Installing and Configuring Avaya CRM Connector 2.1 for Call Center Elite and POM

Release 2.1.0.0
Issue 1
May 2018

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original Published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

HostedService

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/ LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES

THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO

BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER,

THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION,

AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Support Tools:

"AVAYA SUPPORT TOOLS"MEAN THOSE SUPPORT TOOLS PROVIDED TO PARTNERS OR CUSTOMERS IN CONNECTION WITH MAINTENANCE SUPPORT OF AVAYA EQUYIPMENT (E.G., SAL, SLA MON, AVAYA DIAGNOISTIC SERVER, ETC.) AVAYA SUPPORT TOOLS ARE INTENDED TO BE USED FOR LAWFUL DIAGNOSTIC AND NETWORK INTEGRITY PURPOSES ONLY. The customer is responsible for understanding and complying with applicable legal requirements with regard to its network. The Tools may contain diagnostic capabilities that allow Avaya, authorized Avaya partners, and authorized customer administrators to capture packets, run diagnostics, capture key strokes and information from endpoints including contact lists, and remotely control and monitor end-user devices. The customer is responsible for enabling these diagnostic capabilities, for ensuring users are aware of activities or potential activities and for compliance with any legal requirements with respect to use of the Tools and diagnostic capabilities on its network, including, without limitation, compliance with laws regarding notifications regarding capture of personal data and call recording.

Licenses

THE SOFTWARE LICENSE TERMS OR SUPPORT TOOLS LICENSE TERMS AVAILABLE ON THE AVAYAWEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO

OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE

AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software and Support Tools, for which the scope of the license is detailed below Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation

or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products", or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage

Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Support Tools: Avaya Support Tools are provided as an entitlement of Avaya Support Coverage (e.g., maintenance) and the entitlements are established by Avaya. The scope of the license for each Tool is described in its License terms and/or the applicable service description document.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may

not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Table of Contents

Chapter 1: Introduction

About this guide

This document is intended for users who want to install and configure Avaya CRM Connector 2.1.

Business usage scenario

Avaya CRM Connectors 2.1 benefits Avaya customers who wish to use a CRM application together with one or more Avaya platforms, such as CC-Elite and POM via AES.

The current proposed use case support both inbound and outbound Avaya contact center for voice-only communication.

Solution overview

Avaya CRM Connector 2.1 is a new modular software that allows Avaya to quickly integrate voice-only contact center features into Customer Relationship Management (CRM) applications and at the same time provide a highly scalable and robust solution to Avaya contact center customers. A key part of Avaya CRM Connector 2.1 is its modular architecture built as containerized micro-services running on Docker, composed by a common core and adapters to connect to different Avaya platforms and different CRM applications.

Chapter 2: Avaya CRM Connector 2.1 Prerequisites

Important:

It is recommended that you use a thin client to deploy the Avaya CRM Connector 2.1 application.

Pre-deployment checklist

Accesses and Permissions

No.	Accesses	Permissions to:	Notes	✔
1	Avaya Aura® Communication Manager	a. Trace b. Verify configuration	(MST) Trace in case troubleshooting is needed.	
2	SSH access to Avaya CRM Connector™ servers	Check logs		
3	SSH and Web Admin access to Avaya Enablement Services	a. Trace b. Verify configuration	(AES) Trace in case troubleshooting is needed.	
4	Salesforce.com	a. Install Managed Packages b. Create custom fields c. Import and configure Call Center Definitions		

Required External platform configuration

No.	Configuration required	Notes	✔
1	AES connected to CM and CTI link properly established. Ensure DMCC encrypted link is configured and available.		
2	CTI user created on the AES according to the documentation		
3	Test elements on Communication Manager, which includes: a. Skill, Agent, Station, VDN, and Vector to route to the test skill b. PSTN number to dial in the test skill		
4	Salesforce.com test account		

Data gathering

No.	Data required	Notes	✔
1	AES IP address and/or FQDN		
2	CTI user and password		
3	CM IP address and/or FQDN		
4	Salesforce test user account credentials		

Note:

A Salesforce Administrator resource provided by Avaya's Customer is required to perform and support Salesforce deployment and configuration related tasks.

System requirements

- **Avaya CRM Connector™ Release 2.1 Cluster Profile**

  Note

  Avaya CRM Connector™ requires a licensed VMware instance (standard edition or better) and the following versions of the VMware hypervisor and products:

  - ESXi 6.0 or above

  Each Avaya CRM Connector™ node in a cluster is a single vAppliance package with the following characteristics:

  - Operating system: RHEL 7.4 64–bit
  - CPU Core(s): Four floating cores CPU reservation 9480MHz = 4x2370MHz
  - Memory reservation: Minimum 8.0 GB.
  - Storage reservation: Minimum 50 GB
  - Shared NIC(s) Two at 1000 Mbps, used for management interface and security module/public access.

  Note

  All the Avaya CRM Connector™ servers in a cluster must have the same memory reservation. Resource requirements may increase depending on the number of agent using Avaya CRM Connector™ 2.1

Avaya platform requirements

- Avaya Aura ® Communication Manager Releases 6.3, 7.0.1 and 7.1
- Avaya Application Enablement Services (AES) Releases 6.3.3, 7.0.1 and 7.1
  - DMCC Service is installed and configured.
- Avaya Proactive Outreach Manager 3.0.4, 3.0.5, 3.1 (For Outbound support only)
  - POM Agent Manager is installed and configured.

Software requirements

CRMs supported:

CRM	Version	Presentation Modes
Salesforce.com	Latest	Lightning Experience, Classic Console, and Classic Standard

Browsers supported:

- Internet Explorer version 11
- Chrome version 52 and later
- Firefox version 48 and later
- Microsoft Edge version 38 and later

Note

- Only HTML 5 compliant browsers are supported.
- The maximum number of concurrent softphone tabs supported for Salesforce Classic mode is 5.
- Salesforce does not support Internet Explorer 11 when using Lightning Experience mode.

Network port requirements

- Network ports are configurable and can be changed in yml files for each component during the installation.

Avaya CRM Connector Solution port usage

Application	Source	Destination Port	Purpose
Avaya CRM Connector Service	HTTP Client / Browser	8484	HTTPS
Interaction Endpoint Controller Service	HTTP Client / Browser	8483	HTTPS
Outreach Endpoint Controller Service	HTTP Client / Browser	8485	HTTPS
Avaya Web LM	Avaya CRM Connector	52233	WebLM
Avaya Application Enablement Services	Avaya CRM Connector	4722	Secure DMCC Port

Endpoint compatibility

Hardphones

- Recommended type: 96XX
- Supported types: Hardphone models with support for third party call control over AES. This includes SIP, H323 and DCP models.

Softphones

- Recommended type: Avaya Agent for Desktop 1.5 and 1.6
- Supported types: Avaya one-X® Agent 2.5.8 for Windows

Important:

Avaya one-X® Agent is supported, but with limitations. The limitations are as follows:

- The agent state may display incorrectly in Avaya one-X® Agent.
- The agent state reason codes may display incorrectly in Avaya one-X® Agent.

Certificate requirements

- External Certificates
  - Root CA for AE Services CA Trusted certificate
  - Root CA for WebLM
- Hosting Server Certificates
  - Certificate for Server to deliver secure content over HTTPS

    To know more about Server certificate deployment, see *Deploying the Server Certificate*.

License requirements

The licenses are managed by WebLM where the WebLM URL is now configured in the `application.yml` file.

- Application Licenses:
  - License file to be deployed on Avaya Web LM

    Note

    Contact your Avaya sales representative for more information.
- Avaya Platform Licenses
  - CM station port licenses (1 per logged agent)
  - CM agent licenses (1 per agent created on CM).

    Note

    These are the same standard licenses needed to implement a contact center.

List of features

Used By	Feature/Counter Keyword name	Feature Keyword Description	Use Description
AES3PCC-Driver	FEAT_AESO_CALLCENTER	CRM Connector Contact Center	• Checked on application startup
IEC	VALUE_AESO_OPEN_USERS	CRM Connector Inbound Users	• Acquired on Station Registration Request • Released on Station Logout Request
OEC	VALUE_AESO_OUTBOUND_VOICE	CRM Connector Outbound Voice User	• Acquired on Agent Outreach Login Request • Released on Agent Outreach Logout Request

Environment configuration

Communication Manager Configurations

UCID

On Communication Manager, UCID must be generated and sent over ASAI.

Ensure that the following two settings are configured on Communication Manager:

Procedure

1. system-parameters features on page 5:

   UNIVERSAL CALL ID

   Create Universal Call ID (UCID) UCID Y

   UCID Network Node ID: X **(*where x is unique within the network)**

2. Send UCID system-parameters features on page 13:

   Send UCID to ASAI? Y

3. Pass UCID over the trunks (trunk-group x, on page 3)

   UUI Treatment: shared

   Send UCID? y

ASAI

Enable **ASAI Proprietary Features** on the Communication Manager to allow CSC to receive agent events in system-parameters customer-options on page 9. There are licensing aspects for the proprietary features. For more details, see *Avaya Aura™ Communication Manager Feature Entitlements and Settings* guide - https://downloads.avaya.com/css/P8/documents/100093456.

IMS

Communication Manager must not be configured as a Feature Server. On page 1 of the relevant signaling group, ensure that IMS enabled is set to **N**.

```
display signaling-group 13                                    Page   1 of   3
                              SIGNALING GROUP

 Group Number: 13              Group Type: sip
  IMS Enabled? n         Transport Method: tcp
        Q-SIP? n
     IP Video? y          Priority Video? y       Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 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: sm48dot13
 Near-end Listen Port: 5060               Far-end Listen Port: 5060
                                        Far-end Network Region: 1

Far-end Domain: sipccgal.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): 3                    IP Audio Hairpinning? n
        Enable Layer 3 Test? y                 Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n         Alternate Route Timer(sec): 6
```

Figure 1: Disable IMS feature

3PCC Enabled

If SIP stations are being used, ensure that on page 6 of the stations administration page, 3PCC Enabled is set to **Avaya**.

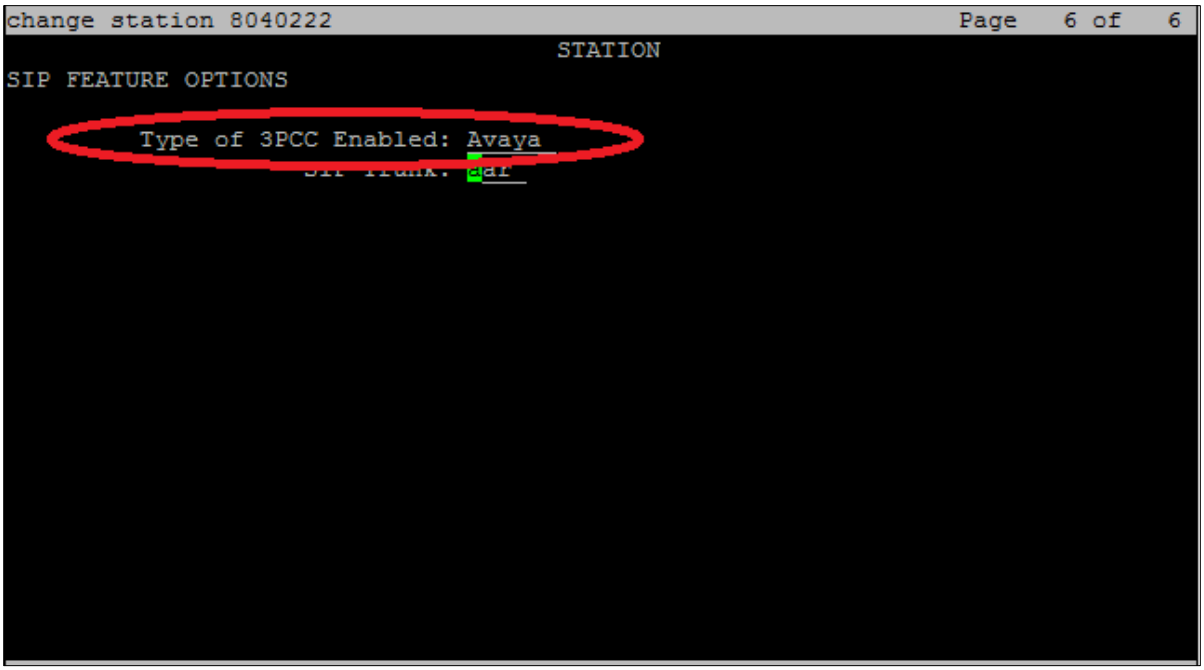

Figure 2: 3PCC settings

Reason Codes

Enabling the reason codes

Procedure

To use client requested reason codes, you must enable the following:

1. Set system-parameters customer-options on page six of 11 Reason Codes set to **Y.**

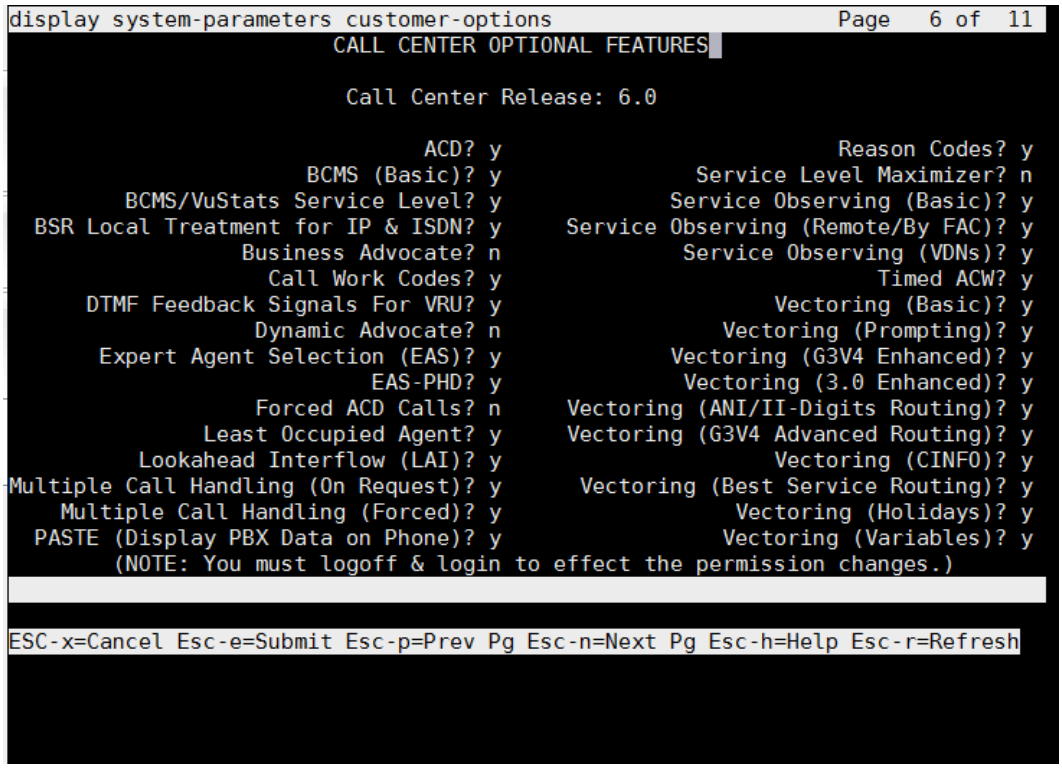

Figure 3: Call Center Optional Features settings

2. Set the system-parameters features page 14 of 20 Reason Codes.

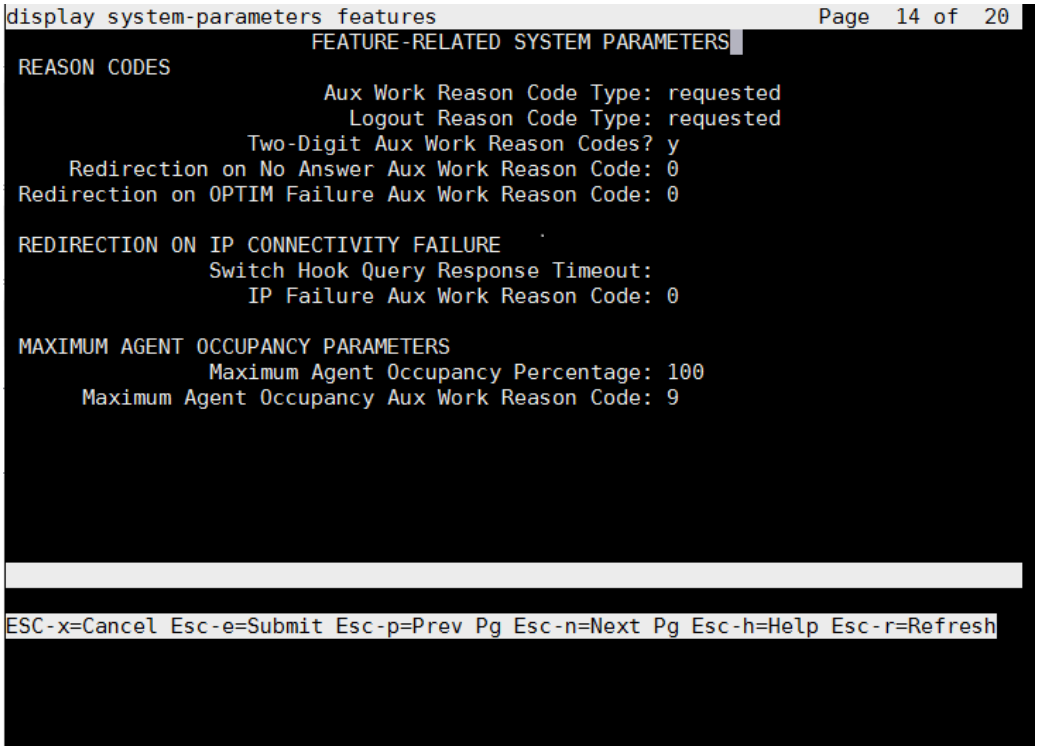

Figure 4: Feature related system parameters settings

Enabling the two-digit reason codes

Procedure

1. To enable the two-digit reason codes in the CM System-parameters features, set **Two-Digit Aux Work Reason Codes** to **y.**

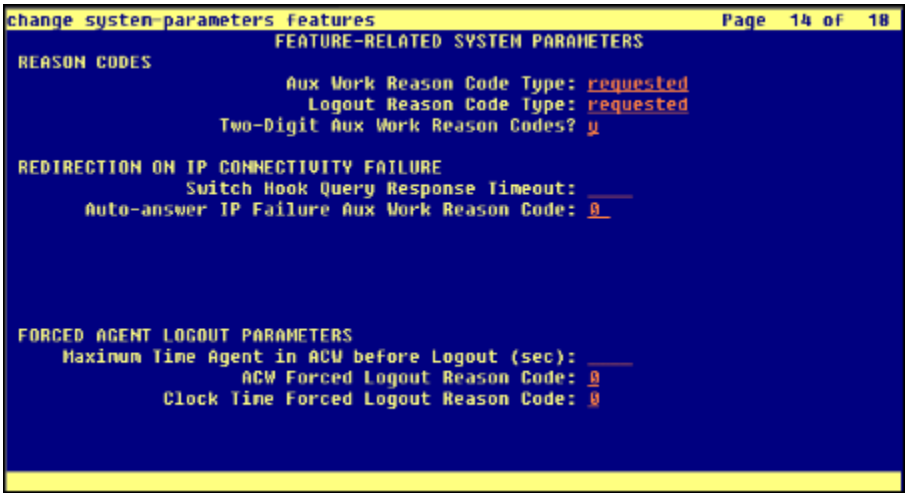

Figure 5: Two-Digit Aux Work Reason Codes

2. Also, the **CTI LINK** must be changed to allow the two-digit reason codes to work with the **CTI LINK**. It is accessed by running change cti <link number>, where <link number> is the CTI LINK number. For details, see the next section.

CTI-Link

The CTI Link to AES must be of type ADJ-IP.

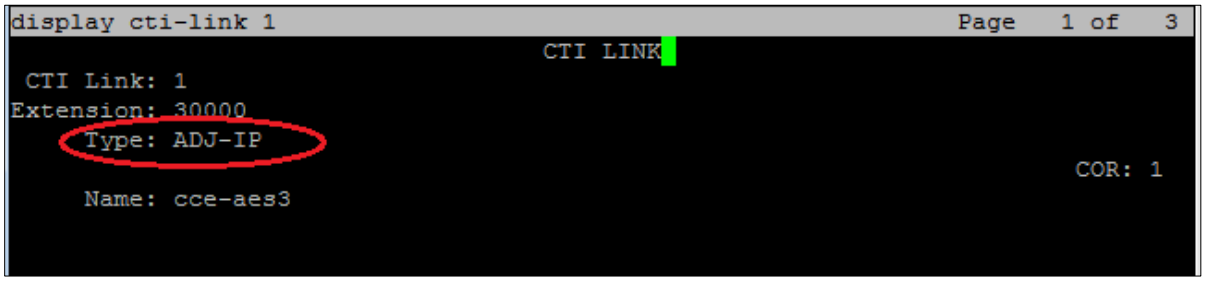

Figure 6: CTI Link settings

On the second page of the CTI LINK, there are two additional settings that must be set.

1. Two-digit reason codes must be enabled if they are enabled in the system. If the CTI LINK settings do not allow you to enable this setting, leave it at **N**.

   Note

   Before setting the Two-digit reason codes to **Y** in CTI Link, you must enable the Two-digit reason codes in Communication Manager. Also, if two-digit reason codes are not set to Y in CTI Link, you cannot use them in Avaya CRM Connectors.

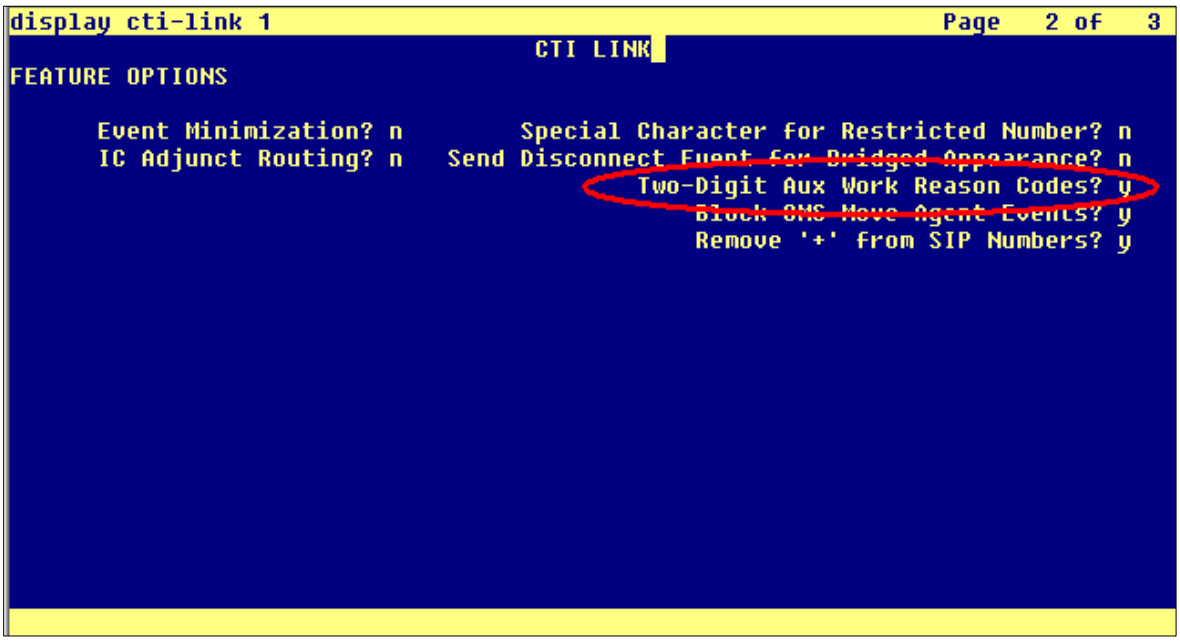

Figure 7: Two-digit Reason codes settings

2. The **Block CMS Move Agent Events** option must be enabled.

   Note

   This must always be set to **Y** to ensure that any logout/login events generated by CMS agent moves are completely ignored. Without this, agents will be completely logged out every time they have a skill change performed while they are logged in.

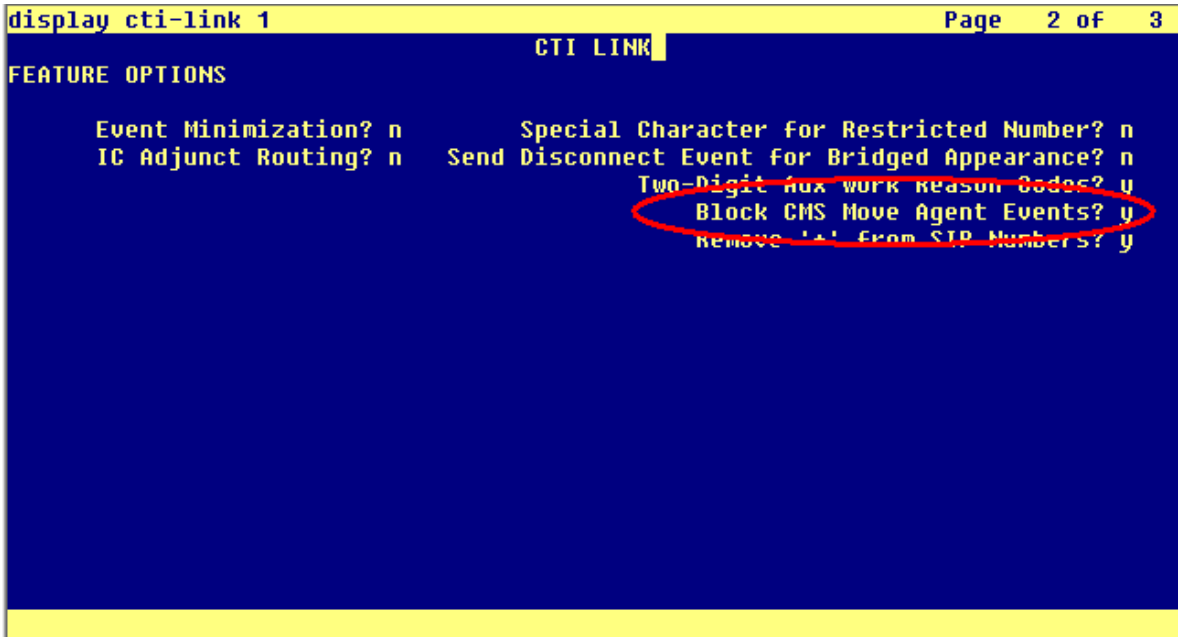

Figure 8: Block CMS Move Agent Events settings

3. Once the setting in the CTI LINK is enabled, you must restart AE Services on AES to start using two-digit reason codes with CTI.

Important

Restarting AE Services will affect the AES active services as all links currently connected to AES will be lost.

AES - TSAPI Link Configuration

Configuring the Security Settings

About this task

The link between AES and Communication Manager must be configured as a secure link.

Procedure

1. Navigate to **AE Services** > **TSAPI** > **TSAPI Links**.
2. Select the link that you want to change and click **Edit Link.**
3. Change the **Security** field value to **Both.**
4. Click **Apply Changes.**

Configuring the ASAI Link Version

Procedure

1. Navigate to **AE Services** > **TSAPI** > **TSAPI Links**.

2. Select the link that you want to change and click **Edit Link.**
3. Change the **ASAI Link Version** field to the latest version available, preferably 7.
4. Click **Apply Changes.**

Configuring the Switch Connection

Procedure

1. Navigate to **AE Services** > **TSAPI** > **TSAPI Links**.
2. If you are creating a new TSAPI link for Communication Manage then add a name in the **Switch Connection** field, if you are using an existing TSAPI link then just note the name used here.
3. The name entered in the **Switch Connection** field is used in the administration of the AES3PCC Service.

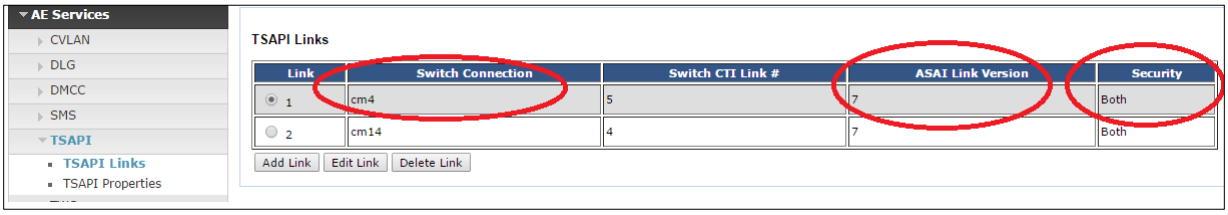

Figure 9 The Switch Connection field settings

Configuring the Ports

About this task

Some debug tools, such as DMCC Dashboard may connect to AES using an unencrypted port. If the tool is connecting through an unencrypted port, you need to enable the unencrypted port to the following settings.

Procedure

1. Navigate to **AES** > **Networking** > **Ports**.
2. Enable the **Unencrypted port** for DMCC.
   The default port value is 4721.
3. Click **Apply Changes**.

Configuring the TCP/TLS settings

Procedure

1. Navigate to **AES** > **Networking** > **TCP/TLS Settings**.
2. Ensure that the TLSv1.2 protocol option is enabled as that is the only protocol supported for secured AES connection.

Adding a new user in AES

Procedure

1. Navigate to **AES** > **User Management > User Admin > Add User.**

   The system displays the **Add User** page.
2. In the **User Id** field, type the user name, such as **crmuser1**.
3. Provide the username in the other two required name fields.
4. Enter the password twice in the remaining two required fields.
5. In the **CT User** field, click the drop-down and select **Yes**.
6. Leave the other fields blank.
7. Click **Apply**.

Configuring the Security Database

Before you Begin

Ensure that you already have a user id with the desired name (such as **crmuser1**).

Procedure

1. Navigate to **AES**>**Security > Security Database > Control**.
2. Select the **Enable SDB for DMCC Service** check box.
3. Navigate to **Security > Security Database > CTI Users > List All Users**.

   The system displays the list of all CTI users.
4. Select the created name (for example **crmuser1**) from the list, and click **Edit**.
5. Select the **Unrestricted Access** check box.
6. Click **Apply Changes**.

Important

After making the required changes in the configurations, restart DMCC and TSAPI services.

Configuring the AES Reserved License settings

About this task

If AES is using WebLM and the WebLM sever becomes unreachable, then this can cause delays within AES processing since AES attempts to check the real-time license status. The solution is to reserve a number of AES licenses to avoid the real-time check.

Procedure

1. Navigate to **AES > Licensing > Reserved Licenses**.
2. Modify the **Reserved Licenses** values.

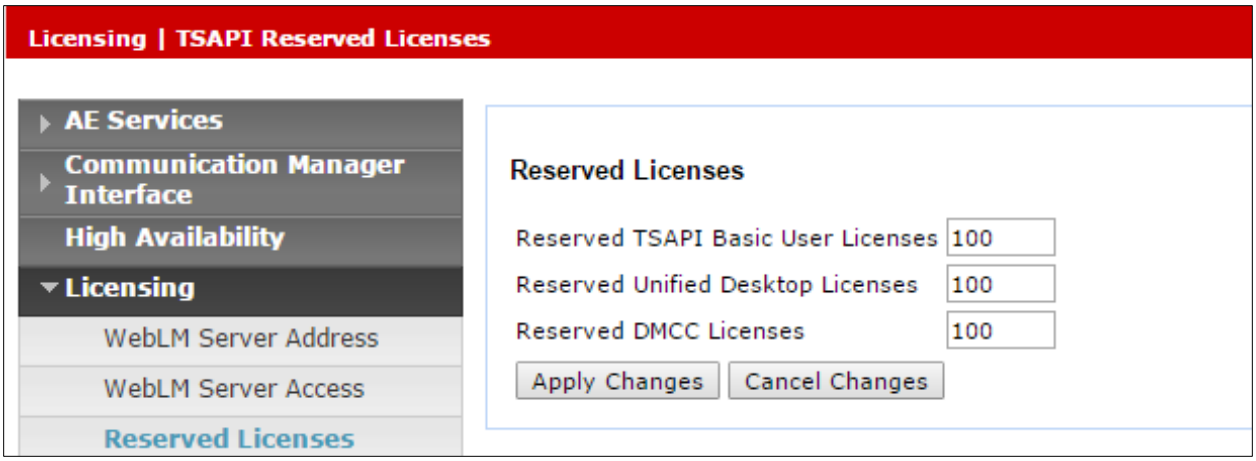

Figure 10: Reserved Licenses settings

3. Click **Apply Changes**.

AES configuration for POM CC Elite

CC Elite Connector Configuration

SMS Web Service

The connector calls Avaya AES SMS web service to read the static agent configurations from Avaya Communication Manager by sending SOAP requests to AES SMS web service: SystemManagementService.php

AES SMS web service is a web-oriented way of configuring and administering Communication Manager. It closely resembles with SAT user interface of CM. This web service runs on AES server that in turn talks with CM.

You must configure the following setting for SMS Web service:

- Enable the Standard Reserved Ports as shown in the following screenshot:

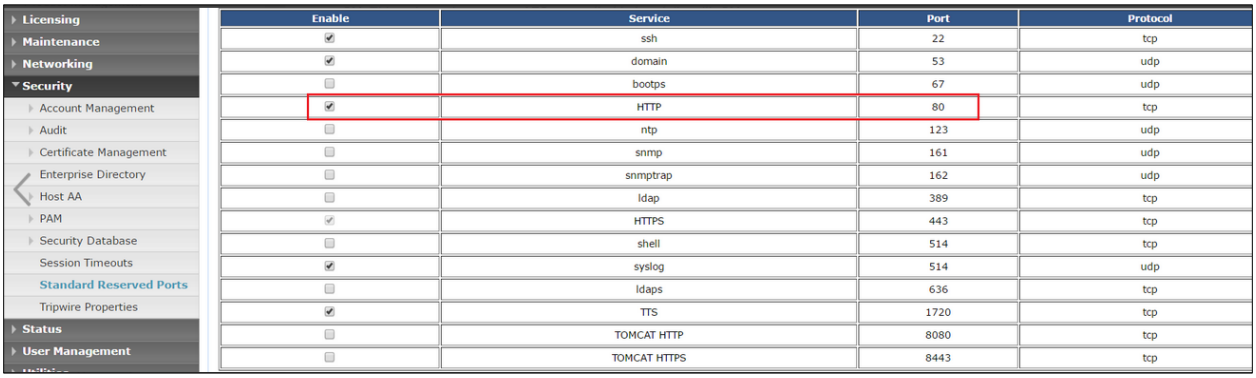

Figure 11: Enable Standard Reserved Ports

- Configure the AES SMS properties as shown in the following screenshot:

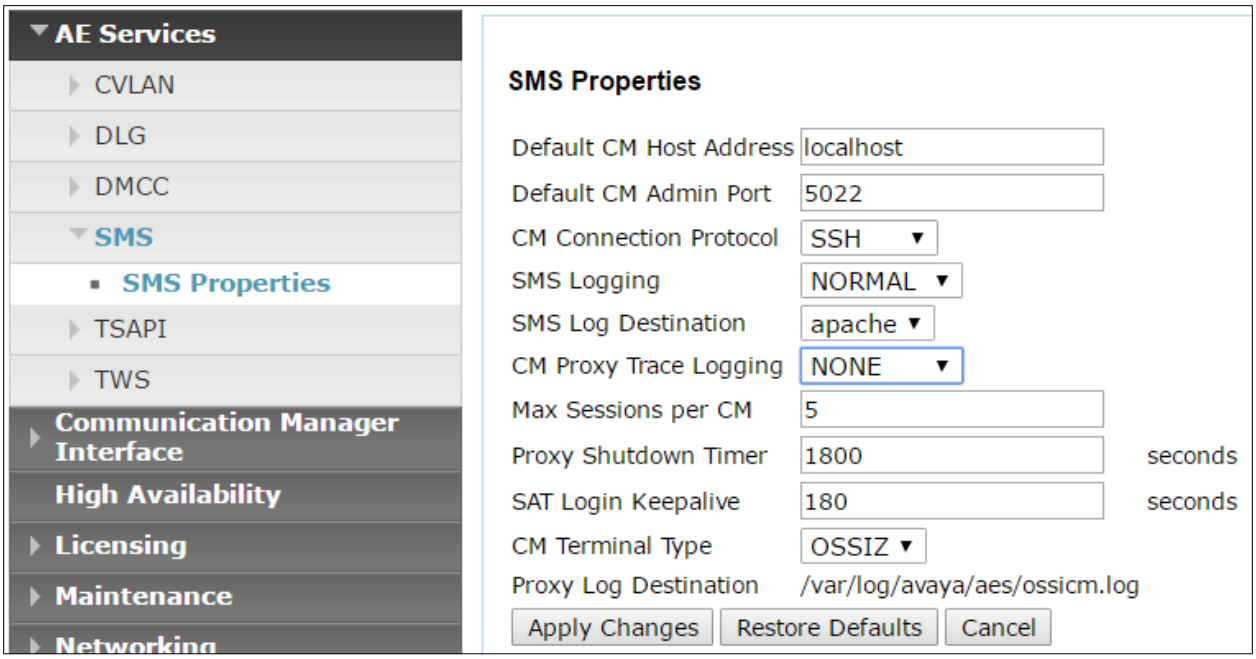

Figure 12: SMS Properties

SMS Testing

To test the SMS web service, AES web service test client must be used.

Users must navigate to the web page: **`http://<AES-IP>/sms/sms_test.php`** and test for the agent related information like extension skills, etc.

CCEliteConnector can get various agent related information.

There are two methods **`SubmitRequest`** and **`ReleaseRequest`** to submit SOAP request and release the SOAP session respectively. The static information about agent used by AgentManager is:

- Getting the name and the password of an agent to show and authenticate on SDK.
- Getting the skills of an agent.
- Getting the ACD Address of a skill,

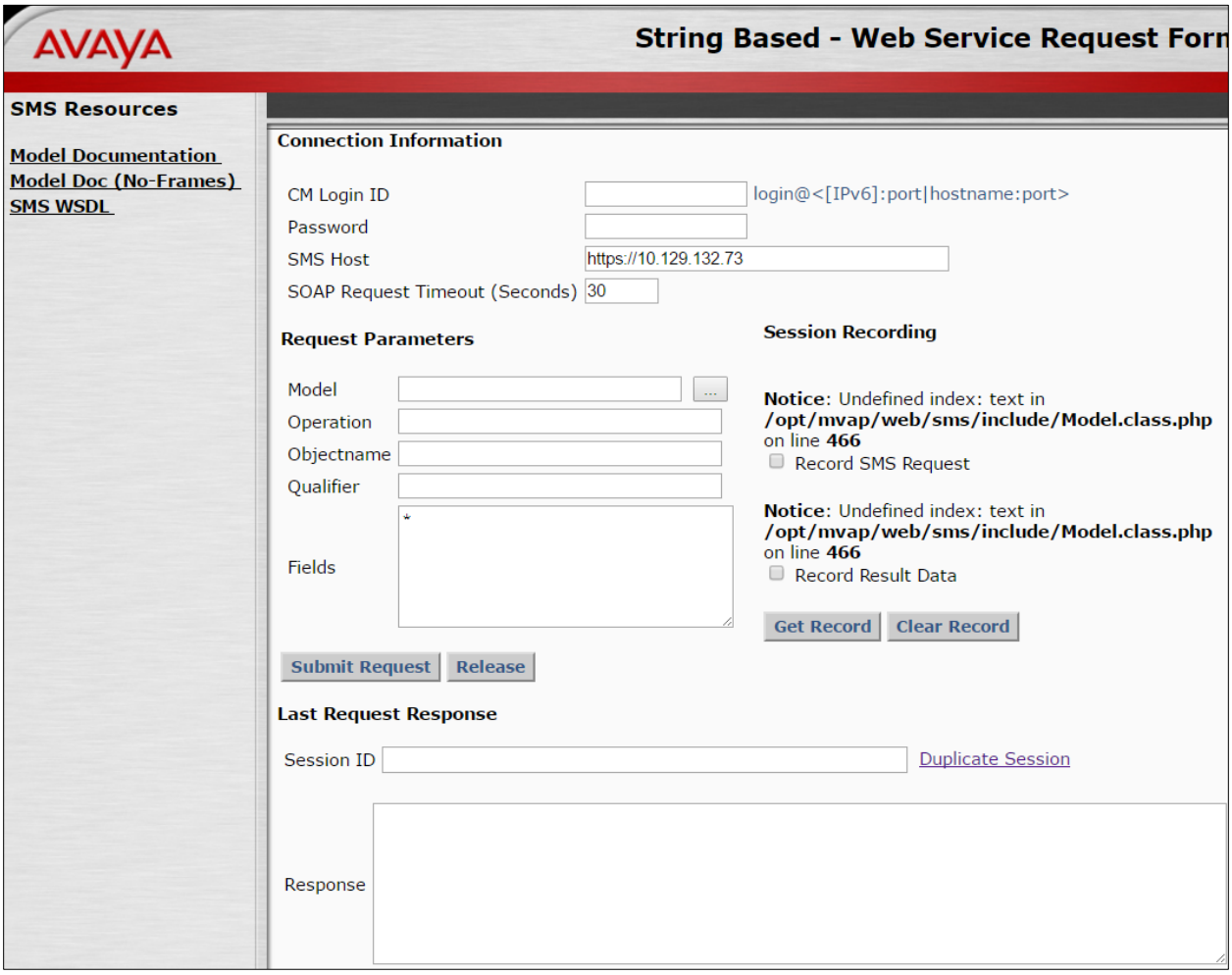

Figure 13: AES SMS Web Service page

Response code

```
Response {

  var $result_code = 0

  var $result_data = 'Login_ID=81-155-1|Name=Haich
Agent1|Direct_Agent_Skill=|AAS=n|AUDIX=n|COR=1|Call_Handling_Preferenc
e=greatest-
need|Service_Objective=n|TN=1|Coverage_Path=|Security_Code=|Check_skil
l_TNs_to_match_agent_TN=n|LWC_Reception=spe|LWC_Log_External_Calls=n|A
UDIX_Name_for_Messaging=|Login_ID_For_ISDN_Display=n|Auto_Answer=stati
on|MIA_Across_Skills=system|ACW_Agent_Considered_Idle=system|Aux_Work_
Reason_Code_Type=system|Logout_Reason_Code_Type=system|Maximum_Time_In
_ACW_Before_Logout=system|Local_Call_Preference=n|Password=123456|Pass
word_Confirmation=123456|Forced_Agent_Logout_Time_Hr=|Forced_Agent_Log
out_Time_Min=|Native_Name_1=|Native_Name_2=|Native_Name_3=|Native_Name
_4=|Native_Name_5=|Native_Name_Scripts=00000000|SN[1]=155|SN[2]=1155|S
N[3]=700|SN[4]=701|SL[1]=16|SL[2]=16|SL[3]=1|SL[4]=1'
```

```
  var $message_text = ''
}
```

Note:

A CTI link is not needed for SMS.

You must also change the `saw.ini` file:

If the password of agent login is correct and still you are getting the error, please do the below change on AES if you are not using init user (CM user) at CCElite configuration page:

The "`ProxyOptions`" parameter needs to be changed from the default value of **`"-n"`** to **`"-n -z"`** in the "**`/opt/mvap/web/sms/saw.ini`**" file on the AES Server.

Environment prerequisites

System Clocks

The systems clocks on the servers and clients must be properly set. This is required to store call logs with correct date and time.

Chapter 3: Installation and configuration

Important:

It is recommended that you use a thin client to deploy the Avaya CRM Connector 2.1 application.

Product Artifacts

The following artifacts must be available in order to be able to continue the installation process.

Name	Type	Description
Avaya CRM Connector 2.1	ova	Avaya Connector VM Image containing all the services needed by the connector.
SFDC CCD	xml	Salesforce Call Center definition files to contain the configuration options for the Salesforce UI.

Deploying VMWare OVA

About this task

The following procedure must be performed using VSphere VCenter Client or VMware Host Client to deploy VMWare OVA.

Procedure

1. Download the OVA file from PLDS.
2. Import the OVA into VMWare.

   A virtual machine is created following the specs described in the Avaya Platform Requirements section
3. Access the newly created virtual machine console.
4. Log into the VMWare using username as **root** and password as **Avaya@123.**
5. Use the **Network Configuration Text User Interface** (**nmtui)** to set the IPs and FQDN designated for the new virtual machine.

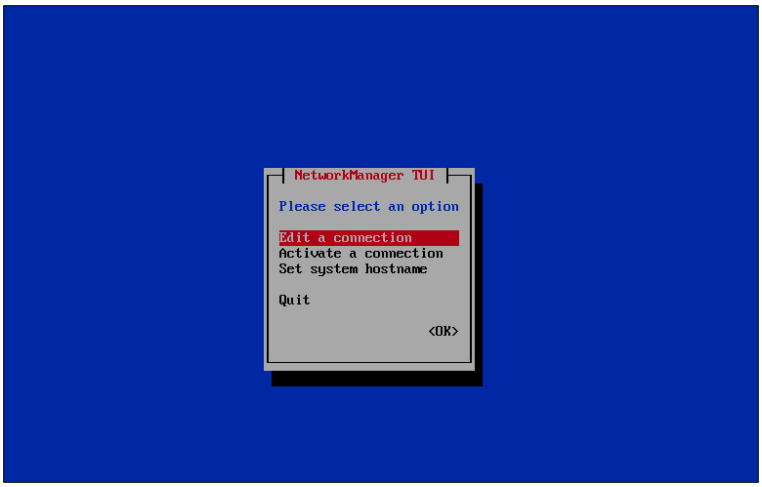

Figure 14: Network Manager

a. Select the configuration suited for the network from the given options: **Manual Static IP assignment** or **Automatic DHCP IP assignment**.

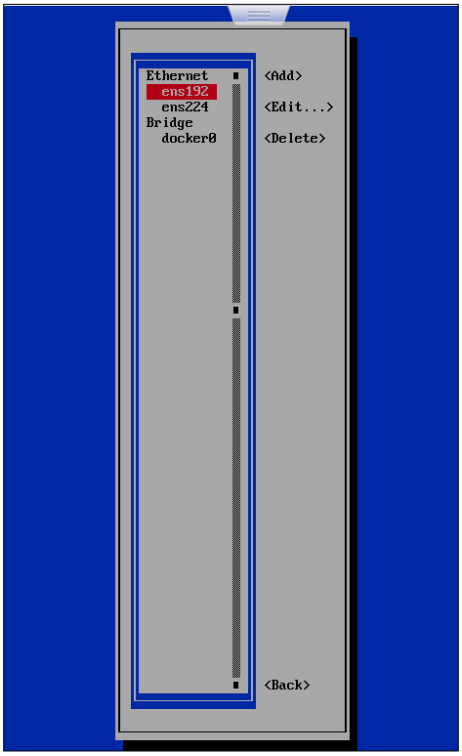

Figure 15: Ethernet selection

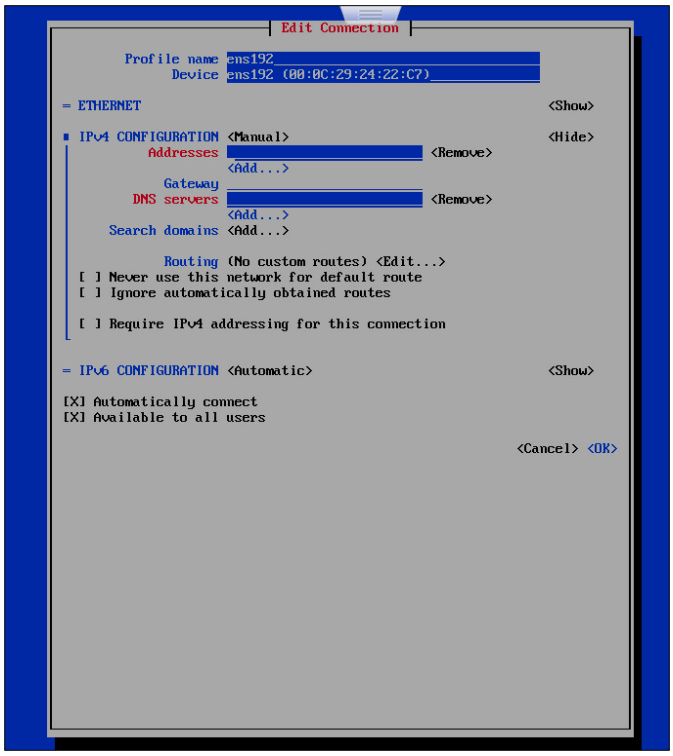

Figure 16: Edit Connection details

b. Set the host name with full qualified domain name (FQDN).

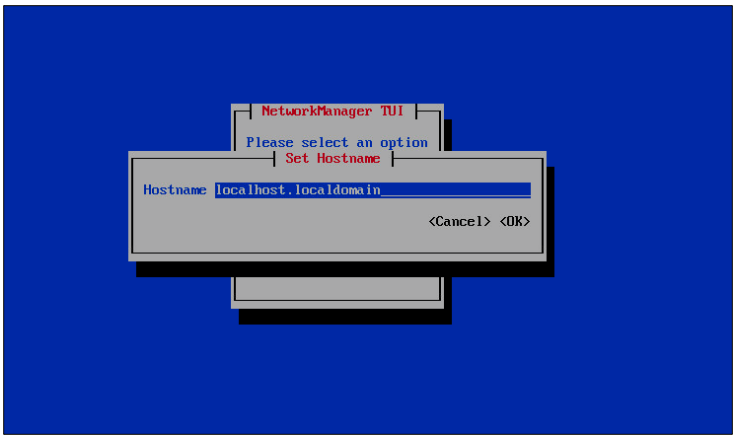

Figure 17: Set Hostname.

c. Activate the connections before exiting the window.

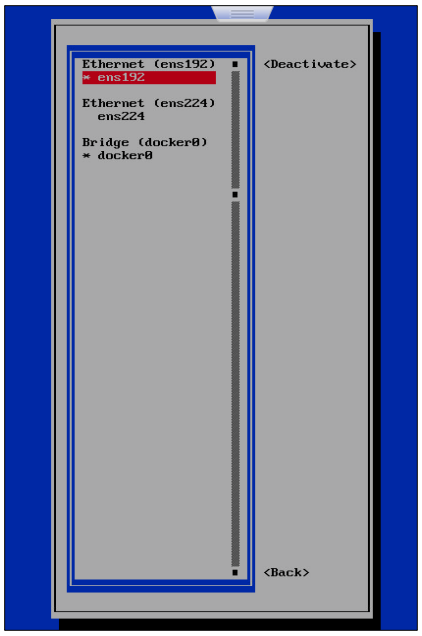

Figure 18: Activate connections

d. Click **OK** to exit.

Note:

1. ens192 is the primary NIC intended for public access.

2. ens224 is the secondary NIC intended for Out of Bound Management.

3. Based on the customer networking requirements, additional NICs can be added and configured.

6. Change or delete the password for root login using the following procedure:

   a. Run the following command to set a stronger password:

```
passwd root
```

   b. Run the following command to delete the password-based access for root:

```
passwd --delete root
```

Note:

a. Deleting the password will allow only EASG based access.

b. SSH access for **`root`** and **`sroot`** accounts is blocked.

c. SSH access will need to be performed with the craft user and later **`su - sroot`** will need to be performed to get the root access.

d. Both **`sroot`** and craft uses EASG to generate challenge responses.

e. **`root`** access is only possible when you are directly accessing the console.

f. SSH requires EASG.

Deploying the Server Certificate

The CRM Connector requires a server certificate for the Docker applications to be able to use HTTPS connections. You can install any of the following types of certificates in the server:

- Self-signed certificate
- Third-party or signed certificate from a request file
- Signed certificate with a private key

Whichever certificate chose will then be used by all the applications on the server.

Self-Signed Certificate

A self-signed certificate is created and signed by itself. Self-signed certificates do not contain a valid signature. As a result, whenever the client uses the CRM Connector, a security warning is displayed. Alternatively, to avoid the security warning, the certificate can be imported by each user's certificate store as a trusted root certificate. While acceptable during initial testing, this is not recommended for long term or production use. It is expected that any self-signed certificate used will be replaced with a signed certificate.

Creating a self-signed certificate and the associated files does not require root privileges. The self-signed certificate can be created using the default user.

Procedure

1. Create a new directory.
   For example, **/opt/avaya/certs**

1. Run the following command to navigate to the newly created directory:

   cd /opt/avaya/certs

2. Create a file called **openssl.cnf** with the following content:

```
[ req ]
default_bits = 2048
distinguished_name = dn
prompt = no
default_md = sha256
x509_extensions = v3_req
req_extensions = v3_req
extensions = v3_req
copy_extensions = copy

[ dn ]
countryName = US
stateOrProvinceName = California
localityName = Santa Clara
organizationName = Avaya
commonName = server.domain.com
```

```
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = server.domain.com
DNS.2 = loadbalancer.domain.com
```

3. Please make sure you change the bold selected text to what you need. The commonName is used to be able to identify the certificate when loaded into a client's certificate store. Without this, it can be hard to identify. The subjectAltName DNS value, must be set to the server's FQDN.

   Note

   The SAN (subjectAltName) is very important. It must match across the server, the corporate DNS, and the URL used to access the CTI Engine. The server must recognize the name as its own. The name must be registered in the Corporate DNS, so it can be resolved by all the user's workstations. The URL configured in the call center definition must use this name. All of these names must match the SAN configured in the certificate.

4. Create the private key (with no password) and the self-signed certificate in a single command:

   openssl req -config openssl.cnf -new -extensions v3_req -x509 -sha256 -newkey rsa:2048 -nodes -keyout private_key.pem -days 365 -out certificate.crt

   To change the amount of time the certificate will be valid, adjust the value for `days`.

   This command creates the key (`private_key.pem`) and creates the self-signed certificate (**certificate.crt**).

5. Verify the certificate by running the following command:

   openssl x509 -text -noout -in certificate.crt

   This will print out the text of the certificate. When examining the output, the third line should show:

   Version: 3 (0x2)
   And farther down we should see:

   X509v3 Subject Alternative Name:

   DNS:server.domain.com

6. Run the following command to generate the `keystore.p12` file:

   openssl pkcs12 -export -in certificate.crt -inkey private_key.pem -out keystore.p12 -name avaya_crm_connector

Note

-name value must equal the value of the **server.ssl.key-alias** field set in all yml files.

7. Type a password and type the same password as a confirmation password to create the file.
8. Run the following command to copy the keystore file into the security directory:

   cp keystore.p12 /opt/avaya/images/security

Now the certificate (in the keystore) is ready for use by Docker. The name of the keystore file (if different from above) and the password used must be retained and entered into the configuration files when designated below.

You must copy a self-signed certificate into each user's workstation. The self-signed certificate should be imported into the Windows Certificate Store for Internet Explorer and Google Chrome or imported as an exception directly into Firefox. This allows the browser to treat the self-signed certificate as a genuine certificate from a trusted entity.

For the self-signed certificate to be properly recognized when imported into the Windows Certificate Store, the certificate must be installed in the Trusted Root Certification Authorities folder. Placing the self-signed certificate in any other store will not allow it to be recognized.

These actions are not required for a signed certificate.

Signed Certificate

Creating a signed certificate and the associated files does not require root privileges. A signed certificate can be created using the default user.

This process assumes a private key and certificate request file for the signed certificate are being created. Even if a self-signed certificate has been used prior to this, it is highly recommended that a completely new private key is used.

Note that this process has two components. First is the creation of the private key and certificate request. Second is the use of the returned signed certificate. How long it takes to get to the component depends on the IT security organization and process involved.

Procedure

1. Create a new directory.
   For example, **/opt/avaya/certs**
2. Run the following command to navigate to the newly created directory:

   cd /opt/avaya/certs
3. Create a file called **openssl.cnf** with the following content:

```
[ req ]
default_bits = 2048
distinguished_name = dn
prompt = no
default_md = sha256
x509_extensions = v3_req
req_extensions = v3_req
```

```
extensions = v3_req
copy_extensions = copy

[ dn ]
countryName = US
stateOrProvinceName = California
localityName = Santa Clara
organizationName = Avaya
commonName = server.domain.com

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = server.domain.com
DNS.2 = loadbalancer.domain.com
```

Please make sure you change the bold selected text to what you need. The commonName is used to be able to identify the certificate when loaded into a client's certificate store. Without this, it can be hard to identify. The subjectAltName DNS value, must be set to the server's FQDN.

Note

The SAN (subjectAltName) is very important. It must match across the server, the corporate DNS, and the URL used to access the CTI Engine. The server must recognize the name as its own. The name must be registered in the Corporate DNS, so it can be resolved by all of the user's workstations. The URL configured in the call center definition must use this name. These names must match the SAN configured in the certificate.

4. Create the private key (with no password) and the certificate request file in a single command:

   openssl req -config openssl.cnf -new -extensions v3_req -sha256 -newkey rsa:2048 -nodes -keyout private_key.pem -out certificate_req.csr

   This command creates the key (**private_key.pem**) and creates the certificate request file (**certificate_req.csr**).

   It is recommended to make the name of the certificate request file be based on the server (e.g. **servername_req.csr**). That way when the request file is sent to get the certificate, it can be easily identified as to which server it applies.

5. Send the certificate request file to the IT security department so that the signed certificate can be issued. Depending on the processes involved, this could take anywhere from minutes to multiple days.

6. Once the certificate is received, place the file into the **/opt/avaya/certs** directory on the server. Make a copy of the file and name it **certificate.crt.**

Note

Use the Base64 encoding when creating the signed certificate. If the DER encoding is used, the certificate will not match up with the private key. To switch the encoding, use the following command:

```
openssl x509 -inform der -in signed_cert.der -out certificate.crt
```

Also, if the signed certificate is a compound certificate (meaning it includes the server certificate, plus one or more intermediate certificates), it is very important to make sure the certificates are ordered correctly. The first certificate must be the server certificate, followed by the intermediate certificates in order.

7. Run the following command to generate the **keystore.p12** file :

```
openssl pkcs12 -export -in certificate.crt -inkey private_key.pem
-out keystore.p12 -name crm_connector
```

Note

-name value must equal the value of the **server.ssl.key-alias** field set in all yml files.

8. Type a password and type the same password as a confirmation password to create the file.
9. Run the following command to copy the keystore file into the security directory:

```
cp keystore.p12 /opt/avaya/images/security
```

Now the certificate (in the keystore) is ready for use by Docker. The name of the keystore file (if different from above) and the password used must be retained and entered into the configuration files when designated below.

Signed Certificate with Key

In case where IT security teams do not allow you to create keys or certificate request files, then you must send the Server FQDNs to the security team to perform these actions. The IT security team will provide both private key and a signed certificate in the form of a single key store file. When sent this way, the key store file must be sent in the PKCS12 format. Such files will usually have the “pfx” extension. The key store will also have a password assigned to it, and that must also be provided to be used.

Fortunately, this is also the format we want the key store to be in, so all we must do is copy the file to the **/opt/avaya/images/security** directory and then enter the name of the key store file and its password into the configuration files when requested below.

Deploying and configuring Docker files

Configuration mechanism

The configuration for the Docker services, such as aes3pcc, pomdriver, iec, oec, and aa4salesforce is a file based. The YML format configuration files are committed to a Git repository. These files are loaded to Consul automatically upon detecting changes. Using this

model, Git can be used as a backing store, an audit trail, and access control mechanism tool for configuration changes and Consul can be used as the delivery mechanism.

Configuration files

The following configuration files are used in an environment. Note: The configuration directory location is /opt/avaya/images/config/git-server/default-config. There is a dedicated configuration file for each service, and a configuration file -*application.yml,* contains common configuration for all services.

- aa4salesforce-prod.yml
- iec-prod.yml
- oec-prod.yml
- aes3pcc-prod.yml
- pomdriver-prod.yml
- application.yml

aa4salesforce-prod.yml

Configuration Key	Sample Configuration Value	Description
jhipster.cors.allowed-origins	"force.com, salesforce.com"	The list of allowed origins for CORS. * for all.
jhipster.cors.allowed-methods	"*"	The list of allowed methods for CORS. * for all.
jhipster.cors.allowed-headers	"*"	The list of allowed headers for CORS. * for all.
jhipster.cors.allow-credentials	true	Flag to control the Access-Control-Allow-Credentials header.
server.ssl.key-store	/security/keystore.p12	The keystore location that contains the server certificate to secure connections. Defaults to /security/keystore.p12. Keystore is created above. Update the file name if different.
server.ssl.key-store-password	password	Keystore password. Use the password created in the keystore creation process.
server.ssl.key-store-type	PKCS12	Keystore type.
server.ssl.key-alias	avaya_crm_connector	Alias for the server certificate.

iec-prod.yml

Configuration Key	Sample Configuration Value	Description
jhipster.cors.allowed-origins	"*"	The list of allowed origins for CORS. * for all.
jhipster.cors.allowed-methods	"*"	The list of allowed methods for CORS. * for all.
jhipster.cors.allowed-headers	"*"	The list of allowed headers for CORS. * for all.
jhipster.cors.allow-credentials	true	Flag to control the Access-Control-Allow-Credentials header.
server.ssl.key-store	/security/keystore.p12	The keystore location that contains the server certificate to secure connections. Defaults to /security/keystore.p12. Keystore is created above. Update the file name if different.
server.ssl.key-store-password	password	Keystore password. Use the password created in the keystore creation process.
server.ssl.key-store-type	PKCS12	Keystore type.
server.ssl.key-alias	avaya_crm_connector	Alias for the server certificate.
application.inactivityTimeout	90	The time (in minutes) of user inactivity after which a session is automatically closed. The default value is 90 minutes.
application.agentPassKey		Cipher key (seed) to encrypt or decrypt the agent's password.
application.aniMasking	A	ANI masking configuration for make call and consult call. Possible values: • A: This is available to any CM version but does not support SIP stations.

Configuration Key	Sample Configuration Value	Description
		• B: This is available to CM 6.x only and supports SIP stations. • C: This is available to CM 6.3.x and 7.x only and supports SIP stations.

oec-prod.yml

Configuration Key	Sample Configuration Value	Description
jhipster.cors.allowed-origins	"*"	The list of allowed origins for CORS. * for all.
jhipster.cors.allowed-methods	"*"	The list of allowed methods for CORS. * for all.
jhipster.cors.allowed-headers	"*"	The list of allowed headers for CORS. * for all.
jhipster.cors.allow-credentials	true	Flag to control the Access-Control-Allow-Credentials header.
server.ssl.key-store	/security/keystore.p12	The keystore location that contains the server certificate to secure connections. Defaults to /security/keystore.p12. Keystore is created above. Update the file name if different.
server.ssl.key-store-password	password	Keystore password. Use the password created in the keystore creation process.
server.ssl.key-store-type	PKCS12	Keystore type.
server.ssl.key-alias	avaya_crm_connector	Alias for the server certificate.
application.inactivityTimeout	90	The time (in minutes) of user inactivity after which a session is automatically closed. The default value is 90 minutes.
application.agentPassKey		Cipher key (seed) to encrypt or decrypt agent password.

aes3pcc-prod.yml

Configuration Key	Sample Configuration Value	Description
application.aesIp	10.10.1.10	The Application Enablement Services IP address. This can be a list of comma-separated IP addresses.
application.aesCmName	CM	The CM name configured on AES. **Important:** CM Name is case sensitive.
application.aesUsername	ctiuser	The Application Enablement Services account (CT user) for all AES 3PCC connections.
application.aesPassword	ctipass	Password for the specified Application Enablement Services account.
useSecureConnection	true	Determines whether a secure connection must be established with the Application Enablement Services. (True/False)
tlsVersion	TLSv1.2	TLS version to be used for a secure connection (1/1.1/1.2). Default value is 1.2.

pomdriver-prod.yml

Configuration Key	Sample Configuration Value	Description
application.pomServerIp	10.10.1.10	POM server IP address.
application.pomSdkPort	9970	POM server port.
application.pomTlsVersion	TLSv1.2	TLS version to be used for a secure connection (1/1.1/1.2). Default value is 1.2.

application.yml

Configuration Key	Sample Configuration Value	Description
application.weblmUrl	https://smgr.avaya.com/WebLM/LicenseServer	WebLM URL to check the license. For example: https://<weblm-server>:52233/WebLM/LicenseServer
application.trustStore	See *Sample configuration value: application.trustStore* for details.	List of certificates that must be treated as trusted ones during secure connection attempts to the external server components: AES, WebLM, and POM server. The definition must follow the syntax rules, otherwise the components will fail to read the configuration and fail to start as well: • Indentation must be the same for the keys and values on the same level. • *alias* must start with a dash (-) character, *certificate* does not. • *alias* value must be unique. • *Certificate* must be indented to start at the same horizontal position as *alias*. • The first line of the *certificate* value must contain: >- • The *certificate* content must be indented one level to the left from *certificate* (and *alias*). See *Sample configuration value: application.trustStore* for reference that follows all rules properly.

Sample configuration value: application.trustStore

```
application:
    truststore:
        - alias: alias_aes
          certificate: >-
            -----BEGIN CERTIFICATE-----
            MIIDsTCCApmgAwIBAgIIMJjyOnc/w20wDQYJKoZIhvcNAQELBQAwOjEZMBcGA1UE
            AwwQU3lzdGVtTWFuYWdlciBDQTENMAsGA1UECwwETUdNVDEOMAwGA1UECgwFQVZB
            WUEwHhcNMTcwNDA0MDkwNjU2WhcNMTkwNDA0MDkwNjU2WjB2MSAwHgYDVQQDDBdh
            ZXM3MDUuY291bGFiLmF2YX1hLmNvbTEZMBcGA1UEAwwQU3lzdGVtTWFuYWdlciBD
            QTENMAsGA1UECwwETUdNVDEOMAwGA1UECgwFQVZBWUExCzAJBgNVBAgMAk1IMQsw
            CQYDVQQGEwJJTjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIt1QWX4
            qCAo8cdHRFcJU2vHbUMPJ2XkCZ0X4AZMOUB74EeenXEBX0e2M1BsZPw3Wxlw8cZd
            rlu4qeusw3zojyhnmjcVxzdD+5VmyK3vO7SWg7nHjqcL9UU9hK5kDjnx1iXYYbjp
            No3SfK+fW2mErZGCGIzxmtq/pQ6o5MLRgYaLNQahuZad3ku45ZuQOk/HgNBuilX3
            tzVbeBSq0TMyOBRUepDhZVCJI2ENT8zqqcYeWkgKnQUAkGZ84y+5MVTn7zg9eKq3
            LbXDfdF9M7qmDGUfd7orF3bHo7Vs+mG1LuZ1soyj+CCQhMieBE7YP7mMPYsh6SsZ
            yHM/Osdz8356Mg0CAwEAAaN/MH0wDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBSy
            mTLUoY+7tKKtRtFnU9e1wrDKKDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
            AwIwHQYDVR0OBBYEFBZeTkA3S2T1zNyMnapZKKB2ZTK2MA4GA1UdDwEB/wQEAwID
            +DANBgkqhkiG9w0BAQsFAAOCAQEAdtf4JsgGzbm9vR8a4Kuit76Q3smczbhXTYit
            WRPh2I38bxr4YPX55Vo8fm1YpMEg02iCk6xh4EfHTb/4hMCJXuT1oYiy2h0soZhA
            tc7A9KZM5JFqBfz0Aw5wD2Gr4/NJq8OzlIJ+1wdmTWDOeh3Rm3Pe62Ri2Pj560nA
            ok4AkWMD+WwRVcUZXIj221/+yGHdXg6set83vYSPfhgpcVUfSyXIyjJ5vyAZm6dw
            4Cumf2JstIDHEFpsDuOFYrJFPOVg1CW3sX10fkLo3gIWoEdWmxA1UfPGnG708an9
            ByS/0u7YOghweRW54VXp/vZ9NYr9GlOsL/1tl1Wf2e0rCmmyJQ==
            -----END CERTIFICATE-----
```

Figure 19: Truststore certificate

GIT configuration changes

Configuration changes must be performed on the Git repository. These changes will be loaded to Consul and distributed among the running services automatically.

Starting the Avaya CRM Connector

The startup of Avaya CRM Connector services is performed by running the script **`start.sh`** located at `/opt/avaya/images/`

Usage

Generating the SSH keys

About this task

You need to create the required SSH keys and copy the keys to the required folders. This is required before a GIT clone as GIT runs as a separate container. GIT clone will not work until Docker is started.

Procedure

1. Run the following command to generate ssh files:

   ```
   ssh-keygen
   ```

   Leave all default options you are prompted with. This generates two files, id_rsa and id_rsa.pub

2. Run the following command:

   ```
   cp /root/.ssh/id_rsa* /opt/avaya/images/security/.shh
   ```

Cloning the GIT repository

About this task

The cloning of GIT repository is optional and must be done only if the configuration is changed.

Procedure

1. Run the following command to clone the config Git repository:

   ```
   git clone ssh://git@DOCKER_HOST_IP:2222/git-
   server/repos/config.git
   ```

2. You may encounter the following error while cloning the repository that indicates missing SSH Key for your user account. Ensure that you have sufficient access rights to perform the cloning actions.

   ```
   git clone ssh://git@localhost:2222/git-server/repos/config.git
   Cloning into 'config'...
   git@localhost: Permission denied (publickey,keyboard-
   interactive).
   fatal: Could not read from remote repository.
   Please make sure you have the correct access rights
   and the repository exists.
   ```

   Note:

   The newly cloned working copy contains the *.yml configuration files.

3. In order to make any configuration changes, do the following:
   a. Edit the corresponding *.yml config file.
   b. Run the following command to add the changes:

      ```
      git add
      ```

   c. Run the following command to commit the changes:

      ```
      git commit -m 'Your commit message'
      ```

   d. Run the following command to push the changes to the remote Git server:

      ```
      git push
      ```

Note:

The changes made directly on the Consul UI will be lost as they are not synchronized to Git. However, you can use the Consul UI to view the current configuration on the K/V tab.

Certificate Management using YML files

Each component in the solution that has an image will have a corresponding YML file which contains the initial configuration. These YML files are loaded into the Consul component which itself runs as a container in the solution when Docker compose is started. The initial configuration which includes CORS filters, configuration for SSL, and certificates can be configured in the YML files.

Three components in the solution expose an HTTP interface and which must be secured:

- The AA4salesforce which is the softphone component
- The IEC
- The OEC which have CometD interfaces

HTTPS has to be enabled for these three components. The configuration pointing to a keystore file that resides in the security directory is defined in the YML file. The system retrieves the certificate from the defined path in the YML file.

The Consul loader also retrieves the contents of the YML files. The certificates are loaded after the installation in the Consul UI.

Stopping the Avaya CRM Connector

The shutdown of Avaya CRM Connector services is performed by running the script **`stop.sh`** located at `/opt/avaya/images/`.

Docker files scripts

- To stop Docker compose, run the following script:

  `stop.sh`

- To load new images, run the following script:

  `load-images.sh`

- To start Docker compose, run the following script:

  `start.sh`

Salesforce Configuration

Prerequisites

To start using Avaya CRM Connector in Salesforce, you must first perform the following tasks:

No.	Task	Reference	Notes	✔
1	Install the APEX package	See Installing the APEX package		
3	Configure the Call Center Detail components	See Configuring the Call Center Definition settings		

Installing the APEX package

Before you begin

Log in as a Salesforce administrator.

Procedure

1. Install the package for a production organization by using the following URL:
2. https://login.salesforce.com/packaging/installPackage.apexp?p0=04t41000002ePFu
3. Install the package into a sandbox by using the following URL:
4. https://test.salesforce.com/packaging/installPackage.apexp?p0=04t41000002ePFu

   If you are not logged in as a Salesforce administrator, the system displays the Salesforce login page.
5. Provide the Salesforce administrator login credentials when prompted.
   The system displays the package page.

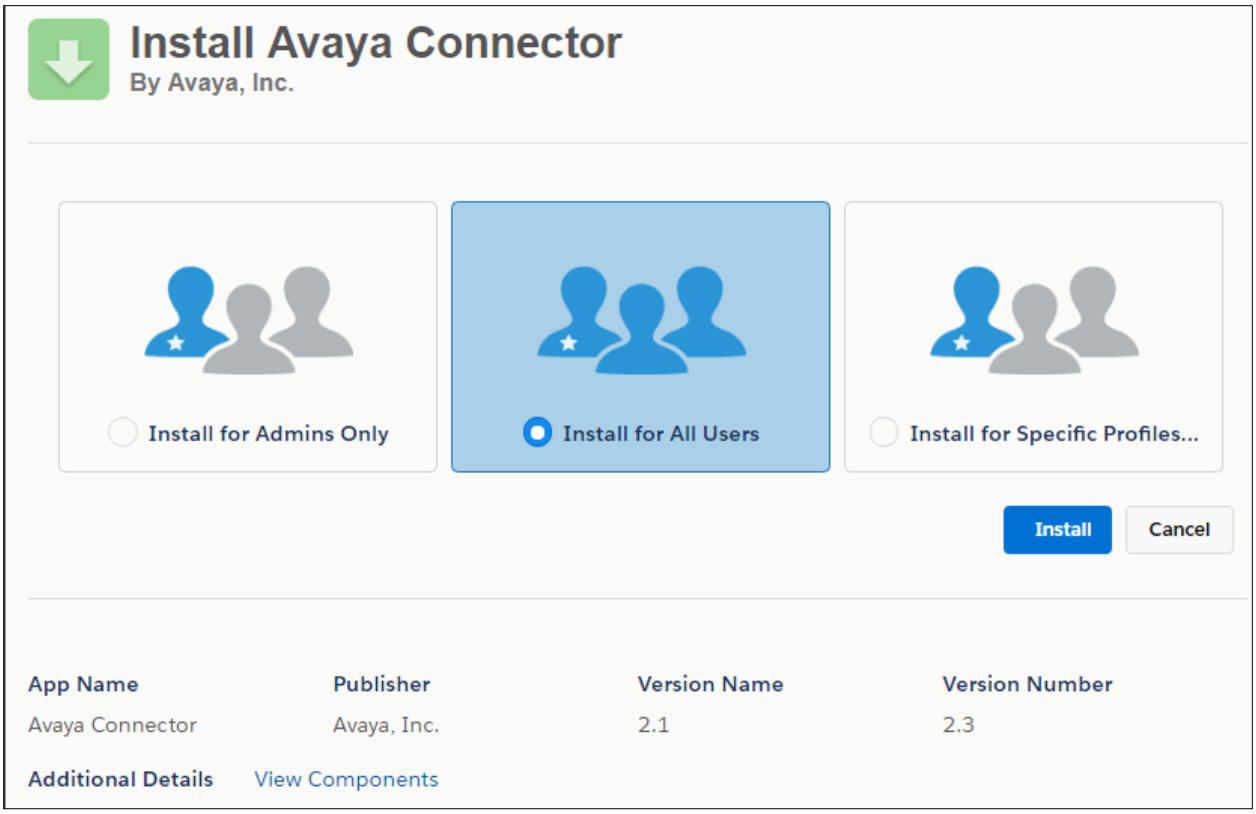

Figure 20: Package page

6. Ensure that the **Install for All Users** option is selected.
7. Click **Install**.
8. After the installation is completed, click **Done**.
   The system installs the APEX package which contains the following components:
   - Apex Class: DataRetrieval
   - Apex Class: UserRetrieval
   - Apex Class: DataRetrievalUnitTest
   - Apex Class: UserRetrievalUnitTest
   - Apex Class: ObjectDetailsRetrieval
   - Apex Class: ObjectDetailsRetrievalUnitTest

Creating the activity custom fields for call logs

About this task

Using the Custom Call Log fields, you can enable enhanced call logging feature which saves additional information into the call log record. Salesforce handles these fields as Activity Custom Fields. The following procedure is optional in context of Avaya CRM Connectors 2.1 and must be performed only in case the customer wants to save the activity information in the call logs.

Procedure

1. Navigate to **<Username> > Setup > App Setup > Customize > Activities > Activity Custom Fields**.
2. Click **New** and create the activities for each of the following custom fields:

Purpose	Suggested field name and label Name	Suggested description and help text	Data type	Suggested API name
Caller ID (ANI)	Caller	Caller's Phone Number (ANI)	Phone	Caller__c
Called Number (DNIS)	Called	Called Phone Number (DNIS)	Phone	Called__c
UUI (User To User Information)	UUI	User to User Information (UUI)	Text(96)	UUI__c
Queue (for ACD Calls)	Queue	ACD Queue	Text(96)	Queue__c
Campaign	Campaign	POM Campaign Name	Text(96)	Campaign__c

3. Follow the table and the on-screen instructions to complete the settings.
4. Click **Save** and repeat steps for all custom fields in the table above.

Note:

Mandatory Call Log Fields for POM

In addition to the three custom call log fields, a campaign, caller, and called variables must be defined in the CCDef:

- Campaign__c
- The value of Caller Field API Name
- The value of Called Field API Name

Configuring the Call Center Definition settings

About this task

Salesforce Call Centers can be created by importing and configuring the Call Center Definition (CCD) XML file into Salesforce.

Procedure

1. Navigate to **<Username> > Setup > App Setup > Customize > Call Center > Call Centers** OR

   Type **Call Centers** in the search field on the left pane. (Do not click the Enter key.)

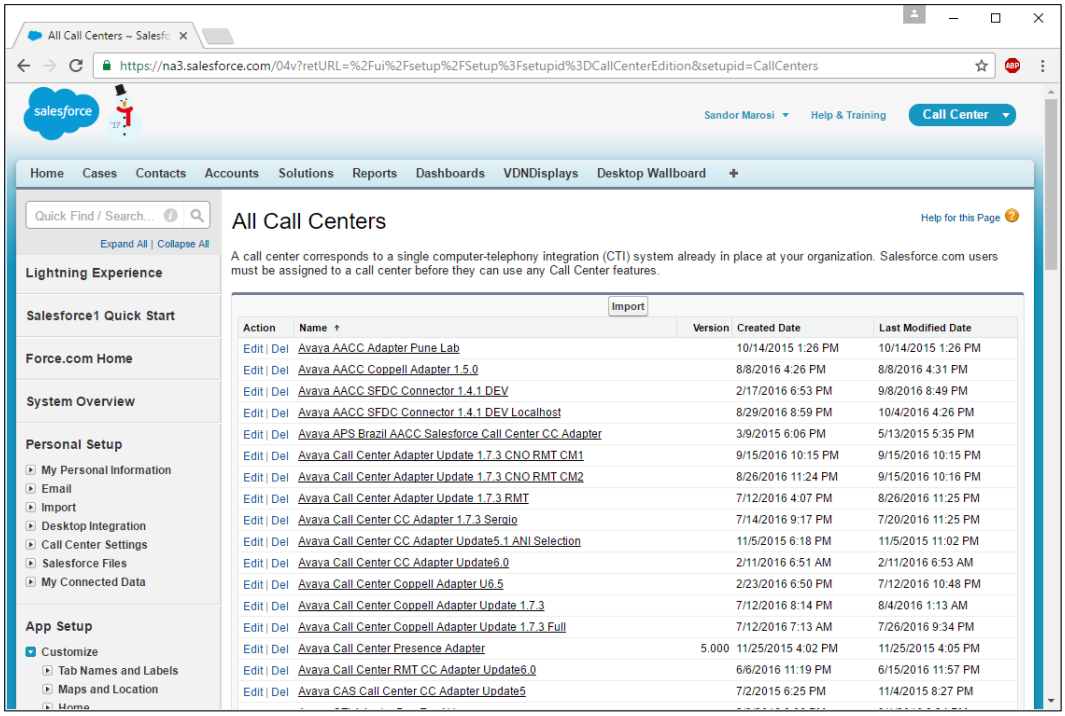

Figure 21: All Call Centers

2. (**Optional**) If the system displays a help page, click **Continue**.

   The system displays the CCD Import page.

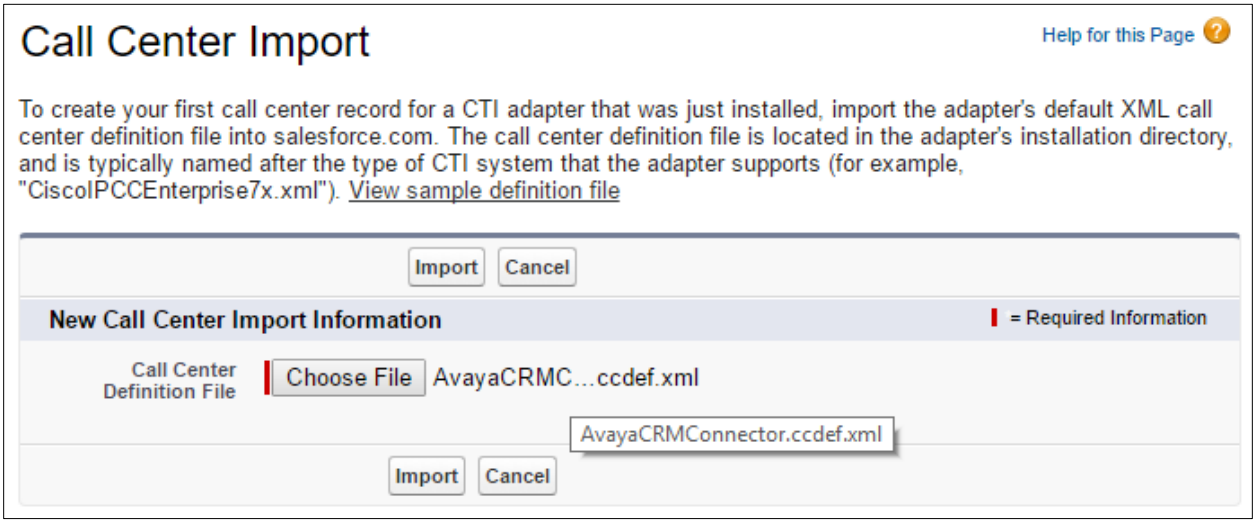

Figure 22: CCD Import

3. Click **Import**.
4. Click **Choose File** and select the desired CCD file.

5. Click **Import** again.
   The system adds the new CCD file in the list of Call Centers.

Call Center components general descriptions

You must configure the following settings of the Call Center Detail component:

- General Information
- Dialing Options
- Softphone Options
- Call Log Options
- Label Options
- Screen Pop Options
- Reason Codes
- CometD Server Configuration

You must add information in the required fields as explained in the field descriptions sections of this guide.

General Information settings field descriptions

Name	Default	Description
Internal Name and **Display Name**	CRMConnector21	The fields to uniquely identify the Call Center definition in Salesforce. If multiple Call Center definitions are present in a Salesforce instance, each name must have a unique Internal Name and Display Name.
Display Name	Avaya CRM Connector 2.1	The field to define the name of a CCD for identifying the CCD in the list of CCD files.
Web Agent Widget URL	https://linpubi145.gl.avaya.com:8484	The Web Agent Widget URL indicates the entry point for the web application letting the browser fetch it from the Web Agent Salesforce Connector Server. The URL pattern follows: *https://<server>:<port>* Where *<server>* is the Server Cluster IP or fully qualified domain name (FQDN).

Name	Default	Description
Use CTI API	True	An option to use CTI API in Call Center Definition. You must always keep this value as True.
Softphone Height	600	These properties are used by Salesforce to define the pixels required by each dimension to properly display the Avaya CRM Connector web page. **Note** • In Salesforce.com, **Standard View** and **Console mode**, the recommended height to properly display the softphone is 560 pixels. In Lightning mode, the recommended height is 600 pixels. • In Salesforce.com, **Standard View**, the width is fixed as 200 pixels and cannot be changed. The height value can be adjusted to allow the widget to display properly.
Softphone Width	260	
Salesforce Compatibility Mode	Classic_and_Lightning	Determines the settings where the softphone is visible. **Note** • To display the softphone in Lightning Experience, select **Lightning**. • To display the softphone in Salesforce Classic, select **Classic**. • To display the softphone in both user interfaces, select **Classic_and_Lightning**.

Dialing Options field descriptions

Name	Default	Description

Name	Default	Description
Outside Prefix	9	**Outside Prefix** is the number used to get external dial tone. **Long Distance Prefix** is the number needed to indicate a long distance call. **International Prefix** is the number needed to indicate an international call.
Long Distance Prefix	1	
International Prefix	011	
Internal Number Length	4	A field to specify the type of number: The options are: • **Internal number**: If the number of digits in a phone number is equal to or less than the given value, then the number is treated as an internal number. • **Inbound** or **outbound external number**: If the number is greater than the given value, the number is treated as an inbound or outbound external number. **Note** If this value is 0, then all numbers are treated as inbound or outbound external numbers. If the local dial plan uses extensions as long as the local number length, set this value to 0.
Country Code	1	A field to specify the dialing country code of the current location. This value is used for the enhanced outbound number processing as the default number processing follows US country code standard.
Local Number Length	7	A field to define the length of an external phone number. If 10-digit local numbers are used, then set this value to 9 and use the Communication Manager routing

Name	Default	Description
		tables to finish handling the number.
Long Distance Length	10	A field to define the length of a long distance external phone number. These values are used to examine an outbound number to determine which prefixes to use.
Do Not Call Prefix		A field to define the Do Not Call Prefix for a number. If there is no default value added, this feature is not enabled. This feature is applicable for click-to-dial calls only.

Softphone Options field descriptions

Name	Default	Description
Is Call Center? (Y/N)	Y	A field to determine whether the ACD is used. The options are: • Y: ACD is used. The ACD agent ID and password fields are included in the login form. The default value is Y. • N: ACD is not used. The ACD agent ID and password fields are not included in the login form and only the extension information is requested.
Transfer Button Enabled? (Y/N)	Y	A field to disable the option to transfer. The options are: • Y: The Transfer call capability is enabled. • N: The Transfer call capability is disabled.
Conference Button Enabled? (Y/N)	Y	A field to disable the option to conference. The options are: • Y: The Conference call capability is enabled. • N: The Conference call capability is disabled.
Call Log Report URL	<Default_URL>	A field to define the URL to use when someone selects My Report Label. If no value is present, then the option is not shown. This is a partial URL. A default value is included in the call

Name	Default	Description
		center definition XML file.
Click-to-Consult Enabled? (Y/N)	Y	A field to extend the basic click-to-dial functionality to allow for click-to-consult. Click-to-dial only works if the phone is currently idle, or if all calls present are held. If there is a single active line, and click-to-dial is invoked, click-to-consult will automatically initiate a consultative call. Once initiated, the consultation can be completed as either a conference or a transfer, or it can be backed out to the original call. The options are: • Y: The option to enable click-to-consult call. If there is a single active line, and click-to-dial is used, then click-to-consult is automatically started. • N: The option to disable click-to-consult call.
Available Type (A/M)?	A	A field to specify the Available type. The options are: • Auto-In (A): Using this option will automatically move the user to an Available state after an ACD call. • Manual-In (M): Using this option will place the user in a Wrap-up state after an ACD call. The user must then manually set them to an Available state to receive another call.
Auxiliary Enabled? (Y/N)	Y	A field to allow users to set the Auxiliary state. The options are: • Y: The option to set Auxiliary state is enabled. • N: The option to set Auxiliary state is disabled. **Note:** Even though if Auxiliary Enabled is set to N, the agent can still change the state to Auxiliary Work using the Outreach tab.
After Call Work Enabled? (Y/N)	Y	A field to allow a user to manually set the After Call Work state. The options are: • Y: Allows user to set After Call Work manually. • N: Do not allow user to manually set the ACD state to After Call Work. It is possible for the user to end up in the After Call Work state automatically. For example, if the Available type used is Manual-In, or if Timed ACW is used with

Name	Default	Description
		Auto-In, the user will automatically change to After Call Work even when set to N.
Auto Login Enabled? (Y/N)	N	A field to automatically log the user into the softphone. The options are: • Y: Automatic login is enabled. This option works only when the login credentials are already stored. If the credentials are not stored, the user is not logged in automatically even when this setting is Y. • N: Automatic login is disabled.
Default Language	en_US	A field which defines the default language of the softphone application.
Password Enabled? (Y/N)	Y	Determines whether a Password field is presented in the login form. If set to N, the login form will only show Extension and Agent Id.
Extension from Salesforce User Profile? (Y/N)	N	A field to take the extension from Salesforce user profile. The options are: • Y: Extension is taken to Salesforce user profile and cannot be changed. If the setting in Salesforce is wrong or missing, the user will not be able to log in. • N: Extension has to be entered manually into the login screen.
Enable Console Logout? (Y/N)	Y	A field to logout the extension from the Softphone in Salesforce Console Mode logout. The options are: • Y: The extension will be automatically logged out of the ACD when the user logs out of the Console. • N: The extension will remain logged in into the ACD even after logging out of Salesforce.
Display login time information? (Y/N)	N	A field to display the login time information. The options are: • Y: The login time information will be showed in the Softphone. • N: The login time information won't be showed in the Softphone

Name	Default	Description
Drop Selected Party Enabled? (Y/N)	N	A field to handle the drop of parties in a conference. The options are: • Y: The user has to indicate which party wants to remove from the conference. • N: The user can remove only the last added party.
Automatically answer incoming calls? (Y/A/N)	N	A field to enable auto answer for incoming calls. The options are: • Y: All the incoming calls will be auto answered. • A: Only the ACD calls will be auto answered. • N: No calls will be auto answered.
Display hold timer? (Y/N)	N	A field to display a hold timer into the softphone. The options are: • Y: The hold timer will be shown in the softphone. • N: The hold timer won't be shown in the softphone.
Display Agent State timer? (Y/N)	N	A field to display a timer for the agent's current state. The options are: • Y: The Agent State timer will be showed in the softphone. • N: The Agent State timer will not be showed in the softphone.
Omnichannel Enabled? (C/S/N)	N	Enable integration with Salesforce Omnichannel when using Console mode. The options are: • C: Omnichannel complimentary mode is enabled. • S: Omnichannel synchronized mode is enabled. • N: Omnichannel integration is disabled.
Omnichannel Ready Status Id	<EMPTY>	In case of Salesforce Omnichannel Enabled, the system allows to select the id for Ready status.
Omnichannel Not Ready Status Id	<EMPTY>	In case of Salesforce Omnichannel Enabled, the system allows to select the id for Auxiliary status.
Omnichannel Not Ready	21=Digital	In case of Salesforce Omnichannel Enabled, the system allows to select the id and the text for the Reason Code to

Name	Default	Description
Reason Code	Ready	be used on Auxiliary status.
Show Device Name? (ADQ)	ADQ	If A/a-ANI or D/d-DNIS or Q/q-QUEUE is present, the corresponding device name is displayed on the call card when a call is either performed or received. If none is configured the ANI, DNIS, and QUEUE will be displayed instead of the name.
Append Agent ID to UUI? (Y/N)	Y	A field to append agent's id to UUI when the agent drops the call.
Outbound ANI Replacement	<EMPTY>	If this field is set for outbound calls, it replaces the ANI with the set value.
ANI Replacement WS URL	<EMPTY>	A field to define the URL of the application that returns the ANI replacement options. The options can be used to replace the ANI when performing an outbound call. This field will not have any effect if 'Outbound ANI Replacement' field is not empty.
ANI Masking on Consult? (Y/N)	N	If field is set to Y, it enables ANI replacement for consult, blind transfer, and blind conference calls. The 'Outbound ANI Replacement' or 'ANI Replacement WS URL' field must be set for this field to have effect.

Call Log Options field descriptions

Name	Default	Description
Call Log Enabled ?	Y	A field to enable call logging. The options are: • Y: Call logs are saved for all calls. • A: Call logs are saved for only ACD calls. • E: Call logs are saved for only inbound and outbound external calls. • N: Call logs are not saved.
Show Call Log?	Y	A field to allow users to view the call logs. The options are: • Y: Allows users to view the call logs. • N: Disallows users to view the call logs.

Name	Default	Description
Save Call Log on Call Start? (Y/N)	N	A field to enable call logging when the call status is in progress at the beginning of the call. The logs are later updated when the call is dropped. The options are: • Y: Call logs are saved at the beginning of the call and later updated. • N: Call logs are saved at the end of the call. The default value is N.
Call Log on Incomplete Calls	N	A field to enable call logging for unanswered calls. The options are: • Y: Call logs are saved for unanswered calls. • N: Call logs are not saved for unanswered calls
Make Call Log Related Data Sticky	Y	Determines how the call log references are saved. The options are: • Y: The application sets the reference to be saved to the first matching resource browsed. The user can always override the selection manually, but continued browsing does not update the selection. Only user intervention can change the selection. The last selection is saved. • N: The application sets the reference to be saved to the latest resource browsed. Every time the user browses to a new resource, the reference selection is updated. The user can override the selection, but any further browser will again update the reference.
Caller Field API Name	Caller__c	A field to define the Activity Custom Field API Name to save the Caller ID (ANI). If it is empty, this parameter will not be saved in the call log.
Called Field API Name	Called__c	A field to define the Activity Custom Field API Name to save the Called Number (DNIS). If it is empty, this parameter will not be saved in the call log.
UUI Field API Name	UUI__c	A field to define the Activity Custom Field API Name to save the UUI (User To User Information). If it is empty, this parameter will not be saved in the call log.
Queue Field API Name	Queue__c	A field to define the Activity Custom Field API Name to save the Queue for ACD Calls. If it is empty, this parameter will not be saved in the call log.
Call History? (Y/N)	Y	A field to enable access to a button to show information about the last calls in which the user was involved. The options are: • Y: The user can view call history.

Name	Default	Description
		• N: The user is not able to view call history.
Show Comments	Y	A field to indicate if the comments entry is displayed in the Log Details. The options are: • Y: The user can view and edit the comments for the call log. • N: The user is not able to view the comments entry and it will be saved empty.
Show Name (Y/N)	Y	A field to store the name of the caller in the logs. • Y: The user can view the name of the caller. • N: The user is not able to view the name of the caller.
Show Related To (Y/N)	Y	A field to store the name of the group/category the caller belongs to in the logs. • Y: The user can view the group/category name of the caller. • N: The user is not able to view the group/category name of the caller.
Enable Task/Call Log link (Y/N)	N	A field to indicate if a new call log will be created for a call placed from a click-to-call from a task. The options are: • Y: The task is reused for call log saving. • N: The task is not reused for call log saving; a new call log will be created.
Update Task Status (Y/N)	N	A field to set the call log status as Completed, if the Enable Task/Call Log link option is enabled. The options are: • Y: The call log status is set as Completed. • N: The call log status is not set. In case of reusing a task will remain in the same state.
Enable UTC time (Y/N)	N	A field to allow the call log time to be saved in a UTC format instead of a local time. The options are: Y: The time in the UTC format is used to be saved in the call log. N: The local time is used to be saved in the call log.
Enable Interaction Log? (Y/N)	N	A field to integrate with the Salesforce Console interaction log and not the call log. The options are: • Y: Enables integration with the Salesforce Console interaction log. This setting must be only when both Call Log Enabled and Show Call Log are set to N. • N: Disables integration with the Salesforce Console interaction

Name	Default	Description
		log.
Custom Call Log Field 1 to 3	<EMPTY>	A set of fields to activate three custom fields in the call log. You can define two different type of fields: • Text Field: Format = “Label:Variable”. This type of field shows textbox free form field. Example: “Description:Description__c” • Pick List: Format = “Label:Variable:Item1:Item2:ItemN”. This type of field shows a drop-down list with a list of items to choose. Example: “Type:Type__c:New:Existing:Returning:Cancelled:Unknown” Where: • Label is the text to display at left of the field. • Variable is the Salesforce API name for the Task/Activity field. • Item1 to ItemN is the elements to be displayed in the drop-down list. Also, in addition to the three custom call log fields, a campaign, caller and called variables must be defined in the call center definition for POM: • Campaign__c • The value of Caller Field API Name • The value of Called Field API Name The customer can define up to three custom call log fields in the call center definition. These custom fields have the following structure: <Field Label>:<Variable_Name>[:<PickList_Value1>:<PickList_Value2>:...:<PickList_ValueN>] If the pick-list values are omitted, the UI will render the custom field as an input text box allowing the customer to enter any kind of value by hand instead of picking a predefined one. **Note:** By design, no value will be implicitly selected for the pick-list.
Call Log Completed Status	Completed	A field to define the default text for a completed call log status.

Name	Default	Description
Call Log In Progress Status	In Progress	A field to define the default text for a call log status which is in progress.
UCID URL Field API Name	<EMPTY>	A field to define the name of a log parameter which will contain a UCID URL.
UCID URL	<EMPTY>	A field to define the URL to be used in the logs in the format **<url>?UCID=<ucid>.** It will populate the parameter set in the 'UCID URL Field API Name' field.
Prioritize Related To (Y/N)	N	If this field is enabled and If Name is Lead and Related To contains a valid reference, then save Related To rather than Name. If the configuration item is disabled, then Name will be Lead and the Related To will be left empty.

Label Options field descriptions

Name	Default	Description
Login Extension	<EMPTY>	If provided, it will override the "Extension" label on the login form.
Login Agent ID	<EMPTY>	If provided, it will override the "Agent Id" label on the login form.
Login Agent Password	<EMPTY>	If provided, it will override the "Agent Password" label on the login form.
Login Accept Button	<EMPTY>	If provided, it will override the "Accept" button name on the login form.
Login Reset Button	<EMPTY>	If provided, it will override the "Accept" button name on the login form.
Available Label	<EMPTY>	If provided, it will override the "Available" option in the agent state pull-down list.

Name	Default	Description
Auxiliary Label	<EMPTY>	If provided, it will override the “Auxiliary” option in the agent state pull-down list.
After Call Work Label	<EMPTY>	If provided, it will override the “After Call Work” option in the agent state pull-down list.
Busy Call Label	<EMPTY>	If provided, it will override the “Busy Call” option in the agent state pull-down list.
Pending Auxiliary Label	<EMPTY>	If provided, it will override the “Pending Auxiliary” option in the agent state pull-down list.
Pending After Call Work Label	<EMPTY>	If provided, it will override the “Pending After Call Work” option in the agent state pull-down list.
On Call Label	<EMPTY>	If provided, it will override the “On Call” option in the agent state pull-down list.
Log Out Label	<EMPTY>	If provided, it will override the “Log Out” option in the agent state pull-down list.
Agent Mode Label	<EMPTY>	If provided, it will override the “Agent Mode” option in the pull-down list.
Zone	<EMPTY>	If provided, it will override the “Zone” option in the pull-down list.

Call ScreenPop Options field descriptions

Name	Default	Description
Pop on ANI	Y	A field to enable screen pops for ANI. The options are: • Y: The screen pop for ANI is enabled. • N: The screen pop for ANI is disabled.

Name	Default	Description
		Note Even if Pop on ANI is set to N, all other screen pop capabilities are still enabled.
Pop on DNIS	N	A field to enable screen pops for DNIS. The options are: • Y: The screen pop for DNIS is enabled. • N: The screen pop for DNIS is disabled. **Note** Even if Pop on DNIS is set to N, all other screen pop capabilities are still enabled.
Pop on Transfer and Conference	N	A field to enable screen pops on a transfer or a conference call. The options are: • Y: The screen pop is enabled. The transfer or the conference call recipient gets the last browsed salesforce object that the original users have browsed. • N: The screen pop is disabled. **Note** This feature uses Original Call Information, and if the transfer/conference is not done through the Connector, the expected pop will not happen.
Use E164 format for ANI search	N	A field to enable searching for ANI Number using E164 format. The options are: • Y: E164 ANI search is enabled. • N: E164 ANI search is disabled.
UUI1 to **UUI5**	<EMPTY>	Each of these components can be handled differently. In general, a given UUI element can be mapped to a given object and column in the Salesforce database (using the object.column form) or in all the columns using *. It can also be used to replace the

Name	Default	Description
		ANI or DNIS values (by specifying ani or dnis), or it can be simply used for display (designated by a value starting with a). For more information, see the following table.
UUI Start and **UUI Stop**	; for start : for stop	A special character that denotes the end of the UUI as the Open CTI Adapter cares about it. The purpose of this character is to allow an arbitrary number of characters at the end of the UUI to be ignored for whatever reason.
UUI Separator	!	A special character that separates each of the UUI fields. It can occur up to four times in the UUI field, and marks the separation between each field.
Suppress Screen Pop (C/A/W/D)		A filed to determine when a screen pop should be suppressed. The options are: • C: If an agent is on a call, the screen pop is suppressed. • A - If an agent is in AUX state, the screen pop is suppressed. • W - If an agent is in ACW state, the screen pop is suppressed. • D – If the agent is on a direct call, the screen pop is suppressed. **Note:** We can have any combination of the above values in the configuration. If no value is provided, then this feature is disabled. When a screen pop is suppressed, the search action can still be performed, and the results will still be shown in the softphone. However, the active screen will not be changed to the results of the search.
End Pop VisualForce Page Name		A field to define the name of the VisualForce page that will be triggered at the end of a call.

Example UUI1 to UUI5

There are three delimiter characters for the UUI field: Start, Stop, and Separator. Start denotes where the Open CTI Adapter will start reading the UUI values. Anything prior to Start is completely ignored. Likewise, Stop denotes where the Open CTI Adapter will stop reading the UUI values. Anything after Stop is also completely ignored. Separator is used to break the fields apart. You only need enough Separator delimiters for the values present.

In general, the solution requires the use of Start and Stop. There is only one exception. If there is no Start delimiter present in the UUI, the entire UUI value will be used as the first element (UUI1).

All examples below assume that Start is ";", Stop is ":", and Separator is "!"

"00022"

";00022:"

";00022!!!!:"

These result in the same action: the value "00022" is placed into UUI1, and the other fields are left empty.

";!00001017:"

";!00001017!!!:"

These result in the value "00001017" placed into UUI2, and the other four fields left empty.

";!00001017!!CSR:"

";!00001017!!CSR!:"

These result in the value "00001017" placed into UUI2, the value "CSR" placed into UUI4, and the other three fields left empty.

Note that all three of the above examples show that any Separator delimiters ("!" in our examples) are not needed after the last field with a value, but can exist if so desired.

";A!B!C!D!E:"

In this example, the value "A" is placed into UUI1, the value "B" is placed into UUI2, the value "C" is placed into UUI3, the value "D" is placed into UUI4, and the value "E" is placed into UUI5. While this would rarely ever be used, it shows all the fields being filled with a simple value.

Keyboard shortcuts

The following are the list of keyboard shortcuts that can be used in the Connector for keyboard navigation. The default values can be changed. If you are defining a combination of keys for an action, the keys should be separated by the + sign.

Name	Keyboard shortcut default
Open Dialpad	Ctrl+Alt+m
Focus Make Call Textfield	Ctrl+Alt+8
Access Directory Popup	Ctrl+Alt+s
Redial	Ctrl+Alt+n
Open My Calls Today Report	Ctrl+Alt+t
Open Call History Popup	Ctrl+Alt+l
Drop Call	Ctrl+Alt+d
Answer Call	Ctrl+Alt+f
Hold Call	Ctrl+Alt+h
Retrieve Call	Ctrl+Alt+r
Consult Call	Ctrl+Alt+c
Blind Transfer	Ctrl+Alt+i
Blind Conference	Ctrl+Alt+o
Complete Transfer	Ctrl+Alt+j
Complete Conference	Ctrl+Alt+k
Drop Last Party	Ctrl+Alt+p
Focus on Subject Field	Ctrl+Alt+9
Focus on Name Dropdown	Ctrl+Alt+z
Focus on Related To Dropdown	Ctrl+Alt+x
Focus on Comments Text Area	Ctrl+Alt+v
Focus on Custom Field 1	Ctrl+Alt+4

Name	Keyboard shortcut default
Focus on Custom Field 2	Ctrl+Alt+5
Focus on Custom Field 3	Ctrl+Alt+6
Focus on Reason Dropdown	Ctrl+Alt+b
Focus First After Call Work Reason	space
Finish After Call Work	Ctrl+Alt+w
Finish After Call Work And Set Available	Ctrl+Alt+q
Previous Cal	[
Next Call	]
Set Agent to Ready State	Ctrl+Alt+1
Set Agent to Auxiliary State	Ctrl+Alt+2
Set Agent to After Call Work State	Ctrl+Alt+3
Close Call History	Esc
Close Parties List	Esc
Cancel Ani Replacement	Esc
Close Ani Replacement	Enter

Reason Codes settings field descriptions

Name	Default	Description
Auxiliary Reason Enabled	N	A field to activate Auxiliary Reason codes. The option explicitly lists all the available Auxiliary Reason Codes. There are 20 slots for Auxiliary reason codes in the XML file. The format of the entry is ID=Label, where ID is the reason code number that is used by CM and Label is the string that is shown to the user. The

Name	Default	Description
		ID values must not be consecutive. If the value is set to Y, you need to select the available Auxiliary Reason Code for selecting the state as Auxiliary. **Note:** If more than 20 slots is required, an alternative XML file can be provided that has all 99 slots.
Logout Reason Enabled	N	A field to activate logout reason codes. The option explicitly lists all the available logout reason codes. There are 9 slots for logout reason codes in the XML file. The format of the entry is ID=Label, where ID is the reason code number that is used by CM and Label is the string that is shown to the user. The ID values must not be consecutive. If the value is set to Y, you need to select the available Logout Reason Code while logging out of a station.
After Call Work Reason Enabled	N	A field to activate after call work reason codes. This option explicitly lists all after call work reason codes. There are 20 slots for after call work reason codes in the XML file. The format of the entry is just the reason code label, as there are no codes or IDs for after call work reason codes.

Server Configuration field descriptions

Name	Default	Description
Host FQDN/IP	linpubi145.gl.avaya.com	The FQDN of the Server Host Name setting points to the server (cluster) on which the IEC is running.

Name	Default	Description
IEC Port	8483	The port number for inbound calls.
OEC Port	8485	The port number for outbound calls.
Use HTTPS? (Y/N)	Y	The Use HTTPS setting must be set to Y or N and indicates whether the connection used supports HTTPS (SSL/TLS) protocol.

Important

Salesforce.com does not provide Call Center Definition validation capabilities and the user is able to enter any text in those fields. If the user enters a value different than the valid one for each configuration parameter, the softphone behavior is not guaranteed.

Outreach Agent Configuration

Name	Default	Description
Agent Mode? (ACD-Only/Blended/Outreach-Only)	Blended	A field to define the agent modes. The options are: • ACD-Only • Blended • Outreach-Only
Outreach Zone	Default	A field to specify the POM zone used by the agent to login. If the value set here actually exists in the POM server, the agents will use this zone to login. If the zone does not exist, then a drop-down with all the existing zones will be shown in the login screen.
Is auto nailup? (Y/N)	Y	When set to **Y**, the nail-up call is initiated by POM Server automatically without the agent's interaction. In this case, the call is not answered automatically. When set to **N**, the nail-up call is not originated until the agent explicitly directs the POM Server about agent's readiness to accept the nail-up call by pressing the **Initiate Nailup call** button.
Enable Preview Cancel?	Y	When set to **Y**, the agent will have the

Name	Default	Description
(Y/N)		capability to cancel a preview contact. When set to **N**, the agent cannot cancel a preview contact.
Nail up Call CLID	<EMPTY>	The number the POM server will use as the CLID of the nail up call.

Outreach Screen pop Configuration

Name	Default	Description
POM Screen pop?	N	A field to enable screen pop for Outreach (POM).
Search Attribute 1 to 6	<EMPTY>	The entries in these fields specify the Salesforce entities to be queried based on the incoming data in the POM record for an outbound call. The format for the configuration is as following: `<POM Contact Attribute key>:<Salesforce entity>`. Where, • *POM Contact Attributes key* determines the purpose for which it must be used and uses the specified value in the Salesforce query. • *Salesforce entity* determines what entity is being queried for the incoming value. Alternatively, the configuration can be in the following format: `<POM Contact Attribute>:<Label>` Where, the *Contact Attribute* value is displayed in the widget.
Display Attribute 1 to 8	<EMPTY>	The entries in these fields determine the Contact Attributes that must be displayed on the screen of a new call. These attributes will be also used to generate the screen pop query string as detailed in the box below. The format for the configuration is as following: `<POM Contact Attribute key>:<Salesforce entity>`. Where, • *POM Contact Attributes key* determines

Name	Default	Description
		the purpose for which it must be used and uses the specified value in the Salesforce query. • *Salesforce entity* determines what entity is being queried for the incoming value. Alternatively, the configuration can be in the following format: `<POM Contact Attribute>:<Label>` Where, the *Contact Attribute* value is displayed in the widget. Two special values can be used as key when the desired behavior is to display the campaign name and the dialed number on the screen. *campaignName* can be used to display the campaign name and *dialed key* to show the dialed number. **Note:** • These attributes must match the contact list attribute (column) names. Otherwise, blank information will be displayed. • A sample configuration can be found in the appendix section.
Outbound Screen POP Visual Force Page URL	POMScreenPop	This field is used to provide the Visual Force page relative URL for the screen pop for POM Outbound calls. If empty, the Salesforce.com default screen pop is triggered.

Note:

Salesforce does not provide the Call Center Definition validation capabilities and the user is able to enter free text on those fields. If the user enters a value different than the valid one for each configuration parameter, the softphone behavior is not guaranteed.

Call Center Agent Assignment

Salesforce users can be assigned to the Call Center that was defined by the Call Center definitions. This way the Salesforce users will be considered to be agents of the Call Center, and Salesforce will display the Salesforce UI for them.

Assigning Bulk Users

Procedure

1. Navigate to **<Username> > Setup > App Setup > Customize > Call Center > Call Centers**.
2. In **All Call Centers** list, select the desired **Call Center** name.
3. Scroll to the bottom of the page till **Call Center Users** and click **Manage Call Center Users**.
4. Use the following screen to assign users to the call center.

Note

Only those Salesforce users will be listed on these configuration pages that are not currently assigned to any Call Centers. If you want to change an existing Call Center agent assignment check the **Individual Assignment** below.

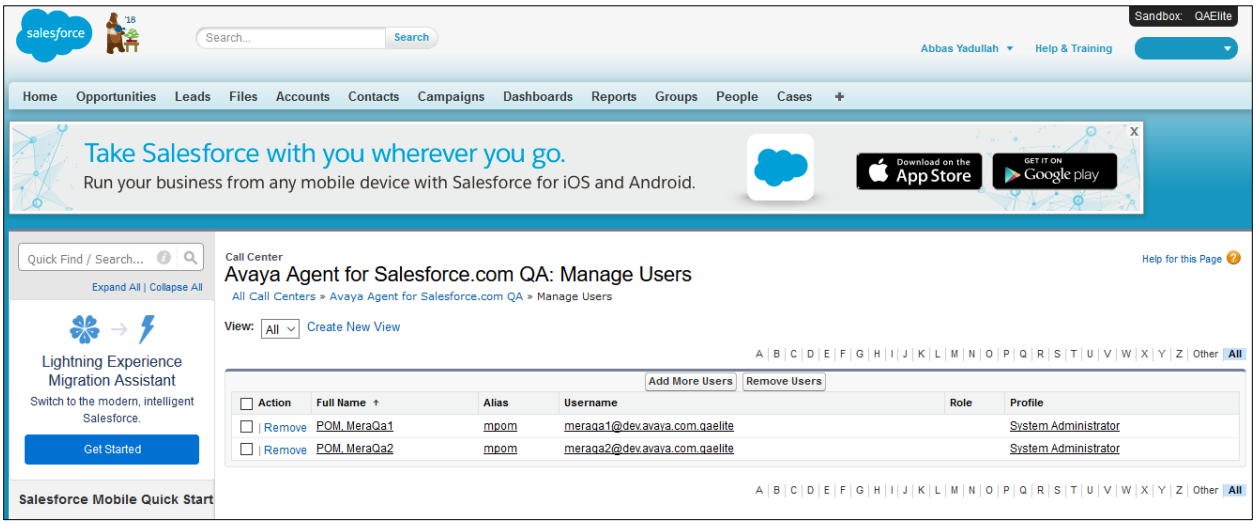

Figure 23: Manage users

Assigning Individual Users

1. Navigate to **<Username> > Setup > Administration Setup > Manage Users > Users**.
2. Select the user to edit from the list and click **Edit**.
3. Use the **Call Center** text field to set the desired Call Center for the user.

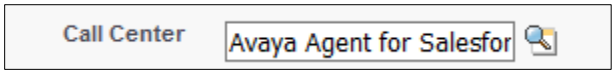

Figure 24: Call center selection

Setting up Avaya CRM Connector in Lightning Experience App Manager

About this task

The following steps must be performed in Salesforce.com setup to enable the Utility Bar which holds the Avaya CRM Connector softphone button and the panel which displays the Avaya CRM Connector in the Lightning Experience view.

Procedure

1. Navigate to **<Username> > Setup**.
2. In the *Quick Find* field, search for **App Manager** as shown in the following screenshot:

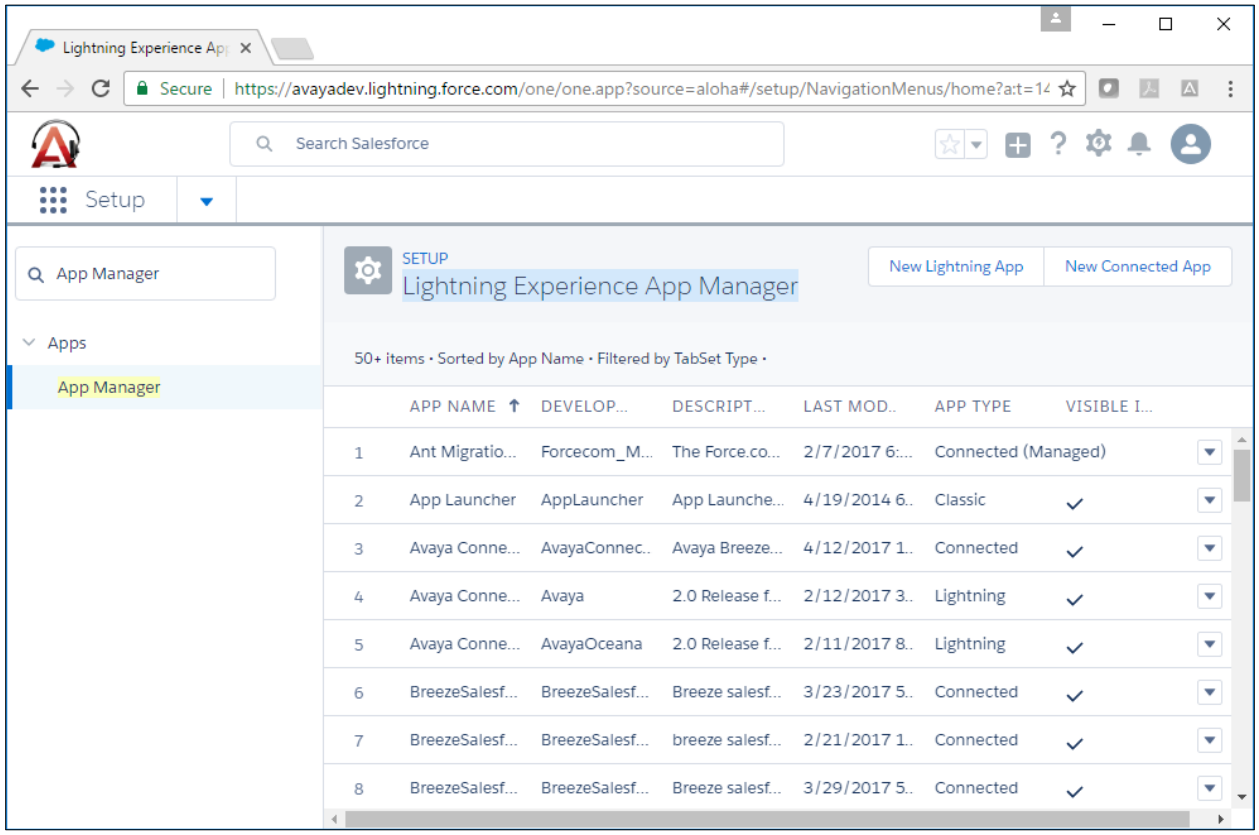

Figure 25: Quick Find – App Manager

3. While either creating or editing a **Lighting App**, navigate to **Utility Bar** > **Add** (**Utility Bar Items**).

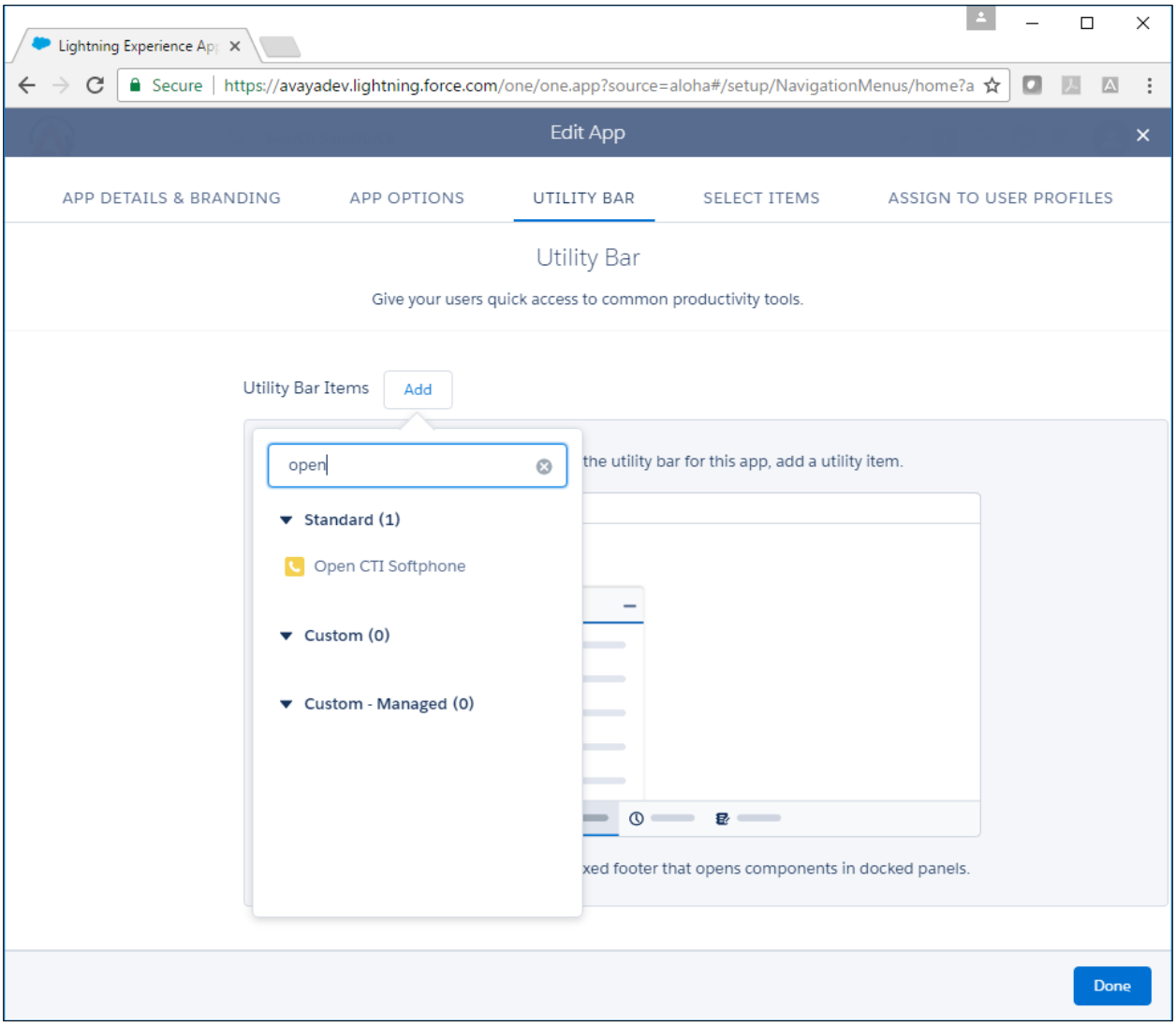

Figure 26: Add Utility Bar

4. Search for **Open CTI Softphone** and click the entry to add it in the **Utility Bar** pane. The system displays the Phone tab configuration properties.

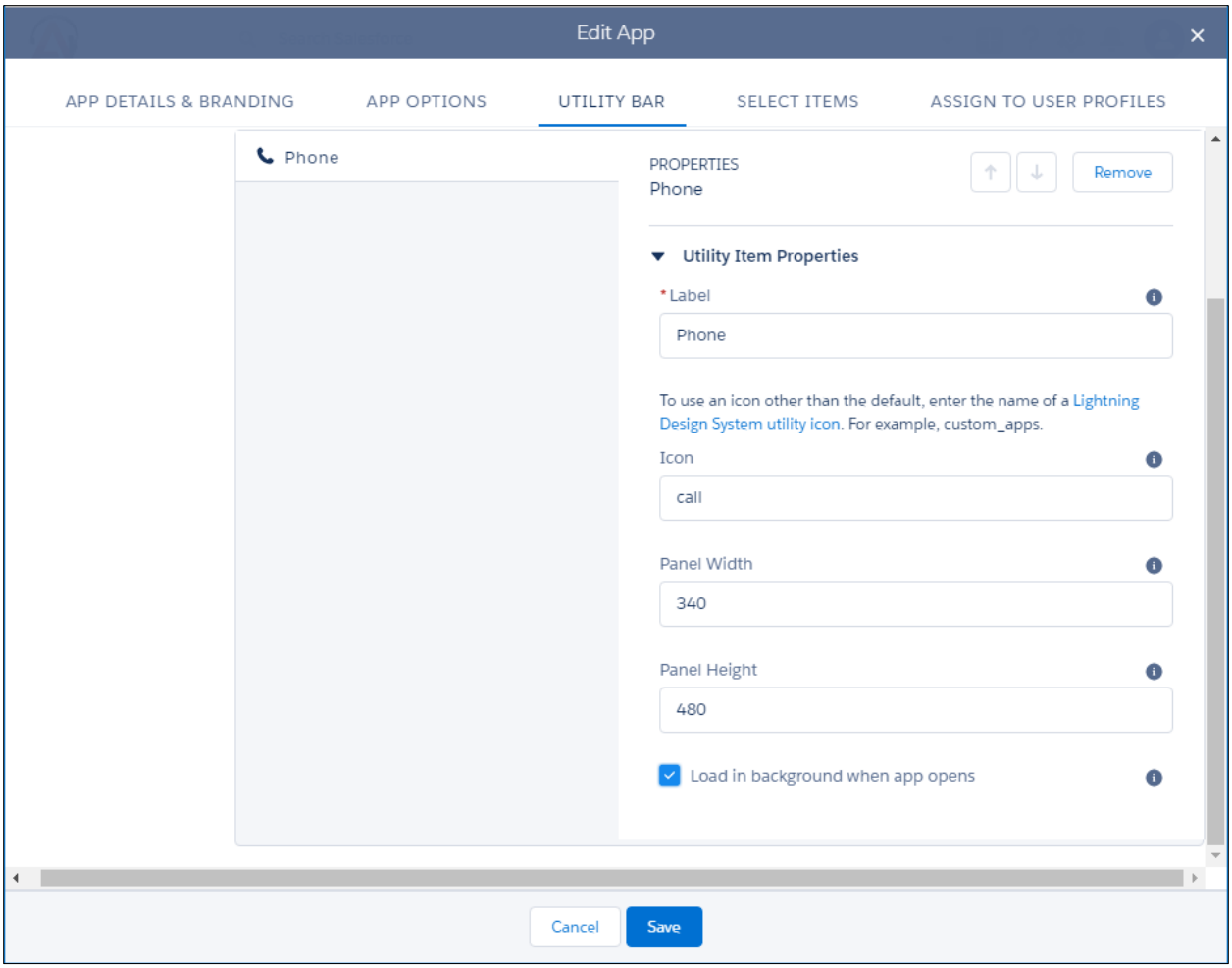

Figure 27: Utility Bar

5. In the **Panel Width** field, set the value to *260*.
6. In the **Panel Height** field, set the value to *600.*
7. If editing a Lightning App, click **Save the Changes**. OR

   If creating a new Lightning App, follow the wizard and complete the details.

   The Utility Bar and the Avaya CRM Connector button are displayed after a new user logs in the Salesforce application as shown in the following screenshot:

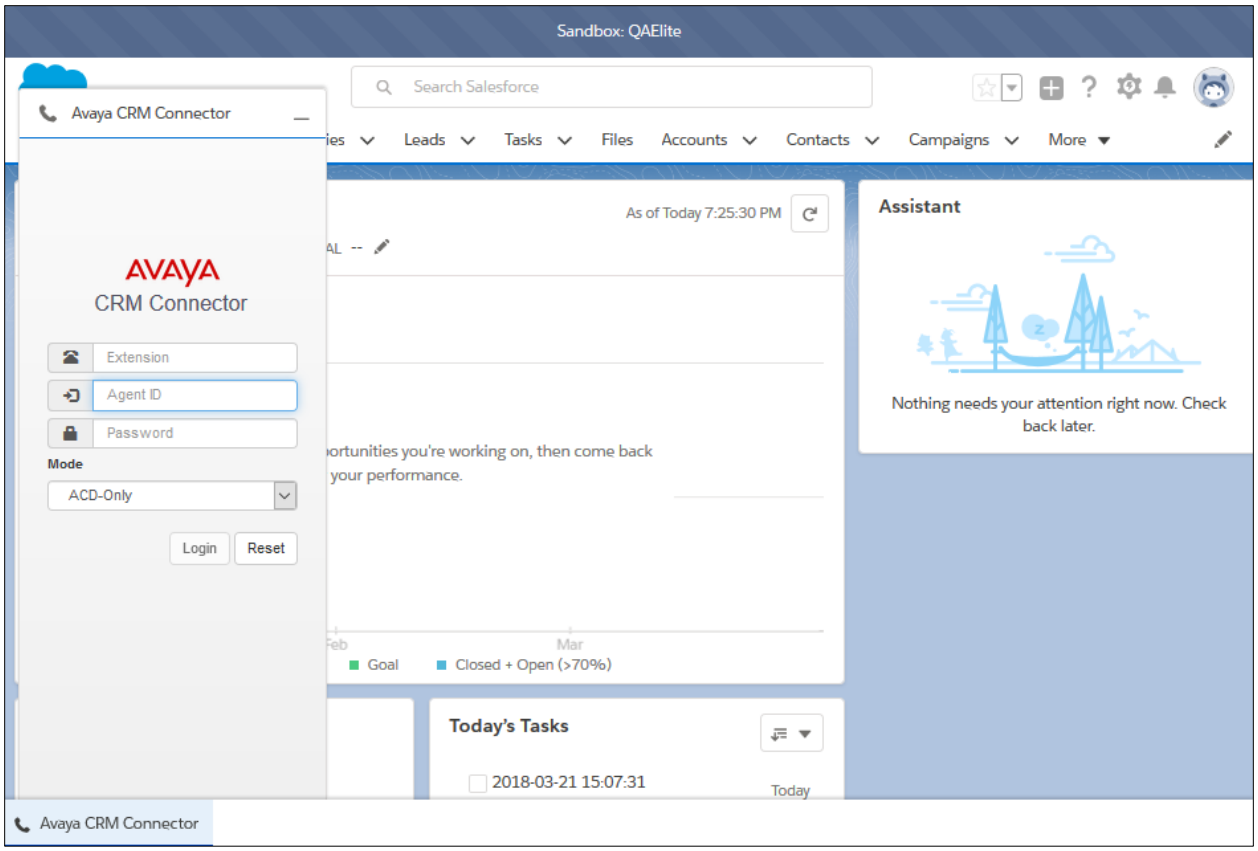

Figure 28: Avaya CRM Connector softphone panel and button

Query parameters on Visualforce page

Salesforce Lightning Standard and Salesforce Classic console modes does not allow the query parameters to be displayed in the URL. You must perform the following steps to test the query parameters that are sent to a VisualForce page.

Note:

To see the Visualforce page in the application, the name of the Visualforce page must be the same as the Outbound Screen POP Visual Force Page URL field in the Call Center Definition.

Procedure

1. Navigate to **Setup** > **Build** > **Develop** > **Apex Classes**.
2. Click **New** to create an Apex Class.
3. Add the following lines here:

```
global class VisualForcePOMQueryParamsController {
        public String campaign {get; private set;}
        public String dialedNumber{get; private set;}
```

```
        public String firstName {get; private set;}
        public String lastName {get; private set;}
        public String phone {get; private set;}
        public String timeZone {get; private set;}
        public String email {get; private set;}
        public String zipCode {get; private set;}
        public VisualForcePOMQueryParamsController() {
                campaign =
ApexPages.currentPage().getParameters().get('CampaignName');
                dialedNumber =
ApexPages.currentPage().getParameters().get('Dialed');
                firstName =
ApexPages.currentPage().getParameters().get('First Name');
                lastName =
ApexPages.currentPage().getParameters().get('Last Name');
                phone =
ApexPages.currentPage().getParameters().get('Phone 1');
                timeZone =
ApexPages.currentPage().getParameters().get('Time Zone');
                email =
ApexPages.currentPage().getParameters().get('E-Mail');
                zipCode =
ApexPages.currentPage().getParameters().get('Zipcode
Predefined');
      }
}
```

4. Navigate to **Setup** > **Build** > **Develop** > **Visualforce pages**.
5. Click **New** to create the VisualForce page.
6. Add the following lines here:

```
<apex:page controller="VisualForcePOMQueryParamsController">
   <apex:pageBlock title="Outbound Call Information">
       <style type="text/css">
       .zui-table {
       border: solid 1px #DDEEEE;
       border-collapse: collapse;
       border-spacing: 0;
       font: normal 13px Arial, sans-serif;
```

```
            }
.zui-table thead th {
    background-color: #DDEFEF;
    border: solid 1px #DDEEEE;
    color: #336B6B;
    padding: 10px;
    text-align: left;
    text-shadow: 1px 1px 1px #fff;
}
.zui-table tbody td {
   border: solid 1px #DDEEEE;
   color: #333;
   padding: 10px;
   text-shadow: 1px 1px 1px #fff;
}
</style>
      <table class="zui-table">
           <tr style="background-color: #DDEFEF;">
               <td>Parameter Name</td>
               <td>Parameter Value</td>
           </tr>
            <tr>
               <td>Campaign Name</td>
               <td>{!campaign }</td>
            </tr>
            <tr>
                <td>Customer</td>
                <td>{!dialedNumber}</td>
            </tr>
            <tr>
                <td>First Name</td>
                <td>{!firstName }</td>
            </tr>
            <tr>
```

```
                <td>Last Name</td>
                <td>{!lastName }</td>
            </tr>
            <tr>
                <td>Phone</td>
                <td>{!phone }</td>
            </tr>
            <tr>
                <td>Time Zone</td>
                <td>{!timeZone }</td>
             </tr>
             <tr>
                <td>E-mail</td>
                <td>{!email }</td>
             </tr>
             <tr>
                <td>Zip Code</td>
                <td>{!zipCode }</td>
              </tr>
         </table>

    </apex:pageBlock>
</apex:page>
```

Chapter 4: System maintenance and monitoring

AES - TLink Status

The TLink Status on AES indicates whether the link between AES and CM is active. To check the TLink status, navigate to **AES > Status > Status and Control > TSAPI Service Summary > Tlink Status**.

Note

It is important that the TLink status has a CSTA[-S] value denoting a secure connection as shown in the following figure.

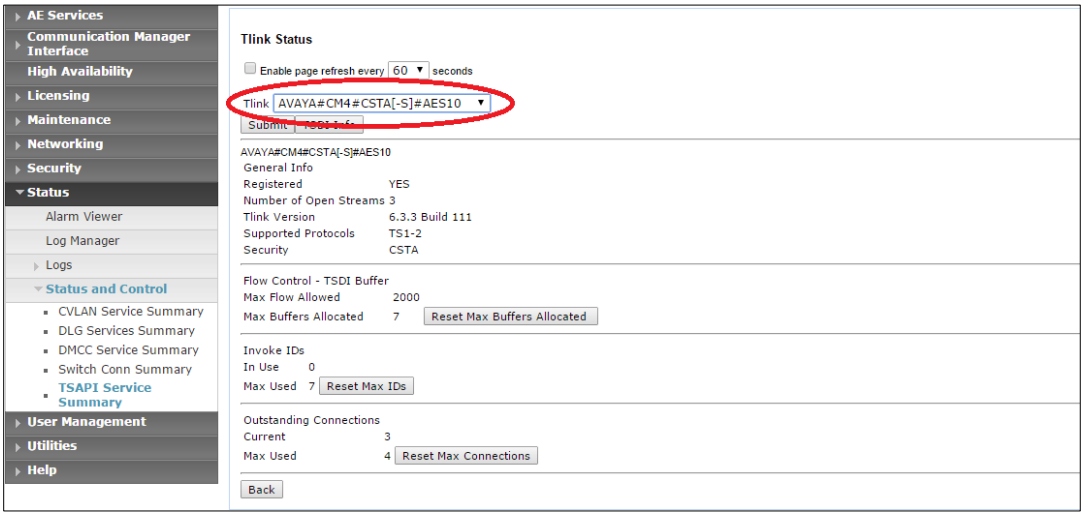

Figure 29: TLink Status

WebLM status

To check the WebLM status, navigate to **Licensing > WebLM Server Address** and check that the WebLM IP address is not set to 127.0.0.1 if the local WebLM is disabled as shown in the following figure:

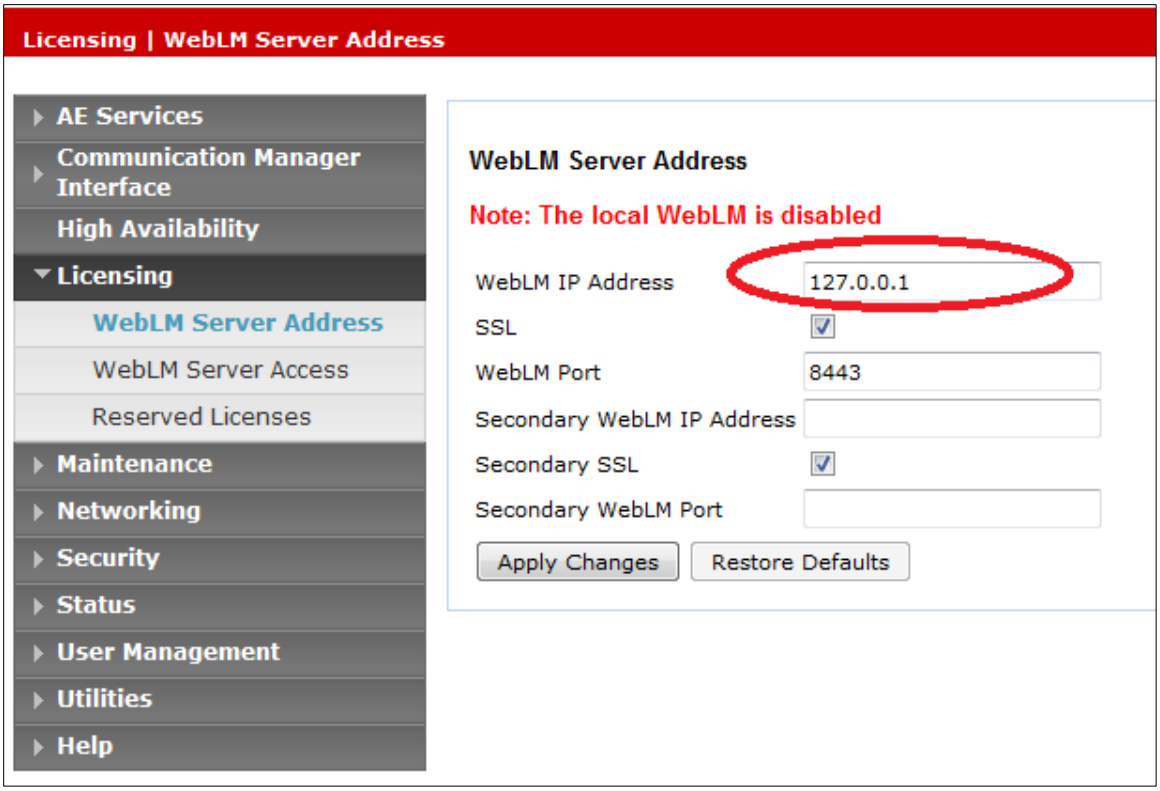

Figure 30: WebLM Server Address

Note

The WebLM IP Address should be administered to a remote location if the local WebLM is disabled.

SIP Endpoints

If a SIP endpoint is registered using an E.164 address, then this will lead to privilege violation exceptions on AES. The SIP endpoints should register using its extension number as configured on Communication Manager.

Appendix A: High Availability and Failover

High Availability and Fault Tolerance

The Avaya CRM Connector 2.1 for Call Center Elite and POM application is implemented as a single node. The scalability and high availability are achieved by deploying multiple nodes deployment without session synchronization among the cluster nodes.

A load balancer must be placed in front of the servers and must be used for distributing the load, monitoring down servers, and redirecting requests to online servers. Thus, you must have at least one additional redundant server in production to allow the solution to continue supporting the load in case one of the servers becomes unavailable.

In the situation where a server faces an issue (for example: network outage), the agent may lose control over the current interactions. When the control is lost the agent must complete the current interactions and start over the login process. In this scenario the load balancer forwards the new login request to another online instance.

To provide geo redundancy, the application needs to be deployed into at least two different sites, this prevents the entire contact center operation to stop due a datacenter outage (for example: power outage, network outage, or communication link outage.

The scalability, the fault tolerance, and disaster recovery will depend on:

- The deployment schema chosen by the customer in accordance with Avaya.
- Load balancers and servers to be provided by the customer.

The scalability, the fault tolerance, and disaster recovery will depend on:

- The deployment schema chosen by the customer in accordance with Avaya.
- POM server’s high availability and fault tolerance
- AES server’s high Availability and fault tolerance
- CM server’s high availability and fault tolerance
- Number of Avaya CRM Connector servers
- Load balancers and servers to be provided

Capacity

A single application instance supports up to 1000 simultaneous logged in agents. Adding new instances increase the capacity in:

```
 ((number of servers -1) * number of agents per server) * (number of
data centers)

 Where number of agents per server = 1000
```

A load balancer must be placed in front of the servers and must be used for distributing the load. Thus, you must have at least one additional redundant server in production to allow the solution to continue supporting the load in case one of the servers becomes unavailable.

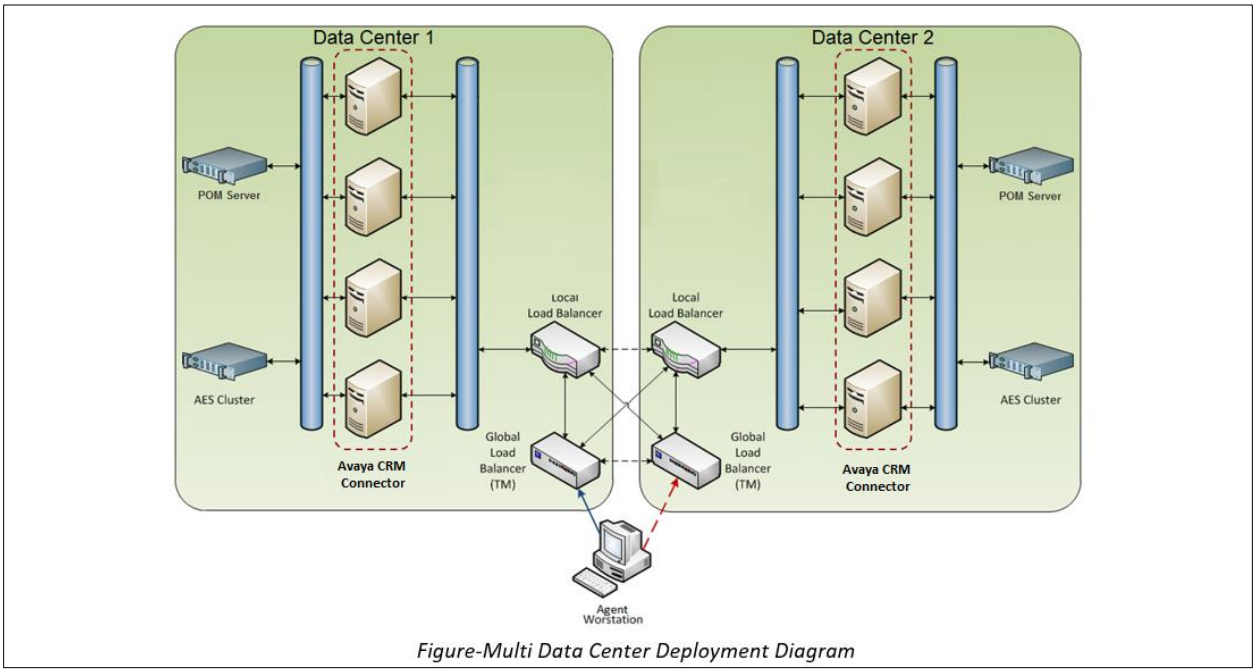

Figure 31: Multi Data Center Deployment Diagram

The Load Balancer depicted in the screenshot is an example of one that has intra-data center and inter-data center balancing features split in to two appliances. Note that, some load balancers perform both features in a single box.

Appendix B: Call Logging

Main scenarios for call logging

The following are the list of main scenarios for call logging in Avaya CRM Connector:

- The call logs are stored on server-side in the session object that refers to a call.
- The Server Start Time is recorded on the Established Event and the End Time on the Release Event.
- The Server Start Time and End Time are based on server's UTC Timestamps.
- The Server Start Time is used to calculate the call log duration.
- The Call Log Duration is calculated from End Date to Server Start Date.
- The Client Start Time is pushed to the server on the Answered Event.
- The Client Start Time is used to reflect the talk time.
- On the client application, the UTC timestamps is displayed in the client's/agent's time zone.

Note:

The timestamps are shared from the server to the client and vice versa in a time format containing values up to milliseconds.

Configuration

The Call Center Definition key value pairs are sent to the server and is stored with the agent's session as soon as the agent log in to the softphone application.

Alternate scenarios

The following are few alternate scenarios for call logs:

- When a call is auto answered, either through CM or IEC (server-side) based on the call center definition, the call log and the call timer will work following the same rules, which is as if the call was manually answer.
- If the **Save Call Log** is set to **N**, then no Information is pushed to the client. Also, the client will not make requests to update the call logs on the server.
- If **Save Incomplete Call** is set to **Y**, then failed and abandoned calls will generate call logs having the Start Time and End Time set to the time the failed event occurred. This will generate a 0-duration call log.

JournalD

JournalD or systemd-journald is a system service that collects and stores logging data. JournalD creates and maintains structured, indexed journals based on the logging information it receives from the various sources.

Avaya CRM Connector leverages Journald log driver for Docker as the default configuration which enables log records to get stored into JournalD.

Journalctl

Journalctl is tool to perform queries on Journal log records. To query logs, use journalctl features, for example: -

```
journalctl -b CONTAINER_NAME=images_aa4salesforce-app_1
```

To know more about the Journalctl tool, view the following links:

- https://docs.docker.com/config/containers/logging/journald/#retrieve-log-messages-with-journalctl
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux_atomic_host/7/html-single/getting_started_with_containers/index

Docker Logs

You can use Docker log commands to see container logs. To query logs, use Docker log features, for example: -

```
docker logs images_aa4salesforce-app_1
```

Appendix C: Troubleshooting

Collecting logs for troubleshooting

- Currently there are two scripts which you can use for troubleshooting:
  - **save-logs.sh:** To save the logs in the integration.log file.
  - **view-logs.sh:** To view the logs on the console.
- You can also run specific Docker commands in case you want some specific information. For instance:-

  `docker logs --since 30m <container ID>`
  This command displays the last 30 minutes of messages for a given container.

Docker services commands

Command	Description
./stop.sh	Use this command to stop a docker service.
./start.sh	Use this command to start a docker service.
docker-compose restart	Use this command to restart a service. You must restart the service in case there are any changes made in the configuration files.
docker –ps	Use this command to view the status of all running services.

Viewing the Docker services individual component logs

To view the individual component logs, you need to navigate to the following locations:

- **docker-compose logs > integration.log**
- **docker-compose logs aes3pcc-app > aes3pcc.log**
- **docker-compose logs iec-app > iec.log**

- **`docker-compose logs pomdriver-app > pomdriver.log`**
- **`docker-compose logs oec-app > oec.log`**

Unable to use the application or open VisualForce page in a lightning mode

If you have a problem using the application in a lightning mode or if you cannot open the VisualForce pages, then you must modify the following file:

`integration/config/git-server/default-config/aa4salesforce-prod.yml`

```
cors:
allowed-origins: "force.com, salesforce.com"
```

Also, you must add their domain in the list.

```
allowed-origins: "force.com, salesforce.com, domain"
```

Appendix D: Resources and Glossary

Resources

The following table lists the documents related to Avaya CRM Connectors. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Use this resource to:	Audience
Avaya Aura® Communication Manager Overview and Specification guide	Understand the key features, the functionalities, and the system requirements of the Avaya Aura® Communication Manager application and the components.	IT Management and support personnel
Avaya Aura® Application Enablement Services Overview and Specification	Gain a high-level understanding of the capabilities of Avaya Aura® Application Enablement Services, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	IT Management and support personnel
Using Avaya CRM Connector 2.1 for Call Center Elite and POM	Understand and use the Avaya CRM Connector 2.1 softphone application	IT Management and support personnel
Avaya Aura® Call Center Elite Multichannel Overview and Specification	Understand the key features, the functionalities, and the system requirements of the *Avaya Aura® Call Center Elite* application.	Sales engineers, Implementation engineers, and System administrators
Avaya Proactive Outreach Manager Overview and Specification	Understand the key features, the functionalities, and the system requirements of the *Avaya Proactive Outreach Manager* application.	Sales engineers, Implementation engineers, and System administrators

Glossary

CTI

Computer Telephony Integration. A technology that integrates the telephone with the computer for managing telephone calls.

Softphone

Software used to make calls over the Internet by using a computer. A softphone functions like a traditional telephone, but without the dedicated hardware, such as telephone cables and phone sets.

Salesforce

An application that manages customer relationships, integrates with other systems, and allows user to build own applications.

ANI

Automatic Number Identification. A display of the calling number so that agents can access information about the caller.