Application Notes for CTIntegrations CT Suite 3.3 with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Session Manager 8.0.1 for Email Integration – Issue 1.1

Abstract

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.3 to interoperate with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Session Manager 8.0.1 for Email 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 Email 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 3.3 to interoperate with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Session Manager 8.0.1 for Email integration. CTIntegrations 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 Email 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 Email work item, using an available local SIP extension on CT Suite Communication Server as calling party and the applicable Email 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 Email 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 Emails were placed with available agents that have web browser connections to the CT Suite server. All necessary Email 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 Email 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 Email requesters from the intranet or internet. For simplicity, all Emails in the compliance testing were initiated from the intranet.

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

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDN</td>
<td>59102</td>
</tr>
<tr>
<td>Skill</td>
<td>59002</td>
</tr>
<tr>
<td>Agent Station</td>
<td>50001, 50002, 51001</td>
</tr>
<tr>
<td>Agent ID</td>
<td>55001, 55002, 55003</td>
</tr>
<tr>
<td>Agent Password</td>
<td>123456</td>
</tr>
</tbody>
</table>

![Figure 1: Compliance Testing Configuration](image-url)
4. Equipment and Software Validated

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

<table>
<thead>
<tr>
<th>Equipment/Software</th>
<th>Release/Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® Communication Manager in Virtual Environment</td>
<td>8.0.1.1.0-FP1SP1</td>
</tr>
<tr>
<td>Avaya Aura® Media Server in Virtual Environment</td>
<td>v.8.0.0.183</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services in Virtual Environment</td>
<td>8.0.1.0.2.5-0</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager in Virtual Environment</td>
<td>8.0.1.1.801103</td>
</tr>
<tr>
<td>Avaya Aura® System Manager in Virtual Environment</td>
<td>8.0.1.1.039340</td>
</tr>
<tr>
<td>Avaya 96x1 IP Deskphones (H.323)</td>
<td>6.8102</td>
</tr>
<tr>
<td>Avaya 96x1 IP Deskphones (SIP)</td>
<td>7.1.5.0.11</td>
</tr>
<tr>
<td>Avaya J169 IP Deskphone (H.323)</td>
<td>6.8102</td>
</tr>
<tr>
<td>Avaya Agent for Desktop</td>
<td>1.7.22.1</td>
</tr>
<tr>
<td>CTIntegrations CT Suite on Microsoft Windows Server 2016</td>
<td></td>
</tr>
<tr>
<td>• CT Admin</td>
<td>3.3</td>
</tr>
<tr>
<td>• CT Web Client</td>
<td></td>
</tr>
<tr>
<td>• CT Device Manager</td>
<td></td>
</tr>
<tr>
<td>• CT Open Queue</td>
<td></td>
</tr>
<tr>
<td>• Avaya DMCC .Net SDK</td>
<td>7.1</td>
</tr>
<tr>
<td>CTIntegrations CT Suite Communication Server on Debian 8</td>
<td></td>
</tr>
<tr>
<td>• FreeSWITCH</td>
<td>4.2</td>
</tr>
<tr>
<td>• FusionPBX</td>
<td>1.6.20</td>
</tr>
<tr>
<td></td>
<td>4.2.0</td>
</tr>
</tbody>
</table>
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 signaling group
- Administer SIP trunk group
- Administer IP network region
- Administer IP codec set
- Administer Email skill
- Administer Email 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.

```plaintext
display system-parameters customer-options

OPTIONAL FEATURES

IP PORT CAPACITIES

<table>
<thead>
<tr>
<th>Feature</th>
<th>Maximum Administered</th>
<th>USED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Administered H.323 Trunks:</td>
<td>12000</td>
<td>10</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP Stations:</td>
<td>18000</td>
<td>4</td>
</tr>
<tr>
<td>Maximum Administered Remote Office Trunks:</td>
<td>12000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered Remote Office Stations:</td>
<td>18000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Concurrently Registered IP eCons:</td>
<td>414</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable Stations:</td>
<td>41000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Video Capable IP Softphones:</td>
<td>18000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Administered SIP Trunks:</td>
<td>24000</td>
<td>30</td>
</tr>
<tr>
<td>Maximum Administered Ad-hoc Video Conferencing Ports:</td>
<td>24000</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Number of DS1 Boards with Echo Cancellation:</td>
<td>522</td>
<td>0</td>
</tr>
</tbody>
</table>
```
5.2. Administer SIP Signaling Group

An existing trunk group between Communication Manager and Session Manager was used. To add a Signaling Group, use the “add signaling-group n” command, where “n” is an available signaling group number, in this case “1”. 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.

```
change signaling-group 1

SIGNALING GROUP
Group Number: 1
Group Type: sip
IMS Enabled? n
Transport Method: tls
Q-SIP? n
Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y
Peer Server: SM
Clustered? n
Remove '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr
Near-end Listen Port: 5061
Far-end Node Name: sm8
Far-end Listen Port: 5061
Far-end Network Region: 1
Far-end Domain: avaya.com
Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate
RFC 3389 Comfort Noise? n
DTMF over IP: rtp-payload
Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 120
IP Audio Hairpinning? y
Enable Layer 3 Test? y
Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n
Alternate Route Timer(sec): 6
```
5.3. Administer SIP Trunk Group

An existing trunk group between Communication Manager and Session Manager was used. To add a Trunk Group, use the “add trunk-group n” command, where “n” is an available trunk group number, in this case trunk group “1”. 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:** “tie”
- **Signaling Group:** The group number configured in previous section.
- **Number of Members:** Enter a value based on requirements.

```
change trunk-group 1
TRUNK GROUP
Group Number: 1
Group Type: sip
Group Name: sm8
Direction: two-way
Dial Access? n
Queue Length: 0
Service Type: tie

CDR Reports: y
COR: 1
TN: 1
TAC: 101
Outgoing Display? y
Night Service:
Auth Code? n
Member Assignment Method: auto
Signaling Group: 1
Number of Members: 10
```

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

```
change trunk-group 1
TRUNK FEATURES
ACA Assignment? n
Measured: none

Numbering Format: private
UUI Treatment: shared
Maximum Size of UUI Contents: 128
Replace Restricted Numbers? n
Replace Unavailable Numbers? n

Hold/Unhold Notifications? y
Modify Tandem Calling Number: no

Send UCID? y
```

Show ANSWERED BY on Display? y
5.4. 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 5.2.

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.

| Region: | 1 | NR Group: | 1 |
| Location: | 1 | Authoritative Domain: | avaya.com |
| Name: | | Stub Network Region: | n |
| MEDIA PARAMETERS | | Intra-region IP-IP Direct Audio: | yes |
| Codec Set: | 1 | 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

5.5. Administer IP Codec Set

Use the “change ip-codec-set n” command, where “n” is the codec set number from Section 5.4. Update the audio codec types in the Audio Codec fields as necessary.

| Codec Set: | 5 |
| Audio Codec | Silence Suppression | Frames Per Pkt | Packet Size (ms) |
| 1: | G.711MU | n | 2 | 20 |
| 2: | | | | |
5.6. Administer Email Skill

Administer a skill group to be used for routing of Email 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 2

Group Number: 2
ACD? y
Group Name: CTI MultiMedia
Queue? y
Group Extension: 59002
Vector? y
Group Type: ucd-mia
TN: 1
COR: 1
Security Code: Local Agent Preference? n
ISDN/SIP Caller Display:

Queue Limit: unlimited
Calls Warning Threshold: Port:
Time Warning Threshold: Port:
```

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

```
add hunt-group 2

Skill? y
Expected Call Handling Time (sec): 180
AAS? n
Service Level Target (% in sec): 80 in 20
Measured: both
Supervisor Extension:
```
5.7. Administer Email 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 Email phantom calls to agents at medium priority. Note that the vector **Number**, **Name**, **queue-to-skill**, and **wait-time** steps may vary.

<table>
<thead>
<tr>
<th>change vector 102</th>
<th>CALL VECTOR</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number:</strong> 102</td>
<td><strong>Name:</strong> CTI MultiMedia</td>
</tr>
<tr>
<td>Multimedia? n</td>
<td>Attendant Vectoring? n</td>
</tr>
<tr>
<td>Variables? y</td>
<td>3.0 Enhanced? y</td>
</tr>
<tr>
<td>01 wait-time</td>
<td>2 secs hearing ringback</td>
</tr>
<tr>
<td>02 queue-to</td>
<td>skill 2 pri m</td>
</tr>
<tr>
<td>03 wait-time</td>
<td>30 secs hearing ringback</td>
</tr>
<tr>
<td>04 goto step</td>
<td>2 if unconditionally</td>
</tr>
<tr>
<td>05 stop</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>add vdn 59102</th>
<th>VECTOR DIRECTORY NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Extension:</strong> 59102</td>
<td><strong>Unicode Name? n</strong></td>
</tr>
<tr>
<td><strong>Name</strong>: CTI MultiMedia</td>
<td><strong>Destination</strong>: Vector Number 102</td>
</tr>
<tr>
<td>Attendant Vectoring? n</td>
<td></td>
</tr>
<tr>
<td>Meet-me Conferencing? n</td>
<td></td>
</tr>
<tr>
<td>Allow VDN Override? n</td>
<td></td>
</tr>
<tr>
<td>COR: 1</td>
<td></td>
</tr>
<tr>
<td>TN*: 1</td>
<td></td>
</tr>
<tr>
<td>Measured: none</td>
<td>Report Adjunct Calls as ACD*? n</td>
</tr>
</tbody>
</table>
5.8. Administer Agent IDs
The newly created Email skill needs to be added to the applicable agents. Use the “change agent-loginID n” command, where “n” is the first available agent ID. Navigate to Page 2, and add the Email skill group number from Section 5.7 to an available SN, and set the desired skill level under the corresponding SL, as shown below.

<table>
<thead>
<tr>
<th>SN</th>
<th>RL</th>
<th>SL</th>
<th>SN</th>
<th>RL</th>
<th>SL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>16:</td>
<td>31:</td>
<td>46:</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>17:</td>
<td>32:</td>
<td>47:</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>18:</td>
<td>33:</td>
<td>48:</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>19:</td>
<td>34:</td>
<td>49:</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>20:</td>
<td>35:</td>
<td>50:</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Login ID</th>
<th>Name</th>
<th>Extension</th>
<th>Dir Agt</th>
<th>AAS/AUD</th>
<th>COR Ag Pr SO</th>
</tr>
</thead>
<tbody>
<tr>
<td>55001</td>
<td>CC Agent 1</td>
<td>unstaffed</td>
<td>1</td>
<td>lvl 1/01</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1/01 2/01</td>
<td>3/01</td>
<td>4/01</td>
<td>5/01</td>
<td></td>
</tr>
<tr>
<td>55002</td>
<td>CC Agent 2</td>
<td>unstaffed</td>
<td>1</td>
<td>lvl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1/01 2/01</td>
<td>3/01</td>
<td>/</td>
<td>/</td>
<td></td>
</tr>
<tr>
<td>55003</td>
<td>CC Agent 3</td>
<td>unstaffed</td>
<td>1</td>
<td>lvl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1/01 2/01</td>
<td>3/01</td>
<td>/</td>
<td>/</td>
<td></td>
</tr>
</tbody>
</table>
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.

![System Manager Login Interface]
6.2. Administer Locations

In the subsequent screen (not shown), select Elements → Routing → Locations and click New in the subsequent screen (not shown) to add a new location. 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.

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.
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.

![SIP Entity Details](image)
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 “sm8”.
- **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.
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.
- **Location:** Select the applicable location for Communication Manager.
- **Time Zone:** Select the applicable time zone.
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 “sm8”.
- **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”
6.4. Administer Routing Policies
Add a new routing policy for routing of Email 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.
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 “5” (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.
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:** Domain as configured in Section 5.4.
- **Proxy:** IP address of the Session Manager signaling interface.
- **Realm:** The applicable domain name.
- **Register:** “False”
- **Profile:** “Internal”
The **Gateways** screen is displayed again, showing the newly added gateway entry. Click **Start** to start the gateway.

7.3. **Administer Destinations**
Select **Dialplan → Destinations** from the top menu, to display the **Destinations** screen. Select the add icon shown below.
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 Email VDN extension number from Section 5.8.

![Destination screen](image)

### 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.

![Outbound Routes screen](image)
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**.

![Outbound Routes Screen](image1)

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

![Dialplan Screen](image2)

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

![Dialplan Screen](image3)
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 Email calls is three minutes. In the compliance testing, the call timeout was set to 7200 minutes, as shown below.

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 Email 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 Email work items. In the compliance testing, the six extensions 200-205 shown below were pre-configured.
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.

![CT Admin v3.3.0 Log In](image)

7.7. Administer CTI Extensions

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

![CT Admin v3.2.12 - Sites](image)
The **Site Resources** screen is displayed next. Select the pertinent logical resource group, in this case “Resources”.

![Site Resources Screen](image)

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.

![View Resources Screen](image)
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 “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.
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 “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 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**.

7.8.3. **Email Server**

Navigate back to the **View Server Group** screen. Scroll the top menu bar as necessary to locate and select **Email**, followed by **Add Email Server** from bottom of screen.
The **Add Edit Email 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 Email server, as shown below.
7.9. Administer Agents
Navigate to Home → Agent Templates.

Select an agent that needs to be assigned to the Email profile. Select the Agent tab and enable Email.
7.10. 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 1
```

```
<table>
<thead>
<tr>
<th>Member</th>
<th>Port</th>
<th>Service State</th>
<th>Mtce Connected Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001/0001</td>
<td>T00001</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0002</td>
<td>T00002</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0003</td>
<td>T00003</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0004</td>
<td>T00004</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0005</td>
<td>T00005</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0006</td>
<td>T00006</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0007</td>
<td>T00007</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0008</td>
<td>T00008</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0009</td>
<td>T00009</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
<tr>
<td>0001/0010</td>
<td>T00010</td>
<td>in-service/idle</td>
<td>no</td>
</tr>
</tbody>
</table>
```

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 1
```

```
| Group ID: | Group Type: sip
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Group State: in-service</td>
</tr>
</tbody>
</table>
```
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 **Elements ➔ 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**.

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

![SIP Entity, Entity Link Connection Status](image)
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 agent screen below is displayed next. Retain the default values, and select LOGIN to log the agent into the ACD on Communication Manager.
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.
Once an email arrives, answer the call and respond to the Email.

9. Conclusion

These Application Notes describe the configuration steps required for CTIntegrations CT Suite 3.3 to successfully interoperate with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Session Manager 8.0.1 for Email integration. All feature and serviceability test cases were completed.

10. Additional References

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


5. Application Notes for CTIntegrations CT Suite 3.3 with Avaya Aura® Communication Manager 8.0.1 and Avaya Aura® Application Enablement Services 8.0.1 for Voice Integration, Release 1.0.

Documentation related to CT Desktop may directly be obtained from CTIntegrations.

6. CTIntegrations CT Suite Admin User Guide, User Guides v3.2
©2019 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.