Avaya Solution & Interoperability Test Lab

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.

Device Type	Extension
VDN	59102
Skill	59002
Agent Station	50001, 50002, 51001
Agent ID	55001, 55002, 55003
Agent Password	123456

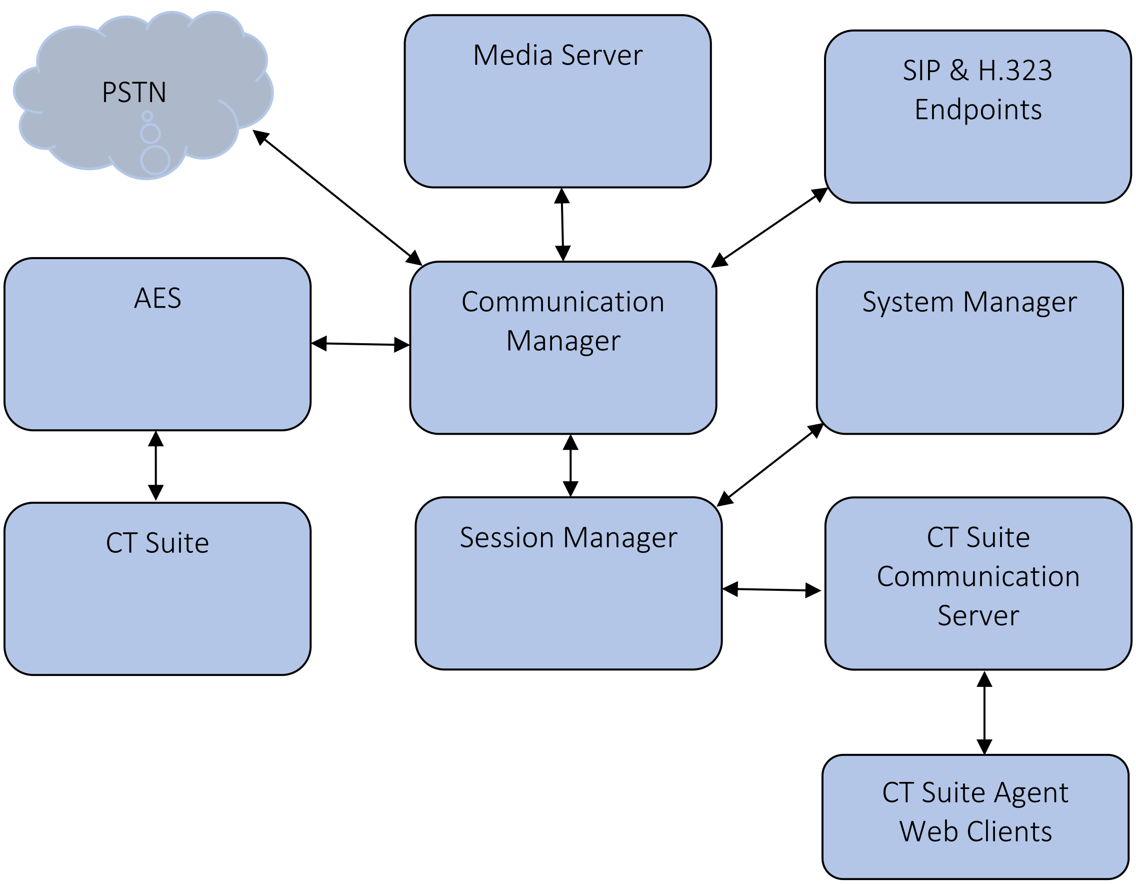


Figure 1: Compliance Testing Configuration

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	8.0.1.1.0-FP1SP1
Avaya Aura® Media Server in Virtual Environment	v.8.0.0.183
Avaya Aura® Application Enablement Services in Virtual Environment	8.0.1.0.2.5-0
Avaya Aura® Session Manager in Virtual Environment	8.0.1.1.801103
Avaya Aura® System Manager in Virtual Environment	8.0.1.1.039340
Avaya 96x1 IP Deskphones (H.323)	6.8102
Avaya 96x1 IP Deskphones (SIP)	7.1.5.0.11
Avaya J169 IP Deskphone (H.323)	6.8102
Avaya Agent for Desktop	1.7.22.1
CTIntegrations CT Suite on Microsoft Windows Server 2016 • CT Admin • CT Web Client • CT Device Manager • CT Open Queue • Avaya DMCC .Net SDK	3.3 7.1
CTIntegrations CT Suite Communication Server on Debian 8 • FreeSWITCH • FusionPBX	4.2 1.6.20 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 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.

```
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 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                                        Page   1 of   2
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? n                                     Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? y  Peer Server: SM                         Clustered? n
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
   Near-end Node Name: procr                  Far-end Node Name: sm8
 Near-end Listen Port: 5061                 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                                            Page   1 of   5
                                TRUNK GROUP

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: sm8                        COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                    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                                            Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



   Suppress # Outpulsing? n  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.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  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.

```
change ip-codec-set 5                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 5

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  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                                           Page   1 of   4
                                  HUNT GROUP

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

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

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

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

                      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.

```
change vector 102                                              Page   1 of   6
                                  CALL VECTOR

    Number: 102              Name: CTI MultiMedia
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? y  G3V4 Adv Route? y   CINFO? y   BSR? y   Holidays? y
 Variables? y   3.0 Enhanced? y
01 wait-time    2   secs hearing ringback
02 queue-to     skill 2    pri m
03 wait-time    30  secs hearing ringback
04 goto step    2             if unconditionally
05 stop
```

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 59102                                               Page   1 of   3
                            VECTOR DIRECTORY NUMBER

                             Extension: 59102                  Unicode Name? n
                                 Name*: CTI MultiMedia
                           Destination: Vector Number       102
                   Attendant Vectoring? n
                  Meet-me Conferencing? n
                    Allow VDN Override? n
                                   COR: 1
                                   TN*: 1
                              Measured: none     Report Adjunct Calls as ACD*? n
```

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.

```
change agent-loginID 55001                                           Page   2 of   2
                                 AGENT LOGINID
      Direct Agent Skill: 1                             Service Objective? n
Call Handling Preference: skill-level               Local Call Preference? n

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

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.

```
list agent-loginID 55001 count 3
                               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

55001            CC Agent 1      unstaffed          1               1   lvl
                  1/01    2/01    3/01    4/01    5/01     /       /       /
55002            CC Agent 2      unstaffed                          1   lvl
                  1/01    2/01    3/01     /       /       /       /       /
55003            CC Agent 3      unstaffed                          1   lvl
                  1/01    2/01    3/01     /       /       /       /       /
```

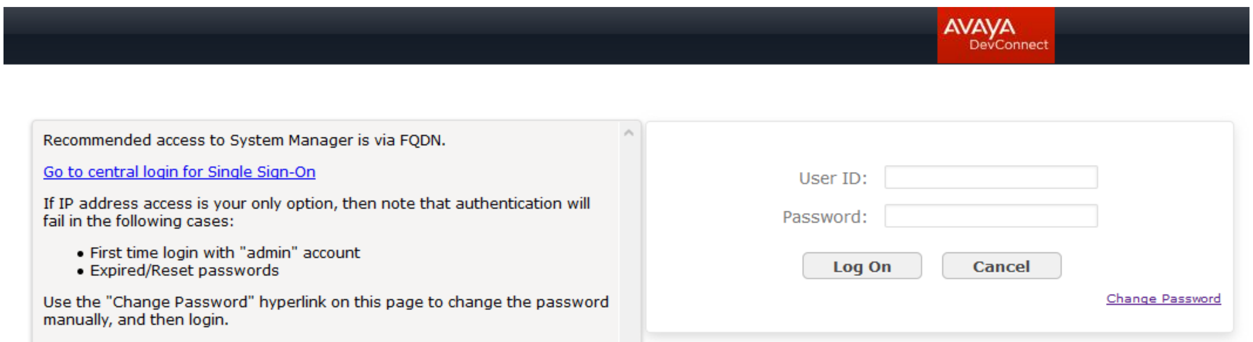
6. Configure Avaya Aura® Session Manager

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

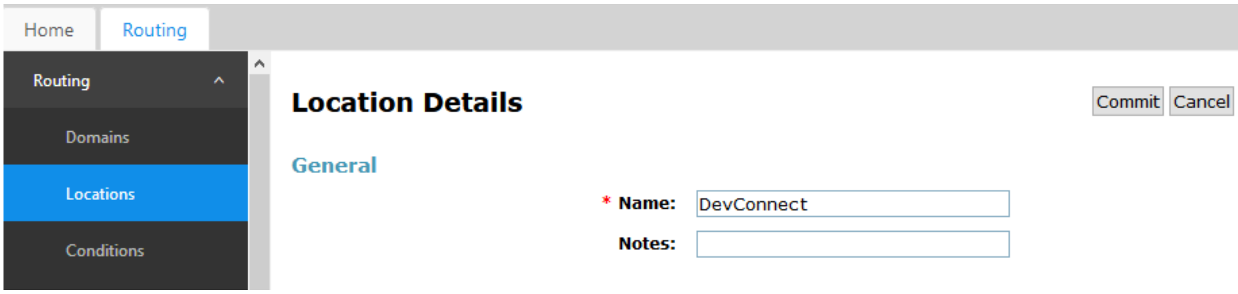
6.1. Launch System Manager

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.

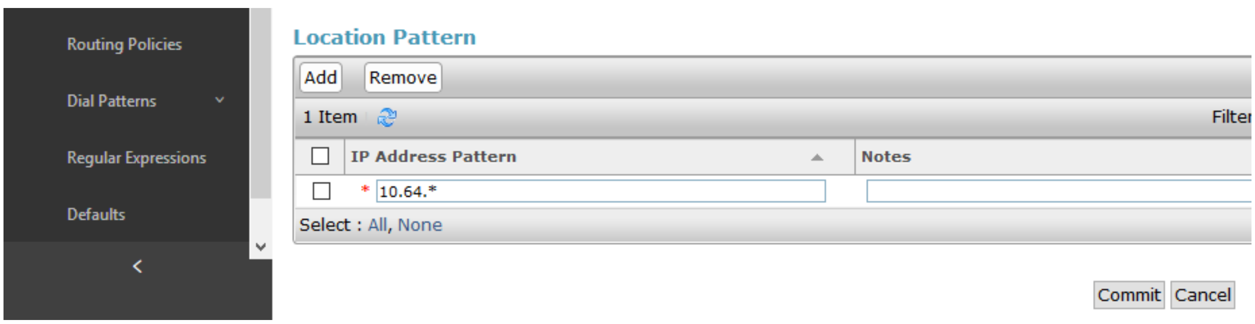


6.2. Administer Locations

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

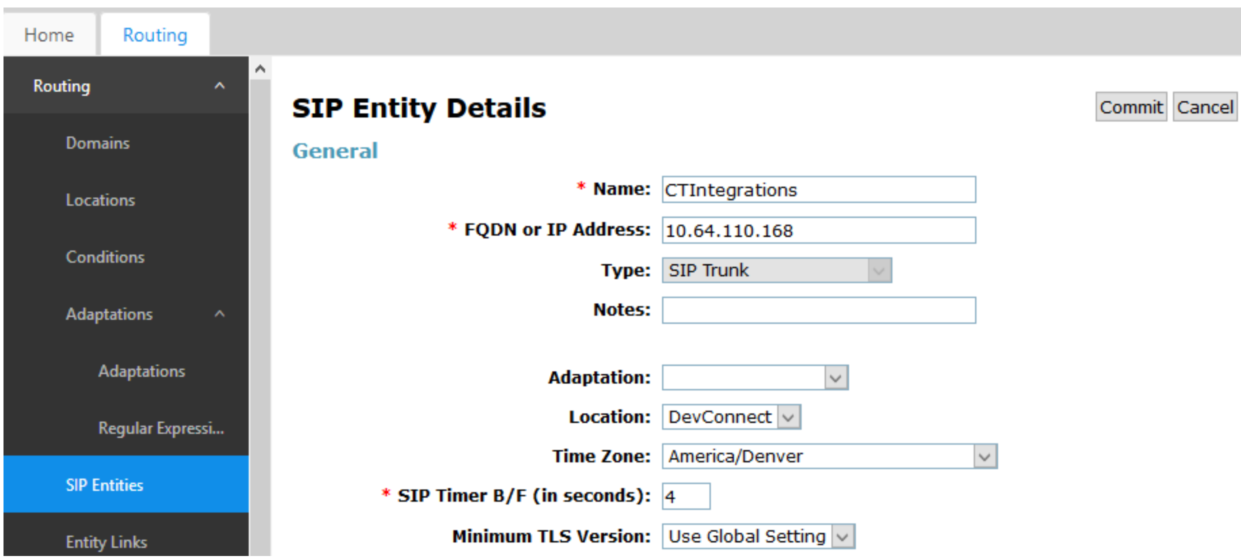
Add two new SIP entities, one for CT Suite and one for the new SIP trunks with Communication Manager.

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.

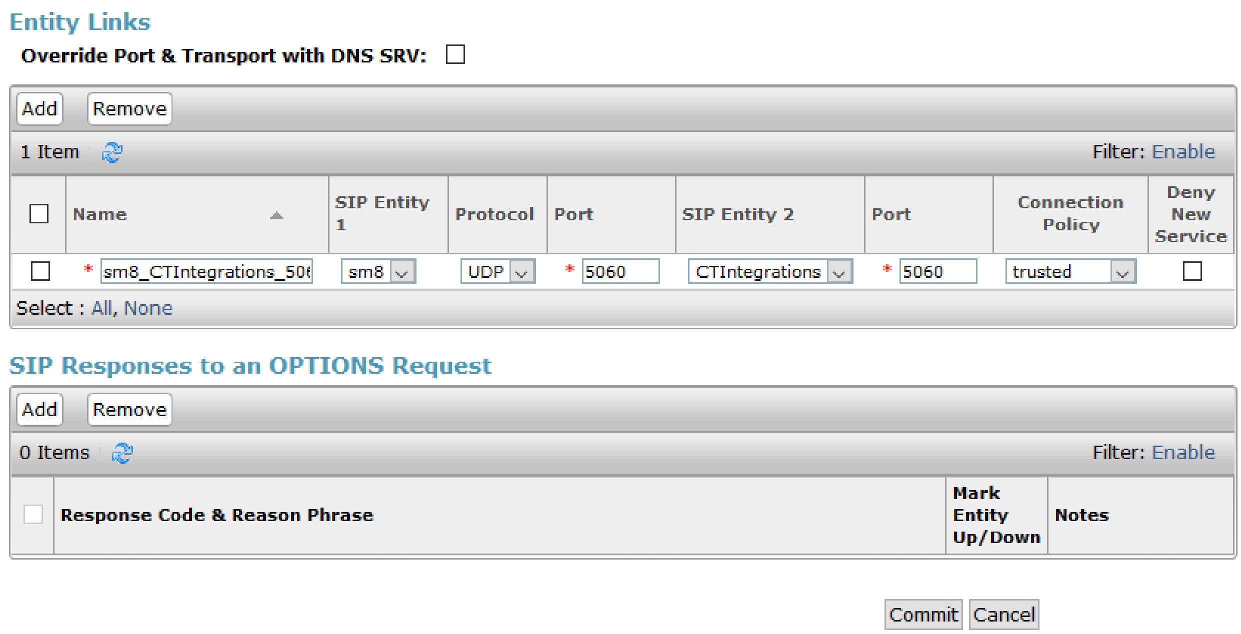
- **Name:** A descriptive name.
- **FQDN or IP Address:** The IP address of the CT Suite Communication Server.
- **Type:** "SIP Trunk"
- **Location:** Select the CT Suite location name from **Section 6.2**.
- **Time Zone:** Select the applicable time zone.



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.

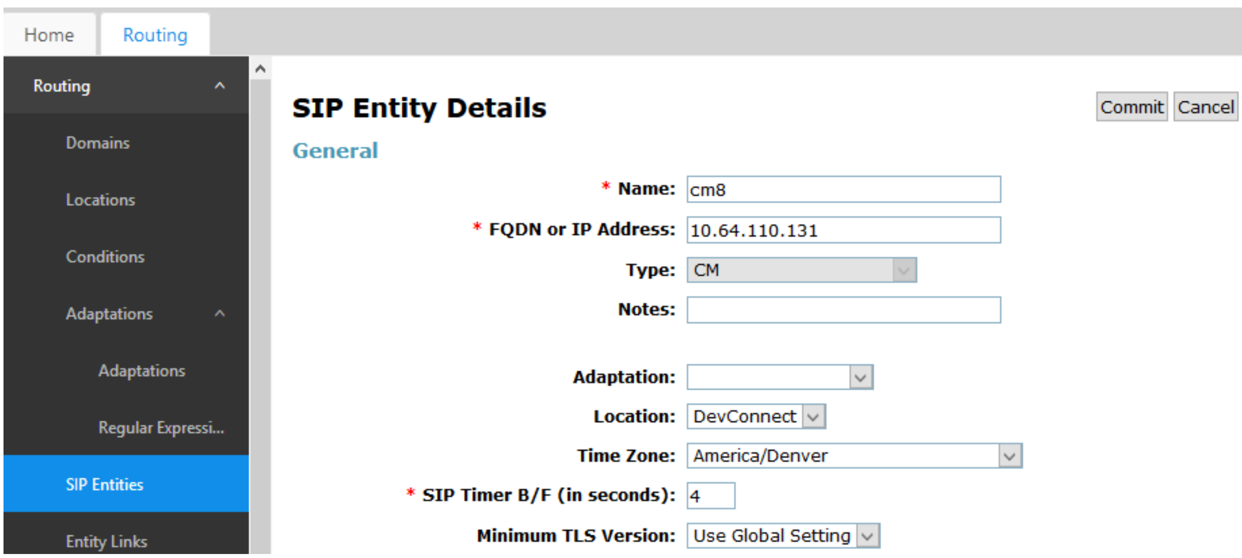


6.3.2. SIP Entity for Communication Manager

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.

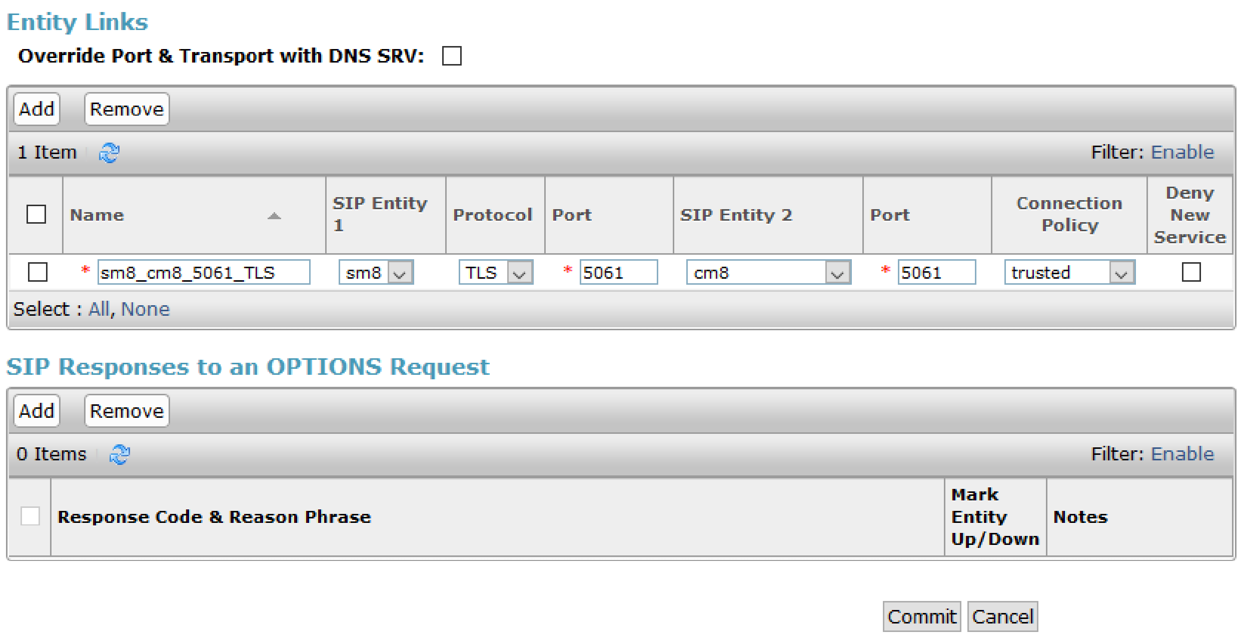
The **SIP Entity Details** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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"



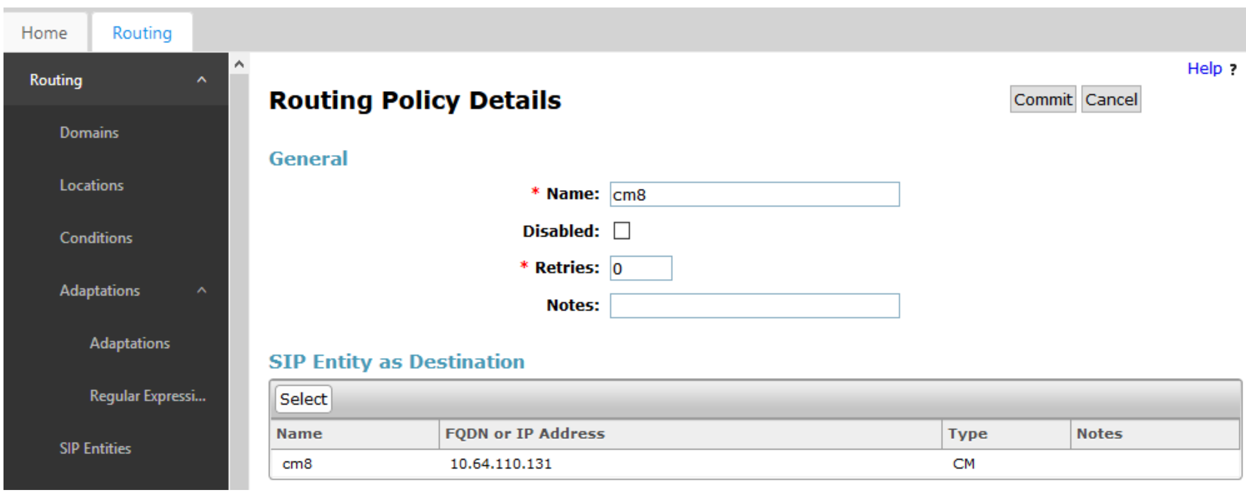
6.4. Administer Routing Policies

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.

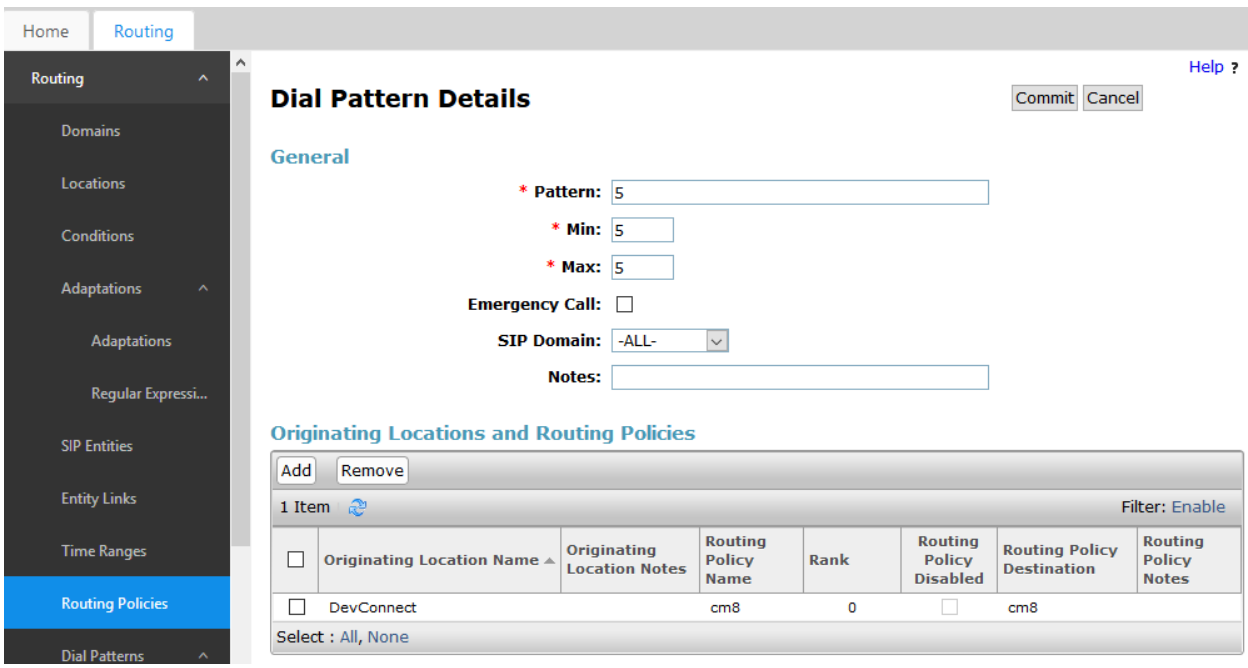


6.5. Administer Dial Patterns

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

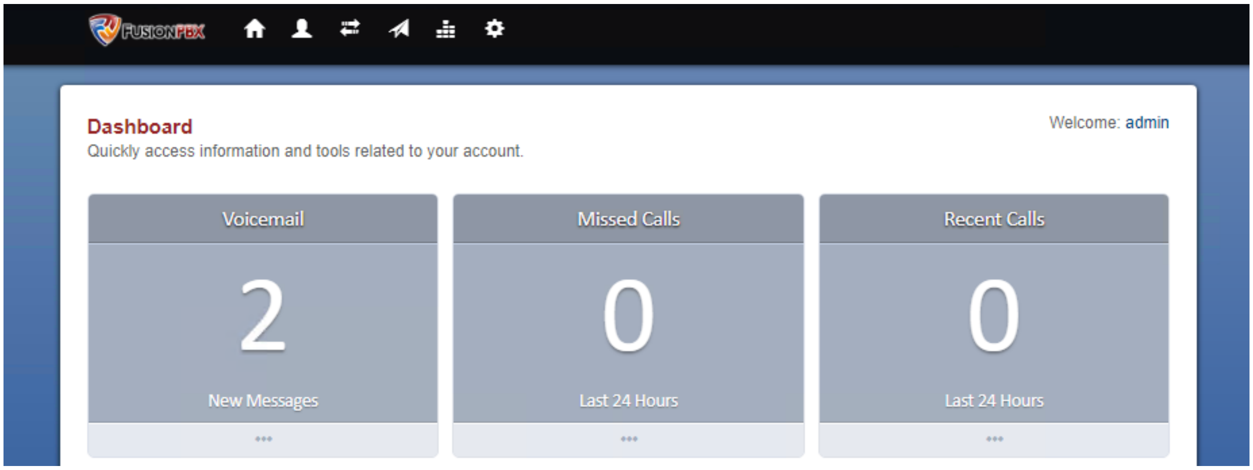
The configuration of CT Suite is typically performed by CTIntegrations system integrators. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch FusionPBX

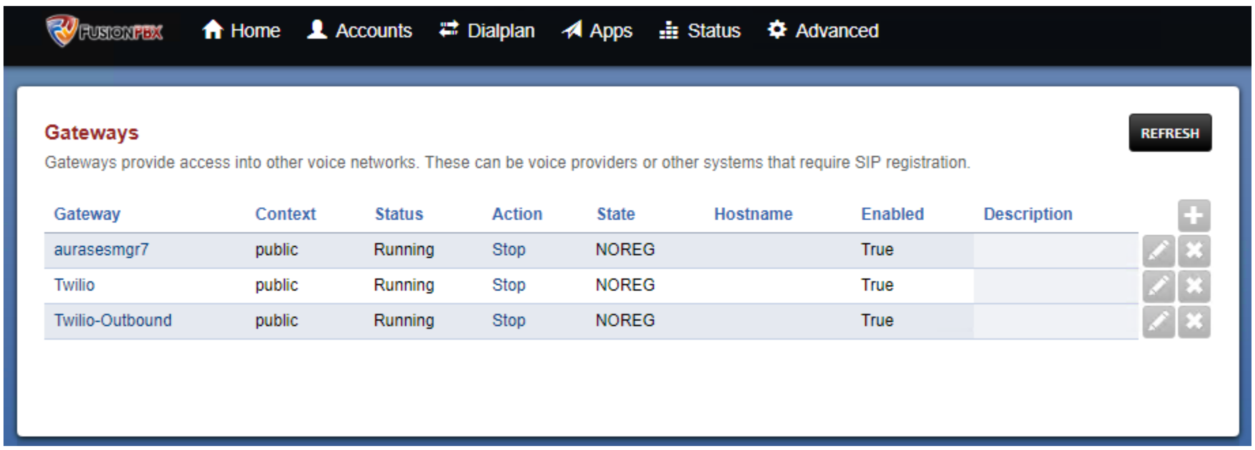
Access the FusionPBX web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of the CT Suite Communication Server. The **FUSIONPBX** screen below is displayed. Log in using the administrator credentials.

7.2. Administer Gateways

The **Dashboard** screen below is displayed.

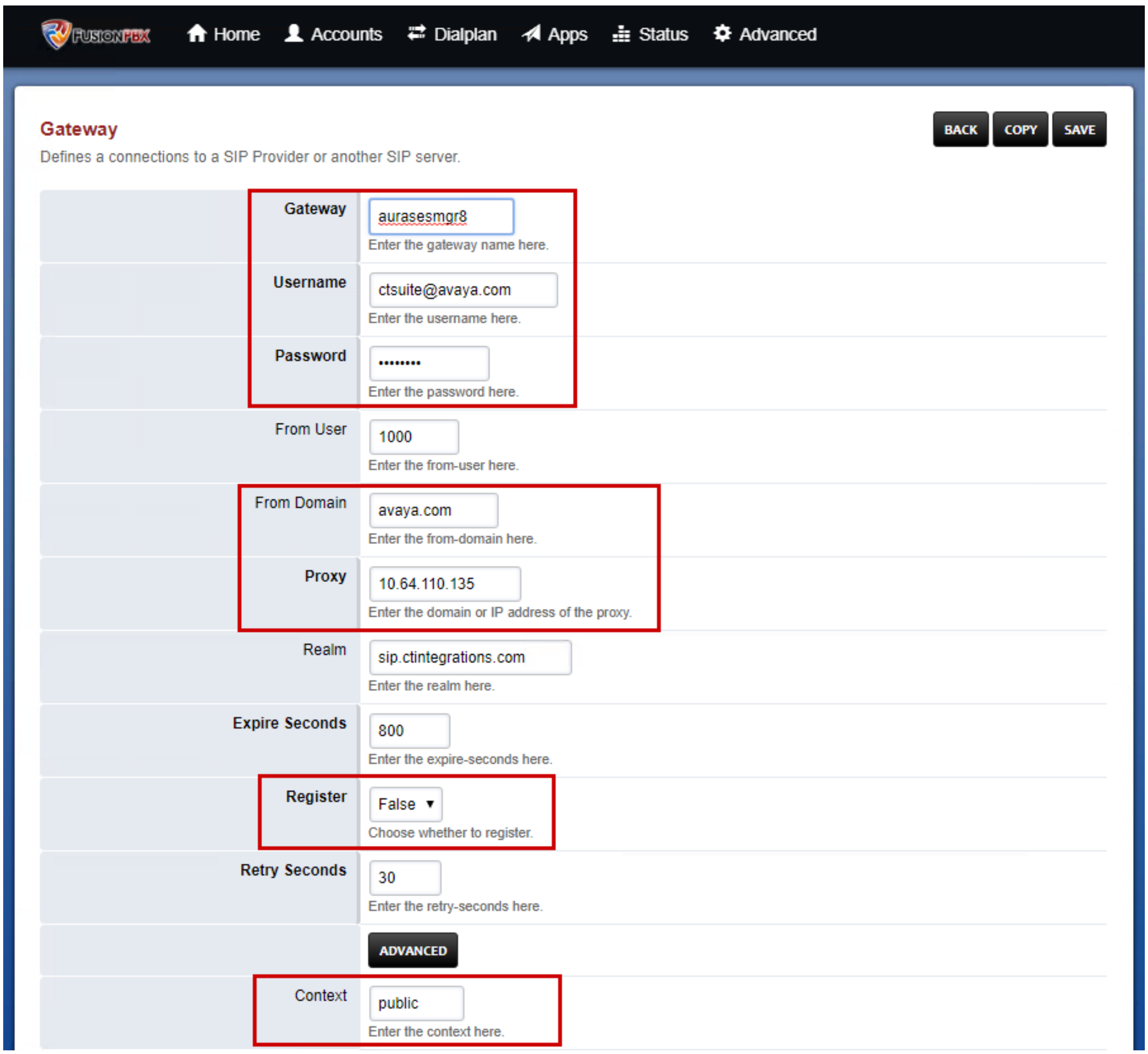


Select **Accounts → Gateways** from the top menu. The **Gateways** screen is displayed next. Select the add icon shown below.

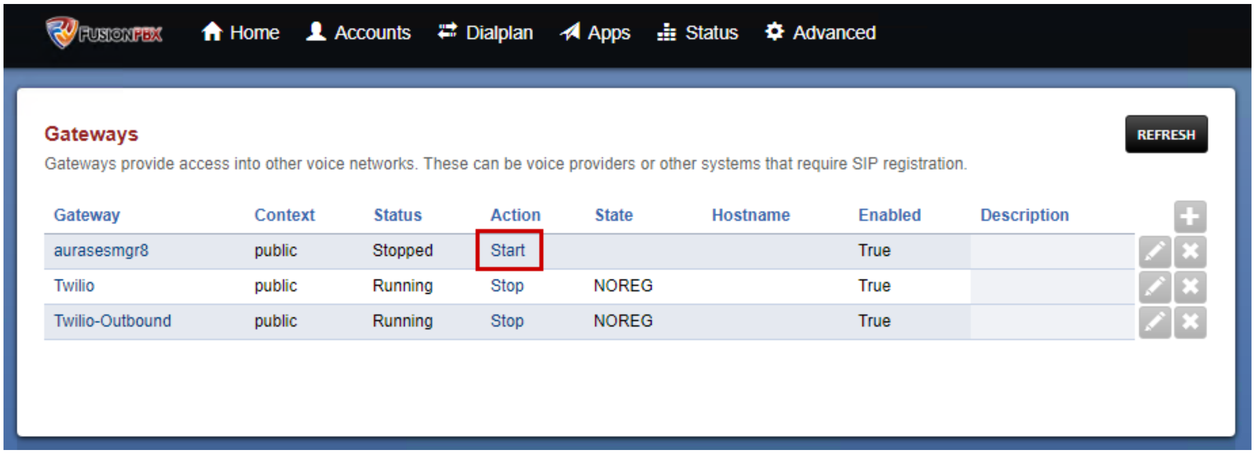


The **Gateway** screen is displayed. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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"

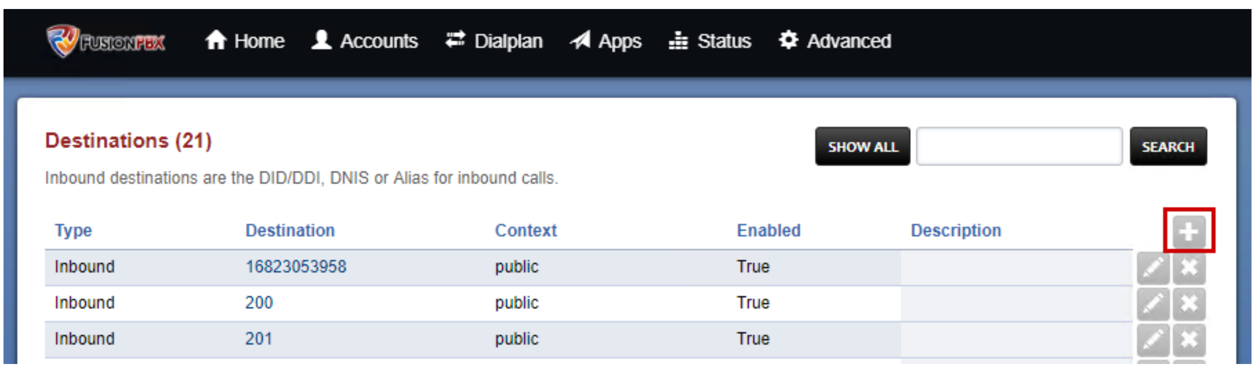


The **Gateways** screen is displayed again, showing the newly added gateway entry. Click **Start** to start the gateway.



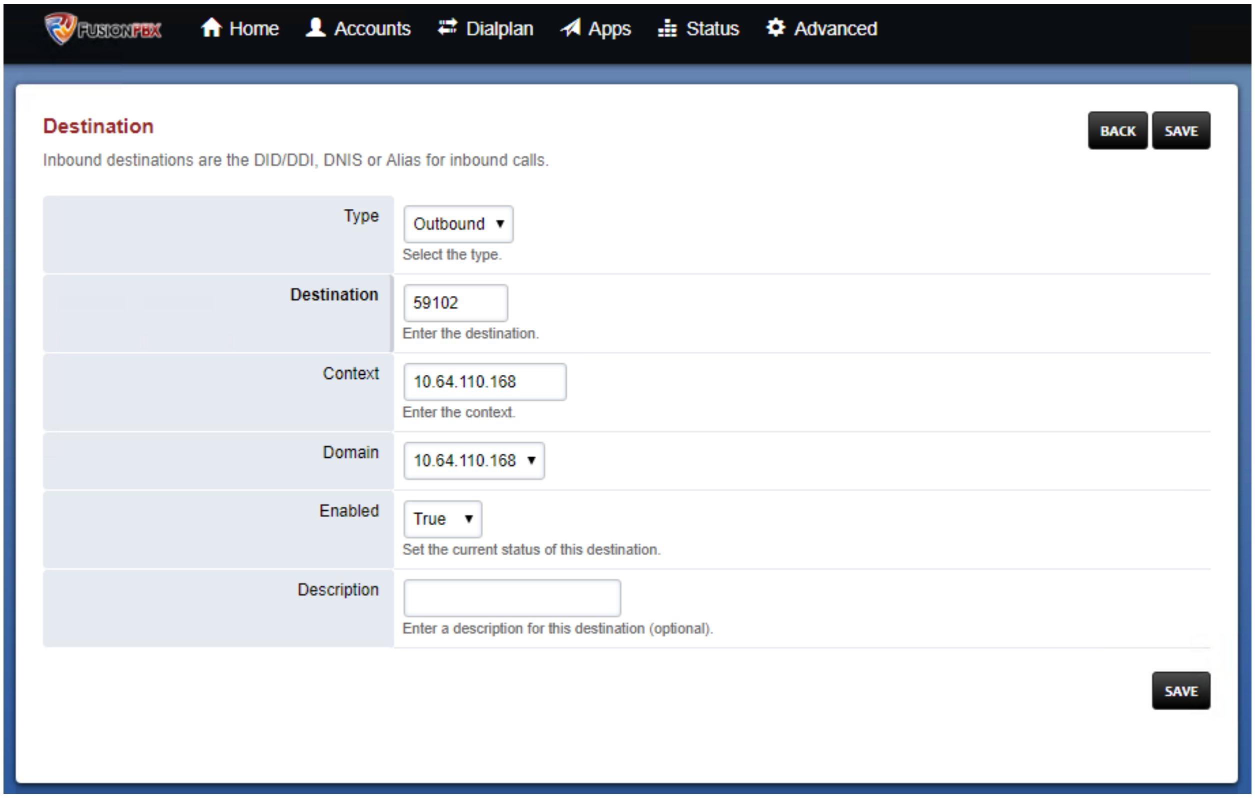
7.3. Administer Destinations

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



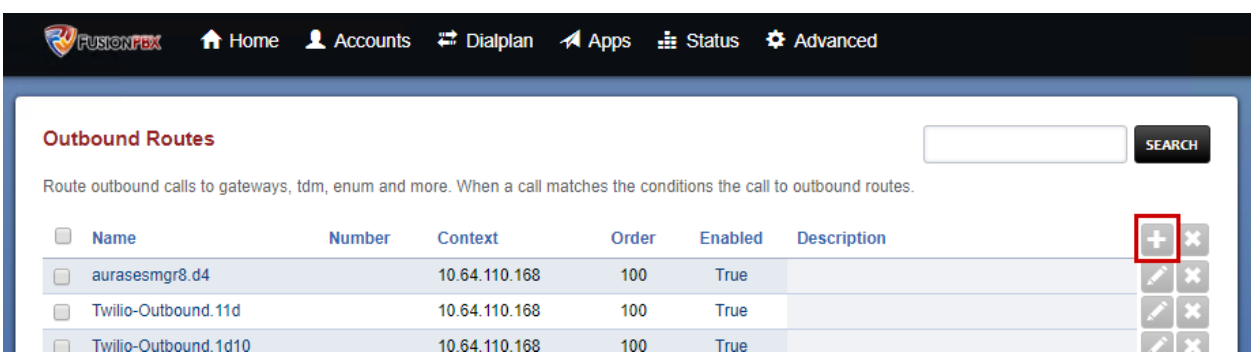
The **Destination** screen is displayed.   Enter the following values for the specified fields, and retain the default values for the remaining fields.

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



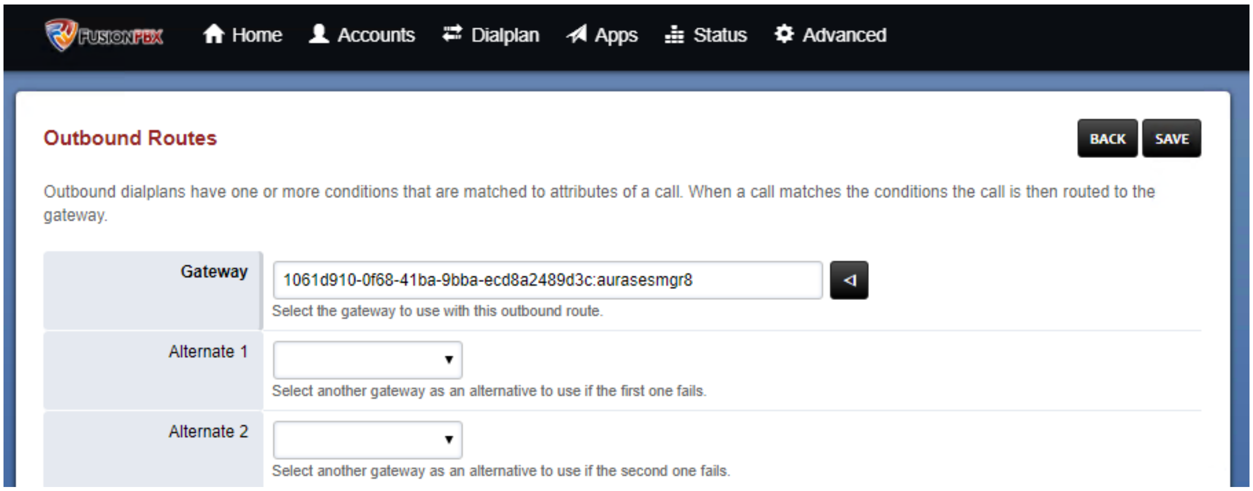
7.4. Administer Outbound Routes

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

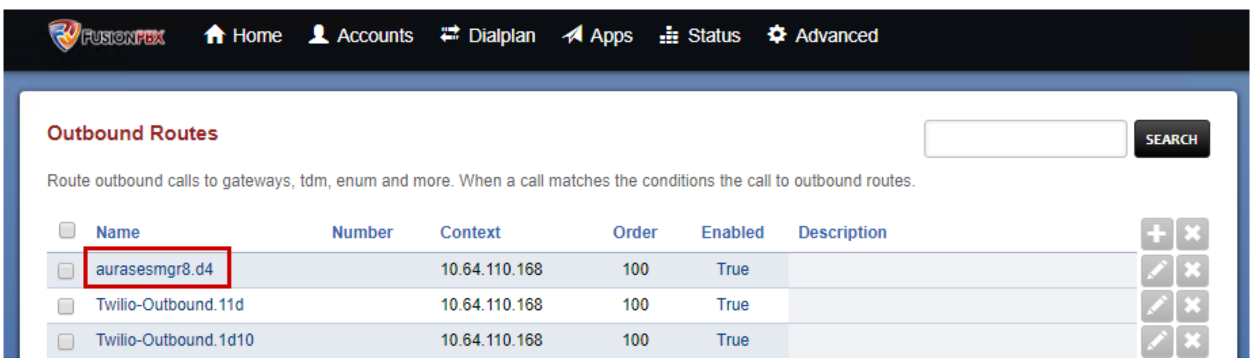


The **Outbound Routes** screen is updated. Enter the following values for the specified fields, and retain the default values for the remaining fields.

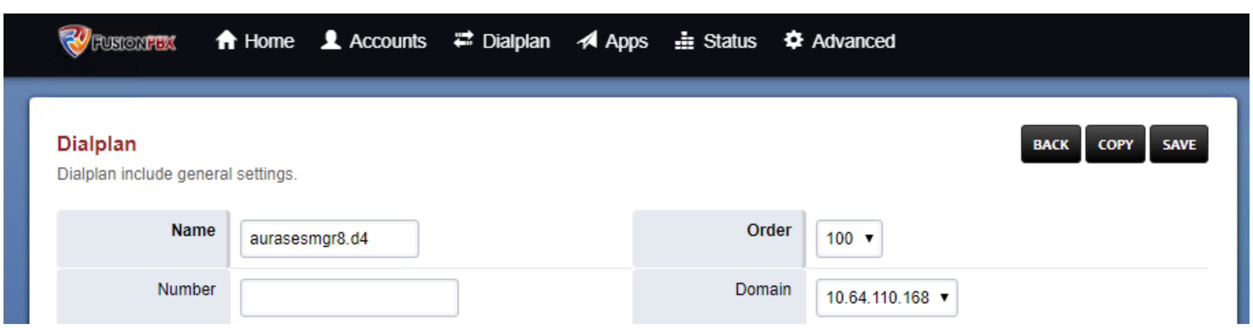
- **Gateway:** Select the pertinent gateway name from **Section 7.2**.



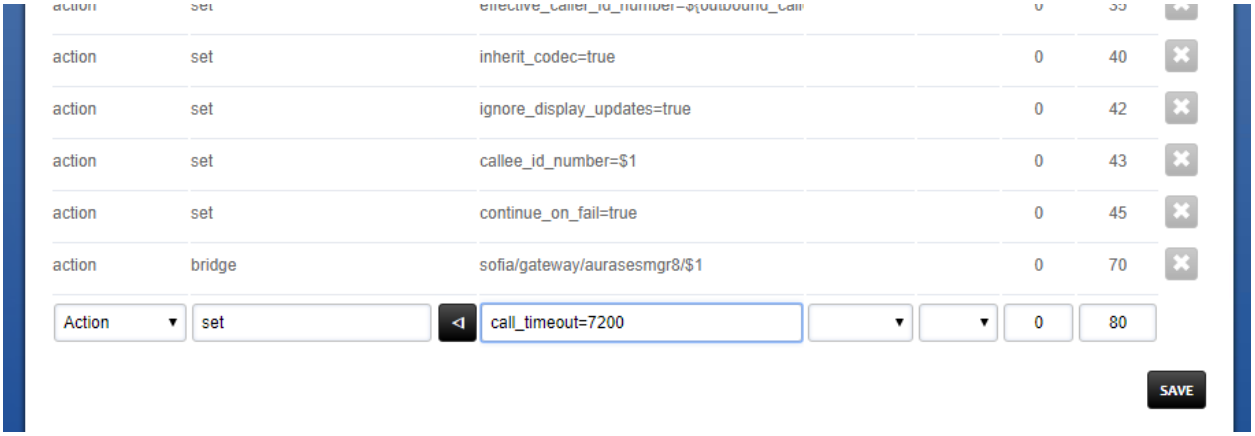
The **Outbound Routes** screen is updated, showing the newly added entry. Click on the **Name** of the new entry.



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



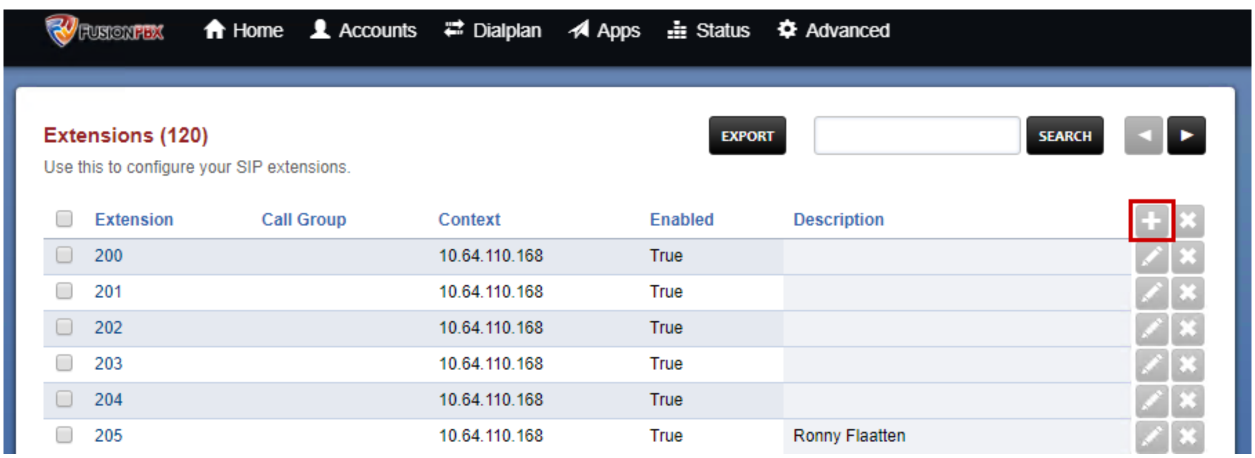
Scroll to the bottom of the screen, add an entry for the call timeout parameter and set to the desired value. The default timeout for the SIP Email calls is three minutes. In the compliance testing, the call timeout was set to 7200 minutes, as shown below.



7.5. Administer SIP Extensions

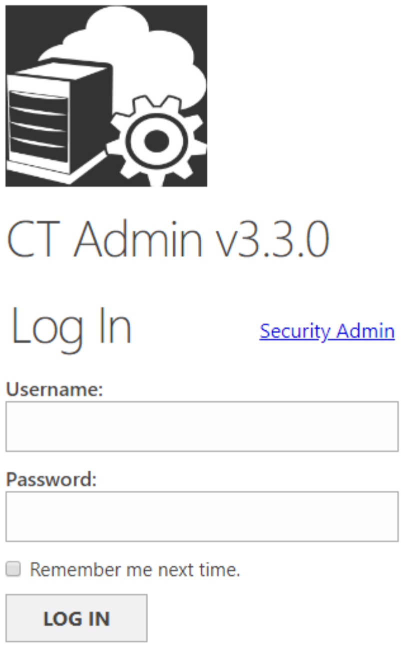
Select **Accounts → Extensions** from the top menu, to display the **Extensions** screen. Select the add icon shown below, to add an extension by following reference [6], the extension will be used as originator of calls for Email work items.

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

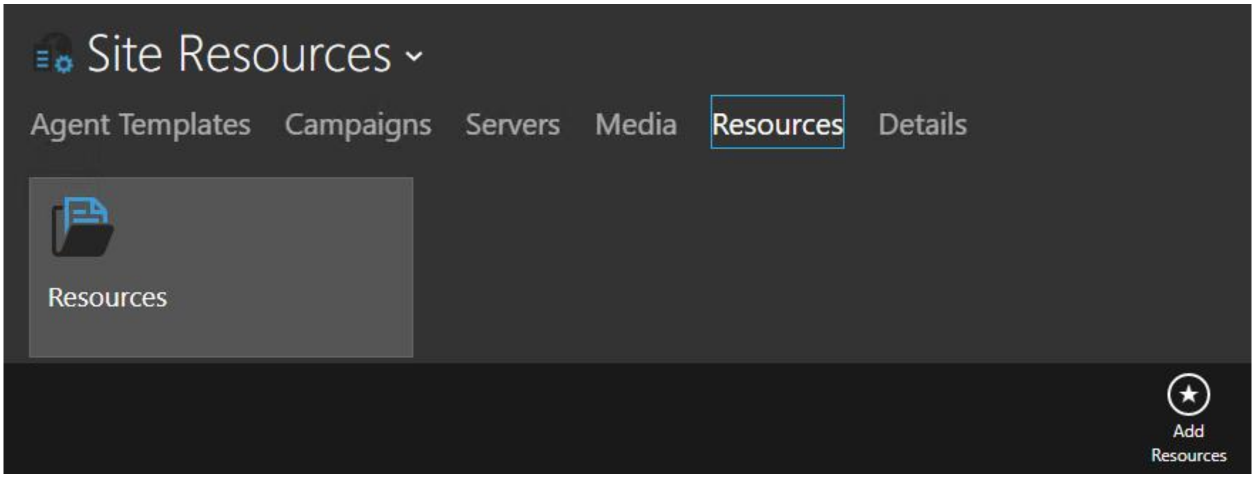
Access the CT Admin web interface by using the URL "http://ip-address/CTAdmin" in an Internet browser window, where "ip-address" is the IP address of the CT Suite server. The **CT Admin** screen below is displayed. Log in using the administrator credentials.



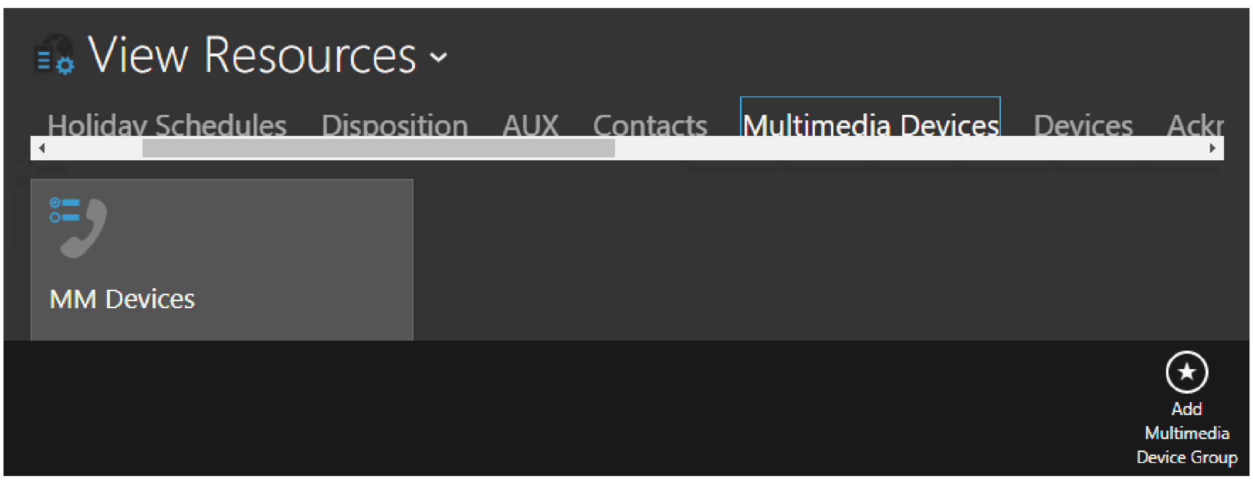
7.7. Administer CTI Extensions

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

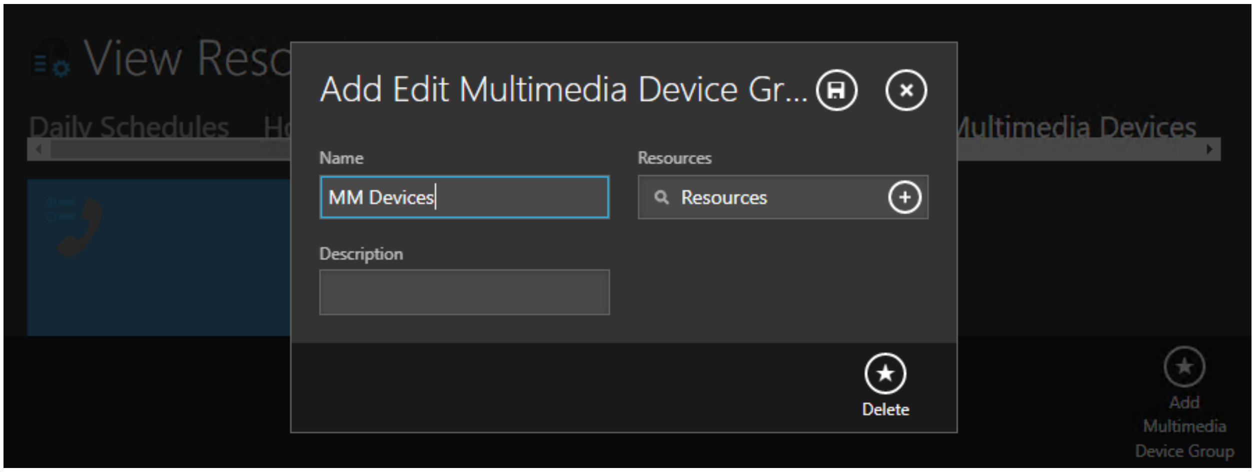
The **Site Resources** screen is displayed next. Select the pertinent logical resource group, in this case “Resources”.



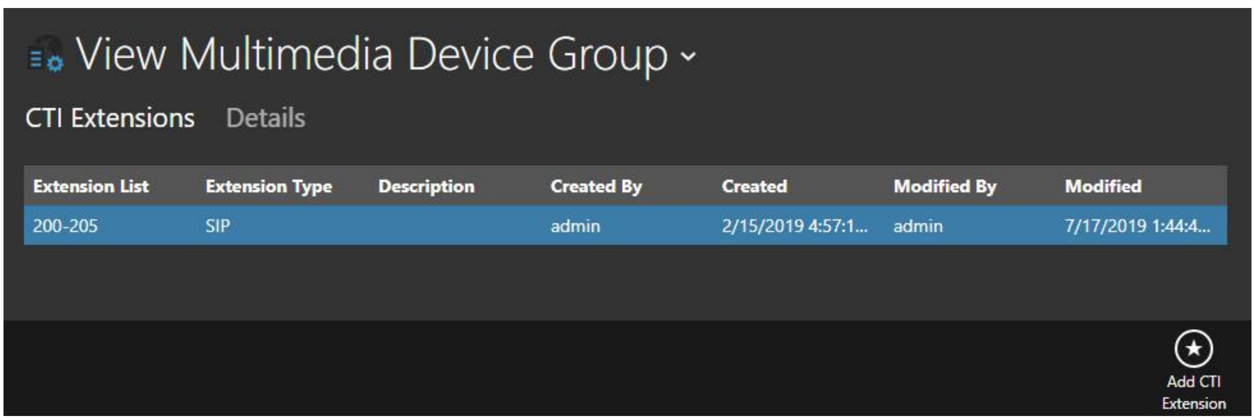
The **View Resources** screen is displayed. Scroll the top menu bar as necessary to locate and select **Multimedia Devices**, followed by **Add Multimedia Device Group** from bottom of screen to add a logical group for multimedia devices.



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.

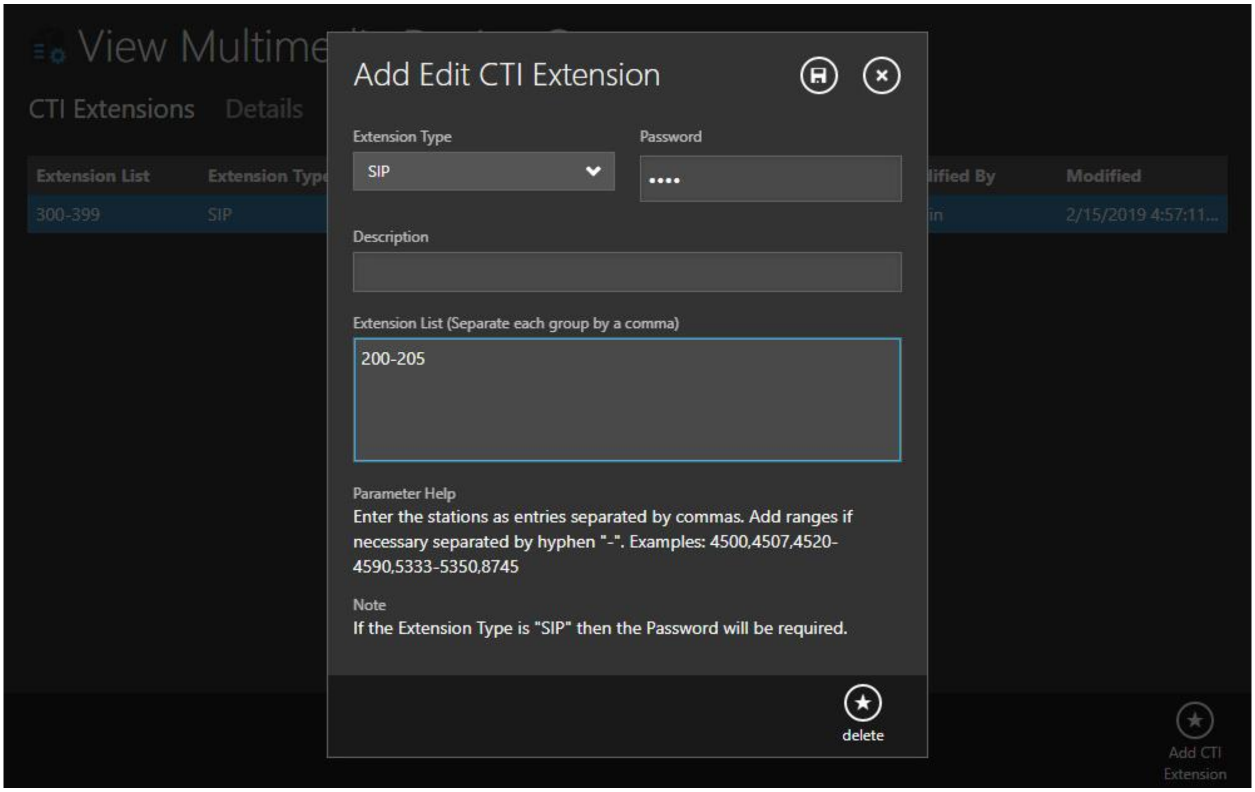


The **View Resources** screen is displayed again. Select the newly added group, in this case "MM_Devices". The **View Multimedia Device Group** screen is displayed next. Select the **CTI Extensions** tab, followed by **Add CTI Extension** from bottom of screen.



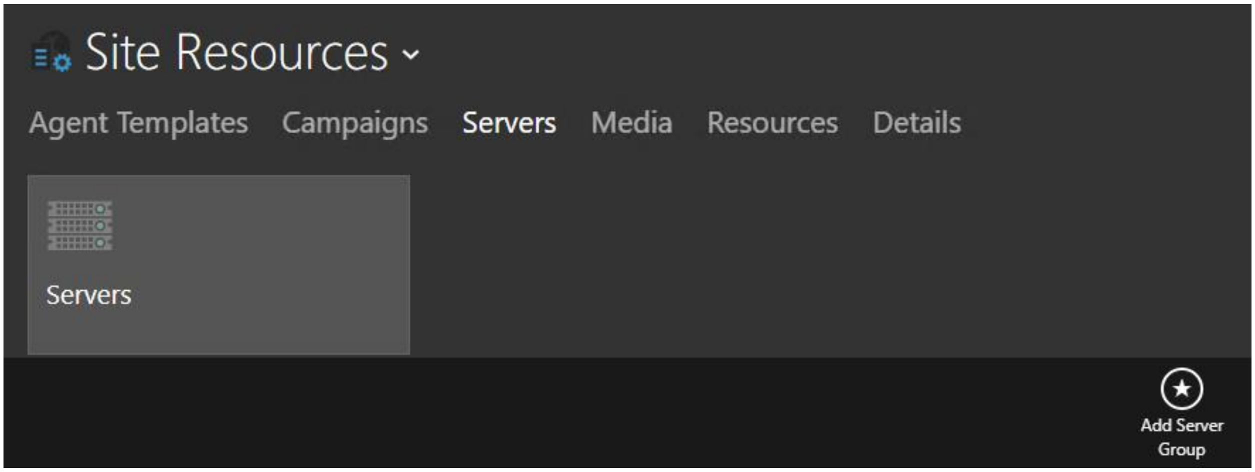
The **Add Edit CTI Extension** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **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**.



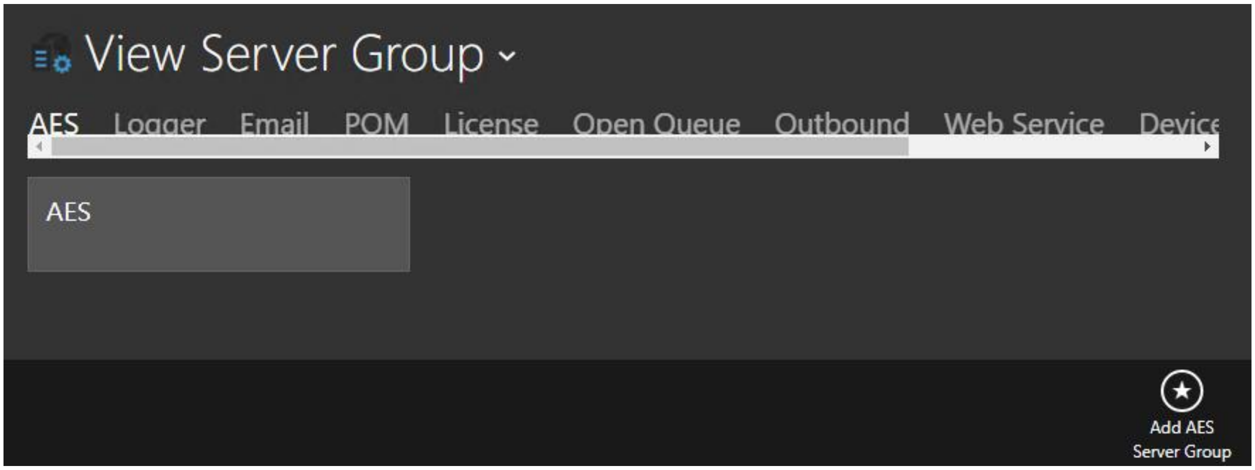
7.8. Administer Servers

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



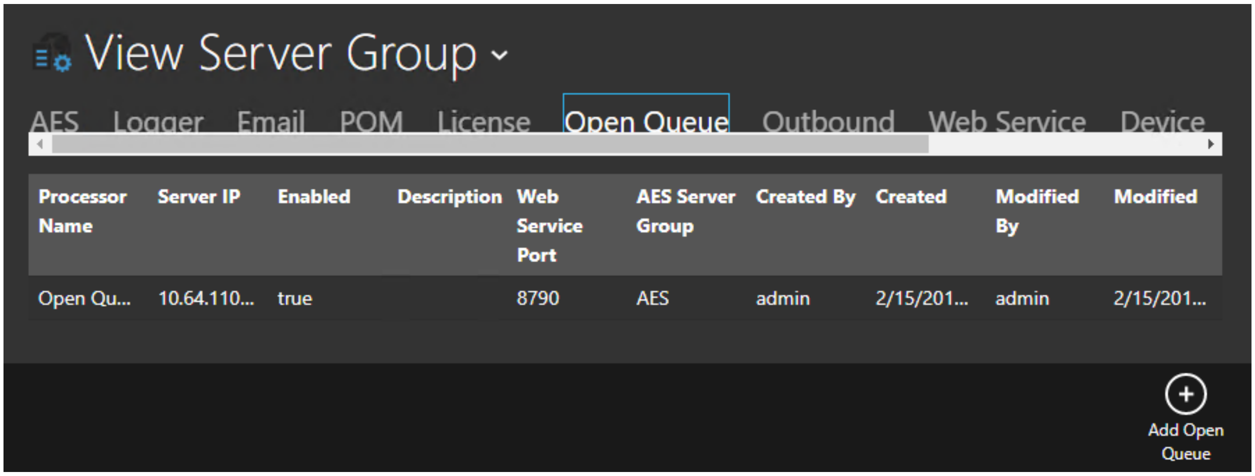
7.8.1. AES Server

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.



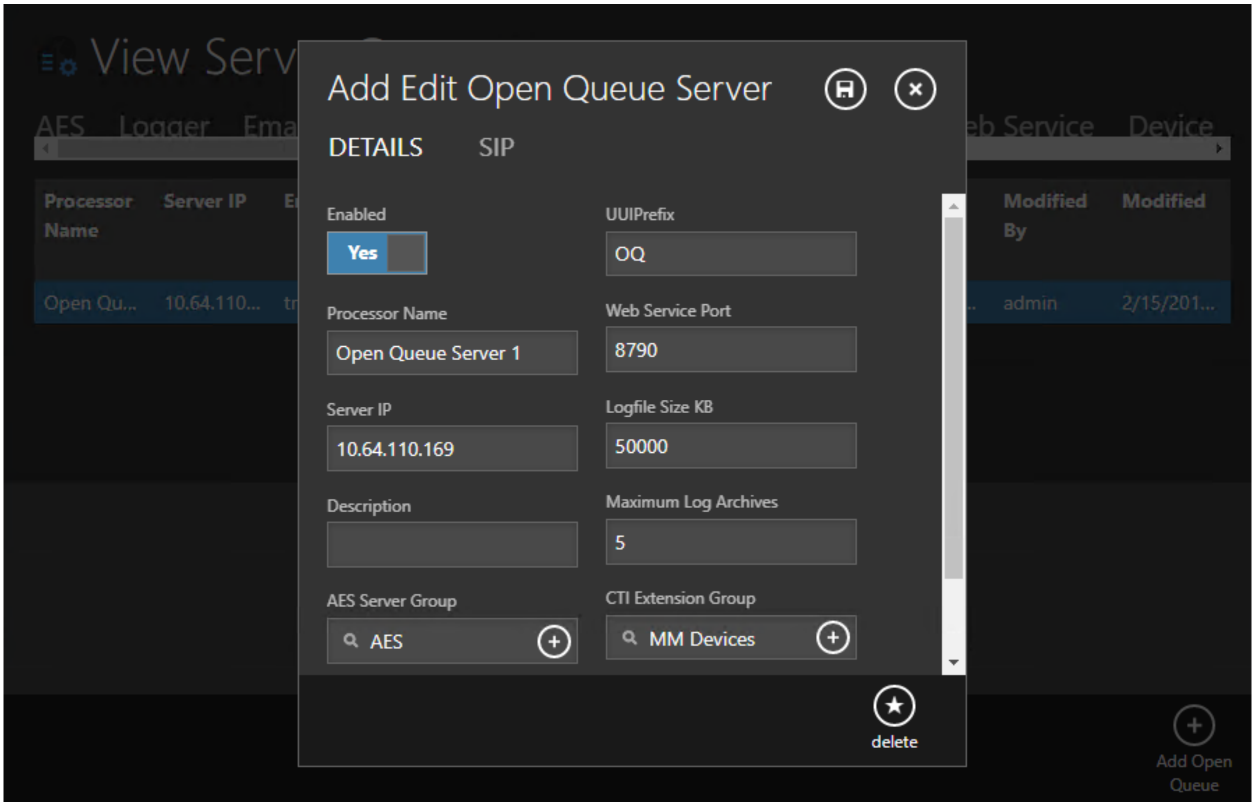
7.8.2. Open Queue Server

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

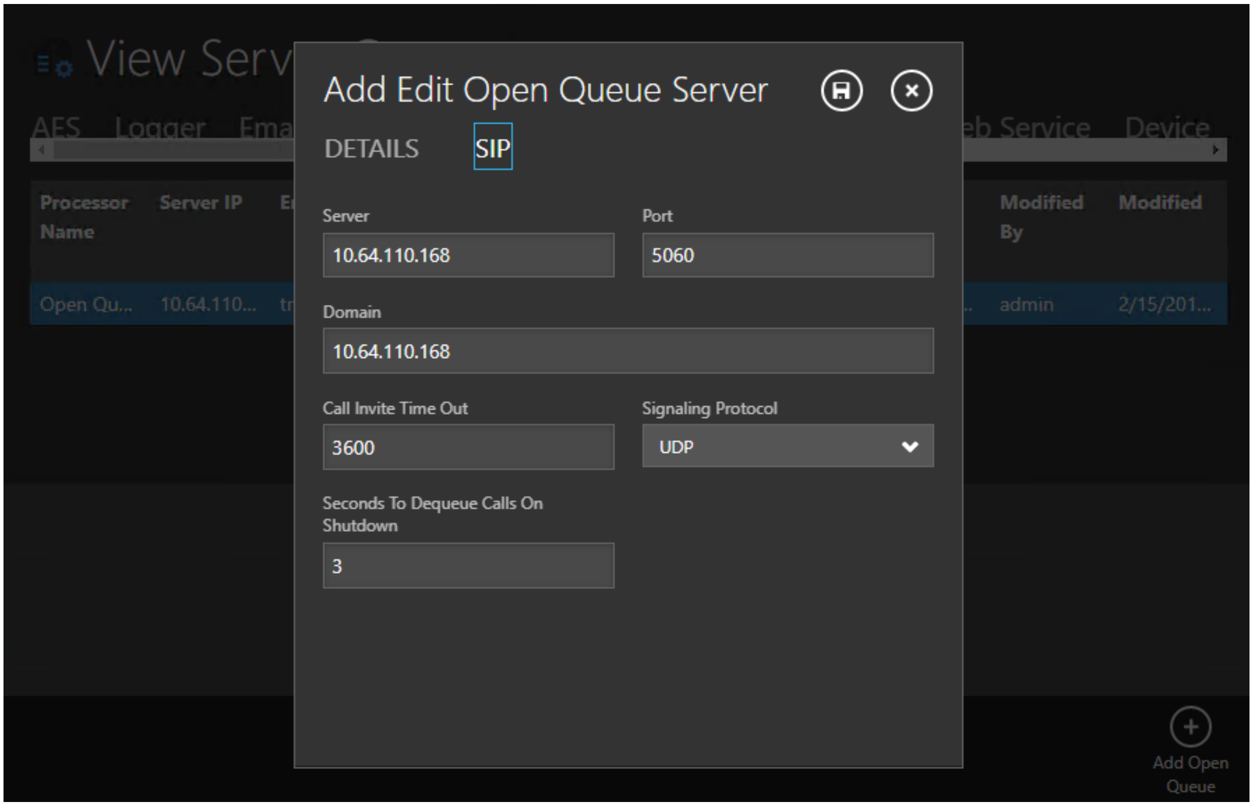


The **Add Edit Open Queue Server** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

- **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**.

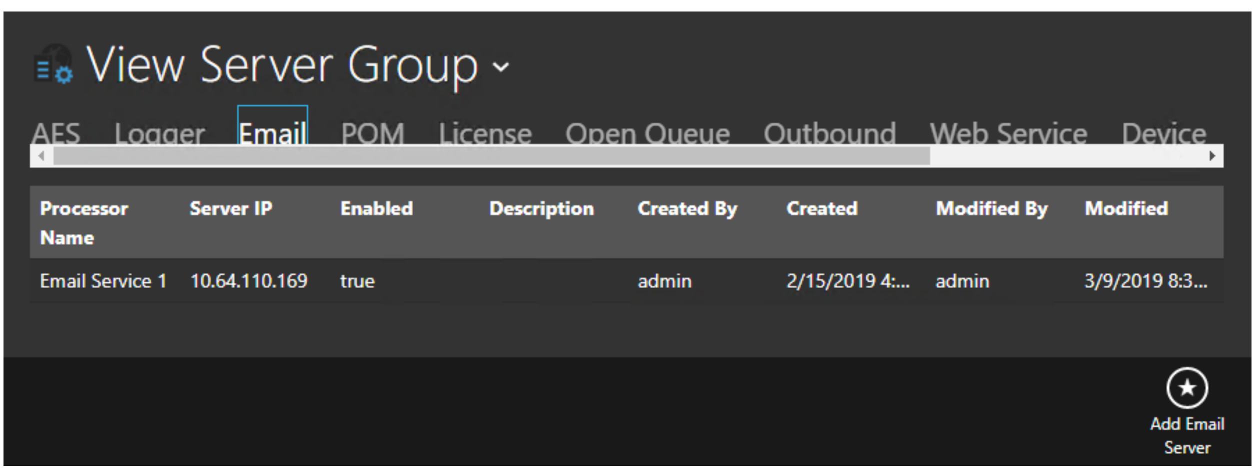


Select the **SIP** tab. For **Server** and **Domain**, enter the IP address of CT Suite Communication Server. For **Port**, enter the CT Suite SIP entity link port number from **Section 6.3.1**.



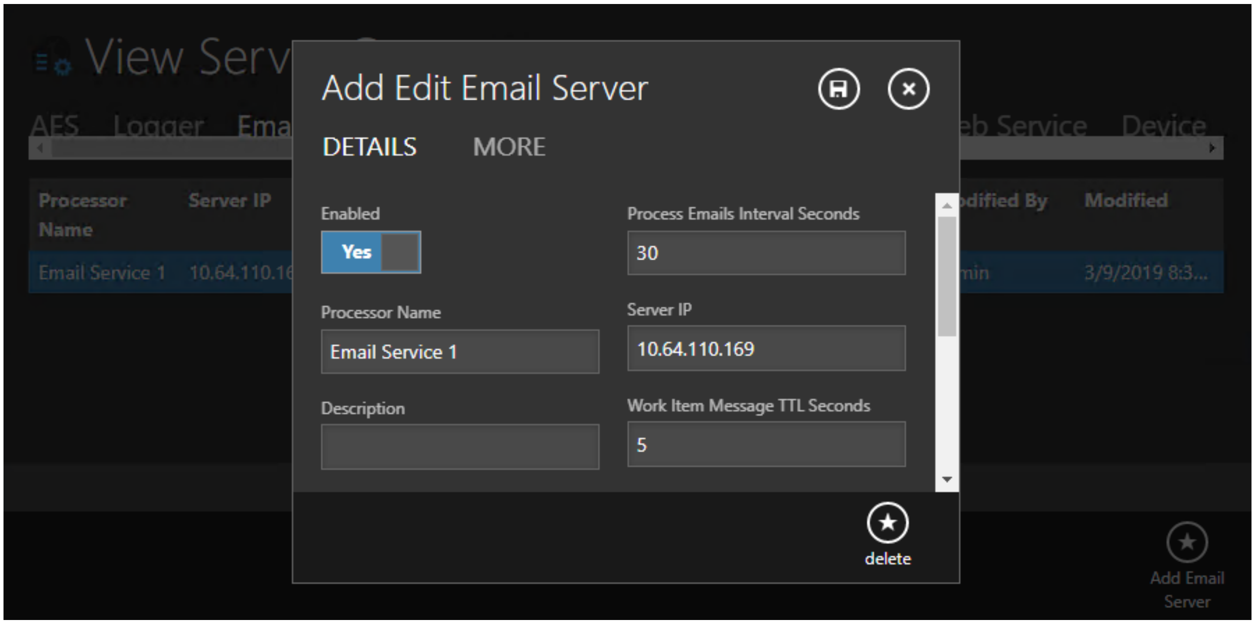
7.8.3. Email Server

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.

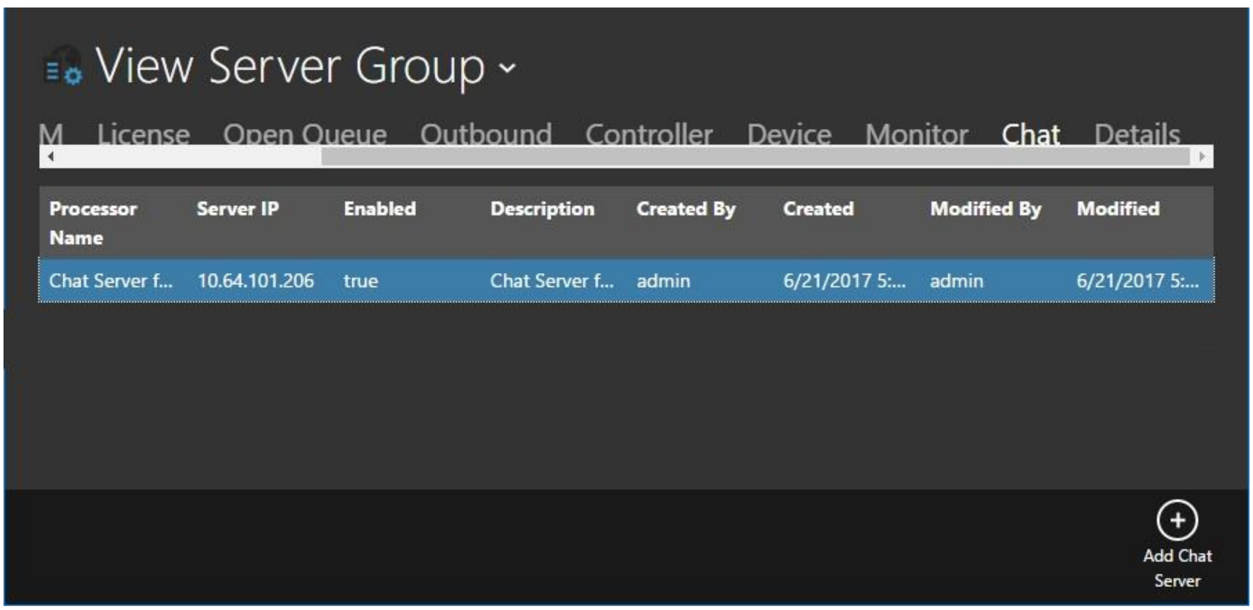


The **Add Edit Email Server** screen is displayed. Enter the following values for specified fields, and retain the default values for the remaining fields.

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

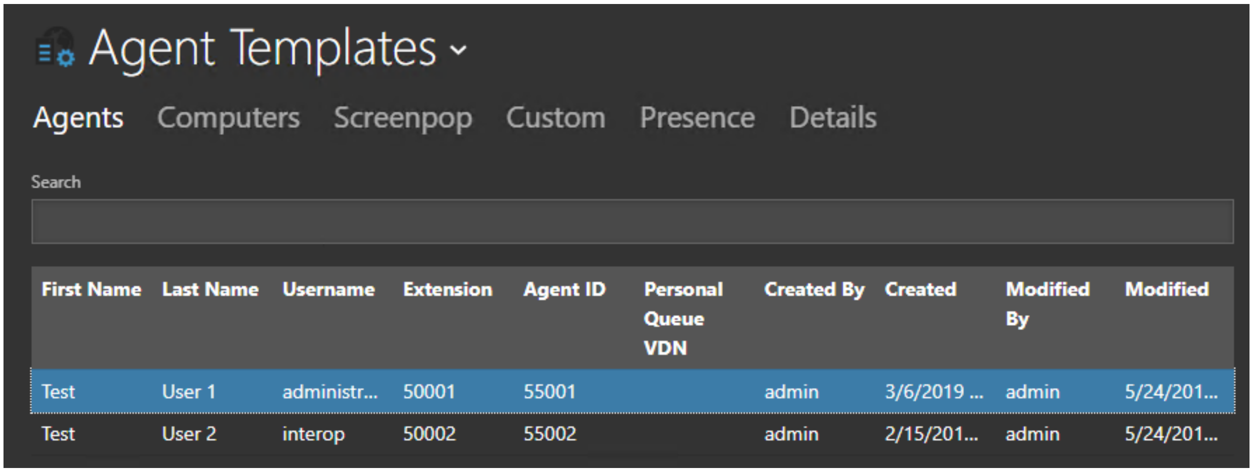


The **View Server Group** screen is displayed again. Select the newly created Email server, as shown below.

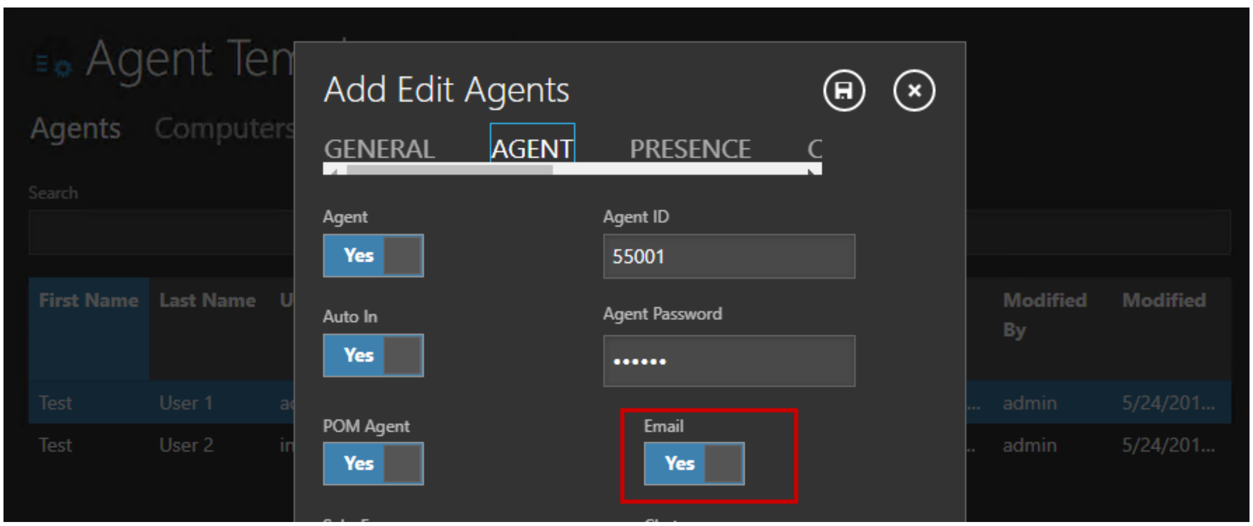


7.9. Administer Agents

Navigate to **Home → Agent Templates.**

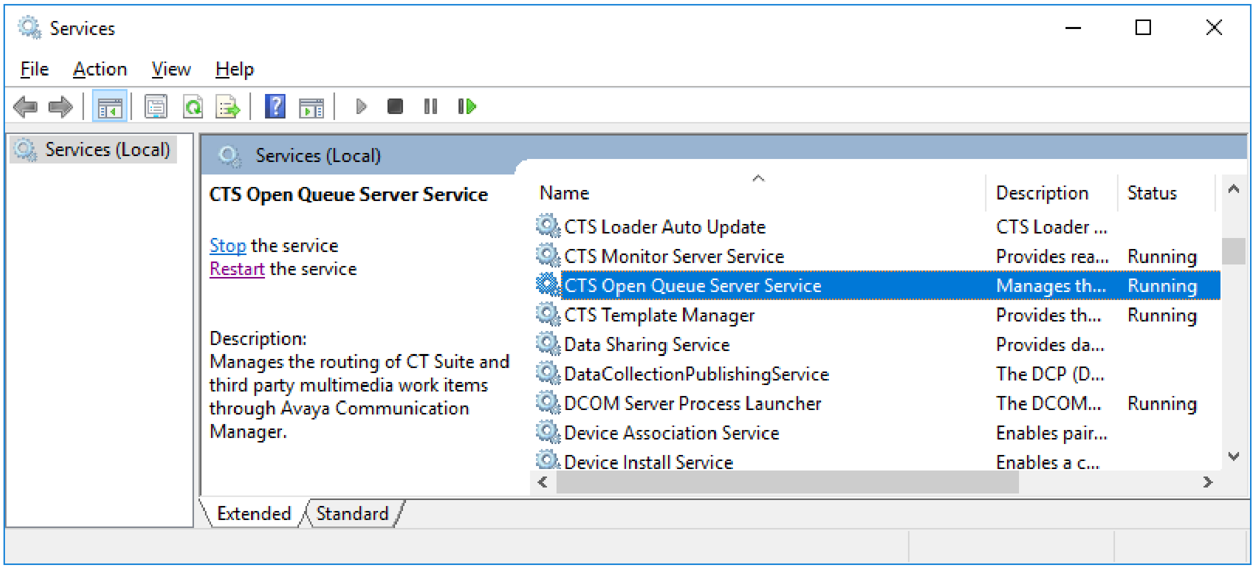


Select an agent that needs to be assigned to the Email profile. Select the **Agent** tab and enable **Email.**



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

                             TRUNK GROUP STATUS

Member    Port    Service State      Mtce Connected Ports
                                     Busy

0001/0001 T00001  in-service/idle    no
0001/0002 T00002  in-service/idle    no
0001/0003 T00003  in-service/idle    no
0001/0004 T00004  in-service/idle    no
0001/0005 T00005  in-service/idle    no
0001/0006 T00006  in-service/idle    no
0001/0007 T00007  in-service/idle    no
0001/0008 T00008  in-service/idle    no
0001/0009 T00009  in-service/idle    no
0001/0010 T00010  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.

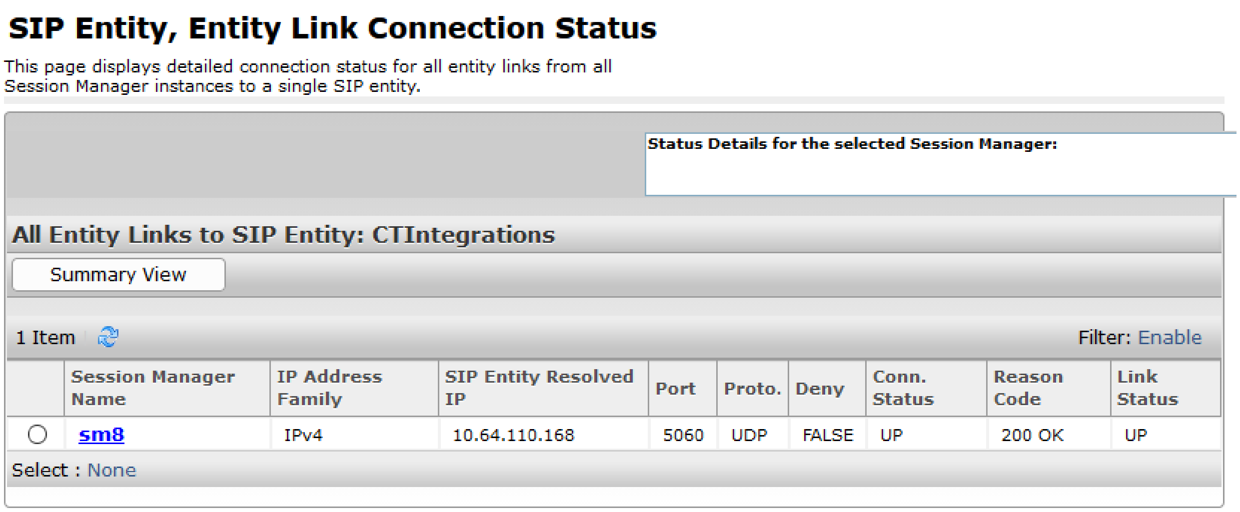
```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      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 **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

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

Status Details for the selected Session Manager:

All Entity Links to SIP Entity: CTIntegrations

Summary View

1 Item Filter: Enable

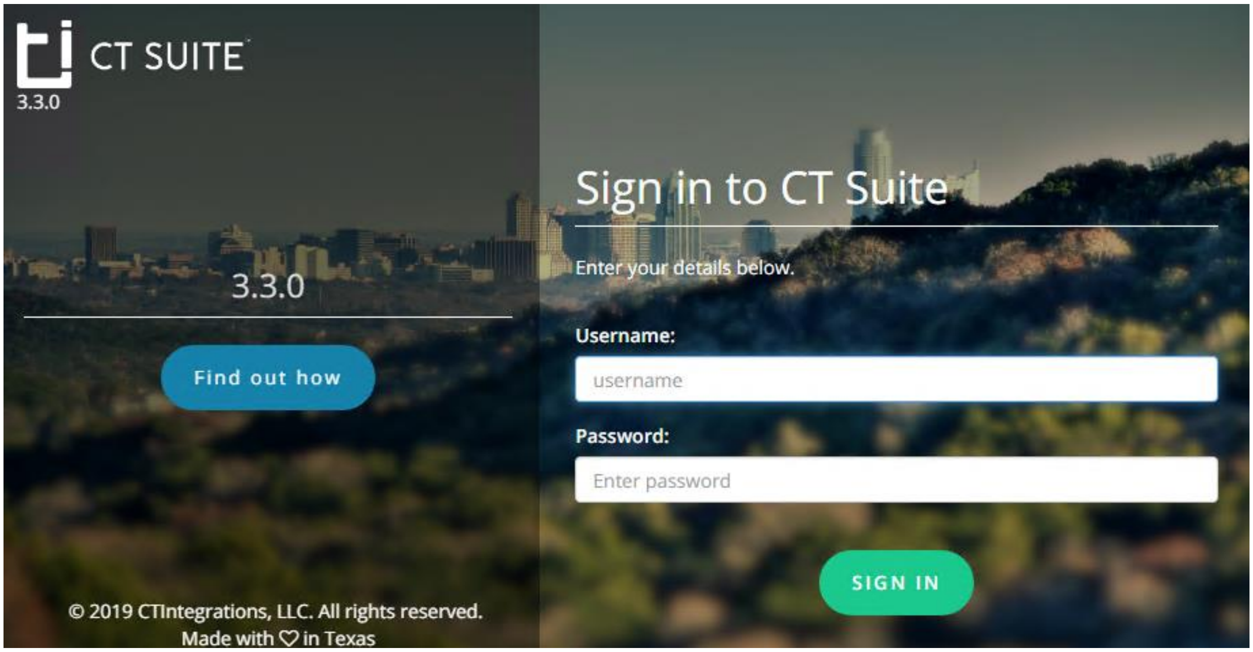
	Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	sm8	IPv4	10.64.110.168	5060	UDP	FALSE	UP	200 OK	UP

Select : None

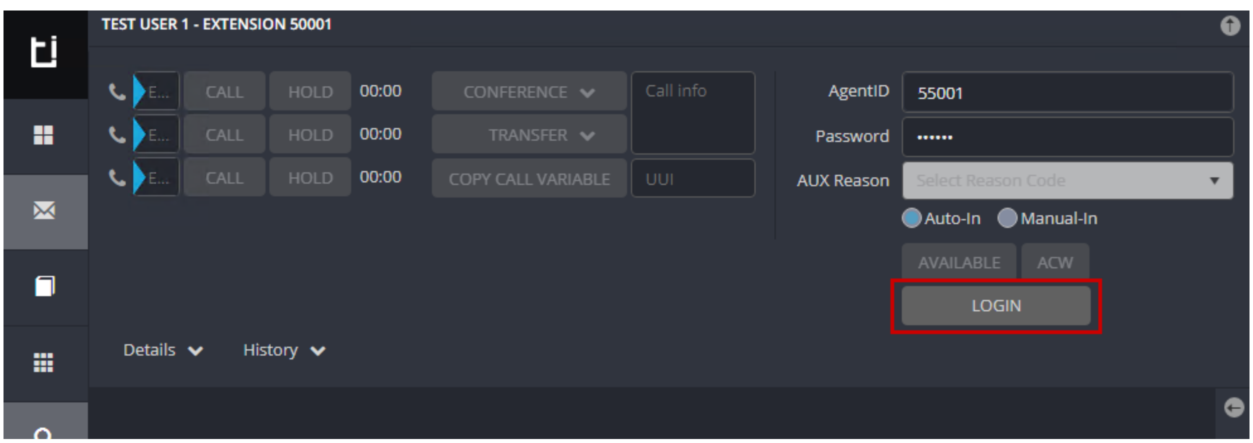
8.3. Verify CTIntegrations CT Suite

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.

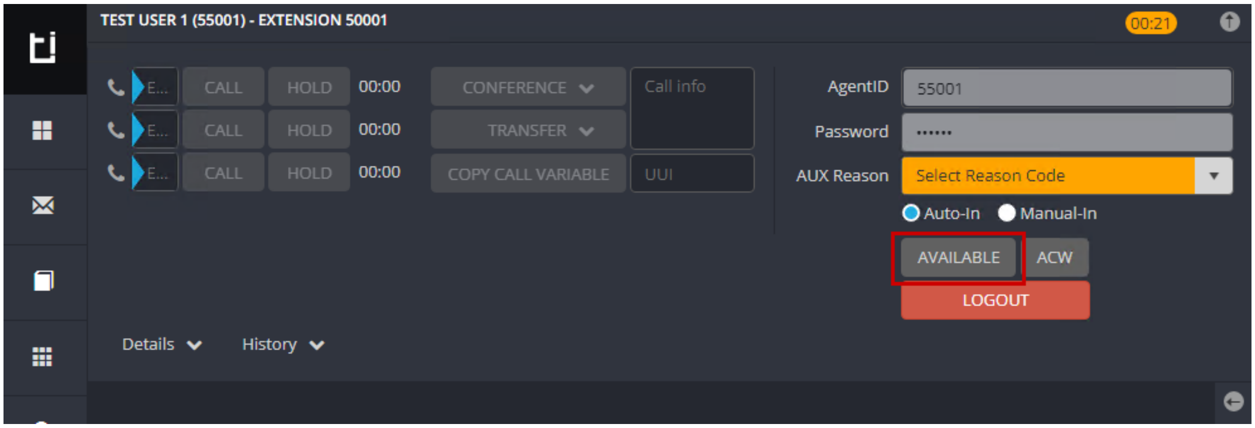
The **Sign in to CT Suite** screen is displayed. For **Username** and **Password**, enter an applicable agent credentials, and retain the default value in the remaining field.



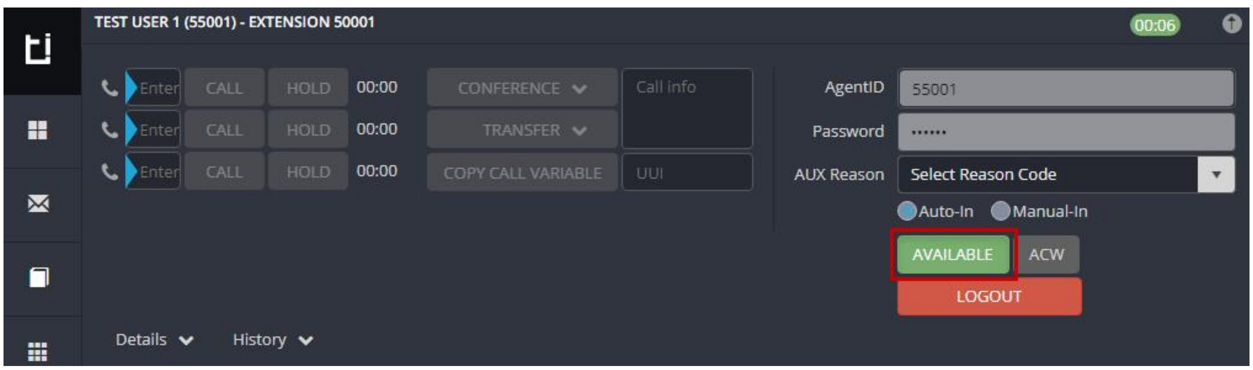
The agent screen below is displayed next. Retain the default values, and select **LOGIN** to log the agent into the ACD on Communication Manager.



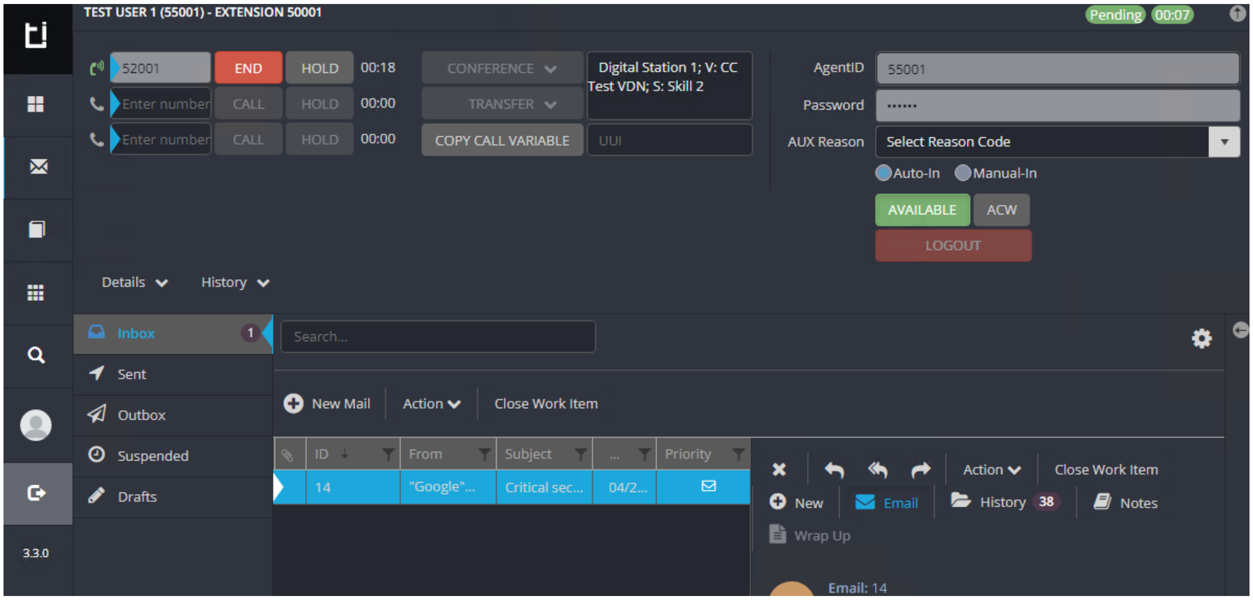
The agent screen is updated, as shown below. Click **AVAILABLE**.



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.

1. *Administering Avaya Aura® Communication Manager*, Release 8.0.x, Issue 4, May 2019.

2. *Administering and Maintaining Aura® Application Enablement Services*, Release 8.0.1, Issue 2, December 2018.

3. *Administering Avaya Aura® Session Manager*, Release 8.0.1, Issue 3, December 2018.

4. *Administering Avaya Aura® System Manager for Release 8.0.1*, Release 8.0.x, Issue 9, May 2019.

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

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.