# Avaya Proactive Outreach Manager Integration

Release 3.1.1
Issue 1.1
September 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 in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. 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 or on the express behalf of 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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” 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.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

**Hosted Service**

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA 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, HTTPS://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.

**License types**

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.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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, 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

**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 is the software contained within the list of Heritage Nortel Products located

at https://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 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.

**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.

**Virtualization**

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

**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 products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. 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.

**Service Provider**

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC 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 FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

**Compliance with Laws**

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

**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: https://support.avaya.com or such successor site as designated by Avaya.

**Security Vulnerabilities**

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

**Downloading Documentation**

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

**Contact Avaya Support**

See the Avaya Support website: https://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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

**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

# Contents

# Chapter 1: Introduction

## Purpose

This document provides information on how to deploy Avaya Proactive Outreach Manager with:

- Avaya Aura® Communication Manager
- Avaya Aura® Session Manager
- Avaya Aura® Experience Portal
- Call Management System
- External Application Server
- Avaya Contact Recorder
- Avaya Oceana™ Solution

This document is intended for users who want to integrate Avaya Proactive Outreach Manager with any of these products.

## Change history

| Issue | Date | Summary of changes |
|---|---|---|
| 1.1 | September 12, 2018 | Made structural changes in the document. |

# Chapter 2: New in this release

POM 3.1.1 has the following enhancements:

- Supporting integration with Avaya Oceana™ to provide outbound capabilities by using Avaya Workspaces for Oceana.
- Multiple REST API for configuring the following POM elements:
  - Campaigns: add, update, delete, list, schedule, clone, get campaign details, and search.
  - Contact list: add, update, delete, list, search, list associated attributes, and get contact list ID.
  - Datasource: list, add, edit, delete, schedule, and get details of datasource.
  - Contacts: get system contact ID, search, and list contacts of specific contact list in batches for pagination.
  - Contact strategies: add, import, list, view, delete with ID or name, clone with ID or name, and search.
  - Completion code: add, update, delete, and list.
  - Contact attribute: list, view, add, add in bulk, delete, update, and generate `csv`.
  - Global configuration: edit, list, bulk edit, get with ID, and name.
  - Purge schedule: edit, list.
  - DNC list configuration: list, add, edit, delete DNC lists, and list addresses of specific DNC list.
  - DNC list configuration: list, add, edit, delete DNC groups, associate and de-associate DNC list, and get and update default DNC list for group.
  - Organization: list organizations.
  - Web service: web service for export column attempt data, zones, EPM servers and addressbook.
- Event SDK to do the following:
  - Receive events published to the Apache Kafka server.
  - Connect to the primary POM server.
  - Hide internal communication between components of the POM server.
  - Provide an interface to clients that is easy to understand.
- Enhanced callback management system to do the following:
  - Reassign an existing agent callback to another agent.

  - Change the type of an existing callback.
  - Change the start time of a callback.
  - Edit the agent ID of a callback.
- Enhanced agent productivity system to do the following:
  - Provide a mechanism to set an agent callback. Any agent can handle the callback.
  - Prevent agents who are not ready from blending.
- Supervisor feature to do the following:
  - Assign agents to a supervisor user.
  - Supervisors are able to see and manage agents assigned to them.
  - Users with an Administrator role can see all agents.
  - Users with Org Administrator role can see all agents belonging to an organization.
- Enhanced area code mapping mechanism to support the following:
  - Configure the guard times at time zone and state level by using the basic and advanced area code mapping mechanism. By using the advanced area code configuration, you can add more granular rules related to the guard time configuration. The advanced area code mapping is disabled by default to ensure backward compatibility.
  - Import or export the area code mapping data from or to a `.CSV` file respectively.
  - Configure new state and wireless attributes for each phone number.
- Enhanced Do Not Call(DNC) list management to have the following capabilities:
  - Associate a DNC list to a campaign. The campaign is organized in DNC groups.
  - Select multiple DNC groups per campaign.
  - Apply DNC at campaign level. This option is enabled by default.
  - Provide a check during a preview dial and a redial attempt. The check is optional.
- Provide geo redundancy support by using an MSSQL high availability feature for Avaya Aura® Call Center Elite mode.

POM raises an SNMP Trap after POM database connectivity fails.

Improvements to Answer Machine Detection (AMD) call handling:

Enhanced CCA:

When Enhanced CCA feature is enabled, POM shows the following behavior:

- If no application is configured for an Answer Machine call, POM disconnects that call to avoid an empty message on an answer machine.
- If an agent node is configured for an answer machine, agent is connected at the start of greeting to hear the answer machine recording and can leave appropriate voice mail. POM assigns new job or contact to the agent at the start of greeting to improve agent utilization rather waiting till the end of the greetings.
- If an agent node is configured for an answer human only, then POM assigns a new job or contact to the agent at the start of greeting to improve agent utilization rather than waiting till the end of the greetings.

Improved DTMF handling:

- POM can send DTMF tones initiated by an agent desktop as out of band RFC 2833 DTMF sequence supported only on Experience Portal 7.2.
- “Restrict Agent to receive out-of-band DTMF” – Out of Band DTMF tones can be “blocked” on agent leg of the call, from POM to agent, so that agent cannot hear DTMF inputs of customer. This feature requires an Experience Portal patch or release that supports unidirectional DTMP clamping. Currently unidirectional DTMP clamping is not supported in Experience Portal version 7.2 or earlier versions. For more information on required Experience Portal or Media Processing Platform patch, see POM 3.1.1 release notes.
- “Restrict Customer to send and receive out-of-band DTMF” – Out of Band DTMF tones can be “blocked” on customer leg of the call (both directions).

Improved Email and SMS handling:

- AvayaPOMEmail: can access and process the content of an email body of an incoming customer reply for a two way email campaign.
- AvayaPOMSMS: can process an incoming SMS (customer reply), even if there is a mismatch of phone numbers of sent and received SMS.

  The mismatch is caused due to the following:

  - An SMS dialing prefix added by POM while sending an SMS.
  - An SMS dialing prefix added by the service provider while replying to the received SMS.

# Chapter 3: Configuring Avaya Aura® Communication Manager

## Log in to the Avaya Aura® Communication Manager server

Log in to the Avaya Aura® Communication Manager server and select the SAT terminal type as **SUNT**.

For details on connecting to Avaya Aura® Communication Manager server using Putty, see *Administering Avaya Aura® Communication Manager* document.

## Adding the IP Address of Session Manager

### About this task

Configure Communication Manager to communicate with Session Manager. Add the Session Manager IP address to Communication Manager node-names list.

### Procedure

1. Log in to the Communication Manager system and select the SAT terminal type as **SUNT**.
2. On the SAT session, in the `Command:` prompt, type `change node-names ip` and press `Enter`.

   The system displays the IP NODE Names screen.
3. Use the **up** or **down** arrow key and scroll to a blank line.
4. In the **Name** column, type the name of the Session Manager server.
5. In the **IP address** column, type the IP address of the Session Manager Security Module.

   **Note:**

   Do not use the management IP address in the **IP address** field.

   The IP NODE Names screen displays the information similar to the following:

```
==========================================================================
change node-names ip                                          Page   1 of   2
IP NODE NAMES
Name                 IP Address
```

```
ASM_Server_Name     192.168.1.11
default             0.0.0.0
procr               192.168.1.12
procr6              ::

( 5  of 5  administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
=========================================================================
```

6. Press **F3** key to save the changes.

# Adding an IP address of Call Management System

## About this task

Configure Communication Manager to communicate with Call Management System. Add an IP address of Call Management System to the node-names list of Communication Manager.

## Procedure

1. Log in to the Communication Manager system and select the SAT terminal type as **SUNT**.
2. On the SAT session, in the `Command:` prompt, type `change node-names ip` and press `Enter`.

   The system displays the IP NODE Names screen.
3. Use the **up** or **down** arrow key and scroll to a blank line.
4. In the **Name** column, type the name of the Call Management System.
5. In the **IP address** column, type the IP address of the Call Management System.

   The IP NODE Names screen displays the information similar to the following:

```
=========================================================================
change node-names ip                                      Page   1 of   2
IP NODE NAMES
Name                IP Address
CMS_Server_Name     192.168.1.13
default             0.0.0.0
procr               192.168.1.12
procr6              ::

(5  of 5  administered node-names were displayed)
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
=========================================================================
```

6. Press **F3** key to save the changes.

# Making a connection between Communication Manager and Call Management System

## About this task

To receive the call center data from Communication Manager to Call Management System, you must establish a connection between Communication Manager and Call Management System. Add the communication-interface processor-channels between Communication Manager and Call Management System.

## Procedure

1. Log in to the Communication Manager system and select the SAT terminal type as **SUNT**.
2. On the SAT session, in the `Command:` prompt, type `change communication-interface processor-channels` and press **Enter**.

   The system displays the change communication-interface processor-channels screen similar to the following:

```
=========================================================================
change communication-interface processor-channels       Page   1 of  24
                           PROCESSOR CHANNEL ASSIGNMENT
Proc        Gtwy           Interface Destination     Session      Mach
Chan Enable Appl. To Mode  Link/Chan Node       Port Local/Remote ID
  1:  y     mis     s     pv4 5000   CMS_server 0      1          1
  2:  n
  3:  n                                                           0
=========================================================================
```

3. Use the **up** or **down** arrow key and scroll to a blank line.
4. In the **Enable** column, type `y`.
5. In the **Appl.** column, type `mis`.
6. In the **Mode** column, type `s`.
7. In the **Link/Chan** column, type `pv4 5001` for procr.

   Set the channel value between 5000 to 64500 for Ethernet.
8. In the **Node** column, type the node name of Call Management System.
9. In the **Port** column, type `0`.
10. In the **Local/Remote ID** column, type `1 1`.
11. Press **F3** key to save the changes.

# Creating a signaling-group

## About this task

Create a signaling–group on Communication Manager.

**Note:**

You must create a separate SIP signalling group for BSR polling.

## Procedure

1. On the SAT session, in the `Command:` terminal, type `add signaling-group n` and press `Enter`.

   The system displays the **SIGNALING GROUP** screen.

   The *n* is the signaling-group number.

2. Use the **up** or **down** arrow key and scroll to the **Group Type** option.

3. In the **Group Type** option, type `SIP` and press tab key.

   The **SIGNALING GROUP** screen displays the information similar to the following:

```
==========================================================================
add signaling-group n                                        Page   1 of   1

SIGNALING GROUP

Group Number: 2       Group Type: sip
IMS Enabled? n        Transport Method: tcp
Q-SIP? n              SIP Enabled LSP? n

Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: Others



Near-end Node Name: procr        Far-end Node Name: ASM_SERVER_NAME
Near-end Listen Port: 5060       Far-end Listen Port: 5060
                                 Far-end Network Region:

Far-end Domain:
                                          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? n           Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n    Alternate Route Timer(sec): 6


F1=Cancel F2=Refresh F3=Submit F4=Clr Fld F5=Help F6=Update F7=Nxt Pg F8=Prv Pg
==========================================================================
```

4. Update the following values:

| Group Type | SIP |
|---|---|
| **Transport Method** | TLS or TCP. |

| Group Type | SIP |
|---|---|
| | **Note:**<br>Ensure that you set the same value for transport method while configuring Entity link on Session Manager |
| **Near-end Node Name** | procr<br>**Tip:**<br>This is the Communication Manager node name. |
| **Near-end Listen Port** | An unused port number for the near-end listen port. |
| **Far-end Node Name** | **Tip:**<br>This is the node name configured for Session Manager. |
| **Far-end Listen Port** | An unused port number for the far-end listen port. |
| **Far-end Network Region** | The number of the network region that is assigned to the far-end of the signaling group. The region is used to obtain the codec set used for negotiation of trunk bearer capability. |
| **Far-end Domain** | The name of the IP domain that is assigned to the far-end of the signaling group. |

5. Press **F3** key to save the changes.

# Creating a Trunk group

## Procedure

1. On the SAT session, in the Command terminal, type `add trunk-group n` and press **Enter**.

   Where, *n* is the trunk group number.

   The system displays the **TRUNK GROUP** screen.

2. Use the **up** or **down** arrow key and scroll to the **Group Type** option.

3. In the **Group Type** option, type `SIP` and press the **TAB** key.

   The system displays the **TRUNK GROUP** screen with information similar to the following:

```
==========================================================================
add trunk-group n                                      Page   1 of  22
                        TRUNK GROUP

Group Number: 2              Group Type: sip       CDR Reports: y
Group Name: trunk to ASM     COR: 1        TN: 1        TAC: #2
Direction: two-way        Outgoing Display? n
Dial Access? n                      Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                    Signaling Group: 2
```

```
                                    Number of Members: 255
==============================================================================
```

4. Update the following values:

| | |
|---|---|
| **Group Type** | sip |
| **Signaling Group** | Signaling group<br>**Note:**<br>You must configure the signaling group value that you created earlier. |
| **Number of Members** | The number of ports for this SIP connection. |
| **Service Type** | Tie |
| **TAC** | The trunk access code as per the dial plan. |

5. Press **F7** key to go to the next page.

   There are no changes required on screen 2.

6. Press **F7** key to go to the next page.

   The page 3 of 22, displays the following information:

```
==============================================================================
                                                          Page   3 of  22
TRUNK FEATURES
   ACA Assignment? n            Measured: none
                                   Maintenance Tests? y



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


                              Modify Tandem Calling Number: no
                Send UCID? y

 Show ANSWERED BY on Display? y
==============================================================================
```

7. Update the following values:

| | |
|---|---|
| **UUI Treatment** | This value must be set to *shared*. |
| **Send UCID** | Set to Yes |

8. Press **F3** key to save the changes.

# Creating Hunt group

## Procedure

1. On the SAT session, in the `Command:` terminal, type `add hunt-group` *n* and press **Enter**. The *n* is the hunt group number.

   The system displays the HUNT GROUP screen. Use the **up** or **down** arrow key to scroll.

2. Update the following values:

| | |
|---|---|
| Group Number | Numeric value |
| Group Extension | Extension of the group |
| Group Type | ead-mia<br>Following are the possible values:<br>• ead-mia<br>• ucd-mia<br>• ead-loa<br>• ucd-loa<br>**Note:**<br>Ensure that the Group Type that you configure on the Hunt group screen matches with the agent strategy that you select on the ICR Skill page. |
| ACD? | Y |
| Vector? | Y |
| Queue? | Y |
| Measured | external or both<br>**Note:**<br>In CMS based routing, if you need the agent and skill data, you must set the **Measured** field to `external`. |

The HUNT GROUP screen displays the information similar to the one provided below.

```
==============================================================================
add hunt-group n                                        Page   1 of   4
                                 HUNT GROUP

        Group Number: 1                                   ACD? y
        Group Name: english                             Queue? y
        Group Extension: 2000                          Vector? y
        Group Type: ead-mia
                  TN: 1
                  COR: 1                MM Early Answer? n
        Security Code:                  Local Agent Preference? n
ISDN/SIP Caller Display:

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

```
  Time Warning Threshold:      Port:
================================================================================
```

3. Press **F7** to go to the next page.
4. Use the **up** or **down** arrow key to scroll. Type the value of the parameter skill? as *Y*.

   The HUNT GROUP screen displays the information similar to the one provided below.

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

                Skill? y      Expected Call Handling Time (sec): 180
                  AAS? n        Service Level Target (% in sec): 80 in 20
                Measured: external
   Supervisor Extension:

   Controlling Adjunct: none

     VuStats Objective:
 Timed ACW Interval (sec):
 Multiple Call Handling: none
================================================================================
```

5. Press **F3** to save the changes.

# Adding the IP network region

You must define the authoritative domain name on the IP-network-region form.

## Procedure

1. On the SAT session, in the `Command:` prompt, type `change ip-network-region 1` and press **Enter**.

   The system displays the IP NETWORK REGION screen.
2. Use the **up** or **down** arrow key to scroll.
3. In the first page, provide the following information:
   - Define the Authoritative Domain name.

   The first screen of IP NETWORK REGION displays the information similar to the following:

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

```
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5   AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                   RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
         Keep-Alive Count: 5
=========================================================================
```

4. Press **F3** key to save the changes.

# Adding the IP codec set

You must add the IP codec set in Communication Manager to establish a successful RTP path with the customer.

### Procedure

1. On the SAT session, in the `Command:` prompt, type `change ip-codec-set n` and press `Enter`.

   The *n* is the ip codec set number.

   The system displays the IP Codec Set screen.

2. Use the **up** or **down** arrow key to scroll.

   On the first page, provide the following information:

   - Audio Codec
   - Silence Suppression
   - Frames Per Packet
   - Packet Size in milliseconds

   The system displays the first screen of IP Codec Set with the information similar to the following:

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

                           IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729             n         2        20
 2: G.711A            n         2        20
 3: G.729A            n         2        20
 4: G.711MU           n         2        20
 5:
 6:
```

```
 7:
==========================================================================
```

3. Press the **F3** key to save the changes.

# Chapter 4: Configuring Avaya Aura® Session Manager

You must configure Avaya Aura® Session Manager to work with POM. For more information, see *Administering Avaya Aura® Session Manager* from the Avaya Support site at: http://support.avaya.com.

The following table explains the SIP/Campaign manager requirement for the agent-based and notification campaigns.

**Table 1: Connection Requirement for Campaigns**

| Campaign type | Connection requirement | |
|---|---|---|
| Agent-based | SIP | Campaign manager |
| Voice notification | SIP PROXY | Not required |
| Email notification | Not required | Not required |
| SMS notification | Not required | Not required |

## Adding SIP Entities

### Adding SIP Entity for SIP Gateway or Session Border Controller

**Procedure**

1. Log in to the System Manager interface with the Administration user role.
2. From the System Manager main menu, select **Elements** > **Routing** > **SIP Entities**.
3. On the SIP Entities page, click **New**.
4. On the SIP Entities Details page, do the following:
   a. In the **Name** field, enter the name of the SIP Gateway or Session Border Controller.

      This name must be unique and can have between 3 and 64 characters.

b. In the **FQDN or IP Address** field, enter the fully qualified domain name or IP address of the SIP Gateway or Session Border Controller configured in the signaling–group on Communication Manager.

c. In the **Type** field, click `Gateway`.

d. In the **Notes** field, specify additional notes about the SIP entity.

e. In the **Location** field, click the SIP entity location from the list of previously defined locations.

f. In the **Time Zone** field, click the default time zone to be used for the entity.

g. In the **SIP Timer B / F (in seconds)** field, keep the default value `4`.

h. In the **Minimum TLS Version** field, keep the default value `Use Global Setting`.

5. Click **Commit**.

## Adding SIP Entities for Communication Manager

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. From the System Manager main menu, select **Elements** > **Routing** > **SIP Entities**.
3. On the SIP Entities page, click **New**.
4. On the SIP Entities Details page, do the following:

   a. In the **Name** field, enter the name of the Communication Manager server.

   This name must be unique and can have between 3 and 64 characters.

   b. In the **FQDN or IP Address** field, enter the fully qualified domain name or IP address of the CLAN/Procr configured in the signaling–group on Communication Manager.

   c. In the **Type** field, click `CM`.

   d. In the **Notes** field, specify additional notes about the SIP entity.

   e. In the **Location** field, click the SIP entity location from the list of previously defined locations.

   f. In the **Time Zone** field, click the default time zone to be used for the entity.

   g. In the **SIP Timer B / F (in seconds)** field, keep the default value `4`.

   h. In the **Minimum TLS Version** field, keep the default value `Use Global Setting`.

5. Click **Commit**.

   Perform these steps to create SIP Entities for all the required Communication Manager servers.

## Adding SIP Entity for Avaya Aura® Experience Portal

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. From the System Manager main menu, select **Elements** > **Routing** > **SIP Entities**.
3. On the SIP Entities page, click **New**.
4. On the SIP Entities Details page, do the following:
   a. In the **Name** field, enter the name of the Avaya Aura® Experience Portal server.

      This name must be unique and can have between 3 and 64 characters.

   b. In the **FQDN or IP Address** field, enter the fully qualified domain name or IP address of Media Processing Platform.

      If you have multiple Media Processing Platform, add all Media Processing Platform with a single FQDN under Local Host Name configured.

   c. In the **Type** field, click `Voice Portal`.
   d. In the **Notes** field, specify additional notes about the SIP entity.
   e. In the **Location** field, click the SIP entity location from the list of previously defined locations.
   f. In the **Time Zone** field, click the default time zone to be used for the entity.
   g. In the **SIP Timer B / F (in seconds)** field, keep the default value `4`.
   h. In the **Minimum TLS Version** field, keep the default value `Use Global Setting`.
5. Click **Commit**.

# Adding SIP Entity links

## Adding SIP Entity Link for SIP Gateway or Session Border Controller

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements** > **Routing** > **Entity Links**.
3. Click **New**.

4. On the Entity Links page, do the following:
   a. In the **Name** field, enter the name of the SIP Entity Link for SIP Gateway or Session Border Controller.

      This name must be unique and can have between 3 and 64 characters.
   b. In the **SIP Entity 1** field, select a SIP entity from the drop-down list.

      This entity must always be a Session Manager instance.
   c. In the **Protocol** field, select the protocol for the entity link.
   d. In the **Port** field, enter the port number for SIP Entity 1.
   e. In the **SIP Entity 2** field, select the entity that you created for SIP Gateway or Session Border Controller.
   f. In the **Port** field, enter the port number for SIP Entity 2.
   g. In the **Connection Policy** field, click `trusted` to specify that the link between the two SIP entities is trusted.
   h. In the **Notes** field, specify additional notes about the entity link.
5. Click **Commit**.

## Adding SIP Entity Link for Communication Manager

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, click **Routing** > **Entity Links**.
3. On the System Manager main menu, select **Elements** > **Routing** > **Entity Links**.
4. Click **New**.
5. On the Entity Links page, do the following:
   a. In the **Name** field, enter the name of the Communication Manager server.

      This name must be unique and can have between 3 and 64 characters.
   b. In the **SIP Entity 1** field, select a SIP entity from the drop-down list.

      This entity must always be a Session Manager instance.
   c. In the **Protocol** field, select the protocol for the entity link.
   d. In the **Port** field, enter the port number for SIP Entity 1.
   e. In the **SIP Entity 2** field, select the entity that you created for Communication Manager.
   f. In the **Port** field, enter the port number for SIP Entity 2.
   g. In the **Connection Policy** field, click `trusted` to specify that the link between the two SIP entities is trusted.

h. In the **Notes** field, specify additional notes about the entity link.

6. Click **Commit**.

## Adding SIP Entity Link for Avaya Aura® Experience Portal

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements** > **Routing** > **Entity Links**.
3. Click **New**.
4. On the Entity Links page, do the following:
   a. In the **Name** field, enter the name of the Avaya Aura® Experience Portal server.

      This name must be unique and can have between 3 and 64 characters.
   b. In the **SIP Entity 1** field, select a SIP entity from the drop-down list.

      This entity must always be a Session Manager instance.
   c. In the **Protocol** field, select the protocol for the entity link.
   d. In the **Port** field, enter the port number for SIP Entity 1.
   e. In the **SIP Entity 2** field, select the entity that you created for Media Processing Platform.
   f. In the **Port** field, enter the port number for SIP Entity 2.
   g. In the **Connection Policy** field, click `trusted` to specify that the link between the two SIP entities is trusted.
   h. In the **Notes** field, specify additional notes about the entity link.
5. Click **Commit**.

# Defining Policies and Time of Day

## Adding Routing Policy for Communication Manager

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements** > **Routing** > **Routing Policies**.
3. On the Routing Policies page, click **New**.

   System Manager displays the Routing Policy Details page.

4. In the General area, do the following:
   a. In the **Name** field, enter the name of the routing policy.
   b. In the **Retries** field, enter the number of retries for the destination SIP entity.

      The permissible values are 0-5 and the default value is 0.
5. In the SIP Entity as Destination area, do the following:
   a. Click **Select**.
   b. On the Sip Entities page, select the Communication Manager SIP Entity and click **Select**.
6. In the Time of Day area, do the following:
   a. Click **Add**.
   b. On the Time Ranges page, select the appropriate time range and click **Select**.
7. Click **Commit**.

## Adding Routing Policy for Avaya Aura® Experience Portal

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements** > **Routing** > **Routing Policies**.
3. On the Routing Policies page, click **New**.

   System Manager displays the Routing Policy Details page.
4. In the General area, do the following:
   a. In the **Name** field, enter the name of the routing policy.
   b. In the **Retries** field, enter the number of retries for the destination SIP entity.

      The permissible values are 0-5 and the default value is 0.
5. In the SIP Entity as Destination area, do the following:
   a. Click **Select**.
   b. On the Sip Entities page, select the Avaya Aura® Experience Portal SIP Entity and click **Select**.
6. In the Time of Day area, do the following:
   a. Click **Add**.
   b. On the Time Ranges page, select the appropriate time range and click **Select**.
7. Click **Commit**.

# Dial Patterns

## Adding dial patterns for Avaya Aura® Experience Portal and Communication Manager

### About this task

**Note:**

You must configure a minimum of two dial patterns.

- Pattern to route calls to Experience Portal Manager for incoming calls to Avaya Aura® Experience Portal.
- Pattern to route calls to agents and for polling/queuing VDN's to Communication Manager.

### Procedure

1. Log in to the System Manager interface with the Administration user role.
2. On the System Manager main menu, select **Elements** > **Routing** > **Dial Patterns**.
3. On the Dial Patterns page, click **New**.

   System Manager displays the Dial Pattern Details page.
4. In the General area, do the following:
   a. In the **Pattern** field, enter the dial pattern.

      The pattern can have between 1 and 49 characters.

      The following are the valid formats for pattern types:

      - For regular patterns, [+*#0-9x][0-9x]{0,35}
      - For pattern ranges, [+0-9][0-9]{0,23}[:][+0-9][0-9]{0,23}

        If you specify a pattern range, System Manager disables the **Min**, **Max**, and **Emergency Call** fields.
      - For patterns with Emergency number, [0-9]{0,35}

   b. In the **Min** field, enter the minimum number of digits to match in the dial pattern.
   c. In the **Max** field, enter the maximum number of digits to match in the dial pattern.
   d. In the **SIP Domain** field, select the domain for which you want to restrict the dial pattern.
   e. In the **Notes** field, specify additional information about the dial pattern.
5. In the Originating Locations and Routing Policies area, do the following:
   a. Click **Add**.

      System Manager displays the Originating Location page.

   b. In the Originating Location area, select the originating location.
   c. In the Routing Policies area, select the routing policy.
   d. Click **Select**.
6. Click **Commit**.

# Chapter 5: Configuring Avaya Aura® Experience Portal

## About configuring Avaya Aura® Experience Portal

POM reads the SIP proxy server configuration from the VoIP Connections Web page of Avaya Aura® Experience Portal. POM is a managed application of Avaya Aura® Experience Portal. Therefore, Media Processing Platform (MPP), Speech servers, SMS server, e-mail server and VOIP connections are already configured on Avaya Aura® Experience Portal. To check the configuring details, see the *Avaya Aura® Experience Portal* documentation.

## Adding a SIP connection for Session Manager

### Procedure

1. Log on to the Experience Portal Manager web-page using an account with the Administrator role.
2. In the navigation pane, click **System Configuration** > **VoIP Connections**.
3. On the VoIP Connections page, click the **SIP** tab.
4. Click **Add**.
5. On the Add SIP Connection page, do the following:
   a. In the **Name** field, enter an appropriate name for the SIP connection.
   b. In the **Enable** field, keep the default value `Yes`.
   c. In the **Proxy Transport** field, select `TCP` or `TLS` based on your configuration.
   d. Select on of the following:
      - **Proxy Servers**
      - **DNS SRV Domain**
   e. **(Optional)** If you select **Proxy Servers**, enter the IP address of the Security module of Session Manager in the **Address** field.
   f. **(Optional)** If you select **DNS SRV Domain**, enter the domain name of the DNS server in the **DNS SRV Domain** field.

For example, `abc.com`.

g. In the **SIP Domain** field, enter the domain of Session Manager.

h. In the **Maximum Simultaneous Calls** field, enter the maximum number of calls that this trunk can handle at a time.

6. Click **Save**.

# Chapter 6: Configuring Call Management System

## Configuring Call Management System

### Before you begin

Note down the port number that you configured when making a connection between Communication Manager and Call Management System.

### Procedure

1. Log on to the Call Management System as a root user.
2. At the prompt, type `cmsadm` and press **Enter**.

   The SSH client displays the Call Management System administration menu.
3. To turn off the Avaya CMS service, do the following:
   a. At the prompt, type `8`.
   b. Press **Enter**.
   c. At the prompt, type `2`.
   d. Press **Enter**.
4. After the Avaya CMS service stops, type `cmsadm` and press **Enter**.

   The SSH client displays the Call Management System administration menu.
5. To define a new ACD, do the following:
   a. At the prompt, type `1`.
   b. Press **Enter**.

      The SSH client displays the list of supported versions of the Communication Manager for the ACD.
   c. Type the appropriate choice.

      For the selected Communication Manager, the SSH client starts displaying the parameters for which you must type appropriate values.
   d. Type the appropriate values for the following parameters:
      - **Is Vectoring enabled on the switch**

- **Is Expert Agent Selection enabled on the switch**
- **Does the Central office have disconnect supervision**
- **Type the local port assigned to switch**
- **Type the remote port assigned to switch**
- **Select the transport to the switch**
- **Type switch host name or IP Address**
- **Type switch TCP port number (5001-5999)**
- **Number of splits/skills (0-8000)**
- **Total split/skill members, summed over all splits/skills (0-100000)**
- **Number of shifts (1-4)**
- **Type the start time for the shift 1 (hh:mmXM)**
- **Type the stop time for the shift 1(hh:mmXM)**
- **Number of agents logged into all splits/skills during shift 1 (0-10)**
- **Number of trunk groups (0-2000)**
- **Number of trunks (0-12000)**
- **Number of unmeasured facilities (0-6000)**
- **Number of call work codes (1-500)**
- **Type number of vectors (0-8000)**
- **Type number of VDNs (0-22990)**

After you type the appropriate values for all parameters, the system updates the database with the specified values.

6. At the prompt, type `cmsadm` and press **Enter**.

   The SSH client displays the Call Management System administration menu.

7. To turn on the Avaya CMS service, do the following:
   a. At the prompt, type `8`.
   b. Press **Enter**.
   c. At the prompt, type `1`.
   d. Press **Enter**.

# Verifying the installation and configuration of the CMS rt_socket

## Procedure

1. Log on to the Call Management System as a root user.
2. At the prompt, type `cmsadm` and press **Enter**.

   The SSH client displays the Call Management System administration menu.
3. Press `Enter` till the system displays the main menu of Call Management System.

```
=====================================
 ┌MainMenu──────────────────────────┐
 │ Reports>                         │
 │ Dictionary>                      │
 │ Exceptions>                      │
 │ Agent Administration>            │
 │ Call Center Administration>      │
 │ Custom Reports>                  │
 │ User Permissions>                │
 │ System Setup>                    │
 │ Maintenance>                     │
 │ RT_Socket>                       │
 │ Logout                           │
 │ ;                                │
 └──────────────────────────────────┘
=====================================
```

4. Verify that the following reports are present inside the **Custom Report** > **Real-time** menu.
   - **tvi**: This report is for the skill feeds.
5. Verify that the main menu displays the **RT_Socket** menu.
6. Select the **RT_Socket** menu and press **Enter**.

   The SSH client displays the Rt_Socket Menu screen.

```
================================
 ------ RT_Socket Menu ------

1) Start RT_Socket Interface
2) Stop RT_Socket Interface
3) Check Status
4) Display License Info
5) View Maintenance Log
6) Show Version
7) Change Input Parameters
8) Display Configuration
0) Exit
=============
Choice ==>
================================
```

7. At the prompt, type `8` for the **Display configuration** menu and press **Enter**.
8. Verify that the following columns display the information based on the configuration of the CMS RT_Socket.

| Columns | Description |
|---|---|
| **Session** | The session ID of the rt_socket session. |
| **ACD** | The ACD number from which POM receives the data feed. |
| **Dest IP** | The IP address of the POM system. |
| **Port** | The port number of the POM system. |
| **Report** | The following data feed reports:<br>• **POM** for ACD skills |

9. From the **Sessions** column, note the RT_Socket sessions that you configured with POM.
10. Press **Enter** to return to the RT_Socket menu.
11. Type the choice 3 for the **Check Status** menu and press **Enter**.
12. Verify that the system displays the status of RT_Socket sessions as **running** and **is connected**.

# Chapter 7: Configuring External Application Server

## Configuring External Application Server-Tomcat

### Before you begin

Ensure that you have installed the following:

- Java 7 or 8.
- Tomcat 7 or 8.

  For more information on the Cipher requirements of Java implementation, see *Appendix A*.

### Procedure

1. Copy the `*.war` files from `$POM_HOME/DDapps` to `<APPSERVER_HOME>/webapps` of the application server to the `$APPSERVER_HOME/lib/` folder.
2. Copy files from `$POM_HOME/DDapps/lib/*` to `<APPSERVER_HOME>/lib` of the application server to the `$APPSERVER_HOME/lib/` folder.
3. Edit `<APPSERVER_HOME>/conf/server.xml` and add the following connector node:

```
<<!-- <Connector port="7080" protocol="HTTP/1.1"
URIEncoding="UTF-8" useBodyEncodingForURI="true"
connectionTimeout="20000" redirectPort="7443" />-->
<!-- ....CHANGES for AVAYA POM START .... --> <Connector
protocol="HTTP/1.1" port="7443" minSpareThreads="5"
maxSpareThreads="75" enableLookups="true"
disableUploadTimeout="true" acceptCount="100" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true" keystoreFile="/opt/
AppServer/Tomcat/tomcat/conf/myTrustStore" keystorePass="changeit"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH
_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDH_ECDSA_
WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_DH
E_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,T
LS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_
SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SH
A,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SH
A,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC
```

```
_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_
CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH
_AES_128_CBC_SHA256,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS
_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_E
CDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH
_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_D
HE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_EM
PTY_RENEGOTIATION_INFO_SCSV"/>
```

4. Edit `<APPSERVER_HOME>/bin/catalina.sh` file to append the *JAVA_OPTS* variable `export JAVA_OPTS="$JAVA_OPTS -Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2″`. If it is not defined, then declare new *JAVA_OPTS* variable `export JAVA_OPTS="-Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2"`.
5. Restart the external application server.

# Exchanging and configuring certificates

### About this task

Use this procedure to exchange and configure certificates for Avaya Aura® Orchestration Designer on a single or multiple application servers.

**Important:**

For multiple application servers, repeat all steps for each application server.

### Before you begin

Configure the POM database.

### Procedure

1. Using the browser window, log in to the EPM as an administrator.

   **Note:**

   For multiple POM servers, log in to the primary EPM.
2. In the navigation pane, click **Security** > **Certificates**.
3. On the **Root Certificates** tab, click **Export**, and then save the certificate on the local system.
4. In the navigation pane, click **POM** > **POM Home**.
5. Click **Configurations** > **POM Servers**.
6. Click **Export** on the listed certificate tab and save it on your local system.

**Note:**

For multiple POM servers, you must export and save all the POM certificates.

7. If you are using external application server, install the Avaya Aura® Orchestration Designer application server on the same server where you install POM. In such cases the IP address of the application server and the IP address of the EPM primary server is the same. The default port is 7443. while installing POM, you must:
   a. Copy the `*.war` files from `$POM_HOME/DDapps` to `$APPSERVER_HOME/webapps` of the external application server.
   b. Copy files from `$POM_HOME/DDapps/lib/*` to `$APPSERVER_HOME/lib` of your external application server. After copying the files, edit `$APPSERVER_HOME/conf/server.xml` and add the following:

```
<Connector protocol="HTTP/1.1"
port="7443" minSpareThreads="5" maxSpareThreads="75"
enableLookups="true" disableUploadTimeout="true"
acceptCount="100"  maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="/opt/AppServer/Tomcat/tomcat/conf/myTrustStore"
keystorePass="changeit"
clientAuth="false" sslEnabledProtocols="TLSv1.2"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_C
BC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
384,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_
ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WI
TH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256
_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SH
A256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA256,TL
S_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS
_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_ECDH
E_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_
AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128
_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TL
S_EMPTY_RENEGOTIATION_INFO_SCSV"/>
```

   c. In the Command Line Interface (CLI), navigate to `$APPSERVER_HOME/conf`.
   d. Run the command **`keytool -keystore myTrustStore -genkey -alias dummy`**.
   e. Type the password as `changeit` and type of other appropriate details.
   f. Restart the external application server.
8. Using the browser window, log in to the Avaya Aura® Orchestration Designer application server by specifying the URL *https://<application server IP address>:port number/runtimeconfig* using the default user name and the password as *ddadmin*.

   The system prompts to set runtimeconfig password at the first login to the local application server.
9. On the Avaya Aura® Orchestration Designer web interface, do the following:
   a. In the navigation pane, Click **Certificates**.

b. On the Certificates page, select the default certificate and click **Delete**.

c. Click **Change**.

   The system displays Change Keystore page.

d. In the `Ketstore Path` field, type *`Absolute-path appserver-home>/conf/myTrustStore`*.

   If you have installed the application server on the same server where you install POM, then the *<Absolute-path-appserver-home>* is set in the *{$APPSERVER_HOME}* environmental variable.

e. In the **Password** field, type `changeit`.

   **Note:**

   To use a different trust store and the password, change the *Absolute-path-appserver-home>/conf/server.xml* file accordingly, and ensure that the *server.xml* keystore path is valid and matches with Avaya Aura® Orchestration Designer application certificate as *<Absolute-pathappserver-home>/conf/myTrustStore.*

f. In the **Confirm** field, type `changeit`.

g. Click **Save**.

h. On the Certificates page, click **Generate**.

i. Enter the appropriate values in all fields. Input for all fields is mandatory. You can enter any custom defined values.

   **Note:**

   For SAN field, enter the values in the `IP:<IP address> or DNS:<hostname>` format.

   The self-signed certificate is valid only for 1186 days.

j. Click **Continue**.

   The system displays the Certificates page.

k. Click **Save**.

l. Click **Add**.

   The system displays the Add Certificate page.

m. Type a name for the EPM certificate and browse to find the path where you saved the primary EPM root certificate exported in step 3.

n. Click **Continue**.

   The system displays the Certificates page.

o. Click **Save**.

p. Select the application server self-signed certificate generated and export the certificate on your local system.

q. Click **Fetch** to fetch the axis2 certificate for primary EPM.

   The system displays the Add Certificate page.

   **Note:**

   In a multiple POM server environment, you must fetch the axis2 certificate from all auxiliary EPM servers.

r. In the **Name** field, type the name of the certificate. For example, axis_prim or axis_aux.

s. In the **Enter Certificate Path** field, type the client URL as *https://<EPM IP address>/axis2*

   The Avaya Aura® Orchestration Designer application fetches the axis2 certificate and adds it to the list of certificates.

t. Click **Continue**.

   The system displays the Certificates page.

u. Click **Save**.

a. Click **Add**.

   The system displays the **Add Certificate** page.

b. In the **Name** field, type a name of the POM certificate.

c. In the **Enter Certificate path** field, click **Browse** and browse the path where you saved the certificate exported in the step 6.

d. Click **Continue**.

   The system displays the Certificates page.

e. Click **Save**.

f. Restart the application server.

10. Using the browser window, log in to the primary EPM as administrator.

11. Click **Security** > **Certificates**.

12. Click the **Trusted Certificates** tab and do the following:

    a. Click **Upload**.

    b. On the Upload Trusted Certificate page, type the name and browse the path where you saved the exported Avaya Aura® Orchestration Designer certificate.

    c. Click **Continue**.

       The system displays the Certificates page.

    d. Click **Save**.

    e. Click **Import**.

       The system displays the Import Trusted Certificate page.

f. On the Import Trusted Certificate page, type the name and type the axis2 certificate path as *https://<EPM Server IP address>/axis2*.

   For a multiple POM server environment, you must fetch the axis2 certificate from all auxiliary EPM servers.

g. Click **Continue**.

   The system displays the Certificates page.

h. Click **Save**.

13. Restart the application server, all MPPs, and all auxiliary servers.

# Configuring External Application Server- WebSphere

### About this task

Use this procedure to configure the WebSphere application server to work with POM.

### Before you begin

- Copy `runtimesupportWebsphere.zip` from `$POM_HOM//DDapps/WebSphere files` to the `$WS_HOME\AppServer\lib\ext folder`.
- Restart WAS server through `services.msc` or its UI tools.
- Ensure that you have installed the following:
  - Java 7 or 8.
  - WebSphere 8.5.5 or above.

  For more information on the Cipher requirements of Java implementation, see *Appendix A*.

### Procedure

1. In the navigation pane, select **Application** > **Application type** > **WebSphere enterprise applications** and browse **WebSphere enterprise applications**.
2. On Specify the EAR, WAR, JAR, or SAR module to upload and install page, browse and upload `runtimeconfig.ear` from the local system.
3. Click **Next**.
4. Select **Show me all installation options and parameters**.
5. Click **Next**.

   The system displays the resulting security warnings from an analysis of this application.
6. Click **Continue**.
7. On the Select installation options page, select **Precompile JavaServer Pages files** and retain the other default values.
8. Click **Next**.

9. On the Map modules to servers page, select the **runtimeconfig.ear**.
10. Click **Next**.
11. On the Choose to generate default bindings and mappings page, click **Next**.
12. On the Map modules to servers page, select **runtimeconfig.ear**.
13. Click **Next**.
14. On the Provide options to compile JSPs page, select **runtimeconfig.ear, WEB-INF/web.xml**
15. In the **JDK Source Level**, type `15`.
16. Click **Next**.
17. On the Provide JSP reloading options for Web modules page, click **Next**.
18. On the Map shared libraries page, click **Next**.
19. On the Map virtual hosts for Web modules page, select **runtimeconfig.ear**.
20. Click **Next**.
21. On the Map context roots for Web modules page, click **Next**.
22. On the Summary page, click **Finish**.
23. Click **Save**.

    **Caution:**

    Make sure you verify that all the configuration has been saved.
24. Restart the application server.

### Next steps

Verify if you can access POM OD runtime.

1. To login browse `http://<App server IP :<port number>/runtimeconfig/login.jsp`
2. Type username and password as `ddadmin`.
3. Navigate **Home** > **Certificates** > **Change Keystore**, and define keystore path as `C:\Program Files\IBM\WebSphere\AppServer\lib\ext\myTrustStoreNew`.
4. Type the password as `changeit`.

# Configuring External Application Server- WebSphere version 8.5.5

### About this task

Use this procedure to configure Websphere version 8.5.5 and later with POM.

### Before you begin

On the POM server, enable **Mutual Certification Authentication** for email and SMS.

### Procedure

1. On IBM Console, select **Environment** > **Shared libraries**.
2. On the Shared Libraries page, select the appropriate **Scope** from the drop-down.
3. Click **New**.
4. Define a name for the newly created shared library.
5. In the **Classpath** field, paste the following entries:

| For Linux | For Windows |
|---|---|
| ${WAS_INSTALL_ROOT}/lib/ext/axiom-api-1.2.13.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axiom-dom-1.2.13.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axiom-impl-1.2.13.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axis2-adb-1.6.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axis2-adb-codegen-1.6.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axis2-json-1.6.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axis2-kernel-1.6.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axis2-saaj-1.6.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axis2-transport-http-1.6.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/axis2-transport-local-1.6.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/neethi-3.0.2.jar<br>${WAS_INSTALL_ROOT}/lib/ext/woden-api-1.0M9.jar<br>${WAS_INSTALL_ROOT}/lib/ext/woden-impl-dom-1.0M9.jar<br>${WAS_INSTALL_ROOT}/lib/ext/woden-tool-1.0M9.jar<br>${WAS_INSTALL_ROOT}/lib/ext/XmlSchema-1.4.7.jar<br>${WAS_INSTALL_ROOT}/lib/ext/VPWebServiceClient-1.0.jar<br>${WAS_INSTALL_ROOT}/lib/ext/VPAppLogClientWS_x.0.0.jar | $WAS_HOME\AppServer\lib\ext\axiom-api-1.2.13.jar<br>$WAS_HOME\AppServer\lib\ext\axiom-dom-1.2.13.jar<br>$WAS_HOME\AppServer\lib\ext\axiom-impl-1.2.13.jar<br>$WAS_HOME\AppServer\lib\ext\axis2-adb-1.6.2.jar<br>$WAS_HOME\AppServer\lib\ext\axis2-adb-codegen-1.6.2.jar<br>$WAS_HOME\AppServer\lib\ext\axis2-json-1.6.2.jar<br>$WAS_HOME\AppServer\lib\ext\axis2-kernel-1.6.2.jar<br>$WAS_HOME\AppServer\lib\ext\axis2-saaj-1.6.2.jar<br>$WAS_HOME\AppServer\lib\ext\axis2-transport-http-1.6.2.jar<br>$WAS_HOME\AppServer\lib\ext\axis2-transport-local-1.6.2.jar<br>$WAS_HOME\AppServer\lib\ext\neethi-3.0.2.jar<br>$WAS_HOME\AppServer\lib\ext\woden-api-1.0M9.jar<br>$WAS_HOME\AppServer\lib\ext\woden-impl-dom-1.0M9.jar<br>$WAS_HOME\AppServer\lib\ext\woden-tool-1.0M9.jar<br>$WAS_HOME\AppServer\lib\ext\XmlSchema-1.4.7.jar<br>$WAS_HOME\AppServer\lib\ext\VPAppLogClientWS_x.0.0.jar<br>$WAS_HOME\AppServer\lib\ext\VPWebServiceClient-0x.00.00.01.jar |

6. Click **Apply**.
7. Save the changes into the Master Configuration.
8. On IBM Console, select **Servers** > **Server Types** > **WebSphere application servers**.

   The system displays the Application Servers page.
9. On the right pane, select **Server Infrastructure** > **Java and Process Management** > **Class Loader**.

10. Click **New**.
11. Select **Classes loaded with local class loader first (parent last)** from the drop-down menu.
12. Click **Apply**.

    On the Configuration page, the system displays the `shared library reference` link.

    **Note:**

    Save the changes into the Master Configuration.
13. Click `shared library reference` link.
14. Click **Add**.

    The system displays the list of all the shared libraries.
15. Select **Servers** > **Server Types** > **WebSphere application servers** > **<Server_name>**.
16. On the Server Infrastructure page, select **Java and process management** > **Process definition** > **Java virtual machine**.
17. In the **Generic JVM arguments** field, type `Dorg.xsocket.connection.client.ssl.sslengine.enabledProtocols=TLSv1.2`.
18. Retain all the other default values.
19. Click **Apply**.
20. Click **Save**.

    **Caution:**

    Make sure you verify all the configuration has been saved.
21. WebSphere requires additional configurations to enforce communication over TLSv1.2. for both incoming and outgoing connections. For more information, see Configuring TLSv1.2 on Websphere on page 74.
22. Restart the application server.

### Next steps

Verify if you can access POM OD runtime.

1. In your web browser, enter the following URL:

   `http://<App server IP :<port number>/runtimeconfig/login.jsp`
2. Type the username and password as `ddadmin`.
3. Navigate to **Home** > **Certificates** > **Change Keystore** and define the keystore path as `C:\Program Files\IBM\WebSphere\AppServer\lib\ext\myTrustStoreNew`.
4. Type the password as `changeit`.

# Exchanging and configuring certificates for WebSphere application server

## About this task

Use this procedure to exchange and configure certificates on a single, or multiple application servers.

**Important:**

For multiple application servers, repeat all steps for each application server.

## Before you begin

Configure the WebSphere application server to work with POM.

## Procedure

1. Using the browser window, log in to the WAS web console as an administrator.
2. Select **Security** > **SSL certificate and key management** > **Key stores and certificates**.
3. Fill the mandatory details and click **OK**.

   The system displays **myTrustStore** on the SSL certificate and key management page.
4. Select **myTrustStore** > **Signer Certificates**.

   The system displays the root certificated generated by WAS.
5. Select the **Root Certificate** tab and click **Extract** and save the certificate to your local system.
6. Type a file name where this certificate will be extracted
7. Using the browser window, log in to the primary EPM as administrator.

   **Note:**

   In case of multiple POM servers, that is, primary or auxiliary, log in to the primary EPM.
8. Select **Security** > **Certificates** > **Upload Trusted Certificate**.
9. On the **Upload Trusted Certificate** tab, specify the name and browse to the path where you save the certificate extracted in the step 5.

   WAS does not provide option to configure the SAN in its self signed/ root certificates. Hence the you must do the following:

   a. Navigate to **POM Home** > **System Configurations** > **Applications**.
   b. Configure POM application URL using host name of the Application Server on `https://<IP address>/VoicePortal/faces/home.jsf`
   c. For the host name resolution, add the entry of the Application Server on EP/MPP and vice versa.
10. Import the axis2 certificate.

11. Select **Security** > **Certificates** > **Import Trusted Certificate**.
12. On the **Root Certificate** tab, click **Export** and save the certificate to your local system.

    **Note:**

    The name of the file is `sipCA.pem`.
13. On the navigation pane, select **POM** > **POM Home**.
14. From the drop-down menu, select **Configurations** > **POM Servers**.
15. Click **Export** on the listed certificate tab and save it on your local system.

    **Note:**

    If you have a multiple POM servers, you must export and save all the POM certificates.
16. On the WAS web console, select **Security** > **SSL certificate and key management** > **Key stores and certificates** > **myTrustStore** > **Personal certificates**.
17. Fill the mandatory details and click **OK**.

    A common name must be hostname of the WAS system.
18. Click **Extract** save the certificated generated in above step to your local system.
19. On EPM, **Trusted Certificates**, tab, upload the certificated saved in the step 18.
20. On the OD runtimeconfig application utility, select **Home** > **Certificates**.
21. Click **Change** and type the path of the keystore to point to **myTrustStore** generated in the step 1.
22. On the **Fetch Certificate** tab, fetch the axis 2 certificate.
23. On the **Add Certificate** tab, click **Add** and upload the sipCA certificate that you saved in step 12.
24. Type a name for the POM certificate and browse to the path where you saved the certificate exported in step 15.
25. Click **Save**.

    **Note:**

    Install all POM applications one by one using detailed option and repeat steps used for deploying `runtimeconfig.ear` file.
26. On the WAS system, in POM Nailer application select data directory . Open `WASConfig.properties` file and provide location of the `keystoreFile` and `keystorePass`.
27. Repeat these steps for POM Driver application.
28. Restart MPP, WAS, and POM Agent Manager.

# Chapter 8: Configuring Avaya Contact Recorder

## Adding ACR configuration on CM

### Verify the Communication Manager license

#### Procedure

1. Log in to the Communication Manager system and select the SAT terminal.
2. On the SAT session, in the Command prompt, type `display system-parameters customer-options` and press `Enter`.
3. Navigate to page 3.
4. Verify that the **Computer Telephony Adjunct Links** customer option is set to **Y**.

   The OPTIONAL FEATURES screen on page 3 displays the information similar to the following:

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? y               Authorization Codes? y
        Analog Trunk Incoming Call ID? y                         CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                           CAS Main? n
Answer Supervision by Call Classifier? y                     Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                  ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? y                       DCS (Basic)? y
          ASAI Link Core Capabilities? y                 DCS Call Coverage? y
          ASAI Link Plus Capabilities? y                DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                            DS1 MSP? y
                                  ATMS? y             DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

5. Navigate to page 4.
6. Verify that the **Enhanced Conferencing** customer option is set to **Y**.

The OPTIONAL FEATURES screen on page 4 displays the information similar to the following:

```
display system-parameters customer-options                      Page   4 of  11
                                OPTIONAL FEATURES

   Emergency Access to Attendant? y                             IP Stations? y
            Enable 'dadmin' Login? y
            Enhanced Conferencing? y                       ISDN Feature Plus? n
                  Enhanced EC500? y        ISDN/SIP Network Call Redirection? y
    Enterprise Survivable Server? n                          ISDN-BRI Trunks? y
       Enterprise Wide Licensing? n                                 ISDN-PRI? y
              ESS Administration? y               Local Survivable Processor? n
          Extended Cvg/Fwd Admin? y                    Malicious Call Trace? y
     External Device Alarm Admin? y                 Media Encryption Over IP? y
  Five Port Networks Max Per MCC? n     Mode Code for Centralized Voice Mail? n
                Flexible Billing? n
   Forced Entry of Account Codes? y                 Multifrequency Signaling? y
      Global Call Classification? y         Multimedia Call Handling (Basic)? y
             Hospitality (Basic)? y      Multimedia Call Handling (Enhanced)? y
 Hospitality (G3V3 Enhancements)? y               Multimedia IP SIP Trunking? y
                        IP Trunks? y

           IP Attendant Consoles? y
```

7. If any option specified in this section does not have a proper value, contact the Avaya sales team or business partner for a proper license file.

# Administering CTI link for TSAPI

## Procedure

1. On the SAT session, in the Command terminal, type `add cti-link n`, where n is the CTI link number from 1 to 64.
2. Press `Enter`.

   The system displays the CTI Link screen.
3. Type the available extension number in the **Extension** field.

   **Note:**

   CTI link number and extension number may vary.
4. In the **Type** field type, `ADJ-IP`.
5. In the **Name** field type the descriptive name.
6. Save the changes.

## Creating Universal Call ID (UCID)

### Procedure

1. On the SAT session, in the command terminal type, `change system-parameters features`.
2. Navigate to page 5.
3. Update the following values:

| | |
|---|---|
| **Create Universal Call ID (UCID)** | Y |
| **UCID Network ID** | Enter an available node ID |

4. Navigate to page 13.
5. In **Send UCID to ASAI** type, `Y`.

   **Note:**

   This parameter allows for the universal call ID to be sent to Avaya Contact Recorder (ACR).

6. Save the changes.

## Administering Class of Restriction (COR)

### Procedure

1. On the SAT session, in the Command terminal, type `change cor n`, where n is the class of restriction (COR) number to be assigned to the target stations and virtual IP softphones.
2. Press `Enter`.
3. Set the **Calling Party Restriction** field to `none`.

   The CLASS OF RESTRICTION screen displays the information similar to the one provided below.

```
change cor 1                                                    Page   1 of  23
                              CLASS OF RESTRICTION
               COR Number: 1
          COR Description:

                      FRL: 0                                 APLT? y
  Can Be Service Observed? y           Calling Party Restriction: none
Can Be A Service Observer? y            Called Party Restriction: none
        Time of Day Chart: 1       Forced Entry of Account Codes? n
         Priority Queuing? n                Direct Agent Calling? y
     Restriction Override: none       Facility Access Trunk Test? n
     Restricted Call List? n                 Can Change Coverage? n

            Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7            Hear VDN of Origin Annc.? n
         Send ANI for MFE? n             Add/Remove Agent Skills? n
            MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? n
                         Can Be Picked Up By Directed Call Pickup? n
                                     Can Use Directed Call Pickup? n
                                     Group Controlled Restriction: inactive
```

4. Save the changes.

# Administering Agent Stations

## About this task

Configure physical stations used by the POM agents to allow the station to be involved in an outbound call using Class of Restriction (COR).

## Procedure

1. On the SAT session, in the Command terminal, type `change station n`, where n is the station extension.
2. Press `Enter`.

   The system displays the change station screen.
3. In **COR** field, type `1`.

   **Caution:**

   Make sure that the **Name** field is populated with the name of the station; else Avaya Contact Recorder reports an error and no recording is done.
4. Save the changes.

# Administering Codec Set

## Procedure

1. On the SAT session, in the Command terminal, type `change ip-codec-set n`, where n is the codec set for the virtual IP softphones.

2. Press `Enter`.

   The system displays the codec set screen.

3. Update the following values:

| Audio Codec | Frames Per Packet |
|---|---|
| G.729A<br>**Note:**<br>Avaya Contact Recorderuses G.729A recording format in the test configuration. | 6 |
| G.711MU | 6 |

4. Retain the values of other fields.

   The IP Codec Set screen displays similar to the one provided below:

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

                           IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A            n         6        20
 2: G.711MU           n         6        20
 3: G.711A            n         6        20
 4:
 5:
 6:
 7:

     Media Encryption
 1: none
 2:
 3:
```

5. Save the changes.

# Administering Network Region

## About this task

Configure the network region for the virtual IP softphones.

## Procedure

1. On the SAT session, in the Command terminal, type `change ip-network-region n`, where n is the network region.
2. Press `Enter`.

   The system displays the IP Network Region Link screen.

3. Type the **Codec Set** field values as added in the *Administer Codec Set*.

   The IP NETWORK REGION screen displays similar to the one provided below:

```
change ip-network-region 1                                      Page   1 of  20
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: sol002.fst.silpunelab.com
    Name: CM1A                  Stub Network Region: n
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

4. Save the changes.

# Administering Virtual IP Softphones

## About this task

Configure Virtual IP Softphones to conference into calls involving target stations and to capture media.

## Procedure

1. On the SAT session, in command terminal type, `add station n`, where n is the available extension number.
2. Update the following values:

| | |
|---|---|
| Type | 4624 |
| Name | Enter a descriptive name |
| Security Code | Enter a desired value |
| COR | 1 |
| IP SoftPhone | Y |

**Note:**

Retain the default values for the remaining fields.

The STATION screen displays similar to the one provided below:

```
add station 3011450                                          Page   1 of   6
                                     STATION

Extension: 301-1450                     Lock Messages? n               BCC: 0
     Type: 4624                         Security Code: 123456           TN: 1
     Port: S00009                     Coverage Path 1:                 COR: 1
     Name: Avaya Contact Recorder Test 1                  Coverage Path 2:
COS: 1
                                      Hunt-to Station:               Tests? y
STATION OPTIONS
                Location:                 Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 301-1450
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? y

                                             IP Video Softphone? n
                              Short/Prefixed Registration Allowed: default
```

3. Navigate to page 4.
4. In **BUTTON ASSIGNMENT 4** field, type `conf-dsp`.
5. Clear the **BUTTON ASSIGNMENT 3** field.

```
change station 3011450                                       Page   4 of   6
                                     STATION
 SITE DATA
       Room:                                            Headset? n
       Jack:                                            Speaker? n
      Cable:                                           Mounting: d
      Floor:                                       Cord Length: 0
   Building:                                         Set Color:

ABBREVIATED DIALING
     List1:                    List2:                    List3:




BUTTON ASSIGNMENTS
 1: call-appr                           7:
 2: call-appr                           8:
 3:                                     9:
 4: conf-dsp                           10:
 5:                                    11:
 6:                                    12:
```

**Note:**

Repeat the above steps to administer the desired number of virtual IP softphones, using sequential extension numbers and the same security code for all virtual IP softphones.

6. Save the changes.

## Assigning Virtual IP Softphones to Network Region

### About this task

Add the IP address of the Application Enablement Services server to the network region.

### Procedure

On the SAT session, in the Command terminal, type `change ip-network-map`.

As all the virtual IP softphones register through the Application Enablement Services server, they are automatically assigned to that network region.

```
change ip-network-map                                          Page   1 of  63
                              IP ADDRESS MAPPING

                                                  Subnet Network     Emergency
 IP Address                                       Bits   Region VLAN Location Ext
 ---------------------------------------------- ------ ------ ---- -------------
 FROM: x.x.x.x                              /       1      1
   TO: x.x.x.x
```

### Next steps

Run the `save translation` command to save changes.

# Configuring AES for ACR

## Administering TSAPI Link

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **AE Services** > **TSAPI** > **TSAPI Links**.

   The system displays the **TSAPI Links** page.
3. Click **Add Link**.

   The system displays the **Add TSAPI Links** screen.
4. In the **Link** filed, enter local available numeric value.
5. From the **Switch Connection** drop-down list, select relevant switch connection.
6. From the **Switch CTI Link Number** drop-down list, select CTI link number that you configured in the section AdministeringCTILinkForTSAPI on page 48.

**Note:**

Retain the default values in the remaining fields.

7. Click **Apply Changes**.

## Obtaining Tlink Name

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **Security** > **Security Database** > **Tlinks**.

   A new Tlink name is automatically generated for the TSAPI service.
3. Locate the Tlink name associated with the relevant switch connection.

## Obtaining H.323 Gatekeeper IP Address

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **Communication Manager Interface** > **Switch Connections**.

   The system displays a listing of the existing switch connections on the **Switch Connections** page.
3. Locate the **Connection** name associated with the relevant Communication Manager.

## Disabling Security Database

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **Security** > **Security Database** > **Control**.

   On the right pane, system displays the **SDB Control for DMCC, TSAPI, JTAPI and Telephony Web Services** screen.
3. Uncheck the following fields:
   - **Enable SDB for DMCC Service**
   - **Enable SDB TSAPI Service**
   - **TAPI and Telephony Service**
4. Click **Apply Changes**.

## Restarting TSAPI Service

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **Maintenance** > **Service Controller**.

   In the right pane, the system displays the **Service Controller** screen.
3. Select the **TSAPI Service**.
4. Click **Restart Service**.

## Administering Avaya Contact Recorder User for DMCC

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **User Management** > **User Admin** > **Add User**.

   In the right pane, the system displays the **Add User** screen.
3. Enter the desired values in the following field:
   - **User Id**
   - **Common Name**
   - **Surname**
   - **User Password**
   - **Confirm Password**
4. From the **CT User** drop-down list, select **Yes**.
5. Retain the default value in the remaining fields.
6. Click **Apply**.

## Administering Avaya Contact Recorder User for TSAPI

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **User Management** > **User Admin** > **Add User**.

   In the right pane, the system displays the **Add User** screen.
3. Enter the desired values in the following field:
   - **User Id**

- **Common Name**
- **Surname**
- **User Password**
- **Confirm Password**

4. From the **CT User** drop-down list, select **Yes**.
5. Retain the default value in the remaining fields.
6. Click **Apply**.

## Verifying Avaya Aura® Application Enablement Services

### Procedure

1. Log in to the Application Enablement Services interface with the Administration user role.
2. In the left navigation pane, click **Status** > **Status and Control** > **DMCC Service Summary**.

   In the right pane, the system displays the **DMCC Service Summary – Session Summary** screen.
3. Verify that an active session with the user name configured in the section *Administer Avaya Contact Recorder User for DMCC* is present.
4. Verify that in the **# of Associated Devices** column reflects the number of virtual IP softphones used by Avaya Contact Recorder.
5. In the left navigation pane, click **Status** > **Status and Control** > **TSAPI Service Summary**.

   In the right pane, the system displays the **TSAPI Link Details** screen.
6. Verify that in the **Status** column reflects the status as **Talking**.

# Configuring POM

## Enabling WFO integration

### Before you begin

Enable the Avaya Contact Recorder port on the POM server.

### Procedure

1. Log on to the POM interface by using a web browser and an administrator user role.

2. In the navigation pane, click **POM** > **POM Home**.
3. On the **Configuration** tab, click **Global Configurations**.
4. In the Recorder settings area, select the following check boxes:
   a. **Enable Recorder**
   b. **Enable Secured Connection**
5. In the **Recorder port** field, type the port number of the Avaya Contact Recorder port.
6. Click **Apply**.

## Configuring POM Applications

### Procedure

1. Log in to the POM interface with the Administration user role.
2. In the left navigation pane, click **System Configuration** > **Applications**.
3. In the right pane, click to edit the driver and nailer app. For details see, *Using Proactive Outreach Manager*.

### Next steps

To restart POM service:

- Log in to the POM server with root credentials.
- Run the command `service POM restart`.

# ACR Configuration

## Administering Recorder Information

### Procedure

1. Log in to the Avaya Contact Recorder interface with the Administration user role.
2. Navigate to **General Setup** > **Recorder**.
3. In the **IP Address on this server to use for recordings (RTP, screen content etc.)** field, type the IP address of Avaya Contact Recorder.

# Administering Contact Center Information

## Procedure

1. Log in to the Avaya Contact Recorder interface with the Administration user role.
2. Navigate to **General Setup** > **Contact Center Interface**.
3. Update the following values:

| Heading for Column 1 | Heading for Column 2 |
|---|---|
| **Switch Type** | Select **Communication Manager** from the drop-down list. |
| **Audio format** | Default value is **G.729A (8kbps)**. |
| **Avaya Communication Manager Name** | Type `H.323 Gatekeeper IP address` obtained in Section *Obtain Tlink Name*. |
| **AE Server Address(es)** | Type `IP address` of the Avaya AESserver. |
| **DMCC Username** | Type the `User Id` configured in Section *Administer Avaya Contact Recorder User for DMCC*. |
| **DMCC Password** | Type the `User Password` configured in Section *Administer Avaya Contact Recorder User for DMCC*. |
| **IP Station Security Code** | Type `Security Code` configured in Section *Administer Virtual IP Softphones*. |
| **AES TSAPI Server(s)** | Type `IP address` of the Avaya AES server |
| **AES TSAPI Service Identifier(s)** | Type `Tlink` Name configured in Section *Administer TSAPI Link*. |
| **AES TSAPI Service Login ID** | Type `User Id` configured in Section *Administer Avaya Contact Recorder User for TSAPI*. |
| **AES TSAPI Service password** | Type `User Password` configured in Section *Administer Avaya Contact Recorder User for TSAPI*. |
| **Extensions assigned to recorder** | Use **Add Port(s)** to add the virtual IP softphone extensions configured in Section *Administer Virtual IP Softphones*. |

# Administering Bulk Recording

## Procedure

1. Log in to the Avaya Contact Recorder interface with the Administration user role.
2. Navigate to **Operations** > **Bulk Recording**.

3. In the **Record calls to or from** group, click **Add address(s)** tab to add the target stations.
4. Retain the default values for other fields.

# Administering POM Interface

## Procedure

1. Log in to the Avaya Contact Recorder interface with the Administration user role.
2. Navigate to **Operations** > **Bulk Recording**.
3. Edit the Avaya Contact Recorder properties file to include all the following lines:

```
acr.dialerlist=POM1
POM1.class=com.swhh.cti.pomdialer.POMDialer
POM1.dialer=x.x.x.x
POM1.port=7999
POM1.username=wfo
POM1.password=Avaya135
POM1.tracing=true
POM1.blockagentids=true
```

**Note:**

The **Dialer** field must be set to the IP address of the POM as obtained in Section *Configure POM*. The **User** and **Password** fields must be set to the user name and password that have the access permission to the POM admin page.

4. Separate the dialer list using "," delimiter in case of the multiple dialers.

   Provide the required information for other dialers as below:

```
acr.dialerlist=POM1, POM2
POM1.class=com.swhh.cti.pomdialer.POMDialer
POM1.dialer=x.x.x.x
POM1.port=7999
POM1.username=wfo
POM1.password=Avaya135
POM1.tracing=true
POM1.blockagentids=true
POM2.class=com.swhh.cti.pomdialer.POMDialer
POM2.dialer=y.y.y.y
POM2.port=7999
POM2.username=wfo
POM2.password=Avaya135
POM2.tracing=true
POM2.blockagentids=true
```

5. Save and close the file.
6. Restart Avaya Contact Recorder service.

# Chapter 9: Integrating POM with Avaya Oceana™ Solution

## Oceana Integration

POM integrates with Avaya Oceana™ Solution so that Avaya Oceana™ Solution can support a fully integrated Outbound channel.

For POM agents to log on to Avaya Workspaces, POM provides JAVA SDK. Avaya Workspaces provides the unified desktop for inbound and outbound channels. JAVA SDK provides API to integrate the POM Agent functionality for desktop implementation. Java SDK is inline with the existing .NET-based SDK except the login-specific enhancements. SDK APIs only support secure communication. Therefore, you must configure the POM certificate in the client API while connecting the client API to POM.

**Note:**

For Avaya Workspaces to dispose calls, Custom Completion Code Name and Completion Code ID in POM and Avaya Oceana™ Solution must be same.

For Oceana integration, you must install POM in the `Oceana` mode. After installing POM, you must log on to the Experience Portal web console, click **POM** > **POM Home** > **Configurations** > **Oceana Configuration**, and configure the IP address or host name of Avaya Oceana™ Cluster 3 that hosts OBCService.

OBCService exposes the REST services through which POM fetches the agent attributes configured in Avaya Oceana™ Solution. You must log on to the Experience Portal web console, click **POM** > **POM Home** > **Campaigns** > **Campaign Strategies**, and select the agent attributes as an outbound skill. POM agents can log on to Avaya Workspaces with attributes assigned to them.

**Note:**

POM does not support skill-based pacing if you install POM in the `Oceana` mode. POM restricts the campaign having skill based pacing.

### Context Store Integration

POM provides outbound attempt information to the Context Store server for customer journey completeness. You can send the data to Context Store in all the POM installation modes. POM uses the Context Store REST web service to create the context. Context Store provides an auto-generated unique identifier that is work request ID for the context record. POM persists this work request ID into the POM database.

While creating the context, POM sets the **persistToEDM** field to `true` to persist the context data in an external database. POM also provides **groupID**, which is presented as Customer ID. One of the contact attribute is configured as Customer ID. Contact browser is enhanced to capture this configuration. The Customer ID uniquely identifies the specific customer record. POM derives the Customer ID based on the **Customer ID Retrieval Mode** configuration on the Contact Browser page.

The following are the retrieval mode configurations:

| Retrieval mode | Description |
|---|---|
| Always | Select after POM does not have a customer ID or administrator chooses to use the customer ID from the customer management snap in. POM fetches a Customer ID from the Customer Management snap-in. The selected attribute value and the attempt address are as an input to fetch Customer ID. POM uses the same network address as that of the configured Context Storeserver while retrieving to the Customer Management snap-in. |
| Never | POM uses the value of the selected attribute as Customer ID. |
| Attribute value is blank | If the attribute value is blank, POM retrieves the Customer ID from the Customer Management snap-in, else POM uses the attribute value as Customer ID. |

**Note:**

To see the customer journey, ensure that you do not mark the contact as `done` in a campaign strategy till the time it is with the agent. If you mark the contact as `done` while it is with the agent, the customer journey might not be displayed in the Avaya Workspaces.

### POM REST web services

The existing SOAP web services are converted into equivalent REST web services. The Engagement Designer workflow in Avaya Oceana™ Solution can use new REST web services to modify entities related to the POM outbound campaign. For more information about POM REST web services, see *Developer Guide for Proactive Outreach Manager* .

# POM - Oceana Integration checklist

Use the following checklist for POM - Avaya Oceana™ Solution integration:

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 1 | Install POM in the Oceana mode. | See *Implementing Avaya Proactive Outreach Manager*. | |

*Table continues…*

| No. | Task | Reference | ✔ |
|---|---|---|---|
| 2 | Deploy Avaya Oceana™ Solution. | See *Deploying Avaya Oceana™ Solution*. | |
| 3 | Loading and installing the OBCService SVAR. | See Loading and installing the OBCService SVAR on page 63. | |
| 4 | Set OBCService attributes. | See Setting OBCService attributes on page 64. | |
| 5 | Import the POM server certificate to Avaya Oceana™ Cluster 3. | See Importing the POM server certificate to Avaya Oceana™ Cluster 3 on page 66. | |
| 6 | Configure Context Store. | For information about how to configure Context Store, see *Avaya Context Store Snap-in Reference*. | |
| 7 | Configure the IP address or FQDN of Avaya Oceana™ Cluster 3. | For information about the fields on the Oceana Server page, see *Using Avaya Proactive Outreach Manager*. | |
| 8 | Add the following to the POM Trust store.<br>• Certificates of all nodes of Avaya Oceana™ Cluster 1<br>• Certificates of all nodes of Avaya Oceana™ Cluster 3<br>• Certificates of AES | For information about how to add certificates to the POM Trust store, see *Implementing Avaya Proactive Outreach Manager*. | |
| 9 | Complete POM configurations such as contact list, campaign strategies, completion codes, and campaigns. | See *Using Avaya Proactive Outreach Manager*. | |
| 10 | Configure an Outbound Provider. | See Configuring an Outbound Provider on page 67. | |
| 11 | Add Disposition Codes for Outbound contacts. | See Adding Disposition Codes for Outbound contacts on page 67 | |
| 12 | Create a user to handle Outbound contacts. | See Creating a user to handle Outbound contacts on page 68. | |
| 13 | Configure After Contact Work (ACW) time. | See Configuring After Contact Work time on page 69. | |

# Loading and installing the OBCService SVAR

## About this task

Use this procedure to load the OBCService SVAR in System Manager and install it to Avaya Oceana™ Cluster 3.

### Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Service Management** > **Services**.
2. On the Services page, click **Load**.
3. In the Load Service dialog box, perform the following steps:
   a. Click **Browse**.
   b. Select the SVAR and click **Open**.
   c. Click **Load**.
4. In the Accept End User License Agreement dialog box, click **Accept**.
5. On the Services page, verify that the state of the SVAR is `Loaded`.
6. On the Services page, select the check box for the SVAR and click **Install**.
7. In the Confirm install service: OBCService dialog box, select the check box for Avaya Oceana™ Cluster 3 and click **Commit**.
8. On the Services page, verify that the state of the SVAR is `Installing`.

   The state changes to `Installed` when the installation is complete.
9. Set OBCService attributes.
10. Restart the Avaya Breeze™ nodes that are added to Avaya Oceana™ Cluster 3.

## Setting OBCService attributes

### About this task

Use this procedure to configure the OBCService attributes for POM integration.

### Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze™** > **Configuration** > **Attributes**.
2. On the Service Clusters tab, do the following:
   a. In the **Cluster** field, select Avaya Oceana™ Cluster 3.
   b. In the **Service** field, select **OBCService**.
3. Configure the attributes of the service.
4. Click **Commit**.

# OBCService attributes

## Startup Configuration

| Name | Description |
|---|---|
| **Deployment type** | The deployment type that determines the memory size of processing units.<br>• For an Avaya Oceana™ Solution deployment that supports up to 4500 active agents, select `OCEANA_3XLARGE`.<br>• For an Avaya Oceana™ Solution deployment that supports up to 2000 active agents, select `OCEANA_XLARGE`.<br>• For an Avaya Oceana™ Solution deployment that supports up to 1000, 500, or 250 active agents, select `OCEANA_LARGE`.<br>• For an Avaya Oceana™ Solution deployment that supports up to 100 active agents, select `OCEANA_SMALL`. |
| **POM Server** | The IP address or FQDN of the POM server that is to be serviced by Outbound Connector. |
| **UAC Cluster** | The cluster that hosts the Unified Agent Controller services.<br>• For an Avaya Oceana™ Solution deployment that supports up to 100 active agents, select Avaya Oceana™ Cluster 1.<br>• For an Avaya Oceana™ Solution deployment that supports up to 4500, 2000, 1000, 500, or 250 active agents, select Avaya Oceana™ Cluster 2. |
| **UCA Cluster** | The cluster that hosts the Unified Collaboration Administrator (UCA) service.<br>To set this attribute, select Avaya Oceana™ Cluster 1. |
| **UCM Cluster** | The cluster that hosts Unified Collaboration Model (UCM) services.<br>To set this attribute, select Avaya Oceana™ Cluster 1. |

### Advanced Configuration

| Name | Description |
|---|---|
| **Secure Connection** | The attribute that enables or disables the secure connection to UAC.<br>• To enable secure connection, select `TRUE`.<br>• To disable secure connection, select `FALSE`. |
| **UAC URL** | The service URL of the UnifiedAgentController service API.<br>For example, `/services/UnifiedAgentContextService/XpsAPI`. |

# Importing the POM server certificate to Avaya Oceana™ Cluster 3

### Before you begin

Log in to the POM server web interface and export the POM server certificate.

### Procedure

1. On the System Manager web console, click **Services** > **Inventory** > **Manage Elements**.
2. On the Manage Elements page, select the check box for one of the nodes of Avaya Oceana™ Cluster 3, and click **More Actions** > **Manage Trusted Certificates**.
3. On the Manage Trusted Certificates page, click **Add**.
4. On the Add Trusted Certificate page, perform the following steps:
   a. Click **Import from file**.
   b. In the **Please select a file** field, click **Browse**.
   c. In the Choose File to Upload dialog box, browse to the POM server certificate, and then click **Open**.
   d. Click **Retrieve Certificate**.
   e. Click **Commit**.
5. Repeat Step 2 to Step 4 for the other node of Avaya Oceana™ Cluster 3.
6. Click **Done**.

# Configuring an Outbound Provider

### About this task

Use this procedure to create a new Outbound Provider through Avaya Control Manager.

### Before you begin

Ensure that Avaya Oceana™ Cluster 1 is in running and accepting state.

### Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Server Details**.
2. On the Avaya Oceana Server List page, double-click the UCAServer server.
3. Select the **Providers** tab.
4. To add the Outbound Provider, do the following:
   a. Click **Add**.
   b. In the **Type** field, select **Outbound**.
   c. In the **Name** field, type `POM`.
   d. In the **Address** field, type `POM`.
   e. Click **Save**.

   **Important:**

   To make the new provider available to Avaya Workspaces agents, you must restart the clusters.

# Adding Disposition Codes for Outbound contacts

### About this task

Use this procedure to add Disposition Codes for Outbound contacts through Avaya Control Manager.

### Before you begin

Ensure that Avaya Oceana™ Cluster 1 is in running and accepting state.

A POM Completion Code is automatically generated. Therefore, Completion Codes must be added to the POM server before adding them to Avaya Oceana™ Solution.

### Procedure

1. On the Avaya Control Manager webpage, click **Configuration** > **Avaya Oceana™** > **Work Codes**.
2. Click the **Disposition Codes** tab.

3. Click **Add** and do the following:
   a. In the **Name** and **Number** fields, type the name and number of the Completion Code configured on the POM server.

      **Important:**

      The complete list of Avaya Oceana™ Solution Outbound Disposition Codes, including numeric codes and text, must match the complete list of POM Completion Codes.

      While creating a POM campaign, the campaign must contain the complete list of all POM Completion Codes.
   b. In the **Contact Type** field, select the **Outbound** check box.
   c. Click **Save**.

# Creating a user to handle Outbound contacts

### About this task

Use this procedure to create an agent to handle Outbound contacts.

### Before you begin

Ensure that Avaya Oceana™ Cluster 1 is in running and accepting state.

### Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Select the location for your Avaya Oceana™ Solution.
4. Perform one of the following steps:
   - Click **Add**.
   - Select an existing user and click **Edit**.
5. Enter appropriate value in each of the following fields:
   a. In the **First Name (English)** field, enter the first name of the user in English.
   b. In the **Surname (English)** field, enter the surname of the user in English.
   c. In the Available applications section, select the **Avaya Oceana** check box.
   d. In the **LDAP Username** field, enter the LDAP user name of the user.

      The LDAP user name must be in the username@domain.com format. This user name is used to log on to Avaya Workspaces.
   e. In the **Username** field, enter a user name.

      In this release, the user name is the internal handle.

f. In the **Password** field, enter a password.

   This password is used to log on to Avaya Control Manager.

g. In the **Confirm Password** field, re-enter the password.

h. In the **Extension** field, enter the station associated with this agent.

   This is used when logging on to Avaya Workspaces.

i. In the **AVAYA Login** field, enter the Elite agent login ID only if the agent also supports Voice contacts. Otherwise, leave this field blank.

j. Click **Save**.

6. Scroll to the right and select the **Avaya Oceana** tab.
7. Select check box for **Outbound** account.

   **Important:**

   - Outbound users can have only Outbound account.
   - Avaya Oceana™ Solution supports Hot Desking for Inbound Voice agents but does not support it for POM Outbound agents.

8. Select the **Attributes** tab.
9. Move the attributes from the **Available Attributes** list to the **Agent Attributes** list.

   **Important:**

   - Ensure that the attributes assigned to the agent match the attributes configured in POM.
   - Do not assign a Work Assignment skill to the user.

10. Click **Save**.

# Configuring After Contact Work time

## About this task

Use this procedure to configure After Contact Work (ACW) time through Avaya Control Manager.

**Important:**

Enabling ACW time is a mandatory global setting that impacts all interaction types.

## Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration** > **Avaya Oceana™** > **Server Details**.
3. Double-click the **UCAServer** instance.

4. Select the **System Properties** tab.
5. Expand **After Contact Work**.
6. Select the **Enable After Contact Work** check box.
7. In the **After Contact Work Timer (Seconds)** field, enter the same time as the POM completion timer.
8. Click **Save**.

# Chapter 10: Resources

## Documentation

For information on feature administration, interactions, considerations, and security, see the following POM documents available on the Avaya Support site at http://www.avaya.com/support:

| Title | Description | Audience |
|---|---|---|
| *Avaya Proactive Outreach Manager Overview and Specification* | Provides general information about the product overview and the integration with other products. | Users |
| *Upgrading Avaya Proactive Outreach Manager* | Provides information about upgrading Proactive Outreach Manager. | Implementation engineers |
| *Implementing Avaya Proactive Outreach Manager* | Provides information about installing and configuring Proactive Outreach Manager. | Implementation engineers |
| *Troubleshooting Avaya Proactive Outreach Manager* | Provides general information about troubleshooting and resolving system problems, and detailed information about and procedures for finding and resolving specific problems. | System administrators<br>Implementation engineers<br>Users |

Install Avaya Aura® Experience Portal before you install POM. You will find references to Avaya Aura® Experience Portal documentation at various places in the POM documentation.

## Finding documents on the Avaya Support website

### Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.

7. Click **Enter**.

# Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

# Appendix A: Cipher requirements of Java implementation

POM uses a set of cipher suites that might not be supported by the Java implementation installed on the application server. This includes the cipher suites that use AES_256 and require installation of the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. To use a stronger algorithm, obtain the JCE Unlimited Strength Jurisdiction Policy Files and install it in the JDK/JRE.

**Note:**

It is the responsibility of the customer to verify that this action is permissible under local regulations. If not, customer can remove the unsupported ciphers from the connector in the `server.xml` of Apache Tomcat. Customers can also use the default ciphers of the installed Java implementation by removing the ciphers attribute from the connector element of `$APPSERVER_HOME/conf/server.xml`. For more information, see *Troubleshooting Avaya Proactive Outreach Manager*.

For WebSphere, POM uses the default cipher suites provided by the IBMJSSE2 provider. However, if the customer wants to use specific cipher suites, then the customer must configure the `enabledCiphers` property in the `WASConfig.properties` file and set those ciphers suites as comma separated values.

For example:
`enabledCiphers=TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_256_CBC_SHA256`.

For more information, see the following Java Implementation links:

- For Oracle Java, see https://docs.oracle.com/javase/8/docs/technotes/guides/security/SunProviders.html.
- For IBM Java, see https://www.ibm.com/support/knowledgecenter/en/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/jsse2Docs/ciphersuites.html.

If there is a mismatch between configured ciphers on the application server and the supported ciphers by the underlying Java implementation, application server logs displays the following exception:

```
java.lang.IllegalArgumentException: Cannot support <Unsupported Cipher name> with
currently installed providers.
```

# Appendix B: Configuring TLSv1.2 on WebSphere

### About this task

Use this procedure to configure TLSv1.2 on a WebSphere application server to work with POM for each incoming and outgoing communication.

When you use IBM WebSphere as an application server in a POM deployment, IBM WebSphere must meet the CEC-security requirement to communicate over TLSv1.2 on each of its interfaces.

### Before you begin

Use the following:

- Java 7 or 8.
- WebSphere 8.5.5 or later versions.

### Procedure

1. Log on to the WebSphere Application Server Integrated Solutions Console by using a web browser.
2. In the navigation pane, click **Security** > **SSL certificate and key management**.
3. On the **Related Items** tab, click **SSL configurations**.
4. Click the **Default SSL settings** link.
5. On the Additional Properties page, click **Quality of protection (QoP) settings**.
6. On the General Properties page, from the **Protocol** list, select **TLSv1.2**.
7. In the **Cipher suite settings** area, from the **Cipher suite groups** list, select **Strong**.
8. In the **Cipher suite settings** area, click **Update selected ciphers**.
9. Click **OK**.

   Save the updated cipher files in the same location as the master configuration.
10. In the navigation pane, click **Security** > **SSL certificate and key management** > **Manage FIPS**.
11. On the **Manage FIPS** page, click **Enable SP800-131** and then click **Transition**.
12. Click **OK**.

13. If the system displays a non-compliant certificate error, perform the following steps:
    a. On the **Related Items**, click **Convert certificates**.
    b. Set the **Algorithm** setting to **Strict**.
    c. From the **New certificate key size** list, select **2048 bits**.
    d. Click **OK**.

       You can save the file in the same location as the master configuration.
14. Navigate to the following location to access the `ssl.client.props` file:

    `WAS_Profile_Dir/properties`
15. Open the `ssl.client.props` file and edit the following:
    a. Set the `com.ibm.security.useFIPS` property to `true`.
    b. Set the `com.ibm.websphere.security.FIPSLevel` property to `SP800-131`.

       If this line already exists, do not write this line again.
    c. Set the `com.ibm.ssl.protocol` property to `TLSv1.2`.
16. Click **Server** > **Server Types** > **WebSphere application servers** > **server1**.
17. On the Server Infrastructure page, click **Java and Process Management** > **Process definition**.
18. On the **Additional Properties** tab, click **Java Virtual Machine** > **Custom properties**.
19. On the Preferences page, create custom properties as follows:
    a. Select the **com.ibm.team.repository.transport.client.protocol** check box and set the corresponding value to **TLSv1.2**.
    b. Select the **com.ibm.jsse2.sp800-131** check box and set the corresponding value to **strict**.
    c. Select the **com.ibm.rational.rpe.tls12only** check box and set the corresponding value to **true**.

# Index

## R



## S



## T



## U



## V



## W