Administering Avaya Workforce Optimization Select

Release 5.2.2
Issue 2
November 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

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, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

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.

Contents

Chapter 1: Introduction

Purpose

This document contains information about how to perform Avaya Workforce Optimization Select administration tasks . These tasks include how to use management tools, how to manage data and security, and how to perform periodic maintenance tasks.

This document is intended for people who perform system administration tasks on Avaya Workforce Optimization Select , such as backing up and restoring data and managing users.

New in this release

Avaya Workforce Optimization Select release 5.2.2 supports the following new features and enhancements for administering:

New feature or enhancement	Name	Description
New feature	Adhoc Interactions	Enable the option to manage adhoc interactions from the Privileges screen. Managing incudes importing recorded interaction, creating a composite interaction, and editing and deleting interactions. You must manually select the Manage Adhoc Interactions checkbox to enable this privilege at a role or at an employee level.
New feature	User Level Queues Access	Manage the queues that a particular employee can have access to from the Employee Access screen.
New feature	Recording Filters	Define recording settings for Vector Directory Numbers (VDNs) and Hunt Groups from the Recording Filters page in Settings. **Note:** The Recording Filters feature is available only when Avaya Workforce Optimization Select is deployed with Avaya Aura® Call Center Elite on Avaya Aura® Communication Manager.

Table continues…

New feature or enhancement	Name	Description
Enhancement	Default records per page	Decide the number of rows to display in the grids of the respective modules for a particular employee from the General Settings screen.

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.

Chapter 3: Administrative tasks

Administrator responsibilities

- Determine whether to import employees through LDAP or through a spreadsheet.
- Map users to their relevant job functions, locations, and departments.
- Manage system security by analyzing different roles in the organization and mapping them to the privileges in the system.
- Identify the need for creating custom groups and associating users to these groups.
- Define recording rules for interactions according to business requirements.
- Define the storage and retention period for interactions according to business requirements for each business unit.
- Manage identity certificates for secured communication among the different Avaya Workforce Optimization Select elements.

Administration checklist

The following administration tasks are required for a new installation of Avaya Workforce Optimization Select:

No.	Task	Reference	Notes	✔
1	Create the following in sequential order to mirror the organizational structure of your company: • Sites • Organization units • Departments • Roles	• Adding sites on page 18 • Adding organization units on page 20 • Adding departments on page 22 • Adding roles on page 23		
2	Configure general settings like time zone, language, consent based recording, and	Configuring general settings on page 80		

Table continues…

No.	Task	Reference	Notes	✔
	screen capture settings that apply globally to all employees.			
3	Add employees and assign the site, department, role, reporting supervisor, and organization unit specific to their job function.	Creating employee profiles on page 27		
4	Configure recording settings for employees to determine how you want to record interactions and corresponding screen shots. You can configure settings based on employee shift, random recording, percentage of interactions to be recorded, and on-demand recording.	Configuring recording settings on page 34		
5	Configure feature privileges to define what an employee can or cannot access in the application.	Assigning Privileges on page 41		
6	Define employee access based on different operations within the organization.	Providing employee access on page 48		
7	Configure report privileges to define the reports that an employee can or cannot access in the application.	Assigning report privileges on page 50		
8	Import employees in bulk using an Excel spreadsheet.	Importing employees on page 52		
9	Configure LDAP setting to synchronize user data when an employee signs in to the application.	Configuring LDAP settings on page 94		
10	Configure Recording Targets to define recording settings based on stations.	Configuring Recording Targets on page 89		
11	Create recording rules to decide what interactions must be recorded at a global level.	Creating recording rules on page 85		
12	Manage and configure storage rules for archiving, compressing, moving, copying, and purging or deleting voice files and screens.	Creating and assigning storage manager rules on page 71		
13	Configure rules for password policy that enhance system security.	Configuring the password policy on page 96		
14	Configure Recording Filters to define recording settings for Vector Directory Numbers (VDNs) and Hunt Groups.	Configuring recording filters on page 92		
15	Update employee profile, privileges, and recording settings in bulk.	Performing bulk actions on page 59		

Table continues…

No.	Task	Reference	Notes	✔
16	Add queues and configure threshold values for alerts.	Adding queues on page 65		
17	Create groups of employees for specific business cases if required.	Creating groups on page 100		
18	Configure settings for windows active directory services to synchronize employee data.	Configuring LDAP settings on page 94		
19	Manage identity certificates for secured communication among the different elements of Avaya Workforce Optimization Select. Replace identity certificates by getting new SSL certificates from the third-party Certification Authority (CA) and deploying the signed certificates in the Apache instances.	• Getting a new SSL identity certificate from the third-party CA on page 103 • Deploying the trusted signed certificate on page 104		

Chapter 4: Accessing Avaya Workforce Optimization Select

Avaya Workforce Optimization Select administration overview

Using the Administration module in Avaya Workforce Optimization Select, you can administer employees by managing sites, departments, organization units, and roles in an organization.

Logging on to Avaya Workforce Optimization Select

Procedure

1. Open a compatible web browser on your computer.
2. Depending on the server configuration, type one of the following:

   - The unique IP address of the Avaya Workforce Optimization Select server in the standard dotted-decimal notation.

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

   - The unique host name of the Avaya Workforce Optimization Select server.

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

   You can now log in to the Avaya Workforce Optimization Select application.
3. Type the user name and password.

   Use the login credentials of the tenant user you created in SysAdmin.
4. Click **Sign in**.

   The system displays the Avaya Workforce Optimization Select home page. When you log in to the application for the first time, the system displays the Settings dialog box to configure data partition.

Configuring data partition

About this task

When you log in to Avaya Workforce Optimization Select for the first time, the system displays the Settings window to configure data partition. Using data partitions, you can restrict data access across various groups within an organization. You can create only one data partition organization unit (OU) type when you log in for the first time. However, you can associate multiple organization units to a data partition OU type at a later stage. You cannot delete a data partition after it is created.

Before you begin

Get your tenant user name and password from the system administrator.

Procedure

1. On the Settings window, in the **Do you wish to enable data partition** field, click one of the following options:

   - **Yes**: The system enables the DP OU Type Name field.
   - **No**: The tenant is enabled without a data partition. You cannot enable the data partitioning at a later date and time.

2. In the **DP OU Type Name** field, type the name of the data partition organization unit type.

   The data partition name must not contain any spaces. You can enter up to 100 characters in this field.

3. Click **Save**.

   The system displays the **Password Change** window.

4. **(Optional)** If you want to change the system-generated tenant administrator password, type your new user password and click **Save**.

Related links

Organization units overview on page 19

Avaya Workforce Optimization Select Home page

When you log in to Avaya Workforce Optimization Select, the Home page displays navigation links for quick access to the modules in the application.

✱ **Note:**

The administrator configures module level access privileges for each user. You can see only those modules for which the application administrator provides you access.

The interface has the following sections:

- The title bar: To navigate to the My Profile settings.

- The main menu: To navigate to the different modules in the application.
- The side bar: To navigate to the submenu within each module.
- The navigation bar: To navigate to the submenu options within each module.

Administration interface

Name	Description
Home	Provides quick access to all modules in the application and back to the Home page from any page.
Administration	Provides administrative owners access to the organization, employee and group configuration, recording rule setting, queue management, account configuration, and general settings.

Authenticating users

About this task

Use this procedure to get access to the **Administration** module or any feature under the **Administration** module when you log in to the application every time. The system displays the authenticate user page for additional security. This step prevents any unauthorized users from making changes in the administration settings, which is crucial for the overall functioning of the application. You can choose to close the authentication window, but closing it logs you out of the application.

Procedure

1. Click **Administration**.

   The system displays the Authenticate User page.

2. In the **Password** field, enter the password and click **Submit**.

Logging off from Avaya Workforce Optimization Select

Procedure

1. In the top right corner of any page, click **admin**.
2. In the drop-down list, click **Log out**.

   The system displays the logging in screen.

Chapter 5: Managing organization

Organization overview

Use the Organization feature in Avaya Workforce Optimization Select as a placeholder to mirror your organizational structure. You can view your organization profile and create sites, organization units, departments, and roles to meet your business requirements, simplify administration, and reduce maintenance tasks.

Viewing an organization profile

Procedure

Click **Administration** > **Organization**.

The system displays the Organization Profile page.

Organization profile field descriptions

Company Details

Name	Description
Name	The name of the company.
Alias	The alias of the company.
Status	The status of the company. The options are: • **Active**: This is the default status. • **Inactive**: You get access to previous records but you cannot create new records in the application.

Primary Contact

Name	Description
Name	The name of the primary contact.
Phone	The contact number of the primary contact.
Email	The email address of the primary contact.

Secondary Contact

Name	Description
Name	The name of the secondary contact.
Phone	The contact number of the secondary contact.
Email	The email address of the secondary contact.

License Details

Name	Description
Edition	The Avaya Workforce Optimization Select edition that your organization has subscribed for.
Purchased Licenses	The number of purchased licenses.
Default Modules	The Avaya Workforce Optimization Select modules subscribed to by default.
Expiry Date	The expiry date of the licenses.
Retention (days)	The number of days that calls and screen captures can be stored on the local server after they get automatically archived.
Storage Capacity (GB)	The file storage capacity provided to the company.
Available Capacity (GB)	The available or remaining file storage capacity. For example, if the total file storage capacity is 10 GB, and you have already stored calls and screens that occupy 5 GB, then the available storage capacity is 5 GB.
Optional Module Name and Expiry Dates (MM/DD/YYYY)	The optional modules that you subscribed to along with expiry dates.

Sites overview

You can use sites to define the location of a company or an organization. Sites can refer to the name of a city, building, floor, or room. Administrators can create multiple sites to reflect the different locations that a company operates from. It is important to associate employees working in different locations to the relevant sites. Based on the association of a site with an employee, supervisors or managers can track interactions belonging to a particular site.

Adding sites

Procedure

1. Click **Administration** > **Organization** > **Sites**.
2. Click **Add Site**.

   The system displays the Add New Site page.

3. Enter the appropriate information in the fields.
4. Click **Save & Close**.

Sites field descriptions

Name	Description
Name	The unique name of the site. You can enter up to 100 characters in this field. This field is mandatory.
Alias	The unique abbreviation that the system automatically creates by taking the first three letters of the site name. For example, AME for America. If the site name is more than one word, the first letter of each word is taken as the site alias. For example, USOA for United States of America. You can enter up to 10 characters in this field. This field is mandatory.
Active	The option to activate and deactivate a site. The allowed values are **Active** and **Inactive**. The default status is **Active**. A site that is active is available for filtering, association, and report generation. You cannot deactivate or delete a site that has users associated with the site. You need to associate the users to another site before deactivating the site.
Time Zone	The time zone of the site. The time zone that you configure in General Settings appears by default. However, you can change the time zone for a site especially when you want to add sites situated in different geographical locations.
Description	The description of the site. You can enter up to 500 characters in this field.
Custom Fields	The option to select an additional custom fields for a site.

Organization units overview

Administrators can create organization units to mirror the functional or business structure, such as clients, services, or business processes of an organization. You can create multiple organization units to reflect different operations. You can manage and control a group of employees based on different operations within the organization. You can track interactions of employees and generate reports based on the organization units that an employee belongs to.

Organization unit (OU) types

Administrators can use organization unit types to group multiple organization units under a category. For example, assume that your contact center provides services to clients such as

Samsung, Idea, Vodafone, and Airtel. You can create an organization unit type called clients and group the different organization units for Samsung, Idea, Vodafone, and Airtel under the client organization unit type.

You can also create multiple organization unit types to group various organization units for customers, business processes, services, or departments.

Data Partition OU types

Administrators might want to restrict data access across various groups within an organization. For example, you might want to restrict employees of the Samsung group from viewing and accessing data of employees belonging to the Airtel group. In such cases, you can define a data partition entity while installing the Avaya Workforce Optimization Select application. Administrators can use the data partition entity to segregate groups within an organization. You must manually group all employees within the available organization unit types.

The main purpose of creating data partition is to secure data access across groups within the organization. You can define only one data partition OU type for an organization. A conscious decision must be taken to define data partition because you cannot modify or delete a data partition after it is defined.

Adding organization units

Before you begin

Ensure you create OU types before adding organization units as it is mandatory to associate an organization unit to an OU type.

Procedure

1. Click **Administration** > **Organization** > **Organization Units**.
2. Click **Add Organization Unit**.
3. On the Add New Organization Unit page, enter the appropriate information in the fields.
4. Click **Save & Close**.

Organization Units field descriptions

Name	Description
Name	The name of the organization unit. You can enter up to 100 characters in this field. This field is mandatory.
Alias	A unique abbreviation that the system automatically creates by taking the first three letters of the organization unit. For example, AME for America. If the organization unit name is more than one word, the first letter of each word is taken as the organization unit alias. For example, TBSS for Tata Business Support Services.

Table continues…

Name	Description
	You can enter up to 10 characters in this field. This field is mandatory.
Active	The option to activate and deactivate an organization unit. The allowed values are **Active** and **Inactive**. The default status is **Active**. An organization unit that is active is available for filtering, association, and report generation. You cannot deactivate or delete an organization unit that has users associated with the organization unit. You need to associate the users to another organization unit before deactivating the organization unit.
OU Type	The type of organization unit. Mapping an OU type is a one-time activity. To remove the OU type association from an organization unit, you must delete the organization unit and create a new one.
Description	A description of the organization unit. You can enter up to 500 characters in this field.
Custom Fields	The option to select an additional custom fields for an organization unit.

Adding OU types

Procedure

1. Click **Administration** > **Organization** > **Organization Units**.
2. Click **Manage OU Types**.
3. On the Manage OU Types page, click **Add OU Type**.
4. Enter the appropriate information in the fields.
5. Click **Save & Close**.

Add OU Type field descriptions

Name	Description
Name	The name of the OU type. This field is mandatory. You can enter up to 100 characters in this field.
Is Default	The option to indicate whether the OU type is a default OU type. You can specify only one OU type as default.
Active	The option to indicate whether the OU type is an active OU type. The default status is **Active**.
Description	The description of the OU type. You can enter up to 500 characters in this field.

Departments overview

In Avaya Workforce Optimization Select, departments refer to the different divisions within an organization. Ideally, administrators add departments to resemble the business model within an organization. Administrators can also use departments to group employees and generate reports based on the department to which an employee belongs.

Adding departments

Procedure

1. Click **Administration** > **Organization** > **Departments**.
2. Click **Add Department**.
3. On the Add New Department page, enter the appropriate details.
4. Click **Save & Close**.

Departments field descriptions

Name	Description
Name	The unique name of the department. You can enter up to 100 characters in this field. This field is mandatory.
Alias	A unique abbreviation that the system automatically creates by taking the first three letters of the department name. For example, QUA for Quality. If the name of the department is more than one word, the first letter of each word is taken as the department alias. For example, SAM for Sales and Marketing. You can enter up to 10 characters in this field. This field is mandatory.
Active	The option to activate and deactivate a department. The allowed values are **Active** and **Inactive**. The default status is **Active**. A department that is active is available for filtering, association, and report generation. You cannot deactivate or delete a department that has users associated with the department. You need to associate the users to another department before deactivating the department.
Description	A description of the department. You can enter up to 500 characters in this field.
Custom Fields	The option to select an additional custom fields for a department.

Roles overview

In Avaya Workforce Optimization Select , roles refer to the designation or job title of an employee.

You can use roles to define the job function of an employee. You can assign privileges to a role to control what a user can or cannot access thereby enhancing security for users. Administrators can create multiple roles and assign privileges to a role. Employees belonging to a role inherit the privileges assigned to the role.

When creating roles, administrators can start with the topmost designation or role to create a reporting hierarchy by specifying who the role reports to. If a supervisor reports to a manager, you create the Manager role first and then the Supervisor role. When you define who the role reports to, Avaya Workforce Optimization Select automatically creates a hierarchy.

Adding roles

Procedure

1. Click **Administration** > **Organization** > **Roles**.
2. Click **Add Role**.
3. On the Add New Role page, enter the appropriate details.
4. Select the required privileges for the role.
5. Click **Save & Close**.

Roles field descriptions

Name	Description
Name	The unique name of the role. You can enter up to 100 characters in this field. This field is mandatory.
Alias	A unique abbreviation that the system automatically creates by taking the first three letters of the role. For example, SUP for Supervisor. If the name of the role is more than one word, the first letter of each word is taken as the role alias. For example, SOM for Senior Operations Manager. You can enter up to 10 characters in this field. This field is mandatory.
Active	The option to activate and deactivate a role. The default status is **Active**. The allowed values are **Active** and **Inactive**.

Table continues…

Name	Description
	A role that is active is available for filtering, association, and report generation. You cannot deactivate or delete a role that has users associated with the role. You need to associate the users to another role before deactivating the role.
Reporting to	The role that the employee reports to. Use this option to create role hierarchy. For example, if a Supervisor reports to a Manager, create the Manager role first. When you create the Supervisor role, select Manager in the **Reporting to** field to define a role hierarchy.
Description	A description of the role. You can enter up to 500 characters in this field.
Privileges	Privileges are module specific and list various actions a user can perform within a module. You can assign privileges to a role. Users that you add to the role automatically inherit the privileges. The various module specific privileges are: • **Interactions**: Defines permissions to playback, record, comment, download, email interactions and manage interaction views. • **Live Monitoring**: Defines permissions to monitor live interactions and manage live monitoring views. • **Evaluate**: Defines permissions to access and manage features, and to manage evaluation related views within the Evaluate module. • **Coach**: Defines permissions to access and manage features, and to manage coaching views within the Coach module. • **Learn**: Defines permissions to access and manage features, and to manage team assignment views within the Learn module. • **Analyze**: Defines permissions to access and manage measures, metric views, and scorecards within the Analyze module. • **Reports and Dashboards**: Defines permissions to manage reports settings and results and the landing page. • **Administration**: Defines permissions to access and manage features within the Administration module.
Report Privileges	Privileges that provide users access to various predefined module specific reports. You can assign privileges to a role. Users that you add to the role automatically inherit the privileges The various report privileges are: • **Interactions**: Defines permissions to view interaction reports such as the Interactions Details, Interactions Summary, Interactions Trend, and AHT Trend reports. • **Evaluations**: Defines permissions to view evaluation reports such as the Evaluations Summary, Evaluation Details, and Evaluation Trend reports.

Table continues…

Name	Description
	- **Coach**: Defines permissions to view coaching reports such as the Coaching Summary report. - **Learn**: Defines permissions to view learn reports such as the Course & Quiz Summary report. - **Administration**: Defines permissions to view common reports such as the Employee Recording Configuration, User Access, and Web Usage Audit reports.
Custom Fields	The option to select an additional custom fields for a role.

Adding custom fields

Procedure

1. Click **Administration** and then click one of the following:
    - **Organization** > **Sites**
    - **Organization** > **Organization Units**
    - **Organization** > **Departments**
    - **Organization** > **Roles**
    - **Queues**
    - **Employee**
2. Click **Custom Fields**.
3. Enter the appropriate information in the fields.
4. Click **Save & Close**.

Custom Fields field descriptions

Name	Description
Custom Field *x*	The name of the custom field that you want to add, where x is the number of the field. The options are: - 1 - 2 - 3 - 4 - 5 You can add up to five custom fields.

Table continues…

Name	Description
List of Values	The values that appear in the drop-down list of a custom field. You can enter multiple values separated by commas.

Chapter 6: Managing employees

Employee management overview

Administration becomes efficient and easy when you create profiles for all employees within the contact center.

Administrators can manage the employees by configuring:

- Employee Profile
- Recording Settings
- Privileges
- Employee Access
- Report Privileges

Employee profile overview

In Avaya Workforce Optimization Select , you can create profiles for each employee and map employees to sites, organization units, departments, and roles. Depending on the authentication method on the General Settings page, you can create an employee profile through LDAP or the Local authentication mode. You must configure employee profiles for Avaya Workforce Optimization Select to record and store interactions depending on the sites and organization units that an employee is associated with.

Creating employee profiles

Procedure

1. Click **Administration** > **Employees** > **Add Employee**.
2. On the Profile page, type the appropriate information in the fields.
3. Click **Save**.

Employee Profile field descriptions

Name	Description
Employee Code	The unique code of the employee. You can enter up to 30 characters in this field. This field is mandatory.
First Name	The first name of the employee. You can enter up to 100 characters in this field. The system displays the first and the last in the Live Monitoring, Interactions, Evaluate, Coach, and Reports modules. This field is mandatory and is a default field.
Last Name	The last name of the employee. You can enter up to 100 characters in this field. The system displays the first and last name in the Live Monitoring, Interactions, Evaluate, Coach, and Reports modules. This field is mandatory and is a default field.
Alias	The unique abbreviation that the system automatically creates by taking the first three letters of the employee name. You can also edit the alias name if needed. You can enter up to 10 characters in this field. This field is mandatory.
Hire Date	The date when the employee was hired in the mm/dd/yyyy format. The system calculates the tenure of the employee based on the hire date. This field is mandatory.
Authentication Mode	The option to define a higher level user authentication method using the following modes: The changes depend on the selections made in the general settings. • LDAP: The option to configure Lightweight Directory Access Protocol (LDAP) authentication method for users. • Local: The option to configure Local authentication method for users. This option prompts users to enter their login credentials to access the application.
Username	The login id of the employee used to log in to the application. The user name must not exceed 30 characters. When you select the LDAP option for **Authentication Mode**, the system displays the validate button to verify if the users exist in the way the name appear in this field in the LDAP server. This field is mandatory and is a default field.
Email	The email address of the employee. Employees receive alerts, notifications, interaction links, and reports in your mail box based on the email address. This field is mandatory.

Table continues…

Name	Description
Department	The department that the employee belongs to. This field is mandatory.
Role	The role or designation that the employee holds. This field is mandatory and is a default field.
LOB	The data partition organization unit that is configured while logging in to the application for the first time. In this instance, LOB stands for Line of Business.
Reporting to	The supervisor that the employee reports to. The **Reporting to** drop-down list displays all the employees above the selected role. This role hierarchy is already defined in Roles. This field is a default field.
Upload	The field to upload an image of the employee. You can upload images in .jpeg and .png formats. You can change or remove the uploaded image at any time.
App User	The option to give the employee access to the application. You can control the modules that an employee can access within the application. You can view and assign permissions to an employee to access specific features within all modules, except the Administration module. Apart from the modules, an app user can also manage the settings of the landing page of an user. Depending on the privilege or role of an employee, an app user can set the Avaya Workforce Optimization Select homepage or the dashboard as the default landing page.
App Admin	The option to give the employee access to the Administration module. You can control which employees must get access to the Administration module. You can view and assign administration permissions to the employee.
Landing Page	The option to set the default landing page of an employee. The options are: • Home • Dashboard This option is only available when you select the **App User** or the **App Admin** check boxes.
Site	The site that the employee belongs to. This field is mandatory.
Time Zone	The time zone that the employee belongs to. The time zone displays a list of options based on the site that you click.

Table continues…

Name	Description
Language	The language selected for the employee. The options are: • English (US) • German (Germany) • Spanish • French • French (Canada) • Italian • Korean • Simplified Chinese • Traditional Chinese • Japanese (Japan) • Portuguese (Brazil) • Russian The default language is **English (US)**. If you configure the language in General Settings, that language becomes the default.
Status	The status of the employee. The options are: • **Active**: The default status. • **Inactive** The field is a default field.
OU Type	The OU Type that the employee is mapped to.
Organization Units	The Organization Unit that the employee is mapped to.
Reset Password	The option to reset the current password of an employee to the default password.
Release Lock	The option to unlock the account of an employee if **Lockout Duration** is set to **Until Unlock By Administrator**.
Custom Fields	The option to select an additional custom fields for an employee.

Recording settings overview

Recording settings is an employee level setting that administrators can use to decide how the interactions must be recorded for an employee.

Configure Recording settings to:

- Record interactions against ID type, ID value, channel of interaction, and contact instances. For agent-based recording, where agents work in shifts, the extension, device ID, and contact instance can be the same for multiple agents. In such cases, administrators can use the organization unit type as the unique identifier to differentiate between two interactions.

The additional recording attributes serve as placeholders for the administrators to associate additional information to a recording target.

- Define the frequency of recording interactions and screens. You can configure interaction and screen recording options that meet the contact center business requirements. You can specify 100% recording of all interactions along with screens. You can also specify random or on demand recording of interactions and screens.
- Specify a certain percentage of interactions you want to record for an employee. The Avaya Workforce Optimization Select application records all the interactions, calculates the specified percentage, and purges the extra interactions at the end of the calendar day. However, the Avaya Workforce Optimization Select application stores the metadata of the interactions even if the interaction is not retained.
- Handle multiple concurrent contacts to improve customer experience and enhance agent productivity and efficiency. Avaya Workforce Optimization Select supports multi-channel communication such as voice, chat, email, and SMS. With multiplicity, a single agent might have multiple data records describing the current agent status. For example, a record is available for each contact that the agent is concurrently handling.

To configure the recording settings for an individual employee profile, see the General Settings field descriptions on page 80.

Agent profiles overview

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.

If an agent profile is configured for 100% recording and if the extension or DN is configured for on demand segment recording, then the agent profile takes priority. However, if the agent has not logged in to the phone or if the agent profile is configured for fixed seating, then the extension or DN takes priority.

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, configure the **Extension** in the Recording Settings for an employee profile.

Free Seating

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

- The **Agent ID** in one employee profile

- The **Extension** in the other employee profile

Deployment specific employee profiles

The tables below lists the number of employee profiles instances you must create for free and/or fixed seating and the ID Type you must configure for each instance.

Avaya Workforce Optimization Select on Avaya Aura® Contact Center and Communication Manager

Deployments	Seating	Instance(s)	ID Type
Avaya Aura® Contact Center on Communication Manager	Fixed	1	Extension
	Free	2	Agent ID
			Extension
Avaya Aura® Contact Center on Communication Manager and Avaya Proactive Outreach Manager	Fixed	1	Extension
	Free	2	Agent ID
			Extension

Avaya Workforce Optimization Select on Call Center Elite and Communication Manager

Deployments	Seating	Instance(s)	ID Type
Call Center Elite on Communication Manager	Fixed	1	Extension
	Free	2	Agent ID
			Extension
Call Center Elite on Communication Manager and Avaya Proactive Contact with CTI	Fixed	1	Extension
	Free	2	Agent ID
			Extension
Call Center Elite on Communication Manager and Avaya Proactive Outreach Manager	Fixed	1	Extension
	Free	2	Agent ID
			Extension
Call Center Elite on Communication Manager and Avaya Session Border Controller	Fixed	2	Extension
			Dummy extension
	Free	3	Agent ID
			Extension
			Dummy extension

Avaya Workforce Optimization Select on Avaya Communication Server 1000

Deployments	Seating	Instance(s)	ID Type
Avaya Aura® Contact Center on Avaya Communication Server 1000	Fixed	1	• Extension • Position ID
	Free	2	Agent ID
			• Extension • Position ID

Avaya Workforce Optimization Select on IP Office

Deployments	Seating	Instance(s)	ID Type
Avaya Contact Center Select on IP Office 9.x	Fixed	1	Extension
	Free	2	Agent ID
			Extension
IP Office Contact Center on IP Office 9.x	Fixed	1	Extension
	Free	2	Agent ID
			Extension
Avaya Contact Center Select on IP Office 10.x	Fixed	1	Extension
	Free	2	Agent ID
			Extension
IP Office Contact Center on IP Office 10.x	Fixed	1	Extension
	Free	2	Agent ID
			Extension

Avaya Oceana™ Solution on Communication Manager

Deployments	Seating	Instance(s)	ID Type
Avaya Oceana™ Solution on Communication Manager with Call Center Elite	Fixed	1	Extension
	Free	2	Agent ID
			Extension
Avaya Oceana™ Solution on Communication Manager with Call Center Elite and Avaya Proactive Outreach Manager	Fixed	1	Extension
	Free	2	Agent ID
			Extension

Configuring recording settings

Procedure

1. Click **Administration** > **Employees** > **Add Employee**.
2. On the Profile page, type the appropriate information in the fields.
3. Click **Save**.

   The system populates the navigation pane.
4. Click **Recording Settings**.

   The system displays the Edit Recording Settings page where the first four fields are prepopulated.
5. Type the details in the following fields:
   - **ID Type**
   - **ID Value**
   - **Channel**
   - **Contact Instance(s)**
6. **(Optional)** To add another instance, click the + Add icon.
7. Click the + icon next to the **ID Type** field and select the required details in the following sections:
   - Additional Attributes
   - Interactions Recording Options
   - Screen Recording Options
8. To save the recording settings, click the ✓ icon.

Configuring agent profiles for fixed seating

Procedure

1. Click **Administration** > **Employees** > **Add Employee**.
2. On the Profile page, type the appropriate information in the fields.
3. Click **Save**.

   The system populates the navigation pane.
4. Click **Recording Settings**.

   The system displays the Edit Recording Settings page.

5. Type of details in the following fields:
    - **ID Type**
    - **ID Value**
    - **Channel**
    - **Contact Instance(s)**
6. Click the + icon, select and type the required details in the following sections:
    - Additional Attributes
    - Interactions Recording Options
    - Screen Recording Options
7. To save the recording settings, click the ✓ icon.
8. Click + Add to add another instance.
9. Type the extension or the domain name in the **Extension** field. Leave all the other fields blank.
10. Click the + icon, select and type the required details in the following sections:
    - Additional Attributes
    - Interactions Recording Options
    - Screen Recording Options
11. To save the recording settings, click the ✓ icon.

Configuring agent profiles for free seating

Procedure

1. Click **Administration** > **Employees** > **Add Employee**.
2. On the Profile page, type the appropriate information in the fields.
3. Click **Save**.

    The system populates the navigation pane.
4. Click **Recording Settings**.

    The system displays the Edit Recording Settings page.
5. Type of details in the following fields:
    - **ID Type**
    - **ID Value**
    - **Channel**

   - **Contact Instance(s)**

6. Click the + icon, select and type the required details in the following sections:
   - Additional Attributes
   - Interactions Recording Options
   - Screen Recording Options
7. To save the recording settings, click the ✓ icon.
8. Type the extension or the domain name in the **Extension** field. Leave all the other fields blank.
9. Click the + icon, select and type the required details in the following sections:
   - Additional Attributes
   - Interactions Recording Options
   - Screen Recording Options
10. To save the recording settings, click the ✓ icon.
11. To create another profile or an extension profile for the same employee, click **Administration** > **Employees** > **Add Employee**.
12. Click + Add to add another instance.
13. On the Profile page, type the appropriate information in the fields.
14. Click **Save**.

    The system populates the navigation pane.
15. Click **Recording Settings**.

    The system displays the Edit Recording Settings page.
16. Type of details in the following fields:
    - **ID Type**
    - **ID Value**
    - **Contact Instance(s)**
17. Click the + icon, select and type the required details in the following sections:
    - Additional Attributes
    - Interactions Recording Options
    - Screen Recording Options
18. Click + Add to add a second instance.
19. In the second instance, type the extension or the domain name in the **Extension** field. Leave all the other fields blank.

20. Click the + icon, select and type the required details in the following sections:
    - Additional Attributes
    - Interactions Recording Options
    - Screen Recording Options
21. To save the recording settings, click the ✓ icon.

Edit Recording Settings field descriptions

General

Name	Description
Employee Name	The first and last name of the employee.
Username	The unique name used to log in to the application.
Max Recording Sessions	The maximum number of recording sessions allowed for the employees that are enabled for recording. in the organization.
Employees Enabled for Recording	The number of employees in the organization that are enabled for recording.
ID Type	The type of station. The options are: • Agent ID: The ID that the agent uses to log in to the phone. If you configure screen captures, the screen captures are recorded against the agent ID. • Extension: The VoIP phone extension of the employee. In a free seating environment, the Extension can be any free and unique extension number. • Port: The dummy recording stations used to record calls in Avaya Session Border Controller for Enterprise deployments for calls that are routed through IVRs. You must configure this port number range in SIP adapter, where Avaya Session Border Controller for Enterprise is enabled. • Position ID: The ID that the agent uses to log in to the phone. If you configure screen capture, the screen captures are recorded against the position ID. This option is used for Avaya Communication Server 1000 deployment. • Account Name: The unique name used for non-voice transactions. For example, the name of the agent. • SIP URI: The unique identification of an extension on which the agent is taking calls in URI. For example, name@domain.com

Table continues…

Name	Description
ID Value	The option to enter the relevant values based on the selected ID Type.
Channel	The channel for recording. The options are: • Voice • Email • Chat ✱ **Note:** SMS is also supported in an Oceana™ deployment configuration.
Contact Instance(s)	The number of voice and nonvoice interactions that you want an agent to handle concurrently. Defining this field ensures that multiple ID types are configured for every employee so that an employee can handle multiple concurrent interactions with different ID types.

Additional Attributes

✱ **Note:**

The additional attributes are available only when the administrator enables these fields in the Recording Attributes section on the General Settings page.

Name	Description
Machine Name	The name of the machine that the agent is using for interactions.
Machine IP	The IP address of the machine that the agent is using for interactions.
Device ID	The MAC (media access control) address of the physical device or phone that the employee uses. ✱ **Note:** If you re-use the same extension, ensure that the Extension and Device ID combination is unique.
Partition Name	The unique partition name used to differentiate an extension.
Alternate ID	The place holder where an agent can have the multiple associated networks. Currently, this parameter is not enabled in the application.
Phone IP	The IP address of the phone that the agent is using for interactions.
Terminal Number	The place holder for different types of recording environments. Currently, this parameter is not enabled in the application.
Security Code	The code used to configure the station password that the agent used to log in to the station. You can configure the code from the application or sync the same using Avaya adapter.

Interactions Recording Options

Name	Description
Interaction Recording Options	The option to enable recording rules for interactions.
Interaction Direction	The option to select the interaction direction. The options are: • **Inbound** • **Outbound** • **Bi-directional**
Monitor and Record All Interactions	The option to enable 100% recording of interactions. Using this option, a user can pause, resume, or cancel a recording but cannot start a recording.
Monitor and Record Complete Interactions On demand	The option to enable monitoring and recording of interactions on demand. On demand recording is initiated when a user selects the Record Call Now option during live monitoring. Using this option, a user can start, pause, resume, or cancel a recording.
Monitor and Record Segment of Interactions On demand	The option to enable monitoring and recording segments of interactions on demand. You can initiate on demand recording and trigger APIs to specify start, cancel, pause, resume, and stop recording for specific segments within an interaction. Using this option, a user can do the following recording options: • Start • Pause • Resume • Stop • Cancel
__ Percent of interactions to be monitored and recorded	The option to specify the percentage of interactions to be recorded. The Avaya Workforce Optimization Select application records all the interactions, calculates the specified percentage, and purges the extra interactions at the end of the calendar day. However, the Avaya Workforce Optimization Select application stores the metadata of the interactions even if the interaction is not recorded.
Do Not Record Interactions	The option to specify that you do not want to record interactions.
Interactions to be monitored and recorded randomly	The option to specify the number of interactions to be monitored and recorded. • If the interaction is already being recorded, a user can only pause, resume, and cancel a recording. The user cannot start a recording. • If the interaction is not recorded, a user can start, pause, resume, and cancel a recording.

Table continues…

Name	Description
Shift based	The option to record interactions according to employee shift. This option is enabled if the employee is part of a recording rule that has shift based enabled.

Screen Recording Options

Name	Description
Screen Recording Options	The option to enable screen recording for interactions.
Record Screens for All Interactions	The option to enable 100% screen recording of all interactions.
__ Percent of interactions with screens	The option to specify the percentage of screens to be recorded. The Avaya Workforce Optimization Select application records all screens, calculates the specified percentage, and purges the extra screens at the end of the calendar day.
Do Not Record Screens	The option to specify that you do not want to record interaction screens.
Screen Recording Interval	The option to select the screen capture recording interval in seconds. You must be judicious while configuring the interval, because with higher frequency, the numbers of screens to capture also increases. Capturing higher screens can lead to the risk of low disk space. For example, if you select 5 seconds, Avaya Workforce Optimization Select captures screens every 5 seconds that amounts to 12 screens a minute. Whereas, if you select 1 second, Avaya Workforce Optimization Select captures 60 screens a minute.
Screen Recording Quality	The option to select the screen recording quality in percentage.

Privileges overview

Administrators can define privileges to control what a user can or cannot access. The best practice is to assign privileges to a role so that employees belonging to that role automatically inherit the privileges. However, Administrators also have the flexibility to assign or modify privileges for a specific set of employees.

Privileges are module specific. Each permission defines one or more actions that a user can perform for a given module. While view permissions allow users to only view, manage permissions allow users to view, add, edit, and delete a particular object in the system.

Note:

If any privilege at an employee level is modified, then any change made thereafter at the corresponding role level does not cascade to the particular employee. You must manually change the privilege.

Privileges are grouped as:

- **Interactions**
- **Live Monitoring**
- **Evaluate**
- **Coach**
- **Learn**
- **Reports and Dashboards**
- **Administration**
- **Analyze**

An administrator can also restrict an employee's access to selected groups using the group-level privileges feature. To know more about group-level privileges, see Group-level privileges overview on page 54.

Assigning Privileges

Before you begin

Ensure that you enable **App User** for permissions to various modules or **App Admin** for administration permissions on the Profile page.

Procedure

1. Click **Administration** > **Employees** > **Add Employee**.
2. On the Profile page, type the appropriate information in the fields.
3. Click **Save**.

   The system populates the navigation pane.
4. Click **Privileges**.

   The system displays the Edit Privileges page.
5. Do any of the following depending on the privileges that you want to assign:
   - To enable all the privileges at one go, select the **All Feature Privileges** check box.
   - To select all the privileges of any module, select the respective module check boxes.
   - To select the privileges that you want to enable or disable for a module, click the module and then select the respective fields check boxes. For example: To assign the privilege for managing interactions playback, select the **Interactions** checkbox, click **Interactions** and select the **Manage Interactions Playback**.

Edit Privileges field descriptions

Interactions

Name	Description
Manage Interactions Playback	To playback interactions of employees that the user has access to.
Manage Interaction Views	To manage views. With the right permissions, users can see the system default views, and edit and delete views that they create in the **Interactions** module. Without permissions, users can see other users shared views and self-created views, but not system default views.
Manage Tags/Reason Codes	To view, add, edit, and delete reasons for using recording control on interactions of employees that the user has access to.
View Comments	To view comments on interactions of employees that the user has access to.
Manage Comments	To view, add, edit, and delete comments on interactions of employees that the user has access to.
Download Interactions	To download the interactions of employees that the user has access to.
Email Interactions	To email the interactions of employees that the user has access to.
Real Time Recording Controls - Start Recording	To record a live interaction.
Real Time Recording Controls - Pause/Resume Recording	To pause or resume a live recording.
Real Time Recording Controls - Stop Recording	To stop a live recording.
Real Time Recording Controls - Cancel Recording	To cancel live recording.
Manage Adhoc Interaction	To manage ad hoc interactions. With the right permissions, users can import, edit, delete, and evaluate these interactions. Currently, Avaya Workforce Optimization Select supports the following media file formats: • `.wav` • `.m4a` • `.mpeg-4` • `.mp3`

Live Monitoring

Name	Description
View Live Monitoring	To view and listen to live interactions of employees that the user has access to.
Manage Live Monitoring Views	To manage views. With the right permissions, users can see the system default views, and edit and delete views that they create in

Table continues…

Name	Description
	the **Live Monitoring** module. Without permissions, users can only see other users shared views, and self-created views.
Manage Feedback	To provide feedback on live interactions to employees that the user has access to.
Random Monitoring	To monitor selected interactions at specified intervals of only those employees that the user has access to.
Monitor next interaction of the selected agent(s)	To monitor the next interaction of selected employee.

Evaluate

Name	Description
View My Assignments	To view interactions that are assigned to the user for review.
Decline Assignments	To decline interactions that are assigned to the user for review.
Create & Edit Evaluation(s)	To evaluate an interaction using another evaluation form.
Delete my Evaluation(s) only	To delete evaluations completed by the user.
Delete Evaluation(s)	To delete all evaluations.
View Evaluation(s)	To view completed evaluations.
Manage Evaluation Views	To manage views. With the right permissions, users can see the system default views, and edit and delete views that they create in the **Evaluate** module. Without permissions, users cannot see system default views and can only see other users shared views, and self-created views.
View Adhoc Evaluations	To view ad hoc evaluations.
Manage Adhoc Evaluation Views	To manage views. With the right permissions, users can see the system default views, and edit and delete views that they create in the **Evaluate** module. Without permissions, users can only see other users shared views, and self-created views.
Mask Reviewer Name	To mask the reviewer’s name on all evaluation details for protecting the reviewer’s identity. The privilege applies to all the instances wherever the reviewer name gets displayed for that evaluation. When this option is selected the reviewer name displays as `xxxxx`. This feature is also available at the role level. Users can inherit this privilege from the role settings. This feature is not applicable to report templates and adhoc evaluations report output.
View Appeals	To view appeals.
Create & Edit Calibration(s)	To create and edit calibrations by assigning an interaction to multiple evaluators and setting a final score for the interaction.
Delete Calibration(s)	To delete calibrations.
View Employee Coverage	To view employees covered under different evaluation plans.

Table continues…

Name	Description
View QA Coverage	To view ad hoc evaluations and evaluations that are completed by employees under different evaluation plans.
Create & Edit Plan(s)	To create and manage evaluation plans for employees.
Delete Plan(s)	To delete evaluation plans.
Distribution Pool - Self Assignment	To view and assign interactions to the My Assignments page.
Distribution Pool - Manage	To view and assign interactions to reviewers.
Add & Edit Form(s)	To create and manage evaluation forms.
Delete Form(s)	To delete evaluation forms.
Manage Response Sets	To create and manage response sets.
Manage Evaluation Types	To create and manage evaluation types.
View Appeals Workflow	To view appeals workflow.
Manage Appeals Workflow	To manage appeals workflow.

Coach

Name	Description
Create & Edit Coaching Assignments	To assign employes to coachings within a specified period.
Delete Coaching Assignments	To remove coaching assignments.
Manage Coaching Views	To manage views. With the right permissions, users can see the system default views, and edit and delete views that they create in the **Coach** module. Without permissions, users can only see other users shared views, and self-created views.
Manage My Assignment	To view all coachings that the user needs to launch and complete.
Create & Edit Coaching Plans	To create and edit coaching plans for employees.
Delete Coaching Plans	To delete coaching plans.
Manage Parameter	To create and manage parameters that specify the areas of focus that a coaching addresses.

Learn

Name	Description
My Assignment	To view and launch courses and quizzes assigned to the user.
Manage Team Assignment	To view and check the status of courses and quizzes assigned to the team members of the user.
Manage Team Assignment Views	To manage views. With the right permissions, users can see the system default views, and edit and delete views that they create in the **Learn** module. Without permissions, users can only see other users shared views, and self-created views.

Table continues…

Name	Description
Manage Library	To create and manage courseware and quizzes for employees. You can upload videos, slide presentations, and other courseware. You can also create task specific quizzes for employees and assign a course or a quiz to employees.

Analyze

Name	Description
View Measure	To view the system measures.
View Metrics	To view the system and custom metrics.
Manage Metrics	To create and edit metrics.
View Score Cards	To view the score cards associated with a particular metric.
Manage Score Cards	To manage scorecards to create and edit existing scorecards.
Manage Metric Views	To manage the different metric views.
Manage Custom Metric Import	To manage all actions related custom metric import values.
Manage Custom Metric Data Entry	To manage all actions related custom metric data entry.

Reports and Dashboards

Name	Description
Manage reports results	To view generated reports.
Manage reports settings	To generate and schedule reports. The user can manage only those reports for which the user has permissions.
Manage reports schedules	To schedule reports. The user can run a report based on a schedule that the user sets. The user can manage only those reports for which the user has permissions.
Allow changing the landing page	To allow user to choose the default landing page.
Create & Edit dashboard	To manage their individual Dashboard view.

Administration

Name	Description
Manage Organization	To view the organization profile and view, add, edit, and delete sites, organization units, departments, and roles. By default, this grid shows only active employees.
View Employees Grid	To view the list of employees that the user has access to.
View Employee Profile — General	To view the profile of the employees that the user has access to.
Manage Employee Profile — General	To view, add, edit, and delete the profile for employees that the user has access to.

Table continues…

Name	Description
View Employee Profile — Recording Settings	To view recording settings of employees that the user has access to.
Manage Employee Profile — Recording Settings	To view, add, edit, and delete recording settings of employees that the user has access to.
View Employee Profile — Access	To view the groups and organization units that an employee belongs and has access to. The user can view employee access of only those employees that the user has access to.
Manage Employee Profile — Access	To view, add, edit, and delete the groups and organization units that an employee belongs and has access to. The user can manage employee access of only those employees that the user has access to.
View Employee Profile — Privileges	To view the privileges of employees that the user has access to.
Manage Employee Profile — Privileges	To view, add, edit, and delete the privileges of employees that the user has access to.
View Employee Profile — Report Privileges	To view the report privileges of employees that the user has access to.
Manage Employee Profile — Report Privileges	To view, add, edit, and delete the report privileges of employees that the user has access to.
Bulk Administer Employees	To edit in bulk the profile, privileges, and report privileges of employees that the user has access to. A user with the App User permission enabled at the Profile page can only see the list of employees that the user has access to within his role hierarchy.
Import Employee Profiles	To import the list of employees through an Excel spreadsheet.
Manage Recording Targets	To define recording settings based on stations and not agents. The stations can be based on extension, position ID, account name, SIP URI, and dummy port for extension based recording. This feature is suitable for a free seating environment where agents take calls on different extensions.
Manage Password Policy	To set system-level password policy rules for users and their login credentials.
Manage LDAP	To import employee data from active directory. The user can configure ADS settings to synchronize user data each time the user signs in. The user can also manually upload employee information using an Excel spreadsheet.
View Storage Manager	To view storage manager settings of call center data across multiple physical locations or remotely by using direct attached storage (DAS), network attached storage (NAS), or storage area networks (SAN).
Manage Storage Manager	To archive, copy, delete, move, or purge voice, screen, speech indexed files and associated metadata XML files for interactions

Table continues…

Name	Description
	such as interaction start time and interaction status. The user can do these functions remotely or across multiple physical locations by using direct attached storage (DAS), network attached storage (NAS), or storage area networks (SAN). Users can also define the storage drives and locations and define storage retention rules.
Manage Recording Rules	To view, add, edit, and delete recording rules for employees that the user has access to.
Manage General Settings	To view and edit time zone, language, consent-based recording, and screen capture settings for employees that the user has access to.
Manage Groups	To view, add, edit, and delete the groups for the employees that the user has access to.
Manage Queues	To do the following: • View, add, edit, and delete queues. • Associate organization units to a queue. • Configure thresholds for business rules such as AHT, number of holds, and hold duration.
Manage Recording Type Configurations	To define recording settings for VDNs and Hunt Groups.

Employee access overview

Based on different operations within an organization, administrators might want to control employee association with different groups. Use employee access to:

- Define queue access to employees. By default, every employee gains access to all the queues in the system. Use this option to restrict users from accessing queues that you do not want them to be a part of.
- Define group access to employees. By default, every employee gains access to all the groups in the system. Use this option to provide users access to specific groups only.
- Restrict an employee’s access to selected groups by using the group-level privileges.
- Associate multiple organization units to an employee to track interaction recordings, filter search results, and generate reports based on the organization unit that an employee belongs to.

Queue access to employees

By default, in Avaya Workforce Optimization Select, access is available to all queues created in the application. You can use the Queue Access feature to restrict interactions and the associated transaction data access to specific queues. For providing employees access to data of specific queues, you can use the Selected Queues option and move the desired queues from the Available Queues to the Assigned Queues section.

Groups an employee belongs to

Avaya Workforce Optimization Select automatically creates a virtual group named after the reporting manager. Every employee automatically belongs to the virtual group that the employee reports to. These groups are not visible in the application. Administrators can also manually associate employees to other groups and restrict an employee's access to selected groups by using the group-level privileges.

Groups an employee has access to

When an employee has access to a group, the employee can access the data of employees within that group. An employee also gains access to the data of employees belonging to all the groups within the role hierarchy. For example, a supervisor reports to a manager who in turn reports to a director. In this scenario, the director has access to the interactions of employees belonging to his group, the manager group, and the supervisor group.

Providing employee access

Procedure

1. Click **Administration** > **Employees** > **Add Employee**.
2. On the Profile page, type the appropriate information in the fields.
3. Click **Save**.

   The system populates the navigation pane.
4. Click **Employee Access**.

   The Employee Access page displays the Edit Employee Access page.
5. To provide employee access based on the privileges, select the options in the following sections:
   - Queues Access to
   - Group Access to
   - Groups Belong to
   - Organization Units
6. To save the current settings, click the ✔ Save icon.

Edit Employee Access field descriptions

Queues Access to

Name	Description
All	The option to allow an employee to have access to all the queues available in the application.

Table continues…

Name	Description
Selected Queues	The option that allows you to assign specific queues to an employee.. The options are: • Available Queues: A list of all the queues available in the application. • Assigned Queues: The queues assigned to a particular employee. An employee can access interaction data pertaining to only those queues assigned to the employee.
Available Queue(s)	The queues available in the application to which an employee can have access to.
Assigned Queue(s)	The queues assigned to a particular employee.

Groups Access to

Name	Description
Groups Access to	The group to which an employee has access to. The employee automatically gains access to everyone within his or her hierarchy. For example, in the Supervisor > Manager > Director role hierarchy, the Director can access the interactions of employees belonging to his own group, the Manager group, and the Supervisor group as well. You can also provide access to other groups using the **Groups Access to** option.
Available Group(s)	The groups that are not assigned to the selected employee.
Assigned Group(s)	The groups that are assigned to the selected employee.

Groups Belong to

Name	Description
Groups Belong to	The group to which an employee belongs.
Available Group(s)	The available custom groups.
Assigned Group(s)	The groups that an employee belongs to. You can assign or remove groups as required.

Organization Units

Name	Description
Organization Units	The organization unit that represents a functional or business process within an organization.
Available Organization Unit(s)	The available organization units.
Assigned Organization Unit(s)	The organization unit that an employee is assigned to. You can assign or remove organization units as required.

DP OU

Name	Description
DP OU Type	The OU type created post installation. This is a custom field. The name of the OU type created post installation to partition and secure data across groups appears as the name of this field.
Available Organization Unit(s)	The available organization units.
Assigned Organization Unit(s)	The organization unit that an employee is assigned to. You can assign or remove organization units as required.

Organization Units

Name	Description
DP OU Type	The OU type created post installation. The name of the OU type created post installation to partition and secure data across groups appears as the name of this field.
Available Organization Unit(s)	The available organization units.
Assigned Organization Unit(s)	The organization unit that an employee is assigned to. You can assign or remove organization units as required.

Report privileges overview

Administrators can use report privileges to define the reports that a user can or cannot access.

Report privileges are grouped as:

- Interactions: To generate reports for Interaction Details, Interaction Summary, Interaction Trend, and AHT Trend.
- Evaluations: To generate reports for Evaluations Summary, Evaluations Details, and Evaluations Trend.
- Coach: To generate Coaching Summary report.
- Learn: To generate Course & Quiz Summary report.
- Administration: To generate reports for Employee Recording Configuration, User Access, Web Usage Audit.

Assigning report privileges

Before you begin

On the Profile page, enable **App User**.

Procedure

1. Click **Administration** > **Employees** > **Add Employee**.
2. On the Profile page, type the appropriate information in the fields.
3. Click **Save**.

   The system populates the navigation pane.
4. Click **Report Privileges**.

   The system displays the Edit Report Privileges page.
5. Do any of the following depending on the privileges that you want to assign:
   - To enable all the report privileges at one go, select the **All Report Privileges** check box.
   - To select all the report privileges of any module, select the respective module check boxes.
   - To select the report privileges that you want to enable or disable for a module, click the module and then select the respective fields check boxes. For example: To assign the privilege for managing interactions playback, select the **Interactions** checkbox, click **Interactions** and select the **Interactions Details**.
6. To save the current settings, click the ✓ Save icon.

Edit Report Privileges field descriptions

Interactions

Name	Description
Interactions Details	For the user to generate and schedule the Interactions Details report.
Interactions Summary	For the user to generate and schedule the Interactions Summary report.
Interactions Trend	For the user to generate and schedule the Interactions Trend report.
AHT Trend	For the user to generate and schedule the AHT Trend report.

Evaluations

Name	Description
Evaluations Summary	For the user to generate and schedule the Evaluations Summary report.
Evaluations Details	For the user to generate and schedule the Evaluations Details report.
Evaluations Trend	For the user to generate and schedule the Evaluations Trend report.

Coach

Name	Description
Coaching Summary	For the user to generate and schedule the Coaching Summary report.

Learn

Name	Description
Course & Quiz Summary	For the user to generate and schedule the Course & Quiz Summary report.

Administration

Name	Description
Employee Recording Configuration	For the user to generate and schedule the Employee Recording Configuration report.
User Access	For the user to generate and schedule the User Access report.
Web Usage Audit	For the user to generate and schedule the Web Usage Audit report.

Importing employees

Before you begin

Ensure to create groups, sites, departments, and roles before you import employees.

Procedure

1. Click **Administration** > **Employees**.
2. Click **Import Employees**.
3. On the Bulk Import pop-up, click **Download** to download the Excel spreadsheet to your computer.
4. Enter the details in the Excel spreadsheet.
5. To select the Excel spreadsheet from your computer, click **Choose File**.
6. To import the Excel spreadsheet, click **Import**.

Import employees field descriptions

The table lists all the fields in the Excel spreadsheet that you can use to import employee details.

Name	Description
S.No	The serial number of records to be imported.
Employee code	The code of the employee. This field is mandatory and has to be unique.
First Name	The first name of the employee. This field is mandatory and is a default field.
Last name	The last name of the employee. This field is mandatory and is a default field.
Alias	The alias name of the employee. This field is mandatory and has to be unique.

Table continues…

Name	Description
Email	The email address of the employee. This field is mandatory.
Hire Date (mm/dd/yyyy)	The date of hire of the employee. This field is mandatory.
Site	The name of the site that the employee is associated to. This field is mandatory.
Department	The name of the department that the employee belongs to. This field is mandatory.
Reporting to	The name of the supervisor that the employee reports to. This field is a default field.
User Name	The login ID or network ID of the employee. This field is mandatory and is a default field. The field must be unique.
Agent ID	The agent ID of the employee that is used for agent based recording. This value populates the **Agent ID** field in the Recording Rules page. This field is a default field.
Extension	The VOIP phone extension of the employee. This value populates the **Extension** field in the Recording Rules page. ID types other than agent ID and Extension also get mapped to Extension when you import employees. You must also enter account name, port, and position ID against Extension in the excel sheet.
Role	The designation of the employee. This field is mandatory and is a default field.
Custom Group	The name of the custom group that the employee belongs to.
Employee For	The import action for each employee. The options are: • I: Create a new record for that employee. • U: Update the record for an existing employee. • X: Ignores update or insert of any record for employees. This field is mandatory.
DP OU	The partition of the organizational unit that the employee belongs to. For example, **Business**, **Client**, **Customer**, or **Line of Business**. This field is available only if you are using a data partitioned environment.
Validate User	The option to validate an employee for the username with the name available in the LDAP server. The options are: • Yes: Authenticates the employee against the LDAP server. • No: Does not validate the employee.
AD Domain name	This option is available when you select the Yes option for **Validate User with AD**. If the AD validation fails, the system displays a cross mark

Table continues…

Name	Description
	against the user or fail the record while importing. You can also filter employee who are AD validated and fail validation.
Authentication Method	The option to configure the authentication method for users. The options are: • LDAP based: The option configure Lightweight Directory Access Protocol (LDAP) as the authentication method for users. • Local: The option to configure Local as the authentication method for users. This option prompts users to enter their login credentials to access the application. • Blended: The option to configure authentication method for users based on the requirement. If this option is selected, the Authentication method can be either LDAP Based or Local option for configuring the employee profile for each employee.

Group-level privileges overview

Using the group-level privileges feature, you can define employee access to feature and report privileges at a group level. By default, if you have already defined some privileges for the employee, then the employee must have the same privileges for all the groups to which the employee has access to. The best practice is to assign privileges to a role, so that employees belonging to that role automatically inherit the privileges. However, you also have the flexibility to assign or modify privileges for a specific set of employees based on a group by group basis. Note that the group privileges can only be same or less than the overall privileges defined.

If a user is modifying the privileges at an employee level while privileges is already customized at few groups, the group privileges also resets to employee privileges.

Group-level privileges are module specific. Each permission defines one or more actions that a user can perform for a given module.

You can either select the group-level privileges based on individual modules or you can select all the modules at one go. Group-level privileges are categorized in the modules as follows:

- **Interactions**
    - Manage Interactions Playback
    - Manage Interaction Views
    - Manage Interactions Tags
    - View Comments
    - Manage Comments
    - Download Interactions
    - Email Interactions
    - Real Time Recording Controls - Start Recording

  - Real Time Recording Controls - Pause/Resume Recording
  - Real Time Recording Controls - Stop Recording
  - Real Time Recording Controls - Cancel Recording
- **Live Monitoring**
  - View Live Monitoring
  - Manage Live Monitoring Views
  - Manage Feedback
  - Random Monitoring
  - Monitor next Interaction of the selected agent(s)
- **Evaluate**
  - View My Assignments
  - Decline Assignments
  - Create & Edit Evaluations
  - Delete my Evaluation(s) only
  - Delete Evaluation(s)
  - View Evaluation(s)
  - Manage Evaluation Views
  - View Adhoc Evaluations
  - Manage Adhoc Evaluation Views
  - View Appeals
  - Create & Edit Calibration(s)
  - Delete Calibrations
  - View Employee Coverage
  - View QA Coverage
  - Create & Edit Plan(s)
  - Delete Plan(s)
  - Distribution Pool - Self Assignment
  - Distribution Pool - Manage
  - Add & Edit Form(s)
  - Delete Form(s)
  - Manage Response Sets
  - Manage Evaluation Types
  - View Appeals Workflow
  - Manage Appeals Workflow

- **Coach**
  - Create & Edit Coaching Assignments
  - Delete Coaching Assignments
  - Manage Coaching Views
  - Manage My Assignment
  - Create & Edit Coaching Plans
  - Delete Coaching Plans
  - Manage Parameter
- **Learn**
  - My Assignment
  - Manage Team Assignments
  - Manage Team Assignment Views
  - Manage Library
- **Analyze**
  - View Measure
  - View Metrics
  - Manage Metrics
  - View Score Cards
  - Manage Score Cards
  - Manage Metric Views
  - Manage Custom Metric Import
  - Manage Custom Metric Data Entry
- **Reports & Dashboards**
  - Manage reports results
  - Manage reports settings
  - Manage reports schedule
  - Allow changing the landing page
  - Create & Edit dashboard
- **Administration**
  - Manage Organization
  - View Employees Grid
  - View Employee Profile - General
  - Manage Employee Profile - General
  - View Employee Profile - Recording Settings

- Manage Employee Profile - Recording Settings
- View Employee Profile - Access
- Manage Employee Profile - Access
- View Employee Profile - Privileges
- Manage Employee Profile - Privileges
- View Employee Profile - Report Privileges
- Manage Employee Profile - Report Privileges
- Bulk Administer Employees
- Import Employee Profiles
- Manage Password Policy
- Manage LDAP
- View Storage Manager
- Manage Storage Manager
- Manage Recording Rules
- Manage General Settings
- Manage Groups
- Manage Queues
- Manage Recording Targets

Caveats

You cannot define group privileges beyond the ones that are defined at the employee level. The Live Monitoring, Interactions, and the Coach modules do not get displayed in the Manage Group Access privilege page if the following privileges are not originally defined for the user:

- **Manage Interaction playback**
- **View Live Monitoring**
- **Coaching Permissions**

Managing group level privileges

About this task

Use this procedure to manage employee privileges on a group-by-group basis. The group privileges can be same or less than the overall privileges defined.

Procedure

1. Click **Administration** > **Employees**.

   The system displays the list of employees that the app administrator has access to.

2. On the Employees page, select the row for the respective employee and click on the row.

3. Click **Employee Access**.
4. Click **Manage Group Privileges**.
5. On the Manage Group Privileges page, do the following:
    a. Select the group to which you want to assign the group privileges.
    b. Click the check boxes of the modules for which you want to provide group privileges.
    c. **(Optional)** Clear the check boxes of the modules for which you do not want to provide group privileges.
6. Click **Apply**.

    The system displays the following message: `Privileges for the selected group(s) have been saved successfully.`

Bulk Actions overview

Using the Bulk Actions feature, you can administer selected employees in bulk. To use this feature, ensure that you have the Bulk Administer Employees privilege enabled in the Privileges section. However, the permission to access employees for bulk administering is based on your role:

- Employees with the App User permission can access only those employees who are within the role hierarchy.
- Employees with the App Admin permission can access all the employees in the application.

Benefits:

- Use the Profile option to bulk administer employee profile and provide access definitions based on existing fields.
- Use the Privileges option to assign or remove one or more feature privileges from employees in bulk. You can also select the feature privileges of all the modules for assigning or removing employees in bulk. If required, you can also select only specific modules or privileges of specific modules for bulk action.

    Note:

    If you select multiple users, their current privileges do not get displayed. Any options that you select during bulk action overrides the current privileges for the selected employees.

- Use the Report Privileges option to assign or remove one or more report feature privileges from employees in bulk. You can also select the report feature privileges of all the modules for assigning or removing employees in bulk. If required, you can select only specific modules or report privileges of specific modules for bulk action.
- Use the Recording settings option for monitoring and recording interactions for employees in bulk. You can also select screen recording options for a group of selected employees. You can disable recording for all the employees that are selected for bulk actions.

Performing bulk actions

Procedure

1. Click **Administration** > **Employees**.
2. Select the list of employees that you want to perform bulk actions for.

   A user with the App User permission selected at the Profile page, can only see those employees that the user has access to within his role hierarchy.
3. In the **Bulk Actions** field, click one of the following:
   - **Profile**: Enter a **Field** and **Value**.
   - **Privileges**: Select the appropriate employee privileges.
   - **Report Privileges**: Select the appropriate report privileges.
   - **Recording Settings**: Select the appropriate recording settings.
4. Click **Save & Close**.

Bulk actions field descriptions

Bulk Actions- Employee Profiles

Name	Description
Field	The list of fields based on which you can create employee profiles. The options are: • **Department**: The option to choose the department that the employee must belong to. • **Employee Status**: The option to select the status of the employee. The options are Active and Inactive. • **Groups Access to**: The option to define groups that an employee can have access to. • **Groups Belong to**: The option to define groups that an employee can belong to. • **App User**: The option to give the employee access to the application. • **Hire Date**: The date when the employee was hired in the mm/dd/yyyy format. • **Landing Page**: The option for the App User to set the default landing page of an employee. The options are Home and Dashboard. • **Language**: The language selected for the employee. The options are English (US), German (Germany), Spanish, French, French (Canada),

Table continues…

Name	Description
	Italian, Korean, Japanese (Japan), Portuguese (Brazil), Russian, Simplified Chinese, and Traditional Chinese. The default language is English (US). • **Organization Unit**: The option to choose the organization unit that the employee is mapped to. • **Role**: The option to select the designation of the employee in the organization. • **Site**: The option to choose the name of the site that the employee is associated to. • **Reporting to**: The option to select the name of the manager that the employee reports to. • **Time Zone**: The option to select the time zone of the employee. However, the time zone selected while configuring the general settings is the default time zone in the Sites and the Profile pages.
Value	Select a value depending on the Field you selected.

Bulk Actions- Employee Privileges

Name	Description
Assign	The option to assign one or more features privileges to employees in bulk.
Remove	The option to remove one or more feature privileges to employees in bulk.
All Feature Privileges	The option to select the feature privileges of all the modules for assigning or removing employees in bulk. You can also select only specific modules or privileges of specific modules for bulk action.

Bulk Actions- Employee Report Privileges

Name	Description
Assign	The option to assign one or more report privileges to employees in bulk.
Remove	The option to remove one or more report privileges to employees in bulk.
All Report Privileges	The option to select the report privileges of all the modules for assigning or removing employees in bulk. You can also select only specific modules or report privileges of specific modules for bulk action.

Bulk Actions- Recording Settings

Name	Description
Selected Employees	
Name	The name of the employee.
ID Type	The options are: • Agent ID: The unique peripheral ID of the employee. • Extension: The VoIP phone extension of the employee. In a free seating environment, the Extension can be any free and unique extension number. • Port: The dummy recording stations used to record calls in Avaya Session Border Controller for Enterprise deployments for calls that are routed through IVRs. You must configure this port number range in SIP adapter, where Avaya Session Border Controller for Enterprise is enabled. • Position ID: The ID which the agent uses to log in to the phone. This field is available for Avaya Communication Server 1000 deployments.
ID Value	The option to enter the relevant values based on the selected ID Type.
Channel	The channel for recording. The options are: • Voice • Email • Chat **Note:** SMS is also supported in an Oceana™ deployment configuration.
Contact Instance(s)	The number of simultaneous transactions that can be handled by a station or extension. For example, a user configures two extensions: 1001 and 1002. The user must enter 2 (numeric value) in the contact instances field, then each station can at any instance handle maximum two transactions. The default value for this field is 1.
Machine Name	The name of the machine that the agent is using for interactions.
Machine IP	The IP address of the machine that the agent is using for interactions.

Table continues…

Name	Description
Device ID	The MAC (media access control) address of the physical device or phone that the employee uses.
Partition Name	The unique partition name. The Partition Name can be any unique name used to differentiate the call, if an employee takes a call from same extension, device, and contact instance.
Alternate ID	The alternate ID that is used to configure recording settings when a user wants to add additional information of the configured agent ID or extension. This information is used in future reference.
Phone IP	The IP address of the phone that the agent is using for interactions.
Terminal Number	The terminal number that is used to configure recording settings when a user wants to add additional information of the configured agent ID or extension. This information is used in future reference.
Recording Settings	
Interaction Recording Options	The option to enable recording rules for interactions.
Interaction Direction	The option to select the interaction direction. The options are: • **Inbound** • **Outbound** • **Bi-directional**
Recording General Rules	
Monitor and Record All Interactions	The option to enable 100% recording of interactions. Using this option, a user can pause, resume, or cancel a recording but cannot start a recording.
Do Not Record Interactions	The option to specify that you do not want to record interactions.
Monitor and Record Complete Interactions On demand	The option to enable monitoring and recording of interactions on demand. On demand recording is initiated when a user selects the Record Call Now option during live monitoring. Using this option, a user can start, pause, resume, and cancel a recording.

Table continues…

Name	Description
__ interactions to be monitored and recorded randomly	The option to specify the number of interactions to be monitored and recorded. • If the interaction is already being recorded, a user can only pause, resume, stop, and cancel a recording. The user cannot start a recording. • If the interaction is not recorded, a user can start, pause, resume, and cancel a recording.
Monitor and Record Segment of Interactions On demand	The option to enable monitoring and recording segments of interactions on demand. You can initiate on demand recording and trigger APIs to specify start, cancel, pause, resume, and stop recording for specific segments within an interaction. Using this option, a user can do all of the following recording options: • Start • Pause • Resume • Stop • Cancel
Shift based	The option to record interactions according to employee shift. This option is enabled if the employee is part of a recording rule that has shift based enabled.
__ Percent of interactions to be monitored and recorded	The option to specify the percentage of interactions to be recorded. The Avaya Workforce Optimization Select application records all the interactions, calculates the specified percentage, and purges the extra interactions at the end of the calendar day. However, the Avaya Workforce Optimization Select application stores the metadata of the interactions even if the interaction is not recorded.
Screen Recording Options	
Screen Recording Options	The option to enable screen recording for interactions.
Record Screens for All Interactions	The option to enable 100% screen recording of all interactions.
Do Not Record Screens	The option to specify that you do not want to record interaction screens.

Table continues…

Name	Description
Screen Recording Interval	The option to select the screen capture recording interval in seconds.
Screen Recording Quality	The option to select the screen recording quality in percentage.

Icon	Name	Description
⊕	Add	To add multiple recording settings for individual user.
⊗	Remove	To remove individual recording settings for each user.

Button Name	Description
Disable Recording	The option to disable recording for all the employees that are selected for bulk actions.

Chapter 7: Managing queues

Queues overview

In Avaya Workforce Optimization Select administrators can configure following support channels for a queue for all the deployment configurations:

- Voice
- Email
- Chat

Note:

SMS is also supported in an Oceana™ deployment configuration.

Administrators can use queues to:

- Activate or deactivate a support channel for a queue.
- Create multiple queues for each support channel.
- Map organization units to a support channel to define an additional level of tracking.
- Configure message threshold for a queue to track mission critical information about the conditions within the contact center.
- Set threshold values for business rules, such as average handle time, number of holds, and hold duration. Alerts are triggered when the employee crosses the threshold value.

Supervisors and managers can use queues to:

- Monitor and track interactions based on queues.
- Run searches based on queues.
- Generate reports that provide insight into the quality and performance of employees.

Adding queues

Before you begin

Ensure you configure the appropriate skill ID parameter for the respective Avaya Workforce Optimization Select deployment configurations. For deployment on IP Office Contact Center, the configuration is a manual process.

Procedure

1. Click **Administration** > **Queues**.
2. Click **Add Queue**.
3. On the Add New Queue page, enter the appropriate information in the fields.
4. Enter threshold values for business rules.
5. Click **Save & Close**.

Add New Queue field descriptions

Add New Queue

Name	Description
Name	The name of the queue. When a skill call happens, a queue is automatically created and the skill ID or the skill group ID populates as the Queue name. This field is a default field.
Alias	The alias name of the queue. This field is a default field.
Active	The option to select if the queue is an active queue.
Description	The description of the queue. This field is a default field.
Organization Units	The organization unit associated with the queue. This field is a default field.
Queue ID	A unique ID of the queue. Avaya Workforce Optimization Select automatically assigns a queue ID when a queue is created in real time. This field is a default field.
Channel	The channel for a queue. The options are: • Voice • Email • Chat • SMS: Available in an Oceana™ deployment configuration. • Social: Available in an Oceana™ deployment configuration. • Generic: Available in an Oceana™ deployment configuration. Apart from these options, the administrator can also create custom interaction types in General settings and associate them to a queue.

Table continues…

Name	Description
	This field is a default field.
Queue Type	The option to select an additional custom fields for a queue.

Thresholds

Name	Description
My AHT exceeded by Queue	The threshold value that you set for the Average Handle Time (AHT) for an interaction in minutes. A notification to employees triggers when the employees exceed the AHT.
Number of holds placed by me in the Queue	The threshold value that you set for the number of holds that an employee places during an interaction. A notification to employees triggers when the employees exceed the number of holds.
My hold duration by Queue	The threshold value that you set for the hold duration for an interaction. A notification to employees triggers when the employees exceed the hold duration.
AHT exceeded by my team in Queue	The threshold value that you set for exceeding the Average Handle Time (AHT) for an interaction in minutes. A notification to the supervisor triggers when the supervisor’s team exceeds the AHT.
Number of Holds by Queue for my team	The threshold value that you set for the number of holds an employee places during an interaction. A notification to the supervisor triggers when the supervisor’s team exceeds the number of holds.
Hold duration by Queue for my team	The threshold value that you set for the hold duration for an interaction. A notification to the supervisor triggers when the supervisor’s team exceeds the hold duration.

Chapter 8: Managing settings

Settings overview

Using the Settings page in Avaya Workforce Optimization Select, you can manage the following:

- Storage Manager Rules to store and manage call center data across multiple physical locations .
- Recording Rules to define the recording settings that you must apply to selected interactions.
- Recording Targets to define recording settings based on stations and not on agents.
- Recording Filters to define recording settings for Vector Directory Numbers (VDNs) and Hunt Groups.
- LDAP Settings to synchronize user data every time an employee signs in to the application.
- Password Policy to define a set of rules that enhance system security by encouraging employees to use strong passwords.
- General Settings to configure time zone, language, week definition for defining a working week in an organization, record NORTP calls during network issues, default number of rows to display in the grids of the different modules, reason code on clicking a recording control, recording attributes, screen recording properties, interaction types, and authentication method.

For more information on the different features on the Settings page, see:

- Storage Manager overview on page 68
- Recording rules overview on page 84
- Recording Targets overview on page 88
- Recording Filters overview on page 91
- Authentication Method overview on page 79
- Password policy on page 96
- General Settings overview on page 80

Storage Manager overview

Using Storage Manager, administrators can store and manage call center data across multiple physical locations. Avaya Workforce Optimization Select supports data storage using direct attached storage (DAS), network attached storage (NAS), storage area networks (SAN), and content address storage (CAS). Depending on the recording rule definition, Storage Manager either retains or purges the interactions after the calendar day.

Administrators can use storage management capabilities to perform the following tasks:

- Archive, copy, move, compress, purge or delete voice, screens, and associated metadata XML files for interactions.
- Manage storage devices to define storage location and other attributes.
- Define storage retention for interactions.
- Create storage rules for interactions based on several filters.
- Track and retrieve archived interactions for playback or analysis.

Storage rules

Administrators can define storage rules to meet specific business requirements for data storage. You can create separate rules for archiving, compressing, moving, copying, and purging of data. Avaya Workforce Optimization Select checks each interaction against all the rules and tags the interaction with the rule that applies to the interaction. If an interaction meets the condition of one or more storage rules, the storage manager processes the interaction based on the priority and action you define for a storage rule. If an interaction does not meet the condition of a rule, Avaya Workforce Optimization Select bypasses the interaction and checks for subsequent rules.

If the voice output format you specify for a rule does not match with the format of the interaction, storage manager processes the rule with the available options instead of dropping the interaction. For example, if the voice output format is MP4 that contains audio and video and the interaction contains only audio with no screens, then the storage manager exports the interaction in M4a format. Similarly, if the voice output format is M4a that contains only audio and the interaction contains both audio and screens, then the storage manager exports the interaction in MP4 format.

Related links

Storage management process on page 69
How storage rules work on page 70
Creating and assigning storage manager rules on page 71
Storage Manager Rules field descriptions on page 72

Storage management process

The following aspects of how Storage Manager works is relevant to administrators:

- After the administrator configures storage rules, the stored procedure picks the interactions that are applicable to the rules. Avaya Workforce Optimization Select checks each interaction against all the rules and tags the interaction with the rule that applies to the interaction. Storage Manager then starts processing interactions based on the rule priority defined earlier.
- When administrators create a rule, interactions are fetched into the storage_rules_tag and calls table. When you modify a rule, an entry is inserted into the storage_rules_queue table with the status as New. The status changes to Complete when the previously fetched interactions get truncated and calls related to the modified rule get fetched into the

storage_rules_tag and calls table. Similarly, when you delete a rule, all interaction tags in the database are removed and the Storage Manager stops processing interactions for that rule.

- A database entry is made for all the interactions for which an action is performed. The action might be: archive, compress, copy, move, purge or delete.
- Administrators can also configure single or multiple Storage Manager instances and define rules for the Storage Manager to perform a specific type of action or a combination of actions separated by commas.
- In the case of multiple Storage Manager instances, Avaya Workforce Optimization Select provides a load balancing mechanism that distributes the load equally among all instances. If any Storage Manager service fails, interactions that are yet to be processed by the failed service get distributed among the remaining active Storage Manager services. Interaction distribution also happens when processing by a Storage Manager service takes longer.
- When administrators give higher priority to the delete operation than a copy or archive operation, Storage Manager performs the delete operation first. Interactions that are deleted are unavailable later to archive or copy.

Related links

Storage Manager overview on page 68

How storage rules work

When an administrator creates and saves a rule, the rules engine validates whether the rule is compatible with the existing rules in the system. If the validation fails, the rules engine specifies the list of rules that are conflicting with the new rule. The administrator must either modify the current rule or an existing rule. Administrators cannot create a rule if it conflicts with actions such as archive, move, copy, and purge of another existing rule.

Use storage manager rules to specify how to manage the storage of your saved data, voice and screens. You can:

- Specify the rule name, priority, and the date when the rule must get executed.
- Define interaction selection criteria for a rule. You can filter interactions based on various parameters.
- Select an action type to specify whether interactions must be archived, compressed, moved, copied, purged or deleted.
- Specify the source from where interactions must be extracted and the destination where interactions must be archived.

For example, you might create a rule whose action is Purge and priority High for a set of interactions. If there is an existing rule for the same set of interactions to copy, move, or archive, the rules engine will fail to create the new rule. Further, your business might require that you retain interactions of a particular queue for 40 days. However, if interactions from the same queue are evaluated, you might want to retain it for 120 days. To implement the requirement, create the following two rules.

The first rule must have the following configurations:

- Rule Name: Purge Evaluations
- Priority: 100
- Older than: 120 days
- Interaction Selection Criteria: Evaluated interactions
- Action: Purge

The second rule must have the following configurations:

- Rule Name: Purge Interactions
- Priority: 102
- Older than: 40 days
- Interaction Selection Criteria: Name of the queue whose interactions you wish to purge
- Action: Purge

When these rules are activated, all evaluated interactions will have two entries in the storage_rules_tags table.

- The first entry will have Rule 1 as priority 100 and activation date equal to 120 days past the interaction start time.
- The second entry will have Rule 2 with priority 102 and activation date as 40 days past the interaction start time.
- Non-evaluated interactions will have only one entry with Rule 2.

Related links

Storage Manager overview on page 68

Creating and assigning storage manager rules

About this task

Use this procedure to create storage manager rules to meet specific business requirements for data storage of different interactions. Note that for interactions that you import manually, you must encrypt these interactions before creating a storage rule.

Procedure

1. Click **Administration** > **Settings** > **Storage Manager Rules**.
2. Click **Add Storage Rule**.
3. On the Add New Storage Manager Rule page, enter the appropriate details.
4. Click one of the following:
    - **Save & Close**: To save your settings.

- **Save & Add Another**: To save the current rule and add another rule.

Avaya Workforce Optimization Select displays the storage manager pop-up.

5. In the **Assigned to Storage Manager?** column, click **No** for a specific storage manager rule.

   The **Storage Manager List** pop-up displays the details of the rule.

6. Select the check box next to the specific storage manager, and click **Save**.

   The **Storage Manager List** pop-up displays the following message: `Storage Manager has been updated successfully.`

7. To close the **Storage Manager List** pop-up, click **Cancel** .

   The status of the rule changes to **Yes** in the **Assigned to Storage Manager?** column for the specific storage manager rule.

8. **(Optional)** To unassign storage server or change the status back to **No**, click **Yes**.

Related links

Storage Manager overview on page 68

Storage Manager Rules field descriptions

General

Name	Description
Rule Name	The name of the rule. For example, Archive Rule 01. This field is the default setting.
Priority	The priority to specify the rule sequence. It is recommended to set priority for storage manager rules from 100. A rule with priority 100 runs first, priority 101 runs after the execution of priority 100, priority 102 runs after the execution of 100 and 101, and so on. This field is the default .
Active	The status of the storage manager rule .
Description	A brief description of the rule.
Rule Activation Date	The date from when the rule must be executed. The current date is set as the effective date by default. You can specify a future activation date for rule execution. You can modify the date if the rule is a new rule or a drafted rule, or for an active rule whose rule activation date is greater than the current date. However, you cannot modify the date after the rule is applied. Rule activation date is based on Company Time Zone, which is UTC.
Lean Period	A specified time period for processing interactions. For example, if you configure a rule to compress calls and specify a period for that rule, then

Table continues…

Name	Description
	the compression happens only during that time. For the rest of the time, the application fetches interactions, but the actions take place only during the lean period. When you change the lean period, the change is effective immediately. Lean period is based on Company Time Zone, which is UTC.

Interaction Selection criteria

Name	Description
Interaction Direction	The interaction direction that the rule must check before storing. The options are: • **Inbound** • **Outbound** • **Bi-directional**
Field	The option to select the interaction based on time. The options are: • **Date Range**: The From/To date range to select interactions within the specified days. • **Last Number of Days** : The value for interactions from the more recent number of days. For example, enter 7 to select interactions within the past seven days. • **Older than**: An option to act on interactions older than the specified number of days from the **Starts From** option till the current date. For example, to move interactions older than 7 days from August 1st 2018, enter 7 in the **Older than** option and select August 1st in the **Starts From** option. The application moves interactions effectively from July 24th till the current date, which keeps incrementing on a daily basis. **Note:** Storage rule does not allow the storage manager to act on the interactions that take place on the current day.
Field	The option to create storage rules for interactions based of the following options: • Audio Codec: To search for interactions that are compressed using the selected audio codec. • Called Party: To search for interactions by the extension number or email ID of the called party.

Table continues…

Name	Description
	• Calling Party: To search for interactions by the extension number or email ID of the calling party. • Commented: To search for interactions that are commented. • Groups: To select interactions of employees who belong to the specified group. • Department: To search for interactions of employees who belong to the specified department • Duration: To search for interactions by the duration specified in the hh:mm:ss format. • Employee: To search for interactions based on the employees that you have access to. • Evaluated: To search for evaluated interactions. • Flagged for QA: To search for interactions that are flagged for QA. • Hold Duration: To search for interactions based on the hold duration. • Hunt Group: To search for interactions based on the grouping of extensions handled by agents for interactions. • Interaction Comments: To search for interactions based on specific comments provided by employees. • Interaction Tags: To search for interactions based on the specific tags used for association. For example, to delete an adhoc interaction from the database, you must select Delete_Interaction. • No of holds: To search for interactions with the specified number of holds. • No of Transfers: To search for interactions with the specified number of transfers. • Organization Unit: To search for interactions based on the name of the organizational unit. • Queue: To search for interactions by the queue that the interaction is associated with. • Screen Captures: To search for interactions with screens. • Site: To search for the interactions of employees belonging to the specified site.

Table continues…

Name	Description
	• Source Type: To search for interaction based on the source of the interaction. • Status: To search for interaction based on the status of the interaction • Reporting to: To search for interactions based on the name of the supervisor. • Tagged: To search for tagged interactions. • Tenure (in weeks): To search for interactions based on the tenure of the employee in weeks. • Transfer type: To search for interactions based on the type of transfer. For example; cold transfer, warm transfer, or conference. • Recorder Server IP: To search for interactions that are recorded and stored on the specified recorder servers. • Var 1–10: To search for interactions based on custom variables defined for your business. • Interaction ended by: To search for interactions based on the party who ended the interaction. An interaction can be ended by either an agent or a customer.
Operator	The Operator relative to the field selected. The options are: • Equals To • Between • Number of Days
Value	The numerical value or value ranges selected. If Between is selected as an operator in the field, enter a numerical value with respect to the attribute and operator selected. For example, for the attribute Interaction Duration (in secs), with the operator selected as Between , entering 120 and 300 in the **Value** text fields executes the action type selected like archive, compress, move, copy, purge/ delete calls between 120 and 300 seconds.

Action

Name	Description
Interaction Type	The type of interaction for storage management. The options are: • Voice: If you select this option, only voice and screen options are available. • Non Voice: If you select this option, only the screen option is available . • Email: If you select this option, only the screen option is available . • SMS: If you select this option, only the screen option is available . • Chat: If you select this option, only the screen option is available for storage management. • All: If you select this option, both the voice and screen options are available .
Action	The storage management action type for the rule. The options are: • Archive: Deletes interactions from the source, places them in the destination location, and updates the archive location details. You cannot archive an interaction that is already archived to a different location. When you select the Archive option, the voice and screen options are enabled by default and you cannot modify these options. • Compress: Compresses voice and screen files into MP4 format and audio files into raw-G729-Mono and raw-G729-Stereo format. You can specify if you want the compressed files to be encrypted and/or deleted from source. • Move: Deletes interactions from the source, moves them to the destination location, and updates the storage details of the destination. You can move interactions that are already moved to a different location. When you move an interaction, the storage address of the new location is updated in the database to allow interaction playback. When you select the **Move**, the voice and screen options are enabled by default and you cannot modify these options.

Table continues…

Name	Description
	• Copy: Creates a duplicate copy of the interactions and copies them to the destination. The storage address of the source is retained in the database. • Purge/Delete: Deletes the interactions from the source location. To delete adhoc interactions from the database, create a separate storage rule using this action. If you select this option, you can select voice and screen together, or only screen. The Include XML option is disabled for this action. If you select the Voice option first, the Screen option gets automatically selected. If you select the Screen option first, then the Voice option remains unselected.
Voice Output Format	The option to specify the format in which the interactions must be archived, compressed, moved, copied or deleted. For example, if a voice file is in Raw-G729-Mono format and the user performs the Archive action by selecting the format as 'Current Format', then the voice files selected gets archived in Raw-G729-Mono format. The options are: • Current Format: This option is available when you select Archive, Move, or Copy. • m4a-AAC-mono: This option is available when you select Archive or Copy. • m4a-AAC-stereo: This option is available when you select Copy. • mp4–H.264–mono: This option is available when you select Archive or Copy. • mp4–H.264–stereo: This option is available when you select Copy. • raw-G.729–mono: This option is available when you select Compress. • raw-G.729–stereo: This option is available when you select Compress. • wav-G.729–mono: This option is available when you select Copy. • wav-G.729–stereo: This option is available when you select Copy. • wav-G.711uLaw–mono: This option is available when you select Copy.

Table continues…

Name	Description
	• wav-G.711uLaw–stereo: This option is available when you select Copy. • wav-G.711aLaw–mono: This option is available when you select Copy. • wav-G.711aLaw–stereo: This option is available when you select Copy. • wav-PCM–mono: This option is available when you select Copy. • wav-PCM–stereo: This option is available when you select Copy.
Encrypt	The option to archive, move, or compress interactions in an encrypted format.
Voice	The option to specify that voice files must be archived, compressed, moved, copied, or purged/ deleted. If only voice is available for an interaction on the disk, the interaction is converted to M4a, wav , or current format even if the selected export format is Mp4.
Screen	The option to specify that screens must be archived, compressed, moved, copied, or purged/ deleted. If only screens are found, the interaction format is converted to Mp4 or current format without any audio, even if the selected output formats are wav or m4a.
Include XML file	The option to export the interaction metadata in xml format to archive, compress, move, and copy interactions. This option is unavailable for pure action.

Storage Location

Name	Description
Source	The storage location from where the storage manager picks interactions to archive, move, copy or purge calls. The options are: • Secure • Voice

Table continues…

Name	Description
	For more information on how to create storage drives, see *Administering SysAdmin*.
Primary Destination	The primary location where interactions must be archived or stored. The options are: • Secure • Voice
Secondary Destination	The secondary location where interactions must be archived or stored after the primary destination is full or if the primary destination is disconnected.

Related links

Storage Manager overview on page 68

Authentication Method overview

In Avaya Workforce Optimization Select, you can configure one of the following authentication methods:

- LDAP based: You can configure Active Directory Services (ADS) settings to synchronize user data every time an employee signs in to the application. Using the Lightweight Directory Access Protocol (LDAP), you can track user names, passwords, and other employee information. You can map users in the LDAP database to import into the application. Currently, Avaya Workforce Optimization Select only supports non-secure connection to LDAP. LDAPS is not supported in this version of Avaya Workforce Optimization Select.

  Avaya Workforce Optimization Select uses LDAP to access information stored in an information directory. You can enhance system security by using LDAP as a shared repository to define permissions that allow only certain employees to access the LDAP database and its contents, thereby enhancing system security.
- Local: Users must log in to the application by using the respective user credentials.
- Blended: you can use a blend of Local and LDAP-based authentication methods, depending on your business requirements. For example, you can use this method for contractors or partners, who are not permanent employees, and are not part of ADS. For these users, you can configure the Local authentication method. Selecting this option enables you to configure the authentication method in the employee profile for each employee.

You can change the authentication method whenever required. The impact of changing the authentication methods is as follows:

- From LDAP based to Local: In this method, the password policy settings get applied to the users. The users must change the default password immediately after the next login.

- From Blended to LDAP based: You must match the user ID of users who are configured for the Local authentication method with the user ID configured in ADS. You can use filters to search for users associated with the Local authentication method.
- From Blended to Local: Employees with local authentication do not get impacted. However, the application applies the password policy settings for employees with LDAP-based authentication, and users must change the default password after the next login.

Configuring general settings

Procedure

1. Click **Administration** > **Settings** > **General Settings**.
2. On the General Settings page, type the appropriate details.
3. Click **Save**.

General Settings field descriptions

Important:

All the user level configurations are available when the user logs in to the application. Any changes made in the general settings get reflected only after the user logs out and logs in again.

Name	Description
Time Zone	The time zone displayed throughout the application. The time zone selected here is the default time zone in the Sites and Profile pages. The time zone you configure in General Settings is used to trigger AD schedules and evaluation plan schedules. **Note:** If you make any change to time zones for specific sites or employee profiles, the change is applicable only to those sites and employee profiles. The rest of the sites and employee profiles still display the time zone that you set in the General Settings page.
Language	The language displayed throughout the application. The default language is English (US).
Week Definition	The unique way that a working week is defined in the organization. You can define the days that comprise a week in the organization. For example, in some organizations, the working week is from

Table continues…

Name	Description
	Monday to Sunday, and in another, the working week can be Sunday to Saturday. After the week is defined, the same applies across the organization. Use this field to schedule or define evaluation plans.
Display NORTP Interactions	The option to record NORTP calls during network issues. Sometimes, the NORTP calls are available depending on the customer deployments. The options are: • No: To see only voice recorded calls. • Yes: To see voice recorded calls and NORTP calls in the Interactions. You can filter calls by interaction status and view all the NORTP calls.
Default records per page	The option to allow users to choose the number of rows to display in the grids of the respective modules. The options are: • 20 • 40 • 60 • 80 • 100 • 120 • 140 • 160 • 180 • 200 • 220 • 240
Allow users to modify the reason code on clicking a recording control	The option to allow users to add reason codes or change the default reason code when using recording control. The options are: • No: When you select this option, users cannot add or change the existing reason for a recording

Table continues…

Name	Description
	control. The user must use the default reason code. • Yes: When you select this option, users can add a reason for a recording control. The user can select an existing code or the new reason code as the default reason. **Note:** Enabling or disabling this option impacts while recording using controls from the Live Monitoring module.
Recording Attributes	The option to add recording attributes that can be associated to a recording target or station while configuring recording profiles. The selected attributes are available against each recording profile for an employee. The options are: • Device ID: The MAC (media access control) address of the physical device or phone that the employee uses. • Partition Name: The unique partition name used to differentiate the call, if an employee takes a call from same extension, device, and contact instance. • Machine Name: The name of the machine that the agent is using for interactions. • Machine IP: The IP address of the machine that the agent is using for interactions. • Alternate ID: The alternate ID that is used to configure recording settings when a user wants to add additional information of the configured agent ID or extension. This information is used in future reference. • Phone IP: The IP address of the phone that the agent is using for interactions. • Terminal Number: The terminal number that is used to configure recording settings when a user wants to add additional information of the configured agent ID or extension. This information is used in future reference. • Security Code: The password to provide security to a station by preventing other users from

Table continues…

Name	Description
	accessing functions associated with the user's station.
Screen Capture	The screen recording properties in the application. The properties defined here are the default values in the employees recording settings. The user can customize these properties in the Recording Settings page.
Interaction Types	The interaction media. The options are: • Voice • Email • Chat • SMS You can also add custom interaction type by clicking **Add New** and adding an optional description.
Authentication	
Authentication Method	The option to configure the authentication method for users. The options are: • LDAP based: To configure Lightweight Directory Access Protocol (LDAP) as the authentication method for users. • Local: To configure Local as the authentication method for users. This option prompts users to enter their login credentials to access the application. • Blended: To configure authentication method for users based on requirement. With this option, the authentication method can be LDAP Based or Local for configuring the employee profile of each employee.
Enable Trusted Authentication	The option to support trusted authentication. By default, this option is not selected. This option is unavailable in the Local authentication mode.

Configuring authentication method

Procedure

1. Click **Administration** > **Settings**.

   The application displays the Authenticate User popup.

2. In **Password**, enter your user password and click **Submit**.
3. In the navigation pane, click **General Settings**.

   The Administration module displays the General Settings page.
4. In the Authentication section, in **Authentication Method**, click one of the following:
   - **LDAP**
   - **Blended**
   - **Local**
5. **(Optional)** To support trusted authentication, select the **Enable Trusted Authentication** check box.

   This option is not available when you select the **Local** authentication method.
6. Click **Save**.

Recording rules overview

Recording rules is a global setting that administrators use to define what recording settings must be applied to selected interactions. As opposed to recording settings, you can define multiple recording rules for employees based on departments, organization units, sites, agent ID, extension, and other filters.

Rules are processed either in real time or processed offline. For rules processed in real time, the recorder checks the rule definition and accordingly records or purges the interaction. For rules that are processed offline, the storage manager checks the rule definition and records or purges the interaction.

If the same interaction is part of multiple rules, the rule with highest priority takes precedence. However, if the rule is set such that the agent level configuration overrides the recording rule, the agent level recording settings take precedence.

Use recording rules to:

- Set a priority to each rule to define a sequence.
- Specify whether an agent-level configuration must override the recording rule you define. The override option defines the relation between a recording rule and the recording setting. If the agent is part of another recording rule that does not have the override option, then the recording rule will take precedence over the agent recording settings.
- Accommodate different shift timings within the organization. The Avaya Workforce Optimization Select application records interactions of agents belonging to the shift timings specified for the recording rule. You can define only one shift per rule.
- Configure interaction and screen recording options that meet the contact center business requirements. You can specify 100% recording of all interactions and screens or random or on-demand recordings.

- Specify a certain percentage of interactions you want to record for employees. The Avaya Workforce Optimization Select application records all the interactions, calculates the specified percentage, and purges the extra interactions at the end of the calendar day. However, the Avaya Workforce Optimization Select application stores the metadata of the interactions even if the interaction is not recorded.

Creating recording rules

Procedure

1. Click **Administration** > **Settings** > **Recording Rules**.
2. Click **Create Rule**.
3. On the Create Recording Rule page, enter the appropriate information in the fields.
4. Click one of the following:
    - **Save & Close** to save the current recording rule
    - **Save & Add Another** to add another rule.

Related links

Recording Rules field descriptions on page 85

Recording Rules field descriptions

General

Name	Description
Name	The name of the recording rule.
Priority	The priority given to the rule. Rules with the lowest priority order take precedence. For example, a rule with priority 1 take precedence over a rule with priority 2. Recording rule priorities have a range limit from 1 to 99.
Active	The option to activate the rule.
Description	The description of the rule.
Agent level configurations can override this rule	The option to select if agent-level configurations must override this rule. Enabling this option makes the recording settings defined at the agent configuration level to override any rules that the employee is part of.
Allow Shift based configuration	The option that records interactions in real time at the specified time. Select **Yes** to specify a time for the shift based rule. For example, from 5:00 PM to 7:00 PM. By default, the option is set to **No** indicating a non shift based configuration.

Table continues…

Name	Description
	You can define a shift based or a non shift based rule to record or delete interactions in real time for the following options: • Agent ID • Called Party • Calling Party • Department • Extension • Organization Unit • Site However, there are rules that are processed offline or not in real time. You can define such rules for the following options: • Duration • Queue

Interactions Recording Options

Name	Description
Interaction Recording Options	The option to enable recording rules for interactions.
Interaction Direction	The option to select the interaction direction. The options are: • **Inbound** • **Outbound** • **Bi-directional**
Monitor and Record All Interactions	The option to enable 100% recording of interactions. Based on whether the rule is defined for real time or offline processing, the recorder records all interactions that meet the rule definition. The storage manager stores the recordings based on the storage rules.
__ Percent of interactions to be monitored and recorded	The option to specify the percentage of interactions to be recorded. For rules that are processed in real time, the recorder calculates the percentage for every interaction and according to the rule definition either records or purges the interaction. For example, assume you specify the percentage of interactions to be recorded as 50%, The recorder will calculate the percentage on a per interaction basis. It will record the first interaction and purge the second one. For rules that are processed offline, the storage manager calculates the percentage based on the agent login and logout time and accordingly records and purges the interactions.
Do Not Record Interactions	The option to specify that you do not want to record interactions.

Table continues…

Name	Description
	Based on whether the rule is defined for real time or offline processing, the recorder or storage manager purges all interactions that meet the rule definition.

Screen Recording Options

Name	Description
Screen Recording Options	The option to enable screen recording for interactions.
Record Screens for All Interactions	The option to enable 100% screen recording of all interactions. Based on whether the rule is defined for real time or offline processing, the recorder or storage manager records all screens that meet the rule definition.
_ Percent of interactions with screens to be recorded	The option to specify the percentage of screens to be recorded. For rules that are processed in real time, the recorder calculates the percentage for every screen and according to the rule definition either records or purges the screen. For example, assume you specify the percentage of screens to be recorded as 50%, The recorder will calculate the percentage on a per screen basis. It will record the first screen and purge the second one. For rules that are processed offline, the storage manager calculates the percentage based on the agent login and logout time and accordingly records or purges the screens.
Do Not Record Screens	The option to specify that you do not want to record interaction screens. Based on whether the rule is defined for real time or offline processing, the recorder or storage manager purges all screens that meet the rule definition.

General

Name	Description
Field	The list of fields for which you can create recording rules. The options are: • Agent ID • Called Party • Calling Party • Department • Duration • Extension • Organization Unit • Queue

Table continues…

Name	Description
	• Site
Operator	The Operator relative to the field selected. The options are: • Equals To • Between • Greater Than • Less Than • Less Than or Equal • Greater Than or Equal • Not Equal To • Contains • Does not Contain • Excludes • Includes • Starts With • Does not Start With • Ends With • Does not End With
Value	The value range corresponding to the field selected for creating recording rules.

Related links

Creating recording rules on page 85

Recording Targets overview

Recording Targets is a setting that you can use to define recording settings based on stations and not on agents. The stations can be based on extension, position ID, and dummy port for extension based recording. This feature is suitable for a free seating environment where agents take calls on different extensions. You can configure stations only within the available recording license limit.

You can choose to define a station range or comma separated values for the configuration. However, even when a range is defined, the system builds out all the extensions or stations in the range. After an extension is configured and saved, the information is displayed on the employee profile page. For dummy profiles, the system displays a standard default name against the extension. You can define only voice recording options and not screen recording options. For every definition, the following details are specified: site, department, role, and optional line instance. Whenever any value is entered, the change applies to all the stations in the range.

However, device ID is not a part of the extension definition because this field is specific to each phone or device.

For editing the extensions in bulk, use the bulk action feature from the employee management screen. Using this functionality, you can search, edit, or delete any existing stations. When there is an overlap of extensions, you cannot create new ones that are already enabled, you can only edit to redefine the recording settings.

Configuring Recording Targets

Procedure

1. Click **Administration** > **Settings** > **Recording Targets**.
2. Enter the appropriate details in the respective fields.
3. Click **Save**.

   The system displays the success or failure of the request. The creation of the recording profile is subjected to license availability.
4. **(Optional)** To know the status of the recording profiles, click **Previous Configurations**.

   If a configuration fails, you can download the details from the Failed Configurations column to know the reason for the failure.

Related links

Recording Targets field descriptions on page 89

Recording Targets field descriptions

Name	Description
ID Type	The type of station. The options are: • Extension: The phone extension of the employee. • Port: The dummy recording stations used to record calls in Avaya Session Border Controller for Enterprise deployments for calls that are routed through IVRs. You must configure this port number range in SIP adapter, where Avaya Session Border Controller for Enterprise is enabled.

Table continues…

Name	Description
	• Position ID: The ID which the agent uses to log in to the phone. This field is available for Avaya Communication Server 1000 deployments.
ID Value	The option to enter the relevant values based on the selected ID Type.
DP OU Type	The data partition organization unit that is configured while logging in to the application for the first time.
Contact Instance	The number of simultaneous transactions that can be handled by a station or extension. For example, a user configures two extensions: 1001 and 1002. The user must enter 2 (numeric value) in the contact instances field, then each station can at any instance handle maximum two transactions.
Site	The name of the site that the employee belongs to. The site is same as the location defined at the organization level.
Department	The name of the department that the employee belongs to.
Role	The designation of the employee in the organization.
Groups Belong to	The name of the group that the employee belongs to.

Interactions Recording Options

Name	Description
Recording General Rules	
Monitor and Record All Interactions	The option to allow users to monitor and record all the interactions.
Do Not Record Interactions	The option to restrict users from recording interactions.
Monitor and Record Complete Interactions On demand	The option where you cannot record on demand interactions.
Monitor and Record Segment of Interactions On demand	The option to records only parts of on demand interactions.

Button Name	Description
Previous Configurations	The option to view the status of the recording profiles. When you click on the Download link in the Failed Configurations column, the system displays the station that failed to get created with the details of the reason for failure.

Previous Configurations

Name	Description
ID Type	The type of station.
ID Value	The relevant values based on the selected ID Type.
Interactions Recording Options	The option to enable recording rules for interactions.
Status	The status of the records. The options are: • New • Completed • Processing
Failed Configurations	The number of the records that failed. Each failed configuration contains of a download link. You can download this file in excel or csv format to know has failed with the reason for failure. For the rest of the configurations the download link is disabled.
Created By	The name of the user who created the records.
Created on	The date and time when the records are created in the mm/dd/yyyy hr:mm:ss format.

Related links

Configuring Recording Targets on page 89

Recording Filters overview

Avaya Workforce Optimization Select supports recording of interactions that are routed to Vector Directory Number (VDNs) and Hunt Groups. A VDN is an extension on an ACD that directs an incoming interaction to a vector. Call vectoring is the process of defining vector programs that determine how a specific call must be routed and what call treatment that call is given. Using vectors, which are a series of user-defined commands, you can direct or route internal and network calls as desired in your contact center and determine how these calls are processed. A Hunt Group refers to a group of extensions that are organized to process specific calls and direct them to a particular group of agents.

Use Recording Filters to define recording settings for Vector Directory Numbers (VDNs) and Hunt Groups. You can specify:

- VDNs for which you want Avaya Workforce Optimization Select to monitor interaction events.
- A list of VDNs or Hunt Groups that must to be recorded.
- A list of VDNs or Hunt Groups that need not be recorded.

- If interactions without any VDN or Hunt Group associations must be recorded or not.

Note:

For VDN based recording, ensure that you configure the following:

- Stations as part of dummy agent profiles for outbound calls.
- Agent IDs as part of agent profiles for inbound calls. No calls are recorded if there are no agent profiles configured.
- Hunt group extensions in AES adapter to send agent information to the Recorder.

Configuring recording filters

Before you begin

Get the required permissions to manage recording filters.

Procedure

1. Click **Administration** > **Settings** > **Recording Filters**.
2. On the Recording Type Configuration page, enter the required fields.
3. Click **Save**.
4. To view the details of the previous recording filters, click **Previous Configurations**.

Related links

Recording Filters field descriptions on page 92

Recording Filters field descriptions

Name	Description
Filter Type	The option to configure the recording filter type. The options are: • VDN • Hunt Group
Monitoring The Monitoring section is available when you select the VDN option.	
Monitor events for	The option to define if you want to monitor interactions events for stations or VDNs.

Table continues…

Name	Description
	The options are: • Stations • VDN: With this option, you can enter the values to be monitored.
VDNs to be monitored	The option to enter the list of VDNs to be monitored for events. You can enter comma separated values. Avaya Workforce Optimization Select will not record interactions routed through VDNs that are not specified in this list.
Recording Filters	
Values to be recorded	The option to enter VDNs or Hunt Groups that you want to record. You can enter comma separated values. Interactions routed through the list of VDNs and Hunt Groups specified in this option are recorded.
Values not to be recorded	The option to enter VDNs or Hunt Groups that you do not want to record. You can enter comma separated values. Interactions routed through the list of VDNs and Hunt Groups specified in this option are not recorded.
Record Interactions with blank values	The option to define if interactions without any filter type association must be recorded or not. The options are: • Yes: Interactions that do not have any VDN or Hunt Group association are recorded. • No: Interactions that do not have any VDN or Hunt Group association are not recorded.
Interaction Association	The option to associate the interaction with the first VDN or Hunt Group.
Notes	The option to add optional notes for future reference.

Button	Description
Previous Configurations	To view the details of the previous recording configurations. This option is important to maintain a history of the filter types. For example, if a user selects the filter type as VDN and later selects Hunt Group, then the records for VDN are still available.

Related links

Configuring recording filters on page 92

Configuring LDAP settings

Before you begin

- When you make any updates to the LDAP settings, ensure that you restart the web application for the changes to take effect.
- For Avaya Workforce Optimization Select to read and upload data, the ADS directory must contain a user without any account options assigned. If such a user does not already exist, you must create one.

Procedure

1. Click **Administration** > **Settings** > **LDAP Settings**.
2. On the LDAP Settings page, enter the appropriate details in the fields.
3. To test the connection to the base provider URL, click **Validate Connection**.

   The system displays the parameters for mapping users to the LDAP directory.
4. Select the appropriate details in the Password Policy section.
5. Enter the appropriate details in the User section.
6. Select the LDAP to Avaya Workforce Optimization Select user mappings that you want to import from the User Mapping drop-down menus.
7. Select all the user mapping criteria you want to map for import, and then click **Test LDAP Users**.
8. Select **Schedule** to define when and how often you want Avaya Workforce Optimization Select to import and sync the LDAP database and directory file with Avaya Workforce Optimization Select .
9. Click one of the following:
   - **Save**: To save your changes.
   - **Save & Import**: To import the selected LDAP directory file information (either ADS or manual) into Avaya Workforce Optimization Select .

Related links

LDAP Settings field descriptions on page 94

LDAP Settings field descriptions

Name	Description
Domain	The name given to an LDAP setting after it is configured with any name or domain address.

Table continues…

Name	Description
	If Authentication Mode is set to Blended in the general settings, then the authentication type options for managing employee profile available are Local and LDAP for the configured domain name.
Base Provider URL	The URL of the server hosting the LDAP directory.
Base DN	The Distinguished Name (DN) of the base provider directory root.
Principal	The DN of the LDAP user that is used to connect to the LDAP server. Note that the directory must contain a user without any account options assigned. If such a user does not already exist, you must create one.
Credentials	The password for the principal.

Password policy

Name	Description
Use LDAP Authentication	The option to set LDAP authentication as required. Based on this option, the application will not allow a user to log in unless he or she can successfully bind to the LDAP directory first. If you do not enable this option, the application allows users to have an account in Avaya Workforce Optimization Select but no LDAP accounts to log in to the portal.
Sync user data post authentication	The option to synchronize user data each time the user logs in.
Enable Subdomain	The option to select multiple domains or sub domains when an organization has multiple domains set up in the organization.

Employee Mapping

Name	Description
Authentication Search Filter	The default AD admin name which is the sAMAccountName.
Import Search Filter	The desired hierarchical level of users you want to import as they appear in the AD database.
Distinguished path	The criteria with the prefixes followed by company specifically. For example, DC= company name as in DC= ABCbank.
Organization Unit	The criteria with the prefixes followed by department/organization unit specifically. For example, OU= department name or OU= Administration.
Site	The site that the employee belongs to.
Employee code	The employee code of the employee.
First Name	The first name of the employee.
Last name	The last name of the employee.
Hire Date	The date when the employee joined the organization.
Email	The email address of the employee.
User Name	The user name of the employee.

Table continues…

Name	Description
Department	The department that the employee belongs to.
Role	The designation or job title that the employee belongs to.
Reporting to	The role that the employee reports to.
Extension	The VoIP phone extension of the employee.
Last updated date	The date when the synchronization was last completed.
Custom Group	The groups that the employee belongs to.
DP OU Type	The OU type created post installation. The name of the OU type created post installation to partition and secure data across groups appears as the name of this field.

Schedule

A schedule is based on general settings time zone.

Name	Description
Time	The time when you want Avaya Workforce Optimization Select to import and sync the LDAP database and the directory file with Avaya Workforce Optimization Select.
Begin schedule on	The date when you want Avaya Workforce Optimization Select to import and sync the LDAP database and the directory file with Avaya Workforce Optimization Select .

Related links

Configuring LDAP settings on page 94

Password policy

Administrators can use password policy to define a set of rules that enhance system security by encouraging employees to use strong passwords.

Administrators can configure the following:

- Password with syntax
- Password history
- Password expiration and lockout

Configuring the password policy

Procedure

1. Click **Administration** > **Settings** > **Password Policy**.

2. Enter the appropriate information in the fields.
3. Click **Save**.

Related links

Password Policy field descriptions on page 97

Password Policy field descriptions

General

Name	Description
Policy Name	The name of the password policy. By default, the name is Password Policy and you cannot edit the name.
Description	The description to specify the options that you can enable for the password policy. By default, the description is Default password policy. You can edit the description. You can enter up to 500 characters in this field.
Changeable	The option to allow users to change their password at any given time. By default, this option is enabled.
Change Required	The option to make it mandatory for users to change their password upon first login. By default, this option is enabled.
Active	The option to activate the password policy. By default, this option is enabled. **Note:** If you deactivate the password policy, users can still access the application with the existing credentials.

Syntax Checking

Name	Description
Enable Syntax Check	The option to enable syntax rules for passwords.
Syntax	The types of passwords that you can use. The options are: • **Alpha only**: To strictly define an alphabetical password. By default, **Alpha only** is selected. • **Numeric only**: To strictly define a numeric password. • **Alpha and Numeric**: To define a password that includes at least one alphabetical and one numeric character. • **Alpha, Numeric and Special**: To define a password that includes at least one alphabetical, one numeric and one special character.

Table continues…

Name	Description
	This field is mandatory.
Minimum Length (characters)	The minimum required character length of the password, alpha or numeric. The default value is 6. The maximum length you can define for a password is 30 characters. However, you can enter a maximum of 2 digits in this field to specify the length of the password. This field is mandatory.
Enable Sequence characters check	The option to enable syntax rules for passwords with sequence characters.
Enable Repeat characters check	The option to enable syntax rules for passwords with repeat characters.

Password History

Name	Description
Enable Password History	The option to enable and enforce that an old password can be reused only after a certain number of unique passwords.
History Count	The number of unique passwords required before reuse of an old password. This field is mandatory.

Password Expiration/Lockout

Name	Description
Enable Expiration/Lockout	The option to enable password expiration and lockout settings.
Expiration	The option to configure expiration details for the password. The options are: • **Validity (weeks)**: The number of weeks that the user password remains valid. The maximum characters allowed in this field are 2 digits. • **Warning Time (days)**: The number of days in advance that users are prompted to change their password. The default value is 1. The maximum characters allowed in this field are 2 digits. ✱ **Note:** Users who have an account in the application receive an alert n number of days in advance before the password expires. Users can view the alert in their inbox. • **Grace Period (days)**: The number of days past the expiration date that the password remains valid.

Table continues…

Name	Description
	The default value is 0. The maximum characters allowed in this field are 2 digits. **Note:** Users who have an account in the application receive an alert n number of days after the user's password expires. If the Grace Time is 2 days, users receive this alert once a day for two days after the password expires. Users can view the alert in their inbox. This field is mandatory.
Lockout	The option to configure failed login attempts for users. The options are: • **Maximum Failure Attempts**: The number of invalid login attempts that a user can make before being locked out. The maximum characters allowed in this field are 2 digits. • **Reset Failure Count (mins)**: The duration to specify when the **Maximum Failure Attempts** field will be reset to zero after the user successfully logs on to the application. The default value is 60. The maximum characters allowed in this field are 2 digits. • **Lockout Duration**: The number of days to lock the user account after the user reaches the maximum failed attempts. You can also specify the lockout duration to **Until Unlock By Administrator**. This option is set by default. You can unlock the account using the **Release Lock** option in the employee Profile section. This field is mandatory.

Related links

Configuring the password policy on page 96

Chapter 9: Managing groups

Groups overview

Using groups, administrators can create heterogeneous groups of employees. You can associate employees with groups formed out of different operations and business processes within the organization.

When you create groups, you can search for employees based on the following criteria:

- Name
- Email
- Site
- User Name
- Extension
- Reporting to
- Role
- Department
- Organization Unit

You can also add employees to multiple groups and define the groups to which employees belong and have access to.

Creating groups

Procedure

1. Click **Administration** > **Groups**.
2. Click **Add Group**.
3. On the Add New Group page, enter the appropriate information in the fields.
4. Click **Save & Close**.

Groups field descriptions

Name	Description
Name	The name of the group.
Active	The option to indicate whether the group is an active group. This option is enabled by default.
Description	The description of the group.
Search By	The option you can use to filter employees by: • **Employee Name** • **Organization Unit** • **Department** • **Role** • **Email** • **Alias** • **Code** • **Site** • **User Name** • **Reporting to** • **Extension** • **Tenure (in weeks)**
Looking for	The values that filter the **Search By** option.
Available Employee(s)	The available employee list that is populated based on what you select in the **Search By** option.
Assigned Employee(s)	The employees that you assign to the group. You can move employees from the **Available Employee(s)** list to the **Assigned Employee(s)** list and vice versa.

Chapter 10: Managing security

Security in Avaya Workforce Optimization Select

You can manage security in Avaya Workforce Optimization Select by configuring the following:

- Password Policy: Define a set of rules that enhance system security by encouraging employees to use strong passwords. For more information, see Configuring Password Policy on page 96.
- Privileges: Define what a user can or cannot access in Avaya Workforce Optimization Select. For more information, see Assigning Privileges on page 41.
- Self-signed (SSL) certificates: Manage the deployment and configuration of SSL certificates manually to ensure secured communication among the different elements of Avaya Workforce Optimization Select. For more information, see Certificate management on page 102.

Certificate management overview

In Avaya Workforce Optimization Select, the installer program installs the SSL certificate. The system administrator then manages the certificate deployment manually and replaces the SSL certificate to ensure secured communication among the different elements of Avaya Workforce Optimization Select.

The SSL certificates are deployed and configured at the Apache service level. The two Apache instances where SSL certificates are configured are:

- Front End Apache Instance: The Apache instance where the SSL certificate is configured for a secured TLS connection between the client web browser and Apache reverse proxy server.
- Unified Messaging Apache Instance: The Apache instance where the SSL certificate is configured for a secured TLS connection between the internal components of the Avaya Workforce Optimization Select application to the Unified Messaging Apache reverse proxy server.

The following are the identity certificates that exist on Avaya Workforce Optimization Select:

Service name	Description	Protocol	Port	Support for 2048 key length and SHA2 signature
AWFOSWebProxy	Secure the connection from the client browser to the Apache proxy server.	HTTPS	443	Yes
AWFOSWSProxy	Secure the connection from the Avaya Workforce Optimization Select internal components to the Unified Messaging server.	HTTPS	8443	Yes

Replacing self-signed certificates with identity certificate

Getting a new SSL identity certificate from the third-party CA

Before you begin

Ensure that each far end entity contains a new root certification authority (CA) certificate in its trusted list.

Procedure

1. Generate the Certificate Signing Request (CSR) for an Apache server using Open SSL.

   Ensure that the CSR that is generated contains the subject alternative name containing the Avaya Workforce Optimization Select FQDN and IP address or only Avaya Workforce Optimization Select FQDN.
2. Save your server key file at a secured place for using while configuring in Apache.
3. Send the CSR to the third-party certificate signing authority.
4. Get the signed certificate from CA in the `.crt` format.
5. Rename the signed certificate to one of the following:
   - For front-end Apache, `server.crt`
   - For Unified Messaging Apache, `awfos_ssl.crt`
6. Rename the key file to one of the following:
   - For front-end Apache, `server.key`
   - For Unified Messaging Apache, `awfos_ssl.key`

Next steps

Deploy the trusted certificate to the front-end Apache and the Unified Messaging Apache instances.

Related links

Certificate management overview on page 102

Deploying the trusted signed certificate

Before you begin

Get the SSL certificate from the third-party CA for both front-end Apache and Unified Messaging Apache instances.

Procedure

1. Log into the Avaya Workforce Optimization Select server as a system administrator.
2. Stop the Avaya Workforce Optimization Select Apache services from the Windows Service Manager.
3. **(Optional)** For front-end Apache, in the Avaya Workforce Optimization Select installation directory, do the following:
    a. In the `AWFOS_INSTALL_DIR/Apache24/conf/ssl.crt/` folder, replace the existing `server.crt` file with the new `server.crt` file.

    b. In the `AWFOS_INSTALL_DIR/Apache24 /conf/ssl.key/` folder and replace the existing `server.key` file with the new `server.key` file.
4. **(Optional)** For Unified Messaging Apache instance, in the Avaya Workforce Optimization Select installation directory, do the following:
    a. In the `AWFOS_INSTALL_DIR/Apache24_WS/conf/ssl.crt/` folder and replace the existing `awfos_ssl.crt` file with the new `awfos_ssl.crt` file.

    b. In the `AWFOS_INSTALL_DIR/Apache24_WS/conf/ssl.key/` folder and replace the existing `awfos_ssl.key` file with the new `awfos_ssl.key` file.

Next steps

Start both the Avaya Workforce Optimization Select Apache services from Windows Service Manager.

Related links

Certificate management overview on page 102

Chapter 11: Troubleshooting

Records do not display in Interactions or View Evaluations

Condition

A user logged in to Avaya Workforce Optimization Select cannot view any records in the Interactions module or in the View Evaluations tab.

Cause

The user access is defined incorrectly on the Edit Employee Access page of the Administration module.

Solution

1. Click **Administration** > **Employees**.
2. On the Employees page, click the row for the employee who has raised the ticket for this issue.
3. In the left column, click **Employee Access**.

   The system displays the Edit Employee Access page.
4. Check the following:
   - The employee is assigned to the correct group in Assigned Group(s) in the Group Access to section.
   - The employee is assigned to the correct organization unit in Assigned Organization Unit(s) in the Organization Units section.
5. **(Optional)** If employee access is not defined correctly, see: Providing employee access on page 48.

TLS connection failed

Condition

The TLS connection is not working. When you open the `Apache24 log ssl log` file located at `AWFOS_INSTALL_DIR/Apache24/logs/ssl_443_error`, the TLS Alert displays one of the following messages:

- `The certificate has expired.`

- The identity certificate is not trusted or the CA (certification authority) is unknown.
- The certificate is not supported.
- Certificate is not yet valid.

Cause

The TLS connection might fail due to an error in the identity certificate from a certification authority (CA).

Solution 1

Complete the tasks that corresponds to the log files error message:

a. For `The certificate has expired.`, see Troubleshooting error1 on page 106.

b. For `The identity certificate is not trusted or the CA (certification authority) is unknown.`, see Troubleshooting error2 on page 106.

c. For `The certificate is not supported.`, see Troubleshooting error3 on page 107.

d. For `Certificate is not yet valid.`, see Troubleshooting error4 on page 107.

The certificate has expired

Condition

TLS connection fails. When you open the `Apache24 log ssl log` file located at `AWFOS_INSTALL_DIR/Apache24/logs/ssl_443_error`, the TLS Alert displays the message: `The certificate has expired.`

Solution

Replace the identity certificate using the following steps:

a. Get a new SSL certificate. See: Getting a new SSL identity certificate from the third-party CA on page 103.

b. Deploy the certificate. See Deploying the trusted signed certificate on page 104.

The identity certificate is not trusted or the CA (certification authority) is unknown

Condition

TLS connection fails. When you open the `Apache24 log ssl log` file located at `AWFOS_INSTALL_DIR/Apache24/logs/ssl_443_error`, the TLS Alert displays the message: `The identity certificate is not trusted or the CA (certification authority) is unknown.`

Solution

Depending on the organization policy, do one of the following:

a. Contact someone in authority to confirm if the certificates were procured from a trusted CA.

b. Import the certificate to the trusted certificate zone.

Unsupported Certificate

Condition

TLS connection fails. When you open the `Apache24 log ssl log` file located at `AWFOS_INSTALL_DIR/Apache24/logs/ssl_443_error`, the TLS Alert displays the message: `Unsupported Certificate`.

Cause

The SSL certificates were not generated correctly.

Solution

Replace the identity certificate using the following steps:

a. Get a new SSL certificate. See: Getting a new SSL identity certificate from the third-party CA on page 103.

b. Deploy the certificate. See Deploying the trusted signed certificate on page 104.

Certificate not yet valid

Condition

TLS connection fails. When you open the `Apache24 log ssl log` file located at `AWFOS_INSTALL_DIR/Apache24/logs/ssl_443_error`, the TLS Alert displays the message: `Certificate not yet valid.`

Cause

A newly generated Identity Certificate with current **Valid From Date/Time** might not be valid for the peer device validating it.

Solution

Install a certificate on the server on the date from which the certificates are valid. You must never install a certificate whose **Valid From Date/Time** is in a future date.

Apache server does not start

Condition

The Apache server does not start. When you open the log files from `INSTALL_DIR\AWFOS5\Apache24\logs`, the files display one of the following errors:

- `Unable to configure RSA server private key`
- `Certificate routines:X509_check_private_key:key values mismatch`
- `Invalid command SSLEngine Error`
- `Untrusted and Missing Intermediate Certificate Errors`
- `SSL received a record that exceeded the maximum permissible length, ssl_error_rx_record_too_long`

Cause

The Apache server does not start due to SSL-related errors.

Complete the task corresponding to the log files error message:

a. For `Unable to configure RSA server private key` or `Certificate routines:X509_check_private_key:key values mismatch`, see Troubleshooting error 1 on page 108.

b. For `Invalid command SSLEngine Error`, see Troubleshooting error 2 on page 109.

c. For `Untrusted and Missing Intermediate Certificate Errors`, see Troubleshooting error 3 on page 109.

d. For `SSL received a record that exceeded the maximum permissible length, ssl_error_rx_record_too_long`, see Troubleshooting error 4 on page 110.

Unable to configure RSA server private key or Certificate routines:X509_check_private_key:key values mismatch

Condition

When the Apache server does not start and you open the log files from `INSTALL_DIR\AWFOS5\Apache24\logs`,the files display one of the following errors:

- `Unable to configure RSA server private key`
- `Certificate routines:X509_check_private_key:key values mismatch`

Cause

The Apache server does not start due to SSL-related errors.

Solution

1. Do the following to check whether the two files match :

   a. In `server.crt`, run **`openssl x509 -noout -modulus.`**

b. In `server.key`, run **`openssl md5openssl rsa -noout -modulus`**.

2. **(Optional)** If the modules do not match, do one of the following:

   - Find the `.key` file matching your `.crt` file and update the VirtualHost in your `httpd-ssl.conf` file.
   - Reissue your certificate by generating two new files with the OpenSSL CSR Wizard. You can also create a new CSR from your existing private key file using the following command: **`openssl req -new -key server.key -out server.csr`**.

     The existing private key must be at least 2048 bits. If the key is less than 2048 bits, recreate the key.

Invalid command SSLEngine Error

Condition

When Apache server does not start and you open the log files from `INSTALL_DIR\AWFOS5\Apache24\logs` the files display the following error: `Invalid command SSLEngine Error`

Cause

The Apache server does not start due to SSL-related errors.

Solution

1. Install the `mod_ssl` module.
2. Enable the `mod_ssl` module from the `httpd.conf` file if the module is already installed.

Untrusted and Missing Intermediate Certificate Errors

Condition

When Apache server does not start and you open the log files from `INSTALL_DIR\AWFOS5\Apache24\logs` the files display the following error: `Untrusted and Missing Intermediate Certificate Errors`

Cause

The Apache server does not start due to SSL-related errors.

Solution

1. Remove the comment from the VirtualHost section of the `httpd-ssl.conf` file for `SSLCertificateChainFile`.
2. Check whether the `SSLCertificateChain` file points to the intermediate CA certificate.

SSL received a record that exceeded the maximum permissible length, ssl_error_rx_record_too_long

Condition

When Apache server does not start and you open the log files from `INSTALL_DIR\AWFOS5\Apache24\logs` the files display the following error: `SSL received a record that exceeded the maximum permissible length, ssl_error_rx_record_too_long`

Cause

The Apache server does not start due to SSL-related errors.

Solution

1. Remove # from `#Include conf/extra/httpd-ssl.conf` in the `httpd.conf` file and restart the Apache server.

   The system loads the `httpd.conf` file.

2. In the `httpd.conf` file, before the *VirtualHost* block is loaded, add: `Listen 443`.

   - For IPv6, add : `Listen 192.168.0.1:443`.
   - For https on a non-standard port, add : `Listen 192.168.0.1:8443 https`

3. For running Apache under Windows, set up the host file on the Windows server at `C:\Windows\System32\Drivers\etc\hosts`.

4. Check if the *VirtualHost* block Apache is configured to use SSL with the SSLEngine directive as follows:

   ```
   VirtualHost your.domain.com:443
   SSLEngine On
   [rest of VirtualHost]
   </VirtualHost>
   ```

5. To test for a misconfigured proxy that is stopping an SSL configuration on port 443, connect to the site from outside your network with different web browsers.

   If you do not receive an error, then the proxy is misconfigured.

Chapter 12: 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 with Avaya Aura® Communication Manager and Avaya Aura® Call Center Elite	Provides checklist and procedures for the installation, configuration, initial administration, and basic maintenance of Avaya Workforce Optimization Select with Avaya Aura® Communication Manager and Avaya Aura® Call Center Elite.	Deployment engineers and support personnel
	Deploying Avaya Workforce Optimization Select with IP Office and IP Office Contact Center	Provides checklist and procedures for the installation, configuration, initial administration, and basic maintenance of Avaya Workforce Optimization Select with IP Office and IP Office Contact Center.	Deployment engineers and support personnel
	Deploying Avaya Workforce Optimization Select with IP Office and Avaya Contact Center Select	Provides checklist and procedures for the installation, configuration, initial administration, and basic maintenance of Avaya Workforce Optimization Select with IP Office and Avaya Contact Center Select.	Deployment engineers and support personnel
	Deploying Avaya Workforce Optimization Select with Avaya Aura® Communication Manager and Avaya Oceana™ Solution	Provides checklist and procedures for the installation, configuration, initial administration, and basic maintenance of Avaya Workforce Optimization Select with Avaya	Deployment engineers and support personnel

Table continues…

Document number	Title	Use this document to:	Audience
		Aura® Communication Manager and Avaya Oceana™ Solution.	
	Deploying Avaya Workforce Optimization Select with Avaya Communication Server 1000 and Avaya Aura® Contact Center	Provides checklist and procedures for the installation, configuration, initial administration, and basic maintenance of Avaya Workforce Optimization Select with Avaya Communication Server 1000 and Avaya Aura® Contact Center.	Deployment engineers and support personnel
	Deploying Avaya Workforce Optimization Select with Avaya Aura® Communication Manager and Avaya Aura® Contact Center	Provides checklist and procedures for the installation, configuration, initial administration, and basic maintenance of Avaya Workforce Optimization Select with Avaya Aura® Communication Manager and Avaya Aura® Contact Center.	Deployment engineers and support personnel
Administering			
	Administering SysAdmin	Provides information on how to perform administration tasks in the SysAdmin application including how to manage tenants, assets, component configuration, and diagnostics.	System administrators
	Avaya Workforce Optimization Select Quick Reference Guide for Administrators	Understand the most common user tasks that an Administrator performs.	Application 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
	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

Table continues…

Document number	Title	Use this document to:	Audience
	Avaya Workforce Optimization Select Quick Reference Guide for QA Analyst	Understand the most common user tasks that a QA Analyst performs.	Users
	Using Desktop Monitor	Explain how to use Desktop Monitor. Supervisors can use this document to create and assign projects to employees in a contact center environment. Employees can use the document to monitor the projects assigned to each employee.	Users

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

  Note:

  Videos are not available for all products.

Support

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

Index