Deploying Avaya Workforce Optimization Select

Release 5.0
May 2016

© 2016, Avaya, Inc.
All Rights Reserved.

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.

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

Contents

Chapter 1: Introduction 8
Purpose 8
Prerequisites 8
Chapter 2: Avaya Workforce Optimization Select overview 9
Components 9
Adapters 11
Topology 12
Deployment configurations 12
Signaling events 13
Integration scenarios 15
Avaya Aura® Contact Center active recording deployments 16
Avaya Aura® Contact Center passive recording deployments 17
Avaya Contact Center Select passive recording deployments 19
IP Office Contact Center on IP Office deployments 21
Agent profiles 22
Chapter 3: Deployment process 24
Chapter 4: Planning and preconfiguration 25
Planning checklist 25
Key customer configuration information 25
Configuration information for Avaya Workforce Optimization Select installation 25
Configuration information for initial administration of Avaya Workforce Optimization Select 26
Configuration tools and utilities 27
Site preparation 27
Site preparation checklist 27
Downloading software 28
Setting environment variables for Java 31
Installing TSAPI client for Windows 31
Network requirements 32
Port assignments 32
Preinstallation checklist 33
Chapter 5: Initial setup and connectivity 35
Hardware requirements 35
Installing Avaya Workforce Optimization Select 37
Standard Profile 38
Standard Profile field descriptions 38
Required Information field descriptions 39
Mail Server Configuration field description 40
Database Settings field descriptions 40

Configuring high availability 42
Changing the node name for high availability configuration 42
WebLM 43
Chapter 6: Configuration 44
Configuration checklist 44
Configuring the Encryption / Decryption service 45
Configuring browser settings for SSL 46
Configuring browser settings for Internet Explorer 46
Configuring browser settings for Google Chrome 46
Configuring browser settings for Mozilla Firefox 47
Installing and configuring TAPI3 driver 48
Installing the TAPI3 driver 48
Configuring TAPI3 driver 48
Enabling the IP Office TAPI tracing 49
Disabling the IP Office TAPI tracing 50
Modifying default values for logs 50
Configuring proxy IP address for multi server deployments 51
SysAdmin 51
Logging on to SysAdmin 51
Tenant management 52
System administration 53
Logging off from SysAdmin 66
Checklist for configuring Avaya Aura® Contact Center on Communication Manager 66
Avaya Aura® Contact Center on Communication Manager adapter parameters 67
Checklist for configuring Avaya Aura® Contact Center on CS 1000 76
Avaya Aura® Contact Center on CS 1000 adapter parameters 77
Checklist to support WebLM for CS 1000 deployments 84
Checklist for configuring Avaya Contact Center Select on IP Office 84
Avaya Contact Center Select on IP Office adapter parameters 85
Checklist for configuring IP Office Contact Center on IP Office 92
IP Office Contact Center on IP Office adapter parameters 92
Limitations 98
Installing and configuring Desktop Monitor application 101
Screen Capture overview 101
Desktop Monitor application 104
Port mirroring 107
Configuring ESXi Server 107
Configuring NIC driver settings 108
Checklist to change the IP address of servers in DNS deployments 109
Stopping the Avaya Workforce Optimization Select components 109
Changing the node name 109
Starting the Avaya Workforce Optimization Select components 110
Configuring component parameters 110

Restarting the Avaya Workforce Optimization Select components 111
Chapter 7: Initial administration 112
Initial administration checklist 112
Setting passwords for services.msc components 113
Starting the Avaya Workforce Optimization Select web application 114
Routine maintenance 114
Backup and restore 114
Backing up the server data 115
Restoring the data 116
Backing up database files 116
Restoring the database files 117
Replacing self-signed certificates with CA-signed SSL certificates 118
Chapter 8: System verification checklist 119
Chapter 9: Resources 120
Documentation 120
Finding documents on the Avaya Support website 121
Viewing Avaya Mentor videos 122
Support 122
Using the Avaya InSite Knowledge Base 122

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
- Avaya Telephony Platforms such as Application Enablement Services, IP Office, Communication Manager, and Avaya Communication Server 1000 (CS 1000)
- Automatic Call Distribution such as Avaya Aura® Contact Center, Avaya Contact Center Select, and IP Office Contact Center

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

The following components contribute to the successful functioning of every module in Avaya Workforce Optimization Select:

Components

Name	Description
Log Manager	Collects and zips log data into a single zip file to debug issues. 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

Table continues…

Name	Description
	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 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 MP4a (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.

Table continues…

Name	Description
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 and provides adapters to receive signaling and media from phones and Automatic Call Distributor (ACD) (CTIOS) data from ICM components.

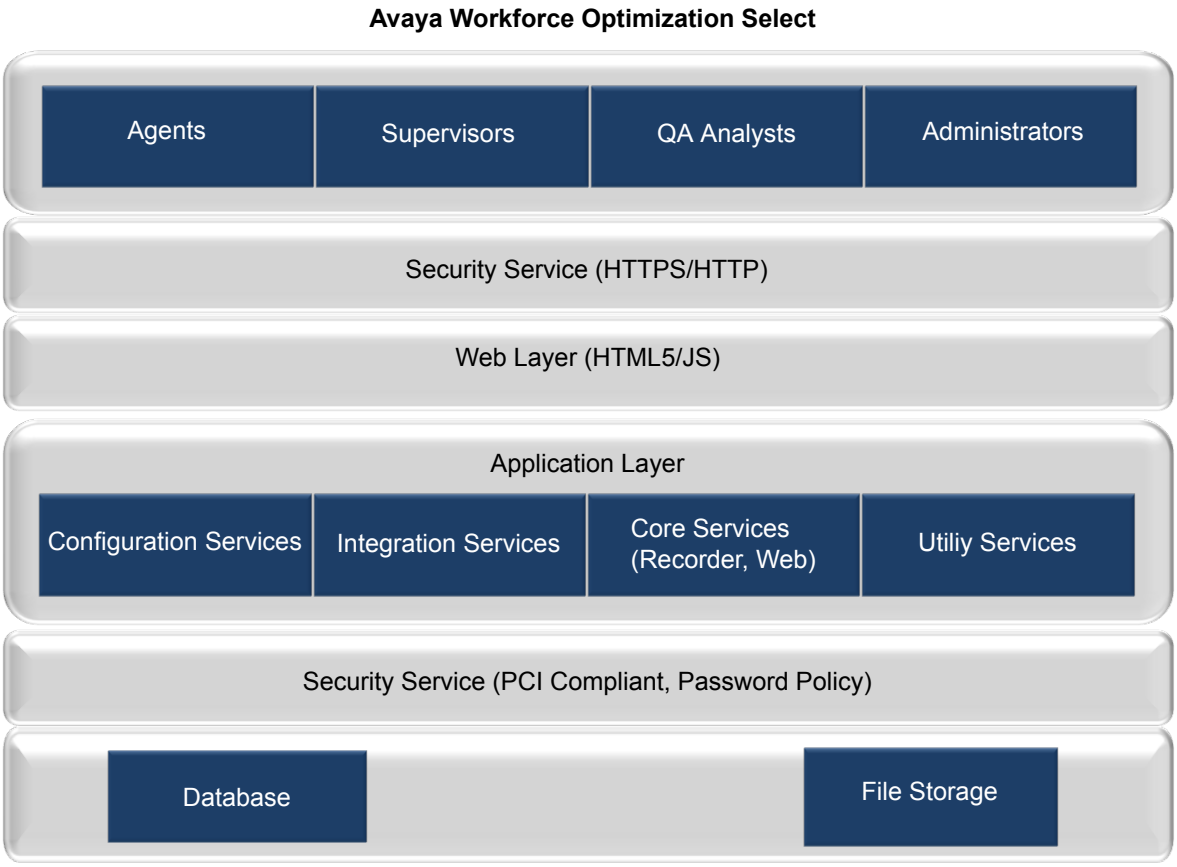
Adapters

The following adapters contribute to the successful functioning of every module in Avaya Workforce Optimization Select:

	Description
Avaya adapter	Connects to Device Media and Call Control (DMCC) service in a single-step conference or multiple registration mode. The adapter collects and sends voice stream information to the Recorder. Avaya adapter also connects to Avaya Aura® Contact Center and IP Office Contact Center to receive and send call signalling and voice streams to the Recorder.
AES adapter	Monitors skill or hunt groups in an Avaya 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.
Avaya CCTNet adapter	Collects Automatic Call Distributor (ACD) events from one or more Avaya Aura® Contact Center or Avaya Contact Center Select servers to the recorder. The adapter connects to the server through the Control Communication Toolkit API.
TAPI adapter	Provides the interface between computer telephony applications and telephony services. TAPI adapter connects to Avaya IP Office server and collects and sends call signalling information to Recorder using TAPI API.

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, with up to 50 users, 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. A single server supports up to 100 agents.

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 server 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
- Voice or RTP
- Agent information and external call variables to tag interaction to agents as per business rules

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.

Voice or RTP

Voice packets or streams reproduce or play what the agent and customer speak over the phone. The Avaya Workforce Optimization Select recorder saves the voice data in a file and names the file with a proper naming convention called the Voice Case ID. Voice is received on a UDP port.

Agent information and external call variables

The Avaya Workforce Optimization Select recorder needs the agent information and external call variables to tag an interaction for 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 info or extended call info, and wrapup data are the events that the recorder tags.

Active recording

Avaya Workforce Optimization Select gets call signaling, voice, agent information, and external call variables in Avaya Active Recording.

Avaya Workforce Optimization Select uses Device Media and Call Control to get voice streams and passes the voice streams to the recorder for recording an interaction. Avaya Workforce Optimization Select uses AES adapter, TAPI adapter, Avaya CCTNet adapter, and Avaya adapter to get agent information and call signaling.

Avaya Workforce Optimization Select allows capturing Voice, Digital, or Analog stations. When you start the Avaya Workforce Optimization Select application registers the virtual IP soft phones with Avaya Aura® Communication Manager. The virtual phones monitor the target stations when inbound calls are received by the target stations. Avaya Workforce Optimization Select uses TSAPI events to trigger the single step conference or the multiple registration request for capturing media. Avaya Aura® Application Enablement Services receives the call signaling information from Communication Manager and then passes the call signaling information to the recorder.

Passive recording

Avaya Workforce Optimization Select gets call signaling, voice, agent information, and external call variables in Avaya Passive Recording.

Avaya Workforce Optimization Select recorder uses SPAN to get voice and AES adapter, TAPI adapter, Avaya CCTNet adapter, and Avaya adapter to get call signaling and agent information. The

call comes from the PSTN and is received by G450 Branch Gateway. The IP phones registered to the CLAN board on G450 Branch Gateway interact with Communication Manager to understand which phone the call must be transferred to. The call traverses through a layer 2 switch to the IP phones. On the Layer 2 switch, the port is configured as SPAN, which mirrors the voice RTP and gives it to the Avaya Workforce Optimization Select recorder. Avaya Aura® Application Enablement Services receives the call signaling information from Communication Manager and then passes the call signaling information to the Avaya Workforce Optimization Select recorder.

Integration scenarios

Avaya Workforce Optimization Select supports integration with Avaya Aura® Contact Center (AACC), Avaya Contact Center Select, and IP Office Contact Center.

Avaya Aura® Contact Center

Avaya Aura® Contact Center offers a comprehensive suite of scalable solutions for dynamic contact center environments. AACC provides skill-based routing of voice, email, web chat, FAX, SMS, scanned documents, and support for video contacts.

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. This 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, call treatments, reporting, unified agent management, and graphical Orchestration Designer utility.

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, email, and outbound capabilities.

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 Workforce Optimization Select deployments

Avaya Workforce Optimization Select supports the following deployments:

- Avaya Aura® Contact Center active recording deployments
  - Avaya Aura® Contact Center on Communication Manager
  - Avaya Aura® Contact Center on CS 1000

- Avaya Aura® Contact Center passive recording deployments
  - Avaya Aura® Contact Center on Communication Manager
  - Avaya Aura® Contact Center on CS 1000
- Avaya Contact Center Select passive recording deployments
  - IP Office extension based recording
  - Avaya Contact Center Select on IP Office
- IP Office Contact Center on IP Office deployment

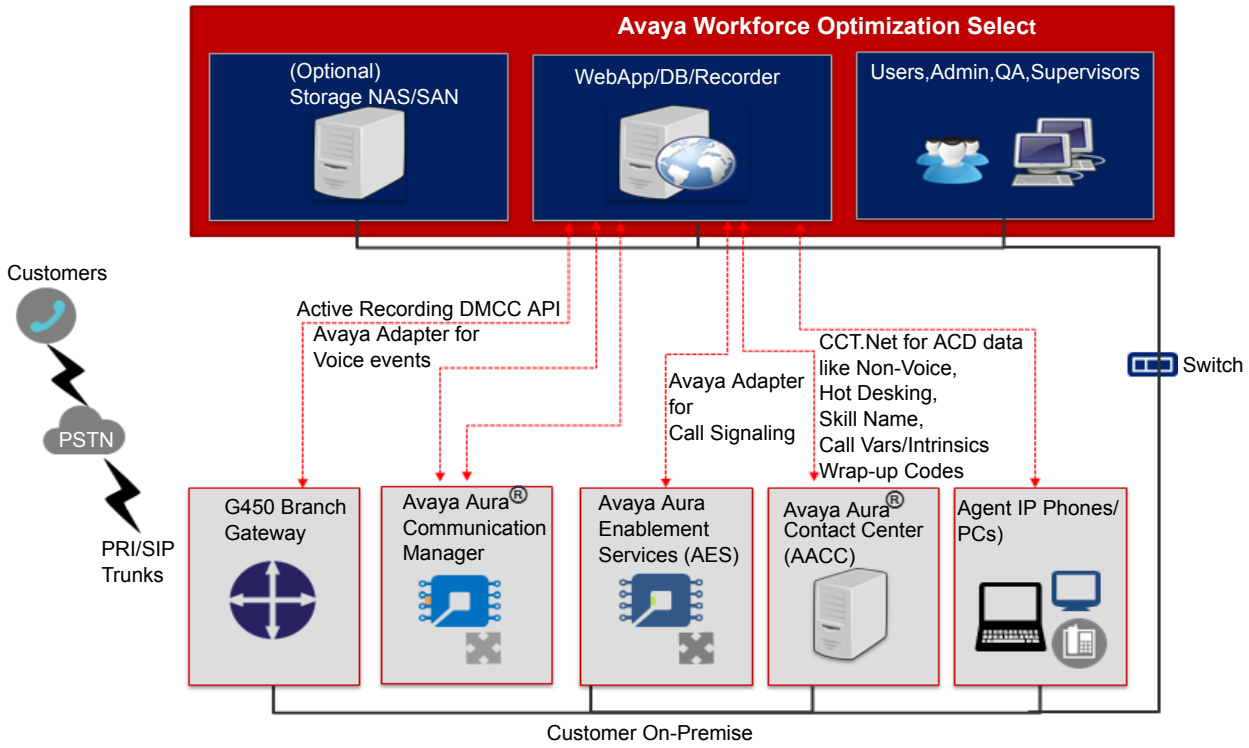
Note:

Secure RTP is not supported in any deployment.

Avaya Aura® Contact Center active recording deployments

Avaya Aura® Contact Center integration supports the following deployment scenarios for active recording:

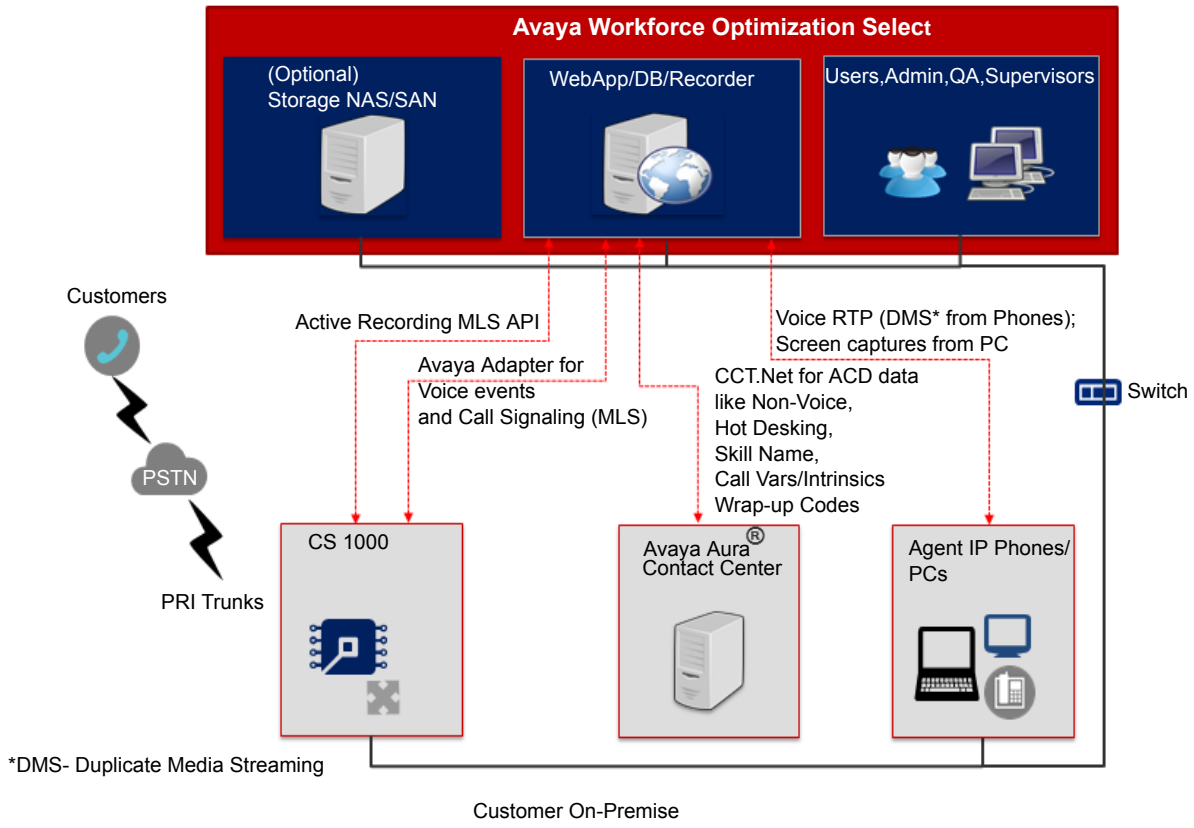
AACC-CM/Agent and extension-based recording



In active recording, the Avaya Workforce Optimization Select Recorder uses Avaya adapter to get voice, AES adapter to get call signaling, and Avaya CCTNet adapter to get business data. The call comes from the PSTN and lands on Avaya Aura® Communication Manager. The call is then routed to the available agent phone. Avaya Aura® Application Enablement Services receives the call

signaling information from Communication Manager and then sends it to the Avaya Workforce Optimization Select Recorder. The call traverses through a layer 2 switch to the IP phones.

CS 1000/AACC/Agent and extension-based recording

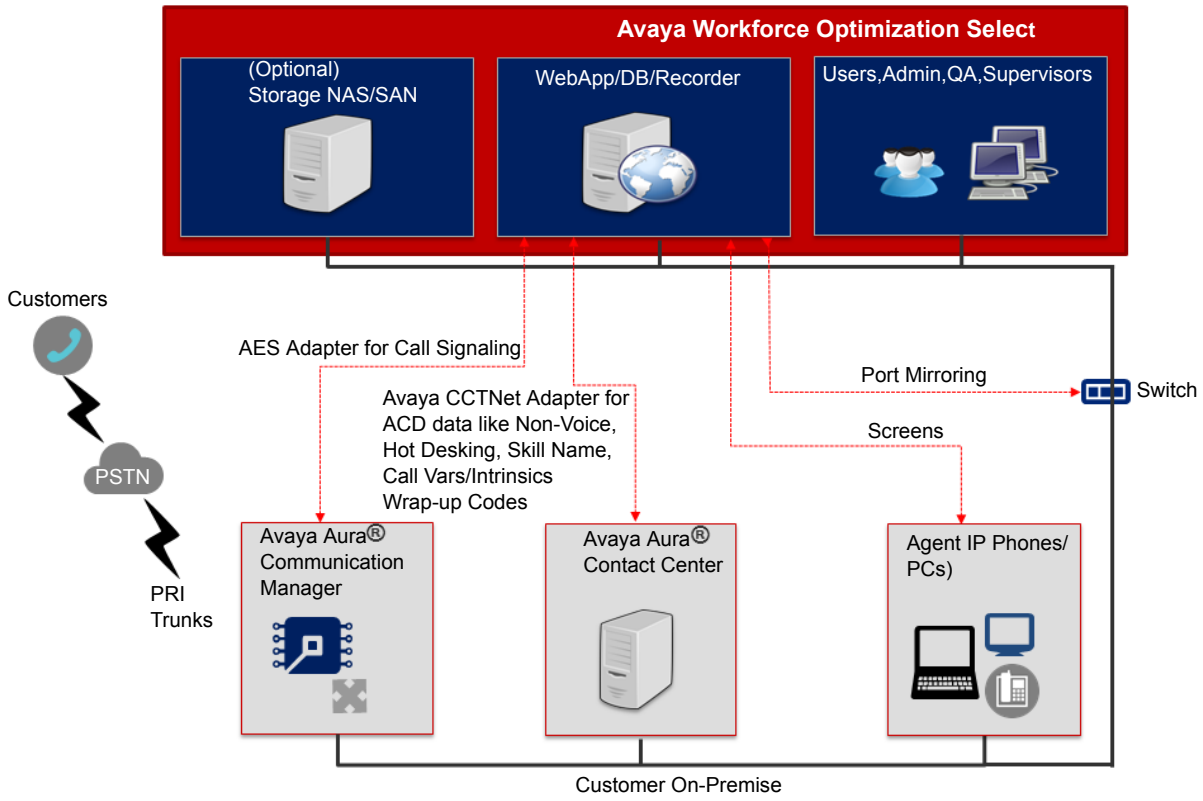


Avaya Communication Server 1000 (CS 1000) uses the Meridian Link Service (MLS) interface to get voice, call signaling, and business data. MLS is an API that fetches and passes call events to CS 1000. Because Avaya Aura® Contact Center and CS 1000 are connected to each other in the deployment itself, CS 1000 sends the information received from MLS to Avaya Aura® Contact Center. Thus, the Avaya Workforce Optimization Select Recorder uses Avaya adapter to get voice and call signaling. The recorder gets business data from Avaya Aura® Contact Center through Avaya CCTNet adapter. The call comes from the PSTN and lands on CS 1000. The call is then routed to the available agent phone. CS 1000 routes the call to Avaya Aura® Contact Center and Avaya adapter receives the call information from Avaya Aura® Contact Center.

Avaya Aura® Contact Center passive recording deployments

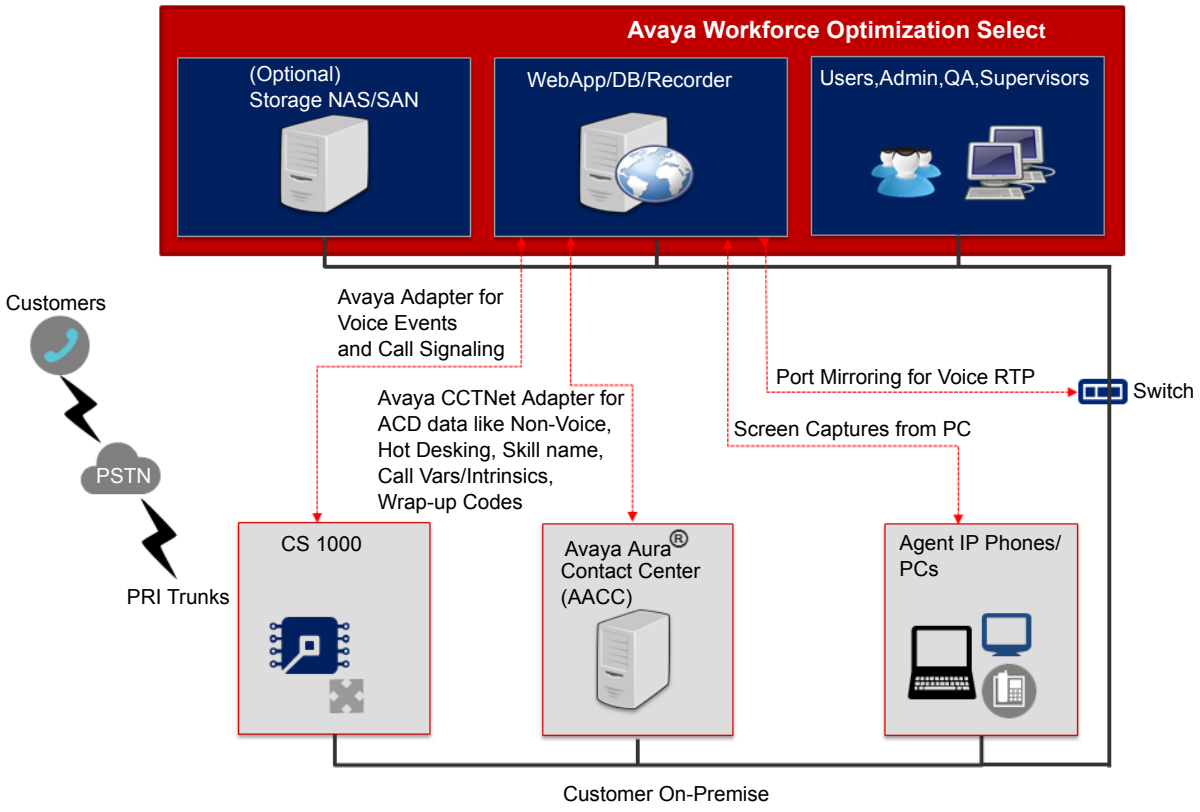
Avaya Aura® Contact Center integration supports the following deployment scenarios for passive recordings:

AACC on Communication Manager/SPAN/Agent and extension-based recording



The Avaya Workforce Optimization Select Recorder uses SPAN to get voice and AES adapter to get call signaling. Additionally, you can configure the Avaya CCTNet adapter to get business data. The call comes from the PSTN and lands on Avaya Aura® Communication Manager. The call is then routed to the available agent phone. Avaya Aura® Application Enablement Services receives the call signaling information from Communication Manager and then sends it to the Avaya Workforce Optimization Select Recorder. The call traverses through a layer 2 switch to the IP phones. On the Layer 2 switch, a port is configured as SPAN, which mirrors the voice RTP and sends it to the Avaya Workforce Optimization Select Recorder.

CS 1000/AACC/SPAN/Agent and extension-based recording

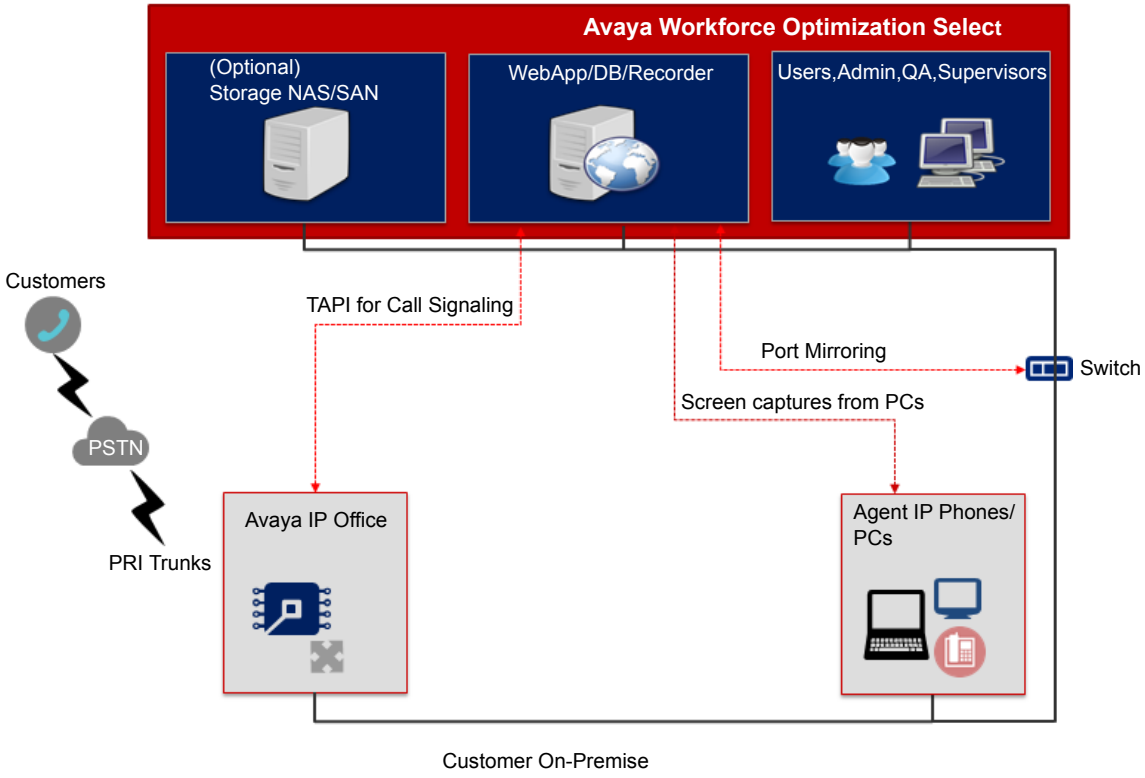


Avaya Communication Server 1000 (CS 1000) uses the Meridian Link Service (MLS) interface to get voice, call signaling, agent information, and business data. MLS is an API that fetches and passes call events to CS 1000. Because AACC and CS 1000 are connected to each other in the deployment itself, CS 1000 sends the information received from MLS to AACC. Thus, the Avaya Workforce Optimization Select Recorder uses Avaya adapter to get voice and call signaling. The recorder gets business data from Avaya Aura® Contact Center through Avaya CCTNet adapter. The call comes from the PSTN and lands on CS 1000. The call is then routed to the available agent phone. CS 1000 routes the call to AACC and Avaya adapter receives the call information from AACC. The call traverses through a layer 2 switch to the IP phones. On the Layer 2 switch, a port is configured as SPAN, which mirrors the voice RTP and sends it to the Avaya Workforce Optimization Select Recorder.

Avaya Contact Center Select passive recording deployments

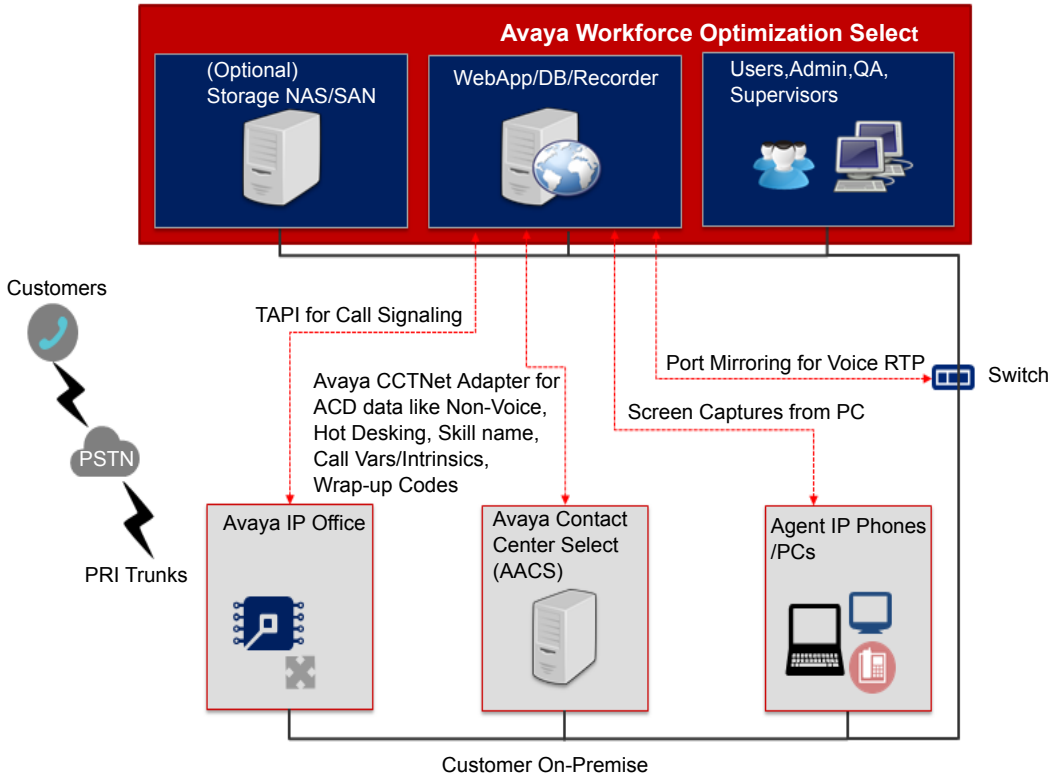
Avaya Contact Center Select integration supports the following deployment scenarios for SPAN-based passive recordings:

IPO/extension based recording



The Avaya Workforce Optimization Select Recorder uses SPAN to get voice and TAPI adapter to get call signaling information and phone extension information. The call comes from the PSTN to Avaya IP Office. Avaya IP Office then routes the call to relevant phone extensions configured in IP Office. After the call lands on the extension, the corresponding desk phone is registered with Avaya IP Office. The call traverses through a layer 2 switch to the IP phones. On the Layer 2 switch, a port is configured as SPAN, which mirrors the voice RTP and sends it to the Avaya Workforce Optimization Select Recorder. Call signaling-related information is sent by Avaya IP Office to Avaya Workforce Optimization Select using the TAPI adapter.

ACCS-IPO/Agent and extension-based recording

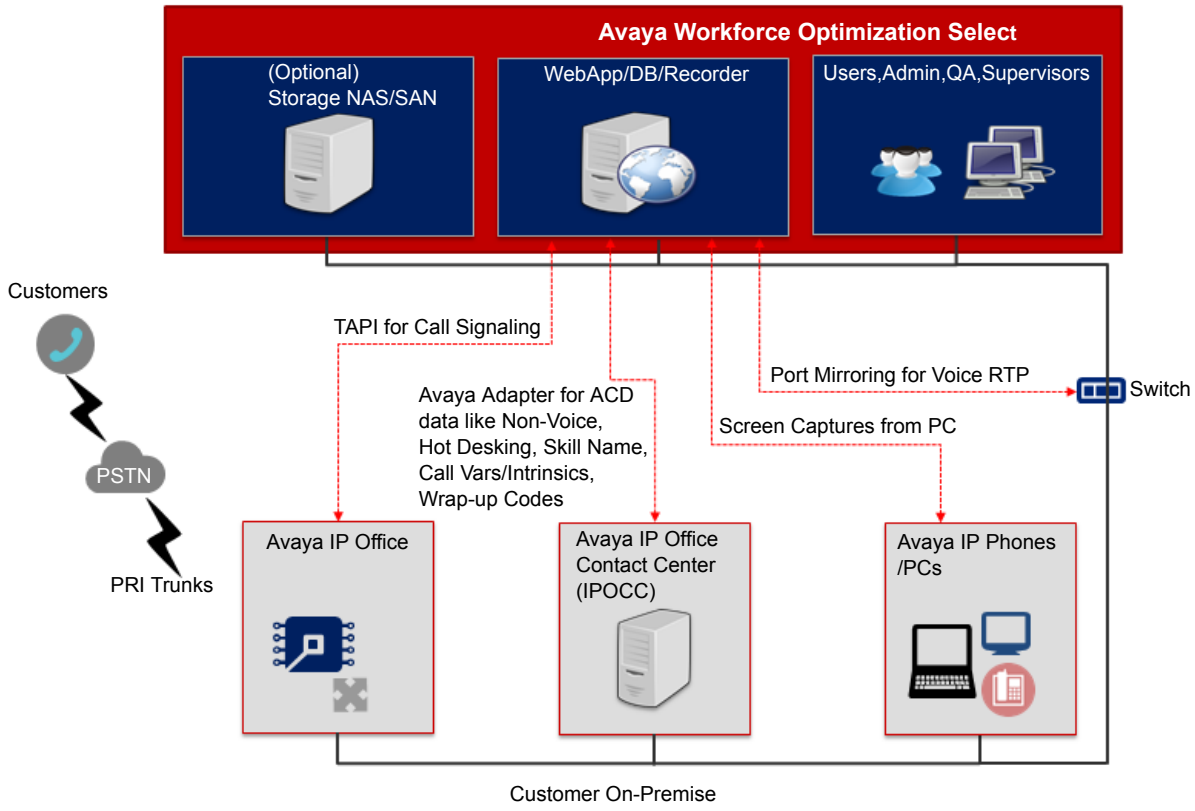


The Avaya Workforce Optimization Select Recorder uses SPAN to get voice, TAPI adapter to get call signaling information, and Avaya CCTNet adapter to get agent information and business data. The call comes from the PSTN to Avaya IP Office. Avaya IP Office then routes the call to Avaya Contact Center Select. Avaya Contact Center Select gets the Control Directory Number (CDN) information from the call and queues the call to the respective skill. After an agent is available for that skill, the call is routed to the agent. The agent receives an active call on Avaya Aura®Agent Desktop and on its corresponding deskphone registered with Avaya IP Office. The call traverses through a layer 2 switch to the IP phones. On the Layer 2 switch, a port is configured as SPAN, which mirrors the voice RTP and sends it to the Avaya Workforce Optimization Select Recorder. Avaya Contact Center Select sends information related to Automatic Call Distribution (ACD) to the Avaya Workforce Optimization Select Recorder through Avaya CCTNet adapter. Call signaling-related information is sent by Avaya IP Office to Avaya Workforce Optimization Select using the TAPI adapter.

IP Office Contact Center on IP Office deployments

IP Office Contact Center integration supports the following deployment scenario for SPAN-based passive recordings:

IPOCC-IPO/Agent and extension based recording



The Avaya Workforce Optimization Select Recorder uses SPAN to get voice, TAPI adapter to get call signaling information, and Avaya adapter to get agent information and business data. The call comes from the PSTN to Avaya IP Office. Avaya IP Office routes the call to Avaya IP Office Contact Center. Avaya IP Office Contact Center queues the call to the respective skill. After an agent is available for that skill, the call is routed to the agent. The agent receives a call on the IP Office Contact Center agent UI and on its corresponding deskphone registered with Avaya IP Office.

The call traverses through a layer 2 switch to the IP phones. On the Layer 2 switch, a port is configured as SPAN, which mirrors the voice RTP and sends it to the Avaya Workforce Optimization Select Recorder. Avaya IP Office Contact Center sends the Automatic Call Distribution (ACD) related information to the Avaya Workforce Optimization Select Recorder through Avaya adapter. Call signaling-related information is sent by Avaya IP Office Contact Center to Avaya Workforce Optimization Select using the TAPI 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.

In CS 1000 deployments, for free seating, calls on position ID will be assigned to an agent ID.

You can configure agent profiles for fixed seating and free seating in 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.

For CS 1000 deployments, the Voice Settings for each employee must have:

- The position ID as the agent ID in one instance
- The extension or DN in another instance.

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 for each employee profile must specify the following:

- The agent ID for one employee profile
- The extension or DN for the second employee profile

For CS 1000 deployments, you must have two employee profiles and the Voice Settings for each profile must specify:

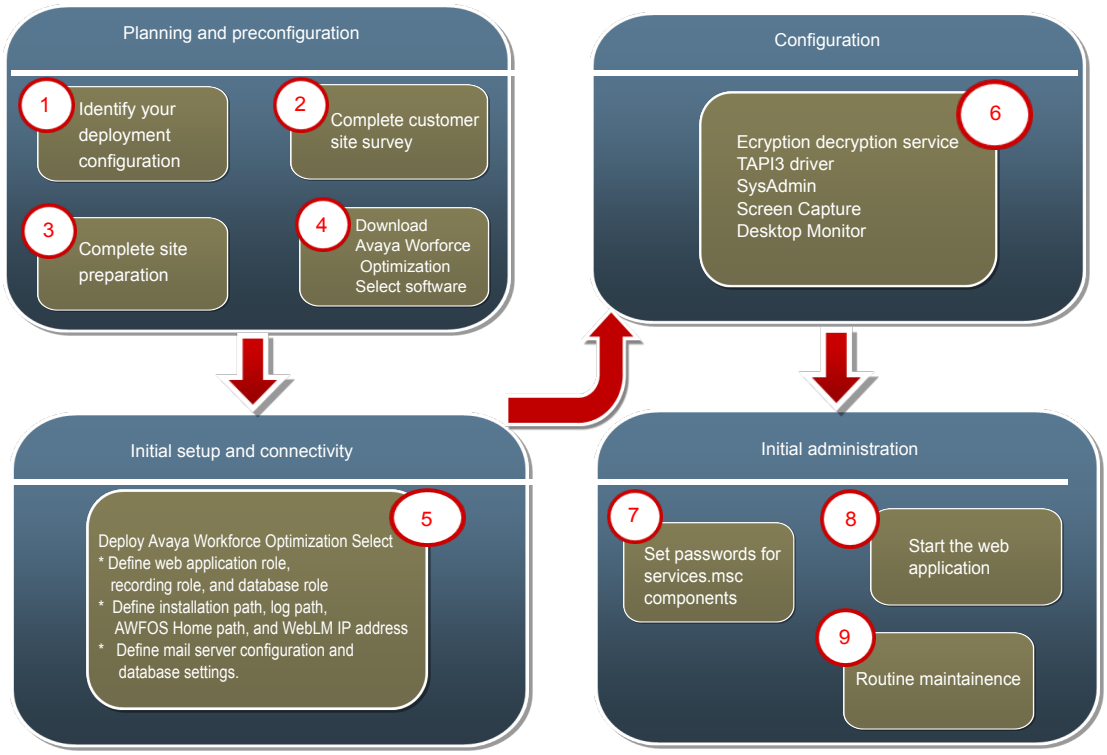
- The agent ID for one employee profile
- The position ID as the agent ID in one instance of the second profile
- The extension or DN in another instance of the second profile

Note:

For free seating environment in CS 1000 deployments, the profile created for the agent ID and the profile created for the position ID and extension should not belong to the same site.

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 120.		
2	Gather customer configuration information.	See Configuration information for Avaya Workforce Optimization Select installation on page 25.		
3	Plan for site preparation.	See Site preparation checklist on page 27.		

Key customer configuration information

Configuration information for Avaya Workforce Optimization Select installation

General Network Settings configuration

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

Name	Value	Description
Default Gateway		The default gateway IP address.
Primary DNS		The primary Domain Name System (DNS) server address.
Secondary DNS		The secondary DNS server address. This is optional.
VLAN		The Virtual Local Area Network (VLAN) IP address of the server where Avaya Workforce Optimization Select is installed.

Table continues…

Name	Value	Description
Static IP Address for Standard Network Access		The IP address to access the standard network.
Static IP Address for Packet Sniffing Interface		The IP address of the server where voice packets are to be sniffed or dumped.

Virtual Machine configuration

Name	Value	Description
Enable Services VM		• Enables or disables remote access. • Supports local or centralized alarm reporting. **Important:** By default, this parameter is Enabled.
Hostname		The name assigned to the services virtual machine.
Static IP Address		The IP address assigned to the services virtual machine.
Virtual Devices		The virtual device port assigned to the services virtual machines.

Database configuration

Name	Value	Description
Database Name		The name of the database that points to the Web application and ICM components. By default the AWFOSDB appears while installing Avaya Workforce Optimization Select. However, you can edit the database name.
Database IP Address		The IP address 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.

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.

Configuration tools and utilities

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

Site preparation

Site preparation checklist

No.	Task	Reference	✔
1	Obtain the Avaya Workforce Optimization Select software.	See Downloading software from PLDS on page 30.	
2	Install the mandatory third party utilities such as Wireshark, WinPCap, 7 Zip, Open JDK, Visual C++ Redistributable, and TAPI3 driver. 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 28.	
3	Download Java security files to `C:\Program Files\Java\JDK8u76\jre8\lib\security`.	See Required software for Avaya Workforce Optimization Select on page 28.	
4	Add environment variables for Java path if you are installing the Avaya Workforce Optimization Select application on Windows 2008 R2 server.	See Setting environment variables for Java on page 31.	

Table continues…

No.	Task	Reference	✔
5	Install TSAPI client for 32–bit Windows if the deployment is for Avaya Aura® Contact Center on Communication Manager.	See Installing TSAPI client for Windows on page 31.	
6	Ensure that network considerations are met.	See Network considerations on page 32.	
7	Configure ports.	See Port assignments on page 32.	
8	Ensure that all pre-installation requirements are met.	See Pre-installation checklist on page 33.	
9	Obtain the license types required for your specific deployment configuration.	See the “Licensing Requirements” chapter in *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	-

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
Windows Server	2008 R2 and 2012 SP2 (64–bit OS)	-
Open SSL	1.0.2e	Open SSL: https://slproweb.com/products/Win32OpenSSL.html

Table 4: Database

Software	Supported version	Notes
SQL Server	2008 R2 SP1/2012 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	-
FireFox	42	-
Chrome	46	-
Citrix or terminal services	-	-
HTML 5 media player	-	-
Graphic and sound card	-	-
Screen capture application	-	-

Table 7: Third party software

Utilities	Supported versions	Location
Wireshark	1.12.8 Windows 64–bit	Server on which the recorder is installed. For example, `C:\Program Files\WireShark`. Wireshark software download link: https://www.wireshark.org/download.html.
WinPCap	4.1.3	Server on which the recorder is installed. For example, `C:\Program Files\WinPCap`.
Notepad++	Latest version	All servers.
7 Zip	Latest version	All servers.
Open JDK	8u76 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: https://jdk8.java.net/download.html
TAPI3 driver	1.0.6	Server where TAPI adapter is installed. TAPI 3 driver download link: https://www.devconnectprogram.com/site/global/downloads/index.gsp?item=ceafc6c9-a37f-4258-8f20-b50573aa1449.
TSAPI client for Windows	6 or 7 32–bit Windows	Server where AES adapter is installed. TSAPI client download link: https://www.devconnectprogram.com/site/global/products_resources/

Table continues…

Utilities	Supported versions	Location
		avaya_aura_application_enablement_services/interfaces/tsapi/releases/7_0/index.gsp

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

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. Create an environment variable named JAVA_HOME that points to the Java directory installed on the machine (64-bit).
5. Mention the path of the Java installed up to the Bin folder.

   For example,`C:\Program Files\Java\JDK 8u76`
6. 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.
7. Extract and place the Java security files in the `C:\Program Files\Java\JDK 8u76\jre/lib/security` folder.
8. 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`.

Installing TSAPI client for Windows

About this task

For Avaya Aura® Contact Center on Communication Manager deployments, ensure you install TSAPI client on the server where AES adapter is installed.

Procedure

1. Download the `setup.exe` from https://www.devconnectprogram.com/site/global/products_resources/avaya_aura_application_enablement_services/interfaces/tsapi/releases/7_0/index.gsp.
2. Double-click the `setup.exe` file and click **Next**.
3. Select the license agreement option and click **Next**.
4. Click **Browse** to specify the destination folder and click **Next**.
5. Enter **Host Name or IP Address** of the AES server and click **Add to List**.

   Note:

   Do not change the default value of the **Port Number**.
6. Click **Next**.
7. Click **Install**.
8. Click **Finish**.

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 the ports shown in the following table.

Note:

The port numbers listed in the following table are mandatory. Do not make any changes to these numbers.

The same ports are also applicable to virtual machines.

Port	Protocol	Description	Direction
443	TCP	The Avaya Workforce Optimization Select application service port number	Bi-directional
9280	TCP	The SysAdmin port number	Bi-directional
80	TCP	The Apache web proxy port number	Bi-directional
4444	UDP	The live interactions port number	Bi-directional
25500	TCP	The screen upload server port number	Bi-directional
55000	TCP	The screen capture application port number	Bi-directional
33000	TCP	The screen capture monitor port number	Bi-directional
25	TCP	The mail server port number	Bi-directional
33035	TCP	The alert manager port number	Bi-directional
33025	TCP	The media manager port number	Bi-directional
33072	TCP	The storage manager port number	Bi-directional
33047	TCP	The ED service port number	Bi-directional
33027	TCP	The File Upload Server port number	Bi-directional
33028	TCP	The Upload Server port number	Bi-directional
33055	TCP	The Process Checklist port number	Bi-directional
33029	TCP	The TAPI adapter port number	Bi-directional
33008	TCP	The local or remote failover server port number	Bi-directional
33049	TCP	The CRM request handler port number	Bi-directional
33024	TCP	The user login handler server port number	Bi-directional
33066	TCP	The media manager server silent monitoring port number	Bi-directional
8443	TCP	The apache port number	Bi-directional
34301	TCP	The Avaya CCTNet adapter port number of Messaging proxy	Bi-directional
33012	TCP	The AES adapter port number	Bi-directional
4721	TCP	The DMCC port number	Bi-directional

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.	-	

Table continues…

No.	Task	Reference	✔
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 your network administrator configures a valid mail server.	-	
4	Ensure that the sound card is available on client machines to listen to live and recorded interactions.	-	
5	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.	-	
6	Install SQL 2008 R2 SP1/2012, 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 ICM components on the same drive to avoid performance issues.	-	
7	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.	-	
8	Install the mandatory third party utilities such as Wireshark, WinPCap, 7 Zip, Open JDK, and TAPI3 driver. 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 28.	
9	Set the environment variables for Java.	See Setting environment variables for Java on page 31.	
10	Install TSAPI client for 32–bit Windows if the deployment is for Avaya Aura® Contact Center on Communication Manager.	See Installing TSAPI client for Windows on page 31.	
11	Ensure there is enough space in the drive in which you want to store voice files.	-	
12	Ensure that your network administrator configures spanning on Virtual Local Area Network (VLAN), Gateway, or Port level on the recording servers.	-	
13	Disable Windows Automatic updates on all the servers and schedule them before installing Avaya Workforce Optimization Select or before installing or running antivirus. Ensure that Windows Automatic updates is a planned activity.	-	
14	Install and run antivirus before you install 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 • Windows 2008 SP2 / 2012 64–bit Standard Edition Server OS • SQL Server 2008 R2 SP1 / 2012 64–bit Standard Edition	• 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	• Requires one VM Recorder instance for every 250 concurrent G.711 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
	• 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 • Windows 2008 SP2 / 2012 64–bit Standard Edition Server OS	
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 • Windows 2008 SP2 / 2012 64–bit Standard Edition Server OS • SQL Server 2008 R2 SP1 / 2012 64–bit Standard Edition	• 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
- A minimum of 50 MB
- Microsoft .NET Framework 3.5 SP1
- Microsoft Visual Studio 2008 Professional or Developers Edition SP1 (Development/Studio only)

- Integrator, Desktop or Studio, Discovery

Installing Avaya Workforce Optimization Select

About this task

Avaya Workforce Optimization Select supports the following deployments:

- Single server: You must install a web application, database, recorder, and the ICM components on one server.
- Multiserver: You must install the web application, database, and recorder components on different servers.

Before you begin

- Install SQL 2008 R2 SP1/2012 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**.
3. In the Setup Type window, select one of the following:
   - **Standard**
   - **Custom**
4. Click **Next**.
5. **(Optional)** If you selected **Standard** in the Standard Profile window, select one of the following:
   - **Web Application Role**
   - **Recording Role**
   - **Database Role**
6. Click **Next**.
7. **(Optional)** If you selected **Custom** in the Custom Setup window, select the components that you want to install.
8. Click **Next**.
9. In the Required Information window, configure the required fields.
10. Click **Next**.

11. In the Mail Server Configuration window, configure the required fields.
12. In the Database Settings window, configure the required fields.

    Note:

    Ensure that you restart all the services with the administrator user privileges.
13. Click **Next**.

    The system displays the Installation Summary screen. You can review or change any installation setting.
14. Click **Install**.

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

    When the installation is complete, the system displays the InstallShield Wizard Completed window.
15. Click **Finish**.

Standard Profile

Using the Standard Profile installation, you can install the web application, database, and recorder components on a single server. To install the web application, database, and recorder on separate server, select the appropriate role and install accordingly on the appropriate server.

For example, if you want to install the recorder on a separate server, select only the **Recording Role**. Similarly, select the **Web Application Role** and **Database Role** if you want to install the web application and database on one server.

Standard Profile field descriptions

Name	Description
Web Application Role	The role to install and access the web application. The options are: • **Web**: 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: - IP Office

Table continues…

Name	Description
	- Communication Manager - CS1000 • **Automatic Call Distributor (ACD)**: The telephony platform options are: - For IP Office, select ACCS or IPOCC. - For Communication Manager, select AACC. - For CS1000, select AACC.
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.

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.
Logs Path	The location of the log files. A log file records the event occurrence during a software or product runtime.
WFO_Home Path	The location of the master database. Database files such as mdf and ldf are saved in this location.
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 where the web application for Avaya Workforce Optimization Select must be installed.
Proxy Server IP Address / Hostname	The IP address or hostname of the proxy server where the web application for Avaya Workforce Optimization Select is to be installed. 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

Table continues…

Name	Description
	name. For more information, see Changing the node name on page 42.
Proxy Port Number	The port number of the proxy server that enables web login and call playback. The default port used is 80. Changing the port number will require change in the parameter configurations for components such as recorder, media manager, and messaging. **Note:** Do not use port number 443.
Server FQDN	The fully qualified domain name of the server. The server can be used to install web application, ICM components, or database.

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 POP3.
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 ICM 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.

Table continues…

Name	Description
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.
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.

Configuring high availability

About this task

Use this procedure to configure high availability for all servers where Avaya Workforce Optimization Select. is installed.

Note:

The `WFO_Home` path must be same in all high availability servers to maintain data consistency.

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 **Stop**.
4. Go to the `WFO_Home` folder located at `C:\Program Data\WFO_Home`.
5. In the `WFO_Home` folder, right-click the `WebappConfig.Properties` file, select **Open with**, and click **Notepad**.
6. Search for the following files and replace the IP address with the floating or virtual IP address:
   - `ProxyIp`
   - `WebappGenericAccessUrl`
   - `webapp.imagesURL`
   - `webapp.ksHomeAccessURL`
7. Click **Save** to close the file.
8. 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 42.

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`.

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: Configuration

Configuration checklist

No.	Task	References	✔
1	Configure the Encryption/Decryption (ED) service.	See Configuring the Encryption / Decryption service on page 45.	
2	Configure browser settings for SSL	See • Configuring browser settings for Internet Explorer on page 46 • Configuring browser settings for Google Chrome on page 46 • Configuring browser settings for Mozilla Firefox on page 47	
3	Install the TAPI3 driver.	See Installing the TAPI3 driver on page 48.	
4	Configure the TAPI3 driver.	See Configuring TAPI3 driver on page 48.	
5	Enable the IP Office TAPI tracing.	See Enabling the IP Office TAPI tracing on page 49.	
6	Modify the default values for logs.	See Modifying default values for logs on page 50.	
7	Configure the proxy IP address for multi server deployments.	See Configuring proxy IP address for multi server deployments on page 51.	
8	Configure SysAdmin.	See SysAdmin on page 51.	
9	Install Screen Capture.	See Screen Capture overview on page 101.	
10	Install the Desktop Monitor application.	See Desktop Monitor application on page 104.	

Configuring the Encryption / Decryption service

About this task

Use this procedure to set environment variables for the Encryption / Decryption (ED) service and connect to OpenSSL to generate secure keys for encryption.

Procedure

1. Go to `https://slproweb.com/download/Win32OpenSSL-1_0_2e.exe`, and download the `OpenSSL` 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**.
9. Click **Program Files (x86)** > **Media Manager** and place the `EDSecurityKeyGeneration.exe` file in the `WFO_Home` folder.
10. Double-click **EDSecurityKeyGeneration.exe**.
11. On the EDSecurityKeyGeneration page, type the required details for the fields.
12. Click **Test connection**.

    The system displays the `The database is connected successfully` message.
13. Enter the passphrase and the number of keys and click **OK**.

    The passphrase that is used to encrypt and decrypt the public and private key can be any combination of alphanumeric letters. The number of keys must be maximum 10.
14. Validate the key values and passphrase by checking the INTERACTIONS_KEY_VALUE and INTERACTIONS_KSEDKEY tables respectively.

    The INTERACTIONS_KEY_VALUE table contains keys to encrypt interactions and the INTERACTIONS_KSEDKEY table 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 the 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 **Certificate information**.
4. Click the **Details** tab and click **Copy to File**.
5. Click **Next**.
6. Select **Base64 encoded X.509 (.CER)**.
7. Click **Next**.
8. Click **Browse** and specify the file name that you want to export to the desktop.
9. Click **Save**.
10. Click **Next** and click **Finish**.
11. Go to the saved folder and double click the certificate.
12. Click **Install Certificate**.
13. Select the **Place all certificates in the following store** check box.
14. Click **Browse** and select **Trusted Root Certification Authorities**.
15. Click **Finish**.

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 Firefox browser.

Installing and configuring TAPI3 driver

Installing the TAPI3 driver

About this task

Install TAPI3 driver on the server where TAPI adapter is installed.

Procedure

1. Download the `tapi3Setup.exe` from https://www.devconnectprogram.com/site/global/downloads/index.gsp?item=ceafc6c9-a37f-4258-8f20-b50573aa1449.
2. Double-click the `tapi3Setup.exe` file and click **Next**.
3. Enter the **User Name**, **User Password**, and **IP Address** of the server to which the TAPI driver needs to connect.
4. **(Optional)** If you come across the following error message: `Unable to detect IP Office address`, while installing TAPI3 Driver, enter the username, password, and IP address of Avaya IP Office
5. Click **Next**.
6. Click **Install**.
7. Click **Yes** to restart the server.
8. Click **Install** after restarting the server.

Configuring TAPI3 driver

About this task

Use this procedure to configure the TAPI3 driver so that the TAPI adapter receives call signaling from Avaya IP Office (IP Office) and sends to the Recorder.

Procedure

1. Click **Start** > **Control Panel**.
2. Click **Phone and Modem** on the Avaya Workforce Optimization Select server that runs the TAPI adapter component.
3. On the Phone and Modem page, in the **Advanced** tab, click **Avaya IP Office TAPI3 Service Provider**.
4. Click **Configure**.
5. On the Avaya TAPI configuration page, in the **Switch IP Address** field, type the IP address of IP Office.
6. Select **Third Party**.
7. In the **Switch Password** field, type the password of the IP Office System.

Next steps

Restart the Avaya Workforce Optimization Select server.

Related links

Starting the Avaya Workforce Optimization Select web application on page 114

Enabling the IP Office TAPI tracing

About this task

Use this procedure to enable debugging and tracing on the Avaya IP Office (IP Office) TAPI driver. To enable debugging and tracing, you must make the necessary changes within the registry of the server running the IP Office TAPI driver. Perform this task only when you want to debug and find issues as the file can become large if left unattended. This large file rapidly fills up the hard drive space of the computer.

Caution:

Incorrect registry changes can cause system failure.

Procedure

1. Click **Start** > **Run** > **regedit** on the machine where TAPI adapter is running.
2. Click **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Wow6432Node** > **Avaya** > **TAPI**.
3. Right-click and add a new string value, and enter the following values:
   - Name: `DebugFile`.
   - Data: `C:\TAPI_Trace`.
4. Restart the computer on which the TAPI adapter is running.

   The system creates a file on the `C Drive` called `TAPI_trace.txt`. The trace file becomes active and logs the initial and subsequent activity of the TAPI driver.

Disabling the IP Office TAPI tracing

About this task

Use this procedure to disable debugging and tracing on the Avaya IP Office TAPI driver.

Caution:

Incorrect registry changes can cause system failure.

Procedure

1. Click **Start** > **Run** > **regedit** on the machine where TAPI adapter is running.
2. Click **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Wow6432Node** > **Avaya** > **TAPI** on the machine where the TAPI adapter is running.
3. To disable the IP Office TAPI tracing, right-click and delete the `DebugFile`.

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. As a result, old logs beyond 20 files and 40 MB cannot be retrieved.

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

Procedure

1. Go to the `WFO_Home` folder located at `C:\Program Data\WFO_Home` by default.
2. In the `ICMCommon.properties` file, update the following parameters:
   - NoOfLogFiles
   - LogFileSize
3. Restart the ICM 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:\Program Data\WFO_Home`.
2. In the `WFO_Home` folder, right-click the `WebappConfig.Properties` file, select **Open with**, and click **Notepad**.
3. For the icm.recordCallUrl=http://10.133.202.159:33023/ parameter, replace the default IP address with the valid IP address of the server where the Unified Messaging component is installed.
4. Click **Save** to close the file.

SysAdmin

SysAdmin is a part of the web installation of the Avaya Workforce Optimization Select application and includes a user interface. Authorized users can perform tenant administration and system administration tasks using the SysAdmin interface.

Tenant management

Tenant management involves administering tenant details, such as contact details, license details, asset mapping details, and data partitioning. After installing the Avaya Workforce Optimization Select application, a default tenant is created for tenant administrators to view and monitor details of the default tenant.

System administration

System administration involves configuring component parameters, monitoring alerts, and managing user accounts. SysAdmin handles alerts from individual components, connects to the mail server, and sends emails using Simple Mail Transfer Protocol (SMTP). The tool also sends Simple Network Management Protocol (SNMP) messages or traps to NMS manager for logging alerts.

Logging on to SysAdmin

Procedure

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

For example, `http://<ServerIP>/sysadmin/index.jsp`.

3. Type your **User Name** and **Password**.
4. Click **Login**.

Tenant management

Creating data partition

About this task

Use this procedure to create a data partition OU type and use it to restrict data access among various groups within an organization. You can create only one data partition OU type and associate multiple organization units.

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

Updating the default tenant name

About this task

Use this procedure to 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. Click **Tenant Management** > **Tenant Administration**.
2. Click the **Edit/View** (›) icon.
3. Type another name for the tenant.
4. Click **Save**.

Viewing license details

About this task

Use this procedure to view and monitor license details of a tenant. The edition and the license expiry date is populated after the customer purchases the license. You can view the modules of the purchased edition and the number of licenses purchased.

Procedure

1. Click **Tenant Management** > **Tenant Administration**.
2. Click the **Edit/View** ( ) icon.
3. Click **License Details**.

   The system displays the license information.

System administration

Configuring component parameters

About this task

Every ICM 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 ICM components to start the service.

While configuring components, you can use the following tabs:

- System: To configure common parameters for components irrespective of their nodes.
- 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. See Configuring dynamic parameters for recorder on page 61.

Procedure

1. Click **System Administration** > **Configuration**.
2. To configure common parameters for a component, click the **System** tab.
3. Click **Save**.
4. To update component parameters for a node, click the **Service** tab.
5. In the **Component** field, select a component.
6. In the **Asset** field, select an asset.
7. In the **Node** field, select a node.
8. 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.

Related links

Restarting the Avaya Workforce Optimization Select components on page 111

Component parameters field descriptions

Name	Description
Component	The ICM components and adapters available for Avaya Workforce Optimization Select. The options are: • Media Manager • Process Checklist • Messaging • Recorder • Log Manager • Packet Sniffer • SysAdmin • Avaya CCTNet adapter • Avaya adapter • AES adapter • TAPI adapter
Asset	The server where the selected component is installed.
Node	A single instance of the selected component installed on the selected server or assets.

Media manager parameters

Parameter	Description
EDServiceIPAddress	To configure the IP address of the server where the Media Manager service is running to perform encryption and decryption of recorded interactions.
AlertManagerIPAddress	To configure the IP address of the server where Alert Manager is running to receive Media Manager-related alerts.
IISServerHost	To configure the host name or IP address of the server where IIS is installed.

Table continues…

Parameter	Description
IISServerPort	To configure the port number for an IIS server. The default value is 80.
StorageManagerInstanceNumber	To configure the Storage Manager instance that is running.
NoOfStorageManagerInstances	To configure the total number of Storage Manager instances that are running.
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.
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 will stop functioning. • False: The value to disable encryption or decryption for calls and screens.
SecureDBUsername	To configure a secure database user name for encrypting and decrypting interactions.
SecureDBPassword	To configure a secure database password for encrypting and decrypting interactions.
StoragePath	To configure a location to store non encrypted audio files and screens.
SecureStoragePath	To configure a location to store encrypted audio files and screens. **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 will get affected after 5 minutes.
DelayBetweenAlerts	To configure the delay between different types of alerts. The default value is 5 minutes.

Table continues…

Parameter	Description
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
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.

Process checklist parameters

Parameter	Description
AlertManagerIPAddress	To configure the Alert Manager IP address so that the Process Checklist component connects to the Alert Manager server.
LongRunningProcessName1	To configure the current, long running, first process name,
AlertManagerPort	To configure the Alert Manager port so that the Process Checklist component connects to the Alert Manager server. The default value is 9280.
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
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

Parameters	Description
nat.apacheIP	To configure the IP address where Apache is running for the Screen Capture to connect to the Unified Messaging component.

Table continues…

Parameters	Description
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`.
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.
MessagingServerIP	To specify the IP address where the Messaging server 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 cofeature the IP address where Unified Messaging is running to move the screens from the agent desktop to a local storage drive.

Recorder parameters

Parameters	Description
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 Avaya CCTNet 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.
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.
CallMaskingEnable	To enable call masking. The options are: • True: The voice data on the file is written. • False: The voice data on the file is muted.
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

Table continues…

Parameters	Description
	• Fatal • Error • Debug
DriveSelect	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.
PCSDialerIntegration	To configure the flag to enable PCS dialer integration. The options are: • True: The value to enable PCS dialer integration. • False: The default value for Avaya Aura® Contact Center on Communication Manager, Avaya Aura® Contact Center on CS 1000, Avaya Contact Center Select on IP Office, and IP Office Contact Center on IP Office environments.
VoiceIPAddress1	To configure 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 adapter server IP address in case of active recording.
SCUploadServerIPAddress	To configure the IP address of the Unified Messaging component where the screen capture service connects to upload screens.
VoiceStreamRecordingEnabled	To configure voice stream recording based on the current agent details. The options are: • True: The value to enable active recording forAvaya Aura® Contact Center on Communication Manager and Avaya Aura® Contact Center on CS 1000 deployments. • False: The default value.
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.
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.
ScreenCaptureProxyIPAddress	To configure the IP address of the Unified Messaging component or screen capture proxy so that the recorder can send all screen capture events.
AdapterWebURLString	To access the Avaya CCTNet adapter and Avaya adapter through an HTTP URL so that the recorder sends site information to the adapter. The default value is /CTIOS_Monitor_Sites.

Table continues…

Parameters	Description
AlertManagerIPAddress	To configure the IP address of Alert Manager so that the recorder connects to Alert Manager.
UseTenantNameInVoiceCaseID	To configure the tenant name in a voice case ID. The options are: • True: The default value. • False: The client name in the voice case ID instead of the tenant name.
ScreenCaptureEnabled	To enable screen capture. The options are: • True: The value to disable screen capture. • False: The default value.
UnifiedMessagingServerPort	To configure the Unified Messaging port so that the recorder connects to the Unified Messaging component. The default value is 33023.
G722RTP320TimeStampRate	To configure parsing of 320 bytes of RTP packets for G722 audio codec. The options are: • True: The default value. • False: The recorder parses 160 bytes of RTP packets.
DelayedExtendedCallInfo	To update the call variable information in the interactions table for calls that have the agent extended call info message. The options are: • True: The value to capture call variable information for delayed or extended calls. • False: The default value.
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.

Log Manager parameters

Parameters	Description
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.

Table continues…

Parameters	Description
MonitorApplciationList	To configure the application names present in the logs folder.
HostDataIP	To configure the connection with the socket.
MonitorApplicationTime	To configure the Monitor Application time, in date and time format, based on the time that logs are generated.
DynamicConfigRecieveTimeout	To configure the time interval to close the dynamic configuration socket after it is created. The default value is 30 minutes.
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.

Packet Sniffer parameters

Parameters	Description
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.
DriveSelect	To configure the current working directory folder where the Sniffer Dumps folder is created.
VoiceIPAddress1	To configure the voice NIC IP address.
TethercallFilesLocation	To configure the dump file location.
TetherealWrapNumber	To create the dump files up to this number. After the system reaches this number, it starts creating files from 1.
DumpFileSize	To configure the size of dump files in MB as per your requirement. The default value is 2 MB.
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.

Table continues…

Parameters	Description
	• Trace: The value that captures logs of all severity types. • Warn • Fatal • Error • Debug

SysAdmin parameters

Parameters	Description
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.
SNMPServerIPAddress	To configure the SNMP server IP address.
SNMPServerPort	To configure the SNMP server port. The default value is 161.
SNMPCommunityString	To configure the SNMP community string especially when SNMP polling is True. The value that is used to configure the SNMP community string is `public`.

Configuring dynamic parameters for the recorder

About this task

Use this procedure to dynamically configure parameters to connect the recorder to adapters or services.

Note:

For on-demand recording, connect the recorder to the Unified Messaging adapter. For call encryption, connect the recorder to the Media Manager service. If you do not want to encrypt calls, ensure you disable the EnableSecurity parameter in Media Manager.

Procedure

1. Click **System Administration** > **Configuration**.

2. Click the **Dynamic** tab.
3. In the **Component** field, select a component.
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. Click **Create Sets**.

Next steps

You can configure specific parameters for an adapter or service. Restart the component service after configuring the parameters.

Related links

Restarting the Avaya Workforce Optimization Select components on page 111

Recorder dynamic configurations field descriptions

Name	Description
Component	The ICM components and adapters available for Avaya Workforce Optimization Select. The options are: • Media Manager • Process Checklist • Messaging • Recorder • Log Manager • Packet Sniffer • SysAdmin • Avaya CCTNet adapter • Avaya adapter • AES adapter • TAPI adapter
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.
Backup Server Address	The IP address of the backup server of the adapter.
Server Port	The port number of the server where the adapter is installed.
Server Local Port	The local port number of the server.
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.
WebURLString	The HTTP URL that the recorder uses to send site information to the adapter. • For Avaya CCTNet 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, Messaging.
IP Address	The IP address of the server where the service is running. For example, the IP address of the server where the Messaging component is running.
Backup IP Address	The IP address of the backup server of the service. For example, the IP address of the backup server where the Messaging component is running.
Port	The port number of the server where the service is running. For example, the port number for Messaging.

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** > **Web** > **Start Web**.
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.

Alerts

Components such as Recorder, Media Manager, PacketSniffer, and Log Manager stop functioning if the disk is full in the respective folder locations. However, you can monitor relevant alerts that trigger when the disk capacity has reached a specified threshold. Ensure you take the required action to clear the disk when you receive such alerts.

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 the Alert Manager component. 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 one or more alerts and click **Disposition** to clear the alerts on the page.
4. 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 tenant details, user details, or configuration details, 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.

Checklist for configuring Avaya Aura® Contact Center on Communication Manager

No.	Task	Reference	Notes	✔
1	Connect Recorder to an AES adapter, an Avaya adapter, and an Avaya CCTNet adapter for active recording. For passive recording, connect the Recorder to an AES adapter and an Avaya CCTNet adapter.	See Configuring dynamic parameters for the recorder on page 61.		
2	Create a CCT user in the Avaya Aura® Contact Center and Avaya Contact Center Select server.	For more information, see *Avaya Aura® Contact Center Server Administration*.		
3	Import and configure Windows user in the CCT console.	For more information, see *Avaya Aura® Contact Center Server Administration*.		
4	Assign agents through the WebAdmin tool on the Avaya Aura® Contact Center or Avaya Contact Center Select server.	For more information, see *Avaya Aura® Contact Center Server Administration*.		
5	Install Dot Net Framework 4 on the server on which the Avaya Workforce Optimization Select application is installed.			
6	Span the traffic between the PBX or Media Server and phones. Connect the traffic to one of the NIC cards in promiscuous mode on the recording server.			

Avaya Aura® Contact Center on Communication Manager adapter parameters

AES adapter

Name	Description
LoginUserName	To configure the CTI username that you created on the AES server.
Password	To configure the CTI user password that you created on the AES server.
MaxSizeOfDatabaseTable	To enable agent-based recording. The options are: • True: The default value. • False: The value to disable agent-based recording.
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.
AlertManagerPort	To configure the port number for Alert Manager. The default value is 9280.
AlertManagerIPAddress	To configure the IP address of the server where Alert Manager is installed.
AESAdapterServerPort	To configure the port number for AES adapter. The default value is 33012.
AESServerID	To configure the AES server name by performing the TSAPI test. The TSAPI test lists the AES server IDs of the AES server.
LogTSAPIEvents	To configure the TSAPI events to be visible in the log file, The options are: • True: The value to configure TSAPI events. • False: The default value.
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

Table continues…

Name	Description
	• Error • Debug
CheckLinkStatusBeforeMonitoring	To configure the AES adapter to check CTI link status before starting to monitor. Retain the default value that is True.
ReopenStreamAfterCTILinkFailure	To reopen the ACS stream connection. Retain the default value that is True.
EnabeSNMPPolling	To enable SNMP polling. AES adapter gets the extension or IP address association from Communication Manager. Retain the default value that is False.
SendRTPMessageFromAdapter	To send the RTP messages from AES adapter to the recorder. Retain the default value that is False.
SendDeletePhoneExtInfo	To delete the phone extension information. Retain the default value that is True.
AgentBasedRecording	To enable agent-based recording for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is False.
SendAgentCallInfo	To send agent call information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendAgentLoginMessage	To send agent login information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendAgentCallStateInfo	To send agent call state information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendAgentExtendedCallInfo	To send agent extended call information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendAgentCallRTPInfo	To send agent call RTP information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendPhoneExtInfo	To send phone extension information messages to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.

Table continues…

Name	Description
SendAgentCallEndResponseCodeInfo	To send agent call end response code information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendAgentCallFailedInfo	To send agent call failed information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendAgentCallTransferInfo	To send agent call transfer information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendAgentCallConferenceInfo	To send agent call conference information to the recorder in Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.

Avaya adapter

Parameters	Description
DMCCEnabled	To enable DMCC for active recording deployments where Avaya adapter is used to get voice. The options are: • True: The value to enable DMCC for active recording deployments. • False: The default value.
MLSEnabled	To enable MLS for CS 1000 active and passive recording deployments. The default value is False.
IPOCCEnabled	To enable IPOCC for IP Office Contact Center deployments. The default value is False.
cmapi.server_IP	To configure the IP address of the server where DMCC is installed.
cmapi.server_port	To configure the port number of DMCC. The default value is 4721.
cnapi.secure_server_port	To configure the secure port number for DMCC. The default value is 4722.
cmapi.username	To configure the username of cmapi server.
cmapi.password	To configure the password of cmapi server.
Application	To configure the name of the application for the adapter. The default value is AWFOS.

Table continues…

Parameters	Description
cmapi.application_description	To configure the application description for the adapter. The default value is AWFOS Avaya Adapter.
version	To configure the application version for the adapter. The default value is 5.0.
dmcc_station_password	To configure the DMCC station password.
dmcc_recording_stations_IPaddress	To configure the IP address for the DMCC recording station.
dmcc_recording_type	To configure the DMCC recording type to a single step conference or multiple registrations. The default value is Multiple registrations.
AlertManagerIPAddress	To configure the IP address of the server on which the Alert Manager is installed.
HostName	To configure the host name of the machine where the Avaya adapter service is running.
HostDataIP	To configure the IP address of the server where the Avaya adapter service is running.
cmapiCallServer	To register the device to Communication Manager or to do call control with a third party device. The default value is cmsim. The value to register the device is `CM105`.
num_dmcc_stations	To configure the number of DMCC stations as `3`. The default value is 100.
first_dmcc_station_extension	To configure the first DMCC station extension as `21003`. The default value is 3101.
dmcc_station_codec	To configure the DMCC station codecs. The options are: • g711U • g711A • g729 • g729A Retain the default value that is g711U.
dmcc_station_conference_participation_type	To configure DMCC station conference participation type. The options are: • Active: The default value. • Silent: The value to configure DMCC station conference participation type for Avaya Aura® Contact Center Communication Managerdeployment.
dmcc_active_recording_enabled	To enable DMCC active recording. Retain the default value that is True.

Avaya CCTNet adapter

Parameters	Description
CCT_Host_Name	To configure the IP address of the AACC or ACCS server running the CCT service.
CCT_Port	To configure the port that the CCT service listens on, in the AACC or ACCS server. The default value is 29373. If you change the default value, update the same in the Avaya CCTNet adapter.
Username	To configure the username of the Windows user to validate the Communication Control Toolkit server. This parameter is created in the CCTAdmin utility.
Password	To configure the password of the Windows user to validate the Communication Control Toolkit server.
Domain	To configure the domain of the Windows user to validate the Communication Control Toolkit server.
LocalhostIP	To configure the IP address of the server on which the Avaya CCTNet adapter is located.
LocalhostPort	To configure the port for which the recorder is configured to communicate. The default value is 34301. If you change the port in the recorder configuration, update the port for the adapter too.
ContentTypesToMonitor	To configure the support for voice, email, and chat. You can set the parameter value to email, IM, or voice.
AlertManagerIPAddress	To configure the IP Address on which Alert Manager is running.
AlertManagerPort	To configure the port number on which the Alert Manager process is listening. The default value is 9280.
HTTPAlertsEnabled	To configure whether or not to send HTTP alerts to Alert Manager. The default value is True.
NonVoiceAgentExtensionPrefix	To configure the prefix in the agent extension for nonvoice calls. Currently, the calls to extension with prefix “x” come to the terminal DefaultNode_CCMM_x. For non-voice calls, remove the prefix from that extension.
SendAgentLoginMessage	To make agent login information available to the recorder when the agent logs in for Avaya Aura®

Table continues…

Parameters	Description
	Contact Center Communication Manager deployments. The options are: • True: The default value. • False: The value to enable for Avaya Aura® Contact Center Communication Manager deployments.
SendAgentLogoutMessage	To make agent logout information available to the recorder when the agent logs out for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is False.
SendCallInfoMessage	To send agent call information to the recorder for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is False.
SendCallStateInfoMessage	To send agent call state information to the recorder for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is False.
SendCallACDInfoMessage	To make agent call ACD information available to the recorder for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendCallWrapupData	To make call wrapup data available to the recorder for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendCallRTPInfo	To send agent call RTP information to the recorder for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is False.
SendContactIDForCallStitching	To send the icmEnterpriseID as the call ID during agent wrapup messages for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is True.
SendScreenCaptureMessage	To send screen capture messages to the recorder for nonvoice transactions for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.

Table continues…

Parameters	Description
SendAgentCallStateInfoForNonVoice	To send agent call state information to the recorder for nonvoice transactions for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
SendCallInfoForNonVoice	To send agent call information to the recorder for nonvoice transactions for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
SendAgentLoginForNonVoice	To make agent login information for nonvoice transactions available to the recorder when the agent logs in for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
SendAgentLogoutForNonVoice	To make agent logout information for nonvoice transactions available to the recorder when the agent logs out for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
SendRTPInfoForNonVoice	To send agent call RTP information to the recorder for nonvoice transactions for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments.

Table continues…

Parameters	Description
	• False: The default value.
SendCallHoldInfoForNonVoice	To send call hold information messages to the recorder for nonvoice transactions for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
SendCallResumeInfoForNonVoice	To send call resume information messages to the recorder for nonvoice transactions for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
SendContactIDForCallStitchingNonVoice	To send the icmEnterpriseID as the call ID during agent wrapup messages for nonvoice transactions for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for nonvoice transactions in Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
SendPhoneExtInfo	To send phone extension information messages to the recorder for Avaya Aura® Contact Center Communication Manager deployments. The options are: • True: The value to enable for Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.
Var 1	To configure business variables for skills for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.Skillset
Var 2	To configure business variables to capture user to user information for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.SIP_RETURNED_DIGITS_1.

Table continues…

Parameters	Description
Var 3	To configure business variables to capture user to user information for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.SIP_RETURNED_DIGITS_2.
Var 4	To configure business variables to capture user to user information for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.UUI.
Var 5	To configure business variables for agent activity code for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is set to ACCS.ActivityCode.
Var 6	To configure business variables for called party for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
Var 7	To configure business variables for calling party for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
Var 8, Var 9, and Var 10	To configure business variables that meet your requirements.
ContactSubType	To configure the sub type of the contact for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.CONTACTSUBTYPE.
TransferredDeviceID	To configure the ID of the transferred device for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
SkillID	To configure the skill ID for Avaya Aura® Contact Center Communication Manager deployments.
CalledParty	To configure the value of the called party for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
CalledPartyName	To configure the name of the called party for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
CallingParty	To configure the value of the calling party for Avaya Aura® Contact Center Communication Manager

Table continues…

Parameters	Description
	deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
CallingPartyName	To configure the name of the calling party for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
EmailCalledParty	To configure the email address of the called party for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.TOADDRESS.
EmailCallingParty	To configure the email address of the calling party for Avaya Aura® Contact Center Communication Manager deployments. Retain the default value that is ACCS.Intrinsics.FROMADDRESS.

Recorder

Parameters	Description
VoiceIPAddress1	To configure the Voice NIC IP address from where the recorder reads the voice packets.
VoiceStreamRecordingEnabled	To configure voice stream recording based on the current agent details. The options are: • True: The value to enable for Avaya Aura® Contact Center Communication Manager deployments. • False: The default value.

Checklist for configuring Avaya Aura® Contact Center on CS 1000

No.	Task	Reference	Notes	✔
1	Connect Recorder to an Avaya adapter and an Avaya CCTNet adapter for both active and passive recording.	See Configuring dynamic parameters for the recorder on page 61.		
2	Configure two instances of Voice Settings for each employee profile in Avaya Workforce Optimization Select application for fixed seating. One instance to specify the agent ID and another to specify the extension and the position ID of CS 1000 as the agent ID.	For more information on how to configure voice settings for employees, see *Administering Avaya Workforce Optimization Select*.		

Table continues…

No.	Task	Reference	Notes	✔
3	Create ELAN for Avaya Aura® Contact Center application on the call server.	For more information, see *Avaya Aura® Contact Center Configuration — Avaya Communication Server 1000 Integration*		
4	Create VAS for the ELAN of Avaya Aura® Contact Center on the call server.	For more information, see *Avaya Aura® Contact Center Configuration — Avaya Communication Server 1000 Integration*		
5	Enable the IPIE feature for IP call recording on the call server.	For more information, see *Avaya Aura® Contact Center Configuration — Avaya Communication Server 1000 Integration*		
6	Enable class of service RECA for IP phone.	For more information, see *Avaya Aura® Contact Center Configuration — Avaya Communication Server 1000 Integration*		
7	Configure the Associated Set Assignment (AST) for IP phone.	For more information, see *Avaya Aura® Contact Center Configuration — Avaya Communication Server 1000 Integration*		

Avaya Aura® Contact Center on CS 1000 adapter parameters

Avaya adapter

Parameters	Description
AlertManagerIPAddress	To configure the IP address of the server on which the Alert Manager is installed.
MLSEnabled	To enable MLS for CS 1000 active and passive recording deployments. The options are: • True: The value to enable for CS 1000 deployments.

Table continues…

Parameters	Description
	• False: The default value.
NumOfMLSClusterConfigs	To specify the number of clusters configured to connect to an MLS Server. Retain the default value that is 1.
Cluster1_MLS1_Host	To configure the host information for the cluster 1 primary server.
Cluster1_MLS1_Port	To configure the port information for the cluster 1 primary server. Retain the default value that is 3000.
Cluster1_MLS2_Host	To configure the host information for the cluster 2 backup server.
Cluster1_MLS2_Port	To configure the port information for the cluster 2 backup server. Retain the default value that is 3000.
Cluster1_MLS_ApplicationID	To configure the name of the application to identify the connection with MLS server.
Cluster1_MLS_HostName	To configure the MLS server link name. Retain the default value that is Lanlink.
MLSClientIP	To configure the IP address of the machine where the MLS application is running.
MLSClientPort	To configure the port information of the server where the MLS application is running. Retain the default value that is 5001.
ServiceIDList	To configure the services that register with MLS server to get call information. Retain the default value that is 97,98,100.
RecordingIPAddress	To configure the IP address of the machine that gets the media from the phones.
SendPhoneExtInfo	To send phone extension information to the recorder in CS 1000 deployments. Retain the default value that is True.
SendMLSAgentLoginInfo	To send agent login information to the recorder in CS 1000 deployments. Retain the default value that is True.
SendMLSAgentCallInfo	To send agent call information to the recorder in CS 1000 deployments. Retain the default value that is True.
SendMLSAgentCallStateInfo	To send agent call state information to the recorder in CS 1000 deployments. Retain the default value that is True.
SendMLSAgentCallRTPInfo	To send agent call RTP information to the recorder in CS 1000 deployments. Retain the default value that is True.

Table continues…

Parameters	Description
SendMLSVoiceStreamRTPInfo	To send voice stream RTP information to the recorder in CS 1000 deployments. Retain the default value that is True.
RegisterPendingDNsFrequency	To configure the frequency in seconds to register the failed devices again with MLS server. Retain the default value that is 60.
PositionIDSitesList	To configure the site alias of the sites in the Avaya Workforce Optimization Select web application. This parameter loads the DNs and Position IDs from the database.
PassiveRecordingEnabled	To enable or disable active or passive recording for CS 1000 deployments. The options are: • True: The value to enable passive recording for CS 1000deployments. • False: The default value.

Avaya CCTNet adapter

Parameters	Description
CCT_Host_Name	To configure the IP address of the AACC or ACCS server running the CCT service.
CCT_Port	To configure the port that the CCT service listens on, in the AACC or ACCS server. The default value is 29373. If you change the default value, update the same in the Avaya CCTNet adapter.
Username	To configure the username of the Windows user to validate the Communication Control Toolkit server. This parameter is created in the CCTAdmin utility.
Password	To configure the password of the Windows user to validate the Communication Control Toolkit server.
Domain	To configure the domain of the Windows user to validate the Communication Control Toolkit server.
LocalhostIP	To configure the IP address of the server on which the Avaya CCTNet adapter is located.
LocalhostPort	To configure the port for which the recorder is configured to communicate. The default value is 34301. If you change the port in the recorder configuration, update the port for the adapter too.
ContentTypesToMonitor	To configure the support for voice, email, and chat. The options are: • Voice • Email

Table continues…

Parameters	Description
	• Chat • Web_Communications
AlertManagerIPAddress	To configure the IP Address on which Alert Manager is running.
AlertManagerPort	To configure the port number on which the Alert Manager process is listening. The default value is 9280.
HTTPAlertsEnabled	To configure whether or not to send HTTP alerts to Alert Manager. The default value is True.
NonVoiceAgentExtensionPrefix	To configure the prefix in the agent extension for nonvoice calls. Currently, the calls to extension with prefix “x” come to the terminal DefaultNode_CCMM_x. For nonvoice calls, remove the prefix from that extension.
SendAgentLoginMessage	To make agent login information available to the recorder when the agent logs in for CS 1000 deployments. The options are: • True: The value to enable for CS 1000 deployments. • False: The default value.
SendAgentLogoutMessage	To make agent logout information available to the recorder when the agent logs out for CS 1000 deployments. The options are: • True: The value to enable for CS 1000 deployments. • False: The default value.
SendCallInfoMessage	To send agent call information to the recorder for CS 1000 deployments. Retain the default value that is False.
SendCallStateInfoMessage	To send agent call state information to the recorder for CS 1000 deployments. Retain the default value that is False.
SendCallACDInfoMessage	To make agent call ACD information available to the recorder for CS 1000 deployments. Retain the default value that is False.
SendCallWrapupData	To make call wrapup data available to the recorder for CS 1000 deployments. Retain the default value that is True.
SendCallRTPInfo	To send agent call RTP information to the recorder for CS 1000 deployments. Retain the default value that is False.

Table continues…

Parameters	Description
SendContactIDForCallStitching	To send the icmEnterpriseID as the call ID during agent wrapup messages for CS 1000 deployments. Retain the default value that is True.
SendScreenCaptureMessage	To send screen capture messages to the recorder for nonvoice transactions for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000 deployments. • False: The default value.
SendAgentCallStateInfoForNonVoice	To send agent call state information to the recorder for nonvoice transactions for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000 deployments. • False: The default value.
SendCallInfoForNonVoice	To send agent call information to the recorder for nonvoice transactions for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000 deployments. • False: The default value.
SendAgentLoginForNonVoice	To make agent login information for nonvoice transactions available to the recorder when the agent logs in for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000deployments. • False: The default value.
SendAgentLogoutForNonVoice	To make agent logout information for nonvoice transactions available to the recorder when the agent logs out for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000deployments. • False: The default value.
SendRTPInfoForNonVoice	To configure to send agent call RTP information to the recorder for nonvoice transactions for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000 deployments. • False: The default value.

Table continues…

Parameters	Description
SendCallHoldInfoForNonVoice	To send call hold information messages to the recorder for nonvoice transactions for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000 deployments. • False: The default value.
SendCallResumeInfoForNonVoice	To send call resume information messages to the recorder for nonvoice transactions for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000 deployments. • False: The default value.
SendContactIDForCallStitchingNonVoice	To send the icmEnterpriseID as the call ID during agent wrapup messages for nonvoice transactions for CS 1000 deployments. The options are: • True: The value to enable for nonvoice transactions in CS 1000 deployments. • False: The default value.
SendPhoneExtInfo	To send phone extension information messages to the recorder for CS 1000 deployments. The options are: • True: The value to enable for CS 1000 deployments. • False: The default value.
PositionIDSitesList	To configure the site information to load DNs and Position IDs from the database for CS 1000 deployments.
Var 1	To configure business variables for skills for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.Skillset
Var 2	To configure business variables to capture user to user information for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.SIP_RETURNED_DIGITS_1.
Var 3	To configure business variables to capture user to user information for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.SIP_RETURNED_DIGITS_2.
Var 4	To configure business variables to capture user to user information for CS 1000 deployments. Retain the default value that is ACCS.UUI.

Table continues…

Parameters	Description
Var 5	To configure business variables for agent activity code for CS 1000 deployments. Retain the default value that is ACCS.ActivityCode.
Var 6	To configure business variables for called party for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
Var 7	To configure business variables for calling party for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
Var 8, Var 9, and Var 10	To configure business variables that meet your requirements.
ContactSubType	To configure the sub type of the contact for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.CONTACTSUBTYPE.
TransferredDeviceID	To configure the ID of the transferred device for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
SkillID	To configure the skill ID for CS 1000 deployments.
CalledParty	To configure the value of the called party for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
CalledPartyName	To configure the name of the called party for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
CallingParty	To configure the value of the calling party for CS 1000 deployments. Retain the default value that is set to ACCS.Intrinsics.AD_CLID.
CallingPartyName	To configure the name of the calling party for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
EmailCalledParty	To configure the email address of the called party for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.TOADDRESS.
EmailCallingParty	To configure the email address of the calling party for CS 1000 deployments. Retain the default value that is ACCS.Intrinsics.FROMADDRESS.

Checklist to support WebLM for CS 1000 deployments

No.	Task	Reference	Notes	✔
1	Deploy the WebLM service on the Avaya Workforce Optimization Select web server.	For more information about WebLM installation, see *Licensing Installation Instructions for WebLM 7.0*.	The Java version specified in the document works even with the version Open JDK 8 available on the Avaya Workforce Optimization Select server.	
2	Specify the **WebLM IP Address / Hostname** as the **Server IP Address / Hostname** while installing the Avaya Workforce Optimization Select application.	See Installing Avaya Workforce Optimization Select on page 37.		

Checklist for configuring Avaya Contact Center Select on IP Office

No.	Task	Reference	Notes	✔
1`	Connect Recorder to an Avaya CCTNet adapter and a TAPI adapter for passive recording.	See Configuring dynamic parameters for the recorder on page 61.		
2	Install and configure TAPI3 driver and use the password given while installing IP Office as the switch password.	Installing TAPI3 driver on page 48. Configuring TAPI3 driver on page 48.		
3	Select the TAPI link as un-secured in the IP Office security settings of IP Office Manager. Else, interactions will not be recorded.	For more information, see *Avaya IP Office™ Platform Security Guidelines*.		
4	Ensure that there is TAPI license in IP Office.			
5	Create a CCT user in the Avaya Aura® Contact Center and Avaya Contact Center Select server.	For more information, see *Avaya Aura® Contact Center Server Administration*.		

Table continues…

No.	Task	Reference	Notes	✔
6	Import and configure Windows user in the CCT console.	For more information, see *Avaya Aura® Contact Center Server Administration*		
7	Assign agents through the WebAdmin tool on the Avaya Aura® Contact Center or Avaya Contact Center Select server.	For more information, see *Avaya Aura® Contact Center Server Administration*		
8	Install Dot Net Framework 4 on the server on which the Avaya Workforce Optimization Select application is installed.			
9	Ensure that you span the traffic between the PBX or Media Server and phones and connect that traffic to one of the NIC card in a promiscuous mode on the recording server.			

Avaya Contact Center Select on IP Office adapter parameters

Avaya CCTNet adapter

Parameters	Description
CCT_Host_Name	To configure the IP address of the or Avaya Aura® Contact Center (AACC) or Avaya Contact Center Select server running the CCT service.
CCT_Port	To configure the port that the CCT service listens on, in the AACC or Avaya Contact Center Select server. The default value is 29373.
Username	To configure the username of the Windows user to validate the Communication Control Toolkit server. This parameter is created in the CCTAdmin utility.
Password	To configure the password of the Windows user to validate the Communication Control Toolkit server.
Domain	To configure the domain of the Windows user to validate the Communication Control Toolkit server.
LocalhostIP	To configure the IP address of the server on which the Avaya CCTNet adapter is located.
LocalhostPort	To configure the port for which the recorder is configured to communicate. The default value is 34301.

Table continues…

Parameters	Description
ContentTypesToMonitor	To configure the support for voice, email, and chat. The options are: • Voice • Email • IM • Web_Communications
AlertManagerIPAddress	To configure the IP address on which Alert Manager is running.
AlertManagerPort	To configure the port number on which the Alert Manager process is listening. The default value is 9280.
HTTPAlertsEnabled	To configure whether or not to send HTTP alerts to Alert Manager. The default value is True.
NonVoiceAgentExtensionPrefix	To configure the prefix in the agent extension for nonvoice calls. Currently, the calls to extension with prefix “x” come to the terminal DefaultNode_CCMM_x. For nonvoice calls, no prefix is required from that extension.
SendAgentLoginMessage	To make agent login information available to the recorder when the agent logs in for IP Office deployments. Retain the default value that is True.
SendAgentLogoutMessage	To make agent logout information available to the recorder when the agent logs out for IP Office deployments. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
SendCallInfoMessage	To send agent call information to the recorder for IP Office deployments. Retain the default value that is False.
SendCallStateInfoMessage	To send agent call state information to the recorder for IP Office deployments. Retain the default value that is False.
SendCallACDInfoMessage	To make agent call ACD information available to the recorder for IP Office deployments. Retain the default value that is True.
SendCallWrapupData	To make call wrapup data available to the recorder for IP Office deployments. Retain the default value that is True.

Table continues…

Parameters	Description
SendCallRTPInfo	To send agent call RTP information to the recorder for IP Office deployments. Retain the default value that is False.
SendContactIDForCallStitching	To send the icmEnterpriseID as the call ID during agent wrapup messages for IP Office deployments. Retain the default value that is True.
SendScreenCaptureMessage	To send screen capture messages to the recorder for nonvoice transactions for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendAgentCallStateInfoForNonVoice	To send agent call state information to the recorder for nonvoice transactions for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendCallInfoForNonVoice	To send agent call information to the recorder for nonvoice transactions for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendAgentLoginForNonVoice	To make agent login information for nonvoice transactions available to the recorder when the agent logs in for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendAgentLogoutForNonVoice	To make agent logout information for nonvoice transactions available to the recorder when the agent logs out for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.

Table continues…

Parameters	Description
SendRTPInfoForNonVoice	To send agent call RTP information to the recorder for nonvoice transactions for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendCallHoldInfoForNonVoice	To send call hold information messages to the recorder for nonvoice transactions for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendCallResumeInfoForNonVoice	To send call resume information messages to the recorder for nonvoice transactions for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendContactIDForCallStitchingNonVoice	To send the icmEnterpriseID as the call ID during agent wrapup messages for nonvoice transactions for IP Office deployments. The options are: • True: The value to enable for nonvoice transactions in IP Office deployments. • False: The default value.
SendPhoneExtInfo	To send phone extension information messages to the recorder for IP Office deployments. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
Var 1	To configure business variables for skills for IP Office deployments. Retain the default value that is ACCS.Intrinsics.Skillset.
Var 2	To configure business variables to capture user to user information for IP Office deployments. Retain the default value that is ACCS.Intrinsics.SIP_RETURNED_DIGITS_1.
Var 3	To configure business variables to capture user to user information for IP Office deployments. Retain

Table continues…

Parameters	Description
	the default value that is ACCS.Intrinsics.SIP_RETURNED_DIGITS_2.
Var 4	To configure business variables to capture user to user information for IP Office deployments. Retain the default value that is ACCS.UUI.
Var 5	To configure business variables for agent activity code for IP Office deployments. Retain the default value that is ACCS.ActivityCode.
Var 6	To configure business variables for called party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
Var 7	To configure business variables for calling party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
Var 8, Var 9, and Var 10	To configure business variables that meet your requirements.
ContactSubType	To configure the sub type of the contact for IP Office deployments. Retain the default value that is ACCS.Intrinsics.CONTACTSUBTYPE.
TransferredDeviceID	To configure the ID of the transferred device for IP Office deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
SkillID	To configure the skill ID for IP Office deployments.
CalledParty	To configure the value of the called party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
CalledPartyName	To configure the name of the called party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.AD_CDN.
CallingParty	To configure the value of the calling party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
CallingPartyName	To configure the name of the calling party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.AD_CLID.
EmailCalledParty	To configure the email address of the called party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.TOADDRESS.
EmailCallingParty	To configure the email address of the calling party for IP Office deployments. Retain the default value that is ACCS.Intrinsics.FROMADDRESS.

TAPI adapter

Parameters	Description
SendAgentLoginMessage	To send agent login event from TAPI adapter to the recorder. Retain the default value that is True.
MaxNoOfLinesForRecording	To configure the maximum number of lines to be recorded for the agent ID if there are multiple line instances. Retain the default value that is 6.
AlertManagerIPAddress	To configure the IP address of the server where Alert Manager is installed.
TAPIApplication	To configure the TAPI application as `APPLICATION_NAME_IAF` for IP Office deployments. .
SkillGroupIDs	To configure the skill group IDs created in IP Office. The parameter value must be `6000`.
TAPIEventTracing	To trace TAPI events. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
LogCallInfoDetails	To log call info details such as called party, calling party, and call identifier in the log file. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
LogCTIOSKeepAliveMessages	To log the CTIOS keep alive messages in the log file. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
EnabeSNMPPolling	To get the phone extension and IP address association from Communication Manager. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
SNMPServerIPAddress	To configure the SNMP server IP address.
SNMPCommunityString	To configure the SNMP community string especially when SNMP polling is set to True. The value that is used to configure the SNMP community string is `public`.

Table continues…

Parameters	Description
IPOfficeAgentBasedRecording	To enable agent-based recording for IP Office deployments. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
IPOfficeExtensionBasedRecording	To enable extension-based recording for IP Office deployments. The options are: • True: The value to enable extension-based recording for IP Office deployments. • False: The default value.
StartMACAddr	To configure the value of StartMACAddr to denote the starting values for MAC address of the phone extension. The value is used to send the MAC address as the device ID to the recorder. For example, the value can be 00005E000000.
SNMPPollingTracing	To configure logs for SNMP. The options are: • True: The value to enable for IP Office deployments. • False: The default value.
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
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.

Checklist for configuring IP Office Contact Center on IP Office

No.	Task	Reference	Notes	✔
1	Connect Recorder to an Avaya adapter and a TAPI adapter for passive recording.	See Configuring dynamic parameters for the recorder on page 61.		
2	Install and configure TAPI3 driver and use the password given while installing IP Office as the switch password.	Installing TAPI3 driver on page 48. Configuring TAPI3 driver on page 48.		
3	Select the TAPI link as un-secured in the IP Office security settings of IP Office Manager. Else, interactions will not be recorded.	For more information, see *Avaya IP Office Platform Security Guidelines*.		
4	Ensure that there is TAPI license in IP Office.			
5	Install Dot Net Framework 4 on the server on which the Avaya Workforce Optimization Select application is installed.			
6	Ensure that you span the traffic between the PBX or Media Server and phones and connect that traffic to one of the NIC card in a promiscuous mode on the recording server.			

IP Office Contact Center on IP Office adapter parameters

Avaya adapter

Name	Description
AlertManagerIPAddress	To configure the IP address of the server on which the Alert Manager is installed.
IPOCCEnabled	To enable IPOCC for IP Office Contact Center deployments. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.

Table continues…

Name	Description
IPOCCClientIP	To configure the IP address of the server where IP Office Contact Center is installed.
WSLoginName	To configure the login of the Web services user. Set the value to `service`.
WSPassword	To configure the password of the Web services user. Set the value to `Ccadmin123`.
DirectoryWSHostName	To configure the IP address or host name of the Directory Web Service.
DirectoryWSPort	To configure the port of the Directory Web Service. The default value is 18080.
ManagementWSHostName	To configure the IP address or host name of the Management Web Service.
ManagementWSPort	To configure the port of the Management Web Service. The default value is 18080.
MonitorWSHostName	To configure the IP address or host name of the Monitor Web Service.
MonitorWSPort	To configure the port of the Monitor Web Service. The default value is 18080.
TaskWSHostName	To configure the IP address or host name of the Endpoint Web Service.
TaskWSPort	To configure the port of the Endpoint Web Service. The default value is 18080.
SendIPOCCAgentLoginInfo	To make agent login information available to the recorder for IP Office Contact Center deployments. Retain the default value that is True.
SentIPOCCAgentCallInfo	To make agent call information available to the recorder for IP Office Contact Center deployments. Retain the default value that is False.
SentIPOCCAgentCallStateInfo	To make agent call state information available to the recorder for IP Office Contact Center deployments. Retain the default value that is False.
SendIPOCCAgentCallRTPInfo	To make agent call RTP information available to the recorder for IP Office Contact Center deployments. Retain the default value that is False.
SendIPOCCVoiceStreamRTPInfo	To make voice stream RTP information available to the recorder for IP Office Contact Center deployments. Retain the default value that is False.
SendIPOCCAgentCallACDInfo	To make agent call ACD information available to the recorder for IP Office Contact Center deployments. Retain the default value that is True.

Table continues…

Name	Description
SendIPOCCScreenCaptureInfo	To make nonvoice screen capture messages available to the recorder from Avaya adapter for IP Office Contact Center deployments. The recorder sends screen start and stop events. Retain the default value that is True.
SendIPOCCCallWrapupData	To make call wrapup data available to the recorder for IP Office Contact Center deployments. Retain the default value that is True.
SendIPOCCAgentLoginInfoForNonVoice	To make agent login information available to the recorder for IP Office Contact Center deployments for nonvoice transactions. The options are: • True: The value to enable for nonvoice transactions in IP Office Contact Center deployments. • False: The default value.
SendIPOCCAgentCallInfoForNonVoice	To make agent call information available to the recorder for IP Office Contact Center deployments for nonvoice transactions. The options are: • True: The value to enable for nonvoice transactions in IP Office Contact Center deployments. • False: The default value.
SendIPOCCAgentCallStateInfoForNonVoice	To make agent call state information available to the recorder for IP Office Contact Center deployments for nonvoice transactions. The options are: • True: The value to enable for nonvoice transactions in IP Office Contact Center deployments. • False: The default value.
SendIPOCCAgentCallRTPInfoForNonVoice	To make agent call RTP information available to the recorder for IP Office Contact Center deployments for nonvoice transactions. The options are: • True: The value to enable for nonvoice transactions in IP Office Contact Center deployments. • False: The default value.
SendIPOCCPhoneExtInfo	To enable phone extension information to be sent to the recorder. Retain the default value that is False.
Var 1	To configure business variables for skills. Retain the default value that is IPOCC.Tags.FirstTopicName.

Table continues…

Name	Description
Var 2	To configure business variables for skills. Retain the default value that is IPOCC.Tags.FirstTopicName.
Var 3	To configure business variables for calling party. Retain the default value that is IPOCC.Tags.CCK_Called_Address
Var 7	To configure business variables for calling party. Retain the default value that is IPOCC.Tags.CCK_Called_Address.
Var 4, Var 5, Var 6, Var 8, Var 9, and Var 10	To configure business variables that meet your requirements.
SkillID	To configure the skill ID for IP Office Contact Center deployments.
CallingParty	To configure the value of the called party for IP Office Contact Center deployments. Retain the default value that is IPOCC.Tags.CCK_CallingAddress.
CallingPartyName	To configure the name of the called party for IP Office Contact Center deployments. Retain the default value that is IPOCC.Tags.CCK_CallingAddress.
CalledParty	To configure the value of the calling party for IP Office Contact Center deployments. Retain the default value that is IPOCC.connectedAddress.
CalledPartyName	To configure the name of the calling party for IP Office Contact Center deployments. Retain the default value that is IPOCC.connectedAddress.

TAPI adapter

Parameters	Description
SendAgentLoginMessage	To send agent login event from TAPI adapter to the recorder. The options are: • True: The default value. • False: The value to enable for IP Office Contact Center deployments.
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 must be `1`.
AlertManagerIPAddress	To configure the IP address of the server where Alert Manager is installed.

Table continues…

Parameters	Description
TAPIApplication	To configure the TAPI application as `APPLICATION_NAME_IAF`for IP Office Contact Center deployments. .
SkillGroupIDs	To configure the skill group IDs created in IP Office. The value to configure skill group ID in IP Office must be `6000`.
TAPIEventTracing	To trace TAPI events. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.
LogCallInfoDetails	To log call info details such as called party, calling party, and call identifier in the log file. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.
LogCTIOSKeepAliveMessages	To log the CTIOS keep alive messages in the log file. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.
EnabeSNMPPolling	To get the phone extension and IP address association from Communication Manager. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.
SNMPServerIPAddress	To configure the SNMP server IP address.
SNMPCommunityString	To configure the SNMP community string especially when SNMP polling is set to True. Change the value to `public`.
IPOfficeAgentBasedRecording	To enable agent-based recording for IP Office deployments. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.

Table continues…

Parameters	Description
IPOfficeExtensionBasedRecording	To enable extension-based recording for IP Office deployments. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.
StartMACAddr	To configure the value of StartMACAddr to denote the starting values for MAC address of the phone extension. For example, you can configure the value as `00005E000000`.
SNMPPollingTracing	To configure logs for SNMP. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.
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
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.

Recorder

Parameters	Description
DelayedExtendedCallInfo	To update the call variable information in the interactions table for calls that have the agent extended call info message. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.
CTIOSIntegration	To enable CTIOS integration. Retain the default value that is False.

Table continues…

Parameters	Description
UpdateICMFromWrapUp	To update ICM Enterprise ID value in database received from CTIOS and not from JTAPI. The default value is True.
UseCTIIntegration	To get events from the CTI adapter to the recorder for recording interactions. The options are: • True: The value that connects the recorder to either TAPI adapter, Avaya adapter, AES adapter, or Avaya CCTNet adapter. • False: The default value.
SaveCTICallIDInConnected	To remember the PBX call identifier in the connected state. Retain the default value that is False.
RecorderPacketFilterString	To configure the string in the recorder to sniff packets coming from certain ports and protocol types. Retain the default value that is (ip proto UDP).
RTCPProcessingEnabled	To enable the recorder to process RTCP packets. The options are: • True: The default value. • False: The value to enable for IP Office Contact Center deployments.
AvayaIntegration	To enable 100% recording in Avaya environment, Retain the default value that is False.
LoginAgentOnPhoneExtTableAdd	To configure to check whether the agent logged in is in SPAN or not. The options are: • True: The value to enable for IP Office Contact Center deployments. • False: The default value.

Limitations

Avaya Aura® Contact Center on Communication Manager deployment limitations

- Calls are not recorded if you configure G722 as the audio codec for active and passive recording.
- 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.
- 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 AES and Avaya Aura® Contact Center servers. The standby secondary server does not become active automatically when the active primary server is down.

Avaya Aura® Contact Center on CS 1000 deployment limitations

- The call end response code information, that 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 active recording deployment with Avaya 1210 model hard phones, the respective DN is unable to register with Meridian Link Service (MLS).
- 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.
- WebLM is not available for both active and passive recording deployments. As a workaround, see Checklist to support WebLM for CS1000 deployments on page 84.
- 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 will be 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.

Avaya Contact Center Select on IP Office 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 NORTP call 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.

IP Office Contact Center on IP Office 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.
- 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.

Installer limitations

- Once 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.

ICM components limitations

- The Avaya Workforce Optimization Select ICM components do not send email alert messages when the connection to the database is lost. However, the components send SNMP traps.

Installing and configuring Desktop Monitor application

Screen Capture overview

To capture screens in Avaya Workforce Optimization Select , the Unified Messaging components acts like a proxy server and interacts directly with the recorder. 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

About this task

Use this procedure to install and configure Screen Capture on agent machines.

Procedure

1. Click **Program Files (x86)** > **Avaya** > **AWFOS5** > **ScreenCapture** 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`

- HarmonyBHO64.dll
- harmonydta.crx
- harmonydta.xml
- harmonydta.xpi
- manifest.json
- DTA.json
- DTAAgents.json
- DTAHlpr.exe
- DTAHook.dll
- DTAHook64.dll
- 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 64

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 tenant 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 on page 101.		
2	Configure the resource files.	Configuring resource files on page 105.		
3	Install the learning console.	Installing Learning Console on page 105.		
4	Execute the script generator.	Executing script generator on page 106.		

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 recorder or the Unified Messaging component is running.

   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.
   - `1B8EE20F-EA5D-42FC-A465-C57174EE2F44.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.

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 the xml file names that you provided. All resource files are placed in the respective folders.
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.

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 109.		
2	Change the node name in the `ini` files.	See Changing the node name on page 109.		
3	Start the Avaya Workforce Optimization Select components.	See Starting the Avaya Workforce Optimization Select components on page 110.		
4	Select the appropriate node to configure the C++ components.	See Configuring component parameters on page 53.		
5	Configure all the component parameters for the new node.	See Configuring component parameters on page 53.		
6	Restart the Avaya Workforce Optimization Select components.	See Restarting the Avaya Workforce Optimization Select components on page 111.		

Stopping 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 **Stop**.

Changing the node name

About this task

Use this procedure to change the node name in the `ini` file of all the ICM 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. In the component folder, right-click the respective `.ini` file.
4. Select **Open with**, and click **Notepad**.
5. Update the value for the following parameter:
   - NodeName: Update the node name.
6. 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 ICM 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 ICM components to start the service.

While configuring components, you can use the following tabs:

- System: To configure common parameters for components irrespective of their nodes.
- 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. See Configuring dynamic parameters for recorder on page 61.

Procedure

1. Click **System Administration** > **Configuration**.
2. To configure common parameters for a component, click the **System** tab.
3. Click **Save**.
4. To update component parameters for a node, click the **Service** tab.
5. In the **Component** field, select a component.
6. In the **Asset** field, select an asset.
7. In the **Node** field, select a node.

8. 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.

Related links

Restarting the Avaya Workforce Optimization Select components on page 111

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 7: 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 113.		
2	Refresh and then restart the AWFOS services.	See Restarting the Avaya Workforce Optimization Select components on page 111.		
3	Start the web application using the following URL: http://HOSTNAME or IP address.			
4	Configure the web application server to launch the AWFOS Login page by entering the URL. Log in as user ADMIN.			
5	Update the organization name, organization unit, site, department, and designation.	For more information, see *Administering Avaya Workforce Optimization Select*.		
6	Upload employee data manually or using an excel spreadsheet.	For more information, see *Administering Avaya Workforce Optimization Select*.		
7	Assign supervisors to the agents.	For more information, see *Administering Avaya Workforce Optimization Select*.		
8	Cross check group access for supervisors and managers.	For more information, see *Administering Avaya Workforce Optimization Select*.		

Table continues…

No.	Task	Reference	Notes	✔
9	Enable recording for voice agents.	For more information, see *Administering Avaya Workforce Optimization Select*.		
10	Enable screen capture for agents.	For more information, see *Administering Avaya Workforce Optimization Select*.		
11	Enable user feature privileges and report feature privileges for the relevant designation.	For more information, see *Administering Avaya Workforce Optimization Select*.		
12	Log in as a supervisor.	For more information, see *Using Avaya Workforce Optimization Select*.		
13	Search for recorded interactions through the Reports module and playback the interactions.	For more information, see *Using Avaya Workforce Optimization Select*.		
14	Playback interactions through the Live Monitoring module and install the Active X control on the machine of the supervisor.	For more information, see *Using Avaya Workforce Optimization Select*.		

Setting passwords for services.msc components

About this task

Use this procedure to change the password for all the components. Use the password that you use to log in to the web application.

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** > **Web** > **Start Web**.
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 back up the data that exists on the server where the web application is installed. For multiserver installations, back up 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, backup the following folders:
   - `WFO_Home` folder located at `C:\Program Data\WFO_Home` by default. Avaya recommends that you install this folder on `E:\` drive so that there is no conflict with the installation directory.
   - `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:\Program Data\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, backup the following folders:
   - `WFO_Home` folder located at `C:\Program Data\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.
   - `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:\Program Data\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 .

Procedure

1. Copy the `WFO_Home` folder and place it at `C:\Program Data\WFO_Home` or `E:\WFO_Home`.
2. Copy the `Voice` folder to the drive you specified during installation.
3. Copy the `Voice Data` folder to the drive you specified during installation.
4. Copy the `Logs` folder and place it at `C:\Program Data\Logs` or `E:\Logs`.

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 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 **Tasks** > **Back Up**.
3. To take a backup of the tenant database, select the tenant database.
4. Browse and expand the path to place the backup of the database.
5. Enter a file name with .bak extension and date and time stamp it for future reference.
6. Click **OK**.
7. Specify a drive, file path, and name of the backup file and click **OK**.

8. 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.
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 8: System verification checklist

Tasks	Reference	✔
Start the SysAdmin service.	See Starting the Avaya Workforce Optimization Select components on page 110.	
Access the SysAdmin URL.	See Logging on to SysAdmin on page 51.	
Start the web application service.	See Starting the Avaya Workforce Optimization Select components on page 110.	
Access the web application URL.	For more information, see *Administering Avaya Workforce Optimization Select*.	

Chapter 9: 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

About this task

Use this procedure to find product documentation on the Avaya Support website.

Procedure

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com/.
2. At the top of the screen, enter your username and password and click **Login**.
3. Put your cursor over **Support by Product**.
4. Click **Documents**.
5. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
6. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
7. Use the **Content Type** filter on the left to select the type of document you are looking for, or click **Select All** to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
8. 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.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation

- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base at no extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base to look up potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya User ID and password.

   The Support page appears.
3. Under **Support by Product**, click **Product-specific support**.
4. Enter the product in **Enter Product Name** text box and press Enter.
5. Select the product from the drop down list and choose the relevant release.
6. Select the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

A

AACC 66, 67, 76, 77
ACCS 84, 85
active recording
  AACC deployments 16
adapter configuration
  AACC-CM 67
  AACC-CS1000 77
  Avaya Contact Center Select 85
  IP Office Contact Center 92
adapter parameters 92
adapters 11
AES adapter 67
alert manager 65
alerts 65
Avaya Adapter 67, 77, 92
Avaya Aura Contact Center 16, 66, 67, 76, 77
Avaya CCTNet Adapter 67, 77, 85
Avaya Contact Center Select 19, 84, 85

B

backing up
  database files 116
  server data 115
backup 114
browser setting
  Google Chrome 46
  Internet Explorer 46
browser settings
  Mozilla Firefox 47

C

call signaling 13
CA-signed SSL certificate
  replacing self-signed certificate 118
Changing server IP address
  DNS deployment 109
changing the node name
  DNS deployments 109
  high availability 42
checklist
  AACC-CM 66
  ACCS-IPO 84
  configuration 44
  configuring Avaya Aura Contact Center 76
  Desktop Monitor 104
  initial administration 112
  IPOCC-IPO 92
  planning 25
  post installation 44
  post installation verification 119
  pre-installation 33
  site preparation 27
CM 66
Communication Manager 66, 67
Communication Server 1000 ..... 76, 77
component parameter
  configuring 53, 110
component parameters 54
components 9
configuration
  network port 32
configuration tools and utilities
  deployment 27
configuring
  component parameters 53, 110
  ED service 45
  ESXi server 107
  high availability 42
  log file parameters 50
  NIC driver settings 108
  resource files 105
  screen capture 101
  TAPI 48
configuring parameters
  recorder 61
configuring proxy IP address
  multi server deployments 51
creating
  data partition 52
CS1000 ..... 76, 77
CS 1000 deployments
  WebLM support 84

D

database files 116, 117
Database Settings 40
Decryption 45
default tenant name
  update 52
deployment
  configuration tools and utilities 27
  deployment tools 8
  limitations 98
  process 24
deployment configurations 12
deployment environments 15
deployment scenarios
  AACC active recording 16
  AACC passive recording 17
  ACCS passive recording 19
  IPOCC IPO passive recording 21

desktop monitor 104
Desktop Monitor 104
desktop trigger client machine 35
disabling
TAPI tracing 50
DNS deployment
Changing server IP address 109
downloading software 30
dynamic configurations
recorder 62

E

enabling
TAPI tracing 49
Encryption 45
environment variables
setting 31
ethernet
network considerations 32
executing
script generator 106

F

field descriptions
component parameters 54
database settings 40
installing required information 39
install mail server configuration 40
install standard profile 38
fixed seating 22
free seating 22

H

hardware requirements
multi box deployment 35
single box deployment 35
high availability 42

I

initial administration
starting web application 114
worksheet 26
InSite Knowledge Base 122
install
custom 37
standard 37
installation
worksheet 25
install database server
field descriptions 40
installing
learning console 105
screen capture 101
TAPI3 driver 48
TSAPI client 31
install mail server configuration
field description 40
integration scenarios 15
IPOCC 92
IP Office 49, 50, 84, 85, 92
IP Office Contact Center 21, 92
IP Office Contact Center Select 92

L

legal notices .....
license manager 43
limitations
deployment 98
log file parameters
configuring 50
logging off
sysadmin 66
logging on
sysadmin 51
Log Manager parameters 59

M

Mail Server Configuration 40
managing
licenses 43
users 65
Media Manager parameters 54
Messaging parameters 56
multi box deployment — application and database server .. 35
multi box deployment — Recorder server 35
multi server deployments
configuring proxy IP address 51

N

network considerations
ethernet 32
network port
configuration 32
NIC driver 108

O

overview 9

P

Packet Sniffer parameters 60
parameter 51
parameters
Log Manager 59

parameters *(continued)*
Media manager 54
Messaging 56
Packet Sniffer 60
Process checklist 56
Recorder 57
SysAdmin 61
passive recording
AACC 17, 19
IPOCC IPO 21
planning
checklist 25
PLDS 30
downloading software 30
port 32
port mirroring 107
post installation verification
checklist 119
pre-installation
checlist 33
prerequisite 8
process 24
Process checklist parameters 56
product compatibility 31

R

recorder
configuring parameters 61
dynamic configurations 62
Recorder dynamic configurations 62
Recorder dynamic parameters 63
Recorder parameters 57
recording
active 13
passive 13
registering 30
related documentation 120
replacing self-signed certificate
CA-signed SSL certificate 118
Required Information 39
requirement
database 28
operating system 28
reporting services 28
restarting
web application service 64
restarting the components
DNS deployments 111
restore 114
restoring
data 116
database files 117

S

Screen Capture 101, 103
script generator
executing 106
server data 115
services.msc components 113
setting
environment variables 31
password 113
single box deployment 35
site preparation
checklist 27
software requirement 28
spanning 107
standard profile 38
field descriptions 38
starting the components
DNS deployments 110
starting web application
initial administration 114
stopping the components
DNS deployments 109
support 122
sysadmin
logging off 66
logging on 51
SysAdmin 51, 61, 65
SysAdmin parameters 61
system administration 51

T

TAPI
configuring 48
TAPI3 driver
installing 48
TAPI Adapter 85, 92
tenant management 51
toplogy 12
TSAPI client
installing 31

U

update
default tenant name 52
uploading
Screen Capture logs 103

V

verifying
agent login 102
Screen Capture logs 103
videos 122
viewing
alerts 65
license details 53

W

web application 114
web application service
    restarting 64
WebLM 43
WebLM support
    CS 1000 deployments 84
worksheet
    initial administration 26
    installation 25