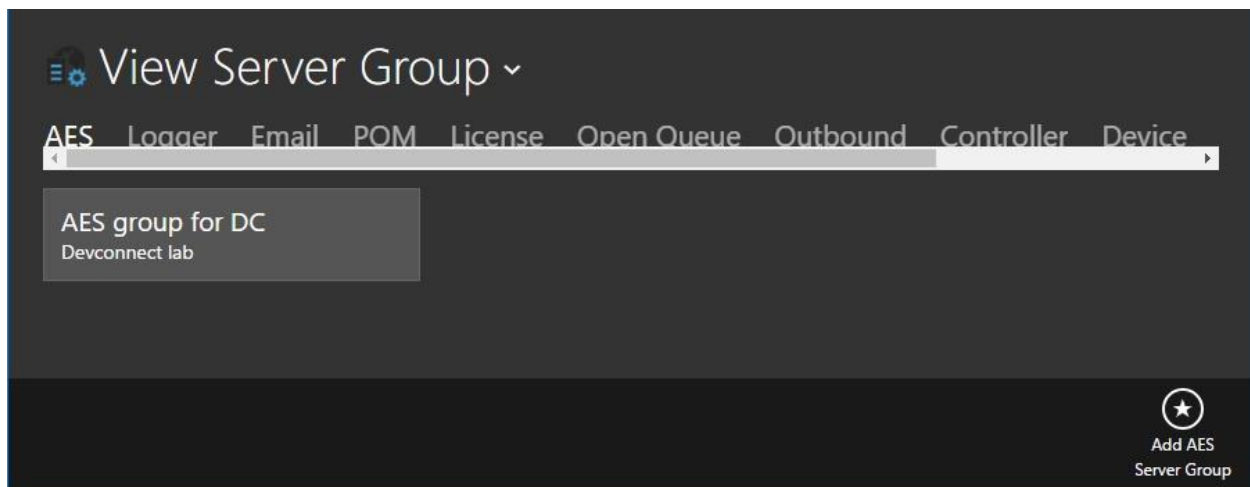
7.8. Administer Servers

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”.



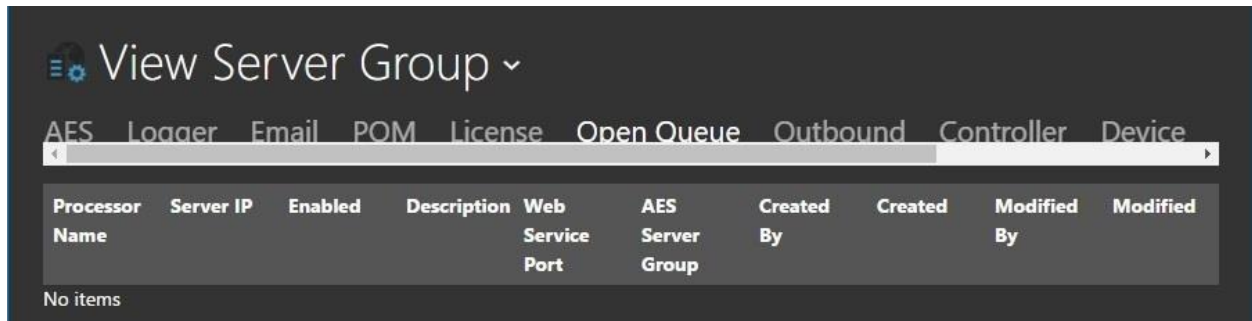
7.8.1. AES Server

The **View Server Group** screen is displayed. 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. Note that an AES server group is required to be configured.



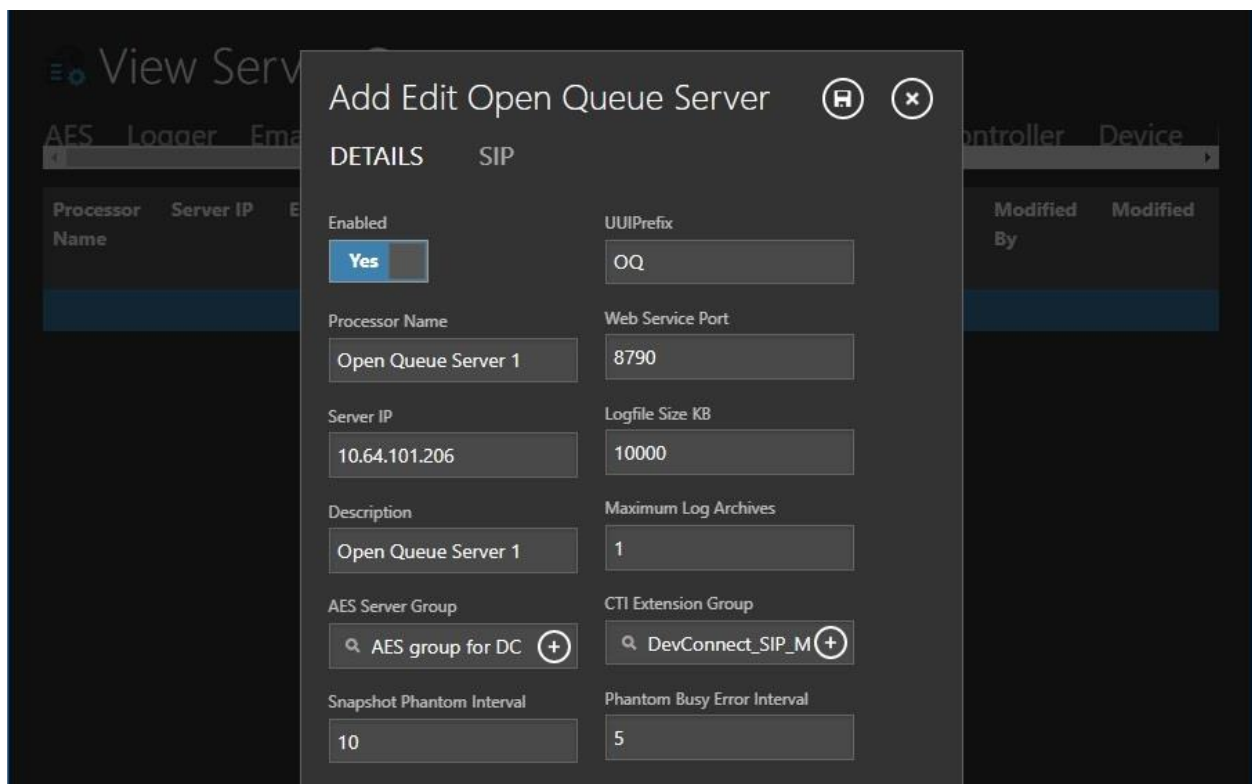
7.8.2. Open Queue Server

Select **Open Queue** from the top menu, followed by **Add Open Queue** from bottom of screen (not shown).



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 7.8.1**.
- **CTI Extension Group:** Select the multimedia device group name from **Section 7.7**.



Select the **SIP** tab. For **Server** and **Domain**, enter the IP address of CT Suite Communication Server. For **Port**, enter the CT Suite SIP entity link port number from **Section 6.3.1**.

Add Edit Open Queue Server

DETAILS SIP

Server	Port
10.64.101.207	5060
Domain	
10.64.101.207	
Call Invite Time Out	
3600	

Background table (View Server Group):

Processor Name	Server IP	Enabled	Description	Created By	Created	Modified By	Modified
Open Qu...	10.64.101...						

7.8.3. 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.

View Server Group

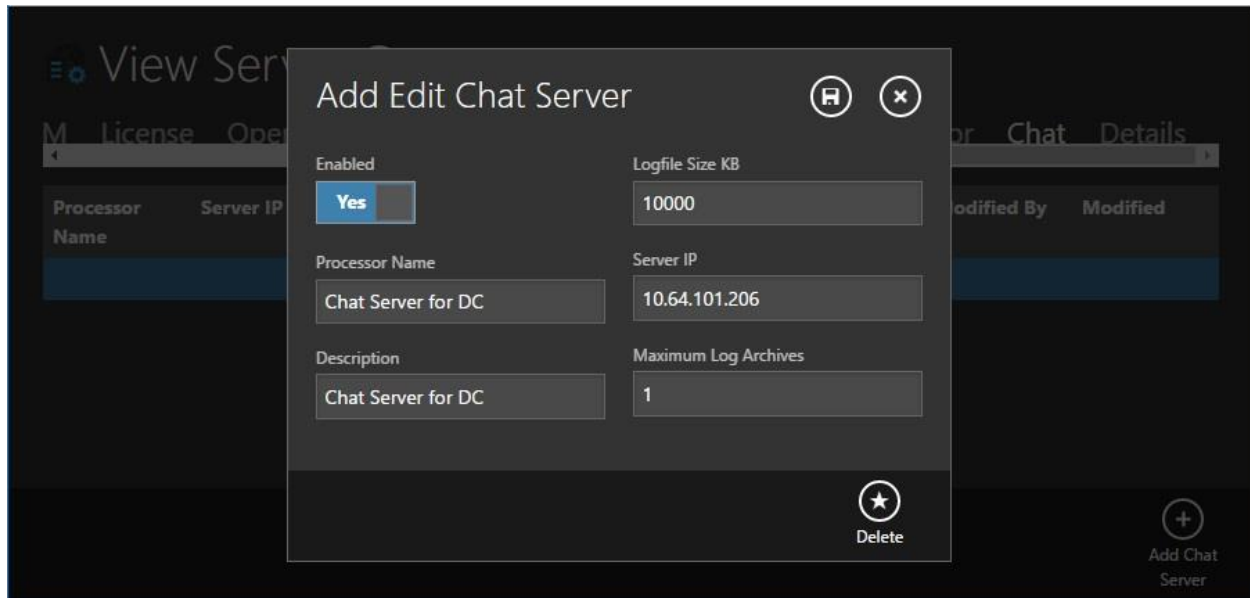
License Open Queue Outbound Controller Device Monitor Chat Details

Processor Name	Server IP	Enabled	Description	Created By	Created	Modified By	Modified
----------------	-----------	---------	-------------	------------	---------	-------------	----------

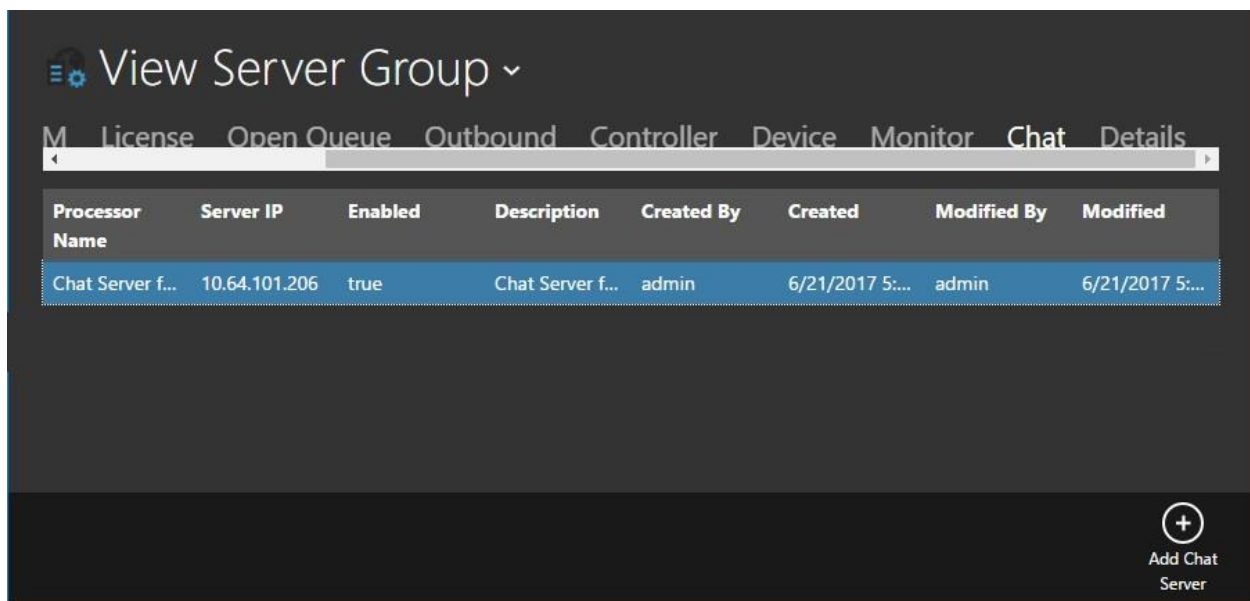
Bottom right button: Add Chat Server

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.

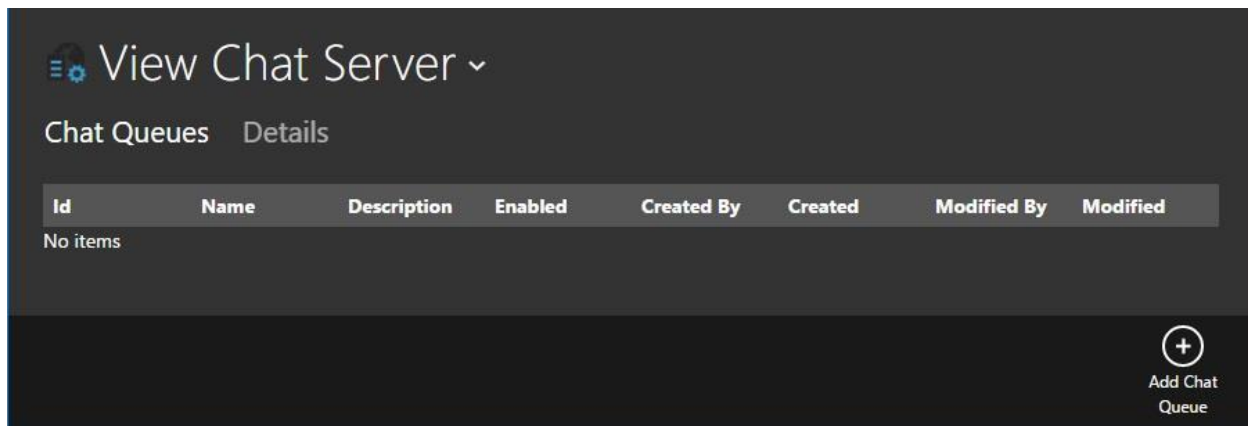


The **View Server Group** screen is displayed again. Select the newly created chat server, as shown below.



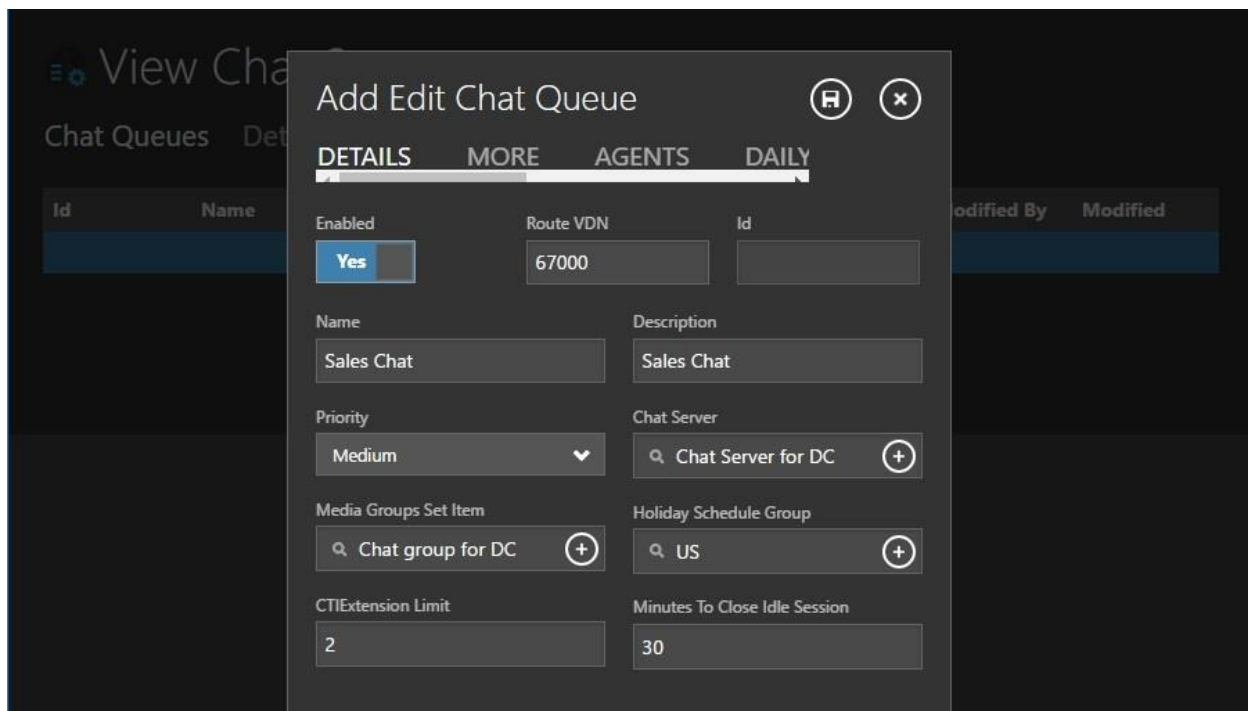
Processor Name	Server IP	Enabled	Description	Created By	Created	Modified By	Modified
Chat Server f...	10.64.101.206	true	Chat Server f...	admin	6/21/2017 5:...	admin	6/21/2017 5:...

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

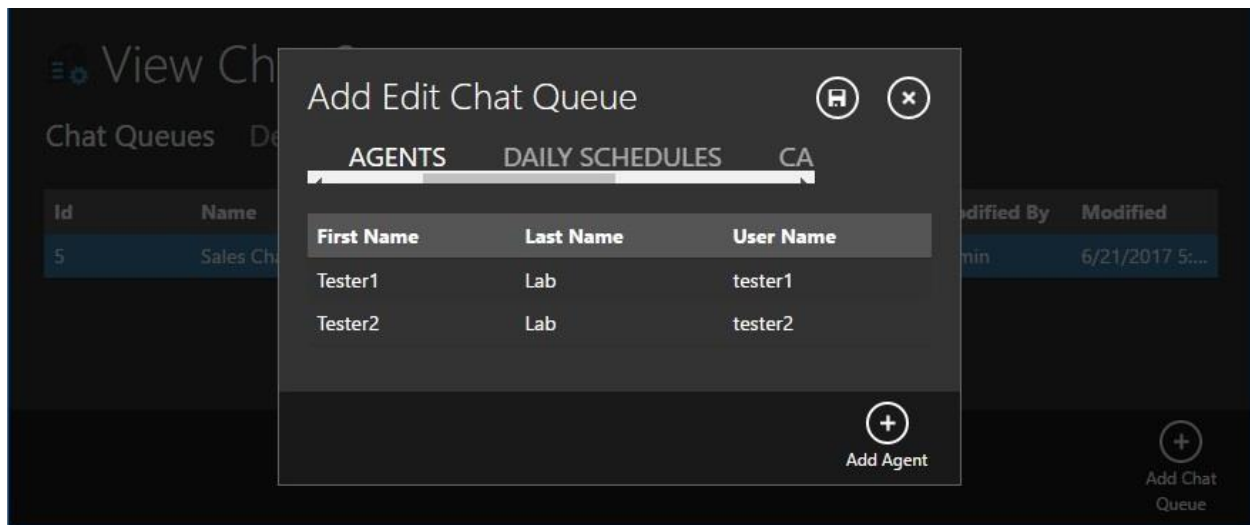


The **Add Edit Chat Queue** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

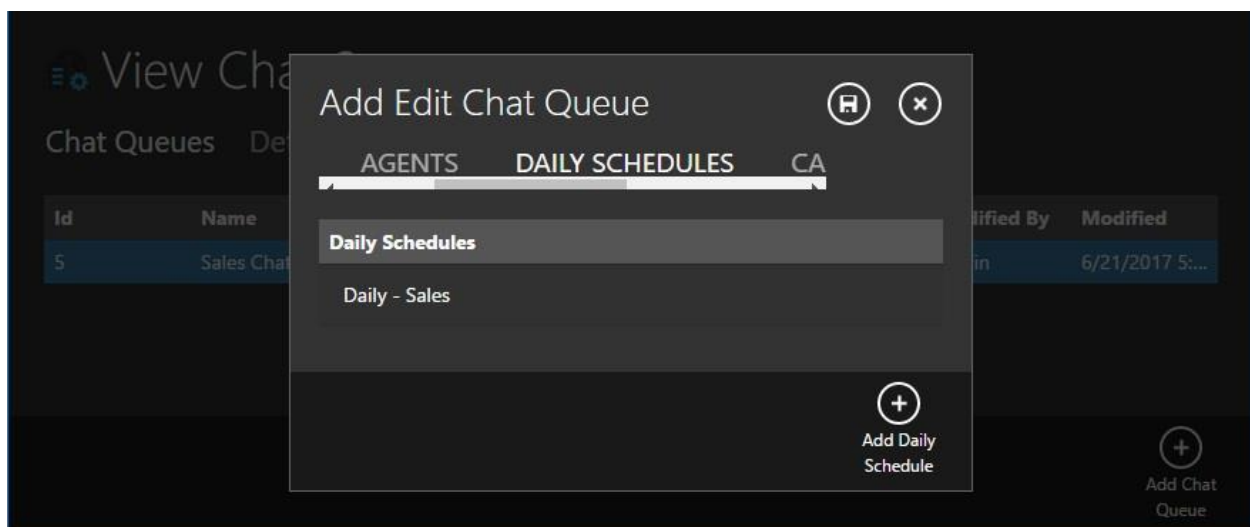
- **Route VDN:** The Chat VDN extension number from **Section 5.8**.
- **Name:** A descriptive name.
- **Description:** A desired description.
- **Media Groups Set Item:** Select the pertinent pre-existing media group.
- **Holiday Schedule Group:** Select the pertinent pre-existing holiday schedule group.
- **CTIExtension Limit:** The number of CTI extensions from **Section 7.7**.
- **Minutes To Close Idle Session:** Enter the desired interval.



Select the **AGENTS** tab. Follow reference [6] to select the pertinent pre-existing agents. In the compliance testing, two agents below were selected.

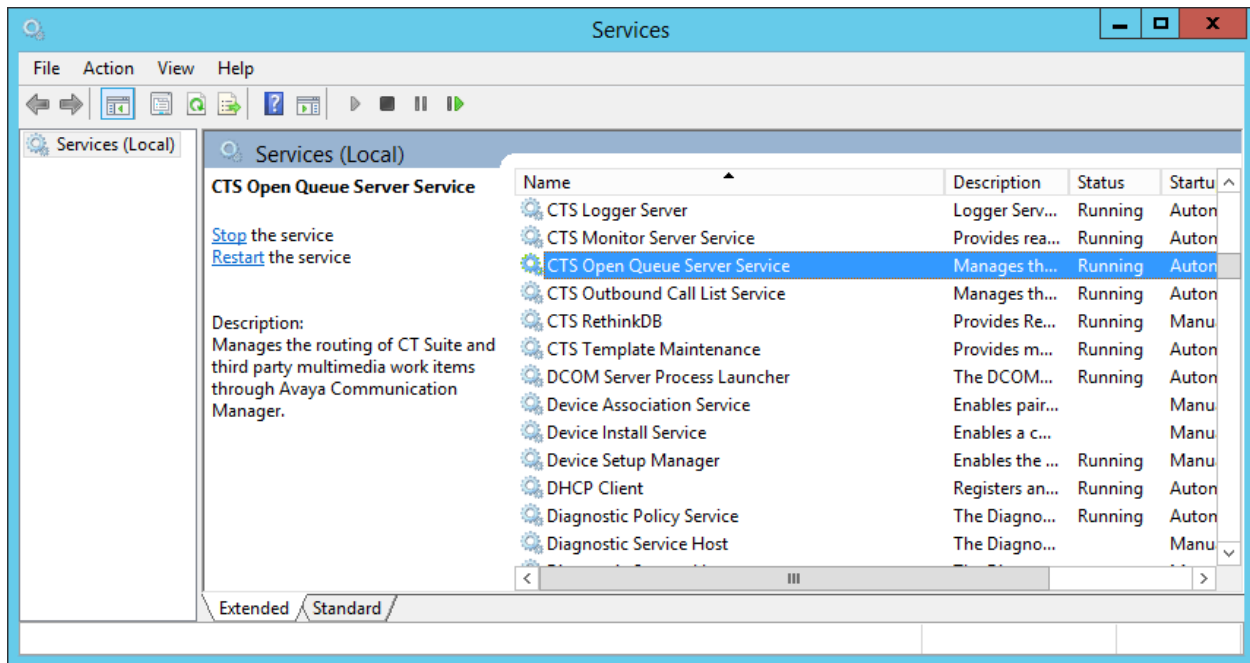


Select the **DAILY SCHEDULES** tab. Follow reference [6] to select the pertinent pre-existing daily schedule, in this case “Daily – Sales”.



7.9. 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.



8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

From the SAT interface, verify the status of the SIP trunk groups by using the “status trunk n” command, where “n” is the trunk group number administered in **Section 5.2**. Verify that all trunks are in the “in-service/idle” state as shown below.

```
status trunk 53
```

TRUNK GROUP STATUS			
Member	Port	Service State	Mtce Connected Ports Busy
0053/001	T00156	in-service/idle	no
0053/002	T00157	in-service/idle	no
0053/003	T00158	in-service/idle	no
0053/004	T00159	in-service/idle	no
0053/005	T00160	in-service/idle	no
0053/006	T00161	in-service/idle	no
0053/007	T00162	in-service/idle	no
0053/008	T00163	in-service/idle	no
0053/009	T00164	in-service/idle	no
0053/010	T00165	in-service/idle	no

Verify the status of the SIP signaling groups by using the “status signaling-group n” command, where “n” is the signaling group number administered in **Section 5.3**. Verify that the **Group State** is “in-service”, as shown below.

```
status signaling-group 53
```

STATUS SIGNALING GROUP	
Group ID:	53
Group Type:	sip
Group State:	in-service

8.2. Verify Avaya Aura® Session Manager

From the System Manager home page (not shown), select **Elements** → **Session Manager** to display the **Session Manager Dashboard** screen (not shown).

Select **Session Manager** → **System Status** → **SIP Entity Monitoring** from the left pane to display the **SIP Entity Link Monitoring Status Summary** screen. Click the CT Suite entity name from **Section 6.3.1**.

AVAYA
Aura® System Manager 7.0

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

SIP Entities Status for All Monitoring Session Manager Instances

Run Monitor

1 Items | Refresh

<input type="checkbox"/>	Session Manager	Type	Monitored Entities				
			Down	Partially Up	Up	Not Monitored	Deny
<input type="checkbox"/>	DR-SM7	Core	6	0	6	0	0
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							
<input type="checkbox"/>							

Select: All, None

All Monitored SIP Entities

Run Monitor

12 Items | Refresh

<input type="checkbox"/>	SIP Entity Name
<input checked="" type="checkbox"/>	CTSuite
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

The **SIP Entity, Entity Link Connection Status** screen is displayed. Verify that the **Conn Status** and **Link Status** are “UP”, as shown below.

AVAYA
Aura® System Manager 7.0

Home / Elements / Session Manager / System Status / SIP Entity Monitoring

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CTSuite

Status Details for the selected Session Manager:

Summary View

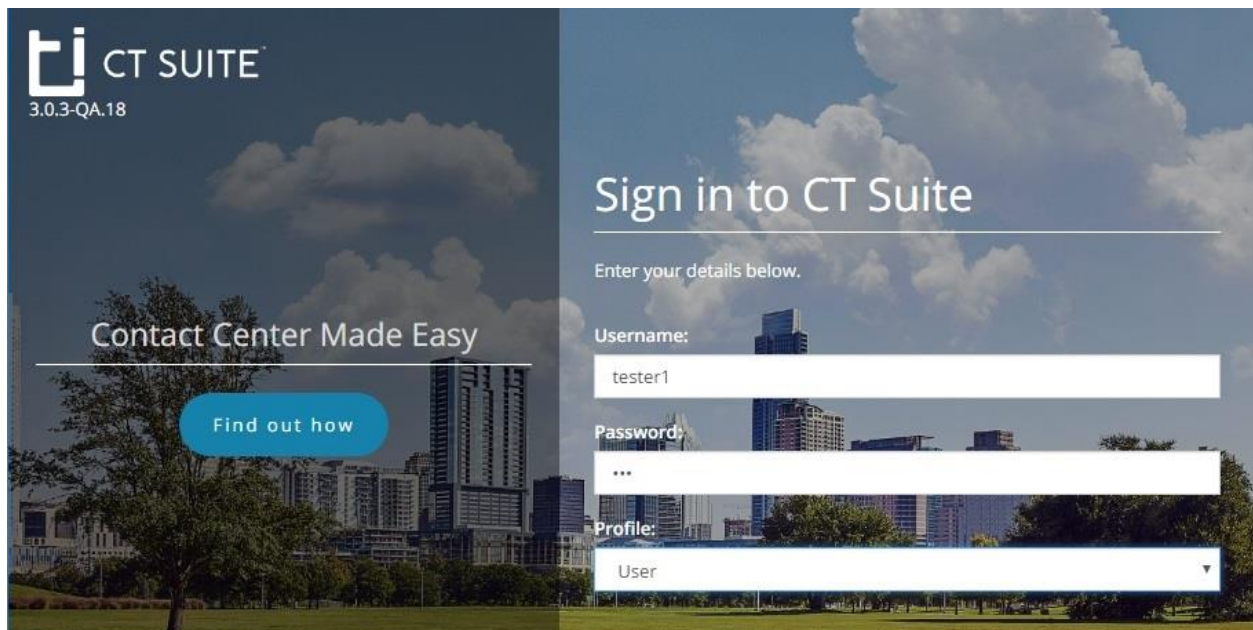
1 Items | Refresh

Session Manager	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code
DR-SM7	10.64.101.207	5060	UDP	FALSE	UP	200 OK

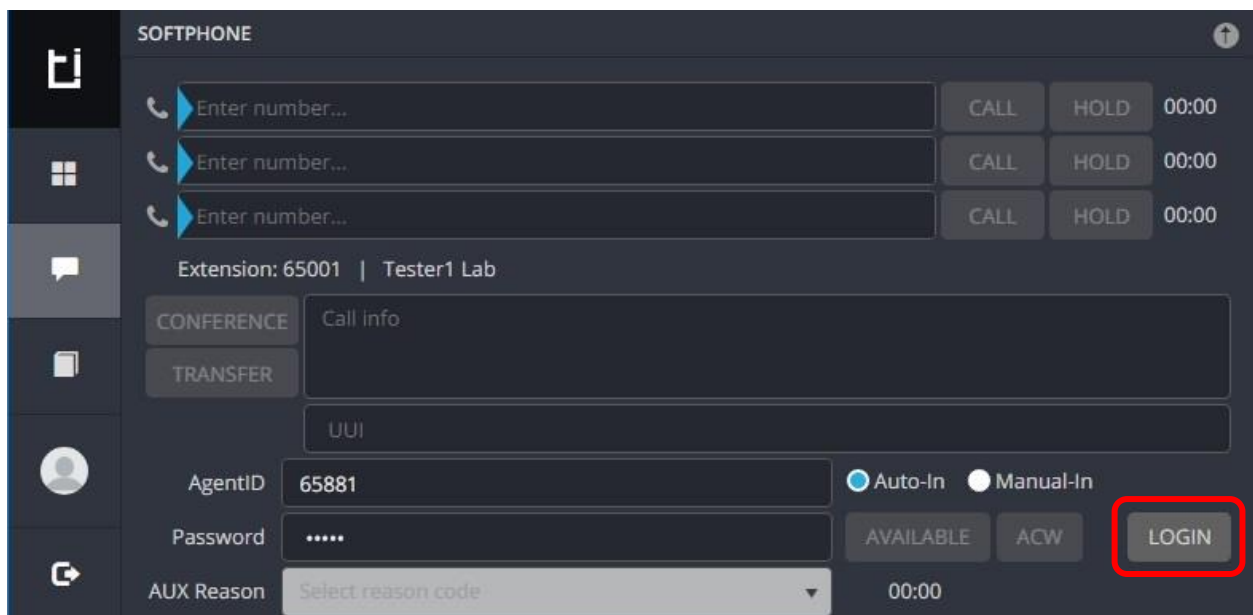
8.3. Verify CTIntegrations CT Suite

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.

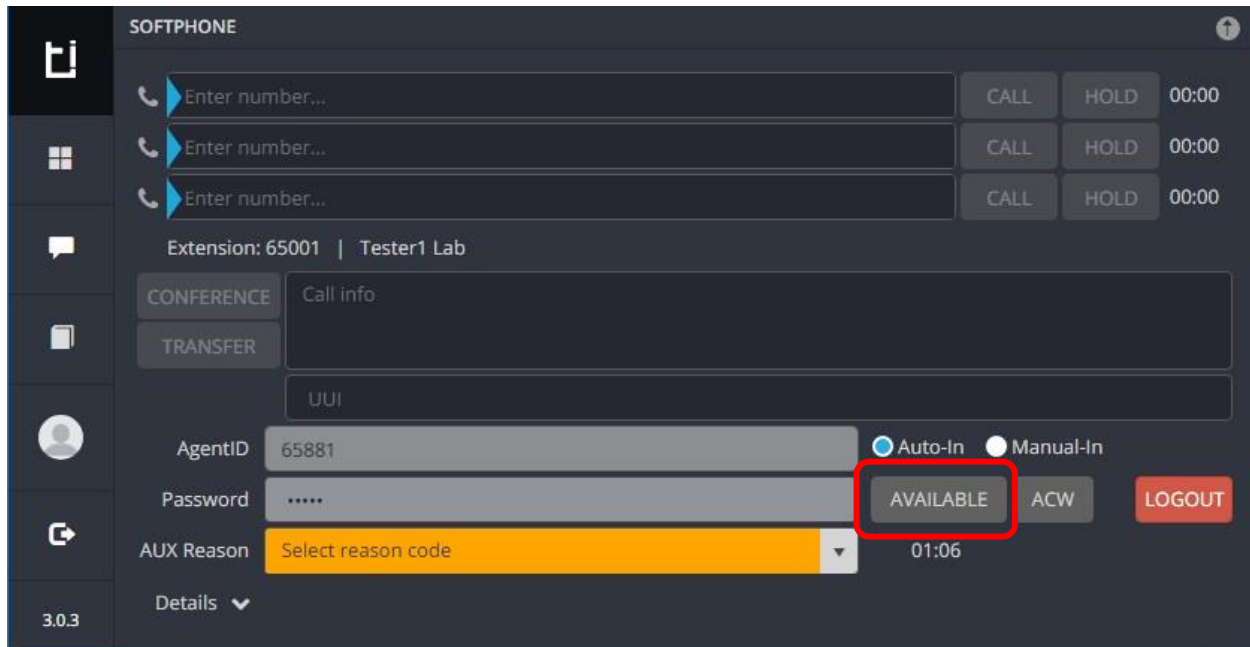
The **Sign in to CT Suite** screen is displayed. For **Username** and **Password**, enter an applicable agent credentials, and retain the default value in the remaining field.

The image shows the 'Sign in to CT Suite' web interface. On the left, there is a logo for 'CT SUITE 3.0.3-QA.18' and a banner that says 'Contact Center Made Easy' with a 'Find out how' button. On the right, there is a login form with the title 'Sign in to CT Suite' and the instruction 'Enter your details below.' The form has three fields: 'Username:' with the value 'tester1', 'Password:' with masked characters '***', and 'Profile:' with a dropdown menu showing 'User'.

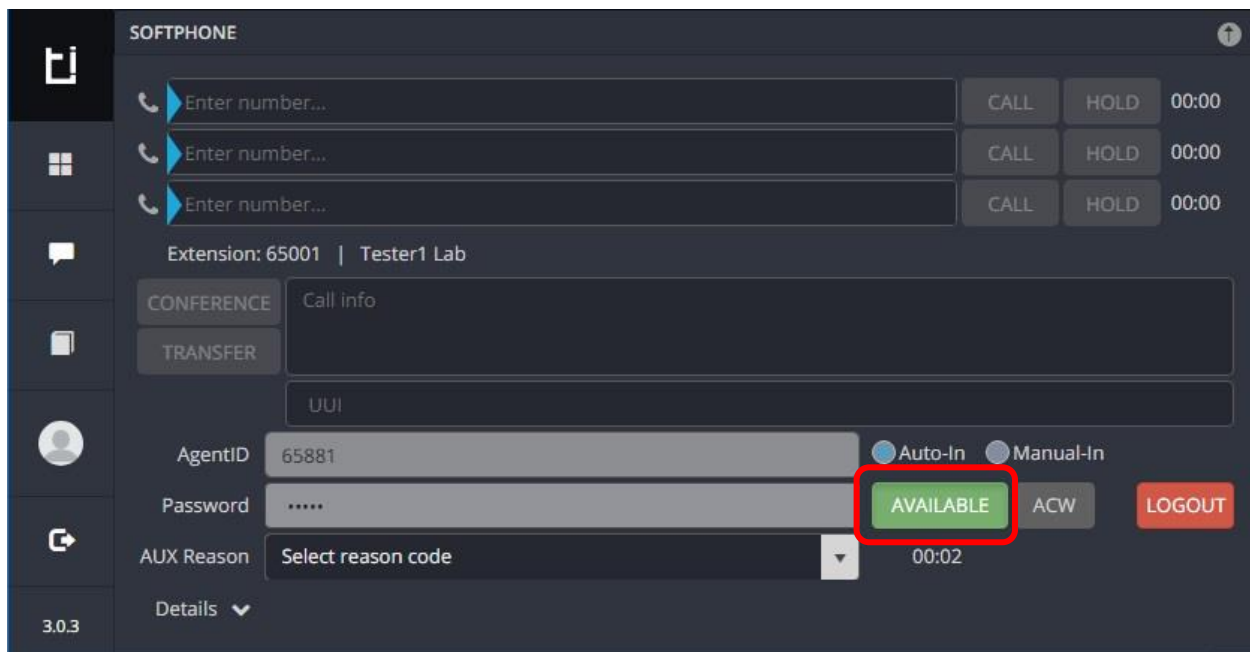
The agent screen below is displayed next. Retain the default values, and select **LOGIN** to log the agent into the ACD on Communication Manager.

The image shows the 'SOFTPHONE' agent interface. It has a dark theme with a sidebar on the left containing icons for calls, windows, messages, documents, and a user profile. The main area shows three call lines, each with 'Enter number...', 'CALL', 'HOLD', and '00:00' buttons. Below the calls, it displays 'Extension: 65001 | Tester1 Lab'. There are buttons for 'CONFERENCE' and 'TRANSFER', each followed by a text input field. Below these are fields for 'AgentID' (65881), 'Password' (masked with '*****'), and 'AUX Reason' (a dropdown menu). To the right of the 'AgentID' field are radio buttons for 'Auto-In' (selected) and 'Manual-In'. At the bottom right, there are buttons for 'AVAILABLE', 'ACW', and 'LOGIN'. The 'LOGIN' button is highlighted with a red rectangle.

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



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



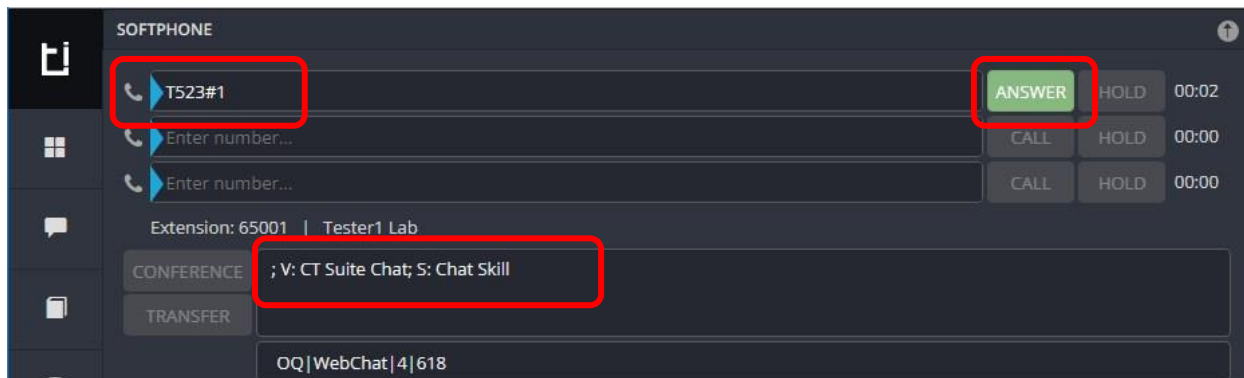
From a PC on the intranet, launch an Internet browser window and enter the URL <http://ip-address:3000> to start a chat session, where “ip-address” is the IP address of the CT Suite server. The screen below is displayed, select **Open Chat**.



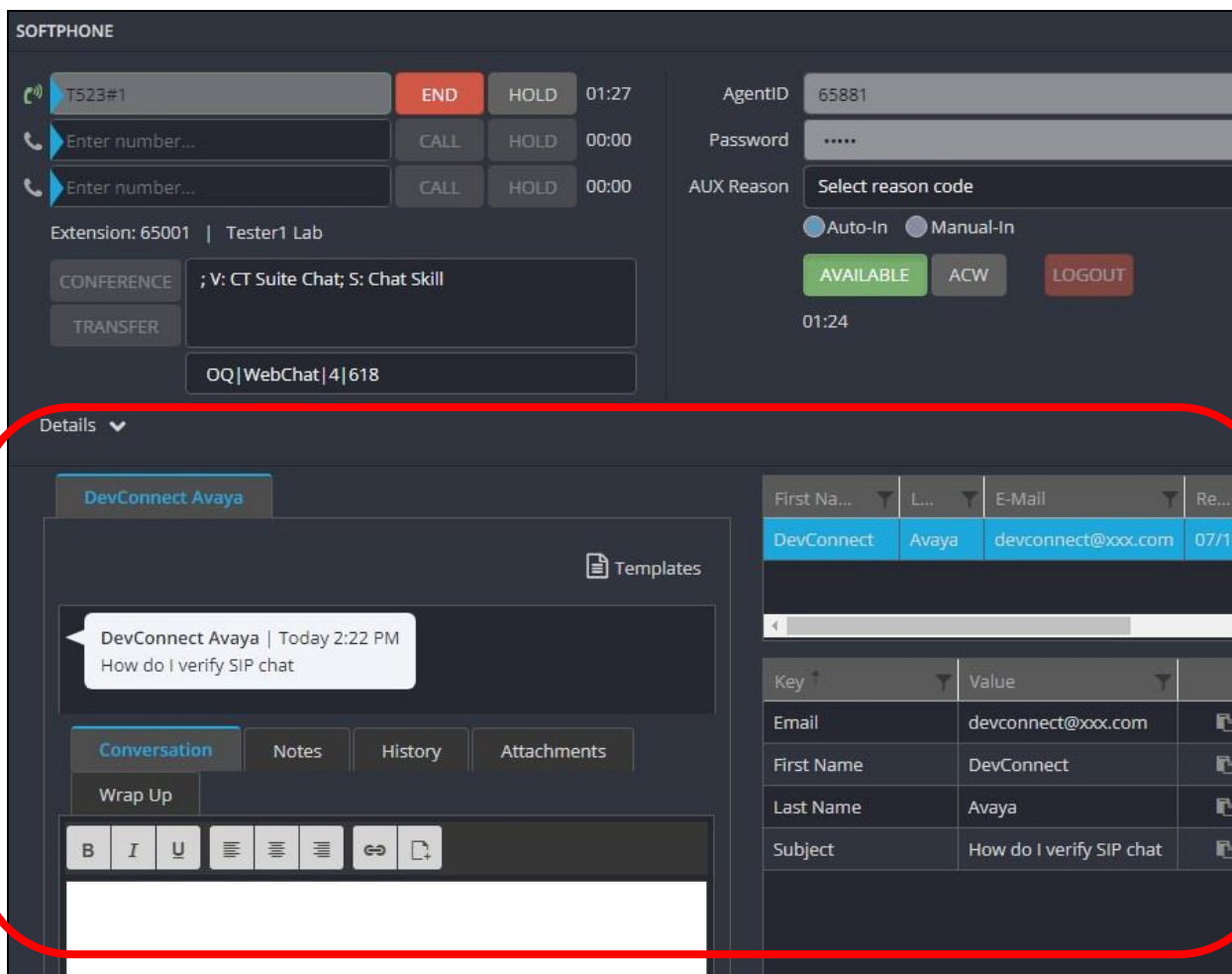
The screen is updated as shown below. Fill out the parameters as desired. For **Department**, select the chat queue name from **Section 7.8.3**. Click **Start Chat**.

A screenshot of the CT Suite chat interface. The background is a blue-tinted image of a server rack. In the top left corner, there is a logo consisting of a stylized 'ti' followed by the text 'CTINTEGRATIONS CONTACT TECHNOLOGY'. On the right side, there is a white chat window with a green header bar that says 'Live 24 / 7'. Inside the chat window, there is a 'CT SUITE' logo and a welcome message: 'Welcome to CTIntegrations Chat. Please fill in the form below before starting chat.' Below the message is a form with the following fields: 'First Name:*' with the value 'DevConnect', 'Last Name:*' with the value 'Avaya', 'Email:*' with the value 'devconnect@xxx.com', 'Subject:' with the value 'How do I verify SIP chat', and 'Department:*' with a dropdown menu showing 'Sales Chat'. At the bottom of the form is a green button labeled 'Start Chat'.

Verify that the top section of the available agent's screen is updated to reflect a trunk as calling party number, along with name of chat VDN from **Section 5.8**, as shown below. Click **ANSWER**.



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



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® Session Manager 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. *Administering Avaya Aura® Session Manager*, Release 7.0.1, Issue 2, May 2016, available at <http://support.avaya.com>.
4. *Administering Avaya Aura® System Manager for Release 7.0.1*, Release 7.0.1, Issue 4, April 2017, available at <http://support.avaya.com>.
5. *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>.
6. *CT Admin Administrator's Guide*, CT Suite v3.0, 5/30/17, available at <https://www.ctintegrations.com/docs>.
7. *CT Suite Web Client*, Web Client User Guide, CT Suite R3.0, 5/30/17, available at <https://www.ctintegrations.com/docs>.

©2017 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.