



Administering Avaya Oceana®

Release 3.10.0.1
Issue 2
August 2025

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

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 media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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](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.

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, 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. Unless otherwise stated, 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

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](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply 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, please contact your Avaya Sales Representative.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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 affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction	11
Purpose	11
Change history	11
New in this release	11
Chapter 2: Overview	12
Avaya Oceana® overview	12
Avaya Workspaces overview	13
Checklist for configuring Avaya Workspaces	14
Chapter 3: Configuration	16
Avaya Workspaces configuration through Avaya Control Manager	16
Functional button descriptions	16
Commission Avaya Control Manager overview	17
Creating a Communication Manager user for Avaya Control Manager	17
Logging in to Avaya Control Manager	18
Creating a location for Avaya Oceana®	19
Adding Communication Manager to Avaya Control Manager	19
Adding Communication Manager to the location	20
Adding a site, department, and team to Avaya Control Manager	20
Synchronizing Avaya Control Manager and Communication Manager	21
Creating a Manager Server for Unified Collaboration Administration	22
Adding an Avaya Oceana® server to a location	24
Adding connectors to Provisioning Server	24
Configuring token-based access between Control Manager and Avaya Oceana®, Avaya Analytics™, or Avaya Workspaces for Call Center Elite	25
Assigning a location to the UCA proxy server	32
Assigning location to Application Server	32
Assigning location to Synchronizer Service Server	33
Testing the UCA REST connection	34
Categories, Attributes, and Attribute Sets	34
Users, Accounts, and Providers	35
Adding Attribute Categories to Avaya Control Manager	35
Adding Attributes to Avaya Control Manager	36
Adding services to Avaya Control Manager	37
Configuring Properties in Avaya Control Manager	38
Configuring a secure connection between Avaya Control Manager and UCA Server	39
Configuring Avaya Oceana® system properties using Control Manager	41
Starting Omnichannel Administration Utility	45
Starting Oceana Customer Management Tool	45
Work Codes, Disposition Codes, and Rejection Codes	46

Configure Alarms and Events.....	46
Creating an SNMPv3 user profile.....	47
Creating an SNMP target profile.....	47
Assigning Serviceability Agents.....	48
Verifying the configuration.....	48
Configure voice resources.....	49
Configuring a Communication Manager Hunt Group.....	49
Creating variables using Avaya Control Manager.....	50
Configuring Vector Directory Numbers.....	52
Adding Provider, Skills, VDN, and Extensions to Avaya Oceana®	53
Creating a user to handle Voice contacts.....	55
Adding attributes to an agent.....	56
Creating a Transfer Target service for Voice.....	57
Restarting the CallServerConnector service.....	57
User management.....	58
Creating a Control Manager role and user to administer Avaya Oceana®	58
Adding a new user.....	60
Configuring concurrent active contacts per agent.....	62
Adding attributes to a user.....	62
Searching users.....	62
Cloning an agent.....	63
Editing a user.....	63
Deleting a user.....	64
Configuration for Avaya Workspaces.....	64
Configuring Avaya Analytics™ 3.x Streams server details for real-time reporting.....	64
Configuring Avaya Analytics™ 4.x server details for real-time reporting.....	66
Configuring CRM integration.....	67
Enabling Avaya Breeze® platform authorization on Avaya Aura® Device Services.....	68
Configuring LDAP integration.....	68
Work Codes, Disposition Codes, and Rejection Codes.....	69
Configuring work codes or user codes.....	70
Configuring disposition codes.....	70
Configuring deferral codes.....	71
Configuring rejection codes.....	72
Configuring deferred email settings.....	72
Enabling email forward.....	73
Enabling multiple replies to email.....	73
Customer Management	73
Create Avaya Oceana user with SIP extension from Avaya Control Manager.....	75
Configuring screenpops.....	88
Configuring transfer to service.....	90
Transfer to User configuration.....	91
Configuring email signature settings.....	94

Channel Exclusivity.....	94
Reserve agents and thresholds.....	97
Configuring Auto answer timeout for a provider.....	98
Creating a user profile template for Auto answer.....	98
Assigning the user profile template to a user.....	99
Handling browser closure and network connection issues.....	99
Adding or removing extensions to or from the forbidden extensions.....	100
Supervisor reporting dashboard - user management.....	100
Adding reporting users.....	101
Assigning reporting access to Avaya Workspaces users.....	102
About routing services groups.....	103
Group management.....	104
Adding a group.....	105
Assigning groups to a user.....	106
Editing a group.....	106
Deleting a group.....	107
Thresholds.....	107
Configuring thresholds in Avaya Control Manager.....	108
Creating new thresholds for Name Services in Avaya Control Manager.....	108
Configuring thresholds for Short Not Ready.....	109
Threshold measures.....	109
Agent Layout Provisioning.....	110
Overview.....	110
Configuring layouts.....	110
Managing layouts.....	111
Customizing layouts.....	111
Adding multiple agents to layout groups.....	112
Cross-channel limit.....	113
Configuring channel limits.....	113
Considering voice contacts in overall cross-channel limit.....	114
Configuring Email limit.....	114
Multiple WhatsApp number and Facebook business pages for Async messaging.....	115
Agent log-off on browser disconnect.....	115
Configuring the Workspaces time-out value and reason code.....	116
Enabling or Disabling re-routing of ongoing contacts.....	116
Mandatory selection of From address for an outbound mail.....	117
Enabling the mandatory selection From address attribute.....	117
Proficiency levels for attributes within the categories.....	118
Setting proficiency levels for attributes within the categories.....	118
Chapter 4: Automation overview.....	119
Automation Overview.....	119
Configuring Automation.....	119
Chapter 5: Chat administration.....	120

Omnichannel Administration Utility.....	120
Creating Web On Hold URL groups using Omnichannel Administration Utility.....	120
Creating Web On Hold comfort groups using Omnichannel Administration Utility.....	121
Creating chat comfort groups.....	122
Creating automatic phrases using Omnichannel Administration Utility.....	123
Creating a Page Push URL for Co-Browsing.....	123
Creating Chat Headers using Omnichannel Administration Utility.....	124
Configuring Web Chat settings.....	125
Web Chat Settings field descriptions.....	125
Configuring CORS for the sample Chat client.....	126
Removing attributes and routepoints from Omnichannel Database.....	127
Setting contacts to closed.....	128
Configuring messaging transcripts.....	129
Configuring regular retry of failed messaging transcripts.....	129
Configuring WhatsApp settings.....	130
Available file types for WhatsApp media types.....	131
Configuring Facebook settings.....	133
Available file types for Facebook media types.....	134
Configuring Twitter settings.....	136
Available file types for Twitter media types.....	137
Configuring Chat for Transfer to Service.....	137
Configuring a Transfer to Service Route Point for Chat.....	137
Creating a Transfer Target service for Chat.....	138
Chapter 6: Email administration.....	139
Configuring an Outbound SMTP server.....	139
Configuring an Inbound Mail server.....	139
Configuring keyword groups.....	140
Configuring an automatic response.....	141
Configuring an automatic suggestion response.....	141
Configuring Basic authentication settings.....	142
Configuring Email inboxes.....	142
Mail Store field descriptions.....	143
Alias field descriptions.....	145
Distribution group field descriptions.....	146
Outbound email approval.....	146
Outbound email approval process.....	147
Configuring percentage of mails going for approval.....	147
Email approval ratios.....	148
Illustration of the approval attribute configuration for outbound emails.....	148
Handling email contact with Send as Group option enabled.....	149
Checklist for configuring email contact with Send as group.....	150
Configuring Office365 distribution list.....	150
Configuring throttling policy.....	150

Configuring Send as group feature for Avaya Oceana® mailbox.....	151
Configuring Avaya Oceana® distribution group.....	152
Disabling polling on a mailbox.....	153
Configuring rule groups.....	154
Configuring system default rule.....	157
Configuring system delivery failure rule.....	157
Configuring email settings.....	158
Configuring holidays.....	159
Configuring office hours.....	160
Applying office hours.....	161
Configuring Email Open Interfaces.....	162
Creating Sender Groups.....	163
Configuring a Chat History Header prepared response.....	164
Enabling the backup for inbound emails.....	164
Configuring email transcripts.....	165
Configuring regular retry of failed email transcripts.....	165
Configuring Ad hoc email rules.....	166
Adding Ad hoc email rules.....	166
Assigning Ad hoc email rule to mailbox.....	167
Editing Ad hoc email rules.....	167
Deleting Ad hoc email rules.....	168
Configuring Email for Transfer to Service.....	168
Configuring a Transfer to Service Route Point for Email.....	168
Creating a Transfer Target service for Email.....	169
Microsoft Graph set up process.....	169
Installing Office 365 certificates on Avaya Aura® System Manager.....	171
Configuring Microsoft Graph authentication with client secret in Omnichannel Administration Utility.....	172
Configuring Microsoft Graph authentication with client certificate in Omnichannel Administration Utility.....	172
Configuring inbox for Microsoft Office 365.....	173
Enabling MS Graph logging.....	174
Chapter 7: SMS administration.....	175
Configuring SMS Gateway.....	175
Configuring SMS for Transfer to Service.....	177
Configuring a Transfer to Service Route Point for SMS.....	177
Creating a Transfer Target service for SMS.....	177
Creating automatic phrases.....	178
Creating a page push URL.....	179
Chapter 8: Social Media administration.....	181
Configuring Social Media for Avaya Messaging Automation.....	181
Configuring Social Media for third-party gateways.....	183
Configuring Social Media for Transfer to Service.....	184

Configuring a Transfer to Service Route Point for Social Media.....	184
Creating a Transfer Target service for Social Media.....	184
Chapter 9: Messaging administration.....	186
Creating automatic phrases for Messaging.....	186
Creating a welcome message.....	187
Configuring Messaging for Transfer to Service.....	187
Configuring a Transfer to Service Route Point for Messaging.....	187
Creating a Transfer Target service for Messaging.....	188
Chapter 10: Oceana Data Management and Purging.....	189
Cleanup and purging overview.....	189
Starting the Oceana Data Management utility.....	194
Creating an Email Rules cleanup rule.....	194
Creating a Customers cleanup rule.....	195
Creating a Channel Types cleanup rule.....	196
Creating a new scheduled cleanup task.....	197
Enabling OFFLINE database purging.....	198
Restoring contacts cleared by a scheduled task.....	199
Configuring session timeout.....	200
Customer privacy.....	201
Customer privacy overview.....	201
Configuring Context Store and Avaya Analytics™ server details.....	201
Configuring Avaya Analytics™ authentication.....	202
Generating a customer information file.....	204
Creating a customer detail audit cleanup rule.....	204
Deleting customer history.....	205
Repeating a customer deletion request.....	206
Adding SSL certificates.....	206
Removing expired SSL certificates.....	207
Database backup and restore.....	208
Database backup and restore overview.....	208
Taking a backup of the Omnichannel database.....	208
Taking a backup of the Omnichannel database from a network location.....	209
Restoring the Omnichannel database.....	210
Restoring the Omnichannel database from a network location.....	212
Creating a new scheduled backup task.....	212
Viewing the details of a scheduled backup task.....	214
Database defragmentation	214
Database defragmentation overview.....	214
Defragmenting the Omnichannel database.....	215
Viewing the defragmentation history.....	216
Database encryption.....	216
Database encryption overview.....	216
Creating and activating an encryption key.....	217

Activating the encryption key.....	217
Encrypting databases.....	218
Decrypting databases.....	219
Checklist for encrypting or decrypting databases in a High Availability deployment.....	220
Checklist for encrypting or decrypting databases in a Disaster Recovery deployment.....	220
Error scenarios.....	221
Chapter 11: Customization.....	222
Customization overview.....	222
Customizing the Transfer to Service list.....	222
Verifying the customized Transfer to Service list.....	223
Configuring email confirmation.....	224
Configuring the custom card limit.....	224
Using the Avaya Workspaces compressed layout.....	225
Enabling finish work confirmation.....	226
Configuring agent toast notifications.....	226
Configuring additional language pack.....	226
Configuring the start work button.....	227
Customer Journey configuration for Outbound agents.....	227
Adding the Customer Journey widget for Outbound agents.....	227
Chapter 12: Resources.....	229
Documentation.....	229
Finding documents on the Avaya Support website.....	230
Avaya Documentation Center navigation.....	231
Training.....	232
Support.....	235
Using the Avaya InSite Knowledge Base.....	235

Chapter 1: Introduction

Purpose

This document describes the administration tasks for Avaya Oceana[®], including general administrative tasks, managing data, and multimedia configuration.

Avaya Oceana[®] administrators can use this document.

Change history

Issue	Date	Summary of changes
2	August 2025	Updated the procedure for Removing expired SSL certificates on page 207.
1	May 2025	Initial issue for Release 3.10.0.1.

New in this release

Avaya Oceana[®] 3.10.0.1 supports the following:

- Avaya Oceana[®] Release 3.10.0.1 supports migration from previous releases. For more information and procedure to migrate, refer to the following documents:
 - Migrating Avaya Oceana[®]
 - Avaya Oceana[®] Disaster Recovery and Migration
- Avaya Oceana[®] Release 3.10.0.1 supports:
 - Breeze Release 3.9.0.2
 - VMWare Release 8.0
 - Centralized Logging on Common Service Platform

Chapter 2: Overview

Avaya Oceana® overview

Avaya Oceana® is the next-generation customer engagement solution. Enterprises can use Avaya Oceana® to seamlessly handle Generic, Voice, Web and Mobile Chat, Web Voice, Web Video, Email, Simple Messaging, Social Media, WebRTC, Video, POM contacts, and Messaging channels using a single intelligent attribute-based call routing through a unified Agent Desktop. Avaya Oceana® is built on the Avaya Breeze® platform using modular snap-ins that can be independently scaled, managed, and extended.

You can merge existing resources into routing strategies of Avaya Oceana® to significantly improve customer service and sales outcomes.

With these routing strategies, you can:

- Obtain customer information from Customer Relationship Management (CRM) of the enterprises and other third-party systems.
- Combine the information with the current journey context of the customer.
- Apply business goals-oriented strategies to match the customer to the best available resource.

The routing strategies also integrate with the back-office systems of enterprises to route work items such as claims and contracts.

Avaya Oceana® provides:

- Functionality to map the customer journey across various self-service and assisted service channels by storing the related data crumbs in the in-memory data grid. Resources and routing workflows use these data crumbs.
- An easy-to-use HTML5-based Desktop for agents and supervisors.
- Reporting and analytics designed to provide new and powerful insights for blended agent contact centers.

Avaya Oceana® consists of the following:

- **Access tier:** Provides media-specific providers such as Chat Provider, Email Provider, SMS Provider, Social Media Provider, Messaging Provider, Generic Provider, Avaya Aura® Communication Manager for Voice, and Avaya Mobile Communication Snap-in for Web Voice and Web Video.
- **Normalizing tier:** Provides a central normalizing tier within Avaya Oceana® that abstracts the media-specific characteristics of the inbound interactions.

- **Application tier:** Provides applications such as agent and supervisor desktops and Avaya Engagement Designer. Business analysts use these applications to author the logic that handles the inbound interactions, such as routing and reporting. They also use the applications for other higher-level functions in a future-proofed contact center product.
- **Components tier:** Provides Avaya Breeze® platform and a set of core components deployed on the Avaya Breeze® platform.

Avaya Aura® and Avaya Breeze® platform application tiers run on the Linux operating system, while Avaya Control Manager and Avaya Omnichannel run on the Microsoft Windows server operating system.

Avaya Oceana® provides the following:

- **Load Balancers:** Each Avaya Breeze® platform cluster in an Avaya Oceana® includes a load balancer. Therefore, Avaya Oceana® does not require external load balancers for the Avaya Oceana® features and functions. In Avaya Oceana® with a disaster recovery feature, only one site is active at a time. Do not use a load balancer between the two disaster recovery sites for Avaya Workspaces agents. In a disaster recovery deployment, the Avaya Session Border Controller for Enterprise diverts traffic between sites A and B. Avaya Session Border Controller for Enterprise is also mandatory for media for WebRTC Connect. Agents can connect directly to the active site. Any requirements for including Avaya Oceana® web traffic with an external load balancer require Avaya Professional Services consulting, outside baseline Avaya Oceana® deployment, or support activities.
- **Reverse Proxies:** Avaya Oceana® supports a properly specified and configured reverse proxy for use with Avaya Workspaces agents. For more information, see *Avaya Oceana® Port Matrix* document.

For information about configuring Avaya Workspaces Widgets when using a reverse proxy, see *Avaya Workspaces Widget Framework* documentation.

Avaya recommends using a reverse proxy with the Avaya Oceana WebChat Reference Frontend. For more information, see the *Avaya Oceana Reference Frontend* documentation.

- **Firewall:** Avaya recommends using properly specified and configured firewall and firewall policies. For more information about supported firewall types and firewall policies, see the *Avaya Oceana® Port Matrix* document.

Avaya Workspaces overview

Avaya Workspaces is a browser-based application with which Contact Center agents can handle outbound and inbound customer interactions. Interactions can be through channels such as Voice, Video, Chat, SMS, Email, Social Media, Generic, and Messaging. Agents can also make outbound voice calls and send outgoing emails. The intuitive user interface provides features for toggling between multiple, simultaneous interactions through different channels.

Avaya Workspaces enables seamless collaboration with customers, partners, and other users within and outside the organization. It also provides relevant information to agents securely and reliably.

Avaya Workspaces displays every interaction as an interaction card. Using interaction cards, agents can:

- Receive the interaction: Accept interactions with a single click.
- Hold or resume the voice interaction: Put an active voice interaction on hold when the agent must attend another interaction with a higher priority.
- Consult another agent: Seek advice about an interaction.
- Transfer the interaction to another agent: Send the interaction to another agent interaction area.
- Add another agent to the interaction: Create a conference with another agent when the other agent can contribute to resolving the customer interaction.
- Record work codes reporting to record work codes: Select from the configured work codes to report the type of work done during the interaction.
- Record disposition codes reporting to record disposition codes: Select from the configured disposition codes to add disposition to the interaction.
- Defer email interaction using interaction cards.
- Approval of outbound agent email replies: Agent email responses can be routed through an approval process.

For accessibility purposes, Avaya Workspaces is optimized to conform with Section 508 and WCAG 2.0 AA standards. Avaya Workspaces provides:

- Access to most content and controls using the keyboard or mouse.
 - Alternative text and labels to assist users with screen-readers.
 - A color palette that meets requirements for users with visual impairments.
 - Screen magnifier tool, such as Magnifier, to zoom in and out of Avaya Workspaces screens.
- Do not use built-in controls of the browser.

Checklist for configuring Avaya Workspaces

You can use the following components to configure Avaya Workspaces:

- Avaya Breeze® platform: To deploy snap-in components in Avaya Oceana®.
- Avaya Aura® Communication Manager: To configure the hunt groups, VDNs, and stations for voice calls.
- Avaya Aura® Call Center Elite: To provide voice capabilities for Avaya Oceana®. Avaya Oceana® leverages Elite features such as Redirection on No Answer (RONA) and Calendaring.
- Application Enablement Services: To enable Call Server Adapter (CSC) Snap-in to communicate with Communication Manager.
- Avaya Control Manager: To administer agents, users, Work Assignment attributes, hunt groups, skills, Vector Directory Number (VDN), and tenants.

- Avaya Co-Browsing Snap-in: To provide web collaboration between two users to enable a customer and agent to browse webpages and complete web forms.
- Avaya Context Store Snap-in: To provide a memory data grid that can store contextual information that the customer's Enterprise applications provide. These applications route data and historical data to share among Avaya Experience Portal, Avaya Engagement Designer, Work Assignment, EPS, and the multimedia snap-ins such as chat and email. The applications display customer data to agents and show historical journey information.

No.	Task	Reference	✓
1	Configure Avaya Aura® Communication Manager and Avaya Aura® Call Center Elite.	Refer <i>Avaya Aura® Communication Manager and Avaya Aura® Call Center Elite in Deploying Avaya Oceana®</i>	
2	Configure Application Enablement Services.	Refer <i>Application Enablement Services in Deploying Avaya Oceana®</i>	
3	Configure the Avaya Oceana® multimedia server.	Refer <i>Avaya Oceana® multimedia server in Deploying Avaya Oceana®</i>	
4	Configure users, work codes, and screenpops in Avaya Control Manager.	See Avaya Workspaces configuration through Avaya Control Manager on page 16.	

Chapter 3: Configuration

Avaya Workspaces configuration through Avaya Control Manager

You can use Avaya Control Manager to configure the following parameters for Avaya Workspaces:

- Users
- Reason codes
- Screenpops
- URLs and phrases for the Suggested Content widget

For information about associating a Communication Manager user to Avaya Control Manager and adding a hunt group, site, location, team, and department to Avaya Control Manager, see *Configuring Avaya Control Manager* and *Using Avaya Control Manager*.

For information about configuring Communication Manager, Call Center Elite and Application Enablement Services, set up routing, and Avaya Breeze® platform clusters, see *Deploying Avaya Oceana®*.

Functional button descriptions

Icon	Name	Description
	Add	Adds a new user or agent.
	Edit	Modifies the selected user or agent.
	Delete	Removes the selected user or agent.
	Search	Filters a user or agent.
	Save	Saves the changes.
	Close	Closes the current screen and returns to the previous screen.

Table continues...

Icon	Name	Description
	Import	Imports users or agents from an Excel file to Avaya Control Manager.
	CM Options	Displays or updates the Communication Manager options for a user or agent.
	Clone	Creates a duplicate user or agent.

Commission Avaya Control Manager overview

This section describes how to commission Avaya Control Manager for Avaya Oceana®.

For information on how to install and commission Avaya Control Manager, see *Installing Avaya Control Manager*.

Creating a Communication Manager user for Avaya Control Manager

About this task

Using the Communication Manager web interface, add a Communication Manager user for use by Avaya Control Manager.

Procedure

1. In your web browser, enter the following URL to open the Communication Manager web console:
`http://<CM IP address or FQDN>`
2. Click **Administration > Server (Maintenance) > Security > Administrator Accounts**.
3. Select **Privileged Administrator**.
4. Click **Submit**.

Note:

The Communication Manager account is used when adding Communication Manager in the Avaya Control Manager config.

The system displays the Administrator Login - Add Login screen.

5. In the **Login name** field, enter an administrator login name.

The login name:

- Can have alphabetic characters
- Can have numbers

- Can have an underscore (_)
 - Cannot have more than 31 characters
6. In the **Primary group** field, enter `susers` for a privileged login.
 7. In the **Additional group (profile)** field, add an access profile.
The system automatically populates the values in the Linux shell and the Home directory fields.
 8. In the **Enter password** field, enter the password for the login.
 9. In the **Re-enter password** field, re-enter the same password.
 10. **(Optional)** To change the password after the first login, in the **Force password/key change on next login** field, select **yes**.
 11. Click **Submit**.

Logging in to Avaya Control Manager

About this task

Use this procedure to log in to Avaya Control Manager to administer Avaya Oceana® resources.

Before you begin

Install SSL certificates on the Avaya Control Manager server. For more information, see Avaya Control Manager documentation.

Procedure

1. In your web browser, enter the following URL:
`https://<acccm_hostname>/ACCCMPortal`
`<acccm_hostname>` is the host name of the Avaya Control Manager server.
2. On the Avaya Control Manager login page, perform the following steps:
 - a. In the **Username** field, enter the user name.
The initial user name is `itnv`.
 - b. In the **Password** field, enter the password.
The initial password is `itnv`.
 - c. Click **Login**.
The system prompts you to change the password.
3. Change the password.
4. Log in to Avaya Control Manager using your new credentials.
5. If you receive any errors in Internet Explorer trying to connect to the ACCCM tiles, add the Avaya Control Manager IP address to the local hosts file.

Creating a location for Avaya Oceana®

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Locations**.
2. On the Location List page, click **Add**.
3. On the Location Add page, perform the following steps:
 - a. In the **Name** field, enter the name of the location.
 - b. In the **Description** field, enter the description of the location.
 - c. **(Optional)** In the **Auditing Location** field, leave the value as `False` or select `True` to activate audit logging for the location.
 - d. Click **Save**.

Adding Communication Manager to Avaya Control Manager

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Team Engagement**.
2. On the Team Engagement page, select **Communication Manager**.
3. On the Communication Manager List page, click **Add**.
4. On the Communication Manager Edit page, do the following:
 - a. In the **CM Alias Name** field, enter the alias name of Communication Manager.
 - b. In the **CM IP Address** field, enter the IP address of Communication Manager.
 - c. In the **CMS ACD** field, type `1`.
 - d. In the **CM Username** field, enter the user name of the Privileged Administrator account that you created earlier.
 - e. In the **CM Password** field, enter the password of the Privileged Administrator account that you created earlier.
 - f. In the **CM Type** field, select `S8700`.
 - g. In the **CM Version** field, select the supported version of Communication Manager.
 - h. In the **Terminal Type** field, select `ossi3`.
 - i. In the **Is Pin Required** field, select `Yes` or `No` based on your requirement.
 - j. In the **Time Of Day tables number** field, type `32`.
 - k. In the **Time Zone** field, select the correct time zone.
 - l. Click **Save**.

The Communication Manager List page displays the entry for the Communication Manager.

Adding Communication Manager to the location

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Locations**.
2. On the Location List page, perform the following steps:
 - a. Select the location to which you want to add the Communication Manager.
 - b. Click **Edit**.
3. On the Location Edit page, perform the following steps:
 - a. Select the **Systems** tab.
 - b. Click the **+** sign.
 - c. In the **System Type** field, select **CM**.
The **System Name** field populates the name of the newly created Communication Manager.
4. Leave the **Sync Schedule** field blank and click **Save**.
5. Click **Confirm** on the Warning message dialog box.

Adding a site, department, and team to Avaya Control Manager

About this task

Use this procedure to add a site, department, and team in an organization tree. The organizational tree manages users, sites, departments, and teams in an organizational chart.

The following are the organizational hierarchy level:

- Site
- Department
- Team

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. In the navigation pane, click **Organization tree**.
4. Click the **Expand** icon next to the **Add** button.
5. Click the **Add Organization Chart Items** icon.
6. On the Site tab, enter the information in the following fields:
 - a. In the **Site Name** field, enter a name for the site.
 - b. In the **Site description** field, enter a description for the site.
 - c. In the **Site location** field, select the location that you created in the previous procedures.

- d. Click **Save**.
 - e. Click **Close**.
7. In the navigation pane, click the newly created site.
8. Click the **Expand** icon next to the **Add** button.
9. Click the **Add Organization Chart Items** icon.
10. On the Department tab, enter the information in the following fields:
 - a. In the **Department name** field, enter a name for the department.
 - b. In the **Department site** field, select the site that you created.
 - c. In the **Department description** field, enter a description for the department.
 - d. Click **Save**.
 - e. Click **Close**.
11. In the navigation pane, click the newly created department.
12. Click the **Expand** icon next to the **Add** button.
13. Click the **Add Organization Chart Items** button.
14. On the Team tab, enter the information in the following fields:
 - a. In the **Team name** field, enter a name for the team.
 - b. In the **Team department** field, select the department that you created.
 - c. In the **Team description** field, enter a description for the team.
 - d. Select the **Default Sync Team** check box.
 - e. Click **Save**.
 - f. Click **Close**.

Synchronizing Avaya Control Manager and Communication Manager

About this task

The initial synchronization process synchronizes all the information from Communication Manager in to the Avaya Control Manager database.

Important:

- Use the initial synchronization process only once. If you use this process multiple times, all data is again pulled into Avaya Control Manager database and duplicate rows appear.
- Perform this procedure on the Avaya Control Manager server.

Procedure

1. Log in to the Avaya Control Manager server.

2. On the Avaya Control Manager server, go to the `<install_path>\Avaya\Avaya Control Manager <version>\Services\ACCCM Synchronizer` folder.
3. Right-click the `NAV360_Synchronizer` file and click **Run as administrator**.
4. Click **Start** to start the synchronization process.
5. Click **Yes** on the confirmation screen.
6. Perform the following steps to verify that the resources are pulled into Avaya Control Manager:
 - a. On the Avaya Control Manager webpage, click **Users**.
 - b. Select the **Users** tab.
 - c. In the navigation pane, select the site that you created in the previous procedure.
 - d. Verify that the pulled resources are available in the right pane.

Creating a Manager Server for Unified Collaboration Administration

About this task

Unified Collaboration Administration (UCA) is an Avaya Breeze® platform service that stores the static administration data for Avaya Oceana®. Control Manager uses the UCA REST API to add agent, attribute, provider, and resource information to the Avaya Breeze® platform components in Avaya Oceana®. Therefore, you must configure the Avaya Oceana® server URL connection information for Control Manager.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Avaya Oceana™ > Server Details**.
3. On the Oceana Server List page, click **Add**.
4. In the Primary Server tab, perform the following steps:
 - a. In the **Alias** field, enter an alias name for the server.
 - b. In the **API URL** field, enter the URL of the UCA ReST interface.

For example: `https://<AvayaOceanaCluster1_FQDN>/services/UCASStoreService/uca`

Important:

- If the Avaya Oceana® and Avaya Analytics™ server use the same UCA server (Common setup), the **API URL** configured on both must match, including using matching address formats. For example, you must not use an IP address on one and FQDN on the other.
- c. In the **Version** field, select the Avaya Oceana® release that you are managing through Control Manager.

- d. **(Optional)** Select the **Enable Authorization** option. For more information about the **Enable Authorization** option and its related parameters, see [Configuring token-based access between Control Manager and Avaya Oceana, Avaya Analytics, or Avaya Workspaces for Call Center Elite](#) on page 25.
 - e. In the **Deployment type** field, select any of following deployment types that shows correct type for Avaya Oceana® server that you configure. Each deployment type enforces respective guardrails for the total number of attributes assigned to all agents in the system. You can move the mouse over the field and view the guardrail details for the selected deployment type.
5. Click **Save**.
 6. Click **Test** to validate the connection details and interoperability configurations required to communicate with the system.

 Note:

- After you upgrade Control Manager, the Avaya Oceana® system that you configured sets Blank as the deployment type by default. Ensure that you change the deployment type to the appropriate value.
- Avaya Oceana® 3.8.2 and later supports the 4X Large deployment type. If the 4X Large deployment type is already selected, you cannot select an Avaya Oceana® version earlier than 3.8.2 as they do not support this deployment type.
- There is a guardrail/threshold value for a maximum number of attributes you can assign to an agent. The default value is 500.

Similarly, there is a guardrail/threshold value for maximum assigned agent attributes in the system. The threshold value depends on the Oceana system's deployment type configured in the location.

The system restricts the attributes assignment operation if the assigned attributes exceed any of the above threshold values.

- You must assign the system to a location before administering the system through Control Manager.

The following table details the total assigned attributes threshold values:

Deployment Type	Total Assigned Agent Attributes Limit in system
Small	16500
Large	165000
Extra Large	330000
3X Large	742500
4X Large	1237500

Adding an Avaya Oceana® server to a location

About this task

Control Manager supports multiple Avaya Oceana® server instances. Each Avaya Oceana® server must be assigned to a different location in Control Manager.

Control Manager does not support sharing of Avaya Oceana® server across multiple locations. Therefore, add a single server to only one location. The Avaya Oceana® system assigned to a location is not available in the **System Name** drop-down for assigning to other locations.

Note:

Control Manager does not support the sharing of the Avaya Oceana® server across multiple locations. Therefore, add the server to only one location.

Before you begin

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

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Locations**.
3. On the Location List page, perform the following steps:
 - a. Select the location to add the Avaya Oceana® server.
 - b. Click **Edit** or double-click the location.
4. On the Location Edit page, perform the following steps:
 - a. Select the **Systems** tab.
 - b. Click the **+** sign.
 - c. In **System Type**, select *Avaya Oceana*.

The **System Name** field displays the name of the newly created Manager Server.

5. Leave **Sync Schedule** blank and click **Save**.
6. Click **Confirm** on the Warning message dialog box.

Adding connectors to Provisioning Server

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Services > Provisioning**.
2. On the Provisioning Services List page, perform the following steps:
 - a. Select the Provisioning Server.
 - b. Click **Edit**, or double-click the location.

3. On the Provisioning Services Edit page, perform the following steps:
 - a. Select the **Location** tab.
 - b. Move the required location from the **Available locations** list to the **Selected locations** list.
 - c. Select the **Connectors** tab.
 - d. Enable or disable a connector by selecting **Yes** or **No** from the drop-down list.
 - e. Click **Save**.

Configuring token-based access between Control Manager and Avaya Oceana®, Avaya Analytics™, or Avaya Workspaces for Call Center Elite

Complete the procedures in this section to configure token-based access between Control Manager and Avaya Oceana®, Avaya Analytics™, or Avaya Workspaces for Call Center Elite.

About this task

Token enforcement requires that the REST API client first requests a token from the Avaya Breeze® platform Authorization Service. The client sends a digitally-signed token request to the service with a list of objects to access. If the Authorization Service recognizes the client and grants access to the resource, the service returns a signed token. The client uses this token in subsequent calls to the target REST service. The service endpoint checks the validity of the token on each request and processes a request only if the token is valid.

For token-based access to work, perform the following procedures:

- Create a trust between Control Manager and Authorization service by:
 1. Obtaining the System Manager root certificate.
 2. Installing the root certificates from the Avaya Breeze® platform cluster to host the Authorization service as a trusted root certificate authority on the Control Manager application server.
 3. Updating the Avaya Oceana® UCA server URL.
- Export the Control Manager public certificate.
- Install the Control Manager public certificates in the Authorization clients list so that the Authorization service recognizes token requests from the Control Manager server.
- Assign Grants to the Control Manager client to define the list of resources that can access the Control Manager server.
- Enable token-based access in Control Manager.
- Configure the Avaya Breeze® platform assigned Client ID for Control Manager in Control Manager.

Note:

For the Multiple HA setup, you must repeat the same procedure on each application server.

Before you begin

- Ensure that you installed the signed certificates on the Control Manager deployment. For information about certificate installation, see *Installing Avaya Control Manager and Upgrading Avaya Control Manager* guides.
- On the System Manager web console, click **Services > Inventory > Manage Elements** and identify the root CA that was used to sign the certificate for one of the nodes in the Avaya Breeze® platform cluster that hosts the Authorization service.

Downloading the root certificate from Avaya Aura® System Manager

About this task

A default root certificate can be generated when Avaya Aura® System Manager is being installed. This section covers how to download and install the default root certificate or any other CA certificate that is loaded in System Manager. System Manager uses a third-party open source application called Enterprise Java Beans Certificate Authority (EJBCA). EJBCA acts as a Certificate Authority for certificate management.

For more information about System Manager, generating the default certificate, and working with certificates, see *Administering Avaya Aura® System Manager*.

* Note:

- If you are using System Manager as Certificate Authority (CA) for Avaya Oceana® and Avaya Aura® applications, then the certificate used in the following instructions is the System Manager Root Certificate or CA Certificate.
- If you are using an enterprise or third-party Certificate Authority (CA) and not System Manager as the CA, then the certificate used in the following instructions is the root certificate of the enterprise or third-party CA. The root certificate for the enterprise or third-party CA is obtained from the enterprise or third-party CA and not from System Manager. For more information, consult the enterprise or third-party CA administrator.

Procedure

1. Log in to Avaya Aura® System Manager using your credentials.
2. Navigate to **Services > Security > Certificates > Authority**.
3. On the EJBCA Administration page, on the left pane, click **Public Web**.

The system displays `Welcome to the public EJBCA pages`.

4. On the public EJBCA screen, on the left pane, in the **Retrieve** section, click **Fetch CA certificates**.
5. To download the certificate, choose any of the following:
 - Download as PEM - To download the certificate `.pem` file.
 - Download to Firefox - To install the certificate in the certificate manager of Firefox browser.
 - Download to Internet Explorer - To install the certificate on a Windows machine containing Microsoft Internet Explorer, Edge, and Chrome browsers.

Adding the System Manager root certificate to the Trusted Root Certification Authorities list

Procedure

1. Log on to the server where Avaya Control Manager is installed.
2. Click **Start > Run**.
3. In the Run dialog box, type `mmc` and click **OK**.
4. On the Console screen, click **File > Add/Remove Snap-in**.
5. On the Add or Remove Snap-ins screen, select **Certificates** from the **Available snap-ins** list and click **Add >**.
6. On the Certificates Snap-in screen, select **Computer account** and click **Next**.
7. On the Select Computer screen, select **Local computer** and click **Finish**.
8. Click **OK**.
9. On the Console screen, in the navigation pane, expand **Certificates**.
10. Right-click **Trusted Root Certification Authorities** and click **All Tasks > Import**.
11. On the Certificate Import Wizard screen, perform the following steps:
 - a. Click **Next**.
 - b. Browse to the location where you downloaded the System Manager root certificate.
For more information about obtaining the root certificate from System Manager, see *Downloading the root certificate from System Manager* in this chapter.
 - c. Select the certificate and click **Next**.
 - d. Select **Place all certificates in the following store** and click **Next**.
 - e. Click **Browse** and select **Trusted Root Certification Authorities**.
 - f. Click **Next**.
 - g. Click **Finish**.

Updating the Avaya Oceana[®] server URL

About this task

After the root certificate is installed on the Avaya Control Manager server, the Avaya Oceana[®] server URL that is used for the communication between Control Manager and the Avaya Oceana[®] server URL can be updated to specify HTTPS usage.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Avaya Oceana[™] > Server Details**.
3. Either double-click the administered Avaya Oceana[®] server, or select the administered Avaya Oceana[®] server and click **Edit**.

4. On the Avaya Oceana Server Edit page, update **API URL** to point to the HTTPS endpoint.

! Important:

- If the Avaya Oceana® and Avaya Analytics™ server use the same UCA server (Common setup), the **API URL** configured on both must match, including using matching address formats. For example, you must not use an IP address on one and FQDN on the other.

Exporting Control Manager certificate

Procedure

1. Log on to the server where Avaya Control Manager is installed.
2. Click **Start > Run**.
3. In the Run dialog box, type `mmc` and click **OK**.
4. On the Console screen, click **File > Add/Remove Snap-in**.
5. On the Add or Remove Snap-ins screen, select **Certificates** from the **Available snap-ins** list and click **Add**.
6. On the Certificates Snap-in screen, select **Computer account** and click **Next**.
7. On the Select Computer screen, select **Local computer** and click **Finish**.
8. Click **OK**.
9. On the Console screen, in the navigation pane, expand **Personal > Certificates**.
10. Select the Control Manager certificate that you want to export for authorization.
See [Adding the Authorization client to System Manager](#) on page 29.
11. Right-click on the Control Manager certificate and then select **All Tasks > Export**.
12. Click **Next** and then click **Finish**.
13. Open the exported certificate and extract the thumbprint.
14. Open the `Nav360Config.xml` file and locate the following line:

```
<certificates> <stores> <store id="Personal"> <thumbprint id="identity"> </thumbprint> </store> </stores>
```

15. Insert the thumb print of the exported certificate.

For example:

```
<certificates> <stores> <store id="Personal"> <thumbprint id="identity"> 1d8294aa33a3b6de8fb49b298c946c50b3ec0eb1</thumbprint> </store> </stores>
```

16. Save and close the `Nav360Config.xml` file.
17. Restart the Control Manager server.

Adding the Authorization client to System Manager

Procedure

1. Log on to System Manager.
2. Navigate to **Elements > Avaya Breeze® > Configuration > Authorization**.
3. On the Authorization Configuration page, click **New**.
4. On the New External Authorization Client page, do the following:
 - a. In the **Name** field, enter the name of the Control Manager server.
 - b. In the **Certificate** field, browse to the Control Manager certificate.
See [Exporting Control Manager certificate](#) on page 28.
 - c. Click **Commit**.

The new client now appears in the list of authorized clients.

Adding Grants to the Control Manager application

Procedure

1. Log on to System Manager.
2. Navigate to **Elements > Avaya Breeze® > Configuration > Authorization**.
3. On the Authorization Configuration page, select the Control Manager client that you added to System Manager.
4. Click **Edit Grants**.
5. On the Edit Grants for Authorization Client page, click **New**.
6. On the Create Grant for Authorization Client page, do the following:
 - a. In the **Resource Name** field, select **UCAStoreService**.
 - b. In the **Resource Cluster** field, select the cluster that hosts UCAStoreService.
 - c. In the **Feature** field, select **ACM**.
 - d. In the **Values** field, select the **delete**, **read**, and **write** check boxes.
7. Click **Commit**.
8. On the Edit Grants for Authorization Client page, click **New**.
9. On the Create Grant for Authorization Client page, do the following:
 - a. In the **Resource Name** field, select **OCPDataServices**.
 - b. In the **Resource Cluster** field, select the cluster that hosts OCPDataServices.
 - c. In the **Feature** field, select **access**.
 - d. In the **Values** field, select the **read** and **write** check boxes.
10. Click **Commit**.

11. Click **Done**.
12. On the Authorization Configuration page, do the following:
 - a. In the **Name** column, locate the entry for the Control Manager client.
 - b. In the **Id** column, locate the ID value for the Control Manager client and make a note of the ID value.

You must use the exact ID value when configuring the Control Manager identity.

Adding Grants to Authorization Service

Procedure

1. Log on to System Manager.
2. Navigate to **Elements > Avaya Breeze® > Configuration > Authorization**.
3. On the Authorization Configuration page, select **AuthorizationService** from the list of clients.
4. Click **Edit Grants**.
5. On the Edit Grants for Authorization Client page, click **New**.
6. On the Create Grant for Authorization Client page, do the following:
 - a. In **Resource Name**, select **UCAStoreService**.
 - b. In **Resource Cluster**, select the cluster that hosts UCAStoreService.
 - c. In **Feature**, select **UserAuthentication**.
 - d. In **Values**, select the **read** check box.
7. Click **Commit**.
8. Click **Done**.

Adding Grants to Engagement Designer

Procedure

1. Log on to System Manager.
2. Navigate to **Elements > Avaya Breeze® > Configuration > Authorization**.
3. On the Authorization Configuration page, select **EngagementDesigner** from the list of clients.
4. Click **Edit Grants**.
5. On the Edit Grants for Authorization Client page, click **New**.
6. On the Create Grant for Authorization Client page, do the following:
 - a. In the **Resource Name** field, select **UCAStoreService**.
 - b. In the **Resource Cluster** field, select the cluster that hosts UCAStoreService.
 - c. In the **Feature** field, select **ED**.

- d. In the **Values** field, select the **read** check box.
7. Click **Commit**.
8. Click **Done**.

Configuring the Control Manager identity

Before you begin

Ensure that you added the ID value of the Control Manager client that you noted from the Authorization Configuration page in System Manager in the `NavConfig.xml` file.

Procedure

1. Log on to Control Manager.
2. Select one of the following servers:
 - a. For Avaya Oceana[®], navigate to **Configuration > Avaya Oceana[™] > Server Details**.
 - b. For Avaya Workspaces for Call Center Elite, navigate to **Configuration > Customer Engagement > Avaya Workspaces for Elite**.
 - c. For Avaya Analytics[™], navigate to **Configuration > Customer Engagement > Avaya Analytics**.
3. Select the respective server and then click **Edit**.
4. On the Connection Details tab, do the following:
 - a. Select the **Enable Authorization** check box.
 - b. In **Authorization Service URL**, enter the following value:


```
https://BreezeClusterFQDN:9443/services/AuthorizationService/
token
```

BreezeClusterFQDN is the FQDN of the cluster that hosts the Authorization service.
 - c. From **Breeze alias**, select the alias of the Breeze instance.
5. Click **Save**.

Enabling the token enforcement in UCA

Procedure

1. On the System Manager web console, click **Elements > Avaya Breeze[®] > Configuration > Attributes**.
2. On the Service Clusters tab, select **UCAStoreService**.
3. In the **Advanced** group, set the **Enable Tokenless Access** attribute to **FALSE**.
4. Click **Commit**.

Personal Certificates pools for Breeze authorization

About this task

If more than one certificate is present in the Personal Certificates pool then you must specify the certificate used for authorization service in the `ACCCMUCAProxyService.exe.config` file of the UCA proxy service.

Procedure

1. Stop the UCA Proxy service.
2. Change to the directory to `<install_path>\Services\ACCCM UCA Proxy Service`
3. Open the `ACCCMUCAProxyService.exe.config` file.
4. Set the valid certificate thumbprint value for "BreezeAuthorizationCertificateThumbnil".

For example:

```
<add key="BreezeAuthorizationCertificateThumbnil"
value="783404B433022475F588333B5A19C013021ABB1C"/>
```

5. Restart the UCA Proxy service.

Assigning a location to the UCA proxy server

About this task

Use this procedure if Avaya Control Manager services are segregated based on the Avaya Control Manager locations.

Before you begin

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

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Services > UCA Proxy**.
3. Double-click the administered UCA proxy server or select the administered UCA proxy server and click **Edit**.
4. Select the **Location** tab.
5. Move the location that contains the UCA server from the **Available locations** list to the **Selected locations** list.
6. Click **Save**.

Assigning location to Application Server

About this task

Use this procedure only if Avaya Control Manager services are segregated based on Avaya Control Manager locations.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Services > Application Server**.
2. On the Application Server List page, perform the following steps:
 - a. Select the Application Server to which you want to assign a location.
 - b. Click **Edit**.
3. On the Application Server Edit page, perform the following steps:
 - a. Select the **Location** tab.
 - b. Move the required location from the **Available locations** list to the **Selected locations** list.

Ensure that you move the location that contains the UCA server to the relevant Avaya Control Manager services.
 - c. Click **Save**.

Assigning location to Synchronizer Service Server

About this task

Use this procedure only if Avaya Control Manager services are segregated based on Avaya Control Manager locations.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Services > Synchronizer**.
2. On the Synchronize Services List page, perform the following steps:
 - a. Select the Synchronizer Service Server to which you want to assign a location.
 - b. Click **Edit**.
3. On the Synchronize Service Edit page, perform the following steps:
 - a. Select the **Location** tab.
 - b. Move the required location from the **Available locations** list to the **Selected locations** list.

Ensure that you move the location that contains the UCA server to the relevant Avaya Control Manager services.
 - c. Click **Save**.

Testing the UCA REST connection

About this task

Use this procedure to test the UCA REST connection.

Note:

By default, UCA requires an authentication token to be supplied in REST request headers. For testing or troubleshooting purposes, you must enable tokenless access by setting the **Enable Tokenless Access** attribute of UCASoreService to `TRUE`. The change is effective as soon as System Manager replicates the setting to the nodes. After you complete the testing or troubleshooting, you must reset this attribute to `FALSE`.

Before you begin

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

Procedure

Perform one of the following steps to view all Providers:

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

```
https://<AvayaOceanaCluster1_FQDN>/services/UCASoreService/uca/  
providers
```

2. Perform the following steps:

- a. Install a REST client on your Internet browser. For example, Postman application on Chrome.
- b. In the **Get** field, enter the following request URL:

```
https://<AvayaOceanaCluster1_FQDN>/services/  
UCASoreService/uca/providers
```
- c. Click **Send**.

The test returns one of the following results:

- On a newly created system, the test returns an empty JSON block (`[]`).
- On a system with providers configured, the test returns the provider information in JSON format.

Note:

If the test returns an HTTP error, you must investigate and resolve the error.

Categories, Attributes, and Attribute Sets

Categories

Categories are the ways of grouping attributes. For example, the French and Spanish attributes are in the Language category. Categories are used in Property Management to configure how property values are derived for attribute sets that do not have explicit property values defined.

Attributes

Attributes are the main basis to select from available resources to be assigned work, or to select waiting work to be assigned to the newly available resources. When selecting a resource to be assigned to incoming work, the resource must have the desired attributes specified in the work request. When selecting a waiting work request for a newly available resource, the work request must have attributes that match those of the resource.

Attribute Sets

Attribute Sets are the collections of attributes. Attribute Sets can be configured for a property value, so that each property can have different values depending on which attributes are used. As an example, for the Proficiency property, a resource has high proficiency in the attribute set “English, Sales, Tablets”, low proficiency for the attribute set “English, Service, Laptops”, and low proficiency for the attribute set “Spanish”.

Users, Accounts, and Providers

Users

A user is at the highest level in the hierarchy and represents a human or an object. A user involved in Work Assignment is referred to as Work Assignment Resource.

Resource Account

A user can have one or more Resource Accounts. A Resource Account is an accessible address such as email and phone number.

Account Sources or Providers

A source is a system that hosts the Resource Accounts. For example, Communication Manager, an external Email provider, or a Chat host.

Assignment Management

The assignment of attributes and property values to users.

Property Management

The configuration of property definitions, including their category list and their default values. For example, Multiplicity Count, Proficiency, and Service Exclusion.

Channel Attributes

By default, Work Assignment contains Default Category Channel and several Default Channel attributes such as Email, Voice, and Chat. Channel Attribute is a special type of attribute that is automatically assigned to the user as Resource Accounts are created for that user. The Channel category cannot be edited. Channels can be included in attribute sets for Property Management.

Adding Attribute Categories to Avaya Control Manager

About this task

Add attribute categories to support Avaya Oceana® contact routing.

! Important:

To use the sample self-service applications or workflows to validate contact routing, you must create the Language, Service and Location categories.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. On the Attribute Categories tab, click **Add**.
3. On the Attribute Category tab, perform the following steps:
 - a. In the **Name** field, enter the name of the category.
For example, Language.
 - b. Click **Save**.

Adding Attributes to Avaya Control Manager

About this task

Add attribute values for categories to support Avaya Oceana® contact routing.

! Important:

- To use the sample self-service applications or workflows to validate contact routing, you must add values for the Language, Service, and Location categories. For the Location category, add the 'Inhouse' value for the sample workflows to function correctly.
- Avaya Oceana® supports viewing Customer Journey in Avaya Workspaces by topic. A topic is an identifier that you can use to correlate intent across multiple channels. For example, a customer inquiry about an insurance claim can traverse across multiple media channels. Topics can unify those interactions in the customer journey. If no topic value exists when a contact is created, a default value is provided. The default value is a combination of the Language and Service attributes, which demonstrates how to link cross-channel interactions that arrived for a topic. The default value can only be provided if Language and Service attribute values exist.

Before you begin

- Avaya Oceana® Cluster 1 should be in a running and accepting state.
- On the UI page, attributes are listed based on the logged-in user's permissions to view the Avaya Control Manager groups of Avaya Oceana® attributes. Users can only view attributes that belong to assigned attribute groups.
- Avaya Control Manager administrators and supervisors should have appropriate Avaya Control Manager groups of attributes assigned as part of groups to view permissions.
- Avaya Control Manager administrators or supervisors with no groups-to-view permission on attribute groups can view all attributes in the location without restrictions.

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. On the Attributes tab, click **Add**.
3. On the Attribute tab, perform the following steps:
 - a. In the **Attribute Category** field, select the attribute category that you have created.
For example, type `Language` or `Location`.
 - b. In the **Attribute Value** field, enter a value for the attribute.
For example, type `English` or `Inhouse`.
 - c. Click **Save**.

Adding services to Avaya Control Manager

About this task

Use this procedure to add services to Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. Click the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a service, do the following:
 - a. In the **Service Name** field, enter the name of the service.
 - b. Select the **Available for Transfer** check box.

The system automatically selects the **Agent Display** check box.

Note:

You must always check the **Agent Display** check box regardless of this service being a normal routed service or a transfer service.

- c. In the **After Contact Work Timer (Seconds) ***, enter a value (in seconds).

Important:

You can set **After Contact Work Timer (Seconds) *** at a channel or at a service basis. If this field is set to 0 and a call comes in on that service, no ACW occurs. If there value is > 0, then this value is used for ACW and it overrides the channel ACW setting. If a call comes in, that does not match a service attributes then the ACW time at a channel level is used.

- d. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
- e. Click **Save**.

When creating service name tags, it is recommended that you use high-level business appropriate designations and do not create a display name for every combination of attributes that can possibly be routed.

- Recommendation 1: Omit the channel from the **Displayname** of the service. For example, instead of creating:

Displayname	Attributes
ChatSales	Department.Sales, Channel.Chat
EmailSales	Department.Sales, Channel.Email
SMSSales	Department.Sales, Channel.SMS

Create:

Displayname	Attributes
Sales	Department.Sales, Channel.Chat

- Recommendation 2: Omit system or functional attributes from the **Displayname** of the service. For example, instead of creating:

Displayname	Attributes
NoviceSupportGroup	Department.Support, AgentExpertise.Novice, Channel.Chat
RegularSupportGroup	Department.Support, AgentExpertise.Regular, Channel.Email
ExpertSupportGroup	Department.Support, AgentExpertise.Expert, Channel.Chat

Create:

Displayname	Attributes
Support	Department.Support, Channel.Chat

Configuring Properties in Avaya Control Manager

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. On the Properties tab, double-click the property that you want to configure.

For example, Multiplicity.

 Note:

- Attributes are listed on the basis of the logged in user's permissions to view the ACM groups of Oceana attributes. Users can view attributes that belong to assigned attribute groups.
- Avaya Control Manager administrators and supervisors must have appropriate ACM groups of attributes assigned as a part of groups to view permissions.
- Avaya Control Manager administrators and supervisors must have permission to view at least one attribute from each category. If you do not have permissions, the system does not display categories and attribute sets.

Administrator and supervisor must have permission to view all the selected attributes set in the attributes set if they click on already configured **Proficiency** or **Service exclude** property for editing. If you do not have permissions, the system does not display categories and attribute sets.

In order to correct permissions, verify the categories configured in the Work Assignment Properties, the attributes of the respective categories and the attributes of the ACM attribute groups assigned to the Administrator/Supervisor as groups to view.

- Avaya Control Manager administrators or supervisors having no groups-to-view permission on attribute groups can view all attributes in the location without any restriction.

3. On the Property tab, make the required changes in the fields and click **Save**.

For example, to configure Multiplicity, you can change the value in the **Default Value** field.

Configuring a secure connection between Avaya Control Manager and UCA Server

Obtaining the root certificate from System Manager

About this task

Use the following procedure to download the root certificate.

 Note:

- If you are using System Manager as Certificate Authority (CA) for Avaya Oceana® and Avaya Aura® applications, then the certificate used in the following instructions is the System Manager Root Certificate or CA Certificate.
- If you are using an enterprise or third-party Certificate Authority (CA) and not System Manager as the CA, then the certificate used in the following instructions is the root certificate of the enterprise or third-party CA.

Procedure

1. In your web browser, enter the following URL for the System Manager installation of EJBCA:

`https://<SMGR_FQDN>/ejbca/`

2. In the Retrieve Certificates section, click **Fetch CA Certificates**.
 3. Based on your browser, perform one of the following steps:
 - To install the certificate in the certificate manager of Firefox, click the **Download to Firefox** link.
 - To install the certificate on a Windows machine containing Microsoft Internet Explorer, Edge, and Chrome, click the **Download to Internet Explorer** link.
- The system prompts you to save the certificate.
4. Save the certificate.

Adding the System Manager root certificate to the Trusted Root Certification Authorities list

Procedure

1. Log on to the server where Avaya Control Manager is installed.
2. Click **Start > Run**.
3. In the Run dialog box, type `mmc` and click **OK**.
4. On the Console screen, click **File > Add/Remove Snap-in**.
5. On the Add or Remove Snap-ins screen, select **Certificates** from the **Available snap-ins** list and click **Add >**.
6. On the Certificates Snap-in screen, select **Computer account** and click **Next**.
7. On the Select Computer screen, select **Local computer** and click **Finish**.
8. Click **OK**.
9. On the Console screen, in the navigation pane, expand **Certificates**.
10. Right-click **Trusted Root Certification Authorities** and click **All Tasks > Import**.
11. On the Certificate Import Wizard screen, perform the following steps:
 - a. Click **Next**.
 - b. Browse to the location where you downloaded the System Manager root certificate.

For more information about obtaining the root certificate from System Manager, see *Downloading the root certificate from System Manager* in this chapter.
 - c. Select the certificate and click **Next**.
 - d. Select **Place all certificates in the following store** and click **Next**.
 - e. Click **Browse** and select **Trusted Root Certification Authorities**.
 - f. Click **Next**.
 - g. Click **Finish**.

Updating the Avaya Oceana[®] server URL

About this task

After the root certificate is installed on the Avaya Control Manager server, the Avaya Oceana[®] server URL that is used for the communication between Control Manager and the Avaya Oceana[®] server URL can be updated to specify HTTPS usage.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Avaya Oceana[™] > Server Details**.
3. Either double-click the administered Avaya Oceana[®] server, or select the administered Avaya Oceana[®] server and click **Edit**.
4. On the Avaya Oceana Server Edit page, update **API URL** to point to the HTTPS endpoint.

Important:

- If the Avaya Oceana[®] and Avaya Analytics[™] server use the same UCA server (Common setup), the **API URL** configured on both must match, including using matching address formats. For example, you must not use an IP address on one and FQDN on the other.

Configuring Avaya Oceana[®] system properties using Control Manager

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Avaya Oceana[™] > Server Details**.
3. Double-click the administered Avaya Oceana[®] server, or select the administered Avaya Oceana[®] server and click **Edit**.
4. Click the **System Properties** tab.
5. Expand **Context Store**.
6. In the **Oceana Core Data Service Collected Digits Key** field, type `CustomerId` or `CollectedDigits`.
7. Expand **Omni Channel**.
8. In the **Omni Channel Database Server** field, enter the name of the Omnichannel Database server as administered in the HTTPS certificate installed on the Omnichannel Database server. The name not only must match the name on the certificate, but the certificate must also be trusted to avoid any certificate errors.
9. In the **Omni Channel Database Server Port Number** field, enter 443.
10. Select the **Https** check box to have a secure communication between Avaya Control Manager and your Omnichannel server.

 Important:

Verify that you are able to communicate with the Omnichannel Database server through the web and without any certificate errors.

11. Expand **RONA**.

12. In the **RONA Timer(Seconds)** field, enter the RONA time for non-voice channels in seconds.

Enter a value in the range of 26 to 100 seconds.

13. Expand **After Contact Work**.

14. Select the **Enable After Contact Work** check box.

15. Select the **Allow agent to extend ACW** check box so that the agents in the After Contact Work state can extend the time they are in After Contact Work.

If you select this check box, interactions in After Contact Work have an **Extend** button on the work card. Agents can click the **Extend** button to extend the After Contact Work time.

16. Enter the **After Contact Work Timer** value in seconds for each channel.

Ensure that you enter a value in the range of 0 to 9999 seconds. These fields become disabled or read-only if you uncheck the **Enable After Contact Work** check box.

 Note:

Avaya Oceana® supports **After Contact Work Timer** per channel settings in version 3.8.1. Avaya Oceana® version 3.8 supports only one global **After Contact Work Timer** setting.

- After Contact Work Timer for Voice (Seconds)
- After Contact Work Timer for Email (Seconds)
- After Contact Work Timer for Chat (Seconds)
- After Contact Work Timer for Messaging (Seconds)
- After Contact Work Timer for Short Messaging Service (Seconds)
- After Contact Work Timer for Social (Seconds)
- After Contact Work Timer for WebVoice (Seconds)
- After Contact Work Timer for Video (Seconds)
- After Contact Work Timer for Generic (Seconds)

 Note:

POM or outbound channel uses Avaya Control Manager setting of Voice channel.

17. Expand **Workspaces**.

18. In the General area, administer the following options:

- a. In the **Avaya Oceana Workspaces Welcome Page URL** field, enter the URL of an optional web page that is to be presented to agents within the Avaya Workspaces welcome widget.

This widget is displayed out-of-the-box when the agent logs in or can be added as part of another layout.

The Welcome page does not support the `X-Frame-Options: deny` HTML tag.

- b. Enter a value in the **Workspaces time-out in seconds** field.

Use this field to configure the time-out value for an idle agent. Time-out count starts when the browser on agent's screen is disconnected. After the time-out, the status of an agent is set to `Not Ready` with a system code as configured in **Default Not Ready code when browser disconnects** parameter. Work is not routed to an agent when in Not Ready state.

The maximum value of time-out is 300 seconds. Until Release 3.5, the value was specified in minutes. You must re-enter this value if you are upgrading from Avaya Oceana® Release 3.5 or earlier to a later Avaya Oceana® Release.

- c. Select the **Enable mandatory disposition code for contacts** check box to mandate the disposition codes. The agents must set a disposition code to close an interaction.
- d. Select the **Outgoing Email address is blank by default** checkbox to display a blank **select a value** drop-down in the **Workspaces**.

19. In the Global Screenpop Behaviours area, do the following:

- a. Select the **Launch external Screen-pops on Agent Accept** check box to open external screen pops in new browser windows when an agent answers an interaction.
- b. Select the **Display internal Screen-pops Widget first on Agent Accept** check box to display the screenpop widget instead of the contact type widget when an agent accepts an interaction.

 Important:

Before enabling this feature, you must configure the Screen-pop widget and verify that the widget is working correctly in Avaya Workspaces. Do not make the Screen Pop tab the default tab until you verify that the screen pops are working correctly.

20. In the Supervisor area, do the following:

- a. Select the **Notify Agent Being Observed by Supervisor** check box to notify an agent that the supervisor is monitoring the agent.
- b. Select the **Supervisor Can Modify Agent State** check box so that all supervisors can modify the state of an agent when the agent is inactive.
- c. In the **Supervisor Custom Link URL** field, enter a custom URL that you can view in Avaya Workspaces.

21. In the Widget Library area, do the following:

- a. Select the **Enable An External Widget Library** check box to enable the external widget library to include additional widgets in Avaya Workspaces.
- b. In the **Workspaces Library URL** field, enter the URL of an external widget library that you want to load in Avaya Workspaces.

 Note:

This is a mandatory field. Do not leave it blank.

22. In the **Avaya Workforce Engagement Select (AWES)** area, select the **Avaya Workforce Engagement Select Enabled** check box to indicate that Avaya Workforce Engagement Select is available as part of the Avaya Oceana® deployment.

23. Expand **Thresholds**.

24. In the **Short Not Ready** field, enter the appropriate value in seconds.

Enter a value of zero (0) to 999999999 seconds. This value is used to identify the number of times agents went into the Not Ready state and remained in that state for a duration less than the value configured in this field.

 Important:

This is a mandatory field. Therefore, you must not leave this field blank.

25. Expand **System Default Codes**.

26. In the **Default Not Ready code when browser disconnects** drop-down list, select a reason code from the available reason codes.

 Important:

Before using this option, ensure that you have created the **not ready reason** code in **Configuration > Avaya Oceana > Reason Codes** as the **User Codes** field. The drop-down contains a list of all user codes created in the UCA.

27. Expand **Transfer to User**.

28. Select the **Enable Transfer to User** check box.

Avaya Control Manager administrators can enable or disable the Transfer to User feature. Based on this configuration, agents or supervisors can view the Transfer to User option in Avaya Workspaces.

29. Expand **Disposition Codes**.

The following are the channels under Disposition Codes. Using Control Manager, you can make disposition codes mandatory for each of the channels below. If you do not have any disposition code configured for a channel, you cannot make it mandatory.

- Voice
- Email

- Social
- Generic
- Messaging
- Short Message Service
- Chat
- Outbound
- Video

30. Click **Save**.

Starting Omnichannel Administration Utility

About this task

Use this procedure to start Omnichannel Administration Utility from the Avaya Control Manager web interface.

Note:

If you are using Chrome or Firefox, then a ClickOnce plugin must be installed on the browser before the user launches the Oceana administration client or the OCMT.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Omnichannel Administration**.
2. Click **Launch OC Database Administration Client**.

Avaya Control Manager starts Omnichannel Administration Utility.

Starting Oceana Customer Management Tool

About this task

Use this procedure to start Oceana Customer Management Tool from the Avaya Control Manager web interface. Oceana Customer Management Tool (OCMT) is a ClickOnce application. You must open the Oceana Customer Management Tool using the browser with which you downloaded the ClickOnce application.

Before you begin

Ensure that you have downloaded and installed the following:

- OmniDB server certificate in the trust store of the client's machine.
- Root CA certificate used to create the OmniDB certificate in the trust store of the client's machine.
- .Net framework that matches the .Net framework version of the OCMT client on the client's machine.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Omnichannel Administration**.
2. Click **Launch Customer Management Client**.

The system starts Oceana Customer Management Tool.

Work Codes, Disposition Codes, and Rejection Codes

Work Codes are tags that an agent can set at any point in a contact. Work Codes describe what is going on with the contact at that time. For example, if a customer calls a television service provider to complain about poor service, the agent can tag the first part of the call as `ServiceComplaint`. After resolving the complaint, the agent can inform the customer about a special offer and tag the call as `UpSell`. If the customer agrees to renew the subscription, the agent can further tag the call as `SubscriptionRenewal`.

Disposition Codes are tags that indicate the final state of the contact when the agent closes the contact. For example, `ComplaintResolved`, `DissatisfiedCustomer`, and `FollowUp`. Agents can also set Disposition Codes during the course of a contact to capture the actions that the agents need to do. For example, `PostBrochure`, `CustomerCallback`, and `LikeOnSocial`.

Defer Codes are tags that an agent can set when deferring an email. For example, `WarehouseContact`, `In-store`, `PhoneRepair`, and `LoyaltyCustomer`.

Rejection Codes are tags that indicate the rejected state of the email when an approver rejects emails. When an approver rejects emails, mandatory rejection reason codes must be assigned to the contacts.

Configure Alarms and Events

System Manager provides an Operating System (OS)-level SNMP Master (Net-SNMP) agent for platform monitoring, notification sending, and notification destination & SNMPv3 user management.

If you change the Trap Listener settings as an administrator, you must create a new SNMP target profile for the System Manager IP address and a new SNMPv3 user profile for System Manager. The values in the new profiles must match the values in the Trap Listener settings. In addition, you must attach the System Manager SNMPv3 user profile to the System Manager target profile, and then attach the new SNMP target profile to all Serviceability Agents.

For more information about creating SNMP user profiles and target profiles and attaching the target profiles to Serviceability Agents, see *Administering Avaya Aura® System Manager*.

For more information about SNMP, see *Avaya Aura® System Manager SNMP Whitepaper*.

Creating an SNMPv3 user profile

About this task

Use this procedure to create a user profile with read and write privileges for SNMP MIBs.

Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Serviceability Agents > SNMPv3 User Profiles**.
2. On the SNMPv3 User Profiles page, click **New**.
3. On the New User Profile page, perform the following steps:
 - a. In the **User Name** field, enter the user name.
Specify the user name as initial.
 - b. In the **Authentication Protocol** field, select the authentication protocol.
 - c. In the **Authentication Password** field, enter an authentication password.
 - d. In the **Confirm Authentication Password** field, re-enter the authentication password.
 - e. In the **Privacy Protocol** field, select the privacy protocol.
 - f. In the **Privacy Password** field, enter a privacy password.
 - g. In the **Confirm Privacy Password** field, re-enter the privacy password.
 - h. In the **Privileges** field, select `Read/Write`.
 - i. Click **Commit**.

Creating an SNMP target profile

About this task

The System Manager TrapListener service receives traps from different applications and displays the information on the System Manager Alarming page.

Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Serviceability Agents > SNMP Target Profiles**.
2. On the SNMP Target Profiles page, click **New**.
3. On the New Target Profile page, on the Target Details tab, perform the following steps:
 - a. In the **Name** field, enter a name for the target profile.
 - b. In the **Description** field, enter a description for the target profile.
 - c. In the **IP Address** field, enter the appropriate IP address.
 - d. In the **Port** field, enter the appropriate port number.
 - e. In the **Notification Type** field, select the notification type.

- f. In the **Protocol** field, select the protocol.

This information must match with the Trap Listener profile. You can view the Trap Listener profile by clicking **Services > Configurations > Settings > SMGR > TrapListener**

4. On the New Target Profile page, on the Attach/Detach User Profile tab, perform the following steps:
 - a. Select the initial user profile.
 - b. Click **Assign**.
 - c. Click **Commit**.

Assigning Serviceability Agents

About this task

The Serviceability Agent is an enhanced version of the SAL agent for forwarding logs, harvesting logs, and alarming. The Serviceability Agent sends SNMPv3 traps and notifies the configured NMS destinations. System Manager and the SAL gateway are the two mandatory destinations.

Using the Serviceability Agent user interface you can:

- Manage and configure SNMPv3 users remotely
- Manage and configure SNMP trap destinations remotely
- Create, edit, view, and delete user and target profiles

Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.
2. On the Serviceability Agents page, select the relevant nodes and click **Manage Profiles**.
3. On the Manage Profile page, perform the following steps:
 - a. Select the **SNMP Target Profiles** tab.
 - b. Select the SNMP target profile that you created.
 - c. Click **Assign**.
 - d. Select the **SNMPv3 User Profiles** tab.
 - e. Select the user profile that you created.
 - f. Click **Assign**.
 - g. Click **Commit**.

Verifying the configuration

Procedure

1. On the System Manager web console, click **Services > Inventory > Manage Serviceability Agents > Serviceability Agents**.

2. Select the nodes for which you want to generate alarms.
3. Click **Generate Test Alarm**.

System Manager generates a test alarm. You can view the alarm by clicking **Services > Events > Alarms**.

Configure voice resources

Configuring a Communication Manager Hunt Group

About this task

Important:

Skip this procedure if you have configured the Communication Manager Hunt Group using the Communication Manager System Access Terminal (SAT) interface.

Use this procedure to configure a Communication Manager Hunt Group. Since all Work Assignment agents must be in a single pool, they must be in the same Hunt Group or Skill.

Procedure

1. On the Avaya Control Manager webpage, click **Communication Manager Objects > Hunt Group**.
2. On the Hunt Group page, click **Add**.
3. In the **Location** field, select the location to which the Hunt Group is assigned.
4. In the **Group Number** field, enter a group number.

This value is used for the Hunt Group as the provider value in the System Manager Source Details section of the Work Assignment agent configuration.

5. In the **Group Name** field, enter the Hunt Group name.
6. In the **Extension** field, enter the Hunt Group extension number.
7. Perform the following steps to add an extension to the Hunt Group:
 - a. In the **Add Extension Number** field, enter the extension number.
 - b. Click **Add Extension**.

The system displays the extension in the bottom of the screen.

8. Perform the following steps to add an extension range to the Hunt Group:
 - a. In the **Start from extension** field, enter the first extension number of the extension range.
 - b. In the **End at extension** field, enter the last number of the extension range.
 - c. Click **Add Range**.

The system displays the extensions in the bottom of the screen.

9. Click **Add Extension From Location List** to get a list of extensions that are assigned to the Hunt Group location.

You must use this option when working in a location-based environment.

10. To add an extension, select the option next to the extension and click **Add**.
11. Click **Save**.

Creating variables using Avaya Control Manager

About this task

Important:

Skip this procedure if you have configured the Communication Manager variables using the Communication Manager System Access Terminal (SAT) interface.

Communication Manager vectors use variables to improve efficiency. Different types of variables are available to meet different types of call processing needs. Vector variables can be added to consider location, messaging, and adjunct routing vector steps. Based on the variable type, variables can use call-specific data or fixed values that are identical for all calls. In either case, an administered variable can be reused in many vectors.

Avaya Oceana[®] has a number of initial vectors:

- Fallback Vector - Automatically routes calls to Elite when Avaya Oceana[®] is down
- Ingress Vector - Initiates the Adjunct Route
- Treatment Vector - Provides treatments for calls that route to Avaya Oceana[®]
- Routing Vector - Collects the digits set by the Adjunct Route application.

These digits contain the Agent ID.

- RONA Vector - To handle Voice Redirect On No Answer (RONA) scenarios
- Coverage Vector - To route callers to a voice mail mailbox
- Transfer to Service Vector - To initiate the Adjunct Route

These vectors require the following variables:

- Routing Vector requires a variable used to collect Agent ID.
- Avaya Oceana[®] vectors require a Persistent variable.

This variable is used to differentiate between the types of call ingress: (1) Elite-anchored / Adjunct Route path or (2) the Web Voice / Avaya Breeze[®] platform-anchored path.

Procedure

1. On the Avaya Control Manager webpage, click **Communication Manager Objects > Variable**.
2. On the Variable page, click **New**.
3. In the **Location** field, select your Communication Manager.

4. In the **Variable** field, enter a name for the variable. For example, A.

 Important:

Ensure that your Communication Manager does not already have a variable configured with the same name.

5. In the **Description** field, enter a description for the variable as `Adjunct Route Digits`.

This standard description makes maintenance and troubleshooting easier.

6. In the **Type** field, select `collect`.
7. In the **Scope** field, select `L`.
8. Click **Save**.
9. On the Variable page, click **New**.
10. In the **Location** field, select your Communication Manager.
11. In the **Variable** field, enter a name for the variable. For example, B.

 Important:

Ensure that your Communication Manager does not already have a variable configured with the same name.

12. In the **Description** field, enter a description for the variable as `Adjunct Route Flag`.

This standard description makes maintenance and troubleshooting easier.

13. In the **Type** field, select `collect`.
14. In the **Scope** field, select `P`.
15. Click **Save**.
16. Add any further variables as required for your solution. For example, add the variables as shown below.

Example

change variables							Page 1 of 39
VARIABLES FOR VECTORS							
Var	Description	Type	Scope	Length	Start	Assignment	VAC
A	Adjunct Route Digits	collect	L	16	1		
B	Adjunct Route Flag	collect	P	1	1		
C	ASAI Data	asaiuui	L	2	1		
D							
E	Collected Digits I	collect	L	6	1		
F	Collected Digits II	collect	L	1	1		
G	Collected Digits III	collect	L	1	1		
H	Collected Digits Concat	collect	L	8	1		
I	Collected Digits UUI	asaiuui	L	8	1		
J							
K	Expected Wait Time	collect	L	5	1		
L							
M							
N							
O	Oceana Routing	collect	P	1	1		
P							
Q	Oceana In Service	value	G	1		1	VV1
R							

Configuring Vector Directory Numbers

About this task

! Important:

Skip this procedure if you have configured the Communication Manager Vector Directory Numbers (VDNs) using the Communication Manager System Access Terminal (SAT) interface.

Use this procedure to configure VDNs for Avaya Oceana®. A VDN is an extension that directs an incoming call to a specific vector. This number is a virtual extension number which is not assigned to an equipment location. VDNs must follow your dial plan.

Create a VDN for each of the following:

- Ingress Vector to Adjunct Route
- Routing Vector
- RONA Vector
- Transfer to Service Vector

Procedure

1. On the Avaya Control Manager webpage, click **Communication Manager Objects > VDN**.
2. On the VDN page, click **Add**.

3. In the **Location** field, select the location.
4. In the **VDN Number** field, enter the VDN.
5. In the **VDN Name (English)** field, enter the VDN name that is added to the Communication Manager.
 - The name must be in English.
 - The name must have up to 22 letters
 - The name must not have any special character other than underscore (_).
6. In the **Description** field, enter a description for the VDN.
7. In the **VDN TEMPLATE** field, select a template.

The VDN default settings are populated based on the selected template.
8. Click **Save**.
9. Repeat step 2 through 8 to add more VDNs.

Adding Provider, Skills, VDN, and Extensions to Avaya Oceana®

About this task

Use the following procedure to configure the required voice resources for Avaya Oceana®.

You can select and use 1 Routing VDN for voice. You can select multiple VDNs for other VDN types. To provide different wait treatments to different callers, Avaya recommends using a single Ingress VDN and multiple Treatment VDNs and vectors. You can configure the voice workflow to differentiate between callers based on data, such as the caller number, routing attributes, or any other available data.

Before you begin

- Ensure that Avaya Oceana® Cluster 1 is in the running and accepting state.
- Ensure that you use Dial Plan when using a shared Communication Manager with Avaya Oceana® or Avaya Workspaces for Call Center Elite.

Procedure

1. Log on to Control Manager.
2. Navigate to **Configuration > Avaya Oceana™ > Server Details**.
3. Do one of the following:
 - Double-click the administered Avaya Oceana® server and click **Edit**.
 - Select the administered Avaya Oceana® server and click **Edit**.
4. Select the **Providers** tab.
5. To add the Voice Communication Manager, do the following:
 - a. Click **Add**.
 - b. From the **Type** drop-down list, select **CM**.

- c. In the **Name** field, type the same name as the `providerId` value that you entered when creating the CSC attributes in the Communication Manager list.

- d. In the **Address** field, type the address in the following format:

`<Oceana Routing VDN>@<domain name>.com`

For example, type: `8284000@domain.com`

`<Oceana Routing VDN>` is the VDN that you configured in Communication Manager.

 Important:

This VDN extension number must match the Routing VDN you configure in Step 12 and Step 13.

- e. **(Optional)** In the **Voice mail Access** field, type the number to access the voice mail system through Avaya Workspaces.

- f. **(Optional)** In the **External Access Code** field, type the number to make an external voice call.

Avaya Workspaces prefixes this number when an agent makes an external call.

- g. Select or clear the **Video Enabled** check box to enable or disable the provider to support video with voice.

When you select this check box, you can assign both voice and video channels to the agents who have accounts for this provider.

- h. Click **Save**.

 Important:

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

6. Select the **Skill** tab.

7. Move the single required Hunt Group from the **Available Skill** list to the **Selected Skill** list.

 Note:

When you use Avaya Control Manager (ACM) for an Avaya Workspaces agent to add or remove a skill, the agent must log out from Avaya Workspaces and log back in for the application to reflect the changes.

8. Click **Save**.

9. Select the **VDN** tab.

10. From the **Avaya Oceana VDN Type** drop-down list, select **Ingress**.

11. Move the required Ingress VDNs from the **CM VDNs** list to the **Selected** list.

12. In the **Avaya Oceana VDN Type** field, select **Routing**.

13. Move the single required Routing VDN from the **CM VDNs** list to the **Selected** list.

14. In the **Avaya Oceana VDN Type** field, select **Treatment**.
15. Move the required Treatment VDNs from the **CM VDNs** list to the **Selected** list.
16. In the **Avaya Oceana VDN Type** field, select **RONA**.
17. Move the required RONA VDNs from the **CM VDNs** list to the **Selected** list.
18. In the **Avaya Oceana VDN Type** field, select **Transfer**.
19. Move the required Transfer to Service VDNs from the **CM VDNs** list to the **Selected** list.
20. In the **Avaya Oceana VDN Type** field, select **Coverage**.
21. Move the required Coverage VDNs from the **CM VDNs** list to the **Selected** list.
22. In the **Avaya Oceana VDN Type** field, select **Fallback**.
23. Move the required Fallback VDNs from the **CM VDNs** list to the **Selected** list.
24. In the **Avaya Oceana VDN Type** field, select **Survey**.
25. Move the required **Survey VDNs** from the **CM VDNs list** to the **Selected** list.
26. Click **Save**.
27. Select the **Extensions** tab.
28. To add DMCC extensions, select the **Recorder Extension**.
29. Move the required extensions from the **Available Extensions** list to the **Selected Extensions** list.
30. Click **Save**.

Creating a user to handle Voice contacts

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.
3. Click **Add**.
4. 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.



Note:

You must enter a value in this field only if the agent has to handle Voice contacts.

- i. In the **AVAYA Login** field, enter the Elite agent login ID.

When creating an agent, if the **Profile** field is set to **Agent** and the **AVAYA Login** field is populated, then this agent is added to Elite. However, if the **AVAYA Login** field is not populated, then this agent is not added to Elite. Therefore, the agent cannot handle Avaya Oceana® Voice contacts. This type of agent can handle only Multimedia contacts.

- j. Select **Team** as required.

- k. Select **Template** as required.

- l. Click **Save**.

5. Scroll to the right and select the **Avaya Oceana** tab.

6. Select the **Voice** check box.



Important:

To change the channel of an agent while the agent is live, the agent must be logged out and logged in again.

7. **(Optional)** Select the **Prompt agent for extension number at login** check box to enable Hot Desking.

If you enable Hot Desking, agents can change their extension number.

8. Click **Save**.

Adding attributes to an agent

About this task

Use this procedure to add routing attributes to an agent.

Procedure

1. On the Avaya Control Manager webpage, click **Users**.
2. Select the **Users** tab.

3. Select a user and click **Edit User**.
4. Scroll to the right and select the **Avaya Oceana** tab.
5. Ensure the user has a Voice account.
6. Select the **Attributes** tab.
7. Move the required attributes from the **Available Attributes** list to the **Agent Attributes** list.
8. Click **Save**.

Creating a Transfer Target service for Voice

About this task

Use this procedure to create a Transfer Target service for Voice through Avaya Control Manager. The service is automatically available to consult, and the user can complete consult calls as transfer or conference. After you create a service, the Transfer Target service is also available to consult on, where the user can complete the consult to service call as a transfer or a conference.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
 - a. In the **Service Name** field, enter the name of the service.
 - b. Select the **Available for Transfer** check box.
The system automatically selects the **Agent Display** check box.
 - c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
 - d. In the Transfer Routepoints section, in the **PSTN Voice** field, select the Transfer VDN that you created for Voice.
 - e. Click **Save**.

Restarting the CallServerConnector service

About this task

Restart the CallServerConnector service to reacquire or acquire the Hunt Group.

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 1.
 - b. In the **Service** field, select **CallServerConnector**.
3. For **Deploy CSC**, type `false` in the **Effective Value** field and wait to ensure that CSC is undeployed.
4. For **Deploy CSC**, type `true` in the **Effective Value** field and wait to ensure that CSC is deployed.

User management

Creating a Control Manager role and user to administer Avaya Oceana®

About this task

This example procedure describes how to create a Control Manager user with the roles and permissions required for routine administration of Avaya Oceana® agents. You can change these roles and permissions as required for your solution.

After Avaya Oceana® administrators log in to Control Manager using this user account, they have only permissions to perform basic administration tasks for Avaya Oceana® agents.

Note:

When creating a user to administer Avaya Oceana® agents, Avaya recommends that you:

- Do not give this user permission to make system-wide changes such as changing Avaya Oceana® server details.
- Do not give this user permission to delete resources.

Procedure

1. Log in to the Avaya Control Manager web interface as an administrator.
2. Click **Roles Management > ACM**.
3. On the Role Management Portal page, click **Add**.
4. In the **Role Name** field, type a name for the new role.
5. In the **Role Description** field, type a description for the new role.
6. Click **Save**.
7. Select the new role and click **Edit**.
8. Select the **Locations** tab.
9. Move the required location from the **Available locations** list to the **Selected Locations** list.

10. Click **Save**.
11. Select the new role and click **Edit**.
12. Select the **Additional Permissions** tab.
13. Select the required permissions.
14. Select the **Permissions** tab.
15. Select the following permissions as required for your solution. Use the **Search** field to find these permissions if required.
 - Select all of the Work Assignment permissions.
 - Select all of the Avaya Oceana® related permissions that you require the user to have access to.
 - Select all of the Template related permissions that you require the user to have access to.
 - Select all of the Location related permissions that you require the user to have access to.
 - Select all of the Extension related permissions that you require the user to have access to.
 - Select the **View Users Portal** permission.
 - Select the **Add user** permission.

These example permissions allow basic administration for Avaya Oceana® agents. Add further permissions if required.

16. From the main Avaya Control Manager portal, click **Users**.
17. On the **Users** tab, click **Add**.
18. In the **First Name** and **Surname** fields, type the name of the new Avaya Oceana® administrator.
19. From the **Profile** list, select **Administrator**.
20. In the **Username** field, type the new user name.
21. In the **Password** field, type the password for the new user.

This password is used to log on to Control Manager.

22. In the **Confirm password** field, re-type the password.
23. From the **Available Applications** list, select **ACM**.
24. Click **Save**.
25. Select the **Permissions** tab.
26. From the **Role** field, select the role created previously for the Avaya Oceana® administrator.
27. Click **Save**.

Next steps

Log in to the Avaya Control Manager web interface as the new Avaya Oceana® administrator, and verify that the user's access is restricted according to the permissions assigned.

Adding a new user

Procedure

1. Log in to the Avaya Control Manager web interface as an administrator.
2. Click **Users**.
3. On the **Users** tab, click a team, and click **Add**.
4. On the User Details page, select the **Avaya Oceana** check box.
5. Type the details in the required fields.

For information about the fields on the Avaya Control Manager web page, see *Using Avaya Control Manager*.

6. To export the user to an external system using Avaya Control Manager, click **Export to external system(s)**.
7. In the **Available Applications** tab, assign the user to the Avaya Oceana application or another available applications.
8. In the **LDAP Username** field, type the user name used in the Authentication server.

You must specify the LDAP user name in the email address format.

For example, `user1@avaya.com`

9. In the **Username** field, type a user name.
10. In the **Password** field, type a password for a user.
11. **(Optional)** In the **AVAYA Login** field, type the agent login ID.
Use this field only for contacts that do not handle voice contacts.
12. In the **Extension** field, type the station associated with the agent.
13. Click **Save**.
14. Click the **Permissions** tab.
15. Select the **agent** or the **supervisor** check box.
16. Click **Save**.
17. Click the **Avaya Oceana** tab.
18. In the **Account (Provider Name)** column, select the providers that the user must support:
 - **Voice**
 - **Video**
 - **Email**

- **SMS**
- **Chat**
- **Messaging**
- **Co-Browse**
- **Social**
- **Outbound**
- **Generic**

Before selecting **Voice**, ensure that you have specified an extension in Step 12.

If you select **Voice**, **Email**, **SMS**, **Chat**, **Social**, **Generic**, or **Messaging**, you cannot select **Outbound**.

19. In the **Multiplicity** column, select a multiplicity value from 1 to 10, that is, the number of contacts that Avaya Control Manager allows the user to handle at a time.

For example, some users can handle one email contact and two chat sessions at one time. For those users, type 1 for **Email** and 2 for **Chat**.

You can configure the user's multiplicity value per channel in the following fields:

- **Email (OCP Email)**
- **Chat (OCP Chat)**
- **Messaging (OCP Messaging)**
- **SMS (OCP ShortMessageService)**
- **Social (OCP Social)**
- **Outbound (POM)**
- **AOC_GenericChannel (GenericChannel)**

 Note:

The overall value of multiplicity for all channels must not exceed value of *Max Agent Channel Multiplicity* parameter.

20. To configure the user as a reserve agent, select the **Reserve Threshold** from the **User Templates** field.
21. In the **Supervisor** field, select the supervisor to which you want to assign the user.
22. To enable Channel Exclusivity, select the **Channel Exclusivity** from the **User Templates** field.

When you enable Channel Exclusivity, agents can only work on one channel at a time.

23. Select the **Prompt agent for extension number at login** field to display the default extension for the user while logging in and to allow changing the extension.

This option is useful if you enable Hot Desking for the user. If you do not select this option, the user can log in with the default extension.

24. Click **Save**.
25. Click the **Attributes** tab.
26. Move the attributes that you want to assign to the user to the right pane.
27. Click **Save**.

Configuring concurrent active contacts per agent

About this task

You can restrict the number of contacts that an agent can work at the same time. Admin can set this parameter ranging from 1 to 20.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Users > Avaya Oceana**.
3. In the **Concurrent Active contacts** field, type any value from 1 to 20.

 Note:

The default value is 12.

4. Click **Save**.

 Note:

Oceana cannot guarantee that agent will work over all configured channels if the total number of multiplicity across all channels is much more than the value of Concurrent Active contacts.

Adding attributes to a user

Procedure

1. Log in to the Avaya Control Manager web interface as an administrator.
2. Click **Users**.
3. On the **Users** tab, select a user.
4. Click the **Attributes** tab.
5. Select the required attributes, and click the greater than symbol (>).
6. Click the Save icon ().

Searching users

About this task

You can search for users through name, login name, or extension. However, you cannot search through team, department, or site.

Procedure

1. Log in to the Avaya Control Manager web interface as an administrator.
2. Click **Users**.
3. In the **Search** field, type a search keyword, and click the Search icon ().

You can search for users by:

- Name
- User name
- Avaya login
- Extension

Cloning an agent

Procedure

1. Log in to the Avaya Control Manager web interface as an administrator.
2. Click **Users**.
3. On the **Users** tab, double-click the agent that you want to clone.
4. Select the agent, and click the Clone icon (.

Depending on the profile selected, Avaya Control Manager copies different properties.

5. Provide values for the following properties that Avaya Control Manager does not copy:
 - **First name**
 - **Last name**
 - **LDAP Username**
 - **Username**
 - **Password**

Editing a user

Before you begin

Ensure that the user is logged off before you edit the user role. You cannot edit the role of a user that is logged in.

Procedure

1. Log in to the Avaya Control Manager web interface as an administrator.
2. Click **Users**.
3. On the **Users** tab, click the team, and select the user.
4. Click the three downward arrows () and click **Edit User**.

5. On the User Details page, type the details in the required fields.
For information about the fields, see *Using Avaya Control Manager*.
6. In the **Username** field, type a user name.
7. In the **Password** field, type a password.
8. Click the Save icon (📁).

Deleting a user

Procedure

1. Log in to the Avaya Control Manager web interface as an administrator.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click the team, and select the user.
4. Click the three downward arrows (⌵), and click **Delete User**.
5. When Avaya Control Manager displays the confirmation message, click **Yes**.

Configuration for Avaya Workspaces

Configuring Avaya Analytics™ 3.x Streams server details for real-time reporting

About this task

The Avaya Analytics™ Streams server provides producers and measures to Avaya Workspaces for use in real-time reporting dashboards. Using Avaya Workspaces, users can view real-time reporting dashboards to monitor up-to-date statistics for your contact center and resources.

You configure the Avaya Analytics™ Streams server details in Avaya Control Manager so that Avaya Workspaces can receive data from Avaya Analytics™.

! Important:

Use this procedure only if your solution uses Avaya Analytics™ 3.x.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Configuration > Customer Engagement > Avaya Analytics™**.
3. On the **Avaya Analytics Server List** page, click **Add**.
4. In the **Alias** field, type an alias name for the Avaya Analytics™ Streams server.

5. In the **API URL** field, type the URL that the Avaya Analytics™ Streams server communicates with. For example, type `https://<AvayaOceanaCluster1_FQDN>/services/UCASStoreService/uca`.

 Important:

- This URL must match the **API URL** configured on the Avaya Oceana® server. Verify that by navigating to **Configuration > Avaya Oceana > Server Details**.

 Important:

- If the Avaya Oceana® and Avaya Analytics™ server use the same UCA server (Common setup), the **API URL** configured on both must match, including using matching address formats. For example, you must not use an IP address on one and FQDN on the other.

6. From the **Version** field, select the appropriate version for your release of Avaya Oceana®.
7. Click **Save**.
8. On the Avaya Control Manager web page, click **Configuration > Locations**.
9. On the Location List page, select the location where you want to add the Avaya Analytics™ server.
10. Click **Edit**, or double-click the location.
11. On the Location Edit page, select the **Systems** tab.
12. Click the **+** sign.
13. In the **System Type** field, select **Avaya Analytics**.
The **System Name** field populates the name of the newly created Avaya Analytics™ server.
14. Click **Save**.
15. Click **Confirm** on the Warning message dialog box.
16. On the Avaya Control Manager web page, click **Configuration > Customer Engagement > Avaya Analytics™**.
17. Select the check box for the Avaya Analytics™ Streams server and click **Edit**.
18. Select the **Stream Servers** tab.
19. On the **Avaya Analytics Stream Server Add** page, click **Add**.
20. In the **Name** field, type a name for the Avaya Analytics™ Streams server.
21. In the **FQDN** field, type the FQDN of the Avaya Analytics™ Streams server.
22. In the **Port** field, type 8443.
23. Select the **TLS Flag** check box.
24. Click **Save**.

Configuring Avaya Analytics™ 4.x server details for real-time reporting

About this task

Avaya Analytics™ provides producers and measures to Avaya Workspaces for use in real-time reporting dashboards. Using Avaya Workspaces, users can view real-time reporting dashboards to monitor up-to-date statistics for your contact center and resources.

You configure the Avaya Analytics™ 4.x server details in Avaya Control Manager so that Avaya Workspaces can receive data from Avaya Analytics™.

! Important:

Use this procedure only if your solution uses Avaya Analytics™ 4.x.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager web page, click **Configuration > Customer Engagement > Avaya Analytics™**.
3. On the **Avaya Analytics Server List** page, click **Add**.
4. In the **Alias** field, type an alias name for the Avaya Analytics™ 4.x server.
5. In the **API URL** field, type the URL that the Avaya Analytics™ 4.x server communicates with. For example, type `https://<AvayaOceanaCluster1_FQDN>/services/UCASStoreService/uca`.

! Important:

- This URL must match the **API URL** configured on the Avaya Oceana® server. Verify that by navigating to **Configuration > Avaya Oceana > Server Details**.

! Important:

- If the Avaya Oceana® and Avaya Analytics™ server use the same UCA server (Common setup), the **API URL** configured on both must match, including using matching address formats. For example, you must not use an IP address on one and FQDN on the other.

6. From the **Version** field, select the appropriate version for your release of Avaya Oceana®.
7. Select the **Enable Authorization** option.

For more information about the **Enable Authorization** option and its related parameters, see [Configuring token-based access between Control Manager and Avaya Oceana, Avaya Analytics, or Avaya Workspaces for Call Center Elite](#) on page 25.

8. Click **Save**.
9. On the Avaya Control Manager web page, click **Configuration > Locations**.

10. On the Location List page, select the location where you want to add the Avaya Analytics™ server.
11. Click **Edit**, or double-click the location.
12. On the Location Edit page, select the **Systems** tab.
13. Click the **+** sign.
14. In the **System Type** field, select **Avaya Analytics**.
The **System Name** field populates the name of the newly created Avaya Analytics™ server.
15. Click **Save**.
16. Click **Confirm** on the Warning message dialog box.
17. On the Avaya Control Manager web page, click **Configuration > Customer Engagement > Avaya Analytics™**.
18. Select the check box for the Avaya Analytics™ 4.x server and click **Edit**.
19. Select the **Stream Servers** tab.
20. On the **Avaya Analytics Stream Server Add** page, click **Add**.
21. In the **Name** field, type a name for the Avaya Analytics™ 4.x server.
22. In the **FQDN** field, type the FQDN of the Avaya Analytics™ 4.x server. This is the cluster FQDN configured during deployment.
23. In the **Port** field, type `443/orca-streams-rest`
24. Select the **TLS Flag** check box.
25. Click **Save**.

Configuring CRM integration

About this task

Avaya Workspaces can integrate with Customer Relationship Management (CRM) systems such as Salesforce.

You can administer only one CRM integration.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > CRM Integration**.
3. Click **Add**.
4. Select the **Enable CRM Integration** check box.
5. In the **Application Name** field, type the name of the CRM integration.

6. In the **Consumer Key** field, type the consumer key value that identifies this installation to Salesforce.
In Salesforce, the Consumer Key is known as client_ID.
7. In the **Consumer Secret Key** field, type the secret key value that identifies this installation to Salesforce.
In Salesforce, this field is known as client_secret.
8. In the **SalesForce Endpoint** field, type the URL of the Salesforce site with which you are integrating Avaya Workspaces.
9. Click **Save**.

Enabling Avaya Breeze® platform authorization on Avaya Aura® Device Services

About this task

The Avaya Workspaces address book uses Avaya Aura® Device Services to search for enterprise directory contacts using LDAP. Use this procedure to enable single sign-on (SSO) capabilities for Avaya Aura® Device Services users that previously authenticated using the Avaya Breeze® platform AuthorizationService. This allows Avaya Workspaces users to use the address book to search for enterprise directory contacts using LDAP, without needing to separately authorize with Avaya Aura® Device Services.

To enable authorization, you must import the Avaya Breeze® platform authorization certificate to Avaya Aura® Device Services. If the certificate is changed, then you must re-upload it to Avaya Aura® Device Services.

For more information about Authorization Service, see [Administering Avaya Breeze® platform](#).

Before you begin

Obtain the Avaya Breeze® platform authorization certificate file in the .PEM format. For more information, see *Deploying Avaya Oceana®*.

Procedure

1. On the Avaya Aura® Device Services web administration portal, navigate to **Security Settings > Authorization**.
2. Click **Choose File** and select the .PEM file that you exported from the Avaya Breeze® platform node.
3. Click **Save**.

Configuring LDAP integration

About this task

The Avaya Workspaces address book uses Avaya Aura® Device Services to search for enterprise directory contacts using LDAP. You must set the Avaya Aura® Device Services fully qualified domain name (FQDN) in Oceana Configuration using the System Manager web console.

Avaya Aura® Device Services queries the Active Directory (AD) global catalogue. All user information fields are not available in the global catalogue by default. Therefore some fields can appear blank in the Avaya Workspaces address book. If you want these missing fields to appear in the address book user profiles, the AD administrator must add these fields to the global catalogue.

Before you begin

- You must install and configure Avaya Aura® Device Services. For more information, see *Deploying Avaya Aura® Device Services*.
- To retrieve contacts from Avaya Aura® Device Services using LDAP, your solution must include Avaya Aura® 7.1.5 or later.
- Ensure that cross origin resource sharing (CORS) is enabled on AADS. For more information, see *Administering Avaya Aura® Device Services*.
- Ensure that the **active users search filter** and **users search additional filter** in AADS are configured to return users only. For more information, see *Deploying Avaya Aura® Device Services*.

Procedure

1. In System Manager, click **Elements > Avaya Breeze® > Configuration > Attributes**.
2. On the Service Clusters tab, in the **Cluster** field, select **ProvisioningCluster**.
3. In the **Service** field, select **Oceana Configuration**.
4. Under **Unified Agent Client**, for **AADS FQDN**, select the **Override Default** check box and type the AADS FQDN.
5. Click **Commit**.

Next steps

Verify that Enterprise Directory contacts appear in the address book on Avaya Workspaces.

Work Codes, Disposition Codes, and Rejection Codes

Work Codes are tags that an agent can set at any point in a contact. Work Codes describe what is going on with the contact at that time. For example, if a customer calls a television service provider to complain about poor service, the agent can tag the first part of the call as `ServiceComplaint`. After resolving the complaint, the agent can inform the customer about a special offer and tag the call as `UpSell`. If the customer agrees to renew the subscription, the agent can further tag the call as `SubscriptionRenewal`.

Disposition Codes are tags that indicate the final state of the contact when the agent closes the contact. For example, `ComplaintResolved`, `DissatisfiedCustomer`, and `FollowUp`. Agents can also set Disposition Codes during the course of a contact to capture the actions that the agents need to do. For example, `PostBrochure`, `CustomerCallback`, and `LikeOnSocial`.

Defer Codes are tags that an agent can set when deferring an email. For example, `WarehouseContact`, `In-store`, `PhoneRepair`, and `LoyaltyCustomer`.

Rejection Codes are tags that indicate the rejected state of the email when an approver rejects emails. When an approver rejects emails, mandatory rejection reason codes must be assigned to the contacts.

Configuring work codes or user codes

About this task

Codes used while handling interactions are called work codes. The agents can use these work codes to record the type of work done during every interaction.

Codes used before and after handling contacts, for example, while changing the state of the user, are called user codes. For example, before going on a break, an agent uses a user code configured to represent break time.

The work codes and user codes displayed for agents that use Avaya Workspaces are configured in Avaya Control Manager.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana® > Reason Codes**.
3. On the **Work Codes** tab, click **Add**.
4. In the **Type** field, do one of the following
 - To create a user code, click **User Code**.
 - To create a work code, click **Work Code**.
5. In the **Name** field, type a name for the work code.

For example, type *Sales*. The agent can then select the Sales work code to track all interactions related to Sales.

The maximum name length is 30 characters.

6. In the **Number** field, type a number to uniquely identify the work code or user code.
7. In the **Contact Type** section, select the channel types for which the work code must be displayed.

You can select from the following options: Voice, ShortMessagingService, EMail, Chat, Social, Outbound, Generic, Video, and Messaging.

Avaya Workspaces does not display these contact types for User Codes.

8. Click **Save**.

Configuring disposition codes

About this task

Administrators can define disposition codes that agents can select through Avaya Workspaces. Agents can select disposition codes while on contact or during the timed after contact work.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana® > Reason Codes**.

2. Select the **Disposition Codes** tab.

3. Click **Add**.

4. In **Name**, type a name for the disposition code.

The maximum name length is 30 characters.

Do not name the disposition code as `UNKNOWN`. This name conflicts with the default disposition code value when the user does not set the disposition code.

5. In **Number**, type a number to uniquely identify the disposition code.

The number must be unique. The disposition code number cannot be the same as a work code or user code number.

6. In the **Contact Type** section, select the channel types for which the work code must be displayed.

You can select from the following options: Voice, ShortMessagingService, EMail, Chat, Social, Outbound, Generic, Video, and Messaging.

7. Click **Save**.

Configuring deferral codes

About this task

Use this procedure to define deferral codes that agents can select through Avaya Workspaces. Agents use the deferral codes to defer an email.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Reason Codes**.

2. Click the **Deferral Codes** tab.

3. Click **Add**.

4. In the **Name** field, type a name for the deferral code.

5. In the **Number** field, type a number to identify the deferral code.

The number must be unique. The deferral code number cannot be the same as a work code or user code number.

6. In the **Contact Type** section, select **Email**.

7. Click **Save**.

Configuring rejection codes

About this task

When an approver rejects emails, mandatory rejection reason codes must be assigned to the contacts. Administrators can create rejection reason codes.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration > Avaya Oceana > Reason Codes**.
3. Click the **Rejection Codes** tab.
4. Click **Add**.
5. In the **Name** field, enter a name for the rejection reason code.
6. In the **Number** field, enter a unique number for the rejection reason code.
7. In the **Contact Type** field, **Email** is selected by default.
8. Click **Save**.

Configuring deferred email settings

Procedure

1. Log on to the Avaya Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Omnichannel**.
3. Click **Email Handling Settings**.
4. Select the **Enable Defer Contact** check box.
5. Select the **Enable Defer Custom Time** check box, to display the custom defer date and time option on the agent or supervisor workspace.
6. In the **Max Defer Time (hh:mm)** field, type the maximum time for which the agent or supervisor can defer an email.
7. In the **Max Deferred Contacts** field, type the maximum number of contacts that an agent or supervisor can defer.

Note:

Based on the configuration, the agents can defer a maximum of 20 email contacts.

8. In the **Defer Time Intervals** field, configure each time interval that an agent or a supervisor can use to defer a contact in the text boxes.

The intervals must:

- Not be null.
- Be in multiples of 5.
- Be in sorted order.

9. Click **Save**.

Enabling email forward

About this task

Use this procedure to enable the forward button for an incoming email in Avaya Workspaces.

Procedure

1. Log on to the Avaya Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Omnichannel**.
3. Click **Email Handling Settings**.
4. Select the **Enable Forward Email** check box.
5. Click **Save**.

Enabling multiple replies to email

About this task

The administrator can configure the Multireplies to Email feature in Avaya Control Manager and enable the **Allow Multireply** parameter in Omnichannel Administration Utility. Agents with such configurations can close the contact card after one response or continue to send multiple replies, defer, forward, or transfer the email interaction.

Procedure

1. Log on to the Avaya Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Omnichannel**.
3. Click **Email Handling Settings**.
4. Select the **Enable Multiple Replies To Email** check box.
5. Click **Save**.

Customer Management

Enabling an external widget library

About this task

Use this procedure to enable an external widget library to load it into Avaya Workspaces.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration > Avaya Oceana™ > Server Details**.
3. On the Avaya Oceana Server List page, select the server from the list and click **Edit**.
4. On the Avaya Oceana Server Edit page, click the **System Properties** tab.

5. Expand **Workspaces**.
6. In the Widget Library section, select the **Enable an External Widget Library** check box.
7. In the **Workspaces Library URL*** field, enter a URL to an external widget library.
The external widget library is loaded into Avaya Workspaces.
8. Click **Save**.

Authorizing the contact to Customer Management service

About this task

Use this procedure to enable authorization to contact the Customer Management service.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements > Avaya Breeze® > Configuration > Attributes**.
3. In the **Cluster** field, select the Contact Center cluster.
4. In the Service field, select `CustomerManagement`.
5. In the Run-time Service Configuration area, for **Authorization Required to contact the CustomerManagement** field, select the **Override Default** check box, and set the **Effective Value** to `true`.

Important:

Setting the **Authorization Required to contact the CustomerManagement** field to `true`, mandates authentication to contact the `CustomerManagement` service. The default value is `false`.

Create Avaya Oceana user with SIP extension from Avaya Control Manager

Checklist for creating Avaya Oceana® user with SIP extension using a custom profile from ACM user portal

No.	Task	Description	✓
1	Create Avaya Control Manager web service user on Avaya Aura System Manager.	• Creating Avaya Control Manager web service user on Avaya Aura System Manager on page 76 • Verifying the role on page 77 • Adding a new administrative user on page 77 • Completing the login process on page 78 • Verifying the ACM web service user permissions on page 78	
2	Integrate Avaya Aura System Manager and configure Avaya Aura System Manager fields in Avaya Control Manager.	• Configuring the connection to System Manager on page 78 • Configuring the System Manager values in Avaya Control Manager on page 80	
3	Create a custom template of CM Endpoint type and set the required fields in the template.	Creating a custom template of CM Endpoint type on page 83	
4	Create Avaya Aura System Manager custom template in Avaya Control Manager (ACM) with the same name as configured in ACM.	Creating a System Manager custom template in Avaya Control Manager on page 83	
5	Create a SIP template in ACM.	Creating a SIP template in Avaya Control Manager on page 83	
6	Create an agent template.	Creating an agent template on page 84	
7	Create ACM user profile using the SIP template and the agent template.	Creating a SIP user profile in Avaya Control Manager on page 84	
8	Create a user based on the ACM user profile.	Creating a user from an Avaya Control Manager profile on page 85	

Table continues...

No.	Task	Description	✓
9	Login the SIP station on an endpoint.	-	
10	Login to Workspaces and activate the agent.	See <i>Using Avaya Workspaces for Avaya Oceana®</i> document.	

Creating Avaya Control Manager web service user on Avaya Aura System Manager

Procedure

1. Log on to Avaya Aura® System Manager Web UI as an administrator user.
2. Navigate to **Avaya Aura System Manager > Users > Administrator > Administrative Users > Roles**.
3. Select **System Administrator** and click **New**.
The application displays Add New Role page.
4. In the **Role Name** field, enter a name for the user management web service role.
5. In the **Role Description** field, enter the description of the user management web service role.
6. Click **Commit and Continue**.
7. Click **Add Mapping**.
8. In the **Element or Resource Type** field, select `users`.
9. In the **Element or Resource Instance** field, select `All`.
10. Click **Next**.
11. Click the **Select/Unselect All** check box.
12. Click **Commit**.
13. Click **Add Mapping**.
14. In the **Element or Resource Type** field, select `Communication Manager`.
15. In the **Element or Resource Instance** field, select `All`.
16. Click **Next**.
17. Click the **Select/Unselect All** check box.
18. Click **Commit**.
19. Click **Add Mapping**.
20. In the **Element or Resource Type** field, select `Communication Manager Templates`.
21. In the **Element or Resource Instance** field, select `All`.
22. Click **Next**.

23. Click the **Select/Unselect All** check box.
24. Click **Commit**.
25. Click **Add Mapping**.
26. In the **Element or Resource Type** field, select `Session Manager and Routing`.
27. In the **Element or Resource Instance** field, select `All`.
28. Click **Next**.
29. Click the **Select/Unselect All** check box.
30. Click **Commit**.
31. Click **Add Mapping**.
32. In the **Element or Resource Type** field, select `Avaya Officelinx`.
33. In the **Element or Resource Instance** field, select `All`.
34. Click **Next**.
35. Click the **Select/Unselect All** check box and click **Commit**.
36. Click **Commit**.

Verifying the role

Procedure

1. Log on to Avaya Aura® System Manager Web UI as an administrator user.
2. Navigate to **Avaya Aura System Manager > Users > Administrator > Administrative Users > Roles**.
3. Expand the **System Administrator** and find the newly created user management web service role.

Adding a new administrative user

Procedure

1. Log on to Avaya Aura® System Manager Web UI as an administrator user.
2. Navigate to **Avaya Aura System Manager > Users > Administrator > Administrative Users**.
3. Click **Add**.
4. In the **User ID** field, enter the user id of the ACM web service user created.
5. In the **Authentication Type** field, choose the required authentication type.
6. In the **Full Name** field, enter the full name of the ACM web service user.
7. In the **Temporary Password** field, enter a temporary password.
8. In the **Re-enter Password**, re-enter the password.

 Important:

Note the password.

9. Click **Commit and Continue**.
10. On the User Roles page, select the user role created earlier, to assign it to this user.
11. Click **Commit**.

The application displays the user role details.

12. Logout as administrator from Avaya Aura® System Manager.

Completing the login process

Procedure

1. Log on to Avaya Aura® System Manager Web UI as the new ACM web service user.
2. Reset initial temporary password and then create a new password.
3. Save the user password on the credentials page.
4. Login with the new password.

Verifying the ACM web service user permissions

Procedure

1. Log on to Avaya Aura® System Manager Web UI as the new ACM web service user.
2. Click the **Elements** tab and ensure that the following menu options are displayed:
 - Communication Manager
 - Routing
 - Session Manager
3. Click the **Users** tab and ensure that the following menu option is displayed:
User Management
4. Click the **Services** tab and ensure that the following menu option is displayed:
Templates

Configuring the connection to System Manager

Before you begin

Confirm that the connector for System Manager has been enabled using the procedure found in [Enabling connectors](#) on page 80. Enable the connector if it is not enabled.

Procedure

1. Log on to the Avaya Control Manager.
2. Click **Add**.

3. On the **Connection Details** tab, enter the values in the fields as described in [Configuring the connection to System Manager field descriptions](#) on page 79.
4. Click **Save**.
5. Assign the System Manager system to the Location.
 - a. Click **Configuration > Locations**.
 - b. In the locations list, double-click the location to which you want to assign the System Manager system.
 - c. Click the **Systems** tab.
 - d. Click **Add**.
 - e. In the **System Type** drop-down list, click **System Manager**.
 - f. In the **System Name** drop-down list, click the System Manager system that you configured.
 - g. **(Optional)** In the **Sync Schedule** drop-down list, click the required sync schedule.
 - h. Click **Save**.
6. Ensure that the Communication Manager alias name administered under **Configuration > Team Engagement > Communication Manager** matches the Communication Manager name under **System Manager > Inventory > Manage Elements**.

Configuring the connection to System Manager field descriptions

Field name	Value
Alias	Any given name.
Host Name	The host name, FQDN, or IP address of your System Manager server.  Important: If the System Manager server has a certificate, the host name used here must match exactly the host name used on the System Manager server.
Port number	Enter the port number as 80.
DB Name	For future use.
Web Service URL	The URL that leads to the System Manager API. The Web Service URL is: https://<your_smgr_server>/web/mgmtwebservice.
Username	The user name of the System Manager that Control Manager uses for this integration. The user requires full administration rights in System Manager equivalent to the admin user.
Password	The password of the System Manager user.
Version	Select the System Manager version. System Manager 6.3.x and higher is supported.

Table continues...

Field name	Value
WS Update Type	The type of Web Service update. The following options are available: • Replace • Merge

Enabling connectors

About this task

Enable all product connectors and then configure and assign the connector to a location or vice versa. Even if a connector is configured and assigned to a location, enable the connector using this procedure.

Before you begin

Ensure that the product for which you enable a connector has a license.

Procedure

1. Log on to the Avaya Control Manager.
2. Double-click the default provisioning server.
3. Click the **Location** tab.
4. Assign a location from **Available Locations**.
5. Click the **Connectors** tab.

Control Manager displays the Provisioning Service Edit screen.

6. From the drop-down list, select **Yes** to enable the connectors used in the deployment.

For Avaya Workspaces for Elite, enable UCA Proxy Connectors.

7. Click **Save**.

Configuring the System Manager values in Avaya Control Manager

About this task

As part of the integration between Avaya Control Manager and System Manager, you can assign System Manager field parameters to one or more locations. This allows tenanting of System Manager fields in SIP templates and user SIP properties.

Before you begin

Confirm that the connector for System Manager has been enabled using the procedure found in [Enabling connectors](#) on page 80. Enable the connector if it is not enabled.

Procedure

1. Log on to the Avaya Control Manager.
2. Navigate to **Configuration > Team Engagement > System Manager > System Manager Fields**.

3. If the System Manager system has not already been added, perform the following steps:

- a. Click **Add**.

The system displays the System Manager Fields Configuration Add screen.

- b. Enter a name for the System Manager system in the **Alias** field.

- c. Click **Save**.

The system displays the System Manager Fields Configuration List screen.

4. In the list of available systems, double-click the System Manager system that you want to configure.

The system displays the System Manager Fields Configuration Edit screen.

5. Select the **Location** tab.

6. Move the Communication Manager systems you want to assign from the **Available Locations** column to the **Assigned Locations** column.

7. Click the **Fields Configuration** tab.

8. Enter the values in the fields as described in [Configuring System Manager values in Control Manager field descriptions](#) on page 82.

 Note:

You can retrieve the configuration values from the System Manager environment where the connector is implemented. You must log in to System Manager and copy the values from System Manager.

9. Click **Add** to save the parameters assigned to the System Manager field.

10. Repeat Steps 7 and 8 to add all required parameters.

11. Click **Save**.

The system displays the System Manager Fields Configuration List screen.

Configuring System Manager values in Control Manager field descriptions

Field name	Value
SMGR Fields	The System Manager parameter that you want to configure. This drop-down list contains the following parameters: • Session Manager • Origination App Seq • Termination App Seq • Conference Factory Set • Survivability Server • Home Location • CS1K.Preferred Handle • Messaging.Preferred Handle • B5800.Preferred Handle • Conf.Preferred Handle • Domain • Target • Messaging System • Presence System • IM Gateway SIP Entity • Breeze.Service Profile • Em.Calling Origination App Seq • Em.Calling Termination App Seq • Officelinx System • Officelinx.Company • Officelinx.Department • Officelinx.Feature Group • Officelinx.Capability
Alias	The alias name of the parameter.
Value	The value of the parameter.

- Click **Test** to validate the connection details and interoperability configurations required to communicate with the system.



Note:

You must assign the system to a location before administering the system through Control Manager.

Creating a custom template of CM Endpoint type

Procedure

1. Log on to Avaya Aura® System Manager Web UI as ACM web service user.
2. Navigate to **Avaya Aura System Manager > Services > Templates > CM Endpoint**.
3. In the **Supported Feature Server Versions** area, select the required CM version.
4. To view the templates created, click **Show List**.
5. Click **New**.
6. In the **General Options (G)** tab, in the **Type of 3PCC Enabled** field, select *Avaya*.
7. In the **Button Assignment (B)** tab, add the required buttons.
For example, **auto-in** , **manual-in**, **agnt-login**, **auxwork**, and **aftercall** .
8. Click **Commit**.

Creating a System Manager custom template in Avaya Control Manager

About this task

Use this procedure to create a System Manager custom template in ACM. The name of the System Manager custom template must be the same name as configured in ACM.

Procedure

1. Log in to Avaya Control Manager.
2. Navigate to **Resources Manager > Templates > System Manager Custom Templates**.
The application displays System Manager Custom Templates List page.
3. Click the **Add (+)** icon.
4. In the **Name** field, enter the same name as configured in ACM.
5. In the **Type** field, select *CM End Point*.
6. In the **Location Name**, select the appropriate CM location name.
7. In the **Extension Template Name**, select the required extension template name.
8. In the **CM Version**, select the appropriate version.
9. Click the **Save** icon.

Creating a SIP template in Avaya Control Manager

Procedure

1. Log in to Avaya Control Manager.
2. Navigate to **Resources Manager > Templates > SIP Templates**.
The application displays the SIP Templates List page.
3. Click **Add (+)**.

4. In the **General** tab, do the following:
 - a. In the **Template Name** field, add a name for the SIP template.
 - b. In the **Location Name** field, enter the location name.
5. In the **Identity** tab, do the following:

In the **Authentication Type** field, select the required authentication type.
6. In the **Communication Profile** tab, do the following:
 - a. Click **Communication Address** , enter all the required field details.
 - b. Click **Session Manager Profile**, enter all the required field details.
 - c. Click the **CM Endpoint Profile**, in the **Template** field, and select the System Manager custom template that you created in [Creating a System Manager custom template in Avaya Control Manager](#) on page 83.
7. Click the **Save** icon.

Creating an agent template

Procedure

1. Log in to Control Manager.
2. Navigate to **Resources Manager > Templates > Agent Templates**.

The application displays the Agent Templates List page.
3. Click the **Add (+)** icon.
4. In the **General** tab, enter all the required field details.
5. In the **Agent Skills** tab, click the **Select Skill** icon and assign the Oceana agent skills.
6. Click the **Save** icon.

Creating a SIP user profile in Avaya Control Manager

Procedure

1. Log in to Avaya Control Manager.
2. Click **Users**.
3. Click the drop-down icon and select **Profile Manager**.
4. Click on the **Add new (+)** profile button.
5. In the **Profile Details** tab, do the following:
 - a. In the **Name** field, enter the name of the profile.
 - b. In the **Location** field, enter the location of the profile.
 - c. In the **Active** field, select *yes* or *no* from the drop-down.
 - d. In the **User Type** field, select the required user type.

- e. Click **Next**.
6. In the **Application Assignment** tab, do the following:
 - a. In the **Application** field, select the required application from the drop-down.
 - b. In the **Role** field, select the role from the drop-down.
 - c. In the **Application Template** field, select the application template from the drop-down.
 - d. Click **Next**.
7. In the **Contact Center** tab, in the **AGENT TEMPLATE** field, select the agent template created.
See [Creating an agent template](#) on page 84.
8. In the **Unified Communication** tab, do the following:
 - a. Select the **Create SIP User** check box.
 - b. In the **SIP User Template** field, select the SIP user template created.
See [Creating a SIP template in Avaya Control Manager](#) on page 83.
9. In the **Summary** tab, verify all the information entered.
10. Click **Save**.

Creating a user from an Avaya Control Manager profile

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and click **Add**.
Control Manager displays the User Details page.
4. In the **Profile** field, select the SIP user profile created.
See [Creating a SIP user profile in Avaya Control Manager](#) on page 84.
5. In the **LDAP Username** field, enter LDAP user name of the user.
6. In the **Domain Name** field, enter the domain name.
The user name is in the **LDAP Username** field and the **Domain Name** is in a separate field separated by the @ symbol.
7. In the **Available applications** area, select *Avaya Oceana*.
8. Enter the appropriate information in all the mandatory fields.
9. Click the **Save** icon.

Checklist for creating Avaya Oceana® user with SIP extension from ACM user portal

No.	Task	Description	✓
1	Create Avaya Control Manager web service user on Avaya Aura System Manager.	• Creating Avaya Control Manager web service user on Avaya Aura System Manager on page 76 • Verifying the role on page 77 • Adding a new administrative user on page 77 • Completing the login process on page 78 • Verifying the ACM web service user permissions on page 78	
2	Integrate Avaya Aura System Manager and configure Avaya Aura System Manager fields in Avaya Control Manager.	• Configuring the connection to System Manager on page 78 • Configuring the System Manager values in Avaya Control Manager on page 80	
3	Create a custom template of CM Endpoint type and set the required fields in the template.	Creating a custom template of CM Endpoint type on page 83	
4	Create Avaya Aura System Manager custom template in Avaya Control Manager (ACM) with the same name as configured in ACM.	Creating a System Manager custom template in Avaya Control Manager on page 83	
5	Create a user with agent profile on the ACM user portal.	Creating Avaya Oceana agent user on page 86	
6	Login the SIP station on an endpoint.	-	
7	Login to Workspaces and activate the agent.	See <i>Using Avaya Workspaces for Avaya Oceana®</i> document.	

Creating Avaya Oceana® agent user

About this task

Use this procedure to add Avaya Oceana® agent user to Avaya Control Manager. This user can log on to Avaya Workspaces as an agent and access the agent features available in Avaya Workspaces.

Before you begin

Ensure that the Avaya Oceana® clusters are in a running and accepting state.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and click **Add**.

Control Manager displays the User Details page.

4. In the **First Name** field, type the first name for the agent.
5. In the **Surname** field, type the surname for the agent.
6. In the **Profile** field, select *Agent*.
7. In the **LDAP Username** field, enter the LDAP user name of the user.
8. In the **Username** field, enter the user name.
9. In the **Password** field, enter the password.
10. In the **AVAYA login** field, enter the agent log-in ID at Avaya softphone.
11. In the **Team** field, enter the name of the team that the user is assigned to.
12. In the **Template** field, enter the required template.
13. In the **SIP URI** field, enter the SIP URI of the user.

This must be a valid email address.

14. In the **Communication Profile Password** field, enter the communication profile password.
15. In the **Extension** field, enter the extension used by the client software to automatically log the user into the system.
16. In the **Available Applications** area, select *Avaya Oceana* and *SIP*.

On selecting *Avaya Oceana* application, LDAP domain field appears.

17. In the **LDAP domain** field, enter the domain name.
18. Click **Save**.

When the user is saved, the **SIP Properties** button is enabled.

19. Click **SIP Properties**.
20. On the **SIP Properties** page, in the **Communication Profile** tab, enter the required SIP properties .
21. Enter the **Communication Address**.
22. In the **Session Manager Profile** tab, enter the required information.
23. In the **CM Endpoint Profile** tab, do the following:

In the **Template** field, select the custom template created. See [Creating a System Manager custom template in Avaya Control Manager](#) on page 83.

- a. In the **Extension** field, specify the extension entered in the user page.

- b. In the **Profile Type** field, select **Endpoint**.
24. Click **Save**.

Configuring screenpops

About this task

Avaya Workspaces provides a Screenpop widget to display external web content that can help an agent to complete an interaction. Avaya Control Manager is used to configure screenpops for Avaya Workspaces.

When you configure both Auto Answer and External Screenpops, the agent's work can be interrupted by a Screenpop from a new interaction that has been automatically answered.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > ScreenPOP Configuration**.
3. **(Optional)** Click the **Screen Pop** filters tab.
 - a. Click **Add**.
 - b. In the **Name** field, type the name of the filter.
 - c. In the **Provider** field, click the provider that must provide the service.
 - d. **(Optional)** If any service has been assigned for the client, in the **Service Name** field, click the assigned service name.

If you specify a service name here, only contacts with a matching service name receive a screenpop that has this filter applied.
 - e. Click **Save**.
4. Click the **Screen Pop Applications** tab.
 - a. Click **Add**.
 - b. In the **Name** field, type the name of the application.
 - c. In the **URL** field, type the URL for the application that must provide the screenpop.

You can add pairs of curly braces {} to represent additional parameters collected from the contact. For example, an account number entered in a voice response interaction. Put a plus sign between each set of curly braces.

Type `http://www.google.com?search={ }+{ }`.
 - d. Click **Save**.
5. Click the **Screen Pops** tab.

Click **Add**.

 - a. In the **Name** field, type a name for the screenpop.

Avaya Workspaces displays this name on the screenpop tab.

- b. In the **Provider** field, click the system that hosts the accounts.

For example, click **CMProvider** to choose Communication Manager as the provider.

- c. In the **Application Name** field, click the application created in the **Screen Pop Application** tab.

- d. **(Optional)** In the **Filter Name** field, click the filter name created in the **Screen Pop Filters** tab.

If you do not assign a filter, the system displays the screenpop for all interactions for the selected provider type.

- e. In the **Event** field, click **ACTIVE**.

The system displays screenpops are displayed for the interaction only when the interaction is in the active state.

- f. In the **Event Direction** field, click INCOMING or OUTGOING to indicate whether the system displays the screenpop for incoming or outgoing interactions.

- g. In the **Auto Close** field, click **Yes** or **No**.

If you click **Yes**, the screenpop closes when you close the interaction card. If you click **No**, the screenpop remains open even after the interaction is closed. You must manually close the screenpop.

- h. In the **Launch Internal** field, click **Yes** or **No**.

If the system must display the screenpop in the Avaya Workspaces client, click **Yes**. If the screenpop must be displayed in a new window, click **No**.

- i. In the **Priority** field, type the order in which the system must display the screenpop.

You must not duplicate the priority. Also, Avaya Workspaces displays only five screenpops. Screenpops with lower priority numbers are considered first. For example, for six screenpops configured for voice service with priorities 1 to 6, only screen pops with priorities 1 to 5 is displayed on Avaya Workspaces.

You can configure up to five screenpops for a single interaction. The value in the **Priority** field determines which screenpops to display if more than five screenpops match the criteria of the contact. The priority value must be unique. Otherwise, screenpops are overridden.

The **URL** field displays the URL created in the **Screen Pop Applications** tab that is associated with the **Application Name** you selected.

- j. **(Optional)** In the **Screen Pop Parameters** section, under the **Intrinsics** column, click a parameter.

The **Parameter Position** field displays the number corresponding to the order in which the parameter is added to the URL. The number of parameters depend upon the number of curly braces at the end of the URL.

This step is mandatory if there are placeholders in the application.

To add the originating address as the first parameter for the URL, click the **Originating Address** parameter in the **Intrinsics** column in row 1.

- k. Click **Save**.

Configuring transfer to service

About this task

Avaya Workspaces provides an option to transfer an interaction to a predefined service. Avaya Workspaces displays the services defined in Avaya Control Manager when an agent clicks **Transfer to Service**.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.
3. Click **Add**.
4. In the **Type** field, click a Route Point or Implicit User.
5. In the **Sub Type** field, click an option corresponding to transfer to service.
6. In the **Name** field, type the name of the route point.
7. Click **Save**.

Avaya Workspaces displays the route points with the sub type transfer in the Transfer Service options.

After creating a route point, you must create a transfer service from the Work Assignment page.

8. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
9. Click the **Services** tab.
10. Click the **Add** icon.
11. In the **Service Name** field, type the name of the transfer service.
The service name must not have any space.
12. Select the **Available for Transfer** check box.
13. From the **Available Attributes** column, select the attributes to be included, and click the **>** icon.
If you select an attribute from the **Available Attributes** column, only the selected attribute associated with Attribute channel is available as a transfer route point.
14. In the Transfer Route points section, from the options for each channel, select the route point that must be used for transferring to service.
Only route points with sub type transfer to service are available in the list of route points for each channel in the Transfer Route point section.
15. Click **Save**.

You can configure up to 1000 transfer services in Avaya Control Manager.

Transfer to User configuration

Avaya Workspaces provides the Transfer to User feature. With this feature, agents or supervisors can transfer interactions to more qualified agents or supervisors within the contact center. To make this feature available to agents or supervisors, you must do the required configurations in Avaya Control Manager.

Transfer to User configuration checklist

Use the following checklist for Avaya Control Manager configurations for the Transfer to User feature:

No.	Task	Reference	✓
1	Enable the Transfer to User feature.	See Enabling the Transfer to User feature on page 91.	
2	Add Transfer to User route points.	See Adding Transfer to User route points on page 92.	
3	For Voice contact, add Transfer to User route point for VDN and ED flow.	See Adding Transfer to User route point for VDN and ED flow on page 92.	
4	Associate Transfer to User route points with channels.	See Associating channels with Transfer to User route points on page 92.	
5	For Voice contact, configure SelectedResourceTime in Engagement Designer.	See Configuring SelectedResourceTime in Engagement Designer on page 93.	

Enabling the Transfer to User feature

About this task

Avaya Control Manager administrators can enable or disable the Transfer to User feature. Based on this configuration, agents or supervisors can view the Transfer to User option in Avaya Workspaces.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Server Details**.
3. Double-click the administered Avaya Oceana® UCA server or select the administered Avaya Oceana® UCA server, and click **Edit**.
4. On the **System Properties** tab, expand **Transfer To User**.
5. Select the **Enable Transfer To User** check box.
6. Click **Save**.

Adding Transfer to User route points

About this task

You can configure Transfer to User route points for digital media channels such as Chat, Email, SMS, Social, Generic, and Messaging.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.
2. Click **Add**.
3. In the **Type** field, select a Route Point.
4. In the **Sub Type** field, click an option corresponding to Transfer to User.
5. In the **Name** field, type the name of the route point.
6. Click **Save**.

The route points list displays the newly created route point with the **Transfer To User** sub type.

Adding Transfer to User route point for VDN and ED flow

About this task

You can use this procedure to add VDN and ED flow route points to Transfer to User of voice contacts.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.
2. Click **Add**.
3. In the **Type** field, select **Implicit User**.
4. In the **Sub Type** field, select **Transfer To User**.
5. In the **Name** field, type the name of the route point.
6. In the **Address** field, type the address of the route point.
7. Click **Save**.

The route points list displays the newly created VDN and ED flow route points with the **Transfer To User** sub type.

Associating Transfer to User route points with channels

About this task

You can use this procedure to associate the Transfer to User route points with different channels.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Transfer to User**.
2. In the **<Channel>** field, select the Transfer to User route point that you created.

You can associate route points with the following channels:

- **Email**
- **Chat**
- **Messaging**
- **SMS**
- **Social**
- **Generic**
- **Web Voice**
- **PSTN Voice**

3. Click **Save**.

Configuring SelectedResourceTime in Engagement Designer

About this task

The SelectedResourceTime in the transfer flow governs the waiting period of the flow before adding the fallback service to the Transfer to User request to find a matching agent.

The default value of SelectedResourceTime timer for different channels include:

Channel	Value
Chat	20 seconds
SMS	300 seconds
Social	300 seconds
Email	600 seconds
Generic	600 seconds
Voice	20 seconds
Messaging	60 seconds

You can use this procedure to configure SelectedResourceTime timer in the Engagement Designer Admin Console.

Procedure

1. In your web browser, enter the following URL to open Engagement Designer **Admin Console**:

```
https://<AvayaOceanaCluster1_FQDN>/services/EngagementDesigner/admin.html
```

2. On the Workflows tab, select the required workflow and click **Attributes**.
3. In the **SelectedResourceTime** value field, enter the value in seconds.
4. Click the **Tick** icon to save the changes.

Configuring email signature settings

Procedure

1. Log on to the Avaya Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Omnichannel**.
3. Click **Email Signature Configuration**.
4. In the **Max Images Per Signature** field, type the maximum number of images that an agent can use for each signature.
5. In the **Max Images Per Agent** field, type the maximum number of images an agent can use.
6. In the **Max File Size (In KB)** field, type the maximum file size of an image.
7. In the **File Types Allowed** field, type the supported file types separated by a comma.
8. In the **Characters Per Signature** field, type the maximum number of characters supported for each signature.
9. Select the **Disable Email Signature** check box to set email without signature.
10. Click **Save**.

Channel Exclusivity

With Channel Exclusivity, an agent is exclusive on one channel while active on that channel. When the agent finishes all contacts on that channel, the agent is available for any channel and becomes exclusive on the next channel the agent works on.

With Channel Exclusivity, an agent can be interrupted by another contact from the same channel only. Additional channels can be selected on any of the rows to enable further Interruptibility for the agent.

Note:

Regardless of whether Channel Exclusivity is enabled, when an agent activates and starts work, the order in which the configured channels go ready cannot be determined. The requests to login to different channel providers are sent in parallel, and the order of the responses cannot be predetermined.

Work Assignment receives the channel states in the order in which the responses are received. After a channel is available, Work Assignment immediately executes a match if there is a contact waiting on that channel regardless of its priority relative to other channel contacts. It does this by design as it does not know if any other channels are available for that agent at that time.

Channel Interruptibility

To configure Channel Interruptibility, all channels must have minimum one check box selected where the corresponding value for the row and column intersect as shown in the following figure. You can avoid the blank rows.

Channel Interruptibility

	Video	Voice	Messaging	Chat	Email	Generic	Short Message Service	Social
Video	☒	☐	☐	☐	☐	☐	☐	☐
Voice	☐	☒	☐	☐	☐	☐	☐	☐
Messaging	☐	☐	☒	☐	☐	☐	☐	☐
Chat	☐	☐	☐	☒	☐	☐	☐	☐
Email	☐	☐	☐	☐	☒	☐	☐	☐
Generic	☐	☐	☐	☐	☐	☒	☐	☐
Short Message Service	☐	☐	☐	☐	☐	☐	☒	☐
Social	☐	☐	☐	☐	☐	☐	☐	☒

Enabled intersection means that Channel in a Column will interrupt Channel in a Row

The Channel interruptibility feature has built-in default behavior designed to prevent misconfiguration of the interruptibility matrix. If a channel has no check box selected in the corresponding row in the matrix, the channel is interruptible by itself and any other channels the user is logged in on. This setting prevents an agent getting locked or stuck on a single channel.

For example, in a configuration where voice must be interruptible by itself and all other channels, configure the matrix as follows:

Channel Interruptibility

	Video	Voice	Messaging	Chat	Email	Generic	Short Message Service	Social
Video	☒	☐	☐	☐	☐	☐	☐	☐
Voice	☒	☒	☒	☒	☒	☒	☒	☒
Messaging	☐	☐	☒	☐	☐	☐	☐	☐
Chat	☐	☐	☐	☒	☐	☐	☐	☐
Email	☐	☐	☐	☐	☒	☐	☐	☐
Generic	☐	☐	☐	☐	☐	☒	☐	☐
Short Message Service	☐	☐	☐	☐	☐	☐	☒	☐
Social	☐	☐	☐	☐	☐	☐	☐	☒

Enabled intersection means that Channel in a Column will interrupt Channel in a Row

For example, in a configuration where voice must not be interruptible by any other channels, but it can interrupt any other channel, configure the matrix as follows:

Channel Interruptibility

	Video	Voice	Messaging	Chat	Email	Generic	Short Message Service	Social
Video	☒	☒	☐	☐	☐	☐	☐	☐
Voice	☐	☒	☐	☐	☐	☐	☐	☐
Messaging	☐	☒	☒	☐	☐	☐	☐	☐
Chat	☐	☒	☐	☒	☐	☐	☐	☐
Email	☐	☒	☐	☐	☒	☐	☐	☐
Generic	☐	☒	☐	☐	☐	☒	☐	☐
Short Message Service	☐	☒	☐	☐	☐	☐	☒	☐
Social	☐	☒	☐	☐	☐	☐	☐	☒

Enabled intersection means that Channel in a Column will interrupt Channel in a Row

To turn off interruptibility, do one of the following:

- Select all check boxes on all channels.
- Select no check boxes on any channel.

*** Note:**

When Administrator will create new Matrix, all diagonal elements is set to default. It is recommended to avoid the blank rows.

Configuring Channel Exclusivity and Interruptibility

Procedure

1. Log on to the Avaya Control Manager interface.
 2. On the Avaya Control Manager webpage, click **Resource Manager**.
 3. Click **Templates**
 4. Click **Oceana Templates**.
 5. Click **Oceana User Templates**.
 6. On the Oceana User Templates screen, click the plus sign (+) to add a template and configure the following fields:
 - **Template Name:** Enter a name for the template.
 - **Location Name:** Enter the location name.
 - **Channel Exclusivity:** Select the check box to enable Channel Exclusivity.
 - **Channel Interruptibility:** Configure the interruptibility rules.
 - **Channel Reserved Status:** Select the channel on which you want the agent to be reserved.
- You can edit or delete a template using this page.
7. To assign the template to a user:
 - a. On to the Avaya Control Manager interface, click **Users**.
 - b. On the **Users** tab, click a team, and select the user.

- c. Select the check box next to the user.
- d. In the right navigation pane, click **Edit User**.
- e. Click the **Avaya Oceana** tab.
- f. In the User Templates field, select the template created earlier.
- g. Click **Save**.

Reserve agents and thresholds

Reserve agents are available on the reserve channel in exceptional circumstances, such as a configured threshold is breached. If channels are within the configured thresholds, reserve agents are unavailable.

The system does not have any default service thresholds. If you want to configure reserve agents and channel prioritisation based on channel overload, you must configure service thresholds. You must set a service threshold for each channel at a minimum. The base channel threshold can be overridden by more specific services. For example, `attributeSet=Channel.Voice,Language.English`.

Configuring the service and reserve-level thresholds

About this task

Use this procedure to configure the service and reserve-level thresholds. You can also edit the attribute set and threshold values.

Procedure

1. Log on to the Avaya Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Avaya Oceana™**.
3. Click **Threshold**.
4. Click **Oceana Routing**.

Avaya Control Manager displays the list of all services with thresholds.

5. To add a new attribute set:
 - a. Click the plus sign (+).
 - b. Move attributes from the **Available Attributes** list to the **Selected Attributes** list using the arrow buttons.
 - c. Set the threshold value.
 - d. Click **Save**.

You can select multiple attributes from the **Available Attributes** list and move them to the **Selected Attributes** list.

6. To edit an attribute set and threshold values, select the attribute set and click **Edit**.

Configuring Auto answer timeout for a provider

About this task

Use this procedure to configure the Auto answer timeout for a provider. You must enter the value in seconds after which the interaction must be auto answered. If you do not configure this value, the interaction is auto answered without any delay.

* Note:

You cannot configure timeout for voice interactions.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™**.
3. Click **Server Details**.
4. Click one of the following:
 - The plus sign (+) to add a server.
 - **Edit** to edit a server.
5. Click the **Providers** tab.
6. Click the plus sign (+).
7. In the **Type** field, select the provider.
8. In the **Name** field, type the provider name.
9. In the **Address** field, type the address in the format: `<VDN number>@SIPDomain.com`
10. In the **Voice mail Access** field, type the number to access the voice mail system through Avaya Workspaces.
11. In the **External Access Code** field, type the number to make an external voice call.
Avaya Workspaces adds a prefix to this number when an agent makes an external call.
12. Click the **Video Enabled** field to enable the provider to support video in addition to voice.
13. In the **Auto Answer Timer (sec)** field, type the time in seconds after which Avaya Workspaces auto answers the interaction.
14. Click **Save**.

Creating a user profile template for Auto answer

About this task

When you configure both Auto Answer and External Screenpops, the agent's work can be interrupted by a Screenpop from a new interaction that has been automatically answered.

Procedure

1. Log on to the Control Manager interface as an administrator.

2. On the Avaya Control Manager webpage, click **Resource Manager**.
3. Click **Templates**.
4. Click **Oceana Templates**.
5. Click **Oceana User Profile Templates**.
6. Click the plus sign (+).
7. In the **Template Name** field, type the template name.
8. In the **Location Name** field, type the location name.
9. In the **Auto answer** field, select the services for which you want to enable Auto answer.
10. Click **Save**.

Assigning the user profile template to a user

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **User**.
3. On the **Users** tab, click a team.
4. Select the check box next to the user.
5. In the right navigation pane, click **Edit User**.
6. Click the **Avaya Oceana** tab.
7. In the **User Profile Templates** field, select the template created in the “Creating a user profile template for Auto answer” section.
8. Click **Save**.

Handling browser closure and network connection issues

About this task

If an agent closes the browser without logging out from Avaya Workspaces or the client session is disconnected, the Work Assignment component stops and no new work is routed to the agent. The client session can be disconnected because of various reasons, such as browser refresh, browser crash, network changes, system shutdown or sleep, and Avaya Breeze® platform load balancer failure.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™**.
3. Click **Server Details**.
4. Do one of the following:
 - Double-click the UCAServer instance.

- Select the check box for the UCAServer instance and click **Edit**.
5. Click the System Properties tab.
 6. Expand **System Default Codes**.
 7. In the **Default Not Ready code when browser disconnects** drop-down list, select a reason code from the available reason codes.
 8. Click **Save**.

Adding or removing extensions to or from the forbidden extensions

About this task

Use the following procedure to block agents from sending specific file attachments when agents are active on email or chat contacts. The following procedure applies to chat and email contacts.

Procedure

1. Start Omnichannel Administration Utility.
 2. Navigate to **General Administration > File Upload Settings**.
The application displays a form for adding or removing extensions to or from the forbidden extensions list. The forbidden extensions list is loaded from the database.
 3. To create a forbidden list of file extensions, move the required file extensions from the **Available** list to the **Selected** list using the arrow (>>,>,<,<<) buttons.
-  **Important:**
- The read-only **Forbidden Types For Outbound Files** area contains all the selected forbidden extensions separated by commas.
4. In the **Add remove forbidden file extension** area, click **Add** or **Remove**, to add or remove any extension absent in the default forbidden extensions list.
 5. Click **Save**.

Supervisor reporting dashboard - user management

In an Avaya Oceana®, the supervisor reporting dashboard provides real-time reporting capabilities. Using Avaya Workspaces, users can view real-time reporting dashboards to monitor up-to-date statistics for your contact center and resources. You can view changes in call activity in real time by using the supervisor reporting dashboard. Avaya Analytics™ provides real-time data for your dashboards.

You can administer permissions for supervisor reporting dashboard users by using Avaya Control Manager. Avaya Control Manager administrators can assign create, modify, delete, and view permissions to users. The types of supervisor reporting dashboard users are:

- **Avaya Analytics™ Administrator:** This user has permissions to access the supervisor reporting dashboard, but does not use any other Avaya Workspaces features. For example, this user cannot handle interactions. This user sees all agents when viewing a dashboard.
- **Avaya Analytics™ Supervisor:** This user has permissions to access the supervisor reporting dashboard, but does not use any other Avaya Workspaces features. For example, this user cannot handle interactions. This user sees agents and routing service groups that are assigned to them in Avaya Control Manager Agent Groups.

You can assign Avaya Oceana® permissions to supervisor reporting dashboard users in conjunction with Avaya Analytics™ permissions. You assign Avaya Oceana® permissions to Avaya Workspaces users. The types of Avaya Workspaces users are:

- **Avaya Workspaces Administrator:** This user is a standard Avaya Workspaces administrator. You can assign this user Avaya Analytics™ administrator or supervisor permissions to access the supervisor reporting dashboard.
- **Avaya Workspaces Supervisor:** This user is a standard Avaya Workspaces supervisor. You can assign this user Avaya Analytics™ supervisor permissions to access the supervisor reporting dashboard.

This chapter describes how to manage user access for the supervisor reporting dashboard.

Adding reporting users

About this task

Use this procedure to add a reporting user to Avaya Control Manager, who can log on to Avaya Workspaces and use the supervisor reporting dashboard. This user does not use any other Avaya Workspaces features. For example, this user cannot handle interactions.

Assign administrator or supervisor permissions to this user.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and click **Add**.
Control Manager displays the User Details page.
4. Under **Available Applications**, select the **Avaya Analytics** check box.
5. In the **First Name** field, type the first name for the reporting user.
6. In the **Surname** field, type the surname for the reporting user.
7. From the **Profile** list, select **Supervisor**.
8. In the **LDAP Username** field, type the username used by the Authentication server.

You must specify the LDAP Username in the email address format.

For example, type user1@avaya.com.

9. In the **Username** field, type a user name.
10. In the **Password** field, type a password for a user.
11. In the **Confirm password** field, type a password for a user.
12. From the **Team** drop-down list, select the team to add this user to.
13. Click **Save**.
14. Select the **Permissions** tab.
15. Under **Avaya Analytics**, from the **Role Permissions** list, select **Administrator** or **Supervisor**.
16. Click **Save**.

Assigning reporting access to Avaya Workspaces users

About this task

Use this procedure to assign reporting access to existing Avaya Workspaces users, who can then use the supervisor reporting dashboard. You can assign reporting access to Avaya Workspaces administrators and supervisors.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and double-click on the user you want to assign reporting access to.

Control Manager displays the User Details page.

4. Select the **Permissions** tab.
5. Under **Avaya Analytics**, from the **Role Permissions** list, select **Administrator** or **Supervisor**.

Note:

Assigning administrator permissions to an Avaya Workspaces supervisor user is not supported.

6. Click **Save**.
7. Under **Available Applications**, select the **Avaya Analytics** check box.
8. Click **Save**.

About routing services groups

With Control Manager you can create named groups of routing services. A routing service group can contain any of the routing services that exist in Avaya Oceana®. Manage routing service groups through the existing group management portal.

Control Manager fetches the routing services from Unified Collaboration Administration (UCA) and uses these services to create routing groups inside the group management portal. If a call is routed by a routing service that is not in a routing service group that is assigned to a reporting supervisor, the call data is not visible to the reporting supervisor. If Avaya Oceana® expands the search pool by removing an attribute from the requested service to route a call, and if this routing service is not in a routing service group then this call data is not visible to the reporting supervisor.

Creating Routing Service groups

About this task

With Control Manager you can create named groups of routing services. A routing service group can contain any of the routing services that exist in Avaya Oceana®. Manage routing service groups through the existing group management portal.

Control Manager fetches the routing services from Avaya Oceana® and uses these services to create routing groups inside the group management portal. If a call is routed by a routing service that is not in a routing service group that is assigned to a reporting supervisor, the call data is not visible to the reporting supervisor. If Avaya Oceana® expands the search pool by removing an attribute from the requested service to route a call, and if this routing service is not in a routing service group then this call data is not visible to the reporting supervisor.

Use this procedure to create a routing service group in Avaya Control Manager and map it to an Avaya Oceana® supervisor or administrator user and Avaya Analytics™ supervisor or administrator user.

Before you begin

- Configure Work Assignment services in Avaya Control Manager.
- Configure agents with the same attributes as the Work Assignment service in Avaya Control Manager.
- Assign the Work Assignment services to a routing service group.
- Assign privileges to the routing service group to the reporting supervisor.

Procedure

1. On the Avaya Control Manager webpage, click **Groups**.

Avaya Control Manager displays the Group Management page with the list of available locations.

2. In the navigation pane, select a location and then click the **Add ACM Group** icon.
3. In the **Entity Type** field on the Group Details page, select **Routing Service**.
4. In the **Name** field, enter a name for the routing group.
5. In the **Description** field, enter a description for the routing group.

6. In the **Systems** field, select the **Oceana** check box.
7. Click **Save**.
8. Click the **Entity Assignment** tab.

 Note:

Routing services under the Entity Assignment tab can be any named service.

9. In the **Available** section, do one of the following:
 - To move one item, select the item and click the arrow icon  to move the selected item to the **Selected** section.
 - To move multiple items, press the **Ctrl** key to select and click the arrow icon  to move the multiple items to the **Selected** section.
10. Click **Save**.

Assigning routing groups to a user

Procedure

1. Navigate to **Users**.
2. On the **Users** tab, click a team, and select a user.
3. Click  > **Edit User**.

The system displays the User Details page.
4. Scroll to the right and click the **ACM Groups** tab.
5. Expand **Avaya Oceana** and then expand **Routing Service Groups**.
6. Select the routing group that you want to assign to the user.
7. Click **Save**.

Group management

Group management, also referred to as data partitioning, provides a data access control mechanism for agents and supervisors within an Avaya Oceana® instance. By creating groups and assigning relevant entities to the groups, you can control data access across agents. You can create customer-defined data groups to restrict the data that agents can see within Avaya Workspaces while handling contacts. You can restrict agents from accessing data that is not relevant to their group or business unit.

You can assign the following Avaya Oceana managed entities to a group:

- Work codes
- Disposition codes

- User codes
- Defer codes
- Transfer services
- Screenpops
- Email template groups
- Outgoing mailboxes

An agent can access only those entities of a group that are assigned to the agent.

 Note:

- Groups are added within the context of the Avaya Control Manager location because locations are the virtual objects that form the core entity of the Avaya Control Manager environment.
- Data partitioning is not supported for rejection codes. There is no group management mechanism to enable different agents to see different rejection codes.

Adding a group

About this task

Use this procedure to add data access groups to the locations created in Avaya Control Manager. You can create maximum 100 groups in Avaya Control Manager.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Groups**.
The system displays a list of available locations in the navigation pane.
3. Select a location and click **Add Parent Group**.
4. In the **Group Details** section, do the following:
 - a. In the **Name** field, enter the name of the parent group.
 - b. In the **Description** field, enter a description of the parent group.
5. Click **Save**.
The page gets refreshed.
6. In the navigation pane, click the parent group that you created earlier and then click **Add ACM Group**.
7. In the **ACM Group Details** section, do the following:
 - a. In the **Entity Type** field, select the entity type that you want to associate with the group.
 - b. In the **Name** field, enter a name for the entity type.

- c. In the **Description** field, enter a description of the entity type.
 - d. In the **Systems** field, select **Oceana**.
 8. Click the **Entity Assignment** tab.
 9. In the **Available** section, do one of the following:
 - To move one item: Select the item and click the arrow icon ➞ to move the selected item to the **Selected** section.
 - To move multiple items: Press the **Ctrl** key to select and click the arrow icon ➞ to move the multiple items to the **Selected** section.
- Repeat Step 6 to Step 9 to add each required **Entity Type** in the data group.
10. Click **Save**.

Assigning groups to a user

About this task

Assign data access groups to a user to restrict the data that a user can see within Avaya Workspaces. The data access rule is the union of the groups assigned to a user. You can assign maximum five groups to a user.

Users can access all the data in the system if:

- No groups are assigned to them.
- Groups assigned to them do not have a selection for a given entity type. For example, if a user is assigned to groups containing work codes and user codes, the user can access only the assigned work codes and user codes.

Procedure

1. Log on to the Avaya Control Manager interface with administrator credentials.
2. On the Avaya Control Manager webpage, click **Users**.
3. On the **Users** tab, click a team, and select a user.
4. Click  > **Edit User**.

The system displays the User Details page.
5. Click the **ACM Groups** tab.
6. Select the groups that you want to assign to the user.
7. Click **Save**.

Editing a group

About this task

Use this procedure to edit a data access group. Changes made to groups are reflected immediately to agents logged into Avaya Workspaces.

! Important:

If Avaya Control Manager administrator renames a group, the group is assigned back to the default layout in Avaya Workspaces.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Groups**.
The system displays a list of available locations in the navigation pane.
3. In the navigation pane, click the parent or child group that you want to edit.
4. Edit information in the appropriate fields.
5. Click **Save**.

Deleting a group

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Groups**.
The system displays a list of available locations in the navigation pane.
3. In the navigation pane, click the parent or child group that you want to delete.
4. Click **Delete**.

When you delete a parent group, the child groups are also deleted.

Thresholds

In Avaya Control Manager, you can configure thresholds for Channels and Named Services from the SLA Threshold Management page.

Thresholds for Channels are defined in UCA and can be configured in Control Manager. When you configure existing thresholds, data is synchronized between Control Manager and UCA.

Thresholds for Named Services are defined in Work Assignment Portal. You can create new thresholds or configure existing thresholds for these Named Services in Control Manager. When you create or configure thresholds, data is synchronized between Control Manager and UCA.

On the SLA Threshold Management page, you can delete the thresholds for Named Services created from this page, but not the Channels.

Configuring thresholds in Avaya Control Manager

About this task

Use this procedure to configure thresholds for Channels and Named Services.

Before you begin

Ensure that UCA is functioning.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Threshold > Analytics Service Levels**.
2. On the SLA Threshold Management page, select the Channel Name whose values you want to change and enter values.
3. To change individual values, click the value that you want to change and enter a new value.
4. Click **Save**.

The system saves the new threshold value and synchronizes the new value between Control Manager and UCA.

Creating new thresholds for Name Services in Avaya Control Manager

About this task

Use this procedure to create new thresholds for Named Services.

Before you begin

Ensure that Work Assignment Portal is functional where Name Services are created.

Important:

Thresholds created for Name Services overwrites the thresholds created for Channels.

Thresholds cannot be configured for the system service name called Specified Resource.

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Threshold > Analytics Service Levels**.
2. On the SLA Threshold Management page, click **New**.
3. On the Add New Threshold page, select the Named Service to which you want to add threshold values.

Ensure that you enter a value for at least one measure.

4. Click **Save**.

The system adds a new Named Service on the SLA Threshold Management page.

Configuring thresholds for Short Not Ready

Procedure

1. Log on to Avaya Control Manager.
2. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Server Details**.
3. Select the check box for the UCA server that you want to configure and then click **Edit**.
4. On the Avaya Oceana Server Edit page, click the **System Properties** tab.
5. Expand **Thresholds** and change the threshold value for **Short Not Ready**.
6. Click **Save**.

Threshold measures

Measures	Description
Answered After	The number of calls answered after the maximum service level threshold.
Abandoned After	The number of calls abandoned after the minimum threshold.
Long Engagements	A count of engagements that the agent was active on for a duration that exceeded the value defined for this measure.
Short Engagements	A count of engagements that the agent was active on for a duration that was below the value defined for this measure.
Long Wrap Ups	A count of engagement wrap-ups whose duration exceeded the value defined for this measure.
Short Wrap Ups	A count of engagement wrap-ups whose duration was less than the value defined for this measure.
Long Holds	A count of engagements that the agent held for a duration that exceeded the value defined for this measure. This measure considers hold time in which the agent focus remained on the held engagement and hold time in which the agent focus changed to a different engagement.

Agent Layout Provisioning

Overview

The Agent Layout Provisioning feature, administrators can create multiple layouts to assign to agent groups. You can create a maximum of 50 layouts using Avaya Workspaces.

Using the Layout Manager, you can do the following:

- View a table with all the available layouts.
- Export each individual layout, import a new layout, edit one of the existing layouts, clone a layout, and create a new layout.
- Delete any of the custom layouts created. The default layout can only be modified but not deleted.

A layout associated with a set of groups can be deleted without removing the groups from the layout. When you click delete, a warning dialog is displayed to confirm if the layout must be deleted. If you confirm, the layout is deleted and all the groups are available for assigning again. If an agent was in a group and that group layout was deleted, the agent is assigned to the default layout when they subsequently log in.

You can choose from a list of available agent groups which can be assigned to the current layout. The grayed-out groups indicate that the group is already assigned to a layout. This allows you to move from the singular layout structure to the new multiple layouts structure to import the layout `.json` files. The imported layouts are available on the **Layout Manager** in the **Layouts** tab. The previously imported layouts adopt the new multi-layout structure and are available for assigning to agent groups. When you upgrade from Avaya Workspaces 3.6.x to a later version, if a layout migration is required, you can migrate each layout individually by clicking the migrate layout button on each of the layouts listed. You can also view the version number of each of the layouts, along with the layout name and description. Each layout has a reset button which resets that specific layout, and does not affect any other layout or custom widgets.

Agents that are in multiple groups with different assigned layouts can select their preferred layout in the **Layouts** tab of the **Settings** widget. The default layout is selected on first login. After that agents can choose their preferred layout from the drop-down menu. The selected layout is applied and is saved as the preferred layout and is loaded on the subsequent logins. If the current preferred layout is removed from the agent's group, the default layout is applied if Avaya Workspaces refreshes, or for subsequent logins.

Configuring layouts

About this task

You can configure a layout while creating a new layout or editing an existing layout.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the Layout Manager icon.

3. Do one of the following:
 - For creating a new layout, click **Create New Layout**.
 - To edit an existing layout, click the edit icon.
4. In the **Name** field, type a name for the layout.
5. In the **Description** field, type the layout description.
6. To use a compressed layout, select **Use compressed**.
7. Use the **+** and **x** buttons on the left and right columns respectively, move the required agent groups from the unselected to the selected area.
8. Click **Save Changes**.

Managing layouts

About this task

The layouts table displays all the available layouts. The layouts have a layout name, a layout version, and a description, along with buttons on each layout. The administrator can migrate, export, edit, clone, reset or delete the layouts. The default layout cannot be deleted.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the Layout Manager icon.
3. An administrator can perform the following actions:
 - Click  to export a layout.
 - Click  to clone a layout.
 - Click  to edit a layout.
 - Click  to migrate a layout.
 - Click  to reset a layout.
 - Click  to delete a layout.

Customizing layouts

About this task

You can customize layouts so that Avaya Workspaces agents and supervisor can see relevant options when they log in. For example, add new sidebar options that display specific default or custom widgets when selected.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the Layout Manager icon.
3. Select a layout to edit.
4. On the CUSTOMIZE LAYOUT tab, select the layout to change.

For example, select Voice.

Important:

Ensure that you configure the widget on the visible pane of the channel, so that the widget is present and visible when the agent views a work card.

5. On the CUSTOMIZE SIDEBAR tab, select a sidebar tab or click **Add New Sidebar Tab**.
6. If this is a new sidebar, in the **Name** field, type the name for the sidebar.
7. If this is a new sidebar, in the **Description** field, type a description for the widget.
8. From the **Icon** list, select an icon for the widget.
9. In the **Align** field, select the required alignment.
10. In the **Role** field, select the required role.
11. From the **Select Layout** list, select a layout.
12. From the **Select Widgets** list, select the widgets that you want to appear on the layout.
13. Click **Save Changes**.

When an agent logs in with this specific layout assigned, the configured widgets appear on the relevant tab.

Adding multiple agents to layout groups

About this task

You can use Avaya Control Manager to associate a user group to a workspaces layout sub type. You can then add agents to the user group using the **Entity Assignment** tab.

Procedure

1. Log on to the Control Manager interface as an administrator.
2. On the Avaya Control Manager webpage, click **Groups**.

The Control Manager interface displays a list of available locations in the navigation pane.

3. Select a location and click **Add ACM Group**.
4. In the **Group Details** section, do the following:
 - In the **Entity Type** field, select **User**.
 - In the **Name** field, enter a name for the entity type.

- In the **Description** field, enter a description of the entity type.
- Select **Workspaces Layout**.

It is mandatory to select any one of the sub types.

5. Click the **Entity Assignment** tab.
6. In the **Available** section, do one of the following:
 - To move one item: Select the item and click the arrow icon ➞ to move the selected item to the **Selected** section.
 - To move multiple items: Press the **Ctrl** key to select and click the arrow icon ➞ to move the multiple items to the **Selected** section.
7. Click **Save**.

Cross-channel limit

Large number of queued contacts in Avaya Oceana® may lead to system failure. To prevent the failure, Avaya Oceana® introduces cross-channel limits. The limits in Avaya Oceana® have been channel based and not an overall limit on the number of contacts. These channel specific limits are still applicable, but Avaya Oceana® introduces an overall limit on the contacts that can be present in the system queue. Avaya Oceana® rejects all new digital contacts when cross-channel limit is reached.

Configuring channel limits

About this task

You can configure an overall limit on the number of contacts in Avaya Oceana® to prevent system failure due to large number of queued contacts.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration**.
3. Click **Channel Limits**.
The Channels Limits Settings page opens.
4. In the **Size of Digital contacts queue** field, select the check box and enter an appropriate value.
For more information, see [Configuring Email limit](#) on page 114.
5. In the **Cross-Channel Limit** field, select the check box and enter an appropriate value.
6. Click **Save**.

Considering voice contacts in overall cross-channel limit

About this task

You must configure the Work Assignment cluster to consider the number of active voice contacts.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements > Avaya > Configuration > Attributes**.
3. Click the **Service Clusters** tab.
4. In the **Cluster** field, select the cluster.
5. In the **Service** field, select `ORCRestService`.
6. In the **Startup** area, in the **WorkAssignment Cluster** field, select the cluster where the Work Assignment service is installed.
7. Click **Commit**.

Configuring Email limit

About this task

You can use an internal Avaya Oceana® queue to increase the number of queued emails. The queue holds the emails in the OCP database, but does not route the contacts to the agents until the overall numbers of contacts are within the system limits. The email specific queue follows the First In First Out (FIFO) order of contact processing. Use the following procedure to enable the internal Avaya Oceana® queue.

Important:

You can limit the internal OCP queue size by configuring the **Size of Digital contacts queue** attribute. For more information, see [Configuring channel limits](#) on page 113.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements > Avaya > Configuration > Attributes**.
3. Click the **Service Clusters** tab.
4. In the **Cluster** field, select the cluster.
5. In the **Service** field, select `ORCRestService`.
6. In the **Advanced** area, in the **Use internal OCP queue** field, do the following:
 - a. Select **Override Default** check box.
 - b. In the **Effective Value** field, select `true`.
7. Click **Commit**.
8. Reboot Avaya Oceana® Cluster 3.

Multiple WhatsApp number and Facebook business pages for Async messaging

Avaya Oceana® supports multiple WhatsApp numbers and Facebook business pages for Async messaging.

WhatsApp business number and Facebook business page ID is requested from digital connection application for every new incoming integration.

WhatsApp number feature

If digital connection applications use several WhatsApp integrations, you can enable the feature to route contacts based on the WhatsApp business number the message was sent to. When the feature is enabled, AsyncMsgConnector sends an attribute with a WhatsApp business number to Avaya Oceana® during contact creation. This attribute is used to route the contact to the required agent.

The format for the attribute is the WhatsApp number, a dot, and phone number. The attribute comprises of numerals without any other symbols. For example, WhatsAppNo.999999999. The maximum value of the phone number depends on the country.

Facebook business page feature

If digital connection applications use several Facebook integrations, you can enable the feature to route contacts based on the Facebook business page ID the message was sent to. When the feature is enabled, AsyncMsgConnector sends an attribute with a Facebook business page ID to Avaya Oceana® during contact creation. This attribute is used to route the contact to the required agent.

The format for the attribute is the Facebook page number, a dot, and page id number. The attribute comprises of numerals without any other symbols. For example, FacebookPageNo.999999999. The Facebook page id is a 15-digit number.

For more information on creating attributes, refer the following topics:

- [Adding Attribute Categories to Avaya Control Manager](#) on page 35
- [Adding Attributes to Avaya Control Manager](#) on page 36

Agent log-off on browser disconnect

For an ongoing agent-customer contact, Avaya Oceana® introduces an automatic agent log-off feature. The feature is based on a fixed time-lapse or a configurable timer during any of the following error conditions:

- Browser disconnect or when the agent accidentally closes the browser
- Browser freeze
- Network disconnect
- System freeze

Configuring the Workspaces time-out value and reason code

About this task

When the browser disconnects, the configured reason code becomes the agent status after the configured time-out period. By default, the agent status is **Not Ready Pending** or **Not Ready** unless configured.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration > Avaya Oceana > Server Details**.
3. On the Avaya Oceana Server List page, select the server from the list and click **Edit**.
4. On the Avaya Oceana Server Edit page, click the **System Properties** tab.
5. Expand **Workspaces**.
6. In the **Workspaces time-out in seconds** field, enter the time-out value in seconds.



Important:

- The browser disconnect feature is disabled when the **Workspaces time-out in seconds** value is not configured or blank.
 - Ensure that the **Workspaces time-out in seconds** field value is always smaller than the **RONA Timer(Seconds)** field value.
7. Expand **System Default Codes**.
 8. In the **Default Not Ready Code when browser disconnects** field, select `Browser Disconnect (996)`.
 9. Click **Save**.

Enabling or Disabling re-routing of ongoing contacts

About this task

When a browser disconnects at the agent workstation during an ongoing agent-customer interaction resulting in a connection lapse, the ongoing contacts are re-routed to another active agent in the service segment.

Use this procedure to enable or disable re-routing of ongoing contacts upon browser disconnect.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements > Avaya Breeze® > Configuration > Attributes**.

3. Click the **Service Clusters** tab.
4. In the **Cluster** field, select the Unified Agent Controller (UAC) cluster.
5. In the **Service** field, select the UAC service.
6. Expand the **Feature Flag** attribute section.
7. In the **Enable automatic rerouting of contacts when the browser disconnects** attribute field, select the **Override Default** check box.
8. To set the **Effective Value**, choose one of the following:
 - **True** - Enables re-routing of ongoing contacts. The default value is **True**.
 - **False** - Disables re-routing of ongoing contacts.
9. Click **Commit**.

Mandatory selection of From address for an outbound mail

For outbound email contacts, the agent can select the email address for the **From** field from the drop-down list. If the agent fails to enter a **From** address, Avaya Workspaces auto-populates the first value from the drop-down, resulting in the wrong sender address selection.

Avaya Oceana® introduces an ability to mandate the selection of **From** address for outbound mail to activate the **Send** button.

Enabling the mandatory selection From address attribute

About this task

Use this procedure to mandate the selection of the correct **From** address for outgoing mail. The agents must select a valid **From** address from the drop-down list for outgoing mail to activate the **Send** button. If the mandatory selection attribute is disabled, Avaya Workspaces auto-populates the first value from the **From** address field drop-down list.

The mandatory selection attribute check box is unchecked by default.

Procedure

1. Log on to Avaya Control Manager.
2. Navigate to **Configuration > Avaya Oceana > Server Details**.
3. On the Avaya Oceana Server List page, select the server from the list and click **Edit**.
4. On the Avaya Oceana Server Edit page, click the **System Properties** tab.
5. Expand **Workspaces**.
6. Select the **Outgoing Email Address is blank by Default** check box.

7. Click **Save**.

Proficiency levels for attributes within the categories

Avaya Oceana® supports the ability to set proficiency levels for attributes within the categories eliminating the validation of selecting attributes from each category. The administrator can create attribute combinations and set proficiency levels at the user level.

Important:

Proficiency levels for attributes within the categories are set at the user level and not on the group level.

Setting proficiency levels for attributes within the categories

About this task

Use the following procedure to select agent attributes within the categories, create a combination, and set proficiency levels at the user level.

Procedure

1. Log on to Avaya Control Manager.
2. Click **Users**.
3. Select a user from the list and click **Edit User**.
4. Click the **Properties** tab.
5. Select **Proficiency**.
6. In the **Proficiency Override** section, select the required attributes.
7. Select a **Proficiency** value from the drop-down list for the selected attributes.
8. Click **Save**.

Chapter 4: Automation overview

Automation Overview

The Omnichannel Administration Utility provides the option to configure startup message for a specific channel type. This functionality enables you to send initial messages from SMS or Social channels to the BotConnector. You can use the **Automation Config** option to configure the message for the following options:

- Enable Startup message for Channel Type.
- Enable sending of initial customer's message for Channel Type.

Configuring Automation

About this task

Use the **Automation** option to enable the startup message for a specific channel type.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Automation**.
3. Click **Config**.
4. Navigate to the **Automation Configuration** section.
5. In the **Enable Startup message for Channel Type** option, select the channel type.
6. Select the channel type **Enable sending of initial customer's messages for Channel Type**.
7. Click **Save**.

Chapter 5: Chat administration

Omnichannel Administration Utility

Use the Omnichannel Administration Utility to commission and maintain multimedia resources.

To assist agents with Chat contacts, you can use automatic phrases to configure text for agents to automatically insert in the text-based conversation. You can also configure page push URLs that are commonly sent to customers. The automatic phrases and page push URLs save the typing time of agents when they are communicating with customers.

The automatic phrases and page push URLs include the following:

- A Web On Hold URL group that creates a list of web pages sent to the customer's desktop while the customer waits for an agent to respond to their initial contact.
- A Web On Hold comfort group that creates a list of messages sent to the customer's desktop while the customer waits for a specified period for an agent to respond to their initial contact.
- A Chat comfort group that creates a list of messages sent to the customer's desktop while the customer waits for a specified period for an agent to respond to their initial contact or during the communication.

Creating Web On Hold URL groups using Omnichannel Administration Utility

About this task

A Web On Hold URL group is a sequence of URLs that can be presented in a customer's web browser while the customer waits for an agent in a web communication. You can define the time for which each URL must appear on the web browser of the customer.

The Web On Hold URL presents each message in the group in a sequence. Every message is presented in a sequence after reaching a specified delay. After reaching the specified delay, the first message is presented, and then the second message in the group is presented. After all the messages in the group are presented, the Web On Hold URL resets to the first sequence in the group to present the first message.

Web On Hold URLs can include multimedia files, such as audio or video files. To run the multimedia files, customers must download the required plug-ins on their web browsers.

The maximum number of URLs that you can add to a Web On Hold URL group is 50. However, you must ensure to not add more than 25 URLs to a Web On Hold URL group.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Web On Hold**.
4. Click the **On Hold URLs** tab.
5. Click **New**.
6. In **Tag**, type a name for the Web On Hold URL group.
7. In **Description**, type a description for the Web On Hold URL group.
8. In **Hold Time**, type the number of seconds to display each URL in the customer's browser.
9. In **URL**, type the URL to display on the web browser of the customer.
10. Click **Add**.
11. Repeat Step 2 to Step 10 to add all URLs to the current Web On Hold URL group.
12. In the Edit Attributes area, select the required attributes.
For example, select `Language.English`.
13. Click **Save**.

Creating Web On Hold comfort groups using Omnichannel Administration Utility

About this task

A Web On Hold comfort group consists of a list of sequential messages sent to the customer's desktop for a specified time while the customer waits for an agent to respond.

You can set the time for which messages display on the customer's desktop.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Web On Hold**.
4. Select the **On Hold Comfort Groups** tab.
5. In the Comfort Group section, click **New**.
6. In **Name**, type a name for a new Web On Hold comfort group.

7. In **Delay**, type the number of seconds to display each comfort message on the customer's desktop.
8. In **Message Text**, type the comfort message.
9. Click **Add**.
10. Repeat this procedure to add messages to the current Web On Hold comfort group.
11. In the Edit Attributes section, select the required attributes.
For example, select `Language.English`.
12. Click **Save**.

Creating chat comfort groups

About this task

A Chat comfort group consists of a list of sequential messages sent to the customer's desktop while they wait for an agent to respond, for a specified time from their initial contact or during the communication.

You can set the time for which the messages must display on the customer's desktop.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Comfort Messages**.
4. In the Comfort Group section, click **New**.
5. In **Name** field, type a name for the comfort group.
6. In **Delay** field, type the number of seconds each comfort message must display on the customer's desktop.
7. In **Message Text** field, type the comfort message.
8. Click **Add**.
9. Repeat this procedure to add messages to the current Web communications comfort group.
10. In the Group Messages section, use the arrow keys to configure the sequence of messages.
11. In the Edit Attributes section, select the required attributes.
For example, select `Language.English`.
12. Click **Save**.

Creating automatic phrases using Omnichannel Administration Utility

About this task

Configure automatic phrases by attributes. You can create a list of commonly used phrases for agents to insert into their Web communications contacts instead of typing individual responses.

To assist agents with Chat contacts, you can use automatic phrases to configure text for agents to automatically insert in the text-based conversation. The automatic phrases save the agent typing time when communicating with the customer.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat**.
3. Click **Auto Phrases**.
4. Perform one of the following steps:
 - From the drop-down list, select an existing Phrase Group.
 - In **Name**, type a name for the Phrase Group and click **Create**.
5. In the Create Auto Phrase section, perform the following steps to create an Auto Phrase:
 - a. In **Name**, type a name to represent the Auto Phrase.
 - b. In **Phrase Text**, type the text that is commonly used for the contacts based on the selected attributes.
 - c. Click **Create**.

The system adds the Auto Phrase in the Phrase not in this group section.
6. In the Phrase not in this group section, select the Auto Phrase and click the < button to add the Auto Phrase to the Phrase Group:

The system moves the Auto Phrase in the Phrase in this group section.
7. In the Edit Attributes section, select the required attributes that you want to add to the Phrase Group.
8. Click **Save**.

Creating a Page Push URL for Co-Browsing

About this task

An agent can start a Co-browsing session to assist a customer. The agent and customer can browse the same web pages simultaneously to collaborate and accomplish certain tasks. The agent can assist the customer to navigate through the web pages and, if required, in filling out

forms. In Avaya Workspaces, an agent can choose a web page, from a list of Page Push URLs, to share and Co-browse with the customer.

Configure the Page Push URLs and ensure that the names are descriptive to assist agents when using Avaya Workspaces.

You can configure maximum 50 URLs.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Page Push URLs**.
4. In **Group Name**, enter a descriptive group name.
5. Click **Create**.
6. In **Page Push Group**, select the group.
7. In **URL**, enter a URL to test Co-browsing.
8. In **Description**, enter a descriptive name for the URL.
9. Click **Create**.

The system adds the test URL to the URLs not in Group section.

10. In the URLs not in Group section, select the test URL and click **Add**.

The system moves the test URL to the URLs in Group section.

Ensure that the **Co-Browse** check box for the test URL is selected.

11. In the Edit Attributes section, select the required attributes for the agents with access to this Co-Browsing Group and URL.
12. Click **Save**.

Creating Chat Headers using Omnichannel Administration Utility

Before you begin

- Configure at least one Chat History Header prepared response.
- Configure an email inbox.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Chat Headers**.

4. In **Chat Header**, select the Chat History Header prepared response that you configured.
5. In **From Address**, select the email inbox that you configured.
6. In **Edit Attributes**, select the attributes for the chat header.
7. In **Default Chat Header**, select the default chat header.
8. In **Default From Address**, select the default email inbox.
9. Click **Save**.

Configuring Web Chat settings

About this task

Use this procedure to configure the web chat settings for an agent.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging > Config**.
3. In the **Web Chat Agent Timers** section, enter appropriate values for each field. For information on each field, see [Web Chat Settings field descriptions](#) on page 125.
4. In the **Chat Conversation** section, enter appropriate values for each field. For more information about each field, see [Web Chat Settings field descriptions](#) on page 125.
5. In the **Web Chat Security/Transcripts access** section, in **External Web Server Domain**, enter an appropriate value. For more information about the field, see [Web Chat Settings field descriptions](#) on page 125.
6. In the **Messaging chat parameters** section, enter appropriate values. For more information about each field, see [Web Chat Settings field descriptions](#) on page 125.
7. In the **Messaging chat file transfer parameters** section, enter appropriate values. For more information about each field, see [Web Chat Settings field descriptions](#) on page 125.
8. Click **Save**.

Web Chat Settings field descriptions

The following table provides the field descriptions for configuring the **Web Chat Settings** option:

Field Name	Description
Web Chat Agent Timers	
Keep Alive Time	The time limit till when a chat is kept alive. Total keep alive time should be between 1 second and 10 minutes.

Table continues...

Field Name	Description
Force Idle Customer Check Timeout	The time limit after which an idle customer chat is timed out. The time limit is 6000 seconds or less.
SaveTimestamp on Chat Messages	Select this check box to save the timestamps on the chats.
Save Chat History	Select this check box to save the chat history.
Concurrent Chats limit per Customer	The maximum number of concurrent chats per customer.
Chat Conversation	
E-mail chat log to customer	Select the check box to send chat logs to customers thru email.
Maximum file transfer size	The maximum file size in MBs to transfer during a chat.
Web Chat Security/Transcripts access	
External Web Server Domain	An HTTP origin point that can access web-chat customer API. For more information, see Configuring CORS for the sample Chat client on page 126.
Messaging chat parameters	
Contact timeout	Time to wait after a socket disconnects before closing contact on Workspaces.
Messages display number	The number of previous messages to display in a messaging chat.
Messaging chat file transfer parameters	
Max outbound file size	The maximum file size in MBs for an outbound file transfer during a messaging chat.
Outbound file types allowed	The file types or the file extensions allowed for the outbound messages. Click Set types to select the required file types.
Max inbound file size	The maximum file size in MBs for an inbound file transfer during a messaging chat in.
Inbound file types allowed	The file types or the file extensions allowed for inbound messages. Click Set types to select the required file types.

Configuring CORS for the sample Chat client

About this task

Use this procedure to Configure Cross-origin Resource Sharing (CORS) for the sample Chat client. CORS is a mechanism by which restricted resources on a node can be requested from another domain outside the domain from which the resource originated.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.

3. Click **Config**.
4. In the Web Chat Security section, in **External Web Server Domain**, enter one of the following values:

- To allow all domains, enter an asterisk wildcard *.

 Important:

- If you keep this field blank, the system does not allow any domains and refuses all chats.
- Do not perform this step in Production.
- To allow a single external server or domain, enter the IP address or FQDN of the server where the sample Chat client is hosted.

Removing attributes and routepoints from Omnichannel Database

About this task

When you remove attributes and routepoints from Avaya Control Manager, they are not removed from Omnichannel Database. Therefore, you must use this procedure to permanently remove them from Omnichannel Database.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration > System > Attribute cleanup**.
3. On the Attributes tab, select the check box for the attribute that you want to remove.
4. In the Groups section, check if any groups are attached to the attribute.
5. If no groups are attached to the attribute, click **Delete**.
6. If any groups are attached to the attribute, do the following:
 - a. Select the group and click **Edit**.
Omnichannel Administration Utility redirects you to the edit page of the group.
 - b. On the edit page of the group, unassign the attribute and click **Save**.
 - c. In the navigation pane, click **General Administration > System > Attribute cleanup**.
 - d. On the Attributes tab, select the check box for the attribute.
 - e. In the Groups section, check if any groups are attached to the attribute.
 - f. Repeat Step a to Step e until you unassign the attribute from all groups.
 - g. After you unassign the attribute from all groups, click **Delete** to remove the attribute.

7. Select the **Routepoints** tab.
8. On the Routepoints tab, select the check box for the route point that you want to remove.
9. In the Rules section, check if any rules are attached to the route point.
10. If no rules are attached to the route point, click **Delete**.
11. If any rules are attached to the route point, do the following:
 - a. Select the rule and click **Edit**.

Omnichannel Administration Utility redirects you to the edit page of the rule.
 - b. On the edit page of the rule, unassign the route point and click **Save**.
 - c. In the navigation pane, click **General Administration > System > Attribute cleanup**.
 - d. On the Routepoints tab, select the check box for the route point.
 - e. In the Rules section, check if any rules are attached to the route point.
 - f. Repeat Step a to Step e until you unassign the route point from all rules.
 - g. After you unassign the route point from all rules, click **Delete** to remove the route point.

Setting contacts to closed

About this task

Omnichannel Administration utility provides a contact cleanup option that sets all contacts of any type to a **Closed** state.

Important:

This option sets all contacts to the closed state. Therefore, you must use this option carefully.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration > System > Contact cleanup**.
3. In the **Set all contacts to closed** field, click **Close Contacts**.

This sets all contacts in the database to closed. As a result, the active sessions of the contacts are terminated.

4. Click **Yes** to confirm.

Configuring messaging transcripts

About this task

Use this procedure to configure the messaging transcripts.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Transcripts**.
3. Click **Config**.
4. Navigate to the Messaging Transcript Access section.
5. In **Web Service**, type the complete URL of the filtering service.

For example, `http://127.0.0.1/CustomerFilterMessages-{$version}/rest/filter`. If your service listens on a port other than 80 or 443, include the port number.

Note:

The URL for transcript server is case sensitive and it is only applicable for the host in case of FQDN use.

6. In **Send Option**, select one of the following options:
 - `Do not send`
 - `Legacy transcript`: Select this option if you are using Avaya Oceana® Release 3.5 or earlier.
 - `Enhanced transcript`: Refers to the extended version of message transcripts, which can store filtered transcripts outside Avaya Oceana®.
Select this option if you are using Avaya Oceana® Release 3.6 or later.
 - `Enhanced transcript API - v2`: Select this option if you are using Avaya Oceana® 3.8.0.1 or later.
7. Click **Save**.

Configuring regular retry of failed messaging transcripts

About this task

Use this procedure to configure regular retry of failed messaging transcripts.

Before you begin

Ensure that you enable messaging transcripts and configure the messaging transcript web service.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Transcripts**.
3. Click **Config**.
4. **(Optional)** In **Number of days to retry**, set the number of days the CustomerControllerService retries to send a transcript to the transcript service.

After reaching this limit, the transcript is set to *Permanently Failed*, and the CustomerControllerService stops the retry. This value applies to email and messaging.
5. Navigate to the **Transcript Resend Schedule** section.
6. In **Messaging retry time**, select the start and end times.

The start and end time in the **Messaging retry time** field must be different from that in the **Email retry time** field. Any change in the start or end time takes 15 minutes to get updated.
7. Click **Save**.

Configuring WhatsApp settings

About this task

Use this procedure to configure WhatsApp settings for the native media types such as documents, audios, images, stickers, and videos. You can configure the file types and file sizes to upload and download to and from WhatsApp messages for each media type.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **WhatsApp**.
4. In **Outbound file types allowed**, click **Set Types** to configure the file types for the outbound transfer of messages.
5. In the **Configure File Transfer Types** dialog box, select the required file extensions from the **Available Types** list to the **Selected** list using the arrow (>>,<<) buttons. For more information on the file types allowed for each media type, see [Available file types for WhatsApp media types](#) on page 131.
6. In **Inbound file types allowed**, click **Set Types** to configure the file types for inbound messages.
7. In the **Configure File Transfer Types** dialog box, select the required file extensions from the **Available Types** list to the **Selected** list using the arrow (>>,<<) buttons.

8. Click **Save**.
9. To set the allowed file sizes, in the **File transfer sizes** section, select the required **Media Type**.

The following are the Media Types and the maximum allowed file size in KB:

- document - 25600
- audio - 16384
- image - 5120
- sticker - 100
- video - 16384

10. Click **Edit**.

The **Edit file transfer sizes for <selected> media type** dialog box is displayed.

11. In **Max outbound file size**, the maximum allowed size is entered by default. You can edit this to decrease the size if required.
12. In **Max inbound file size**, the maximum allowed size is entered by default. You can edit this to decrease the size if required.
13. Click **Save**.

Available file types for WhatsApp media types

Administrators can use this information to select the applicable file types for native WhatsApp media types such as documents, audios, images, stickers, and videos.

Table 1:

WhatsApp Media Type	Allowed File Type
document	video/3gpp2
document	application/x-7z-compressed
document	video/x-msvideo
document	image/bmp
document	text/csv
document	application/msword
document	application/vnd.openxmlformats-officedocument.wordprocessingml.document
document	message/rfc822
document	image/gif
document	text/calendar
document	application/octet-stream

Table continues...

WhatsApp Media Type	Allowed File Type
document	text/plain
document	audio/m4a
document	video/x-m4v
document	video/quicktime
document	application/mp4
document	video/mpeg
document	application/vnd.apple.numbers
document	application/x-iwork-numbers-sffnumbers
document	application/vnd.oasis.opendocument.text
document	application/ogg
document	video/ogg
document	application/vnd.apple.pages
document	application/pdf
document	image/x-png
document	image/x-citrix-png
document	application/mspowerpoint
document	application/powerpoint
document	application/vnd.openxmlformats-officedocument.presentationml.slideshow
document	application/x-mspowerpoint
document	application/vnd.ms-powerpoint
document	application/vnd.openxmlformats-officedocument.presentationml.presentation
document	image/svg+xml
document	image/tiff
document	text/x-vcard
document	audio/x-wav
document	video/webm
document	video/x-ms-wmv
document	application/vnd.ms-excel
document	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
document	application/rss+xml
document	text/yaml
audio	audio/aac
audio	audio/amr
audio	audio/mp4
audio	audio/mpeg

Table continues...

WhatsApp Media Type	Allowed File Type
audio	audio/ogg
image	image/png
image	image/png
sticker	image/webp
video	video/mp4
video	video/3gpp

Configuring Facebook settings

About this task

Use this procedure to configure Facebook settings for the native media types such as audios, images, and videos. You can configure the file types and file sizes to upload and download to and from Facebook for each media type.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Facebook**.
4. In **Outbound file types allowed**, click **Set Types** to configure the file types for the outbound transfer of messages.
5. In the **Configure File Transfer Types** dialog box, select the required file extensions from the **Available Types** list to the **Selected** list using the arrow (>>,<<) buttons. For more information on the file types allowed for each media type, see [Available file types for Facebook media types](#) on page 134.
6. In **Inbound file types allowed**, click **Set Types** to configure the file types for inbound messages.
7. In the **Configure File Transfer Types** dialog box, select the required file extensions from the **Available Types** list to the **Selected** list using the arrow (>>,<<) buttons.
8. Click **Save**.
9. To set the allowed file sizes, in the **File transfer sizes** section, select the required **Media Type**.

The following are the Media types and the maximum allowed file size in KB:

- file - 25600
- audio - 25600
- image - 25600

- video - 25600

10. Click **Edit**.

The **Edit file transfer sizes for <selected> media type** dialog box is displayed.

11. In **Max outbound file size**, the maximum allowed size is entered by default. You can edit this to decrease the size if required.
12. In **Max inbound file size**, the maximum allowed size is entered by default. You can edit this to decrease the size if required.
13. Click **Save**.

Available file types for Facebook media types

Administrators can use this information to select the applicable file types for native Facebook media types such as audios, images, videos, and files.

Table 2:

Facebook Media Type	Allowed File Type
video	video/3gpp
video	video/mp4
image	image/png
image	image/jpeg
audio	audio/ogg
audio	audio/mpeg
audio	audio/mp4
audio	audio/amr
audio	audio/aac
file	image/webp
file	video/x-msvideo
file	video/msvideo
file	video/avi
file	video/vnd.avi
file	image/bmp
file	text/csv
file	application/msword
file	application/vnd.openxmlformats-officedocument.wordprocessingml.document
file	message/rfc822
file	image/gif

Table continues...

Facebook Media Type	Allowed File Type
file	text/calendar
file	application/octet-stream
file	text/plain
file	audio/m4a
file	video/x-m4v
file	video/quicktime
file	application/mp4
file	video/mpeg
file	application/vnd.apple.numbers
file	application/x-iwork-numbers-sffnumbers
file	application/vnd.oasis.opendocument.text
file	application/ogg
file	video/ogg
file	application/vnd.apple.pages
file	application/pdf
file	image/x-png
file	image/x-citrix-png
file	application/mspowerpoint
file	application/powerpoint
file	application/vnd.openxmlformats-officedocument.presentationml.slideshow
file	application/x-mspowerpoint
file	application/vnd.ms-powerpoint
file	application/vnd.openxmlformats-officedocument.presentationml.presentation
file	image/svg+xml
file	image/tiff
file	text/x-vcard
file	audio/x-wav
file	audio/wav
file	video/webm
file	video/x-ms-wmv
file	application/vnd.ms-excel
file	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
file	application/rss+xml
file	text/yaml

Configuring Twitter settings

About this task

Use this procedure to configure Twitter settings for the native media types such as gifs, images, and videos. You can configure the file types and file sizes to upload and download to and from Twitter for each media type.

Twitter supports ten file types or extensions for native media options. Additionally, an agent can send files with 45 extensions based on the configurations.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Twitter**.
4. In the **Default media file transfer settings** section, in **Outbound file types allowed**, click **Set Types** to configure the file types for outbound transfer of messages.
5. In the **Configure File Transfer Types** dialog box, select the required file extensions from the **Available Types** list to the **Selected** list using the arrow (>>,>,<,<<) buttons.

 Note:

The Max outbound file size for the default media files is by default 25600 KB. This file size is not configurable.

6. In the **Natively supported Twitter file transfer extensions** section, in **Outbound file types allowed**, click **Set Types** to configure the file types for outbound transfer of messages.
7. In the **Configure File Transfer Types** dialog box, select the required file extensions from the **Available Types** list to the **Selected** list using the arrow (>>,>,<,<<) buttons. For more information on the file types allowed for each media type, see [Available file types for Twitter media types](#) on page 137.
8. In the **Inbound file types allowed** field, click **Set Types** to configure the file types for inbound messages.
9. In the **Configure File Transfer Types** dialog box, select the required file extensions from the **Available Types** list to the **Selected** list using the arrow (>>,>,<,<<) buttons.
10. In the **Name Parsing Settings** section, in **Twitter name parsing type**, select the display name combination for the customer as required from the options available.

 Note:

The description of the selected option is displayed in the text box next to the options.

11. Click **Save**.
12. In the **Natively supported Twitter file transfer sizes** section, select the required **Media Type** to set the allowed file sizes.

The following are the Native Media types and the maximum allowed file size in KB:

- gif - 15360
- image - 5120
- video - 15360

13. Click **Edit**.

The **Edit file transfer sizes for <selected> media type** dialog box is displayed.

14. In **Max outbound file size**, the maximum allowed size is entered by default. You can edit this to decrease the size if required.

15. In **Max inbound file size**, the maximum allowed size is entered by default. You can edit this to decrease the size if required.

16. Click **Save**.

Available file types for Twitter media types

Administrators can use this information to select the applicable file types for native WhatsApp media types such as documents, audios, images, stickers, and videos.

Table 3:

Twitter Media Type	Allowed File Type
video	video/3gpp
video	video/mp4
image	image/png
image	image/jpeg
image	image/bmp
gif	image/gif

Configuring Chat for Transfer to Service

Configuring a Transfer to Service Route Point for Chat

About this task

Use this procedure to create a new Transfer to Service Route Point for Chat through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
 - a. In the **Type** field, select `Route Point`.
 - b. In the **Sub Type** field, select `Transfer to Service`.
 - c. In the **Name** field, enter a name for the Route Point.
 - d. Click **Save**.

Creating a Transfer Target service for Chat

About this task

Use this procedure to create a Transfer Target service for Chat through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
 - a. In the **Service Name** field, enter the name of the service.
 - b. Select the **Available for Transfer** check box.
The system automatically selects the **Agent Display** check box.
 - c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
 - d. In the Transfer Routepoints section, in the **Chat** field, select the Route Point that you created for Chat.
 - e. Click **Save**.

Chapter 6: Email administration

Configuring an Outbound SMTP server

About this task

The Outbound SMTP server delivers the Email messages sent from the contact center.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. From the list, select **Outbound SMTP Server**.
6. Enter the details of your Outbound Email server.
7. Click **Save**.

Configuring an Inbound Mail server

About this task

Add an Email server for your contact center to poll multiple Email servers for the Email messages to route to agents. The Inbound Mail server handles Email messages coming into the contact center.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. From the list, select **Inbound Mail Server**.
6. Enter the details of your Inbound Email server.
7. Click **Save**.

Configuring keyword groups

About this task

You must assign at least one keyword to a keyword group before you can save the keyword group. The keyword search in an email message is not case sensitive. For example, if you add the word `John`, the Email Manager also matches `JOHN` and `j ohn`. The **Keyword** field supports the Unicode UTF-8 character set.

You can specify a spelling accuracy in the keyword group. Keyword groups support only asterisks (*) and question marks (?) as wildcard characters. The asterisk (*) represents multiple characters. For example, `t*` specifies a list of all the words that start with `t`. The question mark (?) represents a single character. For example, `p?t` specifies all three letter words that start with `p` and end with `t`.

A keyword does not support the following characters: `+ - ! ( ) { } [ ] ^ " ~ : \ & & | # $ % @ € / > < , . ' ; = % £ & ¬ | ` " ' .`. If you use any of these characters in your keywords, you receive an error message stating that the keyword contains invalid characters.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Keyword Groups**.
4. Perform one of the following steps:
 - Click **New**.
 - Select an existing keyword group and click **Edit**.
5. In the Keyword Group section, perform the following steps:
 - a. In the **Group Name** field, enter a unique name for the keyword group.
 - b. In the **Keyword** field, enter a word or a group of words related to the keyword group.
 - c. Select the **Allow spelling inaccuracies** check box to allow close misspellings of the word.

The system displays the following levels of accuracy:

- Low (greater than 70% accuracy)
 - Medium (greater than 80% accuracy)
 - High (greater than 90% accuracy)
6. Select the required level of accuracy.
 7. Click **>**.

The system moves the keyword or expression to the Keywords in Group section.

8. Click **Save**.

Configuring an automatic response

About this task

Use this procedure to create automatic responses. You can also add images for auto-responses.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Perform the following steps:
 - a. Click **New Response**.
 - b. In **Name**, enter a name for the response.
 - c. In **Type**, select **Auto-Response - Regular** or **Auto-Response - Out of Hours**.
 - d. In **Subject**, enter the appropriate subject.
 - e. In **Body**, enter the appropriate text.
 - f. To add an image for auto-response, click the **Image** () icon and select the required image.
 - g. Click **Save**.

Configuring an automatic suggestion response

About this task

Use this procedure to configure an automatic suggestion response.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Perform the following steps:
 - a. Click **New Response**.
 - b. In the **Name** field, enter a name for the response.
 - c. In the **Type** field, select **Auto-Suggest**.
 - d. In the **Subject** field, enter the appropriate subject.
 - e. In the **Body** field, enter the appropriate text.

- f. Click **Save**.

Configuring Basic authentication settings

About this task

Basic authentication such as username and passwords required by Oceana Mailboxes (Mailstores) to access the mail server, send, and retrieve emails.

Use this procedure to configure the basic authentication settings.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Authentication**.
4. In the Mailbox Authentication Settings screen, click **Add**.
5. In the **Name** field, enter a name for the authentication setting.
6. In the **Authentication Type** field, select **Basic**.

Note:

Basic option is selected by default.

7. In the **Basic Authentication Credentials** section, in the **Password** field, enter a password for the authentication credentials.
8. In the **Confirm Password** field, re-enter the password provided in the **Password** field.
9. Click **Save**.

The basic authentication credentials are set.

Configuring Email inboxes

About this task

Create a recipient Email box to ensure that at least one Email inbox is configured for your Contact Center. You must configure one recipient to commission the server.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses**.

4. Click **New**.
5. In the **Mailbox Type** field, select from:
 - **Mail Store** - Select this option to configure the following:
 - A distribution group address for the **From** header of each email that goes out from the Avaya Oceana® mailbox.
 - A specific percentage of outbound reply emails.
 - Outgoing emails to be approved prior to being sent out.

For details on configuring the Mail Store, see [Mail Store field descriptions](#) on page 143.
 - **Alias** - Select this option to create another name for the recipient email box. For details on configuring Alias, see [Alias field descriptions](#) on page 145.
 - **Distribution group** - Select this option to create a new email distribution list. For details on configuring Distribution group, see [Distribution group field descriptions](#) on page 146.
6. Enter the required information.
7. Click **Save**.

Mail Store field descriptions

Use the Mail Store option to:

- Configure a distribution group address for the **From** header of each email that goes out from the Avaya Oceana® mailbox. All outgoing emails from the agents are configured with the email address of the distribution group, instead of the actual mailbox from which the emails are sent.
- Configure the outgoing emails to be approved prior to being sent out to a customer.
- Configure a specific percentage of outbound reply emails from agents to go through an approval process.

Name	Description
Mailbox	Local-part (username) of mailbox email address.
Domain	Domain name of the mailbox email address.
Display Name	The name that appear in the Email From address.
Inbound Server	The host name of configured Inbound Server along with the respective security protocol.
Inbound Mail Threshold	The maximum number of Email messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox.
Outbound (SMTP) Server	The host name of configured Outbound Server.

Table continues...

Name	Description
% of mail to send to approval	The specific percentage of outbound reply emails from agents can be set to go through an approval process.
Approval for Fowards	To enable email approval process for email forwards, that is, if incoming emails are targeted for approval for individual mail box.
Credentials	Credentials to be used to access chosen mail servers.
Rule Group	The name of the Rule Group to be applied on the email messages received from the current Mail Store.
Agent Initiated Email	Sets the mailbox to allow an agent to initiate an Ad-Hoc email (emails that are initiated by agents without an incoming email from customer).  Note: When the Agent Initiated Email option is selected for a mailbox, any email-enabled Avaya Oceana® agent can send out an email from that mailbox. The outbound email comes from that mailbox, and not from the agent.
Allow Multireply	To enable the multireply feature for individual mail boxes.
Send as group	Sets the distribution group address for each outgoing email sent from the current mailbox. The text box next to the check box displays the email address of the distribution group that is used for outgoing emails. All the outbound emails sent from this Mail Store have a group address as the sender address.  Note: The Send as group option is available for authorized SMTP access and when the mailbox is a member of the Avaya Oceana® distribution group.

Table continues...

Name	Description
Shared	Select this option if the mailbox on the mail server is configured as shared. .  Note: If a mail server is configured as a shared server, all the configuration is done on mail server side, you must only provide access information (shared username in addition to mailbox info).
Username	The shared user name of the account used to connect to the mailbox.

Alias field descriptions

Use Alias option to create another name for the recipient email box.

For example, the mailbox `general@magscripts.com` can have the aliases `carz@magsubscriptions.com` and `planez@magsubscriptions.com`. Email messages addressed to either alias are forwarded to the `general@magscripts.com` mailbox. The Email Service routes the email messages according to the rules from the Rule Group assigned to the alias.

Field Name	Description
Mailbox	Local-part (username) of mailbox email address.
Domain	Domain name of the mailbox email address.
Display Name	The name that appear in the Email From address.
Rule Group	The name of the Rule Group to be applied on the email messages received from the current Mail Store.
Outbound (SMTP) Server	The host name of configured Outbound Server.
Username	The user name used to access the mailbox on mail server.
Password	The password for the mailbox.  Important: When you change a password on the Email server, you must update the password in this field.
Confirm Password	Confirmation of the password entered for the mailbox in Password field.

Table continues...

Field Name	Description
Agent Initiated Email	Sets the mailbox to allow an agent to initiate an Ad-Hoc email (emails that are initiated by agents without an incoming email from customer).  Note: When the Agent Initiated Email option is selected for a mailbox, any email-enabled Avaya Oceana[®] agent can send out an email from that mailbox. The outbound email comes from that mailbox, and not from the agent.
Credentials	The credential used to access the mailbox on the MS Graph mail server.  Note: OAuth2.0 credentials are available for the MS Graph SMTP server only and cannot be used with other SMTP servers.

Distribution group field descriptions

Use the Distribution group option to create a new email distribution list.

Name	Description
Mailbox	The group email address.
Available	Displays the list of members available.
Configured	Enables you to assign members to the distribution group by selecting from the Available list to the Configured list.  Note: The Distribution group type is used only if you want to use Send as group feature.

Outbound email approval

Use the following process flow to understand and configure the outbound email approval process.

No.	Tasks	Description	✓
1	Outbound email approval process overview.	See Outbound email approval process on page 147.	
2	Configure rejection codes.	See Configuring rejection codes on page 72.	

Table continues...

No.	Tasks	Description	✓
3	Configure approval attributes.	See Illustration of the approval attribute configuration for outbound emails on page 148.	
4	Configure inbound rule for assigning the approval attributes.	See Configuring rule groups on page 154.	
5	Configure percentage of mails routed for approval.	See Configuring percentage of mails going for approval on page 147.	
6	Email approval ratios.	See Email approval ratios on page 148	
7	Approval process of an outgoing email reply from the agent to the customer.	See “Approving outbound emails from agents to the customer” in the <i>Using Avaya Workspaces for Avaya Oceana®</i> document.	

Outbound email approval process

In Avaya Oceana®, you can configure emails for approval before sending them to a customer. For example, an individual or a group of designated approvers can approve emails. Approving emails is part of quality assurance to ensure the agents respond appropriately to customer queries.

Agents can send approved emails to the customer, which appear in the customer journey. Unapproved emails do not show up in the customer journey, and administrators can use the audit trail to see these emails.

You can use Avaya Analytics™ to view real-time and historical reporting on approving or rejecting outbound emails.

Configuring percentage of mails going for approval

About this task

A specific percentage of outbound reply emails from agents can be set to go through an approval process. You can configure the approval percentage at a mailbox level or at a rule group level.

Use the following procedure to enable outbound reply emails approval for a mailbox, and set a percentage of mails to be sent for approval.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click the mailbox for enabling approval.

5. In the **% of mail to send to approval:** field, set the value for percentage of mails to be marked for approval.
6. Click **Save**.

 Important:

The configured inbox approval ratio may not directly correspond to the percentage of email being sent through the approval process as the approval ratio converge to the percentage set based on sufficient traffic through the system. All the email rules applied to email for the inbox must also be configured with the approval attributes, else some emails do not get sent for approval. See [Configuring rule groups](#) on page 154.

An email approval ratio is also set on inbound email rules, and if the rule approval ratio and the inbox approval ratio differ, then the higher value between the two values is the effective value. For more information on email approval ratios, see [Email approval ratios](#) on page 148.

Email approval ratios

An email approval ratio can be set on both the mail inbox and the mail's inbound mail rules. This introduces possible ambiguity on which approval ratio is the effective one. The higher of the two values is always taken as the effective approval ratio. For example, if a mail arrives through a mailbox where the approval ratio is 50%, and on a rule where the approval ratio is 0%, then the effective email approval ratio for that mail is 50%. That is 50% of mail arriving through that mailbox and rule is marked for approval.

Examples:

Email arriving on Inbox	Inbox approval ratio	Rule approval ratio	Effective approval ratio
A	100%	0%	100% 100% of such email are subject to approval.
B	10%	50%	50%
C	0%	90%	90%

Illustration of the approval attribute configuration for outbound emails

This section describes an example approval attribute configuration for a service.

Consider the following Work Assignment service **EnglishSalesEmail**.

Service Name	Service Attributes
EnglishSalesEmail	<i>Language.English</i> <i>Department.Sales</i> <i>Channel.Email</i>

To send an email associated with this service through the approval service, there is flexibility to configure the system. One approach is to create a new approval attribute, to represent the service.

In Avaya Control Manager, you must create a new Approval attribute for this service with a descriptive name, *Approval.EnglishSalesApproval*. Assign *Approval.EnglishSalesApproval* as the only approval attribute in OCP Administration. See [Configuring rule groups](#) on page 154.

Assign *Approval.EnglishSalesApproval* attribute to the agents or supervisors to be assigned as approvers, for the emails routed through this service.

Handling email contact with Send as Group option enabled

With the **Send as group** option enabled, administrators can configure distribution group address. This address is set to the **From** header of each email that goes out from the Avaya Oceana® mailbox. All outgoing emails from the agents are configured with the email address of the distribution group, instead of the actual mailbox from which the emails are sent.

The EmailService sends emails from an actual mailbox configured. However, EmailService checks if the **Send as group** option is configured for that mailbox. If the **Send as group** option is enabled, the distribution group address is set as the From address for the email.

This is applicable for all the outgoing email, including Ad-hoc emails, forwarded emails, and auto-replies sent from the mailbox for which the **Send as group** is configured.

* Note:

The **Send as group** feature is supported only for Microsoft Office365 email provider.

Example

- A customer sends a new email from customer@mydomain.com to OceanaGroup@avaya.com, which is an email distribution group.
Distribution group address is configured in the mail server and Avaya Oceana® as Distribution group mailbox type.
- Email server receives a new email and places in each mailbox in the distribution group.
- Avaya Oceana® polls a new email from OceanaMailbox@avaya.com mailbox and passes it to the agent.
OceanaMailbox@avaya.com mailbox is configured in Avaya Oceana® for email polling.
- Agent writes a response to customer@mydomain.com.
- Avaya Oceana® EmailService receives a new outbound email to process, checks database configuration for mailbox OceanaMailbox@avaya.com, and sets an appropriate sender address, OceanaGroup@avaya.com, for a new email message.

- The customer receives a new email from OceanaGroup@avaya.com email address.

Checklist for configuring email contact with Send as group

You can use the following checklist for email inbox configurations for Send as group feature:

No.	Task	Description	Notes	✓
1	Configure the distribution list on the Office365 side.	See Configuring Office365 distribution list on page 150.		
2	Configure the throttling policy.	See Configuring throttling policy on page 150.		
3	Enable the Send as group option while configuring the email inbox.	See Configuring Send as group feature for Avaya Oceana mailbox on page 151.		
4	Create a new mailbox of type distribution group.	See Configuring Avaya Oceana distribution group on page 152.		

Configuring Office365 distribution list

About this task

You must use Microsoft Office365 to add Avaya Oceana® mailbox as a member with the permission to send as a group. Avaya Oceana® uses the mailbox configured to poll new emails. You must configure Avaya Oceana® mailbox to have permissions to send as distribution group on Office365 side.

Exchange Admin Center (EAC) configurations

- For information about creating and managing distribution groups in EAC, see [Exchange documentation](#).
- For information about how to grant **Send As** permissions in EAC, see [Exchange documentation](#).

Configuring throttling policy

About this task

You must update the throttling policy on Office365 Exchange side for mailboxes that are configured for **Send As Group** feature.

Exchange PowerShell is used to run all commands for updating the throttling policy.

Procedure

1. In the Exchange PowerShell, run the **New-ThrottlingPolicy** <policy name> command to create a new policy.

2. Run the **Set-ThrottlingPolicy** `<policy name> -RCAMaxConcurrency <limit> -RcaMaxBurst <limit> -RcaRechargeRate <limit> -RcaCutoffBalance <limit> -IsServiceAccount:$true` command to set policy parameters based on mailbox usage.
3. Run the **Set-Mailbox** `<service account> -ThrottlingPolicy <policy name>` command to assign the policy to Avaya Oceana® command mailboxes.

`<policy name>` is the name of the policy to create, `<limit>` is the value for a particular rate limitation, and `<service account>` is the mailbox address configured with **Send As Group** feature.

 Note:

For the actual rate limit values, Office365 Exchange administrator must ensure that rate limits are correct and sufficient per mailbox.

Configuring Send as group feature for Avaya Oceana® mailbox

About this task

If you want to set a configured distribution group address to the **From** header of each email that goes out from the Avaya Oceana® mailbox, then you have to enable **Send as group** option. All outgoing emails from the agents are configured with the email address of the distribution group, instead of the actual mailbox from which the emails are sent.

Before you begin

Before you enable **Send as group** and configure email inbox; you must add Avaya Oceana® mailbox as a member with the permission to send as a group in the Exchange admin center.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.
5. In the **Mailbox Type** field, select `Mail Store`.
6. In the Mailbox Details section, perform the following steps:
 - a. In the **Mailbox** field, enter the SMTP mailbox name.
 - b. In the **Domain** field, enter the domain for your Email server.
 - c. In the **Display Name** field, enter the name to appear in the Email From address.

 Note:

Avaya Oceana® or EmailService logs in to a specific mailbox on the configured mail store by using `username@domain` instead of `username`.

7. In the Password section, perform the following steps:

- a. In the **Password** field, enter the password for the mailbox.

 Important:

When you change a password on the Email server, you must update the password in this field.

- b. In the **Confirm Password** field, re-enter the password for the mailbox.

8. In the Servers section, perform the following steps:

- a. In the **Inbound Server** field, select the hostname of your IMAP server along with the respective security protocols.
- b. In the **Inbound Mail Threshold** field, enter the maximum number of Email messages to be retrieved from the mailbox at every scan interval.

You can enter a different value for this variable for each mailbox.

- c. In the **Outbound (SMTP) Server** field, select the host name of your SMTP server.

9. In the **Rule Group** field, select the name of the Rule Group to assign to the recipient mailbox.

10. Select the **Agent Initiated Email** check box.

11. Select the **Send as group** check box to set the distribution group address for each outgoing email sent from the current mailbox.

The text box next to the check box displays the email address of the distribution group that is used for outgoing emails. All the outbound emails sent from this Mail Store have a group address as the sender address.

 Note:

The **Send as group** option is available for authorized SMTP access and when the mailbox is a member of the Avaya Oceana® distribution group.

12. **(Optional)** If the mailbox is shared, do the following:

- a. Select the **Shared** check box.
- b. In the **Username** field, enter the user name of the account used to connect to the mailbox.

13. Click **Save**.

Configuring Avaya Oceana® distribution group

About this task

You must create a new mailbox of the type **Distribution group**, which represents the Microsoft Office365 distribution list. You have to add a group email address and previously created mailbox to this distribution group.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.
5. In the **Mailbox Type** field, select `Distribution group`.

In the **Distribution group** section, do the following:

- a. In the **Mailbox** field, enter the group email address.
- b. To assign members to the distribution group, select from the **Available** list to the **Configured** list.

 Note:

The **Distribution group** type is to use **Send as group** feature.

6. Click **Save**.

Disabling polling on a mailbox

About this task

The administrator can disable polling on an individual mailbox or multiple mailboxes for a maintenance window.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Select a mailbox to disable and click **Edit > Disable**.
5. **(Optional)** To disable multiple mailboxes, click **Disable All**.

When you click **Disable All**, it takes a maximum of five minutes for Avaya Oceana® to apply the changes and disable email polling. Similarly, when you click **Enable All**, it also takes a maximum of five minutes for Avaya Oceana® to apply the changes and enable email polling.

6. Click **Save**.

Configuring rule groups

About this task

Use this procedure to create or change a rule to route your email contacts.

You can create a rule with one or more of the following routing options:

- Determine when the email was received (Office Hours)
- Determine who sent the email (Sender Groups)
- Determine the specific characters, words, or phrases in the email (Keyword Groups)

Rules can send an automatic response to a customer. Therefore no agent interaction is required.

A rule group contains a default rule for routing an email contact to a specific route point with a priority.

Before you begin

Configure an automatic response and an automatic suggestion response.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Rule Groups**.
4. Perform one of the following steps:
 - Click **New**.
 - Select an existing Rule Group and click **Edit**.
5. In the Rules section, perform one of the following steps:
 - Click the plus sign (+) button.
 - Select an existing rule.
6. In the Current Search Criteria section, click **New**.
7. To add search criteria based on the keyword match, perform the following steps:
 - a. In the Add New Criterion section, select **Keyword Match** and click **Go**.
 - b. In the Keyword Groups section, select the first keyword group and click > in the first row.
 - c. In the Keyword Groups section, select the second keyword group and click > in the second row.
 - d. Select the **AND** or **AND NOT** options to associate the second keyword group with the first keyword group.
 - e. In the Keyword Groups section, select the third keyword group and click > in the third row.

- f. Select the **AND** or **AND NOT** options to associate the third keyword group with the first and second keyword groups.
- g. Click **OK**.

 Note:

The total keyword match weightage must add up to 100 percent.

8. To add search criteria based on the sender group, perform the following steps:
 - a. In the Add New Criterion section, select **Sender Group** and click **Go**.
 - b. In the Sender Groups section, select the required sender group and click **>**.
 - c. Click **OK**.

 Note:

The total keyword match weightage must add up to 100 percent.

9. In the Current Search Criteria Summary section, click the rule name to view the details of each criteria that you configure.
10. Click **Next**.
11. In the Available Auto-Responses section, select a configured automatic response for the rule and click **>**.
12. In the Available Auto-Suggests section, select a configured automatic suggestion for the rule and click **>**.

To remove an automatic suggestion for the rule, click **<**.

13. Click **Next**.
14. Perform the following steps based on your requirement:
 - Select the **Will use Office Hours** check box to apply the Office Hours to the email message.
 - Select the **Respond to original email** check box and select the appropriate recipient Email inbox.
 - Select the **Will Close Contact** check box to close the contact.
 - Select the **Call Open Interface web service** check box and select the Web service associated with the rule.
15. Keep the **WorkFlow** field blank.
16. **(Optional)** To configure different Engagement Designer workflows to meet your specific requirements, perform the following steps:
 - a. In the Engagement Designer Admin Console, select the Event Catalog tab.
 - b. Select the required workflow and click **Edit**.
 - c. In the Event Catalog dialog box, click **Rules Editor**.

- d. In the Edit Rule dialog box, set the criteria for the required workflow based on the WorkflowType value.

 Note:

You must also create a default rule to handle all cases that do not meet the criteria.

17. Click **Next**.

18. In the General Settings section, perform the following steps:

- a. In the **Name** field, enter a name for the rule.
- b. In the **Priority** field, select the priority to assign to the contact.
- c. In the **Route point** field, select the Route Point name to apply for the rule. You must select the Email Route Point that you configured using Avaya Control Manager.

 Important:

You must configure a Route Point when creating rule groups.

- d. In the **CS Lease Time** field, enter the appropriate value.
- e. In the **Disclaimer** field, enter the appropriate text.
- f. In the **Profanity Profile** field, select the required profanity profile.

 Note:

The profanity validation is not applicable if no profile is set. You can also unset profanity profile from Rule by choosing the empty option in the drop-down list of profanity profiles.

19. In the content pane, select the attributes.

For example, Language.English.

20. In the Approval Settings section, perform the following steps:

- a. In the **Priority** field, select the priority to assign to the contact.
- b. In the **% of mail to send to approval:** field, set the value for the percentage of emails to be sent through the approval process.

21. In the content pane, select the Approval attributes for this rule.

If the approval ratio, that is, the percentage of emails to be marked for approval is greater than zero, you must select at least one approval attribute from the Approval category to be saved on the rule.

For example, Approval.Email.

22. Click **Save**.

The configured inbox approval ratio may not directly correspond to the percentage of the email being sent through the approval process as the approval ratio converges to the percentage set based on sufficient traffic through the system.

An email approval ratio is also set on the Inbox in the **Recipient Addresses** configuration section. If the rule approval ratio and the inbox approval ratio differ, the higher value between the two is the effective value. For more information about email approval ratios, see [Email approval ratios](#) on page 148.

Configuring system default rule

About this task

Administrators can configure default behavior if the contacts do not match any rules. When you create a recipient mailbox, the system default rule is copied as the last regular rule into the list of rules for the recipient mailbox.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **System Rules**.
4. In the System Default Rule section, in the **Route point** field, select the route point name to apply for the rule.

You must select the Email Route Point that you configured using Avaya Control Manager.

5. To change the automatic response settings, in the **Auto-Responses** list, select the required response.

An automatic response is a message sent to a customer without an agent's interaction.

6. In the **Priority** list, select the priority for the contact.
7. In the right pane, select the attributes.

For example, Language.English.

If you cannot close an email, you can route it to the agent attribute set that is configured in the **Edit Attributes** section.

8. Click **Save**.

Configuring system delivery failure rule

About this task

You can configure system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent. When you create a recipient mailbox, the

system delivery failure rule is copied as the first regular rule into the list of rules for the recipient mailbox.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **System Rules**.
4. In **System Delivery Failure Rule** section, in the **Route point** field, select a route point name to apply for the rule.

You must select the Email Route Point that you configured using Avaya Control Manager.

5. To change the keyword group, in the **Keyword Group** list, select the keyword that you can search in an email message.
6. In the **Priority** list, select the priority for the contact.
7. In the right pane, select the attributes.

For example, Language.English.

If you cannot close an email, you can route it to agent attribute set that is configured in the **Edit Attributes** section.

8. Select the **Will close contact** check box to have the rule to close the contact.
9. Click **Save**.

Configuring email settings

About this task

You can configure email settings for email messages entering your mailboxes for:

- how frequently you scan the email server for new messages.
- the location in which attachments are stored.
- automatic numbering of email messages.
- text search result for the keywords used for rules.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **General Settings**.
4. In the **Message Properties** section, do the following:
 - In the **AutoNumber outgoing E-mail** field, select the **Customer ID** check box or **Contact ID** check box or both.

Select the check box to number the email message automatically with either the customer ID, the contact ID, or both. The number appears in the subject of the message for identification. You can optionally add customer ID or contact ID, or both to the outgoing emails. This helps customers to track emails.

- Select the **Include E-mail body in keyword search** check box to enable a keyword search in the body of the email message.
 - In the **Search first characters** field, type the number of characters in the content of the body of the email message that you search for keywords.
5. In the **Attachment** section, in the **Maximum outbound attachment size** field, type the size of the email. This indicates the maximum size of outbound email allowed in Avaya Oceana®, including the email attachments.
 6. In the **Mailbox** section, do the following:
 - a. In the **Scan Interval** field, type the time in minutes. This indicates the interval at which the mailbox scans for new incoming email messages from the email servers.
 - b. In the **Max active Emails** field, type the number of active emails.

Active emails are the maximum number of emails in the mailbox that are not closed. After the mailbox reaches this limit, you cannot read any email messages from the mail servers until the current number of emails drop below this limit. Avaya Oceana® supports up to 25000 active emails.

 Important:

- To support 25000 emails in queue, you must increase the **Platform Space Container Heap Size (MB)** attribute value on the Common Cluster to 600.
- To support a maximum of 25000 active emails, you must also configure specific ContextStoreManager attributes.

For more information on queued emails, see the note on Queued emails in the *Capacity specifications* topic of *Deploying Avaya Oceana®*.

7. Click **Save**.

Configuring holidays

Before you begin

- Identify the closed days of the contact center.

About this task

You can configure the days and times that your contact center is open for holidays.

Procedure

1. Start Omnichannel Administration utility.

2. In the navigation pane, click **E-mail**.
3. Click **Office hours**.
4. In **Template** section, type the name of a calendar to configure.
5. In the holiday box, under **Name**, type the name of a public holiday.
6. Select the **Holiday Date** for the holiday and specify the time for the holiday. You can choose from **All Day** or a specify **Start time** and **End time**.
7. Click **Save**.

Configuring office hours

Before you begin

- Know the office hours of the contact center.

About this task

You can configure the days and hours that your contact center is open each week.

It is important configuring the office hours to determine accurate queued time for contacts that can have a delayed response such as email. For example, if a contact is received on Friday and processed on Monday and you configure the office hours to show the contact center is closed over the weekend, the queue time for the contact only includes the time the contact center is open.

You can use the office hour calendar in email rules. The email rules can send a specific response if the office is closed.

The office hour calendar uses sliders to indicate closed times for the contact center. The Start Closed Period slider is a blue triangle (▲). The End Closed Period slider is a red triangle (▼). Each closed period is shown in red with a Start Closed Period and End Closed Period at the beginning and end of the closed office hours.

Note:

You can configure office hours only in the current local time zone of the Omnichannel Database server and not in the UTC time zone.

Procedure

1. Start Omnichannel Administration utility.
2. In the navigation pane, click **E-mail**.
3. Click **Office hours**.
4. In **Template** section, type the name of a calendar to configure.
5. Configure holidays for the office hour template.
6. Beside a day of the week, click .

7. For the day you select, move the Start Closed Period  and End Closed Period  sliders to define a period when the contact center is closed.
Open hours for the contact center are shown by the green bars. Closed hours are in red.
8. Repeat step 6 and step 7 for every day of the week.
9. Click **Save**.

Applying office hours

About this task

You can apply a designated calendar showing open and closed hours of the contact center. This calendar is used in the settings of email rule. You can respond to email messages by selecting the office hours calendar to send automatic messages to incoming email contacts. You can select which rule group to apply the global office hours to.

Note:

You can configure office hours only in the current local time zone of the Omnichannel Database server and not in the UTC time zone.

Before you begin

Create a calendar template with office hours or holidays.

Procedure

1. Start Omnichannel Administration utility.
2. In the navigation pane, click **E-mail**.
3. Click **Rule Groups**.
4. In the **General Settings** section, select the **Will use Office Hours** check box to automatically send an out-of-office type message to the customer when the contact center is closed.
5. In the **Out of hours Auto Response** field, select the automatic response for the out of office hours notice.
6. In the **Calendar** field, select the calendar you want to use to determine the business hours for your contact center.
7. Click **Save**.

Configuring Email Open Interfaces

Before you begin

- Configure a custom Web service that conforms to the Web Service Description Language (WSDL) standards.
- Configure the rule associated with the Web service from the Rule Groups section in the Omnichannel Administration Utility.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Open Interfaces**.
4. Click **New**.
5. In **WSDL URL** field, enter the URL of the WSDL.
6. Click **Discover**.

The system sends a query to the WSDL URL and lists the methods retrieved from the URL in the Open Interfaces method discovery dialog box.

7. In the Open Interfaces method discovery dialog box, select the methods that you want to add to the Web service and click **Add**.

To add all methods, you can click **Add all**.

8. In the Methods section, click **New** to create a new method.

To edit an existing method, you can select the method and click **Edit**.

9. In **Method**, enter a name for the method.
10. In **Display Name**, enter the name that you want to display for the method.

Note:

The display name must be unique across all Web services.

11. In the Input Parameters section, do the following:
 - a. Select the parameter that you want to move to the list of parameters that must be passed to the Web service.
 - b. Click **>**.

The Input parameter list is a static list of the fields from the email.

To remove a parameter from the list of parameters, you can select the parameter and click **<**.

12. In the Output Parameters section, do the following:
 - a. Select the parameter that you want to move to the list of parameters that must be returned from the Web service.

- b. Click **>**.

Output parameters replace or complement the original rule output. For example, the Web service can determine a different skillset or priority for the email, manipulate the body of the email, or return a screen pop or knowledge base links.

To remove a parameter from the list of parameters, you can select the parameter and click **<**.

- 13. Click **Save**.
- 14. Click **Save**.

Creating Sender Groups

About this task

Sender groups are used to match and apply a rule to an email sent to and received from particular email addresses. For example, creating blocklists.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail > Sender Groups**.
3. Click **New**.
4. In the Sender Group section, perform the following steps:

- a. In **Name**, enter a name.

For example, `Blocklist Group`.

- b. In **E-mail Address**, enter the email address or domain to create a sender group for and click **Add Freeform**.

You can repeat this step to add more email addresses or domains that you want to the group.

 Note:

Sender groups support asterisks (*) as wildcard characters when they are placed in the email address.

- c. Click **Save**.

You can now create required rules for the sender groups from the **Rule Groups** option.

Configuring a Chat History Header prepared response

About this task

Use this procedure to create chat history header prepared responses.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Perform the following steps to configure a Chat History Header prepared response:
 - a. Click **New Response**.
 - b. In **Name**, enter a name for the response.
 - c. In **Type**, click **Chat History Header**.
 - d. In **Subject**, enter the appropriate subject.
 - e. In **Body**, enter the appropriate text.
 - f. Click **Save**.

Enabling the backup for inbound emails

About this task

When Avaya Oceana® processes an email from a mailbox, the email is deleted from the mail server. Omnichannel Administration Utility provides an option to retain a copy of the email in a new backup folder in the mail server.

Other external business processes can continue to have access to the original email. This option is applicable only for IMAP but not for POP3. Customers must ensure that they manage the size of the backup folder.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **General Settings**.
4. In the content pane, select the **Backup inbound mails in separate mail store folder** check box.
5. Click **Save**.

Configuring email transcripts

About this task

Use this procedure to configure email transcripts.

Procedure

1. Start Omnichannel Administration Utility.
2. In the left navigation pane, click **Transcripts**.
3. Click **Config**.
4. Navigate to the Email Transcript Access section.
5. In **Web Service**, type the complete URL of the filtering service.

For example, `http://127.0.0.1/CustomerFilterMessages-{$version}/rest/filter/transcript/email`. If your service listens on a port other than 80 or 443, include the port number.

6. In **Send Option**, select the `Send` option.
7. Click **Save**.

Configuring regular retry of failed email transcripts

About this task

Use this procedure to configure regular retry of failed email transcripts.

Before you begin

Ensure that you enable email transcripts and configure the email transcript web service.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Transcripts**.
3. Click **Config**.
4. **(Optional)** In **Number of days to retry**, set the number of days the EmailService retries to send a transcript to the transcript service.

After reaching this limit, the transcript is set to *Permanently Failed*, and the EmailService stops the retry. This value applies to email and messaging.

5. Navigate to the **Transcript Resend Schedule** section.
6. In **Email retry time**, select the start and end times.

The start and end time in the **Messaging retry time** field must be different from that in the **Email retry time** field. Any change in the start or end time takes 15 minutes to get updated.

7. Click **Save**.

Configuring Ad hoc email rules

Adding Ad hoc email rules

About this task

When an agent sends Ad hoc emails, depending on the Ad hoc email rule, the emails are first sent to the approver. After the Ad hoc emails are approved, they are routed to their respective recipients. If an Ad hoc email is rejected, it is routed back to the agent who created it.

Using this procedure, you can configure rules for sending the Ad hoc emails for approval and routing approved and rejected Ad hoc emails.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Select **Outbound Rules > Ad hoc Rules**.
4. Click **Add**.
5. Enter **Name of the rule**.

The next parameters on this page are used for fallback case, when rejected Ad hoc email was not able to be routed to original Contact Center user for rework.

6. Select **Priority** of the Ad hoc rule.

The Priority is used for routing of rejected Ad hoc email to available Contact Center users, when original Ad hoc sender was not available.

7. Select **Routepoint**.

Routepoint is used for routing of rejected Ad hoc email to available Contact Center users, when original Ad hoc sender was not available.

8. Enter **CS Lease Time**.

This field displays **Context Store lease time**. It indicates how long the contacts are stored in CS space. After expiry, Avaya Oceana® retrieves these contacts from the CS EDM if this data is needed.

9. Select **Fallback attributes** such as Language and Department.

Configure Fallback attributes for routing the rejected emails to an agent, when the agent who created the Ad hoc email is not available.

10. Click **Next**.

11. Configure the following Approval settings:

a. Select **Priority** of the approval rule.

The approval Priority is used for routing of Ad hoc email for approval.

b. Select **% of mail to send to approval**.

If you select this field value as more than 1, you must select at least one Approval attribute. If 0% is selected, an Ad hoc email is not send for approval.

c. Select the required **Approval attributes** from the right panel.

Configure Approval attributes to route the approved Ad hoc emails.

12. Click **Save**.

Next steps

Assign Ad hoc rule to email box.

Assigning Ad hoc email rule to mailbox

About this task

Use this procedure to assign Ad hoc email rules to a mailbox.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Click **Recipient Addresses** and select the mailbox to configure the Ad hoc email rule.
4. Under the Email Approval section in the mailbox, select an **Ad hoc Rule**.

Note:

If no Ad hoc Rule is assigned on mailbox, Ad hoc emails sent from that mailbox will not be sent for approval.

5. Click **Save**.

The Ad hoc email rule is applied to the mailbox.

Editing Ad hoc email rules

About this task

Use this procedure to edit the existing Ad hoc email rules.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Select **Outbound Rules > Ad hoc Rules**.
The list of existing Ad hoc email rules is displayed.
4. Select an Ad hoc email rule and click **Edit**.
5. Update the configured attributes and field values as required.
6. Click **Save**.

Deleting Ad hoc email rules

About this task

Use this procedure to delete an Ad hoc email rule that is not required.

Note:

The default Ad hoc email rule or rule assigned to a mailbox cannot be deleted.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **E-mail**.
3. Select **Outbound Rules > Ad hoc Rules**.
The list of existing Ad hoc email rules is displayed.
4. Select the Ad hoc email rule not required and click **Delete**.

Configuring Email for Transfer to Service

Configuring a Transfer to Service Route Point for Email

About this task

Use this procedure to create a new Transfer to Service Route Point for Email through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.

2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
 - a. In the **Type** field, select `Route Point`.
 - b. In the **Sub Type** field, select `Transfer to Service`.
 - c. In the **Name** field, enter a name for the Route Point.
 - d. Click **Save**.

Creating a Transfer Target service for Email

About this task

Use this procedure to create a Transfer Target service for Email through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
 - a. In the **Service Name** field, enter the name of the service.
 - b. Select the **Available for Transfer** check box.
The system automatically selects the **Agent Display** check box.
 - c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
 - d. In the Transfer Route points section, in the **Email** field, select the Route Point that you created for Email.
 - e. Click **Save**.

Microsoft Graph set up process

Use the following process flow for Microsoft Graph set up.

No.	Tasks	Description	✓
1	Install Office 365 certificates on Avaya Aura® System Manager.	See Installing Office 365 certificates on Avaya Aura System Manager on page 171.	
2	Register your application on Microsoft Azure portal.	To authenticate with the Microsoft identity platform endpoint, you must register your application on the Microsoft Azure application registration portal. For detailed steps, see Register your app .	
3	Configure Certificates and Secrets.	See step 5a and 5b.	
4	Configure API permissions.	For your application to access data in Microsoft Graph, you must configure the application permissions and the global administrator must approve the permissions. The pre-configured permissions are in access token authorization information. They are roles or actions that the application is allowed to perform at the API.	
5	Configure credentials.	To be identified in Microsoft authentication service, you must configure the client secret or the client certificate.  Note: For a higher level of security, you must use a client certificate instead of a client secret, as a credential.	
	5a. Configure Microsoft Graph authentication with client secret in Omnichannel Administration Utility.	See Configuring Microsoft Graph authentication with client secret in Omnichannel Administration Utility on page 172.	

Table continues...

No.	Tasks	Description	✓
	5b. Configure Microsoft Graph authentication with client certificate in Omnichannel Administration Utility.	Key store must be in PKCS standard (.p12), with one X.509 certificate and its corresponding RSA private key with length 2048 bits. The entries are as follows: • Entry Name - privatekey • Algorithm - RSA • Key Size - 2048 • Key store password - notasecret • Private key password - notasecret Upload the generated certificate on the application page, in Microsoft Azure portal, in the Certificates and Secrets area. See step 3. See Configuring Microsoft Graph authentication with client certificate in Omnichannel Administration Utility on page 172.	
6	Configure the inbox for Microsoft Office 365.	See Configuring inbox for Microsoft Office 365 on page 173.	

Installing Office 365 certificates on Avaya Aura® System Manager Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements > Avaya Breeze® > Cluster Administration**.
3. Select the cluster for installing certificates.
4. Click the **Certificates Management** drop-down and click **Install Trust Certificate (All Avaya Breeze® Instances)**.

The application displays **Install Trusted Certificate** page.

5. To select a file, click **Choose File**.
6. Click **Retrieve Certificate**.
7. In **Certificate Details** area, review the certificate details.
8. Click **Commit**.

Configuring Microsoft Graph authentication with client secret in Omnichannel Administration Utility

Procedure

1. Start Omnichannel Administration Utility.
2. Navigate to **E-mail > Authentication**.
The application displays **Mailboxes Authentication Settings** page.
3. Click **Add**.
4. In the **Name** field, type a name for the attribute.
5. In the **Authentication Type** field, select `OAuth2.0`.
6. In the **OAuth2.0 Grant Type** field, select `Client Credentials`.
7. In the **Grant Type Configuration** area, do the following:

In the **Token URI** field, enter the token URI `https://login.microsoftonline.com/{tenant id}/oauth2/v2.0/token`.

Tenant id must be entered from the application overview page of the Microsoft Azure portal.

For example, `https://login.microsoftonline.com/efed5fa7-d22d-456e-ab23-7c6ee6192dbd/oauth2/v2.0/token`

- a. In the **Client ID** field, type the ID from the application **Overview** section of the Microsoft Azure portal.
 - b. In the **Client Secret** field, enter the secret from the **Certificates and Secrets** section of the Microsoft Azure portal.
 - c. In the **Scopes** field, enter the scope for Microsoft Graph from `https://graph.microsoft.com/.default`.
8. Click **Save**.

Configuring Microsoft Graph authentication with client certificate in Omnichannel Administration Utility

Procedure

1. Start Omnichannel Administration Utility.
2. Navigate to **E-mail > Authentication**.
The application displays **Mailboxes Authentication Settings** page.
3. Click **Add**.
4. In the **Name** field, type a name for the attribute.
5. In the **Authentication Type** field, select `OAuth2.0`.

6. In the **OAuth2.0 Grant Type** field, select `Client Credentials with certificate`.
7. In the **Grant Type Configuration** area, do the following:

In the **Token URI** field, enter the token URI `https://login.microsoftonline.com/{tenant id}/oauth2/v2.0/token`.

Tenant id must be entered from the application overview page of the Microsoft Azure portal.

For example, `https://login.microsoftonline.com/efed5fa7-d22d-456e-ab23-7c6ee6192dbd/oauth2/v2.0/token`

- a. In the **Client ID** field, type the ID from the application **Overview** section of the Microsoft Azure portal.
- b. In the **GUID** field, type the value of the *key/d* from the **Manifest** section of the Microsoft Azure portal.
- c. In the **Scopes** field, enter the scope for Microsoft Graph from `https://graph.microsoft.com/.default`.
- d. In the **Key Store (.p12)** field, click **Load file** to upload the file.



Note:

To avoid errors, you can verify the key in KeyStore explorer <https://keystore-explorer.org/>.

8. Click **Save**.

Configuring inbox for Microsoft Office 365

Procedure

1. Start Omnichannel Administration Utility.
2. Navigate to **E-mail > Recipient Addresses**.
3. Click **New**.
4. In the **Mailbox Type** field, select `Mail Store`.
5. In the **Mailbox Details** area, do the following:
 - a. In the **Mailbox** field, enter a name for the mailbox.
 - b. In the **Domain** field, enter the domain.
 - c. In the **Display Name** field, enter the display name.
6. In the **Servers** area, do the following:
 - a. In the **Inbound Server** field, select `Microsoft Office365 (MS Graph)`.
 - b. In the **Outbound (SMTP) Server** field, select `Microsoft Office365 (MS Graph)`.

7. In the **Authentication** area, in the **Credentials** field, select the certificate.
8. Click **Save**.

Enabling MS Graph logging

About this task

Microsoft Graph writes the debug logs into a file. Perform the following procedure to enable the Microsoft Graph logging attribute.

Procedure

1. Log on to Avaya Aura® System Manager.
2. Navigate to **Elements > Avaya > Configuration > Attributes**.
3. Click the **Service Clusters** tab.
4. In the **Cluster** field, select the required cluster.
5. In the **Service** field, select `EmailService`.
6. Scroll to the **Advanced** group of attributes.
7. Select the check box for **Enable MSGraph Logging** attribute.



Important:

Enable MSGraph Logging attribute is set to false by default. You must select the check box to enable the logging.

8. Click **Commit**.

Chapter 7: SMS administration

Configuring SMS Gateway

About this task

This gateway ties accounts to a snap-in. The snap-in also uses this gateway when querying for account details.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **SMS/Social**.
3. Click **SMS Configuration**.
4. Click **Create**.
5. On the Account tab, perform the following steps:
 - a. In the Create Snapin section, in the **Name** field, enter the same name that you configured for SMS in the **Messaging Snapin Key** attribute of MessagingService or **Snap-in Key** attribute of the OceanaConfiguration service.
 - b. Click **Create**.
 - c. In the **Snapin** field, select the snap-in that you created.
 - d. Enter appropriate values in the remaining fields.

The following table provides a description of each field:

Field	Description
Name	An account name - Sent back to third-party snap-in when they request their gateways.
API ID	An API ID - Sent back to third-party snap-in when they request their gateways.
API URL	An API URL - Sent back to third-party snap-in when they request their gateways.
API Password	An API Password - Sent back to third-party snap-in when they request their gateways.
Extra1	An extra field - Sent back to third-party snap-in when they request their gateways.

Table continues...

Field	Description
Extra2	An extra field - Sent back to third-party snap-in when they request their gateways.
Snapin	The name of the third-party snap-in you want to link it to. Enter the name created in earlier steps.

6. Click **Save**.
7. Select the **Details** tab.
8. Create an entry for the gateway that you just added.
9. Enter appropriate values in the remaining fields.

The following table provides a description of each field:

Field	Description
Phone Number	A unique telephone number - Sent back to third-party snap-in when they request their gateways. The phone number is used later when sending a SMS through the sample vendor application.
Tag	A TAG to send messages with - Currently not used - One Off SMS Scenario.
Workflow	An Engagement Designer workflow - If none is supplied, the default flow is used. Used for routing SMS chats. Keep this field blank. To meet your specific requirements, you can configure a specific Engagement Designer workflow through the Event Catalog tab in the Engagement Designer Admin Console, and specify the name of the workflow in this field. If you configure a specific workflow by defining the workflow type and creating suitable Engagement Designer rules, you must also create a default rule to handle all cases that do not meet the criteria.
Description	A description of what to use the number for - Currently not used - One Off SMS Scenario.
Extra1	An extra field - Sent back to third-party snap-in when they request their gateways.
Gateway Account	The gateway account to link the telephone to.
Route point	Select a Route Point that you configured using Avaya Control Manager. Route Points are used to route SMS chats.  Important: You must select a Route Point when configuring the SMS Gateway.
Priority	The priority from 1 to 100.
Attributes	Routing attributes of the telephone number. Used for routing SMS chats.

10. Review your configuration details.

11. In the Edit Attributes section, select the attributes which you want the incoming SMS messages to be routed.

For example, select `Language.English`.

12. Click **Save**.

Configuring SMS for Transfer to Service

Configuring a Transfer to Service Route Point for SMS

About this task

Use this procedure to create a new Transfer to Service Route Point for SMS through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
 - a. In the **Type** field, select `Route Point`.
 - b. In the **Sub Type** field, select `Transfer to Service`.
 - c. In the **Name** field, enter a name for the Route Point.
 - d. Click **Save**.

Creating a Transfer Target service for SMS

About this task

Use this procedure to create a Transfer Target service for SMS through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.

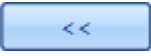
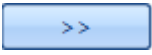
4. To add a Transfer Target service, perform the following steps:
 - a. In the **Service Name** field, enter the name of the service.
 - b. Select the **Available for Transfer** check box.
 The system automatically selects the **Agent Display** check box.
 - c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
 - d. In the Transfer Routepoints section, in the **SMS** field, select the Route Point that you created for SMS.
 - e. Click **Save**.

Creating automatic phrases

About this task

You can create automatic phrases for a phrase group. You can create a list of commonly used phrases for a user group to insert into their instant message or web chat contacts instead of typing individual responses.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Auto Phrases**.
4. In the **Group Phrases** section, select the phrase group.
 Click **Delete** if you can want to remove a group phrase.
5. **(Optional)** You can also create a new group phrase. To create a new phrase group, do the following:
 - a. In the **Create Phrase Group** section, in the **Name** field, type a name for a phrase group.
 - b. Click **Create**.
6. In the **Auto Phrases** section, review and choose an existing phrase from the **Phrases not in group** box and click  to move the phrase to the **Phrases in group** box. Click  to exclude the phrase from the group.

To create a new phrase text, do the following:

- In the **Create Auto Phrase** section, in the **Name** field, type a name for the automatic phrase.
- In the **Phrase Text** field, type the text that is commonly used for the contacts based on the selected group.

- Click **Create**. The newly created phrase appears in the list.

To edit a phrase in the **Phrases not in group** box, do the following:

- Select a phrase from the **Phrases not in group** box.
- Click **Edit**.
- In the **Update Auto Phrase** section, in the **Name** field, type a name for the automatic phrase.
- In the **Phrase Text** field, type the text that is commonly used for the contacts based on the selected group.
- Click **Update**. The updated text appears in the list.

7. In the **Edit Attributes** section, select the required attributes.

For example, select `Language.English`.

8. Click **Save**.

Creating a page push URL

About this task

The agent can choose from a list of Web pages specified for a group assigned to the instant message or web chat contact. You can create the web pages that an agent can view. Ensure that you make the name of the page push URL descriptive to assist the agents. You can configure maximum 50 URLs.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging**.
3. Click **Page Push URLs**.
4. In the **Page Push Group** field, select the page push URL group.
Click **Delete** if you can want to remove the group.
5. **(Optional)** You can also create a new page push URL group. To create a new group, do the following:
 - a. In the **Group Name** field, type a name for a page push URL group.
 - b. Click **Create**.
6. In the **Edit Page Push URL** section, review and choose an existing URL from the **URLs not in group** box and click **Add** to move the URL to the **URLs in group** box. Click **Remove** to exclude the URL from the group.

To create a new URL, do the following:

- In the **Edit Page Push URL** section, in the **URL** field, type the URL for the website to add to the list.
- In the **Description** field, type a description for the page push URL that describes the URL that the agent can push.
- Click **Create**. The newly created URL appears in the list.

To delete a URL from the **URLs not in group** box, do the following:

- Select a URL from the **URLs not in group** box.
- Click **Delete**.

7. In the **Edit Attributes** section, select the required attributes.

For example, select `Language.English`.

8. Click **Save**.

Chapter 8: Social Media administration

Configuring Social Media for Avaya Messaging Automation

About this task

Use this procedure to configure Social Media for Avaya Messaging Automation.

Important:

- Social Media Snap-in is supported with Avaya Oceana® auto-response or Chatbot automation.
- Social Media Snap-in does not support Ava automation. Therefore, you must disable it.
- Social Media Snap-in supports maximum five social gateway accounts.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **SMS/Social**.
3. Click **Social Configuration**.
4. Click **Create**.
5. On the Account tab, do the following:
 - a. In the **Create Snapin** section, in the **Name** field, enter the same name that you configured for Social Media in the **Messaging Snapin Key** attribute of MessagingService or **Snap-in Key** attribute of the OceanaConfiguration service.
You can enter 1 to 100 characters in this field.
 - b. Click **Create**.
 - c. In the **Snapin** field, select the snap-in that you created.
 - d. In the **Name** field, enter the name of the gateway for the snap-in.
Social Media Snap-in can support maximum five incoming social gateway channels.
 - e. In the **Gateway Name** field, enter the name of the gateway.
You can enter up to 50 characters in this field.
 - f. In the **Social Type** field, type `Slate`.

- g. In the **Header Access Key** field, enter the unique access key for this channel.

You can enter up to 50 characters in this field.

- h. In the **Callback URL** field, enter the URL hosted by the gateway.

You can enter 0 to 100 characters in this field.

6. Click **Save**.

7. Select the **Details** tab.

8. On the Details tab, do the following:

- a. Click **Create**.

- b. In the **Social Handle** field, enter the social handle.

You can enter 1 to 100 characters in this field.

For example:

- For Twitter, enter your Twitter handle.

If your Twitter handle is `SocialPage`, you must type `SocialPage` in this field.

- For Facebook, enter the page ID instead of your Facebook handle.

If your Facebook handle is `SocialPage` and the page URL is `https://www.facebook.com/SocialPage-369854850048396/?fref=nf`, you must type `369854850048396` in this field.

- c. Keep the **Workflow** field blank.

To meet your specific requirements, you can configure a specific Engagement Designer workflow through the Event Catalog tab in the Engagement Designer Admin Console, and specify the name of the workflow in this field.

If you configure a specific workflow by defining the workflow type and creating suitable Engagement Designer rules, you must also create a default rule to handle all cases that do not meet the criteria.

You can enter 0 to 100 characters in this field.

- d. In the **Route point** field, select the Route Point name to apply for the rule. You must select the Route Point that you configured using Avaya Control Manager.

 Important:

You must select a Route Point when configuring Social Gateways.

- e. In the **Gateway Account** field, select the account that you created in Step 5.

- f. In the **Edit Attributes** section, select the attributes based on which the incoming Social Media messages must be routed.

! Important:

Skip this step if you already configured the language attributes in MessagingService.

- g. Click **Save**.

Configuring Social Media for third-party gateways

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **SMS/Social**.
3. Click **Social Configuration**.
4. Click **Create**.
5. On the Account tab, perform the following steps:
 - a. In the **Create Snapin** section, in the **Name** field, enter a name for the new snap-in and click **Create**.
 - b. In the **Snapin** field, select the snap-in that you created.
 - c. In the **Name** field, enter the name of the gateway for the snap-in.
Social Media Snap-in can support maximum five incoming social gateway channels.
 - d. In the **Gateway Name** field, enter the name of the gateway.
You can enter up to 50 characters.
 - e. In the **Social Type** field, type `Devconnect`.
 - f. In the **Header Access Key** field, enter the unique access key for this channel.
You can enter up to 50 characters.
 - g. In the **Callback URL** field, enter the URL hosted by the third-party gateway.
You can enter up to 100 characters.
6. Click **Save**.
7. Select the **Details** tab.
8. On the Details tab, perform the following steps:
 - a. Click **Create**.
 - b. In the **Social Handle** field, enter the social handle.
 - c. Keep the **Workflow** field blank.

To meet your specific requirements, you can configure a specific Engagement Designer workflow through the Event Catalog tab in the Engagement Designer Admin Console, and specify the name of the workflow in this field.

If you configure a specific workflow by defining the workflow type and creating suitable Engagement Designer rules, you must also create a default rule to handle all cases that do not meet the criteria.

- d. In the **Gateway Account** field, select the account that you created in Step 5.
- e. In the **Edit Attributes** section, select the attributes based on which the incoming Social Media messages must be routed.
- f. In the **Route point** field, select a routepoint from the list.
- g. Click **Save**.

Configuring Social Media for Transfer to Service

Configuring a Transfer to Service Route Point for Social Media

About this task

Use this procedure to create a new Transfer to Service Route Point for Social Media through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
 - a. In the **Type** field, select `Route Point`.
 - b. In the **Sub Type** field, select `Transfer to Service`.
 - c. In the **Name** field, enter a name for the Route Point.
 - d. Click **Save**.

Creating a Transfer Target service for Social Media

About this task

Use this procedure to create a Transfer Target service for Social Media through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, perform the following steps:
 - a. In the **Service Name** field, enter the name of the service.
 - b. Select the **Available for Transfer** check box.
The system automatically selects the **Agent Display** check box.
 - c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
 - d. In the Transfer Routepoints section, in the **Social** field, select the Route Point that you created for Social Media.
 - e. Click **Save**.

Chapter 9: Messaging administration

Creating automatic phrases for Messaging

About this task

Use this procedure to create automatic phrases for a phrase group. Instead of typing individual responses, you can create a list of commonly used phrases for a user group and insert an instant message.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging > Auto Phrases**.
3. In the Create Phrase Group section, in the **Name** field, type a name for the phrase group and click **Create**.
4. In the Auto Phrases section, move the required phrases from the **Phrases not in group** list to the **Phrases in group** list by clicking the < button.
5. **(Optional)** To create a new phrase text, do the following:
 - a. In the **Create Auto Phrase** section, in the **Name** field, type a name for the automatic phrase.
 - b. In the **Phrase Text** field, type the text that is commonly used for the contacts based on the selected group.
 - c. Click **Create**.

The newly created phrase appears in the list.
6. **(Optional)** To edit a phrase in the **Phrases not in group** list, do the following:
 - a. Select a phrase from the **Phrases not in group** list.
 - b. Click **Edit**.
 - c. In the **Update Auto Phrase** section, in the **Name** field, type a name for the automatic phrase.
 - d. In the **Phrase Text** field, type the text that is commonly used for the contacts based on the selected group.
 - e. Click **Update**.
7. In the **Edit Attributes** section, select the required attributes.

For example, select `Language.English`.

8. Click **Save**.

Creating a welcome message

About this task

Use this procedure to create a welcome message that must be sent to the customer when an agent joins the interaction.

Procedure

1. Start Omnichannel Administration Utility.
2. In the navigation pane, click **Web Chat/Messaging > Resources**.
3. In the **Create Welcome Message** field, type a message.
4. Click **Create**.
5. In the **Welcome Message** list, select the newly created message.
6. In the **Attributes** section, select the required attributes.
For example, select `Language.English`.
7. Click **Save**.

Configuring Messaging for Transfer to Service

Configuring a Transfer to Service Route Point for Messaging

About this task

Use this procedure to create a new Transfer to Service Route Point for Messaging through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Configuration > Avaya Oceana™ > Route Points**.
2. On the Route Points List page, click **Add**.
3. To add the Transfer to Service Route Point, perform the following steps:
 - a. In the **Type** field, select `Route Point`.

- b. In the **Sub Type** field, select `Transfer to Service`.
- c. In the **Name** field, enter a name for the Route Point.
- d. Click **Save**.

Creating a Transfer Target service for Messaging

About this task

Use this procedure to create a Transfer Target service for Messaging through Avaya Control Manager.

Before you begin

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

Procedure

1. On the Avaya Control Manager webpage, click **Avaya Oceana™ > Work Assignment**.
2. Select the **Services** tab.
3. On the Services tab, click **Add**.
4. To add a Transfer Target service, do the following:
 - a. In the **Service Name** field, enter the name of the service.
 - b. Select the **Available for Transfer** check box.

Avaya Control Manager automatically selects the **Agent Display** check box.
 - c. Move the required attributes from the **Available Attributes** list to the **Included Attributes** list.
 - d. In the Transfer Routepoints section, in the **Messaging** field, select the Route Point that you created for Messaging.
 - e. Click **Save**.

Chapter 10: Oceana Data Management and Purging

Cleanup and purging overview

Use the procedures in this chapter to set up the cleanup rules and scheduled tasks to archive closed contacts from the Omnichannel database.

Avaya Oceana® includes the following two databases for multimedia contacts:

- Omnichannel database
- OFFLINE database

The Omnichannel database contains all active contacts. The OFFLINE database maintains an archive of contacts from the Omnichannel database.

A background OFFLINE synchronization task updates the OFFLINE database. To create rules and schedules and clean up the Omnichannel database, remove closed contacts from it and leave them in the OFFLINE database. This keeps the Omnichannel database small and efficient, while also allowing for historical reporting across all the contacts in both the active and the OFFLINE databases.

You can configure the OFFLINE database to purge contacts over a specific age. You specify the age at which Avaya Oceana® purges closed contacts. Avaya Oceana® runs a purge task every day and purges contacts that meet the age criteria. You cannot recover a purged contact other than restore a backed-up OFFLINE database.

Important:

To view the purge job details, check the Oceana Data Management logs.

Database sizing and limits

The Omnichannel database supports a maximum of 7,000,000 contacts. To stay below this limit, you must regularly cleanup contacts from the Omnichannel database. The maximum size of the OFFLINE database is 70% of the database drive size. For example, if the Omnichannel database drive size is 200 GB, then the maximum size of the OFFLINE database is 140 GB. If the OFFLINE database fills up, you can either increase the Omnichannel database disk space or change the OFFLINE database purge interval.

To prevent service interruption, updates to the OFFLINE database stop when the database drive size is 70% full, and the OFFLINE database has less than 5% free space. Updates continue after you purge contacts or if space is freed or added to the drive.

You can check the current sizes of the databases in the Oceana Data Management tool.

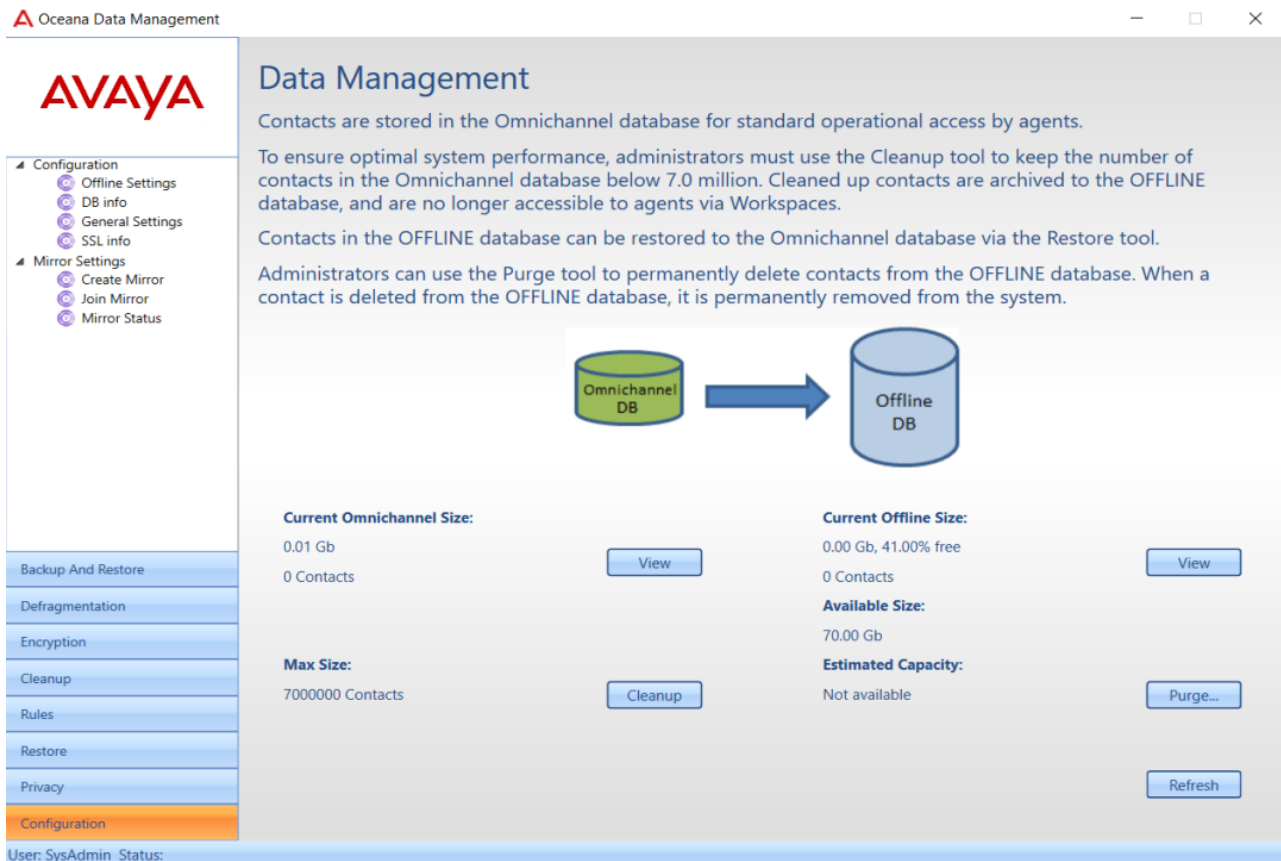


Figure 1: Data Management Configuration screen

Current OFFLINE Size shows the used space, the number of contacts, and the percentage of free space in the OFFLINE database. Here, the value of free size is calculated as the following:

- Memory blocks are allocated dynamically when the OFFLINE database size increases. For example, when data fills in the first allocated memory block, the second memory block is allocated, and so on. The value of free size is measured in the percentage of free size of each allocated memory block and not the total free size on disk available for the OFFLINE database.
- When the value of free space is close to null, it means that the currently allocated memory block is almost filled by data, a new memory block will be allocated soon if required, and there is enough memory on the disk. The value of free size is set to null after completion of the Truncate operation for the OFFLINE database.

When the current size of the OFFLINE database grows to 75% of the maximum size, Avaya Oceana® logs this event to the log file. When the current size of the OFFLINE database grows above 90% of the maximum size, Avaya Oceana® logs events to the event viewer. If the current size of the OFFLINE database exceeds 95%, Avaya Oceana® stops automatically synchronizing contacts from the Omnichannel database, and prevents you from running manual or scheduled cleanups.

You can configure purging of contacts from the OFFLINE database to reduce the database size. Specify the age at which Avaya Oceana® purges closed contacts. Avaya Oceana® runs a purge

task every day and purges contacts that meet the age criteria. You cannot recover a purged contact other than restore a backed-up OFFLINE database.

Cleanup rules

You create a cleanup rule to select contacts for a scheduled cleanup task. Cleanup rules apply to the Omnichannel database only. Cleanup rules select contacts based on the number of days for which they remain in a Closed state, and any one of the following criteria:

- Email rule
- Customer
- Channel type

In addition, there are three system cleanup rules:

- Customers with no contacts: This rule clears customer records with no contacts, which can occur on systems upgraded from an earlier release.
It deletes records of voice customers who do not have any contacts in the Avaya Oceana® database.
- All contacts more than 1 year old: This rule clears all contacts that are more than one year old.
- All contacts more than 5 years old: This rule clears all contacts that are more than five years old.

You cannot modify these rules. They allow you to clear customer records with no contacts that occur in exceptional circumstances. Run scheduled tasks with these rules periodically to clear unwanted customer records from the active database.

Each scheduled cleanup task uses a rule, so you must create a rule before you can create a scheduled task.

Important:

To avoid clearing a large number of customer records at once, configure cleanup rules as soon as the Omnichannel database is operational. Clearing a large number of customer records takes a long time and consumes significant personal computer resources. Run scheduled cleanup tasks on a regular basis to remove a small number of contacts each time.

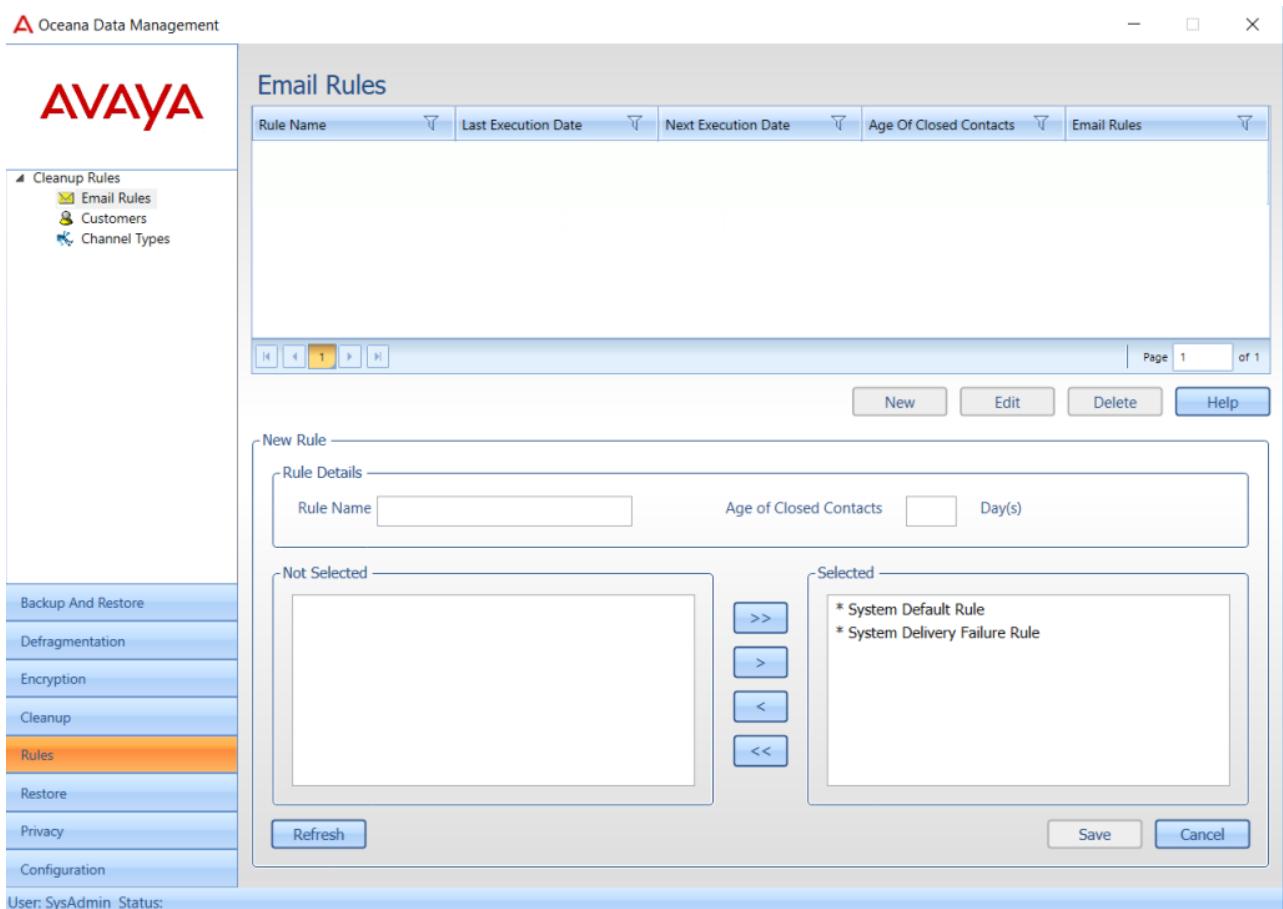


Figure 2: The Oceana Data Management utility rules interface

Scheduled tasks

You create scheduled cleanup tasks to clear contacts from the Omnichannel database. A scheduled task uses a single cleanup rule to select the contacts to clear. The scheduled task checks whether each contact matching the rule is archived in the OFFLINE database. If the contact is archived, the task clears it from the Omnichannel database. If the contact is not archived, the cleanup task copies the contact to the OFFLINE database and then clears it from the Omnichannel database.

The following figure shows the interface that you use to create scheduled cleanups of the Omnichannel database.

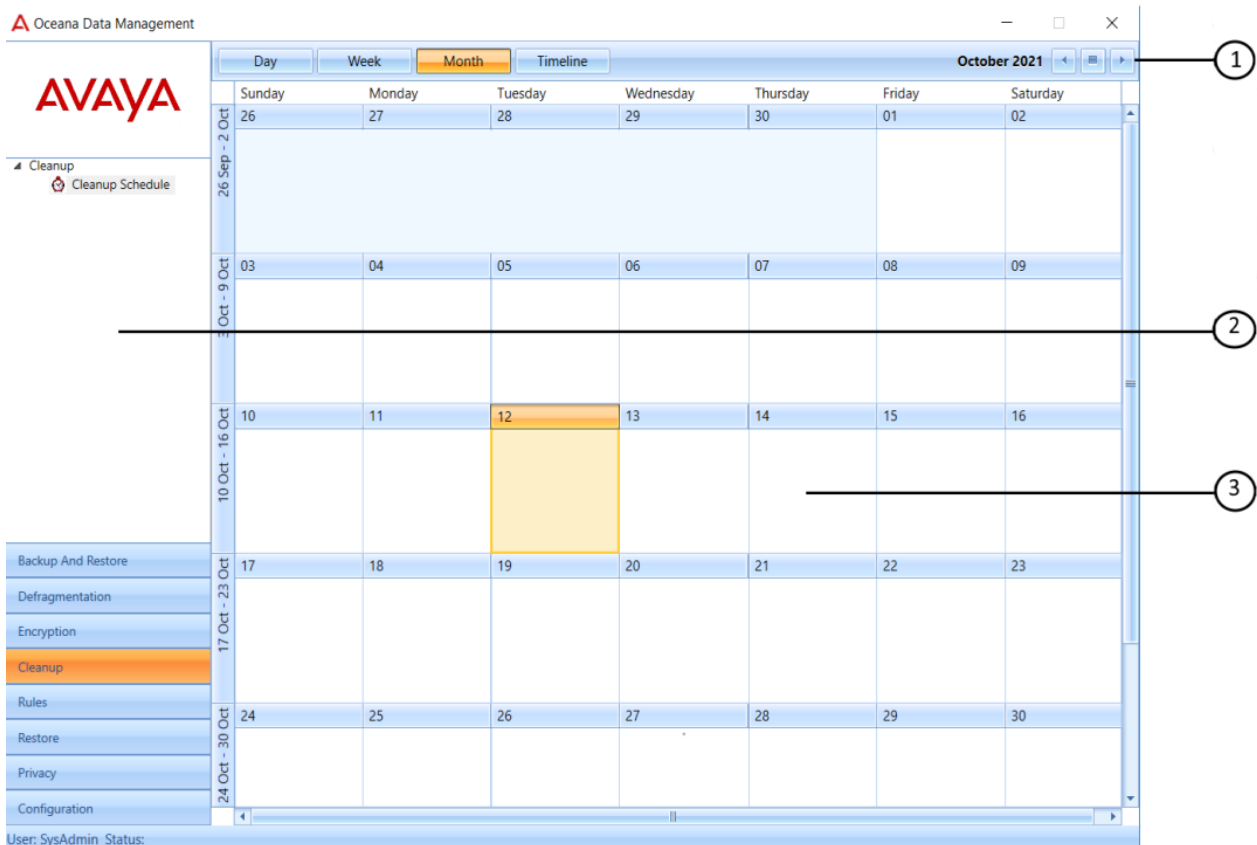


Figure 3: The Oceana Data Management utility scheduling interface

The illustrated interface shows three work areas:

1	Top Bar
2	Navigation Pane
3	Scheduled Task Calendar

Restoring contacts

You can restore the contacts cleared by a scheduled cleanup task. For more information about restoring contacts, see *Deploying Avaya Oceana®*.

Use of Oceana Data Viewer statistics to identify data to clean up

You can use the statistics of Oceana Data Viewer to identify data to clean up. For information about Oceana Data Viewer, see *Deploying Avaya Oceana®*.

Purging of OFFLINE Database

You can purge contacts from the OFFLINE database to reduce the database size. You cannot recover purged contacts, so it is important to back up the OFFLINE database before a purge.

Related links

[Starting the Oceana Data Management utility](#) on page 194

[Creating an Email Rules cleanup rule](#) on page 194

[Creating a Customers cleanup rule](#) on page 195

[Creating a Channel Types cleanup rule](#) on page 196

[Creating a new scheduled cleanup task](#) on page 197

[Enabling OFFLINE database purging](#) on page 198

[Restoring contacts cleared by a scheduled task](#) on page 199

[Configuring session timeout](#) on page 200

Starting the Oceana Data Management utility

About this task

Use this procedure to start the Oceana Data Management utility.

Procedure

1. Log in to the Omnichannel Database server.
2. Go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Double-click the `OceanaDataManagementTool.exe` file.

Related links

[Cleanup and purging overview](#) on page 189

Creating an Email Rules cleanup rule

About this task

Create a cleanup rule to select closed email contacts in the Omnichannel database. You can use this rule in a scheduled cleanup task to clear these contacts from the database. The following are the two criteria that you can use to select email contacts:

- The number of days the contact is in a Closed state.
- The email rule that the incoming email matched when Avaya Oceana® created the contact.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Rules**.
4. In the navigation pane, click **Email Rules**.
5. In the content pane, click **New**.
6. In the **Rule Name** field, enter a descriptive name for this rule.
7. In the **Age of Closed Contacts** field, type the number of days that a contact must be closed to match this rule.
8. For each email rule that you want to add to the cleanup rule, do the following:
 - a. In the **Not Selected** field, select the email rule.

- b. Click the right-arrow button to move the email rule to the **Selected** field.
9. For each email rule that you want to remove from the cleanup rule, do the following:
 - a. In the **Selected** field, select the email rule.
 - b. Click the left-arrow button to move the email rule to the **Not Selected** field.
10. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the Omnichannel database.

Related links

[Cleanup and purging overview](#) on page 189

Creating a Customers cleanup rule

About this task

Create a cleanup rule to select closed contacts in the Omnichannel database based on the contact customer. You can use this rule in a scheduled cleanup task to clear these contacts from the database. The following are the two criteria that you can use to select contacts by customer:

- The number of days the contact is in a Closed state.
- The contact customer.

Note:

The search function returns and displays the First name and Last name of the customer. Different customers can share the same First name and Last name. Therefore, the results of the search function can be identical for different customer's IDs.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Rules**.
4. In the navigation pane, click **Customers**.
5. In the content pane, click **New**.
6. In the **Rule Name** field, enter a descriptive name for this rule.
7. In the **Age of Closed Contacts** field, type the number of days that a contact must be closed to match this rule.
8. For each customer that you want to add to the cleanup rule, do the following:
 - a. In the **Customer Search** field, select the search key for the customer, **ID**, **E-mail**, **Phone**, **Social Detail**, or **Account ID**.
 - b. In the **Equal To** field, type the appropriate value based on the option selected in the drop-down list.

- c. Click **Search**.
 - d. Select the customer that the search function returns.
 - e. Click the right-arrow button to move the customer to the **Selected** field.
9. For each customer that you want to remove from the cleanup rule, do the following:
 - a. In the **Selected** field, select the customer.
 - b. Click the left-arrow button to move the customer to the **Not Selected** field.
10. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the Omnichannel database.

Related links

[Cleanup and purging overview](#) on page 189

Creating a Channel Types cleanup rule

About this task

Create a cleanup rule to select closed contacts in the Omnichannel database based on the channel types such as SMS, Email, Chat, Social, Generic, and Messaging. You can use this rule in a scheduled cleanup task to clear these contacts from the database. The following are the two criteria that you can use to select contacts by channel type:

- The number of days the contact is in a Closed state.
- The channel type.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Rules**.
4. In the navigation pane, click **Channel Types**.
5. In the content pane, click **New**.
6. In the **Rule Name** field, enter a descriptive name for this rule.
7. In the **Age of Closed Contacts** field, type the number of days that a contact must be closed to match this rule.
8. For each channel type that you want to add to the cleanup rule, do the following:
 - a. In the **Channel Types** field, select the channel type.
 - b. Click the right-arrow button to move the channel type to the **Selected** field.
9. For each channel type that you want to remove from the cleanup rule, do the following:
 - a. In the **Selected** field, select the channel type.

- b. Click the left-arrow button to move the channel type to the **Not Selected** field.
10. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the Omnichannel database.

Related links

[Cleanup and purging overview](#) on page 189

Creating a new scheduled cleanup task

About this task

Create a scheduled cleanup task to clear contacts from the Omnichannel contact database. A scheduled task uses a single cleanup rule to select the contacts to clear. Scheduled tasks clear only closed contacts that are already copied to the OFFLINE database. If a contact is not previously copied to the OFFLINE database, the scheduled task copies it before clearing it.

You can select only a single rule for each scheduled task. You can choose to run a scheduled task once, weekly, or monthly. If you select to run a scheduled task weekly or monthly, you can optionally set an end date after which the scheduled task does not run.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. Create a new rule to select the contacts that you want to clear.
4. In the Oceana Data Management utility, click **Cleanup**.
5. In the navigation pane, click **Cleanup Schedule**.
6. In the schedule calendar, select the date on which you want to schedule a cleanup task.
You can use the **Day**, **Week**, **Month**, **Timeline**, **Back**, **Calendar**, and **Forward** controls in the Top Bar to browse to a date if it is not currently visible.
7. Double-click the date on which you want to create the scheduled task.
The Oceana Data Management utility displays the Schedule Cleanup dialog box.
8. In the **Name** field, enter a display name for the scheduled task.
9. In the **Description** field, enter a description for the scheduled task.
10. In the **Select Type** field, select the type of cleanup rule for the scheduled task.
11. In the **Select Rule** field, select an existing cleanup rule that the scheduled task uses to identify the contacts to clear.
12. In the **Schedule** section, select the frequency with which you want this task to run. The options are:
 - **Run Once**

- **Weekly**
- **Monthly**

13. If you select the **Run Once** option, do the following:

In the **Start Date** fields, select the date and time on which you want the task to run.

14. If you select the **Weekly** option, do the following:

- In the **Start Date** fields, select the first date and time on which you want the task to run.
- Select the days of the week on which you want the task to run.
- If you want the scheduled task to stop running after a date in the future, select **End on** and select a date after which this task does not run.

15. If you select the **Monthly** option, do the following:

- In the **Start Date** fields, select the first date and time on which you want the task to run.
- In the **Day** field, enter the day of the month on which you want the task to run.
- In the **of every** field, enter the frequency of this monthly task.

For example, enter 1 to run the task every month, enter 2 to run the task every second month, or enter 12 to run the task once a year.

- If you want the scheduled task to stop running after a date in the future, select **End on** and select a date after which this task does not run.

16. Click **Save**.

Related links

[Cleanup and purging overview](#) on page 189

Enabling OFFLINE database purging

About this task

Enable OFFLINE database purging to permanently remove closed contacts from the OFFLINE database. Choose the length of time for which closed contacts can remain in the OFFLINE database before Avaya Oceana® purges them. Avaya Oceana® runs the purge task every day and deletes contacts that are closed for the duration you configure. Avaya recommends that you do not configure purging unless the OFFLINE database approaches maximum usage.

Important:

When Avaya Oceana® purges a contact from the OFFLINE database, you cannot recover the contact except by retrieving it from a backed-up OFFLINE database. Ensure that the duration you configure to retain contacts is consistent with your local legislative and corporate data retention requirements.

Procedure

1. Log in to the Omnichannel Database server.

2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Configuration**.
4. In the navigation pane, click **Offline Settings**.
5. In the content pane, click **Purge**.
6. In the Purge Settings dialog box, select the **Enable Data Purge** check box.
7. In the **Keep Offline records (months)** field, type the number of months for which a contact must be closed for Avaya Oceana® to purge it from the OFFLINE database.

Ensure the value you enter is consistent with your local legislative and corporate data retention requirements.

8. Click **Save**.
9. In the **Oceana Data Management** dialog box, click **Yes**.
10. In the **Purge Settings** dialog box, click **Close**.

Related links

[Cleanup and purging overview](#) on page 189

Restoring contacts cleared by a scheduled task

About this task

Use this procedure to restore the contacts cleared by a scheduled cleanup task. When you restore a scheduled task, Avaya Oceana® restores all the cleared contacts to the Omnichannel database.

To restore contacts previously cleared by a scheduled task, ensure that an existing scheduled task does not clear the contacts the next time it runs. For example, reopen the contacts, cancel the scheduled task that originally cleared them, or change the cleanup rule that the contacts matched.

The Cleanup History list shows all previously-completed scheduled tasks that cleared contacts. It provides the following information for each task:

- The name of the task.
- The execution date of the task.
- The number of contacts that the task cleared from the Omnichannel database.
- The number of customers whose contacts got cleared from the database.
- The restore status of the task.

Note:

Avaya recommends running one cleanup task at a time. Where more than one cleanup task is run, a contact can be included in each cleanup. Restoring any of the cleanups successfully moves the contact into the active database.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.

3. In the Oceana Data Management utility, click **Restore**.
4. In the navigation pane, click **Restore**.
5. On the Cleanup History screen, review the list of completed scheduled cleanup tasks.
6. Select the scheduled task that cleared the contacts that you want to restore.
7. Click **Restore**.
8. On the Oceana Cleanup Restore screen, click **Yes**.

Avaya Oceana® schedules a task to restore the contacts and shows the start time in the **Restore Status** field. When the restore task starts, the **Restore Status** field shows the task progress.

Related links

[Cleanup and purging overview](#) on page 189

Configuring session timeout

About this task

The Oceana Data Management Tool provides an administrative setting to configure a session timeout for Omnichannel Administration Utility and Oceana Customer Management tool (OCMT). A privileged user can configure a timeout to terminate sessions.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Configuration**.
4. In the navigation pane, click **General Settings**.
5. In the **Administrative Tools Settings** section, in the **Session timeout** field, select the duration.

Administrators who launch Omnichannel Administration Utility and OCMT are logged out after the session timeout interval and have to restart the tools. The maximum timeout duration is 12 hours.

6. Click **Save**.

Related links

[Cleanup and purging overview](#) on page 189

Customer privacy

Customer privacy overview

The Oceana Data Management utility includes the **Privacy** tab. Using this tab, you can act on privacy requests from customers.

You can use the Oceana Data Management utility to address the following customer privacy requests:

- If a customer exercises the right to access information, you can provide the customer with their information stored in the Avaya Oceana® databases. You can save this information in an XML file, which can be modified before you provide it to the customer. The file contains all relevant customer information.
- If a customer exercises the right to be forgotten, you can delete their history records from the Omnichannel, OFFLINE, Context Store, and Avaya Analytics™ databases. In High Availability solutions, the records are also deleted from the standby servers.

 Note:

To prevent the deletion of contacts not yet handled by agents, a customer's history records can be fully deleted only when all their contacts are in a closed status. For example, a customer with contacts in new or open status cannot be deleted.

To configure Context Store and Avaya Analytics™ details, you must use the Oceana Data Management utility and generate an authentication token to authenticate the connection to these databases. This prevents users other than administrators from accessing or deleting customer information stored in the Context Store and Avaya Analytics™ databases.

 Important:

You cannot manage data stored in the Avaya Co-Browsing Snap-in database using the Oceana Data Management utility. For information about how to manage customer data stored in the Avaya Co-Browsing Snap-in database, see *Avaya Co-Browsing Snap-in Reference*, available from the Avaya Support website at <https://support.avaya.com>.

Configuring Context Store and Avaya Analytics™ server details

About this task

The administrator must first configure the server details for both products to retrieve and delete customer information from the Context Store and Avaya Analytics™ databases. The Omnichannel Database server can then establish a connection to both servers.

If the solution includes a second Avaya Analytics™ database server or a second Context Store server located at a second data center for geographic redundancy, the administrator must also add the details of those geographic servers.

Procedure

1. Log in to the Omnichannel Database server.

2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Privacy**.
4. In the left navigation pane, click **Server Configuration**.
5. Click **New**.
6. From the drop-down list, select **Analytics Server**.
7. In the **IP/FQDN** field, type the IP address or FQDN of the Avaya Analytics™ database server.

 Note:

If your solution includes Avaya Analytics™ 3.x, use the Streams Server details.

8. In the **Port** field, update the port number as 443 for secure communication and 80 for non-secure communication. The default port number is 443.
9. If you use a secure connection to the Avaya Analytics™ database server, select the **Enable secure mode (HTTPS)** check box.
10. Click **Save**.
11. On the **Edit Current Servers** page, click **New**.
12. From the drop-down list, select **Context Store Server**.
13. In the **IP/FQDN** field, type the IP address or FQDN of the Context Store cluster.
14. In the **Port** field, update the port number to connect to the Context Store cluster if required. The default port number is 443.
15. If you use a secure connection to the Context Store EDM server, select the **Enable secure mode (HTTPS)** check box.
16. Click **Save**.

Configuring Avaya Analytics™ authentication

About this task

The Omnichannel Database server uses an authentication token to communicate securely to the Avaya Analytics™ servers. You can use the Oceana Data Management utility to generate this authentication token. This prevents users other than administrators from accessing or deleting customer information stored in the Context Store and Avaya Analytics™ databases. The Oceana Data Management utility uses the Avaya Analytics™ token to redact data from the Context Store database.

 Important:

If your solution includes a second Avaya Analytics™ database server located at a second data center for geographic redundancy, generate a token for the second Avaya Analytics™ database server.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Privacy**.
4. In the navigation pane, click **Authenticate**.
5. In the **Analytics Authenticate** section, select **3.x** or **4.x** depending on your solution.
6. In the **IP address/FQDN** field, select the Avaya Analytics™ server for which you want to generate a token.
7. In the **Port** field, type the port number to connect to the Avaya Analytics™ database server. The default port number for Avaya Analytics™ 3.x is 8443, and the default port number for Avaya Analytics™ 4.x is 443.
8. In the **Starting URL** field, type `orca-breeze-authentication`.
9. In the **Username** field, type the user name to connect to the Avaya Analytics™ Oceana/Workspaces Administrator configured in ACM.
The user must be an administrator user.
10. In the **Password** field, type the password for the user.
11. Click **Get Token**.

The Oceana Data Management utility displays the result of the token request.

12. In the **Geo Redundant Analytics Authenticate** section, in the **IP address/FQDN** field, select the second Avaya Analytics™ database server for which you want to generate a token.
13. In the **Port** field, type the port number to connect to the second Avaya Analytics™ database server.
14. In the **Starting URL** field, type the required details.
15. In the **Username** field, type the username to connect to the second Avaya Analytics™ database server.
16. In the **Password** field, type the password for the user.
17. Click **Get Token**.

The Oceana Data Management utility displays the result of the token request.

Next steps

To regenerate an authentication token, click **Refresh Token**.

Generating a customer information file

About this task

If you receive a customer information request, use the Oceana Data Management utility to generate customer information in an XML file. You can modify this file before sending it to the customer if required. The Oceana Data Management utility retrieves customer information from Omnichannel and OFFLINE databases. You can search for customers based on customer ID, email address, phone number, social details, or account ID.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Privacy**.
4. In the navigation pane, click **Information Request**.
5. In the Customer Search area, select one of the following options from the drop-down list:
 - **ID**
 - **E-mail**
 - **Phone**
 - **Social details**
 - **Account ID**
6. In the **Equal To** field, type the appropriate value based on the option selected in the drop-down list.
7. Click **Search**.
8. Select the customer and click **Save As**.
9. Navigate to the folder where you want to save the XML file.
10. In the **File name** box, type a name for the file and click **Save**.
11. Click **OK** in the dialog box confirming the file location.

 Note:

The time taken to generate the file depends on the size of the customer record.

12. **(Optional)** If required, modify the file before sending it to the customer.

Creating a customer detail audit cleanup rule

About this task

Create a cleanup rule to select customer detail audit entries in the Omnichannel database. You can use this rule in a scheduled cleanup task to clear these customer detail audit entries from the database.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Rules**.
4. In the navigation pane, click **Customer detail audit**.
5. In the content pane, click **New**.
6. In the **Rule Name** field, enter a descriptive name for this rule.
7. In the **Age of Entry** field, type the number of days that a customer detail audit entry must be closed to match this rule.
8. Click Save.

Next steps

Create a new scheduled task to use this rule to clear customer detail audit entries from the Omnichannel database.

Deleting customer history

About this task

If you receive a customer right to be forgotten request, use the Oceana Data Management utility to delete customer history records from Omnichannel, OFFLINE, Context Store, and Avaya Analytics™ databases. You can search for customers based on customer ID, email address, phone number, social details, or account ID.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Privacy**.
4. In the navigation pane, click **Delete Request**.
5. In the Customer Search area, select one of the following options from the drop-down list:
 - **ID**
 - **E-mail**
 - **Phone**
 - **Social details**
 - **Account ID**
6. In the **Equal To** field, type the appropriate value based on the option selected in the drop-down list.
7. Click **Search**.
8. Depending on the databases you want to delete the customer history from, select the **Delete from OCP**, **Delete from Analytics**, or **Delete from Context Store** check box.

9. Select the customer and click **Delete**.

 Note:

If a customer history record is not found, you can still choose to delete the history from the Avaya Analytics™ database that corresponds to the identifier used to search for the record. For example, delete data from the Avaya Analytics™ database that corresponds to a phone number.

10. Click **Yes** to confirm that you want to delete the customer history record.

Repeating a customer deletion request

About this task

To repeat a customer deletion previously run, you can use the delete replay option. For example, use this option to delete previously redacted data from the Context Store or Avaya Analytics™ databases after a database restore. You can repeat a previous deletion based on customer ID.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Privacy**.
4. In the navigation pane, click **Delete Replay**.
5. In the **Delete Replay** section, in the **Customer Id** field, type the ID of the customer to repeat the deletion action.
6. To delete previously redacted data from the Context Store and Avaya Analytics™ databases, select the **Analytics** and **Context Store** check boxes.
7. Click **Replay**.

The Oceana Data Management utility displays the result of the replay action.

Adding SSL certificates

About this task

Secure Sockets Layer (SSL) protocols provide communications security over a computer network. Use the following procedure to add the SSL certificate on the Oceana Data Management utility

 Note:

If the SSL certificate is configured on the previous system before upgrading on 3.8.1.0 or 3.8.1.1, delete the SSL certificate via Cache Management Portal and reconfigure the SSL certificate via ODMT to get notifications about expiration of certificates in Oceana Monitor.

Before you begin

Ensure you have the following:

- Issued certificate

- Private key file
- Private key password

 Note:

For more information about generating the certificate, see Manage Security and TLS certificates chapter in Deploying Avaya Oceana guide.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Configuration**.
4. In the left navigation pane, click **SSL info**.
5. In **File containing this configuration's X.509 certificate**, click **Browse** and select the server certificate file.
6. In **File containing associated private key**, click **Browse** and select the key file.
7. In **Private key password**, provide the password that is used during the generation of the certificate.
8. Click **Save**.

If the provided information is incorrect an error message appears.

If the provided information is correct then the **Installed certificates** section displays the following details of the configured SSL certificate:

- SSL Config Name– the name of the configuration.
- Installed date– the installation date of the certificate.
- Expiry date– the date until the certificate is valid.
- Days to expire– the number of days the certificate is valid (the color of this cell is green or red for clarity).

Removing expired SSL certificates

About this task

Use this procedure to remove the expired SSL certificates.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Configuration**.
4. In the left navigation pane, click **SSL info**.
5. Select the expired certificate from the **Installed Certificates** list and click **Remove**.

Database backup and restore

Database backup and restore overview

The Oceana Data Management utility includes the **Backup and Restore** tab. With this tab, you can:

- Take a backup of the Omnichannel database to preserve its data.
- Restore the Omnichannel database.
- Create a schedule task to take a backup of the Omnichannel database.
- View the status of the scheduled backup task.

You perform backup and restore operations mainly during the upgrade process.

Taking a backup of the Omnichannel database

About this task

Use this procedure to take a backup of the Omnichannel database. This procedure applies to a standalone Omnichannel database that does not have a cache mirror.

For information about how to take a backup of the Omnichannel database that has a cache mirror, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

* Note:

- Ensure that you take backups of the Omnichannel database at regular intervals.
- The backup is taken from the active database if it was previously in an HA mirrored configuration on Data Center 1.

Procedure

1. Log in to the Omnichannel server.
2. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
 - For Avaya Oceana® 3.7 or higher version, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
 - For Avaya Oceana® 3.7 or higher version, double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.

6. In the **Select/create file to backup to** field, click **Browse**.
7. On the Save As screen, do the following:
 - a. Select the location to save the backup file.
Do not save the backup file to the software, journal, or multimedia drive.
 - b. Specify a name for the backup file. When naming the file, use English or numeric characters only.
 - c. Click **Save**.
8. Click **Backup Database**.
The utility displays the Backup complete! message when the backup process is complete.
9. Verify that the backup file is created at the specified location.

Taking a backup of the Omnichannel database from a network location

About this task

Use this procedure to take a backup of the Omnichannel database from a network location.

Note:

Ensure that the network location you select for taking the backup has enough free space for saving a backup file.

Procedure

1. Log in to the Omnichannel server.
2. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
 - For Avaya Oceana® 3.7 or later, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
 - For Avaya Oceana® 3.7 or later, double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.
6. In the **Select/create file to backup to > Network details** section, select the **Is this a protected network drive?** check box.

Additional fields for username, password, and drive are displayed.

7. In **Username**, enter the username for the network folder.
8. In **Password**, enter the password for the network folder.
9. In **Drive**, select a drive to be used to substitute the network location.

 Important:

You must select a drive that is not already used.

 Note:

If you use a local drive for backup, clear the **Is this a protected network drive ?** check box.

Restoring the Omnichannel database

About this task

Use this procedure to restore the Omnichannel database onto your Microsoft Windows Server 2019 (Desktop Experience) Omnichannel server. This procedure applies to a standalone Omnichannel database that does not have a database mirror. For more information on how to restore the Omnichannel database that has a database mirror, see *Avaya Oceana® and Avaya Analytics™ Disaster Recovery*.

 Important:

You must install, run, and patch the Omnichannel server software using a Windows Administrator account with full Administrator privileges. You must run the Oceana Data Management Tool using the same account.

Procedure

1. Log in to the Omnichannel server as an administrator.
2. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
 - For Avaya Oceana® 3.7 or later, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
 - For Avaya Oceana® 3.7 or later, double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.
6. Navigate to the **Select file to restore from** section.

7. The **Allow Restore if user file is missing** option is checked by default.

 Note:

The **Allow Restore if user file is missing** option ensures that the restore continues without error, even if a User file is missing while the Restore file is present on a folder.

8. Click **Browse**.
9. Select the backup file and click **Open**.
10. Click **Restore Database**.

The application displays the Drive restore screen.

11. In the **Select your database drive letter** field, select the drive that you specified for the Omnichannel database when installing the Omnichannel server software.
12. In the **Are you restoring a mirrored backup** field, select one of the following options:
 - Select **Yes** if you take the backup from the server with mirroring configured.
 - Select **No** if you take the backup from a system with no mirroring configured.
13. Click **Restore**.

 Important:

If the Omnichannel server displays the Cache Post Restore Script terminal window, keep the window open until the process in the window is completed.

 Note:

If the **Allow Restore if user file is missing** option is cleared and a user file is missing, the restore is not completed, and a message box appears. To complete the restore, you must select the **Allow Restore if user file is missing** option and restart the restore process.

The utility displays the `Restore complete!` message when the restore process is complete.

14. **(Optional)** Modify the passwords again after the restore process because the backup does not contain the previously modified passwords.

 Note:

Perform this step if you had modified the default passwords of the Omnichannel database previously.

15. **(Optional)** Reconfigure the server for secure connections after the restore process.

 Note:

Perform this step if you had previously configured the Omnichannel server for secure connections.

Restoring the Omnichannel database from a network location

About this task

Use this procedure to restore the Omnichannel database from a network location.

Procedure

1. Log in to the Omnichannel server.
2. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\Oceana\BackupAndRestore` folder.
 - For Avaya Oceana® 3.7 or later, go to the `OCEANA_INSTALL_DIR\Avaya\Oceana\MMDataManagement` folder.
3. Do one of the following:
 - For Avaya Oceana® 3.5.x or 3.6, right-click the `BackupAndRestore.exe` file and select **Run as Administrator**.
 - For Avaya Oceana® 3.7 or later, double-click the `OceanaDataManagementTool.exe` file.
4. In the Oceana Data Management utility, click **Backup and Restore**.
5. In the navigation pane, click **Backup and Restore**.
6. In the **Select file to restore from > Network details** section, select the **Is this a protected network drive?** check box.
Additional fields for username, password, and drive are displayed.
7. In **Username**, enter the username for the network folder.
8. In **Password**, enter the password for the network folder.
9. In **Drive**, select a drive to be used to substitute of the network location.

! Important:

You must select a drive that is not already used.

* Note:

If you are use a local drive to restore, clear the **Is this a protected network drive?** check box.

Creating a new scheduled backup task

About this task

In Oceana Data Management utility, you can create a scheduled task to take a backup of the Omnichannel database. You can view each backup status.

You can choose to run a scheduled task daily, weekly, or monthly. You can optionally set a start date for the scheduled task.

 Note:

Backup is only available on the primary OCP Database server. However, it is not available on the mirror backup OCP server. Avaya recommends that you schedule a backup in off-peak time when Avaya Oceana® is not handling peak customer traffic. You must also save backup on a different physical server than the OCP database server.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Backup and Restore**.
4. In the navigation pane, click **Scheduled Backup**.
5. In the schedule calendar, select the date on which you want to schedule a backup task.

You can use the **Day**, **Week**, **Month**, **Timeline**, **Back**, **Calendar**, and **Forward** controls in the Top Bar to browse to a date if it is not currently visible.

6. Double-click the date to create the scheduled task.

The Oceana Data Management utility displays the Schedule Backup dialog box.

7. In the **Backup file path** field, enter the path where you want to save the backup file.

The default path is C : \backup .cbk.

8. In the **Schedule** section, select the frequency with which you want this task to run. The options are:

- **Weekly**
- **Monthly**

9. If you select the **Weekly** option, do the following:

- a. In the **Start Date** field, select the first date on which you want the task to run.

You can also select the time.

- b. Select the days of the week on which you want the task to run.

10. If you select the **Monthly** option, do the following:

- a. In the **Start Date** field, select the first date for the task to run.

You can also select the time.

- b. In the **Day** field, enter the day of the month for the task to run.

11. Click **Save**.

Viewing the details of a scheduled backup task

About this task

The backup task history displays all previously completed scheduled backup tasks. It provides the following information for each task:

- The last start date and time of the backup task.
- The completed date and time of the backup task.
- The result of the backup task.
- The Routine – the name of the backup task.
- The PID – the value of the job when the task is running.
- The date and time the log entry is made.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Backup and Restore**.
4. In the navigation pane, click **Backup History**.

On the Backup Task History screen, you can view the details of each scheduled task. The new backup task details appear on the top of the screen.

Click **Refresh** to refresh the page to list new backup task details.

Database defragmentation

Database defragmentation overview

The Oceana Data Management utility includes the **Defragmentation** tab. Using this tab, you can perform the defragmentation process on the Omnichannel database and view the defragmentation history.

Over time the data in the Omnichannel database becomes fragmented, which can lead to performance degradation. To improve the database performance, you can use defragmentation. Avaya recommends running the defragmentation process every 6-9 months, but only if you experience performance degradation.

Before the defragmentation process starts, Avaya Oceana® performs two checks:

1. Checking if enough disk space is available as the defragmentation process requires additional disk space, up to 100% of the database size. When the defragmentation process is complete, Avaya Oceana® returns the disk space to the operating system.
2. Checking if there is another uncompleted defragmentation process. Avaya Oceana® can run only one defragmentation process at a time.

If the checks are successful, the defragmentation process starts. You can check the defragmentation process status in the Check Defragmentation section.

 Note:

The duration of the defragmentation process depends on the size of the Omnichannel database. It takes approximately one minute per gigabyte of the database size. You can refer to the Defragmentation History tab to see how long the previous defragmentation processes took. This information will help you estimate the duration of the current defragmentation process.

Defragmentation History

On the Defragmentation History tab, you can view the information about previous defragmentation processes, which are listed in chronological order. The information includes start and end times and overall time for the defragmentation in seconds. The Defragmentation History tab displays the following information for the last 100 processes:

- Defragmentation status
- Start time
- End time
- Overall process time

Defragmenting the Omnichannel database

About this task

You can run the defragmentation process to improve the database performance.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Defragmentation**.
4. In the navigation pane, click **Data Defragmentation**.
5. Click **Defragment Now**.
6. In the confirmation window, click **OK**.
7. **(Optional)** To check the defragmentation status, click **Refresh**.

In the Check Defragmentation section, Avaya Oceana® displays the defragmentation status, start and end times, and overall process time.

Next steps

You can view the defragmentation history on the Defragmentation History tab.

Viewing the defragmentation history

About this task

You can view the defragmentation process history using the Defragmentation History tab. The tab displays the table with the information about the previous defragmentation processes, listed in chronological order, with the newest at the top of the table. The information in the table includes the following:

- Defragmentation Status
- Time Started
- Time Ended
- Time Taken

You can use the Time Taken column to estimate how long the next defragmentation process can take. If you add and purge data at a consistent rate, the defragmentation process takes approximately the same time each time you run it.

The defragmentation history tab only displays the information about the last 100 processes.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Defragmentation**.
4. In the navigation pane, click **Defragmentation History**.
5. To view the updated defragmentation history, click **Refresh**.

Database encryption

Database encryption overview

The Oceana Data Management utility includes the **Encryption** tab. With this tab, you can encrypt and decrypt the data stored in the following databases:

- Omnichannel database
- OFFLINE database
- CoBrowse database

The encryption of databases is important because it makes the data useless if the data is stolen. These databases are encrypted locally. Any interruption during the encryption or decryption process can leave the databases in unusable state. Therefore, you must take a backup of the databases before encrypting them. You must also ensure that you perform the encryption or decryption process during a maintenance window.

Encryption protects databases when they are not being used. Avaya Oceana® is configured to allow Cache to start automatically. The purpose of this configuration is to eliminate any human

intervention for providing the encryption credentials every time the server is restarted. Encryption does not change the normal behavior of the Cache terminal or System Management Portal, where normal user credentials are required to connect, regardless of whether or not the databases are encrypted.

Creating and activating an encryption key

About this task

You must create and activate an encryption key to encrypt or decrypt databases.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Encryption**.
4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory where you want to store the encryption key.

The default directory is `C:/Users/<current_user_name>/Documents`.

7. In the Open dialog box, in the **File name** field, do one of the following:
 - To continue with the default name `enc`, click **Open**.
 - To use a new name, type the name for the encryption key and click **Open**.
8. In the **Username** field, type a username for the encryption key.
9. In the **Password** field, type a password for the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Create and activate key**.

The Oceana Data Management utility displays the following message:

Database encryption key successfully enabled.

Activating the encryption key

About this task

Use this procedure to activate an existing encryption key so that you can use the key to encrypt or decrypt databases.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Encryption**.

4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory containing the encryption key.
7. In the Open dialog box, select the encryption key and click **Open**.
8. In the **Username** field, type the user name of the encryption key.
9. In the **Password** field, type the password of the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Activate key**.

The Oceana Data Management utility displays the following message:

Database encryption key successfully enabled.

Encrypting databases

About this task

Use this procedure to encrypt the following databases:

- Omnichannel database
- OFFLINE database
- CoBrowse database

Important:

The encryption of the Omnichannel database does not necessitate you to enter encryption keys when performing database operations such as backup and restore.

Before you begin

Create and activate an encryption key.

Important:

Ensure that the key for encryption is activated. If you activate one key and try to perform the encryption using a different key, it provokes an inconsistent state of databases.

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Encryption**.
4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory containing the encryption key.
7. In the Open dialog box, select the activated encryption key and click **Open**.

8. In the **Username** field, type the user name of the encryption key.
9. In the **Password** field, type the password of the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Encrypt Database**.

After successful encryption, the Oceana Data Management utility displays the following message:

```
All databases are encrypted
```

If an error occurs in the encryption process, check the details of the error in the logs by using the `*ERROR*` prefix. An Inconsistent Database status indicates that some of the databases are encrypted and some are not.

Decrypting databases

About this task

Use this procedure to decrypt the following databases:

- Omnichannel database
- OFFLINE database
- CoBrowse database

Procedure

1. Log in to the Omnichannel Database server.
2. Start the Oceana Data Management utility.
3. In the Oceana Data Management utility, click **Encryption**.
4. In the navigation pane, click **Data Encryption**.
5. In the **Key location** field, click **Browse**.
6. Select the directory containing the encryption key.
7. In the Open dialog box, select the activated encryption key and click **Open**.
8. In the **Username** field, type the user name of the encryption key.
9. In the **Password** field, type the password of the encryption key.
10. In the **Confirm Password** field, retype the password.
11. Click **Decrypt Database**.

After successful decryption, the Oceana Data Management utility displays the following message:

```
No databases are encrypted
```

Checklist for encrypting or decrypting databases in a High Availability deployment

Use the following checklist to encrypt or decrypt databases in a High Availability (HA) deployment:

No.	Task	Description	✓
1	Create and activate an encryption key on the active Omnichannel Database server.	See Creating and activating an encryption key on page 217.	
2	Encrypt or decrypt databases on the active Omnichannel Database server.	See Encrypting databases on page 218 or Decrypting databases on page 219.	
3	Copy the encryption key from the active Omnichannel Database server to the standby Omnichannel Database servers.	-	
4	Activate the encryption key on the standby Omnichannel Database servers.	See Activating the encryption key on page 217.	
5	Encrypt or decrypt databases on the standby Omnichannel Database servers.	See Encrypting databases on page 218 or Decrypting databases on page 219.	

Checklist for encrypting or decrypting databases in a Disaster Recovery deployment

Use the following checklist to encrypt or decrypt databases in a Disaster Recovery (DR) deployment:

No.	Task	Description	✓
1	Create and activate an encryption key on the active Omnichannel Database server.	See Creating and activating an encryption key on page 217.	

Table continues...

No.	Task	Description	✓
2	Encrypt or decrypt databases on the active Omnichannel Database server.	See Encrypting databases on page 218 or Decrypting databases on page 219.	
3	Copy the encryption key from the active Omnichannel Database server to the backup Omnichannel Database servers.	-	
4	Activate the encryption key on the backup Omnichannel Database servers.	See Activating the encryption key on page 217.	
5	Encrypt or decrypt databases on the backup Omnichannel Database servers.	See Encrypting databases on page 218 or Decrypting databases on page 219.	

Error scenarios

The following are the error scenarios for which you must be careful during the encryption and decryption processes:

- Ensure that the key used for encryption of databases is the same key that you activated.
You must also mount the affected databases manually, decrypt all databases, and then encrypt them in the utility.
- Ensure that you use the correct key for decryption of databases.
- Ensure that you provide correct credentials for the encryption key.
- To provide an access to the encryption functionality by SOAP, the utility creates a temporary web application `/csp/encryption`. In the end, the utility deletes the application. If the utility is stopped in an abnormal way and the web application is not deleted, ensure that you manually delete the web application.

Chapter 11: Customization

Customization overview

Avaya Workspaces provides the Widget Framework feature for administrators to:

- Customize the layout and functioning of workspaces in a contact center.
- Access Widget APIs to create customized workspaces.

To use the Widget Framework feature, you must create an administrator user role in Avaya Control Manager and log in to Avaya Workspaces by using the administrator user credentials. On the Avaya Workspaces administrator interface, you can use Widget Framework tools to customize or create Avaya Workspaces widgets.

For more information about Widget Framework, click the **Overview**  button on the Avaya Workspaces administrator interface and see *Widget Framework Developer Documentation*.

Important:

If an Avaya Control Manager administrator renames a group, the group is assigned back to the default layout in Avaya Workspaces.

Customizing the Transfer to Service list

About this task

When agents start working on work cards, Avaya Workspaces provides a Transfer to Service list. The list contains all the available services where the agents can transfer the interactions. By default, Avaya Workspaces retrieves the list from Avaya Oceana®.

Use this procedure to filter the Transfer to Service list so that agents get a reduced Transfer to Service list in their workspaces.

Procedure

1. Log in to Avaya Workspaces as an administrator.
2. On the Activate Agent screen, click **Activate**.
3. On the Avaya Workspaces administrator interface, do the following:
 - a. Click the **Admin Settings**  button.

- b. Select the **Override Transfer to Service Destination List** check box.

Avaya Workspaces overrides the Transfer to Service list. After that, the workspaces under the logged in administrator does not retrieve the list from Avaya Oceana®.

4. Create a third-party widget.

The third-party widget uses the Widget API to set the Transfer to Service list that you want to display in the **Service** drop-down on the work cards.

5. Import the third-party widget in the Avaya Workspaces administrator interface.
6. On the Avaya Workspaces administrator interface, do the following to add the third-party widget to the workspaces of agents:

- a. Click the **Layout**  button.
- b. On the CUSTOMIZE LAYOUT tab, select the layout that you want to change.
For example, Voice.

 Important:

Ensure that you configure the widget on the visible pane of the channel, so that the widget is present and visible when the agent views the work card.

- c. On the CUSTOMIZE SIDEBAR tab, select a sidebar tab.
- d. On the CONFIGURATION tab, select a layout and then select the third-party widget.
- e. Click **Save Changes**.

For more information, click the **Overview**  button on the Avaya Workspaces administrator interface and read *Widget Framework Developer Documentation*.

Verifying the customized Transfer to Service list

Before you begin

Customize the Transfer to Service list.

Procedure

1. Log in to Avaya Workspaces as an agent.
2. On the Activate Agent screen, do the following:
 - a. In the **Profile** and **Extension** fields, specify appropriate values.
 - b. Click **Activate**.
3. Make a test call to the logged in agent.

This step depends on the channel for which you configured the widget. For example, you must make a test call for the Voice channel and send a test message for the SMS channel.

4. From the Avaya Workspaces agent interface, accept the call.
5. Verify the third-party widget on the Avaya Workspaces agent interface.
6. Click the **Transfer**  button.
7. Click **Services**.
8. Verify the customized Transfer to Service list that you supplied in the widget.

 Important:

The Transfer to Service feature works only if the list of all services exists in Unified Collaboration Administrator (UCA). The widget developer must ensure that the content of the Transfer to Service list sent to Avaya Workspaces is a subset of the overall list of services in UCA. If an entry sent to Avaya Workspaces is not available in UCA and an agent tries to use that entry, Avaya Oceana® presents an error message to the agent informing that the request cannot be processed.

Configuring email confirmation

About this task

Use the following procedure to enable email confirmation for all agents before sending an email. When you enable email confirmation, Avaya Workspaces displays a confirmation dialog box when agents attempt to send an email. This setting applies to all agents.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings**  button.
3. Select the **Confirm Before Sending Email** check box.

Configuring the custom card limit

About this task

You can create custom cards using the Avaya Workspaces Widget Framework. Custom cards appear in the interaction area, and are similar to the default interaction cards. You can use this setting to configure the maximum number of custom cards that can appear in the interaction area.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings**  button.

3. In the **Custom Card Limit** field, select the number of custom cards that must appear in the interaction area at a time.

The maximum number of customer cards that can appear in the interaction area is 10.

Using the Avaya Workspaces compressed layout

About this task

Use the following procedure to enable the compressed layout of the Avaya Workspaces interface. The compressed layout setting applies to the agents assigned to a workspace layout group.

Procedure

1. In the Avaya Control Manager, create a user group associated with a workspace layout and add agents to the user group.
2. Log on to Avaya Workspaces as an administrator user.
3. On the Avaya Workspaces administrator interface, click **Layout Manager**.
4. Do one of the following:
 - For creating a new layout, click **Create New Layout**.
 - To edit an existing layout, click **Edit**.
5. In the **Name** field, type a name for the layout.
6. In the **Description** field, type the layout description.
7. Select the **Use compressed** check box.
8. In the **Assign Agent Groups to this Template** area, use the **+** and **x** buttons on the left and right columns, respectively, to move the required agent groups from the unselected to the selected area.

Important:

- The agents in the group are set to the new layout after they log off and log in again.
 - The agents who are not assigned to any specific layout are set to use compressed mode.
9. Click **Save Changes**.

Enabling finish work confirmation

About this task

You can configure Avaya Workspaces to display a confirmation dialog to all agents who click **Finish Work**, if a custom card is still open.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings**  button.
3. Select the **Confirm Before Finish Work** check box.

Configuring agent toast notifications

About this task

Agents can configure the type of toast notifications that they can see on Avaya Workspaces. The configuration settings applies to all agents.

The following are the types of toast notifications available:

- **Information:** Displays general updates, including supervisor broadcast messages.
- **Warnings:** Displays general Avaya Workspaces warnings.
- **Errors:** Displays critical Avaya Workspaces errors that can impact functionality.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings**  button.
3. Under Agent Toast Notifications, depending on your preferences, select the **Information**, **Warnings**, or **Errors** check boxes.
4. **(Optional)** To override the default time for displaying the toast notifications, select the **Override default time for showing toast notifications** check box.
5. **(Optional)** Select the amount of time that elapses, in seconds, before the toast notifications appear.

Configuring additional language pack

About this task

Use this procedure if you want to add extra languages to the language list on Avaya Workspaces.

*** Note:**

Ensure that you enable this option if you want to use Hebrew on Avaya Workspaces.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click the **Admin Settings**  button.
3. In the **Additional language pack** section, select the **Expose additional language pack** check box.

Configuring the start work button

About this task

When an agent starts work in Avaya Workspaces, the agent state is set to ready by default. Use the following procedure to enable the agents to start work in the ready or not ready state. This setting applies to all agents.

Procedure

1. Log on to Avaya Workspaces as an administrator user.
2. On the Avaya Workspaces administrator interface, click .
3. Select the **Allow Agents the choice to Start Work in a Not Ready or a Ready state** check box.

Customer Journey configuration for Outbound agents

Avaya Oceana® supports the Customer Journey feature for Outbound contacts. Avaya Oceana® supports this feature only if you select the **Publish Attempt Data To Context Store** check box in POM campaigns.

You must also add the Customer Journey widget for Outbound agents so that they can view Customer Journey in Avaya Workspaces.

Adding the Customer Journey widget for Outbound agents

About this task

Use this procedure to add the Customer Journey widget for Outbound agents so that they can view Customer Journey in Avaya Workspaces.

Procedure

1. Log in to Avaya Workspaces as an administrator.
2. On the Activate Agent screen, click **Activate**.
3. Click the **Layout**  button.
4. On the CUSTOMIZE LAYOUT tab, select OUTBOUND.
5. On the CUSTOMIZE SIDEBAR tab, click **Add New Sidebar Tab**.

The Avaya Workspaces administrator interface displays the CONFIGURATION tab.

6. In the Sidebar Options area, do the following:
 - a. In the **Name** field, type the name as Customer Journey.
 - b. In the **Description** field, type a description for the sidebar.
 - c. In the **Icon** field, select `aoc-customer-journey`.
7. In the Select Layout area, select the layout single widget.
8. In the Select Widgets area, in the **Widget 1** field, select `Customer Journey`.
9. Click **Save Changes**.

Chapter 12: Resources

Documentation

Title	Use this document to:	Audience
Overview		
<i>Avaya Oceana® Solution Description</i>	Use this guide to know about the tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Implementing		
<i>Deploying Avaya Oceana®</i>	Use this guide to know how to deploy Avaya Oceana® Solution on the customer environment.	• Sales engineers • Business partners • Solution architects • Implementation engineers
<i>Avaya Oceana® and Avaya Analytics™ Disaster Recovery</i>	Use this guide to know how to restore Avaya Oceana®, solution when there is a complete outage at the primary data center.	• Sales engineers • Business partners • Solution architects • Implementation engineers
<i>Migrating Avaya Oceana®</i>	Use this guide to know how to migrate Avaya Oceana® solution from the existing version.	• Sales engineers • Business partners • Solution architects • Implementation engineers
<i>Deploying Avaya Analytics™</i>	Deploy Avaya Analytics™.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Administering		

Table continues...

Title	Use this document to:	Audience
<i>Administering Avaya Oceana®</i>	Administer Avaya Oceana®.	• System administrators • Supervisors
Using		
<i>Using Avaya Workspaces for Avaya Oceana®</i>	Use Avaya Workspaces for Avaya Oceana®.	• Agents • Supervisors
<i>Using Avaya Analytics™</i>	Use the features and capabilities of Avaya Analytics™.	• Supervisors • Administrators • Report designers
<i>Avaya Analytics™ Data Dictionary</i>	Use historical and real-time measures in custom reports.	• Administrators • Report designer
Maintaining and Troubleshooting		
<i>Maintaining and Troubleshooting Avaya Oceana®</i>	Perform maintenance and troubleshooting procedures for routine maintenance and troubleshooting of Avaya Oceana®.	• Support personnel • Implementation engineers • Administrators
<i>Maintaining and Troubleshooting Avaya Analytics™</i>	Perform common maintenance functions of Avaya Analytics™ and use tools and utilities for troubleshooting of Avaya Analytics™.	• Support personnel • Implementation engineers • Administrators
<i>Avaya Oceana® Alarms</i>	View details about Avaya Oceana® alarms.	• Support personnel • Administrators

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.

8. Click  to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** () in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

You can select multiple items in each filter category. For example, you can select a product and multiple user roles.

- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** () to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available for the Avaya Oceana® program.

Table 4: Sales Credentials

Course code	Course title	Course duration in hours	Delivery type
APSS – 1202 Avaya OneCloud™ CCaaS Sales			
41511W	Selling Avaya OneCloud™ CCaaS Solutions	0.75	Web-based Training
41551T	Avaya OneCloud™ CCaaS Sales Specialized Test	1.0	Web-based Training
ALCC –2005 Avaya Multiexperience Solutions Sales (ALCC-2005)			
41710W	The Avaya OneCloud™ Contact Center Automated Story	0.50	Web-based Training
41411W	Selling Avaya Oceana®	0.75	Web-based Training
41401W	Selling Avaya Analytics™	0.50	Web-based Training
41481W	Avaya Oceana® ROI for Sales	0.50	Web-based Training
41770W	Avaya Experience Portal and Proactive Outreach Manager (POM) for Sales	0.25	Web-based Training

Table 5: Pre-Sales Design

Course code	Course title	Course duration in hours	Delivery type
ACDS – 3480 Avaya Oceana® Solution Design			
34211W	Avaya Oceana® Overview for Design	0.75	Web-based Training
34811W	Designing the Avaya Oceana Solution Part 1 of 3	1.0	Web-based Training
34821W	Designing the Avaya Oceana Solution Part 2 of 3	1.0	Web-based Training
34831W	Designing the Avaya Oceana Solution Part 3 of 3	1.0	Web-based Training
34801X	Avaya Oceana® Solution Design Exam	1.50	Exam
ALRI-7001 Avaya Oceana® Product Release Information Collection			
39001W	Avaya Oceana® R3.8 with Breeze Snap-ins Details for Pre-Sales	1.0	Portable Document Format (PDF)
39020W	Avaya Breeze® Snap-ins for Avaya Oceana Details for Pre-Sales	1.0	PDF

Table 6: Technical Services Partner Credentials

Course code	Course title	Course duration in hours	Delivery type
ACIS – 7495 Avaya Oceana® Solution Implement			
74150V	Integrating Avaya Oceana® Core and Workspaces	40.0	Virtual Instructor-Led Training
74950X	Avaya Oceana® Solution Integration Exam	1.50	Exam
ACSS-7497 Avaya Oceana®			
74550V	Supporting Avaya Oceana®	24	Virtual Instructor-Led Training
7497X	Avaya Oceana® Support Exam	1.75	Exam
74360W	Installing Avaya Analytics™ for Oceana®	1.5	Web-based Training

Table 7: Pre-requisite Courseware

Course code	Course title	Course duration in hours	Delivery type
77900W	Avaya Control Manager Training Bundle (5 courses 21900W, 77910W, 77920W, 77930W, 77940W)	5.50	Web-based Training
70160W	Avaya Breeze® Implementation and Support	30.0	Web-based Training

Table 8: End User, Programmer, Administration

Avaya Learning Center				
Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Customizing the Avaya Workspaces® Framework	3.0	Web-based Training	
24150T	Avaya Workspaces® Framework R3 Test	1.0	Online Test	
ASAC-0005 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Administering Avaya Oceana® R3 Omnichannel	40.0	Virtual Instructor-Led Training	Attached with the sale
2430T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin

Table continues...

Avaya Learning Center				
Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ASAC-0031 Avaya Analytics™ R4 for Oceana® Administrator				
24380T	Administering Avaya Analytics1M R4 for Oceana8 Specialized Test	1.0	Online Test	

Table 9: Other Miscellaneous Courseware

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ALCC-0001 Avaya Workforce Optimization Select Integration with Avaya Oceana® Workspaces				
7014W	Integrating Avaya Workforce Optimization Select with Avaya Oceana® Workspaces	3.0	Web-based Training	
7014A	Avaya Workforce Optimization Select with Avaya Oceana® Workspaces Integration Assessment	1.0	Assessment	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	

Support

Go to the Avaya Support website at <https://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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.
- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Index

A

accounts	35	attribute sets	34
activating		attributes	34
encryption key	217	auto answer	
Ad hoc email rule	166	user profile template	98
add		Auto answer	99
attribute categories	35	Auto answer timeout	98
attributes	36, 56	auto phrases	178
Avaya Oceana® Server	24	automatic phrases	123
Communication Manager to Avaya Control Manager	19	automation overview	119
Communication Manager to the location	20	Available file types for Facebook media types	134
connectors to Provisioning Server	24	available file types for Twitter media types	137
department	20	available file types for WhatsApp media types	131
extensions	53	Avaya Analytics	
provider	53	authenticate	202
site	20	Avaya Analytics details	
skills	53	configuring	201
team	20	Avaya Aura Contact Center connector	80
VDN	53	Avaya Control Manager	
add authorization client	29	configuration	16
adding		functional buttons	16
agent	86	Avaya InSite Knowledge Base	235
attributes to a user	62	Avaya one-X Agent connector	80
Customer Journey widget	227	Avaya support website	235
group	105	Avaya Workspaces address book	68
reporting users	101	AWE connector	80
transfer to user route points	92		
users	60	B	
adding grants		backup	
Control manager application	29	Omnichannel database	208
Engagement Designer	30	Omnichannel database from a network location	209
to Authorization Service	30	Basic authentication settings	142
adding SSL certificate	206	browser close and network connection issues	99
administering		browser disconnect	115
checklist	14	C	
administrative user	77	categories	34
Alias field descriptions	145	channel exclusivity	94, 96
Analytics server IP address	66	channel exclusivity and interruptibility	96
applying office hours	161	channel interruptibility	95
archive rule	189	channel limits	113
archive scheduled task	189	checklist	
assign		administering	14
location to Application Server	32	send as group	150
location to Synchronizer Service Server	33	transfer to user	91
Serviceability Agents	48	cleanup rule	
assign Ad hoc rule to mailbox	167	channel types	196
assigning		customer	195
groups to a user	106	email rules	194
location to UCA proxy server	32	cloning agent	63
routing groups to a user	104	collection	
associating		delete	231
transfer to user	92		

defragmenting	
Omnichannel database	215
Delete Ad hoc email rule	168
deleting	
customer history	205
data access group	107
users	64
disable polling	153
disposition codes	
configuring	70
Distribution group field descriptions	146
distribution list	
Microsoft Office365	150
document changes	11
documentation center	231
finding content	231
navigation	231
documentation portal	231

E

editing	
data access group	106
users	63
Editing Ad hoc email rule	167
email approval	146
email approval ratios	148
email confirmation	
configuring	224
email signature settings	94
enabling	
connectors	80
transfer to user	91
encrypting	
database	218, 219
encryptings	
database	218, 219
endpoint template	83
error scenarios	221
Experience Portal connector	80
expose additional language pack	226
external widget library	73

F

Facebook pages	115
facebook settings	133
finding content on documentation center	231
finish work confirmation	
enable	226
forward email	
settings	73
functional button descriptions	16

G

general settings	158
group management	104

I

importing identity certificate to AADS	68
inbound emails	164
Interaction Center connector	80
interruptibility	95, 96

K

KB	
Support site	235

L

layouts	110
LDAP	
address book	68
log in to Avaya Control Manager	18
logging	174
login	78

M

mail approval	147
Mail Store field descriptions	143
managing layouts	111
messaging connector	80
MS graph	174
multiple replies	
settings	73

N

new thresholds	
creating	108

O

Oceana administrator	
Control Manager	58
Oceana Customer Management Tool	45
Oceana Data Management	194
Oceana role	58
Oceana server URL	27, 41
Oceana user	58
office 365 certificates	171
Office365	
throttling policy	150
OFFLINE database	189
Omnichannel Administration Utility	45, 120
outbound email	146

overview	12, 13
customer privacy	201
defragmentation	214

P

page push URL	179
Page Push URL	123
personal certificates pools for breeze authorization	32
Proactive Contact connector	80
proficiency levels	118
providers	35
purging	
OFFLINE database	198

R

real-time reporting	64, 66
rejection codes	72
related documentation	229
removing expired SSL certificate	207
repeat	
customer deletion	206
reporting access	
Avaya Workspaces users	102
reserve agents	97
reserve-level threshold	97
restart	
CallServerConnector service	57
restore	
Omnichannel database to a network location	212
restoring	
contacts	199
Omnichannel database	210
root certificate	26, 39
routing service groups	103
assigning to a user	104
routing services groups	103

S

scheduling	
backup	212
screenpops	
configuring	88
searching for content	231
searching users	62
send as group	149
sender groups	163
service-level threshold	97
Session Manager connector	80
sharing content	231
Short Not Ready	
configuring thresholds	109
SMGR root certificate	27, 40
sort documents	231

start work button	
behavior	227
starting	194
Streams server IP address	64
supervisor reporting dashboard	64, 66
user management	100
support	235
synchronization	21
system delivery failure rule	157
System Manager	29, 78–80
System Manager connector	80

T

test	
UCA REST connection	34
threshold	
configuring	108
measures	109
thresholds	97, 107
timer in ED	93
toast notifications	
configuring	226
token enforcement in UCA	31
training	232
transfer to service	
configuring	90
transfer to user for VDN and ED flow	92
twitter settings	136

U

UCA proxy connector	80
user configuration	55
user permissions	78
user profile template	
assigning	99
users	35

V

verify	
configuration	48
verifying	
Transfer to Service list	223
viewing	
backup history	214
defragmentation history	216

W

watchlist	231
web chat settings	125
Web Chat Settings field descriptions	125
Web On Hold comfort groups	121
web service	76

WhatsApp numbers	115
whatsppp setting	130
work codes	
configuring	70
Work Codes	46 , 69