Administering Avaya Workforce Optimization Select

Release 5.0
Issue 1
May 2016

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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 a 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 IF YOU PURCHASE A 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. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

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

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

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

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

Virtualization

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

Third Party Components

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

The following applies 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

Customer acknowledges and agrees that it is responsible 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

Contents

Chapter 1: Introduction

Purpose

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

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

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 flexible and 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.

Benefits of Avaya Workforce Optimization Select

You can use Avaya Workforce Optimization Select for:

- Capturing and reviewing interactions, emails, and chat sessions in a secure, service-oriented enterprise portal.
- Reducing operating expenses and liability risks using analytically oriented advanced reporting and real-time dashboards.
- Providing all stakeholders access to valuable analytics through any device.
- Enabling the management to identify and address customer and operational issues and opportunities in a timely fashion.
- Adhering to Payment Card Industry (PCI) compliance including encryption, watermarking, masking, multilayer password protection, and audit trails.
- Improving revenue generation by identifying up-sell and cross-sell opportunities.

Administration checklist

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

No.	Task	Reference	Notes	✔
1	Configure rules for password policy that enhance system security.	Configuring the password policy on page 14		
2	Create sites, organization units, departments, and roles that mirror the organizational structure of your company.	Adding sites on page 19 Adding organization units on page 20 Adding departments on page 22 Adding roles on page 24		
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 voice 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 voice settings on page 30		
5	Define employee access based on different operations within the organization.	Providing employee access on page 32		
6	Configure feature privileges and report privileges to define what an employee can or cannot access in the application.	Assigning privileges on page 34 Assigning report privileges on page 39		
7	Import employees in bulk using an Excel spreadsheet.	Importing employees on page 41		
8	Update employee profile, privileges, and voice settings in bulk.	Performing bulk actions on page 42		
9	Add queues and configure threshold values for alerts.	Adding queues on page 43		
10	Create groups of employees for specific business cases if required.	Creating groups on page 46		
11	Create recording rules to decide what interactions must be recorded at a global level.	Creating recording rules on page 49		

Table continues…

No.	Task	Reference	Notes	✔
12	Configure general settings like time zone, language, consent based recording, and screen capture settings that apply globally to all employees.	Configuring general settings on page 47		
13	Configure settings for windows active directory services to synchronize employee data.	Configuring LDAP settings on page 53		
14	Manage and configure storage rules for archiving, compressing, moving, copying, and purging or deleting voice files and screens.	Managing storage devices on page 57 Creating storage manager rules on page 59		

Administrator responsibilities

- Determine whether to import users 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.

Chapter 3: Management tools

Avaya Workforce Optimization Select administration overview

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

Logging on to Avaya Workforce Optimization Select

Procedure

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

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

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

   You can now log in to the Avaya Workforce Optimization Select application.
3. Enter your user name and password.
4. Click **Sign in**

   The Avaya Workforce Optimization Select home page appears.

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.

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 that you have access to.

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

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

About this task

Use this procedure to set system-level rules for the login credentials of all users.

Note:

If you use LDAP authentication, your LDAP settings will override your password policy configuration.

Procedure

1. Click **Administration** > **Settings** > **Password Policy**.
2. Enter the appropriate information in the fields.
3. Click **Save**.

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. 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.

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.

Table continues…

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>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.

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.</td></tr>
<tr><td>Lockout</td><td>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.</td></tr>
</table>

Chapter 4: Avaya Workforce Optimization Select management

Organization

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

About this task

Use organization profile to view the following details in read-only mode:

- Important information regarding licenses and storage of the organization.
- Details of the organization.

The information on the organization profile page is populated from Sys Admin.

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.

Table continues…

Name	Description
	• **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

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

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. 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

About this task

Use OU types to group organization units into a category. OU types are major groupings to which the organization units (OU) will belong. The OU and OU type association is mandatory and created to support data partitioning across selected OUs.

You can modify OU types that you create but cannot modify those created as data partition entities during installation.

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

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

About this task

Use departments to group employees within your organization.

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

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

About this task

Use roles to:

- Create designations or roles for users.
- Assign privileges and report privileges to a role. Users belonging to the role inherit the privileges automatically.

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**. 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

Table continues…

Name	Description
	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, comment, download, and email interactions. • **Live Monitoring**: Defines permissions to monitor live interactions. • **Evaluate**: Defines permissions to access and manage features within the Evaluate module. • **Coach**: Defines permissions to access and manage features within the Coach module. • **Learn**: Defines permissions to access and manage features within the Learn module. • **Reporting**: Defines permissions to manage reporting settings and results. • **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. • **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 Voice Configuration, User Access, and Web Usage Audit reports.
Custom Fields	The option to select an additional custom fields for a role.

Adding custom fields

About this task

Use custom fields across the Administration module to specify additional properties for sites, organization units, departments, roles, and queues. For example, you might want to add or apply additional properties such as zone, area or region across all sites, organization units, and queues.

Using custom fields, you can define your search criteria and generate reports.

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	The name of the custom field that you want to add. You can add up to five custom fields.
List of Values	The values that appear in the drop-down list of a custom field. You can enter multiple values separated by commas.

Employee management

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

Administrators can manage Employees by configuring:

- Employee Profile
- Voice Settings

- Employee Access
- Privileges
- Report Privileges

Employee profile

In Avaya Workforce Optimization Select, you can create profiles for each employee and map employees to sites, organization units, departments, and roles. It is important to configure employee profiles because Avaya Workforce Optimization Select records and stores 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**.

Profile field descriptions

Name	Description
Employee code	The unique code of the employee. You can enter up to 30 characters in this field. The employee code is used in bulk import of employees and in LDAP mapping. This field is mandatory.
First Name	The first name of the employee. You can enter up to 100 characters in this field. The first and last name appears in the list pages of other modules like Live Monitoring, Interactions, Evaluate, Coach, and Reports. This field is mandatory.
Last name	The last name of the employee. You can enter up to 100 characters in this field. The first and last name appears in the list pages of other modules like Live Monitoring, Interactions, Evaluate, Coach, and Reports. This field is mandatory.
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.

Table continues…

Name	Description
	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.
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.
User Name	The unique name of the employee used to login in to the application. The user name must not exceed 30 characters. This field is mandatory.
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.
DP OU Type (created post installation)	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 the field. Every employee must belong to a DP OU.
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.
Upload Image	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 what modules 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.
App Admin	The option to give the employee access to the Administration module. You can control which employees need access to the Administration module. You can view and assign administration permissions to the employee.
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 Canadian** • **Italian** • **Korean** 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** • **Inactive** The default status is Active.
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.

Voice settings

Voice settings is an employee level setting that administrators can use to decide what interactions must be recorded.

Configure Voice settings to:

- Differentiate between any two interactions. Configure options such as **Agent ID**, **Extension**, **Device ID**, **Partition Name**, and **Line Instance** to differentiate between two interactions. The combination of the options you configure must be unique. For agent-based recording, where agents work in shifts, the extension, device ID, and line instance can be the same for multiple agents. In such cases, administrators can use **Partition Name** as the unique identifier to differentiate between two interactions.
- 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.

Configuring voice settings

About this task

To cater to agent based recording and extension based recording, ensure you configure two instances of voice settings for each employee profile. You need to add one instance to specify the agent ID and another to specify the extension of the employee. For CS 1000 deployments, ensure you add one instance to specify the agent ID and another to specify the extension and the position ID of CS 1000.

Procedure

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

   Voice Settings is enabled.

   To support agent and extension based recording, add two instances where you configure **Agent ID**in one instance and **Extension** in another.

Edit Voice Settings field descriptions

General

Name	Description
Employee Name	The first and last name of the employee.
User Name	The unique name used to log in to the application.
Recording Licenses Purchased	The number of recording licenses that the organization purchases.
Recording License Consumed	The number of recording licenses that the organization uses.
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.
Device ID	The MAC (media access control) address of the physical device or phone that the employee uses.
Partition Name	The unique partition name.

Table continues…

Name	Description
	The Partition Name can be any unique name used to differentiate the call, if an employee takes a call from same extension, device, and line instance.
Line Instance	The line instance that is configured for recording. It is the line to which an employee's phone is connected.

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.
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.
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, stop, cancel, mute, unmute recording for specific segments within an interaction.
__ 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.
Monitor and Record randomly __ Interactions	The option to specify the number of interactions to be monitored and recorded.
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.

Table continues…

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

Employee access

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

- Define groups that an employee can belong and have access to.
- 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.

Groups an employee belongs to

Avaya Workforce Optimization Select automatically creates a virtual default group named after the **Reporting to** employee. Every employee automatically belongs to the virtual default group that the employee reports to. These groups are not visible in the application. Administrators can also manually associate employees to other groups.

Groups an employee has access to

When an employee has access to a group, the employee can access the interactions of employees within that group. An employee also gains access to the interactions 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 following buttons are enabled:

- **Voice Settings**
- **Employee Access**
- **Privileges**
- **Report Privileges**

Edit Employee Access field descriptions

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 (created post installation)	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.

Privileges

Administrators can define privileges to control what a user can or cannot get access to. 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.

Privileges are grouped as:

- Interactions
- Live Monitoring
- Evaluate
- Coach
- Learn
- Reporting
- Administration

Assigning Privileges

About this task

Use Privileges to define what an employee can or cannot access in the system.

Note:

A best practice is to assign Privileges to a role so that employees belonging to that role automatically inherit the privileges. Changes you make to the privileges at an employee level will not impact privileges defined for a role.

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 following buttons are enabled:

   - **Voice Settings**
   - **Employee Access**
   - **Privileges**: Use the Edit Privileges page, to select the privileges that you want to enable or disable. You can also directly select **All Feature Privileges** to enable all the privileges at once.
   - **Report Privileges**

Edit Privileges field descriptions

Interactions

Name	Description
Manage Interactions Playback	For the user to playback interactions of employees that the user has access to.
Manage Interaction Tags	For the user to manage tags for live and recorded interactions of employees that the user has access to.
View Comments	For the user to view comments on interactions of employees that the user has access to.
Manage Comments	For the user to view, add, edit, and delete comments on interactions of employees that the user has access to.
Download Interactions	For the user to download the interactions of employees that the user has access to.
Email Interactions	For the user to email the interactions of employees that the user has access to.

Live Monitoring

Name	Description
View Live Monitoring	For the user to view and listen to live interactions of employees that the user has access to.
Record an Interaction on Demand	For the user to record calls on demand.

Table continues…

Name	Description
Manage Feedback	For the user to provide feedback on live interactions to employees that the user has access to.
Random Monitoring	For the user 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)	For the user to monitor the next interaction of selected employee.

Evaluate

Name	Description
View My Assignments	For the user to view interactions that have been assigned to the user for review.
Decline Assignments	For the user to decline interactions that have been assigned to the user for review.
Create & Edit Evaluation(s)	For the user to evaluate an interaction using another evaluation form.
Delete my Evaluation(s) only	For the user to delete evaluations completed by the user.
Delete Evaluation(s)	For the user to delete all evaluations.
View Evaluation(s)	For the user to view completed evaluations.
View Adhoc Evaluations	For the user to view ad hoc evaluation.
View Appeals	For the user to view appeals.
Create & Edit Calibration(s)	For the user to create and edit calibrations by assigning an interaction to multiple evaluators and setting a final score for the interaction.
Delete Calibration(s)	For the user to delete calibrations.
View Employee Coverage	For the user to view employees covered under different evaluation plans.
View QA Coverage	For the user to view ad hoc evaluations and evaluations that are completed by employees under different evaluation plans.
Create & Edit Plan(s)	For the user to create and manage evaluation plans for employees.
Delete Plan(s)	For the user to delete evaluation plans.
Distribution Pool - Self Assignment	For the user to view and assign interactions to the My Assignments page.
Distribution Pool - Manage	For the user to view and assign interactions to reviewers.
Add & Edit Form(s)	For the user to create and manage evaluation forms.
Delete Form(s)	For the user to delete evaluation forms.
Manage Response Sets	For the user to create and manage response sets.
Manage Evaluation Types	For the user to create and manage evaluation types.
View Appeals Workflow	For the user to view appeals workflow.
Manage Appeals Workflow	For the user to manage appeals workflow.

Coach

Name	Description
Create & Edit Coaching Assignments	For a user to assign employes to coachings within a specified period.
Delete Coaching Assignments	For a user to remove coaching assignments.
Manage My Assignment	For a user to view all coachings that the user needs to launch and complete.
Create & Edit Coaching Plans	For the user to create and edit coaching plans for employees.
Delete Coaching Plans	For the user to delete coaching plans.
Manage Parameter	For the user to create and manage parameters that specify the areas of focus that a coaching addresses.

Learn

Name	Description
My Assignment	For the user to view and launch courses and quizzes assigned to the user.
Manage Team Assignment	For the user to view and check the status of courses and quizzes assigned to the team members of the user.
Manage Library	For the user 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.

Reporting

Name	Description
Manage Reporting Results	For the user to view generated reports.
Manage Reporting Settings	For the user to generate and schedule reports. The user can manage only those reports for which the user has permissions.
Manage Reporting Schedules	For the user 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.

Administration

Name	Description
Manage Organization	For the user to view the organization profile and view, add, edit, and delete sites, organization units, departments, and roles.
View Employee Grid	For the user to view the list of employees that the user has access to.
Manage Queues	For the user to: • View, add, edit, and delete queues. • Associate organization units to a queue.

Table continues…

Name	Description
	• Configure thresholds for business rules such as AHT, number of holds, and hold duration.
Manage Groups	For the user to view, add, edit, and delete the groups for the employees that the user has access to.
View Employee Profile — General	For the user to view the profile of the employees that the user has access to.
Manage Employee Profile — General	For the user to view, add, edit, and delete the profile for employees that the user has access to.
View Employee Profile — Voice Settings	For the user to view voice settings of employees that the user has access to.
Manage Employee Profile — Voice Settings	For the user to view, add, edit, and delete voice settings of employees that the user has access to.
View Employee Profile — Access	For the user 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	For the user 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	For the user to view the privileges of employees that the user has access to.
Manage Employee Profile — Privileges	For the user to view, add, edit, and delete the privileges of employees that the user has access to.
View Employee Profile — Report Privileges	For the user to view the report privileges of employees that the user has access to.
Manage Employee Profile — Report Privileges	For the user to view, add, edit, and delete the report privileges of employees that the user has access to.
Bulk Administer Employees	For the user 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	For the user to import the list of employees through an Excel spreadsheet.
View Storage Manager	For the user 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	For the user to archive, copy, delete, move, or purge voice, screen, speech indexed files, and associated metadata XML files for interactions like interaction start time, interaction status, and so on. The user can do these functions remotely or across multiple physical

Table continues…

Name	Description
	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	For the user to view, add, edit, and delete recording rules for employees that the user has access to.
Manage LDAP Settings	For the user 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.
Manage Password Policy	For the user to set system-level password policy rules for users and their login credentials.
Manage General Settings	For the user to view and edit time zone, language, consent-based recording, and screen capture settings for employees that the user has access to.

Report privileges

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 Coach & Quiz Summary report.
- Administration: To generate reports for Employee Voice Configuration, User Access, Web Usage Audit.

Assigning report privileges

About this task

Use report privileges to define the reports an employee can or cannot access in the system.

Note:

A best practice is to assign report privileges to a role so that employees belonging to that role automatically inherit the report privileges. Changes you make to the report privileges at an employee level will not be inherited by the role assigned to the employee.

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 following buttons are enabled:

   - **Voice Settings**
   - **Employee Access**
   - **Privileges**
   - **Report Privileges**: Use the Edit Report Privileges page, to select the report privilege that you want to enable or disable. You can also directly select **All Report Privileges** to enable all the report privileges at once.

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 Voice Configuration	For the user to generate and schedule the Employee Voice 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

About this task

Use this procedure to manually bulk upload employee profiles into Avaya Workforce Optimization Select using an Excel spreadsheet.

An App User can then view only those employees that the App User has access to.

Before you begin

Create groups, sites, departments, and roles.

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**.

Importing 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.
Last name	The last name of the employee. This field is mandatory.
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.
User Name	The login ID or network ID of the employee. This field is mandatory and has to 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.
Extension	The VOIP phone extension of the employee. This value populates the **Extension** field in the Recording Rules page.
Role	The designation of the employee. This field is mandatory.
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.
Client	The name of the DP-enabled client.

Performing bulk actions

About this task

You can perform bulk actions to:

- Update profile information.
- Update privileges and report privileges of employees.
- Update voice settings of employees.

Note:

While it is a best practice to assign privileges to a role, updating privileges for specific employees in bulk will does not affect the privileges assigned to roles. Use this option judiciously because the permissions that you update for employees in bulk take precedence over the permission that are assigned to or updated for a role.

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.
   - **Voice Settings**: Select the appropriate voice settings.
4. Click **Save & Close**.

Queues

In Avaya Workforce Optimization Select, administrators can configure three support channels, namely voice, email, and chat for a queue.

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

About this task

Typically, you do not need to create queues in the application. When a skill call happens, Avaya Workforce Optimization Select automatically creates a queue in real time. The skill ID or the skill group ID is populated as the Queue name and the application automatically assigns a Queue ID to the queue.

Before you begin

Ensure you configure the skill ID parameter in the relevant adapter for the appropriate deployment.

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.
Alias	The alias name of the queue.
Active	The option to select if the queue is an active queue.
Description	The description of the queue.
Organization Units	The organization unit associated with the queue.
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.
Channel	The channel for a queue. The options are: • **Voice** • **Email** • **Chat**
Custom Fields	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 queues	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.

Table continues…

Name	Description
My hold duration by Queue (mins)	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 (mins)	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 (mins) 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.

Custom groups

Groups

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.

Configuring general settings

About this task

Use general settings to configure settings that will apply globally to all employees.

Procedure

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

General Settings field descriptions

Name	Description
Time Zone	The time zone displayed throughout the application. The time zone selected here will be the default time zone in theSites and Profile pages. **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**.
Consent based Recording	The party with whom consent-based recording for interactions is enabled. The options are: • **Agent** • **Customer** • **Dual Party** **Note:** This setting reflects in read-only mode in the employee voice settings.
Week Definition	The unique way that a week is defined in the organization. You can define the days that comprise a week in the organization. For example, Sunday to Saturday. After the week is defined, the same applies across the organization. This field is helpful in scheduling or defining evaluation plans.
Screen Capture	The screen recording properties in the application. The properties defined here will be the default values in the employees voice settings. The user can customize these properties in the Voice Settings page.

Table continues…

Name	Description
	The properties are: • **Screen Recording Interval** (in seconds) • **Screen Recording Quality** (in percentage)

Recording rules

Recording rules is a global setting that administrators use to decide what interactions must be recorded. As opposed to voice 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 offline. For rules processed in real time, the recorder checks the rule definition and accordingly records or purges the interaction. For rules that are processes offline, the storage manager checks the rule definition and records or purges the interaction.

Employees can be part of multiple recording rules. In such cases, the rule priority and the option for agent-level configurations to override the recording rule, defines the precedence.

Using recording rules to:

- Set a priority to each rule to define a sequence. Rules with the lowest priority order take precedence. For example, a rule with priority 1 takes precedence over a rule with priority 2. Recording rule priorities have a range limit from 1 to 99.
- 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 voice 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 voice 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.

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 voice 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. 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 • Department • Extension • Organization Unit • Site

Table continues…

Name	Description
	However, there are rules that are processed offline or not in real time. You can define such rules for the following options: • ANI • DNIS • 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 or storage manager records all interactions that meet the rule definition.
__ 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. 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.

Table continues…

Name	Description
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	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** • **ANI** • **Department** • **DNIS** • **Extension** • **Organization Unit** • **Queue** • **Site**
Operator	The Operator relative to the field selected. The options are: • **Equals** • **Between** • **Greater Than** • **Less Than** • **Less Than or Equal** • **Greater Than or Equal**

Table continues…

Name	Description
	• **Not Equal To** • **Contains** • **Does not Contain** • **Excludes** • **Includes** • **Starts With** • **Ends With**
Value	The value range corresponding to the field selected for creating recording rules.

Chapter 5: Data management

LDAP management

LDAP support

Administrators can use LDAP like the database of Microsoft's Active Directory Services (ADS) to track user names, passwords, and other employee information. You can configure ADS settings to synchronize employee data every time an employee signs in. You can map users in the LDAP database for import into the application.

Avaya Workforce Optimization Select uses Lightweight Directory Access Protocol (LDAP) to access information stored in an information directory. 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.

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 **Test 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.

For example, in the employee management database, Avaya Workforce Optimization Select has a field for VOIP extension. If this field is ipPhone in your LDAP database, select ipPhone from the VOIP Extension drop-down menu. Note that you must select user mappings for Distinguished Path, Network ID, Client, Site, Department, and Designation.

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.

LDAP Settings field descriptions

Name	Description
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.

User

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.

Table continues…

Name	Description
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.
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 (created post installation)	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

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.

Storage management

Data storage

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, or purge 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 devices

From the Manage Storage page, administrators can perform the following tasks:

- Define multiple machines and external drives to specify storage location for interactions.
- Specify the storage location as primary or secondary.
- Assign backup storage destination in case of overcapacity or failure of primary destination.

Storage rules

Administrators can define storage rules to meet specific business requirements for data storage. You can create separate rules for archiving, 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.

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_queuetable 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, copy, move, 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.

Managing storage devices

About this task

Use Manage Storage to:

- Add storage devices such as machines or external drives to define storage for interactions.
- Define storage location as primary and secondary.
- Assign secondary or back-up storage destination during overcapacity or failure of primary destination.

Procedure

1. Click **Administration** > **Settings** > **Storage Manager Rules**.
2. Click **Manage Storage**.

   The system displays the existing storage devices.
3. To add storage devices, click **Add Storage** .
4. On the Add New Storage page, enter the appropriate details in the fields.
5. Click **Save & Close**.

Storage Devices field descriptions

Name	Description
Name	The unique name of the storage destination.
Path	The directory where interactions must be archived. For example, `\\IP address\d$\ArchivedLocation01` which is the physical address of the selected storage location.
Host (IP address/DNS)	The host address of the storage location.

Table continues…

Name	Description
User Name	The user who can access this location.
Password	The password for the user created.
Type	The type of the storage location. The options are: • **Primary** • **Secondary** If you make it a Secondary location, data is stored in the location only when the Primary location fails or is unavailable.
Active	The option to indicate whether the storage device is an active storage device.

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 or compressed.
- 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 Type: 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 Type: 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.

Creating storage manager rules

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 in the fields.
4. Click one of the following:
   - **Save & Close**: To save your settings.
   - **Save & Add Another**: To save the current rule and add another rule.

Storage Manager Rules field descriptions

General

Name	Description
Rule Name	The name of the rule. For example, Archive Rule 01.
Priority	The priority to specify the rule sequence. It is recommended to set priority for storage manager rules from 100. Therefore, a rule with priority 100 will run first, priority 101 will run after the execution of priority 100, priority 103 will run after the execution of 100 and 102, and so on.
Active	The option to indicate whether the storage manager rule is an active rule.

Table continues…

Name	Description
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.

Interaction Selection criteria

Name	Description
Interaction Direction	The interaction direction that the rule must check for before storing. The options are: • **Inbound** • **Outbound** • **Bi-directional**
Field (Specific to **Interaction Direction**)	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, entering 7 will select interactions within the past seven days. • **Older than**: Enter a value for interactions older than the number of days you specify. For example, entering 7 will select all interactions older than or before 7 days. Also select a date to specify a start date for the Older than option.
Field	The options are: • **Called Party** • **Calling Party** • **Commented** • **Groups** • **Custom Transaction Date** • **Duration** • **DNIS** • **Employee** • **Hold Duration** • **No of Holds** • **No of Transfers** • **Organization Unit**

Table continues…

Name	Description
	• **Queue** • **Screen Captures** • **Site** • **Reporting to** • **Tagged** • **Tenure (in weeks)** • **Transaction Date**
Operator	The Operator relative to the field selected. The options are: • **Equals** • **Between** • **Greater Than** • **Less Than** • **Ends With** • **Starts With** • **Not Equal To** • **Contains** • **Does not Contain** • **Less Than or Equal** • **Greater Than or Equal** • **All** • **Active** • **Resigned** • **Terminated**
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 **Between** selected, entering 120 and 300 in the **Value** text fields will execute the action type selected like archive, compress, move, copy, purge/ delete calls between 120 and 300 seconds.

Action Type

Name	Description
Action Type	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. • **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. • **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.
Encrypt	The option to archive or compress interactions in an encrypted format.
Voice Output Format	The option to specify the format in which the interactions must be archived, compressed, moved, copied or deleted. The options are: • **Current Format** • **M4a-Aac-Mono** • **Mp4-H264-Mono** • **Raw-G729-Mono** • **Raw-G729-Stereo** 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 will get archived in Raw-G729-Mono format.
Voice	The option to specify that voice files must be archived, compressed, moved, copied, or purged/ deleted.
Screen	The option to specify that screens must be archived, compressed, moved, copied, or purged/ deleted.

Storage Location

Name	Description
Source	The storage location from where the storage manager picks interactions to archive, move, copy or purge calls.
Primary Destination	The primary location where interactions must be archived or stored.

Table continues…

Name	Description
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.

Chapter 6: 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 14.
- Privileges: Define what a user can or cannot access in Avaya Workforce Optimization Select. For more information, see Assigning Privileges on page 34.

Chapter 7: 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 Workforce Optimization Select application.	All
Implementing			
	Deploying Avaya Workforce Optimization Select	Provide an end-to-end deployment scenario including all products that must function together, checklists, and initial administration.	Deployment engineers and support personnel
Administering			
	Administering Avaya Workforce Optimization Select	Explain how to use Workforce Optimization Interface (WFO) to configure your system, employees, settings, and recording rules and perform routine maintenance tasks. The content is available in two formats: HTML and PDF.	Administrators
Using			
	Using Avaya Workforce Optimization Select	Explain how to use the Workforce Optimization Interface (WFO) to configure settings such as user preferences, monitor and record interactions, and access and generate reports. The content is available in two formats: HTML and PDF.	Users

Table continues…

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

Finding documents on the Avaya Support website

About this task

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

Procedure

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

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

Index

V