Deploying Avaya Workforce Optimization Select

Release 5.0.2.1
Issue 2
May 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

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

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Regulatory Statements

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 Inc.

Contents

Chapter 1: Introduction

Purpose

This document contains the checklist and procedures for the installation, configuration, initial administration, and basic maintenance of Avaya Workforce Optimization Select.

Prerequisites

Before deploying Avaya Workforce Optimization Select, ensure that you have the following knowledge, skills, and tools:

Knowledge

- Spanning or Port Mirroring
- Depending on the Avaya Telephony Platforms, Automatic Call Distribution, and Dialer you choose for your deployment, you must have knowledge on the following:
  - Avaya Telephony Platforms such as Application Enablement Services, IP Office 9.x, IP Office 10.x, Communication Manager, and Avaya Communication Server 1000 (CS 1000)
  - Automatic Call Distribution such as Avaya Aura® Contact Center, Avaya Contact Center Select, IP Office Contact Center, Avaya Aura® Call Center Elite, and Avaya Oceana™ Solution
  - Dialers such as Avaya Proactive Contact with CTI.

Skills

- How to execute SQL scripts and queries.
- How to validate logs.
- How to run switch commands for spanning or port mirroring.

Tools

- Wireshark
- Notepad ++
- TSAPI test
- MIB Browser

Chapter 2: Avaya Workforce Optimization Select overview

Avaya Workforce Optimization Select is a web-based suite of tightly integrated tools, designed to enhance and improve all aspects of your contact center operations and performance. The solution is easy to implement, maintain, and manage in a variety of contact center deployment models from centralized contact centers to distributed branches and work-at-home agents. Avaya Workforce Optimization Select offers contact centers the ultimate workforce optimization functionality and flexibility.

It is a comprehensive solution that provides contact center staff and businesses with scalable applications that synchronize and unify the entire workforce, regardless of VoIP architecture.

Avaya Workforce Optimization Select has sophisticated yet easy-to-use monitoring, recording, quality assurance, reporting, and analytic features. It provides contact center management and agents alike with all the tools necessary to effectively manage the entire agent life cycle process.

Components

Name	Description
Log Manager	Collects and zips log data into a single zip file to debug issues and fetches packet dumps from the Packet Sniffer component. You can configure the period for which you want to maintain the zipped files.
Media Manager	Manages media files for conversion, encryption, storage, video generation, download, and compression. Media manager comprises of the following components: • Converter: Retrieves audio recordings that are in G.711, G722, and G.729 codec from storage and converts them to browser media player-friendly formats such as WAV/MP4/MP4a. The conversion is done based on the call codec or mixed codec call recorded. • Encryption Decryption (ED) Service: Encrypts and decrypts recorded calls. Recorder sends a message to ED Service to encrypt and move the call to local storage. From the 256–bit keys, ED Service randomly selects one key and encrypts the call. The

Table continues…

Name	Description
	pass phrases used for generating the keys are stored in an encrypted format in the database. ED Service zips the `fwd`, `bwd`, and `inf` files into one compressed file and screens into another compressed file. Then ED Service encrypts these compressed files. • Storage Manager: Archives, copies, moves, compress, and deletes calls and screens across physical locations. You can define storage rules as per your requirements. For example, you can specify retention periods, storage locations, clients, sites, groups, employees, ANI number, DNIS number, call duration, and call hold duration. • Video Generator: Processes requests to download calls with screens in MP4 and M4a (only audio without screens) format. The component checks for requests in the database, processes the same by mixing both audio and video files, and then saves them for download in MP4 format. • G729 Compressor: Retrieves G.711 and G.722 calls from storage and compresses them to G.729 format to reduce storage size.
Messaging	Acts like a proxy between the Recorder and Screen component. The Recorder directly interacts with the Messaging component which in turn checks for bandwidth availability and accordingly processes screen requests. Integrates with Customer Relationship Management (CRM) applications to receive different types of HTTP events. The component captures additional customer information such as Credit Card details and passes the information to the Recorder for processing.
Process Checklist	Monitors all components and checks if the processes are running. Process Checklist sends appropriate alerts and restarts the services that are not running.
Packet Sniffer	Sniffs Network Interface Card (NIC) data and saves them as files for debugging. Packet sniffer writes all the received packets into local files along with a timestamp. You can limit the storage consumed by specifying the file size and the number of files before wrapping. You can also upload the sniffed packets to a central location.
Recorder	Records interactions based on events received from RTP and CTI information. Recorder supports recording up to 450 concurrent G. 711 calls. The recorder uses adapters to receive signaling and media from phones. The recorder receives Automatic Call Distribution (ACD) information from other Avaya Workforce Optimization Select components.
Web Application	Provides an interface that allows users to monitor live interactions, playback recorded interactions, perform quality evaluations on agent interactions, and supports quiz, coaching, and report functionalities.

Table continues…

Name	Description
SysAdmin	Provides an interface to manage tenants, configure parameter values for components and adapters, and monitor alerts.
Screen Capture	Runs on Agent desktop and captures screens during an interaction. Screens are uploaded to the server and tagged to an interaction.
Adapters	Connects the Avaya Automatic Call Distributors to Avaya PBXs to provide voice streams, call signaling, dialer, and agent information. Different adapters are used in the respective Avaya Workforce Optimization Select deployment configurations. The Avaya Workforce Optimization Select Recorder receives data from the adapters and annotates the interaction entries in the database along with the metadata.

Adapters

Adapters connect Avaya Automatic Call Distributors to Avaya PBXs to provide voice streams, call signaling, dialer, and agent information.

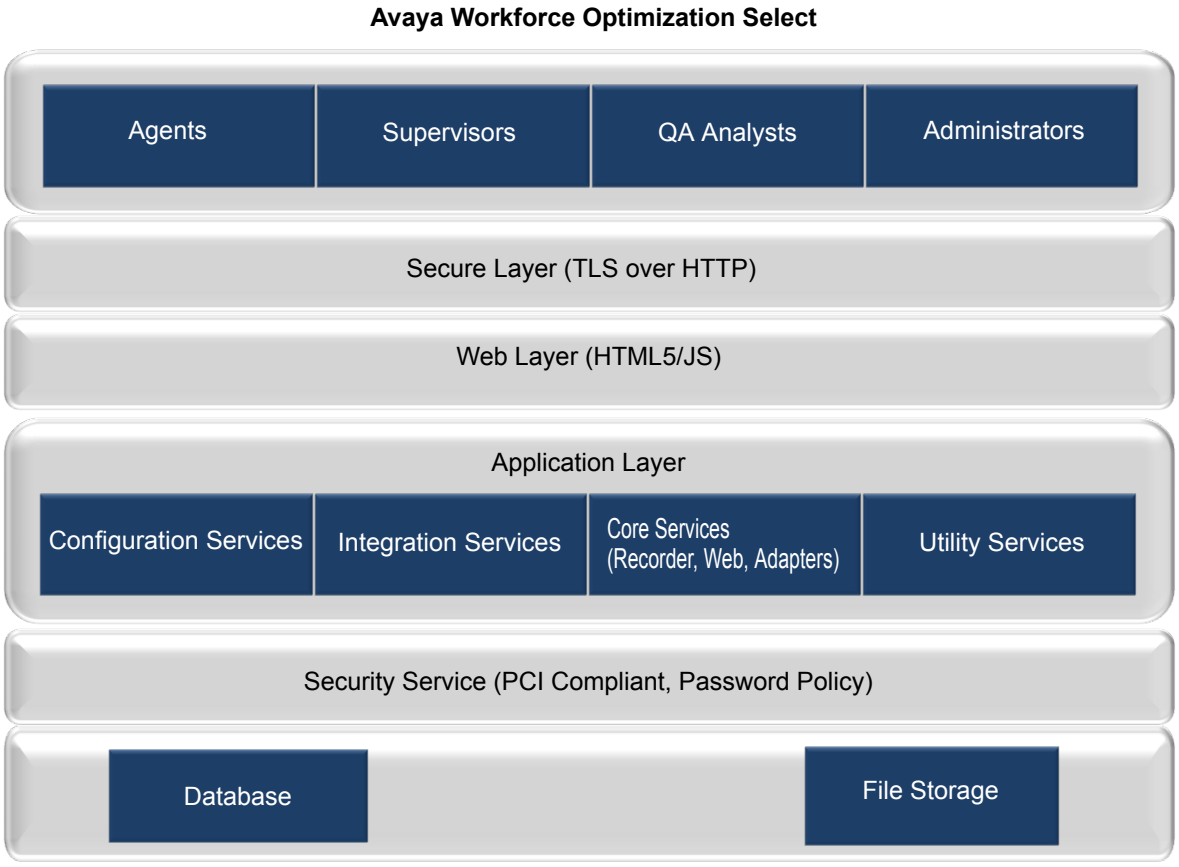
	Description
Avaya adapter	Used to connect to • Communication Manager through AES server using the Device Media and Call Control (DMCC) interface to receive voice streams and send voice streams to the Recorder. • Avaya Communication Server 1000 through Avaya Aura® Contact Center using the MLS interface to receive and send call signaling and voice streams to the Recorder. • IP Office Contact Center to receive and send agent information and business data to the Recorder.
AES adapter	Used to • Connect to Communication Manager through AES server using TSAPI events to receive and send call signaling to the Recorder. • Monitor skill or hunt groups in Avaya Aura® Call Center Elite environment. When an agent logs in or logs out from a skill or hunt group, AES adapter sends agent-extension association information to the Recorder. AES adapter starts monitoring call events for the extensions configured.
AACCNet adapter	Used to connect to Avaya Aura® Contact Center and Avaya Contact Center Select to receive and send agent information and business data to the Recorder.
TAPI adapter	Used to connect to Avaya IP Office server to send call signalling information to Recorder using TAPI API. TAPI adapter provides the

Table continues…

	Description
	interface between computer telephony applications and telephony services.
PCS adapter	Used to connect to Avaya Proactive Contact with CTI to fetch ACD data for agents assigned for outbound calls and send agent information and business data to the Recorder. Integrates with Avaya Proactive Contact through event services APIs to send dialer information, call signalling, and agent information to the Recorder.
Devlink3 adapter	Used to connect to Avaya IP Office server to send call signalling and agent information to Recorder. Devlink3 adapter establishes a TCP channel with Avaya IP Office using Devlink3 protocol and receives events from Avaya IP Office.
SIP adapter	Used to connect to Avaya IP Office server to receive voice streams and send voice streams to the Recorder. Devlink3 adapter adapter sends requests to Avaya IP Office for RTP information and SIP adapter IP address. Avaya IP Office establishes a SIP channel between Avaya IP Office and SIP adapter and forks stream to SIP adapter.
Oceana adapter	Used to connect to Avaya Oceana™ Solution to receive and send agent information and business data to the Recorder.

Topology

The following diagram shows the high-level topology for deploying Avaya Workforce Optimization Select:



Deployment configurations

Avaya Workforce Optimization Select supports the following deployment models:

- Single site, single server
- Single site, multiple servers
- Multiple sites, multiple servers

Avaya Workforce Optimization Select scales from single site environments to distributed multisite enterprises. Avaya Workforce Optimization Select also supports multiple accounts across multiple site configuration models where recorded interactions are stored at individual sites or a central repository.

Single Site, Single Server

In a single site deployment model, all users are located within the same physical location. A typical single site, single server deployment implements all the necessary components such as storage, database, application, and recording servers using one server. This deployment is cost-effective for organizations with limited hardware budgets.

The single site, single server deployment contains a single server where all necessary components are installed. Components for recording, monitoring, web application, database, storage, and reporting are all plugged into the network's data switch. Voice traffic is captured in the server through port spanning and switch configuration. You can capture interactions between agents and customers. If needed, you can also monitor agent-to-agent conversations by spanning each individual agent phone to Avaya Workforce Optimization Select.

Single Site, Multiple Servers

A single site, multiserver deployment can accommodate as many users as required by distributing the server components across multiple physical servers. Typically, separate physical servers exist for the application, database, and recording components.

In a single site, multiple servers deployment model, the Avaya Workforce Optimization Select server is linked to the data switch of the network through the Voice NIC configured on the server. The switch is configured to copy all voice traffic to the Avaya Workforce Optimization Select server through the use of port spanning.

Multiple Sites, Multiple Servers

In a multiple sites, multiple servers deployment model:

- Agents are spread across multiple geographical locations.
- Multiple instances of recording, monitoring, and storage services are installed to scale to handle larger number of agents.
- Only one instance of the web application and database is installed.
- All the services are split and deployed across multiple physical server spread across multiple geographical locations.

The number of agents that a multisite environment can handle depends on the underlying network infrastructure such as routers used and available bandwidth.

Signaling events

Avaya Workforce Optimization Select supports different Avaya environments for recording interactions. However, the primary requirement for any environment is to capture signaling events. You can successfully trace every interaction if you capture the following signaling events:

- Call signaling events
- Media stream events
- Automatic Call Distribution (ACD) signaling and external call variables to tag interaction to agents as per business rules
- PBX and ACD link status that provides status about connectivity of adapters to server.

Call signaling

Call signaling triggers the following events:

- Offhook event gets triggered when the phone goes off hook and a dial tone is heard.

- Connected event gets triggered when the call is answered.
- Hold event gets triggered when the agent puts the call on hold.
- Resume event gets triggered when the agent resumes the on-hold call.
- Onhook event gets triggered when the receiver is put down or when the call ends.
- Transfer Info event gets triggered when the agent does a blind or consultation transfer to a supervisor or another agent. The recorder receives the event from the adapter.
- Conference Info event gets triggered when the agent starts a conference between a customer and a supervisor or another agent. The recorder receives the event from the adapter.
- RTP Started Info event provides information about the IP address and ports of the local and remote phones to the recorder.
- Phone extension information is sent to the recorder by adapter to provide IP phone extension mapping.
- Call information is sent to the recorder by adapter to provide called party, calling party, and call direction.
- Voice stream information is sent to the recorder by adapter to provide media end point information.
- SNMP events for getting IP address in SPAN based recording.

ACD signaling and external call variables

The Avaya Workforce Optimization Select recorder needs the agent information and external call variables to tag an interaction with the agent who is handling the interaction. The recorder tags each interaction with the business data that the agent enters in the desktop tools for each interaction. Agent login, agent logout, ACD information or extended call info, and wrapup data are the events that the recorder tags.

Link status

Link status provides information about the connectivity status of connectors or adapters with their respective servers. There are signalling events that capture and process the link status to inform if the PBX and ACD link is functional.

Passive recording

Passive recording is a recording method used for IP recording deployments to capture voice transmission or RTP through a network spanning configuration also known as port mirroring. The call events and RTP stream are mirrored directly to the recording server. However, the network switch must support port mirroring capabilities. There are no additional PBX licenses required. IP recording or passive recording cannot be used for analog or digital extension.

Avaya Workforce Optimization Select recorder uses SPAN to get voice and adapter to get call signaling and agent information.

Active recording

Active recording, also known as Conference Mode Recording, conferences the agent call to the recording server. The recording system captures voice transmission by integrating with specific PBX models. You might need to get additional PBX licenses. Active recording does not require port mirroring and supports end points such as analog or digital.

Avaya Workforce Optimization Select uses PBX to get voice streams and passes the voice streams to the recorder for recording an interaction. Avaya Workforce Optimization Select uses adapter to get agent information and call signaling.

Avaya Workforce Optimization Select allows call recording for Voice, Digital, or Analog stations.

DMCC single-step conference and multiple registration

Single-step conference

The Avaya Workforce Optimization Select uses the AES Device Media Call Control (DMCC) service to register a pool of standalone recording devices. The application uses the AES TSAPI service to monitor the target extension for Established Call events. Whenever the extension joins a call, an Established Call event occurs that triggers the application to use the Single Step Conferencing method to add a recording device to the call. The application receives the call RTP media stream through the recording device and records the call.

Multiple registration

The Avaya Workforce Optimization Select uses the AES Device Media Call Control (DMCC) service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call RTP media stream through the recording device and records the call. Information about the call is derived from the Established event that is generated when the target extension joins the call.

Recording Tone

Recording Tone is a feature that inserts a tone in the audio stream to indicate that a call is being recorded.

The Recording Tone feature is available in the following Avaya Workforce Optimization Select deployments:

- Avaya Aura® Contact Center on Communication Manager active recording
- Avaya Aura® Contact Center on Avaya Communication Server 1000 active recording
- Avaya Aura® Call Center Elite on Communication Manager active recording
- Avaya Aura® Call Center Elite on Communication Manager and Avaya Proactive Contact with CTI active recording
- IP Office 10.x extension based active recording
- Avaya Contact Center Select on IP Office 10.x active recording
- IP Office Contact Center on IP Office 10.x active recording

Integration scenarios

Avaya Workforce Optimization Select supports integration with the following Avaya products:

Avaya Aura® Contact Center

Avaya Workforce Optimization Select integrates with Avaya Aura® Contact Center to offer a comprehensive suite of scalable solutions for dynamic contact center environments. AACC integrates with Avaya Workforce Optimization Select to offer voice, email and web chat only.

Avaya Contact Center Select

Avaya Contact Center Select uses the Avaya IP Office telephone system to provide a real-time telephony platform. IP Office is a flexible and scalable phone system designed specifically for small and midsize enterprises. IP Office supports a wide range of phones and devices for use in contact centers.

Avaya Contact Center Select uses SIP and CTI interfaces to communicate with the IP Office platform. The Avaya Workforce Optimization Select integration gives Avaya Contact Center Select access to and control of a wide range of IP Office phones and features. Customers integrating Avaya Contact Center Select with the IP Office platform gain skill-based routing.

IP Office Contact Center

IP Office Contact Center is part of the Avaya Contact Center Solutions for the IP Office portfolio. IP Office Contact Center is a fully integrated contact center specifically built for IP Office and its addressable market. IP Office Contact Center is scalable to meet the market needs of IP Office customers requiring skills-based routing, call recording, and multichannel such as chat and email.

Avaya Workforce Optimization Select integration with IP Office Contact Center is a complete customer interaction suite consisting of call recording for all agents, skills-based routing, and voice, email, and chat multichannel capabilities including historical and real time reporting.

Avaya Aura® Call Center Elite

Call Center Elite is the Avaya flagship voice product for assisted experience management. The product coresides with Avaya Aura® Communication Manager, which is a key component of the Avaya Aura® communications platform. Call Center Elite integrates with the Avaya Workforce Optimization Select to offer voice only.

Avaya Oceana™ Solution

Avaya Oceana™ Solution is the next generation customer engagement solution. Enterprises can use Avaya Oceana™ Solution to seamlessly handle Voice, Web and Mobile Chat, WebRTC Voice, Email, Simple Messaging, and Social Media channels using a single intelligent attribute-based call routing through a unified Agent Desktop. Avaya Oceana™ Solutionis integrates with the Avaya Workforce Optimization Select to offer voice, email, and chat capabilities.

Avaya Aura® Communication Manager

Communication Manager is the open, highly-reliable and extensible IP Telephony foundation on which Avaya delivers Unified Communications solutions to large and small enterprises. The product delivers rich voice and video capabilities and provides for a resilient, distributed network of gateways and analog, digital and IP-based communication devices. Communication Manager includes advanced mobility features, built-in conference calling and contact center applications, and E911 capabilities.

Avaya Communication Server 1000

Avaya Communication Server 1000 (CS 1000) is a server-based, fully-featured IP PBX. It provides the benefits of a converged network, advanced applications, and over 750 call processing and telephony features. The product provides a rich set of interfaces that enable third party applications to access its call data and communications capabilities.

IP Office

IP Office is Avaya's global midsize solution for enterprises, supporting up to 3,000 users at a single location with IP Office Select editions. For businesses with multiple locations, the product provides a powerful set of tools to help streamline operations, centralize management, and reduce total cost of ownership for converged networks. Apart from basic telephony services and voicemail, IP Office includes a robust set of tools for administration, call tracking, and system monitoring and diagnostics.

Avaya Proactive Contact with CTI

The Avaya Proactive Contact solution is a suite of hardware and software products that facilitates proactive and opportunistic management of customer relationships within a contact center. With the Avaya Proactive Contact solution, you can reach your customers at the lowest possible cost per call, irrespective of whether a calling mission requires an inbound, outbound, or blended solution.

Avaya Workforce Optimization Select integration with Avaya products

Note:

None of the deployments support SRTP.

Avaya Workforce Optimization Select on Communication Manager

Deployments	Automatic Call Distributor	Recording type	Voice stream events	Call signaling	Agent login information	Business call variables	Dialer information
Avaya Aura® Contact Center on Communication Manager	AACC	Active	Avaya adapter	AES adapter	AACCNet adapter	AACCNet adapter	
		Passive	SPAN	AES adapter	AACCNet adapter	AACCNet adapter	
Call Center Elite on Communication Manager	Call Center Elite	Active	Avaya adapter	AES adapter	AES adapter	AES adapter	
		Passive	SPAN	AES adapter	AES adapter	AES adapter	
Call Center Elite on Communication Manager and Avaya Proactive Contact with CTI	Call Center Elite and Avaya Proactive Contact with CTI	Active	Avaya adapter	AES adapter	AES adapter	AES adapter for Elite calls. PCS adapter	PCS adapter

Table continues…

Deployments	Automatic Call Distributor	Recording type	Voice stream events	Call signaling	Agent login information	Business call variables	Dialer information
						for PC calls.	
		Passive	SPAN	AES adapter	AES adapter	AES adapter for Elite calls. PCS adapter for PC calls.	PCS adapter
Avaya Proactive Contact with CTI on Communication Manager		Active	Avaya adapter	AES adapter	PCS adapter	PCS adapter	PCS adapter
		Passive	SPAN	PCS adapter	PCS adapter	PCS adapter	PCS adapter

Avaya Workforce Optimization Select on Avaya Communication Server 1000

Deployments	Automatic Call Distributor	Recording type	Voice stream events	Call signaling	Agent login information	Business call variables	Dialer information
Avaya Aura® Contact Center on Avaya Communication Server 1000	AACC	Active	Avaya adapter	Avaya adapter	AACCNet adapter	AACCNet adapter	
		Passive	SPAN	Avaya adapter	AACCNet adapter	AACCNet adapter	

Avaya Workforce Optimization Select on IP Office

Deployments	Automatic Call Distributor	Recording type	Voice stream events	Call signaling	Agent login information	Business call variables	Dialer information
IP Office 9.x extension based recording		Passive	SPAN	TAPI adapter			
Avaya Contact Center Select on IP Office 9.x	Avaya Contact Center Select	Passive	SPAN	TAPI adapter	AACCNet adapter	AACCNet adapter	

Table continues…

Deployments	Automatic Call Distributor	Recording type	Voice stream events	Call signaling	Agent login information	Business call variables	Dialer information
IP Office Contact Center on IP Office 9.x	IP Office Contact Center	Passive	SPAN	TAPI adapter	Avaya adapter	Avaya adapter	
IP Office 10.x extension based recording		Active	SIP adapter	Devlink3 adapter			
		Passive	SPAN	Devlink3 adapter			
Avaya Contact Center Select on IP Office 10.x	Avaya Contact Center Select	Active	SIP adapter	Devlink3 adapter	AACCNet adapter	AACCNet adapter	
		Passive	SPAN	Devlink3 adapter	AACCNet adapter	AACCNet adapter	
IP Office Contact Center on IP Office 10.x	IP Office Contact Center	Active	SIP adapter	Devlink3 adapter	Avaya adapter	Avaya adapter	
		Passive	SPAN	Devlink3 adapter	Avaya adapter	Avaya adapter	

Avaya Oceana™ Solution on Communication Manager

Deployments	Automatic Call Distributor	Recording type	Voice stream events	Call signaling	Agent login information	Business call variables	Dialer information
Avaya Oceana™ Solution on Communication Manager with Call Center Elite	Avaya Oceana™ Solution	Active	Avaya adapter	AES adapter	Oceana adapter	Oceana adapter	
		Passive	SPAN	AES adapter	Oceana adapter	Oceana adapter	

Agent profiles

Based on the signaling event, the recorder tags an interaction with the agent ID or extension. Skill calls are assigned to an agent ID, whereas extension or directory number (DN) calls are assigned to an extension. When an agent takes a call by logging into the phone, the call gets assigned to the agent ID. If an agent takes calls on an extension or DN without logging into the phone, the call gets assigned to the extension.

You can configure agent profiles for fixed seating and free seating in Avaya Workforce Optimization Select. For more information on how to configure agent profiles for fixed and free seating, see *Administering Avaya Workforce Optimization Select.*

Fixed Seating

In a fixed seating environment, an agent is allocated an extension. The agent can log in to only that extension with the individual agent ID. To implement fixed seating in Avaya Workforce Optimization Select, the Voice Settings for an employee profile must have the extension or DN.

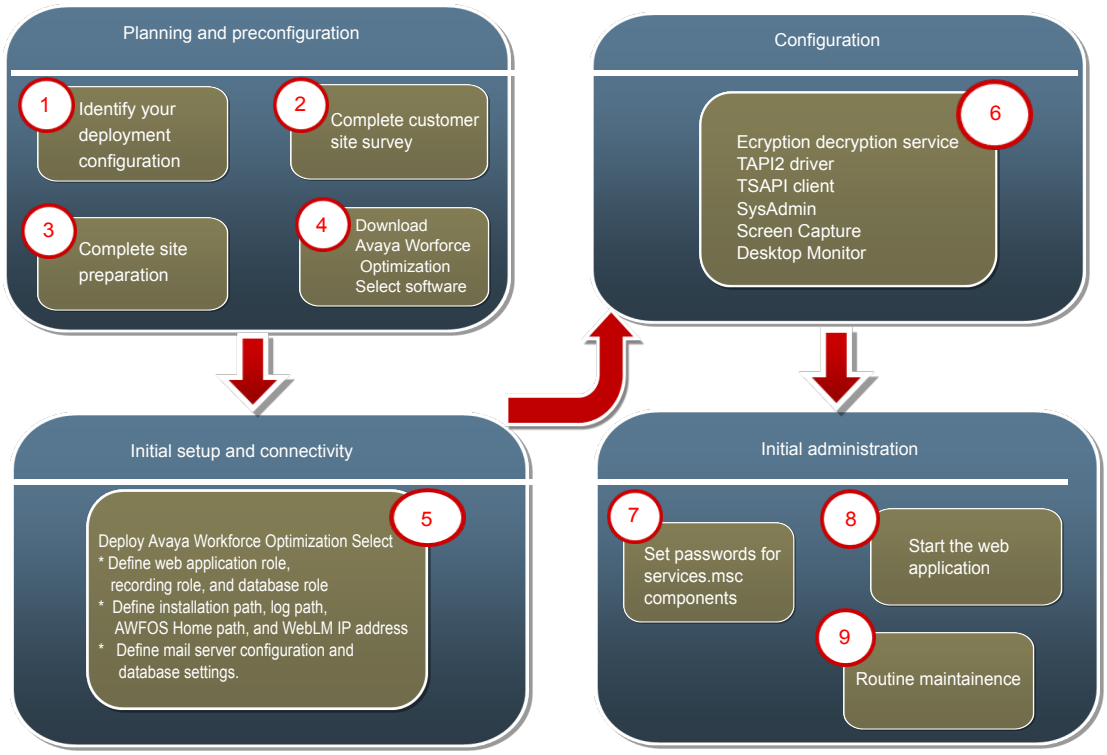
Free Seating

In a free seating environment, an agent can log in to any extension using the individual agent ID. To implement free seating in Avaya Workforce Optimization Select, you must have two employee profiles and the Voice Settings must specify the following:

- The agent ID in one of the employee profiles
- The extension or DN in the other employee profile

Chapter 3: Deployment process

The following image shows the high-level tasks for deploying Avaya Workforce Optimization Select :



Chapter 4: Planning and preconfiguration

Planning checklist

No.	Task	Reference	Notes	✔
1	Download the required documentation.	See Documentation on page 137.		
2	Gather configuration information.	See Configuration information for Avaya Workforce Optimization Select installation on page 24.		
3	Gather configuration information for initial administration of Avaya Workforce Optimization Select .	See Configuration information for initial administration of Avaya Workforce Optimization Select on page 27.		
4	Plan for site preparation.	See Site preparation checklist on page 28.		

Key customer configuration information

Configuration information for Avaya Workforce Optimization Select installation

To maintain a record of the Avaya Workforce Optimization Select installation information, take a printout of the following table and work with your network administrator to fill the empty cells:

Web server details

Name	Value	Description
Server IP address		The IP address of the server where Avaya Workforce Optimization Select is installed.

Table continues…

Name	Value	Description
Server Hostname		The hostname of the server where Avaya Workforce Optimization Select is installed.
Avaya Workforce Optimization Select Operating System Domain/Login		The login credentials of the user who has administrator privileges on the server where Avaya Workforce Optimization Select is installed.
Avaya Workforce Optimization Select Operating System Password		The password of the user who has administrator privileges on the server where Avaya Workforce Optimization Select is installed.
Avaya Workforce Optimization Select Services Account Domain/ Login		The username of the user whose default sender email address is configured.
SMTP Server IP address or Hostname		The IP address or the hostname of the email exchange server.
Default Sender Email Address		The default sender email address that is used to send emails related to alerts and notifications triggered by the web application and Avaya Workforce Optimization Selecto components.
Default Sender Name		The name of the user that appears in the **From** list of the email.

SysAdmin server details

Name	Value	Description
SMTP Server IP address or Hostname		The IP address or the hostname of the email exchange server.
SMTP port		The SMTP port number.
Default Sender Email Address		The default sender email address that is used to send emails related to alerts and notifications triggered by the web application and Avaya Workforce Optimization Selecto components.
Default Sender Name		The name of the user that appears in the **From** list of the email.
SNMP Server IP address or Hostname		The IP address or the hostname of the system where MIB browser is installed to get SNMP traps. The IP address is configured as NMS server IP address in SysAdmin.
SNMP port		The NMS server port number.

Database server details

Name	Value	Description
Database Name		The name of the database that points to the Web application and Avaya Workforce Optimization Select components. By default the AWFOSDB

Table continues…

Name	Value	Description
		appears while installing Avaya Workforce Optimization Select. However, you can edit the database name.
Database Server IP address or Hostname		The IP address or hostname of the server where the database is installed.
Database User ID		The user ID of the database to connect to the SQL server. You can only use `sa` as the user ID.
Database Password		The password of the database to connect to SQL server. You can configure a password as suggested by the customer.
Authentication mode		The type of authentication modes. You can choose either: • Windows: The windows authentication credentials of the user to install the database. • SQL: The option to connect to the database or login as the database administrator using `sa` credentials.

Recording server details

Name	Value	Description
Server IP address		The IP address of the server where recorder is installed.
Server Hostname		The hostname of the server where recorder is installed.
Avaya Workforce Optimization Select Recorder Operating System Domain/Login		The login credentials of the user who has administrator privileges on the server where recorder is installed.
Avaya Workforce Optimization Select Recorder Operating System Password		The password of the user who has administrator privileges on the server where recorder is installed.
Sever Voice NIC IP address		The IP address of the server where voice NIC is configured for SPAN-based recording.

Storage details

Name	Value	Description
Directory/Path		The location path on the server where calls must be stored. **Note:** If Network Attached Storage (NAS) or Storage Area Networks (SAN) is configured, you must mount the location path to the local server.

Configuration information for initial administration of Avaya Workforce Optimization Select

License management

To maintain a record of the Avaya Workforce Optimization Select administration information, print the following table and work with your network administrator to fill the empty cells:

Name	Value	Description
WebLM user ID		The administrator user ID to access WebLM.
WebLM password		The administrator password to access WebLM.
WebLM IP address		The IP address of the server on which WebLM is installed.

Assigning metrics to Network Interface Cards

About this task

Metrics are assigned to network interface cards (NICs) when the routing table contains multiple routes for the same destination. For a FQDN based installation with multiple NICs, assign a metric value higher than 10 to set priority to get the data NIC IP address.

Note:

Ensure that you do not assign a metric value to the data NIC.

Procedure

1. Log in to the server where the Recorder is installed.
2. Click **Start** > **Control Panel** > **Network and Sharing Center**.
3. Click **Change adapter settings**.
4. Right-click the network adapter on which the voice traffic comes.
5. Click **Properties**.
6. Double click the Internet Protocol Version 4 (TCP/IPv4).
7. Click the **Advanced** tab period.
8. Clear **Automatic Metric.**
9. In the **Interface Metric** field, enter a value higher than 10.
10. Click **OK**.
11. Click **OK**.

Configuration tools and utilities

- One or more Windows servers or virtual machines with the following:
  - A user with administrator privileges.
  - An SQL server with Mixed Mode Authentication and SQL server agent service enabled.
- Two network interface cards, one for data NIC and another for voice NIC.
- Agent or client machines to install client applications such as Desktop Trigger and Home Agent Screen.

Site preparation

Site preparation checklist

No.	Task	Reference	✔
1	Obtain the Avaya Workforce Optimization Select software.	See Downloading software from PLDS on page 32.	
2	Install the mandatory third party utilities such as Wireshark, WinPCap, 7 Zip, Open JDK, Microsoft Visual C++ 2010 Redistributable Package (x86) 32–bit, and Microsoft Dot Net Framework 32–bit version. Notepad ++ is an optional third party utility that you can install to analyze and troubleshoot log files.	See Required software for Avaya Workforce Optimization Select on page 29.	
3	Download Java security files to `C:\Program Files\Java\JDK8u122\jre8\lib\security`.	See Required software for Avaya Workforce Optimization Select on page 29.	
4	Set environment variables for Java. If you are installing the Avaya Workforce Optimization Select application on Windows 2008 R2 server, add environment variables for Java path.	See Setting environment variables for Java on page 33.	
5	Ensure that network considerations are met.	See Network requirements on page 34.	
6	Enable ports based on your specific deployment configuration.	See Port assignments on page 35.	
7	Ensure that all pre-installation requirements are met.	See Preinstallation checklist on page 35.	
8	Obtain the license types required for your specific deployment configuration.	See the “Licensing Requirements” chapter in	

Table continues…

No.	Task	Reference	✔
		Avaya Workforce Optimization Select Overview and Specification.	

Downloading software

Required software for Avaya Workforce Optimization Select

Table 1: Avaya Workforce Optimization Select software

Software	Supported version	Notes
Avaya Workforce Optimization Select	5.0, 5.0.1, 5.0.2	-

Table 2: License management

Software	Supported version	Notes
Avaya WebLM	6.3.8 and above	-

Table 3: Operating systems and software

Software	Supported version	Location	Reference
Windows Server	2008 R2, 2010, and 2012 (64–bit OS)	-	-
OpenSSL	Win32 OpenSSL v1.0.2h **Note:** Do not download OpenSSL version 1.1x. Use only the latest 1.0.2x versions.	Download OpenSSL from https://slproweb.com/products/Win32OpenSSL.html If the library is updated (the last character gets updated in the filename), use the latest one available at the same site.	See Setting environment variables for OpenSSL on page 34.

Table 4: Database

Software	Supported version	Notes
SQL Server	2012/2016 Standard Edition	

Table 5: Reporting services

Software	Supported version	Notes
Adobe Reader	8.0 or later	-

Table 6: Client software

Software	Supported version	Notes
Windows Operating System	7 and 8 with 32–bit and 64–bit	-
Internet Explorer	11	-
Mozilla FireFox	42	-
Google Chrome	46	-
Citrix or terminal services	• Citrix 7.5 • Terminal services on Windows server 2008 and 2012	-
HTML 5 media player	NA	-
Graphic and sound card	Depends on compatibility with customer site.	-

Table 7: Third party software

Utilities	Supported versions	Location	Reference
Wireshark	2.2.3 Windows 64–bit	Server on which the recorder is installed. For example, `C:\Program Files\WireShark`. Download Wireshark software from https://www.wireshark.org/download.html. **Note:** While installing Wireshark, selecting the option to install WinPCap installs both Wireshark and WinPCap.	
WinPCap	4.1.3	Server on which the recorder is installed. For example, `C:\Program Files(x86)\WinPCap`.	
Notepad++	Latest version	All servers.	
7 Zip	Latest version	All servers.	
Open JDK	8u122 64–bit Windows	Server on which the Avaya Workforce Optimization Select application is installed. For example, `C:\Program Files\Java(64-bit)`. Open JDK software download link at https://jdk8.java.net/download.html If the library is updated (the last character gets updated in the filename), use the latest JDK 8 updates available at the same site. The recommended Java package to download is JDK 8u122. You can download the latest Java package, provided it is JDK 8.	See Setting environment variables for Java on page 33.

Table continues…

Utilities	Supported versions	Location	Reference
Java security files		Download Java security files `local_policy.jar` and `US_export_policy.jar` from http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html. **Note:** You do not have to download and install Java security files if you are installing a JDK version that is greater than 8u76. The Java security files are embedded in the JDK versions greater than 8u76. Extract the `jce_policy-8.zip` file and place Java security files `local_policy.jar` and `US_export_policy.jar` files in the `C:\Program Files\Java\JDK 8u122\jre\lib\security` folder.	See Setting environment variables for Java on page 33.
Microsoft Visual C++ 2010 Redistributable	Microsoft Visual C++ 2010 Redistributable Package (x86) 32–bit.	Server on which the PCS adapter is installed. Download the redistributable from the location https://www.microsoft.com/en-us/download/details.aspx?id=5555.	
Microsoft Dot Net Framework	32–bit version	Server on which the Avaya Workforce Optimization Select application is installed. **Note:** The PCS adapter service is not installed without Microsoft Dot Net framework.	

Registering for PLDS

Procedure

1. Go to the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

   The PLDS website redirects you to the Avaya single sign-on (SSO) webpage.
2. Log in to SSO with your SSO ID and password.
3. On the PLDS registration page, register as:
   - An Avaya Partner: Enter the Partner Link ID. To know your Partner Link ID, send an email to prmadmin@avaya.com.
   - A customer: Enter one of the following:
     - Company Sold-To
     - Ship-To number

- License authorization code (LAC)

4. Click **Submit**.

   Avaya sends the PLDS access confirmation within one business day.

Downloading software from PLDS

About this task

Note:

You can download product software from http://support.avaya.com also.

Procedure

1. In your web browser, type http://plds.avaya.com to go to the Avaya PLDS website.
2. Enter your Login ID and password to log on to the PLDS website.
3. On the Home page, select **Assets**.
4. Select **View Downloads**.
5. Search for the available downloads by using one of the following:
   - An application type and the version number
   - Download name
6. Click the download icon from the appropriate download.
7. When the system displays the confirmation box, select **Click to download your file now**.
8. If you receive an error message, click the message, install Active X, and continue with the download.
9. When the system displays the security warning, click **Install**.

   When the installation is complete, PLDS displays the downloads again with a check mark next to the downloads that have completed successfully.

Product compatibility

Avaya Workforce Optimization Select Release 5.0.2 supports the following versions of Avaya products:

Product/Application name	Supported versions
Avaya Aura® Contact Center	• 6.4.2 • 7.0
Avaya Contact Center Select	• 6.4.2 • 7.0.1
Communication Manager	• 6.3 • 7.0

Table continues…

Product/Application name	Supported versions
	• 7.0.1
Avaya Communication Server 1000	• 7.6.7
IP Office	• 9.1.4 • 9.1.5 • 9.1.7 • 10.0
IP Office Contact Center	• 9.1.6 • 9.1.8
Call Center Elite	7.0.1
Avaya Proactive Contact with CTI	5.1.2
AES Server	• 6.3.3 • 7.0 • 7.0.1
Avaya WebLM	6.3.8 and above
Avaya Control Manager	8.0.1
Avaya Aura® Session Manager	7.0.1.2
Avaya Oceana™ Solution	3.2.2

For the latest and most accurate compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx

Setting environment variables for Java

Procedure

1. Click **Start** > **Computer** > **Properties** on the server where you are going to install Avaya Workforce Optimization Select .
2. In the navigation pane, click **Advanced system settings**.
3. Click **Environment Variables**.
4. In the System variables section, click **New**.
5. In the **Variable name** filed, type **JAVA_HOME** as the environment variable name.
6. In the **Variable value** field, type the path that points to the Java directory installed on the machine (64-bit).

   For example,`C:\Program Files\Java\JDK 8u122.`
7. If you are installing the Avaya Workforce Optimization Select application on Windows 2008 R2 server, set the following environment variables:
   a. Select the environment variable named **Path** and click **Edit**.

b. In the **Variable value** field, add the java path `C:\ProgramData\Oracle\Java\javapath`.

Setting environment variables for OpenSSL

About this task

Use this procedure to set environment variables for OpenSSL so that Media Manager uses OpenSSL for call encryption. Ensure that you install and set environment variables for OpenSSL on the server where Media Manager is running.

Procedure

1. Go to https://slproweb.com/products/Win32OpenSSL.html, and download the `Win32 OpenSSL v1.0.2h` file.
2. Copy the `OpenSSL` file to `C:\`.
3. Click **Start** > **Computer** > **Properties**
4. In the navigation pane, click **Advanced system settings**.
5. Click **Environment Variables**.
6. Click one of the following:
   - **Edit**: To append a value to the existing string.
   - **New**: To set a environment variable path.
7. To append a value to the existing string or to set a environment variable path for user variables, type the following:
   - **Variable name**: `Path`
   - **Variable value**: `C:\OpenSSL-Win32\bin`
8. Click **OK**.

Network requirements

- Deployment models must use Fast Ethernet LAN connections. Minimum 1000BASE-T is preferred.
- Multisite deployments must use T1, E1, MPLS, or its equivalent connection to utilize the bandwidth between site locations.
- Each recording server must install two 1-Gbps network interface cards (NICs). Each NIC must have a distinct static IP address. Use one card for standard network access and the other as a packet sniffing interface.
- You must direct the SPAN traffic in your SPAN configuration to the IP address of the NIC. When you run the Avaya Workforce Optimization Select installer, the packet sniffing NIC is referred to as the Voice NIC.

- You must configure the Session Initiation Protocol (SIP) and Real-time Transport Protocol (RTP) traffic to route to the Voice NIC of the recording server in the SPAN configuration.

Port assignments

If the Avaya Workforce Optimization Select deployment is limited to the local intranet, then you do not need to open any ports on the firewall. If you want to provide external access to Avaya Workforce Optimization Select, with firewalls on both ends of a private WAN, open relevant ports. For complete port matrix information, see *Avaya Port Matrix: Avaya Workforce Optimization Select 5.0* available on the support website at http://support.avaya.com.

Preinstallation checklist

No.	Task	Reference	✔
1	Ensure that the servers with required operating system and Windows service packs are available, as per system requirements. The Windows server should have all the latest patches.	-	
2	Ensure that your network administrator enables the Data Network Interface Card (NIC) and Packet Sniffer or Voice NIC on the servers where the recorder is installed.	-	
3	Ensure that network considerations are met.	See Network requirements on page 34.	
4	Ensure that your network administrator configures a valid mail server.	-	
5	Ensure that the sound card is available on client machines to listen to live and recorded interactions.	-	
6	Stop the World Wide Service in Windows 2008 R2 server that uses port 80 by default if you are installing the Avaya Workforce Optimization Select application on Windows 2008 R2 server.	-	
7	Install SQL 2012/2016 standard edition, with the latest service pack on the server where you want to create the database for the Avaya Workforce Optimization Select application. Also, ensure that the SQL server agent is running. Ensure that you do not install the SQL server and the Avaya Workforce Optimization Select components on the same drive to avoid performance issues.	-	

Table continues…

No.	Task	Reference	✔
8	Enable TCP/IP service on the server where SQL is installed irrespective of the SQL edition. Restart the SQL service after enabling the TCP/IP service.	-	
9	Install the mandatory third party utilities such as Wireshark, WinPCap, 7 Zip, and Open JDK. Notepad ++ is an optional third party utility that you can install to analyze and troubleshoot log files.	See Required software for Avaya Workforce Optimization Select on page 29.	
10	Ensure that you assign metrics to NICs for a FQDN based installation with multiple NICs.	See Assigning metrics to Network Interface Cards on page 27.	
11	Set the environment variables for Java.	See Setting environment variables for Java on page 33.	
12	Ensure there is enough space in the drive in which you want to store voice files. The required space depends on the number of interactions you want to store.	-	
13	Ensure that your network administrator configures spanning on Virtual Local Area Network (VLAN), Gateway, or Port level on the recording servers.	-	
14	Ensure you enable ports based on your specific deployment configuration.	See Port assignments on page 35.	
15	Obtain the license types required for your specific deployment configuration.	See the “Licensing Requirements” chapter in *Avaya Workforce Optimization Select Overview and Specification*.	
16	Ensure that Windows updates are completed on all the servers before installing Avaya Workforce Optimization Select . Ensure that Windows Automatic updates is a planned activity.	-	
17	Install and run antivirus before or after you install Avaya Workforce Optimization Select . Ensure you disable antivirus before installing Avaya Workforce Optimization Select . Ensure that scanning is done during the lean period or non production hours.	-	

Chapter 5: Initial setup and connectivity

Hardware requirements

Server	Specifications	VMware (ESXI 5.1, 5.5, and 6) requirements
Single box deployment Supports up to 150 concurrent calls.	• Intel/AMD 64–bit Dual CPU Quad Core (Total 8 Core) with 2.4 GHz • 16 GB RAM • 500 GB Hard Disk • 64 bit Operating System with Service Pack • One C drive with 75 GB SAS 10 K/15K RPM RAID1 or RAID5 HDD for Operating System, Database and System Databases • One D drive with 300 GB SAS 10 K/15K RPM RAID5 HDD for web application, dumps, log files, and configuration files • One E drive with 125 GB SAS 10 K/15K RPM RAID5 HDD for database storage and local call storage • Two 1 Gbps NIC cards	• vCPU: 8 with 2.4 GHz/CPU Reservation • vRAM: 16 GB • vDisk: C: 75 GB, D: 300 GB • vNIC: 2
Multi box deployment — Recorder server Supports 150 to 500 concurrent calls with one recorder for every concurrent calls.	• Intel/AMD 64–bit Dual CPU Quad Core (Total 8 Core) with 2.4 GHz • 8 GB RAM • 500 GB Hard Disk • 64 bit Operating System with Service Pack • One C drive with 75 GB SAS 10 K/15K RPM RAID1 or RAID5 HDD for Operating System, Database and System Databases • One D drive with 300 GB SAS 10 K/15K RPM RAID5 HDD for web application, dumps, log files, and configuration files • One E drive with 125 GB SAS 10 K/15K RPM RAID5 HDD for database storage and local call storage	• Requires one VM Recorder instance for every 250 concurrent G.711, G722, or 450 concurrent G.729 calls • vCPU: 8 with 2.4 GHz/CPU Reservation • vRAM: 8 GB • vDisk: C: 75 GB, D: 300 GB • vNIC: 2

Table continues…

Server	Specifications	VMware (ESXI 5.1, 5.5, and 6) requirements
	• Two 1 Gbps NIC cards	
Multi box deployment — Application and Database server Supports 150 to 500 concurrent calls.	• Intel/AMD 64–bit Dual CPU Quad Core (Total 8 Core) with 2.4 GHz • 16 GB RAM • 500 GB Hard Disk • 64 bit Operating System with Service Pack One C drive with 75 GB SAS 10 K/15K RPM RAID1 or RAID5 HDD for Operating System, Database and System Databases • One D drive with 150 GB SAS 10 K/15K RPM RAID5 HDD for web application, dumps, log files, and configuration files • One E drive for database storage • Two 1 Gbps NIC cards	• vCPU - 4 with 2.4 GHz/CPU Reservation • vRAM - 16 GB • vDisk - C: 75 GB, D: 300 GB • vNIC - 2

Optional modules

Desktop Monitor client machine specifications:

- Windows XP SP3, Windows 7 (32–bit or 64–bit) with latest service packs and security updates
- 2 GHz or faster
- Windows XP with 2 GB minimum and 2+ GB recommended
- Windows 7 with 4 GB minimum and 4+ GB recommended
- 1280 x 1024 minimum graphics display resolution
- Microsoft .NET Framework 3.5 SP1
- Microsoft Visual Studio 2008 Professional or Developers Edition SP1 (Development/Studio only)

Installing Avaya Workforce Optimization Select on a single server

Starting the installation

Before you begin

- Install SQL 2012/2016 standard edition with the latest service pack and ensure SQL agent is running.

- Install third-party software utilities.
- Set environment variables for Java.

Procedure

1. Right-click **AWFOS.exe** click **Run as Administrator**, and click **Next**.

   The installer displays a warning message if the system does not have 8 GB of RAM. You can choose to ignore and proceed. However, you must upgrade the RAM to meet the 8 GB recommendation before moving to production.

2. Select the license agreement option and click **Next**.

Next steps

Select Setup Type.

Selecting Setup Type

Procedure

1. In the Setup Type window, select one of the following:
   - **Standard**: Allows users to choose the telephony platform and automatic call distributor (ACD) against the **Recording Role** option. Avaya Workforce Optimization Select automatically installs the relevant recorder components.
   - **Custom**: Allows users to manually choose and install components of their choice for any deployment.
2. Click **Next**.

Next steps

Do one of the following:

- Select the required role for Standard Setup.
- Select the component type for Custom Setup.

Selecting the required role for Standard Setup

Procedure

1. In the Standard Setup window, select the following:
   - **Web Application Role**
   - **Recording Role**
   - **Database Role**
2. Click **Next**.

Next steps

Configure Required Information.

Related links

Standard Setup field descriptions on page 46

Selecting the component for Custom Setup

Procedure

1. In the Custom Setup window, select all the components that you want to install.
2. Click **Space** to view the volume, disk space, available space, and required space for a component.
3. Click **Next**.

Next steps

Configure Required Information.

Related links

Custom Setup field descriptions on page 47

Configuring Required Information

Procedure

1. In the Required Information window, configure the required fields.
2. Click **Next**.

Next steps

Configure Mail Server.

Configuring Mail Server

Procedure

1. In the Mail Server Configuration window, configure the required fields. This screen is displayed only when you select **Web Application Role**
2. Click **Next**.

Next steps

Configure Database Settings.

Configuring Database Settings

Procedure

1. In the Database Settings window, configure the required fields.
2. Click **Next**.

The system displays the Installation Summary screen. You can click **Back** to review or change any installation setting.

Next steps

Complete the installation.

Completing the installation

Procedure

1. Click **Install**.

   You can click **Cancel** anytime to cancel the installation.

   When the installation is complete, the system displays the InstallShield Wizard Completed window.

2. Select the **Show the Windows Installer** log check box if you want to view and save the installation log after installing the Avaya Workforce Optimization Select application.
3. Click **Finish**.

Next steps

Restart the services with the administrator user privileges.

Installing Avaya Workforce Optimization Select on multiple servers

Avaya Workforce Optimization Select multibox installation

Avaya Workforce Optimization Select multibox installation depends on the following factors:

- The number of concurrent calls
- The number of web application users including agents, supervisors, and quality managers.

If the number of concurrent calls ranges from 150 to 500, install the following on separate servers:

- A Recorder and other Avaya Workforce Optimization Select components
- The web application and database

If the number of concurrent calls are more than 500, install:

- One recorder and other Avaya Workforce Optimization Select components on one server for each 500 concurrent calls.
- The web application on a separate server.

- The database on a separate server.

You can install the Avaya Workforce Optimization Select application using the following two methods:

- **Standard**: Choose the telephony platform and automatic call distributor in the **Recording Role** option. Avaya Workforce Optimization Select automatically installs the relevant recorder components.
- **Custom**: Choose individual components that you want to install for any deployment.

Starting the installation

Before you begin

- Install SQL 2012/2016 standard edition with the latest service pack and ensure SQL agent is running.
- Install third-party software utilities.
- Set environment variables for Java.

Procedure

1. Right-click **AWFOS.exe** click **Run as Administrator**, and click **Next**.

   The installer displays a warning message if the system does not have 8 GB of RAM. You can choose to ignore and proceed. However, you must upgrade the RAM to meet the 8 GB recommendation before moving to production.

2. Select the license agreement option and click **Next**.

Next steps

Select Setup Type.

Selecting Setup Type

Procedure

1. In the Setup Type window, select one of the following:
   - **Standard**: Allows users to choose the telephony platform and automatic call distributor (ACD) against the **Recording Role** option. Avaya Workforce Optimization Select automatically installs the relevant recorder components.
   - **Custom**: Allows users to manually choose and install components of their choice for any deployment.
2. Click **Next**.

Next steps

Do one of the following:

- Select the required role for Standard Setup.
- Select the component type for Custom Setup.

Selecting the required role for Standard Setup

Procedure

1. In the Standard Setup window, select the following:
   - **Web Application Role**
   - **Recording Role**
   - **Database Role**

Table 8: If the number of concurrent calls range from 150 to 500

Server	Role	Notes
Server 1	• **Web Application Role** • **Database Role**	Installs the web application and database.
Server 2	• **Recording Role**	Installs the Recorder and other Avaya Workforce Optimization Select components.

Table 9: If the number of concurrent calls are more than 500

Server	Role	Notes
Server 1	• **Database Role**	Installs the database.
Server 2	• **Web Application Role**	Installs the web application.
Server 3	• **Recording Role**	For each 500 concurrent calls, install a new recorder server. Installs the Recorder and other Avaya Workforce Optimization Select components.

2. Click **Next**.

Next steps

Configure Required Information.

Selecting the component for Custom Setup

Procedure

1. In the Custom Setup window, select all the components that you want to install.

Table 10: If the number of concurrent calls range from 150 to 500

Server	Component	Notes
Server 1	• Web • Database	-
Server 2	• Recorder • Avaya Workforce Optimization Select components	-

Table 11: If the number of concurrent calls are more than 500

Server	Component	Notes
Server 1	• Database	-
Server 2	• Web	-
Server 3	• Recorder • Avaya Workforce Optimization Select components	For each 500 concurrent calls, install a new recorder server.

2. Click **Space** to view the volume, disk space, available space, and required space for a component.
3. Click **Next**.

Next steps

Configure Required Information.

Configuring Required Information

Procedure

1. In the Required Information window, configure the required fields.
2. Click **Next**.

Next steps

Configure Mail Server.

Configuring Mail Server

Procedure

1. In the Mail Server Configuration window, configure the required fields. This screen is displayed only when you select **Web Application Role**

2. Click **Next**.

Next steps

Configure Database Settings.

Configuring Database Settings

Procedure

1. In the Database Settings window, configure the required fields.
2. Click **Next**.

   The system displays the Installation Summary screen. You can click **Back** to review or change any installation setting.

Next steps

Complete the installation.

Completing the installation

Procedure

1. Click **Install**.

   You can click **Cancel** anytime to cancel the installation.

   When the installation is complete, the system displays the InstallShield Wizard Completed window.
2. Select the **Show the Windows Installer** log check box if you want to view and save the installation log after installing the Avaya Workforce Optimization Select application.
3. Click **Finish**.

Next steps

Restart the services with the administrator user privileges.

Standard Setup field descriptions

Name	Description
Web Application Role	The role to install and access the web application. The options are: • **WebApp Service**: You are authorized to access the Avaya Workforce Optimization Select application. • **SysAdmin**: You are authorized to access the SysAdmin module.
Recording Role	The role to install and enable the recording facility in the product. The options are: • **Telephony Platform**: The options for recording calls are: - Communication Manager - CS1000 - IPO 10.x - IPO 9.x and below • **Automatic Call Distributor (ACD)**: The telephony platform options are: - For Communication Manager, select AACC or CC Elite or Oceana based on the deployment. - For CS1000, select AACC. - For IPO 10.x, select ACCS or IPOCC based on the deployment **Note:** IP Office 10.x deployments support active and passive recording and use the Devlink3 adapterto get call signaling events. - For IPO 9.x and below, select ACCS or IPOCC based on the deployment. **Note:** IP Office9,x deployments support passive recording and use the TAPI adapter to get call signaling events. • **Dialer**: The dialer options are: - For CC Elite, select PC if you want to capture calls for Avaya Proactive Contact with CTI and Call Center Elite deployments. - None
Database Role	The role to create database. By default, the installation creates two databases, one for Host and another for Tenant. A database role is a collection of permissions and privileges that can be assigned to one or more users. SQL must be installed before Avaya Workforce Optimization Select installation.

Custom Setup field descriptions

Name	Description
AACCNet adapter	The option to install AACCNet adapter for Avaya Aura® Contact Center on Communication Manager active and passive deployments, Avaya Aura® Contact Center on CS 1000 active and passive deployments, and Avaya Contact Center Select on IP Office passive deployments.
Avaya adapter	The option to install Avaya adapter for Avaya Aura® Contact Center on Communication Manager active deployments, Avaya Aura® Contact Center on CS 1000 active and passive deployments, and IP Office Contact Center on IP Office passive deployments.
AES adapter	The option to install AES adapter for Avaya Aura® Contact Center on Communication Manager active and passive deployments.
PCS adapter	The option to install PCS adapter for Avaya Aura® Call Center Elite on Communication Manager active and passive deployments.
Devlink3 adapter	The option to install Devlink3 adapter for IP Office 10.x extension based recording active and passive deployments, Avaya Contact Center Select on IP Office 10.x active and passive deployments, and IP Office Contact Center on IP Office 10.x active and passive deployments.
Database	The option to install the database. By default, the installation creates two databases, one for Host and another for Tenant.
Screen Capture	The option to install the Screen Capture application.
Log Manager	The option to install the Log Manager component.
Media Manager	The option to install the Media Manager component.
Packet Sniffer	The option to install the Packet Sniffer component.
Process Checklist	The option to install the Process Checklist component.
Recorder	The option to install the Recorder component.
SIP adapter	The option to install SIP adapter for IP Office 10.x extension based recording active and passive deployments, Avaya Contact Center Select on IP Office 10.x active and passive deployments, and IP Office Contact Center on IP Office 10.x active and passive deployments.
SysAdmin	The option to install the SysAdmin application.
TAPI adapter	The option to install TAPI adapter for Avaya Contact Center Select on IP Office passive deployments and IP Office Contact Center on IP Office passive deployments.
Unified Messaging	The option to install the Unified Messaging component.
Web	The option to install the Avaya Workforce Optimization Select web application.

Required Information field descriptions

Name	Description
Installation Path	The location for installing the product Avaya Workforce Optimization Select. . All components get extracted to this location, and each folder has an executable file and dependent files. The default installation path is `C:\Program Files (x86)\Avaya\AWFOS5`.
Logs Path	The location of the log files. A log file records the event occurrence during a software or product runtime. By default, the logs folder is located at `C:\ProgramData\Logs`.
WFO_Home Path	The location of the master database. Database files, such as mdf and ldf, are saved at this location. By default, **WFO_Home Path** is located at `C:\ProgramData\WFO_Home`. **Note:** The `ProgramData` folder is a hidden folder. Ensure that you enable the option to show hidden files in the folder option.
Voice Drive	The drive where the voice folder is created to store interaction data. The recorder records interactions and stores voice files, such as bwd and fwd, and screens in the voice folder.
WebLM IP Address / Hostname	The IP address or hostname of the server where WebLM is installed so that the SysAdmin connects to WebLM to fetch and validate the licenses.
Server IP Address / Hostname	The IP address or hostname of the server on which you want to install one or all of the following: • Web application • Database • Recorder and Avaya Workforce Optimization Select components
Proxy Server IP Address / Hostname	The IP address or hostname of the server on which you want to install the Avaya Workforce Optimization Select web application, irrespective of single-box or multibox deployments. The AWFOSWebProxy service is installed as a component, and the `Apache24` folder is created in the installation path. For high availability, this is the floating or virtual IP address of the network load balancer. Change the node name in each high availability server so that every web application has a unique node name. For more information, see Changing the node name on page 69.
Proxy Port Number	The port number of the proxy server that enables web login and call playback. The default port is 80. Changing the port number requires change in the parameter configurations for components such as Recorder, Media Manager, and Messaging.

Table continues…

Name	Description
	Note: Do not use port number 443.
Server FQDN	The fully qualified domain name of the server on which you want to install one or all of the following: • Web application • Database • Recorder and Avaya Workforce Optimization Select components **Note:** For IP-based installation, ensure that you configure FQDN with an IP address. Else, in multibox deployments, you will encounter issues when importing SSL certificates.

Mail Server Configuration field description

Name	Description
Mail Server IP Address / Hostname	The IP address or the hostname of the email exchange server
Mail Server Port Number	The port number of the email exchange server.
Mail Server Protocol	The types of mail server protocol such as SMTP or SMTPS.
Mail Server Authentication	The option to enable mail server authentication.
Username	The username of the user whose default sender email address is configured.
Password	The password of the user whose default sender email address is configured.
Default Sender Email Address	The default sender email address that is used to send emails related to alerts and notifications triggered by the web application and Avaya Workforce Optimization Select components.
Default Sender Name	The name of the user that appears in the **From** list of the email.

Database Settings field descriptions

Name	Description
Database Server IP Address / Hostname	The IP address or hostname of the server where you are creating the database. You can also point to an existing database.
Named Instance	The option to install the database using the named instance mode. You can point to a named instance of the SQL installation and enter the name of the instance.
Port Number	The port number of the server where the database is installed. The default port number is 1433.
Database Backup IP Address / Hostname	The IP address or hostname of the server that acts as a secondary database server when the primary database server fails.
Windows authentication credentials of current user	The option to install the database using Windows Authentication credentials of the current user. You must have: • Created a Windows domain account for the Avaya Workforce Optimization Select application services. • Run the `0-Harmony-Admin.sql` script on the SQL server machine,
SQL server authentication credentials	The option to install the database using SQL server authentication. You can connect to the database or login as the database administrator. The installer creates the following users in the database: • harmonyadmin: Username used to create databases and database tables. • harmonysec: Username used for encryption and decryption services. • harmony: Username used for all components to connect to the database. • sa: Username with superadmin privileges. **Note:** A user with system administrator privileges must be created if the sa user is not available.
Login ID	The username to access the database.
Password	The password to access the database.
Name of database catalog	The name of the database that you want to create.

WebLM

Avaya provides a web-based license manager (WebLM) to manage licenses of one or more Avaya software products.

To track and manage licenses in an organization, WebLM requires a license file from the Avaya Product Licensing and Delivery System (PLDS) website at https://plds.avaya.com.

The license file is in XML format and contains information about the product such as the licensed capacities of each feature that you purchase. You activate the license file in PLDS and install the license file on the WebLM server.

You must run WebLM as a separate VMware virtual machine or use the WebLM running on System Manager. For more information about WebLM administration, see *Administering Avaya Aura® System Manager*.

Chapter 6: High availability and redundancy

High availability and redundancy

High availability of Avaya Workforce Optimization Select is achieved in a cost-effective manner by using various failover strategies .

Database redundancy

Database redundancy is achieved using the Always On Availability Groups option in the SQL server for database high availability. This option meets both local high availability and geo-redundancy needs provided you are using MS SQL server 2012/2016 Enterprise Edition .

The SQL database in Avaya Workforce Optimization Select can be shared with other applications as long as appropriate resources are allocated. To minimize MS SQL servers, sharing is possible with other applications that support SQL 2012/2016. Depending on no local high availability and other deployment aspects, such as dedicated tenant or less number of tenants, the Basic Availability Group option in SQL server 2016 Standard Edition can be used. This option supports two nodes where one node is primary in data center and the other is secondary in disaster recovery. This supports geo-redundancy but not high availability.

Web application server redundancy

Web application servers are deployed as active-active servers to meet local high availability and geo-redundancy requirements. However, Network Load Balancers (NLBs) are required to ensure that users are split evenly between multiple web application servers. If one of the web application server becomes nonfunctional, the NLB routes users to the available server. Web application servers can be split across data centers for geo-redundancy purposes.

Note:

Note that Avaya recommends an external NLB, not the NLB function provided by Microsoft .

The DNS entry pointing to a virtual IP address on the load balancer distributes the user sessions across all the web application instances. The web application instances are independent, and no session replication is done between them. If any web application instance fails, user sessions on that instance are forced to log out and log in to another instance through the NLB.

Storage server redundancy

During storage server failure, the Avaya Workforce Optimization Select recorder component has the capability to write files locally to avoid loss of data. If the recorder loses connectivity to the storage server, voice and screen capture files are written locally within the storage space of the recorder. These files are moved to central storage when connectivity is restored. This is the reason for separating the recorder server component from the primary application server in a single-server deployment. The recorder cannot write files locally in a single-server deployment if the server fails.

Multiple SPAN ports

Avaya recommends multiple SPAN ports to avoid loss of recording due to port failure. Because Avaya Workforce Optimization Select relies on SPAN, failure occurring at the data switch level must be mitigated in the best way possible.

Multi-interface support

In the absence of a multiple server model, installing multiple NIC cards in a single server can provide redundancy at the NIC level. Normally, if a NIC fails, all traffic stops. However, by grouping together several NICs into one logical NIC, availability is maximized. With teaming, if one NIC fails, the network connection continues to operate on the other NICs.

A multi-interface NIC configuration can also be used to connect multiple SPANs to the recording server. The traffic in each SPAN can be forwarded to a separate interface. A multi-interface NIC configuration also supports failover at the switch level. Two switches in failover mode connected to two SPANs can direct traffic to the two NICs. If the primary switch fails and the backup switch becomes primary, Avaya Workforce Optimization Select still continues to record interactions.

Avaya Workforce Optimization Select supports maximum five NICs in a multi-interface NIC configuration.

Recording server redundancy

On the recorder side, high availability is implemented by deploying the recorders in pairs: one is active while the other one is in hot standby mode. Based on this deployment mode, the following failover strategy is provided:

- A heartbeat mechanism is used between the active and standby server. The recording media can be sent to both recorders simultaneously for a more robust solution, for example, Active-Active recording. If the primary recorder is healthy at the end of the recording, the recording is discarded by the standby server to avoid storing duplicate files. However, if the primary recorder or server? fails in the middle of a call, the full recording is captured by the standby server. If the heartbeat fails, the standby server takes over without losing any recording data. Note that when a failure occurs, the standby server stays as the primary server until a restart occurs or until it fails or gets restarted.
- If the recorder loses connectivity to the storage server, voice and screen capture files are written locally within the storage space of the recorder. These files are moved to central storage when connectivity is restored.
- If the recorder loses connectivity to the database, all database updates are queued to the local file system and applied after connectivity is restored.
- Multiple NIC cards can be installed and configured on the recorder to account for NIC failures. The recorder can read data from multiple NIC cards.

Configuring database redundancy

Setting up Windows 2012 cluster

Installing the failover clustering feature

About this task

Use this procedure to install the Failover Clustering feature on the two member servers on which you want to configure database redundancy.

Before you begin

- Install two Windows 2012 R2 Standard servers in AD domain that are needed to be a part of the cluster.
- Create a cluster administrator account that is a member of local administrator groups for both the member servers. Get administrator privileges on both the servers.
- Create a shared folder in any domain server.
- Install MS SQL 2016 Standard on both the member servers.
- Create the database and take full back up on one of these two member servers.

Procedure

1. Click **Start** > **Server Manager**.
2. On the **Manage** menu, click **Add Roles and Features**.
3. On the Before you begin page, click **Next**.
4. On the Select installation type page, click **Role-based** or **feature-based installation** and click **Next**.
5. On the Select destination server page, click the server where you want to install the feature and click **Next**.
6. On the Select server roles page, click **Next**.
7. On the Select features page, select the **Failover Clustering** check box.
8. To install the failover cluster management tools, click **Add Features** and click **Next**.
9. On the Confirm installation selections page, click **Install**.
10. Select the **Create the cluster now using the validated nodes** check box, and click one of the following:
    - **Finish**: If the results indicate that the tests were completed successfully and you want to create a cluster immediately.
    - **View Reports**: If the results indicate that there were warnings or failures.

Creating the failover cluster

Procedure

1. Click **Start** > **Server Manager**.
2. Click **Tools** > **> Failover Cluster Manager** on the menu bar.

   The system displays the Failover Cluster Manager page.
3. To create a cluster, click Create Cluster at one of the following locations:
   - On the Failover Cluster Manager option
   - In the Actions column on the right pane
   - In Management section of the Failover Cluster Manager page

   The system starts the **Clear Cluster** wizard .
4. On the Before you begin page, review the information and click **Next**.

   To ensure that the servers are connected, configured correctly, and supported by Microsoft, validate the configuration before creating the cluster.
5. Type the names of all the servers that will be part of the cluster.

   You can specify more than one node at a time using comma separation. For example: `MyServer1`, `MyServer2`, `MyServer3`.
6. **(Optional)** Click one of the following if the system displays the Validation Warning page to indicate that the nodes are not validated, and . :
   - `Yes. When I click Next, run configuration validation tests, and then return to the process of creating cluster.`
   - `No. I do not require support from Microsoft for this cluster, and there do not want to run the validation tests. When I click Next, continue creating the cluster.`
7. On the Access Point for Administering the Cluster page, do the following:

   In the **Cluster Name**, type the NetBIOS name that connects to the cluster.
8. Click **Next**.
9. Review the Confirmation screen.
10. Do one of the following:
    a. To add all eligible storage to the cluster, select the **Add all eligible storage to the cluster** check box and click **Next**.
    b. If you choose not to add all eligible storage to the cluster, you can add specific disks after the cluster is created.
11. Review the summary report and click **Finish**.

    A Failover Cluster Manager automatically connects to the cluster when the wizard finishes what?.

Next steps

Configure a File Share Witness on a server that is not part of the cluster.

Failover cluster field descriptions

Name	Description
Cluster Name	The NetBIOS name used to connect to the cluster. During cluster creation, a computer object is also created in the Active Directory domain and in the Organizational Unit where the cluster nodes computer objects are located. If the servers have no NICs configured for DHCP, then a static IP address is prompted. If any of the networks are configured for DHCP, then an IPv4 DHCP assigned address will be used. **Note:** If you do not want the Active Directory object for the cluster to be placed in the same Organizational Unit (OU) as the servers, the specific OU can be designated by specifying the full distinguished name. For more details on how to create a cluster in a restrictive active directory environment, see http://blogs.msdn.com/b/clustering/archive/2012/03/30/10289577.aspx.

Node and file majority quorum

You must configure node and file share majority quorum in the absence of a shared storage. A file share witness must be configured on a server that is not part of the cluster. A file share witness is a basic file share that the cluster computer name has read and write access. The first step involves creating the file share. For example, if the cluster computer name is MYCLUSTER, then create a file share on your data center and provide read or write access to MYCLUSTER. The file share does not need to reside on a Windows 2012 server but the file must be on a Windows Server in the same domain as the cluster.

Configuring the Node and File Majority Quorum

About this task

Use this procedure to provide read or write access to the cluster computer name that you create at both the share level and NTFS level.

Procedure

1. Click **Start** > **Server Manager**.
2. Click **Files and Storage Services** on the left pane.
3. In the **TASKS** tab in the right corner of the page, click **New Share**.

The system displays the New Share Wizard page.

4. On the Select the profile for this share page, click the file share profile that you want to share files with and click Next.
5. On the Select the server and path for this share page, do the following:
   a. In **Server**, select the server where you want to do the file share.
   b. In **Share location**, click an option depending on the location that you want to choose for file share.
6. Click **Next**.
7. On the Specify share name page, do the following:
   a. In **Share name**, type a share name.
   b. In **Local path to share**, provide the path of the location where the folder is to be shared.
   c. In **Remote path to share**, provide the remote path for the share.
8. Click **Next**.

   The system displays .
9. On the Configure share settings page, clickone of the following options depending on your requirements:
   - **Enable access-based enumeration**
   - **Allow caching of share**

     Caching of shares is not required for a file share witness.
   - **Encrypt data access**
10. Click **Next**.
11. On the Specify permissions to control access page, click **Customize permissions** and click **Next**.
12. On the Advanced Security Settings for FSW page, click **Add**.
13. On the Permission Enter for FSW page, click **Select a principal**.
14. On the Select User, Computer, Service Account, or Group page, click **Object Types**.
15. On the Object Types page, select the **Computers** check box and click **OK**.
16. On the Select User, Computer, Service Account, or Group page, in the **Enter the object name to select** field, type the name of your cluster and click **Check Names**.
17. On the Permission Entry for FSW page, in the Basic permissions section, select the **Modify** check box to allow your cluster to get read or write access to the file share.
18. On the Advanced Security Settings for FSW page, check whether the cluster you specified is showing the Allow in the Type column.

19. On the Advanced Security Settings for FSW page, click the **Share** tab and repeat the process so that your cluster gets access permissions at both the NTFS and Share level and click **Apply**.
20. On the New Share Wizard page, in Confirm selections section, confirm that the settings are correct and click **Create**.

    The system displays the View results section with the confirmation that the share is successfully created.
21. Click **Close**.
22. Change the quorum type of the primary server using Failover Cluster Manager.
    a. On the Failover Cluster Manager page, right-click **mycluster**, and click **More Actions** > **Configure Cluster Quorum Settings** period?
    b. On the Configure Cluster Quorum Wizard page, in the Select Quorum Configuration Option section, select the **Add or change the quorum witness** option and click **Next**.
23. On the Configure Cluster Quorum Wizard page, in the Select Quorum Configuration Option section, do the following:
    a. Select the **Configure a file share witness (recommended for special configuration)** option
    b. Browse the path of the file share witness that you created on the data center
24. Click **Next**.

    The system displays the Confirmation section with the message: `Your cluster quorum configuration will be changed to the configuration shown above.`
25. Click one of the following depending on your requirements:
    - **View Report**: To view the report.
    - **Finish**: To close the wizard.

Installing and configuring SQL Server 2016 basic availability group

Setting up basic availability groups in SQL server 2016

About this task

As against database mirroring where you can use only synchronous commit mode, in the basic high availability groups in SQL server 2016, you can configure both synchronous and asynchronous commit modes. You can use the asynchronous commit mode to create your secondary replica in Azure. As a result, you can also create a basic disaster recovery solution with SQL Server Standard Edition. The endpoint configuration is required, and there is no difference in the configuration when compared to the traditional Enterprise Availability Groups.

Procedure

1. Click **Start** > **SQL Server Management Studio**.
2. On Object Explorer, right-click **AlwaysOn High Availability** > **New Availability Group Wizard**.
3. On the New Availability Group Wizard of the Management Studio, do the following:
   - In the **Availability group name** field, type an availability group name.
   - To specify that you want to create basic availability group in standard edition, select the **Basic Availability Group** check box.
   - To configure Always On Availability Groups to failover when a database goes offline, select the **Database level Health Detection** check box.
4. On the Select Databases page, select the user database for the availability groups and click **OK**.

   Only one database can be added to a basic availability group.
5. On the Specify Replicas page, click **Add Replica**.

   You cannot specify more than two replicas: Primary and secondary.
6. On the Specify an instance of SQL Server to host a secondary replica page, click the **Replicas** tab.

   The system displays the Availability Replicas section.
7. Depending on your requirements, select the check boxes in the Automatic Failover and the Synchrous Commit columns.
8. (Optional) In the Readable Secondary section, select whether you want to configure a readable secondary for Primary Initial Role.

   Read access is unavailable on the secondary replica.
9. Click the **Endpoints** tab.
10. Click the **Backup Preferences** tab, and ensure that the page is completely disabled.

    The disabled page indicates that the secondary replica does not support backups. However, you can take snapshots of the secondary what? for a static reporting copy.
11. To create an availability group listener, click the **Listener** tab and do the following:

    You can create only one listener for a basic high availability group.

    a. Select the **Create an availability group listener** check box.

    b. Type the required details in the **Listener DNS Name**, **Port**, and **Network Mode** fields.

    c. Select the Subnet and IP Address.

       The secondary machine can be in the same data center and IP subnets or on a different one.

Setting up data synchronization between two replicas

Procedure

1. On the Select your data synchronization preference page, select one of the following check boxes :
   - **Full**
   - **Join only**
   - **Skip initial data synchronization**
2. After the availability group wizard shows task complete, right-click your Availability Group in Object Explorer and click **Show Dashboard**.

   The system displays the details of the basic availability group.

Basic availability groups in SQL server 2016 field descriptions

Name	Description
Synchronous Commit	Emphasizes high availability over performance at the cost of increased transaction latency. Under synchronous commit mode, transactions wait to send the transaction confirmation to the client until the secondary replica has hardened the log to disk. When data synchronization begins on a secondary database, the secondary replica begins applying incoming log records from the corresponding primary database. As soon as every log record has been hardened, the secondary database enters the SYNCHRONIZED state. Thereafter, every new transaction is hardened by the secondary replica before the log record is written to the local log file. When all the secondary databases of a given secondary replica are synchronized, synchronous commit mode supports manual failover and, optionally, automatic failover.
Automatic Failover	Supports database mirroring sessions running with a witness in high-safety mode. In high-safety mode with automatic failover, after the database is synchronized, if the principal database becomes unavailable, an automatic failover occurs. An automatic failover causes the mirror server to take over the role of principal server and bring its copy of the database online as the principal database. Synchronizing the database prevents data loss during failover because every transaction committed on the principal database is also committed on the mirror database.

Table continues…

Name	Description
Readable Secondary	Allows read-only access to all its secondary databases. However, readable secondary databases are not set to read-only. They are dynamic. A given secondary database changes as changes on the corresponding primary database are applied to the secondary database. For a typical secondary replica, the data, including durable memory optimized tables, in the secondary databases is in near real time. Furthermore, full-text indexes are synchronized with the secondary databases. In many circumstances, data latency between a primary database and the corresponding secondary database is only a few seconds.

Configuring web application server redundancy

Setting up the first instance of the web application on a server

Starting the installation

Before you begin

- Install SQL 2012/2016 standard edition with the latest service pack and ensure SQL agent is running.
- Install third-party software utilities.
- Set environment variables for Java.

Procedure

1. Right-click **AWFOS.exe** click **Run as Administrator**, and click **Next**.

   The installer displays a warning message if the system does not have 8 GB of RAM. You can choose to ignore and proceed. However, you must upgrade the RAM to meet the 8 GB recommendation before moving to production.

2. Select the license agreement option and click **Next**.

Next steps

Select Setup Type.

Selecting Setup Type

Procedure

1. In the Setup Type window, select one of the following:
   - **Standard**: Allows users to choose the telephony platform and automatic call distributor (ACD) against the **Recording Role** option. Avaya Workforce Optimization Select automatically installs the relevant recorder components.
   - **Custom**: Allows users to manually choose and install components of their choice for any deployment.
2. Click **Next**.

Next steps

Select the required role for Standard Setup

Selecting the required role for Standard Setup

Procedure

1. In the Standard Setup window, select the **Web Application Role**.
2. Click **Next**.

Next steps

Configure Required Information.

Configuring Required Information

Procedure

1. In the Required Information window, configure the required fields.
2. Click **Next**.

Next steps

Configure Mail Server.

Configuring Mail Server

Procedure

1. In the Mail Server Configuration window, configure the required fields. This screen is displayed only when you select **Web Application Role**
2. Click **Next**.

Next steps

Configure Database Settings.

Configuring Database Settings

Procedure

1. In the Database Settings window, configure the required fields.

2. Click **Next**.

   The system displays the Installation Summary screen. You can click **Back** to review or change any installation setting.

Next steps

Complete the installation.

Completing the installation

Procedure

1. Click **Install**.

   You can click **Cancel** anytime to cancel the installation.

   When the installation is complete, the system displays the InstallShield Wizard Completed window.

2. Select the **Show the Windows Installer** log check box if you want to view and save the installation log after installing the Avaya Workforce Optimization Select application.
3. Click **Finish**.

Next steps

Restart the services with the administrator user privileges.

Setting up a second instance of the web application on the same server

Changing the binding port of the second instance of jetty

About this task

Use this procedure to set up a second instance of the web application on the same server.

Before you begin

Ensure you stop the following services if they are running:

- AWFOS WebProxy service
- WebApp service

Next steps

Change the port and node of the second instance of the web application.

Changing the port and node of the second instance of the web application

Before you begin

Change the binding port of the second instance of jetty.

Procedure

1. Go to `AWFOS_INSTALLATION_DIR/Web/jetty-1/`
2. Open the `start.ini` file with a standard text editor and do the following:
   a. Search for `Dserver.node` and change the value from `Node1` to `Node2`.
   b. Search for `DWebappPort` and change the value from `9690` to `9691` or any other available port.
   c. Search for `DWebappWebsocketPort` and change the value of this property from `9390` to `9391` or any other available port.
3. Save and close the file.

Next steps

Create the wrapper folder for the second instance of the web application

Creating the wrapper folder for the second instance of the web application

Before you begin

- Change the binding port of the second instance of the jetty.
- Change the port and node of the second instance of the web application.

Procedure

1. Go to `AWFOS_INSTALLATION_DIR/Web/`.
2. Search for the `Wrapper` folder, copy this folder under the same directory, and rename it to `wrapper-1`.
3. Go to `AWFOS_INSTALLATION_DIR/Web/wrapper-1/conf/`.
4. Open the `wrapper.conf` file with a standard text editor and do the following:
   a. Search for `wrapper.app.env.server.node` and change the value from `Node1` to `Node2`.
   b. Search for `webwrapper.log` and change the name of the log file from `webwrapper.log` to `webwrapper-1.log`.
   c. Search for `wrapper.working.dir` and change the working directory to the newly created jetty-1 directory, `AWFOS_INSTALLATION_DIR/Web/jetty-1`.
   d. Search for `wrapper.console.title` and change the value of this property from `WebApp Service` to `WebApp Service-2`.
   e. Search for `wrapper.ntservice.name` and change the value of this property from `AWFOSWebApp` to `AWFOSWebApp-2`.
   f. Search for `wrapper.ntservice.displayname` and change the value of this property from `WebApp Service` to `WebApp Service-2`.
   g. Search for `wrapper.ntservice.description` and change the value of this property from `AWFOS WebApp Service` to `AWFOS WebApp Service-2`.

h. Search for `DWebappPort` and change the port number from `9690` to `9691` or any available port.

   The port number in `DWebappPort` must be the same as the `DWebappPort` in `AWFOS_INSTALLATION_DIR/Web/jetty-1/`.

i. Search for `DWebappWebsocketPort` and change the port number from `9390` to `9391` or any available port.

   The port number in `DWebappWebsocketPort` must be the same as the `DWebappWebsocketPort` in `AWFOS_INSTALLATION_DIR/Web/jetty-1/`.

5. Save and close the file.

Next steps

Install the second instance of jetty as a Windows service.

Installing the second instance of jetty as a Windows server

About this task

Use this procedure to set up a second instance of the web application on the same server.

Before you begin

- Change the binding port of the second instance of the jetty.
- Change the port and node of the second instance of the web application.
- Create the wrapper folder of the second instance of the web application.

Procedure

1. Open a command prompt.
2. In command prompt, go to `AWFOS_INSTALLATION_DIR/Web/wrapper-1/bat/`.
3. Run the batch file `installService.bat`.
4. Open the Windows service manager and click **Refresh**.

   The system displays the `WebApp Service-2` component.

5. Save and close the file.

Next steps

Specify the log location of the second instance of the web application.

Specifying the log location of the second instance of the web application

Before you begin

- Change the binding port of the second instance of the jetty.
- Change the port and node of the second instance of the web application.
- Create a wrapper folder for the second instance of the web application.
- Install the second instance of jetty as a Windows service.

Procedure

1. Go to the `WFO_HOME` folder.
2. Search for the `Webapp_logback_Node1.xml` file, copy this file under the same folder, and rename the file to `Webapp_logback_Node2.xml`.
3. Open `Webapp_logback_Node2.xml` with a standard text editor.
4. Search for `<property name="logsDir"`.

   The system displays <property name="logsDir" value="<<LOGS_FOLDER>>/Webapp" />

   where, <<LOGS_FOLDER>> is any folder according to your installation.
5. Change `Webapp` to `Webapp-2`.

   The system appends Webapp-2 to the logs of the second instance of the Webapp service.
6. Save and close the file.

Next steps

Configure Apache Load Balancer.

Configuring Apache load balancer

About this task

Use this procedure to configure Apache as a load balancer for multiple instances of web applications.

Procedure

1. Go to `AWFOS_INSTALLATION_DIR/Apache24/conf/` .
2. Open the `httpd.conf` file with a standard text editor and enable the following modules in Apache, if not already enabled:
   - `LoadModule heartbeat_module modules/mod_heartbeat.so`
   - `LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so`
   - `LoadModule proxy_balancer_module modules/mod_proxy_balancer.so`
   - `LoadModule slotmem_shm_module modules/mod_slotmem_shm.so`
3. Save and close the file.
4. Go to `AWFOS_INSTALLATION_DIR/Apache24/conf/extra`.
5. Open the `httpd-ssl.conf` file with a standard text editor and do the following:
   a. Add the proxy balancer above the Proxy Rules section for webapp services as follows:

```
<Proxy balancer://webappcluster>
Order Deny, Allow
```

```
Allow from all
BalancerMember http://SERVER_IP:9690
BalancerMember http://SERVER_IP:9691
</Proxy>
```

b. Replace `SERVER_IP` with the real IP of the server where the webapp is installed.

c. Ensure that the port number 9691 is same as the port set for `DWebappPort` in the jety-1 file located at `AWFOS_INSTALLATION_DIR/Web/jetty-1/`.

d. Add the proxy balancer for the UI application service as follows:

```
<Proxy balancer://uicluster>
Order Deny, Allow
Allow from all
BalancerMember http://SERVER_IP:9290
BalancerMember http://SERVER_IP:9292
</Proxy>
```

e. Replace `SERVER_IP` with the real IP of the server where the service is installed.

f. Ensure that the port number 9292 is same as the port set for `jetty.port` in the `jetty.xml` file located at `AWFOS_INSTALLATION_DIR/Web/jetty-1/etc/`.

6. Search for the following proxy rule for web application:

```
ProxyPassMatch ^/webapp/(.*) http://SERVER_IP:9690/webapp/$1
ProxyPassReverse ^/webapp/(.*) http://SERVER_IP:9690/webapp/$1
```

7. Change the proxy rule in Step 6 to use the cluster as follows:

```
ProxyPassMatch ^/webapp/(.*) balancer://webappcluster/webapp/$1
ProxyPassReverse ^/webapp/(.*) balancer://webappcluster/webapp/$1
```

8. Search for the following proxy rule for the UI:

```
ProxyPassMatch ^/awfos/(.*) http://SERVER_IP:9290/awfos/$1
ProxyPassReverse ^/awfos/(.*) http://SERVER_IP:9290/awfos/$1
```

9. Change the proxy rule in Step 8 to use the cluster as follows:

```
ProxyPassMatch ^/awfos/(.*) balancer://uicluster/awfos/$1
ProxyPassReverse ^/awfos/(.*) balancer://uicluster/awfos/$1
```

10. Save and close the file.

Next steps

Start the Avaya Workforce Optimization Select components.

Starting the Avaya Workforce Optimization Select components

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Start** > **Run** > **services.msc**
3. Right-click the following components and click **Restart**:
   - **WebApp Service**

- **WebApp Service**-2
- **AWFOS WebProxy**

Configuring high availability

About this task

Use this procedure to configure high availability for servers where Avaya Workforce Optimization Select is installed. You can deploy an additional server for each web application server. You must configure the IP address of the external load balancer in the Avaya Workforce Optimization Select web application to proxy web requests coming to the Avaya Workforce Optimization Select web services. To maintain data consistency across all web nodes, configure Windows DFS on `WFO_Home` directory.

Note:

The `WFO_Home` path must be same in all high availability servers to maintain data consistency. Ensure you stop all web nodes in all the servers where the web application is installed.

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Start** > **Run** > **services.msc** > **WebApp Service** > **Stop**.
3. Go to the `WFO_Home` folder located at `C:\ProgramData\WFO_Home`.
4. In the `WFO_Home` folder, right-click the `WebappConfig.Properties` file, select **Open with**, and click **Notepad**.
5. Search and change the value for `ProxyIp` to the load balance IP address or domain name.
6. Search and change the value for `ProxyPort` to the port of the external load balancer.
7. Search and change the value for `WebappGenericAccessUrl` to the external load balancer `IP/FQDN:PORT`. For example, if the existing value is https://<<PROXY IP>>:443/awfos/harmonyPage.html, change `<<PROXY_IP>>` to the external load balancer IP or FQDN and 443 to the external load balancer port.
8. Search for `webapp.imagesURL` and change the value to the external load balancer `IP/FQDN:PORT`.
9. Search for `webapp.ksHomeAccessURL` and change the value to the external load balancer `IP/FQDN:PORT`.
10. Click **Save** to close the file.
11. Change the node name in the high availability server so that every web application has a unique node name. For more information, see Changing the node name on page 69.

Next steps

Restart all the Avaya Workforce Optimization Select. services.

Changing the node name for high availability configuration

About this task

Follow this procedure to change the node name of any Avaya Workforce Optimization Select. WebApp server.

Procedure

1. **(Optional)** Stop the AWFOS WebApp service from the service manager if it is running.
2. Navigate to `AWFOS_INSTALLATION_DIR/Web/jetty/`.
3. Open the `start.ini` file with a standard text editor.
4. Search for `Dserver.node` and change the value from `Node1` to `Node2`.
5. Click **Save** to close the file.
6. Navigate to `AWFOS_INSTALLATION_DIR/Web/wrapper/conf/`.
7. Open the `wrapper.conf` file with a standard text editor and search for `wrapper.app.env.server.node` and change the value of this property from `Node1` to `Node2`.
8. Click **Save** to close the file.
9. Navigate to the `WFO_HOME` folder.
10. Search for the `Webapp_logback_Node1.xml` file and rename this file to `Webapp_logback_Node2.xml`.

Chapter 7: Configuration

Configuration checklist

No.	Task	References	✔
1	Insert security keys for call encryption.	See Inserting security keys on page 71.	
2	Configure browser settings for SSL.	See • Configuring browser settings for Internet Explorer on page 72 • Configuring browser settings for Google Chrome on page 72 • Configuring browser settings for Mozilla Firefox on page 74	
3	Modify the default values for logs.	See Modifying default values for logs on page 74.	
4	Configure the proxy IP address for multi server deployments.	See Configuring proxy IP address for multi server deployments on page 75.	
5	Configure SysAdmin.	See SysAdmin on page 75.	
6	Integrate and configure Avaya Workforce Optimization Select on Avaya Aura® Communication Manager.	See *Configuring Avaya Workforce Optimization Select on Avaya Aura® Communication Manager* on the Avaya Support site.	
	Integrate and configure Avaya Workforce Optimization Select on Avaya Communication Server 1000.	See *Configuring Avaya Workforce Optimization Select on Avaya Communication Server 1000* on the Avaya Support site.	
	Integrate and configure Avaya Workforce Optimization Select on IP Office.	See *Configuring Avaya Workforce Optimization Select on IP Office* on the Avaya Support site.	
7	Install Screen Capture.	See Screen Capture overview on page 101.	
8	Install the Desktop Monitor application.	See Desktop Monitor application on page 107.	

Inserting security keys

About this task

Use this procedure to insert security keys in the database for encryption and decryption. The keys are used by the Media Manager component to encrypt interactions or decrypt an encrypted interaction.

Note:

If you do not insert security keys, you cannot encrypt interactions or decrypt an encrypted interaction.

Procedure

1. Go to **Program Files (x86)** > **Avaya** > **AWFOS5** > **Media Manager**.
2. Double-click **EDSecurityKeyGeneration.exe**.
3. On the EDSecurityKeyGeneration page, type the following:
   - **Database IP Address**: The IP address of the server where the database is installed.
   - **Database Name**: The name of the tenant database created during installation.
   - (Optional) **Named Instance**: For named instance deployments
   - **Database User**: The username created by the installer for encryption and decryption services. The default username is harmonysec.
   - **Database Password**: The password created by the installer for encryption and decryption services. The default password is harmonysec@123.
4. Click **Test connection**.

   The system displays the message `Database Opened Successfully`.
5. Click **OK**.
6. Click **Next** to enter the passphrase and the number of keys.

   The system displays the message `Values Are Stored Into Database Successfully`.

   The passphrase that is used to encrypt and decrypt the public and private key can be any combination of alphanumeric letters. The maximum number of keys you can use is 10. For example, alph@12345.
7. Click **OK**.
8. Validate the key values and passphrase by checking whether the keys are inserted in the following tables:
   - INTERACTIONS_KEY_VALUE: The table that contains keys to encrypt interactions.
   - INTERACTIONS_KSEDKEY: The table that uses the passphrase you enter to encrypt and decrypt the public and private keys.

Configuring browser settings for SSL

Configuring browser settings for Internet Explorer

About this task

Use this procedure to import the self-signed certificate to the browser trust store. In a multibox deployment with SSL support, call playback takes place only when the browser sources the self-signed certificates from the browser trust store.

Procedure

1. In the address bar of your browser, type the IP address of the server where the media manager and the recorder is installed with the https protocol.

   The systems displays the following error message: `There is a problem with this website's security certificate.`
2. Click **Continue to this website (not recommended)**.
3. On the address bar, click **Certificate error**.
4. In the Untrusted Certificate popup, click **View certificates**.
5. In the Certificate window, click **Install Certificate**.
6. Click **Next**.
7. In Certificate Store, select **Place all certificates in the following store**, and click **Browse**.
8. Select the **Show physical stores** check box.
9. Click **Trusted Root Certification Authentications** and click **OK**.
10. Click **Next**.
11. Click **Finish**.
12. In the Security Warning dialog box, click **Yes**.

    The system displays the message: `The import was successful.`

Next steps

Restart your Internet Explorer browser.

Configuring browser settings for Google Chrome

About this task

Use this procedure to import the self-signed certificate to the browser trust store. In a multibox deployment with SSL support, call playback takes place only when the browser sources the self-signed certificates from the browser trust store.

Before you begin

Download the certificate to your local server.

Procedure

1. In your browser address bar, type the IP address of the server where the media manager and the recorder is installed with the https protocol.

   The system displays an error message.
2. On the address bar, click the **View site information** () icon.
3. Click **Details**.
4. Click **View Certificate**.

   The system displays the Certificate pane.
5. Click the **Details** tab and click **Copy to File**.
6. Click **Next**.
7. Select **Base64 encoded X.509 (.CER)**.
8. Click **Next**.
9. Click **Browse** and specify the file name that you want to export to the desktop.
10. Click **Save**.
11. Click **Next** and click **Finish**.

    The system displays the message that the export is successful.
12. Click **OK**.
13. Go to the saved folder and double click the certificate.
14. Click **Install Certificate**.
15. Click **Next**.
16. Select the **Place all certificates in the following store** check box.
17. Click **Browse** and select **Trusted Root Certification Authorities**.
18. Click **Next**.
19. Click **Finish**.
20. The system displays the **Security** dialog box.
21. Click **Yes**.

    The system displays the message that the import is successful.
22. Click **OK**.

Next steps

Restart your Google Chrome browser.

Configuring browser settings for Mozilla Firefox

About this task

Use this procedure to import the self-signed certificate to the browser trust store. In a multibox deployment with SSL support, call playback takes place only when the browser sources the self-signed certificates from the browser trust store.

Procedure

1. In your browser address bar, type the IP address of the server where the media manager and the recorder is installed with the https protocol.

   The system displays an error message.

2. Do one of the following whichever is displayed for your version of Firefox:
   - Click the **Advanced** button.
   - Click **I Understand the Risks**.
3. Click **Add Exception**.
4. Click **Confirm Security Exception**.

   The system automatically imports the root signer certificate into the Firefox certificate trust store.

5. Close all instances of Firefox in your system.

Next steps

Restart your Mozilla Firefox browser.

Modifying default values for logs

About this task

The logs folder contains log files that help in debugging issues. However, the default limit for the number of log files is 20 and the size for each log file is 40 MB.

Use this procedure to change the default value for log file size and the number of the log files.

Procedure

1. Go to the `WFO_Home` folder located at `C:\ProgramData\WFO_Home` by default.

   Note:

   The `ProgramData` folder is a hidden folder. Ensure you enable the option to show hidden files in folder options.

2. In the `ICMCommon.properties` file, update the following parameters:
   - NoOfLogFiles
   - LogFileSize
3. Click **Save**.
4. Restart the Avaya Workforce Optimization Select components.

Configuring proxy IP address for multi server deployments

About this task

Use this procedure to configure proxy IP address for multi server deployments to record on demand calls.

Procedure

1. Go to the `WFO_Home` folder located at `C:\ProgramData`.
2. In the `WFO_Home` folder, right-click the `WebappConfig.Properties` file, select **Open with**, and click **Notepad**.
3. For the icm.recordCallUrl=http://<IPaddress>:33023/ parameter, replace the default IP address with the valid IP address of the server where the Unified Messaging component is installed and the port number for the Messaging component is 33023.
4. Click **Save** to close the file.

SysAdmin

SysAdmin is a part of the web installation of the Avaya Workforce Optimization Select application and has a user interface. After installing the Avaya Workforce Optimization Select application, perform tenant management and system administration tasks using the SysAdmin interface.

Tenant management

The tenant management tasks that you need to perform are:

- Create data partition, if required, based on your business needs.
- Activate the default tenant.
- Update the default tenant name to a more meaningful name, if required.

System administration

The system administration tasks that you need to perform are:

- Configure component parameters either using the Bulk Action feature or through the SysAdmin interface.
- Manage users.

After configuring parameters for components, you can monitor alerts to understand the general health of the components and services.

Logging on to SysAdmin

About this task

Before you login into the SysAdmin application for the first time, ensure you clear the browser cache.

Procedure

1. Open a compatible web browser on your computer.
2. Type the IP address of SysAdmin server in the standard dotted-decimal notation.

   For example, `http://<ServerIP>/sysadmin/index.jsp` where server IP is the IP address of the server where the web application is installed.
3. Type your **User Name** and **Password**.
4. Click **Login**.

Tenant management

Creating data partition

About this task

After installing the Avaya Workforce Optimization Select application, you have to decide whether you want to create data partition to restrict data access among various groups within an organization.

Use this procedure to create a data partition OU type. You can create only one data partition OU type in the SysAdmin interface. However, you can associate multiple organization units to a data partition OU type using the Avaya Workforce Optimization Select application.

Note:

You cannot delete a data partition after it is created.

For more information about data partitioning, see *Avaya Workforce Optimization Select Overview and Specification*.

Procedure

1. Log in to SysAdmin.
2. Click **Tenant Management** > **Tenant Administration**.
3. Click the **Edit/View** (›) icon.
4. Click the **Data Partition OU Types** tab.
5. Select the **Data Partition OU Types** check box.
6. In the **DP OU Type 1** field, enter the name of the data partition.

   Note:

   The data partition name must not contain any spaces.
7. Click **Save**.
8. In the Confirmation Message window, click **Confirm** to save the changes.

Activating the default tenant

About this task

The Avaya Workforce Optimization Select installation creates a tenant by default. Use this procedure to activate the default tenant which is in Draft status post installation.

You can also change the default tenant name, which is Default, to a more meaningful name. The tenant name reflects in the web application, database, and other component logs.

Procedure

1. Log in to SysAdmin.
2. Click **Tenant Management** > **Tenant Administration**.
3. Click the **Edit/View** (›) icon.
4. Click **Tenant Details**
5. In the **Status** field, select **Active**.
6. In the **Tenant Name** field, type another name for the tenant.
7. Click **Save**.

Next steps

Restart the web application service.

Related links

Restarting web application service on page 93

System administration

Performing bulk actions

About this task

Use this procedure to download the parameter configurations for a component in an excel spreadsheet. You can change the parameter values and import the spreadsheet. The spreadsheet you download highlights all the mandatory parameters in red color. You cannot import the spreadsheet if the mandatory values highlighted in red are not configured.

While performing bulk actions, you can use the following tabs:

- System: To update common parameter values for components irrespective of their nodes. You can update parameter values for a component only if the mandatory parameters for that component are configured.
- Service: To update system level component parameter values for each node. You can select the server where the component is installed and the node instance of the component.

Procedure

1. Log in to SysAdmin.
2. Click **System Administration** > **Configuration**.
3. To update common parameter values for a component, click the **System** tab.
4. In the **Component** field, select a component.
5. Click **Bulk Action**.
6. Click **Download** to download the template and change the parameter values in an excel spreadsheet.
7. Click **Browse** to select the updated spreadsheet you want to import.
8. Click **Bulk Import**.
9. To update system level component parameter values for a node, click the **Service** tab and do the following:
    a. In the **Component** field, select a component.
    b. In the **Asset** field, select an asset.
10. Click **Bulk Action**.
11. Click **Download** to download the template and change the parameter values in an excel spreadsheet.
12. Click **Browse** to select the updated spreadsheet you want to import.
13. Click **Bulk Import**.

Media manager parameters

Use the procedure Configuring component parameters to select the Media Manager component and use the table below to configure parameters for Media Manager.

Parameter	Description
Alert Configuration	
AlertManagerIPAddress	To configure the IP address of the server where Alert Manager is running to receive Media Manager-related alerts.
Component Options	
StorageManagerInstanceNumber	To configure the Storage Manager instance that is running. If you have two storage manager instances running, you can provide 1 as the storage manager instance for one and 2 for the other instance.
NoOfStorageManagerInstances	To configure the total number of Storage Manager instances that are running. For example, 2.
StorageManagerAction	To add the action that Storage Manager needs to perform. The options are: • Archive • Compress • Copy • Move • Purge You can configure multiple actions separated by a comma. Do not replace the Purge action with Delete.
StorageManagerName	To configure the Storage Manager name. For example, SM1.
EDServiceIPAddress	To configure the IP address of the server where the Media Manager service is running to perform encryption and decryption of recorded interactions.
Debug	
EnableSecurity	To enable encryption or decryption for a call. The options are: • True: The default value that functions only when you configure the secure storage path parameter. Else, Media Manager stops functioning. • False: The value to disable encryption or decryption for calls and screens.

Table continues…

Parameter	Description
LogDatabaseQueries	To enable recorder to log all database queries in the media manager specific log file. The options are: • True: The value that is required for all deployments. The default value. • False:
SecureDBUsername	To configure a secure database user name for encrypting and decrypting interactions. The user name is `harmonysec`.
SecureDBPassword	To configure a secure database password for encrypting and decrypting interactions.
LogLevel	To set the log level for the recorder component. The default value is TRACE. The other options are: • ALL: The value that captures logs of all severity type. • TRACE: The value that captures logs of all severity types. • WARN • FATAL • ERROR • DEBUG
IISServerHost	To configure the host name or IP address of the server where IIS is installed.
WorkingDir	To configure the current working directory folder where the recorder stores interaction data. For example, D:\. where the voice folder is created to store interaction data.
Server Ports	
IISServerPort	To configure the port number for an IIS server. The default value is 443.
Storage Configuration	
StoragePath	To configure a location to store non encrypted audio files and screens. For example, `D:\Voice`.
SecureStoragePath	To configure a location to store encrypted audio files and screens. For example, `D:\Secure`. **Note:** The storage path for the device must be defined in the Avaya Workforce Optimization Select web application. The details are available in the Managing storage devices

Table continues…

Parameter	Description
	topic in *Administering Avaya Workforce Optimization Select*. The time taken by Media Manager to load storage details is 5 minutes. Rules for the specified storage path gets affected after 5 minutes.
Timers	
ConfigLoadInterval	To configure the load interval in minutes for those parameters that do not require service restart. The values that you modify for these parameters get applied only after the specified load interval time. The default value is 15.
DelayBetweenAlerts	To configure the delay between different types of alerts. The default value is 5 minutes.

Process checklist parameters

Use the procedure Configuring component parameters to select the Process Checklist component and use the table below to configure parameters for Process Checklist.

Parameter	Description
Component Options	
AlertManagerIPAddress	To configure the Alert Manager IP address so that the Process Checklist component connects to the Alert Manager server.
LongRunningProcessName1 to LongRunningProcessName10	To configure all the processes that the Process Checklist component needs to monitor. The Process Checklist monitors processes for each component and sends alerts when the process stops or starts. You can map the service names you want to monitor to the parameter values ranging from LongRunningProcessName1 to LongRunningProcessName10.
Debug	
LogLevel	To set the log level for the recorder component. The default value is Info. The other options are: • ALL: The value that captures logs of all severity type. • TRACE: The value that captures logs of all severity types. • WARN • FATAL • ERROR

Table continues…

Parameter	Description
	• DEBUG
Server Ports	
AlertManagerPort	To configure the Alert Manager port so that the Process Checklist component connects to the Alert Manager server. The default value is 9280.
Timers	
ConfigLoadInterval	To configure the load interval in minutes for those parameters that do not require service restart. The values that you modify for these parameters get applied only after the specified load interval time.

Messaging parameters

Use the procedure Configuring component parameters to select the Messaging component and use the table below to configure parameters for Messaging.

Parameter	Description
UM_Core	
nat.apacheIP	To configure the IP address where Apache is running for the Screen Capture to connect to the Unified Messaging component.
proxyIP	To specify the host name or IP address where the web application server is deployed. You can view screen captures while monitoring live interactions.
HarmonyRMSApplication	To configure the application name for Harmony Recorder Middleware Service (HRMS). The default value is AWFOS. For Desktop Monitor application, to start and stop screen capture for nonvoice transactions, the value must be `boffice`.
UM_Core_IP_Ports	
MessagingServerIP	To specify the IP address where the Messaging service is running.
RecorderServerIP	To specify the IP address where the recorder server is running to send the Screen Login information to the recorder.
EDServiceIPAddress	To configure the IP address where Media Manager is running to encrypt and decrypt screens.
ScreenStorageIPAddress	To configure the IP address where Unified Messaging is running to move the screens from the agent desktop to a local storage drive.
UM_Core_Schedulers	

Table continues…

Parameter	Description
dtaNotifier	To configure the cron expression for the Desktop Monitor application. The default value is 0 0/1 * 1/1 * ?. **Note:** Ensure you change the value by replacing 1 with another number. For example, 0 0/2 * 1/1 * ?.
UM_Core_Locations	
uploadLocation	To configure the location for temporary storage of screen capture images. For example `D:\\voice\\screen` or `D:/voice/screen`.
logdumpLocation	To configure the log file dump location for the Screen Capture application. For example `D:\\dump` or `D:/dump`.

Recorder parameters

Use the procedure Configuring component parameters to select the Recorder component and use the table below to configure parameters for Recorder.

Parameter	Description
Adapter Configuration	
DelayedExtendedCallInfo	To update the call variable information in the interactions table for calls that have the agent extended call information message. The options are: • True: The value to capture call variable information for delayed or extended calls. The value to enable all for ACD deployments. • False: The default value.
UseCTIIntegration	To get events from the respective adapters to the recorder for recording interactions. The options are: • True: The value for the recorder to connect to either TAPI adapter, Avaya adapter, AES adapter, or AACCNet adapter. • False: The default value.
SaveCTICallIDInConnected	To remember the PBX call identifier in the connected state. The options are: • True: The value that is required for Cisco environment. • False: The default value.

Table continues…

Parameter	Description
UpdateICMFromWrapUp	To update ICM Enterprise ID value in database that comes in wrapup data. The default value is True.
Alerts	
AlertManagerIPAddress	To configure the IP address of Alert Manager so that the recorder connects to SysAdmin.
HTTPAlertsEnabled	To enable HTTP alerts. The options are: • True: The default value that sends recorder-related alerts to Alert Manager. • False: The recorder does not send any alerts to Alert Manager.
Component Options	
CallMaskingEnabled	To enable call masking. The options are: • True: The default value. The voice data on the file is not written or muted. • False: The voice data on the file is written but muted.
Debug	
LogLevel	To set the log level for the recorder component. The default value is INFO. The other options are: • ALL: The value that captures logs of all severity type. • TRACE: The value that captures logs of all severity types. • WARN • FATAL • ERROR • DEBUG
LogDatabaseQueries	To enable recorder to log all database queries in the recorder specific log file. The options are: • True: The value that is required for all deployments. • False: The default value.
Recording	
DriveSelect	To configure the current working directory folder where the recorder stores ongoing interaction data. For example, D:\. where the voice folder is created to store ongoing interaction data.

Table continues…

Parameter	Description
MaxNoOfLinesForRecording	To configure the maximum number of lines to be recorded for the agent ID if there are multiple line instances. The default value is 6. The value to configure maximum number of lines for Avaya Aura® Contact Center on Communication Manager deployments must be `1`.
VoiceIPAddress1	To configure the IP address from where the recorder reads the voice packets. The recorder reads the voice packets from the voice NIC IP address in case of passive recording and the data NIC IP address in case of active recording.
RecorderPacketFilterString	To configure the network packet filter in recorder to sniff the packets coming from certain ports and from certain protocol type. The format of the value must be identical to the WinCap packet filter format. The options are: • (((ip proto TCP) and (((tcp port 5060) or (ip proto UDP)): The value to enable this parameter for IP Office, SIP, and SPAN recording. • (ip proto UDP)): The value to enable this parameter for Communication Manager, AES, and IP Office, TAPI, CS 1000, and SPAN recording.
AvayaIntegration	To enable 100% recording in Avaya environment, Retain the default value that is False.
RTCPProcessingEnabled	To enable the recorder to process RTCP packets to get phone extension information. Retain the default value that is True for Avaya Aura® Contact Center on Communication Manager passive deployments.
LoginAgentOnPhoneExtTableAdd	To add the IP address of a phone to the table so that the recorder can record interactions of that phone. The options are: • True: The value to enable for Avaya Aura® Contact Center on Communication Manager deployments. • False: The default value.
SIPRecording	
VoiceStreamRecordingEnabled	To configure voice stream recording based on the current agent details. The options are: • True: The value to enable for active recording deployments. • False: The default value.

Table continues…

Parameter	Description
	The value to enable passive or SPAN-based recording.
ScreenCapture	
ScreenCaptureEnabled	To enable screen capture. The options are: • True: The value to enable screen capture of agent desktop. • False: The default value.
SCUploadServerIPAddress	To configure the IP address of the Unified Messaging component where the screen capture service connects to upload screens.
SilentMonitor	
PublicIPAddress	To configure the public IP address used for live monitoring as the IP address of the server where recorder is running.
ApplicationServerIPAddress	To configure the IP address of the web application server.
AppServerPort	To configure the port number for the application server. The default value is 443.
Storage Configuration	
StorageServerIPAddress	To configure the IP address of the server where the recorder is running to store interactions.
StoragePath	To configure the location to store audio files. For example, `D:\Voice`. **Note:** The storage path for the device must be defined in the Avaya Workforce Optimization Select web application. The details are available in the Managing storage devices topic in *Administering Avaya Workforce Optimization Select*. The time taken by Media Manager to load storage details is 5 minutes. Rules for the specified storage path gets affected after 5 minutes.
Timers	
ConfigLoadInterval	To configure the load interval in minutes for those parameters that do not require service restart. The values that you modify for these parameters get applied only after the specified load interval time.
UnifiedMessaging	
ScreenCaptureProxyIPAddress	To configure the IP address of the Unified Messaging component or screen capture proxy so

Table continues…

Parameter	Description
	that the recorder can send all screen capture events.
UnifiedMessagingServerPort	To configure the Unified Messaging port so that the recorder connects to the Unified Messaging component.

Log Manager parameters

Use the procedure Configuring component parameters to select the Log Manager component and use the table below to configure parameters for Log Manager.

Parameters	Description
AlertsConfiguration	
AlertManagerIPAddress	To configure the IP address of the server where Alert Manager is running to receive Log Manager-related alerts.
AlertManagerPort	To configure the port number for Alert Manager. The default value is 9280.
HTTPAlertsEnabled	To enable the HTTP alerts to send Alert Manager-related alerts. The options are: • True: The default value. • False: With this value, you cannot view Alert Manager-related alerts.
ComponentOptions	
MonitorApplicationsList	To configure the list of components. Log files are created by each component like Recorder,MediaManager,AvayaAdapter separated by a comma.
Debug	
HostDataIP	To configure the IP address of the server where Log Manager is running.
Timers	
ConfigLoadInterval	To configure the load interval in minutes for those parameters that do not require service restart. The values that you modify for these parameters get applied only after the specified load interval time.
MonitorApplicationTime	To configure the Monitor Application time, in date and time format, based on the time that logs are generated. The date format is yyyymmdd and time format is hhmmss.

Packet Sniffer parameters

Use the procedure Configuring component parameters to select the Packet Sniffer component and use the table below to configure parameters for Packet Sniffer.

Parameters	Description
AlertsConfiguration	
AlertManagerIPAddress	To configure the IP address of the server where Alert Manager is running to receive Log Manager-related alerts.
AlertManagerPort	To configure the port number for Alert Manager. The default value is 9280.
HTTPAlertsEnabled	To enable the HTTP alerts to send Alert Manager-related alerts. The options are: • True: The default value. • False: With this value, you cannot view Alert Manager-related alerts.
Component Configuration	
DriveSelect	To configure the current working directory folder where the Sniffer Dumps folder is created.
VoiceIPAddress1	To configure the voice NIC IP address.
TetherealFilesLocation	To configure the dump file location.
DumpFileSize	To configure the size of dump files in MB as per your requirement. The default value is 2 MB.
ComponentOptions	
TetherealWrapNumber	To enable the Packet Sniffer to create dump files up to this number that is specified. For example, if the value for this parameter is 10, then the Packet Sniffer will create 10 dump files. After the 10th file, it starts creating files from 1. The default value is –1. This value enables the Packet Sniffer to create dump files without a maximum limit.
Debug	
LogLevel	To set the log level for the recorder component. The default value is Trace. The other options are: • ALL: The value that captures logs of all severity type. • TRACE: The value that captures logs of all severity types. • WARN • FATAL • ERROR • DEBUG

SysAdmin parameters

Use the procedure Configuring component parameters to select the SysAdmin component and use the table below to configure parameters for SysAdmin. You cannot configure the SysAdmin parameters from the Service tab.

Parameters	Description
Email Configuration	
SenderEmailAddress	To configure the sender email address for all the alerts that get triggered from Alert Manager.
SenderEmailPassword	To configure the sender email password.
EmailAddress1	To configure the recipient email address. You can add multiple email addresses separated by a comma. The recipients receive all alerts from Alert Manager.
MailServerIPAddress	To configure the IP address of the local SMTP mail server.
MailServerPort	To configure the local SMTP server listening port. The default value is 25.
EmailAlertsEnabled	To configure alert manager to send alerts to a local SMTP server. The default value is True.
SNMP Configuration	
EnableSNMPTraps	To enable or disable the SNMP traps.
NMSServerIPAddress	To configure the NMS server IP address.
NMSServerPort	To configure the NMS server port. The default value is 161.
NMSCommunityString	To configure the NMS community string especially when NMS polling is True. The value that is used to configure the NMS community string is `public`.
SeverityLevel	To configure the SNMP traps as per log level. The default value is INFO. The other options are: • ALL: The value that captures logs of all severity type. • TRACE: The value that captures logs of all severity types. • WARN • FATAL • ERROR • DEBUG

Configuring component parameters

About this task

Every component has a corresponding service that starts and stops the processing of the component. After installing Avaya Workforce Optimization Select, you must configure few mandatory parameters for each of the components to start the service.

While configuring component parameters, you can use the following tabs:

- System: To configure common parameters for components irrespective of their nodes. You can configure common parameter values for a component only if the mandatory parameters are configured.
- Service: To update system level component parameters for each node. You can select the server where the component is installed and the node instance of the component.
- Dynamic: To connect the recorder to an adapter or service. You can select the server where the recorder is installed and the node instance of the recorder. Use sets to connect the recorder to more than one adapter or service. See Configuring dynamic parameters for recorder on page 91.

Procedure

1. Log in to SysAdmin .
2. Click **System Administration** > **Configuration**.
3. To configure common parameters for a component, click the **System** tab.
4. In the **Component** field, select a component.
5. In the **Value** column, click to type the values for the parameters you want to configure.

   You can type values for parameters only if the mandatory parameters are configured.
6. Click **Save**.
7. To update system level component parameters for a node, click the **Service** tab and do the following:
   a. In the **Component** field, select a component.
   b. In the **Asset** field, select the asset you want to configure.
   c. In the **Node** field, select the node you want to configure.
8. In the **Value** column, click to type the values for the mandatory parameters.

   The systems accepts the default value for the parameters that are not mandatory.
9. Click **Save**.

Next steps

Restart the component service after configuring the parameters.

Configuring dynamic parameters for the recorder

About this task

Use this procedure to connect the recorder to an adapter or service. Based on the deployment, create multiple sets so that the recorder gets connected to the relevant adapters and services. For example, for IP Office Contact Center on IP Office 9.x deployments, the recorder must connect to an Avaya adapter and a TAPI adapter. Therefore, create two adapter sets for the recorder to connect to an Avaya adapter and a TAPI adapter. Similarly, create service sets for the recorder to connect to a service like Media Manager.

You can configure specific parameters for an adapter or service.

Procedure

1. Click **System Administration** > **Configuration**.
2. Click the **Dynamic** tab.
3. In the **Component** field, select a component.

   Note:

   This field applies only to recorder.
4. Select the **Dynamic Type** as **Adapter** or **Service**.
5. In the **Asset** field, select an asset.
6. In the **Node** field, select a node.
7. In the **No. of Sets** field, type the number of sets you want to create.
8. Click **Create Sets**.

Next steps

Restart the component service after configuring the parameters.

Recorder dynamic configurations field descriptions

Name	Description
Component	The recorder component supported for dynamic configuration in Avaya Workforce Optimization Select.
Dynamic Type	The option to connect the recorder to an adapter or service.
Asset	The server where the selected component is installed.
Node	A single instance of the selected component installed on the selected server or assets. You can install multiple instances of a component on a single server.

Recorder dynamic parameters

Adapter dynamic parameters

Parameters	Description
Name	The name of the adapter that must connect to the recorder. For example, Avaya adapter.
Server Address	The IP address of the server where the adapter is installed.
BackupServerAddress	The IP address of the backup server of the adapter.
Server Port	The port number of the adapter.
Server Local Port	The local port number on which recorder establishes connection with the above configured adapter.
Type	The type of adapter configuration. The options are: • Normal: The default value. The recorder does not switch its role from primary to secondary even if the recorder receives inactive keep alive events from any of the adapters. In such cases, the recorder only prints log messages and sends alerts with adapter connectivity status. • Critical: The recorder switches its role from primary to secondary or vice versa when the upstream connectivity is lost. The keep alive events with inactive status determines a lost upstream connectivity.
KeepAliveTimeOut	The time out interval for the keep alive events. The default value is 45 seconds. The recorder switches its role if it does not receive keep alive events from any of the adapters for the specified interval.
KeepAliveWindowSize	The option to specify the window size of the keep alive events for the recorder to switch roles. The default value is 4. The recorder switches its role if it does not receive keep alive events within the specified time out interval and within the specified window size. The time out interval multiplied by the window size determines when the recorder must switch roles.
InactiveKeepAliveCount	The count of inactive keep alive events. The default value is 3. The recorder switches its role if it receives the specified count of inactive keep alive events within the specified time out interval and window size.

Table continues…

Parameters	Description
	The count of inactive keep alive events must be less than the value you specify for the keep alive window size.
IsCritical	The critical state of the adapter. The value for this parameter must be set to True if the parameter value for Type is set to Critical. The value for this parameter can be empty if the parameter value for Type is set to Normal.
WebURLString	The HTTP URL that the recorder uses to send site information to the adapter. • For AACCNet adapter, the web URL is / AACCAdapter/MonitorSitesRecorderRequest. • For Avaya adapter, the web URL is / AvayaAdapter/MonitorSitesRecorderRequest.

Service dynamic parameters

Parameter	Description
Name	The name of the service that you want to connect to the recorder. For example, Media Manager.
IPAddress	The IP address of the server where the service is running. For example, the IP address of the server where the Media Manager component is running.
BackupIPAddress	The IP address of the backup server of the service. For example, the IP address of the backup server where the Media Manager component is running.
Port	The port number of the server where the service is running. For example, 33047 the port number for Media Manager.

Restarting web application service

About this task

Use this procedure to restart the web application service to load the tenant after you install Avaya Workforce Optimization Select and configure the components.

Procedure

1. Log in to the server that hosts the web application component.
2. Click **Start** > **Run** > **services.msc** > **WebApp Service** > **Start**.
3. When the service starts, enter the following URL in your browser: `http://WebserverIP`, where server name is the Avaya Workforce Optimization Select web application host server system name or IP address.
4. Type your **Username** and **Password**.

5. **(Optional)** If you are logging in to the web application service for the first time, change the password.

Related links

Activating the default tenant on page 77

Alerts

Components such as Recorder, Media Manager, PacketSniffer, and Log Manager stop functioning if the disk is full in the respective folder locations. Alerts help you monitor components or services especially when there is a risk. For example, the risk of a component or service not functioning due to disk capacity reaching a specified threshold. You can take the necessary steps to resolve or mitigate such risks.

Note:

- The disk threshold for voice drive in Recorder and storage drive in Media Manager are set in the database in the Storage_Threshold_Space column of the System_Storage_Details table.
- For PacketSniffer and Log Manager, configure the DiskSizeforTetherealDumps and LogDirThresholdSpace parameters respectively to specify the threshold for disk capacity.
- For log folder location and voice data folder, configure the LogsFolderThresholdDiskSpace and VoicedataDirThresholdSpace parameters respectively to specify the threshold for disk capacity.

Viewing alerts

About this task

Use this procedure to view alerts sent by components and services. You can search by severity, host name, component, and host IP to view relevant alerts. Read the description to understand what triggered the alert and what action needs to be taken.

Procedure

1. Click **System Administration** > **Alert Manager**.

   The system displays a list of alerts triggered by **Alert Manager**.

2. Click **Description** to view the Message and Action of the alert.
3. Select the alert and click **Disposition**.
4. Enter a comment for the alert you want to dispose and click **Confirm**.

   You can select multiple alerts if you have common comments to enter for more than one alert.

5. Click **Save**.

Managing users

About this task

Use this procedure to create users in SysAdmin mainly for audit logging purposes. Users have access to all the features available in the SysAdmin application. Therefore, when a user adds, edits, or deletes a record in the SysAdmin interface, an entry is logged and stored in the Host_Audit and Host_Audit_Change_Set tables of the database.

Procedure

1. Click **System Administration** > **User Management**.
2. Click **Create User**.
3. Type the required details in the fields.
4. Click **Save**.

Logging off from SysAdmin

Procedure

1. On the upper-right corner of any page, click the **admin** tab.
2. Click **Log Off**.

   The system displays the Logon screen.

Avaya Workforce Optimization Select configurations

Avaya Workforce Optimization Select supports integration with the different Avaya products. The reference column lists the documents that contain the tasks related to the respective configurations.

Avaya Workforce Optimization Select configurations	Reference
On Communication Manager • Avaya Aura® Contact Center • Call Center Elite • Call Center Elite and Avaya Proactive Contact with CTI • Avaya Proactive Contact with CTI	See *Configuring Avaya Workforce Optimization Select on Avaya Aura® Communication Manager* on the Avaya Support site.
On Avaya Communication Server 1000 • Avaya Aura® Contact Center	See

Table continues…

Avaya Workforce Optimization Select configurations	Reference
	Configuring Avaya Workforce Optimization Select on Avaya Communication Server 1000 on the Avaya Support site.
On IP Office 9.x and 10.x • Avaya Contact Center Select • IP Office extension based recording • IP Office Contact Center	See *Configuring Avaya Workforce Optimization Select on IP Office* on the Avaya Support site.

Limitations

Avaya Aura® Contact Center on Communication Manager deployment limitations

- Call recording does not work for any SIP phones as the phone IP address is not available for passive recording. As a workaround, you must configure a second recorder instance on the same recorder server for SIP based recording.
- High availability fails when there is a network disconnection for AES and Avaya Aura® Contact Center servers. The standby secondary server does not become active automatically when the active primary server is down.
- In multiple transfer and conference scenarios, calls are not stitched together because the ICM_ENTERPRISE ID appears different for agent and supervisor calls.
- When Avaya adapter loses connection with Device Media Call Control (DMCC) during a live call and regains connection, the recording tone that was previously heard is not heard anymore for the live call. This happens in active recording in single step conference.

Avaya Aura® Contact Center on CS 1000 deployment limitations

- The call end response code information, which specifies who ended the call is not updated for interactions.
- In active and passive recording deployments, the transfer number for agent call is updated as NULL in the metadata table for inbound and outbound cold transfer scenarios with skill.
- When agent nonvoice email transaction is transferred to another supervisor, the transfer information is not updated in the metadata table for agent calls.
- In outbound warm transfer and conference scenarios, the skill group ID is updated even for agent calls.
- In active recording deployment, Avaya 1210 and 1220 model hard phones do not support duplicate media stream to record CDN and ACD calls.
- In inbound and outbound warm transfer and conference scenarios with skill, the transfer number is updated as the position ID instead of the dialed number in the metadata table for agent calls in both active and passive deployments.
- In an on-demand agent call, when you conference a supervisor, Avaya adapter updates called party number as the customer extension number instead of dialed skill number for the

supervisor call. This happens because, in Avaya Aura® Contact Center, the agent and supervisor dashboard are updated with the same call information.

- When an agent consults or conferences a call, the Var2 variable of supervisor is updated with the same value which is on the agent Avaya Agent Desktop.
- High availability fails when there is a network disconnection for Avaya Aura® Contact Center server. The standby secondary server does not become active automatically when the active primary server is down.
- The Cluster1_MLS2_Host parameter, although not mandatory, must be configured in Avaya adapter. Else, the configured parameters for Avaya adapter do not get loaded in SysAdmin.
- When you reboot CS 1000 service, calls are not recorded until you restart Avaya adapter to get call signaling.
- When you configure the MLS application name in Avaya adapter in SysAdmin, ensure it does not exceed 20 characters and does not contain special characters.

Avaya Contact Center Select on IP Office 9.x deployment limitations

- TAPI adapter fails to load extensions and send call state events to recorder if you reboot IP Office. Ensure you restart the TAPI adapter service in case you reboot IP Office.
- When you enable agent based recording in TAPI adapter, calls are recorded on agent ID. However, called party and calling party values are not updated and an extra call with no voice or audio is recorded.
- The call end response code information, that specifies who ended the call, is not updated for interactions.
- TAPI adapter does not support site based recording when two recorders are running on the same server as node 1 and node 2.
- Call recording does not work on soft phones below IP Office version 9.1.7. As a workaround, you must configure a second recorder instance on the same recorder server for SIP based recording. However, the workaround does not support call stitching for transfer and conference scenarios.
- In multiple transfer or conference scenarios, an extra call for Supervisor is recorded.
- During high availability failover, the secondary IP Office server becomes active and establishes connection with the secondary TAPI adapter. However, the secondary TAPI adapter does not receive any events from secondary IP Office server.

IP Office Contact Center on IP Office 9.x deployment limitations

- TAPI adapter fails to load extensions and send call state events to recorder if you reboot IP Office. Ensure you restart the TAPI adapter service in case you reboot IP Office.
- The call end response code information, that specifies who ended the call, is not updated for interactions.
- The skill group ID is not updated for non voice interactions such as email and chat.
- The calling party is updated as the skill number for all outbound calls including outbound transfers and conference made from desk phones.
- The conference number is updated as the extension number of the supervisor because the TAPI adapter does not fetch the skill information.

- In a normal agent to agent extension call, calling party is updated as skill number.
- When agent nonvoice email transaction is transferred to another supervisor, the transfer information is not updated in the metadata table for agent calls.
- For conference and inbound multiple transfer scenarios, the UCID which is the ICM_ENTERPRISE ID is incorrectly updated in the metadata table for agent and supervisor calls.
- When you enable agent based recording in TAPI adapter, calls are recorded on agent ID. However, called party and calling party values are not updated and an extra NORTP call is recorded.
- In conference and inbound multiple warm transfer scenarios, the ICM_ENTERPRISE ID appears different for agent and supervisor calls.
- Call recording does not work on soft phones below IP Office version 9.1.7. As a workaround, you must configure a second recorder instance on the same recorder server for SIP based recording. However, the workaround does not support call stitching for transfer and conference scenarios.
- In multiple transfer or conference scenarios, an extra call for Supervisor is recorded.
- When you delete an agent and add another agent on the same extension, TAPI adapter fails to send signaling events and the recorder fails to record calls for that extension.
- During high availability failover, the secondary IP Office server becomes active and establishes connection with the secondary TAPI adapter. However, the secondary TAPI adapter does not receive any events from secondary IP Office server.
- In IP Office Contact Center on IP Office 10.x deployments, Avaya adapter does not connect to IP Office Contact Center server when Apache is nonfunctional. However, Avaya adapter is not connecting to IP Office Contact Center server even after Apache is functional until you restart Avaya adapter.

IP Office 10.x deployments

- During high availability failover of IP Office 10.x, ongoing calls are not recorded. The Avaya Workforce Optimization Select Recorder starts recording calls after phones are moved to the secondary IP Office 10.x.
- The calling party for the second conference party is not updated in conference calls with multiple parties.
- In active recording deployments, the recording tone is not heard for consult conference calls.
- In consult call scenarios, the metadata value that reflects the supervisor number in the `INTERACTION_METADATA` table is blank .
- In Avaya Contact Center Select on IP Office 10.x deployments, the transfer number is updated incorrectly for skill transfer calls.
- The ANI number for supervisor recording is not updated in conference calls.
- In IP Office Contact Center on IP Office 10.x deployments, the ANI number is not updated in consult transfer scenarios.

- In passive recording deployments, when the primary IP Office 10.x is nonfunctional and the secondary IP Office 10.x becomes active, then call recording fails:
  - For newly added phones.
  - When the existing phones get re-registered with a new IP address due to DHCP.
  - When Devlink3 adapter restarts.
- In passive recording deployments, high availability fails when an ongoing call is put on hold. When the primary IP Office 10.x fails, calls that are put on hold are merged with the new call on the secondary IP Office 10.x for the same agent.
- During high availability failover:
  - The call end response code and the interaction metadata are not updated for ongoing calls.
  - The recording tone is not heard when the primary IP Office 10.x fails. The call moves to the secondary IP Office 10.x for ongoing calls.
- Avaya Workforce Optimization Select does not record the call if the agent uses the call park feature on one phone but continues the same call on another phone.
- When Devlink3 adapter stops or restarts, IP Office 10.x stops sending media events till the Devlink3 adapter restarts.
- In IP Office Contact Center on IP Office 10.x deployments, the Avaya Workforce Optimization Select web application does not allow you to configure same values for IP Office user ID and IP Office Contact Center agent ID in the Voice Settings page of the Administrator module. As a workaround, ensure that the values configured for IP Office user ID in IP Office and IP Office Contact Center agent ID in IP Office Contact Center are different and not identical.
- In IP Office Contact Center on IP Office 10.x deployments, Avaya adapter does not connect to IP Office Contact Center server when Apache is nonfunctional. However, Avaya adapter is not connecting to IP Office Contact Center server even after Apache is functional until you restart Avaya adapter.

Avaya Aura® Call Center Elite on Avaya Aura® Communication Manager deployment limitations

- Call recording is not supported for Supervisor calls that are in listen and talk mode.
- The call end response code information, that specifies who ended the call, is not updated for inbound and outbound conference scenarios.
- Call information such as UCID, call conference number, call end response code in multiple transfer, multiple conference, and multiple consult scenarios are incorrectly updated.
- When Avaya adapter loses connection with Device Media Call Control (DMCC) during a live call and regains connection, the recording tone that was previously heard is not heard anymore for the live call. This happens in active recording in single step conference.

Avaya Aura® Call Center Elite on Avaya Aura® Communication Manager and Avaya Proactive Contact with CTIdeployment limitations

- Whenever you restart the Avaya Proactive Contact server, you must restart the PCS adapter. Else, the PCS adapter fails to establish connection with the Avaya Proactive Contact server.
- Outbound calls made through the Avaya Proactive Contact with CTI are marked as inbound in Avaya Workforce Optimization Select.

- The Recorder fails to record calls when AES adapter does not send call signaling events to the Recorder. However, the Avaya Proactive Contact with CTI dialer information of the call that is not recorded is appended in the previous call.
- When Avaya adapter loses connection with Device Media Call Control (DMCC) during a live call and regains connection, the recording tone that was previously heard is not heard anymore for the live call. This happens in active recording in single step conference.

Avaya Proactive Contact with CTI on Avaya Aura® Communication Manager deployment limitations

- When you use Avaya Proactive Contact with CTI, AES adapter sends call signaling events to the Recorder. When you use hard dialer, PCS adapter sends call signaling events to the Recorder.
- An extra call is recorded in Avaya Workforce Optimization Select when an agent logs out from the Avaya Proactive Contact with CTI agent desktop,

Avaya Oceana™ Solution on Communication Manager with Call Center Elite deployments

- The Avaya Oceana™ Solution on Communication Manager with Call Center Elite deployment does not support the data partition feature.
- When the status of Avaya Breeze™ nodes change to deny service and accept service, the Oceana adapter does not receive events for Oceana ACD calls even after the Oceana adapter is successfully connected to an active Avaya Breeze™ node. As a workaround, you must restart the Oceana adapter service to receive the events.
- When the Avaya Breeze™ nodes are rebooted and when a REF cluster is removed and added, the REF events are not received by the Messaging component and Oceana adapter. As a workaround, you must restart the Messaging component and Oceana adapter service.
- When an agent is created or modified in Avaya Control Manager, Avaya Oceana™ Solution sends events to Avaya Workforce Optimization Select. However, the same does not happen when an agent is deleted or an extension is dissociated from an agent. Such changes reflect in Avaya Workforce Optimization Select when the hourly job runs to synchronize users.
- When Avaya adapter loses connection with Device Media Call Control (DMCC) during a live call and regains connection, the recording tone that was previously heard is not heard anymore for the live call. This happens in active recording in single step conference.

Installer limitations

- After you install the Avaya Workforce Optimization Select application, you cannot install a single component. You need to uninstall the Avaya Workforce Optimization Select application and install the component.
- When you uninstall the Avaya Workforce Optimization Select application, the log manager component is not removed from services.msc and appears as running in disabled state.

Avaya Workforce Optimization Select components limitations

- The Avaya Workforce Optimization Select components do not send email alert messages when the connection to the database is lost. However, the components send SNMP traps.
- When you disable and enable the data NIC on a server, you must restart all Avaya Workforce Optimization Select components running on that server.

- Avaya Workforce Optimization Select supports only 40 characters for interaction metadata values. If an automatic call distribution (ACD) or a customer relationship management (CRM) system sends values more than 40 characters, the values will be truncated to 40 characters.
- Avaya Workforce Optimization Select does not record supervisor calls (voice or non-voice) when the coaching, intrusion, whisper, or barge feature is enabled for an agent.

Installing and configuring Desktop Monitor application

Screen Capture overview

Avaya Workforce Optimization Select call center quality management software enables silent monitoring with Screen Capture that allows supervisors to stay involved and in control of contact center operations by monitoring agent interactions from anywhere.

The Unified Messaging component acts like a proxy server and interacts directly with the recorder to capture screens in Avaya Workforce Optimization Select. The Unified Messaging component checks for bandwidth availability and accordingly processes screen requests.

The benefits of implementing Unified Messaging as a proxy server are:

- Reduces bandwidth issues and latency.
- Increases processing speed.
- Controls and checks for the bandwidth limit.

Note:

The Unified Messaging component stops capturing screens if the disk is full on the agent machine. Even after you create some free disk space on the agent machine, screens get captured only when you restart the screen service.

Installing and configuring Screen Capture using MSI packager

About this task

Use this procedure to install Screen Capture on agent machines. The installation creates browser add-ons automatically. However, you must manually configure the Unified Messaging IP address for screen in the registry.

Ensure you install Screen Capture on the Supervisor machine who installs and configures the Learning Console to create projects.

Procedure

1. Click **Program Files (x86)** > **Avaya** > **AWFOS5** > **Screen Capture** located on the server that hosts the web application components.
2. Copy the `ScreenCaptureMSIPackager.msi` to any drive on the agent machine.

3. Open command prompt as an administrator and navigate to `D:\ \ScreenCaptureMSIPackager.msi`.
4. Press `Enter`.

   The system installs `Screen Capture MSI` packager and creates the `Screen` folder on `C:\Program Files(x86)\Avaya` with the following files:

   - `Logs`: The folder where screen capture logs are saved.
   - `Knoahsoft.pem`: Key certificates
   - `Screen.exe`: Service
   - `ScreenCapture.exe`: An application that captures desktop images.
   - `Start.bat`: The file to start the service from the service.msc.
   - `ChromeNMH.exe`: Browser add-ons for Chrome.
   - `HarmonyBHO.dll`: Browser add-ons for IE 32–bit.
   - `HarmonyBHO64.dll`: Browser add-ons for IE 64–bit.
   - `harmonydta.crx`: Browser add-on for Chrome.
   - `harmonydta.xml`: Browser add-ons for Chrome.
   - `harmonydta.xpi`: Browser add-ons for Firefox.
   - `manifest.json`: Browser support for Chrome.
   - `DTA.json`: Contains project XML and resource files .
   - `DTAAgents.json`: Contains project names created by agent when the agent logs in with network ID.
   - `DTAHlpr.exe`: Native application support.
   - `DTAHook.dll`: Native application add-on 32–bit support.
   - `DTAHook64.dll`: Naive application add-ons 64–bit support.
   - `knoahsoft.cer`
5. Open the Screen registry located on: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node \Avaya\Screen`.
6. Configure the values of the following parameters:
   a. ConnectURL: Replace the IP address of the server where Unified Messaging is running in the URL `wss://127.0.0.1:8443/ws/netty/`
   b. DataPath: Enter the path as `C:\ProgramData\Avaya` to specify storage of screens or desktop trigger as.
   c. Tenant: Enter the tenant alias as `Default`.

Next steps

Start the Screen Capture service.

Related links

Restarting web application service on page 93

Installing Screen Capture using bat file

About this task

Use the procedure to ease the installation of the Screen Capture application on agent desktops using the command line option. The bat file automatically configures the Unified Messaging IP address for screen in the registry. The installation also creates browser add-ons automatically.

Procedure

1. Click **Program Files (x86)** > **Avaya** > **AWFOS5** > **Screen Capture** located on the server that hosts the web application components.
2. Copy the `InstallScreenCaptureServiceOnDesktop.bat` to any drive on the agent machine.
3. Right-click `InstallScreenCaptureServiceOnDesktop.bat` file and select **Edit**.
4. In the msiexec -i ScreenCaptureMSIPackager.msi IPADDRESS parameter, type the IP address of the server where Unified Messaging component is installed.
5. Save and close the file.
6. Open command prompt as an administrator and navigate to `D:\ \InstallScreenCaptureServiceOnDesktop.bat`.
7. Press `Enter`.

   The system creates the Screen registry located on: `HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\Avaya\Screen` and the `Screen` folder on `C:\Program Files(x86)\Avaya` with the following files:

   - `Logs`: The folder where screen capture logs are saved.
   - `Knoahsoft.pem`: Key certificates
   - `Screen.exe`: Service
   - `ScreenCapture.exe`: An application that captures desktop images.
   - `Start.bat`: The file to start the service from the service.msc.
   - `ChromeNMH.exe`: Browser add-ons for Chrome.
   - `HarmonyBHO.dll`: Browser add-ons for IE 32–bit.
   - `HarmonyBHO64.dll`: Browser add-ons for IE 64–bit.
   - `harmonydta.crx`: Browser add-on for Chrome.
   - `harmonydta.xml`: Browser add-ons for Chrome.
   - `harmonydta.xpi`: Browser add-ons for Firefox.
   - `manifest.json`: Browser support for Chrome.

- `DTA.json`: Contains project XML and resource files .
- `DTAAgents.json`: Contains project names created by agent when the agent logs in with network ID.
- `DTAHlpr.exe`: Native application support.
- `DTAHook.dll`: Native application add-on 32–bit support.
- `DTAHook64.dll`: Naive application add-ons 64–bit support.
- `knoahsoft.cer`

Next steps

Start the Screen Capture service.

Reinstalling Screen Capture

Before you begin

Ensure to close all the browsers before reinstalling the Screen Capture application.

About this task

Use this procedure to reinstall the Screen Capture application on agent machine when the screen folder and registry get deleted but the screen service is present. The bat file automatically configures the Unified Messaging IP address for screen in the registry. The installation creates browser add-ons automatically.

Note:

You can successfully reinstall the Screen Capture application only if the screen service is present.

Procedure

1. Click **Program Files (x86)** > **Avaya** > **AWFOS5** > **Screen Capture** located on the server that hosts the web application components.
2. Copy the `ReinstallScreenCaptureServiceOnDesktop.bat` to any drive on the agent machine.
3. Right-click `ReinstallScreenCaptureServiceOnDesktop.bat` file and select **Edit**.
4. In the msiexec -i ScreenCaptureMSIPackager.msi IPADDRESS parameter, type the IP address of the server where Unified Messaging component is installed.
5. Save and close the file.
6. Open command prompt as an administrator and navigate to `D:\ \ReinstallScreenCaptureServiceOnDesktop.bat`.
7. Press **Enter**.

Next steps

Start the Screen Capture service.

Verifying agent login

About this task

You can view and verify agent login when the proxy server receives the agentDesktopLogin request. The request is sent when the screen capture component is started on an agent machine or when an agent logs in to his desktop.

The request must contain the following parameters:

- Network_id
- AgentMachineName
- AgentMachineIP
- appname
- uuid
- tenant
- SessionID

Procedure

1. Click **Start** > **SQL Server Management Studio** on the server where the Avaya Workforce Optimization Select database is installed.
2. Select the master database and click **New Query**.
3. Type the query, `Select * from AGENT_SCREEN_LOGIN` and click **Execute**.
4. Verify if the proxy server has inserted a record in the Agent_Screen_Login table with the following columns updated:
   - Agent_Screen_Login_Id: A number generated for indexing.
   - S_NetworkID: The desktop login user ID.
   - UUID: Agent machine generated unique ID.
   - Machine_IP: Agent machine IP address.
   - Machine_Name: Agent machine name.
   - Harmony_networkID: Network ID configured in the Employee table for this agent.
   - Login_Time: Agent login time into the desktop.
   - Login_Status: S for a successful login and F for a failed login.
   - Var1 to var5: For future usage.
   - Status: A for active and I for Inactive.

   The proxy server must send a response back to the screen with upload port details and silent monitor details.

Uploading Screen Capture logs

About this task

Avaya Workforce Optimization Select supports uploading of Screen Capture log files from agent machine to the central storage feature.

Procedure

To upload the log files, type the URL in your browser: `http://IP address:port number/generalCommand?request=LOGDUMP&sNetworkId=username&uuId=user ID&tokenEnabled=TRUE`

Verifying Screen Capture logs

About this task

Use this procedure to verify if the database table is updated with relevant information after uploading the Screen Capture logs.

Procedure

1. Click **Start** > **SQL Server Management Studio** on the server where the Avaya Workforce Optimization Select database is installed.
2. Select the tenant database and click **New Query**.
3. Type the query, `Select * from PROXY_SCREEN_RECON` and click **Execute**.
4. Verify if the Proxy_Screen_Recon table is updated with the following columns:
   - Proxy_Screen_Recon_Id: The ID generated by the database for indexing.
   - Emp_Id: The employee id of the agent configured in the Employee table.
   - Tenant: Tenant alias to which the agent belongs to.
   - Source_File_Path: The location where screens are uploaded. For example, `D:\Voice \Screens`.
   - Target_File_Path: The voice case ID path where screens must exist along with voice files.
   - KS_Call_Identifier: The unique ID generated by the recorder for each call.
   - Screen_Capture_File_Name: The file name format. For example, `Scr_0.7z`.
   - Interval: The Interval between two screen captures.
   - SC_End_At_Count: The total number of screens captured for a call.
   - Status: A for action not completed and I for action completed.
   - Execution_Type: B for failure to move files and execute queries. Q for successful files movement and query execution.

Desktop Monitor application

The Desktop Monitor application is a software utility that captures end user activity thereby identifying areas for process improvement. You can track business data across multiple users and measure against a defined expected business process.

Desktop Monitor installation checklist

No.	Task	Reference	Notes	✔
1	Install Screen Capture.	Installing and configuring Screen Capture using MSI packager on page 101.		
2	Configure the resource files.	Configuring resource files on page 107.		
3	Install the learning console.	Installing Learning Console on page 108.		
4	Execute the script generator.	Executing script generator on page 108.		

Configuring resource files

About this task

Use this procedure to configure resource files so that the spy icon captures the required values you specify while configuring the Learning Console.

Procedure

1. Create a folder manually on the server where the database is installed.

   Give an appropriate name to the folder. For example, Desktop Monitor.

2. In the folder that you create, add a dummy xml file by saving a text file with .xml extension.
3. Copy the resource files from the `LearningResource` folder given by the Release Management team and place them in the folder that you create in step 1.
4. Click **Start** > **SQL Server Management Studio** on the server where the Avaya Workforce Optimization Select database is installed.
5. Select the tenant database and click **New Query**.
6. Type the query, `Insert into DTA_Projects (Name, Project_UUID,RESOURCE_TYPE,CREATE_BY,CREATE_DATE,Data) values ('LearningProject1', 'LearningProject1','xml',1,getdate() ,(select BulkColumn From Openrowset(Bulk 'E:\DTA\LearningProject1.xml', Single_Blob) As Img))` and click **Execute**.

   The query inserts the project XML file in the DTA_Projects table.

7. Type the query, `Insert into DTA_PROJECTS_RESOURCES (Dta_Projects_Id, Name, Resource_UUID, Resource_Type,CREATE_BY,CREATE_DATE, Data) values (1,'LearningResource1', '1B8EE20F-EA5D-42FC-A465-C57174EE2F44','js',1,getdate() ,(select BulkColumn From Openrowset(Bulk 'E:\DTA\1B8EE20F-EA5D-42FC-A465-C57174EE2F44.js', Single_Blob) As Img))` and click **Execute**.

   The query inserts the resource files in the DTA_Projects_Resources table.

8. Type the query, `Insert into DTA_PROJECTS_USER_ACCESS (Dta_Projects_Id, EMP_ID,STATUS,CREATE_DATE,CREATE_BY) values(1,4,'A',GETDATE(),1)` and click **Execute**.

   The query inserts the agent details such as employee ID in the DTA_Projects_User_Access table.

Installing Learning Console

About this task

The supervisor must install Learning Console and create projects to configure data points such as applications, web pages, windows, or screens. Using projects, the supervisor defines what must be captured and pushed to all agent desktop machines.

Procedure

1. Extract the `Learning Console.zip` file onto a folder in your local drive.
2. In the `LearningConsole folder`, double-click the `LearningConsole.exe` file.

   The Desktop Monitor installation folder contains the following files:

   - `ScreenCaptureMSIPackager.msi`: File that installs home agent screen.
   - `Learning Console`: Folder that contains the executable file to install the learning console.
   - `Script Generator`: Folder that contains the script generator.
   - `Learning Resource`: Folder that contains two learning scripts namely `1B8EE20F-EA5D-42FC-A465-C57174EE2F44.js` and `2C9FF31G-FB6E-53GD-B576-D68285FF3E55.js`
   - `DB Scripts`: Folder that contains database scripts.
   - `ReadMe.txt`: ReadMe text file.

Executing script generator

About this task

After you install and configure the Learning Console, the Learning Console processes the data and generates XML files. However, you need to copy the XML project files into the resource generator to generate project resource files. You must then manually insert project resource files into the database using SQL queries.

Note:

Before generating script files, ensure you place the Java security files `local_policy.jar` and `US_export_policy.jar` on the supervisor machine at `C:\Program Files\Java \JDK 8u122\jre\lib\security` folder.

Before you begin

Install and configure the Learning Console by creating one or more projects. For more information about how to create projects, see *Using Avaya Workforce Optimization Select*

Procedure

1. Go to the `Script Generator` folder located in the Desktop Monitor installation folder, right-click the `ScriptGenerator.bat` file, and select **Edit**.
2. In the `ScriptGenerator.bat` file, after `java- jar ScriptGenerator. Jar`, enter the names of xml files generated by the Learning Console and save it.
3. Double-click the same `ScriptGenerator.bat` file.

   In the `ScriptGenerator.bat` file, the system creates xml folders with js files. The script generator generates one js file for one single native application and two js files for single document in the web application.
4. Copy the resource files (js) and the XML project and place them in the folder you created manually on the server where the database that is connected to Unified Messaging component is running.
5. Click **Start** > **SQL Server Management Studio** on the server where the Avaya Workforce Optimization Select database is installed.
6. Select the tenant database and click **New Query**.
7. Type the query, `select * from DTA_Projects --Insert into DTA_Projects (Name, Project_UUID,RESOURCE_TYPE,create_by,CREATE_DATE,Data) values ('yogi_reg', 'iyogi(6D7667EA284E4810BD0B196534BC8634)','xml',1,getdate() , (select BulkColumn From Openrowset(Bulk 'E:\DTA \iyogi(6D7667EA284E4810BD0B196534BC8634).xml', Single_Blob) As Img))` and click **Execute**.

   The query inserts the project XML file in the DTA_Projects table.
8. Type the query, `select * from DTA_PROJECTS_RESOURCES ---Insert into DTA_PROJECTS_RESOURCES (Dta_Projects_Id, Name, Resource_UUID, Resource_Type,CREATE_BY,CREATE_DATE, Data) values (82,'yogi', '04F554E7D0F042099C18B4D662718B1E','js',1,getdate() ,(select BulkColumn From Openrowset(Bulk 'E:\DTA \iyogi(6D7667EA284E4810BD0B196534BC8634).xml_ \04F554E7D0F042099C18B4D662718B1E.js', Single_Blob) As Img))` and click **Execute**.

   The query inserts the resource files in the DTA_Projects_Resources table.

9. Type the query, `select * from DTA_PROJECTS_USER_ACCESS --Insert into DTA_PROJECTS_USER_ACCESS (Dta_Projects_Id, EMP_ID,STATUS,CREATE_DATE,CREATE_BY) values(82,3,'A',GETDATE(),1)` and click **Execute**.

   The query inserts the agent details such as employee ID in the DTA_Projects_User_Access table. The query assigns a project to any agent with employee ID and project ID.

Port mirroring

Spanning or port mirroring must be set up to record all segments of a call especially when there are more than one switches connecting customers to agents. When a call comes in to a core switch and is then routed to a second or access switch to connect to the agent, then port mirroring needs to be configured for both switches.

Note:

Ensure you configure ESXi server and NIC driver settings.

Configuring ESXi Server

About this task

Use this procedure only when the client is using Avaya ERS Swtiches and Recorder is a Virtual Machine (VM) in ESXi.

Before you begin

Configure the monitoring parameter XrxOrXtx or ManyToOneRxTx in the switch.

Procedure

1. On the ESXi server, log in to Vsphere or vCenter.
2. Select the ESXi host where the recorder is hosted.
3. Click the **Configuration** tab.
4. Click **Properties** of the vSwtich of which the network card/connected for Span/Monitor port in Switch.
5. Double click on **Vswitch**, and click the **Security** tab.
6. Select **Accept** for all the following fields:
   - **Promiscuous mode**
   - **MAC address changes**
   - **Forged Transmits**

7. Click **Ok** and close.
8. Double click on the **Port** group.
9. **(Optional)** In the General tab, select **All (4095)** for Vlan ID.
10. In the Security tab, select **Accept** for all the following fields:
    - **Promiscuous mode**
    - **MAC address changes**
    - **Forged Transmits**
11. Click **Ok** and close.

Configuring NIC driver settings

Procedure

1. Log in to the recording server.
2. Click **Start** > **Control Panel** > **Network and Sharing Center**.
3. Click **Change adapter settings**.
4. Right-click on the network adapter on which the voice traffic comes.
5. Click **Properties**.
6. Click on the **Configure** button and click the **Advanced** tab.
7. From the property list box, select Packet Priority & VLAN.
8. From the value drop-down list, select Packet Priority & VLAN Enabled .
9. Click **OK**.

Checklist to change the IP address of servers in DNS deployments

No.	Task	Reference	Notes	✔
1	Stop all the Avaya Workforce Optimization Select components.	See Stopping the Avaya Workforce Optimization Select components on page 112.		
2	Change the node name in the `ini` files.	See Changing the node name on page 112.		

Table continues…

No.	Task	Reference	Notes	✔
3	Start the Avaya Workforce Optimization Select components.	See Starting the Avaya Workforce Optimization Select components on page 113.		
4	Select the appropriate node to configure the C++ components.	See Configuring component parameters on page 90.		
5	Configure all the component parameters for the new node.	See Configuring component parameters on page 90.		
6	Restart the Avaya Workforce Optimization Select components.	See Restarting the Avaya Workforce Optimization Select components on page 114.		

Stopping the Avaya Workforce Optimization Select components

Procedure

1. Log in to the server that hosts the Avaya Workforce Optimization Select components.
2. Click **Start** > **Run** > **services.msc**.
3. Right-click the component and click **Stop**.

Changing the node name

About this task

Use this procedure to change the node name in the `ini` file of the Avaya Workforce Optimization Select components: Every component has a corresponding `ini` file named after the component name. The `ini` file for the recorder is located at `C:\Program File (x86)\Avaya \AWFOS5\Recorder\recorder.ini`.

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Program Files (x86)** > **Avaya** > **AWFOS5** to access the component folder.
3. Change the node name in the `ini` file of the following:
   - Recorder
   - Log Manager
   - Media Manager
   - Process Checklist

- Packet Sniffer
- AES adapter
- TAPI adapter
- PCS adapter
- SIP adapter

4. In the component folder, right-click the respective `.ini` file.
5. Select **Open with**, and click **Notepad**.
6. Update the value for the following parameter:
   - NodeName: Update the node name.
7. Click **Save** to close the file.

Starting the Avaya Workforce Optimization Select components

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Start** > **Run** > **services.msc**.
3. Right-click the component and click **Start**.

Configuring component parameters

About this task

Every component has a corresponding service that starts and stops the processing of the component. After installing Avaya Workforce Optimization Select, you must configure few mandatory parameters for each of the components to start the service.

While configuring component parameters, you can use the following tabs:

- System: To configure common parameters for components irrespective of their nodes. You can configure common parameter values for a component only if the mandatory parameters are configured.
- Service: To update system level component parameters for each node. You can select the server where the component is installed and the node instance of the component.
- Dynamic: To connect the recorder to an adapter or service. You can select the server where the recorder is installed and the node instance of the recorder. Use sets to connect the recorder to more than one adapter or service. See Configuring dynamic parameters for recorder on page 91.

Procedure

1. Log in to SysAdmin .

2. Click **System Administration** > **Configuration**.
3. To configure common parameters for a component, click the **System** tab.
4. In the **Component** field, select a component.
5. In the **Value** column, click to type the values for the parameters you want to configure.

   You can type values for parameters only if the mandatory parameters are configured.
6. Click **Save**.
7. To update system level component parameters for a node, click the **Service** tab and do the following:
   a. In the **Component** field, select a component.
   b. In the **Asset** field, select the asset you want to configure.
   c. In the **Node** field, select the node you want to configure.
8. In the **Value** column, click to type the values for the mandatory parameters.

   The systems accepts the default value for the parameters that are not mandatory.
9. Click **Save**.

Next steps

Restart the component service after configuring the parameters.

Restarting the Avaya Workforce Optimization Select components

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Start** > **Run** > **services.msc**.
3. Right-click the component and click **Restart**.

Chapter 8: Initial administration

Initial administration checklist

No.	Task	Reference	Notes	✔
1	Change the password for all the components. Use the password that you use to log in to web application.	See Setting passwords for services.msc components on page 116.		
2	Refresh and then restart the web services.	See Restarting the Avaya Workforce Optimization Select components on page 114.		
3	Start the web application using the following URL: http://HOSTNAME or IP address. Log in as user `admin` and perform the following: • Add organization, organization units, sites, departments, and designations. • Upload employee data manually or by using an excel spreadsheet. • Assign supervisors to agents or employees. • Configure agent ID, extension, device ID, partition name, or line instance for employees. • Cross check group access for supervisors and managers. • Enable settings for voice and screen capture for agents. • Configure user and report privileges for the respective designations.	For more information, see *Administering Avaya Workforce Optimization Select*.		

Setting passwords for services.msc components

About this task

Use this procedure to change the password for all the components.

Procedure

1. Click **Start** > **Run**.
2. In the Run window, type `services.msc`.
3. Click **OK**.
4. Right-click on any of the Avaya Workforce Optimization Select components and click **Properties**.
5. In the new window, click **Log On Tab**.
6. Change the password to the local system administrator password, confirm the password, and click **OK**.

   The system displays a dialog box with the following message: `The account <username> has been granted the Log on as a service right.`
7. Click **OK**.

Starting the Avaya Workforce Optimization Select web application

About this task

After the installation, you can start the Avaya Workforce Optimization Select web application and log in as the administrator.

Procedure

1. Log in to the server hosting the web application component.
2. Click **Start** > **Run** > **services.msc** > **WebApp Service** > **Start**.
3. When the service starts, enter the following URL in your browser: `http://WebServerIP`, where server name is the Avaya Workforce Optimization Select web application host server system name or IP address.
4. Log in with the following credentials:
   - **UserID**: `admin`
   - **Password**: `password`
5. Change the password after you log in for the first time.

Routine maintenance

Backup and restore

Backup and restore is an important maintenance activity that must be performed on a regular basis as a precautionary measure. Take a backup of the server and the database so that, in case of any failure, you can revert to the original state using the restoration procedures.

For the Avaya Workforce Optimization Select application, you can take a complete backup of the server as an image using external tools. You can also take an image of the server in case the server is hosted on virtual machines. Apart from the database, also back up the following folders:

- `WFO Home`: Contains the master database properties, Avaya WebLM configuration properties, and mail configuration properties.
- `Voice`: Contains recorded voice and screen files.
- `Voice Data`: Contains sniffer files.
- `Logs`: Contains log files that record the event occurrence during a software or product runtime.

Backing up the server data

About this task

Use this procedure to take a backup of the data that exists on the server where the web application is installed. For multiserver installations, take a backup pf the data that exists on the web application server and the recorder server.

Before you begin

Stop the services of all components. Stop the Process Checklist service first. Otherwise, the Process Checklist service restarts other services when it finds a service in a stopped state.

Procedure

1. In the Avaya Workforce Optimization Select web application server, copy the following folders to take a backup:
   - `WFO_Home` folder located at `C:\ProgramData\WFO_Home` by default. Avaya recommends that you install this folder on `E:\` drive so that there is no conflict with the installation directory.
   - Working directory folder located at `C:\ProgramData\<Working_Directory>` by default. Avaya recommends that you install this folder on `E:\` drive.
   - Registry key located at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya`.
   - `Voice` folder from the drive you specified during installation. .

- `Voice Data` folder from the drive you specified for `Voice` folder during installation.
- `Logs` folder located at `C:\ProgramData\Logs` by default. Avaya recommends that you install this folder on `E:\` drive as logs can occupy lot of space.

2. In the Avaya Workforce Optimization Select Recorder server, copy the following folders to take a backup:
   - `WFO_Home` folder located at `C:\ProgramData\WFO_Home` by default. Avaya recommends that you install this folder on `E:\` drive so that there is no conflict with the installation directory and voice directory.
   - Working directory folder located at `C:\ProgramData\<Working_Directory>` by default. Avaya recommends that you install this folder on `E:\` drive.
   - Registry key located at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya`.
   - `Voice` folder from the drive you specified during installation.
   - `Voice Data` folder from the drive you specified for `Voice` folder during installation.
   - `Logs` folder located at `C:\ProgramData\Logs` by default. Avaya recommends that you install this folder on `E:\` drive as logs can occupy lot of space.

Restoring the data

About this task

Use this procedure to restore the data on the server with the same IP address.

Before you begin

- Install the same operating system with the same version (64 bit) on the new server.
- Maintain the same partitions with the same drives.
- Install the same version of the database.
- Install all third-party software.
- Uninstall the Avaya Workforce Optimization Select application in case there is an existing version and reinstall the Avaya Workforce Optimization Select application. While reinstalling, use the same drives and folder names that is used for the previous installation.

Procedure

1. Stop the Avaya Workforce Optimization Select services.
2. Restore the `WFO_Home` folder at `C:\ProgramData\WFO_Home` or `E:\WFO_Home`
3. Restore the working directory folder at `C:\ProgramData\<Working_Directory>` or `E:\<Working_Directory>`.
4. Restore the registry key located at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Avaya`

5. Restore the `Voice` folder on the drive you specified during installation.
6. Restore the `Voice Data` folder on the drive you specified during installation.
7. Restore the `Logs` folder at `C:\ProgramData\Logs` or `E:\Logs`.
8. Start the Avaya Workforce Optimization Select services.

Backing up database files

About this task

Use this procedure to take a complete backup of the master database of the Avaya Workforce Optimization Select application and the tenant database during lean period. Store the backup files on a server that is different from the location where SQL is running.

Procedure

1. Click **Start** > **SQL Management Studio** on the server where the Avaya Workforce Optimization Select database is installed.
2. Login using sa credentials.
3. Select the master database of Avaya Workforce Optimization Select and right-click **Tasks** > **Back Up**.
4. To take a backup of the tenant database, select the tenant database.
5. Select **Backup type** as **FULL**, click **Options** in the left pane and select the **Overwrite** option, and select the Verify option if you want the system to check for database backup completion.
6. Click **Add** to add the location and name of the backup file.
7. Enter a file name with .bak extension and date and time stamp it for future reference.
8. Click **OK** to close the screen.
9. Click **OK** to start the database backup process and click **Stop action now** to terminate the backup process.

   The Progress pane indicates the percentage of completion. After the backup is complete, a message indicating successful backup is displayed.

Restoring the database files

About this task

Use this procedure to restore the master database files or the tenant database files thereby ensuring database recovery.

Before you begin

Before you restore either the master database of Avaya Workforce Optimization Select or the tenant database, delete the existing database that you want to restore.

Procedure

1. Click **Start** > **SQL Server Management Studio** on the server where the Avaya Workforce Optimization Select database is installed.
2. Select the master database of Avaya Workforce Optimization Select and right-click **Delete**.
3. To restore the tenant database, select the tenant database and right-click **Delete**.
4. Select **Databases** and right-click **Restore**.
5. In the Restore Database dialog box, use the Source section to specify the source and location of the backup sets to be restored.
6. Select **Database** to restore the database from the list of backed up files.

   In the Destination section, the **Database** field is populated with the name of the database to be restored.
7. In the Backup sets to restore grid, select the backup files to be restored.
8. Click **OK**.

Replacing self-signed certificates with CA-signed SSL certificates

About this task

Use this procedure to replace the self-signed Avaya Workforce Optimization Select certificate with a CA-signed SSL certificate.

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Start** > **Run** > **services.msc**.
3. Right-click the **AWFOS WebProxy** service and click **Stop**.
4. Copy the SSL key file to the Apache installation folder located at the installation path you specify during installation. For example, `C:\Program Files (x86)\Avaya\AWFOS5\Apache24\conf\ssl.key\`.
5. Copy the CA-signed certificate file to the Apache installation folder located at the installation path you specify during installation. For example, `C:\Program Files (x86)\Avaya\AWFOS5\Apache24\conf\ssl.crt\`.

6. Right-click the `httpd-ssl.conf` file located at the installation path in the `extra` folder. For example, `C:\Program Files (x86)\Avaya\AWFOS5\Apache24\conf\extra`.
7. Click **Edit with Notepad ++**.
8. Search for `/conf/ssl.crt/server.crt`.
9. Replace server.crt with the name of the CA-signed certificate file.
10. Search for `/conf/ssl.key/server.key`.
11. Replace server.key with the name of the SSL key file.
12. Click **Save** to close the file.
13. Restart the **AWFOS WebProxy** service.

Next steps

Open the Avaya Workforce Optimization Select application on a web browser using the URL: `http://<IPAddress>` depending on the server configuration. The URL automatically gets redirected to `https://<hostname>`.

Chapter 9: Postinstallation verification

System verification checklist

No.	Tasks	Reference	✔
1	Start the SysAdmin service.	See Logging on to SysAdmin on page 76.	
2	Access the SysAdmin URL.	See Starting the SysAdmin service on page 122.	
3	Start the web application service.	See Starting the web application service on page 123.	
4	Access the web application URL.	See Logging on to Avaya Workforce Optimization Select on page 123.	
5	Verify the log files of the following components:	See Verifying Avaya Workforce Optimization Select service logs on page 124.	
	• Log manager	See Log Manager log messages on page 125.	
	• Media manager	See Media Manager log messages on page 125.	
	• Messaging	See Messaging log messages on page 126.	
	• Process checklist	See Process Checklist log messages on page 126.	
	• Packet sniffer	See Packet Sniffer log messages on page 127.	
	• Recorder	See Recorder log messages on page 127.	

Starting the SysAdmin service

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Start** > **Run** > **services.msc**.
3. Right-click **SysAdmin Service** and click **Restart.**

Logging on to SysAdmin

About this task

Before you login into the SysAdmin application for the first time, ensure you clear the browser cache.

Procedure

1. Open a compatible web browser on your computer.
2. Type the IP address of SysAdmin server in the standard dotted-decimal notation.

   For example, `http://<ServerIP>/sysadmin/index.jsp` where server IP is the IP address of the server where the web application is installed.
3. Type your **User Name** and **Password**.
4. Click **Login**.

Starting the web application service

About this task

Verify that the Avaya Workforce Optimization Select instance is installed in your system.

Procedure

1. Log in to the server that hosts the web application components.
2. Click **Start** > **Run** > **services.msc**.
3. Right click **WebApp Service** and click **Restart**.

Logging on to Avaya Workforce Optimization Select

Procedure

1. Open a compatible web browser on your computer.
2. Depending on the server configuration, type one of the following:
   - The unique IP address of the Avaya Workforce Optimization Select server in the standard dotted-decimal notation.

   For example, `http://<IPAddress>`, where *<IPAddress>* is the unique IP address of the Avaya Workforce Optimization Select server.
   - The unique host name of the Avaya Workforce Optimization Select server.

For example, `http://<hostname>`, where *<hostname>* is the unique host name of the Avaya Workforce Optimization Select server.

You can now log in to the Avaya Workforce Optimization Select application.

3. Enter your user name and password.
4. Click **Sign in**.

   The Avaya Workforce Optimization Select home page appears.

Verifying Avaya Workforce Optimization Select service logs

About this task

After installing the Avaya Workforce Optimization Select application, verify log files to ensure that all the services are functional. The location of the `Logs` folder is specified during installation. By default, the `Logs` folder is located at `C:\ProgramData\Logs`.

Procedure

1. Go to the `Logs` folder at `C:\ProgramData\Logs` or at a location specified during the Avaya Workforce Optimization Select installation.
2. Verify whether the component services in the following log files are functional:
   - `LogManager.log`
   - `MediaManager.log`
   - `Messaging.log`
   - `ProcessChecklist.log`
   - `PacketSniffer.log`
   - `Recorder.log`
3. Verify whether the adapter services in the following log files are functional:
   - `AESAdapter.log`
   - `AvayaAdapter.log`
   - `AACCNetAdapter.log`
   - `TAPIAdapter.log`
   - `PCSAdapter.log`
   - `Devlink3Adapter.log`
   - `SIPAdapter.log`

Next steps

Based on the deployment, verify the deployment-specific adapter logs for Automatic Call Distributor (ACD) connection, recorder connection, and agent login information.

Component log verification

Log Manager log messages

Message	Description
`LogManager started: Running build....`	The Log Manager service is functional.
`Connection opened with database at ip address : 10.133.204.67 and database name AWFOSDB_Feb14th_FP2`	The Log Manager component is connected to the database on the server with IP address 10.133.204.67 and database name AWFOSDB_Feb14th_FP2.

Media Manager log messages

Message	Description
`MediaManager started: Running build...`	The Media Manager service is functional.
`Connection opened with database at ip address : 10.133.204.67 and database name AWFOSDB_Feb14th_FP2`	The Media Manager component is connected to the master database on the server with IP address 10.133.204.67 and database name AWFOSDB_Feb14th_FP2.
`EDSecureKnoahSoftDB : Connection opened with database at ip address : 10.133.204.122 and database name AWFOSDB_FP2_Oceana_Mar13_Tenant`	The Media Manager connects to the tenant database to fetch the encryption decryption secure keys.
`PassPhrase value bRGqbb7rCgBYGvvK`	The Media Manager is loading the passphrase value as present in the tenant database.
`2 storage server details loaded from database`	The Media Manager is loading storage server details from the tenant database.
`Using local path "D:\Voice\" for storage`	The Media Manager is validating the storage path created in web application.

Messaging log messages

Message	Description
`Messaging started: Running build...`	The Messaging service is functional.
`Connection opened with database at ip address : 10.133.204.67 and database name AWFOSDB_Feb14th_FP2`	The Messaging component is connected to the database on the server with IP address 10.133.204.67 and database name AWFOSDB_Feb14th_FP2.

Process Checklist log messages

Message	Description
`ProcessCheckList started: Running build`	The Process Checklist service is functional.
`Connection opened with database at ip address : 10.133.204.67 and database name AWFOSDB_Feb14th_FP2`	The Process Checklist component is connected to the database on the server with IP address 10.133.204.67 and database name AWFOSDB_Feb14th_FP2.
`"devlink3adapter service" service is installed`	The Process Checklist validates that the Devlink3 adapter service is installed.
`"mediamanager service" service is installed`	The Process Checklist validates that the Media Manager service is installed.
`"avayaadapter service" service is installed`	The Process Checklist validates that the Avaya adapter service is installed.
`Running as "devlink3adapter service" in service manager`	The Process Checklist validates that the Devlink3 adapter service is running.
`Running as "mediamanager service" in service manager`	The Process Checklist validates that the Media Manager service is running.
`Running as "avayaadapter service" in service manager`	The Process Checklist validates that the Avaya adapter service is running.
`An ERROR has occurred: avayaadapter service is down`	The Process Checklist validates that the Avaya adapter service is nonfunctional.
`avayaadapter service start pending...`	The Process Checklist is starting the Avaya adapter service.
`avayaadapter service started successfully`	The Process Checklist started the Avaya adapter service successfully.
`Stopping service "ProcessCheckList Service"`	The Process Checklist service stopped.

Packet Sniffer log messages

Message	Description
`PacketSniffer started: Running build...`	The Packet Sniffer service is functional.
`Connection opened with database at ip address : 10.133.204.67 and database name AWFOSDB_Feb14th_FP2`	The Packet Sniffer component is connected to the database on the server with IP address 10.133.204.67 and database name AWFOSDB_Feb14th_FP2.

Recorder log messages

Message	Description
`Recorder started: Running build...`	The Recorder service is functional.
`Connection opened with database at ip address : 10.133.204.67 and database name AWFOSDB_Feb14th_FP2`	The Recorder component is connected to the database on the server with IP address 10.133.204.67 and database name AWFOSDB_Feb14th_FP2.
`ConfigDatabase : Select STORAGE_ID,STORAGE_NAME,STORAGE_PATH,USER_NAME,PASSWORD,HOST_IP,UPDATE_DATE, STORAGE_THRESHOLD_SPACE from SYSTEM_STORAGE_DETAILS where host_ip = '10.133.204.121' or host_ip='10.133.204.121'`	The Recorder is validating the following storage details: • Storage ID • Storage name • Storage path • Username • Password • Host IP • Update date • Storage threshold space
`Storage server details loaded from database 1`	The Recorder loaded the storage server details.
`02/28/17 22:35:47 (PST) [22156] CKnoahsARKDatabase.c :356 INFO - {Call up_icm_s_GetAgentsInfo('','')}`	The Recorder validates the Voice Settings configurations for all agents in the Avaya Workforce Optimization Select application every minute using the stored procedure `{Call up_icm_s_GetAgentsInfo('','')}`.
`Recorder connected to primary AACC Adapter at ip address 10.133.204.121 and port 34301`	The Recorder is connected to the primary AACCNet adapter on the server with IP address 10.133.204.121 and port number 34301.

Table continues…

Message	Description
`Recorder connected to primary AES Adapter at ip address 10.133.204.121 and port 33012`	The Recorder is connected to the primary AES adapter on the server with IP address 10.133.204.121 and port number 33012.
`Recorder connected to primary Avaya Adapter at ip address 10.133.204.121 and port 34101`	The Recorder is connected to the primary Avaya adapter on the server with IP address 10.133.204.121 and port number 34101.
`Recorder connected to primary AACC Adapter at ip address 10.133.204.121 and port 34301`	The Recorder is connected to the primary TAPI adapter on the server with IP address 10.133.204.121 and port number 34301.
`Recorder connected to primary AES Adapter at ip address 10.133.204.121 and port 33012`	The Recorder is connected to the primary PCS adapter on the server with IP address 10.133.204.121 and port number 33012.
`Recorder connected to primary Avaya Adapter at ip address 10.133.204.121 and port 34101`	The Recorder is connected to the primary Devlink3 adapter on the server with IP address 10.133.204.121 and port number 34101.
`Recorder connected to primary AES Adapter at ip address 10.133.204.121 and port 33012`	The Recorder is connected to the primary SIP adapter on the server with IP address 10.133.204.121 and port number 33012.
`Recorder connected to primary Avaya Adapter at ip address 10.133.204.121 and port 34101`	The Recorder is connected to the primary Oceana adapter on the server with IP address 10.133.204.121 and port number 34101.
`Received VOIP_CTIOS_AGENT_LOGIN with agentID 20001 and agentExtension 20001`	The Recorder received the login information for the agent with ID 20001 and extension 20001 from the relevant adapter based on the deployment.
`Received CTIOS_AGENT_LOGIN with agent_id 20001 for agent with extension 20001 and line_instance 1`	The Recorder received the login information for the agent with ID 20001, extension 20001, and line instance 1 from the relevant adapter based on the deployment.
`Received VOIP_CTIOS_AGENT_CALL_STATE with agentExtension 20001 and agentState OFF_HOOK for deviceId 20001`	The Recorder received call state information as off hook for the agent with extension 20001 and device ID 20001 from the signalling adapter based on the deployment.
`Received VOIP_CTIOS_AGENT_CALL_INFO with agentExtension 20001`	The Recorder received call information for the agent with extension 20001 from the signaling adapter based on the deployment.
`Received VOIP_CTIOS_AGENT_CALL_STATE with agentExtension 20001 and agentState ON_CONNECTED for deviceId 20001`	The Recorder received call state information as connected for agent with extension 20001 and device ID 20001 from the signaling adapter based on the deployment.
`Received VOIP_CTIOS_AGENT_EXTENDED_CALL_INFO with agentExtension 20001 and callIdentifier 1638`	The Recorder received extended call information for agent with extension 20001 and call identifier 1638 from the signaling adapter based on the deployment.

Table continues…

Message	Description
`Received VOIP_CTIOS_AGENT_CALL_ACD_INFO with agentExtension 20001 and lineInstance 1`	The Recorder received call ACD information for agent with extension 20001 and line instance 1 from the ACD adapter based on the deployment.
`Received CTIOS_CALL_ACD_INFO_MESSAGE for agent with extension 20001 and call_identifier 37496593`	The Recorder received call ACD information message for agent with extension 20001 and call identifier 37496593 from the ACD adapter based on the deployment.
`Received VOIP_CTIOS_PHONE_EXT_INFO`	The Recorder received phone extension information from the relevant adapter based on the deployment.
`Received CTIOS_PHONE_EXT_INFO for extension 20001, ip address 1.0.78.33 and extension status Added`	The Recorder received phone extension information for extension 20001 on IP address 1.0.78.33 and extension status as added.
`Received CTIOS_CALL_STATE_MSG_OFF_HOOK for agent with extension 20001 and line_instance 1 with call_identifier 37496593`	The Recorder received call state message as off hook for agent with extension 20001, line instance 1, and call identifier 37496593 from the signaling adapter based on the deployment.
`Received CTIOS_CALL_INFO_MESSAGE with called party "20001", calling party "20012" and call_type CALL_TYPE_INBOUND for agent with extension 20001 and skill_group_id 0 and line_instance 1 with call_identifier 37496593`	The Recorder received call information message with the following call details: • Called party: 20001 • Calling party: 20012 • Call type: Inbound • Extension: 20001 • Skill group ID: 0 • Line instance: 1 • Call identifier: 31496593
`Received CTIOS_VOICE_STREAM_RTPINFO for agent voice_stream for agent with extension 20001, device_id 20001, line_instance 1, call_identifier 1638, remote_call_id 1638, localIP 10.133.204.121, localRTPPort 16386, remoteIP 1.2.3.4, remoteRTPPort 1234, callingParty 20012, calledParty 20001`	The Recorder received voice stream RTP information for agent voice stream with the following details: • Agent extension: 20001 • Device ID: 20001 • Line instance: 1 • Call identifier: 1638 • Remote call ID: 1638 • Local IP address: 10.133.204.121 • Remote IP address: 1.2.3.4 • Remote RTP port: 1234 • Calling party: 20012

Table continues…

Message	Description
	• Called party: 20001
`Received CTIOS_VOICE_STREAM_RTPINFO for customer voice_stream for agent with extension 20001, device_id 20001, line_instance 1, call_identifier 1638, remote_call_id 1638, localIP 10.133.204.121, localRTPPort 3456, remoteIP 1.2.3.4, remoteRTPPort 1234, callingParty 20012, calledParty 20001`	The Recorder received voice stream RTP information for customer voice stream with the following details: • Agent extension: 20001 • Device ID: 20001 • Line instance: 1 • Call identifier: 1638 • Remote call ID: 1638 • Local IP address: 10.133.204.121 • Remote IP address: 1.2.3.4 • Remote RTP port: 1234 • Calling party: 20012 • Called party: 20001
`Received VOIP_CTIOS_AGENT_CALL_END_RESPONSE_CODE with end cause AGENT_ENDED`	The Recorder received call end response code that states that the agent ended the call from the signaling adapter based on the deployment.
`Received VOIP_CTIOS_AGENT_CALL_STATE with agentExtension 20001 and agentState ON_HOOK for deviceId 20001`	The Recorder received call state as on hook for agent with extension 20001 and device ID 20001 from the signaling adapter based on the deployment.
`Received VOIP_CTIOS_VOICE_STREAM_STOP_RTPINFO for agent voice_stream of agent with extension 20001, device_id 20001, line_instance 1, call_identifier 1638, remote_call_id 1638, phone_ip 10.133.204.121, calling_party 20012, called_party 20001, call_type INBOUND`	The Recorder received agent voice stream stop RTP information with the following details: • Agent extension: 20001 • Device ID: 20001 • Line instance: 1 • Call identifier: 1638 • Remote call ID: 1638 • Phone IP address: 10.133.204.121 • Calling party: 20012 • Called party: 20001 • Call type: Inbound
`Received VOIP_CTIOS_VOICE_STREAM_STOP_RTPINFO for customer voice_stream of agent with extension 20001, device_id 20001, line_instance 1, call_identifier 1638,`	The Recorder received customer voice stream stop RTP information with the following details: • Agent extension: 20001 • Device ID: 20001

Table continues…

Message	Description
`remote_call_id 1638, phone_ip 10.133.204.121, calling_party 20012, called_party 20001, call_type INBOUND`	• Line instance: 1 • Call identifier: 1638 • Remote call ID: 1638 • Phone IP address: 10.133.204.121 • Calling party: 20012 • Called party: 20001 • Call type: Inbound
`Received VOIP_CTIOS_AGENT_CALL_WRAPUP_DATA with agentExtension 20001 callWrapUpData and lineInstance 1`	The Recorder received call wrap up data for agent with extension 20001, call wrap up data, and line instance 1 from the signaling adapter based on the deployment.

Chapter 10: Troubleshooting

Sysadmin login page displays the Invalid License key message

Condition

While logging into Sysadmin, the system displays the following error message: `Invalid License key`.

Cause

Avaya Workforce Optimization Select does not support the Avaya WebLM version.

Solution

1. Check the Avaya WebLM version.
2. If the version is earlier than 6.5, then reinstall the latest version.

Emails are not delivered to recipients

Condition

When a user sends a report through an email, the recipient does not receive the email.

Cause

The email settings are set incorrectly.

Solution 1

1. Go to the `WFO_Home` folder located at `C:\ProgramData`.

   Note:

   The Program Data folder is a hidden folder. Ensure that you enable the option to show hidden files in folder options.

2. In the `WFO_Home` folder, do the following:
   a. Right-click the `MailConfig.Properties` file.
   b. Select **Open with**, and click **Notepad**.

c. Check whether the following properties are configured correctly:

- mail.smtp.host
- mail.smtp.port
- mail.smtp.auth
- mail.transport.protocol
- mail.smtp.username
- mail.smtp.password
- mail.default.fromAddress
- mail.default.fromName

3. Click **Save** to close the file.
4. Restart the web application service.

Solution 2

1. Restart web application service.
2. Log in to the server that hosts the web application component.
3. Click **Start** > **Run** > **services.msc** > **WebApp Service** > **Start**.

Interaction playback fails

Condition

Interaction playback fails, and the system displays the following error message: `You cannot play this interaction as the audio could not be loaded either because of unsupported file formant or server/ network failure.`

Cause

- Avaya Workforce Optimization Select components cannot find the interaction files at the configured storage location.
- The browser does not support the file format.

Solution 1

1. Confirm that the browser supports HTML5.
2. The following browser version are certified:
   - Internet Explorer 11 and above
   - Google Chrome 43.x and above
   - Mozilla FireFox 33.x and above

Solution 2

1. Verify that the proxy is configured to the correct location where the interactions exist.

2. Go to `C:\Program Files (x86)\Avaya\AWFOS5\Apache24\conf\extra`.
3. Right-click the `httpd-ssl.conf` file.
4. Click **Edit with Notepad ++**.
5. Point the parameter DocumentRoot to the WFO_HOME path.

   DocumentRoot "E:/Avaya_14Feb_FP2/WFO_HOME"
6. Point the parameter Directory to the WFO_HOME path.

   Directory "E:/Avaya_14Feb_FP2/WFO_HOME"
7. Click **Save** to close the file.

Solution 3

1. Start the Media Manager service.
2. Log in to the server that hosts the web application components.
3. Click **Start** > **Run** > **services.msc**.
4. Right-click Media Manager Service and click **Start**.

Solution 4

1. Verify the Media Manager log file.
2. Go to the `Logs` folder at `C:\ProgramData\Logs` or at a location specified during the Avaya Workforce Optimization Select installation.
3. Right-click the `MediaManager.log` file.
4. Click **Edit with Notepad ++**.
5. Check for the message `Sending Response is result=SUCCESS&callURL=https://10.133.202.245:443/default_FLDR/VoiceConvertedFiles/JUDITH%5Fdefault%5FCS1K%5F7002%5F03152016%5F152740%5F000241%5F0%2E50/JUDITH%5Fdefault%5FCS1K%5F7002%5F03152016%5F152740%5F000241%5F0%2E50.wav&scEndCount=324.`

   The message contains a URL with the IP address of the web application server and the voice case ID located at `C:\ProgramData\WFO_Home\default_FLDR\VoiceConvertedFiles`.
6. Change the file format from `.wav` to `.jpeg` in the URL:
7. On the address bar of your browser, type the URL: `https://10.133.202.245:443/default_FLDR/VoiceConvertedFiles/JUDITH%5Fdefault%5FCS1K%5F7002%5F03152016%5F152740%5F000241%5F0%2E50/JUDITH%5Fdefault%5FCS1K%5F7002%5F03152016%5F152740%5F000241%5F0%2E50.jpeg&scEndCount=324.`

   The system displays the audio graph of the interaction.
8. On the address bar of the client browser, type the URL: `https://10.133.202.245:443/default_FLDR/VoiceConvertedFiles/JUDITH%5Fdefault%5FCS1K%5F7002%5F03152016%5F152740%5F000241%5F0%2E50/`

```
JUDITH%5Fdefault%5FCS1K
%5F7002%5F03152016%5F152740%5F000241%5F0%2E50.jpeg&scEndCount=324.
```

The system displays the audio graph of the interaction on the client browser.

9. (Optional) If you get an error message in the `MediaManager.log` file, based on the message information, do the following:
   - Check whether physical file is available in the storage location.
   - Check whether the physical file is encrypted.

Recorder service fails to start

Condition

When a user tries to start the recorder service, the service fails to start.

Cause

The encryption keys are unavailable in the tenant database. After inserting encryption keys ensure that you start the Recorder and Media Manager service.

Solution 1

1. Insert the security keys in the database for encryption and decryption.
2. Go to **Program Files (x86)** > **Avaya** > **AWFOS5** > **Media Manager**.
3. Double-click **EDSecurityKeyGeneration.exe**.
4. On the EDSecurityKeyGeneration page, type the following:
   - **Database IP Address**: The IP address of the server where the database is installed.
   - **Database Name**: The name of the tenant database created during installation.
   - (Optional) **Named Instance**: For named instance deployments.
   - **Database User**: The username created by the installer for encryption and decryption services. The default username is harmonysec.
   - **Database Password**: The password created by the installer for encryption and decryption services. The default password is harmonysec@123.
5. Click **Test connection**.

   The system displays the message `The database is connected successfully.`
6. Click **OK**.
7. Click **Next** to enter the passphrase and the number of keys.

   The system displays the message `Database opened successfully.`

   The passphrase that is used to encrypt and decrypt the public and private keys can be any combination of alphanumeric letters. The number of keys must be maximum 10. For example, alph@123.

8. Click **OK**.
9. Validate the key values and passphrase by checking whether the keys are inserted in the following tables:
   - INTERACTIONS_KEY_VALUE: The table that contains keys to encrypt interactions.
   - INTERACTIONS_KSEDKEY: The table that uses the passphrase you enter to encrypt and decrypt the public and private keys.

Solution 2

1. Start the Recorder and Media Manager service.
2. Log in to the server that hosts the web application components.
3. Click **Start** > **Run** > **services.msc**.
4. Right-click Media Manager Service and click **Start**.
5. Right-click Recorder Service and click **Start**.

Failed to join the instance NODE2 to the availability group AG1

Condition

While setting up the basic availability groups in SQL Server 2016, the system might display the following error message: `Failed to join the instance 'NODE2' to the availability group 'AG1'.(Microsoft.SqlServer.Management.SDK.TaskForms)`

Cause

The endpoint is blocked by firewall.

Solution

1. Ensure that the endpoint Hadr_endpoint on default port 5022 is not blocked by firewall.
2. Confirm the following:
   - Startup account of primary server is added to all the secondary servers
   - Startup accounts of all secondary servers are added to primary servers
   - Startup account of each replica is added to other replicas
3. If the logon account of SQL Server is “Nt service\” or local system account, then, ensure that the system account (Domainname\systemname$) of each replica is added to other replicas.
4. Grant connect on endpoints created on each replicas for startup account of other replica servers (Grant connect on endpoints even if startup account of other replicas are added as sysadmins).
5. Ensure that the SQL Server name (select @@servername) matches with the hostname.
6. Ensure cluster service startup account is part of the SQL Server logins.

Chapter 11: Resources

Documentation

See the following related documents at http://support.avaya.com:

Document number	Title	Use this document to:	Audience
Overview			
	Avaya Workforce Optimization Select Overview and Specification	Provide a high-level functional description of the capabilities of the Avaya Workforce Optimization Select application.	All
Implementing			
	Deploying Avaya Workforce Optimization Select	Provide an end-to-end deployment scenario including all products that must function together, checklists, and initial administration.	Deployment engineers and support personnel
Administering			
	Administering Avaya Workforce Optimization Select	Explain how to use Avaya Workforce Optimization Select to configure your system, employee data, settings, and recording rules and perform routine maintenance tasks. The content is available in two formats: HTML and PDF.	Administrators
Using			
	Using Avaya Workforce Optimization Select	Explain how to use the Avaya Workforce Optimization Select to configure settings such as user preferences, monitor and record interactions, and access and generate reports. The content is available in two formats: HTML and PDF.	Users

Table continues…

Document number	Title	Use this document to:	Audience
	Avaya Workforce Optimization Select Quick Reference Guide for Supervisors	Understand the most common user tasks that a Supervisor performs.	Users
	Avaya Workforce Optimization Select Quick Reference Guide for Call Center Agents	Understand the most common user tasks that an Agent performs.	Users
	Avaya Workforce Optimization Select Quick Reference Guide for QA Analyst	Understand the most common user tasks that a QA Analyst performs.	Users
	Avaya Workforce Optimization Select Quick Reference Guide for Administrators	Understand the most common user tasks that an Administrator performs.	Administrators

Finding documents on the Avaya Support website

Procedure

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

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

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Support

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

Index

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V

W